IBM Security Guardium V10.1

目次

IBM Security Guardium V10.1

IBM Security Guardium 資料のページにようこそ。このページでは、IBM Guardium のインストール方法、保守方法、使用方法に関する情報を参照することができます。

始めに

製品の概要
製品に関する特記事項
新機能
リリース情報
インストール
アップグレード

共通タスク

機密データのディスカバー
適用状態のモニター
S-TAP 状況のモニター
構成プロファイルの配布
ロールと権限の管理

トラブルシューティングとサポート

Guardium サポート・ホーム
Guardium サポート・リソース
Guardium サポート・ビデオ
Guardium の IBM developerWorks Answers

詳細情報

IBM Security Learning Academy
IBM データ・セキュリティーと保護
IBM developerWorks Guardium コミュニティー
Guardium Tech Talk ビデオ

製品の概要

Guardium® ソリューションの製品およびリリース情報。

- IBM Guardium
  IBM Guardium は、データベース、データウェアハウス、ビッグデータ環境 (Hadoop など) からの情報漏えいを防ぎ、情報の整合性を確保し、異種混合環境全体のコンプライアンス制御を自動化します。
- このリリースの新機能
  新機能、機能、および機能拡張。
- リリース情報
  最新の機能と機能拡張、システム要件、そしてアップグレード、インストール、およびサポート情報について説明します。

IBM Guardium

IBM Guardium は、データベース、データウェアハウス、ビッグデータ環境 (Hadoop など) からの情報漏えいを防ぎ、情報の整合性を確保し、異種混合環境全体のコンプライアンス制御を自動化します。

データベース、ビッグデータ環境、およびファイル・システム内の構造化データおよび非構造化データを脅威から保護し、コンプライアンスを確保します。

構造化データおよび非構造化データのトラフィックを継続してモニターすること、および機密データへのアクセスに関するポリシーを企業規模で実施することができる、拡張が容易なプラットフォームを提供します。

安全な中央監査リポジトリーと統合ワークフロー自動化プラットフォームの組み合わせにより、多種多様な要件に関するコンプライアンス検証アクティビティーが簡素化されます。

IT 管理ソリューションおよびその他のセキュリティー管理ソリューションとの統合を活用して、企業全体に対する包括的なデータ保護を実現します。

これらの目的は、拡張が容易なプラットフォームを使用して、各種のデータベースおよび文書共有インフラストラクチャーを継続してモニターできるようにすること、および機密データへのアクセスに関するポリシーを企業全体に対して実施できるようにすることです。セキュリティーを最大化するよう設計された中央監査リポジトリーと、統合コンプライアンス・ワークフロー自動化アプリケーションの組み合わせにより、製品で多種多様な要件に関するコンプライアンス検証アクティビティーを簡素化できます。

IBM Security Guardium は、重要なデータを保護するように設計されています。 Guardium は、包括的なデータ保護プラットフォームであり、セキュリティー・チームが機密データ環境 (データベース、データウェアハウス、ビッグデータ・プラットフォーム、クラウド環境、ファイル・システムなど) の状況を自動的に分析して、リスクを最低限に抑え、内外の脅威から機密データを保護し、データ・セキュリティーに影響を与える可能性がある IT の変更にシームレスに適合できるようにします。 Guardium は、データ・セ ンターの情報の整合性を確保して、コンプライアンス管理を自動化する上で役立ちます。

IBM Security Guardium ソリューションは、以下に示す 2 つのバージョンで提供されます。

- IBM Security Guardium データベース・アクティビティー・モニター (DAM)
- IBM Security Guardium ファイル・アクティビティー・モニター (FAM): Guardium のファイル・アクティビティーのモニター機能を使用して、ファイル・サーバーに対するモニター機能を拡張します。

IBM Guardium 製品は、データベースやファイルからのデータ漏えいを防止するためのシンプルで堅固なソリューションを提供する製品であり、データ・センターの情報の保全性を確保し、コンプライアンス制御を自動化します。

Guardium 製品の支援により、以下を行うことができます。

- データベースを見つけ出し、そのデータベースに入っている機密情報を検出して分類する処理を自動化できます。
- データベースの脆弱性と構成の問題点を自動的に評価できます。
- 推奨された変更を実装した後に、構成が確実にロックダウンされるようにできます。
- 機密データにかかわるデータベース・トランザクションを詳細なレベルまで可視化できます。
- エンタープライズ・アプリケーションを経由してデータに間接的にアクセスするエンド・ユーザーのアクティビティーを追跡できます。
- 機密データのアクセス、データベースの変更制御、特権ユーザーの操作などに関する多種多様なポリシーを適用し、実施状況をモニターできます。
- 異種混合の多数のシステムやデータベースのための、一元管理型でセキュアな、単一の監査リポジトリーを作成できます。
- レポートの作成と配布、コメントやシグニチャーの取り込みなどに関するコンプライアンス監査プロセス全体を自動化できます。

Guardium ソリューションは、簡単に使用および拡張できるように設計されています。単一のデータベース、または企業各所にある数千の各種データベースに対して構成できます。

このソリューションは、IBM® が提供する事前構成済みアプライアンスとして、またはプラットフォームにインストールされるソフトウェア・アプライアンスとして利用できます。インストール後、オプションの機能をシステムに簡単に追加できます。

Guardium のデータベース・セキュリティー・ソリューションには、以下の主要な機能領域があります。

- 脆弱性評価。データベース製品で既知の脆弱性を検出するだけでなく、複雑なデータベース・インフラストラクチャーの完全な可視性を提供し、構成の誤りを検出するとともに、それらのリスクを評価して緩和します。
- データのディスカバリーと分類。分類だけでは保護は提供されませんが、データの重要性とコンプライアンス要件に基づいて、さまざまなデータに応じた適切なセキュリティー・ポリシーを定義する際の重要な最初のステップとなります。
- データ保護。Guardium は、保存中および転送中のデータ暗号化、静的および動的データ・マスキングなど、データの保全性と機密性を保護するためのテクノロジーに対応します。
- モニターおよび分析。これには、データベースのパフォーマンス特性のモニター、および各インスタンスのすべてのアクセスおよび管理アクションの完全な可視性が含まれます。これに加え、高度なリアルタイム分析、異常検出、および Security Information and Event Management (SIEM) 統合を使用できます。
- 脅威に対する保護。これは、分散型のサービス妨害 (DDoS) や SQL インジェクションなどのサイバー攻撃から保護し、パッチが適用されていない脆弱性を緩和するなど、データベース固有のセキュリティー対策を講じる手法を指します。
- アクセス管理。データベース・インスタンスに対する基本的なアクセス制御を超える機能を提供します。より高度かつ動的なポリシー・ベースのアクセス管理を焦点としたレーティング・プロセスでは、過剰なユーザー特権の識別と削除、共有アカウントとサービス・アカウントの管理、疑わしいユーザー・アクティビティーの検出とブロックに対応できます。
- 監査およびコンプライアンス。これには、ネイティブ機能を超えた高度な監査メカニズム、複数のデータベース環境にわたる監査およびレポート作成の一元化、職務分離の適用、およびフォレンジック分析とコンプライアンス監査のサポート・ツールが含まれます。
- パフォーマンスおよびスケーラビリティー。本質的にはセキュリティー機能ではありませんが、すべてのデータベース・セキュリティー・ソリューションが高負荷に耐え、パフォーマンス・オーバーヘッドを最小限にし、高可用性構成でのデプロイメントをサポートするためには重要な要件です。

Guardium 製品ファミリーについて詳しくは、http://www.ibm.com/software/data/guardium/ を参照してください。

親トピック: 製品の概要

このリリースの新機能

新機能、機能、および機能拡張。

IBM Security Guardium V10.1.4

ネイティブの監査統合を使用した Amazon Oracle v11 RDS DBaaS モニター

TLS1.0/1.1 を無効化し、TLS1.2 を有効化

VA で Oracle 12.2 をサポート

簡略説明を表示するよう VA GUI を拡張

Windows/UNIX S-TAP 用に OpenSSL を更新

EMC ATMOS のサポート

z/OS 用の GDPR アクセラレーター

分類機能を強化

GIM により S-TAP のデプロイメントを簡素化

グループ・ビルダーの新しい GUI バージョン

管理対象ユニットを割り振る前にスニファーが稼働していることを確認するよう、エンタープライズ・ロード・バランサーを拡張

5 つを超えるコレクターで複数の KTAP バッファーに対応

接続パケットを通常のパケットに優先

IBM Security Guardium V10.1.3

クイック・スタート・コンプライアンス・モニター

- モニター・エージェントのデプロイ - GIM クライアントの検出とアクティブ化、S-TAP のインストール、検査エンジンの作成、S-TAP とコレクターのマッピングを行って、データベース・モニターを迅速に準備します。
- コンプライアンス・モニターのセットアップ - ポリシーを素早くインストールして、グループにデータを設定し、データベース・アクティビティーをモニターするためのレポートを実行することで、コンプライアンス標準への準拠を支援します。

Cloudera Hadoop - Guardium は MongoDB のサポートにより、初めて NoSQL スペースで脆弱性評価を実現しました。現在、Guardium は Cloudera プラットフォームのサポートにより、Hadoop/ビッグデータ・スペースにまで進出しています。Guardium 脆弱性評価は、システムを評価してセキュリティーのベスト・プラクティスに合わせて修正できるようにすることで、組織がより確信を持って Cloudera を使用できるようにします。リアルタイムの監査、コンプライアンス、およびセキュリティー分析に対応する Guardium アクティビティー・モニターとの結合により、Guardium は Cloudera だけでなく、典型的なエンタープライズ環境内でより一般的に使用されているデータベースとデータウェアハウスの総括的なセキュリティー・ソリューションになります。

z/OS 対応の Guardium S-TAP - IBM Security Guardium は以下の機能拡張により、メインフレーム上のデータ・セキュリティーを強化します。

- 無許可の Db2 for z/OS ユーザー・アクティビティーをブロックするデータ保護
- オーバーヘッドを削減するパフォーマンスおよび最適化
- データ保護とリアルタイム分析をさらに拡張する監査機能とフィルタリング機能
- デプロイメントおよび診断を加速化する使いやすさとサポート性

IBM Security Guardium V10.1.2

1. 異常値検出の強化

   異常値を定義するのは、特定のソース (データベース、データベースの特定のユーザー、サーバー、または OS ユーザー) によるアクティビティーの「通常」の時間フレームまたは範囲から外れた特定の期間に発生した、その特定のソースの動作です。異常値検出は、従来のデータベース・モニターを高度なインテリジェンスによって拡張し、ソースの動作における変化を分析することにより、稼働時に潜在的な攻撃を早期に検出可能にします。このリリースでは、以下のものが導入されます。

   - FAM サポート
   - アグリゲーター上で、複数のコレクターからのデータに対して実行されます。
   - 「異常値マイニングの状況」ページ: すべての管理対象ユニットでの異常値マイニング・プロセスの現在の状況を確認できるだけでなく、正常に完了しなかった異常値プロセスにドリルダウンできます。
   - 調査ダッシュボードの結果表の 2 つのタブ: 「要約」タブの各行は、1 時間を単位として異常値が検出されたソースのそれぞれを表し、異常スコアと理由を表示します。「詳細」タブでは、各行が 1 つの異常値を表し、異常スコア、異常値の理由、および詳細 (ソース・プログラム、オブジェクト、動詞など) を示します。

2. Hadoop アクティビティー・モニターおよび Cloudera 5.7+ 統合/Ranger の機能拡張

   このリリースでは、Cloudera Navigator を使用した Cloudera の統合と、Apache Ranger を使用した Hortonworks の統合により、Hadoop データのモニターに対する Guardium サポートが拡張されています。Hadoop データにアクセスする必要があるクライアントに対して SSL 暗号化を可能にする、これらの統合は、新しい Hadoop モニター UI でサポートされます。

3. 分類機能の拡張および新しい Cleversafe バックアップ/アーカイブ・オプション

   Guardium で複数の分類プロセスの同時実行がサポートされるようになりました。複数の分類プロセスを同時に実行できるため、使用可能なシステム CPU リソースをより有効に活用できます。

   Guardium の分類プロセスで、データベース・ソフトウェア・プロバイダーが使用する複数のシステム・データベースとスキーマがデフォルトで除外されるようになりました。これらのデータベースとテーブルを除外することで、分類プロセスがより効率的に実行され、返されるエラーの数が減少する可能性があります。

   Cleversafe バックアップ/アーカイブは、同じ SDK を使用して Amazon S3 インターフェースをサポートします。Cleversafe に対する Guardium インターフェースは、(同じく Guardium でサポートされている) Amazon S3 と類似しています。Guardium のクラウド・サポートには現在、Cleversafe、SoftLayer、および Amazon S3 が含まれています。

4. エンタープライズ正常性ビュー

   新しい適用状態ダッシュボードにより既存の「適用状態」ビューが拡張され、Guardium デプロイメント全体での正常性の問題を一覧する要約が表示されるようになっています。問題が識別された個々のシステムを調査する前に、正常性データのパターンと傾向を識別するには、このダッシュボードがとりわけ役立ちます。

5. FAM の機能拡張 - UID チェーニングとマルチアクション・ルールおよび異常値

   Windows FAM の UID チェーン - 現在、Windows FAM エージェントは、ファイル・イベントに割り当てられたプロセスのユーザー名を返します。Windows FAM エージェントは、その単一のユーザー名を、プロセスの履歴に属するユーザー名のチェーン (UID チェーン) に変更するようになりました。例えば、プロセス 1 (ユーザー janedoe) がプロセス 2 (ユーザー johndoe) を作成した場合、プロセス #2 に関連するファイル・イベントについて、FAM は {janedoe, johndoe} からなる UID チェーンを報告します。

   FAM のマルチアクション・ルール - マルチアクション・ルールは、複数のアクション (指定されたコマンド・カテゴリーまたは指定されたグループごとに 1 つのアクション) で構成されます。FAM のコンテキストでは、これらのコマンドは読み取り、書き込み、削除、実行、およびファイル操作です。

6. 資格最適化

   資格最適化は、ジョブを効率的に実行するために必要な資格をユーザーに提供する上でのデータベース管理者のロールと、システムの脆弱性を防ぐために資格をできる限り正確に、かつ可能な限り最小限に抑える上でのセキュリティーのロールの間を仲介するものです。資格最適化には、「ディスカバー」>「データベース資格」>「資格最適化」によってナビゲートします。

7. HP Vertica のサポート

   HP Vertica は、Hadoop と競合するビッグデータ・システムです。HP-Vertica は、標準の Postgres SQL インターフェースとともに、独自の拡張機能を提供します。

   HP Vertica は、照会パフォーマンスの大幅な高速化のためにデータウェアハウスで使用されます。HP Vertica は、ユーザー対話の分析、広告追跡、クリック・ストリーム・アプリケーション、脅威評価、財務予測に使用されます。

8. UNIX S-TAP RPM の変更

   - /opt/guardium にインストールされます (場所を変更することはできません)。
   - RPM のデフォルト構成

   ktap_installed=1

   RPM をインストールする前に NI_ALLOW_MODULE_COMBOS="Y" をエクスポートすることで、Flex Loading が使用可能になります。

   sqlguard_ip は 127.0.0.1 に設定されます。

   tap_ip は ホスト名に設定されます。

   RPM ログは /opt/guardium/rpm_logs に保存されます。

   - ライブ・アップデートがサポートされています。

   KTAP 要求アップデートは、既存のプロセスによりサポートされます (増分パッケージ・バージョン)。

   - RPM インストール済み環境が検出された場合、シェルおよび GIM インストーラーはインストールを拒否します。
   - STAP はインストール後に実行されますが、構成する必要があります。
   - インストール後の構成を容易にするために、guard-config-update という新しいスクリプトが用意されています。

9. GDPR アクセラレーター

   データ・プライバシーとセキュリティーは、すべての組織が向き合わねばならない最も差し迫った課題です。これまで欧州連合内の各国は、異なるレベルのコンプライアンスを要求していましたが、新たに公表された一般データ保護規則 (GDPR) では、データ保護規則を欧州連合全体にわたって拡大し標準化しています。

   Guardium GDPR アクセラレーターは、GDPR のグループおよびポリシーに基づく事前定義レポートを提供します。GDPR アクセラレーターの処理を開始するには、GDPR ロールを Guardium ユーザーに割り当ててから、そのユーザー・アカウントを使用して「アクセラレーター」>「GDPR」にナビゲートします。

10. データの洞察

    データの洞察は、データ・フローの全体像を把握し、予期しない動作を識別するために人間の視覚能力を利用するという革新的なパラダイムを導入します。Guardium は、累積された経験と知識に基づいて、監査を支援し、攻撃を検出するための堅牢な機械学習機能とデータ分析機能を既に提供しています。データの洞察は、人間の視覚認知の柔軟性を追加して、既知の攻撃タイプとは関係なく、これまでは検出できなかった生データの関連と移動を特定します。

    例えば、街中の道路にできた穴を識別することを目的としたオブジェクト認識プロジェクトでは、近所をうろつく像を識別することはできません。しかし、人間の目であれば直ちに発見できます。 同様に、棒グラフで監査済みデータをレビューする際に、ユーザーは既知の問題タイプを探しますが、新しい (未知の) 逸脱は容易に見逃してしまう可能性があります。

    データの洞察は、監査対象データを 3-D で可視化されたデータ・ソースおよび宛先に時系列で変換し、発生したとおりに展開されたデータ・トランザクションを表示します。

    可視化スペースには 2 つのプレーンがあり、それぞれが特定のタイプの監査ドメインのエンティティーを表します。監査データ内のすべてのエントリーは、上部プレーンのオブジェクト (クライアント IP、OS ユーザー、データベース・ユーザー、ソース・プログラムのうちの 1 つ) から下部プレーンのオブジェクト (データベース、オブジェクト、サーバーのうちの 1 つ) に移動する「点滅線」として表されます。ソースと宛先の間の点滅線は、特定のソースと宛先の間で相互作用があったことを示す証跡 (点線) を残します。それは背景へと徐々に消えていきます。証跡は、選択された期間のソースと宛先の間の相互作用の概要を示します。ソースは、宛先の近くおよび他の類似したソースの近くにあります。宛先エンティティーのサイズは、他の宛先エンティティーとの相対的なトランザクションの量に比例します。この表示を変更する方法は多数あります。例えば、上部エンティティーの色分け (データ・ソースの詳細が変更されると色が変わります)、データの洞察グラフのフィルタリング、調査ダッシュボードのファセットなどです。また、VR ヘッドセットを使用してデータの洞察を表示することもできます。

    データの洞察にアクセスするには、調査ダッシュボードで「グラフの追加」>「データの洞察グラフ」をクリックします。

IBM Security Guardium V10.1

- インフラストラクチャーおよびプラットフォーム:
  - セキュリティー、グローバリゼーション、およびアクセシビリティーの拡張によるプラットフォームの強化
  - Hyper-V 環境で稼働する Guardium アプライアンスのサポート。 Hyper-V は Microsoft の仮想化ソリューションです。
- Guardium デプロイメントの改善されたサポート性と管理:
  - S-TAP エージェントと収集解析の安定度と信頼性が拡張されました。

    - 中央マネージャー正常性ビューは、デプロイされた Guardium コンポーネントの状況を評価するための中央ダッシュボードを提供します。
    - UNIX/Linux および Windows の S-TAP Watchdog (guard_monitor) は、S-TAP のパフォーマンスと反応性をモニターするために設計されたプロセスです。 S-TAP の CPU 使用率が構成されたしきい値を超えた場合、または S-TAP がコンソールの要求に反応しない場合、以下のアクションが実行される可能性があります。
        - guard_diag の自動実行;
        - S-TAP プロセスの自動強制終了;
        - 自動的にコア・ダンプが行われ、S-TAP プロセスを強制終了。
- エンタープライズ準備機能の拡張により、大規模な環境で Guardium コンポーネントをより簡単にデプロイおよび使用できるようになりました。以下に例を示します。
    - 細分性を改善し、要求のリバランスを向上させる自動ロード・バランシングに対する更新。
    - 長時間実行ジョブの進行状況アラートのレポート作成
    - 顧客がロールと Guardium へのアクセス権限を分割する際に役立つ、ユーザー・インターフェース (UI) コンソールに対するよりきめ細かいアクセス権限
    - 中央マネージャーからのデプロイメントと制御を容易にする、テンプレートとプロファイルの構成
    - 大規模環境でのレポート作成を簡素化する選択的な集計
    - 7 要素のタプルのサポート - タプルでは、複数の属性を組み合わせて 1 つの複合グループ・メンバーを形成することができます。7 タプル・グループの例 - クライアント IP/ソース・アプリケーション/データベース・ユーザー/サーバー IP/サービス名/OS ユーザー/データベース名
- 拡張されたデータ・ソースの範囲:
    - System i の S-TAP エージェントのフェイルオーバー、暗号化、およびレポート作成の改善
    - z/OS データ・ソースの S-TAP エージェントのフィルタリング、UID チェーン、および使いやすさの拡張
    - より多くのビッグデータ・プラットフォームのための追加のデータ・セキュリティー機能: MongoDB の動的データ・マスキング、HortonWorks のブロッキングと Ranger セキュリティー・プラットフォームおよび Cassandra Kerberos との統合。
        - Ranger 統合 - Ranger は、Hadoop や関連コンポーネント (Hive、HBase、HDFS、Yarn) できめ細かいアクセス制御を管理するための一元化管理型セキュリティー・フレームワークを提供します。 ユーザーは、Ranger 管理コンソールを使用して、特定のユーザーやグループのセットについてリソース (ファイル、フォルダー、データベース、表、列など) へのアクセスに関するポリシーを容易に管理して、Hadoop 内でポリシーを適用することができます。 また、環境の制御を強化するために監査のトラッキングおよびポリシー分析を実行できます。
    - RedHat 7.1 on Power 8 (リトル・エンディアンとビッグ・エンディアン) アーキテクチャーの S-TAP エージェントのサポート。 エンディアンは、コンピューター・メモリー内の、デジタル・ワードで構成されるバイトの順番を示します。ワードはビッグ・エンディアンまたはリトル・エンディアンの形式で提示されます。 リトル・エンディアン形式では、最下位バイトを最低位メモリーアドレスで、最上位バイトを最上位メモリー・アドレスで保存します。
    - Db2 Analytics Accelerator for z/OS に対する新規サポート
    - PostgreSQL 9.4 および SSL の暗号化サポート
    - Db2 UDB および MS SQL の場合、Guardium は count_big(*) をサポートします。
- 複数の IT サイロにまたがる難解なセキュリティー問題のための相乗的ユースケースを提供する、セキュリティー統合:
    - 内部脅威からの保護。 内部の脅威を明らかにするため IBM Security Privileged Identity Manager との統合を利用します。
    - 脅威保護システム。 IBM Security QRadar および IBM Security XGS と連動して、脅威がデータ・ソースに到達する前に検出し、データ侵害を防いだり、モニターの警戒を高めたりします。
- 追加のデータ・アクセス分析ツールのためのテクノロジー・プレビュー:
    - 調査センターは、監査レコードに基づくフォレンジック追跡を実行するための中心的な場所を提供します。

IBM Security Guardium Vulnerability Assessment V10.1

- 新しい共通の脆弱性イベント (CVE) とその他の脆弱性テストで更新されたセキュリティー認識
- IBM Security AppScan との統合による、アプリケーション層からバックエンド・インフラストラクチャーまで共有される脆弱性評価のための共通フレームワーク

IBM Security Guardium for Files (FAM) V10.1

- 大規模組織でのデプロイを支援するスケーラビリティーとパフォーマンスの改善
- ファイル・アクティビティー・モニターのディスカバリー・パフォーマンスの改善
- AIX 6.1 および AIX 7.1 での FAM ディスカバリーのサポート (分類なし)。 FAM クローラーの共有ドライブ・ディスカバリーと分類のサポート。

親トピック: 製品の概要

リリース情報

最新の機能と機能拡張、システム要件、そしてアップグレード、インストール、およびサポート情報について説明します。

新機能と機能拡張の説明

Guardium の最新バージョンには、数多くの新機能および既存の機能に対する機能拡張が含まれています。詳細なリリース・ノートについては、以下のリンク先を参照してください。

- Guardium V10.1.4 リリース・ノート
- Guardium V10.1.3 リリース・ノート
- Guardium V10.1.2 リリース・ノート
- Guardium V10.1 リリース・ノート

発表資料

以下の情報については、IBM Guardium の発表資料を参照してください。

- 詳細な製品説明 (新機能の説明を含む)
- 製品の位置付けに関する説明
- パッケージと発注方法に関する情報
- 多国語間の互換性情報

システム要件

Guardium V10.1 のシステム要件およびサポートされるプラットフォームの情報については、http://www-01.ibm.com/support/docview.wss?uid=swg27047801 を参照してください。

Guardium のアップグレード

Guardium の最新バージョンへのアップグレードについては、Guardiumシステムのアップグレードを参照してください。

Guardium のインストール

最新バージョンの Guardium のインストールについては、Guardiumシステムのインストールを参照してください。

既知の問題

既知の問題は文書化されており、IBM サポート Web サイトで確認できます。

問題が発見および解決されると、IBM サポート Web サイトが更新されます。ダウンロードや詳細なシステム要件に関する資料などに加えて、IBM サポート Web サイトを検索することにより、問題の回避策や解決策を素早く見つけることができます。

サポートのライフサイクル

Guardium ソフトウェアの古いバージョンを使用している場合、アップグレードすることを早めに計画してください。IBM 製品のサポート終了日に関する情報は、IBM Software Support Lifecycle Web サイトで確認できます。

親トピック: 製品の概要

始めに

- ユーザー・インターフェースの概要
  Guardium ユーザー・インターフェースの基礎 (初回ログイン、バナーおよびナビゲーション・メニュー、ユーザー・インターフェース、データ検索など) について説明します。
- ユーザー・インターフェースのカスタマイズ
  Guardium では、特定のユーザーとロールについて、ナビゲーション・メニューをカスタマイズすることができます。
- モニターおよびコンプライアンスのクイック・スタート
  モニター・エージェントをデータベース・サーバーにデプロイし、データベース・モニターをセキュリティー基準と規制に準拠するように構成する方法について説明します。
- システム・ビュー
  「システム・ビュー」は、多くのユーザーにとってのデフォルトの初期ビューです。 これにより、システム状況の重要な要素を確認できます。
- データ・アクティビティーのモニター
  Guardium データ・アクティビティー・モニターで使用される重要なセキュリティー概念について説明します。
- ファイル・アクティビティー・モニター
  ファイル・アクティビティー・モニターはサーバー上の機密データをディスカバーします。また、事前定義の定義またはユーザー定義の定義を使用してコンテンツを分類します。さらに、データ・アクセスに関するルールおよびポリシーや、ルールが満たされたときに実行されるアクションを構成します。
- 重要な概念とツール
  Guardium の管理に関連した重要な概念について説明します。

関連情報:
Guardium の概要、アーキテクチャー、およびユーザー・インターフェース (ビデオ)

ユーザー・インターフェースの概要

Guardium ユーザー・インターフェースの基礎 (初回ログイン、バナーおよびナビゲーション・メニュー、ユーザー・インターフェース、データ検索など) について説明します。

ナビゲーション

Guardium ユーザー・インターフェースに初めてログインする際には、バナーとナビゲーション・メニューの 2 つのメインメニューがあります。

ナビゲーション・メニューを展開/省略するには、シェブロン・アイコン をクリックします。ナビゲーション・メニューを完全に非表示にするには、表示/非表示アイコン をクリックします。

画面の初期レイアウトは、適用されているライセンス、ロールに基づいて許可されるアクセス、マシン・タイプ、可視性要因によって決まります。ロールの例としては、ユーザー、管理者、アクセス・マネージャー、CLI などがあります。ロールは、ユーザーに特定のアクセス権を付与するためにユーザーとアプリケーションに割り当てられます。

サポート対象の Web ブラウザー

Internet Explorer 9 (IE9) 以上 (Windows 7)。IE9 使用時の警告 - (1) 会社の Web サイトが Internet Explorer の「互換表示」選択項目にリストされていないことを確認してください。 (2) ファイルのエクスポート時、ファイルのダウンロードは「暗号化されたページをディスクに保存しない」IE 9 オプションによってブロックされます。 このオプションの設定を変更すると、エクスポート/ダウンロードが適切に機能するようになります。

Firefox ESR 24 以上

Chrome 28 以上

最小画面解像度 - 1366 x 768

バナー・メニュー

バナーには以下の項目が含まれています。

項目	記述
システム時刻クロック	Guardium システム上の世界時。
To-do リスト	ユーザーによってフィルタリング可能な「監査プロセスの To-do リスト」と、「保留中の結果がない処理」が含まれています。
ヘルプ	製品ヘルプを開くには、「ヘルプ」 > 「Guardium ヘルプ」をクリックします。 Guardium システムに関する情報 (バージョン番号など) を表示するには、「ヘルプ」 > 「Guardium バージョン情報」をクリックします。 操作している画面や機能に固有のヘルプ内容を表示するには、画面のペインに組み込まれている小さいヘルプ・アイコンをクリックします。 注: どちらのヘルプ・アイコンをクリックしても、同じインフォメーション・センターに移動します。ここで、すべてのヘルプ内容を検索してアクセスすることができます。
ユーザー・インターフェース/データ/ファイルの検索	ユーザー・インターフェースの一部、データの断片、またはファイルを検索します。 例えば、「ポリシー・ビルダー」を検索したい場合は、検索を「ユーザー・インターフェース」に切り替え、「`policy builder`」という入力を開始します。任意の結果をクリックすると、ユーザー・インターフェースのその部分に移動します。
アカウント・タイプ	ユーザーのアカウントのタイプを示します。アカウントの詳細 (パスワードまたは名前) の編集、UI レイアウトのカスタマイズ、Guardium からの確実なサインアウトを行います。
マシン・タイプ	稼働中のマシンのタイプ (スタンドアロン、管理対象ユニット、中央マネージャー、アグリゲーターなど) を示します。

バナー・メニューには、重要な始動メッセージ (RAM メモリー不足、クイック検索メモリーおよび CPU 4 コアの最小要件、証明書の有効期限切れ、一元管理の障害、SSLv3 が有効または無効、ライセンスなし、など) も含まれます。

注: Guardium では SSLv3 を無効にすることを推奨しています。 ただし、最新リリースがインストールされていない旧バージョンの Guardium の利用時、SSLv3 が無効であると、中央マネージャーと管理対象ユニットの間で一元管理機能が低下します。

ナビゲーション・メニュー

ナビゲーション・メニュー内の各アイコンは、Guardium セキュリティー・ライフサイクルの 1 フェーズを表しています。任意のアイコンをクリックすると、そのフェーズが展開され、フェーズに含まれる各コンポーネントが表示されます。ライフサイクルに基づくナビゲーション・メニューは、ユーザー・インターフェースをナビゲートする機能の 1 つであり、すべてのロールにわたって一貫性があります。メニュー項目をカスタマイズし、ロールに基づいてメニュー項目を表示または非表示にできます。

フェーズ	記述
設定	ネットワーク設定の構成、サービス状況の確認、データ・ソース定義、グループ、別名、およびアラートの設定を行います。
管理	現行環境の全体的な正常性、S-TAP、データ、モジュール、メンテナンス、レポートを管理します。

ディスカバー	現行環境に導入された新規データベースを自動的にディスカバーし、機密データの検索と分類を行います。
強化	脆弱性評価で現行環境の現在の弱点を評価し、構成監査システム (CAS) で現行環境に加えられた変更をモニターします。
調査	データベース・アクティビティーをモニターし、現行環境の各部に疑わしいアクティビティーがないか調査します。
保護	疑わしいアクティビティーをブロックし、データへの無許可アクセスを防止するデータ・セキュリティー・ポリシーを使用して、現行環境を保護します。 ポリシーについて詳しくは、『ポリシー』を参照してください。
順守	監査プロセスと細分度の高いレポート作成によって、コンプライアンス・イニシアチブを実現します。
レポート	独自のレポートを作成するか、各種の事前定義レポートのいずれかを使用して、現行環境の任意の部分に関するレポートを作成します。レポートについて詳しくは、レポートを参照してください。
マイ・ダッシュボード	関心の高いレポートを容易にレビューできるように、独自のダッシュボードを作成します。ダッシュボードについて詳しくは、ダッシュボードの作成を参照してください。

共通して使用されるアイコン

以下の一連のアイコンは、Guardium の多くのファインダー・アプリケーションとビルダー・アプリケーションで共有されます。

アイコン	記述
新規	新規項目 (グループやデータ・ソース定義など) を作成します。
変更	項目を変更します。 注: 項目を変更する際のベスト・プラクティスは、その項目のコピーを作成し、そのコピーに変更を加えることです。
コピー	項目を複製し、その項目のコピーを作成します。
削除	項目を削除します。

親トピック: 始めに

ユーザー・インターフェースのカスタマイズ

Guardium では、特定のユーザーとロールについて、ナビゲーション・メニューをカスタマイズすることができます。

「ナビゲーション・メニューのカスタマイズ (Customize Navigation Menu)」ツールと「ユーザー/ロールのカスタマイズ」ツールにより、ナビゲーション・メニューの内容と構成を簡単に変更することができます。これらのツールは、複数の場所で使用することができます。

- すべてのユーザーは、Guardium バナーの「ユーザー」メニューを開いて「カスタマイズ」を選択することにより、自分専用のナビゲーション・メニューをカスタマイズすることができます。
- 管理ユーザーは、「ユーザー」メニューを開いて「ユーザー/ロールのカスタマイズ」を選択するか、「設定」 > 「ツールとビュー」 > 「ユーザー/ロールのカスタマイズ」にナビゲートすることにより、他のユーザーやロールのナビゲーション・メニューをカスタマイズすることができます。
- *accessmgr* としてログインしたユーザーは、「アクセス」 > 「アクセス管理」にナビゲートして「ロール・ブラウザー」を選択し、「ナビゲーション・メニューのカスタマイズ (Customize Navigation Menu)」リンクをクリックすることにより、他のユーザーやロールのナビゲーション・メニューをカスタマイズすることができます。

ツールでのカスタマイズ操作は、すべてのユーザーで共通しています。

「ナビゲーション・メニュー」リストには、Guardium ナビゲーション・システムの構成と内容が反映されます。項目を「ナビゲーション・メニュー」リストに追加するには、「使用可能なツールとレポート (Available Tools and Reports)」リストでツールとレポートを選択し、  アイコンを使用します。「ナビゲーション・メニュー」リストから項目を削除するには、削除したい項目の横に表示されている  アイコンをクリックします。「ナビゲーション・メニュー」リスト内の項目の配置を変更するには、ドラッグ・アンド・ドロップ機能を使用するか、アイコン・コントロールを使用します。

「ナビゲーション・メニュー」リストの項目を選択して  アイコンをクリックすることにより、Guardium の新しいホーム・ページ (システムにログインしたときに最初に表示されるページ) を定義することができます。

「OK」ボタンをクリックすると Guardium のナビゲーション・メニューが更新され、「ナビゲーション・メニュー」リストで行ったすべての変更内容が反映されます。

これらのツールを使用する場合は、以下の制約事項が適用されます。

- 「マイ・ダッシュボード」グループは削除できませんが、グループ内のダッシュボードは個別に削除することができます。
- 新しいグループを作成しても、そのグループが空の場合は保存されません。
- 「ナビゲーション・メニュー」リストに表示されているグループのうち、空のグループは Guardium のナビゲーション・メニューには表示されません。

親トピック: 始めに
関連情報:
ロールと権限の管理

モニターおよびコンプライアンスのクイック・スタート

モニター・エージェントをデータベース・サーバーにデプロイし、データベース・モニターをセキュリティー基準と規制に準拠するように構成する方法について説明します。

このタスクについて

モニターおよびコンプライアンスのクイック・スタートは、次の 2 つのツールで構成されます。

モニター・エージェントのデプロイ

モニター・エージェントのデプロイ・ツールを使用して、GIM クライアントを自動的にアクティブ化し、S-TAP をインストールして、データベース・トラフィックのモニターを開始します。

モニター・エージェントのデプロイ・ツールは、Guardium デプロイメントを設定するプロセスを単純化します。既存の Guardium Installation Manager (GIM) のインフラストラクチャーで構築されているモニター・エージェントのデプロイ・ツールは、データベース・サーバーを素早く検索し、モニター・エージェント (S-TAP) をインストールし、検査エンジンをデータベース用に構成するのに役立ちます。 また、このツールは、デプロイメント状況を追跡して検討するための中央ビューを備えています。

コンプライアンス・モニター

モニター・エージェント (S-TAP) をデプロイした後、コンプライアンス・モニター・ツールを使用して、特定のセキュリティー基準および規制のモニターを設定します。

Guardium は、以下のような特定の基準および規制に対応するグループ、セキュリティー・ポリシー、およびレポートなどの、コンプライアンス・モニター・テンプレートをいくつか備えています。

- バーゼル銀行監督委員会 (BASEL II)
- 一般データ保護規則 (GDPR)
- Db2 for z/OS 用の一般データ保護規則 (Db2 for z/OS の GDPR)
- 医療保険の相互運用性と説明責任に関する法律 (HIPAA)
- クレジット・カード業界データ・セキュリティー基準 (PCI)
- 個人情報 (PII)
- サーベンス・オクスリー (SOX) 法への準拠

これらのクイック・スタート・コンプライアンス・モニター・テンプレートは、関連する基準または規制のいずれかに短期間で準拠する必要がある組織に特に役立ちます。セキュリティー・ポリシーをインストールした後、コンプライアンス・モニター・ツールは、初期セットアップやグループへの組織固有の情報 (クライアント IP アドレスや特定の特権ユーザー ID など) の取り込みについて、管理者およびコンプライアンス担当者にガイドを提供します。 さらに、コンプライアンス・モニター・ツールは、Guardium 環境を定期的に検査して、コンプライアンス・モニター・テンプレートを使用してモニターできる新規のデータベースを調べます。

手順

1. ツールについて詳しく理解するために以下の情報を確認します。
   - モニター・エージェントをデプロイするためのクイック・スタート
   - コンプライアンス・モニターのクイック・スタート
2. データベース・サーバー用のモニター・エージェントをデプロイします。
   a. モニター・エージェントのデプロイ・ツールを使用するための前提条件を満たしていることを確認します: モニター・エージェントをデプロイするための前提条件。
   b. モニター・エージェントをデータベース・サーバーにデプロイします: モニター・エージェントのデプロイ。
3. データベース・サーバー用にコンプライアンス・モニターを構成します。
   a. コンプライアンス・モニター・ツールを使用するための前提条件を満たしていることを確認します: コンプライアンス・モニターの前提条件
   b. コンプライアンス・モニターを構成します: コンプライアンス・モニターのセットアップ。
   c. データベースへのアクセスが許可されているユーザーおよびアプリケーションを識別するためにグループにデータを設定します: グループへのデータの設定。
   d. 機密データのディスカバリーおよび分類のためにデータベースへのアクセスを Guardium に許可する資格情報を提供します: 機密データのスキャンの有効化

タスクの結果

モニター・エージェントを正常にデプロイし、データベース・サーバー用にコンプライアンス・モニターを構成すると、Guardium はデータベース・トラフィックのモニターを開始します。

コンプライアンス・モニター・ページに表示される内容の解釈について詳しくは、コンプライアンス・モニター・ビューの概要を参照してください。

親トピック: 始めに

システム・ビュー

「システム・ビュー」は、多くのユーザーにとってのデフォルトの初期ビューです。 これにより、システム状況の重要な要素を確認できます。

「システム・ビュー」の下の 3 つのタブは、さまざまなタイプの状況情報を表示します。

- 「S-TAP 状況モニター」は、環境にデプロイされている S-TAPs の要約データを表示します。アイコンは状況の概要を表し、検査エンジンについての情報を確認するためにドリルダウンできます。
- 「ユニット使用状況」タブは、各 Guardium システムの使用状況についての情報を表示します。
- 「システム・モニター」タブには、着信データ、CPU 使用量、およびその他の情報に関する最新の詳細が表示されます。

親トピック: 始めに

データ・アクティビティーのモニター

Guardium データ・アクティビティー・モニターで使用される重要なセキュリティー概念について説明します。

- ポリシーおよびルール
  セキュリティー・ポリシーには、データベース・クライアントとサーバーとの間の監視対象トラフィックに適用される順序付きルール・セットが含まれています。各ルールは、クライアントからの要求、またはサーバーからの応答に適用できます。1 つの Guardium システムに、同時に複数のポリシーを定義することも、複数のポリシーをインストールすることもできます。
- ワークフロー
  ワークフローは、いくつかのデータベース・アクティビティー・モニター・タスクを統合します。このタスクには、資産のディスカバリー、脆弱性評価と強化策、データベース・アクティビティーのモニターと監査レポートの作成、レポートの配布、主要な利害関係者によるサインオフ、エスカレーションなどがあります。
- 監査
  Guardium には、データベース表内の値の変更をトラッキングする「値変更監査」機能があります。
- 分類
  Guardium は、機密データのディスカバリーと分類をサポートすることにより、効果的なアクセス・ポリシーの作成と適用を可能にします。

親トピック: 始めに

ポリシーおよびルール

セキュリティー・ポリシーには、データベース・クライアントとサーバーとの間の監視対象トラフィックに適用される順序付きルール・セットが含まれています。各ルールは、クライアントからの要求、またはサーバーからの応答に適用できます。1 つの Guardium システムに、同時に複数のポリシーを定義することも、複数のポリシーをインストールすることもできます。

ポリシー内の各ルールは、条件付きアクションを定義します。条件は、許可されたクライアント IP グループ内で見つからないクライアント IP アドレスからのアクセスがないか検査するなどの単純なテストにすることも、複数のメッセージおよびセッション属性 (データベース・ユーザー、ソース・プログラム、コマンド・タイプ、時刻など) を評価する複雑なテストにすることもできます。ルールは、指定の時間フレーム内で条件が満たされる回数を識別するようにすることもできます。

ルールで起動されるアクションは、通知アクション (例えば、1 人以上の受信者に対する E メール通知)、ブロッキング・アクション (クライアント・セッションが切断されるなど) のほか、イベントがポリシー違反としてログに記録されるだけの場合もあります。所定の環境やアプリケーションに固有と見なされる条件に対して必要とされるすべてのタスクを実行するカスタム・アクションを開発することができます。

親トピック: データ・アクティビティーのモニター

ワークフロー

ワークフローは、いくつかのデータベース・アクティビティー・モニター・タスクを統合します。このタスクには、資産のディスカバリー、脆弱性評価と強化策、データベース・アクティビティーのモニターと監査レポートの作成、レポートの配布、主要な利害関係者によるサインオフ、エスカレーションなどがあります。

ワークフローは、データベース・セキュリティーの管理を、時間のかかる定期的な手動アクティビティーから、企業のプライバシー要件とガバナンス要件 (PCI-DSS、SOX、データ・プライバシー、HIPAA など) をサポートする継続的な自動化プロセスに変換します。さらに、ワークフローを使用すると、Syslog、CSV/CEF ファイル、外部フィードを介して、追加のフォレンジック分析用に監査結果を外部リポジトリーにエクスポートすることができます。

例えば、コンプライアンス・ワークフロー自動化プロセスは、「必要なレポート、アセスメント、監査証跡、分類のタイプは?」、「この情報の受信者と、サインオフの処理方法は?」、「配布のスケジュールは?」などの質問を処理することができます。

親トピック: データ・アクティビティーのモニター

監査

Guardium には、データベース表内の値の変更をトラッキングする「値変更監査」機能があります。

変更のトラッキング対象にする各表において、モニター対象にする SQL 値変更コマンド (INSERT、UPDATE、DELETE) を選択できます。 モニター対象の表に対して値変更コマンドが実行されるたびに、before 値および after 値が収集されます。 この変更アクティビティーは定期的に Guardium にアップロードされ、その後、Guardium のすべてのレポート機能およびアラート機能を使用できるようになります。

デフォルトの「変更された値」レポートから値変更データを表示できます。あるいは、「値変更のトラッキング」ドメインを使用してカスタム・レポートを作成することもできます。

親トピック: データ・アクティビティーのモニター

分類

Guardium は、機密データのディスカバリーと分類をサポートすることにより、効果的なアクセス・ポリシーの作成と適用を可能にします。

分類ポリシーは、機密データ・エレメントのディスカバリーとタグ付けを行うために設計された一連のルールです。分類ポリシー内で、ルールごとにアクションを定義することができます (例えば、E メール・アラートの生成や、Guardium グループへのメンバーの追加など)。また、分類ポリシーは、指定のデータ・ソースに対して実行するようにスケジュールすることも、ワークフロー内のタスクとして実行するようにスケジュールすることもできます。

組織の規模が大きくなり、クレジット・カード番号や個人の金融データなどの機密情報が複数のロケーションに存在するようになると (そのデータの現在の管理責任者が分からないという場合がよくあります)、ディスカバリー・ルーチンと分類ルーチンの重要性が増します。 こうした状況は、合併買収の際や、元の所有者がいなくなった後もレガシー・システムを引き続き使用している場合に、多く発生します。 Guardium の分類ポリシーは、このような機密データのディスカバリーとタグ付けを行うことにより、適切なアクセス・ポリシーを適用できるようにします。

親トピック: データ・アクティビティーのモニター

ファイル・アクティビティー・モニター

ファイル・アクティビティー・モニターはサーバー上の機密データをディスカバーします。また、事前定義の定義またはユーザー定義の定義を使用してコンテンツを分類します。さらに、データ・アクセスに関するルールおよびポリシーや、ルールが満たされたときに実行されるアクションを構成します。

ファイル・アクティビティー・モニターは、以下の機能で構成されます。

- ディスカバリーには、ファイルおよびフォルダーのメタデータおよび資格の収集が含まれます。
- 分類では、*判定プラン*を使用して、ファイル内の機密データと見なされるデータ (クレジット・カード情報、個人を特定できる情報など) が識別されます。
- 監査情報のモニターと収集、ポリシー・ルール、および疑わしいユーザーや接続のリアルタイム・アラートまたはブロック。

ファイル・アクティビティー・モニター:

- 費用対効果の高い方法で法規制に適合する
    - 制御を自動化および一元化し、監査証跡を提供します。
    - HIPAA、PCI DSS、自治体レベルおよび国レベルのプライバシー規則など、多様な規則への適合を実現します。
- データ量の増加や企業要件の増大に合わせた規模の拡大が可能
- すべての一般的なシステムに対応する広範な異種混合サポートを提供

ユース・ケース 1

アプリケーション・サーバーやデータベース・サーバーに対するバックエンド・アクセスを通じて、重大なアプリケーション・ファイルがアクセスまたは変更される可能性や、破壊される可能性もある。

解決策: ファイル・アクティビティー・モニターにより、構成ファイル、ログ・ファイル、ソース・コード、およびその他多くの重大なアプリケーション・ファイルをディスカバーしてモニターし、無許可ユーザーや無許可プロセスがアクセスを試みた場合に、アラートの発行やブロックを実行できる。

ユース・ケース 2

個人情報 (PII) や専有情報を含むファイルを、日常の業務に影響を与えずに保護する必要がある。

解決策: ファイル・アクティビティー・モニターにより、多くのファイル・システムに保管された機密文書へのアクセスをディスカバーしてモニターできる。ファイル・アクティビティー・モニターは、データを集約して、アクティビティーに対する情報を提供し、疑わしいアクセスが行われた場合にアラートを発行し、特定のファイルおよびフォルダーに対する特定のユーザーからのアクセスをブロックできるようにする。

ユース・ケース 3

アプリケーションが管理する文書へのバックエンド・アクセスをブロックする必要がある。

解決策: ファイル・アクティビティー・モニターにより、通常はアプリケーションのフロントエンド (Web ポータルなど) を通じてアクセスする文書に対するバックエンド・アクセスをディスカバーしてモニターし、これをブロックすることができる。

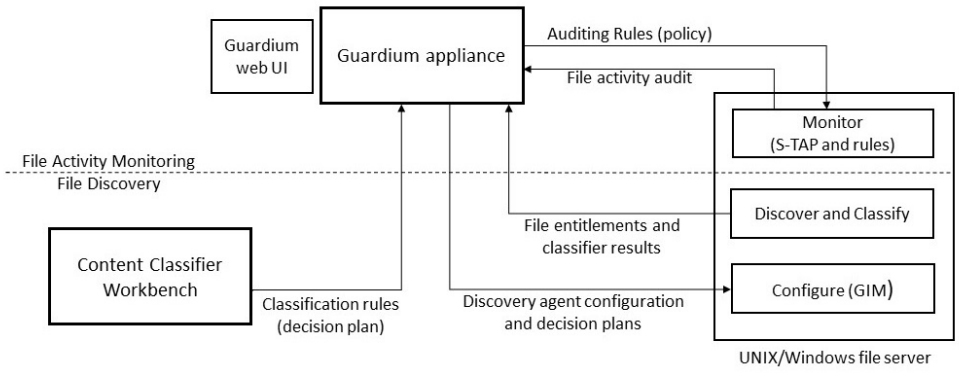
- ファイル・アクティビティー・モニターの概要および概念
- ファイル・アクティビティー・モニターの前提条件
- ファイル・アクティビティー・モニターの上位ワークフロー
  この一般ワークフローを使用して、ファイル・アクティビティー・モニターを計画および実行します。

親トピック: 始めに
関連情報:
Guardium を使用したファイル・アクティビティーのモニター (ビデオ)

ファイル・アクティビティー・モニターの概要および概念

ファイル・サーバーのファイル・アクティビティー・モニターは、以下の機能からなります。

- ディスカバリーには、ファイルおよびフォルダーのメタデータおよび資格の収集が含まれます。
- 分類では、*判定プラン*を使用して、ファイル内の機密データと見なされるデータ (クレジット・カード情報、個人を特定できる情報など) が識別されます。
- 監査情報のモニターと収集、ポリシー・ルール、および疑わしいユーザーや接続のリアルタイム・アラートまたはブロック。



ディスカバリーと分類

基本的な**ディスカバリー**・スキャンにより、フォルダーおよびファイルと、それぞれの所有者、アクセス権限、サイズ、および最終更新日時のリストが識別されます。また、ユーザー権限とグループ権限も識別されます。ディスカバリーではすべてのファイル・タイプがサポートされます。**分類**は、*判定プラン*により定義されています。各判定プランには、特定タイプのデータを認識するためのルールが含まれます。(ファイル・アクティビティー・モニターの判定プランは、データ・アクティビティー・モニターの分類ポリシーと類似しています)。分類では、プレーン・テキスト、HTML、Office、PDF を含め、さまざまなタイプのファイルがサポートされます。HIPAA、PCI、SOX、およびソース・コードには、デフォルトの判定プランがあります。 デフォルトの判定プランを使用して、結果のレポート/調査ダッシュボードから分類エンティティーを変更できます。さらに、コンテンツ分類ワークベンチ (コレクター・アプライアンスにアップロードする Windows アプリケーション) を使用して、新しいプランを作成したり、既存のプランを変更したりすることもできます。IBM Content Classification バージョン 8.8 の要件については、IBM 技術情報 (http://www-01.ibm.com/support/docview.wss?uid=swg27020838) を参照してください。Guardium Installation Manager (GIM) を使用してプランをアクティブ化および構成します。

ディスカバリーと分類は、ファイル・クローラーと呼ばれるディスカバリー・エージェントによって処理されます。ファイル・クローラーは、ファイル・メタデータとデータをディスカバリーおよび分類プロセスから Guardium システムに送信します。スキャンのスケジュールは構成可能です。初期ディスカバリーおよび分類が完了すると、以降の (増分) スキャンでは、新規ファイルおよび変更後のファイルのみの増分の変更が識別されます。ファイル・クローラーは、他のバンドルと同様に Guardium Installation Manager (GIM) を使用してインストールし、構成します。

モニター、監査、ブロック

ファイル・アクティビティー・モニターは、ファイル・サーバー上で稼働する S-TAP によって実装されます。(アクティビティー・モニターには、ディスカバリーと分類で使用される FAM バンドルは必要ありません)。NFS ボリュームでは、それらのボリュームにアクセスするすべてのマシンに S-TAP がインストールされ、構成されていることが重要です。S-TAP は、Guardium のポリシー・ルールに従って、ファイル・アクセスの継続モニター、アラート生成、ブロックを管理します。これらのルールは、モニター対象のファイル・サーバーおよびファイルと、ポリシー・ルールに違反している場合に実行するアクション (例えば、違反の記録、アラート生成、アクセスのブロック) を指定します。モニター対象の操作は、読み取り、書き込み、実行、削除、および所有者、許可、プロパティーの変更です。セキュリティー・ポリシー・ルールの基準に一致するアクティビティーは、いずれも Guardium コレクターに送信されて、Guardium リポジトリーに保管されます。(データベース・アクティビティー・モニターでは、S-TAP により、すべてのデータ・アクティビティーが Guardium に送信され、そこでモニターされます)。Guardium リポジトリーに記録されるイベントは、いずれも監査済みイベントです。

S-TAP でファイル・モニター・ルールがアクティブ化されるため、ブロックはただちに実行されます。ユーザーが要求するデータがディスクから読み取られることは決してありません。そのような操作は、S-TAP がブロックして防ぐためです。また、オペレーティング・システムがファイルへのアクセスを許可している場合でも、そのアクセスをブロックできます。

モニター・アクティビティーは、定義済みのレポート (ユーザー特権、ファイル特権、ユーザーあたりのアクティビティー数、クライアントあたりのアクティビティー数、「公開」されているファイル、休止ユーザー、休止ファイルなど)、FAM – アクセス・レポート (すべてのモニター対象のアクティビティーのログ)、および調査ダッシュボードに表示されます。

重要: Windows 管理者と Linux ROOT ユーザーのアクティビティーは、ファイル・アクティビティー・モニターではモニターされず、またブロックもされません。

1 つの S-TAP エージェントが、ファイル・サーバーのアクティビティー・モニターとデータベースのアクティビティー・モニターの両方を管理します。両方の機能のライセンスがある場合は、同じ S-TAP エージェントをファイル・アクティビティー・モニターとデータベース・アクティビティー・モニターの両方に使用できます。S-TAP は、他のバンドルと同様に、Guardium Installation Manager (GIM) を使用してインストールし、構成します。

親トピック: ファイル・アクティビティー・モニター

ファイル・アクティビティー・モニターの前提条件

ファイル・アクティビティー・モニターを実行するには、以下のコンポーネントをインストールします。

- GIM クライアント (すべてのファイル・サーバー上)
- S-TAP
- ライセンス・キー
- FAM ディスカバリー・エージェント (別名 FAM バンドルまたは FAM エージェント。ディスカバリーおよび分類のために必要)
- オプションの IBM Content Classification (デフォルト以外の判定プランの場合。http://www-01.ibm.com/support/docview.wss?uid=swg27020838を参照)

ファイル・アクティビティー・モニターは UID チェーンをサポートしています。つまり、FAM エージェントは単一のユーザー名を、プロセスの履歴に属するユーザー名のチェーン (UID チェーン) に変更します。例えば、プロセス 1 (ユーザー janedoe) がプロセス 2 (ユーザー johndoe) を作成した場合、プロセス #2 に関連するファイル・イベントについて、FAM は {janedoe, johndoe} からなる UID チェーンを報告します。

以下は、ファイル・アクティビティー・モニターのサポート対象外です。

- Network Attached Storage

ファイル・アクティビティー・モニターでは、以下のサーバーがサポートされます。

プラットフォームのバージョン	FAM モニター	FAM ディスカバリー	FAM 分類
aix-7.1-aix-powerpc	はい	はい	いいえ
aix-6.1-aix-powerpc	はい	はい	いいえ
Red Hat 4 PowerPC	はい	いいえ	いいえ
Red Hat 5 S390X	はい	いいえ	いいえ
rhel-4-linux-i686	はい	いいえ	いいえ
rhel-4-linux-ia64	いいえ	いいえ	いいえ
rhel-4-linux-x86_64	はい	いいえ	いいえ
rhel-5-linux-i686	はい	はい	はい
rhel-5-linux-ia64	いいえ	いいえ	いいえ
rhel-5-linux-ppc64	はい	いいえ	いいえ
rhel-5-linux-x86_64	はい	はい	はい
rhel-6-linux-i686	はい	はい	はい
rhel-6-linux-ppc64	はい	いいえ	いいえ
rhel-6-linux-s390x	はい	いいえ	いいえ
rhel-6-linux-x86_64	はい	はい	はい
rhel-7-linux-x86_64	はい	はい	はい
suse-10-linux-i686	はい	はい	はい
SharePoint 2013	いいえ	いいえ	はい
suse-10-linux-ppc64	はい	いいえ	いいえ
suse-10-linux-s390x	はい	いいえ	いいえ
suse-10-linux-x86_64	はい	はい	はい
suse-11-linux-i686	はい	はい	はい
suse-11-linux-s390x	はい	いいえ	いいえ
suse-11-linux-x86_64	はい	はい	はい
suse-12-linux-x86_64	はい	はい	いいえ
Ubuntu 10 x86/64	はい	はい	いいえ
Ubuntu 12 x86/64	はい	はい	はい
Ubuntu 14 x86/64	はい	はい	いいえ
Windows 2008 Server	はい	はい	はい
Windows 2012 Server	はい	はい	はい

親トピック: ファイル・アクティビティー・モニター

ファイル・アクティビティー・モニターの上位ワークフロー

この一般ワークフローを使用して、ファイル・アクティビティー・モニターを計画および実行します。

ファイル・アクティビティー・モニターの上位ワークフロー

1. すべてのファイル・サーバーでのファイル・アクティビティー・モニター・コンポーネントのインストールおよびアクティブ化。
2. ファイル・サーバー内での機密データのディスカバーおよび分類.
3. オプションのFAM 判定プランのカスタマイズ。デフォルトの判定プランを使用することも、IBM Content Classification を使用して独自のプランを作成することもできます。
4. モニターおよび監査
   - ファイル・アクティビティーは、次の定義済みレポートを含むレポートに含めることができます。事前定義レポート : ユーザー特権、ファイル特権、ユーザーあたりのアクティビティー数、クライアントあたりのアクティビティー数、「公開」されているファイル、休止ユーザー、休止ファイルなど。
   - 継続的な調査および分析には、調査ダッシュボードを使用します。調査ダッシュボードには、テキスト検索や異常値の機能、および拡張された可視化が含まれます。以下を参照してください。
     - ファイルの調査ダッシュボード
     - ファイル・アクティビティーの異常値の解釈
5. 保護: 進行中のモニターおよび保護のポリシーを作成して適用します。ファイル・アクティビティーのポリシーおよびルールを参照してください。

- UNIX: デバッグ・レベルは、tap_debug_output_level によって構成されます。FAM エラーおよびデバッグ・ログは guard_stap.fam.txt という名前になります。UNIX でのデフォルトの場所は ¥tmp であり、tap_log_dir によって設定されます。
- Windows: FAM エージェント・ログ・ファイルは StapAT.ctl と呼ばれ、C:¥Program Files¥IBM¥Windows S-TAP¥Logs フォルダーにあります。

親トピック: ファイル・アクティビティー・モニター

重要な概念とツール

Guardium の管理に関連した重要な概念について説明します。

- 照会およびレポート
  Guardium 照会は、収集したデータから取得される情報セットを記述します。 レポートは、Guardium 照会によって識別されるデータの表示方法を定義します。
- アクセス制御
  Guardium には、データベース・クライアントとデータベース・サーバー間のデータ・アクセスを簡単に表示する手段として、アクセス・マップが用意されています。
- ユーザー・ロール
  ロールは、同じアクセス権を共有する Guardium ユーザーのグループを定義します。
- グループ
  Guardium では、エレメントのグループ化がサポートされているため、ポリシーの作成と管理を簡単に行い、分かりやすいレポートを表示することができます。
- データのアーカイブとパージ
  「データ・アーカイブ」は、Guardium システムによってキャプチャーされたデータをバックアップします。 データ・アーカイブを構成する際に、データ・パージの基準を指定することもできます。
- Guardium Installation Manager
  Guardium Installation Manager (GIM) を使用して、管理対象システム上で Guardium コンポーネントのインストールと保守を行います。

親トピック: 始めに

照会およびレポート

Guardium 照会は、収集したデータから取得される情報セットを記述します。 レポートは、Guardium 照会によって識別されるデータの表示方法を定義します。

Guardium 照会は、収集したデータから取得される情報セットを記述します。 照会は、エンティティー、フィールド、および条件の 3 つの要素で構成されます。 エンティティーは照会の範囲を定義し、フィールドは照会によって返されるデータの列をリストし、条件はデータに対して突き合わせるテストを定義します (より大きい、より小さい、含むなど)。

レポートは、照会で収集したデータの表示方法を定義するものです。 デフォルトのレポートは表形式のレポートであり、照会の構造を反映して、各属性が別個の列に表示されるものになります。 すべてのランタイム・パラメーターと表形式レポートの表示構成要素はカスタマイズ可能です。

親トピック: 重要な概念とツール

アクセス制御

Guardium には、データベース・クライアントとデータベース・サーバー間のデータ・アクセスを簡単に表示する手段として、アクセス・マップが用意されています。

アプリケーションとツールによるデータ・アクセスは、さまざまな次元 (アクセスされているデータ、アクセスの方法、SQL 呼び出しの実行回数など) に従って分類することができます。 エンタープライズ環境では、データベース・アクセスを適切に処理することが非常に重要です。 このような要件が生じる要因として、コンプライアンス主導で管理する必要があるため、さらにはデータベース環境を調整および最適化する必要があるために、データベース・アクセスについて理解し保護する必要が高まっているという状況があります。 エンタープライズ環境にはさまざまなデータベースと非常に多くのデータベース・クライアントが存在する場合があるため、データ・アクセス・パスを適切に処理することが困難になる場合があります。

「適用状態トポロジー」ビューおよび「適用状態表」ビューには、環境内のシステム間のデータ・フロー関係が表示されます。これらのビューにより容易に、問題のあるシステムを識別し、根本的な問題を調査できます。トポロジー・ビューにアクセスするには、「管理」 > 「システム・ビュー」 > 「適用状態トポロジー」にナビゲートします。表ビューにアクセスするには、「管理」 > 「システム・ビュー」 > 「適用状態表」にナビゲートします。

親トピック: 重要な概念とツール

ユーザー・ロール

ロールは、同じアクセス権を共有する Guardium ユーザーのグループを定義します。

ロールがアプリケーションまたは項目の定義 (特定の照会など) に割り当てられると、そのロールを割り当てられた Guardium ユーザーのみがそのコンポーネントにアクセスできます。 どのセキュリティー・ロールもコンポーネント (レポートなど) に割り当てられていないと、そのコンポーネントを定義したユーザーおよび admin ユーザーのみがそれにアクセスできます。

インストール時に、Guardium はデフォルトのロールセットおよびデフォルトのユーザー・アカウントのセットを使用して構成されます。 Guardium アクセス・マネージャーでは、新しいロールを作成したり、必要に応じて既存のロールを変更したりすることができます。

親トピック: 重要な概念とツール

グループ

Guardium では、エレメントのグループ化がサポートされているため、ポリシーの作成と管理を簡単に行い、分かりやすいレポートを表示することができます。

グループ化によって、 ポリシー作成および照会定義のプロセスが簡略化されます。 多くの場合、同じタイプのエレメントをグループ化すると便利です。グループ化することにより、レポートの情報をより分かりやすい形式で表示することができます。グループはすべてのサブシステムによって使用され、すべてのユーザーが単一のグループ・セットを共用します。

グループ化の例として、従業員の機密情報が含まれている個別のデータ・オブジェクトが社内に 25 個あり、これらの項目に対するすべてのアクセス権についてレポートする必要があるとします。 25 項目それぞれについてテストする、非常に長い照会を編成することができます。 あるいは、これらの 25 オブジェクトを含んだ、「sensitive employee info」という名前の単一のグループを定義することもできます。その方法では、照会またはポリシー・ルール定義において、オブジェクトがそのグループのメンバーであるかどうかのテストのみが必要とされます。

グループには、その他にも、グループの構成変更時に、保守要件が緩和されるという利点があります。 上記の例では、「sensitive employee info」グループにさらに 2 つのオブジェクトを追加する必要があると社内で決定した場合、更新する必要があるのはグループ定義だけです。そのグループを参照するすべての照会、レポート、ポリシーを更新する必要はありません。

親トピック: 重要な概念とツール

データのアーカイブとパージ

「データ・アーカイブ」は、Guardium システムによってキャプチャーされたデータをバックアップします。 データ・アーカイブを構成する際に、データ・パージの基準を指定することもできます。

「データ・アーカイブ」と「結果アーカイブ」という 2 つのアーカイブ操作があります。これらのアーカイブ操作へのパスは、「管理」>「データ管理」>「データ・アーカイブ」または「結果アーカイブ (監査)」です。

データ・アーカイブ
「データ・アーカイブ」を使用すると、通常、キャプチャーされた日の最後にデータがアーカイブされます。これにより、災害が発生した場合、その日のデータだけが失われることになります。 データのパージは、アプリケーション、ビジネス要件、監査要件に基づいて行われますが、ほとんどの場合、データはマシン上に 6 カ月以上保持することができます。

結果アーカイブ
「結果アーカイブ」は、監査タスクの結果 (レポート、アセスメント・テスト、エンティティー監査証跡、プライバシー・セット、分類プロセス) だけでなく、表示とサインオフの証跡と、ワークフロー・プロセスからの調整コメントもバックアップします。 結果セットは、ワークフロー・プロセスの定義に従ってシステムからパージされます。

統合環境では、データはコレクター、アグリゲーター、またはその両方のロケーションからアーカイブできます。 データは、一度だけアーカイブするのが最も一般的です。 アーカイブ元となるロケーションは、ユーザーの要件に応じて異なります。

親トピック: 重要な概念とツール

Guardium Installation Manager

Guardium Installation Manager (GIM) を使用して、管理対象システム上で Guardium コンポーネントのインストールと保守を行います。

GIM コンポーネントには、Guardium システムの一部としてインストールされる GIM サーバーと、モニターするデータベースとファイル・サーバーをホストするサーバー上にインストールされている必要がある GIM クライアントがあります。インストールされた GIM クライアントは、GIM サーバーと連携して以下のタスクを実行します。

- インストールされたソフトウェアの更新がないか検査する
- 新規ソフトウェアを転送およびインストールする
- ソフトウェアをアンインストールする
- ソフトウェア・パラメーターを更新する

中央マネージャーとして構成されている Guardium システムが現在の環境に存在する場合は、GIM サーバーとして使用する Guardium システムを決定する必要があります。 中央マネージャーなどの単一の Guardium システムからすべての GIM クライアントを管理することも、複数の Guardium システムから GIM クライアントをグループ単位で管理することもできます。 単一の Guardium システムからすべての GIM クライアントを管理する場合は、単一のインターフェースですべての GIM クライアントの状況を表示し、関連するタスクを実行することができます。個別の Guardium システムから GIM クライアントをグループ単位で管理する場合は、各システムを使用して、そのシステムで管理される GIM クライアントを処理できますが、全体的なビューや、環境全体にわたるビューは使用できません。

親トピック: 重要な概念とツール

ディスカバー

ディスカバリーとは、セキュリティーやコンプライアンス上の目的でトラッキングする必要のある、環境内のオブジェクトを見つけて識別するプロセスを指します。

ディスカバリーは、特権ユーザー、機密データ、データ・ソースなどの重要なオブジェクトを検出するプロセスです。分類は、セキュリティーやコンプライアンス上の目的でディスカバーされたものを適切に識別するプロセスです。これらのディスカバリー・プロセスと分類プロセスは、大規模な組織で合併や買収、レガシー・システムによって、新しいオブジェクトが非構造化形式または予測不能な方法で現行環境に導入される場合に重要となります。Guardium® は、有効なセキュリティー・ポリシーを施行してコンプライアンスを実現できるようにこれらのオブジェクトを現行環境に取り込むのに役立ちます。

一般的なシナリオには、機密データのディスカバリーがあります。機密データとは、クレジット・カード番号、個人の金融データ、社会保障番号、その他特殊な取り扱いを必要とする情報など、規制が掛けられている情報を指します。Guardium では、2 種類の方法で機密データをディスカバーできます。1 つは「機密データのディスカバー」ワークフロー・ビルダーを使用する方法で、もう 1 つはポリシー・ビルダーを他の Guardium ツールとともに使用する方法です。 「機密データのディスカバー」ワークフロー・ビルダーは、機密データのディスカバリーおよび分類プロセスを設定するための包括的なツールとして設計されています。これを使用して、ディスカバリー・ルールの指定、ディスカバーされたデータに対して実行するアクションの定義、スキャンするデータ・ソースの指定、レポートの配布、自動スケジュールでのワークフローの実行を行います。上級者用に、より細分度の高いディスカバリー・ルールおよび分類ルールがポリシー・ビルダーでサポートされています。これらのルールは、既存のプロセスや Guardium アプリケーションに容易に取り込むことができます。

- データ・ソース
  データ・ソースには、データベースやリポジトリーに関する情報 (データベースのタイプ、リポジトリーの場所、関連付けられる可能性のある資格情報など) が格納されます。Guardium アプリケーションでデータ・ソースを使用するには、データ・ソースを定義する必要があります。
- クラウド・データベース・サービス保護
  クラウド・データベース保護は、クラウド・データベースにおける分類、脆弱性評価、およびオブジェクト監査を提供します。
- データベース・オートディスカバリー
  オートディスカバリー・アプリケーションは、サーバーをスキャンおよびプローブしてオープン・ポートを調べ、ネットワークに対して不明な接続や望ましくない接続が行われるのを防ぎます。オートディスカバリー・プロセスはオンデマンドで実行することも、定期的に実行されるようスケジュールすることもできます。
- 分類
  分類ポリシーと分類プロセスは、Guardium が機密データ (クレジット・カード番号、社会保障番号、個人の金融データなど) をディスカバーして処理する方法を定義します。
- 機密データのディスカバー
  機密データをディスカバーして分類するためのエンドツーエンドのシナリオを作成します。
- 正規表現
  正規表現を使用して、データに含まれる複合パターンを求めてトラフィックを検索することができます。

- ファイル・サーバー内での機密データのディスカバーおよび分類
  ファイル・アクティビティー・モニターは、UNIX ファイル・サーバーおよび Windows ファイル・サーバー上の機密データの保全性と保護を確保します。
- 資格最適化
  資格最適化は、ジョブを効率的に実行するために必要な資格をユーザーに提供する上でのデータベース管理者のロールと、システムの脆弱性を防ぐために資格をできる限り正確に、かつ可能な限り最小限に抑える上でのセキュリティーのロールの間を仲介するものです。

データ・ソース

データ・ソースには、データベースやリポジトリーに関する情報 (データベースのタイプ、リポジトリーの場所、関連付けられる可能性のある資格情報など) が格納されます。Guardium® アプリケーションでデータ・ソースを使用するには、データ・ソースを定義する必要があります。

- データ・ソース定義の作成
  「データ・ソース・ビルダー」を使用して、Guardium アプリケーションで使用するデータ・ソース定義を作成します。
- 既存のデータ・ソースの操作
  データ・ソース定義を作成したら、そのデータ・ソースのコピー、変更、または削除を行うことができます。
- データ・ソースについてのレポート
  Guardium は、現行環境内のデータ・ソースと、それらに加えられた変更内容についてのレポートを提供します。
- サービス名を使用したデータ・ソースの定義
  カスタム URL を使用することで、ユーザーがサービス名を使用して Oracle データベースに接続できるようにするデータ・ソースを定義できます。
- KDC 定義の管理
  データ・ソースが Kerberos を使用する認証を必要とする場合、接続を確立する前に、Guardium が Kerberos チケットを取得するために必要な情報を指定できます。

親トピック: ディスカバー

データ・ソース定義の作成

「データ・ソース・ビルダー」を使用して、Guardium アプリケーションで使用するデータ・ソース定義を作成します。

このタスクについて

データ・ソース定義を作成するための一般的なプロセスは 2 つあります。1 つは、「データ・ソース・ビルダー」からデータ・ソース定義を追加した後、そのデータ・ソースを使用するアプリケーションを指定する方法です。もう 1 つは、使用したいアプリケーションに移動してから、そのアプリケーション内でデータ・ソースを作成する方法です。特定のアプリケーション内でデータ・ソース定義を追加するためのナビゲーションは、選択したアプリケーションや、選択したデータベースのタイプによって異なります。例えば、監査データベースを作成する場合は、「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「値変更監査データベースの作成」にナビゲートし、「データ・ソースの追加」をクリックします。

手順

- 「データ・ソース・ビルダー」を開きます。これを行うには、「設定」 > 「データ・ソース定義」にナビゲートします。
- ⊕ をクリックして、データ・ソース定義を追加します。
- 「データ・ソースの作成」ダイアログを使用して、今後使用するために保管するデータ・ソースに関する情報を指定します。選択したアプリケーションおよびデータベースと、使用するデータ・ソースのタイプに応じて、このダイアログは若干異なります。
  1. 「アプリケーション・タイプ」を選択します。
  2. データ・ソースに固有の「名前」を入力します。
  3. 「データベース・タイプ」メニューから、データベースまたはファイル・タイプを選択します。アプリケーションによっては、データ・ソースがテキスト・ファイルではなくデータベースでなければならない場合があります。選択したデータベースのタイプによっては、パネル上の一部のフィールドが無効になったり、ラベルが変更されたりすることがあります。 例えば、「資格情報の割り当て」はオプションまたは必須のどちらかの可能性があります。必須の場合、それは無効になり、「ユーザー名」フィールドと「パスワード」フィールドが必須になります。オプションの場合、「ユーザー名」と「パスワード」は、「資格情報の割り当て」を選択するまで無効になっています。
  4. 「データ・ソースの共有」を選択し、すべてのアプリケーション間でデータ・ソース定義を共有します。データ・ソースを共有しない場合、作成した定義は選択したアプリケーションのみで使用可能になります。
  5. オプションで、追加の資格情報を構成します。
     - SSL の使用: SSL を使用する場合に選択します。次に、オプションで 「サーバーの SSL 証明書をインポートします」を選択し、「証明書の追加」をクリックして証明書を選択します
     - LDAP の使用: LDAP を使用する場合に選択します。次に、「資格情報の割り当て」をクリックして、「ユーザー名」と「パスワード」を入力します
     - Kerberos を使用: 事前定義の Kerberos 構成を使用する場合に選択します。「Kerberos 構成」を選択して、「レルム」および「KDC」を入力します。データ・ソースはこれを自身の KDC およびレルムと比較して、一致することを確認します。
  6. 「パスワードの保存」を選択し、Guardium アプライアンスへの認証資格情報の保存と暗号化を行います。(オンデマンドではなく) スケジュールされたタスクとして実行されるアプリケーションでデータ・ソースを定義する場合は、「パスワードの保存」が必須になります。「パスワードの保存」を選択した場合は、ログイン名とパスワードが必須になります。
  7. 「ログイン名」と「パスワード」に資格情報を入力します。
  8. 「ホスト名/IP」フィールドに、データ・ソースのホスト名または IP アドレスを入力します。
  9. 以下の表を使用して、データ・ソース・タイプに応じた「ポート」を入力します。

  データ・ソース・タイプとポート番号の表

データベース・タイプ	ポート番号
Aster データ	2046
Db2	50000 Db2 UDB の場合、Guardium は count_big(*) をサポートします。非常に大容量の表では、標準の count(*) は失敗する可能性があります。
Db2 for i	446

データベース・タイプ	ポート番号
Db2 for z/OS	446
GreenplumDB	5432
Hadoop	21000-21050
Informix	1526
MS SQL Server (動的ポート) および MS SQL Server (DataDirect - 動的ポート)	グレー表示のポート番号 - このデータ・ソースを使用することで、定義済みのポート値のないクライアント、または動的関数が MS SQL Server データベース・サーバーから有効化されているクライアントは、MS SQL Server データベースに動的に接続できます。 動的ポートを定義するには、MS SQL Server のデータベース・サーバーに移動して、動的ポート・タイプに 0 を定義し、デフォルトでポート 1433 の TCP/IP を削除してください。 動的ポートの値を 0 に設定して、サービスを再始動すると、動的 IP が設定されます。 MS SQL の場合、Guardium は count_big(*) をサポートします。非常に大容量の表では、標準の count(*) は失敗する可能性があります。 MS SQL Server 用の DataDirect ドライバー 以前、NTLM および NTLMv を使用して Windows 認証をサポートするには、jTDS ドライバーをダウンロードする必要がありました。 今後は、Guardium DataDirect ドライバーがこれを許可します。 パラメーター Guardium ユーザーが Windows 認証を使用する場合、次のパラメーターを接続プロパティーに追加します。 domain=domain_name;AuthenticationMethod=ntlmjava Windows 認証に NTLMv2 を使用している場合、次のパラメーターを接続プロパティーに追加します。 domain=domain_name;AuthenticationMethod=ntlm2java AuthenticationMethod 目的 接続の確立時にドライバーが使用する認証方式を決定します。指定された認証方式がデータベース・サーバーによってサポートされていない場合、接続は失敗し、ドライバーは例外をスローします。 有効な値 auto | kerberos | ntlm | ntlmjava | ntlm2java | userIdPassword 注意 LMCompatabilityLevel が NTLMv2 に制限されているときに AuthenticationMethod=ntlmjava を指定すると、エラーが返されます。LMCompatabilityLevel が NTLMv2 に制限されている場合、AuthenticationMethod を ntlm2java に設定する必要があります。 AuthenticationMethod=ntlmjava または AuthenticationMethod=ntlm2java を指定する場合、データベースを管理するドメイン・サーバーの名前を指定する必要があります。ドメイン・サーバーは、ドメイン・プロパティーを使用して指定できます。 ドメイン・プロパティーが指定されていない場合、ドライバーはユーザー・プロパティーからドメイン・サーバーを判別しようとします。ドライバーがドメイン・サーバー名を判別できない場合は、例外がスローされます。 ユーザー・プロパティーはユーザー ID を提供します。パスワード・プロパティーはパスワードを提供します。 値「type4」、「type2」、および「なし」は非推奨ですが、後方互換性のために認識されます。代わりに、kerberos、ntlm、および userIdPassword 値をそれぞれ使用してください。 NTLM 認証には、Microsoft SQL Server 2000、サービス・パック 3 以上が必要です。 Guardium ユーザーが Azeri_Cyrillic_100_CI_AS または Chinese_Hong_Kong_Stroke_90_CI_AS などの非標準のデータベース Unicode を使用している場合は、このパラメーターを接続プロパティーに追加します。 CodePageOverride=UTF-8 SSL (Force encryption=Yes) を使用している場合、以下を追加します。 encryptionMethod=SSL;validateServerCertificate=false
MS SQL サーバー (DataDirect)	1433
MongoDB	27017
MySQL	3306

データベース・タイプ	ポート番号
Netezza	5480
Oracle (DataDirect)	1521
PostgreSQL	5432
Sybase	4100
Sybase IQ	2638
Teradata	1025
テキスト	0
Text:HTTP	8000
Text:FTP	21
Text:SAMBA	445
Text:HTTPS	8443
N_A	0
MS SQL サーバー (オープン・ソース) (「強化」 > 「脆弱性評価」 > 「カスタム・アップロード」を使用して、これらの JDBC ドライバーをアップロードします。『サブスクライブしたグループのアップロード』を参照してください。)	1433
Oracle (オープン・ソース) (「強化」 > 「脆弱性評価」 > 「カスタム・アップロード」を使用して、これらの JDBC ドライバーをアップロードします。『サブスクライブしたグループのアップロード』を参照してください。)	1521
HIVE、HiveServer2	10000
HADOOP、Hive CLI は非推奨	9083
HIVE、Hue からの Impala	21050
HADOOP、Impala シェル	21000
HUE、Oracle Hue バックエンド	1521
HUE、MySQL Hue バックエンド	3306
HUE、PostgreSQL Hue バックエンド	5432
WEBHDFS	50070

注: SSL データ・ソースを使用して初めて接続しようとすると、接続のテスト中にこのエラーが発生することがあります。

エラー
接続に失敗しました
```
Could not connect to: 'jdbc:db2://su11u1x64t-va:55000/VA_DB' for user: '(DELETE ME) db2 10.1 SSL_DB2(Security
Assessment)'. DataSourceConnectException: Could not connect to: 'DB2 (DELETE ME) db2 10.1 SSL 9.70.146.39:55000' for
user: 'db2inst1'. Exception: com.ibm.db2.jcc.am.DisconnectNonTransientConnectionException: [jcc][t4][2030][11211]
[4.15.134] A communication error occurred during operations on the connection's underlying socket, socket input stream,
```

これは、メモリーにロードされた証明書の正しい鍵ストア・ファイルが GUI にないためです。これを修正するには、GUI を再起動してください。そうすると、このエラーが解決して、接続が成功するはずです。

10. データ・ソース・タイプに応じて、このダイアログの「ポート」の後のフィールドが若干異なります。
    - Db2 の場合は、データベース名を入力します。
    - Db2 iSeries または Oracle の場合は、サービス名を入力します。
    - Informix の場合は、Informix サーバー名を入力します。
    - テキスト以外のデータベース・タイプの場合は、「データベース」ボックスにデータベース名を入力します (Informix、Sybase、MS SQL サーバー、PostgreSQL、または Teradata の場合のみ)。Sybase または MS SQL サーバーの場合にこれをブランクのままにすると、デフォルトでマスターが使用されます。Sybase データベースの場合、「データベース」テキスト・ボックスにはデータベース名を指定するか、ブランクにした場合はマスターにデフォルト設定されます (これは「資格レポート」および「分類」の場合に機能します。VA の場合はデータベース・インスタンス名を使用してください。)
    - Db2、Db2 iSeries、または Oracle の場合は、「スキーマ」ボックスに使用する有効なスキーマ名を入力します。
    - テキスト・ファイルのデータベース・タイプの場合は、「ファイル名」ボックスにファイル名を入力します。
11. このデータ・ソースとの JDBC 接続を確立するために、追加の接続プロパティーを JDBC URL に含める必要がある場合にのみ、「接続プロパティー」ボックスを使用します。使用するフォーマットは、「property=value」である必要があります。このとき、プロパティーと値の各ペアはコンマで区切ります。
    - Roman8 をデフォルトの文字セットとする Sybase データベースの場合、次のプロパティーを入力します。 charSet=utf8
    - Oracle 暗号化接続の場合は、接続プロパティーを oracle.net.encryption_client=REQUIRED;oracle.net.encryption_types_client=RC4_40 (モニター対象インスタンスで必要とされる暗号化アルゴリズム (タイプを問わない) と置換) のように定義する必要があります。
    - 3DES168 暗号化には問題があることに注意してください。 3DES168 暗号化を使用するよう定義されたデータ・ソースは、SQL エラーの検出時に誤って「ORA-17401 プロトコル・エラー」または「ORA-17002 チェックサム・エラー」をスローします。その後、接続を閉じてから再度開くまで、接続が機能しなくなります。
    - Db2 暗号化接続の場合は、接続プロパティーを securityMechanism=13 のように定義する必要があります。
    - Db2 iSeries 接続の場合は、接続プロパティーを property1=com.ibm.as400.access.AS400JDBCDriver;translate binary=true のように定義します。
    - Db2 z/OS データ・ソースの場合、データベース・パフォーマンスを向上させるために、次の接続プロパティーを追加してください。 resultSetHoldability=2

- Oracle では、sys は Oracle デフォルト・ユーザーであり、データベース・インスタンスの所有者であり、かつスーパーユーザー特権を持ちます。これは Unix の root に似ています。 SYSDBA はロールであり、データベースの始動と停止やバックアップ/リカバリー操作の実行などの多くのハイレベルな管理操作を行うために必要な管理特権を持ちます。 このロール (SYSDBA) を他のユーザーに与えることもできます。 `sys as SYSDBA` 句は、sys ユーザーとして接続するのに必要な接続方式を参照します。
- Oracle 10 (sys as SYSDBA) のモニター値 (これは Oracle オープン・ソース・ドライバー用です) には、internal_logon=sysdba を入力します。
- DataDirect (Oracle ドライバー) の場合は SysLoginRole=sysdba を入力します。
- さらに、CRYPTO_CHECKSUM_TYPES を sqlnet.ora 内で使用する場合は、以下の例を使用してください。
- oracle.net.encryption_client=aes256;oracle.net.crypto_checksum_types_client=SHA1
- oracle.net.encryption_client=rc4_256;oracle.net.crypto_checksum_types_client=MD5
- oracle.net.encryption_client=aes256;oracle.net.crypto_checksum_types_client=MD5
- oracle.net.encryption_client=rc4_256;oracle.net.crypto_checksum_types_client=SHA1
- 例: OID と呼ばれる Oracle LDAP に対する認証を使用します。 必要な値は、LDAP サーバー・ホストまたは IP、LDAP サーバー・ポート、Oracle インスタンス名、およびレルムです。カスタム URL は、次のように正確に入力する必要があります。
  jdbc:guardium:oracle:@ldap://wi3ku2x32t4:389/on0maver,cn=OracleContext,dc=vguardium,dc=com

12. 必要に応じて、データ・ソースに対する「カスタム URL」接続文字列を入力します。 「カスタム URL」フィールドがブランクの場合は、他のデータ・ソース定義フィールドに入力したプロパティー (ホスト、ポート、インスタンスなど) を使用して接続が行われます。
    重要:
    - 「カスタム URL」フィールドを Oracle オープン・ソース形式で指定する場合は、`jdbc:guardium:oracle://;SID=<SID>` と指定します。
    - Oracle Advanced Security を有効にして Oracle データベースのデータ・ソースを作成する場合は、データ・ソース定義の「カスタム URL」フィールドに `EncryptionLevel=required` と指定します。
    -
13. 「拡張オプションの表示」をクリックして、ロールおよび CAS オプションを表示します。
14. オプションで「ロール」をクリックして、データ・ソースのロールを割り当てます。データ・ソースにロールを追加すると、ユーザーはデータ・ソース構成を表示できます。所有者および管理者だけがデータ・ソースを変更および削除できます。
15. オプションで、CAS 情報を入力を入力します。

    a. ベンダーはインストールに柔軟性を持たせるよう工夫しているため、データ・ソース定義で必要な 2 つのフィールドをユーザーが決めるようになっています。

    CAS では、UNIX でデータベース・ツールの一部を実行するためのデータベース・インスタンス・アカウントと、モニター対象のファイルを検出するためのデータベース・インスタンス・ディレクトリーの名前の、2 種類の情報が必要です。一般的に、データベース・インスタンス・アカウントおよびディレクトリーがデータ・ソース定義に正しく入力されない場合、CAS でデータを検出できなかったテストで使用できる `CAS データがない` というメッセージが表示されます。

    CAS により使用される「データベース・インスタンス・アカウント」(ソフトウェア所有者) および「データベース・インスタンス・ディレクトリー」(データベース・ソフトウェアがインストールされたディレクトリー) を入力します。

    以下に、データ・ソース用の CAS 情報を入力するために必要な情報を見つける方法の推奨事項を示します。この情報は、インストール済み環境によって異なる場合があります。UNIX で使用する方法の 1 つに、特定のデータベース・インストール済み環境で /etc/passwd ファイルをリストして、データベース・インスタンス・アカウントおよびインスタンス・ディレクトリーを指定できるよう使用するといった方法があります。インストール中の任意の時点で、インスタンス・ディレクトリー (ORACLE_HOME など) を指定する環境変数が、データベース・インスタンス・アカウントに定義されます。この場合、データ・ソース定義フォームの「データベース・インスタンス・ディレクトリー」フィールドに「$ORACLE_HOME」と入力します。この変数が展開され、データベース・サーバー上の正しいディレクトリー名が検出されます。
    注: 複数のディレクトリーを検索するには、「データベース・インスタンス・ディレクトリー」に複数のファイル・パスを定義します。この例は、MongoDB の行を参照してください。

表 1. データベース・インスタンス

データベース・タイプ	データベース・インスタンス・アカウント	データベース・インスタンス・ディレクトリー / 追加ヒント
Db2	通常は db2inst1	db2inst1 のホーム・ディレクトリーまたは Windows の C:¥Program Files¥IBM¥SQLLIB。 プログラム db2cmd.exe は、システム・パス上、またはデータベース・インスタンス・ディレクトリーの「bin」サブディレクトリー内にある必要があります。
Informix	通常は informix	UNIX の「/opt/IBM/informix」など、または「C:¥Program Files¥IBM¥Informix」。環境変数 INFORMIXDIR を定義できます。 プログラム <servicename>.cmd はシステム・パス上にある必要があります。ここで、<servicename> はデータ・ソース定義の「Informix サーバー」に入力されている値です。

データベース・タイプ	データベース・インスタンス・アカウント	データベース・インスタンス・ディレクトリー / 追加ヒント
MongoDB	通常は mongodb または mongos	MongoDB では、データベース・インスタンス・ディレクトリーに複数のパスを指定する必要があります。パスを区切るにはパイプ記号 (|) とスペースを使用します。 例えば、/var/lib/mongo | MongoBinary=/usr/bin | dbpath=/var/lib/mongo | logpath=/var/log/mongodb | keytab=/home/keytab | dbdumppath=/opt/backup | sslpath=/etc/ssl | keyfile=/home/mongod/mongo_server.keyfile です。 /var/lib/mongo パスは mongo ユーザーのホーム・パスなので必須です。 MongoBinary=/usr/bin は、mongo バイナリーのパスです。変数 (大/小文字の区別あり) を指定し、その後に等号とパスを指定する必要があります。 dbpath=/var/lib/mongo は、データ・ファイルのパスです。このケースでは、偶然 MongoDB ホーム・ディレクトリーと同じになっています。 logpath=/var/log/mongodb は、MongoDB ログのパスです。 keytab=/home/keytab は、MongoDB キータブ・ファイルのディレクトリーです。 dbdumppath=/opt/backup は、MongoDB バックアップ・ダンプのディレクトリーです。 sslpath=/etc/ssl は、MongoDB SSL ファイルのパスです。 keyfile=/home/mongod/mongo_server.keyfile は、MongoDB 鍵ファイルを指しています。 リストされたパスをすべて定義する必要はありません。定義されていないパスは分析されません。
Oracle	通常は oracle、またはバージョンが特定された oracle9 または oracle10 など	例えば、UNIX の/home/oracle9や、Windows のC:¥oracle¥product¥10.2.0¥db_1 です。環境変数 ORACLE_HOME を定義できます。 Windows では、環境変数 PERL5LIB および ORACLE_HOME を定義する必要があります。また、プログラム「opatch.bat」はシステム・パス上にある必要があります。
SQL サーバー	Windows 認証が使用されている場合を除き、必要ありません。Windows 認証が使用されている場合は、Windows 認証で受け入れられる「ドメイン/ユーザー名」という形式である必要があります。	SQL サーバーで CAS を使用するために「データベース・インスタンス・ディレクトリー」にデータを取り込むには、2 つの方法があります。 脆弱性評価のテストにデータ・ソースを使用している場合は、この列にデータベース・インスタンス・ホーム・ディレクトリーを設定する必要があります。 例 MSSQL2000、64 ビット・サーバー上の名前インスタンス C:¥Program Files (x86)¥Microsoft SQL Server¥MSSQL$MSSQL2000 MSSQL2000、32 ビット・サーバー上のデフォルト・インスタンス C:¥Program Files¥Microsoft SQL Server¥MSSQL MSSQL2005 C:¥Program Files¥Microsoft SQL Server¥MSSQL.1¥MSSQL MSSQL2008 C:¥Program Files¥Microsoft SQL Server¥MSSQL10.MSSQLSERVER¥MSSQL 脆弱性評価以外のテストで、CAS によるファイルまたはレジストリーのモニター用にデータ・ソースを使用している場合があります。 その場合、この列は「Program Files」の「Microsoft SQL Server」ディレクトリーになります。 例: C:¥Program Files (x86)¥Microsoft SQL Server または C:¥Program Files¥Microsoft SQL Server 注: 脆弱性評価テストおよび CAS によるファイルのモニターを行う場合は、データ・ソースが 2 つ必要です。
Sybase	通常は「sybase」	UNIX の場合は /home/sybase、Windows の場合は C:¥sybase です。環境変数 SYBASE を定義できます。
MySQL		環境変数 MYSQL_HOME を定義できます。 注: データベース名が Unicode の MySQL データ・ソースはサポートされていません。MYSQL のデータ・ソース名は ASCII でなければなりません。

データベース・タイプ	データベース・インスタンス・アカウント	データベース・インスタンス・ディレクトリー / 追加ヒント
Teradata		必要ありません。インストール済み環境の構造はすべて同じように見えます。
Netezza		必要ありません。インストールは、すべてのマシンで同じロケーションにあります。
PostgreSQL		これは、最も柔軟なインストールです。ユーザーは、Postgres データベース・サーバーに 2 つの環境変数を定義する必要があります。PostgreSQL_BIN はインストールのバイナリーのロケーション、PostgreSQL_DATA はデータのロケーションである必要があります。

注: 「データベース・インスタンス・ディレクトリー」フィールド内で環境変数を使用する場合は、データベース・サーバーでその環境変数が定義されている必要があります。

b. データ・ソースの「重大度分類」 (または影響レベル) を選択します。レポートや結果の表示中には、重大度分類を使用してデータ・ソースのソート、フィルタリング、フォーカスを行うことができます。
c. 「保存」をクリックして、データ・ソース定義を保存します (定義が保存されるまで、ロールまたはコメントを追加できません)。
d. オプションで「コメントの追加」をクリックして、定義にコメントを追加します。
e. オプションで「接続のテスト」をクリックして、定義したデータ・ソースの接続をテストします。
f. 定義が完了したら、「閉じる」をクリックします。

親トピック: データ・ソース

既存のデータ・ソースの操作

データ・ソース定義を作成したら、そのデータ・ソースのコピー、変更、または削除を行うことができます。

手順

- 「データ・ソース・ビルダー」を開きます。これを行うには、「設定」 > 「データ・ソース定義」にナビゲートします。
- 「アプリケーション選択」メニューに、データ・ソース定義を使用できるアプリケーションがすべてリストされます。 変更したいデータ・ソースが作成された対象のアプリケーションを選択し、「次へ」をクリックして「データ・ソース・ファインダー」に進みます。

親トピック: データ・ソース

データ・ソースのコピー

手順

- 「データ・ソース・ファインダー」からコピーするデータ・ソースを選択し、「コピー」をクリックします。
- データ・ソース定義の作成時に入力した情報が「データ・ソース定義」ダイアログに表示され、元のデータ・ソース名の前に「copy Of」と表示されます。 必要なフィールドに変更を加えます。
- 「適用」をクリックし、コピーしたデータ・ソースを保存します。

データ・ソースの変更

手順

- 「データ・ソース・ファインダー」から変更するデータ・ソースを選択し、「変更」をクリックします。
- データ・ソース定義の作成時に入力した情報が「データ・ソース定義」ダイアログに表示されます。 必要なフィールドに変更を加えます。
- 「適用」をクリックし、データ・ソースに加えた変更内容を保存します。

データ・ソースの削除

手順

「データ・ソース・ファインダー」から削除するデータ・ソースを選択し、「削除」をクリックします。

データ・ソースについてのレポート

Guardium® は、現行環境内のデータ・ソースと、それらに加えられた変更内容についてのレポートを提供します。

手順

- 「データ・ソース」レポートを開きます。これを行うには、「レポート」 > 「レポート構成ツール」 > 「データ・ソース」にナビゲートします。 表示される表に、すべてのデータ・ソースと、各データ・ソース定義に保管されている情報がリストされます。
- 表内のセルを右クリックすると、「データ・ソース・バージョン履歴」と「呼び出し」の 2 つのオプションが表示されます。
  - データ・ソース定義に加えられた変更内容を表示するには、「データ・ソース・バージョン履歴」をクリックします。
  - データ・ソースに使用可能な API のいずれかを選択して実行するには、「呼び出し」をクリックします。

  注: 鉛筆のアイコンをクリックすると、データ・ソース・レポートのランタイム・パラメーターと表示パラメーターをカスタマイズできます。

親トピック: データ・ソース
関連概念:
GuardAPI データ・ソース関数

サービス名を使用したデータ・ソースの定義

カスタム URL を使用することで、ユーザーがサービス名を使用して Oracle データベースに接続できるようにするデータ・ソースを定義できます。

このタスクについて

カスタム URL のほか、ホスト名、ポート、サービス名を入力する必要があります。

手順

1. Oracle サービス名を決定します。 次のようなコマンドを使用できます。

```
SQL> set line size 5000;
SQL> select host_name, instance_name from v$instance;
SQL> select name from v$database;
SQL> show parameter service
```

「値」列に表示される名前を使用します。
2. 適切な Oracle JDBC シン・ドライバーを Guardium システムにロードします。
   a. 次の URL から、Oracle データベース用のドライバーを見つけてダウンロードします。http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-112010-090769.html
   b. 「カスタム・アップロード」ウィンドウを開きます。これを行うには、「強化」 > 「脆弱性評価」 > 「カスタム・アップロード」にナビゲートします。
   c. 「Oracle JDBC ドライバーのアップロード」というタイトルのセクションを見つけます。 「参照」をクリックし、ファイルをダウンロードした場所を参照します。「すべてにオープン・ソース・ドライバーを使用」をクリックします。
   d. アップロードが完了したら、Guardium ユーザー・インターフェースを再始動します。
3. このデータベースのデータ・ソースを定義します。
   a. 「データ・ソース・ビルダー」を開きます。これを行うには、「設定」 > 「データ・ソース定義」にナビゲートします。
   b. 「アプリケーション選択」メニューに、データ・ソース定義を使用できるアプリケーションがすべてリストされます。 変更したいデータ・ソースが作成された対象のアプリケーションを選択し、「次へ」をクリックして「データ・ソース・ファインダー」に進みます。
   c. 「サービス名」フィールドにサービス名を入力します。「カスタム URL」フィールドに、「`jdbc:oracle:thin@//hostname:port/svcname`」と入力します。ここで、hostname と port はデータベースの標準値、svcname はサービス名 (「サービス名」フィールドに入力した値と同じ) です。

親トピック: データ・ソース

KDC 定義の管理

データ・ソースが Kerberos を使用する認証を必要とする場合、接続を確立する前に、Guardium が Kerberos チケットを取得するために必要な情報を指定できます。

このタスクについて

Guardium V.10.1.3 以降、KDC を特定のデータ・ソースまたは管理対象ユニット・グループに割り当てて、Guardium 認証を Mongo データベースおよび Hive データベースに提供できます。アプライアンスは JDBC 接続を介してチケットを取得するため、ユーザーは自分自身でチケットを取得する必要はありません。これは、アプライアンス自体が使用するように設定されているものとは無関係であることに注意してください。

最大 5 つの Kerberos 鍵配布センター (KDC) を中央マネージャーで定義し、1 つをスタンドアロンの Guardium で定義できます。鍵配布センターを Guardium に追加するには、次のように指定します。

- レルム: 大文字のドメイン・ネーム
- KDC: Kerberos サーバーのホスト名
- Kerberos チケットの暗号化タイプ
  - des-cbc-md5
  - des-cbc-crc
  - rc4-hmac
  - des3-cbc-sha1
  - aes128-cts-hmac-sha1-96
  - aes256-cts-hmac-sha1-96

  デフォルトは aes256-cts-hmac-sha1-96 です。これは最も安全な暗号化タイプです。

手順

1. 「設定」 > 「ツールとビュー」 > 「Kerberos 構成」をクリックします。
2.  をクリックして、新しい構成を作成します。
3. 「名前」、「KDC」、および「レルム」を指定します。
4. 「暗号化タイプ」を指定します。デフォルトは aes256-cts-hmac-sha1-96 です。
5. 「保存」をクリックします。

次のタスク

Kerberos KDC を作成したら、データ・ソースのセットアップを構成するときに、それを選択できます。

親トピック: データ・ソース

クラウド・データベース・サービス保護

クラウド・データベース保護は、クラウド・データベースにおける分類、脆弱性評価、およびオブジェクト監査を提供します。

Guardium とクラウドの接続を一度セットアップすると、以下を実行できるようになります。

- データベース・インスタンスを検出し、それらを Guardium にカタログします。
- 分類プロセスにカタログされたデータ・ソースを割り当てるか、新しいプロセスを作成します。分類はクラウド・データベースに対して実行され、定義されたルールに従ってオブジェクトを識別します。
- カタログされたデータ・ソースを脆弱性評価プロセスに割り当てるか、新しいプロセスを作成します (有効な VA ライセンスが必要)。VA はクラウド・データベースに対して実行され、そのデータを Guardium レポートで使用します。
- DB 監査の有効化: Oracle 標準監査データが、インストールされたポリシーに従って、Guardium レポート用にクラウドからプルされます。(https://docs.oracle.com/cd/B28359_01/server.111/b28337/tdpsg_auditing.htm#TDPSG50051 の Oracle 定義を参照してください)。
- オブジェクト監査を有効にします (Oracle の監査証跡)。分類結果を確認し、オブジェクト監査の対象とするオブジェクトを選択します。(DB 監査が有効になっている必要があります)。オブジェクト監査は、オブジェクトに対して実行されるすべてのアクティビティーを追跡します。Guardium はこのデータをレポートや調査ダッシュボードなどに使用します。Guardium は、データ・ソース別にオブジェクトを自動的に追加するように構成できます。さらに、そのすべてのデータ・ソースで継承される、アカウントごとのデフォルトも設定できます。 これは監査を必要としていて、それ以上の評価は必要ないオブジェクトを持つデータベースに特に有用です。 分類プロセスでの検出が予期される妥当な上限を設定します。分類に誤りがあった場合でもオブジェクトがオーバーフローしないようにするために、設定値は高すぎないようにします。(オーバーフローはデータベースのパフォーマンスに影響を与える可能性があります)。

クラウド DB で Guardium 機能を実行するには、AWS 権限が必要です。AWS IAM 定義を参照してください。

オンプレミス・データベースでは、データベースにインストールされている S-TAP は、すべてのデータベース・トラフィックを Guardium システムに送信します。 クラウド環境では、Guardium はクラウド DB からログ・ファイルをプルし、S-TAP データと同じようにデータを処理します。相違点として、S-TAP ではすべてのデータベース・アクティビティーが記録されるのに対し、クラウド環境では選択した表のみが監査されます。クラウドからのデータの取得が多少遅れる可能性があるという相違点もあります。

監査対象のデータベースおよびオブジェクトに対するアクティビティーは、データベース・ログに書き込まれます。ログ・アクティビティーの量は、モニター対象項目の数により増大します。大量のログ・アクティビティーは、データベースのパフォーマンスに影響を与える可能性があります。すべての関連データが収集されており、なおかつシステムが過負荷になっていないことを確認する必要があります。

CM 環境内およびスタンドアロンの Guardium コレクター上で、クラウド・データベース・サービス保護を実行できます。

クラウド DB サービス保護のコンテキストでは、データベースはクラウド上のデータベースのことであり、データ・ソースは Guardium カタログ・データベースのことです。

1 つの Guardium システムのみが、任意の 1 つの DB の DB 監査およびオブジェクト監査を所有できます。他の Guardium システムも同じクラウド・アカウントにアクセスし、DB 詳細を表示できますが、DB 監査を無効にしたり、オブジェクト監査データにアクセスしたりすることはできません。例えば、ある Guardium システムがダウンして復旧を予期できない場合は、そのシステムから別のシステムに所有権を移動することができます。

すべての AWS RDS データベース・エンジンで、ディスカバリー、分類、および VA がサポートされます。

DB 監査の制限事項

- RDS 定義を (例えば、DB インスタンスの削除や資格情報の変更において) 最新の状態に保つ必要があります。
- Guardium v10.1.4 は、AWS クラウド上の Oracle V.11 データベースのみをサポートします。
- 戻りデータのパターンの編集やテストなどの抽出ルールはサポートされません。
- バインド変数値のロギングや影響を受けるレコードなどの戻りデータはサポートされません。
- S-GATE ターミネート、無視、照会再書き込みなど、S-TAP と対話するルール・アクションはサポートされません。
- 失敗したログインは Oracle のネイティブ監査ではキャプチャーされないため、Guardium に転送されません。
- Oracle ネイティブ監査でキャプチャーされないステートメント (例えば、構文エラーが含まれているステートメント) は、モニターできません。

- クラウド・データベース・サービス保護のワークフロー
- AWS IAM 定義
  必要な権限に応じて、AWS アカウントの IAM ポリシーを定義します。
- クラウド・アカウントの作成、変更、削除
  DB 資格情報を使用して、クラウド・データベース・サービス・アカウントを作成するか、クラウド・アカウントを変更または削除します。
- クラウド・データベースのディスカバー
  検索するリージョンを選択することで、クラウド・アカウント内のデータベースをディスカバーします。
- データベースのカタログおよび管理
  Guardium でデータ・ソースを作成するためのデータベースをカタログし、ユーザーとパスワードを変更し、データベース構成を更新します。
- 分類および脆弱性評価の管理
  データ・ソースを既存の分類プロセスまたは脆弱性評価プロセスに割り当てます。または新規プロセスを作成します。
- データベース監査の構成
  データベース上での監査を有効にし、オブジェクト監査データを Guardium がプルできるようにします。 分類に自動的に追加されるオブジェクトの制限を変更し、コレクターを変更します。
- オブジェクト監査の管理
  管理しているデータベースの分類プロセスによって識別された潜在的な機密オブジェクトを表示し、これらのオブジェクトに実行されるすべてのアクティビティーをモニターするために、選択したオブジェクトに対するオブジェクト監査を有効にします。

親トピック: ディスカバー

クラウド・データベース・サービス保護のワークフロー

このタスクについて

これは一般的なワークフローです。具体的なワークフローは、クラウド・データベース監査の目的に応じて異なります。

手順

1. クラウド・アカウントを作成します。
2. そのデータベース・インスタンスをディスカバーします。

3. 処理するデータベースをカタログします。カタログにより Guardium 内にデータ・ソースが作成され、特定のデータベース上のクラウド・データベース Guardium 機能を管理できます。
4. 必要に応じて、新規または既存の VA プロセスにデータ・ソースを追加します (脆弱性評価ライセンスが必要です)。
5. 必要に応じて、新規または既存の分類プロセスにデータ・ソースを追加します。
6. オプションで、関連データベース上で DB 監査を有効にして、今すぐ Guardium UI から、または後で DB コンソールから、データベースを再始動します。DB 監査は、有効になると標準 Oracle 監査を実行します。DB 監査を有効にすると、Guardium システムは、その DB 上の DB 監査の固有の所有者になります。他の Guardium システムは、DB 監査およびオブジェクト監査を変更できません。分類結果を表示するには、DB 監査を有効にした後に分類を 1 回実行するか (今すぐ 1 回実行)、またはスケジュールされた次の実行を待機します。(データ・ソースを分類プロセスに割り当てる必要があります。)
7. データ・ソースの分類結果を次のように確認します (分類プロセスと DB 監査が必要です)。
    - オブジェクトごとまたはオブジェクトを識別した分類プロセスごとにオブジェクトをグループ化して表示し、結果をさらに絞り込むためにフィルターを使用します。
    - オブジェクト監査を、個別、または表別に有効または無効にします。
    - オブジェクト・グループからドリルダウンして、分類結果内の選択したオブジェクトを含むすべてのデータベースのリストを開きます。このビューで、オブジェクト監査を有効/無効にすることもできます。
8. 定期的にステップ 2 から 7 を繰り返します。
9. 定期的にデータ・ソースをレビューして、新しいオブジェクトを確認し、オプションでオブジェクト監査のオブジェクトを追加または削除します。例えば、自動的に追加されたオブジェクトに監査を必要としないと決定したオブジェクトが含まれているか、データベースにパフォーマンスの問題がある場合は、オブジェクトを削除できます。または、監査されていない疑わしいオブジェクトを特定し、それをオブジェクト監査に追加することができます。

親トピック: クラウド・データベース・サービス保護

AWS IAM 定義

必要な権限に応じて、AWS アカウントの IAM ポリシーを定義します。

IAM の最小限の権限には、構成の表示とタグの変更が含まれます。DB 監査の有効化や DB の再始動は含まれません。この JSON では最小限の権限を定義します。これがないと、クラウド・データベース・サービス保護を実行することはできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "rds:DescribeDBParameters",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DownloadDBLogFilePortion",
                "rds:DescribeDBLogFiles",
                "rds:ListTagsForResource",
                "rds:RemoveTagsFromResource",
                "rds:AddTagsToResource",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

全権限はこれらのパラメーターで使用可能になります。

インスタンスに対する DB 監査を有効、無効にする
構成されていない場合、「DB 監査を有効にする」ボタンと「DB 監査を無効にする」ボタンはグレー表示になり、AWS コンソールで DB インスタンスを有効または無効にするよう DBA に要求する必要があります。

```
"rds:CopyDBParameterGroup",
"rds:CreateDBParameterGroup",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
```

DB インスタンスを再始動する
構成されていない場合、「再始動」ボタンはグレー表示になり、AWS コンソールで DB インスタンスを再始動するよう DBA に要求する必要があります。

```
"rds:RebootDBInstance",
```

サポートされているプラットフォームが EC2 の場合のセキュリティー・グループの操作
構成されていない場合は、DBA が Guardium IP をセキュリティー・グループに追加する必要があります。構成されている場合は、Guardium がその IP を DB インスタンスのセキュリティー・グループに追加します。ネットワーク構成により、Guardium システムが自身の IP を識別できない場合は、DBA が AWS コンソールで IP を追加する必要があります。

```
 "rds:ModifyDBInstance"
"rds:AuthorizeDBSecurityGroupIngress",
"rds:CreateDBSecurityGroup",
```

サポートされているプラットフォームが VPC の場合のセキュリティー・グループの操作
構成されていない場合は、DBA が Guardium IP をセキュリティー・グループに追加する必要があります。構成されている場合は、Guardium がその IP を DB インスタンスのセキュリティー・グループに追加します。ネットワーク構成により、Guardium システムが自身の IP を識別できない場合は、DBA が AWS コンソールで IP を追加する必要があります。

```
 "rds:ModifyDBInstance"
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateSecurityGroup",
```

これらのパラメーターの構成時に、Guardium は、コレクターのパブリック IP CIDR マスクを 24 に指定して、RDS インスタンス・セキュリティー・グループにインバウンド・ルールを作成します。

親トピック: クラウド・データベース・サービス保護

クラウド・アカウントの作成、変更、削除

DB 資格情報を使用して、クラウド・データベース・サービス・アカウントを作成するか、クラウド・アカウントを変更または削除します。

親トピック: クラウド・データベース・サービス保護

クラウド・アカウントの作成

このタスクについて

前提条件: AWS IAM ポリシーを定義します。AWS IAM 定義を参照してください。

ヒント: このアカウントで多数のデータベースを管理している場合は、デフォルトの分類プロセスを定義することを検討してください。それにより、ディスカバーされた各データベースのプロパティーを定義する手間を省けます。

手順

1. 「ディスカバー」 > 「データベース・ディスカバリー」 > 「クラウド DB サービスの保護」をナビゲートします。
2. をクリックして、「クラウド DB サービス・アカウント定義の作成 (Create Cloud DB Service Account Definition)」ペインを開きます。
3. アカウントを定義します。
   - 固有アカウント名
   - プロバイダー
   - クラウド・サービス・プロバイダーから提供される固有のアクセス・キー ID および秘密アクセス・キー ID。アカウント秘密鍵はパスワードとして機能します。アクセス・キーとタイトルの両方を固有にして、同じ access_id で複数のアカウント名を使用できないようにする必要があります。
   - 自動的に追加されるオブジェクトを制限 (オプション): これは DB 監査が有効である場合に、オブジェクト監査に対して自動的に有効にできる、分類により検出されるオブジェクトの最大数です。これは、ディスカバー後、データベースごとに変更できます。有効にされたオブジェクトは、「管理対象オブジェクト (Managed Objects)」ウィンドウで自動的に「有効」と表示されます。Guardium にオブジェクトを自動的に追加させるには、分類プロセスでの検出が予期される妥当な上限を設定します。分類に誤りがあった場合でもオブジェクトがオーバーフローしないようにするために、設定値は高すぎないようにします。(オーバーフローはデータベースのパフォーマンスに影響を与える可能性があります)。ゼロ (0) は、オブジェクト監査に対して自動的に有効になるオブジェクトがないことを意味します。 監査済みのオブジェクトの数に、新しく分類されたオブジェクトの数を加えると、この制限を超える場合、新しいオブジェクトは、オブジェクト監査が有効になりません。例えば、15 に設定され、分類が最初の実行時に 5 個のオブジェクトを識別する場合、その 5 個のオブジェクトに監査証跡が割り当てられます。設定が 15 であり、既に 5 つのオブジェクトがオブジェクト監査に有効になっており、分類の次の実行で 16 オブジェクトが識別されると、新しいオブジェクトはどれもオブジェクト監査が有効になりません。設定が 15 であり、既に 5 つのオブジェクトがオブジェクト監査に有効になっており、分類の次の実行で 5 オブジェクトが識別されると、新しい 5 オブジェクトはオブジェクト監査で有効になります。
4. オプションで、デフォルトの分類を定義します。このアカウントのすべてのカタログ済みデータベースは、この分類プロセスに割り当てられます。分類プロセスは、カタログ後に、データベースごとに変更できます。
5. クラウドへのアクセスをテストします。
   a. 「アクセスのテスト」をクリックします。Guardium はクラウドへのアクセスを試行します。
   b. Guardium がクラウドへのアクセスに失敗する場合は、Guardium システムが Amazon にアクセスできることを確認します。指定したキーを調べます。
6. 「作成」をクリックします。
   アカウントが作成され、「クラウド DB サービス・アカウント」リストは新しいクラウド・アカウントで更新され、そのアカウントの詳細が右ペインに表示されます。

次のタスク

データベースを検出してカタログし、分類と脆弱性評価、およびオブジェクト監査をセットアップします。

クラウド・アカウントの変更

プロバイダー以外のすべてのパラメーターを変更できます。

手順

1. 「クラウド DB サービス・アカウント」からクラウド・アカウントを選択し、右ペインの をクリックします。
2. 構成を変更します。
3. 変更された資格情報がある場合は、「アクセスのテスト」をクリックしてクラウドへのアクセスをテストします。
4. 「保存」をクリックします。

クラウド・アカウントの削除

アカウントを削除すると、現在の環境によって所有されているすべてのデータベース上のオブジェクト監査と DB 監査が無効になります。

手順

1. 「クラウド DB サービス・アカウント」ペインでアカウントを選択し、をクリックして、確認します。
2. DB を DB コンソールから再始動します。DB への Amazon アクセス権限がない場合は、DB 監査を無効にして DB を再起動するように DBA に依頼してください。 監査を停止し、DB を再始動することで、DB が Guardium によって使用されるログ・ファイルへの書き込みを停止することは重要です。

クラウド・データベースのディスカバー

検索するリージョンを選択することで、クラウド・アカウント内のデータベースをディスカバーします。

このタスクについて

ディスカバーを実行すると、「データベース」表にデータが追加されて更新されます。ディスカバーされたデータベースは、そのデータベースがまだクラウドにあるかどうかに関係なく、表に残ります。

「ディスカバリー」 > 「データベース・ディスカバリー」 > 「クラウド DB サービスの保護」にナビゲートするたびに、Guardium はクラウド内の DB 監査ステータスが UI で報告されるステータスと異なる場合に、データベース表の上に次のメッセージを表示して通知します。「一部のデータベースで DB 監査状況が変更されました。「リフレッシュ」をクリックして表を更新してください」。このメッセージが表示されたら、「リフレッシュ」をクリックして表示を最新表示します。

この確認は「状況の取得」をクリックしてオンデマンドで実行することもできます。 この取得には数分かかる場合があります。完了したら、DB 監査状況が変更されている場合にのみメッセージが表示されます。変更がある場合は、「リフレッシュ」をクリックします。

クラウド・データベース定義は CSV ファイルでもアップロードできます。必須パラメーターは『GuardAPI クラウド・データ・ソース関数』にリストされます。API パラメーター cloudTitle をパラメーター environmentTitle (機能は同じですが、名前は異なります) に置き換える必要があります。『カスタム・アップロード』の『CSV のアップロード・メニューにより CSV をアップロードしてデータ・ソースを作成する』のアップロード手順を参照してください。ファイルをアップロードするには、「強化」 > 「脆弱性評価」 > 「カスタム・アップロード」に移動します。

手順

1. 「ディスカバリー」 > 「データベース・ディスカバリー」 > 「クラウド DB サービスの保護」とナビゲートして、サービス・アカウント名をクリックします。 クラウド・アカウントを作成すると、「データベースのディスカバー」表が開き、すべての領域のリストがその RDS エンドポイントとともに表示されます。
2. その後このページにアクセスすると、表は閉じます。「データベースのディスカバー」をクリックします。 表が開き、領域が表示されます。
3. ディスカバーするデータベースがある各領域の行を選択します。関係する場合はフィルターを使用します。
4. 「ディスカバー」をクリックします。 Guardium は領域を検索し、過去にディスカバーされていないデータベースをデータベース表に追加します。

親トピック: クラウド・データベース・サービス保護

データベースのカタログおよび管理

Guardium でデータ・ソースを作成するためのデータベースをカタログし、ユーザーとパスワードを変更し、データベース構成を更新します。

このタスクについて

カタログにより、分類、脆弱性評価、監査、およびレポートに使用される、Guardium 内のデータ・ソースが作成されます。カタログされていないデータベースの場合、DB 表の「Guardium データ・ソース」列に赤色のアイコンが表示されます。

手順

1. 監査するデータベースをカタログします。
   a. 「データベース」表で、1 つ以上のデータベースを選択します。
   b. 「データ・ソース」 > 「データ・ソースのカタログ」をクリックします。
   c. DBA から受け取った、大/小文字を区別する DB ユーザーとパスワードを入力します。複数のデータベースを選択した場合は、それらで必ず同じユーザーとパスワードのペアを使用するようにしてください。
   d. オプションで、デフォルトの分類プロセスを選択、変更、またはクリアします。
   e. 「カタログ」をクリックします。
   Guardium データ・ソース名が「データベース」表に表示されます。
2. ユーザーまたはパスワードを更新します。
   a. 「データベース」表で、1 つ以上のデータ・ソースを選択します。
   b. 「データ・ソース」 > 「ユーザーとパスワードの更新」をクリックし、詳細を変更します。 両方のフィールドを指定する必要があります。
   c. 「カタログ」をクリックします。
3. データ・ソース定義を変更します。
   a. データ・ソースを選択し、「データ・ソース」 > 「データ・ソース定義を開く (Open Datasource Definition)」をクリックします。
   b. 必要に応じて変更します。データ・ソース定義の作成でパラメーターの詳細を参照してください。
   c. オプションで、「接続のテスト」をクリックしてデータベースへの接続をテストします。
   d. 「保存」をクリックします。

親トピック: クラウド・データベース・サービス保護

分類および脆弱性評価の管理

データ・ソースを既存の分類プロセスまたは脆弱性評価プロセスに割り当てます。または新規プロセスを作成します。

このタスクについて

「脆弱性評価」メニューは、有効な VA ライセンスをお持ちの場合にのみ使用可能です。

分類プロセスをデータ・ソースに割り当てると、分類データが収集され、オンプレミス・データベースと同じように処理されます。所有者以外でも分類を割り当てることはできますが、オブジェクト監査を有効にして結果を表示するためには所有権を取得する必要があります。

緑色のアイコンはプロセスが実行中であることを示します。黄色のアイコンは、プロセスに対してスケジュールが定義されていないことを意味します。「分類プロセス」列または「VA」列の赤色のアイコンは、分類および VA が割り当てられていないか、エラーであることを示します。VA エラーは、「強化」 > 「脆弱性評価」 > 「アセスメント・ビルダー」 > 「結果の表示」で表示します。分類エラーは、「ディスカバー」 > 「エンドツーエンド・シナリオ」 > 「機密データのディスカバー」 > 「レポートのレビュー」リボン > 「プロセス・ログ」で表示します。

「BDUMP でファイル bdump-file-listing が見つかりません。結果を取得できません: 'RDSADMIN.TRACEFILE_」という分類エラーが表示された場合は、グループ・ビルダーで定義済みスキーマ・グループ「除外する分類スキーマ - Oracle (Excluded Classification schemas - Oracle)」に RDSADMIN を追加します。

手順

1. 既存の分類プロセスに 1 つ以上のデータ・ソースを割り当てます。
   a. 1 つ以上のデータ・ソースを選択します。
   b. 「分類」 > 「分類への追加」をクリックします。
   c. 分類プロセスを選択して、「保存」をクリックします。
   d. オプションで「編集/表示 (Edit/View)」をクリックして、分類プロセスを変更または実行します。
   e. 分類プロセスで検出されたオブジェクトに対してオブジェクト監査を自動的に有効にする場合は、**「編集/表示 (Edit/View)」**をクリックして、分類プロセスを開きます。その後、「検索場所」リボンで「Cloud DB のオブジェクト監査の有効化」チェック・ボックスを選択します。
   f. あるいは、次のようにして分類を実行します。「ディスカバー」 > 「エンドツーエンド・シナリオ」 > 「機密データのディスカバー」に移動し、「ディスカバリーの実行」リボンで「今すぐ実行する」をクリックします。
2. 新規分類プロセスを作成し、1 つ以上のデータ・ソースをそれに割り当てます。
   a. 1 つ以上のデータ・ソースを選択します。
   b. 「分類」 > 「分類の作成」をクリックします。
   c. 機密データのディスカバーの手順に従います。デフォルトでは「Cloud DB のオブジェクト監査の有効化」が選択されています。これは選択されたままにしておきます。
   d. 次のようにして分類を実行します。「検索場所」の定義後に、「今すぐ実行する」をクリックします。またはプロセスの保存後に、「ディスカバリーの実行」リボンで「今すぐ実行する」をクリックします。
3. 既存の脆弱性評価に 1 つ以上のデータ・ソースを割り当てます。
   a. 1 つ以上のデータ・ソースを選択します。
   b. 「脆弱性評価」 > 「脆弱性評価への追加」をクリックします。
   c. 脆弱性評価プロセスを選択して、「保存」をクリックします。
   d. 次のようにしてプロセスを実行します。「強化」 > 「脆弱性評価」 > 「アセスメント・ビルダー」とナビゲートし、プロセスを選択して、「今すぐ 1 回実行」をクリックします。
4. 新規脆弱性評価を作成し、1 つ以上のデータ・ソースをそれに割り当てます。
   a. 1 つ以上のデータ・ソースを選択します。
   b. 「脆弱性評価」 > 「脆弱性評価の作成」をクリックします。
   c. 脆弱性評価の説明を入力します。定義した監査プロセスの一部として結果を受け取る場合は、1 つ以上の E メール・アドレスを (複数の場合はコンマで区切って) 入力します。
   d. 「保存」をクリックします。
   すべてのテスト、選択したデータ・ソース、およびユーザーが定義したレシーバーを使用して VA プロセスがで作成されます。
   e. 次のようにしてプロセスを実行します。「強化」 > 「脆弱性評価」 > 「アセスメント・ビルダー」にナビゲートし、プロセスを選択して、「今すぐ 1 回実行」をクリックします。

親トピック: クラウド・データベース・サービス保護

データベース監査の構成

データベース上での監査を有効にし、オブジェクト監査データを Guardium がプルできるようにします。 分類に自動的に追加されるオブジェクトの制限を変更し、コレクターを変更します。

このタスクについて

「データベース」表には、ディスカバーされたデータベースのさまざまな詳細が表示されます。表内の色付きの標識を使用すると、素早く一目でデータ・ソースの状況を確認できます。赤は構成がないこと、つまり例えばデータベースがカタログされていない、またはデータ・ソースが分類または VA プロセスに割り当てられていないといったことを示します。色分けされた状況標識には吹き出しヒントがあり、色が赤または黄色の場合に詳細が提供されます。 事前定義フィルター・リストを使用して、色分けされた状況標識がある列をフィルタリングできます。その他の値にはフリー・テキスト・フィルターを使用できます。

データ・ソースに対してコレクターが定義されている場合、ユーザーが所有者である場合は「アクティブなコレクター」列に表示されます。それ以外の場合、列はブランクです。

DB 監査の所有者は、CM 環境内の CM ホスト名です。スタンドアロン・システムでは、この値はコレクターのホスト名です。

「DB 監査」列には以下のいずれかの値が示されます。

- 有効。再始動の保留中が後に続く場合、状況はインスタンスの再始動時に有効になることを示します。
- 無効。再始動の保留中が後に続く場合、状況はインスタンスの再始動時に有効になることを示します。
- 構成が要件と一致していません。(AWS パラメーター監査証跡が、Guardium の要件 XML, EXTENDED に従って構成されていません。この値を変更するように DBA に依頼してください。)再始動の保留中が後に続く場合、状況はインスタンスの再始動時に有効になることを示します。
- この DB エンジンではサポートされていません。アクティビティー・モニターは現在、Guardium でサポートされていません。

インスタンスを所有しており、分類プロセスが割り当てられている状態で、DB 監査が有効な場合は、「オブジェクト」列に結果が表示されます。合計は、このインスタンスに割り当てられている分類プロセスで識別されるオブジェクトの数です。「監査済み」は、オブジェクト監査で有効なオブジェクトの数です。「新規」は、分類プロセスで検出されたが、自動的に有効になっていないオブジェクトの数です。これらのオブジェクトは検討が必要です。オブジェクト監査の管理を参照してください。

データ・ソースが分類プロセスに割り当てられており、そのプロセスが DB 監査を有効にして後に実行されており、ユーザーが所有者である場合には、結果が「オブジェクト」列に表示されます。オブジェクトが表示されない場合は、分類プロセスを確認し、再度実行してください。

親トピック: クラウド・データベース・サービス保護

自動的に追加されるオブジェクトとコレクターの制限の変更

自動的に追加されるオブジェクトとコレクターの制限を、1 つ以上のデータベースで同時に変更できます。ブランクのままになっているフィールドは変更されません。

手順

1. 1 つ以上のデータベースを選択します。
2. 「DB 監査」 > 「DB 監査構成」をクリックします。
3. 「自動的に追加されるオブジェクトを制限」の数を変更します。 これは DB 監査が有効である場合に、オブジェクト監査に対して自動的に有効にできる、分類により検出されるオブジェクトの最大数です。これは、ディスカバー後、データベースごとに変更できます。有効にされたオブジェクトは、「管理対象オブジェクト (Managed Objects)」ウィンドウで自動的に「有効」と表示されます。Guardium にオブジェクトを自動的に追加させるには、分類プロセスでの検出が予期される妥当な上限を設定します。分類に誤りがあった場合でもオブジェクトがオーバーフローしないようにするために、設定値は高すぎないようにします。(オーバーフローはデータベースのパフォーマンスに影響を与える可能性があります)。ゼロ (0) は、オブジェクト監査に対して自動的に有効になるオブジェクトがないことを意味します。 監査済みのオブジェクトの数に、新しく分類されたオブジェクトの数を加えると、この制限を超える場合、新しいオブジェクトは、オブジェクト監査が有効になりません。例えば、15 に設定され、分類が最初の実行時に 5 個のオブジェクトを識別する場合、その 5 個のオブジェクトに監査証跡が割り当てられます。設定が 15 であり、既に 5 つのオブジェクトがオブジェクト監査に有効になっており、分類の次の実行で 16 オブジェクトが識別されると、新しいオブジェクトはどれもオブジェクト監査が有効になりません。設定が 15 であり、既に 5 つのオブジェクトがオブジェクト監査に有効になっており、分類の次の実行で 5 オブジェクトが識別されると、新しい 5 オブジェクトはオブジェクト監査で有効になります。
4. コレクターが「中央マネージャー」環境に表示されます、コレクターはこの環境に必須です。CM 環境内のすべてのコレクターのドロップダウン・リストからコレクターを選択します。これは監査データ (アクティビティー) を DB からプルするコレクターです。
5. 「適用」をクリックします。

1 つのデータベースの監査の有効化

DB 監査は一度に 1 つのデータベース上で有効にできます。

このタスクについて

「自動的に追加されるオブジェクトを制限」パラメーター、または任意の許可レベルのコレクターを構成できます。その他の変更には DB 許可が必要です。アクセス・キーにはこれらの許可が含まれる場合もあれば、含まれない場合もあります。以下の説明は、すべてのレベルの許可を対象にしています。

DB 監査を有効にすると、Guardium システムは、この DB 上の DB 監査の固有の所有者になります。他の Guardium システムは DB 監査およびオブジェクト監査を変更しません。「DB 監査の所有の開始 (Start owning DB Audit)」をクリックすることで、別のシステムが強制的に所有権を取得することができます。

DB 監査で監査用オブジェクトを表示して管理できるようにしたら、少なくとも 1 回分類を実行します。 オブジェクトが見つからない場合は、ポリシーを確認します。

注意:
データベースの管理を開始すると、Amazon RDS タグ IBM Guardium IP が Guardium ホスト名の値で作成されます。このタグを変更したり、削除したりしないでください。

手順

1. データベースの行を選択します。
2. 「DB 監査」 > 「DB 監査構成」をクリックします。
3. オプションで、オブジェクト監査に自動的に追加されたオブジェクトの値を変更します。
4. CM 環境で、コレクターが定義されていない場合は、ドロップダウン・リストからコレクターを 1 つ選択して、「適用」をクリックします。 ダイアログがリフレッシュされ、ボタンが有効になります。
5. 「DB 監査を有効にする」が使用可能になっていれば、それをクリックします。ダイアログおよび表がリフレッシュされ、ユーザーが DB 監査の現在の所有者であることが表示されます。ダイアログ・ボックスがリフレッシュされます。「再始動」をクリックしてデータベースを今すぐ再始動するか (確認メッセージが表示されます)、または、例えば保守期間を待機するには、「次の手動再始動の待機 (Wait for next manual restart)」をクリックします。 「次の手動再始動の待機 (Wait for next manual restart)」を選択した場合は、クラウド・コンソールに後で直接アクセスする必要があります。 「再始動」をクリックした場合に十分なアクセス権限がない場合には、エラーが表示されます。DBA に、**監査証跡**を XML, EXTENDED として構成し、インスタンスを再始動するように依頼してください。
6. 「DB 監査を有効にする」が使用可能になっていなければ、「DB 監査の所有」をクリックします。ダイアログ・ボックスがリフレッシュされます。 「次の手動再始動の待機 (Wait for next manual restart)」をクリックし、DBA に、**監査証跡**を XML, EXTENDED として構成し、インスタンスを再始動するように依頼してください。
7. DB 監査状況を変更した場合は、「状況の取得」をクリックし、状況が変更されたことを示すメッセージが表示されるまで待ってから「リフレッシュ」をクリックします。「DB 監査の所有者」列に CM のホスト名またはスタンドアロン Guardium のコレクターのホスト名が表示され、「DB 監査」のアイコンが緑になります。

1 つのデータベースの監査の無効化

DB 監査は一度に 1 つのデータベース上で無効にできます。DB 監査を無効にすると、DB 監査の所有権も放棄することになります。

このタスクについて

DB 監査の所有を停止するかまたは DB 監査を無効にすると、オブジェクト監査全体も無効になり、監査可能なオブジェクトのリスト (分類結果からの成果物) は削除されます。

手順

1. データベースの行を選択します。
2. 「DB 監査」 > 「DB 監査構成」をクリックします。
3. 「DB 監査を無効にする」をクリックし、次に、例えば保守期間を待機するには「次の手動再始動の待機 (Wait for next manual restart)」をクリックし、データベースをすぐに再始動するには、「再始動」をクリックします。 「次の手動再始動の待機 (Wait for next manual restart)」を選択した場合は、クラウド・コンソールに後で直接アクセスする必要があります。 構成を変更する権限がない場合は、「DB 監査の所有の停止」をクリックし、DBA にこのインスタンスの DB 監査を無効にするように要求します。
4. 「状況の取得」をクリックして、クラウドからの最新の状況で表示を最新表示します。

タスクの結果

変更がある場合は、「一部のデータベースで DB 監査状況が変更されました。「リフレッシュ」をクリックして表を更新してください」というメッセージが表示されます。「リフレッシュ」をクリックします。状況は「無効」または「無効、再始動の保留中」に変わり、「DB 監査」のアイコンは赤になり、「DB 監査の所有者」列はブランクになります。

DB 監査所有権の開始および停止

このタスクについて

一度に 1 つのデータベースの DB 所有権状況を変更できます。

DB 監査を所有すると、DB 監査およびオブジェクト監査の定義への排他的権限と、オブジェクト監査データへのアクセス権限が付与されます (オブジェクト監査の管理を参照)。 他の Guardium システムも同じクラウド・アカウントにアクセスできますが、表示できるのは DB 詳細のみです。

全アクセス権限がある場合、DB 監査を有効にすると、DB の所有権も取得します。アクセス・キーが全アクセス権限を提供していない場合は、DB 監査を有効にせずに所有権を取得します。 DB 監査が (DBA により) 有効になると、監査データにアクセスできるようになります。逆に、DB 監査を無効にすると、所有権を放棄することになります。アクセス・キーが全アクセス権限を提供していない場合、DB 監査の所有が停止され、DBA に DB 監査を無効にするように要求することになります。

ある Guardium システムから別のシステムに所有権を移動することができます。

2 つのライブ・システム間で所有権を移動する場合、まず現行所有者での DB 監査の所有を停止してから、2 つ目の Guardium システムで所有権を取得します。一方の Guardium システムが所有権を放棄すると、すべての監査が停止します。新しい Guardium システムで監査プロセスを定義する (分類への DB の割り当て、プロセスの実行、オブジェクト監査へのオブジェクトの追加を行う) 必要があります。
注意:
一方で DB 監査の所有を停止してから、もう一方でそれの所有を開始してください。 そうしないと、データは、新しいコレクターだけでなく、以前のコレクターにも送信されます。異なるポリシー (異なる CM) を持つ 2 つのコレクターが同じアクティビティーを受け取ると、それぞれのコレクターで異なる (あるいは不完全な) 結果が生成されます。

ある Guardium システムがダウンし、リカバリーが期待されないときに、そのシステムから所有権を移動する場合、監査定義を維持しながら、所有権のみを変更して、別の Guardium システムから DBA 監査の所有を開始できます。このシナリオでは、DB コンソールで、元の Guardium による DB 監査の所有を停止します。

手順

1. 「データベース」表で、データベースの行を選択します。
2. DB 監査を停止するには、「DB 監査」 > 「DB 監査構成」 > 「DB 監査の所有の停止」をクリックします。
3. DB 監査の所有を開始するには、「DB 監査」 > 「DB 監査構成」 > 「DB 監査の所有の開始 (Start owning DB audit)」をクリックします。

オブジェクト監査の管理

管理しているデータベースの分類プロセスによって識別された潜在的な機密オブジェクトを表示し、これらのオブジェクトに実行されるすべてのアクティビティーをモニターするために、選択したオブジェクトに対するオブジェクト監査を有効にします。

このタスクについて

前提条件: DB 監査が有効かつユーザーにより所有されており、分類がこのデータ・ソースに対して少なくとも 1 回実行される必要があります。

新規オブジェクトとは、分類プロセスによって検出されたオブジェクトのうち、監査が有効になっていないオブジェクトのことです。すべての新規オブジェクトをフィルタリングして、それらのオブジェクト監査を有効にするか、または「新規」フラグをクリアすることができます。新規オブジェクトがないときは、新規オブジェクトの評価は最新です。Guardium は分類プロセスが実行されるごとに新規データを受け取る可能性があることを覚えておいてください。オブジェクト監査に自動的に追加されなかった新規オブジェクトが検出された場合、「新規オブジェクトが検出されました (New objects were found)」という通知が出されます。

「分類による検出」列には、そのオブジェクトを特定したすべての分類プロセスがリストされます。

「オブジェクト監査の状況」列の「混合」状況は、いくつかのデータ・ソースではオブジェクト監査が有効で、他のデータ・ソースでは無効であることを意味します。

オブジェクト監査の有効化および無効化は負荷が高いプロセスであり、数分かかる場合があります。クラウドが監査変更を処理している間は、待機中アイコンが表示されます。

「データベース」表からレビューするデータ・ソースの行を選択することで、1 つ以上のデータ・ソースで検出されたオブジェクトをレビューできます。 「オブジェクト監査」ウィンドウには、選択したデータベースに対するすべての分類プロセスによって検出された、すべてのオブジェクトが表示されます。

- 1 つのデータベースでのオブジェクト監査の管理
- 複数のデータベースでのオブジェクト監査の管理

親トピック: クラウド・データベース・サービス保護

1 つのデータベースでのオブジェクト監査の管理

このタスクについて

「データ・ソース <name> 内のオブジェクト (Objects in Datasource <name>)」ウィンドウには、このデータ・ソースに対して実行された分類プロセスにより検出されたすべてのオブジェクトがリストされます。オブジェクトは、複数の分類プロセスによって見つかる可能性があります。

オブジェクトが分類プロセスによって特定されているが、オブジェクト監査が自動的に有効にならなかったときは、オブジェクト表の上に「検出された新規オブジェクト」が表示されます。「新規のみ」をクリックしてフィルターに掛けることで、処理が必要な、すべての検出された新規オブジェクトを表示します。 新規オブジェクトは、分類を実行するたびに見つかる可能性があります。新規オブジェクトがないときは、新規オブジェクトの評価に遅延はありません。

定期的にデータ・ソースをレビューして、新しいオブジェクトを確認し、オプションでオブジェクト監査のオブジェクトを追加または削除します。例えば、自動的に追加されたオブジェクトに監査を必要としないと決定したオブジェクトが含まれているか、データベースにパフォーマンスの問題がある場合は、オブジェクトを削除できます。または、監査されていない疑わしいオブジェクトを特定し、それをオブジェクト監査に追加することができます。

監査の必要があることが分かっているオブジェクトには、分類フィルターを使用します。フィルタリング済みのビューですべてのオブジェクトを選択し、オブジェクト監査を有効にします。

手順

1. DB 監査を有効にする**前に**分類プロセスを割り当てた場合には、ここで分類を 1 回実行して、Guardium がオブジェクトを識別するのを数分待機します (またはスケジュールされた次の実行を待機します)。
2. データ・ソースを 1 つ選択します。新規オブジェクトがあるデータ・ソースを識別するために、「検出された新規オブジェクト」フィルターを使用できます。
3. 「DB 監査」 > 「オブジェクト監査の管理」を選択します。 「オブジェクト監査の管理」ウィンドウが開き、このデータ・ソースが割り当てられている、分類プロセスによって検出されたすべてのオブジェクトのリストが表示されます。
4. 新規として分類されているすべてのオブジェクトを識別するために、「新規のみ」フィルターを使用できます。
5. 表から 1 つ以上のオブジェクト (行) を選択します。
6. 監査証跡を有効にするには、「アクション」 > 「監査を有効にする」を選択します。 システムは、操作の成功または失敗で応答します。
7. 「新規」フラグをクリアするには、「アクション」 > 「新しいフラグのクリア」をクリックします。
8. 監査証跡を無効にするには、「アクション」 > 「監査を無効にする」を選択します。 システムは、操作の成功または失敗で応答します。

親トピック: オブジェクト監査の管理

複数のデータベースでのオブジェクト監査の管理

このタスクについて

このビューには、選択したデータ・ソースに対して実行された分類プロセスによって見つかったすべてのオブジェクトがリストされます。オブジェクトは、複数の分類プロセスによって見つかる可能性があります。オブジェクトをオブジェクトごと (デフォルト)、または種別ごとにグループ化して表示します。「分類による検出」列には、オブジェクトを特定したすべての分類プロセスがリストされます。

オブジェクトが分類プロセスによって特定されたが、オブジェクト監査が自動的に有効にならなかったときは、オブジェクト表の上に「検出された新規オブジェクト」が表示されます。「新規のみ」をクリックしてフィルターに掛けることで、処理が必要な、すべての検出された新規オブジェクトを表示します。「新規」オブジェクトを確認して、オブジェクト監査を有効にするか、「新規」フラグをクリアします。

新規オブジェクトは、分類を実行するたびに見つかる可能性があります。新規オブジェクトがないときは、新規オブジェクトの評価に遅延はありません。

定期的にデータ・ソースをレビューして、新しいオブジェクトを確認し、オプションでオブジェクト監査のオブジェクトを追加または削除します。例えば、自動的に追加されたオブジェクトに監査を必要としないと決定したオブジェクトが含まれているか、データベースにパフォーマンスの問題がある場合は、オブジェクトを削除できます。または、監査されていない疑わしいオブジェクトを特定し、それをオブジェクト監査に追加することができます。

オブジェクトごとにグループ化: 新しく見つかったオブジェクトをすべて表示するには、テキスト・フィルターに「新規」と入力します。

選択したすべてのデータ・ソースであるオブジェクトのオブジェクト監査を有効または無効にするには、行を選択し、「アクション」>「有効化/無効化」をクリックします

データ・ソースごとにアクションを実行するには、「オブジェクトが存在しているデータ・ソースの数」をクリックして、選択したオブジェクトを分類プロセスが特定したすべてのデータ・ソースを表示します

分類ごとのグループ化: これは監査を必要としていて、それ以上の評価は必要ないオブジェクト (例えば GDPR など) を持つ、ほとんど同一のデータ・ソース、または分類ポリシーがあるときは特に有用です。

手順

1. DB 監査を有効にする**前に**分類プロセスを割り当てた場合には、ここで分類を 1 回実行して (またはスケジュールされた次の実行を待機して) 、Guardium がオブジェクトを識別するのを数分待機します。
2. オブジェクトごとのグループ化の場合には、次のようにします。
    a. データベース表の「オブジェクト」列に新規オブジェクトがある複数のデータ・ソースを選択します。 それらのデータ・ソースを識別するには、「検出された新規オブジェクト」フィルターを使用します。
    b. 「DB 監査」 > 「オブジェクト監査の管理」をクリックします。「オブジェクト監査の管理」ウィンドウが開きます。
    c. このオブジェクトを常にすべてのデータ・ソース内で監査する必要がある場合には、行を選択し、「アクション」 > 「監査を有効にする」をクリックします。 システムは、操作の成功または失敗で応答します。
    d. 個々のデータベースでオブジェクト監査を有効にする場合は、オブジェクトの行にある「オブジェクトが存在しているデータ・ソースの数」列の番号をクリックし、「<object> を含むデータ・ソース」ウィンドウを開きます。このウィンドウは、分類プロセスが選択したオブジェクトを識別したすべてのデータ・ソースを示します。1 つ以上のデータ・ソース行を選択し、「アクション」 > 「監査を有効にする」をクリックします。
3. 識別されたオブジェクトが常に監査を必要とし、それ以上の評価は必要としない分類プロセスの場合は、「分類」ラジオ・ボタン (表の上にある) をクリックし、分類プロセスの 1 つ以上の行を選択して、「アクション」 > 「監査を有効にする」をクリックします。

親トピック: オブジェクト監査の管理

データベース・オートディスカバリー

オートディスカバリー・アプリケーションは、サーバーをスキャンおよびプローブしてオープン・ポートを調べ、ネットワークに対して不明な接続や望ましくない接続が行われるのを防ぎます。オートディスカバリー・プロセスはオンデマンドで実行することも、定期的に実行されるようスケジュールすることもできます。

データベース・オートディスカバリーの概要

ネットワーク上にデータベースが未検出の状態で存在し、ネットワークが潜在的なリスクにさらされる可能性のあるシナリオには、さまざまなものがあります。例えば、古いデータベースがモニターされずに忘れられている場合や、新規データベースがアプリケーション・パッケージの一部として追加される場合などが考えられます。また、不正なデータベース管理者が、データベースの新規インスタンスを作成し、モニターされているデータベース以外に対して悪質なアクティビティーを実行する可能性もあります。

オートディスカバリーはスキャン・ジョブとプローブ・ジョブを使用して、環境内に未検出のデータベースが存在しないようにします。

- *スキャン・ジョブ*は、指定した各ホスト (または指定したサブネット内のホスト) をスキャンし、そのホストに指定されているオープン・ポートのリストを作成します。
- *プローブ・ジョブ*は、スキャンの結果を使用して、オープン・ポート上で実行中のデータベース・サービスがあるかどうかを判別します。プローブ・ジョブを実行するには、最初にスキャンを実行する必要があります。「ディスカバーされたデータベース」事前定義レポートで、このジョブの結果を確認できます。

始める前に、オートディスカバリー・アプリケーション用のパッチをダウンロードしてインストールしてください。このパッチは、IBM Fix Central で入手できます。

オートディスカバリー・アプリケーションを使用するには、次のステップを実行します。

1. 特定の IP アドレスまたはサブネットでオープン・ポートを検索するオートディスカバリー・プロセスを作成します。
2. オートディスカバリー・プロセスを、オンデマンドで、またはスケジュールに従って実行します。
3. オートディスカバリー・レポートでプロセスの結果を確認するか、カスタム・レポートを作成します。

オートディスカバリーには、監査プロセスに依存しない独自のプロセスがありますが、それらは監査プロセスと全く同じように動作します。

スキャンを行う場合はホスト名ではなく IP のみを入力できますが、Guardium はレポートの一部としてホスト名を検出します。Guardium は、Guardium 製品内でホスト名を切り捨てることはありません。ただし、列の幅がより広くなるようにレポートを構成する必要があるかもしれません。

Guardium オートディスカバリーでは、プローブ中に表示されるデータベースを推測することはありません。Guardium オートディスカバリーがデータベースを検出したことを示した場合、そのデータベースが何であるかは 100% 明確です。

注: ディスカバリーでは、実行中のデータベースのみが検出されます。 インストール時にディスカバリーを使用する予定の場合は、データベースを始動する必要があります。AIX KTAP インターセプトの機能上の理由から、初めて S-TAP を実行した後に、データベースを再始動しなければなりません。データベースを再始動しないと、一部のインターセプトが動作しません。

オートディスカバリー・プロセスの作成

オートディスカバリー・プロセスがスキャンするホストとポートを指定します。

1. 「ディスカバー」 > 「データベース・ディスカバリー」 > 「オートディスカバリーの構成」をクリックし、オートディスカバリーを構成します。
2. 「新規」をクリックして新規プロセスを作成し、「オートディスカバリー・プロセス・ビルダー」を開きます。
3. Guardium® システム上で固有の「プロセス名」を入力します。
4. スキャン・ジョブの完了直後にプローブ・ジョブを実行するには、「スキャン後にプローブを実行」チェック・ボックスにチェック・マークを付けます。
5. スキャンするホストまたはサブネットごとに、ホストとポートを入力して「スキャンの追加」をクリックします。スキャンを追加するたびに、スキャンがタスク・リストに追加されます。
   注:
   - ワイルドカード文字が使用可能です。例えば、192.168.2 で始まるアドレスをすべて選択するには、「192.168.2.*」と指定します。
   - 一定範囲のポートを指定するには、その範囲内の最初のポート番号と最後のポート番号の間にダッシュを入れます。例: 4100-4102。
   - スキャンを追加した後、ホストまたはポートを上書き入力で変更します。 「適用」をクリックして、変更を保存します。
   - デュアル・スタック構成がある場合は、IPV4 アドレスと IPV6 アドレスの両方に対してスキャンを設定する必要があります。
   - スキャンを削除するには、そのスキャンの「このタスクを削除」アイコンをクリックします。タスクに、それに従属するスキャン結果がある場合は、そのスキャンは削除できません。
6. スキャンの追加が完了したら「適用」をクリックし、ジョブを実行するか、ジョブを後で実行するようスケジュールします。

スケジュールの定義のヘルプ情報が必要な場合は、『スケジューリング』を参照してください。

オートディスカバリー・プロセスの実行またはスケジュール

スキャン・ジョブとプローブ・ジョブをオートディスカバリー・プロセスの一部として実行またはスケジュールします。

1. 「ディスカバー」 > 「データベース・ディスカバリー」 > 「オートディスカバリーの構成」をクリックします。
2. 「オートディスカバリー・プロセス・セレクター」リストから実行するプロセスを選択し、以下のいずれかを実行します。
3.
   - ジョブを即時に実行するには、「今すぐ 1 回実行」をクリックします。
   - 今後ジョブをスケジュールするには、「スケジュールの変更」をクリックします (スケジュール定義のヘルプ情報が必要な場合は、『スケジューリング』を参照してください)。
     注: プローブ・ジョブは、スキャン・ジョブの結果がないと実行できません。これら 2 つのジョブを個々に実行するようスケジュールすることも、スキャン・ジョブの後にプローブ・ジョブを実行するよう構成することもできます。後者の場合は、プロセスに変更を加え、「スキャン後にプローブを実行」チェック・ボックスにチェック・マークを付けます。
4. ジョブを開始またはスケジュールした後、「進行状況/サマリー」をクリックすると、このプロセスの状況を表示できます。

オートディスカバリー・レポート

オートディスカバリー・レポートを開くには、「ディスカバー」 > 「レポート」をクリックし、使用可能なレポートから選択します。

「オートディスカバリー・クエリー・ビルダー」で、カスタム・レポートを作成することができます。「オートディスカバリー・クエリー・ビルダー」を開くには、「ディスカバー」 > 「データベース・ディスカバリー」 > 「オートディスカバリー・クエリー・ビルダー」をクリックします。

「ディスカバーされたデータベース」レポート

「ディスカバーされたデータベース」レポートを開くには、「ディスカバー」 > 「レポート」 > 「ディスカバーされたデータベース」をクリックします。

このレポートのメイン・エンティティーは「ディスカバーされたポート」です。ディスカバーされた各ポートは、レポート内でそれぞれの行に表示されます。「プローブ時間」、「サーバーの IP アドレス」、「サーバー・ホスト名」、「データベース・タイプ」、「ポート」、「ポート・タイプ」(通常は TCP)、およびオカレンス数の各列がリストされます。

このレポートには、特殊なランタイム・パラメーターはありませんが、 データベース・タイプが「不明」であるディスカバーされたポートは除外されます。

オートディスカバリー・プロセス定義を変更すると、そのプロセスの統計はリセットされます。

「オートディスカバリーのトラッキング」ドメイン

「オートディスカバリーのトラッキング」ドメインには、オートディスカバリー・プロセスによってレポートされたすべてのデータが含まれます。エンティティー名をクリックして、その属性を表示します。

「オートディスカバリーのトラッキング」ドメインのエンティティー

- 「オートディスカバリー・スキャン」には、各スキャン操作のタイム・スタンプが示されます。
- 「ディスカバーされたホスト」には、ディスカバーされた各ホストの IP アドレスとホスト名が示されます。
- 「ディスカバーされたポート」には、オープン状態がディスカバーされたポートごとに、タイム・スタンプ、ポート、およびデータベース・タイプが示されます。

親トピック: ディスカバー

分類

分類ポリシーと分類プロセスは、Guardium® が機密データ (クレジット・カード番号、社会保障番号、個人の金融データなど) をディスカバーして処理する方法を定義します。

組織の規模が大きくなり、クレジット・カード番号および個人の金融データなどの機密情報が複数のロケーションに存在するようになると (そのデータの現在の管理責任者が分からないという場合がよくあります)、ディスカバリー・プロセスと分類プロセスが重要になります。こうした状況は、合併買収の際や、元の所有者がいなくなった後もレガシー・システムを引き続き使用している場合に、多く発生します。 機密データをディスカバーするためのワークフローを作成すると、現行環境内の機密データを特定し、適切なアクション (アクセス・ポリシーの適用など) を実行できるようになります。

分類プロセス は、1 つ以上のデータ・ソースと関連付けられた分類ポリシーから成ります。分類プロセスは、1 回だけ実行するように処理依頼することも、コンプライアンス・ワークフロー自動化プロセスで定期的に実行するようスケジュールすることもできます (プロセスで使用されるすべてのデータ・ソースに対してログイン資格情報が保管されている場合)。

分類ポリシー は、指定されたデータ・ソース内の機密データを見つけてタグ付けするよう設計された、分類ルールと分類ルール・アクションから成ります。

分類ルール は、正規表現、Luhn アルゴリズム、およびその他の基準を使用して、分類ポリシーの適用時に内容を突き合わせるためのルールを定義します。

分類ルール・アクション は、分類ポリシー内の各ルールに対して実行する一連のアクションを指定します。例えば、アクションによって E メール・アラートを生成したり、Guardium グループにオブジェクトを追加したりすることができます。ルールが満たされるたびにそのイベントがログに記録されるため、それについてレポートすることができます (実行するアクションとして「無視」が指定された場合は例外で、その場合にはそのルールのログは記録されません)。

- 分類プロセスのパフォーマンス
  分類プロセスの処理には、サンプリング・ルーチンとタイムアウト・パラメーターが使用されます。これにより、データベース・サーバーに対するパフォーマンス上の影響が最小限に抑えられます。
- 分類ルールの処理
  分類ルールは、柔軟なマッチングおよびグループ化基準に従って処理されます。
- 分類プロセスの操作
  分類プロセス・ビルダーを使用して、分類プロセスの作成、実行、表示を行います。
- 分類ポリシーの操作
- 分類ルールの操作
- 分類ルール・アクションの操作

親トピック: ディスカバー

分類プロセスのパフォーマンス

分類プロセスの処理には、サンプリング・ルーチンとタイムアウト・パラメーターが使用されます。これにより、データベース・サーバーに対するパフォーマンス上の影響が最小限に抑えられます。

分類機能の実行時には、レコードのサンプリング方法を指定するオプションがあります。デフォルトの動作では、該当するデータベース・プラットフォームに適したステートメントを使用して、行がランダムにサンプリングされます。例えば SQL データベースの場合、分類機能は rand() ステートメントを使用してサンプリングを行います。代替動作は順次サンプリングです。この場合は、指定されたサンプル・サイズになるまで順番に行が読み取られます。ランダム・サンプリングはデフォルトの動作であり、より典型的な結果が得られるため、一般的にはこのサンプリングをお勧めします。ただし、ランダム・サンプリングは順次サンプリングと比べて、パフォーマンスが若干低下する可能性があります。ランダム・サンプリングと順次サンプリングのどちらも、デフォルトのサンプル・サイズは、2000 行か使用可能な行の総数のいずれか少ない方になります。これより大きい、または小さいサンプル・サイズを指定することもできます。

分類プロセスがデータベース・サーバーに与える影響をさらに最小化するため、長時間実行されている照会はキャンセルされ、ログに記録されて、表の残りはスキップされます。このポイントまでに取得された行はすべて、表のルールを評価する際に使用されます。同様に、分類プロセスを長時間実行しても完了しない場合は、プロセス全体が一時停止され、プロセス統計とともにログに記録されて、次の分類プロセスが開始されます。これが発生するのはまれで、通常は、既にパフォーマンス上の問題があるサーバーでのみ発生します。

分類機能は定期的に分類をアイドル状態にして、データベース・サーバーに対する要求が過剰になることを防ぎます。 データをサンプリングしている分類ルールが多数あってもデータベース・サーバー上の負荷は一定のはずですが、プロセスの実行時間が増える可能性があります。

分類機能は、除外されたグループを、スキーマ、表、表の列に対して使用することにより、誤検出を処理します。将来的な分類スキャンのために誤検出の結果を無視するように Guardium を設定するのは、これまでは複雑な作業でした。現在では、分類結果をレビューする際に、誤検出の結果を除外グループに簡単に追加し、そのグループ

を分類ポリシーに追加すれば、それ以降のスキャンでそれらの誤検出の結果が無視されるようになりました。

親トピック: 分類

分類ルールの処理

分類ルールは、柔軟なマッチングおよびグループ化基準に従って処理されます。

「限定起動」マーカー

「限定起動」マーカーを使用すると、まったく同一の名前によって分類ルール・タイプをグループ化することができます。さらに、1 つのマーカーを使用して返されるルールはすべて、同じ名前の表に基づいてデータを返す必要があります。 同じマーカーを使用して 2 つ以上のルールが定義されている場合、それらのルールは一緒に起動されます (すなわち、両方のルールが同じ表で起動された場合に、それらは両方ともログに記録され、それらのアクションが呼び出されます)。 反対に、ある表でいずれか一方のルールのみが起動された場合、ルールはどちらもログに記録されず、それらのアクションも呼び出されません。 複数のルールを一緒に起動できるようにすることは、同じ表内に複数の機密データが同時に現れる場合が懸念されるときに重要になります。 例えば、1 つの表に社会保障番号とマサチューセッツ州の運転免許証の両方が含まれる場合に、それを知ることができます。

「限定起動」マーカーは定数値であり、任意の値を指定でき、グループ化するルール全体でまったく同じ値でなければなりません。つまり、1 つのルールのマーカー名が ABC であれば、そのルールと一緒にグループ化する他のルールのマーカー名も ABC でなければなりません。 それ以外のマーカー値およびルールは、グループに含まれなくなります。

同じ名前の表内でデータを探索することが基本条件である場合、任意の同じ値を持つルールを少なくとも 2 つ使用する必要があります。

突き合わせを続行

限定起動マーカーは、「突き合わせを続行」にも基づいています。一例として、以下のルールが定義されており、ルール 3 が「突き合わせを続行」と一致しない場合、他の 3 つのマーカー・ルールがすべて正となったかどうかに関係なく、結果は返されません。 これは、ルール 4 の実行まで至らなかったためです。必ずすべての限定起動マーカーが実行され、結果が正になる必要があるので、このグループは起動されません。

ルール 1. 起動マーカー・ルール ABC (突き合わせを続行)

ルール 2. 起動マーカー・ルール ABC (突き合わせを続行)

ルール 3. 起動マーカー以外のルール・タイプ (突き合わせを続行)

ルール 4. 起動マーカー・ルール ABC (突き合わせを続行)

一致しない列のみ

結果データの細分度を下げる場合は、このオプションを使用します。組織によっては、組織内のデータを調査し、機密データが含まれている表や列だけを確認したいという場合があります。こうした場合、必ずしも、その列に含まれているすべてのタイプの機密データを検索する必要はありません。「突き合わせを続行」の新しいオプションである「一致しない列のみ」を選択すると、対象の列で一致が見つかった場合、分類機能はその列を無視して処理を続行します。

表 1. 分類プロセスで使用できるオプションの概要

突き合わせを続行	一致しない列のみ	結果の細分度
いいえ	N/A	表が返されます。表内で最初のヒットが見つかると、ルールの処理が停止します。
はい	はい	表と列が返されます。特定の列内の最初のヒットが記録され、それ以降のルールでは、その列が無視されます。
はい	いいえ	詳細な情報が返されます。すべてのルールで、すべての列についてヒットが記録されます。

Luhn アルゴリズムによる分類

ルール名が guardium://CREDIT_CARD で始まり、「検索式」ボックスに 有効なクレジット・カード番号パターンが指定されている場合、分類ポリシーは、標準の パターン・マッチングに加えて Luhn アルゴリズム (クレジット・カード番号などの ID 番号 検証のために幅広く使用されているアルゴリズム) を使用します。 Luhn アルゴリズムは追加の検査であり、パターン検査の代わりにはなりません。 有効なクレジット・カード番号は、16 桁の数字文字列、または 4 桁の数字 4 セット (各セットの間がブランクで区切られる) です。 このパターン・マッチングに Luhn アルゴリズムを組み込むには、「検索式」ボックスに guardium://CREDIT_CARD ルール名と有効な [0-9]{16} 数値の両方が指定されている必要があります。

親トピック: 分類

分類プロセスの操作

分類プロセス・ビルダーを使用して、分類プロセスの作成、実行、表示を行います。

手順

「分類プロセス・ビルダー」を開きます。これを行うには、「ディスカバー」 > 「分類」 > 「分類プロセス・ビルダー」にナビゲートします。
親トピック: 分類

分類プロセスの作成

手順

1. 「分類プロセス・ビルダー」から、  アイコンをクリックして、「分類プロセスの定義」パネルを開きます。
2. 「プロセスの記述」フィールドに、プロセス名を入力します。
3. リストから分類ポリシーを 1 つ選択します。「変更」をクリックすると、必要な場合にポリシーを表示および編集できます。
4. オプションで、「ランダム・サンプリング」チェック・ボックスをクリアします。この機能は、表内のレコードの数がサンプル・サイズを超える場合にのみ適用されます。ランダム・サンプリングは、表内のいくつかのレコードを、定義されたサンプル・サイズまでランダムに検索します。これは、結果がデータを適切に代表するため、質の高い検索です。「ランダム・サンプリング」チェック・ボックスのチェック・マークを外すと、動作が変更され、定義されたサンプル・サイズまで表内のレコードが順次検索されます。順次検索はランダム・サンプリングより実行速度が速い場合がありますが、結果は使用可能なすべてのデータを代表するものとはならない場合があります。
5. データを検索する場合、「サンプル・サイズ」に入力します (『分類ポリシー・ルールの定義』/『データの検索ルールの定義』を参照)。表内のレコードの数が「サンプル・サイズ」以下の場合、それらのすべてのレコードを対象に検索が行われ、一致が検出されます。表内のレコードの数が「サンプル・サイズ」を超える場合、ランダム・サンプリングが使用される場合があります。
6. 「データ・ソースの追加」ボタンをクリックして、1 つ以上のデータ・ソースを追加します。
7. 「保存」をクリックします。これで、分類プロセスの定義が完了します。
8. オプションで、定義にコメントを追加します。共通ツール・ヘルプ・ブックの『コメント』を参照してください。
9. オプションで、セキュリティー・ロールを追加します。アクセス管理ヘルプ・ブックの『セキュリティー・ロール』を参照してください。
10. オプションで、分類プロセスを実行依頼します。『分類プロセスの実行』を参照してください。
11. 完了したら、「完了」をクリックします。

分類プロセスの実行

このタスクについて

分類プロセスには、次の 3 とおりの実行方法があります。

- 「分類プロセス・ビルダー」からオンデマンドで実行する方法 (このタスクで説明します)。
- *コンプライアンス・ワークフロー自動化プロセス* 内のタスクとして実行する方法 (別のトピックで説明します)。
- *機密データのディスカバー・ワークフロー* の一部として実行する方法 (別のトピックで説明します)。

手順

1. 「分類プロセス・ビルダー」から、実行するプロセスを選択し、「変更」をクリックして分類プロセス・ビルダーを開きます。
2. 「今すぐ 1 回実行」ボタンをクリックして、ジョブを実行依頼します。 これによって、Guardium ジョブ・キューにプロセスが配置され、このキューから Guardium システムは一度に 1 つのジョブを実行します。「Guardium ジョブ・キュー」を使用すると、ジョブ状況を表示できます。
3. 完了したら、「完了」ボタンをクリックします。

分類結果の表示

手順

1. 「分類プロセス・ビルダー」で、「結果の表示」ボタンをクリックします。結果が別ウィンドウで開きます。
2. 「プロセス実行ログ」の任意の行で、「詳細」をクリックして詳細を表示します。
3. (オプション) データ・ユーザー・セキュリティーが有効である場合、「グローバル・プロファイル」でチェック・ボックスが表示されます。これを使用して、定義した「フィルタリング」に従って結果セット内の行を制御/切り替えできます。
4. 結果の確認終了後、「このウィンドウを閉じる」をクリックします。また、分類プロセスの状況を表示する分類プロセス・ログ・レポートがあります。

ジョブ・キューの表示

始める前に

Guardium ジョブ・キューは、管理者ポータルからのみ使用可能です。

手順

レポートを表示するには、「Guardium ジョブ・キュー」を開きます。これを行うには、「ディスカバー」 > 「分類」 > 「Guardium ジョブ・キュー」にナビゲートします。

分類ポリシーの操作

手順

「分類ポリシー・ビルダー」を開きます。これを行うには、「ディスカバー」 > 「分類」 > 「分類ポリシー・ビルダー」にナビゲートします。
親トピック: 分類

分類ポリシーの作成

手順

1. 「新規」をクリックして、「分類ポリシー定義」パネルを開きます。
2. 「名前」フィールドに、固有の名前を入力します。
3. 「カテゴリー」フィールドにカテゴリーを、「分類」フィールドに分類を入力します。これらはいずれも必須であり、レポートでデータをグループ化および編成するために使用されます。
4. オプションで、「記述」に入力します。
5. オプションでコメントを入力します。これらは、ポリシーの保存後いつでも入力可能です。『コメント』を参照してください。

6. 「ルールの編集」をクリックして、ルールおよびそれらに関連付けられたアクションを定義します。詳しい手順については、『分類ポリシー・ルールの定義』を参照してください。既存の分類ポリシーを変更する場合は、「機密データのディスカバー」シナリオ (「ディスカバー」 > 「エンドツーエンド・シナリオ」 > 「機密データのディスカバー」) を使用することをお勧めします。分類ポリシー・グループを作成する場合は、同じ「機密データのディスカバー」シナリオを使用してください。グループを作成した場合も、それらのグループを明示的に選択する必要があります。

分類ポリシーの変更

手順

1. 変更する分類ポリシーを選択し、以下のいずれかを実行します。
   - ポリシー・ルールを変更するには、「ルールの編集」をクリックし、『分類ポリシー・ルールの定義』を参照してください。
   - 定義のその他のエレメントを変更するには、「変更」ボタンをクリックします。
2. 必要に応じて任意の項目を上書きします。
3. 「保存」をクリックして変更を保存し、完了後「完了」をクリックします。

分類ポリシーのコピー作成

手順

1. コピーを作成する分類ポリシーを選択し、「コピー」ボタンをクリックします。
2. 必要に応じて、コピーしたポリシーの任意の項目を上書きします。 コピーのデフォルト名 (選択したポリシーの名前に接頭部 Copy of が付いたもの) を置き換えることを推奨します。
3. 「コピーの保存」ボタンをクリックして、新規分類ポリシーを保存します。 ポリシーは、「分類ポリシー定義」パネルに再表示されます。
4. 新規分類ポリシー定義のコンポーネントを変更する方法の説明については、『分類ポリシーの変更』を参照してください。

分類ルールの操作

手順

1. 「分類ポリシー・ファインダー」から「分類ポリシー・ルール」パネルを開きます。これを行うには、「ディスカバー」 > 「分類」 > 「分類ポリシー・ビルダー」にナビゲートします。
2. 既存の分類ポリシーを変更する場合は、「機密データのディスカバー」シナリオ (「ディスカバー」 > 「エンドツーエンド・シナリオ」 > 「機密データのディスカバー」) を使用することをお勧めします。分類ポリシー・グループを作成する場合は、同じ「機密データのディスカバー」シナリオを使用してください。グループを作成した場合も、それらのグループを明示的に選択する必要があります。

親トピック: 分類

新規分類ポリシー・ルールの追加

手順

1. 「ルールの追加」ボタンをクリックして、「分類ルール定義」パネルを開きます。
2. 「ルール名」を入力します。
3. オプションでルールの新規カテゴリーまたは分類 (あるいはその両方) を入力します。 デフォルトは、ポリシーの「分類ポリシー定義」から取られます。
4. このルールが一致した後で、分類ポリシーの次のルールを評価する必要がある場合は、 「突き合わせを続行」チェック・ボックスにマークを付けます。 デフォルトでは、ルールの一致後にルールの評価が停止されます。
5. 「ルール・タイプ」を選択します。 新規ルールの場合、「ルール・タイプ」は選択されていません。「ルール・タイプ」を選択すると、 そのルール・タイプの定義に必要なフィールドを組み込むことができるように、パネルが展開表示されます。 各ルール・タイプの定義方法の詳細については、以下のいずれかのセクションを参照してください。
   - カタログ検索ルールの定義 - 表または列の名前をデータベース・カタログで検索します。
   - データの検索ルールの定義 - データ内の特定の値またはパターンをマッチングします。
     注: 使用されるデータ・ソース定義内に定義されているデータベース認証 (ユーザー/パスワード) には、定義されるルール/検索に適切なレベルのアクセス権が必要です。例えば、Oracle の場合、 適切なロール (SYSTEM や DBA など) を持つユーザーは、 データベース・カタログ内でアクセス権を適切に検索できます。この注意は、「データ・ルール・タイプの検索」を使用する場合のシステム表の選択に適用されます。 ユーザーに SYSTEM ロールがない場合は、システム表をチェックしないでください。
   - 非構造化データの検索ルールの定義 - 非構造化データ・ファイル (CSV、テキスト、HTTP、HTTPS、Samba) 内の特定の値またはパターンをマッチングします。
6. 「新規アクション」ボタンをクリックして、 このルールが一致した場合に実行するアクションを追加します。 『分類ルール・アクションの追加』を参照してください。
7. 「OK」をクリックしてポリシーにルールを追加します。

カタログ検索ルールの定義

このタスクについて

カタログ検索ルールでは、 データベース・カタログで、指定されたパターンに一致する表または列 (あるいはその両方) の名前を検索します。 ワイルドカード文字 (0 個以上の任意の数の文字を表す %、 または単一文字を表す _ (下線)) を使用できます。

手順

1. 「表タイプ」行で、 検索対象となる表のタイプ (「シノニム」、「表」、または「ビュー」) の少なくとも 1 つにマークを付けます。 (デフォルトでは「表」が選択されています。)

2. オプションで、「表名 LIKE」ボックスに 具体的な名前またはワイルドカードに基づいたパターンを入力します。 これを省略すると、すべての表名が選択されます。
3. オプションで、「列名 LIKE」ボックスに 具体的な名前またはワイルドカードに基づいたパターンを入力します。 これを省略すると、すべての列名が選択されます。
4. 完了したら、「OK」ボタンをクリックします。

データの検索ルールの定義

このタスクについて

データの検索ルールでは、1 つ以上の列で、特定のデータ値を検索します。 ワイルドカード文字 (0 個以上の任意の数の文字を表す %、 または単一文字を表す _ (下線)) を使用できます。例えば「ルール・タイプ」が「データの検索」、「表タイプ」が「表」、 「表名 LIKE」が「CREDIT%」のように指定できます。

手順

1. 「表タイプ」行で、 検索対象となる表のタイプ (「シノニム」、「表」、または「ビュー」) の少なくとも 1 つにマークを付けます。 (デフォルトでは「表」が選択されています。)
2. オプションで、「表名 LIKE」行に 具体的な名前またはワイルドカードに基づいたパターンを入力します。 これを省略すると、すべての表名が選択されます。
3. 「データ・タイプ」行で、 検索する 1 つ以上のデータ・タイプを選択します。
4. オプションで、「列名 LIKE」行に 具体的な名前またはワイルドカード・パターンを入力します。 これを省略すると、すべての列名が選択されます。
5. オプションで、「最小長」を入力します。 これを省略すると、長さ制限がなくなります。
6. オプションで、「最大長」を入力します。 これを省略すると、長さ制限がなくなります。
7. オプションで、「検索 LIKE」フィールドに具体的な値またはワイルドカードに基づいたパターンを入力します。これを省略すると、すべての値が選択されます。
8. オプションで、「検索式」フィールドに、マッチングするパターンを定義するための正規表現を入力します。正規表現をテストするため、「正規表現」ボタンをクリックして、 「正規表現の作成」パネルを別ウィンドウで開きます。 正規表現の使用方法について詳しくは、『正規表現』を参照してください。
9. 「評価名」に、作成およびアップロード済みの完全修飾 Java™ クラス名をオプションで入力します。この Java クラス名は、文字列の起動および評価に使用されます。 入力されたクラス名がロード済みであるか、およびインターフェースに順応しているかどうかの検証は行われません。Java クラス・ファイルの作成とアップロードについて詳しくは、『カスタム評価』および『カスタム・クラスの管理』を参照してください。
10. オプションで、「限定起動」マーカーの名前を入力します。『「限定起動」マーカー』を参照してください。
11. 「ヒット率」フィールドに、このルールを起動するために達成しなければならない一致データのパーセンテージをオプションで入力します。検査された一致データのパーセンテージが入力したパーセンテージ値以上(>=) であれば、データが返されます。ただし、項目が空の場合、それは条件ではなく、ルールが起動されるかどうかに影響せず、ビュー画面にデータが返されることを意味します。パーセンテージ 0 を指定すると、そのルールはこの条件で起動され、データがビュー画面に返されます。パーセンテージ 100 を指定すると、すべてが一致することが求められます。
12. 「SQL の値と比較」フィールドに、SQL ステートメントをオプションで入力します。入力した SQL (唯一の列から情報が返されることが基本条件となっている必要があります) は、選択された表または列 (あるいはこの両方) に対して検索を行うための値グループとして使用されます。 「SQL の値と比較」を使用する場合には、以下のルールに従う必要があります。
    - SQL ステートメントは SELECT で始まる必要がある。
    - SQL ステートメントにセミコロン (;) は使用できない。
    - 入力した SQL で、正確に結果が返されるようにスキーマ値の名前を指定する必要がある。
    - 良い例:

      ```
      SELECT ename FROM scott.emp
      select EMPNUMBER from SYSTEM.EMP where EMPNUMBER in(5555,4444)
      select DNAME from SCOTT.DEPT where DNAME like 'A%G'
      SELECT ZIP from SCOTT.FOO where ZIP in (SELECT ZIP FROM SCOTT.FOO)
      ```

13. 「グループの値と比較」フィールドで、グループをオプションで選択します。 選択されたグループは、選択された表または列 (あるいはこの両方) に対して検索を行うための値グループとして使用されます。 グループ (PUBLIC または分類グループ) 内の値のいずれかが一致していれば、値のルールによってデータが返されます。
14. 「固有値の表示」チェック・ボックスにマークを付け、「コメント」に、分類ポリシー・ルールと一致し、起動した値の詳細を追加します。固有値を編集する場合は、「固有値のマスク」フィールドで正規表現を使用します。例えば、「固有値」チェック・ボックスにマークを付け、「固有値のマスク」フィールドで「([0-9]{2}-[0-9]{3})-[0-9]{4}」を使用して、最後の 4 桁をログに記録してから接頭部の数字を編集します。

非構造化データの検索ルールの定義

このタスクについて

非構造化データの検索ルールでは、非データベース・ファイルを検査します。

手順

1. オプションで、「検索 LIKE」ボックスに 具体的な値またはワイルドカードに基づいたパターンを入力します。これを省略すると、すべての値が選択されます。
2. オプションで、「検索式」ボックスに、 マッチングするパターンを定義するための正規表現を入力します。 正規表現をテストするため、RE アイコンをクリックして、「正規表現の作成」パネルを別ウィンドウで開きます。正規表現の使用方法について詳しくは、『正規表現』を参照してください。
3. オプションでマーカー名を入力します。

分類ルール・アクションの操作

手順

1. ルールの保存後、そのルールの「カスタマイズ」ボタンをクリックして ルール定義パネルに戻り、そこから 1 つ以上のルール・アクションを追加することができます。
2. 「新規アクション」ボタンをクリックして、「アクション」パネルを開きます。
3. 「アクション名」を入力します。
4. オプションで、「記述」に入力します。

5. リストからアクション・タイプを 1 つ選択します。 選択したアクションに応じて、パネルに表示されるフィールド・セットが異なります。
    - 「無視」および「結果をロギング」アクションでは、追加の情報は不要です。
        - 「無視」- 一致をログに記録せず、追加のアクションを実行しません。
        - 「結果をロギング」- 一致をログに記録し、追加のアクションを実行しません。
    - その他すべてのアクションについては、パネルに追加のフィールドが表示され、 追加の情報の入力が必要になります。
        - 「オブジェクト/フィールドのグループに追加」アクション
        - 「オブジェクトのグループに追加」アクション
        - 「アクセス・ルールの作成」アクション
        - 「プライバシー・セットの作成」アクション
        - 「ポリシー違反をロギング」アクション
        - 「アラートを送信」アクション
6. 「分類ルール」パネルにアクションを追加した後で、表に示すコントロールを使用して、定義されたアクションを変更できます。
7. ルール定義の処理が完了した後で、「OK」をクリックします。

親トピック: 分類

「オブジェクト/フィールドのグループに追加」アクション

このタスクについて

分類ルールが一致するごとに、Guardium システム上の選択したオブジェクト/フィールド・グループにメンバーが追加されます。全メンバーを置換したり、新規メンバーを追加したりするためのオプションがあります。

データベース・ファイルの場合、メンバーのオブジェクト・コンポーネントがデータベース表名になり、 フィールド・コンポーネントが列名になります。

非構造化データ・ファイルの場合、メンバーのオブジェクト・コンポーネントが (引用符で囲まれた) ファイル名になり、 フィールド・コンポーネントが列名になります。しかし、列名が判別できない場合、列には column1、 column2、のように名前が付けられます。

手順

1. 以下のいずれかを実行します。
    - リストからオブジェクト/フィールド・グループを 1 つ選択します。または、
    - 「グループ」ボタンをクリックして、グループ・ビルダーを使用して新規グループを定義し、その後、リストからそのグループを選択します。
2. オプションで「グループ内容の置換」ボックスにマークを付け、 選択したグループのメンバーシップを、このルールによって返されるメンバーによって完全に置き換えます。 デフォルトでは、このボックスにマークは付けられていません。 これはつまり、新規メンバーがグループに追加されますが、メンバーは削除されないことを意味します。 オンデマンドで実行されるジョブの場合、このボックスは無視され、 「結果の表示」パネルでメンバーを追加または置換する機会がユーザーに与えられます。
3. 「保存」ボタンをクリックしてルール定義にアクションを追加し、「アクション」パネルを閉じて、ルール定義パネルに戻ります。

「オブジェクトのグループに追加」アクション

このタスクについて

分類ルールが一致するごとに、Guardium システム上の選択したオブジェクト・グループにメンバーが追加されます。

データベース・ファイル・タイプの場合、メンバーがデータベース表名になります。 非構造化ファイル・タイプの場合、メンバー名がファイル名になります。

すべてのエントリーを置換したり、新規エントリーのみを追加したりするためのオプションがあります。

手順

1. 以下のいずれかを実行します。
    - リストからオブジェクト・グループを 1 つ選択します。または、
    - 「グループ」ボタンをクリックして、グループ・ビルダーを使用して新規グループを定義し、その後、リストからそのグループを選択します。
      注: 分類から生成されたグループで別名を使用する場合は、グループ・ビルダーを開き、分類から生成されたオブジェクト・グループを選択し、「変更」をクリックします。「グループ」ボタンの「別名」ボタンをクリックして、オブジェクト・グループの名前を変更します。
2. オプションで「グループ内容の置換」ボックスにマークを付け、 選択したグループのメンバーシップを、このルールによって返されるメンバーによって完全に置き換えます。 デフォルトでは、このボックスにマークは付けられていません。 これはつまり、新規メンバーがグループに追加されますが、メンバーは削除されないことを意味します。 オンデマンドで実行されるジョブの場合、このボックスは無視され、 「結果の表示」パネルでメンバーを追加または置換する機会がユーザーに与えられます。
3. 「実際のメンバー内容」から、schema.tablename が「Full」、tablename が「Name」であるグループにメンバーを追加するために使用される命名規則を選択してください。
4. 「保存」をクリックしてルール定義にアクションを追加し、「アクション」パネルを閉じて、ルール定義パネルに戻ります。

「アクセス・ルールの作成」アクション

このタスクについて

分類ルールが一致するごとに、既存のセキュリティー・ポリシー定義にアクセス・ルールが挿入されます。 更新後のセキュリティー・ポリシーは、インストールされません (このタスクは、通常は Guardium 管理者によって個別に実行されます)。

手順

1. リストからアクセス・ポリシーを 1 つ選択します。 そのポリシーに対するアクセス権限を保持している必要があります。
2. 「ルールの記述」ボックスにルール名を入力します。
3. 「アクセス・ルール・アクション」リストから、アクションを 1 つ選択します。

4. オプションでコマンド・グループを選択するか、「グループ」ボタンをクリックして、 グループ・ビルダーを使用して新規コマンド・グループを定義し、 その後、リストからそのコマンド・グループを選択します。
5. フィールド値を個別にログに記録するには、「フィールドの組み込み」チェック・ボックスにマークを付けます。それ以外の場合、表だけが記録されます (デフォルト)。
6. サーバー IP アドレスを組み込むには、「サーバー IP の組み込み」チェック・ボックスにチェックマークを付けます。
7. アラート・アクションを選択している場合、パネルに「受信者」行が 表示されるので、少なくとも 1 人以上のアラートの受信者を追加する必要があります。 「受信者の変更」をクリックして、1 人以上の受信者を追加します。
8. 「OK」をクリックして、 ルール定義にアクションを追加し、「アクション」パネルを閉じ、ルール定義パネルに戻ります。

「プライバシー・セットの作成」アクション

このタスクについて

分類ルールが一致するごとに、選択したプライバシー・セットのオブジェクト/フィールド・リストが置換されます。

データベース・ファイルの場合、プライバシー・セットのオブジェクト・コンポーネントがデータベース表名になり、 フィールド・コンポーネントが列名になります。

非構造化データ・ファイルの場合、プライバシー・セットのオブジェクト・コンポーネントが (引用符で囲まれた) ファイル名になり、 フィールド・コンポーネントが列名になります。しかし、列名が判別できない場合、列には column1、 column2、のように名前が付けられます。

手順

1. 以前に定義した、内容を置換する「プライバシー・セット」を選択します。
2. 「OK」ボタンをクリックして、 ルール定義にアクションを追加し、「アクション」パネルを閉じ、ルール定義パネルに戻ります。

「ポリシー違反をロギング」アクション

このタスクについて

分類ルールが一致するごとに、ポリシー違反がログに記録されます。 これはつまり、分類ポリシー違反が、生成されたアクセス・ポリシー違反 (およびオプションで相関アラート) と一緒にログに記録される (そしてレポート可能である) ことを意味します。

手順

1. リストから重大度コードを 1 つ選択します。
2. 「OK」ボタンをクリックして、 ルール定義にアクションを追加し、「アクション」パネルを閉じ、ルール定義パネルに戻ります。

「アラートを送信」アクション

このタスクについて

「OK」ボタンをクリックして、 ルール定義にアクションを追加し、「アクション」パネルを閉じ、ルール定義パネルに戻ります。

手順

1. リストから通知タイプ・コードを 1 つ選択します。
2. 「受信者の変更」ボタンをクリックして、1 人以上の受信者を追加します。 指定された受信者は、データ・ソースごと、ルールごと、アクションごとに 1 つのメールを受信します。したがって、データ・ソースに 3 つのルールがあり、各ルールに (少なくとも 1 つの一致がある) 2 つのアクションがある場合、 ユーザーは 2 * 3 = 6 通のメールを受け取ることになります。
3. 「OK」ボタンをクリックして、 ルール定義にアクションを追加し、「アクション」パネルを閉じ、ルール定義パネルに戻ります。

機密データのディスカバー

機密データをディスカバーして分類するためのエンドツーエンドのシナリオを作成します。

このタスクについて

組織の規模が大きくなり、クレジット・カード番号や個人の金融データなどの機密情報が複数のロケーションに伝搬するにつれて、ディスカバリー・プロセスと分類プロセスが重要になります。 こうした状況は、合併および買収の際や、元の所有者がいなくなった後もレガシー・システムを引き続き使用している場合に、多く発生します。その結果、現在、データを所有している人の知らない場所に機密データが存在する可能性があります。 機密データが存在することを知らなければ、それを保護することができないため、これはよくあるが非常に脆弱なシナリオです。

機密データのディスカバリー・シナリオは、以下のような企業セキュリティーの 3 つの重要な側面にわたります。

- ディスカバリー: 現行環境のどこかに存在する機密データの場所を探索する
- 保護: 機密データへのアクセス時にモニターとアラート処理を行う
- コンプライアンス: 機密データのディスカバリー・プロセスの結果をレビューするための監査証跡を作成する

「機密データのディスカバー」エンドツーエンド・シナリオ・ビルダーを使用して、複数の Guardium ツールを使いやすい、単一のインターフェースに統合することにより、ディスカバリー、保護、およびコンプライアンスのプロセスを簡素化します。

表 1. 機密データ・ディスカバー・ツールの一覧

値	シナリオ・タスク	記述	結果

値	シナリオ・タスク	記述	結果
ディスカバー	名前および記述	シナリオと、そのシナリオに関連するプロセスとポリシーについて、名前と記述を指定します。	分類プロセスと分類ポリシーが作成されます。 オプションで、新しいデータ・ソース定義が作成されます。
	ディスカバー対象	データのディスカバーと分類を行うためのルールとルール・アクションを作成します。	
	検索場所	スキャンするデータ・ソースを特定します。	
	ディスカバリーの実行	シナリオを実行して結果を確認し、特別なグループ化アクションとアラート・アクションを定義します。	
保護	レポートのレビュー		アクセス・ポリシーが作成されます。
順守	監査	受信者、配布順序、レビュー・オプションを定義します。	監査プロセスが作成されます。
	スケジュール	指定した間隔で実行されるスケジュールを作成します。	

この一連のタスクでは、新規ディスカバリー・シナリオを作成するプロセスについて説明します。 また、機密データをディスカバーするためのルールとルール・アクションから構成される*分類ポリシー*の作成方法、機密データをスキャンするためのデータ・ソースを特定して*分類プロセス*を作成する方法、グループ化やアラート処理などを行う特別なポリシーの定義方法、およびスケジュールされた間隔でさまざまな利害関係者に監査の結果を配布する*監査プロセス*の作成方法についても説明します。

機密データのディスカバー・シナリオにより、他の Guardium ツール (「分類ポリシー・ビルダー」や GuardAPI コマンドなど) を使用してアクセスできる基礎的なポリシーとプロセスを作成することができますが、ディスカバリー・シナリオの作成や修正を行うための GuardAPI コマンドは用意されていません。

1. ディスカバリー・シナリオ
   新規ディスカバリー・シナリオを作成するか、既存のディスカバリー・シナリオを選択してコピーまたは編集します。
2. 名前および記述
   ディスカバリー・シナリオの名前と記述を入力します。
3. ディスカバー対象
   機密データをディスカバーして分類するためのルールとルール・アクションから成るポリシーを作成します。
4. 検索場所
   機密データをスキャンするデータ・ソースを特定します。
5. ディスカバリーの実行およびレポートのレビュー
   オプションでディスカバリー・シナリオを実行し、結果をレビューします。
6. 監査
   オプションで、ディスカバリー・レポートおよび分類レポート用の受信者、配布順序、およびレビュー・オプションを定義することによって監査プロセスを作成します。
7. スケジューリング
   オプションで、定義された間隔で実行するように監査プロセスをスケジューリングすることによって、監査プロセスをアクティブにします。

次のタスク

次のセクションに進み、ディスカバリーおよび分類のシナリオの「名前および記述」を指定してください。
親トピック: ディスカバー

ディスカバリー・シナリオ

新規ディスカバリー・シナリオを作成するか、既存のディスカバリー・シナリオを選択してコピーまたは編集します。

手順

1. 「ディスカバー」 > 「エンドツーエンド・シナリオ」 > 「機密データのディスカバー」をナビゲートします。
2. ディスカバリー・シナリオを作成、コピー、または編集します。
   - アイコンをクリックして新規シナリオを作成します。
   - アイコンをクリックして、既存のシナリオまたはテンプレートをコピーします。
   - 「ディスカバリー・シナリオ」リストから既存のシナリオ名をクリックし、そのシナリオの編集を開始します。

   いくつかのディスカバリー・シナリオおよびテンプレートがデフォルトで提供され、以下が含まれます。

   GDPR [テンプレート]
   「GDPR [テンプレート]」シナリオは、GDPR コンプライアンス戦略のための最新セットのディスカバリー・ルールと言語サポートを提供します。テンプレートはコピーまたは編集して別の名前で保存できます。「GDPR [テンプレート]」は常に最新の GDPR ディスカバリー・ルールと言語サポートを受け取ります。

   GDPR
   「GDPR」シナリオは、GDPR コンプライアンス戦略の一部として使用できるディスカバリー・ルールの基本セットを提供します。 「GDPR」シナリオを編集して変更内容を保存できますが、このシナリオは時間の経過に伴い更新されたルールおよび言語サポートを受け取りません。
   重要: 「GDPR [テンプレート]」が使用できる場合、古い「GDPR」シナリオは更新を受け取らないため、「GDPR」シナリオを使用することは推奨されません。

親トピック: 機密データのディスカバー
次のトピック: 名前および記述

名前および記述

ディスカバリー・シナリオの名前と記述を入力します。

このタスクについて

ディスカバリー・シナリオに指定する名前は、基礎となるポリシーおよびプロセスの命名にも使用されます。

このステップの間に、ディスカバリー・シナリオにアクセス可能な*セキュリティー・ロール*を指定することもできます。

手順

1. 「名前および記述」セクションを開き、シナリオの名前と記述 (オプション) を指定または編集します。 ここで指定した名前を使用して、ディスカバリー・シナリオによって作成される、基礎となる分類プロセスと分類ポリシーの名前も設定されます。
   例: 「Find PCI」という名前のディスカバリー・シナリオの場合、「Find PCI」という名前の*分類プロセス*と、「Find PCI Classification Policy」(この後に日時スタンプが付加されます) という名前の*分類ポリシー*が作成されます。
2. タグ付け違反用のカテゴリー・ラベルと分類ラベルを指定します。 カテゴリー・ラベルと分類ラベルのデフォルト値は「機密 (Sensitive)」です。
3. オプションで「ロール」ボタンをクリックして、ディスカバリー・シナリオにアクセスできる*セキュリティー・ロール*を指定します。

次のタスク

ディスカバリー・シナリオの次のセクション、「ディスカバー対象」に進みます。
親トピック: 機密データのディスカバー
前のトピック: ディスカバリー・シナリオ
次のトピック: ディスカバー対象

ディスカバー対象

機密データをディスカバーして分類するためのルールとルール・アクションから成るポリシーを作成します。

このタスクについて

*分類ポリシー*には、機密データを特定してアクションを実行する一連のルールとルール・アクションが、順序を付けて格納されます。ポリシー内の各ルールは、そのルールと一致した場合に実行される条件付きアクションを定義します。条件付きテストは単純なものでも (表内のどこでも検出されるワイルドカード文字列など)、複数の条件を考慮する複雑なテストでも構いません。機密データのディスカバリー・シナリオの場合、ルールによってトリガーされるアクションとして、指定されたグループにオブジェクトを追加するグループ化アクションや、ルールが一致すると通知がトリガーされるアラート・アクションが可能です。 複数のグループ化アクションとアラート・アクションを結合して、一致したルールに対する高度な応答を作成するように指示することができます。

このタスクでは、ディスカバリー・シナリオで使用する分類ルールとルール・アクションを作成および編集するプロセスについて説明します。

手順

1. 「ディスカバー対象」セクションを開き、データをディスカバーするためのルールを定義します。
2. 「言語」メニューを使用して、選択した言語、および選択した言語が国語である国によって、ルール・テンプレートをフィルタリングします すべての「言語」メニュー選択項目で、クレジット・カード番号や E メール・アドレスのような汎用パターンのテンプレートが表示されます。
3. 以下のいずれかを行うことにより、ルールをディスカバリー・シナリオに追加します。
   - アイコンをクリックし、新規ルールを作成します。
   - 「分類ルール・テンプレート」表からルールを選択し、アイコンをクリックして事前定義ルールを追加します。
4. 新規ルールを定義するか、ルール・テンプレートを選択し、アイコンをクリックしてルール・テンプレートを編集します。
   a. 実行する検索のタイプに基づいて、「ルール・タイプ」を選択します。
      - 「データの検索」は、データ内の特定のパターンまたは値に一致します
      - 「カタログ検索」は、データベース・カタログ内の表名または列名に一致します
      - 「非構造化データの検索」は、非構造化データ・ファイル (例えば、CSV ファイル、TXT ファイル、または CEF ファイル) 内の特定の値またはパターンに一致します
   b. 名前と記述を指定します。その際にオプションで、「名前」フィールドの先頭に*特殊パターン・テスト*を指定できます。 ルール名は、「分類ポリシー・ビルダー」で、分類ポリシーと関連付けられたルールの命名にも使用されます。特殊パターン・テスト が必要な場合は、それに対応するテンプレートで作業をすることをお勧めします (例えば、クレジット・カード番号の場合は、銀行カード - クレジット・カード番号 を使用します)。
   c. 「ルール基準」セクションを開き、このルールの*正規表現*およびその他の検索条件を定義します。ルール・テンプレートで作業をしている場合は、デフォルトで適切な*正規表現*が指定されます。
      重要: 「機密データのディスカバー」シナリオで作成されたルールの場合、デフォルトの「データ・タイプ」には、「数値」と「テキスト」の両方が含まれます。
   d. 「アクション」セクションを開き、ルール基準と一致した場合に実行する*ルール・アクション*を定義します。
   e. 複数の*ルール・アクション*を定義するとき、オプションでアイコンをクリックし、アイコンとアイコンを使用してアクションの実行順序を変更できます。
   f. ルール定義の追加または編集が完了したら、「保存」をクリックし、ディスカバリー・シナリオの「ディスカバー対象」セクションに戻ります。
5. オプションで、アイコンをクリックして、アイコンとアイコンを使用してルールを適用する順序を変更します。 デフォルトの動作では、「ルール基準」で「突き合わせを続行」が選択されていない限り、最初の一致後にルールの実行が停止するため、ルールの順序は重要です。
6. ルールの作業が完了したら、「次へ」をクリックし、ディスカバリー・シナリオの次のセクションの作業を始めます。

次のタスク

ディスカバリー・シナリオの次のセクション、「検索場所」に進みます。
親トピック: 機密データのディスカバー
前のトピック: 名前および記述

次のトピック: 検索場所
関連概念:
正規表現
関連タスク:
分類ルール・アクションの操作
関連資料:
実際のメンバー内容
ルール基準
特殊パターン・テスト

ルール基準

表 1.

属性	記述
表タイプ	検索対象の表タイプとして、「シノニム」、「表」、または「ビュー」のうち 1 つ以上を選択します。デフォルトでは「表」が選択されています。
データ・タイプ	検索対象のデータ・タイプとして、「数値」、「テキスト」、または「日付」のうち 1 つ以上を選択します。デフォルトでは「数値」と「テキスト」が選択されています。
検索式	オプションで、マッチングする検索パターンを定義するための正規表現を入力します。正規表現をテストするには、「RE」ボタンをクリックし、正規表現エディターを開きます。
表名 LIKE	オプションで、特定の名前またはワイルドカード・パターンを入力します。これを省略すると、すべての表名が選択されます。
列名 LIKE	オプションで、特定の名前またはワイルドカード・パターンを入力します。これを省略すると、すべての列名が選択されます。
突き合わせを続行	このルールが一致した後で、分類ポリシーの次のルールを評価する必要がある場合は、「突き合わせを続行」チェック・ボックスにマークを付けます。 デフォルトでは、ルールが一致した時点でルールの評価が停止します。
検索ワイルドカード	オプションで、特定の値またはワイルドカード・パターンを入力します。これを省略すると、すべての値が選択されます。
最小長	オプションで、「最小長」を入力します。これを省略すると、長さ制限がなくなります。
最大長	オプションで、「最大長」を入力します。これを省略すると、長さ制限がなくなります。
評価名	オプションで、作成およびアップロード済みの完全修飾 Java™ クラス名を入力します。 この Java クラス名は、文字列の起動および評価に使用されます。 注: 入力されたクラス名がロード済みであるか、およびインターフェースに順応しているかどうかの検証は行われません。
「限定起動」マーカー	「限定起動」マーカーを使用すると、分類ルールをグループ化することができます。同じマーカーを持つルールは同時に起動されます。さらに、1 つのマーカーを使用して返されるルールはすべて、同じ名前の表に基づいてデータを返す必要があります。 同じマーカーを使用して 2 つ以上のルールが定義されている場合、それらのルールは一緒に起動されます。両方のルールが同じ表で起動された場合、それらは両方ともログに記録され、それぞれのアクションが呼び出されます。 これに対して、ある表でいずれか一方のルールのみが起動された場合、ルールはどちらもログに記録されず、それらのアクションも呼び出されません。複数のルールを一緒に起動できるようにすることは、同じ表内に複数の機密データが同時に現れる場合が懸念されるときに重要になります。 例えば、1 つの表に社会保障番号とマサチューセッツ州の運転免許証の両方が含まれる場合に、それを知ることができます。 「限定起動」マーカーは定数値であり、任意の値を指定でき、グループ化するルール全体でまったく同じ値でなければなりません。 つまり、1 つのルールのマーカー名が ABC であれば、そのルールと一緒にグループ化する他のルールのマーカー名も ABC でなければなりません。 「限定起動」マーカーは、「突き合わせを続行」フラグとも連携します。 例えば、以下のルールが定義されており、ルール 3 が「突き合わせを続行」と一致しない場合、他の 3 つのマーカー・ルールがすべて正となったかどうかに関係なく、結果は返されません。これは、ルール 4 の実行まで至らなかったためです。必ずすべての「限定起動」マーカーが実行され、結果が正になる必要があるので、このグループ化は起動されません。 ルール 1. 起動マーカー・ルール "ABC"(突き合わせを続行) ルール 2. 起動マーカー・ルール ABC (突き合わせを続行) ルール 3. 起動マーカー以外のルール・タイプ (突き合わせを続行) ルール 4. 起動マーカー・ルール "ABC"(突き合わせを続行)
ヒット率	オプションで、このルールを起動するために達成しなければならない一致データのパーセンテージを入力します。検査された一致データのパーセンテージが入力したパーセンテージ値以上 (>=) であれば、データが返されます。ただし、項目が空の場合、それは条件ではなく、ルールが起動されるかどうかに影響せず、ビュー画面にデータが返されることを意味します。 パーセンテージ 0 を指定すると、そのルールはこの条件で起動され、データがビュー画面に返されます。パーセンテージ 100 を指定すると、すべてが一致することが求められます。

属性	記述

SQL の値と比較	オプションで、「SQL ステートメント」を入力します。入力した SQL (唯一の列から情報が返されることが基本条件となっている必要があります) は、選択された表および列に対して検索を行うための値グループとして使用されます。
	注: 「SQL の値と比較」を使用する場合には、以下のルールに従う必要があります。
	• SQL ステートメントは `SELECT` で始まる必要がある。
	• SQL ステートメントには ; (セミコロン) を使用できない。
	• 入力した SQL で、正確に結果が返されるようにスキーマ値の名前を指定する必要がある。
	• 良い例:
	`SELECT ename FROM scott.emp`
	`select EMPNUMBER from SYSTEM.EMP where EMPNUMBER in(5555,4444)`
	`select DNAME from SCOTT.DEPT where DNAME like 'A%G'`
	`SELECT ZIP from SCOTT.FOO where ZIP in (SELECT ZIP FROM SCOTT.FOO)`

グループの値と比較	オプションで、グループを選択します。選択されたグループは、選択された表および列に対して検索を行うための値グループとして使用されます。グループ (PUBLIC または分類グループ) 内の値のいずれかが一致していれば、値のルールによってデータが返されます。
固有値の表示	「固有値の表示」チェック・ボックスにマークを付けると、分類ポリシー・ルールと一致した値の詳細が結果レポートのコメント・フィールドに追加されます。
固有値のマスク	固有値を編集する場合は、「固有値のマスク」フィールドで正規表現を使用します。例えば、「固有値の表示」チェック・ボックスにマークを付け、「固有値のマスク」フィールドで「`([0-9]{2}-[0-9]{3})-[0-9]{4}`」を使用して、最後の 4 桁をログに記録し、接頭部の数字を編集します。

親トピック: ディスカバー対象

実際のメンバー内容

「実際のメンバー内容」フィールドを使用して、「オブジェクトのグループに追加」ルール・アクションによるオブジェクトのラベル付け方法を定義します。

表 1.

「実際のメンバー内容」の選択肢	グループの値
オブジェクト名のみ	表名
Like Name%	tableName%
Like %Name	%tableName
Like %Name%	%tableName%
%/%.Name	%%.tableName
完全修飾名	schemaName.tableName
Like Full%	schemaName.tableName%
Like %Full	%schemaName.tableName
Like %Full%	%schemaName.tableName%
%/Full	%%.schemaName.tableName
Read/%.Name	Read/%.tableName
Change/%.Name	Change/%.tableName
Read/Full	Read/schemaName.tableName
Change/Full	Change/schemaName.tableName

ルールによって表名 `JJ_CREDIT_CARD` がスキーマ `DB2INST1` から返され、なおかつ「オブジェクトのグループに追加」アクションが指定されている場合、「実際のメンバー内容」の各選択項目は以下のように動作します。

- 「完全修飾名」を選択した場合は、`DB2INST1.JJ_CREDIT_CARD` が選択したグループに追加されます。
- 「オブジェクト名のみ」を選択した場合は、`JJ_CREDIT_CARD` が選択したグループに追加されます。
- 「Change/Full」を選択した場合は、`Change/DB2INST1.JJ_CREDIT_CARD` が選択したグループに追加されます。

親トピック: ディスカバー対象

検索場所

機密データをスキャンするデータ・ソースを特定します。

このタスクについて

データ・ソースには、データベースやリポジトリーに関する情報 (データベースのタイプ、リポジトリーの場所、関連付けられる可能性のある認証資格情報など) が格納されます。データ・ソースをディスカバリー・シナリオに追加すると、選択されたデータ・ソースに*分類ポリシー*が適用されている場所に*分類プロセス*が作成されます。

このタスクでは、機密データの検索対象となるデータ・ソースを特定します。

手順

1. 「検索場所」セクションを開き、機密データの検索対象となるデータ・ソースを特定します。

2. 以下のいずれかを行うことにより、データ・ソースをディスカバリー・シナリオに追加します。
   -  アイコンをクリックして「データ・ソースの作成」ダイアログを開き、新規のデータ・ソース定義を追加します。
   - 「選択可能なデータ・ソース」表からデータ・ソースを選択し、  アイコンをクリックして、既存のデータ・ソースを追加します。
3. 新規のデータ・ソースを定義するか、または既存のデータ・ソースを選択し、  アイコンをクリックしてそのデータ・ソースを編集します。 ディスカバリー・シナリオ経由で定義された新規データ・ソースは、「データ・ソース定義」ツールを使用して表示や編集を行うこともできます。
   a. データ・ソースの名前を入力または編集します。
   b. 「データベース・タイプ」メニューから適切なデータベース・タイプを選択し、データ・ソース定義を完了するために必要な情報を入力します。使用可能なフィールドは、選択したデータベース・タイプによって異なります。
   c. データ・ソース定義の編集が完了したら、「保存」をクリックして作業内容を保存します。オプションで「接続のテスト」をクリックし、データ・ソース接続を検査します。
   d. データ・ソース定義の作業が完了したら、「閉じる」をクリックしてダイアログを閉じます。
4. クラウド・データベースにこの分類プロセスを使用する場合は、「Cloud DB のオブジェクト監査の有効化」も選択します。
5. データ・ソースの追加が完了したら、「次へ」をクリックし、ディスカバリー・ワークフローの次のセクションの作業を始めます。

タスクの結果

分類プロセス は、データ・ソースをディスカバリー・シナリオに追加して、そのシナリオを保存した後に作成されます。 このプロセスを表示して直接編集するには、「分類プロセス・ビルダー」を使用します。

次のタスク

ディスカバリー・ワークフローの次のセクション、「ディスカバリーの実行」に進みます。
親トピック: 機密データのディスカバー
前のトピック: ディスカバー対象
次のトピック: ディスカバリーの実行およびレポートのレビュー
関連概念:
データ・ソース
関連タスク:
データ・ソース定義の作成

ディスカバリーの実行およびレポートのレビュー

オプションでディスカバリー・シナリオを実行し、結果をレビューします。

このタスクについて

機密データをディスカバーし、検索するデータ・ソースを特定するためのポリシーを定義した後、*分類プロセス* を実行して結果をレビューすることができます。プロセスを実行して結果をレビューすると、ポリシーを改良することができます。例えば、結果の範囲が広すぎる場合は、追加の検索条件を指定します。希望どおりの結果を得るには、ポリシーの改良、プロセスの実行、および結果の評価を数回繰り返すことが必要な場合があります。

手順

1. 「ディスカバリーの実行」セクションを開き、ディスカバリー・シナリオをテストします。
2. 「今すぐ実行する」をクリックして開始します。
   重要:
   - 指定したポリシーと、検索対象として選択したデータ・ソースの数によっては、機密データの特定プロセスが完了するまで数分以上かかる場合があります。このプロセスの状況は、「今すぐ実行する」ボタンの横に表示されます。また、「Guardium ジョブ・キュー」オプションを使用して、プロセスをモニターすることもできます。
   - 「分類プロセス・ビルダー」にアクセスして、*分類プロセス* を選択し、「今すぐ 1 回実行」をクリックすることで、*分類プロセス* を実行することもできます。
3. ディスカバリー・シナリオの実行が完了したら、「レポートのレビュー」セクションを開いて結果を確認します。
4. 結果をレビューしながら、結果に基づいて追加のルールやアクションを定義できます。 結果を絞り込む場合は、「フィルター」を使用します (結果の数が 10,000 件を超えている場合、フィルタリング機能は使用できません)。
   a. アクションを定義する対象のデータを含む行 (複数可) を選択します。
   b. 「グループに追加」をクリックしてグループ化アクションを定義するか、「拡張アクション」をクリックして、アラート、ロギング、または無視などの他のアクションを定義します。
   c. アクションを定義するダイアログの入力が完了したら、「OK」をクリックして結果レポートに戻ります。
   重要:
   - 結果表から追加されたアクションは、結果表から呼び出した場合にのみ実行される特別なアクションとして認識されます。これらのアクションは、ディスカバリー・シナリオの「ディスカバー対象」 > 「ルールの編集」 > 「アクション」セクションには表示されません。また、ディスカバリー・シナリオや関連する *分類プロセス* の一部として自動的に実行されることもありません。
   - アラート・アクションおよびアクセス・ルールのレビュー、編集、インストールを行うには、「ポリシー・ビルダー」を使用します。
   - グループ化アクションをレビューおよび編集するには、「グループ・ビルダー」を使用します。
   - プライバシー・セットのアクションをレビューするには、「プライバシー・セット・ビルダー」を使用します。
   - ポリシー・ロギング・アクションをレビューするには、「インシデント管理」ツールを使用します。
5. 結果レポートのレビューが完了したら、「次へ」をクリックし、ディスカバリー・シナリオの次のセクションの作業を始めます。

タスクの結果

機密データの検索を実行したら、「今すぐ実行する」ボタンの横に表示される検索プロセスの状況をモニターします。または、「Guardium ジョブ・キュー」オプションを使用することもできます。「グループ・ビルダー」を使用すると、任意のグループ化アクションをレビューすることができます。「ポリシー・ビルダー」を使用すると、結果表から追加された任意のアラート・アクションのレビューとインストールを行うことができます。

次のタスク

(オプション) ディスカバリー・シナリオの次のセクション、「監査」に進みます。
親トピック: 機密データのディスカバー
前のトピック: 検索場所
次のトピック: 監査

監査

オプションで、ディスカバリー・レポートおよび分類レポート用の受信者、配布順序、およびレビュー・オプションを定義することによって監査プロセスを作成します。

このタスクについて

ディスカバリー・ワークフローの結果に対して、任意の数の受信者を定義できます。また、受信者が結果を受け取る順序を制御することもできます。さらに、結果が次の受信者に送信される前に、受信者が結果に署名する必要があるかどうかなどのプロセス制御オプションも指定できます。

ディスカバリー・シナリオに受信者を追加することによって作成された*監査プロセス*は、シナリオの名前を継承します。 例えば、「Find PCI」という名前のディスカバリー・シナリオに受信者を追加すると、「Find PCI Audit process」 (後に日時スタンプが続く) という名前の*監査プロセス*が作成されます。

手順

1. 「監査」セクションを開き、ディスカバリー・レポートの受信者を定義します。
2. アイコンをクリックし、レポートの配布方法を指定するオプションを定義して、レポートの受信者をディスカバリー・シナリオに追加します。
   - Guardium ユーザー、ロール、またはグループにレポートを送信する場合は、プロセス制御オプションを定義する必要があります。
   - E メール受信者にレポートを送信する場合は、E メール・アドレスを指定し、その E メール受信者に適した Guardium ユーザー名でレポートをフィルターに掛けます。
3. 「OK」をクリックして、受信者をディスカバリー・ワークフローに追加します。 必要に応じて、追加の受信者をシナリオに追加します。
4. オプションで、アイコンをクリックして、アイコンと アイコンを使用して、レポートが受信者に配布される順序を変更します。 これにより、レポートが次の受信者に送信される前にどの受信者がレポートのレビューまたは署名を行う必要があるかが決まるため、*順次*配布を使用する場合はこれが重要です。
5. 受信者の追加、編集、順序付けが完了したら、「次へ」をクリックし、ディスカバリー・ワークフローの次のセクションの作業を始めます。

タスクの結果

*監査プロセス*は、受信者を定義して、ディスカバリー・シナリオを保存した後に作成されます。 このプロセスの表示、編集、実行を直接行うには、「監査プロセス・ビルダー」を使用します。

*監査プロセス*は、ディスカバリー・シナリオの「スケジュール」セクションを使用してスケジュールされるか、「監査プロセス・ビルダー」を使用してスケジュールされるまで、非アクティブのままです。「監査プロセス・ビルダー」にアクセスして、*監査プロセス*を選択し、「今すぐ 1 回実行」をクリックすることで、*監査プロセス*を実行することもできます。

次のタスク

(オプション) ディスカバリー・ワークフローの次のセクション、「スケジュール」に進みます。
親トピック: 機密データのディスカバー
前のトピック: ディスカバリーの実行およびレポートのレビュー
次のトピック: スケジューリング
関連概念:
監査プロセスの作成

スケジューリング

オプションで、定義された間隔で実行するように監査プロセスをスケジューリングすることによって、監査プロセスをアクティブにします。

このタスクについて

スケジュールは、ディスカバリー・シナリオの「監査」セクションで受信者が指定されていれば、それと合わせて*監査プロセス*の一部となります。 スケジュールを定義することにより、指定した間隔で*監査プロセス*が実行され、関連付けられている*分類プロセス*からの結果が定期的に配布されてレビューされるようになります。

手順

1. 「スケジュール」セクションを開き、データをディスカバーするためのスケジュールを定義します。
2. 「スケジュールの基準」メニューを使用して、*監査プロセス*の間隔 (日次または月次) を設定します。
3. 「スケジュール開始間隔」チェック・ボックスと「繰り返しの間隔」チェック・ボックスを使用して、*監査プロセス*を実行する 1 日あたりの回数と毎時間内の回数を定義します。
4. 「開始日時」コントロールを使用して、スケジュールを開始する明示的な日時を定義します。
5. 「スケジュールのアクティブ化」チェック・ボックスをクリアして、スケジューリング情報を後で使用できるように保持しながら、*監査プロセス*を非アクティブにします。 「スケジュールのアクティブ化」ボックスは、デフォルトではチェック・マークが付いています。これは、スケジュールを保存した後、監査プロセスがアクティブになることを意味します。
6. スケジュールの定義が完了したら、「保存」をクリックして編集を完了し、ワークフロー・エディターを閉じます。

タスクの結果

監査プロセス は、スケジュールを定義して、ディスカバリー・シナリオを保存した後に作成されます。 この監査プロセスを表示して直接編集するには、「監査プロセス・ビルダー」を使用します。スケジュールされている監査タスクの状況、開始時刻、次回の起動時間を確認するには、「スケジュール済みジョブ」レポートを表示します。

親トピック: 機密データのディスカバー
前のトピック: 監査
関連概念:
監査プロセスの作成

正規表現

正規表現を使用して、データに含まれる複合パターンを求めてトラフィックを検索することができます。

IBM Guardium の正規表現の実装は POSIX 1003.2 に準拠します。詳しくは、Open Group の Web サイト www.opengroup.org を参照してください。 正規表現を使用して、データに含まれる複合パターンを求めてトラフィックを検索することができます。例については、『ポリシー』を参照してください。

このヘルプ・トピックでは、正規表現の作成ツールの使用法について説明し、一般的に使用される特殊文字や構造の表を示します。 正規表現の構造や使用方法についての包括的な説明は しません。詳しくは、Open Group の Web サイトを参照してください。

正規表現を使用したパターン・マッチングまたは XML マッチングで 注意すべき重要なポイントは、一致の検索は文字列の先頭から開始し、 その表現と一致する最初のシーケンスが検出されると停止する ということです。異なる正規表現または同じ正規表現を、パターン・マッチングおよび XML マッチングに同時に使用できます。

注: IBM Guardium は、英語以外の言語の正規表現はサポートしていません。

正規表現の作成ツールの使用

入力フィールドで正規表現の入力が要求される場合、正規表現の作成ツールを使用して、 正規表現のコード化およびテストを行うことができます。「正規表現の作成」アイコンは、ポリシー・ビルダーの「ルールの追加」の下にあります。

正規表現の作成ツールを開くには、正規表現を入力するフィールドの隣にある アイコンをクリックします。フィールドに既に何か入力されている場合は、入力された内容が「正規表現の作成」パネルの「正規表現」ボックスにコピーされます。

1. ドロップダウン・リストから正規表現のカテゴリーを選択します。
2. ドロップダウン・リストからパターンを選択します。
3. 「正規表現 」ボックスで、表現を入力または変更します。
4. 表現をテストするには、「突き合わせるテキスト」ボックスにテキストを入力して、「テスト」ボタンをクリックします。
   - 表現にエラー (右中括弧の欠落など) が含まれている場合は、 「構文エラー」メッセージ で通知されます。
   - 「一致するものが見つかりました」というメッセージは、入力したテキスト内に正規表現との一致が検出されたことを示します。
   - 一致が検出されない場合は、「一致するものが見つかりません」というメッセージが表示されます。
5. ステップを何度も繰り返し、目的に合わせて、正規表現が予想どおりに一致すること、および一致しないことを検査することをお勧めします。
6. 表現の最後に特殊文字を入力する場合は、 「要素の選択 」リストから選択できます。他の場所に特殊文字を入力する場合は、 その文字を入力するか、コピーする必要があります。
7. 変更およびテストが終了したら、 「OK」をクリックし、 「正規表現の作成」パネルを閉じて、正規表現を定義パネルにコピーします。

特殊文字と構造

以下の表に、一般的に使用される特殊文字と構造のサマリーを 示します。

表 1. 特殊文字と構造

文字	使用法	例	一致	不一致
リテラル	以下に示す 特殊文字以外の文字 (大/小文字の区別あり) の正確なシーケンスに一致	can	can	Can cab caN
. (ドット)	復帰 または改行 (¥n) 文字を含む、すべての文字に一致	ca.	can cab	c cb
*	先行する 文字のゼロ個以上のインスタンスに一致	Ca*n	Cn Can Caan	Cb Cabn
^	後続の文字で 始まる文字列に一致	^C.	Ca	ca a
$	先行する文字で 終了する文字列に一致	C.n$	Can Cn	Cab
+	先行する文字の 1 つ以上のインスタンスに一致	^Ca+n	Can Caan	Cn
?	先行する文字の ゼロまたは 1 つのインスタンスに一致	Ca?n	Cn Can	Caan
|	先行するパターン または後続のパターンのいずれかと一致	Can|cab	Can cab	Cab
(x ...)	括弧で 囲まれたシーケンスと一致	(Ca)*n	Can XaCan	Cn CCnn
{n}	先行する文字の正確に n 個のインスタンスと一致	Ca{3}n	Caaan	Caan Caaaan
{n,}	先行する文字の n 個以上のインスタンスに一致	Ca{2,}n	Caan Caaaan	Can Cn
{n,m}	先行する文字の n 個から m 個のインスタンスに一致	Ca{2,3}n	Caan Caaan	Can Caaaan
[a-ce]	セット内の 単一文字に一致。ダッシュは連続するシーケンスを示す。 例えば、[0-9] は任意の数字に一致。	[C-FL]an	Can Dan Lan	Ban
[^a-ce]	指定したセットに ない文字に一致	[^C-FL]an	aan Ban	Can Dan
[[.char.]]	囲まれた文字、または「名前付き文字の表」に含まれる名前付き文字に一致	[[.~.]]an または [[.tilde.]]an	~an	@an

文字	使用法	例	一致	不一致
[[:class:]]	「文字クラス表」の指定された文字クラスに含まれる任意の文字に一致	[[:alpha:]]+	abc	ab3

名前付き文字の表 (英語)

以下の表で、正規表現の大括弧ペア内で使用できる標準文字名について説明します ([[.char]])。 文字名はロケーション固有であるため、 英語版以外の Guardium® では異なる文字名のセットを使用している場合があります。

- NUL ¥0
- SOH ¥001
- STX ¥002
- ETX ¥003
- EOT ¥004
- ENQ ¥005
- ACK ¥006
- BEL ¥007
- alert ¥007
- BS ¥010
- backspace ¥b
- HT ¥011
- tab ¥t
- LF ¥012
- newline ¥n
- VT ¥013
- vertical-tab ¥v
- FF ¥014
- form-feed ¥f
- CR ¥015
- carriage-return ¥r
- SO ¥016
- SI ¥017
- DLE ¥020
- DC1 ¥021
- DC2 ¥022
- DC3 ¥023
- DC4 ¥024
- NAK ¥025
- SYN ¥026
- ETB ¥027
- CAN ¥030
- EM ¥031
- SUB ¥032
- ESC ¥033
- IS4 ¥034
- FS ¥034
- IS3 ¥035
- GS ¥035
- IS2 ¥036
- RS ¥036
- IS1 ¥037
- US ¥037
- space ' '
- exclamation-mark !
- quotation-mark "
- number-sign #
- dollar-sign $
- percent-sign %
- ampersand &
- apostrophe ¥'
- left-parenthesis (
- right-parenthesis)
- asterisk *
- plus-sign +
- comma ,
- hyphen -
- period .
- full-stop .
- slash /
- solidus /
- zero 0
- one 1
- two 2
- three 3
- four 4
- five 5
- six 6
- seven 7

- eight 8
- nine 9
- colon :
- semicolon ;
- less-than-sign <
- equals-sign =
- greater-than-sign >
- question-mark ?
- commercial-at @
- left-square-bracket [
- right-square-bracket]
- backslash ¥
- reverse-solidus ¥¥
- circumflex ^
- circumflex-accent ^
- underscore _
- low-line _
- grave-accent `
- left-brace {
- left-curly-bracket {
- right-brace }
- right-curly-bracket
- vertical-line |
- tilde ~
- DEL 177
- NULL 0

名前付き文字クラス表 (英語)

以下の表で、正規表現の大括弧ペア内で参照できる標準文字クラスについて説明します ([[:class:]])。 文字クラスはロケーション固有であるため、英語版以外の Guardium では異なる文字名のセットを使用している場合があることに注意してください。

- alnum - 英数字 (a-z、A-Z、0-9)
- alpha - 英字 (a-z、A-Z)
- blank - 空白文字 (ブランク、改行、復帰)
- cntrl - 制御
- digit - 0-9
- graph - グラフィックス
- lower - 英小文字 (a-z)
- print - 印刷可能文字
- punct - 句読文字
- space - スペース、タブ、改行、および復帰
- upper - 英大文字
- xdigit - 16 進数の数字 (0-9、a-f)

正規表現の例

任意の正規表現をコピーして、 正規表現の入力が要求されるフィールドに貼り付けることができます。これらの例を使用する場合は、正規表現の作成ツールでその例を使用し、一致または不一致のさまざまな値を入力して試すことを強くお勧めします。これによって、その表現と突き合わせられるものを正確に理解することができます。

正規表現の例

社会保障番号 (ハイフンが必要) [0-9]{3}-[0-9]{2}-[0-9]{4}

電話番号 (北アメリカ - 3334445555、333.444.5555、333-444-5555、333 444 5555、(333) 444 5555、およびそのすべての組み合わせと一致) ¥(?[0-9]{3}¥)?[-.]?[0-9]{3}[-.]?[0-9]{4}

郵便番号 - (カナダ) [ABCEGHJKLMNPRSTVXY][0-9][A-Z] [0-9][A-Z][0-9]

郵便番号 - (英国) [A-Z]{1,2}[0-9][A-Z0-9]? [0-9][ABD-HJLNP-UW-Z]{2}

郵便番号 - (米国) (5 桁が必須で、ハイフンと 4 桁が続く場合がある) [0-9]{5}(?:-[0-9]{4})?

クレジット・カード番号 [0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}

親トピック: ディスカバー

ファイル・サーバー内での機密データのディスカバーおよび分類

ファイル・アクティビティー・モニターは、UNIX ファイル・サーバーおよび Windows ファイル・サーバー上の機密データの保全性と保護を確保します。

- ファイル・アクティビティー・モニター・コンポーネントのインストールおよびアクティブ化
  GIM クライアントをファイル・サーバーにインストールしてから、それを使用してファイル・アクティビティー・モニター S-TAP およびディスカバリー・エージェントをインストールします。
- ファイルのディスカバリーおよび分類 GIM パラメーター
  以下の GIM パラメーターを使用して、コレクターごとにファイル・ディスカバリーと分類を構成します。
- FAM 判定プランのカスタマイズ
  判定プランは、ファイル内の機密の内容を識別するために使用されます。Guardium FAM ディスカバリー・エージェントは、HIPAA、PCI、SOX、およびソース・

コードのデフォルトの判定プランを提供します。デフォルトの判定プランを使用して、結果のレポート/調査ダッシュボードから分類エンティティーを変更できます。また、IBM コンテンツ分類ワークベンチを使用して、新しいプランを作成したり、既存のプランを変更したりできます。

親トピック: ディスカバー
関連情報:
Guardium を使用したファイル・アクティビティーのモニター (ビデオ)

ファイル・アクティビティー・モニター・コンポーネントのインストールおよびアクティブ化

GIM クライアントをファイル・サーバーにインストールしてから、それを使用してファイル・アクティビティー・モニター S-TAP およびディスカバリー・エージェントをインストールします。

始める前に

- ライセンス・キーをインストールする必要があります。『ライセンス・キーのインストール』を参照してください。
- S-TAP のインストールが必須。ファイル・モニターおよびポリシー実施のために必要です。
- FAM ディスカバリー・エージェント (別名 FAM バンドルまたは FAM エージェント) にアクセスできなければなりません。これはファイルのディスカバリーおよび分類に必須です。

ヒント: FAM ディスカバリー・エージェントを AIX で正常にインストールするには、/etc/security/limits file: default: data = -1 の行を変更して、プロセス・データのサイズを無制限に設定することが推奨されます。

このタスクについて

手順

1. ファイル・サーバーに GIM クライアントをインストールします。『Guardium Installation Manager』を参照してください。
2. S-TAP および FAM バンドルをダウンロードし、アクセス可能なドライブに保存します。 ファイル・サーバー OS 用の正しいモジュールを選択します。UNIX バンドルの名前は次のようになります。 guard-bundle-FAM_r*****_trunk_*****.gim. Windows バンドルは次のようになります。 guard-FAM-guardium_r*****Windows-Server-x86_x64_ia64.gim.
3. 中央マネージャーが存在する場合は中央マネージャーで、存在しない場合はアプライアンスで、S-TAP モジュールと FAM バンドルをアップロードしてインポートします。
   a. 「管理」 > 「モジュール・インストール」 > 「モジュールのアップロード」にナビゲートします。
   b. 「モジュールのアップロード」で「参照」をクリックし、S-TAP バンドルにナビゲートして選択します。「アップロード」をクリックします。
   c. 「参照」をクリックして、FAM バンドルにナビゲートします。「アップロード」をクリックします。
   d. 「アップロード済みモジュールのインポート」で、S-TAP および FAM バンドルを選択して、「インストール/更新」をクリックします。
4. 以下のようにして S-TAP をインストールします。
   a. S-TAP モジュールをファイル・サーバーにインストールします。「管理」 > 「モジュール・インストール」 > 「クライアント別の設定」(レガシー) にナビゲートします。すべての登録済みクライアントを表示するには、「検索」をクリックします。
   b. ファイル・サーバー (複数可) を選択し、「次へ」をクリックします。 ファイル・アクティビティー・モニターに固有の S-TAP パラメーターはありません。
   c. 「選択したものに適用」をクリックしてから「インストール/更新」をクリックします。ただちにインストールすることも、後でインストールを実行するようスケジュールすることもできます。
   d. Guardium レポートの「S-TAP 状況モニター」を表示することで (「マイ・ダッシュボード」からレポートを追加)、S-TAP が正しくインストールされたか検査します。FAM 接尾部のある S-TAP ホストを探します。
5. 以下のようにして FAM バンドルをインストールして構成します。
   a. 「管理」 > 「モジュール・インストール」 > 「クライアント別の設定」(レガシー) にナビゲートします。すべての登録済みクライアントを表示するには、「検索」をクリックします。
   b. ファイル・サーバーを選択し、「次へ」をクリックします。
   c. アップロードした FAM モジュールを選択します。(Windows では、「バンドルのみの表示」チェック・ボックスのチェック・マークを外すことが必要な場合があります。)
   d. 注: grdapi コマンド gim_update_client_params を使用して GIM パラメーターを構成することもできます。
   スキャンするディレクトリーの SOURCE_DIRECTORIES など、FAM ディスカバリー・エージェントのパラメーターを構成します。デフォルトでは、エージェントはライセンス情報の基本スキャンのみ実行します。SOX、HIPAA など、判定プランに基づいたスキャンを有効にするには、FAM_IS DEEP_ANALYSIS を true に設定する必要があります。 デフォルトでは、すべてのデフォルト判定プランが使用されます。使用される判定プランを指定できます。スキャンのデフォルト・スケジュールは 12 時間ごとで、構成直後に開始されます。GIM パラメーター FAM_SCHEDULER_HOUR_TIME_INTERVAL、FAM_SCHEDULER_START、および FAM_SCHEDULER_REPEAT を使用して、これらの設定を変更できます。 ファイルのディスカバリーおよび分類 GIM パラメーターにある完全なパラメーター・リストを参照してください。
   e. 「選択したものに適用」をクリックし、次に「インストール/更新」をクリックします。ここで、ただちにインストールすることも、後でインストールするようスケジュールすることもできます。
6. Guardium レポートの「S-TAP 状況モニター」を表示することで (「マイ・ダッシュボード」からレポートを追加)、FAM ディスカバリー・エージェントが正しくインストールされたか検査します。S-TAP ホストの IP アドレスで FAM_Agent 接尾部を探します。
7. FAM バンドルをアンインストールして再インストールせずに、後でファイルの再ディスカバリーをトリガーするには、次のようにします。
   a. 作業ディレクトリーの下のファイルを削除します。Guardium がデフォルト・ディレクトリーにインストールされている場合、削除対象のファイルはファイル・サーバーのディレクトリー /usr/local/IBM/modules/FAM/current/files/work にあります。
   b. GIM の任意の FAM パラメーターを変更します。例えば、時間間隔を 5 分から 10 分に変更します。
   c. 「選択したものに適用」をクリックしてから「インストール/更新」をクリックします。

タスクの結果

ディスカバリーおよび分類の結果: FAM ディスカバリー・エージェント (ファイル・クローラー) のインストールが完了すると、インストール中に指定した初期パスを使用してファイル・クローラーの基本実行が開始されます。クローラーは、実行を完了するたびに、「ファイル: クローラー構成」レポートに含まれる状況メッセージを送信します。このプロセスでは、フォルダーとファイル、それらの所有者、アクセス許可、サイズ、および最終更新日時のリストが収集されます。

親トピック: ファイル・サーバー内での機密データのディスカバーおよび分類
関連情報:
GuardAPI ファイル・アクティビティー・モニター関数
GuardAPI ファイル・アクティビティー・モニター関数

ファイルのディスカバリーおよび分類 GIM パラメーター

以下の GIM パラメーターを使用して、コレクターごとにファイル・ディスカバリーと分類を構成します。

ファイルのディスカバリーと分類をコレクターごとに構成します。これらのパラメーターはインストール時に構成するか、または後で GIM (「管理」 > 「モジュール・インストール」 > 「クライアント別の設定」) または GuardAPI コマンド gim_update_client_params を使用して構成できます。GuardAPI を使用する場合、一度に更新できるのは 1 つのコレクターのみです。

GIM パラメーター	記述	GUI	grdapi
FAM_CLASSIFICATION_LANGUAGES	内部。デフォルトで FAM_CLASSIFICATION_LANGUAGES は英語に設定されています。 自動言語検出の場合は、GenericLanguage に設定してください。 Linux の場合は、Linux サーバーに必要な言語サポートがインストールされていることを確認してください。例えば、中国語の文書の分類をサポートするには、中国語のサポートを Linux にインストールする必要があります。 IBM Content Classification でサポートされている言語について詳しくは、http://www-01.ibm.com/support/knowledgecenter/SSBRAM_8.8.0/com.ibm.classify.workbench.doc/c_WBG_available_languages.htm%23wp9000332?lang=enを参照してください。	X	
FAM_DEBUG	0=OFF 1= ON ファイル・サーバーのログが収集され、Guardium アプライアンスに送信されます。	X	
FAM_ENABLED	0 = FAM ディスカバリー・エージェントは無効化されます。 1 = FAM ディスカバリー・エージェントは有効化されます。デフォルト 2 = FAM ディスカバリー・エージェントを再始動します。 GIM インストール済み環境の場合、v10.1.4 から、デフォルトでは無効です。シェル S-TAP インストール済み環境では、デフォルトでは有効です。 FAM の再始動方法: GIM GUI の FAM_ENABLED パラメーターを 2 に変更し、「インストール/更新」をクリックしてクライアントに適用します。 **Unix:** ファイル・サーバーの FAM サービスは、PID を変更して、再始動したことを示します (ps -ef | grep fam)。また、事前定義の GUI レポートである「ファイル: クローラー構成」に新しい項目があります。 GIM GUI で構成を 1 に戻すと、プロセスを繰り返して再始動できます。 **Windows:** イベント・ビューアー (Windows ログ >「システム」`IBM Guardium FAM サービスは停止状態になりました (The IBM Guardium FAM service entered the stopped state)` および `IBM Guardium FAM サービスは実行状態になりました (The IBM Guardium FAM service entered the running state)`) に示されるように、FAM サービスが再始動します。 定義済みの GUI レポート「ファイル: クローラー構成」に新規の項目は**ありません**。GIM GUI では、構成は 2 のままです。次回の再始動のために、パラメーターを 1 に変更します。	X	
FAM_ICM_CLASS_DECISION_PLANS	判定プランの名前と分類エンティティーを含めることで、その判定プランを有効化します。 DecisionPlanName1{Entity1.1,Entity1.2,..}:DecisionPlanName2{Entity2.1,Entity2.2,..} 判定プランごとに、エンティティーをセミコロンで区切った判定プランのリストを設定します。 形式: エンティティーは、中括弧とコロンで区切ってリストされます。 一部の判定プランで中括弧が空または欠落している場合、すべての分類エンティティーは FAM レポート/調査ダッシュボードの分類結果に示されます。 中括弧が空または欠落している例は次のとおりです: DecisionPlanName1{}:DecisionPlanName2{} DecisionPlanName1:DecisionPlanName2"~		
FAM_ICM_CLASS_THREAD_COUNT	使用する分類のスレッドの数。デフォルトは 5 で、これが推奨値です。	X	
FAM_ICM_URL	IBM Content Classification Server の URL。デフォルトは http://localhost:18087 です。	X	
FAM_INSTALLER	Windows のみ。 インストーラー・パッケージへのパス。		
FAM_INSTALL_DIR	Windows のみ。 ファイル・アクティビティー・モニター・ソフトウェアがインストールされている場所。		

GIM パラメーター	記述	GUI	grdapi
FAM_IS_DEEP_ANALYSIS	False で分類が無効化されます。メタデータおよびアクセス許可の基本スキャンのみです。 True の場合、ファイルの内容に基づいて分類が有効化されます。 判定プランが有効化されていない場合 (FAM_ICM_CLASS_DECISION_PLANS が未定義の場合)、基本スキャンのみ実行されます。	X	
FAM_SCAN_EXCLUDE_DIRECTORIES	ディスカバリーおよび分類から除外するディレクトリー。ワイルドカードはサポートされません。 フォーマット: ディレクトリーへの絶対パス	X	
FAM_SCAN_EXCLUDE_REMOTE_DIRECTORIES	True/false。デフォルトは true です。リモート・ディレクトリーをスキャンするには、false に設定します ディスカバリーおよび分類から除外するリモート・ディレクトリーです。ワイルドカードはサポートされません。 Windows では、次のように設定します。¥¥¥¥RemoteMachine¥sharefolder¥directoryA	X	
FAM_SCAN_EXCLUDE_EXTENSIONS	指定されたファイル拡張子、または拡張子が設定されていない文書を FAM スキャンから除外します。Windows と Linux の両方に適用されます。 フォーマット: セミコロンで区切られたリスト 設定では大/小文字が区別されます。除外する拡張子の例: pdf;txt;doc。拡張子のない文書を除外するには、「NO_EXTENSION」に設定します。	X	
FAM_SCAN_EXCLUDE_FILES	ディスカバリーおよび分類から除外するファイル。 フォーマット: 有効なファイル名。ワイルドカードはサポートされません。	X	
FAM_SCAN_MAX_DEPTH	指定された開始ディレクトリー (FAM_SOURCE_DIRECTORIES) に対するスキャンの深さを制限します。	X	
FAM_SCHEDULER_HOUR_TIME_INTERVAL	ディスカバリーおよび分類のスキャンが実行される時間単位の頻度。 フォーマット: 整数 デフォルトは 12 時間です。	X	
FAM_SCHEDULER_MINUTE_TIME_INTERVAL	これはスキャンの分単位の間隔で、時間単位の間隔と共に使用します。例えば、スキャンを 12 時間 30 分おきに実行する場合、時間として 12 を指定し、分としてここで 30 を指定します。 フォーマット: 整数	X	
FAM_SCHEDULER_REPEAT	True = 指定された時間間隔でディスカバリー・プロセスを繰り返します。 False = スキャンを繰り返しません。	X	
FAM_SCHEDULER_START_TIME	ディスカバリー・プロセスおよび分類プロセスの最初のアクティブ化時刻。 フォーマット: MM-DD-YYYY HH:mm 例えば、01-02-2016 18:00 と入力すると、スキャンは 2016 年 1 月 2 日の午後 6 時に開始されます。時間間隔が 12 時間の場合、プロセスは毎日午後 6 時と午前 6 時に実行されます。	X	
FAM_SERVER_PORT	Guardium コレクターのポート (16022)。	X	
FAM_SOURCE_DIRECTORIES	スキャンを開始する対象の 1 つ以上のディレクトリー。ワイルドカードはサポートされていません。例: /home/test。 形式: セミコロンで区切られた FAM ソース・ディレクトリーのリストを設定します。 例: %IBM_FAM_HOME%/test/dir1;%IBM_FAM_HOME%/test/dir2 ~ FILE_SYSTEM_ROOTS を使用して、サーバー内のすべてのファイルをスキャンします。特に大量のファイルがサーバーに含まれている場合は、お勧めできません。	X	

親トピック: ファイル・サーバー内での機密データのディスカバーおよび分類
関連情報:
GIM - GUI
GIM - CLI

FAM 判定プランのカスタマイズ

判定プランは、ファイル内の機密の内容を識別するために使用されます。Guardium FAM ディスカバリー・エージェントは、HIPAA、PCI、SOX、およびソース・コードのデフォルトの判定プランを提供します。デフォルトの判定プランを使用して、結果のレポート/調査ダッシュボードから分類エンティティーを変更できます。また、IBM コンテンツ分類ワークベンチを使用して、新しいプランを作成したり、既存のプランを変更したりできます。

始める前に

Guardium 環境に接続できる Windows ワークステーションに IBM Content Classification 8.8 をインストールします。

ファイル・アクティビティー・モニター中、GIM インストール・ユーザーは、ファイル・アクティビティー・モニターの GIM 構成ページで ICM 判定プラン設定を構成する必要があります。

ユーザーは、判定プラン (カテゴリー) と各判定プランのエンティティー (NVP フィールド) のリストをコロンで区切って構成する必要があります。

この構成は、ファイル・アクティビティー・モニターによる内容分類で使用されます。

カスタマーは、ファイル・アクティビティー・モニターのインストール中に使用できる、各判定プラン・テンプレートの使用可能なすべてのエンティティーを構成できる必要があります。

判定プランの分類は、ファイルが機密ファイルであり、分類が空ではない場合のみ表示されます。

ファイル・アクティビティー・モニターのインストール後、以下の 4 つの判定プラン・テンプレートを使用できます。

- HIPAA、PCI、SOX、ソース
- 医療情報の検出に使用される HIPAA 判定プラン
- クレジットカード番号を検出するための PCI
- 財務文書用の SOX

「ソース」判定プランは、「ソース」判定プランが構成されるとデフォルトでロードされる 2 つの知識ベース (CodeKB および DocumentTypeKB) を参照します。

以下に、各判定プランで使用できるエンティティーのリストを示します。これらはファイル・アクティビティー・モニターでただちに使用でき、GIM を通じて構成できます。

HIPAA

SSN、Name、License、GovermentID、PassportContext、BankAccount、Address、IPAddress、EmailAddress、URL、Phone、CreditCard、possibleHealthPlan、Confidential_match、HIPAA_match

PCI

SSN、Name、License、GovermentID、PassportContext、BankAccount、Address、IPAddress、EmailAddress、URL、Phone、BankAccountContext、CreditCard、CreditContext、containCardIssuer、PCI_match、Confidential

SOX

SSN、Name、License、GovermentID、PassportContext、BankAccount、Address、IPAddress、EmailAddress、URL、Phone、BankAccountContext、CreditCard、CreditContext、containCardIssuer、piiMatch、Confidential、SOXContext、SOX_match

ソース

containDate、hasSSN、hasBirthDate、containCardIssuer、hasCreditCard、PCIViolation、HIPAA_Match、ConfidentialMatch、Source_match

判定プランは、IBM Classification モジュールがコンテンツ項目を分類する方法を決定するためにユーザーが構成する、一連のルールです。ルールはトリガーとアクションで構成されます。トリガーは、アクションを開始するために満たす必要のある条件を決定します。アクションは、文書の分類方法を決定します。判定プランは、ルール (キーワード・ベースの分類と統計を使用したテキスト・ベースの分類) を組み合わせるために、1 つ以上の知識ベースを参照することもできます。

知識ベースは、コンテンツ項目の分析と分類に使用される、一連の収集データです。知識ベースは、システムが処理することを期待されるデータの種類を反映します。知識ベースでテキストを分析できるようにするには、適切にカテゴリー分けされた十分な数のコンテンツ項目例によって、知識ベースが調整されている必要があります。調整された知識ベースは、項目の関連性を示す数値的尺度から各カテゴリーを割り出すことができます。

注: 中国語名を持つ判定プランの場合、ICM は機能しません。中国語のコンテンツ・ドキュメントと、中国語の判定プラン・ルールはサポートされますが、中国語の名前が指定された判定プランはサポートされていません。
注: 中央マネージャーから管理対象ユニットへの判定プランの配布は、サポートされていません。
注: 各判定プランの分類結果は、適切に構成されて認識されたエンティティーごとに指定する必要があります。分類は、ファイルが機密ファイルであり、分類が空ではない場合のみ表示されます。デバッグ・レベルでは、ICM エラーおよび判定プランの失敗に関する文書があります。

このタスクについて

このことを説明するために、会社に「ProjectA」という名前の機密プロジェクトがあると仮定します。この文字列を含むすべてのファイルを識別およびモニターする必要があります。

手順

1. Windows の「スタート」メニューを使用して IBM Content Classification 8.8 Classification Workbench を開きます。
2. 「プロジェクトを開く (Open Project)」ダイアログで「新規...」をクリックします。
3. 「新規プロジェクト (New Project)」ダイアログで、プロジェクト・タイプに対応する判定プランを選択します。この判定プランの名前 (`ProjectA_DP` など) を入力します。必要に応じて説明を入力します。
4. 「新規プロジェクトのオプション (New Project Options)」ダイアログで「空のプロジェクトを作成 (Create an empty project)」を選択します。
5. 「プロジェクト・エクスプローラー」で「語および文字列のリスト・ファイル (Word and string list files)」をクリックします。「語および文字列のリスト・ファイル (Word and string list files)」ダイアログで、「新規...」をクリックして新規ファイルを作成します。「新規ファイル (New File)」ダイアログで、ファイル・タイプ

として「語のリスト (Word list)」を選択し、ファイルの名前を選択します。この例では、ファイルに `Names` という名前を付けます。 Wordlist_Names.txt がファイルのリストに表示されます。
6. ファイル名をダブルクリックし、ファイルを編集します。`~ProjectA~` という文字列を含む単一の行を挿入し、ファイルを保存します。
7. 「プロジェクト・エクスプローラー」で、「判定プラン」 > 「新しいグループ」 > 「新規ルール (New Rule)」をクリックします。ルールの名前を `ProjectA` に変更します。
8. 「新規ルール (New Rule)」ダイアログで、「トリガー」タブを開きます。「条件」をクリックします。
9. 「フィールドに特定の語または句が含まれている場合にトリガー (Trigger when fields contains specific words or phrases)」を選択します。「語のリスト・ファイル (Word list file)」を選択します。「OK」をクリックします。
10. 「アクション」タブを開きます。「新規ルールの追加」をクリックします。
11. 「アクション・タイプ」リストから「拡張アクション」を選択します。「内容フィールドの設定 (Set content field)」アクションを選択します。 指定のトリガーが起動すると、この内容フィールドが作成されます。この内容フィールドは FAM レポートで確認できます。
12. 「アクションの追加」ダイアログで、内容フィールド名として `ProjectA_match` と入力し、「値」フィールドに `found` と入力します。
13. 内容セットを判定プラン・プロジェクトにインポートします。
    a. 「ProjectA」という文字列を含むテキスト文書を作成します。
    b. 「プロジェクト・エクスプローラー」で、ProjectA_DP プロジェクトを展開します。「内容セット (Content Set)」を右クリックし、「内容セットのインポート (Import Content Set)」を選択します。
    c. 「ファイル・システム・フォルダー内のファイル (Files from a file system folder)」をクリックします。 ステップ a で作成したファイルを参照します。「次へ」をクリックし、その後「次へ」、「次へ」、「完了」を順番にクリックします。
14. 定義が成功したことを検査します。
    a. 「プロジェクト・エクスプローラー」で、「内容セット (Content Set)」タブを開きます。ファイルを右クリックし、「判定プランを通じて項目を実行 (Run Item through Decision Plan)」を選択します。
    b. 「分析済み項目 (Analyzed item)」ダイアログで、判定プランおよびグループを展開します。Rule:ProjectA が [Triggered] とマークされていることを確認します。
    c. 「内容フィールド... (Content Fields...)」をクリックします。「内容フィールドの選択 (Select Content Fields)」ダイアログで、「ProjectA_match」が「変更済みフィールド (Changed fields)」ボックスに表示されていることを確認し、また「found」が「内容」ボックスに表示されていることを確認します。
15. 「プロジェクト・エクスプローラー」で、「プロジェクト」 > 「保存」をクリックして ProjectA_DP プロジェクトを保存します。
16. 「プロジェクト・エクスプローラー」で、「プロジェクト」 > 「エクスポート」をクリックして ProjectA_DP プロジェクトを dpn ファイルにエクスポートします。
17. GIM を使用して、判定プランを使用するファイル・サーバーに dpn ファイルをプッシュします。

親トピック: ファイル・サーバー内での機密データのディスカバーおよび分類

資格最適化

資格最適化は、ジョブを効率的に実行するために必要な資格をユーザーに提供する上でのデータベース管理者のロールと、システムの脆弱性を防ぐために資格をできる限り正確に、かつ可能な限り最小限に抑える上でのセキュリティーのロールの間を仲介するものです。

資格最適化は Guardium V10.1.2 で導入されました。

システムの日常の管理には、脆弱性をもたらす状況が必然的に発生します。例えば、以下のようなものがあります。

- アクセスが一般化し過ぎている
- ユーザーに与えられた特権は一回限りの使用に必要だったが、その後に除去されなかった
- ユーザーと表の経時的変化により休止ユーザーや休止表が発生する
- あるユーザーから別のユーザーに特権が渡される

資格は、絶えず継続的に注視する必要があります。例えば、Advanced Persistent Threat (APT) 攻撃は、通常、こうした背後の入口のいずれかからシステムに侵入することで発生します。

資格最適化は、ユーザーの特権とアクションを絶えず分析し、ユーザー・アクセスを必要最小限に抑えることを目的とした固有のアクションを特定する推奨事項を作成します。分析はすべてシステムによって実行されます。管理者は結果を検討し、各ケースを調べ、適切なアクション (例えば、データベース・ユーザーからの特権の除去や休止ロールの削除など) を実行します。

また、過去 1 週間にわたる資格の変更、ユーザーとロールの完全なリスト、データ・ソース特権と実際の使用法、および特定のユーザーとロールの組み合わせのシミュレートされた理由を調査することもできます。これらのビューは推奨に関連する情報を提供します。また、他の調査の開始点ともなります。

Guardium レポートに対する資格最適化の利点は、すべてのデータベース・タイプの情報 (複数の Guardium レポートに表示される) を統合し、それ自体の包括的な統合レポートに新しい分析を追加し、資格管理を簡素化することにより、システム・セキュリティーを向上させる点です。

資格最適化は、データベース・タイプとして Microsoft SQL Server および Oracle をサポートします。SQL Contained Database はサポートしません。(Guardium レポートはデータベース・タイプ別になっています。)

資格最適化アクティビティー・モニターは、現在 Guardium によってモニターされているデータに制限されます。推奨、資格の参照、および仮定の分析の正確性は、モニター対象のデータの関連性に依存します。このツールの能力を最大限に高めるには、 userScope パラメーターおよび objectScope パラメーターを構成し、セキュリティー・ポリシーを変更することを検討してください。

資格最適化を使用したモニターの開始時から休止しているユーザーは、資格最適化レポートに含まれません。モニターされているが、推奨がない特定のユーザーを監視するには、資格の参照またはその他のいずれかの Guardium アクティビティー・モニター・ツールを使用して、ユーザーのアクティビティーを手動で確認してください。 ポリシーが正しく定義されている場合、ツールにはすべての情報が含まれます。

資格分析はコレクターごとに実行され、grdapi によって構成されたデータ・ソースでのみ機能します。

Must Gather 機能は資格最適化をサポートします。『IBM サポートのための基本情報』を参照してください。

「ディスカバー」 > 「データベース資格」 > 「資格最適化」から資格最適化にアクセスします。

- 資格最適化の有効化および構成
  資格最適化を有効化および構成するには、次の grdapi コマンドを使用します。

- 資格最適化の新機能
  「新機能」タブは、暦週の日曜日から日曜日までに、システムに対して行われた追加と変更を要約します。
- 資格最適化のユーザーおよびロール
  「ユーザーおよびロール」タブには、このコレクターで資格最適化に対して有効になっているすべてのデータ・ソースの、すべてのユーザーとそのロールがリストされます。
- 資格最適化に関する推奨
  推奨は、ユーザー・アクセスを必要最小限に抑えることを目的とした固有のアクションを特定します。
- 資格最適化の資格の参照
  このウィンドウのビューおよびフィルターを使用して、資格のアクティビティー・レベルおよび資格のリネージュを表示します。
- 資格最適化の仮定
  仮定は、(資格が存在するかどうかに関係なく) 特定のオブジェクトに対して 1 つ以上の特定の動詞を持つ特定のユーザーの資格に関する推定理由を示します。

親トピック: ディスカバー

資格最適化の有効化および構成

資格最適化を有効化および構成するには、次の grdapi コマンドを使用します。

すべてのコマンドはコレクターで実行され、既に定義されている Guardium データ・ソースを使用します。まず、コレクターで機能を有効にし、データ・ソースを指定して、特定の機能を有効にします。

資格最適化に含まれるデータを微調整することによって、最も正確な結果が得られます。

ユーザーおよびロールと資格の参照はデフォルトで有効になっていますが、関連データを抽出するには、extractActivity および extractEntitlement を `true` に設定する必要があります。その他の 3 つの機能 (「新機能」、「推奨」、「仮定」) は個別に有効化されます。例えば、「仮定」を無効にしたまま「推奨」を有効にすることができます。

資格の推奨は、userScope パラメーターおよび objectScope パラメーターによってフィルタリングされたデータのサブセットを使用します。資格の参照は、データのフィルタリングに userScope パラメーターを使用します。どちらのパラメーターも Guardium グループを 1 つ以上指定します。通常、この目的に使用するための特定のグループを作成します。ストレージおよび処理を最小化するために、必要なデータだけを抽出するようにグループを定義してください。 すべてのデータが分析され、最終的な結果が得られるようにするため、グループには完全な監査が必要です。完全な監査を持つグループを使用する場合、資格の参照は、アクティビティーに関係なく、すべてのユーザーのすべての権限を表示します。userScope 定義以外のユーザーがウィンドウに表示されますが、そのアクティビティー・カウントは「不明」です。

ベスト・プラクティスは、まれにしか変更されないデータ収集スキームを慎重に評価して設計することです。これには 2 つの理由があります。1 つ目の理由は、構成を変更するたびに、レポートのデータを生成するために 1 週間かかることです。2 つ目の理由は、データは過去 3 週間のデータと比較されるため、データ定義を変更すると、最初の 3 週間分の比較の意義が薄れることです。

個々の機能を有効にすると、データは最初の日曜日から各タブに表示されます。

『GuardAPI 資格最適化機能』でコマンドの完全な詳細を参照してください。

前提条件

- クイック検索は有効になっています。(仮定、推奨、および資格の参照でのアクティビティーの更新に必要です。)
- 資格最適化を構成するユーザーは、構成されたデータ・ソース内にあるすべてのメタデータおよびスキーマ表に対する許可を持っている必要があります。

コレクターでの entitlement_optimization の有効化

コレクターで資格最適化を有効にします。

構文:

grdapi enable_entitlement_optimization

コレクターでの entitlement_optimization の無効化

コレクターで資格最適化を無効にします。

構文:

grdapi disble_entitlement_optimization

資格最適化へのデータ・ソースの追加

1 つ以上のデータ・ソースを資格最適化に追加して、個々の分析を有効にします。

構文:

grdapi add_datasource_to_entitlement_optimization datasourceName=[datasource] isEnabled=[true/false] userScope=[USER SCOPE] objectScope=[OBJECT SCOPE] extractActivity=[true/false] extractEntitlement=[true/false] generateRoleClusters=[true/false] generateNews=[true/false] generateRecommendations=[true/false]

この表を使用して、機能ごとに必要な抽出を判別します。

表 1. 分析タイプごとに必要な enable_entitlement_optimization パラメーター

	新機能 (generateNews)	ユーザーおよびロール	推奨 (generateRecommendations)	資格の参照	仮定 (generateRoleClusters)
extractActivity				X	X

	新機能 (generateNews)	ユーザーおよびロール	推奨 (generateRecommendations)	資格の参照	仮定 (generateRoleClusters)
extractEntitlement	X	X	X	X	

資格最適化からのデータ・ソースの除去

データが収集されないように、資格最適化から 1 つ以上のデータ・ソースを除去します。

remove_datasource_from_entitlement_optimization datasourceName=[datasource name]

資格データ・ソース・パラメーターの変更

資格最適化に既に有効になっているデータ・ソースのパラメーターを変更します。

構文:

grgapi set_entitlement_datasource_parameter datasourceName=[datasource name] parameterName=[value] parameterName=[value]

ここで、parameterName は次のいずれかです。

isEnabled

userScope

objectScope

extractActivity

extractEntitlement

generateRoleClusters

generateNews

generateRecommendations

filterTempObjects

filterIgnoreVerbs

最適化情報の表示

構文:

grdapi get_entitlement_optimization_info

一般的な出力:

資格最適化は有効です

```
==================================
Datasource: SCALE-DB16
==================================
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
```

親トピック: 資格最適化

資格最適化の新機能

「新機能」タブは、暦週の日曜日から日曜日までに、システムに対して行われた追加と変更を要約します。

この機能を有効にすると、データは最初の日曜日からタブに表示されます。

「新機能」タブには、次のものが表示されます。

- 新規のユーザー、ロール、オブジェクトの数、およびこれらの追加項目に関連付けられているデータベースの数
- 新規の被付与者と付与者の数と、付与の数

何を確認すべきか

現在の傾向を調べます。例えば、ドリルダウンして以下を検索します。

- 資格における異常なタイプまたは変更の数量
- 最もアクティブな付与者/被付与者

いずれかのトピックの「詳細」をクリックして、追加項目の詳細表を開きます。例えば、新規ユーザーの詳細はサーバー名とサービス名です。

親トピック: 資格最適化

資格最適化のユーザーおよびロール

「ユーザーおよびロール」タブには、このコレクターで資格最適化に対して有効になっているすべてのデータ・ソースの、すべてのユーザーとそのロールがリストされます。

この機能を有効にすると、データは最初の日曜日からタブに表示されます。

このタブは、1 つのデータベース・タイプのみでデータを表示する標準の Guardium ユーザーおよびロール・レポートに基づきます。次の項目が表示されます。

- ホスト
- サービス名
- データベース・タイプ
- 被付与者
- 被付与者のタイプ
- ロール

標準のレポート・ビルダー機能を使用できます。これには表の上にあるアイコンでアクセスします。

親トピック: 資格最適化

資格最適化に関する推奨

推奨は、ユーザー・アクセスを必要最小限に抑えることを目的とした固有のアクションを特定します。

この機能を有効にすると、データは最初の日曜日からタブに表示されます。

システムはユーザーおよび特権を継続的に評価しています。週次資格推奨レポートは過去 3 週間のデータ (デフォルト) に基づいており、それぞれの新規レポートが前のレポートのデータと重複するようになっています。「推奨」タブは「レポート」の推奨レポートに相当します。このレポートは配布レポートとして有効にすることができます。

userScope パラメーターをカスタマイズした場合、推奨には指定されたユーザー・グループのユーザーのみが含まれます。userScope パラメーターと objectScope パラメーターは、推奨の範囲を明示的に定義するために使用されます。ユーザーおよびオブジェクトに関する推奨の正確さを最大限にするには、指定されたグループのユーザーとオブジェクトに完全な監査が必要です。

実装の前に、特定のサーバー、データベース、オブジェクト、および推奨タイプをドリルダウンすることにより、管理者はすべての推奨を徹底的に調査する必要があります。

タブの上部には、推奨をタイプ別に表示する円グラフが含まれています。ウィンドウの下部にある表には、推奨がリストされています。標準のレポート・アイコンを使用して推奨レポートを変更したり、「エクスポート」をクリックしてレポートをエクスポートしたり、「アクション」をクリックして API にマップしたりできます。

推奨タイプは以下のとおりです。

表 1. 推奨タイプ

タイプ	文字列	詳細
ANOMAL USER	ロール {source} の中でユーザー {object} に異常なアクティビティーがあります (User {object} has anomal activity within role {source})	特定のロール内のユーザー・アクティビティー・カウントが異常です。これは、当該ユーザーが他のユーザーよりも極端にアクティブであるか、または極端にアクティブでないことを意味します。
ALERT ACTIVITY (特別ユーザー)	ユーザー {source} が特権 {verb}-{object} を使用しましたが、資格は検出されませんでした	標準的な特別ユーザーは自分自身に許可を付与し、アクションを実行してから、許可を削除します。ユーザーは、資格の変更とそのアクティビティーの時差のため、誤って特別ユーザーとして識別されることがあります。Guardium アクティビティー・モニター・ツールを使用して、特権が正当かどうかを判別します。
DORMANT_USER	非アクティブまたは空のユーザー {object} を削除します	ユーザーに特権が割り当てられていないか、特定の間隔内にアクティビティーがありませんでした。
DORMANT_ROLE	非アクティブまたは空のロール {role} を削除します	ユーザーがないか、ユーザーによるアクティビティーがないか、または特権が空になっています
REVOKE_FROM_USER	ユーザー {source} から {verb}-{object} を取り消します	ユーザーは関連するオブジェクト、動詞に対してどのアクティビティーも実行しませんでした。
REVOKE _FROM_ROLE	ロール {source} から {verb}-{object} を取り消します	特定のロール内のすべてのユーザーは、オブジェクト、動詞に対してどのアクティビティーも実行しませんでした。
REMOVE_FROM_ROLE	ユーザー {object} をロール {source} から削除します	ユーザーは、ロールによって付与されたどの特権も使用しませんでした。
INACTIVE DATABASE	データベースにはアクティビティーがありません (Database has no activity)	未使用のデータベースを正当化できない場合は、除去してください。

親トピック: 資格最適化

資格最適化の資格の参照

このウィンドウのビューおよびフィルターを使用して、資格のアクティビティー・レベルおよび資格のリネージュを表示します。

この機能を有効にすると、データは最初の日曜日からタブに表示されます。最初の日曜日以降、アクティビティーは毎日更新されます。

この情報は一般的な資格の調査や、推奨レポートの推奨事項をさらに評価するのに役立ちます。このウィンドウのデフォルトのビューは、最高レートの未使用の特権を含むデータ・ソースを示した棒グラフです。

資格の参照は、extractEntitlement が使用可能な grdAPI で定義されているデータ・ソースのすべての資格を表示します。これは、アクティビティー収集がオフの場合およびユーザー有効範囲とオブジェクト有効範囲が定義されている場合に当てはまります。いつでも、すべてのユーザーの許可を検索して表示することができます。

アクティビティー・カウント・フィールドの結果は、以下のように userScope パラメーターの影響を受けます。

- userScope に含まれているユーザー:
  - アクティブ・ユーザーは緑で表示され、「アクティビティー・カウント」列に数値結果が示されます。
  - 非アクティブ・ユーザーは赤で表示され、アクティビティー・カウントは「非アクティブ」です。
- userScope に含まれないユーザー:
  - アクティブ・ユーザーは緑で表示され、アクティビティー・カウントに数値結果が示されます。
  - 非アクティブ・ユーザーはグレーで表示され、アクティビティー・カウントは「不明」です。

一般的な調査:

- ユーザーが許可を持つオブジェクトと、ユーザーがそれらを使用するかどうかを判別します
- ユーザーが、許可された特定の時刻にオブジェクトに対する許可を使用したかどうかを判別します
- 予想を上回って使用された許可があるかどうか
- 1 回だけ使用された許可があるかどうか
- 親ロールまたはロール階層から継承された、著しく使用されている許可のリネージュ (明示的または暗黙的) は何であるか

完全な SQL を使用して特定の特権がどのように使用されているかを詳しく調べるには、データ・アクティビティーを検索し (「調査」 > 「データ・アクティビティーの検索」)、「結果表」の「データベース・ユーザー」または「ソース・プログラム」を右クリックして、「データベース・ユーザー別の完全な SQL」を選択します。

未使用の資格は、通常、以下のいずれかです。

- アクションはほとんど実行されないが、有効な資格 (例えば、四半期レポートの生成など)
- 未使用のため、認められない (脆弱点)

特定のサーバーの特定のサービスに関する資格の使用状況を表示するには、次のようにします。

1. 左側で、サーバー IP とサービスを選択します。
2. 「名前」、「オブジェクト名」を 1 つ以上指定してフィルタリングします。
3. オプションで、動詞または日付範囲を入力します。

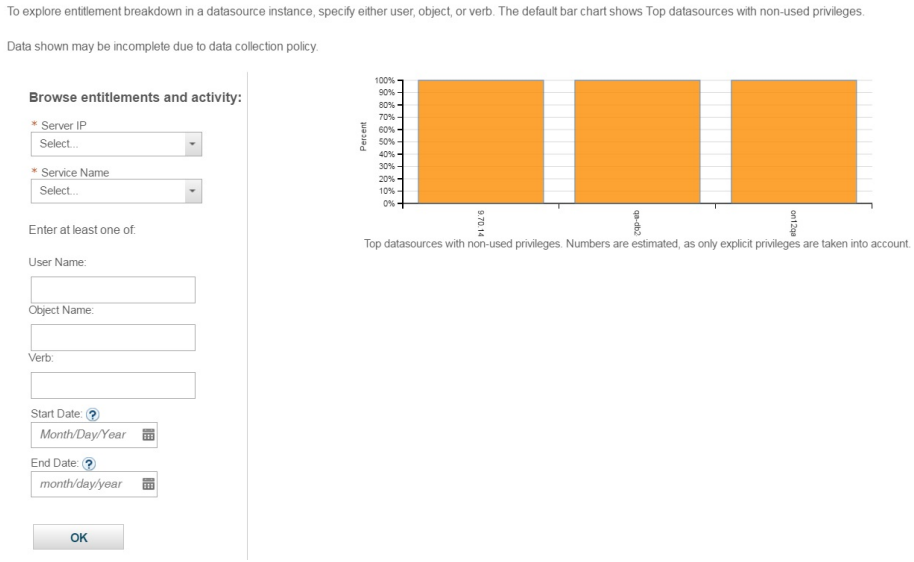


図 1. 資格基準の選択

この表は、「被付与者のタイプ」、「被付与者」、「動詞」、「名前」、「アクティビティー・カウント」、および「リネージュ」を示します。1 人のユーザーは、親ロールまたはロール階層から継承された複数の特権リネージュ (明示的または暗黙的) を持つことができます。

親トピック: 資格最適化

資格最適化の仮定

仮定は、(資格が存在するかどうかに関係なく) 特定のオブジェクトに対して 1 つ以上の特定の動詞を持つ特定のユーザーの資格に関する推定理由を示します。

機能を有効にすると、データは最初の日曜日からこのタブに表示されます。

Guardium は類似したユーザーの動作を分析して、推定理由を作成します。これは非常に関連性の高い情報を提供する場合があります。この分析は、未使用の資格および REVOKE_FROM_USER の推奨を調べる際に役立ちます。これは一般的な指示であり、他の資格最適化機能とともに使用する必要があります。

次の詳細を入力し、「OK」をクリックして、可能性を導出します。

- ユーザー名
- オブジェクト名
- 動詞 (1 つ以上)
- サーバー IP
- サービス名

可能な応答は次のとおりです。

- このデータベース・ユーザーがこの特権を使用する可能性は **n%** です。可能性が 100% の場合、ユーザーがアクティビティーを少なくとも 1 回使用したことを示します。
- サーバー上でデータ・ソースが見つかりませんでした。
- オブジェクトおよび DB ユーザーは範囲内にありません。
- データベース・ユーザーおよび特権の十分な証拠が見つかりません。選択されたデータベースにユーザー/オブジェクト/動詞が存在しない、ユーザーのアクティビティーが見つからない、またはオブジェクト/動詞タプルのアクティビティーが見つからない、のいずれかです。考えられる修正: アクティビティーの収集が実行されるのを待機してください。入力が正確であることを確認してください。

親トピック: 資格最適化

保護

機密データを含むデータベースおよびファイル・システムを識別した後、いくつかのステップを実行することで、そのデータを保護できます。保護オプションには、データのマスキング、データ・アクセスに基づく担当者へのアラート生成、アクセス制限を強制するポリシーの確立などがあります。

- ベースライン
  ベースラインとは、 過去に実行されたアクセス・コマンドのプロファイルであり、 正常なアクティビティーおよび (通常、正常、あるいは予期される振る舞いから矛盾または逸脱する) 異常な振る舞いを識別するのに役立ちます。
- ポリシー
  セキュリティー・ポリシーには、データベース・クライアントとサーバーとの間の監視対象トラフィックに適用される順序付きルール・セットが含まれています。各ルールは、クライアントからの要求、またはサーバーからの応答に適用できます。1 つの Guardium® アプライアンスに、同時に複数のポリシーを定義することも、複数のポリシーをインストールすることもできます。
- 相関アラート
  アラートは、例外またはポリシー・ルール違反が検出されたことを示すメッセージです。
- 相関アラートを使ってイベントを通知する方法
  アプリケーションのいずれかの個別ユーザーで最近 3 時間に 15 個より多い SQL エラーが存在する場合、相関アラートをトリガーします。
- インシデント管理
  統合インシデント管理 (IIM) アプリケーションには、 データベースのセキュリティー・インシデントをトラッキングして解決するワークフロー自動化機能を備えたビジネス・ユーザー・インターフェースがあります。
- 複数のデータベース・セキュリティー・インシデントのレビュー管理方法
  インシデントの管理を行い、データベースのセキュリティー・インシデントをトラッキングして解決します。
- 照会再書き込み
  照会再書き込み機能を使用してデータベース照会をインターセプトし、そのデータベース照会をセキュリティー・ポリシーで定義された条件に基づいて再書き込みすることにより、データベースに対するアクセス権を詳細に制御することができます。
- ファイル・アクティビティーのポリシーおよびルール
  ファイル・アクティビティー・モニターは、UNIX ファイル・サーバーおよび Windows ファイル・サーバー上の機密データの保全性と保護を確保します。

ベースライン

ベースラインとは、 過去に実行されたアクセス・コマンドのプロファイルであり、 正常なアクティビティーおよび (通常、正常、あるいは予期される振る舞いから矛盾または逸脱する) 異常な振る舞いを識別するのに役立ちます。

ベースライン・ビルダーは、Guardium システムで以前にログに記録され、現在有効なアクティビティーを検査することにより、ベースラインを生成します。

セキュリティー・ポリシーに組み込まれたベースラインは、 ベースラインに含まれているすべてのデータベース・アクセスを許可するベースライン・ルールになります。

ポリシー内のベースライン・ルールには、以下の特性があります。

- 1 つのベースライン・ルールのみ存在可能です。
- ベースライン・ルールのアクションは常に「許可」になります。 これはつまり、コマンドを受け入れ、ポリシー内の次のルールに継続しないことを意味します。
- ベースライン・ルールは、ポリシーに追加すると、ルール・リストの最初に配置されます。このルールは、ポリシーに合わせて、(順次評価される) ルール・セットの任意の場所に移動できます。
- 一度ポリシーに組み込んだベースライン・ルールは、削除できません。

重要: 「ベースライン・ビルダー」と関連機能は、Guardium V10.1.4 から非推奨になりました。

ポリシー・ビルダーは、ベースラインから推奨ポリシー・ルールを生成できます。 推奨ルールを編集し、ポリシー内のベースライン・ルールの前に組み込み、 ベースライン期間中に確認される一部のコマンドに対して代替アクション (例えば、アラートなど) を実行可能にすることができます。 さらに、推奨ルールを検査することで、監視される実際のトラフィック・パターン (コマンド・タイプおよび頻度) に ついて有益な洞察が得られます。

ベースライン・ビルダーには、ベースラインに組み込まれる内容を制御する方法がいくつかあります。

- しきい値を指定することにより、 何回出現するとコマンドがルールに組み込まれるかを制御する方法。 しきい値が 1 の場合、監視されるすべてのコマンドが組み込まれます。 しきい値が 1,000 の場合、1,000 回以上出現するコマンドのみが組み込まれます。

- 1 つ以上の属性に対する感度を制御する方法。 例えば、ベースラインがデータベース・ユーザーを識別する場合、 そのベースラインには特定のユーザーに関するコマンドのみが組み込まれます。 ベースライン期間中にコマンドを実行しなかったユーザーは、そのベースライン・ルールでは許可されません。
- 組み込まれる接続を、サーバーのサブセットおよびクライアント IP アドレスに限定する方法。 ベースラインでは、常に単一のクライアント・ネットワーク・マスクおよび単一のサーバー・ネットワーク・マスクが指定されます。 各マスクは、必要に応じて、包括的にすることも、排他的にすることも可能です。
- 別の期間のデータをマージする方法。ベースラインに組み込む必要のある、 連続しない期間中に出現したトラフィックがある場合があります。 単一のベースラインに、任意の数の期間からのデータをマージすることができます。 さらに、特定のクライアントおよびサーバーのアドレスについてデータをフィルターに掛けることもできます。

ベースライン検出感度の設定について

ベースライン検出感度の設定は、以下の任意の組み合わせをベースとすることができます (それぞれについて、後ほど詳しく説明します)。

- データベース・ユーザー
- データベース・プロトコル
- データベース・プロトコル・バージョン
- 期間
- ソース・プログラム
- シーケンス

ベースライン検出感度の設定は、指定されたしきい値によって決まります。 しきい値では、コマンドをベースラインに組み込むまでに、ベースライン期間中にそのコマンドが 監視される必要のある最小回数を定義します。

感度を選択しない場合、 しきい値を上回った各コマンドが、ベースラインに組み込まれます。

1 つの感度タイプを選択した場合、 その感度タイプ (例えば、データベース・ユーザー) の値ごとに、各コマンドの個別のカウントが保守されます。

複数の感度タイプを選択した場合、 選択した各タイプの値の組み合わせごとに (例えば、データベース・ユーザーとソース・プログラムの組み合わせごとに)、 各コマンドの個別のカウントが保守されます。 したがって、組み込まれる感度タイプごとに、組み合わせの数が劇的に増加する可能性があります。

シーケンス感度について

ベースラインがコマンド・シーケンスを識別する場合、ベースライン・ルールは、ポリシーに組み込まれると、 ベースライン期間中に監視されたコマンドのシーケンスのみを許可します。 非常な単純な例で説明します。ベースライン期間中に 2 つのコマンド・シーケンス (A-B および B-C) だけが監視された場合を想定し、 以下の表に、そのベースライン・ルールで許可されるコマンド・シーケンスを示します。

表 1. シーケンス感度について

コマンド・シーケンス	許可されるかどうか
A - B	Y
A - その他すべて	N
B - C	Y
B - その他	N
A 以外	N

期間感度について

ベースラインが期間を識別する場合、定義された期間ごとに、個別のカウントが保守されます。 オーバーラップする期間が定義された (これは正常な状態です) 場合、 コマンドは、それが出現した最も限定的な期間中に 1 回だけカウントされます。 期間が連続していない (例えば、各平日の 00:00 から 08:00 まで、など) 場合、 期間中の 1 つの連続するセグメントのみ (この例の場合、8 時間) が検討されます。

ベースライン・ビルダーが要求を期間に割り当てる方法を説明するに当たって、 土曜日が次の 3 つの期間に組み込まれると想定します。

- 24x7 (24 時間、1 週間に 7 日間)
- 土曜日 (24 時間のみ)
- 週末 (48 時間 - 土曜日 + 日曜日)

「土曜日」と名付けられた期間は最も限定的 (24 時間のみ) であるため、 「土曜日」にタイム・スタンプが付けられたすべての要求は その期間中にカウントされ、より包括的な「週末」または「7x24」期間ではカウントされません。

統合環境および中央マネージャー環境におけるベースラインについて

統合環境または中央マネージャー環境 (あるいはその両方) に複数の Guardium® アプライアンスが ある場合は、ベースラインを生成および使用する際に注意を要する重要なポイントが 1 つあります。

ベースラインは、そのベースラインを生成しているアプライアンスで 現在使用可能であるデータのみを使用して生成されます。

これは、次のことを意味します。

- コレクターで生成されるベースラインは、 そのユニットで使用可能なトラフィックのみを使用して作成されます。
- アグリゲーターで生成されるベースラインは、 そのアグリゲーターで現在使用可能なデータ (通常、一定の期間中に複数のコレクターから送信されたデータ) から作成されます。
- アグリゲーターを兼ねていない中央マネージャーで生成されるベースラインは空になります。 これは、中央マネージャーが (アグリゲーターを兼ねている場合を除いて) データを収集しないためです。
- 一元管理環境では、管理対象ユニットで生成されるベースライン はそのユニットからのデータのみを使用して作成されますが、 作成したベースラインは中央マネージャーに格納され、その他のユニットでも使用可能になります。

- 一元管理環境では、複数管理対象ユニットから単一のベースラインを 生成する場合、最初の管理対象アプライアンスからのデータを使用してベースラインを作成し、 その後他のアプライアンスからのデータを一度に 1 つずつ使用してマージすることができます。

推奨ルールについて

ベースラインをポリシーに組み込む際に、ポリシー・ビルダーは、ベースラインから推奨ルールを生成できます。 その際には、ベースラインに組み込まれるすべての内容を表すのに必要最小限の数のルールが生成されます。 その後、推奨ルールの一部またはすべてを受け入れ、受け入れたルールを必要に応じて変更することができます。 これは、(ベースラインのみに基づく暗黙的なポリシーではなく) 明示的なポリシーを生成する 便利な方法であるのに加えて、ベースライン期間中に出現した可能性のある、悪意のあるアクティビティーや 誤りのあるアクティビティーがベースラインに含まれないことを検証する重要なステップでもあります。

ベースライン期間中に出現した、以後モニターまたはアラートする アクティビティーをディスカバーした場合に、推奨ルールを変更することができます。 その処理は、ベースラインから推奨された該当するルールを調整し、必要なアクションを割り当てるだけです。 デフォルトでは、推奨ルールはベースライン・ルールの前に配置されるので、 ベースライン・ルールが実行される前に、指定されたアクションが実行され、それ以上ルールをテストすることなくそのコマンドが許可されます。

注: ポリシー・ビルダーは、データベース ACL からルールを生成することもできます。 詳しくは、ポリシーを参照してください。

推奨オブジェクト・グループについて

ベースラインまたはデータベース ACL (アクセス制御) のいずれかから推奨ルールを生成する際に、 ポリシー・ビルダーは推奨オブジェクト・グループを作成して推奨ルールの数を最小化します。 例えば、ベースラインに AAA、BBB、および CCC の 3 つのオブジェクトのみを参照する特定のコマンドが含まれており、 これら 3 つのオブジェクトだけで構成されるオブジェクト・グループがまだ定義されていないと想定します。 ポリシー・ビルダーはこれらのオブジェクトの推奨オブジェクト・グループを作成し、 その推奨オブジェクト・グループを参照する 1 つのルールをそのコマンド用に生成します。

推奨オブジェクト・グループのメンバーシップを表示可能であり、 各グループを受け入れる、または拒否するオプションがあります。 先ほどの例で、推奨オブジェクト・グループを拒否した場合、 そのグループを参照する 1 つのルールは、3 つの推奨ルール (AAA、BBB、および CCC それぞれに 1 つずつ) に置き換えられます。

ベースラインの作成

1. 「保護」 > 「セキュリティー・ポリシー」 > 「ベースライン・ビルダー」をクリックして「ベースライン・ファインダー」を開きます。
2. 「新規」をクリックして「ベースライン・ビルダー」を開きます。
3. 「ベースラインの記述」ボックスに、 固有のベースライン名を入力します。 ベースラインの記述にはアポストロフィ文字を含めないでください。
4. 「ベースライン検出感度の設定」ペインで、 ベースラインが識別する各エレメントにマークを付けます。 ベースラインの感度が増すほど、ベースラインの作成時と、さらに重要なトラフィックの検査時の両方において 実行されるテストがより複雑になります。 ベースライン検出感度の設定について詳しくは、概要を参照してください。
5. 「ベースラインしきい値」ペインで、 コマンドがベースラインに組み込まれるまでの、ベースライン期間中のそのコマンドの最小出現数を入力します。 1 つ以上の感度ボックスにマークが付けられている場合、このカウントは それらの感度の値の組み合わせに適用されます。

   セキュリティー・ポリシー構築のために使用するアプローチが 過去に最も多く発行されたコマンドを常に許可することである場合、 この数を適切なレベルまで上げて設定してください。 一方、ベースラインを確実に包括的にするには、この値を 1 に設定したままにしてください。 いずれの場合も、ポリシー・ビルダーにベースラインからルールを推奨させることができます。 推奨ルールはベースライン期間中の頻度別に降順にソートされるので、 その時点で、発行される固有のコマンドごとに、ルールを組み込むか、変更するかを判断することができます。

6. 「ベースライン・ネットワーク情報」ペインを使用して、 ベースラインに組み込むサーバーおよびクライアントを指定します。 ベースラインの構成に使用する IP アドレスの選択に使用するメソッドは、 サーバーの場合もクライアントの場合も同じです。

   ベースライン・データで検出される各アドレスでは、オプションのタグ付きグループ内のメンバーシップが最初に検討されます。 タグ付きグループは、ベースラインの構造が生成される具体的な IP アドレスのリストです。 タグ付きグループが選択され、ベースライン・データで検出された IP アドレスが対応するタグ付きグループに組み込まれている場合、 そのエレメントはその具体的な IP アドレスのベースラインに組み込まれます。 例えば、ZoneAGroup という名のタグ付きクライアント IP グループが選択されており、 そのグループにクライアント・アドレス 192.162.14.33 が含まれているとします。 ベースライン・ジェネレーターがその IP アドレスからコマンド SELECT abc FROM xyz を 検出すると、そのコマンドがその具体的なアドレスでカウントされます。

   一方、タグ付きグループが選択されない、または選択したタグ付きグループのメンバーではない IP アドレスがベースライン・データで検出された場合、そのコマンドは、対応するネットワーク・マスクから 送信された、別の IP アドレスからの同じコマンドと一緒にカウントされる可能性があります。

   ネットワーク・マスクは、 クライアントおよびサーバー IP アドレスの両方をグループ化するために必要です。 選択項目には、255.255.255.255 (4 つのオクテットすべてが一致する必要がある) と 0.0.0.0 (すべてのオクテットが任意) の間のサブネット・マスクの各種バリエーションがすべて含まれます。

   以下は常に必須です。

   - 「サーバー・ネットワーク・マスク」ボックスにサブネット・マスクを入力する。
   - 「クライアント・ネットワーク・マスク」ボックスにサブネット・マスクを入力する。

   ベースライン・ビルダーがネットワーク・マスクを使用して アドレスをグループ化する方法について説明するに当たって、以下のことを想定します。
   - クライアント・ネットワーク・マスクが 255.255.0.0 である。 つまり、最初の 2 つのオクテットは一致する必要があるが、残りの 2 つのオクテットは任意です。
   - ベースライン・データでは、クライアント IP アドレス 192.168.3.211 の要求が検出されている。
   - クライアント IP アドレスが選択したタグ付きクライアント IP グループ内にない (または、タグ付きクライアント IP グループが選択されていない)。
   - コマンドは SELECT abc FROM xyz である。

   ベースラインの生成時に、このコマンドは 192.168.0.0 サブネットからの すべてのクライアント IP アドレスのすべての SELECT abc FROM xyz コマンドの カウントに組み込まれます。

7. 「保存」をクリックして、 ベースライン定義を妥当性検査して保存します。必須フィールドを省略した、または無効な値を入力した場合、 定義は保存されず、再度保存を試みる前にすべての問題を解決する必要があります。
8. オプションで「ロール」をクリックして、ポリシーのロールを割り当てます。
9. オプションで「コメント」をクリックして、定義にコメントを追加します。
10. ベースラインの保存が成功した後で、パネルに「ベースライン生成」および「ベースライン・ログ」ペインが表示されます。
11. 「ベースライン生成」ペイン・タイトルの任意の場所をクリックして、 ペインを展開します。

12. 「開始」と「終了」の日付を両方指定して、ベースラインを生成する期間を定義します。 複数の日付の入力方法があります。詳しくは、『日付とタイム・スタンプ』を参照してください。日付の入力方法に関係なく、指定されたすべての分または秒は無視されます。
13. 「生成」ボタンをクリックして、ベースラインを生成します。 ベースライン定義を変更している場合、ベースラインを生成する前に定義の保存を求めるプロンプトが出されます。

注: 最初にベースラインの生成が成功した後で、 「ベースライン生成」パネルに追加のフィールドが表示されます。 これらのフィールドを使用して、追加の期間のデータをベースラインにマージすることや、 各追加の期間中に使用されるクライアントおよびサーバーの IP アドレスを制限することができます。

ベースライン情報のマージ

ベースライン情報をマージする (例えば、追加の期間または別のクライアントおよびサーバーのグループ (あるいはその両方) からの情報を組み込む) 手順は、以下のとおりです。

1. 「保護」 > 「セキュリティー・ポリシー」 > 「ベースライン・ビルダー」をクリックして「ベースライン・ファインダー」を開きます。
2. 「ベースライン定義」リストから、 追加のベースライン情報をマージするベースラインを選択します。
3. 「変更」をクリックして「ベースラインの編集」パネルを開きます。
4. 「ベースライン検出感度の設定」の選択内容を変更しないでください。 ベースライン検出感度の設定を変更すると、既存のベースラインを置き換える完全に新しいベースラインの生成を求めるプロンプトが出されます。
5. オプション。「ベースラインしきい値」ペインの「ベースラインへの追加の最小出現回数」の値を設定します。 ここで入力した値は、それ以前にベースラインに組み込まれた情報には影響を与えません。 ベースラインに追加したものは、マージ操作の間には削除できません。
6. オプション。「ベースライン・ネットワーク情報」ペインに、 代替ネットワーク情報を入力します。 最新の生成またはマージ操作の値が表示されます。マージされる情報が、同じサーバーおよび/またはクライアントのセット をソースとする場合、これらのフィールドを変更しません。 それ以外の場合は、このペインで適切な変更を加えて、ベースラインに組み込むトラフィックを選択します。
7. 「ベースライン生成」ペイン・タイトルの任意の場所をクリックして、 ペインを展開します。
8. 「開始」と「終了」の日付を両方指定して、ベースラインを生成する期間を定義します。 複数の日付の入力方法があります。詳しくは、『日付とタイム・スタンプ』を参照してください。日付の入力方法に関係なく、指定されたすべての分または秒は無視されます。
9. 「マージ」ラジオ・ボタンを選択します。
10. オプション。「フィルター選択」ペインで、IP アドレスに続けてネットワーク・マスクを入力し、 ベースライン生成を特定のクライアントまたはサーバー (あるいはその両方) の IP アドレスに制限します。 例えば、192.168.9.x サブネットからのすべてのクライアント IP アドレスを選択するには、 最初の「クライアント IP」ボックスに 192.168.9.1 を、2 番目のボックスに 255.255.255.0 を入力します。 追加のアドレスを組み込むには、「追加」ボタンをクリックしてから、追加のアドレス情報を入力します。
11. 「生成」をクリックして、ベースラインを生成します。 ベースライン定義を変更している場合、ベースラインを生成する前に定義の保存を求めるプロンプトが出されます。

ベースラインの変更

注意: ベースライン定義を変更する前に、 変更すること (特に、定義を変更および再生成する対象のベースラインが、 インストールしたポリシーで使用されている場合) の影響について、必ず理解しておいてください。 インストールしたポリシーに含まれるベースラインを変更および再生成する場合、 そのポリシーを再インストールする際には、新しいベースラインが使用されます。 インストールしたポリシーが使用するベースラインのフォールバック・オプションを提供する際には、 代わりに、これらのベースラインおよびポリシーのコピーを作成し、 コピーの定義に変更を加えて生成することを検討してください。 詳しくは、『ベースラインのコピー作成』を参照してください。

1. 「保護」 > 「セキュリティー・ポリシー」 > 「ベースライン・ビルダー」をクリックして「ベースライン・ファインダー」を開きます。
2. 「ベースライン定義」リストから、変更するベースラインを選択します。「変更」ボタンをクリックして「ベースラインの編集」パネルを開きます。このパネルは、パネル・タイトルを除いて、「ベースラインの追加」パネルと同じです。このパネルの使用手順については、『ベースラインの作成』を参照してください。

ベースラインのコピー作成

オリジナルの定義に変更を加えずに、既存のベースラインに基づいて新規ベースラインを定義するシチュエーションが多々あります。『注意』を参照してください。

1. 「保護」 > 「セキュリティー・ポリシー」 > 「ベースライン・ビルダー」をクリックして「ベースライン・ファインダー」を開きます。
2. 「ベースライン定義」リストから、コピーを作成するベースラインを選択します。
3. 「コピー」をクリックして、「ベースラインのコピー作成」パネルを開きます。
4. 「新規ベースラインの記述」ボックスに、新規ベースラインの固有の名前を入力します。 新規ベースラインの記述にはアポストロフィ文字を含めないでください。
5. コピー中のベースラインに関して生成されたベースライン構成体 (基本的にコマンド) のコピーを作成するには、「構成体のコピー作成」チェック・ボックスにマークを付けます。
6. 「OK」をクリックして、新規ベースラインを保存します。 これで、ベースライン・ファインダーを使用して新規ベースラインを開き、編集できるようになります。

ベースラインの削除

1. 「保護」 > 「セキュリティー・ポリシー」 > 「ベースライン・ビルダー」をクリックして「ベースライン・ファインダー」を開きます。
2. 「ベースライン定義」リストから、削除するベースラインを選択します。
3. 「削除」をクリックします。アクションの確認を求めるプロンプトが出されます。

親トピック: 保護

ポリシー

セキュリティー・ポリシーには、データベース・クライアントとサーバーとの間の監視対象トラフィックに適用される順序付きルール・セットが含まれています。各ルールは、クライアントからの要求、またはサーバーからの応答に適用できます。1 つの Guardium® アプライアンスに、同時に複数のポリシーを定義することも、複数のポリシーをインストールすることもできます。

ポリシー内の各ルールは、条件付きアクションを定義します。条件は、単純なテスト (例えば、「許可されたクライアント IP」グループに属していないクライアント IP アドレスからのすべてのアクセスを検査する) にすることも、複数のメッセージおよびセッション属性 (データベース・ユーザー、ソース・プログラム、コマンド・タイプ、時刻など) を考慮した複雑なテストにすることもできます。また、指定された時間フレーム内で条件が満たされた回数を識別する場合もあります。

ルールで起動されるアクションは、通知アクション (例えば、1 人以上の受信者に対する E メール通知)、ブロッキング・アクション (クライアント・セッションが切断されるなど) のほか、イベントがポリシー違反としてログに記録されるだけの場合もあります。所定の環境やアプリケーションに固有と見なされる条件に対して必要とされるすべてのタスクを実行するカスタム・アクションを開発することができます。アクションの完全なリストについては、『ルール・アクションの概要』を参照してください。

ポリシー違反は、アラートまたは「ロギングのみ」アクションが起動されるごとにログに記録されます。オプションで、ルールを起動した SQL (データ値も含む) を、ポリシー違反で記録することができます。ポリシー違反をインシデントに割り当てるには、プロセスを使用して自動的に行うか、権限のあるユーザーが手動で行うことができます (「Guardium GUI」の『インシデント管理』タブを参照してください)。詳しくは、インシデント管理を参照してください。

注: 相関アラートをポリシー違反ドメインに書き込むこともできます (『相関アラート』) を参照してください。

ポリシー・ルールは、違反をロギングするほか、クライアント・トラフィックのロギング (構成体および構成体インスタンスとしてログに記録される) に影響を与える場合があります。

- 構成体は、基本的に、Guardium がトラフィック内で検出する要求のプロトタイプです。構成体に含まれるコマンド、オブジェクト、およびフィールドの組み合わせは非常に複雑な場合がありますが、それぞれの構成体は基本的に固有性がきわめて高いアクセス要求のタイプを表します。新しい構成体の検出およびロギングは、検査エンジンの開始時に始まり、デフォルトではセキュリティー・ポリシー・ルールに関係なく続行します (説明した例外は除きます)。
- トラフィック内で検出された構成体の各インスタンスもログに記録されます。各インスタンスは、特定のクライアント/サーバー・セッションに関連付けられます。構成体インスタンスの SQL は、ポリシー・ルールによりそのインスタンスまたはそのインスタンスの特定のクライアント/サーバー・セッション (値の有無に関わらず) の SQL のロギングが要求された場合を除いて、保管されません。

セキュリティー・ポリシー・ルールは、クライアント構成体インスタンスへの SQL の組み込みを制御するほか、セッションの残りの構成体およびインスタンスのロギングを無効にすることができます。

ボリュームが非常に大きい場合は、情報の解析や構成体およびインスタンスへの統合は、未解析ログ・オプションを使用して据え置くことができます。未解析ログを使用すると、アラートおよびレポートの生成は、ログに記録された情報が統合されるまで遅延されます。このトピックで後ほど説明する『未解析ログ』を参照してください。

ログに記録されるクライアント・トラフィックを完全に制御するために、ポリシーを選択的な監査証跡ポリシーとして定義することができます。このタイプのポリシーでは、監査のみ ルールおよびオプション・パターンによって、ログに記録されるすべてのクライアント・トラフィックが識別されます。このトピックで後述する『選択的な監査証跡の使用』を参照してください。

管理コンソール/ポリシー・インストールの ポリシー・インストーラー 画面から新規ポリシーをインストールすることに加えて、以下のことが可能です。

- 新規ポリシーを「ポリシー・ファインダー」画面からインストールできます。
- 「ポリシー定義」画面から、インストール済みの 1 つのポリシーを再インストールできます (その際、他のインストール済みポリシーが再インストールされることはありません)。
- 「ポリシー・ルール」画面から、インストール済みのポリシー・ルールを再インストールできます (その際、ポリシー全体が再インストールされることはありません)。

デフォルト・ポリシーが存在するのは、新規インストール (アップグレードではない) の場合のみです。ルールは存在しませんが、「選択的な監査」がチェックされています (これは Guardium システムがデフォルト・ポリシーによって収集するトラフィックはないということを意味します)。64 ビットの Guardium (新規インストール) のデフォルト・ポリシーは、デフォルト - 不明な接続に対するデータ・アクティビティーを無視です。

ポリシー・ルールの基本

ポリシー内では、ルールは、トラフィックの各エレメントが分析されるに従って、出現順に評価されます。

ルールには、次の 3 つのタイプがあります。

- クライアント要求に適用されるアクセス・ルール。例えば、特定の IP アドレス・グループから発行された UPDATE コマンドをテストするなど。
- サーバーから返される例外 (応答) を評価する例外ルール。例えば、1 分間に 5 回のログイン失敗があるかどうかの検査など。
- (要求に応じて) サーバーからの戻りデータを評価する抽出ルール。例えば、社会保障番号やクレジット・カード番号など、数値パターンに従って戻りデータをテストするなど。

カテゴリー、分類、および重大度

ルールごとに、オプションで「カテゴリー」または「分類」の一方、または両方を割り当てることができます。これらは、レポートおよびインシデント管理の両方について、ポリシー違反をグループ化するために使用します。

最小数およびリセット間隔

一部のアクティビティーは、特定の発生率を下回る場合には正常かつ受け入れ可能です。しかし、これら同じアクティビティーの発生率が許容可能なしきい値を超える場合には、注意を要します。例えば、対話式のデータベース・アクセスが許可されている場合、ログインの失敗が一定して、しかし比較的低い比率で発生することは想定内ですが、急激に発生率が上昇する場合は、アタックを受けていることを示す可能性があります。

しきい値を処理するために、各ポリシー・ルールに最小数とリセット間隔を指定できます。これは例えば、ログイン失敗数が、1 分 (リセット間隔) 以内に 100 (最小数) を上回ったときに、ルール・アクションを起動させる場合などに使用できます。この指定を省略した場合、デフォルトではルールが満たされるごとにルール・アクションが実行されます。

次のルールに進む

デフォルトでは、1 つのトラフィック単位に対するアクセス・ルールおよび例外ルールの評価は、1 つのルールに複数のアクションが含まれている場合を除いて、ルールの起動時に終了します。同じ、または類似した条件に対して複数のアクションを実行する必要がある場合、そのルールの「次のルールに進む」ボックスにマークを付けてください。

注: 「次のルールに進む」は、アクセス・ルールに続くアクセス・ルールおよび例外ルールに続く例外ルールには適用されますが、アクセス・ルールに続く例外ルールまたは例外ルールに続くアクセス・ルールには適用されません。

抽出ルールは、そのルールに先行するアクセス/例外ルールの終了に関係なく処理されます。このトピックの最後のルール定義参照表の抽出ルール「取り消し」で、ポリシー内の先行するルールによって既にロギングが選択されている応答をロギングから除外する方法について参照してください。

ポリシー違反による値の記録

これにマークを付けると、ルールが満たされる原因となった実際の構成体が SQL 文字列属性に記録され、レポートで使用可能になります。マークを付けないと、SQL ステートメントは記録されません。ポリシー違反にすべての値を含めるには、そのルールの「値の記録」ボックスにマークを付けてください。

注: 値が指定された全 SQL は、ポリシー違反レコードの、ポリシー違反レポート・ドメイン内でのみ使用可能になります。クライアント・トラフィック・ログや、データ・アクセス・ドメインからのレポートでは使用可能になりません。(データ値の有無に関係なく) 全 SQL をクライアント・トラフィック・ログに含めるには、「全 SQL をロギング」ルール・アクションを使用してください。

ルールの処理について詳しくは、以下のトピックを参照してください。

- インストールしたポリシーのポリシー・ルールを表示
- ルールでの値および/またはグループ値の指定
- ルールをフィルターに掛けサブセットのみを表示
- ルールのコピー
- データベース ACL から推奨されるルールの使用
- ルールの追加または編集
- ポリシー・シミュレーターの使用

ルールでの値および/またはグループ値の指定

多くのルール属性では、単一の値、グループ値、またはその両方を、アプリケーション・ユーザーについて説明しているものと同様の制御を使用して指定できます。

グループ・メンバーにはワイルドカード (%) 文字が含まれる場合があり、グループの各メンバーが複数の実値に一致することがあるのでご注意ください。

グループを選択する際には、グループにワイルドカードが含まれる場合がある点にご注意ください。

- **ネガティブ・ルール**:「Not」ボックスにマークを付けて、ネガティブ・ルールを作成します。例えば、指定したアプリケーション・ユーザーではない、選択したグループのメンバーではない、あるいは指定したアプリケーション・ユーザーと選択したグループのメンバーのどちらでもない、など。
- 空の値: トラフィック内の空の値を検査するために、特殊値 guardium://empty を入力します。この値は、フィールド「データベース名」、「データベース・ユーザー」、「アプリケーション・ユーザー」、「OS ユーザー」、「ソース・アプリケーション」、「イベント・タイプ」、「イベント・ユーザー名」、および「アプリケーション・イベント・テキスト」にのみ指定可能です。
- テストする新規グループを定義するには:「グループ」ボタンをクリックして新規グループを定義し、「グループ」リストからそのグループを選択します。
- 任意の値とマッチングするには: 値ボックスをブランクのままにして、「グループ」リストから何も選択しません (例のように、ダッシュ線が選択されていることを確認してください)。
- 特定の値のみとマッチングするには: マッチングする値を値ボックスに入力し、「グループ」リストからは何も選択しません。
- グループの任意のメンバーとマッチングするには: 値ボックスをブランクのままにして、リストから該当グループを選択します。最小数が 1 より大きい場合、カウンターは 1 つになり、グループの任意のメンバーが一致するごとに増分されます。
- 個々の値またはグループの任意のメンバーとマッチングするには: 値ボックスに具体的な値を入力し、リストからグループを選択します。最小数が 1 より大きい場合、カウンターは 1 つになり、個々の値またはグループの任意のメンバーが一致するごとに増分されます。
- 最小数が 1 より大きい場合に、個々の値をそれぞれ個別にカウントする: 値ボックスにドット (.) を入力し、グループ・リストからは何も選択しません。「サービス名」または「ネット・プロトコル」ボックスでは、ドット・オプションを使用できないので注意してください。最小数が 1 より大きい場合に、グループのメンバーをそれぞれ個別にカウントする: 値ボックスにドット (.) を入力し、リストからグループを選択します。「サービス名」または「ネット・プロトコル」ボックスでは、ドット・オプションを使用できないので注意してください。

正規表現を使用したパターン・マッチング

特殊パターン・テストに加えて、正規表現を使用してトラフィックでデータの複合パターンを検索することができます。UNIX の正規表現の実装とは異なり、Guardium の正規表現の実装は POSIX 1003.2 に準拠します。正規表現は、後ろに「正規表現の作成」ボタンがあるすべてのフィールドで使用可能です。

注: 正規表現は、「データベース・ユーザー」、「アプリケーション・ユーザー」、「ソース・アプリケーション」、「フィールド名」、「オブジェクト」、「アプリケーション・イベント値テキスト」などのフィールドでも使用可能です。その際には、フィールドに対応するテキスト・ボックスに特殊値 guardium://regexp/(正規表現) を入力します。
注: IBM Security Guardium は、英語以外の言語の正規表現はサポートしていません。
正規表現の使用方法について詳しくは、『正規表現』を参照してください。

- 特殊パターン・テスト
  これらの特殊パターン・テストを使用することで、データベース・サーバー とクライアントの間で送受信されるトラフィックに含まれる機密データを識別できます。
- ルール・アクション
  ルールが満たされた場合に実行されるアクションを選択する際には、検討しなければならないいくつかの要因があります。
- ポリシーの作成
  ポリシーを作成するだけでなく、ポリシーの変更、複製、削除を行うことができます。
- ポリシーのインストール
  このトピックを使用して、Guardium コレクターにポリシーをインストールし、スケジュールを変更します。
- ルール定義フィールド
  ポリシー・ルールを定義する際に、以下のフィールドを使用することができます。
- カスタム・ルールを Guardium ポリシーに統合する方法
  カスタム資格のシステムから Guardium ポリシーを自動的に変更する、または派生させる方法を説明します。
- 適切な無視アクションの使用方法
  ポリシー・ルールで無視アクションを使用した場合のデータの処理方法を詳しく説明します。
- 文字セット
  抽出ルールで文字セット・コードを使用できます。

親トピック: 保護

特殊パターン・テスト

これらの特殊パターン・テストを使用することで、データベース・サーバー とクライアントの間で送受信されるトラフィックに含まれる機密データを識別できます。

各ポリシー・ルールには、1 つの特殊パターン・テストを含めることができます。これらのテストのいずれかを使用するには、最初にいずれかの特殊パターン・テスト名、次に 1 つのスペースとルール名を固有にするための 1 つ以上の追加の文字を含むルール名を使用します。例えば、従業員の社会保障番号を検索する場合、ルールに `guardium://SSEC_NUMBER employee` という名前を付けます。ルールの他のすべてのコンポーネント (特定のクライアント、サーバーの IP アドレス) も指定できます。

これらのテストは文字パターンに一致しますが、その一致では、対象の項目 (社会保障番号など) が確実に検出されるわけではありません。さまざまな環境下 (特に、データ内で長い数値シーケンスが連結されている場合など) においては、誤検出が生じる可能性があります。

guardium://CREDIT_CARD

クレジット・カード番号パターンを検出します。16 桁の数字文字列のテスト、または各セットの間がブランクで区切られた 4 桁の数字 4 セットのテストを行います。 この特殊パターン・テストは、アメリカン・エキスプレスの 15 桁のクレジット・カード番号パターン (最初の数字が 3、2 番目の数字が 4 または 7) についても機能します。例: `1111222233334444` または `1111 2222 3333 4444`

ルール名が "guardium://CREDIT_CARD" で始まり、「データ・パターン」フィールドに 有効なクレジット・カード番号パターンが指定されている場合、ポリシーは、標準の パターン・マッチングに加えて Luhn アルゴリズム (クレジット・カード番号などの ID 番号 検証のために幅広く使用されているアルゴリズム) を使用します。Luhn アルゴリズムは追加の検査であり、パターン検査の代わりにはなりません。 有効なクレジット・カード番号は、16 桁の数字文字列、または 4 桁の数字 4 セット (各セットの間がブランクで区切られる) です。 このパターン・マッチングに Luhn アルゴリズムを組み込むには、「検索式」ボックスに guardium://CREDIT_CARD ルール名と有効な [0-9]{16} 数値の両方が指定されている必要があります。

guardium://PCI_TRACK_DATA

磁気ストライプ・データの 2 つのパターンを検出します。最初のパターンは、セミコロン (;)、16 桁の数字、および等号 (=)、20 桁の数字、および疑問符 (?) で構成されています。 以下に例を示します。

```
;1111222233334444=11112222333344445555?
```

2 つ目のパターンは、パーセント記号 (%)、文字 B、16 桁の数字、カラット記号 (^)、スラッシュ (/) で終了する可変長の文字文字列、カラット記号 (^) で終了する 2 つ目の可変長文字文字列、31 桁の数字、および疑問符 (?) で構成されています。 以下に例を示します。

```
%B1111222233334444^xxx/xxxx x^11112222333344445555666677778888?
```

guardium://SSEC_NUMBER

社会保障番号形式 (3 桁の数字、ダッシュ記号 (-)、2 桁の数字、ダッシュ記号 (-)、4 桁の数字) の数値を検出します (`123-45-6789` など)。ダッシュ記号はいずれも必須です。

guardium://CPF

Cadastro de Pessoas Físicas (CPF)、ブラジルの個人識別用の ID。`nnn.nnn.nnn-nn` 形式の 11 桁の数字が含まれます。最後の 2 桁はチェック・ディジットです。番号が有効であるか検査できるようにするために、元の 9 桁の数字からチェック・ディジットが計算されます。式内の書式制御文字はオプションです。式に一致する場合、チェック・ディジットが検査されます。

guardium://CNPJ

Cadastro Nacional de Pessoas Jurídicas (CNPJ)、ブラジル企業に使用される ID 番号。`00.000.000/0001-00` 形式の 14 桁の数字が含まれます。

- 最初の 8 つの数字は登録番号を表します。
- 次の 4 つの数字はそのエンティティーの支社を示します。0001 が本社を示すデフォルト値です。
- 最後の 2 つの数字はチェック・ディジットです。

式内の書式制御文字はオプションです。式に一致する場合、チェック・ディジットが検査されます。

親トピック: ポリシー

ルール・アクション

ルールが満たされた場合に実行されるアクションを選択する際には、検討しなければならないいくつかの要因があります。

ブロッキング・アクション (S-TAP/S-GATE)

このセクションでは、S-TAP® ターミネートおよび S-GATE のアクションについて説明します。

S-TAP ターミネート・アクション

S-TAP ターミネート・アクションは、データベース接続 (セッション) を終了し、そのセッションでの追加の要求をブロックします。このアクションは、S-GATE が使用されているかどうかに関わらず、S-TAP で使用可能です。

注: S-TAP ターミネートを使用すると、起動している要求は通常ブロックされませんが、そのセッションからの追加の要求は (高確率で) ブロックされます (複数の要求が、セッション終了前に通過する場合があります)。

S-GATE アクション

S-GATE は、ネットワーク接続とローカル接続の両方に関して、S-TAP を通じたデータベース保護を提供します。

S-GATE が有効な場合、すべてのデータベース接続 (セッション) は評価され、以下の S-GATE モードのいずれか 1 つでモニターされるようにタグ付けされます。

- 接続 (S-GATE は「オン」) - S-TAP は、そのセッションに対してファイアウォール・モードになります。このモードでは、データベース要求は保留され、要求ごとに判定を待機してからその応答をリリースします。このモードでは、待ち時間が想定されます。ただし、問題要求は確実にブロックされます。

- 切断 (S-GATE は「オフ」) - S-TAP は、そのセッションに対して通常のモニター・モードになります。このモードでは、遅延なしで要求がデータベース・サーバーに渡されます。このモードでは、待ち時間は想定されません。

「guard_tap.ini」の S-GATE 構成は、すべてのセッションにデフォルト S-GATE モード (「接続」または「切断」) を定義するほか、コレクターが応答しない場合の S-GATE 判別に関連するその他のデフォルトを定義します。 S-GATE は、デフォルト S-GATE 構成以外には、以下の S-GATE ポリシー・ルール・アクションを使用するリアルタイム・ポリシー・メカニズムを通じて制御されます。

- S-GATE ATTACH: 特定のセッションに対して S-GATE モードを「接続」に設定します。

  そのセッションのトラフィックを慎重に監視 (そして必要に応じてブロック) する必要が生じる特定の基準が満たされた場合の使用が想定されています。
- S-GATE DETACH: 特定のセッションに対して S-GATE モードを「切断」に設定します。

  「安全」と見なされるセッションや、待ち時間が許容されないセッションでの使用が想定されています。
- S-GATE ターミネート: セッションが接続されている場合にのみ効果があります。これは、ファイアウォール保護された要求の応答をドロップし、同じデータベースのセッションを終了させます。S-GATE ターミネート・ポリシー・ルールは、その前に監視されていたセッションを終了させます。

注:

- S-GATE/S-TAP ターミネートは、ワイルドカード文字のあるメンバーを含むクライアント IP グループでは動作しません。 S-GATE/S-TAP ターミネートは単一の IP アドレスでのみ動作します。 お客様が複数の IP エントリーを使用することを希望する場合は、ワイルドカートをグループで処理する必要があります。お客様は、ポリシーでビジネス・ニーズに対応するために、信頼できるユーザー/クライアントのグループ、または信頼できないユーザー/クライアントのグループを作成できます。
- ATAP および S-GATE には、下位の Linux カーネルに関する制限事項があります。基本的に、10.1.2 以降の S-TAP では、2.6.36 より前の ATAP およびカーネルを使用する Linux を除き、どのような場合でも S-GATE がサポートされます。
- MySQL データベースの場合、MySQL のデフォルト・コマンド行接続が 'mysql -u<user> -p<pass> <dbname>'であることに注意してください。

  このモードでは、MySQL は最初にこのデータベース内のすべてのオブジェクトおよびフィールドをマップして (TAB による) オートコンプリートをサポートします。このマッピングに関与するオブジェクトまたはフィールドに終了ルールが指定されている場合、それにより接続セッションが即時に無効になります。これを防ぐには、「-A」フラグ (「オートコンプリート」機能を無効にして、「終了」ルールを起動しない) を指定して MySQL に接続します。 もう 1 つのオプションとして、ルールを適切に調整し、これらのオブジェクト/フィールドに対するいかなるアクセスにおいても終了せず、代わりにより絞り込まれた基準を検出し、ログイン・シーケンスでルールが起動されないようにする方法があります。

アラート・アクション

アラート・アクションは、1 人以上の受信者に通知を送信します。

アラート・アクションごとに複数の通知を送信することが可能です。その通知は、以下の通知タイプを 1 つ以上組み合わせたものであってもかまいません。

- E メール・メッセージ。 Guardium® ユーザーにアドレス指定する必要があり、Guardium の SMTP サーバー構成を通じて送信されます。リアルタイム E メール通知の追加の受信者は、「起動者」(ポリシー起動の原因となった実際の SQL コマンドを開始したユーザー) と「所有者」(データベースの所有者) です。起動者と所有者は、Guardium API を通じて構成されたユーザー ID (IP ベース) を取得することによって識別されます。選択項目「ユーザー・データベース関連付けによるデータ・セキュリティー」(accessmgr から選択可能) は、マッピングを表示します (これは、Guardium API コマンド「list_db_user_mapping」を実行すると表示される内容に類似しています)。
- SNMP トラップ。Guardium アプライアンス用に構成されたトラップ・コミュニティーに送信されます。
- Syslog メッセージ。syslog に書き込まれます。
- カスタム通知。ユーザー作成の通知ハンドラーで、Java™ クラスとして実装されます。

注: アラート定義および通知は、データ・レベル・セキュリティーの影響を受けません。その理由として、アラートがユーザーとの関連で評価されないことや、アラートが複数のユーザーに関連付けられたデータベースに関連している可能性があり、そのアラート通知の受信者が 1 人もいないという状態を回避するためなどが挙げられます。

メッセージ・テンプレートを使用してアラートが生成されます。「グローバル・プロファイル」から、複数の名前付きメッセージ・テンプレートが作成され、変更を加えられます。アラート・アクションには、それぞれ異なるタイプの状態に適合するいくつかのタイプがあります。

- 毎日アラートは、毎日、ルールの初回マッチング時にのみ通知を送信します。
- セッションごとに 1 回アラートは、ルールがマッチングしたセッションごとに 1 回のみ通知を送信します。このアクションは、特定のイベント発生の通知を受けるが、単一セッションの間にそのイベントのインスタンスごとに通知を受ける必要がない場合などに適しています。例えば、特定の機密オブジェクト更新時に通知の送信を受けるとしても、プログラムが単一セッションの間にそのオブジェクトの数千個のインスタンスを更新する場合、アラート受信者に数千もの通知が送信されることは望ましくないはずです。

- アラートのみ - 「アラートのみ」の場合、タイプ syslog を使用すると、メッセージは /var/log/messages に直接送信されます。 「アラートのみ」のその他のタイプでは、メッセージは MESSAGE 表に送信されます。「アラートのみ」は、ポリシー違反を通知しません。

- 一致ごとにアラートは、ルールが満たされるごとに通知を送信します。これは、発生するごとに注意を要する条件に適しています。
- 時間間隔ごとにアラートは、 ログ細分度期間ごとに 1 回通知を送信します。例えば、ログ細分度が 1 時間に設定された場合、通知は毎時ルールへの最初の一致時にのみ送信されます。(Guardium の管理者は、ログ細分度を「検査エンジン構成」パネルで設定します。)

ロギング・アクションまたは無視アクション

これらのアクションは、監視対象トラフィックに基づいてロギングのレベルを制御します。

ロギング・コマンドおよび無視コマンドは、通常いつでも使用できますが、監査のみアクションは選択的な監査証跡ポリシーでのみ使用可能です。アクセス・ルール、例外ルール、および抽出ルールは、許可されるアクションに応じて異なります。「アクションの追加」ボタンをクリックして、提供される内容を参照してください。

- 監査のみ: 選択的な監査証跡ポリシーでのみ使用可能です。ルールを起動した構成体をログに記録します。選択的な監査証跡ポリシーでは、デフォルトでは構成体はログに記録されないため、この選択を使用してログに記録される内容を指定します。アプリケーション・イベント API を使用している場合、データベース・ユーザー名の情報をレポートで使用できるようにするには、このアクションを使用してデータベース・ユーザー名のロギングを強制する必要があります (そうしないと、この場合、ユーザー名はブランクになります)。
- 許可: 一致する場合、ポリシー違反をログに記録しません。「許可」アクションを選択した場合、他のアクションをルールに追加することはできません。構成体は、ログに記録されます。

- FAM アラートおよび監査: アラートと監査という 2 つのルール・アクションがあります。アラート・アクションでは、一致するイベントが見つかった場合に、受信者とテンプレートを使用してアラートがトリガーされます。監査アクションでは、ルールをトリガーした構成体がログに記録されます。
- FAM 監査のみ: ルールをトリガーした構成体がログに記録されます。
- FAM 無視: イベントはログに記録されません。
- FAM アクセス違反のロギングのみ: FAM のアクセス違反がログに記録されます。
- ロギングのみ: ポリシー違反のみをログに記録します。ルールがポリシー違反として起動されたという事実を参照します。許可アクションを例外として、ポリシー違反は (アクションがロギングを抑止している場合を除いて) ルールが起動されるごとにログに記録されます。
- マスクされた詳細をロギング: この要求の全 SQL を、値を疑問符 (???) に置き換えてログに記録します。このアクションは、アクセス・ルールおよび抽出ルールで使用可能です。
- 全詳細をロギング: この要求の全 SQL 文字列と正確なタイム・スタンプをログに記録します。詳細と例については、注を参照してください。
- 値を含む全詳細をロギング: 「全詳細をロギング」と似ていますが、それに加えて、各値が個別のエレメントとして保管されます (値が解析され、データベースの個別の表に記録されます)。このロギング・アクションでは、関連するコマンドの具体的な値もログに記録されるため、より多くのシステム・リソースが使用されます。このロギング・アクションは、これらの値について具体的な条件を持つレポートを生成する必要がある場合にだけ使用してください。このロギング・アクション活動化の選択項目は、技術サービス (admin user/Tools/Support Maintenance) に確認の上で使用可能になります。
- セッションごとに全詳細をロギング: この要求およびセッションの残りについて、全 SQL 文字列と正確なタイム・スタンプをログに記録します。
- セッションごとに値を含む全詳細をロギング: 「値を含む全詳細をロギング」および「セッションごとに全詳細をロギング」の説明を参照してください。このロギング・アクション活動化の選択項目は、技術サービス (admin user/Tools/Support Maintenance) に確認の上で使用可能になります。
- ロギングをスキップ: 一致する場合、ポリシー違反はログに記録されず、構成体のロギングが停止します。これは許可アクションに似ていますが、それに加えて、構成体のロギングを停止します。このアクションは、重要性がないことが認識されている要求の構成体のロギングを除外するために使用します。ルールが適用される前に構成体の分析またはロギングが発生するため、GDM_CONSTRUCT がログに記録される場合があります。 ただし、構成体がセッションに組み込まれることはありません。 この機能は、データベース・エラー・コードのみに関する例外ルールにも適用され、アプリケーションが大量のエラーを生成し、ユーザーにそのアプリケーション・エラーを停止する術がない場合に、エラーをログに記録しないことをユーザーに許可します。
- セッションごとに応答を無視: セッションの残りに対する応答が無視されます。このアクションはポリシー違反をロギングしませんが、セッションの残りに対する応答の分析を停止します。 このアクションは、以後のデータベース応答が重要でないことがわかっている場合に役立ちます。このアクションは、S-TAP からデータをスニッフィングする場合に機能します。SPAN ポートからデータをスニッフィングする場合には、このアクションは機能しません。
  注: 「セッションごとに応答を無視」の場合、スニファーは照会に対する応答を 1 件も受信しないか、応答が無視されるため、COUNT_FAILED および SUCCESS の値は表のデフォルトが何であっても、この場合は COUNT_FAILED=0 および SUCCESS=1 です。
- セッションを無視: 現行の要求およびセッションの残りが無視されます。このアクションは、ポリシー違反をログに記録しませんが、構造のロギングを停止し、そのセッションの残りのいずれのタイプのポリシー違反もテストしません。このアクションは、例えば、データベースにテスト領域が含まれ、データベースのその領域に対してポリシー・ルールを適用する必要がない場合などに役立ちます。「セッションを無視」ルールは、トラフィックのフィルター処理のための最も効率的な手段になります。「セッションを無視」ルールを適用すると、個々のセッションからのアクティビティーが S-TAP によって削除されるか、スニファーによって完全に無視されます。 ただし、セッションが無視されても、接続 (ログイン/ログアウト) の情報は、常にログに記録されます。
- S-TAP セッションを無視: 現行の要求および S-TAP セッションの残りが無視されます。このアクションは、大量のネットワーク・トラフィックを生成する特定のシステム、ユーザー、またはアプリケーションのポリシー・ビルダー・メニュー画面での指定と組み合わせて実行されます。このアクションは、S-TAP セッションからの以後のデータベース応答が重要でないことがわかっている場合に役立ちます。「S-TAP セッションを無視」には 2 つのオプションがあります。
  IGNORE_ENTIRE_STAP_SESSION は「ハード型」の無視で、取り消すことができません。IGNORE_STAP_SESSION (REVOCABLE) は「ソフト型」の無視で、このルール・アクションでは、データベースへの新しい接続を必要とせずにセッション・トラフィックを再送信できます。ignore_stap_session (取り消し可能) に関する注記 - 「STAP の無視の取り消し」コマンドは、1 つのスニファー・プロセスで S-TAP ホストに対して永続します。S-TAP が無視の取り消し状態になった後に開かれた新しいセッションは、(ルール「S-TAP セッションを無視 (取り消し可能)」がトリガーされたとしても) 無視されません。無視の取り消し - アクション「S-TAP セッションを無視 (取り消し可能)」によって無視されていたセッションが再開します。つまり、「無視の取り消し」コマンドが S-TAP によって受信された後、トラフィックが Guardium システムに送信されます。 (このコマンドは S-TAP 制御-->送信コマンドから送信できます)。
- セッションごとに SQL を無視: セッションの残りについて SQL がログに記録されません。例外は引き続きログに記録されますが、システムは、その例外に対応する SQL 文字列をキャプチャーしない場合があります。
- 抽出カウンターのロギング: 抽出ルールでのみ使用可能。このアクションは、カウンターを更新しますが、戻りデータをログに記録しません。このアクションは、カウンター値が最重要であり、戻り値の重要度が最小の場合に、ディスク・スペースを節約します。
- マスクされた抽出カウンターのロギング: 抽出ルールでのみ使用可能。このアクションは、カウンターを更新し、値を疑問符に置き換えて SQL 要求をログに記録しますが、戻されたデータ (応答) はログに記録しません。
- 隔離: アクセス、例外、抽出の各ルールで使用可能。 このアクションの目的は、特定の期間中に、同一ユーザーが同一サーバーにログインすることを防止することです。ユーザーが隔離される時間の値を指定せずに、ルールに QUARANTINE アクションを指定することはできないという検証項目があります。「検疫分数」を参照し、この検疫時間を設定してください。セッションが監視されている (S-GATE シナリオ) 場合、ドロップ判定を送信します。セッションが監視されていない (S-TAP ターミネート・シナリオ) 場合、S-TAP にセッションを停止させます。 現在時刻を取得し、リセット間隔フィールドから得た分数を追加します。新しいタイム・スタンプを入手します。新しい構成では、(このタイム・スタンプでソートされた) ソート済みリストを保持します。各エレメントには、タイム・スタンプに加えて、サーバー IP、サーバー・タイプ、データベース・ユーザー名、サービス名、およびこれが監視セッションであるかどうかを示すフラグがそれぞれ 1 つずつあります。
- 解析なし - SQL ステートメントは解析されません。
- クイック解析フィールドなし - SQL ステートメント内のフィールドは解析されません。すべてのクイック解析ルールは、SQL 文字列が 100 文字を超える場合にのみ適用されます。
- クイック解析ネイティブ - Guardium S-TAP for Db2 on z/OS でのみ使用されます。このルール・アクションは、大量のトラフィックのためにスニファーが過負荷になっている環境で使用します。 このルール・アクションを使用すると、S-TAP for Db2 on z/OS のパフォーマンスが向上します。
- クイック解析: アクセス・ルールについてのみ解析を行い、セッションの残りの部分では SQL ステートメントの解析は行いません。 これにより、構文解析時間が削減されます。このモードでは、アクセスを受けるすべてのオブジェクトを判別可能 (オブジェクトは WHERE 節よりも前に出現するため) ですが、影響を受ける正確なオブジェクト・インスタンスは WHERE 節によって判別されるため、不明になります。
- 編集: 抽出ルールについてのみ、ユーザーはこの機能を使用して、レポート内の特定ユーザーのデータベース照会出力の一部分 (例えば、クレジット・カード番号) にマスクを掛けることができます。抽出ルール・メニュー選択項目の「データ・パターン」セクションの「置換文字」の選択内容により、マスク文字が定義されます。抽出ルールによって生成された出力がデータ・パターンの正規表現に一致する場合は、括弧「(」および「)」で囲まれたサブ表現に一致する部分がマスキング文字に置き換えられます。事前定義した正規表現 (fast regexp) も使用可能です。詳しくは、ルール定義フィールドの『データ・パターン』を参照してください。
  制約事項:
  - S-TAP ライブ・アップグレード後のオープン・セッションでは、編集は機能しません。
  - フィールドと数値型を指定して作成されたテーブルでは、編集は機能しません。
  - SQL パターンは、編集ルールではサポートされません。
- 値を別々に記録する/値を別々に記録しない: このアクションはセッション・ベースのアクセス・ルールです。トランザクション間の区別を行うために、リプレイ機能で使用されます。
- 自動コミットをオンとしてマーク/自動コミットをオフとしてマーク: このアクションはセッション・ベースのアクセス・ルールです。異なるデータベースでは自動コミット・モデルが各種あるため、リプレイ機能で使用されます。

- z/OS 監査: z/OS コレクション・プロファイル・ポリシー・ルール (IMS、データ・セット、および Db2) で特に使用されます。これらのルールは、z/OS サーバーで収集するトラフィックを指定するために使用されます。このアクションは、フィルター条件を満たすトラフィックをコレクターに送信することを指定します。これが、コレクション・プロファイル・ルールで指定できる唯一のアクションです。

注:

Linux では、編集 (修正) はバージョン 9.1 の時点でサポートされています。すべての UNIX プラットフォームで、修正は ANSI 文字セットに対してのみサポートされます。

編集 (修正) ルールは、(OBJECT_NAME や VERB のように) SQL レベル/属性ではなく、セッション・レベルで設定する (つまり、IP やユーザーなどのセッション属性でルールを起動する) 必要があります。修正を必要とする SQL で修正ルールを設定すると、修正命令が S-TAP に到達するまでに数ミリ秒の時間がかかってしまい、一部の結果がマスクを掛けられずに通過する可能性があるからです。

すべての SQL が確実に修正されるようにするには、(guard_tap.ini で) すべてのセッションの S-TAP (S-GATE) デフォルト・モードを「接続」に設定します。こうすることで、通過するすべてのコマンドがルール・エンジンの検査を受けることになり、各要求が保留されて、その要求に関するポリシーの判断を待機するようになります。 これをデプロイすると若干の待ち時間が必要になりますが、この方法により 100% 確実にデータを修正できます。

Informix データベースの場合、データ型として char が使用されると、各列の終わりが Null で終了されません。したがって、sendmsg システム呼び出しでは、4 つのすべての列が 1 つの列としてキャプチャーされます。KTAP はキャプチャーしたデータが何であろうと、そのデータの編集を試みます。これは、編集と Informix データベースを使用する際の制限事項です。

注:

HTTP サポートについては、ポリシー・アクションに制限があります。 以下のポリシー・アクションは HTTP ではサポートされません: 「S-TAP ターミネート」、および「ロギングをスキップ」。

その他のアクションについては、以下のものは HTTP によりサポートされません。

- 「セッションごとに応答を無視」: HTTP が例外と抽出をサポートしていないためです。
- 「セッションごとに SQL を無視」: HTTP に SQL が含まれていないためです。
- 「隔離」: このアクションはユーザー隔離に使用されますが、HTTP は DBUser および OSUser をサポートしていません。
- 「クイック解析」: このアクションはログ SQL 用です。
- 「SGate ターミネート」: このアクションは Hadoop ではサポートされません。すべての強制終了アクションは HTTP には機能しません。

ポリシー条件について - 以下の条件は、HTTP ではサポートされません。

クライアント MAC、データベース名、データベース・ユーザー、アプリケーション・ユーザー、OS ユーザー、ソース・アプリケーション、マスキング・パターン、置換文字、隔離時間 (分)、影響を受けるレコードしきい値、XML パターン、イベント・タイプ、イベント・ユーザー名、アプリケーション・イベント値テキスト、アプリケーション・イベント値テキスト・グループ、アプリケーション・イベント値テキストおよびグループ、数値、日付。

詳細な説明と例

全詳細をロギング

デフォルトでは、Guardium コレクターは、SQL 文字列をロギングするときに、すべての値にマスクを掛けます。以下に例を示します。

```
insert into tableA (name,ssn,ccn) values ('Bob Jones', '429-29-2921','29249449494949494')
```

この場合、ログには次の値が記録されます: `insert into tableA (name,ssn,ccn) values (?, ?,?)`. これは、次の 2 つの理由から、デフォルトの振る舞いになります。

1. 値は、機密情報を含んでいることがあるため、デフォルトでログに記録するべきではない。
2. 値なしのロギングにより、アプライアンス内部におけるシステム・パフォーマンスとデータ保存に要する時間が増大する可能性がある。データベース・トラフィックには、1 時間に数百、数千、あるいは数億回繰り返される値以外はすべて同一の大量の SQL 要求が含まれていることがよくあります。 Guardium は、値をマスキングすることにより、これらの繰り返される SQL 要求を「構成体」と呼ばれる 1 つの要求に統合することができます。個々の SQL 要求/構成体をそれぞれ個別にログに記録する代わりに、構成体をログに記録すると、構成体が実行された回数のカウンターとともに、毎時 (セッションごとに) 1 回だけログへの記録が行われます。こうすることで、データベース内に数百 (あるいは数億) の行が作成される代わりに、新しい行が 1 つだけ追加されるので、ディスク・スペースの大幅な節約になります。

「全詳細をロギング」では、Guardium はマスクの解除された値および各個別の要求とともにデータをログに記録します。「全詳細をロギング」では正確なタイム・スタンプも提供されます。一方、詳細なしのロギングでは、ログ細分度期間 (通常は 1 時間) 内における構成体の最新のタイム・スタンプが提供されます。

S-TAP セッションを無視 -「S-TAP セッションを無視」が起因となり、コレクターは S-TAP に特定のセッションに対するログアウト通知を除くすべてのトラフィックの送信を停止するよう指示するシグナルを送信します。`where DBUserName?=scott, Ignore S-TAP Session` というルールがある場合の例を以下に示します。

- Scott がデータベース・サーバーにログインすると、S-TAP はコレクターに接続情報を送信します。
- コレクターは、接続をログに記録します。セッション情報 (ログイン/ログアウト) は、常にログに記録されます。
- コレクターは、この特定のセッションからのトラフィックの送信を以後停止するように S-TAP にシグナルを送信します。これは、Scott がデータベース・サーバーに対して実行するすべてのコマンド、およびデータベース・サーバーから Scott 宛てに送信されるすべての応答 (結果セット、SQL エラー、その他) が S-TAP によって廃棄され、以後コレクターに到着しなくなることを意味します。
- Scott がデータベース・サーバーからログアウトすると、S-TAP はこの情報をコレクターに送信します (ログイン/ログアウト情報は、セッションが無視される場合であっても常に記録されます)。
- Scott が再度ログインすると、これらのステップが繰り返されます。どのセッションを無視するかのロジックは、S-TAP ではなくコレクターが保守します。

選択的な監査証跡を使用している場合であっても、ポリシーに「セッションを無視」ルールを組み込むことが引き続き非常に重要である点に十分注意してください。「セッションを無視」ルールを使用すると、コレクターの負荷を大幅に削減できます。これは、S-TAP レベルで情報をフィルター操作することにより、コレクターがその情報を受信することがなくなり、最終的にログに記録されることのないトラフィックの分析にリソースを消費する必要がなくなるためです。「セッションを無視」ルールが指定されていない「選択的な監査証跡」ポリシーは、すべてのトラフィックがデータベース・サーバーからコレクターに送信され、コレクターがデータベース・サーバーの生成したすべてのコマンドおよび結果セットを分析することになることを意味します。

Guardium アプリケーションでの MS-SQL または Sybase バッチ・ステートメントの使用

制限

MS-SQL または Sybase バッチ・ステートメント内の SQL コマンドの成功または失敗が、正しく表示されない場合があります。

MS-SQL または Sybase SQL バッチ・ステートメントは、複雑なプロシージャーを作成する場合に主に使用されます。

SQL ステートメントを個別に実行すると、各ステートメントの状況は個別に追跡され、正しい成功値または失敗値が示されます。

(MS-SQL または Sybase で使用される) SQL ステートメントのバッチがまとめて実行されると、返される状況は、バッチ内の最後のトランザクションの単一の状況となります。

Guardium の例

[SQL バッチの開始]

SQL 1 ステートメント - 失敗 (SQL 1 statement - failed)

SQL 2 ステートメント - 失敗 (SQL 2 statement - failed)

SQL 3 ステートメント - 成功 (SQL 3 statement - success)

[SQL バッチの終了]

Guardium アプリケーションでは、MS-SQL または Sybase バッチ・ステートメントで、最後の SQL ステートメントの成功または失敗のみがレポートされます。この例では、SQL 1 および SQL 2 は失敗していますが、MS-SQL または Sybase バッチ・ステートメントは成功とレポートされます。

文字セットの設定

代替文字セットをセッションにアタッチするには、ポリシー抽出ルールでアクションを使用できます。

文字セットを使用した特殊パターン・ルール

抽出ルールの例 (hint を使用):

文字セット EUC-JP (コード 274)。

抽出ルール・パターン: `guardium://char_set?hint=274`

結果として、抽出ルールはセッションにアタッチされ、他の文字セットがない場合、アナライザーはセッションで EUC-JP を使用します。

抽出ルールの例 (force を使用):

文字セット EUC-JP (コード 274)。

抽出ルール・パターン: `guardium://char_set?force=274`

結果として、抽出ルールはセッションにアタッチされ、アナライザーはどのような場合でもセッションで EUC-JP 文字セットを使用します。前に使用されていた文字セットの代わりに EUC-JP が使用されます。

抽出ルールは、通常、少し遅れてセッションにアタッチされるので注意してください。したがって、短いセッションやセッションの最初の方では、文字セットの変更が直ちに反映されない場合があります。スキーマは、Oracle、Sybase、MY SQL、および MS SQL に適用されます。

アナライザー・ルール

アナライザー・レベルには特定のルールを適用することができます。アナライザー・ルールの例としては、ユーザー定義文字セット、ソース・プログラムの変更、ファイアウォール・モードへの監視判定の発行などがあります。以前のリリースでは、ポリシーやルールは、ロギング状態での要求処理の最後に適用されていました。一部のケースにおいて、これは、これらのルールに基づいた決定が遅れることを意味していました。アナライザー・レベルでルールを適用するということは、より早い段階で決定を行えることを意味します。

未解析ログ

「ポリシー・ビルダー」の「ポリシー定義」にリストされている「未解析ログ」オプションを使用すると、Guardium アプライアンスは情報を即時に解析することなくログに記録することができます。

こうすることで、処理リソースが節約され、より大量のトラフィックを処理できるようになります。そのデータは、コレクターまたは統合サービス単位のいずれかで、後ほど Guardium の内部データベースに対して解析およびマージすることができます。

「未解決ログ」にチェック・マークを付けると、以下のようになります。

- データはリアルタイムでは解析されません。
- 未解析ログは、指定された「未解析ログ・リスト」レポートで確認できます。
- データを解析し、標準アクセス・ドメインにマージするオフライン処理は、「マージ」>「アクティビティー・モニター」>「未解析ログ処理」を通じて構成することができます。

未解析ログに関するルール

このセクションでは、未解析ログに関するルールを使用した場合の相違点について説明します。

「未解析ログに関するルール」にチェック・マークを付けると、以下のようになります。

- セッション・レベルのルールがリアルタイムで検査されます。
- オフライン処理が行われない場合、ルールは評価されません。

「未解析ログに関するルール」にチェック・マークを付けないと、以下のようになります。

- ポリシー・ルールは、現行のインストール・ポリシーを使用して処理時に起動します。

注: 未解析ログに関するルールは、フィールド、オブジェクト、SQL 動詞 (コマンド)、オブジェクト/コマンド・グループ、およびオブジェクト/フィールド・グループを含んだポリシー・ルールでは機能しません。未解析ログ処理において、「未解析」とは構文ツリーが構築されていないことを意味します。 構文ツリーがない場合、フィールド、オブジェクト、および SQL 動詞は判別できません。

LOG_FULL_DETAILS、LOG_FULL_DETAILS_PER_SESSION、LOG_FULL_DETAILS_VALUES、LOG_FULL_DETAILS_VALUES_PER_SESSION、LOG_MASKED_DETAILS の各アクションは、フラット・ポリシーのルールでは機能しません。

選択的な監査証跡の使用

「ポリシー・ビルダー」の「ポリシー定義」セクションにある「選択的な監査証跡」オプションを使用して、Guardium アプライアンスにおけるロギングの量を制限します。

これは、検査エンジンで受信されているトラフィックのうち重要なトラフィックの割合が比較的小さい場合や、レポート対象となり得るすべてのトラフィックが完全に識別可能である場合に適しています。

選択的な監査証跡ポリシーを指定しない場合、Guardium アプライアンスは検査エンジンで受信したすべてのトラフィックをログに記録します。 アプライアンスまたは S-TAP の検査エンジンは、それぞれ 1 つ以上のポートで特定のデータベース・プロトコル (例えば、Oracle など) をモニターするように構成されています。さらに、クライアント/サーバー接続のサブセットからトラフィックを受信するように検査エンジンを構成することができます。この場合、選択的な監査証跡ポリシーよりも多くの情報が取り込まれる傾向にあります。ただし、ユーザーのセキュリティー要件および規制要件を満たすために必要とされるもの以外にも大幅に多くの情報が Guardium アプライアンスにより処理および保管される可能性があります。

選択的な監査証跡ポリシーをインストールすると、ポリシーが要求したトラフィックのみがログに記録されます。そのトラフィックは、次の 2 とおりの方法で識別できます。

- 重要なトラフィックを識別するために使用可能な文字列を、「ポリシー定義」パネルの「監査パターン」ボックスに指定する方法。これにより、例えば、データベースやデータベース表のグループを識別できます。監査パターンは、ロガーが (正規表現のマッチングを通じて) 一致するかどうかを確認するために処理する各 SQL に適用されるパターンである点に注意してください。このパターン・マッチングは、厳密には文字列マッチングです。ポリシー・ルールの場合のような、セッション変数 (例えば、データベース名など) とのマッチングは行われません。
- あるいは、「ルール定義」パネルの 1 つ以上のポリシー・ルールに、「監査のみ」またはロギング・アクションのいずれか (「ロギングのみ」、「全詳細をロギング」など) を指定する方法。ポリシー・ルールを使用すると、考えられるすべての属性のタイプ (データベース・タイプ、データベース名、ユーザー名など) に対してマッチングする、正確な値、グループ、またはパターンを、高精度で指定することができます。

Guardium セキュリティー・ポリシーで「選択的な監査証跡」を有効にした状態で、オブジェクト・グループについてルールが作成された場合、そのグループ内の各エレメントの文字列が検査されます。一致が検出されると、情報をログに記録するかどうかの決定が下され、処理が続行されます。Guardium セキュリティー・ポリシーで「選択的な監査証跡」を有効にした状態で、「NOT」指定を使用してオブジェクト・グループについてルールが作成された場合、やはりグループ内の各エレメントの文字列を検査する必要があり、いずれのエレメントも一致しない場合にのみ、ログに記録して続行することが決定されます。NOT が指定されたルールは、「選択的な監査証跡」とともに使用すると、通常のルールと同様に振る舞います。

以下のような内容です。

- 複数のオブジェクトまたはコマンドに基づくルールのような、OR 状態。
- 2 つの NOT 条件を持つ (例えば、NOT オブジェクト・グループの一部、および NOT コマンド・グループの一部) 状態。および
- 1 つの NOT 条件および 1 つの YES 条件 (例えば、NOT オブジェクト・グループの一部、および YES コマンド・グループの一部) を持つ状態。

注: (少なくとも選択的な監査モードでは) SELECT /*+ ORDERED USE_MERGE(m) */ SELECT /*+ ORDERED */ SELECT /*+ all_rows */ などの照会ヒントを使用した SELECT ステートメントは、それらのステートメントをスキップするためのルール定義にかかわらず、パーサーをパススルーしてログに記録することができます。これは、選択的な監査ポリシーでは、他の機能 (アプリケーション・ユーザー・トランスレーションなど) に必要になる可能性がある特定の SQL のロギングを防いではならないためです。

選択的な監査証跡およびアプリケーション・イベント API

「選択的な監査証跡」ポリシーを使用する場合で、アプリケーション・ユーザーまたはイベントがアプリケーション・イベント API を使用して設定されているときは、アプリケーション・イベントの設定/クリア、またはアプリケーション・ユーザー・コマンドの設定/クリアが検出されるごとに起動される「監査のみ」ルールをポリシーに含める必要があります。 アプリケーション・イベント API を使用したアプリケーション・ユーザーの設定について詳しくは、API によるユーザーの識別を参照してください。

選択的な監査証跡およびアプリケーション・ユーザー・トランスレーション

「選択的な監査証跡」ポリシーを使用する場合、「アプリケーション・ユーザー・トランスレーション」も使用されます。

- ポリシーは、アプリケーション・ユーザー・トランスレーション・ルールに合致しない (例えば、 アプリケーション・サーバーが発信元ではない) すべてのトラフィックを無視します。
- そのポリシーのパターンに合致する SQL だけが、 特殊アプリケーション・ユーザー・トランスレーション・レポートで有効になります。

選択的な監査証跡および空のグループの指定

ルールに付加された空のタプルにより、ルール・アクションが一致しなくなります。

親トピック: ポリシー

ポリシーの作成

ポリシーを作成するだけでなく、ポリシーの変更、複製、削除を行うことができます。

ポリシーの作成

このセクションを使用してポリシーを作成します。各ステップは、「ポリシー・ビルダー」画面のメニュー・フィールドで実行します。

以下の手順を行います。

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開きます。
2. 保護メカニズムを侵害する試みを示すデータベース・イベントに対して、(ポリシーのコピー作成に使用可能な) 一連の事前定義ポリシーが、アクセス権、例外、および抽出のルールとともに作成されています。ロギング・アクションやアラートを生成するこのようなイベントには、特定のグループまたはサーバーからのログイン失敗や SQL エラー、特定のユーザーやグループによる特定のデータベース・オブジェクトのアクセス、SQL GRANT コマンド変更の試みなどがあります。これらの事前定義ポリシーにより、コンプライアンスのポリシーの作成が迅速化されます。例えば、GDPR、Basel II、PCI などが対象です。
   重要: 事前定義ポリシーの [テンプレート] バージョンが使用可能な場合、古いバージョン ([テンプレート] とマークされていないもの) は、更新を受け取らないため、その使用はお勧めできません。代わりに、[テンプレート] バージョンのコピーを作成し、必要に応じてカスタマイズしてください。
3. 事前定義ポリシーのコピーを作成するか、「新規」をクリックして「ポリシー定義」パネルを開きます。
4. 「ポリシーの記述」ボックスに、ポリシーの固有の名前を入力します。記述にはアポストロフィ文字を含めないでください。
5. オプション。「カテゴリー」ボックスにカテゴリーを入力します。カテゴリーは、レポート目的でポリシー違反をグループ化するために使用可能な、任意のラベルです。ここで指定したカテゴリーは、各ルールのデフォルト・カテゴリーとして使用されます (これは、ルール定義でオーバーライドすることができます)。
6. オプション。「ポリシー・ベースライン」リストから、使用するベースラインを選択します。必ず生成済みのベースラインを選択してください。生成されていないベースラインを選択した場合、ポリシー・ビルダーはそのベースラインからのルールを推奨できません。使用するベースラインがリストに表示されない場合、ご使用の Guardium ユーザー ID に、そのベースラインの使用権限があるセキュリティー・ロールが割り当てられていません。詳しくは、Guardium® 管理者にお問い合わせください。

   ポリシーにベースラインが含まれる場合、そのポリシー定義には、最初はベースラインだけが含まれています。ベースラインへのアクションは、次のルールに進むことなく常に許可されます。

   既存のポリシーにベースラインを追加すると、そのベースラインは最初のルールとして追加されます。ベースライン・ルールは、ポリシーの任意のロケーションに移動できます。(ベースラインを最後のルールとして移動すると、効果がなくなる点に注意してください。)

   重要: 「ベースライン・ビルダー」と関連機能は、Guardium V10.1.4 から非推奨になりました。
7. オプションで「未解析ログ」にマークを付けて、Guardium がデータをログに記録するが、内部データベースでのデータの分析および統合はしないことを指定します。
8. 「未解析ログ」が選択されている場合、「未解析ログに関するルール」にマークを付けて、未解析ログ・データ用のポリシー・ルールを (統合データ用と異なり) 適用することもできます。
9. オプションで「選択的な監査証跡」にマークを付けて、このポリシーのインストール時にログに記録する内容を制限します。
   - マークを付けると、このポリシーが要求したトラフィックのみがログに記録されます。これは、検査エンジンが確認しているトラフィックのうち、重要なトラフィックの割合が比較的小さい場合に適しています。マークを付ける場合、ログに記録するトラフィックをシグナル通知する方法は、重要なトラフィックを識別するために使用可能な文字列を「監査パターン」ボックスに指定する方法と、1 つ以上のポリシー・ルールに「監査のみ」またはロギング・アクションのいずれかを指定する方法 (ルール・アクションについては以降で説明します) の 2 とおりあります。
   - マークを付けない場合 (デフォルトの状態)、Guardium アプライアンスは、検査エンジンが確認しているすべてのトラフィックをログに記録します。これは、総合的な監査証跡機能を提供しますが、必要とするよりはるかに多くの情報を取り込んで分析する結果につながります。
   - 詳しくは、『選択的な監査証跡の使用』を参照してください。
10. 「保存」をクリックして、ポリシー定義を保存します。
11. オプションで「ロール」をクリックして、ポリシーのロールを割り当てます。
12. オプションで「コメント」をクリックして、定義にコメントを追加します。

次に何を行うか

新規ポリシー定義の作成後、「ポリシー・ファインダー」パネルを使用してその定義にアクセスします。以下のタスクを 1 つ以上実行し、ポリシー定義を完了します。

- 手動でポリシー・ルールを作成します。『ルールの追加または編集』を参照してください。
- ポリシーにベースラインが含まれる場合、ポリシー・ビルダーにそのベースラインからルールを推奨させます。オプションで、生成されたルールを必要に応じて受け入れることも、調整することもできます。『ベースラインから推奨されるルールの使用』を参照してください。
- ポリシー・ビルダーに、そのデータベースに関して定義されたデータベース・アクセス制御 (ACL) からルールを推奨させます。各ルールは、必要に応じて、拒否することも、受け入れることも、オプションで調整することもできます。『データベース ACL から推奨されるルールの使用』を参照してください。

ポリシーの変更/コピー/削除

このセクションを使用して、ポリシーの変更、コピー作成、または削除のステップを確認します。

ポリシーの変更

ポリシー定義を変更する前に、使用中のポリシーを変更することの影響について、必ず十分に理解しておいてください。既存のポリシーを、すべての改訂が完了する前に再インストールする必要がある場合、ポリシーがインストールされなかったり、インストールされても必要な結果が得られなかったりすることがあります。このため、ポリシーのコピーを作成し、オリジナルを常にインストール可能にしておくことが推奨されます。

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開きます。
2. 「ポリシーの記述」リストから、変更するポリシーを選択します。
3. 以下のいずれかを実行します。
   - 全体的なポリシー設定 (「カテゴリー」、「未解析ログ」オプション、その他) を編集する場合、「変更」をクリックします。これらの設定のいずれかを変更する場合は、『ポリシーの作成』を参照してください。
   - ルールのみを編集する場合、「ルールの編集」をクリックします。ルール定義のコンポーネントの変更については、『ルールの追加または編集』を参照してください。

ポリシーのコピー作成

オリジナルの定義に変更を加えずに、既存のポリシーに基づいて新規ポリシーを定義するシチュエーションが多々あります。

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開きます。
2. 「ポリシーの記述」リストから、コピーするポリシーを選択します。
3. 「コピー」 をクリックして、「ポリシーのコピー作成」パネルを開きます。
4. 「新規名」ボックスに、新規ポリシーの固有の名前を入力します。名前にはアポストロフィ文字を含めないでください。
5. コピー中のベースラインに関して生成されたベースライン構成体 (基本的にコマンド) のコピーを作成するには、「構成体のコピー作成」チェック・ボックスにマークを付けます。
6. 「保存」をクリックして、新規ポリシーを保存します。これで、ポリシー・ファインダーを使用して新規ポリシーを開き、編集できるようになります。『ポリシーの変更』を参照してください。

ポリシーの削除

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開きます。
2. 「ポリシーの記述」リストから、コピーするポリシーを選択します。
3. 「削除」ボタンをクリックします。アクションの確認を求めるプロンプトが出されます。

ルールの追加または編集

このセクションを使用して、ポリシー内のルールの追加または編集を行います。

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開きます。
2. 「ポリシーの記述」リストから、編集するポリシーを選択します。
3. 「ルールの編集」ボタンをクリックして、「ポリシー・ルール」パネルを開きます。
4. 以下のいずれかを実行します。
   - ルールを編集するには、「このルールの個別編集」ボタンをクリックします。
   - 新規ルールを追加するには、以下のいずれかのボタンをクリックします。

     アクセス・ルールの追加

     例外ルールの追加

     抽出ルールの追加 (管理者ユーザーが検査エンジン構成を戻りデータを検査するように設定している場合にのみ使用可能になります。)

     抽出のマッチングにより、ユーザーは、Guardium によるロギングおよびレポートの際に、まとめてグループ化する一致したレコードの数を定義することができます。抽出ルールには、「全詳細をロギング」アクションと、guardium://(some text)?split=(number) を含むルール名が必要です (ここで、(some text) は任意のテキストか CREDIT CARD のような事前定義されたワードの 1 つ、(number) は Guardium ログ・レコードごとの戻りデータ・レコードの数になります)。

5. ルールのタイプごとにテスト可能な属性は異なりますが、各ルール定義は、ルール・タイプを問わず、以下の 4 つの項目で開始されます。
   - ルールの記述 - ルールの簡潔な記述名を入力します。特殊パターン・テストを使用するには、特殊パターン・テスト名に続けて 1 つのスペースおよびルール名を固有にするための 1 つ以上の追加の文字を入力します (例: `guardium://SSEC_NUMBER employee`)。
   - カテゴリー - カテゴリーは違反とともにログに記録され、グループ化およびレポート目的で使用されます。何も入力しないと、ポリシーのデフォルトが使用されます。
   - 分類 - オプションで、「分類」ボックスに分類を入力します。カテゴリー同様、これらは例外とともにログに記録され、グループ化およびレポート目的で使用できます。
   - 重大度 - 重大度コード (「情報」、「低」、「中」、または「高」) を選択します (デフォルトは「情報」です)。
6. 「ルール定義」パネルの残りのフィールドを使用して、ルールのマッチング方法を指定します。それらのフィールドのほとんどが、アクセス、例外、抽出ルールで選択可能です。一部のフィールドは、その他の各種オプションを選択することで選択可能になります。『ルール定義の解説』で、「ルール定義」パネルで選択可能な全フィールドについて英字順に解説しています。また、グループ値や個々の値の組み合わせの使用手順については、『ルールでの値および/またはグループ値の指定』を参照してください。
7. 各タイプのルールについて、トラフィック内の文字列とマッチングする 1 つ以上の正規表現を「パターン」ボックスに入力できます。正規表現を手動で入力するか、  アイコンをクリックして正規表現の作成ツールを開きます。このツールでは、正規表現を入力してテストすることができます。
8. 例外ルールの場合のみ、「例外タイプ」ボックスから、ルールが識別する単一の例外タイプを選択します。ルール・カウントは、選択した例外タイプが発生したときにのみ増分されます。
9. ルール・アクションを選択すると、以下の 2 つのフィールドが選択可能になります。
   - 最小数 - ルール・アクションが起動されるまでにルールが一致する必要のある最小回数を入力します。ルールが満たされる必要のある回数は、アクションが起動されるごとに、またはリセット間隔が満了になるとリセットされます。デフォルトのゼロは 1 と同じであり、ルールが一致するごとにアクションが起動されることを意味します。
   - リセット間隔 (分) - 最小数がゼロより大きい場合にのみ使用されます (その場合は必須です)。ここに入力した分数の経過後に、ルール・カウンターがゼロにリセットされます。カウンターはまた、ルール・アクションが起動するごとにゼロにリセットされます。
10. 「次のルールに進む」ボックスにチェックマークを付けます。これにより、このルールが成立してルールのアクションが起動されると、同じ要求、同じ例外、または同じ結果のテストが次のルールに進みます。これは、1 つの要求または例外に基づいて、複数のルールが成立し、複数のアクションが実行される可能性があることを意味します。 マークを付けないと (デフォルト)、このルールが成立すると、追加のルールはテストされません。マークを付けると、ルールのテストは (そのルールが満たされているかどうかを問わず) 次のルールに進みます。
11. 「値の記録」ボックスにマークを付けると、ルールが満たされる原因となった実際の構成体が SQL 文字列属性に記録され、レポートで使用可能になります。マークを付けないと、SQL ステートメントは記録されません。
12. メッセージ・テンプレートを使用してアラートが生成されます。「グローバル・プロファイル」から、複数の名前付きメッセージ・テンプレートが作成され、変更を加えられます。
13. ルールが成立する場合に実行するアクションを選択します。
14. アラート・アクションを指定した場合は、「通知」ペインが開き、少なくとも 1 つの通知タイプを定義する必要があります。通知の追加方法に関する説明については、『通知』を参照してください。
15. 「保存」をクリックしてルールを保存します。すると、「ルール定義」パネルが閉じられ「ポリシー・ルール」パネルに戻ります。

ルールをフィルターに掛けサブセットのみを表示

ポリシーに多数のルールが含まれる場合、共通属性を持つルールのサブセットを表示できると便利な場合があります。

そのために、「ルール定義」パネルの「フィルター」ボックスを使用できます。フィルターを定義する処理は、ルールを定義する処理に似ています。

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開きます。
2. 「ポリシーの記述」リストから、表示または変更するポリシーを選択します。
3. 「ルールの編集」をクリックします。
4. 「フィルター」ボックスで、以下のいずれかを実行します。
   - 「フィルター」リストからフィルターを選択します。
   - 「編集」 をクリックして、フィルター定義を変更します。
   - 「新規」 をクリックして、新規フィルターを定義します。

   フィルターに掛けられたルール・セットが表示されると、表示されるルールについて、このセクションで説明されているすべてのアクションを実行可能です。

ルールのコピー

この手順を実行して、選択したルールをあるポリシーから別のポリシーにコピーしたり、同じポリシーの別のロケーションにコピーしたりすることができます。

コピーされるすべてのルールは、単一のロケーション (例えば、ルール 3 の後ろなど) にコピーされます。コピー先ポリシー内の別のロケーションにルールをコピーするには、複数のコピー操作を実行するか、一度の操作ですべてのルールをコピーしてからコピー先ポリシーを編集し、必要に応じてルールを移動します。

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開きます。
2. 「ポリシーの記述」リストから、1 つ以上のルールのコピー元となるポリシーを選択します。
3. 「ルールの編集」をクリックします。
4. コピーする各ルールのチェック・ボックスにマークを付けます。
5. 「ルールのコピー」をクリックします。
6. 「選択したルールを次のポリシーにコピー」リストから、コピーしたルールのコピー先ポリシーを選択します。
7. 「次のルールの後に挿入」リストで、コピーしたルールがその後ろに挿入されるルールを選択するか、「先頭」を選択してコピーしたルールをリストの先頭に挿入します。
8. 「コピー」をクリックします。操作の成功が通知されます。
9. ここで、ルールのコピー先ポリシーを編集し、正しいルールを正しいロケーションにコピーしたことを検証する必要があります。

ベースラインから推奨されるルールの使用

「ポリシー・ビルダー」を使用して、ポリシーに含まれているベースラインからルールを推奨させます。

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開きます。
2. 「ポリシーの記述」リストから、処理するポリシーを選択します。(そのポリシーには、ベースラインが含まれていなければなりません。)
3. 「ルールの編集」ボタンをクリックします。
4. 「ルール最小数」の値を設定します。これは、システムがルールを推奨するために検索しなければならない同種コマンドの最小数です。デフォルトはゼロです。入力する数値が小さいほど、システムが生成する推奨ルールの数が多くなります。(推奨ルールのパネルに表示されるカウントが、この値を反映しない点にご注意ください。)
5. システムが推奨オブジェクト・グループを生成するために検索しなければならないオブジェクト・グループのインスタンスの数を決定するため、「オブジェクト・グループ最小数」の値を設定します。デフォルトは 1 です。ここに入力する数値が小さいほど、推奨オブジェクト・グループの数が多くなります。
6. 「ルールの推奨」ボタンをクリックします。「推奨ルール」パネルに、推奨ルールが別ウィンドウで表示されます。
7. 推奨ルールは、ベースライン期間における発生回数別に降順でソートされます (発生回数は推奨ルールごとにリストされます)。推奨ルールを 1 つ以上選択して「保存」をクリックすると、それらのルールは同じ順序で「ポリシー・ルール」パネルのベースライン・ルールのすぐ前に挿入されます。そうすると、「ポリシー・ルール」パネルから推奨ルールの順序を変更したり、必要に応じてそれらを編集したりすることができます。
8. ルールを展開表示し、推奨オブジェクト・グループのメンバーシップを確認します。「推奨ルール」パネルの「オブジェクト」列に、作成された推奨オブジェクト・グループがある場合、それらは「Suggested Object Group」という名前で始まり、ハイパーテキスト・リンクとして表示されます。推奨オブジェクト・グループを表示、受け入れ、または拒否する方法について詳しくは、『推奨オブジェクト・グループの使用』を参照してください。
9. ポリシーに含める各推奨ルールの「選択」ボックスにマークを付けます。
10. 「保存」 をクリックして、選択したルールを受け入れます。
11. これで、推奨ルールを手動で追加したルールと同じように編集したり変更したりできるようになります。

推奨オブジェクト・グループの使用

ポリシー・ビルダーは、ポリシーに含まれるベースラインと、サーバーに定義されたデータベース・セキュリティー・ポリシー (DBMS に対して内部) の両方からルールを推奨できます。

いずれの場合も、データベース・オブジェクト (表、プロシージャー、またはビュー) を推奨オブジェクト・グループにグループ化することによる、最小ルール・セットの生成が試みられます。推奨オブジェクト・グループは受け入れることも拒否することもできます。

推奨オブジェクト・グループを受け入れる前に、生成された「グループの記述」フィールド (例えば、Suggested Object Group603-25 11:54) を編集してより意味のある名前を指定できます。推奨オブジェクト・グループを受け入れた後で、そのメンバーシップを表示できます。推奨ルール内でそのグループの使用を拒否することはできますが、そのグループのメンバーシップを編集することはできません。

推奨オブジェクト・グループを拒否すると、そのグループの推奨ルールは、拒否されたグループの各メンバーの個別の推奨ルールで置き換えられます。これらの各推奨ルールは、個別に受け入れることも、拒否することもできます。推奨ルールを受け入れた後で、そのルールを編集できます。

推奨オブジェクト・グループの表示

推奨オブジェクト・グループは、「推奨ルール」パネルの「オブジェクト」列に、「Suggested Object Group」というワードで始まるハイパーテキスト・リンクとして表示されます。

推奨オブジェクト・グループのメンバーシップを表示するには、そのグループのハイパーテキスト・リンクをクリックします。グループ・メンバーシップは、グループがまだ受け入れられていない場合は「グループの編集」パネルに表示されます。グループか既に受け入れられている場合は「グループの表示」パネルに表示されます。

推奨オブジェクト・グループの受け入れ

推奨オブジェクト・グループを受け入れる手順は、次のとおりです。

1. 「グループの編集」パネルの「グループの記述」フィールドに、意味のある名前を入力します。(必須ではありませんが、強く推奨されます。)名前にはアポストロフィ文字を含めないでください。これがこのグループに命名する唯一の機会になります。名前が入力されないと、既に説明したように、グループには Suggested Object Group で始まり、1 つの数字が続く名前が付けられます。
2. 「保存」をクリックして推奨ルールの編集済みグループを受け入れるか、「すべてのルールで保存」をクリックして編集済みグループをそのグループが表示されるすべての推奨ルールで受け入れます。新しいオブジェクト名がルール内の古いオブジェクト名を置き換えます。

推奨オブジェクト・グループの拒否

推奨オブジェクト・グループを拒否すると、そのグループの使用は、1 つ以上の推奨ルールで置き換えられます。推奨オブジェクト・グループを拒否するには、以下のいずれかを実行します。

- この推奨ルールについてのみグループを拒否する場合: 「拒否」ボタンをクリックします。
- すべての推奨ルールについてグループを拒否する場合: 「すべてのルールで拒否」ボタンをクリックします。

注: 1 つのルールでその推奨オブジェクト・グループを受け入れる場合、別のルールからその同じ推奨オブジェクト・グループを再度開いて、「すべてのルールで拒否」ボタンをクリックします。そのグループは、明示的に受け入れ済みであるルールでは保持されますが、それ以外のそのグループが使用されたルールでは拒否されます。

データベース ACL から推奨されるルールの使用

指定されたデータベース・サーバーでは、ポリシー・ビルダーが、DBMS によって内部的に定義されたセキュリティー・ポリシーを使用して、アクセス・ルールを推奨できます。

ポリシー・ビルダーは、DBMS 内のユーザー・グループおよびデータベース・オブジェクト (表、プロシージャー、およびビュー) に対して認可されたアクセス権を調べることによってこれを行い、データベース・オブジェクトを推奨オブジェクト・グループにグループ化して、推奨ルールの総数を最小化します。推奨オブジェクト・グループは、受け入れることも拒否することもできます (『推奨オブジェクト・グループの使用』を参照してください)。同様に、推奨ルールも受け入れることも拒否することもできます。

ポリシー・ビルダーに、データベース ACL からルールを推奨させる手順は、次のとおりです。

注: データベース ACL からルールを推奨する場合、システムは「ルール最小数」や「オブジェクト・グループ最小数」フィールドを使用しません。これらのフィールドは、ベースラインからルールを推奨する場合にのみ使用します。

1. 「DB に基づいた推奨」をクリックして、「データベース定義」パネルを別のブラウザー・ウィンドウで開きます。
2. 「データ・ソースの追加」をクリックして、DB ACL へのアクセス元となるデータベースを選択します。
   注: DB ACL にアクセスするために Oracle、DB2®、または DB2 for z/OS® データ・ソースを追加する場合、「データベース定義」ポップアップ・ウィンドウ内の「照会パラメーター」セクションは無効になります。
3. 「推奨ルール」をクリックして、ルールを生成します。「推奨ルール」パネルが (上記の『ベースラインから推奨されるルール』で説明したように) 別ウィンドウで開きます。推奨ルールを 1 つ以上選択して「保存」をクリックすると、それらのルールは同じ順序で「ポリシー・ルール」パネルのルール・リストの、ベースライン・ルールのすぐ前に挿入されます。ベースライン・ルールがない場合は、リストの先頭に挿入されます。「ポリシー・ルール」パネルに挿入した推奨ルールは、必要に応じて順序を変更したり、編集したりすることができます。
4. 推奨オブジェクト・グループのメンバーシップを確認します。「オブジェクト」列の、作成された推奨グループは、「Suggested Object Group」という名前で始まり、ハイパーテキスト・リンク (下線付きの青字) で表示されます。推奨オブジェクト・グループを表示、編集、受け入れ、または拒否する方法について詳しくは、『推奨オブジェクト・グループの使用』を参照してください。
5. ポリシーに含める各推奨ルールの「選択」ボックスにマークを付けます。「保存」 をクリックして、選択したルールを受け入れます。

ポリシー・シミュレーターの使用

ポリシー・シミュレーターを使用して、ポリシーをインストールせずにアクセス・ルールをテストします。

例外ルールや抽出ルールはテストしません。シミュレーターはログに記録されたネットワーク・トラフィックをリプレイし、ポリシーにすべてのアクセス・ルールを適用します。すると、アラートやロギングのみアクションを起動した SQL をリストした特殊レポートが、別ウィンドウで開きます。このレポートには、「タイム・スタンプ」、「カテゴリー名」、「アクセス・ルールの記述」、「クライアント IP」、「サーバー IP」、「データベース・ユーザー名」、「SQL 文字列全体」、「重大度の記述」、および「ポリシー・ルール違反の数」という列があります。CLI コマンド「store allow_simulation」を使用して、GUI で「ポリシー・シミュレーション」ボタンをアクティブにします。

ポリシー・シミュレーターを使用してテストできるのは、以下のタイプのアクセス・ルール・アクションのみです。

- ロギングのみ
- 任意のアラート・アクション: 毎日アラート、セッションごとに 1 回アラート、一致ごとにアラート、時間間隔ごとにアラート

ポリシー・シミュレーターは、ポリシーに「ロギングのみ」以外のロギング・アクションが含まれている場合は結果を生成しません。そのようなポリシーにシミュレーターを使用するには、一時的にすべてのロギング・アクションを「ロギングのみ」に変更してください。

ポリシー・シミュレーターの使用手順は、以下のとおりです。

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開きます。
2. 「ポリシーの記述」リストから、処理するポリシーを選択します。
3. 「ルールの編集」をクリックします。
4. 「ポリシー・シミュレーター」ボタンをクリックして、「ポリシー・シミュレーター」パネルを開きます。
5. 「開始」と「終了」をいずれも指定して、シミュレーションに使用する期間を定義します。

注: Guardium 管理者が定義した Guardium アプライアンスのスケジュールから、履歴データをアーカイブすることも、パージすることもできます。指定した期間のデータが使用可能であること (およびパージされていないこと) を確認してください。

6. 「テスト」をクリックします。テストが開始して実行している間、「ポリシー・シミュレーター」パネルにメッセージ「* は実行中です」が表示されます。テストが完了すると、ログに記録されたすべてのルールの一致をリストした特殊レポートが別ウィンドウで開きます。「アラート」または「ロギングのみ」ルールが起動されなかった場合、「使用可能なドリルダウン・レポートはありません」というメッセージを受信します。その場合、テスト期間に十分なデータが含まれていない可能性があります。

親トピック: ポリシー
関連情報:
ポリシーの作成とインストール (ビデオ)
Guardium のグループとポリシー (ビデオ)

ポリシーのインストール

このトピックを使用して、Guardium コレクターにポリシーをインストールし、スケジュールを変更します。

複数ポリシーのサポート

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・インストール」をクリックして「ポリシー・インストーラー」を開きます。
2. 「ポリシーの記述」ボックスからインストールするポリシーを選択します。
3. 以下のいずれかを実行します。
   - 「インストール」をクリックすると、ポリシーが直ちにインストールされます。
   - 「スケジュールの変更」をクリックすると汎用スケジューリング・ユーティリティーが開くので、ポリシーのインストールをスケジュールに入れます。

インストールしたポリシーのポリシー・ルールを表示

複数のインストール済みポリシーを同時に使用できます。 インストールされたポリシーはすべて、操作に使用できます。ここで 2 つの制限があります。つまり、選択的な監査ポリシーとして定義されたポリシーは、選択的な監査ポリシーとして定義されていないポリシーと混用できません。さらに、未解析ログとして定義されたポリシーは未解析ログとして定義されていないポリシーと混用できません。 ポリシーを混用しようとすると、これらの混合ポリシーのインストール時にエラー・メッセージが発生します。

表示される順番は、最初、最後、または中間のどこか、というように、ポリシーのインストール中に制御できます。 しかし表示順は後日編集することができません。

さらに、以前にインストールしたポリシーを削除するための「ポリシーのアンインストール」というボタンもあります。

最初にインストールしたポリシーには特別な意味があります。このポリシーはグローバルなポリシー・パラメーターの値を設定します。 これらのパラメーターには、グローバルなパターン、選択的な監査かどうか、クライアントおよびサーバーのネットマスク、タグ付きクライアントおよびタグ付きサーバーのグループ ID があります。

この複数ポリシーのサポートは GUI (「設定」 > 「ツールとビュー」 > 「ポリシー・インストール」) および GuardAPI から使用できます。

インストールしたポリシーのポリシー・ルールを表示

「現在インストール済みのポリシー」パネルから、すべてのユーザーはインストール済みポリシーのルールを表示でき、さらに、許可されたユーザーはポリシーを開いて編集できます。

1. 「設定」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開くか、「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・インストール」をクリックして「ポリシー・インストーラー」を開きます。
2. 「インストール済みポリシー」のリンクをクリックして、ポリシー・ルールを表示します。許可されたユーザーには追加のボタンが有効になります。ポリシー・ビルダーでポリシーを開いて編集するには、「インストール済みポリシーの編集」ボタンをクリックします。

ジョブ依存関係スケジューラー

Guardium コレクターには、「ポリシー・インストール」、「監査プロセス」、「グループ更新 (Group updates)」など、定期的に実行されるようスケジュールする多数のタスクがあります。「ジョブ依存関係」機能では、直接関係があり、スケジュールするタスクが正常に実行されるかどうかに影響するすべてのジョブが検出されます。スケジュールするジョブの前提条件として定義されているジョブを検出しないと、タスクが不適切なデータに基づく可能性があり、これにより誤った結果または不適切な結果が発生します。

主要機能

- ユーザーは、実行時に依存関係を検出および実行するために、スケジュール済みのジョブにマークを付けます。
- スケジューラーによりジョブが実行されると、すべての従属ジョブが自動的に検出され、順番に実行されます。
- 失敗した場合の再試行手順があります。

依存関係の検出

- 依存関係が必要なシナリオを識別します。
- 実行可能なジョブと実行不可のジョブを識別します。
- 事前定義のジョブ依存関係を計算します。

ジョブ	推奨される前提条件ジョブ	理由
ポリシー・インストール	(インストールする) ポリシーで定義されていて、「照会から取り込み」メカニズムでデータを取り込むようにスケジュールされている、またはスケジュールされていないグループ。	グループを使用するポリシー・ルールには、インストール前に、最新のグループ・データを取り込む必要があります。

ポリシー・インストール	分類タスクに「オブジェクトのグループに追加」アクション、「オブジェクト/フィールドのグループに追加」アクション、または「アクセス・ルールに追加」アクションのある、分類監査タスクを含む監査プロセス。	グループを使用するポリシー・ルールには、インストールの前に、最新のグループ・データを含める必要があります。
監査プロセス	カスタム表名がレポート・タイプの監査タスクで (「from」節により) 参照されるカスタム表アップロード・ジョブ。	監査プロセスの実行をスケジュールする前に、レポート・タイプの監査タスクで参照されるカスタム表に最新のデータを取り込む必要があります。
監査プロセス	レポート・タイプの監査タスクの条件で定義されていて、「照会から取り込み」メカニズムでデータを取り込むようにスケジュールされている、またはスケジュールされていないグループ。	レポート・タイプの監査タスクを実行する前に、照会条件で参照されるグループに最新のデータを取り込む必要があります。
照会から取り込み	グループにデータを取り込むために使用される照会のエンティティーを含むカスタム・アップロード表。	
監査プロセス	インポート	アグリゲーターのみに関連します。この前提条件により、監査プロセスの実行前に、すべての統合ユニットから情報が確実にインポートされます。

スケジューラーの機能拡張

- スケジュール済みジョブの実行時にジョブの依存関係を検出します。
- ジョブの依存関係を順番に実行します。

実行可能ジョブはスケジュールでき、実行不可のジョブはスケジュールできません。

グループは実行不可のジョブです。

グループに対する「照会から取り込み」は実行可能です。

直接依存関係は、定義により結び付けられたオブジェクトです。例えば、ポリシーはルールに依存し、ルールはグループに依存します。

間接依存関係は、論理的に結び付けられたオブジェクトです。例えば、ポリシーをインストールする前に監査プロセスを実行します。

GUI サポート

1. 「ポリシー・インストール」から「スケジュールの作成」を選択した後、「従属ジョブの自動実行」チェック・ボックスにチェック・マークを付けます。
2. 「保存」をクリックしてプロセスをスケジュールします。これにより、ユーザーに依存関係の状況が通知されます。

GuardAPI サポート

GuardAPI ジョブ従属関係コマンド:

CLI> grdapi add_job_dependency

関数パラメーター:

dependOnJobExecutedWithin - 文字列

dependOnTrigger - 文字列 - 必須

intervalBetweenRetries - 整数

jobRetries - 整数

jobTrigger - 文字列 - 必須

runIfDependOnJobReturns - 文字列

api_target_host - 文字列

依存関係を自動実行するには、次の GuardAPI コマンドを使用します。

> grdapi auto_execute_suggested_dependencies jobTrigger=*<trigger name of the scheduled job>*

CLI> grdapi auto_execute_suggested_dependencies

関数パラメーター:

jobTrigger - 文字列 - 必須

api_target_host - 文字列

CLI> grdapi delete_job_dependencies

関数パラメーター:

dependOnTrigger - 文字列

jobTrigger - 文字列 - 必須

api_target_host - 文字列

CLI> grdapi disable_auto_execute_suggested_dependencies

関数パラメーター:

jobTrigger - 文字列 - 必須

api_target_host - 文字列

CLI> grdapi list_job_dependencies_tree

関数パラメーター:

jobTrigger - 文字列 - 必須

api_target_host - 文字列

すべてのスケジュール済みジョブ/トリガーのリストを取得するには、次の GuardAPI コマンドを実行します。

> grdapi list_scheduler_jobs

CLI> grdapi list_suggested_job_dependencies

関数パラメーター:

jobTrigger - 文字列 - 必須

api_target_host - 文字列

CLI> grdapi list_existing_job_dependencies

関数パラメーター:

jobTrigger - 文字列 - 必須

api_target_host - 文字列

CLI> grdapi modify_job_dependency

関数パラメーター:

dependOnJobExecutedWithin - 文字列

dependOnTrigger - 文字列 - 必須

intervalBetweenRetries - 整数

jobRetries - 整数

jobTrigger - 文字列 - 必須

runIfDependOnJobReturns - 文字列

api_target_host - 文字列

CLI> grdapi show_job_dependency_execution_profile

関数パラメーター:

dependOnTrigger - 文字列 - 必須

jobTrigger - 文字列 - 必須

api_target_host - 文字列

スケジューラーの実行

スケジューラーは、ジョブの実行時に、ジョブの依存関係をチェックします。

依存関係は逆順に実行されます。

例: 次のような依存関係ツリーがあるとします。

ポリシーのインストール (実行可能)						
	監査プロセス (実行可能/間接依存関係)					
		監査タスク				
			分類プロセス			
				分類ポリシー		
					分類ポリシー・アクション	
						グループ (実行可能/直接 - 照会から取

						り込み)

実行順は以下のようになります: 照会から取り込み → 監査プロセス → ポリシーのインストール

スケジューラーは依存関係を 1 つずつ実行し、それらが終了するのを待機します。

依存関係ツリーの実行がすべて完了するまで長時間かかる場合がありますが、依存関係はすべて正しい順番で確実に実行されます。

エラーの処理

いずれかの依存関係の実行が失敗した場合、スケジューラーにより現在実行されているジョブが実行されなくなります。

障害が発生した場合、エラー・メッセージが「スケジュール済みジョブ例外」レポートに書き込まれます。

前のジョブに依存するジョブの再試行回数を設定できます。デフォルトは 3 です。有効な値は ≥ 0 です。再試行間の間隔は分単位で設定できます。 デフォルトは 3 です。有効な値は ≥ 0 です。

親トピック: ポリシー

ルール定義フィールド

ポリシー・ルールを定義する際に、以下のフィールドを使用することができます。

表 1. ルール定義フィールドの参照表

フィールド	記述
アクション	ルールが真の場合に実行されるアクションを示します。すべてのルール・アクションの総合的な説明については、『ルール・アクションの概要』を参照してください。
アプリケーション・イベントの存在	アプリケーション・イベントのみをマッチングします。『アプリケーション・イベントの注』を参照してください。
アプリケーション・イベントの値	指定されたアプリケーション・イベントの「テキスト」、「数値」または「日付」の値がマッチングされます。 オプションで、イベント文字列として「グループ」を選択することもできます。『アプリケーション・イベントの注』を参照してください。
(アプリケーション) イベント・タイプ	指定されたアプリケーション・イベントをマッチングします。『アプリケーション・イベントの注』を参照してください。
(アプリケーション) イベント・ユーザー名	指定されたアプリケーション・イベント・ユーザー名のみをマッチングします。『アプリケーション・イベントの注』を参照してください。
アプリケーション・イベントの注	アプリケーション・イベント・フィールドは、「未解析ログ」ボックスにマークが付いている場合は使用できません。
アプリケーション・ユーザー	アプリケーション・ユーザー。「ルールでの値および/またはグループ値の指定」を参照してください。
カテゴリー	レポート目的でポリシー違反をグループ化するために使用可能な、任意のラベル。デフォルト・カテゴリーは、ポリシー定義で指定できますが、このデフォルトは各ルールでオーバーライドされます。
分類	レポート目的でポリシー違反をグループ化するために使用可能な、任意のラベル。デフォルトの分類は、ポリシー定義で指定できますが、このデフォルトは各ルールでオーバーライドされます。
クライアント情報	DB2® クライアント情報: アクセス・ルールのみ。z/OS® のみ。DB_TYPE が DB2、DB2 COLLECTION Profile、VSAM COLLECTION Profile のいずれかの場合は、CLIENT INFO フィールド (および CLIENT_INFO_GROUP_ID) が表示されます。 このフィールドに入力できる情報のタイプは USER=x; WKSTN=y; APPL=z です。
クライアント IP	含める場合は「Not」ボックスをクリアし、除外する場合は「Not」ボックスにマークを付けます。 • 任意のクライアント: すべてのクライアント・フィールドをブランクのままにします。カウントは任意のクライアントがルールを満たすごとに増分されます。(「Not」ボックスにマークが付けられている場合は、すべてのフィールドをブランクのままにすることはできません。) • IP アドレスとマスクによって選択されたすべてのクライアント: 最初のボックスにクライアント IP アドレスを、2 番目のボックスにネットワーク・マスクを入力します。カウントは、指定された任意のクライアントがルールを満たすごとに増分されます。例えば、サブネット 192.168.9.x のすべてのクライアントを選択するには、最初のボックスに 192.168.9.1 を、2 番目のボックスに 255.255.255.0 を入力します。IP アドレスの選択について詳しくは、『マスクを使用した IP アドレスの選択』を参照してください。 • クライアントのグループ: クライアント IP アドレスのグループを「グループ」ドロップダウン・リストから選択するか、「グループ」ボタンをクリックして新規グループを定義し、そのグループを選択します。カウントは、選択したグループの任意のメンバーがルールを満たすごとに増分されます。 • IP アドレスとマスク、およびクライアントのグループによって選択されたすべてのクライアント: 「クライアント IP」および「グループ」フィールドの両方を使用します。カウントは、いずれかの方法を使用して指定された任意のクライアントがルールを満たすごとに増分されます。 IP アドレスでのワイルドカードの使用が可能になります。 クライアント IP グループには、ワイルドカード % をポリシー内で使用できます。

フィールド	記述
クライアント IP/ソース・プログラム/データベース・ユーザー/サーバー IP/サービス名	7 タプル・グループ - クライアント IP/ソース・アプリケーション/データベース・ユーザー/サーバー IP/サービス名/OS ユーザー/データベース アクセス、例外、および抽出の各ルールでは、5 タプルのグループ・タイプが使用可能です。 タプルでは、複数の属性を組み合わせて 1 つのグループ・メンバーを形成することができます。 タプルには、1 つのスラッシュおよび 1 つのワイルドカード文字 (%) を使用できます。ダブルスラッシュは使用できません。 クライアント IP/ソース・プログラム/DB ユーザー/サーバー IP/サービス名グループには、ワイルドカード % をポリシー内で使用できます。
クライアント MAC	ルールで 1 つのクライアント MAC アドレスを識別するには、アドレスを「nn:nn:nn:nn:nn:nn」フォーマットで入力します (ここで、各 n は 16 進数の数字 (0-F) です)。または「クライアント MAC」ボックスにドット (.) を入力して、クライアント MAC アドレスごとに個別のカウントを保持するよう示します。あるいは「クライアント MAC」ボックスを空のままにして、クライアント MAC アドレスを無視します。
コマンド	コマンド。コマンド・グループを編集できない場合は『ルールでの値および/またはグループ値の指定』を参照してください。また、「および/またはグループ」ラベルが「収集のみ」に切り替わり、選択したグループのコマンドのみが選択されることを示していることを確認してください。 「全て」ボックスにチェック・マークが付けられている場合、SQL ステートメントのすべてのフィールドがグループのメンバーでなければなりません。
次のルールに進む	マークを付けると、ルールのテストは (そのルールが満たされているかどうかを問わず) 次のルールに進みます。これは、1 つの SQL ステートメントまたは例外で、複数のルールが満たされ、(さらに複数のアクションが実行される) 可能性があることを意味します。マークを付けない場合 (デフォルト)、このルールが満たされる際に、現行のトランザクションの追加のルールはテストされません。

フィールド	記述
データ・パターン	すべてのタイプのルール (アクセス、例外、抽出) でデータ・パターンを持つことができますが、抽出ルールでは必須です。 抽出ルールの定義に使用する場合、「データ・パターン」ボックスの正規表現がマッチングされます。「正規表現」ボタンをクリックして「正規表現の作成」ツールを開き、そのツールを使用して正規表現を入力し、テストすることができます。これにより、さらに複雑なパターンのマスキングが可能になります。マスクを掛けるセクションを括弧で囲んでください。この機能は、データベースから取得したデータにマスクを掛けるときに使用します。 例えば、次のようにします。 Windows S-TAP: ([0-9][0-9][0-9][0-9[-,]?[0-9][0-9][0-9][0-9][-,]?[0-9][0-9][0-9][0-9][-,]?)[0-9][0-9][0-9][0-9] Unix S-TAP: ([0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}[-,]?)[0-9]{4}[ ]{0,20} 編集 (修正) のアクションと併用する「データ・パターン」でのみ使用できる追加の正規表現 (Regex): For Windows S-TAP Name: Pattern: Masked to: SCRUB_SSN_ANSI AAA-AA-AAAA ***-***-AAAA SCRUB_SSN_UNICODE UUU-UU-UUUU ***-***-UUUU SCRUB_CC_SPACES_ANSI AAAA AAAA AAAA AAAA **** **** **** AAAA SCRUB_CC_SPACES_UNICODE UUUU UUUU UUUU UUUU **** **** **** UUUU SCRUB_CC_SOLID_ANSI AAAAAAAAAAAAAAAA ************AAAA SCRUB_CC_SOLID_UNICODE UUUUUUUUUUUUUUUU ************UUUU SCRUB_CC_AX_SOLID_ANSI AAAAAAAAAAAAAAA ***********AAAA SCRUB_CC_AX_SOLID_UNICODE UUUUUUUUUUUUUUU ***********UUUU UNIX S-TAP Name: Pattern: Masked to: SCRUB_SSN_ANSI AAA-AA-AAAA ***-***-AAAA SCRUB_SSN_UNICODE UUU-UU-UUUU ***-***-UUUU SCRUB_CC_SPACES_ANSI AAAA AAAA AAAA AAAA A*** **** **** 1234 SCRUB_CC_SPACES_UNICODE UUUU UUUU UUUU UUUU U*** **** **** **** SCRUB_CC_SOLID_ANSI AAAAAAAAAAAAAAAA A*************** SCRUB_CC_SOLID_UNICODE UUUUUUUUUUUUUUUU U*************** SCRUB_AMEX_SOLID_ANSI AAAAAAAAAAAAAAAA A*************** SCRUB_AMEX_SOLID_UNICODE UUUUUUUUUUUUUUU U*************** 正規表現と編集機能の併用 - IBM Security Guardium ソリューションで正規表現 (Regex) を使用すると (例えば、ポリシーでマスキング機能を使用すると)、その処理がアプライアンスで実行され、正規表現の機能が拡張されます。 ただし、編集機能と一緒に使用できる正規表現ライブラリーは、データベース・サーバーのカーネルで実行され、基本的な正規表現だけに限定されています。したがって、編集機能と一緒に使用できるのは、基本的な正規表現パターンに限られます。 例えば、任意の数の数字を指定するために [0-9]* という正規表現体系を使用することはできません。一連の数字を指定するには、[0-9]-[0-9]-[0-9]... という基本的な正規表現体系を使用する必要があります。 注: S-TAP® では、事前定義の修正パターン名だけが有効であり、それ以外の名前は無視されます。 アクセス・ルール、データ・パターン、置換文字 - [a-z,2]{3}([_][0-9]{1,2}) などのデータ・パターンと置換文字 * を併用すると、データ・パターンの小括弧内の値が *** に変更されます。値にマスクを掛けるために、この機能を使用できます。 ユーザー定義文字セット Oracle、Sybase、MySQL、および MSSQL に対し使用可能、および抽出ルールに対してのみ使用可能です。ユーザーは、特別な抽出ルールを定義することで、文字セットを操作できます。これらの 文字セット ポリシー・ルールは、ユーザーがトラフィックを変換する先の文字セットを設定するためにのみ使用され、アクションの設定は関係しません。そのトラフィックに対してアクションを使用するには、その文字セットルールの後に追加ルールを定義する必要があります。次の例で定義されているように、文字セットルールの設定方法は 2 つあります (hint または force): 抽出ルールの例 (hint を使用) 通常の変換が失敗した場合に限り、インストール済みポリシーの抽出ルールで定義されている文字セットにより、トラフィックが変換されます。 文字セット EUC-JP (コード 274)。 抽出ルール・パターン: guardium://char_set?hint=274 抽出ルールの例 (force を使用) すべてのデータに対し、インストール済みポリシーの抽出ルールで定義されている文字セットにより、トラフィックが変換されます。 文字セット EUC-JP (コード 274)。 抽出ルール・パターン: guardium://char_set?force=274 このトピックの最後にある『使用可能な文字セット・コードのリスト』を参照してください。 注: 抽出ルールは、通常、遅れてセッションにアタッチされるので注意してください。したがって、短いセッションやセッションの最初の方では、文字セットの変更が直ちに反映されない場合があります。

フィールド	記述
データベース名	データベース名。「ルールでの値および/またはグループ値の指定」を参照してください。
データベース・タイプ	サポートされる DB タイプ アクセス・ルールの場合: Cassandra、CIFS、CouchDB、DB2、DB2 COLLECTION PROFILE* (z/OS で使用する場合のみ)、FTP、GreenPlumDB、Hadoop、HTTP、IBM® INFORMIX (DRDA)、IBM iSeries、IMS™、IMS COLLECTION PROFILE (z/OS で使用する場合のみ)、Informix®、MongoDB、MS SQL SERVER、MYSQL、NETEZZA、Oracle、PostgreSQL、Sybase、TERADATA、VSAM、または VSAM COLLECTION PROFILE* (z/OS で使用する場合のみ)。 例外ルールと抽出ルールの場合: Cassandra、CIFS、CounchDB、DB2、FTP、GreenPlumDB、Hadoop、IBM INFORMIX (DRDA)、IBM iSeries、Informix、MongoDB、MS SQL SERVER、MYSQL、NETEZZA、Oracle、PostgreSQL、Sybase、または TERADATA。注: Informix は 2 つのプロトコル、SQLEXEC (ネイティブ Informix プロトコル) または DRDA (IBM プロトコル) をサポートします。これらのプロトコルは、追加の設定を行わなくても、Informix トラフィックでは自動的に識別されます。サーバー・タイプ属性には、INFORMIX (SQLEXEC プロトコルの場合) および IBM INFORMIX (DRDA) (DRDA プロトコルの場合) が表示されます。 注: TERADATA にはサイレント・ログインがあり、クライアントは自動再接続することが可能です。ポリシー内で Teradata ステートメントをブロックするには、デフォルト状態を「オン」にして S-TAP ファイアウォール機能を使用し、セーフ・ユーザーを監視対象から除外します。
データベース・ユーザー	データベース・ユーザー。「ルールでの値および/またはグループ値の指定」を参照してください。
エラー・コード	エラー・コード (例外の)。「ルールでの値および/またはグループ値の指定」を参照してください。
例外タイプ	例外のタイプ (リストから選択)。 注: 例外ルールに基づいて GUI のタイムアウトによってセッションが 閉じた場合、セッション・エラー (Session_Error) は生成されません。
フィールド名	フィールド名。「ルールでの値および/またはグループ値の指定」を参照してください。 「全て」ボックスにチェック・マークが付けられている場合、SQL ステートメントのすべてのフィールドがグループのメンバーでなければなりません。
最小 カウント	(「リセット間隔」に関連して) ルールが満たされるまでに、ルールに含まれる条件が一致しなければならない最小回数。
ネットワーク・プロトコル	ネットワーク・プロトコル。「ルールでの値および/またはグループ値の指定」を参照してください。
オブジェクト	オブジェクト名。「ルールでの値および/またはグループ値の指定」を参照してください。 Sybase および MS SQL Server それぞれについて、ストアード・プロシージャーの名前を含んだ MASKED_SP_EXECUTIONS_SYBASE および MASKED_SP_EXECUTIONS_MS_SQL_SERVER という 2 つのグループがあります。含まれるプロシージャーが実行される場合、すべてにマスクが掛けられます。 「全て」ボックスにチェック・マークが付けられている場合、SQL ステートメントのすべてのフィールドがグループのメンバーでなければなりません。
オブジェクト/コマンド・グループ	選択したオブジェクト/コマンド・グループのメンバーをマッチングします。
オブジェクト/フィールド・グループ	選択したオブジェクト/フィールド・グループのメンバーをマッチングします。
OS ユーザー	オペレーティング・システム・ユーザー。「ルールでの値および/またはグループ値の指定」を参照してください。
パターン	「パターン」ボックスに指定された、マッチングする正規表現。正規表現を手動で入力することも、「正規表現」ボタンをクリックして「正規表現の作成」ツールを開き、そのツールを使用して正規表現を入力およびテストすることもできます。
期間	ルールに 1 つの期間を識別させるには、「期間」リストから事前定義された期間を選択するか、「期間」ボタンをクリックして新しい期間を定義します。
値を記録	マークを付けると、ルールが満たされる原因となった実際の構成体が SQL 文字列属性で記録され、レポートで使用可能になります。ポリシー違反に限り、マークを付けないと SQL ステートメントは記録されません。
影響を受けるレコードしきい値	アクセス・ルールのみ。 一致するレコードに関するしきい値を設定します。 例: 1000 個のインスタンスが発生したらアクションをとるようにします。 このフィールドはルールの定義に影響するのではなく、ルールの出力に影響します (例えば、いつトリガーされるかではなく、トリガーされると何が起きるか)。 影響を受けるレコードしきい値は、ルールとセッションに基づきます。 それは、ルール条件を満たすすべての照会から返される累積行数です。 すべての影響を受けるレコードの累積がしきい値に達すると、ルールがトリガーされ、(全詳細をロギングするアクションの場合) ステートメントの影響を受けるレコードは、影響を受けるレコードの累積値になります。
置換文字	マスク文字を定義します。 抽出ルールによって生成された出力が正規表現に一致する場合、括弧「(」および「)」で囲まれたサブ表現に一致する部分がマスキング文字に置き換えられます。
リセット間隔	「最小数」フィールドがゼロより大きい場合にのみ使用されます。この値は分数で指定し、その経過後に条件一致数カウンターがゼロにリセットされます。

フィールド	記述
取り消し	このチェック・ボックスは、抽出ルールの場合のみ表示されます。これを使用すると、ポリシー内の先行するルールによって既にロギングが選択されている応答を、ロギングから除外することができます。ほとんどの場合、1 つ以上の「NOT」条件を指定した 1 つのルールを定義して、不要な応答を除外し、ルールを満たす残りの応答をロギングすることで、同様の結果がより簡単に得られます。(「取り消し」チェック・ボックスは「NOT」条件よりも古い機能であり、主に既存のポリシーをサポートする後方互換性のために提供されています。)
ルールの記述	ルールの名前。ルールで特殊パターン・テストを使用するには、特殊パターン・テスト名に続けて 1 つのスペースおよびルール名を固有にするための 1 つ以上の追加の文字を入力します (例: guardium://SSEC_NUMBER employee)。(詳しくは、『特殊パターン・テスト』を参照してください。) 表示される際には、名前の前にルール番号と、ルール・タイプを識別する Access Rule、 Exception Rule、または Extrusion Rule というラベルが付けられます。ルールが「DB に基づいた推奨」機能を使用して生成された場合、生成される名前の形式は「Suggested Rule <n>_mm-dd hh:mm」になります。各コンポーネントの意味は以下のとおりです。 n は、生成されるルールのシーケンス番号です。 mm-dd は、ルールが生成された月日です。 hh:mm は、ルールが生成された時刻です。
サーバー IP	含める場合は「Not」ボックスをクリアし、除外する場合は「Not」ボックスにマークを付けます。 • 任意のサーバー: すべてのサーバー・フィールドをブランクのままにします。カウントは任意のサーバーがルールを満たすごとに増分されます。(「Not」ボックスにマークが付けられている場合は、すべてのフィールドをブランクのままにすることはできません。) • IP アドレスとマスクによって選択されたすべてのサーバー: 最初のボックスにサーバー IP アドレスを、2 番目のボックスにネットワーク・マスクを入力します。カウントは、指定された任意のサーバーがルールを満たすごとに増分されます。例えば、サブネット 192.168.3.x のすべてのサーバーを選択するには、最初のボックスに 192.168.3.1 を、2 番目のボックスに 255.255.255.0 を入力します。 • サーバーのグループ: サーバー IP アドレスのグループを「グループ」ドロップダウン・リストから選択するか、「グループ」ボタンをクリックして新規グループを定義し、そのグループを選択します。カウントは、指定されたグループの任意のメンバーがルールを満たすごとに増分されます。 • IP アドレスとマスク、およびサーバーのグループによって選択されたすべてのサーバー: 「サーバー IP」および「グループ」フィールドの両方を使用します。カウントは、いずれかの方法を使用して指定された任意のサーバーがルールを満たすごとに増分されます。 IP アドレスでのワイルドカードの使用が可能になります。 サーバー IP グループには、ワイルドカード % をポリシー内で使用できます。
サービス名	サービス名。「ルールでの値および/またはグループ値の指定」を参照してください。
重大度	リストから重大度コード (「情報」、「低」、「なし」、「中」、または「高」) を選択します。「高」が選択され、このルールで E メール・アラートが送信される場合、その E メールには緊急フラグが付けられます。
SQL パターン	「パターン」ボックスに指定された、マッチングする正規表現。正規表現を手動で入力することも、「正規表現」 をクリックして「正規表現の作成」ツールを開き、そのツールを使用して正規表現を入力およびテストすることもできます。 制約事項: SQL パターンは、編集ルールではサポートされません。
ソース・アプリケーション	アプリケーション・ソース・プログラム。「ルールでの値および/またはグループ値の指定」を参照してください。
セッションごとに 1 回起動	最初の一致の後には、同じルールに対してセッションを分析しません。 特に、「選択的な監査」ポリシーに有効です。
XML パターン	「パターン」ボックスに指定された、マッチングする正規表現。正規表現を手動で入力することも、「正規表現」 をクリックして「正規表現の作成」ツールを開き、そのツールを使用して正規表現を入力およびテストすることもできます。 このボックスでは、マッチングのための正規表現を使用できます。
MSSQL 使用時の FULL_SQL 戻り値	MSSQL では、SELECT データベース照会にストアード・プロシージャー sp_cursoropen および sp_cursorfetch が使用されます。 sp_cursoropen にはオリジナル・ステートメントが保持されます。それに対し、抽出ルールの FULL_SQL 戻り値は、Select * from _____ でなく sp_cursorfetech として表現されます。

親トピック: ポリシー

カスタム・ルールを Guardium ポリシーに統合する方法

カスタム資格のシステムから Guardium ポリシーを自動的に変更する、または派生させる方法を説明します。

この例では、Oracle のサンプル表 (CUSTOM_ENTITLEMENT) をカスタム資格データの例として使い、 Oracle スクリプトを使用してこの表からデータを選択して、GuardAPI コマンドでファイルを生成します。 このファイルには、新規ポリシー・ルールの作成または既存のポリシー・ルールの修正、ポリシー・ルール順序の変更、およびポリシーの再インストールを行うコマンドが含まれるようになります。 また、生成したスクリプトを実行して、Guardium GUI でポリシーの変更を表示する方法も説明します。

付加価値: Guardium API は、コマンド行またはスクリプトからの Guardium 機能へのアクセスを提供します。これにより、大規模な実装において特に役に立つ反復作業の自動化が可能になります。 これらの GuardAPI 関数を呼び出すことで、ユーザーは Guardium ポリシーの保守などの操作を素早く実行することができます。

以下の手順を行います。

1. すべてのデータベース操作 (DML) コマンドのすべての詳細を記録するルール構造を定義します。これを新しいルールを作成するためのテンプレートとして使用します。 このルールは、テンプレート・ポリシーに属します。
2. 以下の GuardAPI コマンドでファイルを生成する Oracle スクリプトの作成:
    - copy_rule - インストール済みのポリシーにルール・テンプレートのコピーとして新規ルールを追加
    - update_rule - CUSTOM_ENTITLEMENT Oracle 表の関連データにより、コピーしたルールを更新
    - update_rule - この表のデータにより、既存のルールを更新
    - change_rule_order - ルールの位置を変更
    - policy_install、reinstall_policy - ポリシーのインストール/再インストール
3. 生成したスクリプトの実行
4. インストールされたポリシー変更の表示

手順:

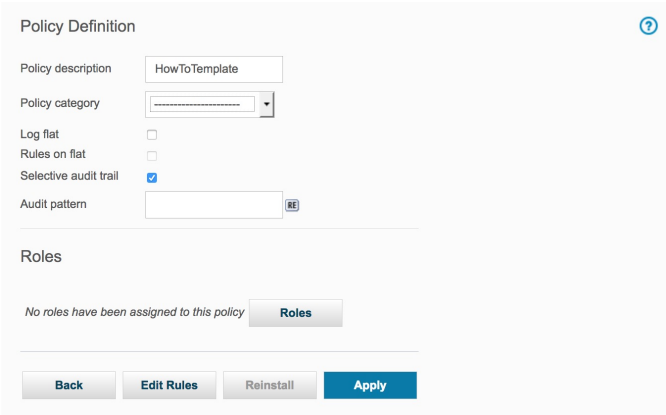
1. ルール・テンプレートの定義

    所定のポリシー・ルールでは多くのアクションが許可されているため、Guard API を使用してルールに持たせる複雑な階層構造を定義するのは非常に困難になります。 しかし、多くの場合にルールは条件別に異なり、アクションと受信者の構造は、 通常は異なるオプションの小さなグループに分かれます。 このため API は、ルール・テンプレートの役割をする既存のルールの複製をベースとしており、 このテンプレートでアクションと受信者の構造を定義し、その上で API を使用して条件を変更しています。

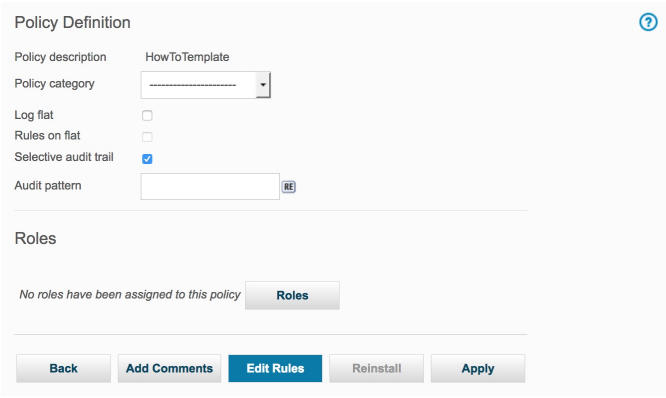
    ここで作成するルール・テンプレート (HowToTemplate) には、ルール・アクションの定義が含まれます。このタイプの新規ルールをポリシーに追加するごとに、これを複製して更新します。

    「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」を開き、テンプレート・ポリシーを作成します。
    S

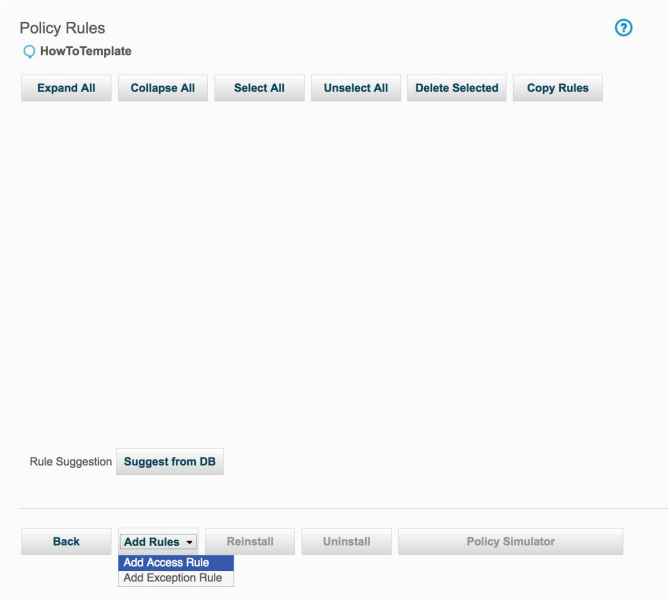
    「新規」をクリックして、テンプレート・ポリシーを作成します。「ポリシーの記述」に入力し、「選択的な監査証跡」チェック・ボックスにチェックを付けて、「保存」ボタンをクリックします。



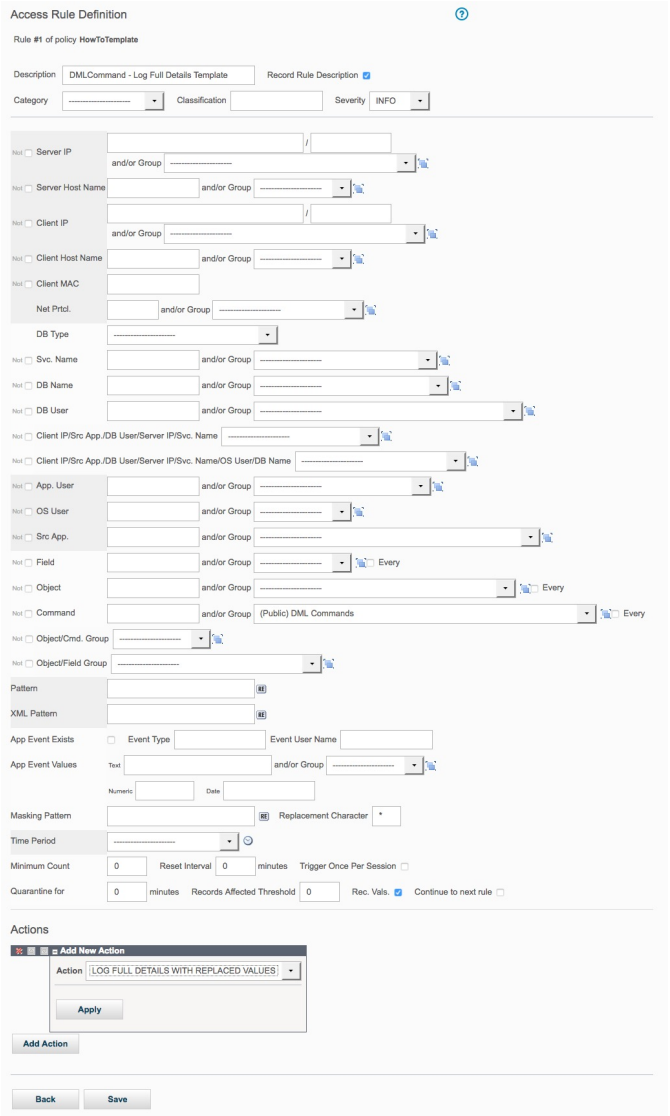
「ルールの編集」ボタンをクリックして、このポリシーにテンプレート・ルールを追加します。

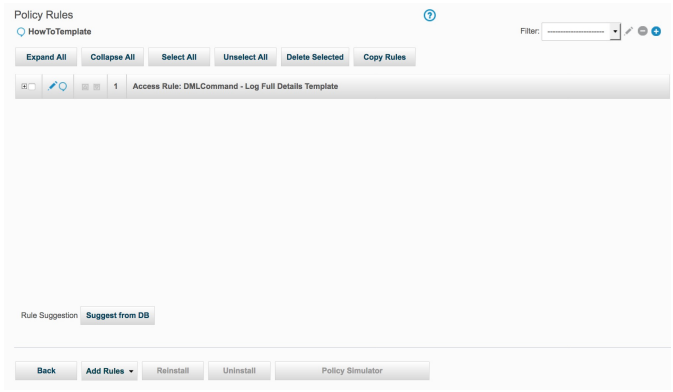


「**アクセス・ルールの追加**」ボタンをクリックして、「アクセス・ルール定義」パネルを表示し、ルールを追加します。



ルールを追加するために、「記述」ボックスに**「DML Command - Log Full Details Template」**と入力し、「コマンド」ボックスで**「(パブリック) DML コマンド」**を選択し、「アクション」セクションで**「全詳細を値とともにロギング」**を強調表示にして**「保存」**ボタンをクリックします。





2. GuardAPI コマンドでファイルを生成する Oracle スクリプトの作成

スクリプト作成の前に知っておきたい基本事項:

- GuardAPI は一連の CLI コマンドで、すべてキーワード **grdapi** で始まります。 使用可能なすべての GuardAPI コマンドをリストするには、引数なしでコマンド「grdapi」を入力します。 特定のコマンドのパラメーターを表示するには、コマンドに続けて「--help=yes」を入力します。

例

CLI>grdapi copy_rule --help=yes

ID=0

関数パラメーター:

fromPolicy - required

ruleDesc - required

toPolicy - required

ok

- パラメーターの構成要素となるキーワードと値には、いずれも大/小文字の区別があります。
- パラメーター値に 1 つ以上のスペースが含まれる場合は、二重引用符文字で囲む必要があります。 例:

```
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" ...
```

- 関数でサポートされる使用可能なすべてのパラメーターを使用する必要はありません。 必須のパラメーターに加え、変更したいパラメーターを使用してください。
- GuardAPI を呼び出すスクリプトには、データ・ソースのパスワードなどの機密情報が含まれる場合があります。 機密情報を常に暗号化しておくため、**grdapi** コマンドは 1 つの暗号化されたパラメーターを API 関数に渡すことができます。この暗号化は、システムの共有パスワードを使用して行われます。これは、管理者によって設定され、複数のシステム、一元管理/統合クラスターの全ユニット間で共有することができます。これにより、暗号化されたパラメーターを含むスクリプトを同じ共有パスワードを持つマシンで実行することが可能です。 この点についての詳細は、Guardium ヘルプを参照してください。
- 複数のポリシーがインストールされている場合は、ポリシーのインストール・コマンド (**policy_install**) に、すべてのインストール済みポリシーの記述をパイプ文字で区切って含める必要があります。 これは、1 つのポリシーだけ変更がある場合でも行う必要があります。 ポリシーの記述は、ポリシーをインストールする順序にする必要があります。

HowTo 1 ポリシーとHowTo 2 ポリシーをインストールするためのコマンドの例

```
grdapi policy_install policy="HowTo 1|HowTo 2"
```

スクリプト作成のロジック - 現在インストールされているポリシー HowTo は以下の方法で変更します。

a. CUSTOM_ENTITLEMENT 表で、 IS_NEW_FLAG が「1」に等しい各レコードについて、RULE_DESC 列に保存された記述による新しいアクセス・ルールを "HowTo" ポリシーに追加します。 このルールにより、OS ユーザー (OS_USER フィールド値)、クライアント IP (CLIENT_IP)、サービス名 (SERVICE_NAME) を伴ったサーバー IP (SERVER_IP) からのすべての DML コマンドの全詳細がログに記録されます。

b. IS_NEW_FLAG 値が「0」である場合、RULE_DESC 列の値に等しい記述を含むルールが、表のこのレコードの関連データを元に変更されます。

c. Rule3 は最初のルール (**change_rule_order** 関数の使用方法を示す) として設定されます。

d. すべての変更を適用するため、ポリシーが再インストールされます。

custom_entitlement 表のデータ

表 1. カスタム・ライセンス

os_user	client_ip	server_ip	rule_desc	service_name	is_new_rule	seq
User1	192.168.7.101	192.168.7.201	Rule1	PROD1	1	1
User2	192.168.7.102	192.168.7.202	Rule2	PROD2	1	2
User3	192.168.7.103	192.168.7.203	Rule3	PROD3	1	3

os_user	client_ip	server_ip	rule_desc	service_name	is_new_rule	seq
User4	192.168.7.104	192.168.7.204	Rule2	PROD4	0	4

ロジックと表データに基づく変更の説明:

a. 新しいアクセス・ルール Rule1 を追加します。 このルールは、ユーザー "user1"、クライアント IP "192.168.7.101" からのすべての DML コマンドの全詳細を "192.168.7.201" サーバー (サービス名 "PROD1") の Oracle データベースに記録します。

b. 新しいアクセス・ルール Rule2 を追加します。 このルールは、ユーザー "user2"、クライアント IP "192.168.7.102" からのすべての DML コマンドの全詳細を "192.168.7.202" サーバー (サービス名 "PROD2") の Oracle データベースに記録します。

c. 新しいアクセス・ルール Rule3 を追加します。 このルールは、ユーザー "user3"、クライアント IP "192.168.7.103" からのすべての DML コマンドの全詳細を "192.168.7.203" サーバー (サービス名 "PROD3") の Oracle データベースに記録します。

d. Rule2 を変更します。OS ユーザーを "user4"、クライアント IP を "192.168.7.104"、サーバー IP を "192.168.7.204"、サービス名を "PROD4" に変更します。

e. Rule3 をポリシーの最初のルールに設定します。

f. 上記のすべての変更を適用するため、ポリシーを再インストールします。

Oracle スクリプト

```
SET LINESIZE 2000
SET TERMOUT OFF
SET FEEDBACK OFF

SET SERVEROUTPUT ON SIZE 1000000
spool update_policy.txt

declare cursor CUSTOM_TABLE is
select OS_USER,CLIENT_IP,SERVER_IP,SERVICE_NAME,RULE_DESC,IS_NEW_RULE
  from CUSTOM_ENTITLEMENT order by SEQ;
S_RULE_DESC VARCHAR2(100);
BEGIN
    FOR CUR_W IN CUSTOM_TABLE
    LOOP
        IF NVL(CUR_W.IS_NEW_RULE,'0') = '1' THEN
           -- copy rule
           DBMS_OUTPUT.PUT_LINE('grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate
toPolicy=HowTo ');
           S_RULE_DESC := 'DMLCommand - Log Full Details Template';
        ELSE
           S_RULE_DESC := CUR_W.RULE_DESC;
        END IF;
        -- update rule
        DBMS_OUTPUT.PUT_LINE(
        'grdapi update_rule ruleDesc="'||S_RULE_DESC||'"'||
        ' fromPolicy=HowTo newDesc="'|| CUR_W.RULE_DESC ||'" clientIP='||CUR_W.CLIENT_IP ||
        ' clientNetMask=255.255.255.0 serverIP='||CUR_W.SERVER_IP||' serverNetMask=255.255.255.0 '||
        ' serviceName='||CUR_W.SERVICE_NAME ||' osUser='||CUR_W.OS_USER||' dbType=ORACLE');
    END LOOP;
    -- set Rule3 to be the first one
    DBMS_OUTPUT.PUT_LINE('grdapi change_rule_order ruleDesc=Rule3 fromPolicy=HowTo order=1');
    -- reinstall policy
    DBMS_OUTPUT.PUT_LINE('grdapi policy_install policy=HowTo');
END;
/
spool off
```

GuardAPI コマンドにより生成されるスクリプト

Oracle スクリプトが SQL*Plus で実行されてスプールに入ると、次のようなファイル (update_policy.txt) が作成されます。

```
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate toPolicy=HowTo
grdapi update_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowTo newDesc="Rule1" clientIP=192.168.7.101
clientNetMask=255.255.255.0 serverIP=192.168.7.201 serverNetMask=255.255.255.0  serviceName=PROD1 osUser=user1 dbType=ORACLE
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate toPolicy=HowTo
grdapi update_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowTo newDesc="Rule2" clientIP=192.168.7.102
clientNetMask=255.255.255.0 serverIP=192.168.7.202 serverNetMask=255.255.255.0  serviceName=PROD2 osUser=user2 dbType=ORACLE
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate toPolicy=HowTo
grdapi update_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowTo newDesc="Rule3" clientIP=192.168.7.103
clientNetMask=255.255.255.0 serverIP=192.168.7.203 serverNetMask=255.255.255.0  serviceName=PROD3 osUser=user3 dbType=ORACLE
grdapi update_rule ruleDesc="Rule2" fromPolicy=HowTo newDesc="Rule2" clientIP=192.168.7.104 clientNetMask=255.255.255.0
serverIP=192.168.7.204 serverNetMask=255.255.255.0  serviceName=PROD4 osUser=user4 dbType=ORACLE
grdapi change_rule_order ruleDesc=Rule3 fromPolicy=HowTo order=1
grdapi policy_install policy=HowTo
```

注: 最後の grdapi コマンドは、ポリシーを再インストールしてルールをシステムに適用します。

3. 生成したスクリプトの実行

このスクリプトを実行するため、以下のコマンド構造を使用します。

ssh cli@[Guardium appliance name] < [script name]

例えば、 update_policy.txt スクリプトをホスト 192.168.12.5 で実行するには、次のようにします (パスワードのプロンプトが出ます)。

ssh cli@192.168.12.5 <update_policy.txt

出力例:

192.168.12.5> ok

ID=20002

192.168.12.5> 192.168.12.5> ok

ID=20015

192.168.12.5> 192.168.12.5> ok

ID=20002

192.168.12.5> 192.168.12.5> ok

ID=20016

192.168.12.5> 192.168.12.5> ok

ID=20002

192.168.12.5> 192.168.12.5> ok

ID=20017

192.168.12.5> 192.168.12.5> ok

ID=20016

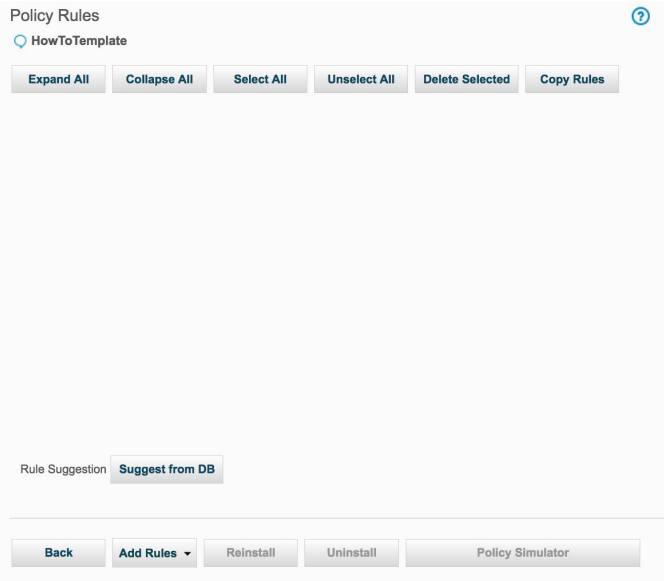
192.168.12.5> 192.168.12.5> ok

ID=20002

192.168.12.5> 192.168.12.5>

4. インストールされたポリシー変更の表示

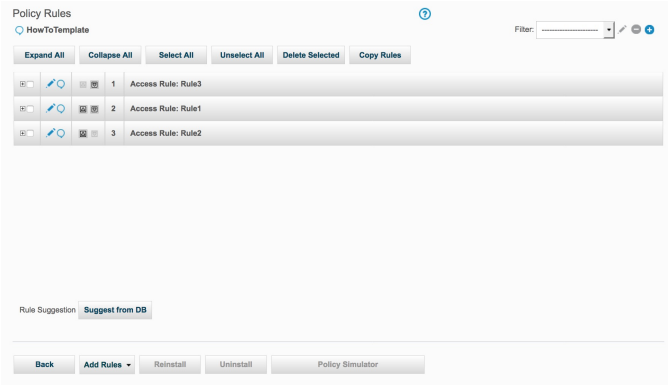
   スクリプトを実行する前には、次のプレビューに示すように、HowTo ポリシーにルールは定義されていませんでした。



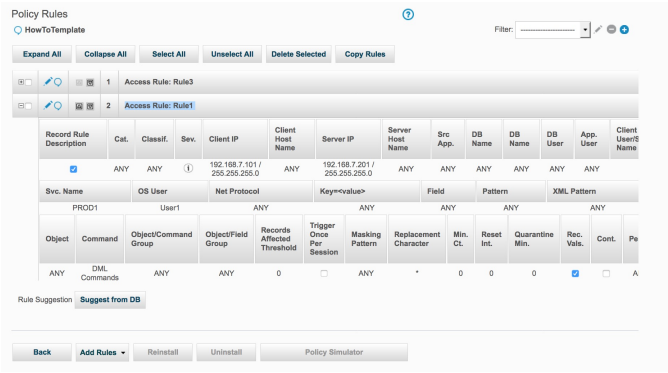
   スクリプトを実行した後は、次のようになります。

   copy_rule の結果、HowTo ポリシーに 3 つのアクセス・ルールがあるようになりました。

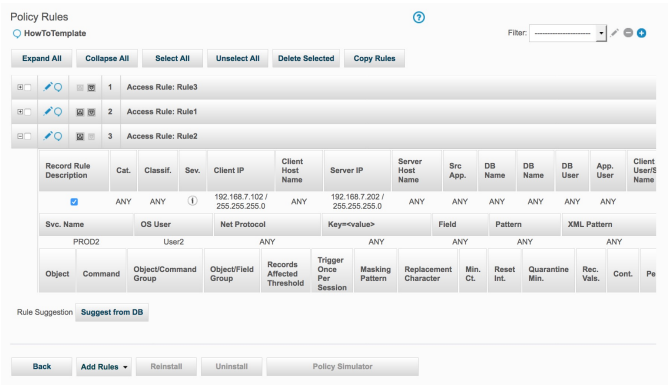
   change_rule_order コマンドの結果、Rule3 が最初のルールになりました。



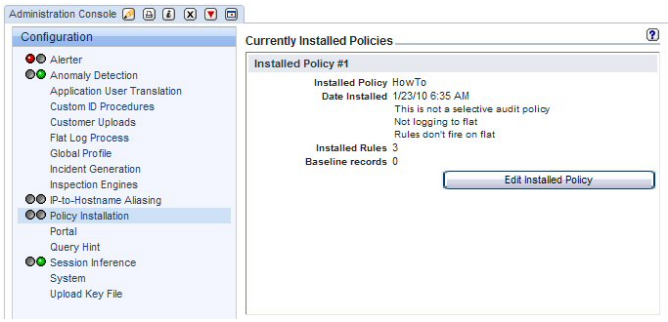
いずれかのポリシー・ルール (ここでは Rule1) を拡張することで、**update_rule** コマンドで変更された各種フィールドを検証することができます。



update_rule コマンドの結果、Rule2 が変更されました。



また、**policy_install** コマンドの結果、現在インストールされているポリシーは、3 つのルールがインストールされた HowTo ポリシーとなりました。



親トピック: ポリシー

適切な無視アクションの使用方法

ポリシー・ルールで無視アクションを使用した場合のデータの処理方法を詳しく説明します。

付加価値: ポリシー・ルールで (ロギングのレベルを制御する) ログまたは無視のアクションの選択を行った場合に、監視対象トラフィックに基づいてどのような処理が行われるかを明らかにします。

詳しい情報は、『ポリシー』を参照してください。

セッションを無視

現行の要求およびセッションの残りが無視されます。 このアクションは、ポリシー違反をログに記録しませんが、構造のロギングを停止し、そのセッションの残りのいずれのタイプのポリシー違反もテストしません。このアクションは、例えば、データベースにテスト領域が含まれ、データベースのその領域に対してポリシー・ルールを適用する必要がない場合などに役立ちます。

表 1. セッションを無視

クライアントおよび DB サーバー/S-TAP 間でログに記録または無視されるデータ	DB サーバー/S-TAP からコレクターに送られるデータ	スパン・ポート/ネットワーク TAP からコレクターへのデータ
無視 - SQL コマンド、SQL エラー、 結果セット	ログイン/ログアウト スニファーから S-TAP - S-TAP への 1 シグナルによりこのセッションの送信アクティビティーを停止。 追加のアクティビティーが S-TAP により送られる場合、これはスニファー・レベルでのみ無視される。 SQL コマンドを無視 SQL エラーを無視 結果セットを無視	無視 – SQL コマンド、SQL エラー、 結果セット。 スパン・ポート/ネットワーク TAP からの SQL コマンドとエラーは、 スニファーでフィルター処理される。

S-TAP セッションを無視

現行の要求および S-TAP セッションの残りが無視されます。 このアクションは、大量のネットワーク・トラフィックを生成する特定のマシン、ユーザー、またはアプリケーションのポリシー・ビルダー・メニュー画面での指定と組み合わせて実行されます。 このアクションは、S-TAP セッションからの以後のデータベース応答が重要でないことがわかっている場合に役立ちます。

表 2. S-TAP セッションを無視

クライアントおよび DB サーバー/S-TAP 間でログに記録または無視されるデータ	DB サーバー/S-TAP からコレクターに送られるデータ	スパン・ポート/ネットワーク TAP からコレクターへのデータ
無視 - SQL コマンド、SQL エラー、 結果セット	スニファーから S-TAP へのログイン/ログアウト - S-TAP への 1 シグナルによりこのセッションの送信アクティビティーを停止。 S-TAP に追加のシグナルが送られると、このセッションへの送信アクティビティーを停止。	適用外 スパン・ポート/ネットワーク TAP からのトラフィックを無視する必要がある場合は、 代わりに「セッションを無視」を使用する。

セッションごとに応答を無視

セッションの残りに対する応答が無視されます。 このアクションは、ポリシー違反をログに記録しますが、セッションの残りの部分に対する応答の分析を停止します。このアクションは、以後のデータベース応答が重要でないことがわかっている場合に役立ちます。

注:「セッションごとに応答を無視」の場合、スニファーは照会に対する応答を 1 件も受信しないか、応答が無視されるため、COUNT_FAILED および SUCCESS の値は表のデフォルトが何であっても、この場合は COUNT_FAILED=0 および SUCCESS=1 です。

表 3. セッションごとに応答を無視

クライアントおよび DB サーバー/S-TAP 間でログに記録または無視されるデータ	DB サーバー/S-TAP からコレクターに送られるデータ	スパン・ポート/ネットワーク TAP からコレクターへのデータ
ログ – SQL コマンド、無視 - SQL エラー、結果セット	スニファーから S-TAP へのログイン/ログアウト SQL コマンド - S-TAP への 1 シグナルによりこのセッションの送信アクティビティーを停止。 S-TAP に追加のシグナルが送られると、このセッションへの送信アクティビティーを停止。	適用外 このルール・アクションは S-TAP のみの実装。

セッションごとに SQL を無視

セッションの残りの部分に関する SQL はログに記録されません。例外は引き続きログに記録されますが、システムは、その例外に対応する SQL 文字列をキャプチャーしない場合があります。

表 4. セッションごとに SQL を無視

クライアントおよび DB サーバー/S-TAP 間でログに記録または無視されるデータ	DB サーバー/S-TAP からコレクターに送られるデータ	スパン・ポート/ネットワーク TAP からコレクターへのデータ

クライアントおよび DB サーバー/S-TAP 間でログに記録または無視されるデータ	DB サーバー/S-TAP からコレクターに送られるデータ	スパン・ポート/ネットワーク TAP からコレクターへのデータ
無視 - SQL コマンド ログ - SQL エラー、 結果セット	ログイン/ログアウト スニファーから S-TAP - S-TAP への 1 シグナルによりこのセッションの送信アクティビティーを停止。 追加のアクティビティーが S-TAP により送られる場合、これはスニファー・レベルでのみ無視される。 SQL コマンドをログ SQL エラーをログ 結果セットをログ - 抽出ルール使用の場合	無視 - SQL コマンド ログ - SQL エラー、 結果セット SQL コマンドはスニファーでフィルターされる。

選択的な監査証跡

「選択的な監査証跡」ポリシーを使用して、アプライアンスでのロギングの量を制限します。 これは、検査エンジンで受信されているトラフィックのうち重要なトラフィックの割合が比較的小さい場合や、レポート対象となり得るすべてのトラフィックが完全に識別可能である場合に適しています。

選択的な監査証跡を使用している場合であっても、ポリシーに「セッションを無視」ルールを組み込むことが引き続き非常に重要である点に十分注意してください。「セッションを無視」ルールを使用すると、コレクターの負荷を大幅に削減できます。これは、S-TAP レベルで情報をフィルター操作することにより、コレクターがその情報を受信することがなくなり、最終的にログに記録されることのないトラフィックの分析にリソースを消費する必要がなくなるためです。「セッションを無視」ルールが指定されていない「選択的な監査証跡」ポリシーは、すべてのトラフィックがデータベース・サーバーからコレクターに送信され、コレクターがデータベース・サーバーの生成したすべてのコマンドおよび結果セットを分析することになることを意味します。

表 5. 選択的な監査証跡

クライアントおよび DB サーバー/S-TAP 間でログに記録または無視されるデータ	DB サーバー/S-TAP からコレクターに送られるデータ	スパン・ポート/ネットワーク TAP からコレクターへのデータ
無視 - SQL コマンド ログ - SQL エラー、 結果セット	ログイン/ログアウト SQL コマンドを無視 (「監査のみ」ルールまたは「全詳細をロギング」ルールで定義されているものを除く)。 SQL エラーをログ 結果セットをログ - 抽出ルール使用の場合	無視 - SQL コマンド ログ - SQL エラー、 結果セット SQL コマンドはスニファーでフィルターされる。

親トピック: ポリシー

文字セット

抽出ルールで文字セット・コードを使用できます。

使用可能な文字セット・コードのリスト

ANSI_X3.4-1968 - 1
ANSI_X3.4-1986 - 2
ASCII - 3
CP367 - 4
IBM367 - 5
ISO-IR-6 - 6
ISO646-US - 7
ISO_646.IRV:1991 - 8
US - 9
US-ASCII - 10
CSASCII - 11
UTF-8 - 12
ISO-10646/UCS2 - 13
UCS-2 - 14
CSUNICODE - 15
UCS-2BE - 16
UNICODE - 17
UNICODEBIG - 18
TSCII - 19
UCS-2LE - 20
UNICODELITTLE - 21
ISO-10646/UCS4 - 22
UCS-4 - 23
CSUCS4 - 24
UCS-4BE - 25
UCS-4LE - 26
UTF-16 - 27
UTF-16BE - 28
UTF-16LE - 29

UTF-32 - 30
UTF-32BE - 31
UTF-32LE - 32
UTF7 - 33
UTF-7 - 34
UTF-8 - 35
UCS2 - 36
UCS2 - 37
UCS4 - 38
UCS4 - 39
UTF8 - 40
UTF8 - 41
CP819 - 42
IBM819 - 43
ISO-8859-1 - 44
ISO-IR-100 - 45
ISO8859-1 - 46
ISO_8859-1 - 47
ISO_8859-1:1987 - 48
L1 - 49
LATIN1 - 50
CSISOLATIN1 - 51
ISO-8859-2 - 52
ISO-IR-101 - 53
ISO8859-2 - 54
ISO_8859-2 - 55
ISO_8859-2:1987 - 56
L2 - 57
LATIN2 - 58
CSISOLATIN2 - 59
ISO-8859-3 - 60
ISO-IR-109 - 61
ISO8859-3 - 62
ISO_8859-3 - 63
ISO_8859-3:1988 - 64
L3 - 65
LATIN3 - 66
CSISOLATIN3 - 67
ISO-8859-4 - 68
ISO-IR-110 - 69
ISO8859-4 - 70
ISO_8859-4 - 71
ISO_8859-4:1988 - 72
L4 - 73
LATIN4 - 74
CSISOLATIN4 - 75
CYRILLIC - 76
ISO-8859-5 - 77
ISO-IR-144 - 78
ISO8859-5 - 79
ISO_8859-5 - 80
ISO_8859-5:1988 - 81
CSISOLATINCYRILLIC - 82
ARABIC - 83
ASMO-708 - 84
ECMA-114 - 85
ISO-8859-6 - 86
ISO-IR-127 - 87
ISO8859-6 - 88
ISO_8859-6 - 89
ISO_8859-6:1987 - 90
CSISOLATINARABIC - 91
ECMA-118 - 92
ELOT_928 - 93
GREEK - 94
GREEK8 - 95
ISO-8859-7 - 96
ISO-IR-126 - 97
ISO8859-7 - 98
ISO_8859-7 - 99
ISO_8859-7:1987 - 100
CSISOLATINGREEK - 101
HEBREW - 102
ISO-8859-8 - 103
ISO-IR-138 - 104
ISO8859-8 - 105
ISO_8859-8 - 106
ISO_8859-8:1988 - 107
CSISOLATINHEBREW - 108
ISO-8859-9 - 109

ISO-IR-148 - 110
ISO8859-9 - 111
ISO_8859-9 - 112
ISO_8859-9:1989 - 113
L5 - 114
LATIN5 - 115
CSISOLATIN5 - 116
ISO-8859-10 - 117
ISO-IR-157 - 118
ISO8859-10 - 119
ISO_8859-10 - 120
ISO_8859-10:1992 - 121
L6 - 122
LATIN6 - 123
CSISOLATIN6 - 124
ISO-8859-13 - 125
ISO-8859-13 - 126
ISO-8859-13 - 127
ISO-8859-13 - 128
L7 - 129
LATIN7 - 130
ISO-8859-14 - 131
ISO-CELTIC - 132
ISO-IR-199 - 133
ISO8859-14 - 134
ISO_8859-14 - 135
ISO_8859-14:1998 - 136
L8 - 137
LATIN8 - 138
ISO-8859-15 - 139
ISO-IR-203 - 140
ISO8859-15 - 141
ISO_8859-15 - 142
ISO_8859-15:1998 - 143
ISO-8859-16 - 144
ISO-IR-226 - 145
ISO8859-16 - 146
ISO_8859-16 - 147
ISO_8859-16:2000 - 148
KOI8-R - 149
CSKOI8R? - 150
KOI8U? - 151
KOI8R? - 152
CP1250 - 153
MS-EE - 154
WINDOWS-1250 - 155
CP1251 - 156
MS-CYRL - 157
WINDOWS-1251 - 158
CP1252 - 159
MS-ANSI - 160
WINDOWS-1252 - 161
CP1253 - 162
MS-GREEK - 163
WINDOWS-1253 - 164
CP1254 - 165
MS-TURK - 166
WINDOWS-1254 - 167
CP1255 - 168
MS-HEBR - 169
WINDOWS-1255 - 170
CP1256 - 171
MS-ARAB - 172
WINDOWS-1256 - 173
CP1257 - 174
WINBALTRIM - 175
WINDOWS-1257 - 176
CP1258 - 177
WINDOWS-1258 - 178
850 - 179
CP850 - 180
IBM850 - 181
CSPC850MULTILINGUAL? - 182
862 - 183
CP862 - 184
IBM862 - 185
CSPC862LATINHEBREW? - 186
866 - 187
CP866 - 188
IBM866 - 189

CSIBM866 - 190
MAC - 191
MACINTOSH - 192
MACUK - 193
CSMACINTOSH - 194
MACIS - 195
MAC - 196
MAC - 197
MAC - 198
MAC - 199
MACUKRAINIAN - 200
MAC - 201
MAC - 202
MAC - 203
MAC - 204
MAC - 205
HP-ROMAN8 - 206
R8 - 207
ROMAN8 - 208
HPROMAN8 - 209
ROMAN8 - 210
ARMSCII-8 - 211
GEORGIAN-ACADEMY - 212
GEORGIAN-PS - 213
KOI8-T - 214
KOI8-T - 215
CP1133 - 216
IBM-CP1133 - 217
ISO-IR-166 - 218
TIS-620 - 219
TIS620 - 220
TIS620-0 - 221
TIS620.2529-1 - 222
TIS620.2533-0 - 223
TIS620.2533-1 - 224
CP874 - 225
WINDOWS-874 - 226
VISCII - 227
VISCII - 228
VISCII - 229
TCVN - 230
TCVN-5712 - 231
TCVN5712-1 - 232
TCVN5712-1:1993 - 233
ISO-IR-14 - 234
ISO646-JP - 235
JIS_C6220-1969-RO - 236
JP - 237
CSISO14JISC6220RO? - 238
JISX0201-1976 - 239
JIS_X0201 - 240
X0201 - 241
CSHALFWIDTHKATAKANA - 242
ISO-IR-87 - 243
JIS0208 - 244
JIS_C6226-1983 - 245
JIS_X0208 - 246
JIS_X0208-1983 - 247
JIS_X0208-1990 - 248
X0208 - 249
CSISO87JISX0208? - 250
ISO-IR-159 - 251
JIS_X0212 - 252
JIS_X0212-1990 - 253
JIS_X0212.1990-0 - 254
X0212 - 255
CSISO159JISX02121990? - 256
CN - 257
GB_1988-80 - 258
ISO-IR-57 - 259
ISO646-CN - 260
CSISO57GB1988? - 261
CHINESE - 262
GB_2312-80 - 263
ISO-IR-58 - 264
CSISO58GB231280? - 265
CN-GB-ISOIR165 - 266
ISO-IR-165 - 267
ISO-IR-149 - 268
KOREAN - 269

KSC_5601 - 270
KS_C_5601-1987 - 271
KS_C_5601-1989 - 272
CSKSC56011987 - 273
EUC-JP - 274
EUCJP - 275
EXTENDED_UNIX_CODE_PACKED_FORMAT_FOR_JAPANESE - 276
CSEUCPKDFMTJAPANESE - 277
MS_KANJI - 278
SHIFT-JIS - 279
SHIFT_JIS - 280
SJIS - 281
CSSHIFTJIS - 282
CP932 - 283
ISO-2022-JP - 284
CSISO2022JP? - 285
ISO-2022-JP-1 - 286
ISO-2022-JP-2 - 287
CSISO2022JP2? - 288
CN-GB - 289
EUC-CN - 290
EUCCN - 291
GB2312 - 292
CSGB2312 - 293
CP936 - 294
GBK - 295
GB18030 - 296
ISO-2022-CN - 297
CSISO2022CN? - 298
ISO-2022-CN-EXT - 299
HZ - 300
HZ-GB-2312 - 301
EUC-TW - 302
EUCTW - 303
CSEUCTW - 304
BIG-5 - 305
BIG-FIVE - 306
BIG5 - 307
BIGFIVE - 308
CN-BIG5 - 309
CSBIG5 - 310
CP950 - 311
BIG5-HKSCS - 312
BIG5HKSCS? - 313
EUC-KR - 314
EUCKR - 315
CSEUCKR - 316
CP949 - 317
UHC - 318
CP1361 - 319
JOHAB - 320
ISO-2022-KR - 321
CSISO2022KR? - 322
IBM037 - 323
IBM038 - 324
IBM256 - 325
IBM273 - 326
IBM274 - 327
IBM275 - 328
IBM277 - 329
IBM278 - 330
IBM280 - 331
IBM281 - 332
IBM284 - 333
IBM285 - 334
IBM290 - 335
IBM297 - 336
IBM367 - 337
IBM420 - 338
IBM423 - 339
IBM424 - 340
IBM437 - 341
IBM500 - 342
IBM775 - 343
IBM813 - 344
IBM819 - 345
IBM848 - 346
IBM850 - 347
IBM851 - 348
IBM852 - 349

IBM855 - 350
IBM856 - 351
IBM857 - 352
IBM860 - 353
IBM861 - 354
IBM862 - 355
IBM863 - 356
IBM864 - 357
IBM865 - 358
IBM866 - 359
IBM866NAV? - 360
IBM868 - 361
IBM869 - 362
IBM870 - 363
IBM871 - 364
IBM874 - 365
IBM875 - 366
IBM880 - 367
IBM891 - 368
IBM903 - 369
IBM904 - 370
IBM905 - 371
IBM912 - 372
IBM915 - 373
IBM916 - 374
IBM918 - 375
IBM920 - 376
IBM922 - 377
IBM930 - 378
IBM932 - 379
IBM933 - 380
IBM935 - 381
IBM937 - 382
IBM939 - 383
IBM943 - 384
IBM1004 - 385
IBM1026 - 386
IBM1046 - 387
IBM1047 - 388
IBM1089 - 389
IBM1124 - 390
IBM1129 - 391
IBM1132 - 392
IBM1133 - 393
IBM1160 - 394
IBM1161 - 395
IBM1162 - 396
IBM1163 - 397
IBM1164 - 398
MSCP949 - 399
EUC-JISX0213 - 400
UJIS - 401
CP852 - 402
EUCJP-MS - 403
IBM902 - 404
IBM921 - 405
WINDOWS-31J - 406
IBM1025 - 407
IBM1140 - 408
IBM1137 - 409
IBM1122 - 410
IBM1141 - 411
IBM1142 - 412
IBM1143 - 413
IBM1144 - 414
IBM1145 - 415
IBM1146 - 416
IBM1147 - 417
IBM1148 - 418
IBM1149 - 419
IBM1153 - 420
IBM1155 - 421
IBM1157 - 422
EBCDICUS - 423
IBM1112 - 424
IBM1158 - 425
437 - 426
500g - 427
500V1g - 428
851g - 429

852g - 430
855g - 431
856g - 432
857g - 433
860g - 434
861g - 435
863g - 436
864g - 437
865g - 438
866NAVg - 439
869g - 440
874g - 441
904g - 442
1026g - 443
1046g - 444
1047g - 445
8859_1g - 446
8859_2g - 447
8859_3g - 448
8859_4g - 449
8859_5g - 450
8859_6g - 451
8859_7g - 452
8859_8g - 453
8859_9g - 454
10646-1:1993g - 455
10646-1:1993/UCS4/ - 456
ANSI_X3.4g - 457
ANSI_X3.110-1983g - 458
ANSI_X3.110g - 459
ARABIC7g - 460
ASMO_449g - 461
BALTICg - 462
BIG-5g - 463
BIG-FIVEg - 464
BIG5-HKSCSg - 465
BIG5g - 466
BIG5HKSCSg? - 467
BIGFIVEg - 468
BS_4730g - 469
CAg - 470
CN-BIG5g - 471
CN-GBg - 472
CNg - 473
CP-ARg - 474
CP-GRg - 475
CP-HUg - 476
CP037g - 477
CP038g - 478
CP273g - 479
CP274g - 480
CP275g - 481
CP278g - 482
CP280g - 483
CP281g - 484
CP282g - 485
CP284g - 486
CP285g - 487
CP290g - 488
CP297g - 489
CP420g - 490
CP423g - 491
CP424g - 492
CP437g - 493
CP500g - 494
CP737g - 495
CP775g - 496
CP803g - 497
CP813g - 498
CP851g - 499
CP852g - 500
CP855g - 501
CP856g - 502
CP857g - 503
CP860g - 504
CP861g - 505
CP863g - 506
CP864g - 507
CP865g - 508
CP866NAVg? - 509

CP868g - 510
CP869g - 511
CP870g - 512
CP871g - 513
CP875g - 514
CP880g - 515
CP891g - 516
CP901g - 517
CP902g - 518
CP903g - 519
CP904g - 520
CP905g - 521
CP912g - 522
CP915g - 523
CP916g - 524
CP918g - 525
CP920g - 526
CP921g - 527
CP922g - 528
CP930g - 529
CP932g - 530
CP933g - 531
CP935g - 532
CP936g - 533
CP937g - 534
CP939g - 535
CP949g - 536
CP950g - 537
CP1004g - 538
CP1008g - 539
CP1025g - 540
CP1026g - 541
CP1046g - 542
CP1047g - 543
CP1070g - 544
CP1079g - 545
CP1081g - 546
CP1084g - 547
CP1089g - 548
CP1097g - 549
CP1112g - 550
CP1122g - 551
CP1123g - 552
CP1124g - 553
CP1125g - 554
CP1129g - 555
CP1130g - 556
CP1132g - 557
CP1137g - 558
CP1140g - 559
CP1141g - 560
CP1142g - 561
CP1143g - 562
CP1144g - 563
CP1145g - 564
CP1146g - 565
CP1147g - 566
CP1148g - 567
CP1149g - 568
CP1153g - 569
CP1154g - 570
CP1155g - 571
CP1156g - 572
CP1157g - 573
CP1158g - 574
CP1160g - 575
CP1161g - 576
CP1162g - 577
CP1163g - 578
CP1164g - 579
CP1166g - 580
CP1167g - 581
CP1361g - 582
CP1364g - 583
CP1371g - 584
CP1388g - 585
CP1390g - 586
CP1399g - 587
CP4517g - 588
CP4899g - 589

CP4909g - 590
CP4971g - 591
CP5347g - 592
CP9030g - 593
CP9066g - 594
CP9448g - 595
CP10007g - 596
CP12712g - 597
CP16804g - 598
CPIBM861g - 599
CSA7-1g - 600
CSA7-2g - 601
CSA_T500-1983g - 602
CSA_T500g - 603
CSA_Z243.4-1985-1g - 604
CSA_Z243.4-1985-2g - 605
CSA_Z243.419851g - 606
CSA_Z243.419852g - 607
CSDECMCSg - 608
CSEBCDICATDEg - 609
CSEBCDICATDEAg - 610
CSEBCDICCAFRg - 611
CSEBCDICDKNOg - 612
CSEBCDICDKNOAg - 613
CSEBCDICESg - 614
CSEBCDICESAg - 615
CSEBCDICESSg - 616
CSEBCDICFISEg - 617
CSEBCDICFISEAg - 618
CSEBCDICFRg - 619
CSEBCDICITg - 620
CSEBCDICPTg - 621
CSEBCDICUKg - 622
CSEBCDICUSg - 623
CSEUCKRg - 624
CSEUCPKDFMTJAPANESEg - 625
CSGB2312g - 626
CSIBM037g - 627
CSIBM038g - 628
CSIBM273g - 629
CSIBM274g - 630
CSIBM275g - 631
CSIBM277g - 632
CSIBM278g - 633
CSIBM280g - 634
CSIBM281g - 635
CSIBM284g - 636
CSIBM285g - 637
CSIBM290g - 638
CSIBM297g - 639
CSIBM420g - 640
CSIBM423g - 641
CSIBM424g - 642
CSIBM500g - 643
CSIBM803g - 644
CSIBM851g - 645
CSIBM855g - 646
CSIBM856g - 647
CSIBM857g - 648
CSIBM860g - 649
CSIBM863g - 650
CSIBM864g - 651
CSIBM865g - 652
CSIBM868g - 653
CSIBM869g - 654
CSIBM870g - 655
CSIBM871g - 656
CSIBM880g - 657
CSIBM891g - 658
CSIBM901g - 659
CSIBM902g - 660
CSIBM903g - 661
CSIBM904g - 662
CSIBM905g - 663
CSIBM918g - 664
CSIBM921g - 665
CSIBM922g - 666
CSIBM930g - 667
CSIBM932g - 668
CSIBM933g - 669

CSIBM935g - 670
CSIBM937g - 671
CSIBM939g - 672
CSIBM943g - 673
CSIBM1008g - 674
CSIBM1025g - 675
CSIBM1026g - 676
CSIBM1097g - 677
CSIBM1112g - 678
CSIBM1122g - 679
CSIBM1123g - 680
CSIBM1124g - 681
CSIBM1129g - 682
CSIBM1130g - 683
CSIBM1132g - 684
CSIBM1133g - 685
CSIBM1137g - 686
CSIBM1140g - 687
CSIBM1141g - 688
CSIBM1142g - 689
CSIBM1143g - 690
CSIBM1144g - 691
CSIBM1145g - 692
CSIBM1146g - 693
CSIBM1147g - 694
CSIBM1148g - 695
CSIBM1149g - 696
CSIBM1153g - 697
CSIBM1154g - 698
CSIBM1155g - 699
CSIBM1156g - 700
CSIBM1157g - 701
CSIBM1158g - 702
CSIBM1160g - 703
CSIBM1161g - 704
CSIBM1163g - 705
CSIBM1164g - 706
CSIBM1166g - 707
CSIBM1167g - 708
CSIBM1364g - 709
CSIBM1371g - 710
CSIBM1388g - 711
CSIBM1390g - 712
CSIBM1399g - 713
CSIBM4517g - 714
CSIBM4899g - 715
CSIBM4909g - 716
CSIBM4971g - 717
CSIBM5347g - 718
CSIBM9030g - 719
CSIBM9066g - 720
CSIBM9448g - 721
CSIBM12712g - 722
CSIBM16804g - 723
CSIBM11621162g - 724
CSISO4UNITEDKINGDOMg? - 725
CSISO10SWEDISHg? - 726
CSISO11SWEDISHFORNAMESg? - 727
CSISO15ITALIANg? - 728
CSISO16PORTUGESEg? - 729
CSISO17SPANISHg? - 730
CSISO18GREEK7OLDg? - 731
CSISO19LATINGREEKg? - 732
CSISO21GERMANg? - 733
CSISO25FRENCHg? - 734
CSISO27LATINGREEK1g? - 735
CSISO49INISg? - 736
CSISO50INIS8g? - 737
CSISO51INISCYRILLICg? - 738
CSISO58GB1988g? - 739
CSISO60DANISHNORWEGIANg? - 740
CSISO60NORWEGIAN1g? - 741
CSISO61NORWEGIAN2g? - 742
CSISO69FRENCHg? - 743
CSISO84PORTUGUESE2g? - 744
CSISO85SPANISH2g? - 745
CSISO86HUNGARIANg? - 746
CSISO88GREEK7g? - 747
CSISO89ASMO449g? - 748
CSISO90g - 749

CSISO92JISC62991984Bg? - 750
CSISO99NAPLPSg? - 751
CSISO103T618BITg? - 752
CSISO111ECMACYRILLICg? - 753
CSISO121CANADIAN1g? - 754
CSISO122CANADIAN2g? - 755
CSISO139CSN369103g? - 756
CSISO141JUSIB1002g? - 757
CSISO143IECP271g? - 758
CSISO150g - 759
CSISO150GREEKCCITTg? - 760
CSISO151CUBAg? - 761
CSISO153GOST1976874g? - 762
CSISO646DANISHg? - 763
CSISO2022CNg? - 764
CSISO2022JPg? - 765
CSISO2022JP2g? - 766
CSISO2022KRg? - 767
CSISO2033g - 768
CSISO5427CYRILLICg? - 769
CSISO5427CYRILLIC1981g? - 770
CSISO5428GREEKg? - 771
CSISO10367BOXg? - 772
CSKSC5636g - 773
CSNATSDANOg - 774
CSNATSSEFIg - 775
CSN_369103g - 776
CSPC8CODEPAGE437g? - 777
CSPC775BALTICg? - 778
CSPCP852g - 779
CSSHIFTJISg - 780
CSUCS4g - 781
CSWINDOWS31Jg? - 782
CUBAg - 783
CWI-2g - 784
CWIg - 785
DEg - 786
DEC-MCSg - 787
DECg - 788
DECMCSg - 789
DIN_66003g - 790
DKg - 791
DS2089g - 792
DS_2089g - 793
E13Bg? - 794
EBCDIC-AT-DE-Ag - 795
EBCDIC-AT-DEg - 796
EBCDIC-BEg - 797
EBCDIC-BRg - 798
EBCDIC-CA-FRg - 799
EBCDIC-CP-AR1g - 800
EBCDIC-CP-AR2g - 801
EBCDIC-CP-BEg - 802
EBCDIC-CP-CAg - 803
EBCDIC-CP-CHg - 804
EBCDIC-CP-DKg - 805
EBCDIC-CP-ESg - 806
EBCDIC-CP-FIg - 807
EBCDIC-CP-FRg - 808
EBCDIC-CP-GBg - 809
EBCDIC-CP-GRg - 810
EBCDIC-CP-HEg - 811
EBCDIC-CP-ISg - 812
EBCDIC-CP-ITg - 813
EBCDIC-CP-NLg - 814
EBCDIC-CP-NOg - 815
EBCDIC-CP-ROECEg - 816
EBCDIC-CP-SEg - 817
EBCDIC-CP-TRg - 818
EBCDIC-CP-USg - 819
EBCDIC-CP-WTg - 820
EBCDIC-CP-YUg - 821
EBCDIC-CYRILLICg - 822
EBCDIC-DK-NO-Ag - 823
EBCDIC-DK-NOg - 824
EBCDIC-ES-Ag - 825
EBCDIC-ES-Sg - 826
EBCDIC-ESg - 827
EBCDIC-FI-SE-Ag - 828
EBCDIC-FI-SEg - 829

EBCDIC-FRg - 830
EBCDIC-GREEKg - 831
EBCDIC-INTg - 832
EBCDIC-INT1g - 833
EBCDIC-IS-FRISSg - 834
EBCDIC-ITg - 835
EBCDIC-JP-Eg - 836
EBCDIC-JP-KANAg - 837
EBCDIC-PTg - 838
EBCDIC-UKg - 839
EBCDIC-USg - 840
EBCDICATDEg - 841
EBCDICATDEAg - 842
EBCDICCAFRg - 843
EBCDICDKNOg - 844
EBCDICDKNOAg - 845
EBCDICESg - 846
EBCDICESAg - 847
EBCDICESSg - 848
EBCDICFISEg - 849
EBCDICFISEAg - 850
EBCDICFRg - 851
EBCDICISFRISSg - 852
EBCDICITg - 853
EBCDICPTg - 854
EBCDICUKg - 855
EBCDICUSg - 856
ECMA-128g - 857
ECMA-CYRILLICg - 858
ECMACYRILLICg - 859
ESg - 860
ES2g - 861
EUC-CNg - 862
EUC-JISX0213g - 863
EUC-JP-MSg - 864
EUC-JPg - 865
EUC-KRg - 866
EUC-TWg - 867
EUCCNg - 868
EUCJP-MSg - 869
EUCJP-OPENg - 870
EUCJP-WINg - 871
EUCJPg - 872
EUCKRg - 873
EUCTWg - 874
FIg - 875
FRg - 876
GBg - 877
GB2312g - 878
GB13000g - 879
GB18030g - 880
GBKg - 881
GB_1988-80g - 882
GB_198880g - 883
GOST_19768-74g - 884
GOST_19768g - 885
GOST_1976874g - 886
GREEK-CCITTg - 887
GREEK7-OLDg - 888
GREEK7g - 889
GREEK7OLDg? - 890
GREEKCCITTg - 891
HUg - 892
IBM-803g - 893
IBM-856g - 894
IBM-901g - 895
IBM-902g - 896
IBM-921g - 897
IBM-922g - 898
IBM-930g - 899
IBM-932g - 900
IBM-933g - 901
IBM-935g - 902
IBM-937g - 903
IBM-939g - 904
IBM-943g - 905
IBM-1008g - 906
IBM-1025g - 907
IBM-1046g - 908
IBM-1047g - 909

IBM-1097g - 910
IBM-1112g - 911
IBM-1122g - 912
IBM-1123g - 913
IBM-1124g - 914
IBM-1129g - 915
IBM-1130g - 916
IBM-1132g - 917
IBM-1133g - 918
IBM-1137g - 919
IBM-1140g - 920
IBM-1141g - 921
IBM-1142g - 922
IBM-1143g - 923
IBM-1144g - 924
IBM-1145g - 925
IBM-1146g - 926
IBM-1147g - 927
IBM-1148g - 928
IBM-1149g - 929
IBM-1153g - 930
IBM-1154g - 931
IBM-1155g - 932
IBM-1156g - 933
IBM-1157g - 934
IBM-1158g - 935
IBM-1160g - 936
IBM-1161g - 937
IBM-1162g - 938
IBM-1163g - 939
IBM-1164g - 940
IBM-1166g - 941
IBM-1167g - 942
IBM-1364g - 943
IBM-1371g - 944
IBM-1388g - 945
IBM-1390g - 946
IBM-1399g - 947
IBM-4517g - 948
IBM-4899g - 949
IBM-4909g - 950
IBM-4971g - 951
IBM-5347g - 952
IBM-9030g - 953
IBM-9066g - 954
IBM-9448g - 955
IBM-12712g - 956
IBM-16804g - 957
IBM037g - 958
IBM038g - 959
IBM256g - 960
IBM273g - 961
IBM274g - 962
IBM275g - 963
IBM277g - 964
IBM278g - 965
IBM280g - 966
IBM281g - 967
IBM284g - 968
IBM285g - 969
IBM290g - 970
IBM297g - 971
IBM420g - 972
IBM423g - 973
IBM424g - 974
IBM437g - 975
IBM500g - 976
IBM775g - 977
IBM803g - 978
IBM813g - 979
IBM848g - 980
IBM851g - 981
IBM852g - 982
IBM855g - 983
IBM856g - 984
IBM857g - 985
IBM860g - 986
IBM861g - 987
IBM863g - 988
IBM864g - 989

IBM865g - 990
IBM866NAVg? - 991
IBM868g - 992
IBM869g - 993
IBM870g - 994
IBM871g - 995
IBM874g - 996
IBM875g - 997
IBM880g - 998
IBM891g - 999
IBM901g - 1000
IBM902g - 1001
IBM903g - 1002
IBM904g - 1003
IBM905g - 1004
IBM912g - 1005
IBM915g - 1006
IBM916g - 1007
IBM918g - 1008
IBM920g - 1009
IBM921g - 1010
IBM922g - 1011
IBM930g - 1012
IBM932g - 1013
IBM933g - 1014
IBM935g - 1015
IBM937g - 1016
IBM939g - 1017
IBM943g - 1018
IBM1004g - 1019
IBM1008g - 1020
IBM1025g - 1021
IBM1026g - 1022
IBM1046g - 1023
IBM1047g - 1024
IBM1089g - 1025
IBM1097g - 1026
IBM1112g - 1027
IBM1122g - 1028
IBM1123g - 1029
IBM1124g - 1030
IBM1129g - 1031
IBM1130g - 1032
IBM1132g - 1033
IBM1133g - 1034
IBM1137g - 1035
IBM1140g - 1036
IBM1141g - 1037
IBM1142g - 1038
IBM1143g - 1039
IBM1144g - 1040
IBM1145g - 1041
IBM1146g - 1042
IBM1147g - 1043
IBM1148g - 1044
IBM1149g - 1045
IBM1153g - 1046
IBM1154g - 1047
IBM1155g - 1048
IBM1156g - 1049
IBM1157g - 1050
IBM1158g - 1051
IBM1160g - 1052
IBM1161g - 1053
IBM1162g - 1054
IBM1163g - 1055
IBM1164g - 1056
IBM1166g - 1057
IBM1167g - 1058
IBM1364g - 1059
IBM1371g - 1060
IBM1388g - 1061
IBM1390g - 1062
IBM1399g - 1063
IBM4517g - 1064
IBM4899g - 1065
IBM4909g - 1066
IBM4971g - 1067
IBM5347g - 1068
IBM9030g - 1069

IBM9066g - 1070
IBM9448g - 1071
IBM12712g - 1072
IBM16804g - 1073
IEC_P27-1g - 1074
IEC_P271g - 1075
INIS-8g - 1076
INIS-CYRILLICg - 1077
INISg - 1078
INIS8g - 1079
INISCYRILLICg - 1080
ISIRI-3342g - 1081
ISIRI3342g - 1082
ISO-2022-CN-EXTg - 1083
ISO-2022-CNg - 1084
ISO-2022-JP-2g - 1085
ISO-2022-JP-3g - 1086
ISO-2022-JPg - 1087
ISO-2022-KRg - 1088
ISO-8859-9g - 1089
ISO-8859-10g - 1090
ISO-8859-11g - 1091
ISO-8859-16g - 1092
ISO-10646g - 1093
ISO-10646/UTF-8/ - 1094
ISO-10646/UTF8/ - 1095
ISO-IR-4g - 1096
ISO-IR-8-1g - 1097
ISO-IR-9-1g - 1098
ISO-IR-10g - 1099
ISO-IR-11g - 1100
ISO-IR-15g - 1101
ISO-IR-16g - 1102
ISO-IR-17g - 1103
ISO-IR-18g - 1104
ISO-IR-19g - 1105
ISO-IR-21g - 1106
ISO-IR-25g - 1107
ISO-IR-27g - 1108
ISO-IR-37g - 1109
ISO-IR-49g - 1110
ISO-IR-50g - 1111
ISO-IR-51g - 1112
ISO-IR-54g - 1113
ISO-IR-55g - 1114
ISO-IR-57g - 1115
ISO-IR-60g - 1116
ISO-IR-61g - 1117
ISO-IR-69g - 1118
ISO-IR-84g - 1119
ISO-IR-85g - 1120
ISO-IR-86g - 1121
ISO-IR-88g - 1122
ISO-IR-89g - 1123
ISO-IR-90g - 1124
ISO-IR-92g - 1125
ISO-IR-98g - 1126
ISO-IR-99g - 1127
ISO-IR-103g - 1128
ISO-IR-111g - 1129
ISO-IR-121g - 1130
ISO-IR-122g - 1131
ISO-IR-127g - 1132
ISO-IR-139g - 1133
ISO-IR-141g - 1134
ISO-IR-143g - 1135
ISO-IR-150g - 1136
ISO-IR-151g - 1137
ISO-IR-153g - 1138
ISO-IR-155g - 1139
ISO-IR-156g - 1140
ISO-IR-166g - 1141
ISO-IR-193g - 1142
ISO-IR-197g - 1143
ISO-IR-209g - 1144
ISO/TR_11548-1/ - 1145
ISO646-CAg - 1146
ISO646-CA2g - 1147
ISO646-CNg - 1148
ISO646-CUg - 1149

ISO646-DEg - 1150
ISO646-DKg - 1151
ISO646-ESg - 1152
ISO646-ES2g - 1153
ISO646-FIg - 1154
ISO646-FRg - 1155
ISO646-FR1g - 1156
ISO646-GBg - 1157
ISO646-HUg - 1158
ISO646-ITg - 1159
ISO646-JP-OCR-Bg - 1160
ISO646-KRg - 1161
ISO646-NOg - 1162
ISO646-NO2g - 1163
ISO646-PTg - 1164
ISO646-PT2g - 1165
ISO646-SEg - 1166
ISO646-SE2g - 1167
ISO646-YUg - 1168
ISO2022CNg? - 1169
ISO2022CNEXTg? - 1170
ISO2022JPg? - 1171
ISO2022JP2g? - 1172
ISO2022KRg? - 1173
ISO6937g - 1174
ISO8859-11g - 1175
ISO11548-1g - 1176
ISO88591g - 1177
ISO88592g - 1178
ISO88593g - 1179
ISO88594g - 1180
ISO88595g - 1181
ISO88596g - 1182
ISO88597g - 1183
ISO88598g - 1184
ISO88599g - 1185
ISO885910g - 1186
ISO885911g - 1187
ISO885913g - 1188
ISO885914g - 1189
ISO885915g - 1190
ISO885916g - 1191
ISO_2033-1983g - 1192
ISO_2033g - 1193
ISO_5427-EXTg - 1194
ISO_5427g - 1195
ISO_5427:1981g - 1196
ISO_5427EXTg - 1197
ISO_5428g - 1198
ISO_5428:1980g - 1199
ISO_6937-2g - 1200
ISO_6937-2:1983g - 1201
ISO_6937g - 1202
ISO_6937:1992g - 1203
ISO_8859-7:2003g - 1204
ISO_8859-16:2001g - 1205
ISO_9036g - 1206
ISO_10367-BOXg - 1207
ISO_10367BOXg - 1208
ISO_11548-1g - 1209
ISO_69372g - 1210
ITg - 1211
JIS_C6229-1984-Bg - 1212
JIS_C62201969ROg - 1213
JIS_C62291984Bg - 1214
JOHABg - 1215
JP-OCR-Bg - 1216
JSg - 1217
JUS_I.B1.002g - 1218
KOI-7g - 1219
KOI-8g - 1220
KOI8g - 1221
KSC5636g - 1222
L10g - 1223
LATIN-9g - 1224
LATIN-GREEK-1g - 1225
LATIN-GREEKg - 1226
LATIN10g - 1227
LATINGREEKg - 1228
LATINGREEK1g - 1229

MAC-CYRILLICg - 1230
MAC-ISg - 1231
MAC-SAMIg - 1232
MAC-UKg - 1233
MACCYRILLICg - 1234
MIKg - 1235
MS-MAC-CYRILLICg - 1236
MS932g - 1237
MS936g - 1238
MSCP949g - 1239
MSCP1361g - 1240
MSMACCYRILLICg - 1241
MSZ_7795.3g - 1242
MS_KANJIg - 1243
NAPLPSg - 1244
NATS-DANOg - 1245
NATS-SEFIg - 1246
NATSDANOg - 1247
NATSSEFIg - 1248
NC_NC0010g - 1249
NC_NC00-10g - 1250
NC_NC00-10:81g - 1251
NF_Z_62-010g - 1252
NF_Z_62-010_(1973)g - 1253
NF_Z_62-010_1973g - 1254
NF_Z_62010g - 1255
NF_Z_62010_1973g - 1256
NOg - 1257
NO2g - 1258
NS_4551-1g - 1259
NS_4551-2g - 1260
NS_45511g - 1261
NS_45512g - 1262
OS2LATIN1g? - 1263
OSF00010001g - 1264
OSF00010002g - 1265
OSF00010003g - 1266
OSF00010004g - 1267
OSF00010005g - 1268
OSF00010006g - 1269
OSF00010007g - 1270
OSF00010008g - 1271
OSF00010009g - 1272
OSF0001000Ag? - 1273
OSF00010020g - 1274
OSF00010100g - 1275
OSF00010101g - 1276
OSF00010102g - 1277
OSF00010104g - 1278
OSF00010105g - 1279
OSF00010106g - 1280
OSF00030010g - 1281
OSF0004000Ag? - 1282
OSF0005000Ag? - 1283
OSF05010001g - 1284
OSF100201A4g? - 1285
OSF100201A8g? - 1286
OSF100201B5g? - 1287
OSF100201F4g? - 1288
OSF100203B5g? - 1289
OSF1002011Cg? - 1290
OSF1002011Dg? - 1291
OSF1002035Dg? - 1292
OSF1002035Eg? - 1293
OSF1002035Fg? - 1294
OSF1002036Bg? - 1295
OSF1002037Bg? - 1296
OSF10010001g - 1297
OSF10020025g - 1298
OSF10020111g - 1299
OSF10020115g - 1300
OSF10020116g - 1301
OSF10020118g - 1302
OSF10020122g - 1303
OSF10020129g - 1304
OSF10020352g - 1305
OSF10020354g - 1306
OSF10020357g - 1307
OSF10020359g - 1308
OSF10020360g - 1309

OSF10020364g - 1310
OSF10020365g - 1311
OSF10020366g - 1312
OSF10020367g - 1313
OSF10020370g - 1314
OSF10020387g - 1315
OSF10020388g - 1316
OSF10020396g - 1317
OSF10020402g - 1318
OSF10020417g - 1319
PTg - 1320
PT2g - 1321
PT154g - 1322
RK1048g - 1323
RUSCIIg - 1324
SEg - 1325
SE2g - 1326
SEN_850200_Bg - 1327
SEN_850200_Cg - 1328
SHIFT-JISg - 1329
SHIFT_JISg - 1330
SHIFT_JISX0213g - 1331
SJIS-OPENg - 1332
SJIS-WINg - 1333
SJISg - 1334
SS636127g - 1335
STRK1048-2002g - 1336
ST_SEV_358-88g - 1337
T.61-8BITg - 1338
T.61g - 1339
T.618BITg - 1340
TS-5881g - 1341
UHCg - 1342
UJISg - 1343
UKg - 1344
UTF8g - 1345
UTF16g - 1346
UTF16BEg? - 1347
UTF16LEg? - 1348
UTF32g - 1349
UTF32BEg? - 1350
UTF32LEg? - 1351
WCHAR_Tg - 1352
WIN-SAMI-2g - 1353
WINDOWS-31Jg - 1354
WINDOWS-936g - 1355
WINSAMI2g - 1356
WS2g - 1357
YUg - 1358

親トピック: ポリシー

相関アラート

アラートは、例外またはポリシー・ルール違反が検出されたことを示すメッセージです。

アラートは次の 2 つの方法で起動します。

- *相関アラート*は、指定期間をさかのぼってアラートしきい値が満たされたかどうかを判別する照会によって起動されます。 Guardium® 異常検出エンジンは、スケジュールに基づいて相関照会を実行します。 デフォルトでは、相関アラートはポリシー違反をログに記録しませんが、記録するように構成することもできます。
- *リアルタイム・アラート* は、セキュリティー・ポリシー・ルールにより起動されます。Guardium 検査エンジン・コンポーネントは、データベース・トラフィックをリアルタイムに収集および分析するときに、セキュリティー・ポリシーを実行します。

起動方法に関係なく、Guardium はすべてのアラートを同じ方法 (アラート情報を Guardium 内部データベースに記録する) でログに記録します。 ログに記録される情報の量およびタイプは、具体的なアラート・タイプによって異なります。 同じくスケジュールに基づいて実行される Guardium アラート機能コンポーネントでは、それぞれの新しいアラートが処理されます。 このとき、アラートごとにログに記録された情報は、以下の通知メカニズム (任意の組み合わせが可能) に渡されます。

- SMTP - SMTP (E メール発信) サーバー。 アラート機能により、標準 E メール・メッセージが、構成済み SMTP サーバーに渡されます。
- SNMP - SNMP (ネットワーク情報および制御) サーバー。 アラート通知用に SNMP を選択すると、アラート機能により、そのタイプのすべてのアラート・メッセージは、アラート機能が構成されている単一のトラップ・コミュニティーに渡されます。
- Syslog - アラートは Guardium アプライアンスの syslog に 書き込まれます (Guardium 管理者は、syslog メッセージをリモート・システムに書き込むようにこのアプライアンスを構成することもできます)。
  注: SNMP または SYSLOG では、最大メッセージ長は 3000 文字です。 それを超える長さのメッセージは切り捨てられます。
- カスタム - ユーザーがアラート処理のために作成した Java™ クラス。 アラート機能により、アラート・メッセージとタイム・スタンプは、カスタム・アラート・クラスに渡されます。 複数のカスタム・アラート・クラスが存在する場合があり、あるカスタム・アラート・クラスが別のカスタム・アラート・クラスの拡張である場合もあります。

注: アラート定義および通知は、データ・レベル・セキュリティーの影響を受けません。その理由として、アラートがユーザーとの関連で評価されないことや、アラートが複数のユーザーに関連付けられたデータベースに関連している可能性があり、そのアラート通知の受信者が 1 人もいないという状態を回避するためなどが挙げられま

す。
注: カウンターを含めて 30 以上のフィールドのある照会を使用するアラートがあると、配列境界外の例外 (Array out of bound exception) エラー・メッセージが出され、異常検出は失敗に終わります。アラートには、30 以上の列を持つ照会を使用できません。そのような照会は、しきい値アラートに使用可能な照会のリストに表示されません。

管理者用のアラート・タスク

Guardium 管理者は、以下のタスクを実行します。

- 「グローバル・プロファイル」を使用して、アラート・メッセージ・テンプレートをカスタマイズします。
- 「アラート機能」を構成し、開始します。そうすることにより、メッセージが SMTP、SNMP、Syslog、またはカスタム・アラート・クラスに送信されます。
- 定義されたスケジュールに従って相関アラートを実行する異常検出エンジンを開始および停止します。
- カスタム・アラート・クラスを Guardium システムにアップロードします。

ユーザー用のアラート・タスク

Guardium ユーザー (および管理者) は、以下の相関アラート・タスクを実行できます。

- 相関アラートに使用可能な照会を定義します。
- 相関アラートを定義します。
- カスタム・アラート・クラスを作成します。

相関アラート照会について

相関アラートは、いずれかのレポート・ドメインの照会に基づいています。 その照会は、アラートを定義する前に定義しておく必要があります。 照会には、少なくとも 1 つの日付フィールドが含まれていないと、相関アラートで使用できません。

相関アラートの作成

1. 「保護」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックして「アラート・ファインダー」を開きます。
2. 「アラート・ファインダー」パネルで「新規」をクリックして、「アラートの追加」パネルを表示します。
3. 「名前」ボックスに、アラートの固有の名前を入力します。 アラート名にはアポストロフィ文字を含めないでください。
4. 「記述」ボックスに、アラートについて説明する短い文を入力します。
5. 「カテゴリー」ボックスに、オプションでカテゴリーを入力します。
6. 「分類」ボックスに、オプションで分類を入力します。
7. 「推奨アクション」には、特定のアラートに対する推奨アクションとしてのフリー・テキストをユーザーが追加できます。
8. リアルタイム・アラートの場合と同様に、ユーザーは、しきい値アラートが起動した場合に送信されるメッセージのテンプレートを選択できます。このテンプレートでは、特定のアラート用に適切な値に置換される変数の定義済みリストが使用されます。デフォルト・テンプレートおよび変数のリストについては、『グローバル・プロファイル』ヘルプ・トピックにある『名前付きテンプレート』セクションで詳細を説明しています。
9. 「重大度」リストから重大度レベルを選択します。 E メール・アラートで「高」を設定すると、E メールに「高」のフラグが付きます。
10. 照会の実行間隔を「実行頻度」フィールドに分単位で入力します。
11. 「アクティブ」ボックスにマークを付けるとアラートはアクティブになり、ボックスをクリアすると実行を開始せずにアラート定義が保存されます (後ほどアクティブにできます)。 中央マネージャー環境では、このボックスにマークを付けるとすべての管理対象ユニットでアラートがアクティブになり、 クリアするとアラートが停止します。 中央マネージャー環境の特定のアプライアンスでアラートを無効にするには、「管理者コンソール」の「異常検出」パネルを使用します。
12. このアラートの起動時にポリシー違反をログに記録する場合、「ポリシー違反をロギング」ボックスにマークを付けます。デフォルトでは、相関アラートは「アラートのトラッキング」ドメインにのみ記録されます。 このボックスにマークを付けると、相関アラートおよびリアルタイム・アラート (データ・アクセス・セキュリティー・ポリシーから発行される) を「ポリシー違反」ドメインに一緒に表示できます。
13. 「アラート定義」パネルの「照会」リストから、このアラートのために実行する照会を選択します。 表示される照会のリストには、次のことが定義された照会がすべて含まれます。
    - 少なくとも 1 つの日付フィールド (タイム・スタンプ) を含んでいる (タイム・スタンプ・フィールドは必須)
    - 1 つのカウント・フィールドを含んでいる (カウント・フィールドは必須)
    - ご使用の Guardium ユーザー・アカウントでアクセスできる

    トラブルシューティングのヒント
    - カスタム照会を「レポートのビルド」にあるいずれかのクエリー・ビルダーで作成したのに、照会リストに表示されていない場合は、そのカスタム照会にタイム・スタンプ (日付フィールド) があることを確認してください。
    - 「アラートの追加」画面の「アラート定義」パネルにある照会リストから照会を選択した後、その照会を編集する必要があるが、(「編集」アイコンで) 照会を編集できない場合には、クエリー・ビルダー (「ツール」 > 「レポートのビルド」) に移動して照会を編集してください。
14. 選択した照会にランタイム・パラメーターが含まれる場合、「アラート定義」ペインに「照会パラメーター」パネルが表示されます。アプリケーションに適したパラメーター値を指定してください。
15. 「集計間隔」ボックスに、時間間隔の長さ (分単位) を入力します。 照会時に、現在時刻からこの間隔をさかのぼって監査リポジトリーが検査されます (例えば、10 と入力すると、過去 10 分間のデータが検査されます)。
    注: アグリゲーターで実行されるアラートは、定義されたマージ期間内のデータのみに基づくものです。
16. アラートと共にレポート全体をログに記録するには、「全照会結果をロギング」ボックスにチェック・マークを付けます。
17. 選択した照会に数値データの列が 1 つ以上含まれる場合、それらの列の 1 つを選択してテストに使用します。 デフォルトは、最後にリストされる項目であり、照会の最後の列になります。これは常に、その行に統合されたオカレンス数になります。
18. 「アラートしきい値」ペインで、相関アラートが生成される際のしきい値を以下のように定義します。
    - 「しきい値」フィールドに、パネルの残りのフィールドの名前に従って適用されるしきい値の数値を入力します。
    - 「値が次のときにアラート」リストから、アラート生成のためのレポート値としきい値との関連付けを示す演算子 (より大きい、以上、より小さいなど) を選択します。
    - しきい値の数値をレポートの合計に適用する場合は「レポート当たり」を選択します。しきい値をレポートの 1 行に適用する場合は「行当たり」を選択します (レポートは、選択した、指定した集計時間をさかのぼって実行される照会の出力です)。

      指定した「集計間隔」の間にデータが存在しない場合には、以下のようになります。

      しきい値が「レポート当たり」である場合、間隔の値は 0 (ゼロ) であり、 しきい値条件が満たされる場合 (例えば指定される条件が「値が 1 未満のときにアラート」である場合など) にアラートが生成されます。

しきい値が「行当たり」である場合、指定した条件に関係なくアラートは生成されません (これは、出力行が存在しないためです)。

- 「絶対制限として」を選択して入力されたしきい値が絶対数であることを指定するか、 「次の期間内のパーセンテージ変化として」を選択してしきい値が「開始」および「終了」フィールドで指定した期間内における変化のパーセンテージを表すことを指定します。

  「次の期間内のパーセンテージ変化として」 オプションを選択した場合、日付ピッカー・コントロールを使用して「開始」および「終了」の日付を選択します。

  「同じ「統合期間」の次の相対時間におけるパーセンテージ変化として」を選択した場合、1 つの相対日付が入力され、 アラートによって現行期間および相対期間 (同じ間隔を使用する) の照会が実行されて、ベース期間の値のパーセンテージとして値が検査されます。
  注: 相対期間を使用する場合、アラートが検査されるたびに照会が 2 回 (現行期間について 1 回と、相対期間について 1 回) 実行されます。

19. 「通知頻度」ボックスでは、アラート条件が満たされる場合にアラート受信者が通知を受ける頻度 (分単位) を指定します。
20. 「保存」をクリックしてアラート定義を保存します。
    注: 定義が保存されるまでは、受信者やロールを割り当てたり、コメントを入力したりすることはできません。
21. 「アラート受信者」パネルで、このアラート条件が満たされる場合に通知を受けるユーザーまたはグループを、オプションで 1 つ以上指定します。 受信者を追加するには、「受信者の追加」ボタンをクリックして、「アラート受信者の選択」パネルを開きます。
    注: アラートの受信者が管理者ユーザーである場合、その管理者にアラートの送信先 E メールを割り当てる必要があります。
    注: しきい値アラートの追加の受信者は、「所有者」(データベースの所有者) です。 アラートに関連付けられた照会に、サーバー IP およびサービス名が含まれており、アラートが「行当たり」として評価される場合、受信者を「所有者」にすることができます。 その場合のアラート通知は、「アラート通知タイプ: メール、アラート・ユーザー ID: 0、アラート宛先: 所有者」でなければなりません。 リアルタイム・アラートの追加の受信者については、『ポリシー』の『アラート・アクション』を参照してください。
22. オプションで「ロール」をクリックして、アラートのロールを割り当てます。
23. オプションで「コメント」をクリックして、定義にコメントを追加します。
24. 「適用」をクリックし、完了したら「完了」をクリックします。

相関アラートの変更

1. 「保護」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックして「アラート・ファインダー」を開きます。
2. 「アラート・ファインダー」パネルで、変更する相関アラートを選択します。
3. 「変更」をクリックして、「アラートの変更」パネルを開きます。
4. 『相関アラートの作成』トピックを参照して、アラート定義に変更を加えます。
5. 「保存」をクリックします。

相関アラートの削除

1. 「保護」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックして「アラート・ファインダー」を開きます。
2. 「アラート・ファインダー」パネルで、削除する相関アラートを選択します。
3. 「削除」ボタンをクリックします。アクションの確認を求めるプロンプトが出されます。

親トピック: 保護

相関アラートを使ってイベントを通知する方法

アプリケーションのいずれかの個別ユーザーで最近 3 時間に 15 個より多い SQL エラーが存在する場合、相関アラートをトリガーします。

このタスクについて

相関アラートを使用することで、一定時間に累積されたイベントについて通知します。通常、アプリケーションでは SQL エラーが発生しません。あるアプリケーションで SQL エラーが増加している場合、SQL インジェクションが試みられている可能性があり、警戒すべき徴候です。詳しくは、オンライン・ヘルプのトピック『相関アラート』および『照会』を参照してください。

前提条件

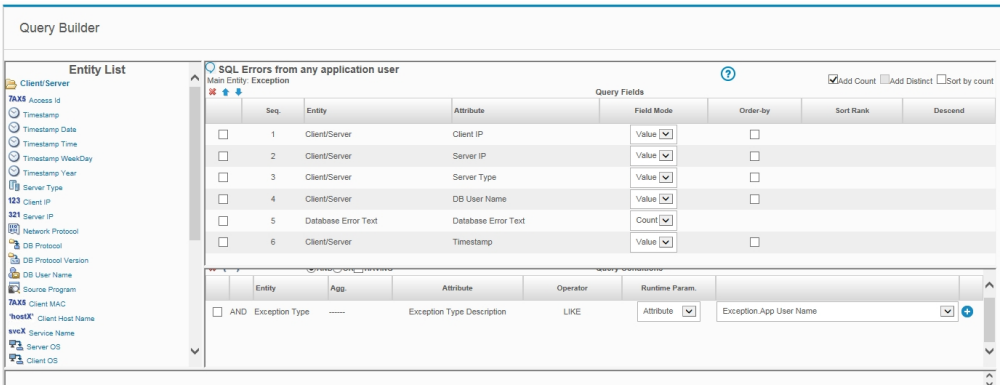
- E メール (SMTP) サーバーを構成します (「設定」 > 「ツールとビュー」 > 「アラート機能」)
- 相関アラートを完全に構成した後、それがアクティブ状態で、実行中であることを確認します (「設定」 > 「ツールとビュー」 > 「異常検出」)

アラートは、例外 (相関アラートの場合) またはポリシー・ルール違反 (リアルタイム・アラートの場合) が検出されたことを示すメッセージです。

相関アラートは、指定された期間をさかのぼって、アラートしきい値が満たされたかどうかを判別する照会によって起動されます。

相関アラートの手順の概要

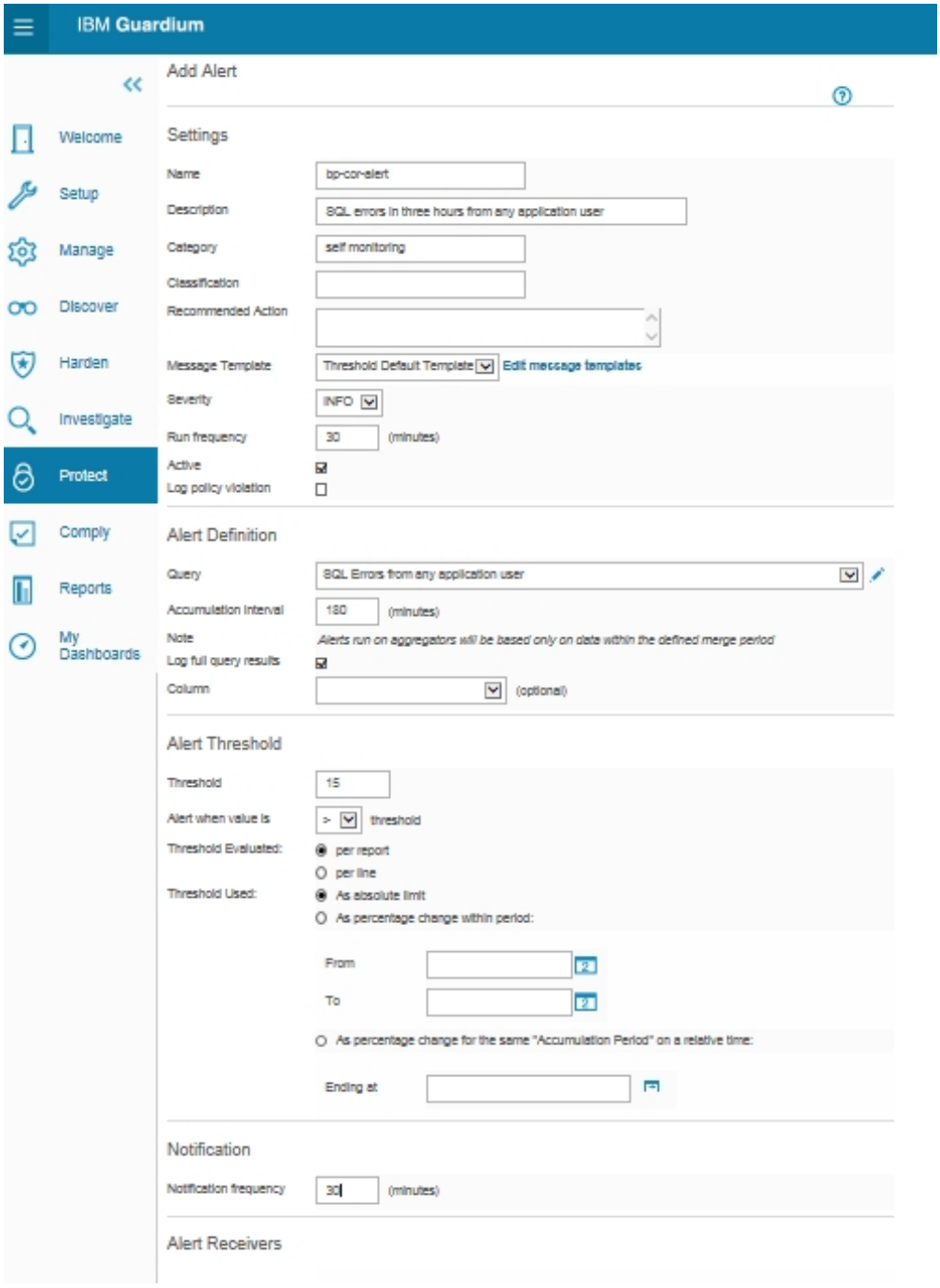
1. SQL エラーのフィールド (カウント付き) およびアプリケーション・ユーザーの条件を使用して、例外トラッキングからカスタム照会を作成します。アラート・ビルダーの中でこのカスタム照会を使用するには、日付フィールド (タイム・スタンプ) が必要です。
2. 「保護」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックして「アラート・ファインダー」を開きます。
3. 「新規」をクリックします。アラート・ビルダーのメニュー画面が表示されたら、説明に従って各フィールドに入力します。
4. 受信者を追加します。



「例外」ドメイン、SQL エラーの照会

手順

1. 例外のトラッキング - 照会ファインダーを開く
   - ユーザー:「ツール」>「レポートのビルド」を選択した後、「例外」ドメインのみを選択します。
2. 照会のドロップダウン選択項目を開きます。「SQL エラー」を選択します。SQL エラーがメイン・タイトルとなった構成画面が開きます。
3. 照会のテキスト・ボックスに固有の名前を入力して、この選択項目のコピーを作成します。照会名にはアポストロフィ文字を含めないでください。
4. カスタム照会では、照会フィールドの下で、クライアント/サーバー・エンティティー・リストから日付フィールド (タイム・スタンプ) を追加して、データベース・エラー・テキスト・フィールドをカウント・フィールド・モードに変更します。「照会条件」の下にある、例外タイプの「ランタイム・パラメーター」を「属性」に変更して、「例外: アプリケーション・ユーザー名」を選択します。
5. 「保存」をクリックします。これで、任意のアプリケーション・ユーザーからの SQL エラーに関するこのカスタム照会をアラート・ビルダーで使用できます。



アラート・ビルダーのメニュー画面

6. アラート・ビルダー - 相関アラートの作成
7. 「保護」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックして「アラート・ファインダー」を開きます。
8. 「アラート・ファインダー」パネルで「新規」ボタンをクリックして、「アラートの追加」パネルを表示します。
9. 「名前」ボックスに、アラートの固有の名前を入力します。 アラート名にはアポストロフィ文字を含めないでください。
10. 「記述」ボックスに、アラートについて説明する短い文を入力します。
11. 「カテゴリー」ボックスに、オプションでカテゴリーを入力します。この場合は自己モニターが使用されました。
12. 「分類」ボックスに、オプションで分類を入力します。
13. 「重大度」リストから重大度レベルを選択します。 E メール・アラートの場合、「高」に設定すると、E メールに緊急フラグが付けられます。
14. 照会の実行間隔を「実行頻度」フィールドに分単位で入力します。
15. 「アクティブ」ボックスにマークを付けると、アラートがアクティブになります。
16. このアラートの起動時にポリシー違反をログに記録する場合、「ポリシー違反をロギング」ボックスにマークを付けます。デフォルトでは、相関アラートは「アラートのトラッキング」ドメインにのみ記録されます。 このボックスにマークを付けると、相関アラートおよびリアルタイム・アラート (データ・アクセス・セキュリティー・ポリシーから発行される) を「ポリシー違反」ドメインに一緒に表示できます。
17. 「アラート定義」パネルの「照会」リストから、このアラートのために実行する照会を選択します。表示される照会のリストには、次のことが定義された照会がすべて含まれます。
    - 少なくとも 1 つの日付フィールド (タイム・スタンプ) を含んでいる (タイム・スタンプ・フィールドは必須)
    - 1 つのカウント・フィールドを含んでいる (カウント・フィールドは必須)
    - ご使用の Guardium® ユーザー・アカウントでアクセスできる

トラブルシューティングのヒント: カスタム照会を「レポートのビルド」にあるいずれかのクエリー・ビルダーで作成したのに、照会リストに表示されていない場合は、そのカスタム照会にタイム・スタンプ (日付フィールド) があることを確認してください。

トラブルシューティングのヒント: 「アラートの追加」画面の「アラート定義」パネルにある照会リストから照会を選択した後、その照会を編集する必要があるが、(「編集」アイコンで) 照会を編集できない場合には、クエリー・ビルダー (「ツール」>「レポートのビルド」) に移動して照会を編集してください。

18. 選択した照会にランタイム・パラメーターが含まれる場合、「アラート定義」ペインに「照会パラメーター」パネルが表示されます。アプリケーションに適したパラメーター値を指定してください。
19. 「集計間隔」ボックスに、時間間隔の長さ (分単位) を入力します。 照会時に、現在時刻からこの間隔をさかのぼって監査リポジトリーが検査されます (例えば、10 と入力すると、過去 10 分間のデータが検査されます)。
20. アラートと共にレポート全体をログに記録するには、「全照会結果をロギング」ボックスにマークを付けます。
21. 選択した照会に数値データの列が 1 つ以上含まれる場合、それらの列の 1 つを選択してテストに使用します。 デフォルトは、最後にリストされる項目であり、照会の最後の列になります。これは常に、その行に統合されたオカレンス数になります。
22. 「アラートしきい値」ペインで、相関アラートが生成される際のしきい値を以下のように定義します。
    - 「しきい値」フィールドに、パネルの残りのフィールドの名前に従って適用されるしきい値の数値を入力します。
    - 「値が次のときにアラート」リストから、アラート生成のためのレポート値としきい値との関連付けを示す演算子 (より大きい、以上、より小さいなど) を選択します。
    - しきい値の数値がレポート総計に適用される場合は、「レポートごと」を選択します。

    指定された「集計間隔」においてデータが存在しない場合: しきい値がレポートごとである場合、その間隔における値は 0 (ゼロ) であり、しきい値条件が満たされるならアラートが生成されます (例えば「値が次のときにアラート通知: < 1」という条件が指定されている場合)。
23. 「通知頻度」ボックスでは、アラート条件が満たされる場合にアラート受信者が通知を受ける頻度 (分単位) を指定します。
24. 「適用」ボタンをクリックして、アラート定義を保存します。
    注: 定義が保存されるまでは、受信者やロールを割り当てたり、コメントを入力したりすることはできません。
25. 「アラート受信者」パネルで、このアラート条件が満たされる場合に通知を受けるユーザーまたはグループを、オプションで 1 つ以上指定します。 受信者を追加するには、「受信者の追加」ボタンをクリックして、「アラート受信者の選択」パネルを開きます。 受信者の追加について詳しくは、『通知』を参照してください。
26. オプションで「ロール」ボタンをクリックして、アラートのロールを割り当てます。『セキュリティー・ロール』を参照してください。
27. オプションで「コメント」ボタンをクリックして、定義にコメントを追加します。
28. 完了したら、「適用」ボタン、「完了」ボタンの順にクリックします。

    いずれかのアプリケーション・ユーザーで最近 3 時間に 15 個より多い SQL エラーが存在する場合、指定された受信者にアラートが送信されます。

親トピック: 保護

インシデント管理

統合インシデント管理 (IIM) アプリケーションには、 データベースのセキュリティー・インシデントをトラッキングして解決するワークフロー自動化機能を備えたビジネス・ユーザー・インターフェースがあります。

このインターフェースでは、一連の関連するポリシー違反をグループにして 1 つのインシデントとし、 特定の個人に割り当てることを管理者に可能にすることで、インシデント管理を簡略化します。 これにより、監視チームによるレビューが必要なポリシー違反の数が減らせます。

インシデントの生成プロセスを定義してスケジュールすることで、ポリシー違反ログの読み取りや、新規インシデントの生成が行えます。 インシデントの生成プロセスでは、選択される各インシデントは次のようになります。

- 固有のインシデント番号が割り当てられる。
- ユーザーに割り当てられる。
- 重大度コードが割り当てられる。
- カテゴリーに割り当てられる。

さらに、ポリシー違反は、「ポリシー違反/インシデント管理」レポートから (権限を持つユーザーが) 手動で新規インシデントまたは既存のインシデントに割り当てることができます。

インシデントが生成されると、管理者および他のユーザーは、(admin ポータルとユーザー・ポータルに含まれる) 「インシデント管理」タブからインシデントを操作します。 ここからは、他のすべてのタスク (インシデントの割り当て、通知の送信、状況の割り当て、など) を実行できます。

インシデント管理機能は、「インシデント管理」レポートのドリルダウン・メニューからアクセスできます。 各ユーザーは、ユーザー・アカウントに割り当てられたセキュリティー・ロールに応じて、 レポートや機能のサブセットのみ使用できます。

インシデント管理レポートの独自のコピーを作成できますが、これらのコピーには 「インシデント管理」タブの事前構成されたレポートから使用可能なすべての機能が備わっているわけではありません。 インシデント、重大度コードなどを割り当てるには、「インシデント管理」タブのレポートを使用します。

インシデント生成プロセスの定義

インシデントの生成プロセスでは、ポリシー違反ログへの照会が実行され、 その照会に基づいてインシデントが生成されます。デフォルトでは、インシデント生成プロセスの定義およびスケジューリングは、admin ロールを持つユーザーに制限されます。

1. 「順守」>「ツールとビュー」>「インシデント生成」をクリックして、「インシデント生成プロセス」を開きます。
2. 「プロセスの追加」をクリックして、「インシデント生成プロセスの編集」パネルを開きます。
3. 「照会」リストから照会を選択します。 インシデント生成プロセスで使用される照会に適用されるいくつかの制約があります。 クエリー・ビルダーで照会を開き、次の条件が満たされていることを確認することを推奨します。
    - 照会はポリシー違反ドメインのものであること。
    - 照会の「カウントの追加」チェック・ボックスにチェックが付いていること。詳しくは、照会を参照してください。
    - 照会のメイン・エンティティーがポリシー・ルール違反エンティティーであること。
    - 照会の照会フィールドに SQL 文字列 (SQL エンティティーのもの、またはポリシー・ルール違反エンティティーの「SQL 文字列全体」属性のもの) が含まれないこと。
4. インシデントの重大度を選択します (デフォルトは「情報」)。
5. オプションで、インシデントのカテゴリーを入力します (デフォルトは「なし」)。

6. オプションで、インシデント生成のしきい値を入力します。 デフォルトは 1 で、照会で返されるすべての行がインシデントを生成します。
7. 「ユーザーに割り当て」リストから、インシデントを割り当てるユーザーを選択します。
8. 照会の開始日と終了日を入力します。 スケジュールした照会の場合、相対日付を使用します (例: 「現在 -1 日」や「現在」)。
9. 「保存」をクリックして、プロセスの定義を保存します。プロセスは、保存しないと実行またはスケジュールできません。
10. ここで照会を実行するには、「今すぐ 1 回実行」をクリックします。
11. 照会をスケジュールするには、「スケジュールの変更」をクリックして、汎用のスケジューリング・ユーティリティーを開きます。

インシデントへの割り当て/再割り当て

1. いずれかの「インシデント管理」レポートで、割り当て/再割り当てをするポリシー違反をダブルクリックします。
2. ドリルダウン・メニューから「インシデントに割り当て/再割り当て」を選択します。このメニューを選択すると、オープン・インシデント (例えば、「インシデント #123 に割り当て」) のリストと 1 つの追加オプション (「新規インシデントに割り当て」) を含む新しいメニューが表示されます。
3. この違反を割り当てるインシデントを選択するか、「新規インシデントに割り当て」を選択して次の使用可能なインシデント番号 (順に番号が付けられます) にポリシー違反を割り当てます。

   変更が完了するとメッセージが表示され、「インシデント管理」パネルが更新されます。新しいインシデントが作成されると、「オープン・インシデント」レポートの最初にリストされます。

ユーザーへの割り当て

1. いずれかの「インシデント管理」レポートで、別のユーザーに割り当てるインシデントをダブルクリックします。
2. ドリルダウン・メニューから「ユーザーに割り当て」を選択します。 このメニューを選択すると、ユーザーのリストと 1 つの追加オプション「割り当て解除」を含む新しいメニューが表示されます。
3. ユーザーを選択してインシデントに割り当てます。あるいは、「割り当て解除」を選択して現在割り当てられているユーザーを削除します。 ユーザーが割り当てられている場合「状況の記述」は割り当て済みとなり、割り当てを解除すると「状況の記述」はオープンになります。

   変更が完了するとメッセージが表示され、「インシデント管理」パネルが更新されます。

重大度の変更

1. いずれかの「インシデント管理」レポートで、重大度を変更するインシデントをダブルクリックします。
2. ドリルダウン・メニューから「重大度の変更」を選択します。 このメニューを選択すると、 重大度コード (情報、低、中、高) のリストを含む新しいメニューが表示されます。
3. 新規の重大度コードを選択します。

   変更が完了するとメッセージが表示され、「インシデント管理」パネルが更新されます。

通知

1. いずれかの「インシデント管理」レポートで、ユーザーが通知を受け取るインシデントをダブルクリックします。
2. ドリルダウン・メニューから「通知」を選択します。 このメニューを選択すると、 ユーザーのリストを含む新しいメニューが表示されます。
3. ユーザーを選択します。

   ユーザーが通知を受けるとメッセージが表示されます。

状況の変更

1. いずれかの「インシデント管理」レポートで、状況を変更するインシデントをダブルクリックします。
2. ドリルダウン・メニューから「状況の変更」を選択します。 このメニューを選択すると、 状況コードのリストを含む新しいメニューが表示されます。
   - 割り当て済み - インシデントがこの状況になると、 ポリシー違反をこれ以上追加できません。ポリシー違反を追加するには、 インシデントの状況を「オープン」に戻し、違反を追加してから状況を「割り当て済み」に戻します。
   - クローズ済み - インシデントに「クローズ済み」のマークが付くと、変更ができなくなり、 リストに含まれなくなります。
   - オープン - 新規インシデントの初期の状況です。
3. 新規の状況コードを選択します。

   変更が完了するとメッセージが表示され、「インシデント管理」パネルが更新されます。

コメントの追加

1. いずれかの「インシデント管理」レポートで、コメントを追加するインシデントをダブルクリックします。
2. ドリルダウン・メニューから「コメント」を選択して、 「ユーザー・コメント」ウィンドウを開きます。 コメントの追加方法に関する説明については、『コメント』を参照してください。

親トピック: 保護

複数のデータベース・セキュリティー・インシデントのレビュー管理方法

インシデントの管理を行い、データベースのセキュリティー・インシデントをトラッキングして解決します。

このタスクについて

管理者は、一連の関連するポリシー違反をグループにして 1 つのインシデントとし、特定の個人に割り当てることができます。これにより、監視チームによるレビューが必要なポリシー違反の数が減らせます。

前提条件

- ポリシーを作成します (『ポリシー』を参照)。
- 検査エンジンを起動します (『検査エンジン構成』を参照)。

セキュリティー・ポリシーには、データベース・クライアントとサーバーとの間の監視対象トラフィックに適用される順序付きルール・セットが含まれています。

ポリシー違反は、ルールが起動されるごとにログに記録されます。 ポリシー違反は、プロセスによって自動的に、または権限を持つユーザーによって手動でインシデントに割り当てられます (『インシデント管理』を参照してください)。

手順の要約

1. 「順守」 > 「ツールとビュー」 > 「インシデント生成」をクリックして、「インシデント生成プロセス」を開きます。
2. インシデント生成プロセス (照会、重大度、しきい値、スケジューリング) の編集。
3. 「インシデント管理」タブのレポートを参照します。

インシデント管理

インシデント管理アプリケーションには、データベースのセキュリティー・インシデントをトラッキングして解決するワークフロー自動化機能を持つビジネス・ユーザー・インターフェースがあります。

インシデントの生成プロセスを定義してスケジュールすることで、ポリシー違反ログの読み取りや、新規インシデントの生成が行えます。インシデントの生成プロセスでは、選択される各インシデントは次のようになります。

- 固有のインシデント番号が割り当てられる。
- ユーザーに割り当てられる。
- 重大度コードが割り当てられる。
- カテゴリーに割り当てられる。

さらに、ポリシー違反は、「ポリシー違反/インシデント管理」レポートから (権限を持つユーザーが) 手動で新規インシデントまたは既存のインシデントに割り当てることができます。

インシデントが生成されると、管理者および他のユーザーは、(admin ポータルとユーザー・ポータルに含まれる) 「インシデント管理」タブからインシデントを操作します。 ここからは、他のすべてのタスク (インシデントの割り当て、通知の送信、状況の割り当て、など) を実行できます。

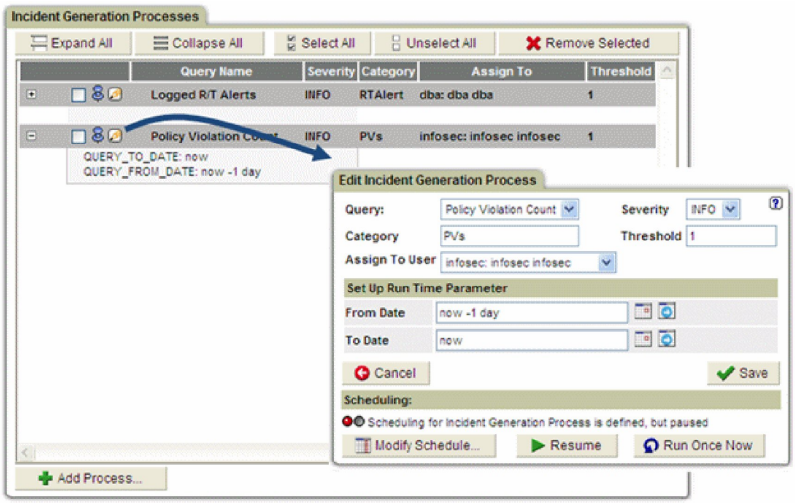
インシデント管理機能は、「インシデント管理」レポートのドリルダウン・メニューからアクセスできます。 各ユーザーは、ユーザー・アカウントに割り当てられたセキュリティー・ロールに応じて、 レポートや機能のサブセットのみ使用できます。

インシデント生成プロセスの定義

インシデントの生成プロセスでは、ポリシー違反ログへの照会が実行され、その照会に基づいてインシデントが生成されます。デフォルトでは、インシデント生成プロセスの定義およびスケジューリングは、admin ロールを持つユーザーに制限されます。

手順

1. 「順守」 > 「ツールとビュー」 > 「インシデント生成」をクリックして、「インシデント生成プロセス」を開きます。
2. 「プロセスの追加」ボタンをクリックして、「インシデント生成プロセスの編集」パネルを開きます。
3. 「照会」リストから照会を選択します。 インシデント生成プロセスで使用される照会に適用されるいくつかの制約があります。 クエリー・ビルダーで照会を開き、次の条件を満たすことを確認します。
   - 照会はポリシー違反ドメインのものであること。
   - 照会の「カウントの追加」チェック・ボックスにチェックが付いていること。 詳しくは、クエリー・ビルダーの概要 (『照会』) を参照してください。
   - 照会のメイン・エンティティーがポリシー・ルール違反エンティティーであること。
   - 照会の照会フィールドに SQL 文字列 (SQL エンティティーのもの、 またはポリシー・ルール違反エンティティーの「SQL 文字列全体」属性のもの) が含まれないこと。
4. インシデントの重大度を選択します (デフォルトは「情報」)。
5. オプションで、インシデントのカテゴリーを入力します (デフォルトは「なし」)。
6. オプションで、インシデント生成のしきい値を入力します。 デフォルトは 1 で、 照会で返されるすべての「行」がインシデントを生成します。
7. 「ユーザーに割り当て」リストから、インシデントを割り当てるユーザーを選択します。
8. 照会の開始日と終了日を入力します。 スケジュールした照会の場合、相対日付を使用します (例: 「現在 -1 日」や「現在」)。
9. 「保存」をクリックして、プロセスの定義を保存します。 プロセスは、保存しないと実行またはスケジュールできません。
10. ここで照会を実行するには、「今すぐ 1 回実行」をクリックします。
11. 照会をスケジュールするには、「スケジュールの変更」をクリックして、スケジューリング・ユーティリティーを開きます。スケジューラーの使用手順については、共通ツール・ブックの『スケジューリング』を参照してください。

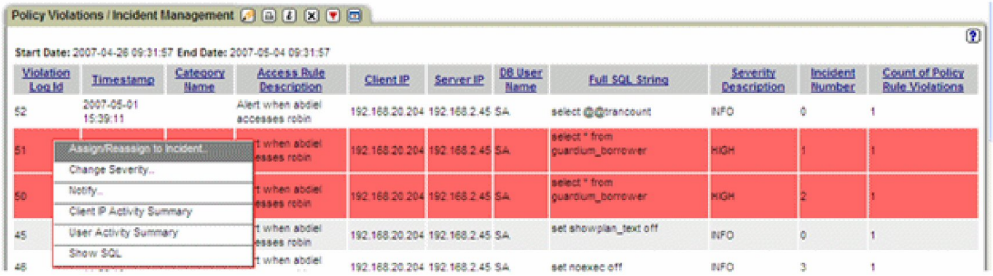


12. インシデントへの割り当て/再割り当て - いずれかの「インシデント管理」レポートで、割り当て /再割り当てを行うポリシー違反をダブルクリックします。
13. ドリルダウン・メニューから「インシデントに割り当て/再割り当て」を選択します。 このメニューを選択すると、オープン・インシデント (例えば、「インシデント #123 に割り当て」) のリストと 1 つの追加オプション (「新規インシデントに割り当て」) を含む新しいメニューが表示されます。
14. この違反を割り当てるインシデントを選択するか、「新規インシデントに割り当て」を選択して次の使用可能なインシデント番号 (順に番号が付けられます) にポリシー違反を割り当てます。

    変更が完了するとメッセージが表示され、「インシデント管理」パネルが更新されます。 新しいインシデントが作成されると、「オープン・インシデント」レポートの最初にリストされます。

    インシデントの「ポリシー違反/インシデント管理」レポートからは、以下が行えます。

    - インシデントへの割り当て/再割り当て (このポリシー違反からインシデントを作成)。
    - インシデントの重大度の変更。
    - 1 名以上のユーザーにインシデントを通知する。
    - インシデントからクライアント IP アクティビティー、ユーザー・アクティビティー、または SQL のレポートを表示する。



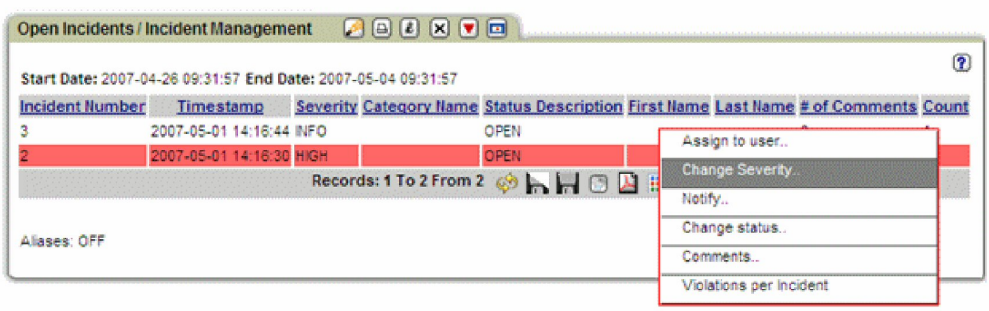
15. ユーザーに割り当てる - いずれかの「インシデント管理」レポートで、別のユーザーに割り当てるインシデントをダブルクリックします。
16. ドリルダウン・メニューから「ユーザーに割り当て」を選択します。 このメニューを選択すると、ユーザーのリストと 1 つの追加オプション「割り当て解除」を含む新しいメニューが表示されます。
17. ユーザーを選択してインシデントに割り当てます。あるいは、「割り当て解除」を選択して現在割り当てられているユーザーを削除します。 ユーザーが割り当てられている場合「状況の記述」は割り当て済みとなり、割り当てを解除すると「状況の記述」はオープンになります。

    変更が完了するとメッセージが表示され、「インシデント管理」パネルが更新されます。

18. 重大度の変更 - いずれかの「インシデント管理」レポートで、重大度を変更するインシデントをダブルクリックします。
19. ドリルダウン・メニューから「重大度の変更」を選択します。 このメニューを選択すると、 重大度コード (情報、低、中、高) のリストを含む新しいメニューが表示されます。
20. 目的の重大度コードを選択します。

    変更が完了するとメッセージが表示され、「インシデント管理」パネルが更新されます。

    ポリシー違反をインシデントに割り当てると、そのインシデントは「オープン・インシデント」レポートに表示されます。 「オープン・インシデント」レポートからは、次のようなアクションを実行できます。



21. 通知 - いずれかの「インシデント管理」レポートで、ユーザーが通知を受け取るインシデントをダブルクリックします。

22. ドリルダウン・メニューから「通知」を選択します。 このメニューを選択すると、 ユーザーのリストを含む新しいメニューが表示されます。
23. ユーザーを選択します。

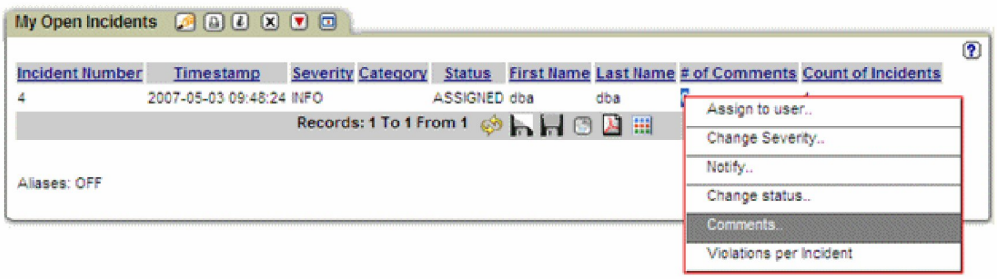
    通知が行われると、メッセージが表示されます。

24. 状況の変更 - いずれかの「インシデント管理」レポートで、状況を変更するインシデントをダブルクリックします。
25. ドリルダウン・メニューから「状況の変更」を選択します。 このメニューを選択すると、 状況コードのリストを含む新しいメニューが表示されます。
    - 割り当て済み - インシデントがこの状況になると、 ポリシー違反をこれ以上追加できません。ポリシー違反を追加するには、インシデントの状況を「オープン」に戻し、違反を追加してから状況を「割り当て済み」に戻します。
    - クローズ済み - インシデントに「クローズ済み」のマークが付くと、変更ができなくなり、 リストに含まれなくなります。
    - オープン - 新規インシデントの初期の状況です。
26. 目的の状況コードを選択します。

    変更が完了するとメッセージが表示され、「インシデント管理」パネルが更新されます。

27. コメントの追加 - いずれかの「インシデント管理」レポートで、コメントを追加するインシデントをダブルクリックします。
28. ドリルダウン・メニューから「コメント」を選択して、「ユーザー・コメント」ウィンドウを開きます。コメントの追加手順については、『コメント』を参照してください。

    ユーザー・ポータルに、それぞれそのユーザーの「マイ・オープン・インシデント」レポートが表示されます。 「マイ・オープン・インシデント」レポートからは、次のようなアクションを実行できます。



親トピック: 保護

照会再書き込み

照会再書き込み機能を使用してデータベース照会をインターセプトし、そのデータベース照会をセキュリティー・ポリシーで定義された条件に基づいて再書き込みすることにより、データベースに対するアクセス権を詳細に制御することができます。

照会の変更は、処理中に透過的に行われるため、照会を発行したユーザーが、再書き込みされた SQL ステートメントに基づく結果をシームレスに受信できます。

照会再書き込み機能は、照会の変更方法や補完方法を示す照会再書き込み定義と、その照会再書き込み定義を適用する特定の状況を示すランタイム・コンテキストを組み合わせることによって実装されます。

データベース照会に対して処理中に再書き込みを行うことで、管理者は、以下の例に示すいくつかのタイプのアクセス制御を実装できるようになります。

表 1. 照会再書き込みによるアクセス制御の例

アクセス制御	元の SQL	再書き込み後の SQL
WHERE 節を追加して行へのアクセスを制限する	`SELECT C from T`	`SELECT C from T WHERE [values]`
SELECT リストを変更して列へのアクセスを制限する	`SELECT C1 from T`	`SELECT C2 from T`
	`SELECT C1,C2 from T`	`SELECT C2 from T`
SQL ステートメントに再書き込みして何もしないようにすることで、データベース・アクティビティーを制限する	`SELECT EMAIL from T`	`SELECT++ EMAIL from T`
照会 verb (SELECT、INSERT、UPDATE など) を変更して、ユーザーが実行できる操作を制限する	`DROP TABLE T`	`UPDATE T SET [values]`
照会オブジェクト (TABLE、VIEW、COLUMN など) を変更して、ユーザーが実行できる操作を制限する	`SELECT C from T1`	`SELECT C from T2`

データベース照会の再書き込みをシームレスに実行できることにより、非常に強力かつ柔軟性の高い方法でアクセス制御を適用できるため、組織はセキュリティーについてのさまざまな懸念に迅速に対応できます。例えば、照会再書き込み定義を作成することで、以下の対策を実施することができます。

- 複数のユーザーおよびアプリケーションが単一のデータベースを共有するが、すべてのユーザーおよびアプリケーションにすべてのデータへのアクセス権限を与えるわけではないマルチテナンシー・シナリオで、セキュリティーを適用する
- データベース全体を公開せずに、テスト目的でデータベースを実稼働環境に公開する
- 脆弱性に対するデータベース・レベルまたはアプリケーション・レベルの永続的な解決策を考案している間に、重大なセキュリティー上の脆弱性を直ちに修正する

以下のセクションを参照して、照会再書き込みのしくみや、Guardium 環境で照会再書き込みを使用できるように構成する方法に関する詳細情報を確認してください。

注: S-TAP が firewall_default_state=1 (照会再書き込みのデフォルト状態) に設定されている場合、qrw_default_state=1 を同時に設定することはできません。

- 照会再書き込みのしくみ
  照会再書き込み機能が Guardium でどのように実装されているかについて説明します。

- 照会再書き込みの使用
  照会再書き込み機能を有効化して使用する方法について説明します。

親トピック: 保護

照会再書き込みのしくみ

照会再書き込み機能が Guardium でどのように実装されているかについて説明します。

概要

S-TAP でサポート対象データベース・サーバーに対して照会再書き込みが有効化されると (照会再書き込みの有効化参照)、以下の 3 つのポリシー・ルール・アクションを通じて照会再書き込み機能が実装されます。

- 照会再書き込み: アタッチ (QUERY REWRITE: ATTACH)
- 照会再書き込み: 定義の適用
- 照会再書き込み: デタッチ (QUERY REWRITE: DETACH)

これらのルール・アクションは、アクセス・ポリシー・ルールとしてインストールされます。これらのアクセス・ポリシー・ルールは、照会の再書き込み方法を示す照会再書き込み定義と、それらの定義がいつ適用されるのかを示すランタイム・コンテキストの両方を指定します。

照会再書き込みルールが指定されると、セッションが以下のように処理されます。

1. SQL 要求が「照会再書き込み: アタッチ (QUERY REWRITE: ATTACH)」ルールをトリガーし、セッションに含まれる以降のすべてのアクティビティーが、照会再書き込みによって監視されます。
2. 照会再書き込みによってセッションの監視が行われている間、トラフィックは S-TAP で保持され、セッション情報がアクセス・ポリシー・ルールと比較して検査されます。
3. 監視対象セッション内の照会が「照会再書き込み: 定義の適用」ルールに一致した場合、その照会は、定義に従って再書き込みが行われ、その後 S-TAP に送信されます。
4. S-TAP が再書き込みされた照会をデータベース・サーバーにリリースします。
5. 「照会再書き込み: デタッチ (QUERY REWRITE: DETACH)」ルールがトリガーされると、照会再書き込みがセッションの残りの照会に対する監視を中止するか、「照会再書き込み: アタッチ (QUERY REWRITE: ATTACH)」ルールが再度トリガーされるまで監視を中止します。

要件と制限事項

照会再書き込みは、以下のデータベース・サーバーと連動するよう意図されています。

- Oracle
- DB2 (Linux および Unix のみ)
- Microsoft SQL

サポートされるデータベース・サーバーおよび関連する制約事項については、『Platforms supported for IBM Guardium 10.1』を参照してください。照会再書き込みに対するデータベース・クライアント・サポートについて詳しくは、IBM Guardium サポートにお問い合わせください。

重要: 照会再書き込みでセッションを監視するときは、セッション内の各 SQL 要求について S-TAP にエンジンの判定を送信するために、スニファーが必要です。このプロセスは非同期で行われ、スニファーと S-TAP の間に待ち時間が発生します。パフォーマンスの影響を受けやすいアプリケーションやトラステッド・アプリケーションの場合は、セッションへのアタッチを防止する照会再書き込みのルール条件を作成してください。
親トピック: 照会再書き込み
関連タスク:
照会再書き込みの有効化

照会再書き込みの使用

照会再書き込み機能を有効化して使用する方法について説明します。

このタスクについて

照会再書き込み機能を有効化して使用を開始するには、以下のタスク・シーケンスを実行します。

1. 照会再書き込みの有効化
   照会再書き込み機能を使用できるように S-TAP を構成する方法について説明します。
2. 照会再書き込み定義の作成
   データ・マスキングやアクセス制御を行う場合に照会再書き込み定義を作成する方法について説明します。
3. 照会再書き込み定義のテスト
   サンプル入力に対して照会再書き込み定義をテストし、再書き込み定義が期待どおりに動作することを確認する方法について説明します。
4. 照会再書き込みをアクティブ化するセキュリティー・ポリシーの定義
   照会再書き込み定義を実際の照会に対して使用するアクセス・ポリシー・ルールを作成する方法について説明します。
5. 照会再書き込み結果を検証するためのカスタム・レポートの作成
   照会再書き込みアクティビティーを監査するための照会再書き込みトラッキング・レポートを作成する方法について説明します。

親トピック: 照会再書き込み

照会再書き込みの有効化

照会再書き込み機能を使用できるように S-TAP を構成する方法について説明します。

このタスクについて

照会再書き込み機能は、以下の条件がどちらも満たされている場合にのみ有効化されます。

- guard_tap.ini ファイルで照会再書き込みが有効化されている
- 照会再書き込みポリシー・ルールが存在し、セッション・トラフィックによってトリガーされる

このタスクでは、guard_tap.ini ファイルで行う必要のある変更を示します。

手順

1. guard_tap.ini をテキスト・エディターで開きます。
2. パラメーター qrw_installed = 0 を探し、これを qrw_installed = 1 に変更します。 照会再書き込み機能を有効化するには、パラメーター qrw_installed を値 1 に設定する必要があります。照会再書き込み機能を無効化するには、qrw_installed = 0 に設定してください。
3. guard_tap.ini への変更を保存します。
4. Guardium システムで、CLI ユーザーとしてログインし、restart_inspection_engines CLI コマンドを使用して検査エンジンを再始動します。

タスクの結果

このタスクが完了すると、照会再書き込み機能が有効化され、照会再書き込みアクションを含むポリシー・ルールに応答するようになります。
親トピック: 照会再書き込みの使用
次のトピック: 照会再書き込み定義の作成

照会再書き込み定義の作成

データ・マスキングやアクセス制御を行う場合に照会再書き込み定義を作成する方法について説明します。

手順

1. 「保護」 > 「セキュリティー・ポリシー」 > 「照会再書き込みビルダー」を開きます。
2. 照会再書き込み定義の分かりやすい固有の名前を「名前」フィールドに入力します。
3. モデル照会を作成して解析します。
   a. 「モデル照会を入力」フィールドにモデル照会を入力します。

      例えば、`SELECT * from` ステートメントの使用を禁止する再書き込み定義を作成するには、モデルとして `SELECT * from EMPLOYEE` と入力します。

   b. 「データベース・タイプ」メニューをクリックし、モデル照会に使用する SQL パーサーを選択します。
   c. 「解析」をクリックしてモデル照会を処理します。

      モデル照会が個別のコンポーネントに分解されます。このとき、アクション可能な各コンポーネントが下線付きテキストで強調表示されます。

4. モデル照会の特定のコンポーネントに再書き込みを行う方法を定義します。
   a. 解析された照会の下線付きコンポーネントのうち、再書き込みを行うコンポーネントをクリックします。照会再書き込み定義を作成できるようにするためのダイアログが開きます。

      オプション:

      - 解析された照会の個別の verb、フィールド、またはオブジェクトを選択して変更します
      - 照会にコンポーネントを追加します (解析された照会の横にグレーの下線付きテキストとして表示されます)
      - 解析された照会の横にあるグレーの下線付きの [R] をクリックして、照会全体を書き換えます

      `SELECT * from EMPLOYEE` の例 (`SELECT * from` ステートメントの使用を禁止する) では、「*」をクリックして再書き込み内容を指定します。

   a. 「変更前:」フィールドは再書き込みの対象を示します。
   b. 「終了」フィールドは再書き込み後のコンポーネントを定義します。

      例えば、`SELECT * from` ステートメントの使用を禁止するには、`*` コンポーネントを特定オブジェクトのリスト (`EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX`) に置き換えます。

      重要:

      再書き込み定義は構文に基づいているため、`SELECT * from [OBJECT]` という形式のすべてのステートメントが例に一致します。例えば、`SELECT * from DEPARTMENT` というステートメントと `SELECT * from EMPLOYEE` というステートメントは、どちらも上記の例に一致します。

      照会再書き込み定義を特定のオブジェクトに制限するには、アクセス・ポリシー・ルールを使用します。その方法については、照会再書き込みをアクティブ化するセキュリティー・ポリシーの定義を参照してください。

   c. 「保存」をクリックして再書き込み定義を保存し、次に「戻る」をクリックしてダイアログを閉じます。
5. 「リアルタイム・プレビュー」フィールドを使用して照会再書き込み定義の出力を確認し、必要に応じて変更を加えます。

   上記の例では、`SELECT * from EMPLOYEE` が `SELECT EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from EMPLOYEE` として再書き込みされます。

6. 結果に問題がなければ、「保存」をクリックして照会再書き込み定義を保存します。

   照会再書き込み定義が保存され、「照会再書き込みビルダー」の使用可能な照会再書き込み定義のリストに表示されます。

次のタスク

照会再書き込み定義の操作を続けます。

- 追加の定義を作成するには、「新規」をクリックして、このタスクの手順を繰り返します。
- 既存の照会再書き込み定義を編集するには、使用可能な照会再書き込み定義のリスト内の項目をダブルクリックします。
- 既存の照会再書き込み定義をコピーして編集するには、使用可能な照会再書き込み定義のリスト内の項目を選択し、「コピー」をクリックします。
- 既存の照会再書き込み定義を削除するには、使用可能な照会再書き込み定義のリスト内の項目を選択し、「削除」をクリックします。

照会再書き込み定義の操作が完了したら、以下のシーケンスの次の手順に進んで、定義のテストと実装を行います。
親トピック: 照会再書き込みの使用
前のトピック: 照会再書き込みの有効化
次のトピック: 照会再書き込み定義のテスト
関連タスク:
照会再書き込みをアクティブ化するセキュリティー・ポリシーの定義

照会再書き込み定義のテスト

サンプル入力に対して照会再書き込み定義をテストし、再書き込み定義が期待どおりに動作することを確認する方法について説明します。

始める前に

このタスクを実行するには、1 つ以上の照会再書き込み定義が作成されている必要があります。

手順

1. 「保護」 > 「セキュリティー・ポリシー」 > 「照会再書き込みビルダー」を開きます。
2. 「テストのセットアップ」をクリックしてダイアログを開き、テストする照会再書き込み定義を選択します。
   a. 「使用可能な照会再書き込み定義」フィールドから「照会再書き込み定義のテスト」フィールドに項目をドラッグ・アンド・ドロップします。
   b. 「照会再書き込み定義のテスト」フィールドで項目をドラッグ・アンド・ドロップして、複数の定義をアクセス・ポリシーと同様に並べ替えます。
   c. 完了したら、「保存」をクリックしてダイアログを閉じます。
3. 「テスト」フィールドにテスト照会を入力するか貼り付けます。

   例えば、`SELECT * from` ステートメントの使用を禁止する再書き込み定義 (照会再書き込み定義の作成を参照) をテストするには、以下のようなサンプル照会を入力します。

```
SELECT * from DEPARTMENT
SELECT * from EMPLOYEE
SELECT FIRSTNME, case
when SALARY > 150000 then 'high'
when SALARY > 100000 then 'medium'
when SALARY > 80000 then 'fair'
else 'poor'
end from EMPLOYEE
DELETE from EMPLOYEE where EMPNO=100
INSERT into TEMP_EMP SELECT * from EMPLOYEE
```

4. 「テストの実行」をクリックしてサンプル照会を処理し、結果を確認します。

   例えば、前のステップで示したサンプル照会をテストすると、以下の結果が返されます。

表 1. 照会再書き込みのテスト結果

元の SQL	再書き込み後の SQL	変更
`SELECT * from DEPARTMENT`	`SELECT EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from DEPARTMENT`	YES
`SELECT * from EMPLOYEE`	`SELECT EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from EMPLOYEE`	YES
`SELECT FIRSTNME, case when SALARY > 150000 then 'high' when SALARY > 100000 then 'medium' when SALARY > 80000 then 'fair' else 'poor' end from EMPLOYEE`	`SELECT FIRSTNME, case when SALARY > 150000 then 'high' when SALARY > 100000 then 'medium' when SALARY > 80000 then 'fair' else 'poor' end from EMPLOYEE`	NO
`DELETE from EMPLOYEE where EMPNO=100`	`DELETE from EMPLOYEE where EMPNO=100`	NO
`INSERT into TEMP_EMP SELECT * from EMPLOYEE`	`INSERT into TEMP_EMP SELECT * from EMPLOYEE`	NO

   重要:

   再書き込み定義は構文に基づいているため、`SELECT * from [OBJECT]` という形式のすべてのステートメントが例に一致します。例えば、`SELECT * from DEPARTMENT` というステートメントと `SELECT * from EMPLOYEE` というステートメントは、どちらも上記の例に一致します。

   照会再書き込み定義を特定のオブジェクトに制限するには、アクセス・ポリシー・ルールを使用します。その方法については、照会再書き込みをアクティブ化するセキュリティー・ポリシーの定義を参照してください。

5. 引き続きサンプル照会を入力して、再書き込み定義をテストします。 「テストのセットアップ」をクリックして、テストに使用する再書き込み定義を変更するか並べ替えます。

次のタスク

テスト結果に問題がなければ、セキュリティー・ポリシーを作成して、実際の照会への照会再書き込み定義の使用を開始します。

親トピック: 照会再書き込みの使用
前のトピック: 照会再書き込み定義の作成
次のトピック: 照会再書き込みをアクティブ化するセキュリティー・ポリシーの定義
関連タスク:
照会再書き込みをアクティブ化するセキュリティー・ポリシーの定義
照会再書き込み定義の作成

照会再書き込みをアクティブ化するセキュリティー・ポリシーの定義

照会再書き込み定義を実際の照会に対して使用するアクセス・ポリシー・ルールを作成する方法について説明します。

始める前に

このタスクを実行するには、1 つ以上の照会再書き込み定義が作成およびテストされている必要があります。また、セキュリティー・ポリシーの作成方法を理解しておく必要があります。

手順

1. 「保護」 > 「セキュリティー・ポリシー」 > 「ポリシー・ビルダー」を開きます。
2. 新規ポリシーを作成するか、既存のポリシーを変更して、照会再書き込み定義を使用します。
   ヒント: 新規ポリシーを作成して、照会再書き込み定義をテストすることを検討してください。テスト・ポリシーの動作に問題がなければ、既存のセキュリティー・ポリシーに再書き込みルールを追加します。
3. 選択したポリシーへの再書き込みルールの追加を開始するには、「ルールの編集」をクリックして、「ルールの追加」 > 「アクセス・ルールの追加」を選択します。
   注: 照会再書き込みルールは、常にアクセス・ルールとして分類されます。
4. 「照会再書き込み: アタッチ (QUERY REWRITE: ATTACH)」ルール・アクションを使用してルールを追加します。「次のルールに進む」チェック・ボックスに必ずチェック・マークを付けてください。このルールは、照会再書き込みセッションをトリガーするために突き合わせる必要のある特定のセッション・パラメーターを識別します (特定のデータベース・ユーザー名やクライアント IP アドレスなど)。
5. 1 つ以上の「照会再書き込み: 定義の適用」ルール・アクションを使用してルールを追加し、適用する照会再書き込み定義を選択します。「次のルールに進む」チェック・ボックスに必ずチェック・マークを付けてください。このルールは、再書き込み定義を適用して元の照会を変更するために突き合わせる必要のある特定のオブジェクトまたはコマンドを識別します。

   例えば、「オブジェクト」フィールドを「EMPLOYEE」に設定すると、SELECT * from 再書き込み定義が EMPLOYEE オブジェクトに制限されます。

6. 「照会再書き込み: デタッチ (QUERY REWRITE: DETACH)」ルール・アクションを使用してルールを追加します。これにより、照会再書き込みセッションが閉じられ、以降はセッション・トラフィックのモニターが行われなくなります。
7. 新規ポリシーをインストールするには、「ポリシー・ファインダー」に戻り、セキュリティー・ポリシーを選択して、「インストール・アクションの選択 (Select an installaction action)」 > 「インストールおよびオーバーライド」を選択します。ポリシーのインストールを確認するよう求められたら、「OK」をクリックします。
8. データベース・サーバーにログインし、テスト照会を実行して、アクセス・ポリシーの再書き込みルールが意図したとおりに機能していることを確認します。
   a. データベース・サーバーにログインします。
   b. インストールしたアクセス・ポリシー・ルールをトリガーする (またはトリガーしない) 照会を実行し、照会再書き込み定義の基準と突き合わせます。

      例えば、SELECT * from EMPLOYEE を実行して、SELECT * from 再書き込み定義が EMPLOYEE オブジェクトに適用されることを確認し、SELECT * from DEPARTMENT を実行して、同じ定義が DEPARTMENT オブジェクトには適用されないことを確認します。

   c. 再書き込みされた SQL が結果に反映されていることを確認します。

親トピック: 照会再書き込みの使用
前のトピック: 照会再書き込み定義のテスト
次のトピック: 照会再書き込み結果を検証するためのカスタム・レポートの作成
関連概念:
ポリシー

照会再書き込み結果を検証するためのカスタム・レポートの作成

照会再書き込みアクティビティーを監査するための照会再書き込みトラッキング・レポートを作成する方法について説明します。

始める前に

このタスクを実行するには、照会再書き込み定義を適用するアクセス・ポリシー・ルールが作成およびインストールされている必要があります。また、レポートの作成方法を理解しておく必要があります。

このタスクについて

照会再書き込みトラッキング・レポートは、テスト環境と実稼働環境の両方における照会再書き込みアクションの検証に役立ちます。

手順

1. 「レポート」 > 「レポート構成ツール」 > 「クエリー・ビルダー」を開きます。
2. 「ドメイン」メニューから「照会再書き込み」を選択します。
3. アイコンをクリックして新規照会を定義します。
4. 照会の分かりやすい固有の名前を「照会名」フィールドに入力します。

例えば、「My query rewrite report」などとします。

5. 「メイン・エンティティー」メニューからいずれかの使用可能なオプションを選択します。

   使用可能なオプションは次のとおりです。

   - 照会再書き込みログ (Query Rewrite Log)
   - クライアント/サーバー
   - セッション
   - アクセス期間

6. 「次へ」をクリックして「レポート・ビルダー」を開きます。
7. 「エンティティー・リスト」内のセクションを展開し、項目を選択してレポートを作成します。
   - 項目をレポートの列として追加するには、項目をクリックして「フィールドの追加」を選択します。
   - レポートに条件フィルターを追加するには、項目をクリックして「条件の追加」を選択します。
   - 別の方法として、「エンティティー・リスト」から「照会フィールド」表と「照会条件」表に項目をドラッグ・アンド・ドロップして、これらをレポートに適用することもできます。

   照会再書き込みレポートの開始点として以下の項目を追加してください。

   - クライアント/サーバー: タイム・スタンプ
   - クライアント/サーバー : DB ユーザー名
   - クライアント/サーバー: サーバー・タイプ
   - 照会再書き込みログ (Query Rewrite Log): 適用される QR 定義名 (Applied QR Definition Names)
   - 照会再書き込みログ (Query Rewrite Log): 入力 SQL (Input SQL)
   - 照会再書き込みログ (Query Rewrite Log): 出力 SQL (Output SQL)

8. レポートの作成が終了したら「保存」をクリックします。
9. 「レポートの作成」をクリックしてレポートを作成します。
10. 「マイ・カスタム・レポートに追加」をクリックしてレポートをカスタム・レポートに追加します。
11. 「レポート」 > 「マイ・カスタム・レポート」を開き、作成したレポートを選択して、照会再書き込みアクションのレポートを表示します。

親トピック: 照会再書き込みの使用
前のトピック: 照会再書き込みをアクティブ化するセキュリティー・ポリシーの定義

ファイル・アクティビティーのポリシーおよびルール

ファイル・アクティビティー・モニターは、UNIX ファイル・サーバーおよび Windows ファイル・サーバー上の機密データの保全性と保護を確保します。

- ファイル・アクティビティーのポリシーおよびルールの機能
  ファイル・アクティビティー・モニターのポリシーは、Guardium で各種のファイル・アクティビティー・イベントをどのように処理するかを指定します。各ポリシーは、順序付けられた一連のルールで構成されます。ポリシー内の各ルールは、そのルールと一致した場合に実行される条件付きアクションを定義します。条件付きテストは単純なものにすることも (ある特定のユーザーは特定の場所にアクセスするなど)、複数の条件を考慮する複雑なテストにすることもできます。アクションは、何もしないというものから、イベントをブロックするというアクションまで、多岐に及びます。複数のグループ化アクションとアラート・アクションを結合して、一致したルールに対する高度な応答を作成するように指示することができます。
- FAM ポリシーおよびそのルールを初めから作成する
  ファイル・アクティビティー・モニターをセットアップするには、「ファイルのためのポリシー・ビルダー」ウィンドウでポリシーとルールを定義して管理します。
- 調査ダッシュボードの「資格」タブでの FAM ポリシー・ルールの作成
  調査ダッシュボードの結果表のモニター対象データ (データ・ソース名、ユーザー名、アクション、ファイル・パスなど) を使用して、ポリシー・ルールを作成できます。

親トピック: 保護
関連情報:
Guardium を使用したファイル・アクティビティーのモニター (ビデオ)

ファイル・アクティビティーのポリシーおよびルールの機能

ファイル・アクティビティー・モニターのポリシーは、Guardium で各種のファイル・アクティビティー・イベントをどのように処理するかを指定します。各ポリシーは、順序付けられた一連のルールで構成されます。ポリシー内の各ルールは、そのルールと一致した場合に実行される条件付きアクションを定義します。条件付きテストは単純なものにすることも (ある特定のユーザーは特定の場所にアクセスするなど)、複数の条件を考慮する複雑なテストにすることもできます。アクションは、何もしないというものから、イベントをブロックするというアクションまで、多岐に及びます。複数のグループ化アクションとアラート・アクションを結合して、一致したルールに対する高度な応答を作成するように指示することができます。

例えば、以下のケースに対するポリシーを定義できます。

- John が CONFIDENTIAL フォルダーに書き込んだ場合にポリシー違反をログに記録する。
- 特定のグループのユーザーがファイル SALARIES.XLS を削除するのをブロックする。
- JENNY が、名前が sample* で始まるファイルから読み取りを行った場合に Krishna に E メールを送信する。
- PCI に関連する機密データが含まれているとして分類されたファイルへのすべてのアクセスを監査する。

グループ: Guardium では、ポリシーおよびレポートの作成のためにグループという概念が使用されます。

Guardium グループは、Guardium コレクターまたは中央マネージャーで作成され、保持されます。Guardium グループとファイル・システム・グループを混同しないでください。

グループの命名方法を考慮することをお勧めします。例えば、データ・ソース (ファイル・サーバー) のグループ、ファイルのグループ (機密レベル別、または機密レベルとアプリケーションの組み合わせ別など)、ユーザーのグループ (既知のすべてのユーザー、許可されたユーザー、特権があるユーザーのリスト) などです。

ルールのガイドライン

- 範囲が広すぎるルール (モニターするファイルが多すぎるルール) は、システムが過負荷になり、処理時間と応答時間が長くなる可能性があります。
- 1 つの FAM ルールに複数のパターンを含めることができます。ディレクトリーとその内容の両方を保護するには、「/FAMtest/*」と「/FAMtest」という 2 つのパターンを持つルールを定義します。
- ファイル・パスからなるグループの場合、大/小文字とは関係なく、各パスが固有でなければなりません。例えば、1 つのグループに、C:¥ABC と C:¥abcdef という 2 つのパスを共存させることはできます。一方、1 つのグループに C:¥ABC と C:¥abc という 2 つのパスを共存させることはできません。グループ・ビルダーは大/小文字を区別しません。そのため、すべて大文字またはすべて小文字でメンバーを入力する必要はありません。 ただし、大/小文字を区別する UNIX では、パス /IBM/Guardium はパス /ibm/guardium と異なります。 これら両方のパスをモニターしたい場合、現在のグループ・ビルダーには制限があり、これらのパスは別個の 2 つのパスとして見なされません。
- セキュリティー・ポリシーのルールの順序は非常に重要です。ルールはセットとして S-TAP に送信され、厳密に順番通りに処理されます。所定のユーザー・アクティビティーが、ポリシー内の各ルールと順番に照合されチェックされます。このファイル・アクセスの条件を満たす最初のルールが適用され、後続のルールは無視されます。ほとんどの場合、固有性の最も高いルールを最初に配置し、一般性の最も高いルールを最後に配置します。例えば、以下の 2 つのルールがあるとします。
  - **ルール A:** /data/* へのすべてのアクセスの*監査のみ*行います。
  - **ルール B:** ユーザー「joe」が /data/salaries にアクセスするのを *ブロックし*、*違反をログに記録し*、*監査します*。

  ルール A を最初に配置した場合、Joe が /data/salaries を読み取ろうとすると、次のルールに進む必要はなく、Joe のアクセスの監査のみ行われます。ルール B を最初に配置すると、Joe の /data/salaries へのアクセスはブロックされ、次のルールに進む必要はありません。

(マルチアクション・サポートが組み込まれた) 10.1.2 以降のスニファーで (マルチアクションをサポートしていない) 10.1.2 より前の S-TAP を使用する場合の FAM の動作

- マルチアクション・ルールを使用する新しい 10.1.2 スニファー/UI で 10.1.2 より前の S-TAP を使用する場合、ブロッキングは正しく実装されます。このアクションは、S-TAP 側で行われるためです。
- スニファー側でのこのアクションは、指定されているすべてのアクションが累積されたものとなります。
- 例えば、READ コマンドに対して「監査のみ」を選択し、DELETE コマンドに対して「ブロック」、「違反のロギング」、および「監査」を選択すると、DELETE コマンドはブロックされますが、READ コマンドはブロックされません。一方、READ コマンドと DELETE コマンドの両方は、READ コマンドが「監査のみ」であっても、監査、違反のロギング、およびアラートの生成をトリガーします。
- ユーザーが 10.1.2 の S-TAP と 10.1.2 より前のスニファー/UI を使用する他の例では、マルチアクション・ルールを定義する手段はないため (したがって、サポートする UI や GuardAPI がないため)、問題なく機能します。

ルールの属性

ルール名

固有の名前

データ・ソース

データ・ソースには、以下を指定できます。

- ドロップダウン・リストから選択したデータ・ソース
- ドロップダウン・リストから選択したグループ
- 「新規ルールの作成」ウィンドウで、選択したグループから作成したグループ
- 手動で入力したパス

ルール・アクション

ルール・アクションは、基準を満たした場合に実行されるアクションです。アクションは、以下のいずれかです。

- ルール基準に一致するすべてのファイル・アクセスに対する単一のアクション
- 複数のアクション (指定されたコマンド・カテゴリーまたは指定されたグループごとに 1 つのアクション) からなるマルチアクション・ルール。マルチアクション・ルールを使用する場合、**「次のルールに進む」**はサポートされないことに注意してください。

以下のルール・アクションがあります。

- アラートおよび監査: 指定された動作によりスニファーから直接生成されたアラートを送信し、イベントをログに記録します。
- 監査のみ: GDM 表にイベントのログを記録します。
- ブロック、違反のロギング、および監査: オブジェクトへのアクセスをブロックし、ポリシー違反とイベントをログに記録します。ブロック・アクションでは、アラート構成も必要です。
- 無視: アクションはとられません。
- 違反として記録、および監査: 対象をポリシー違反としてログに記録し、イベントをログに記録します。

アクセス・コマンド: 数百のファイル・システム・コマンドがあることから、コマンドは以下のカテゴリーに分類されています。

- 読み取り
- 書き込み
- 実行
- 削除
- ファイル操作。これには、ファイル・メタデータに影響する呼び出し (ファイル所有権の変更、ファイル許可の変更、および類似する呼び出し) が含まれます。

これらのカテゴリーはシステムで固定されており、変更できません。ただし、カテゴリーの任意の組み合わせで含めた Guardium グループを作成し、そのグループをセキュリティー・ポリシーで使用できます。例えば、「書き込み」と「実行」をメンバーとして含めた Guardium グループを作成できます。

コマンドを未指定のままにすると、すべてのファイル・システム・コマンドが一致としてカウントされます。一部の呼び出し (システム時刻の取得など) は、ファイルにまったく影響せず、無視されます。

ルール基準

所定のファイル・アクセスに対して、ルール基準を使用して、特定のアクションを実行するかどうかが判断されます。データ・ソース、またはデータ・ソースのグループ (ファイル・サーバー) に対して指定できるルール基準を以下に示します。

ユーザー: ファイルにアクセスする OS ユーザーです。Guardium グループでの定義に従い、ユーザーのグループも使用できます。ブランクのままにすると、root 以外のすべてのユーザーにルールが適用されます。

ファイル・パス: Windows または UNIX のファイル・パス、個々のファイル・パス、または Guardium グループで定義されたファイル・パスのグループを使用できます。これをブランクにすることはできません (取り外し可能メディアが選択されている場合を除く)。ファイル・パスに含まれるサブディレクトリーをモニター対象として選択することもできます。

名前の指定でのワイルドカードは以下のようになります。

- 「*」文字は、任意の数の文字に一致します。
- 「?」文字は、単一の文字に一致します。
- UNIX では、円記号を使用して * および ? をエスケープします。

ヒント: ワイルドカードでは追加の処理が発生します。ワイルドカードを使用し過ぎると、パフォーマンスに影響します。

UNIX

使用法:

ディスク上のすべてのファイルに一致させるには、/* と入力します。

/tmp/My*File.txt に正確に一致させるには、/tmp/My¥*File.txt を使用します。

/tmp 内の .txt 拡張子のファイルと一致させるには、/tmp/*.txt を使用します。

例: 以下の FAM ルール・パターンを使用します。/FAM*

意味

- ディレクトリー: /
- ファイル名: FAM*

所定の位置の FAM ルールには、選択したサブディレクトリーがあります。(Subdirs: Yes)

以下のファイルがアクセスされます。

/guardium/modules/SUPERVISOR/10.0.0/FAM.output

この場合、「FAM.output」というファイル名が「FAM」という名前に一致します。このファイルは、指定されたディレクトリー「/」のサブディレクトリー内に存在しています。

Windows: Windows では、ドライブ (C:¥ など) を指定する必要があります。

使用法:

C ドライブ上のすべてのファイルをモニターするには、C:¥ と入力し、「サブディレクトリーのモニター (Monitor subdirectories)」チェック・ボックスにマークを付けます。

C:¥tmp 内の .txt 拡張子のファイルに一致させるには、C:¥tmp¥*.txt を使用します。

GuardAPI の例: 2 つのルールを使用したポリシーの作成

```
grdapi create_policy ruleSetDesc=policy1 isFam=true
grdapi create_fam_rule policyName=policy1 ruleName=rule1 serverHost="x.x.x.x" filePath="/famtest/*" command="DELETE"
actionName="Alert and Audit" notificationType="SYSLOG"
grdapi create_fam_rule policyName=policy1 ruleName=rule2 serverHost="x.x.x.x" filePath="/famtest/*" command="READ"
actionName="Alert and Audit" notificationType="MAIL"
```

policy1 -> rule1 -> "DELETE" -> "Alert and Audit" -> "SYSLOG"

policy1 -> rule2 -> "READ" -> "Alert and Audit" -> "MAIL"

GuardAPI の例: マルチアクション・ルールを使用したポリシーの作成

FAM のマルチアクション・ルール - マルチアクション・ルールは、複数のアクション (指定されたコマンド・カテゴリーまたは指定されたグループごとに 1 つのアクション) で構成されます。FAM のコンテキストでは、これらのコマンドは読み取り、書き込み、削除、実行、およびファイル操作です。システムがマルチアクション・ルールをサポートしていない場合、システムはルールを無視して次のルールに進みます。

```
grdapi create_policy ruleSetDesc=policy1 isFam=true
grdapi create_fam_rule policyName=policy1 ruleName=rule1 serverHost="x.x.x.x" filePath="/famtest/*"
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="DELETE, READ" actionName="Alert and Audit"
notificationType="SYSLOG"
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="WRITE" actionName="Alert and Audit" notificationType="MAIL"
```

policy1 -> rule1 -> "DELETE, READ" -> "Alert and Audit" -> "SYSLOG"

policy1 -> rule1 -> "WRITE" -> "Alert and Audit" -> "MAIL"

commandGroupId=20000 が存在し、"DELETE, WRITE" が含まれるという前提で、commandGroupId を使用して別のアクションを追加します。

```
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="READ" commandGroupId=20000 actionName="Ignore"
notificationType=""
```

policy1 -> rule1 -> "READ, DELETE, WRITE" -> "Ignore"

V.10.1.2 より前の S-TAP と V.10.1.2 以降のスニファーでの FAM の動作

FAM のマルチアクションは V.10.1.2 で導入されました。10.1.2 より前の S-TAP では FAM のマルチアクションがサポートされませんが、V.10.1.2 以降のスニファーではマルチアクションがサポートされます。スニファー側でのこのアクションは、指定されているすべてのアクションが累積されたものとなります。

例えば、ポリシーで READ コマンドには「監査のみ」が指定されていて、DELETE コマンドには「ブロック」、「違反のロギング」、および「監査」が指定されている場合、DELETE コマンドはブロックされますが、READ コマンドはブロックされません。一方、READ コマンドと DELETE コマンドの両方は、READ コマンドが「監査のみ」であっても、監査、違反のロギング、およびアラートの生成をトリガーします。

親トピック: ファイル・アクティビティーのポリシーおよびルール

FAM ポリシーおよびそのルールを初めから作成する

ファイル・アクティビティー・モニターをセットアップするには、「ファイルのためのポリシー・ビルダー」ウィンドウでポリシーとルールを定義して管理します。

このタスクについて

「ファイルのためのポリシー・ビルダー」を開き、ポリシー・ビルダー内で他のビューを開いた後は、ページの下部にある「ファイルのためのポリシー・ビルダー」、「新規ポリシー」、および「新規ルールの作成」をクリックすることで、各種のビューを切り替えることができます。

GuardAPI を使用してポリシーおよびルールを作成することもできます。

手順

1. スタンドアロンまたは MU で FAM ポリシー・ビルダーにアクセスします。「保護」 > 「セキュリティー・ポリシー」 > 「ファイルのためのポリシー・ビルダー」にナビゲートします。
2. 新規ポリシーの名前を入力します。(ルールの定義後にポリシーを保存できます)。
3. 既存のルールをポリシーに追加するには、以下のようにします。
   a. 「テンプレートの表示」をクリックします。「ルール・テンプレート」表が開きます。
   b. オプションで、フィルター機能を使用してリストをフィルタリングします。
   c. 1 つ以上のルールを選択して、右矢印 をクリックします。
4. 新規ルールを作成するには、以下のようにします。
   a. をクリックして「新規ルールの作成」ウィンドウを開きます。
   b. ルールの名前を入力し、その属性を定義してから、「保存」をクリックします。
5. 既存のルールを変更してからポリシーに追加するには、以下のようにします。
   a. ルールを選択し、 をクリックします。
   b. をクリックして、名前を変更し、必要に応じてその他の属性を変更してから、「保存」をクリックします。
6. ルールの順序を変更するには、 を使用します。
7. ルールを削除するには、ルールを選択してから ルールの削除 をクリックします。
8. 「保存」をクリックしてポリシーを保存するか、「保存およびインストール」をクリックしてポリシーを直ちにインストールします。(ポリシーのインストールを参照)。

親トピック: ファイル・アクティビティーのポリシーおよびルール
関連情報:
GuardAPI ファイル・アクティビティー・モニター関数

調査ダッシュボードの「資格」タブでの FAM ポリシー・ルールの作成

調査ダッシュボードの結果表のモニター対象データ (データ・ソース名、ユーザー名、アクション、ファイル・パスなど) を使用して、ポリシー・ルールを作成できます。

始める前に

- FAM バンドルをインストールして構成する必要があります。
- ディスカバリーおよび分類を有効にする必要があります。
- 調査ダッシュボードを有効にする必要があります (調査ダッシュボードの有効化と無効化を参照)。

このタスクについて

手順

1. 製品バナーのドロップダウン・リストから「ファイル」を選択し、検索アイコンをクリックして、ファイル・データの調査ダッシュボードを開きます。
2. 結果表の「資格」タブを開きます。「詳細」をクリックして個々のエントリーを表示します。
3. ルールを取り込むために使用する、結果内の 1 つ以上のエントリーを選択します。「すべて選択」チェック・ボックスを使用すると、現在表示されているすべてのエントリー (データベース内のすべてのエントリーではない) を含めることができます。
4. 右クリックし、「ポリシー・ルールの追加」を選択します。「ルールの作成」ダイアログが開き、選択したエントリーの値が表示されます。複数のエントリーを選択した場合、それらのエントリーの値を含むグループが作成されます。既存のポリシーに追加するルールを作成することや、新規ルールを含む新規ポリシーを作成することができます。
   注: ルールの範囲が広すぎる (モニターするファイルが多すぎる) 場合は、システムが過負荷になり、処理時間と応答時間が長くなります。
   注: 1 つの FAM ルールに複数のパターンを含めることができます。ディレクトリーとその内容の両方を保護するには、「/FAMtest/*」と「/FAMtest」という 2 つのパターンを持つルールを定義します。
   注: FAM ポリシーを使用する場合、モニター対象ファイル・パスを定義するグループを設定する際に大/小文字の区別について考慮する必要があります。そうしないと、グループを正常に作成できません。 回避策は、異なる 2 つの FAM ポリシー・ルールを作成することです。 分類 - グループのメンバーとして定義する文字列が、大/小文字が区別されない場合でも異なるときに、グループは正常に作成できます。例えば、1. C:¥ABC 2. C:¥abcdef です。グループのメンバーとして定義する

文字列が、大/小文字が区別されないと同じである場合にはグループを作成できません。例えば 1. C:¥ABC 2. C:¥abc の場合などです。そのため、すべて大文字またはすべて小文字でメンバーを入力する必要はありません。 グループ・ビルダーは大/小文字を区別しません。 ただし、大/小文字を区別する UNIX では、パス /IBM/Guardium はパス /ibm/guardium と異なります。 これら両方のパスをモニターしたい場合、現在のグループ・ビルダーには制限があり、同じパスとして見なしません。

5. データ・ソース、アクション、および条件を選択します。変更したい値を上書きします。「編集」をクリックして各フィールドを変更します。
6. 新規ポリシーを作成し、それをインストールするには、「作成およびインストール」をクリックします。ポリシーを作成し、それをインストールしない場合は、「OK」をクリックします。

親トピック: ファイル・アクティビティーのポリシーおよびルール

モニターおよび監査

機密データを識別し、それを保護するステップを実行した後、このデータにアクセスするアクティビティーをモニターする必要があります。多くの場合、モニターにより生成されるデータを使用することで、監査要件 (法的または内部) を順守できます。

- 監査プロセスの作成
  資産ディスカバリー、脆弱性評価と強化策、 データベース・アクティビティー・モニターおよび監査のレポート作成、レポートの配布、 主要な利害関係者によるサインオフ、およびエスカレーションなどの データベース・アクティビティー・モニター・タスクを、1 つのスポットに統合することにより、 コンプライアンス・ワークフロー・プロセスを合理化します。
- 監査およびレポート
  Guardium® は、収集したデータをドメイン・セットに編成します。 各ドメインには、特定の関心領域 (データ・アクセス権、例外、ポリシー違反など) に関連する異なるタイプの情報が格納されます。
- 外部データ相関
  このトピックでは、既存の Guardium 内部データに加えて必要なエンタープライズ情報のカスタム表の作成について説明します。
- プライバシー・セット
  プライバシー・セットとは、特別なモニターを行うために使用できる要素の集合です。
- カスタム・アラート
  アラート・メッセージを配布する方法として、E メール、SNMP、syslog、またはユーザー作成の Java™ クラスが可能です。この最後のオプションを「カスタム・アラート」といいます。
- 未解析ログ処理
  未解析ログ・オプションは、Guardium アプライアンスが情報を即時に解析することなくログに記録できるようにする処理です。
- 照会条件での式の作成
  「値」、「パラメーター」、「属性」の選択項目の横にある「式の追加」アイコンを使用して、ユーザー定義文字列と数式を含む照会条件を入力します。
- データベース・ライセンス・レポート
  ライセンス・レビューは、ユーザーがそれぞれの業務を行うために必要な特権のみを持っていることを検証および確認するプロセスです。
- ユーザー識別
  Guardium には、データベース・トラフィックから実際のデータベース・ユーザーが識別できない場合に、アプリケーション・ユーザーを識別する方法がいくつか用意されています。
- 値変更監査
  値変更監査フィーチャーは、データベース表内の値の変更をトラッキングします。
- 監査データベースの作成
  監査データベースを作成して値変更モニター・アクティビティーを実行します。
- モニター対象表アクセス
  この機能は、Optim™ Designer データ・ライフサイクル製品との相互作用を可能にするために、「最後の評価」フィールドを関連する表に追加します。
- コンプライアンス・モニターのクイック・スタート
  モニター・エージェント (S-TAP) をデプロイした後、コンプライアンス・モニター・ツールを使用して、特定のセキュリティー基準および規制のモニターを設定します。
- PCI/DSS アクセラレーターを使用して PCI コンプライアンスを実装する方法
  PCI/DSS 要件を満たすために、IBM Security Guardium の PCI/DSS アクセラレーターを構成し、一連のポリシーとレポートを作成します。
- ワークフロー・ビルダー
  ワークフロー・ビルダーは、監査プロセスで使用する、カスタマイズされたワークフロー (ステップ、移行、およびアクション) を定義するために使用します。
- 脅威検出分析
  Guardium には、監査済みデータをスキャンおよび分析して、さまざまなタイプのデータベース攻撃を示す可能性のある徴候を検出するための特殊な脅威検出分析が組み込まれています。
- 調査ダッシュボード
  調査ダッシュボードは、Guardium 環境に存在する可能性がある問題を特定して評価するための強力なツールを提供します。これはローカルまたはシステム全体のフィルタリングされていないデータを使用し、Guardium 環境全体で、その環境内のすべての Guardium コレクターを対象としてデータを照会するための多くのフィルタリング・オプションを提供します。
- Outliers Detection
  2 つの簡単なステップで Outliers Detection を有効にして、Outliers Detection の監査を開始できます。これにより、Guardium が異常なサーバーの動作とユーザーの動作を識別し、考えられる攻撃を早期に検出するための処理を行えるようになります。
- データ保護ダッシュボード
  Guardium のデータ保護ダッシュボードは、上級セキュリティー担当者のためにリスクおよびコンプライアンスのデータの要約ビューを提供します。

監査プロセスの作成

資産ディスカバリー、脆弱性評価と強化策、 データベース・アクティビティー・モニターおよび監査のレポート作成、レポートの配布、 主要な利害関係者によるサインオフ、およびエスカレーションなどの データベース・アクティビティー・モニター・タスクを、1 つのスポットに統合することにより、 コンプライアンス・ワークフロー・プロセスを合理化します。

以下の監査アクティビティーを自動化し、コンプライアンス・ワークフローに統合します。

- 複数の監査タスク (レポート、脆弱性評価など) を 1 つのプロセスにグループ化する機能。
- これらのプロセスの定期的な実行をスケジュールする。
- これらのタスクをバックグラウンドで実行する。

- タスクの結果を Comma-Separated Value (CSV) ファイルまたは ArcSight Common Event Format (CEF) ファイルに 書き込むか、Syslog を使用して他のシステムに転送する。あるいは、その両方を行う。
- コメントおよびメモを追加する。
- プロセスをその発信者に割り当て、表示可能にする (結果が準備できると、発信者の To-Do リストに新規項目が追加されます)。
- プロセスを他のユーザー、ユーザー・グループ、またはロールに割り当てる。
- これらの割当先が結果にサインオンするための要件を作成する。
- 結果のエスカレーション (オリジナルの監査証跡の外部にいるユーザーへの割り当て) を許可する。

データベース・セキュリティーの管理を、定期的に実行される、時間を要する手動のアクティビティーから、 継続的な、企業のプライバシーおよびガバナンス要件 (PCI-DSS、SOX、データ・プライバシーおよび HIPAA など) を サポートする自動化プロセスに変換します。

監査結果を、追加のフォレンジック分析のために外部リポジトリー (Syslog、CSV/CEF ファイル、外部フィード) にエクスポートします。

「監査プロセス・ログ」レポートには、すべてのタスクに関する 詳細なアクティビティー・ログが、開始時刻および終了時刻も含めて示されます。 このレポートは、admin ユーザーが「Guardium® モニター」タブを通じて入手可能です。監査タスクには、開始および終了時刻が示されますが、セキュリティー・アセスメントおよび分類 (キューに入れられます) の開始および終了は同じになります。

各ワークフロー・プロセスの結果 (レビュー、サインオフ証跡、およびコメントなど) はアーカイブ可能であり、 後ほど調査センターを通じてリストアし、レビューすることができます。

コンプライアンス・ワークフロー自動化プロセスは、以下の疑問に答えます。

- 必要とするレポート、アセスメント、監査証跡、または分類のタイプは?
- この情報の受信者およびサインオフの処理方法は?
- 配布のスケジュールは?

コンプライアンス・ワークフロー自動化プロセスには、さらに次のようなエレメントも含まれます。

- プロセス定義
- 配布計画。以下を行います。
  - 受信者 (個々のユーザー、ユーザー・グループ、またはロールのいずれであっても可) を定義します。 (『プロセス受信者』を参照してください。)
  - 各受信者に、レビュー/署名の責務を定義します。
  - 「継続」フラグを設定することにより、配布シーケンスを定義します。
- タスク・セット (『プロセス・タスクのタイプ』を参照してください。)
- スケジュール - 監査プロセスはすぐに実行することも、スケジュールを定義して定期的に実行することもできます。

プロセス・タスクのタイプ

ワークフロー・プロセスには、以下の監査タスクを任意の数、組み込むことができます。

- レポート (カスタムまたは事前定義)。 Guardium は、100 を超える調整固有のレポートのほか、数百もの事前定義レポートを提供します。
- セキュリティー・アセスメント・レポート。 セキュリティー・データベース・アセスメントは、データベース・インフラストラクチャーで脆弱性をスキャンし、アセスメントリアルタイムの測定および履歴測定の両方による、データベースおよびデータ・セキュリティーの正常性のアセスメントを提供します。 このアセスメントでは、カスタム・テストを取り込むほか、共通データベース・セキュリティー・ベスト・プラクティス (STIG および CIG1 など) を使用してグループ化された、既知の問題および脆弱性に基づく 事前定義脆弱性テストと、現行の環境を対比します。アプリケーションは、 (ベスト・プラクティスに基づく) 重み付け測定基準を取り入れた セキュリティー・ヘルス・レポート・カードを生成し、 データベース・セキュリティーを強化するためのアクション計画を推奨します。
- エンティティー監査証跡。 特定のエンティティー (例えば、クライアント IP アドレスまたはアドレス・グループなど) に 関連するアクティビティーの詳細なレポートが作成されます。
- プライバシー・セット。 オブジェクト/フィールド・ペア (例えば、社会保障番号と生年月日など) のグループに対するアクセスについて詳述したレポートが、 指定された期間中に作成されます。
- 分類プロセス。 既存のデータベースのメタデータおよびデータがスキャンされ、機密である可能性のある情報 (社会保障番号や クレジット・カード番号など) についてレポートを作成します。
- 外部フィード。 データを外部の特殊なアプリケーションにエクスポートして、さらに詳細なフォレンジック分析を行うことができます。
  注:「オプション外部データ・フィード」は、プロダクト・キーによって使用可能になるオプション・コンポーネントです。このフィーチャーは、使用可能になっていない場合には「監査タスク」選択項目には表示されず、 「フィード・タイプ」リストは空になります。

ワークフロー・プロセス、一元管理および統合

中央マネージャーにおいて、レポートはリモート・データ・ソース (管理対象ユニット) から データを参照可能です。これらのレポートを使用する監査プロセスは、中央マネージャーからのみアクセス可能であり、 管理対象ユニットからは不可視になります。

アグリゲーター・サーバーのワークフロー自動化 (監査処理) に、各アグリゲーター・タスクの一時データベースを作成し、 そのタスクに関連する日のみを指定するための機能が組み込まれました。

注: 統合サーバーの一時データベースは、必要に応じて Guardium サポート・サービスによる実行後分析を行うため、 (CLI コマンド drop_ad_hoc_audit_db の値に応じて) 最大 14 日 までシステムに保持することができます。

監査プロセスでレポートを定義するとき、(FROM-TO フィールドで定義される) レポートの日数は特定のしきい値を超えることができません (デフォルトでは 1 カ月)。このしきい値を超えると、アグリゲーターで監査タスクの実行を試行中にランタイム・エラーが発生します。

(CLI で設定された) max_audit_reporting 値を 超える FROM-TO 範囲を指定した監査タスクを作成することが許容されています。これは、アグリゲーターに定義された監査プロセスが、 (このアグリゲーターがマネージャーである場合に) 管理対象コレクターで実行される場合があるからです。 コレクター・ユニットで実行される監査タスクには、max_audit_reporting 制限がありません。

したがって、許容範囲を超えるタスクを保存することは有効ですが、アグリゲーターでタスクを実行する際に、 実行時例外が発生する可能性があります。

監査レポートのしきい値は、CLI コマンド show max_audit_reporting または store max_audit_reporting を使用して構成できます。 無効な FROM-TO 範囲を指定してレポートを作成しても、警告メッセージは出されません。 代わりに、「監査プロセス」設定メニュー画面の「タスク・パラメーター」パネルに、固定メッセージが表示されます (「ツール」/「監査プロセス・ビルダー」。「監査タスク」を開いて、「タスク・パラメーター」を表示)。固定メッセージを以下に示します。

アグリゲーターに関しては、許容される時刻範囲 (CLI: max_audit_reporting) を超えないレポートのみが実行されます。

注: パッチ・インストールの実行中は、すべての監査プロセスが停止します。

監査プロセスの停止

監査プロセスの停止は、監査タスクが実行されていない場合、または実行中の場合にのみ実行可能です。 監査プロセスを停止すると、以後、まだ開始されていないタスクは実行されません。 監査プロセスを停止しても、部分的な結果は送信されません。 監査プロセスが停止した結果として、停止したことを示すエラー・メッセージが出されます。 ただし、タスクが完了している場合、監査プロセスを停止しても、結果の送信は停止されません。

「順守」 > 「ツールとビュー」 > 「監査プロセス・ログ」レポートから起動した GuardAPI (カーソルを任意の行に置いてダブルクリックし、ドリルダウン) を使用して、監査プロセスを停止します。

任意のユーザーの場合、監査プロセスを停止すると、そのユーザーに属する行 (タスクのみ、全詳細は含まれない) が表示されます。 admin ユーザーは全詳細を確認可能であり、すべてのユーザーの監査プロセスを停止できます。 その他のユーザーは、自身の監査プロセスのみ停止できます。

注:

リモート・ソースを使用している照会は停止できません。リモート・ソースを使用している オンライン・レポートは停止できません。

監査プロセスの停止は、プライバシー・セット監査タスクや、外部フィード監査タスクには適用されません。 プライバシー・セット・タスクや外部フィード・タスクが開始した場合、 プロセスが停止されてもこれらのタスクは完了します。

結果の配布

監査プロセスの受信者は、E メール、または各自の To-Do リスト (あるいはその両方) によって、処理中の監査プロセスの結果について通知を受けます。任意の受信者をプロセスの署名者に指定できます。 その場合、配布リストのその受信者のポイントで、受信者によって電子署名が付けられるかリリースされるまで、 結果をオプションで保留にすることができます。 受信者は、個々のユーザー、ユーザー・グループ、またはロールのいずれであってもかまいません。

監査プロセス・サマリー

「監査プロセス・ファインダー」画面内に「監査プロセス状況サマリー (Audit Process Status Summary)」があります。このセクションには、スケジュールされた監査プロセス、結果、未処理の受信者およびエラーに関する情報が含まれています。 このサマリーは、複数の監査プロセス・レポートからのデータを統合したものです。

監査プロセスの結果を削除するためのボタンもあります。「監査プロセス・ファインダー」画面を参照してください。 「今すぐ 1 回実行」ボタンの横にある「結果」ボタンを見つけます (選択肢は「表示」または「削除」)。

監査プロセスの結果が削除されますが、レポートの削除者がトラッキングされ、ログに記録されます。 audit-delete ロールは、監査プロセスの結果が削除された場合のトラッキングまたはロギングに使用されます。 audit-delete ロールを持っているユーザーは、レポートを削除することができます。管理ユーザーも、レポートを削除することができます。トラッキングは、ユーザー・アクティビティー監査証跡レポートを使用して実行されます。

注: リモート・ソースの監査プロセスの結果は、100,000 件までに制限されています。 この制限を超える場合は、CLI コマンドの store save_result_fetch_size (show save_result_fetch_size) を使用してください。

プロセス受信者

ワークフロー自動化プロセスには、任意の数の受信者を定義でき、各受信者が結果を受け取る順番を制御することができます。 また、受信者は、「エスカレート」機能を使用して他の受信者に通知することができます。 受信者を定義せずに監査プロセスを実行することも可能です。 例えば、syslog に書き込みを行い、結果のレビュー (署名) を必要としない、 受信者のいない監査プロセスなど。

誰を受信者とするか?

「プロセス定義」パネルの受信者のドロップダウン・リストには、全 Guardium ユーザー、 ユーザー・グループ、およびロール (グループおよびロールには、そのようにラベルが付けられています) が含まれています。 グループまたはロールを選択すると、そのグループに属する、またはそのロールを持つすべてのユーザーが、結果を受信します。

グループ受信者を選択した場合、 いずれかのワークフロー自動化タスクで照会条件に特殊ランタイム・パラメーター ./LoggedUser が使用されていると、 その照会はグループ内のユーザーごとに個別に実行され、各ユーザーは自身の結果だけを受信します。

例えば、会社に 3 つの DBA があり、各 DBA がそれぞれ異なるサーバー・セット の管理下にあるとします。「カスタム・データのアップロード」機能を使用して、各 DBA の責務分野を (サーバー IP とともに) Guardium システムにアップロードし、それをデータベース・アクティビティー・ドメインに相関し、このカスタム・ドメインでレポートを監査タスクとして使用します。3 つの DBA を含んだユーザー・グループが受信者に指定された場合、各 DBA は受信者の サーバーのコレクションに関連するレポートのみを受信します。

グループ受信者を選択し、 サインオフが必要とされる場合、各グループ・メンバーが結果に個別に署名する必要があります (前述の 説明のとおり、グループのメンバーごとに表示される結果セットが異なる可能性があります)。

E メール・アドレスだけを受信者とし、 結果がその E メール・アドレスに送信されるようにすることができます。 E メール・アドレスを入力するユーザーは、データをフィルターに掛けるために 使用されるユーザーを入力する必要があります。このユーザーは、ログイン・ユーザーと同じであるか、 データ階層でログイン・ユーザーの下位にいるユーザーでなければなりません。

ロール受信者を選択した場合、 結果に署名する必要があるのは、そのロールの 1 人のユーザーだけであり、 同じロールの他のユーザーは、結果に署名が付けられた際に通知を受けます。

注:

ワークフロー・イベントが作成された際には、 そのイベントが使用するすべての状況にロールを割り当てることができます (つまり、 その状況にある場合、イベントはこのロールからのみ参照可能になります)。 イベントを監査プロセスに割り当てる際には、このイベントの状況に割り当てられた すべてのロールに、この監査プロセスの受信者がいることが重要です。 そうでないと、監査結果行が、この行を参照したり、状況を変更したりできる受信者が いない状況に置かれる可能性があります。

この場合、admin ユーザー (ロールに関係なくすべてのイベントを参照可能) が、この行を確認し、その状況を変更できます。ただし、データ・レベル・セキュリティーがオンになっていると、admin ユーザーがこの行を参照できない可能性があります。admin ユーザーは、 (「グローバル・プロファイル」から) データ・レベル・セキュリティーをオフにするか、 dataset_exempt ロールを保持することが必要になります。 監査プロセスは、その監査プロセスに関連するイベントに対処する必要があるすべてのロールが受信者となるように構成することが重要です。

E メール通知

オプションで、受信者は、E メールを通じて新規プロセスの結果の通知を受けることができます。結果を E メールで配布するためのオプションとして、次の 2 つがあります。

- リンクのみ - E メール通知には、Guardium システムに格納された結果へのハイパーテキスト・リンクが含まれます。リンクを機能させるには、Guardium システムに対するアクセス権を保持しているシステムからメールにアクセスする必要があります。E メール・リンクについて詳しくは、以下のセクションを参照してください。
- 全結果 - 結果を含んだ PDF ファイルまたは生成された CSV ファイルが E メールに添付されます。 ただし、オリジナルの配布リストに含まれない受信者を指定する「エスカレーション」については例外であり、 この場合は PDF ファイルや CSV ファイルは添付されません。「全結果」オプションを選択する際には、 PDF ファイルや CSV ファイルに機密データやプライベート・データが含まれる可能性があるため、 注意が必要です。監査プロセスを実行しており、「全結果を CSV で」にチェック・マークが付けられた受信者がいる場合、 タイプが「アセスメント」、「分類」、または「外部フィード」のタスクでは、CSV ファイルは生成されません。 これらのタイプのタスクでは、エクスポート用の CSV/CEF/PDF ファイルも生成できません。 タイプが「レポート」、「プライバシー・セット」、または「エンティティー監査証跡」のタスクで、 「全結果を CSV で」にチェック・マークが付けられている受信者がいる場合にのみ、 CSV ファイルが生成されます。
  注: 監査結果を表示する際に、生成済みの PDF が既存の場合は、「PDF の再作成」ボタンが表示され、そのボタンを使用して PDF を再作成し、ダウンロードすることができます。

プロセス結果へのハイパーテキスト・リンク

E メール・メッセージでは、Guardium システム上のプロセス結果へのリンクが機能しない条件があります。例:

- 通常 Guardium システムにアクセスできないロケーションから E メールにアクセスしている場合、リンクは機能しません。例えば、オフィス外にいるときには、インターネット経由で自身の E メールにアクセスすることはできますが、システムがインストールされている社内のプライベート・ネットワークや LAN にはアクセスできません。
- レポート結果が保持されるよりも長い期間、自身の E メールにアクセスしていない場合、それらの結果はリンクをクリックしても使用可能になりません。例えば、結果が 7 日間保持されるのに対し、2 週間の休暇を取っていたユーザーの E メールには、7 日よりも前の結果に対するリンクが含まれている可能性があり、それらのリンクは機能しません。

凍結される受信者リンクについて

プロセスが一度実行されると、既存の受信者リストは凍結されます。 これは、以下のことを意味します。

- リストから受信者を削除できません。
- 既存の受信者をリスト内で上位または下位に移動できません。
- リストの末尾にはいつでも受信者を追加でき、追加した時点で新規受信者を位置変更することは可能です。
- リスト上の受信者の Guardium ユーザー・アカウントが削除された場合、 その受信者は admin ユーザー・アカウント (削除不可) で 置き換えられます。したがって、削除された受信者に送信される予定であったすべての E メール通知を admin ユーザーが受信し、admin ユーザーはその受信者に対してリリースされたすべての結果に対処する必要があります。
- 既存のプロセスに対して完全に異なる受信者セットを作成する必要がある場合、 オリジナルのプロセスを非アクティブ化し、そのコピーを作成して、 コピー・バージョンの受信者リストに変更を加えた後、保存します。

結果を受信者にリリースする方法

結果は、受信者リストにリストされている Guardium ユーザーにリリースされます。このとき、以下のように「継続」チェック・ボックスに準拠します。

- 「継続」チェック・ボックスにマークが付けられている場合、配布は中断なしでリストの次の受信者に継続されます。
- 「継続」チェック・ボックスがクリアされている場合、次の受信者への配布は、現行の受信者が必要なアクション (レビューまたは署名) を実行するまで保留になります。

例えば、以下のようにワークフロー・プロセスを定義するとします。

- DBA - すべての DBA は、同時に結果を受け取ります。 各 DBA は、それぞれに関連付けられたサーバー IP に基づいて異なる結果セットを受信します。
- すべての DBA が署名付けされたときにのみ、DBA マネージャーが結果を表示できます。
- DBA マネージャーがレポートをリリースしたときにのみ、監査員が結果を表示できます。
- すべての監査員は、同時にレポートを受け取りますが、各結果に署名する必要があるのは、そのうちの 1 人 (任意) の監査員だけです。 その他の監査員は、結果に署名が付けられたときに更新されます。
- 監査員は、結果を監査マネージャーにエスカレートすることができます。

このフローを定義する手順は、次のとおりです。

- DBA グループが最初の受信者として指定されます。
- DBA マネージャーは、リストでその次に位置します。
- 監査員ロール (グループではない) は、リストでその次に位置します。 いずれかの監査員が署名し、他の監査員は通知を受けることができます。 また、監査員は結果セットを監査マネージャーにエスカレートすることができます。
  注: 現行の受信者によって「継続」ボタンにマークが付けられている場合にのみ、次の受信者に結果が配布されます。 これは、レビュー/署名機能とは完全に異なるもので、レビュー/署名機能には全く依存しません。
  注: CSV または CEF ファイルにエクスポートされたプロセス結果は、Guardium アーカイブおよびエクスポート・メカニズムによって、別のネットワーク・ロケーションに送信されます。これらの結果は、受信者リストや署名アクションの影響を受けません。 これらは、Guardium CSV/CEF エクスポート・スケジュール (定義されている場合) の対象となり、 最終的な格納先となるディレクトリーに認可されているアクセス権限の影響を受けます。

監査タスク出力を CSV、CEF、または PDF ファイルにエクスポート

他のアプリケーションが使用可能な情報を含んだレポート、または 大量のデータを含んだレポートを、別のファイル・フォーマットでエクスポートすることができます。レポート、エンティティー監査証跡、およびプライバシー・セット・タスクの出力は CSV (Comma Separated Value) ファイルに、 データベース・アクティビティー・レポートの出力は ArcSight Common Event Format (CEF) ファイルにエクスポートすることができます。

さらに、CEF および CSV ファイルの出力を syslog に書き込むことができます。 リモート syslog 機能を使用する場合、出力 CEF/CSV ファイルがリモート syslog のロケーションに 直ちに送信されます。remote syslog 関数により、 メッセージを各ファシリティーと重大度の組み合わせから、特定のリモート・システムに送信することができます。 詳しくは、remotelog (syslog) CLI コマンドの説明を参照してください。

CSV ファイルや CEF ファイルの各レコードは、レポートの 1 行を表しています。

標準タスク出力に置き換わるのではなく、追加する形で、エクスポート・ファイルが作成されます。 これらのファイルは、以下を行う必要がある場合に便利です。

- インフラストラクチャー (Qradar、ArcSight、Network Intelligence、LogLogic、TSIEM など) 内の 既存の SIEM (Security Incident and Event Manager) との統合。
- 非常に大規模なコンプライアンス・タスク結果セットのレビューおよび分析。 (Web での表示用のタスク結果セットの出力は、5,000 行までに制限されています。一方、CSV または CEF エクスポート・ファイルに書き込まれる行数に制限はありません。)

CSV および CEF エクスポート・ファイルは、次のフォーマットで名前が付けられ、Guardium システムに格納されます。

```
process_task_YYYY_MMM_DD-HHMMSS.<csv | cef>
```

ここで、process は監査プロセス定義で定義したラベル、 task はプロセス内の各タスクに定義可能な第 2 レベルのラベル、 YYYY_MMM_DD-HHMMSS はタスク実行時に作成される日時スタンプです。

Guardium システム上の CSV または CEF エクスポート・ファイルには、直接アクセスすることはできません。Guardium 管理者は、「CSV/CEF エクスポート」機能を使用して、これらのファイルを Guardium システムからネットワーク上の他のロケーションに移動する必要があります。これらのファイルにアクセスするには、Guardium 管理者に確認の上、 これらのファイルがコピーされたロケーションを判別してください。

エクスポート・ファイルが Guardium システムの外部に送信されることには、次の 2 つの重要な意味があります。

- これらのファイルのリリースは、監査プロセスに定義された結果配布計画に関連付けられていません。 これらのファイルは、Guardium 管理者が定義したスケジュールでエクスポートされます。
- 一度「CSV/CEF エクスポート」機能を実行すると、「CSV/CEF エクスポート」操作で 定義された宛先ディレクトリーにアクセス可能なユーザーであれば (Guardium ユーザーであるかどうかを問わず)、 すべてのエクスポート・ファイルを使用できるようになります。このため、Guardium 管理者は、 Guardium CSV/CEF エクスポート宛先ディレクトリーから、適切なアクセス権限を備えた ディレクトリーに、エクスポート・ファイル・セットをコピーする追加の ジョブを (Guardium システムの外側で) スケジュールする場合があります。

CSV/CEF エクスポート・アクティビティーは、統合/アーカイブ・アクティビティー・レポートで使用可能です。

注: 監視データ・レベルでのセキュリティーが有効になっている場合、監査プロセスの出力 (ファイルを含む) がフィルタリングされ、ユーザーは、自身に割り当てられたデータベースの情報だけを見ることができます。E メール受信者に添付ファイルとして送信されるファイル がフィルターに掛けられます。ただし、マシンにローカルにダウンロードされ、「結果エクスポート」機能を使用して他の場所に移動されたファイルは、データ・レベル・セキュリティー・フィルター操作の対象になりません。CSV/CEF エクスポートについて詳しくは、 このトピックで後述する『CSV/CEF エクスポート』を参照してください。

次の表は、監査プロセス・ファイルを CSV/CEF/PDF にエクスポートした場合の動作を要約しています。

表 1. 監査タスク出力を CSV、CEF、または PDF ファイルにエクスポート

機能	レベル	CSV	CEF	PDF
E メールに添付	受信者	「全詳細」ラジオ・ボタン -->「PDF」チェック・ボックス	N/A	「全詳細」ラジオ・ボタン -->「PDF」チェック・ボックス ラジオ・ボタンは、受信者 PDF のみを対象としています。
ファイルのエクスポート	タスク	「CSV ファイルへのエクスポート」チェック・ボックス	「CSV ファイルへのエクスポート」チェック・ボックス	「CSV ファイルへのエクスポート」チェック・ボックス
空の場合に報告、および Empty = yes の場合に承認	受信者	エクスポートに影響なし (空のファイルはエクスポートされます) 添付ファイル、E メールを添付しません	エクスポートに影響なし (空のファイルはエクスポートされます) 添付ファイル、E メールを添付しません	エクスポートに影響なし (空のファイルはエクスポートされます) 添付ファイル、E メールを添付しません
zip 添付ファイル	監査プロセス	ファイルが生成されない場合、何も zip しません すべての CSV を 1 つの zip ファイルにマージ	N/A	ファイルが生成されない場合、何も zip しません PDF は zip されません
圧縮 (エクスポート)	タスク	CSV ファイルごとに別ファイルで圧縮	CSV ファイルごとに別ファイルで圧縮	PDF は圧縮されません

監査タスク出力における「zip して E メール」および「圧縮」の機能

「zip して E メール」は、「監査タスク・エクスポート」の最上位レベルのコントロールです。 「zip して E メール」することで、CSV または CEF ファイル・セットが生成されます。 PDF は zip されることも、圧縮されることもありません。

圧縮は個々のファイルに対して機能します。

注: CSV 添付ファイルでは、「zip して E メール」がクリアされている場合で あっても、「圧縮」を適用できます。「圧縮」は、タスクごとに行えます。 そのため、同じ E メールで、1 つの監査タスクは .csv ファイルを、別の監査タスクは .csv.gz ファイルを送信することができます。

「zip して E メール」および「圧縮」の相互作用は、以下のようになります。

- 「zip して E メール」がチェックされている場合 (「圧縮」がチェックされているかどうかに関係なく) CSV ファイルの 1 つの zip ファイルが添付ファイルになります。

- 「zip して E メール」がチェックされておらず、「圧縮」がチェックされている場合、 csv.gz ファイル・セットが添付ファイルになります。
- 「zip して E メール」と「圧縮」がいずれもチェックされていない場合、 csv ファイル・セットが添付ファイルになります。
- 「圧縮」がチェックされている場合、「すべてダウンロード」は csv.gz になります。
- 「圧縮」がクリアされている場合、「すべてダウンロード」は csv になります。
- 「圧縮」がチェックされている場合も、クリアされている場合も、「表示のダウンロード」は csv のままになります。
- 「圧縮」がチェックされている場合、CSV/CEF ファイルのエクスポートは gzip されます。
- 「圧縮」がクリアされている場合、CSV/CEF ファイルのエクスポートは gzip されません。

SCAP または AXIS へのエクスポート

「監査プロセス定義」の「タスクの新規追加」セクションで、「セキュリティー・アセスメント」の「タスク・タイプ」を 選択すると、いくつかの選択項目 (「AXIS xml のエクスポート」および 「SCAP xml のエクスポート」) が表示されます。監査プロセスの結果を保存するには、および「結果エクスポート」(「管理」 > 「データ管理」 > 「結果エクスポート (ファイル)」) でセットアップした宛先に XML ファイルを転送するには、これらの選択肢のいずれかを選択します。他の選択項目 (「レポート」、「差異」、「レポートと差異」) は PDF 形式を構成するためのものです。

SCAP は、Security Content Automation Protocol です。AXIS は、Apache EXtensible Interaction System であり、 QRadar によって使用されます。

レポートの作成または変更

「レポート・ビルダー」を使用すると、レポートを作成またはカスタマイズできます (行への強調表示色の適用など)。「レポート・ビルダー」を開くには、「レポート」 > 「レポート構成ツール」 > 「レポート・ビルダー」にナビゲートします。

監査ワークフロー・プロセスの作成

1. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートして「監査プロセス・ビルダー」を開きます。
2. 「新規」ボタンをクリックして「監査プロセス定義」パネルを開きます。「監査プロセス定義」パネルは、「一般」、 「受信者」、および「タスク」という 3 つのセクションに分割されます。
3. 最初に、「タスク」セクションに進みます。 プロセスを保存する前に、少なくとも 1 つの監査タスクを定義する必要があります。選択項目を設定する各タスクを順に実行します。 監査プロセスに含める各監査タスクに該当する手順を実行してください。このセクションで詳細を示すタスクの選択項目は、 以下のとおりです。
   - レポート・タスクの定義
   - セキュリティー・アセスメント・タスクの定義
   - エンティティー監査証跡タスクの定義
   - プライバシー・セット・タスクの定義
   - 分類プロセス・タスクの定義
   - 外部フィード・タスクの定義
4. 「受信者」セクションに進みます。 ドロップダウン・ボックスを開いて、プロセスの受信者を追加します。『受信者の追加』を参照してください。必要なアクション、To-do リストへの追加、E メール通知、および継続的な配布を決定するには、チェックを付ける必要があります。 この場合も、『受信者の追加』で、これらの選択項目の設定に関する完全な詳細を参照してください。
5. 「一般」セクションに進みます。「記述」ボックスに名前を入力します。 アポストロフィ文字は含めないでください。
6. 「アクティブ」ボックスにチェック・マークを付け、 このプロセスにスケジュールを関連付けます。
7. 保存期間の期限が切れた後にオフラインで結果を保存する場合は、「結果のアーカイブ」ボックスにマークを付けます。 アーカイブされた結果は、後ほど、システムにリストアして再度表示することができます。
8. 「Archive Result purge before Reviewed」ボックスを使用すると、すべてのレビューアーのレビューが完了し、すべてのサインオフが行われ、すべてのワークフロー・アクティビティーが満たされるまで結果を保持せずに特別プロセスの結果が削除されます。 この機能により、ユーザーは、結果がレビューされたかどうかに関係なく、指定した期間 (1 日など) の結果をオプションで削除することができます。
9. 「最低保持期間」の「(n) 日」または「(n) 実行」ボックスに、結果を保存する期間を入力します。 期間は日数 (デフォルトは 0) または実行数 (デフォルトは 5) のどちらかで入力します。 その後、結果がアーカイブされ (「最低保持期間」ボックスにマークが付けられている場合)、システムからパージされます。
   注: 結果は、結果の受信者がいる場合に限り表示されます。受信者を追加し、結果を再実行すると、その実行がドロップダウン・リストに表示されます。
10. 1 つ以上のタスクで CSV または CEF ファイルが作成される場合は、 オプションとして、すべてのファイルに含めるラベルを「CSV/CEF ファイル・ラベル」ボックスに入力できます。 これらのファイルも (Zip 形式に) 圧縮ができます。圧縮するには、「zip してメール」をクリックしてチェック・マークを付けます。
    注: 10240 MB (10.240 GB) を超えるサイズの CSV/CEF ファイルのエクスポートは制限されます。 推奨されるベスト・プラクティスは、「.zip してメール」ボックスにチェック・マークを付けることです。
11. 監査プロセス定義の「E メールの件名」フィールドは、 その監査プロセスの全受信者の E メールに使用されます。 件名には、実行時にその件名を置き換える以下の変数を 1 つ (以上) 含めることができます。
    - %%ProcessName は、監査プロセスの記述に置き換えられます。
    - %%ExecutionStart は、最初のタスクの開始日時に置き換えられます。
    - %%ExecutionEnd は、最後のタスクの終了日時に置き換えられます。

    件名の入力時には、変数 (%% で始まる) の有無と、それらすべてが有効な変数であるかどうかが確認されます。
12. オプションで、セキュリティー・ロールを割り当てます。
13. オプションでコメントを追加します。
14. 該当するボタンをクリックして、監査ワークフロー・プロセスをスケジュールまたは実行します。
15. 「保存」をクリックします。作業を保存する前に、このメニュー画面を離れて他の構成を実行しないでください。 このセクションを離れて、監査タスクに必要な他のものを作成する作業に移ると、 処理中の作業は保存されず、途中まで作成して中断した内容は保持されません。

    例えば、監査プロセス・ビルダーでアセスメント・タスクを定義する場合、 最初に「セキュリティー・アセスメント・ビルダー」に進んでアセスメント・テストを作成し、 次に「データ・ソース定義」に進んでアセスメント対象のデータベースを指定する必要があります。 監査ワークフローの作成時には、作業内容を保存してから他のタスクに進むか、 それら他のタスクを最初に実行してから監査ワークフロー・プロセスを作成してください。

受信者の追加

1. 「受信者」列で、 Guardium 個人ユーザー、グループ、またはロールのドロップダウン・リストから 受信者を選択します。グループまたはロールを選択すると、そのグループの全メンバーまたはそのロールを持つ全ユーザー が結果を受信します。署名が必須の場合、結果に署名する必要があるのは、1 人のメンバーまたはユーザーだけです。
2. 「必要なアクション」列で、次のいずれか 1 つのオプションを選択します。

- レビュー (デフォルト) - この受信者が、結果に署名する必要がないことを指定します。
- レビューと署名 - この受信者が、 (結果をオンラインで表示中に「結果に署名」ボタンをクリックして電子的に) 結果に 署名を付ける必要があることを指定します。

3. 「To-Do リスト」列で、「追加」チェック・ボックスにマークを付けるかクリアして、この受信者が処理中の結果についてそれぞれの「監査プロセスの To-Do リスト」に通知を受けるかどうかを指定します。
   注: 外部サーバーへのファイルの送信を、結果の To-Do リストへの追加や E メールの送信をせずに行う場合は、受信者を指定しない監査プロセスを 定義します。さらに、結果を To-Do リストに追加しないようにするために、「受信者の追加」セクションで「To-Do リスト」チェック・ボックスをクリアし、「受信者」セクションに受信者がある場合はすべて削除し、受信者の追加は行わないでください。
4. 「E メール通知」列で、次のいずれか 1 つのオプションを選択します。
   - なし - この受信者に E メールは送信されません。
   - リンクのみ - E メール通知には、(Guardium システム上の) 結果に対するハイパーテキスト・リンクが含まれます。
   - 結果 - E メールには、結果のコピーが PDF または CSV フォーマットで含まれます。分類タスクやアセスメント・タスクの結果、機密情報が返されることがあるので注意してください。
5. 「継続」列のチェック・ボックスによって、結果の配布が次の受信者に継続される (デフォルト) か、この受信者が適切なアクションを実行するまで停止するどうかが制御されます。「継続」ボックスがクリアされており、 この受信者がグループまたはロールに属している場合、そのグループまたはロールのメンバーである いずれかのユーザーが選択されたアクションを実行すると、結果がリスト上の次の受信者にリリースされます。
   注: 現行の受信者によって「継続」ボタンにマークが付けられている場合にのみ、次の受信者に結果が配布されます。 これは、レビュー/署名機能とは完全に異なるもので、レビュー/署名機能には全く依存しません。
6. 「追加」をクリックしてリストの末尾に受信者を追加し、受信者ごとにこれらのステップを繰り返します。1 人の受信者は必須です。
7. ユーザーではない受信者も許可されます。「E メール」を選択して E メール・アドレスを 入力すると、結果はその E メール・アドレスに送信されます。 ユーザー以外の E メール・アドレスを入力する際には、 データのフィルター操作に使用されるユーザー名の要件があります。 このユーザーは、ログイン・ユーザーと同じであるか、 階層でログイン・ユーザーの下位にいるユーザーでなければなりません。このユーザーは、画面の「受信者」セクションの 新しい列に保存されます。
8. 空の場合は承認 - このチェック・ボックスをチェックすると、タスクのすべてのレポートが空の場合、 次の動作を行います。自動的に結果に署名 (および/または確認済みのマークを付ける)、 自動的に「続行」をクリック (関連付けられている場合)、 E メール通知を送信しない、タスクをそのユーザーの To-Do リストに追加しない、 PDF/CSV/CEF ファイルを作成しない。このチェック・ボックスを使用すると、空の監査結果に自動的に署名が付けられ、その結果は監査結果ログ内で、他の完了した (確認済み/署名済み) 監査結果と同じように表示されます。このアクションは、空のレポートおよび空のセキュリティー・アセスメント結果に適用されます。 セクション『監査タスク出力を CSV、CEF、または PDF ファイルにエクスポート』で、Empty = YES の場合に承認する際の動作を要約した表を参照してください。

CSV または CEF ファイルのエクスポート

レポート、エンティティー監査証跡、およびプライバシー・セット監査タスクの出力は CSV ファイルに、 レポート監査タスクの出力は CEF ファイルにエクスポートすることができます。 「監査タスク」の下の「レポート」、「エンティティー監査証跡」、または「プライバシー・セット」セクションから、 以下手順を実行します。

1. タイトルを選択します。
2. 「CSV/CEF ファイル・ラベル」ボックスに、オプションでファイル・ラベルを入力します。 デフォルトでは、タスクの「記述」がファイル・ラベルになります。このラベルは、生成されるファイル名の 1 コンポーネントになります (他のコンポーネントは、 ワークフロー自動化プロセスで定義されたラベルです)。
3. 「CSV ファイルへのエクスポート」または 「CEF ファイルのエクスポート」にマークを付けます。
   注: CEF ファイル出力は、データ・アクセス・ドメインのレポート (例えば、 アクセス、例外、またはポリシー違反など) にのみ適しています。Guardium セルフ・モニター・ドメイン (統合/アーカイブ、監査プロセス、Guardium ログインなど) のようなその他のドメインは、 CEF 拡張子にマップされません。
4. 「CEF のエクスポート」ファイルを選択した場合、オプションで「CEF を Syslog に書き込む」ボックスにマークを付けて、CEF レコードを syslog に書き込みます。 リモート syslog ファシリティーが有効になっている場合、CEF ファイル・レコードはリモート syslog に書き込まれます。
5. 「圧縮」ボックスがチェックされている場合、 CSV/CEF エクスポート・ファイルは圧縮されます。
6. 「PDF ファイルのエクスポート」ボックスがチェックされている場合、 この監査タスクの (CSV エクスポート・ファイルと同様の名前が付けられた) PDF ファイルが作成され、 CSV/CEF ファイルと一緒にエクスポートされます。
   注: PDF エクスポート・ファイルは、前のステップで「圧縮」ボックスがチェックされている場合であっても、 圧縮されません。

レポート・タスクの定義

コンプライアンス・ワークフロー自動化プロセスの定義をまだ開始していない場合は、この手順を実行する前に、ワークフロー・プロセスを作成してください。使用するレポートがまだ定義されていない場合は、最初に定義してください。

1. 「新規タスクの追加」ペインが開いていない場合、「監査タスクの追加」をクリックします。
2. 「レポート」ラジオ・ボタンをクリックします。
3. 「CSV/CEF ファイル・ラベル」、「CSV/CEF のエクスポート」、「PDF のエクスポート」、「Syslog に書き込む」、「圧縮」には、いくつかの選択項目があります。 『CSV または CEF ファイルのエクスポート』を参照してください。
4. 「PDF オプション」の選択項目には、「レポート」(現在の結果)、「差異」(1 つ前のレポートと新しいレポートの間の差異)、「レポートと差異」(その両方) があります。
   注: 「PDF オプション」の選択内容は、PDF 添付ファイルと PDF エクスポート・ファイルの両方に適用されます。「差異」の結果は、このタスクの初回実行後にのみ適用されます。 前の結果がない場合に、前の結果との差異は存在しません。一度に比較可能な行の最大数は、5000 です。 結果行の数が最大数を超える場合、差異の結果にメッセージ

   「(最初の 5000 行のみ比較)」

   が表示されます。
5. 「タスク・パラメーター」ペインに、すべてのパラメーター値を入力します。 パラメーターは、選択したレポートに応じて異なります。
6. 「適用」をクリックします。

自動実行のための API

デフォルトでは、Guardium アプリケーションにはレポートへの多くの API 関数にリンクした設定データが添付されています。ユーザーには、GUI を通じてレポート・データの API への作成済み呼び出しが提供されます。「レポート」の「API 割り当て」を使用して、事前定義された Guardium レポートまたはカスタム・レポートへの追加 API 関数にリンクできます。メニュー選択項目「自動実行のための API」が「監査タスクの追加」に表示されます。 レポート内に API パラメーターにリンクされたフィールドがある、 該当する事前定義 Guardium レポートまたはカスタム・レポートを選択する際にレポートします。 自動実行のための API メニュー項目が表示される事前定義レポートの例として、 「アクセス・ポリシー違反」、「ディスカバーされたデータベース」、および「Guardium グループの詳細」があります。

ワークフロー・ビルダー

ワークフロー・ビルダーで作成されるイベント・タイプの 正式な順序の管理は、「監査タスク」ウィンドウの「イベントおよび追加列」ボタンをクリックして行います。このボタンは、監査タスクを作成して保存すると表示されます。この追加のボタンは、監査タスクを保存しないと表示されません。以下の手順で、監査タスクを追加する際にこれらのワークフロー・アクティビティーを構成します。

1. 監査タスクを作成して保存します。保存後、追加の「イベントおよび追加列」ボタンが表示されます。
2. この追加のボタンをクリックします。
3. 次の画面で、「イベントおよびサインオフ」ボックスにチェック・マークを付けます。 ワークフロー・ビルダーで作成したワークフローが「イベントおよびサインオフ」の選択項目として表示されます。
4. この選択項目を強調表示します。選択内容を適用 (保存) します。
5. 追加の情報 (会社コード、ビジネス・ユニット・ラベルなど) が、ワークフロー・レポートの 一部として必要である場合は、この情報を画面の「追加列」セクションに追加して、「適用」(保存) をクリックします。 事前定義グループ列または作成したグループ列を選択するには、「タイプ」列を「グループ」に変更します。 完了したら、このウィンドウを閉じます。
6. 監査タスクを適用 (保存) します。監査プロセス定義全体を適用 (保存) します。

この「イベントおよび追加列」ボタンは、すべての監査タスクで表示されます。 このボタンの上にカーソルを置くと、特定の監査タスクにリンクされた「イベント」または「サインオフ」列が監査タスクにある かどうかをユーザーに通知する情報バルーンが表示されます。

注:

監視データ・レベルでのデータ・レベル・セキュリティーが有効な場合、ユーザーに対してユーザーのデータベース情報のみが表示されるよう、監査プロセスの出力がフィルタリングされます。

「監査タスクの追加」内の「レポート」の選択項目は、 「未処理のイベント」および「イベント状況の移行」の 2 つのプロシージャー型レポートです。これら 2 つのレポートを 2 つの新規監査タスクに追加して、すべてのワークフロー・イベントおよび移行の詳細を表示します。 これら 2 つのレポートは、フィルターに掛けられません (監視データ・レベル・セキュリティー・フィルター操作は適用されません)。 これら 2 つのレポートは、admin ユーザーおよび admin ロールを持つユーザー に対するレポート・リストでのみ、デフォルトで選択可能です。

「追加列」ボタンは分類タスクでは使用不可になっています。

監査タスクのコピーを作成。プロセスのコピーを作成している場合、コピー・プロセスを保存する前にコピー・タスクに変更を加えた場合、オリジナル・タスクに関連付けられたワークフローのコピーは作成されません。

イベント状況の削除は、その状況が何らかのイベントの最初の状況ではなく、アクションに使用されていない場合にのみ許可されます。検証では、状況の削除を防止するイベント/アクションのリストが提供されます。

ワークフロー・イベントの所有者または作成者は、このイベントのすべての状況を、これらの状況に対してどのようなロールが割り当てられているかに関係なく、常に見ることが可能です。

セキュリティー・アセスメント・タスクの定義

コンプライアンス・ワークフロー自動化プロセスの定義をまだ開始していない場合は、この手順を実行する前に、ワークフロー・プロセスを作成してください。使用するアセスメントがまだ定義されていない場合は、最初に定義してください。

1. 「新規タスクの追加」ペインが開いていない場合、「監査タスクの追加」をクリックします。
2. 「セキュリティー・アセスメント」ボタンをクリックします。
3. 「セキュリティー・アセスメント」リストから、セキュリティー・アセスメントを選択します。
4. 「PDF の内容」の選択項目には、「レポート」(現在の結果)、「差異」(1 つ前のレポートと新規レポートの間の差異)、 および「レポートと差異」(その両方) があります。
5. 「適用」をクリックします。

注:

監視データ・レベルでのデータ・レベル・セキュリティーが有効な場合、ユーザーに対してユーザーのデータベース情報のみが表示されるよう、監査プロセスの出力がフィルタリングされます。

セキュリティー・アセスメント・タスクが空である場合 (例えば、ロール・セットなしのセキュリティー・アセスメントなど)、 この空のセキュリティー・アセスメントは、「監査ビルダー」のドロップダウン・リストには表示されません。

エンティティー監査証跡タスクの定義

コンプライアンス・ワークフロー自動化プロセスの定義をまだ開始していない場合は、この手順を実行する前に、ワークフロー・プロセスを作成してください。

1. 「新規タスクの追加」ペインが開いていない場合、「監査タスクの追加」をクリックします。
2. 「エンティティー監査証跡」ボタンをクリックします。
3. 監査するエンティティーのタイプを選択します。選択したタイプに応じて、 以下の情報の指定が必要になります。
   - オブジェクト: オブジェクト名を入力します。
   - オブジェクト・グループ: リストからオブジェクト・グループを選択します。
   - クライアント IP: クライアント IP アドレスを入力します。
   - クライアント IP グループ: クライアント IP グループを選択します。
   - サーバー IP: サーバー IP アドレスを入力します。
   - アプリケーション・ユーザー名: アプリケーション・ユーザー名を入力します。
4. 「CSV/CEF ファイル・ラベル」、「CEF を Syslog に書き込む」、「圧縮」、および「PDF のエクスポート」には、いくつかの選択項目があります。『CSV または CEF ファイルのエクスポート』を参照してください。
5. 「タスク・パラメーター」ペインで、ランタイム・パラメーター値を指定します (「開始」および「終了」期間のみが必須です)。
6. 「適用」をクリックします。

注: 監視データ・レベルでのデータ・レベル・セキュリティーが有効な場合、ユーザーに対してユーザーのデータベース情報のみが表示されるよう、監査プロセスの出力がフィルタリングされます。

プライバシー・セット・タスクの定義

コンプライアンス・ワークフロー自動化プロセスの定義をまだ開始していない場合は、この手順を実行する前に、ワークフロー・プロセスを作成してください。使用するプライバシー・セットがまだ定義されていない場合は、最初に定義してください。

1. 「新規タスクの追加」ペインが開いていない場合、「監査タスクの追加」をクリックします。
2. 「プライバシー・セット」ボタンをクリックします。
3. 「プライバシー・セット」リストから、プライバシー・セットを選択します。
4. 「アクセス詳細別レポート」または「アプリケーション・ユーザー別レポート」のいずれかを選択して、 結果のソートおよび表示方法を指定します。
5. 「CSV/CEF ファイル・ラベル」、「CEF を Syslog に書き込む」、「圧縮」、および「PDF のエクスポート」には、いくつかの選択項目があります。『CSV または CEF ファイルのエクスポート』を参照してください。
6. 「期間の開始」および「期間の終了」ボックスに、レポートの開始および終了の日付を入力します。
7. 「適用」をクリックします。

注: 監視データ・レベルでのデータ・レベル・セキュリティーが有効な場合、ユーザーに対してユーザーのデータベース情報のみが表示されるよう、監査プロセスの出力がフィルタリングされます。

分類プロセス・タスクの定義

コンプライアンス・ワークフロー自動化プロセスの定義をまだ開始していない場合は、この手順を実行する前に、ワークフロー・プロセスを作成してください。使用する分類プロセスがまだ定義されていない場合は、最初に定義してください。

1. 「新規タスクの追加」ペインが開いていない場合、「監査タスクの追加」をクリックします。
2. 「分類プロセス」ボタンをクリックします。
   注: 分類プロセスで機密データが返されることがあり、これらの結果が PDF ファイルや CSV ファイルに追加されることに対する警告があります。
3. 「分類プロセス」リストから、分類プロセスを選択します。「適用」をクリックします。

注: 監視データ・レベルでのデータ・レベル・セキュリティーが有効な場合、ユーザーに対してユーザーのデータベース情報のみが表示されるよう、監査プロセスの出力がフィルタリングされます。

外部フィード・タスクの定義

このタイプのワークフロー自動化タスクは、Guardium が収集したデータを外部アプリケーションにフィードし、 データをそのアプリケーションが認識するフォーマットにマッピングします。このタスク・タイプは、 パッチによって使用可能になる、追加のコストを要するフィーチャーです。

注: このフィーチャーを中央マネージャー環境で使用する場合、 外部フィード・パッチを中央マネージャーおよびこのタスクが実行されるすべての管理対象ユニットにインストールする必要があります。

Guardium から外部アプリケーションへのデータのマップについて詳しくは、 購入したオプションの資料を参照してください。

コンプライアンス・ワークフロー自動化プロセスの定義をまだ開始していない場合は、この手順を実行する前に、ワークフロー・プロセスを作成してください。

1. 「新規タスクの追加」ペインが開いていない場合、「監査タスクの追加」をクリックします。
2. 「外部フィード」をクリックします。
3. 「フィード・タイプ」リストからフィード・タイプを選択します。
4. 次に表示されるコントロールは、選択したフィード・タイプに応じて異なります。 特定の外部フィード・タイプに関する追加情報については、『オプションの外部フィード』を参照してください。
5. 「イベント・タイプ」リストから、イベント・タイプを選択します。
6. 「レポート」リストからレポートを 1 つ選択します。選択したレポートに応じて、「タスク・パラメーター」ペインに表示されるパラメーターの数が異なります。
7. 「抽出ラグ」ボックスにフィードが遅延される時間数を入力するか、「継続」ボックスにマークを付けて監査タスクが実行される直前の時間までのデータを組み込みます。
8. 「データ・ソース」ペインで、外部フィードの 1 つ以上のデータ・ソースを指定します。
9. 「タスク・パラメーター」ペインに、すべてのパラメーター値を入力します。 パラメーターは、選択したレポートに応じて異なります。
10. 「適用」をクリックします。

結果の表示または署名

1. コンプライアンス・ワークフロー自動化の結果を開きます。
2. 署名が必要な場合は、「結果に署名」ボタンをクリックしてください。
3. オプション。2これらの結果を別のユーザーに転送するには、「エスカレート」をクリックしてください (セクションの『プロセス結果のエスカレート』を参照)。
4. 「このウィンドウを閉じる」をクリックします。

注: 未処理のイベントがある場合、監査ビューアーからも To-do リストからも結果に署名できません。 未処理のイベントがある場合に、結果への署名が試みられると、以下のメッセージが表示されます。

監査プロセスに署名できません。保留イベントがあります。

この結果に署名する前に、未解決のイベントをすべて更新してください。

注: 監査プロセスの結果を表示している際に、その結果に関連付けられたイベントがある場合、 すべてのイベントが最終状態になるまでは、その結果についての「結果に署名」ボタンが使用可能にならないか、 このユーザーでは (データ・レベル・セキュリティーにより) 表示できない可能性があります。
注: このレポートには、 日付または最終アクション時刻も含まれます。これらは「受信者」と「状況」の間の列にあります。 このレポートには、結果がユーザー AAA によって署名されたことの他に、そのユーザー AAA がこの結果に署名した時間も示されます。

署名または表示せずに結果をリリース

1. 「To-Do リスト」パネルを開きます。
2. 配布リストの次の受信者にリリースする結果の「続行」ボタンをクリックします。
3. 「このウィンドウを閉じる」をクリックします。

結果配布の表示

1. コンプライアンス・ワークフロー自動化の結果を開きます。
2. 「詳細を表示」ボタンをクリックして、「配布状況」パネルを展開します。
3. 「このウィンドウを閉じる」をクリックします。

結果に追加された受信者コメントの表示

1. コンプライアンス・ワークフロー自動化の結果を開きます。
2. 「詳細を表示」ボタンをクリックして、「コメント」パネルを展開します。
   注: これらは、Guardium システムからレポート・ページが取り出された際に結果に添付されたコメントです。独自にコメントを追加する場合、または他の受信者が同時にコメントを追加している場合、(ブラウザーのリフレッシュ機能を使用して) ページをリフレッシュするまでこれらのコメントは表示されません。
3. 「このウィンドウを閉じる」をクリックします。

プロセス結果のエスカレート

プロセス結果の受信者は、結果通知をレビューまたはサインオフ (あるいはその両方) のために、他の受信者に転送できます。 結果をオリジナルの監査およびサインオフ証跡の外側の受信者にエスカレートする場合、 結果に CSV ファイルが含まれていると、そのファイルは通知には組み込まれません。

「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」メニューで「結果をすべてのユーザーにエスカレート」ボックスがチェックされている場合、監査結果の受信者が誰かに関係なく、エスカレーションにシステムのどのユーザーも含めることができます。このボックスにチェック・マークを付けると、監視データ・レベルでのデータ・レベル・セキュリティー が有効になっている場合であっても、監査プロセスの結果がすべてのユーザーにエスカレートされます。 デフォルトでは有効に設定されています。チェック・ボックスが無効になっている (チェック・ボックスに チェック・マークが付けられていない) 場合、監査プロセスのエスカレーションは ユーザー階層の上位レベルのユーザーに対してのみ許可されます。 チェック・ボックスが無効になっており、ユーザー階層がない場合、エスカレーションは許可されません。

また、イベント権限に応じても異なります。例えば、infosec ユーザーは status1 のイベントのみ 表示可能であり、dba ユーザーは status2 のイベントのみ表示可能です。dba ユーザーが受け取る結果は、infosec ユーザーが「エスカレート」をクリックすると表示される結果とは異なります。 infosec が dba に対してエスカレートすることは可能であり、その場合 dba は行が含まれない監査結果を受け取ることになります。

1. 転送するワークフロー自動化結果が開かれていない場合は、開いてください。
2. 「エスカレート」をクリックします。
3. 「受信者」リストから受信者を選択します。
4. 「必要なアクション」列で、 「レビュー」(デフォルト) または「レビューと署名」を選択します。
5. 「エスカレーション」ボタンをクリックして、操作を完了します。

注:

監査プロセスの結果をユーザー・グループに対してエスカレートすることはできません。ユーザーまたはロールに対してのみエスカレートできます。

To-Do リストに既に結果を得ているユーザーに対してエスカレートする際には、 追加の E メールを送信するかどうかを訊ねるポップアップ・メッセージが表示されます。yes の場合、追加の E メールがそのユーザーに送信されますが、To-Do リストは増分されません。

コンプライアンス・ワークフロー自動化プロセスのスケジュールまたは実行

1. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートして「監査プロセス・ビルダー」を開きます。
2. 「プロセス選択リスト」からプロセスを選択します。
3. 「変更」をクリックして、「監査プロセス定義」パネルを開きます。
4. プロセスを 1 回実行する場合は「今すぐ 1 回実行」を、 プロセスのスケジュールを定義する場合は「スケジュールの変更」をクリックします。
   注: プロセスにスケジュールを定義した後、 プロセスは「アクティブ」とマークが付けられている場合のみ、そのスケジュールに従って実行されます。監査プロセスをアクティブまたは非アクティブにする方法については、次のセクションを参照してください。

コンプライアンス・ワークフロー自動化プロセスのアクティブ化または非アクティブ化

監査プロセスにスケジュールを定義した後、プロセスは「アクティブ」とマークが付けられている場合のみ、 そのスケジュールに従って実行されます。

監査プロセスをアクティブまたは非アクティブにする手順は、次のとおりです。

1. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートして「監査プロセス・ビルダー」を開きます。
2. 「プロセス選択リスト」から監査プロセスを選択します。
3. 「変更」をクリックします。
4. 「監査プロセス定義」パネルで、「アクティブ」ボックスにマークを付けて、プロセスをスケジュールに従って実行開始します。 または、「アクティブ」ボックスをクリアして、(定義されたスケジュールを無視して) プロセスの実行を停止します。
   注: プロセスをアクティブにしているが、 スケジュールがない場合は、「スケジュールの変更」をクリックしてプロセス実行のスケジュールを定義してください。
5. 「保存」をクリックします。

- 監査ワークフローの作成方法
  あらかじめ設定したスケジュールで事前定義されたレポートを作成する監査プロセス・ワークフローを作成し、レビューと署名のためにレポートをデータベース管理者に割り当て、レビュー済みのレポートがさらに上司のレビューと署名のために送られるようにします。
- ワークフロー・プロセスの結果を開く
  「表示」を使用して、ワークフロー・プロセスの結果を表示します。
- Guardium グループを使用してワークフローを配布する方法
  受信者グループ・オプションを使用することによって、事前定義されたカスタム・マッピングに基づいてそれぞれの結果をそれぞれの Guardium ユーザーに送信する、単一のコンプライアンス・ワークフロー監査プロセスを定義します。

- 監査プロセスの To-do リスト
  このトピックでは、「監査プロセスの To-do リスト」と、これを開いて使用するために必要なステップについて説明します。

親トピック: モニターおよび監査

監査ワークフローの作成方法

あらかじめ設定したスケジュールで事前定義されたレポートを作成する監査プロセス・ワークフローを作成し、レビューと署名のためにレポートをデータベース管理者に割り当て、レビュー済みのレポートがさらに上司のレビューと署名のために送られるようにします。

このタスクについて

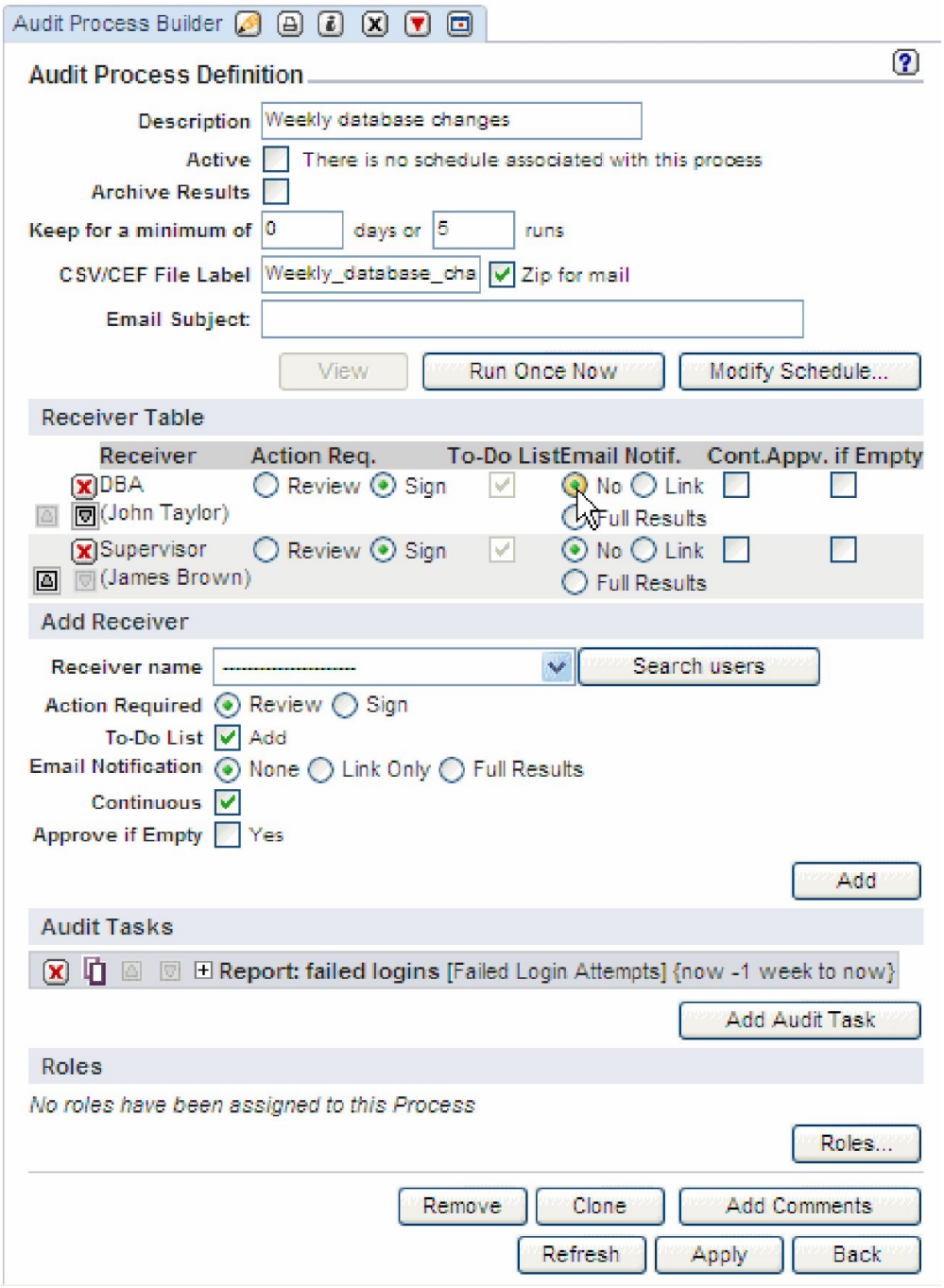
顧客の監査プロセスのワークフロー・ステップを自動化します。

これについての詳細は、『コンプライアンス・ワークフロー自動化』トピックを参照してください。

手順

1. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートして「監査プロセス・ファインダー」を開きます。
2. 「新規」ボタンをクリックして、「監査プロセス定義」パネルを開きます。

   「監査プロセス定義」パネルは、「一般」、「受信者の表」および「監査タスク」の 3 つのセクションに分かれています。



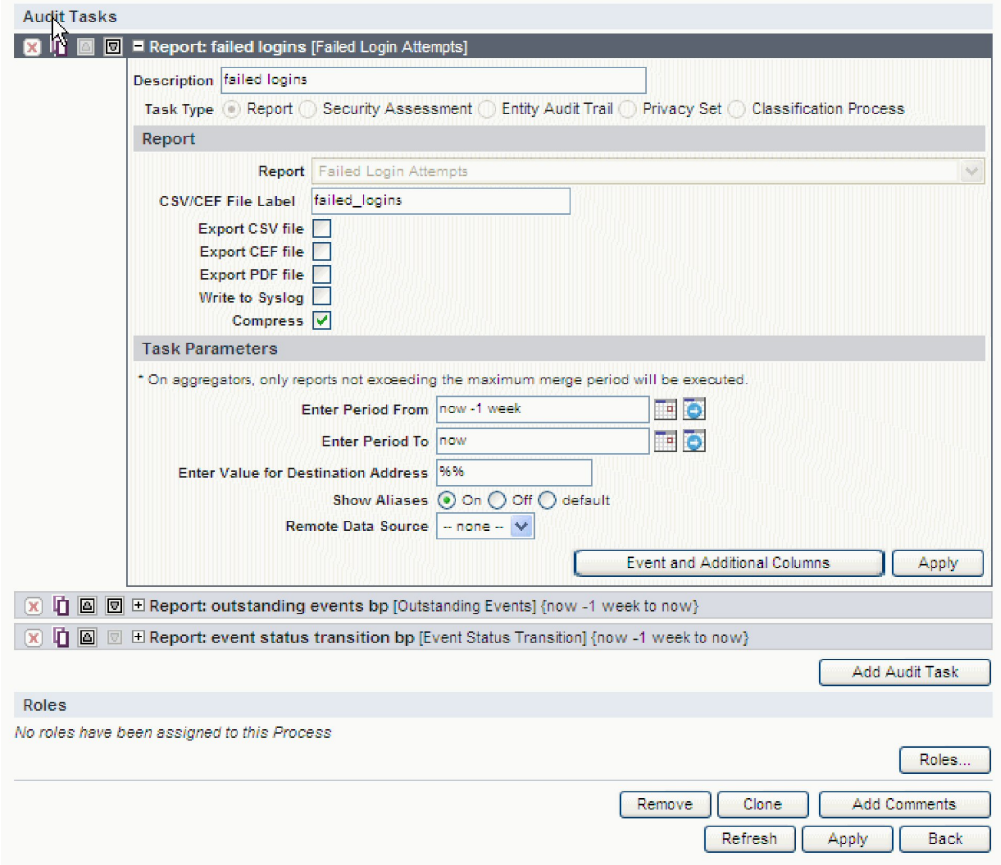
「監査プロセス・ビルダー」メニュー画面

3. 「一般」セクションに進みます。「記述」ボックスに名前を入力します。 アポストロフィ文字は含めないでください。
4. 「アクティブ」ボックスにチェックを付けて、プロセスにスケジュールを関連付けます。 プロセスを保存するには、少なくとも 1 つの監査タスクが定義されている必要があります。
5. 保存期間の期限が切れた後にオフラインで結果を保存する場合は、「結果のアーカイブ」ボックスにマークを付けます。 アーカイブされた結果は、後ほど、アプライアンスにリストアして再度表示することができます。
6. 「最低保持期間」の「(n) 日」または「(n) 実行」ボックスに、結果を保存する期間を入力します。 期間は日数 (デフォルトは 0) または実行数 (デフォルトは 5) のどちらかで入力します。 その後、結果はアーカイブされ (アーカイブ・ボックスにマークが付いている場合)、アプライアンスからパージされます。
7. 1 つ以上のタスクで CSV または CEF ファイルが作成される場合は、 オプションとして、すべてのファイルに含めるラベルを「CSV/CEF ファイル・ラベル」ボックスに入力できます。 これらのファイルも (Zip 形式に) 圧縮できます。圧縮するには、「CSV を zip してメール」ボックスをクリックしてチェック・マークを付けます。
8. 監査プロセス定義の「E メールの件名」フィールドは、その監査プロセスの全受信者の E メールに使用されます。 件名には、実行時にその件名を置き換える以下の変数を 1 つ (以上) 含めることができます。
   - %%ProcessName は、監査プロセスの記述に置き換えられます。
   - %%ExecutionStart は、最初のタスクの開始日時に置き換えられます。
   - %%ExecutionEnd は、最後のタスクの終了日時に置き換えられます。

   件名の入力時には、変数 (%% で始まる) の有無と、それらすべてが有効な変数であるかどうかが確認されます。
9. 「受信者」セクションに進みます。 ドロップダウン・ボックスを開いて、プロセスの受信者を追加します。 詳しい説明は、 『コンプライアンス・ワークフロー自動化』のトピックの「受信者の追加」を参照してください。 必要なアクション、To-do リストへの追加、E メール通知、および継続的な配布を決定するには、チェ

ックを付ける必要があります。 これら項目の設定についても、詳しい説明は『受信者の追加』を参照してください。 この例では、受信者の「継続」ボックスにはチェックを付けません。 「継続」チェック・ボックスにマークが付けられている場合、 配布は中断なしでリストの次の受信者に継続されます。 「継続」チェック・ボックスがクリアされている場合、 次の受信者への配布は、現行の受信者が必要なアクション (レビューまたは署名) を実行するまで保留になります。 この例では、上司に送る前に、DBA がレポートを見て署名する必要があります。

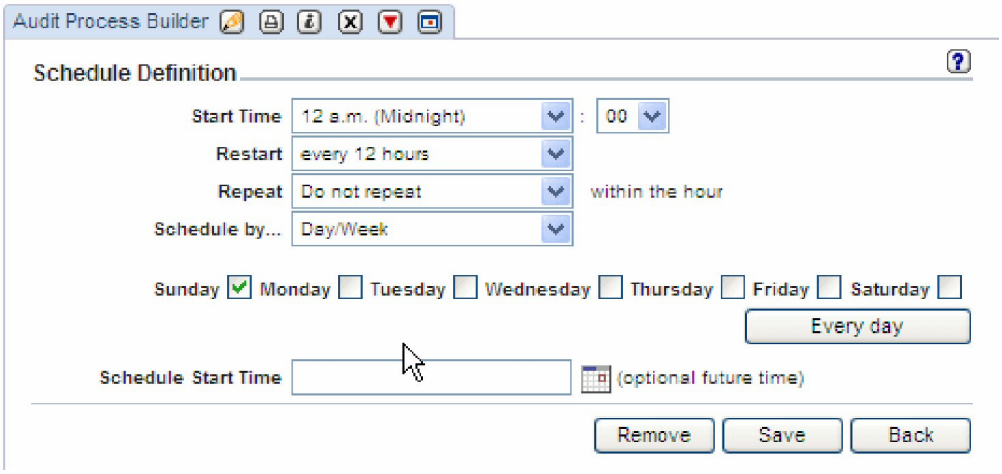
10. 「タスク」セクションに進みます。 プロセスを保存する前に、少なくとも 1 つの監査タスクを定義する必要があります。
11. レポート・タスクを定義します。
    a. 「タスクの新規追加」ペインが開いていない場合は、 「監査タスクの追加」をクリックします (図を参照)。
    b. 「レポート」ボタンをクリックします。
    c. 必要に応じて、CSV または CEF ファイル出力を作成して、syslog に書き込みます。
    d. 「タスク・パラメーター」ペインに、すべてのパラメーター値を入力します。 パラメーターは、選択したレポートに応じて異なります。
    e. 「適用」をクリックします。



監査タスク - レポート

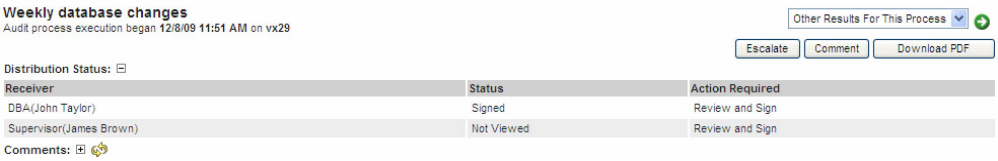
12. オプションでセキュリティー・ロールを割り当てます。
    a. 1 つ以上のセキュリティー・ロール (レポート定義など) を割り当てる 項目を開くか、選択します。
    b. 「ロール」ボタンを クリックします。
    c. 「セキュリティー・ロールの割り当て」パネルで、割り当てるすべてのロールにマークを付けます (自分のアカウントに 割り当てられたロールのみが表示されます)。
    d. 「適用」をクリックします。
13. オプションでコメントを追加します。
14. 監査ワークフロー・プロセスをスケジュールまたは実行するためのボタンをクリックします (リンクを参照)。
15. 「適用」をクリックします。
16. コンプライアンス・ワークフロー自動化プロセスのスケジュールまたは実行
    「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートして「監査プロセス・ファインダー」を開きます。
    a. 「プロセス選択リスト」からプロセスを選択します。
    b. 「変更」をクリックして、 「監査プロセス定義」パネルを開きます。
    c. プロセスを 1 回実行する場合は「今すぐ 1 回実行」をクリックし、プロセスのスケジュールを定義する場合は「スケジュールの変更」をクリックします。

注: プロセスにスケジュールを定義した後、 プロセスは「アクティブ」とマークが付けられている場合のみ、そのスケジュールに従って実行されます。



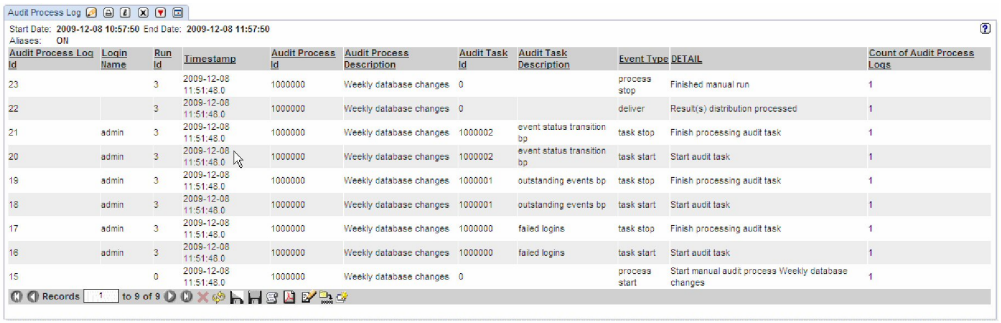
17. レポートの署名とレビュー

    レポートを実行すると、レポートから配布状況を監視できます。 この例では、DBA はレポートを表示、署名していますが、上司はまだです。



    配布状況

    「監査プロセス・ログ」レポートには、すべてのタスクに関する 詳細なアクティビティー・ログが、開始時刻および終了時刻も含めて示されます。 このレポートは、「レポート」 > 「Guardium 運用レポート」 > 「監査プロセス・ログ」にナビゲートすると使用できます。監査タスクには、開始時刻と終了時刻が示されます。



    監査プロセス・ログの例

親トピック: 監査プロセスの作成

ワークフロー・プロセスの結果を開く

「表示」を使用して、ワークフロー・プロセスの結果を表示します。

以下のいずれかを実行します。

- 「ワークフロー自動化 To-Do リスト」(『監査プロセスの To-do リスト』を参照) を開き、表示または署名する結果の「表示」をクリックします。
- To-do リストまたは結果へのハイパーテキスト・リンクが含まれている E メール通知を受信した場合は、それらのリンクの 1 つをクリックして、E メールから直接 To-do リストまたは結果を開きます。E メールにアクセスしているロケーションにおける Guardium システムへのアクセス権限を持っている必要があります (持っていない場合、これらのリンクは機能しません)。Guardium システムにログインしていない場合は、ログインするようプロンプトが表示されます。

注: 新しい管理対象ユニットを中央マネージャーに登録するときに、監査結果が表示できないことがあります。アプリケーションは、管理対象ユニットが中央マネージャーに登録される前のタイム・スタンプが含まれている結果を表示しません。登録のタイム・スタンプには中央マネージャーの時刻が使用され、監査結果のタイム・スタンプには管理対象ノードの時刻が使用されます。このため、中央マネージャーの時刻が管理対象ユニットの時刻より先行している場合、管理対象ユニットの時刻が登録の時刻を過ぎるまでは、管理対象ユニットで生成された結果は表示されません。 これは、2 台のマシンのロケーションによって発生する可能性は低く、24 時間以内で起こります。管理対象ユニットでの監査プロセスの結果は、登録後 24 時間以内に表示できる必要があります。
親トピック: 監査プロセスの作成

Guardium グループを使用してワークフローを配布する方法

受信者グループ・オプションを使用することによって、事前定義されたカスタム・マッピングに基づいてそれぞれの結果をそれぞれの Guardium ユーザーに送信する、単一のコンプライアンス・ワークフロー監査プロセスを定義します。

得られる価値: 単一の監査プロセスを設定し、適切な結果を適切なマネージャーに配布します。これにより、受信者ごとに別個の監査プロセスを作成せずに済みます。

IBM Security Guardium のコンプライアンス・ワークフロー自動化では、スケジュールに基づいて、レポート、分類結果、およびセキュリティー・アセスメントの結果を Guardium ユーザーに自動配信します。結果の受信者は、Guardium ユーザー、Guardium のロール、またはユーザー・グループとして定義できます。

例えば、15 人の DBA マネージャーがいる大規模な組織において、マネージャーは他のマネージャーの DBA の活動を見ることなく、自らが管理する DBA の活動をレビューする必要がある、という場合を考えてみます。1 つの解決方法としては、マネージャーごとに 1 つずつの 15 種類の監査プロセスを設定する方法があります。 この方法は構成にたいへん時間がかかります。また、各監査プロセスのスケジュールを別々に設定する必要があり、15 種類すべての監査プロセスに対してすべての全体的な変更を個別に行う必要があるため、管理が困難です。

一方、ユーザー・グループ配布方式では、単一の監査プロセスの設定が可能で、マネージャー/DBA のマッピングに基づいて、適切な結果が各マネージャーに配布されます。このプロセスでは事前に必要な構成が多くなりますが、保守時間が削減されます。 スケジュールする必要がある監査プロセスは 1 つだけであり、変更を適用する必要があるロケーションも 1 つだけです。

ユーザー・マッピング

プロセスの最初のステップは、レポート配布の基礎となる、Guardium 内のデータ・エレメントに、ユーザーをマップすることです。このドキュメントで使用される例はオブジェクトに基づいていますが、これらの概念は Guardium 内の任意のデータ・エレメントに適用することもできます。

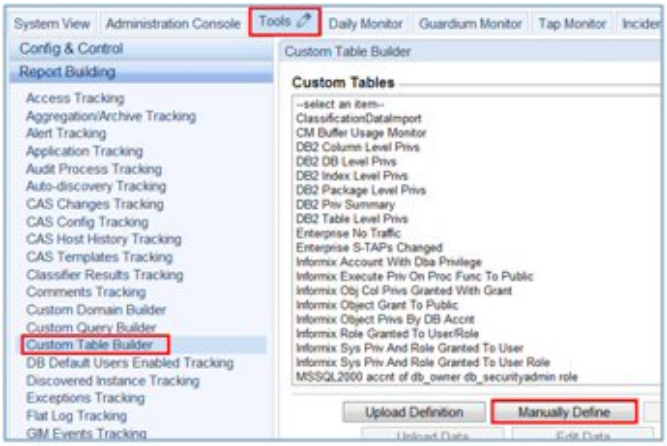
例: 3 人のユーザーは、データベース・サーバー内の監査要件 (PCI、HIPPA、および CCI) に基づいて、3 つの異なる表のセットに対し、以下のような責任を持っています。

表 1. ユーザーと表/オブジェクト

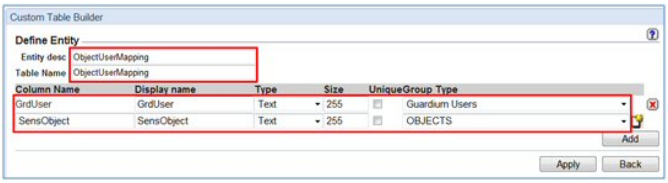
ユーザー	表/オブジェクト
User01	db2inst1.cc_numbers
User01	db2inst1.ccn
User02	db2inst1.ADDRESSES
User02	db2inst1.SSN_NUMBERS
User02	db2inst1.G_CUSTOMERS
User02	db2inst1.G_EMPLOYEES
User02	db2inst1.G_FUNDS
User03	db2inst1.doctor
User03	db2inst1.medicare
User03	db2inst1.med_history

この表を、手動またはデータ・アップロードによって、Guardium 内にカスタム表として追加する必要があります。以下のステップで、カスタム表を手動で作成する方法について説明します。スクリーン・ショットは「管理者」ユーザー・インターフェースのものですが、「ユーザー」ユーザー・インターフェース内からもアクセスできます。

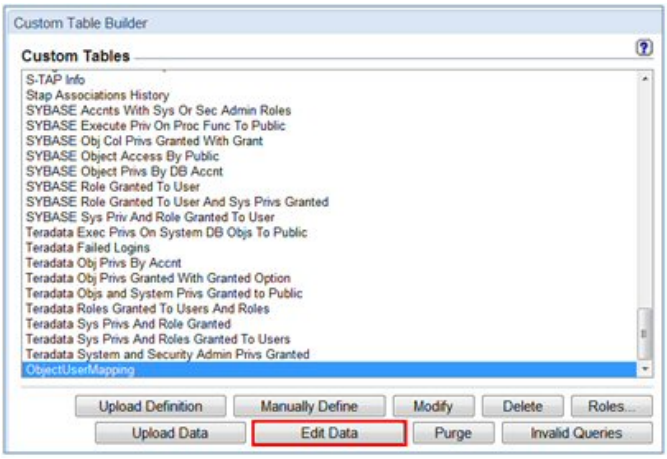
1. 「レポート」 > 「レポート構成ツール」 > 「カスタム表ビルダー」にナビゲートし、**「手動定義」**ボタンを押します。



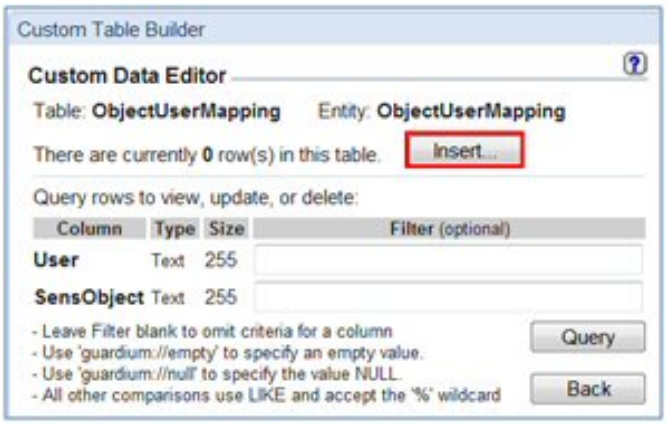
2. **「カスタム表ビルダー」**画面で、表のレイアウトを定義します。**「グループ・タイプ」**が Guardium 内の正しいデータ・エレメントと一致していることを確認します。完了したら**「適用」**および**「戻る」**を押します。



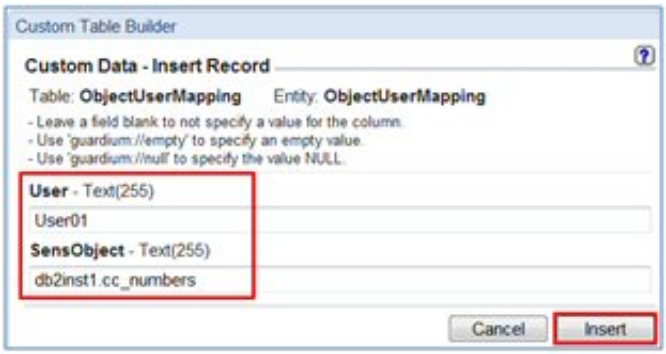
3. **「データの編集」**を押して、レコードを手動で追加します。なお、大量のデータがある場合は、**「データのアップロード」**を選択して外部データ・ソースからインポートします。



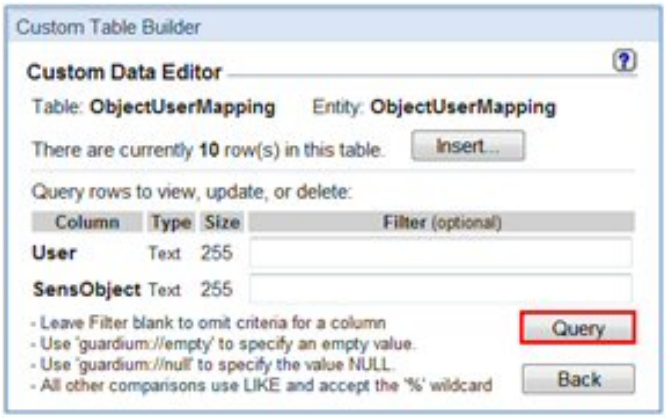
4. 「**挿入**」を押します。



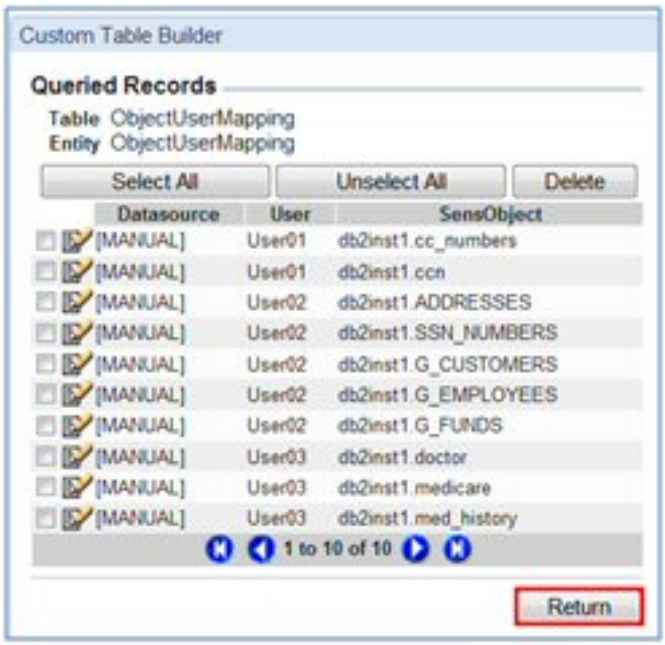
5. 値の組み合わせを入力し、すべての必須レコードを追加したら、「**挿入**」を押します。



6. 完了したら、「**照会**」ボタンを押して、データをレビューします。



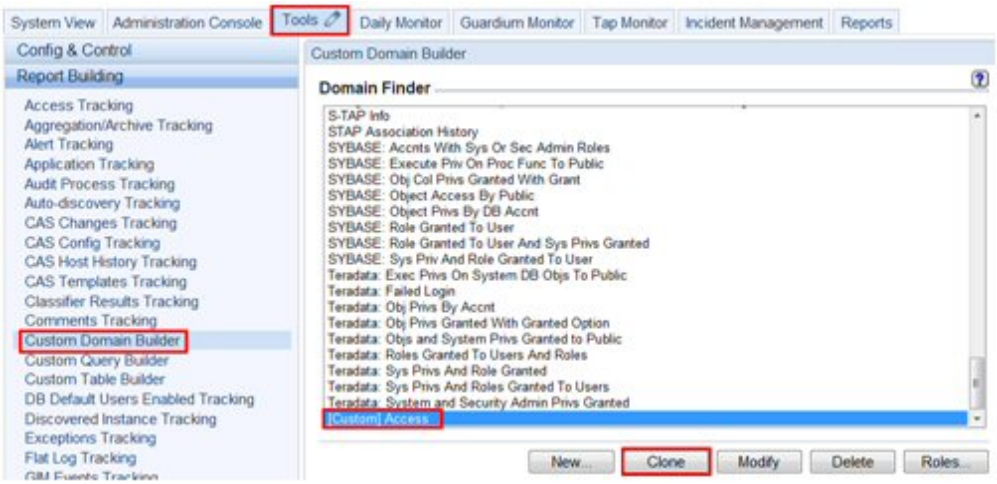
7. 完了したら、「先頭に戻る」を押します。



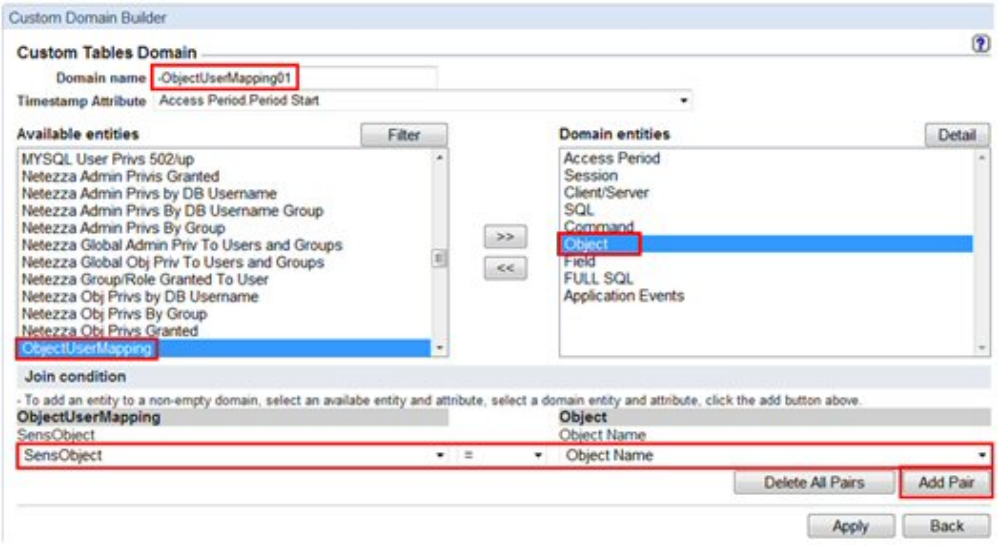
カスタム・ドメイン

次に、カスタム・ドメインを使用して、このカスタム表を Guardium 表構造に結合します。

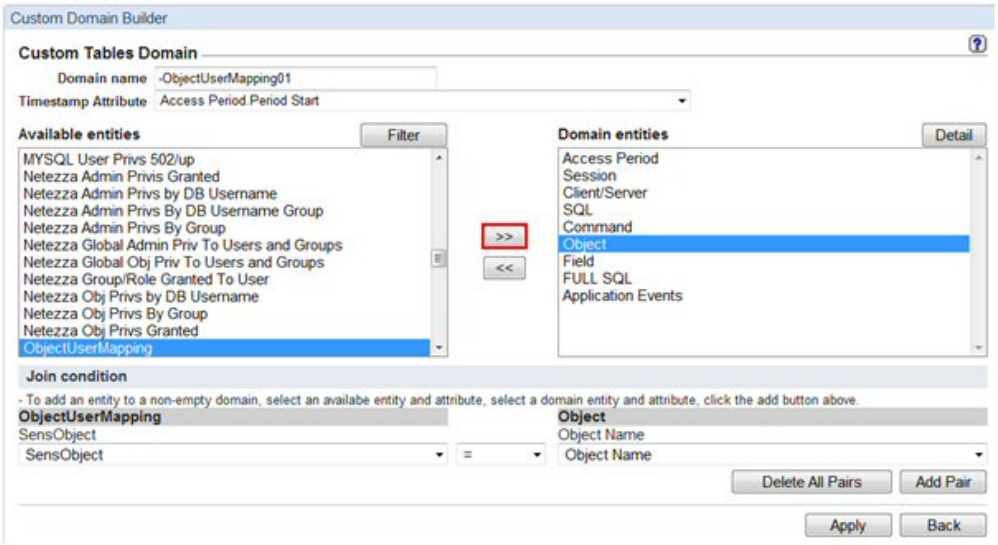
1. 「レポート」 > 「レポート構成ツール」 > 「カスタム・ドメイン・ビルダー」にナビゲートします。 *「[カスタム] アクセス」*を強調表示して、**「コピー」**を押します。



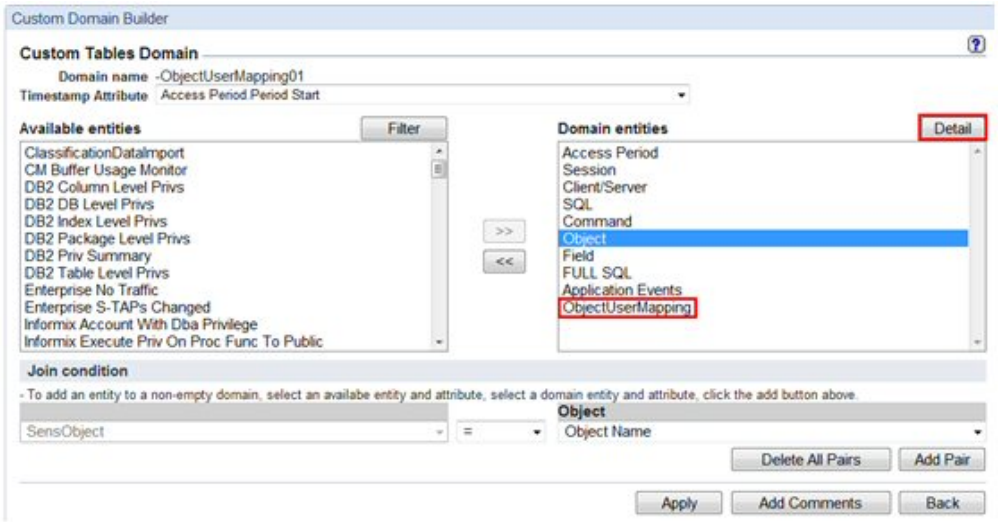
2. 「カスタム・ドメイン・ビルダー」で、次を行います。
   a. **「使用可能エンティティー」**で作成された新しい表を強調表示します
   b. **「ドメイン・エンティティー」**にある、カスタム表を結合する表を強調表示します。
   c. **「結合条件」**で、結合を作成する各表のフィールドを選択し、**「ペアの追加」**を押します



3. 矢印 (>>) ボタンを押して、**「使用可能エンティティー」**から**「ドメイン・エンティティー」**にカスタム表を移動します。

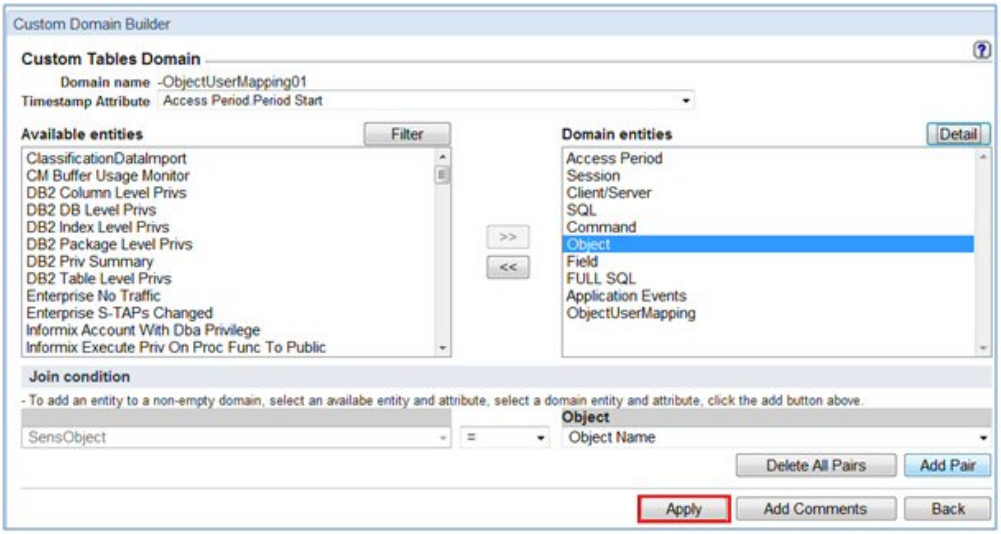


4. **「詳細」**ボタンを押して、結合をレビューします。



5. 結合が正しいことを確認し、**「閉じる」**を押します。

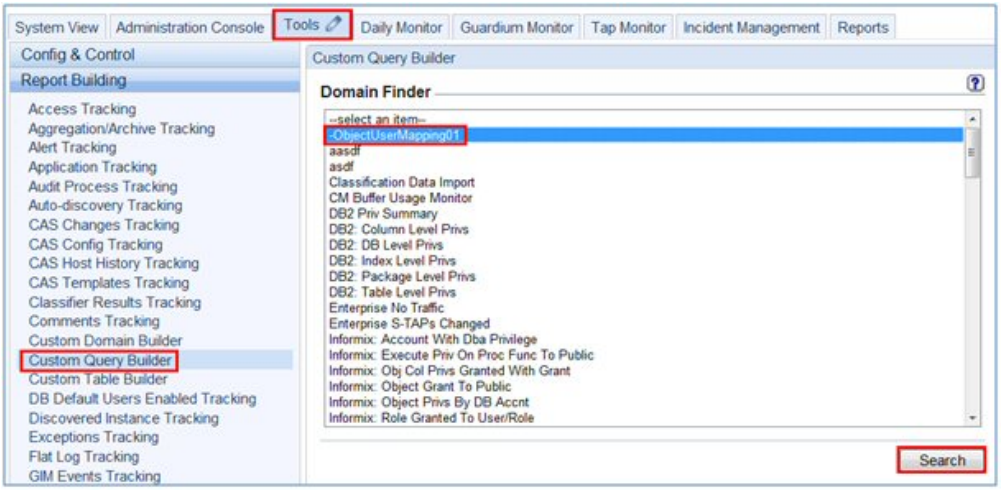
6. 「適用」を押して新しいカスタム・ドメインを保存します。



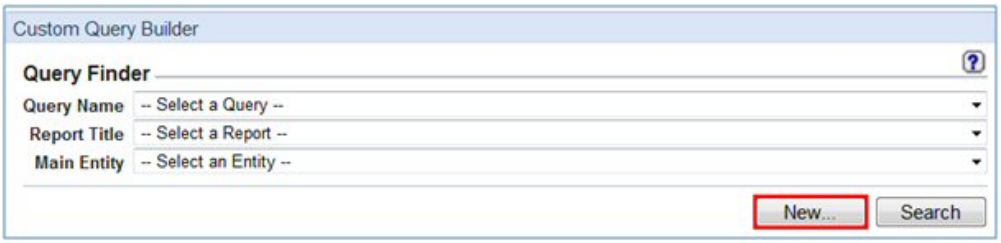
カスタム・レポート

次に、ユーザーに配布するレポートを作成します。

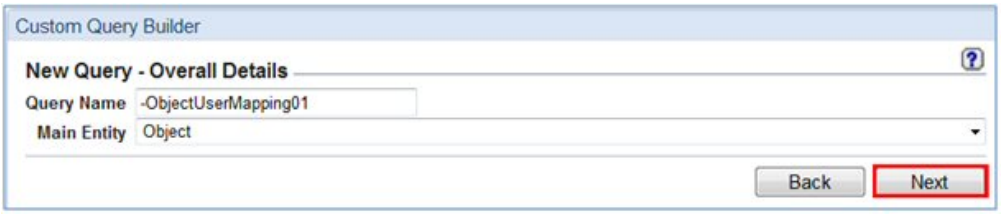
1. 「レポート」 > 「レポート構成ツール」 > 「レポート・ビルダー」にナビゲートし、「ドメイン」ドロップダウン・メニューから新規ドメインを選択します。



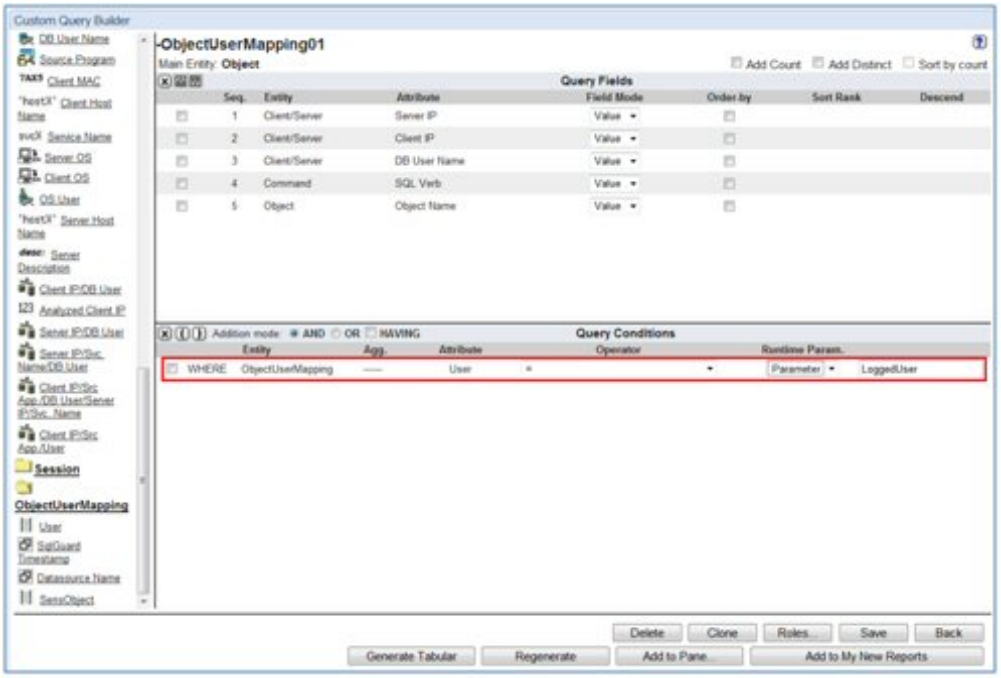
2. 「新規」をクリックします。



3. 「照会名」および「メイン・エンティティー」を入力し、「次へ」を押します。



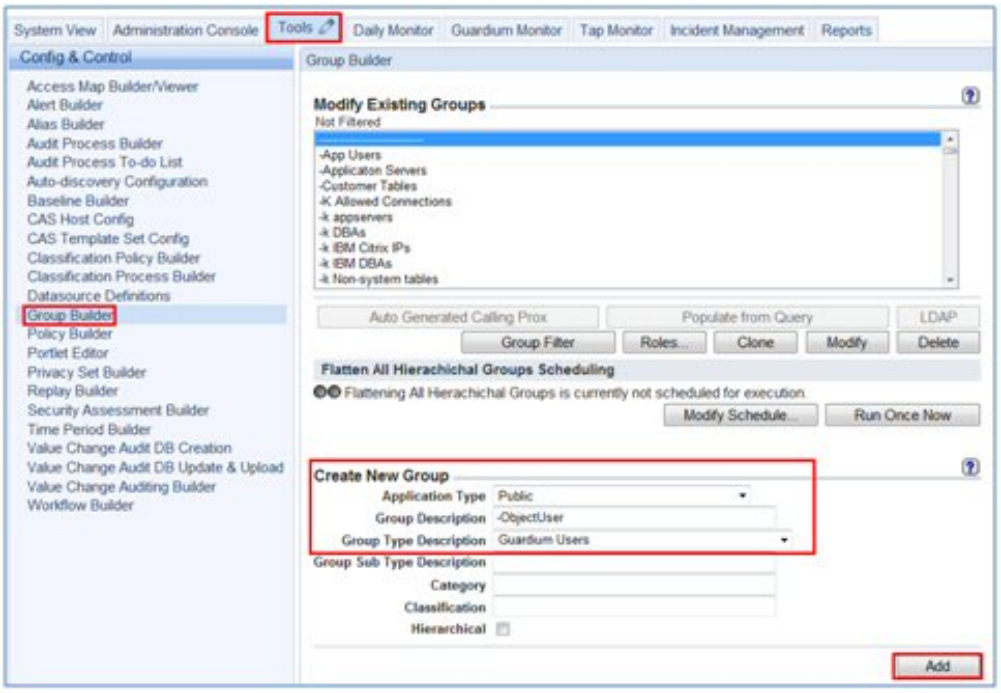
4. カスタム表内に作成されたユーザー・フィールドに対するランタイム・パラメーターを持つ新規レポートを作成します。



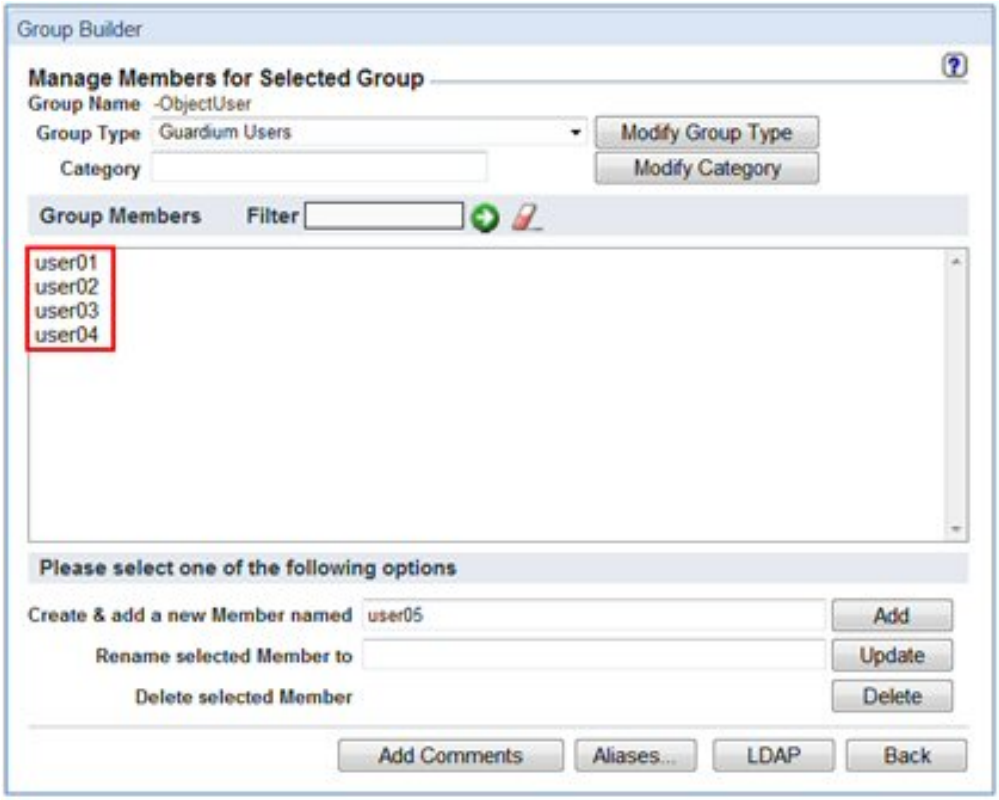
ユーザー・グループ

カスタム表に基づいて、新しいグループ「Guardium Users」を作成します。

1. 「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」にナビゲートし、**「グループ・タイプ」**として**「Guardium ユーザー」**が設定された新規グループを作成します。

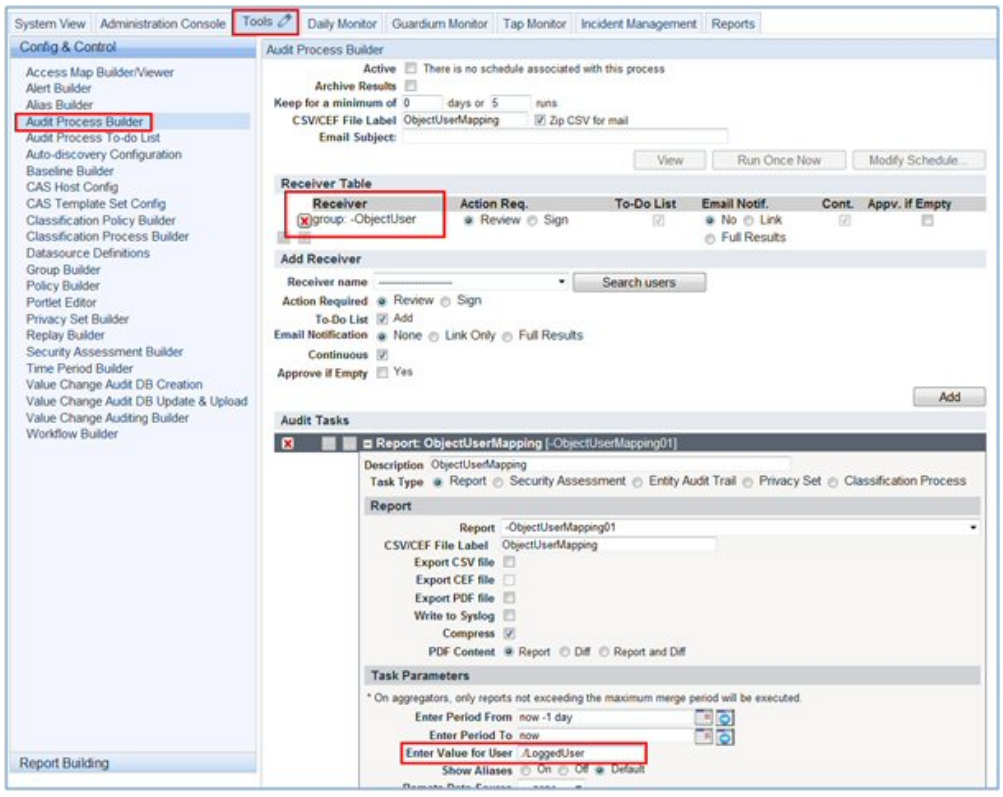


2. カスタム表からすべてのユーザーを追加します。



監査プロセス

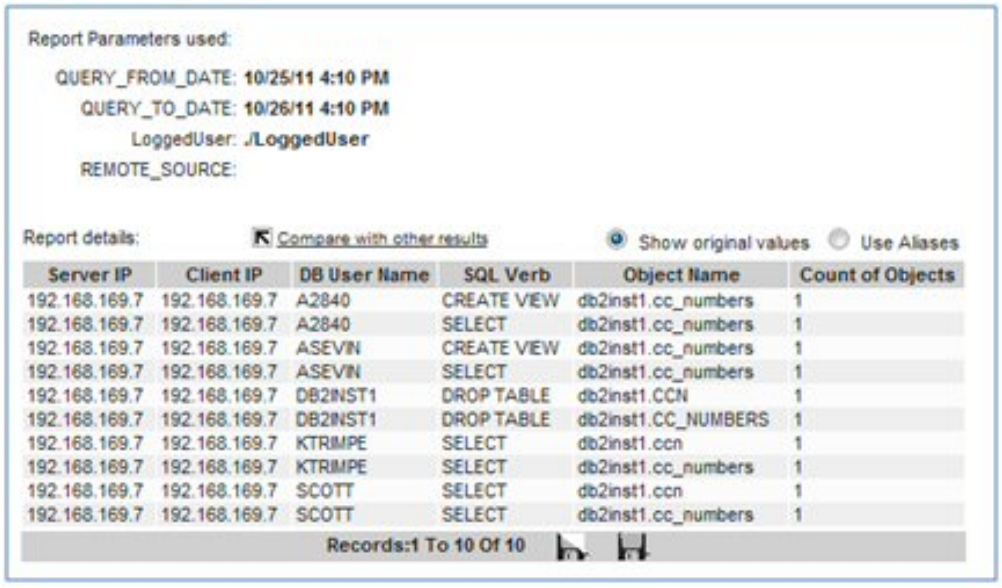
1. 新しい監査プロセスを作成します。
2. 『ユーザー・グループ』で作成されたグループを「**受信者**」として選択します。
3. ステップ 4 で作成されるカスタム・レポートをタスクとして選択します。
4. ランタイム・パラメーターに、特殊なタグ「./LoggedUser」を入力します。 これにより、カスタム・マッピングに基づいて結果が配布されます。
5. 「**今すぐ 1 回実行**」を押して監査プロセスを実行します



監査プロセスが完了すると、各受信者はマッピングに基づいて、それぞれの結果セットを受け取ります。

ユーザー

User01



Report Parameters used:

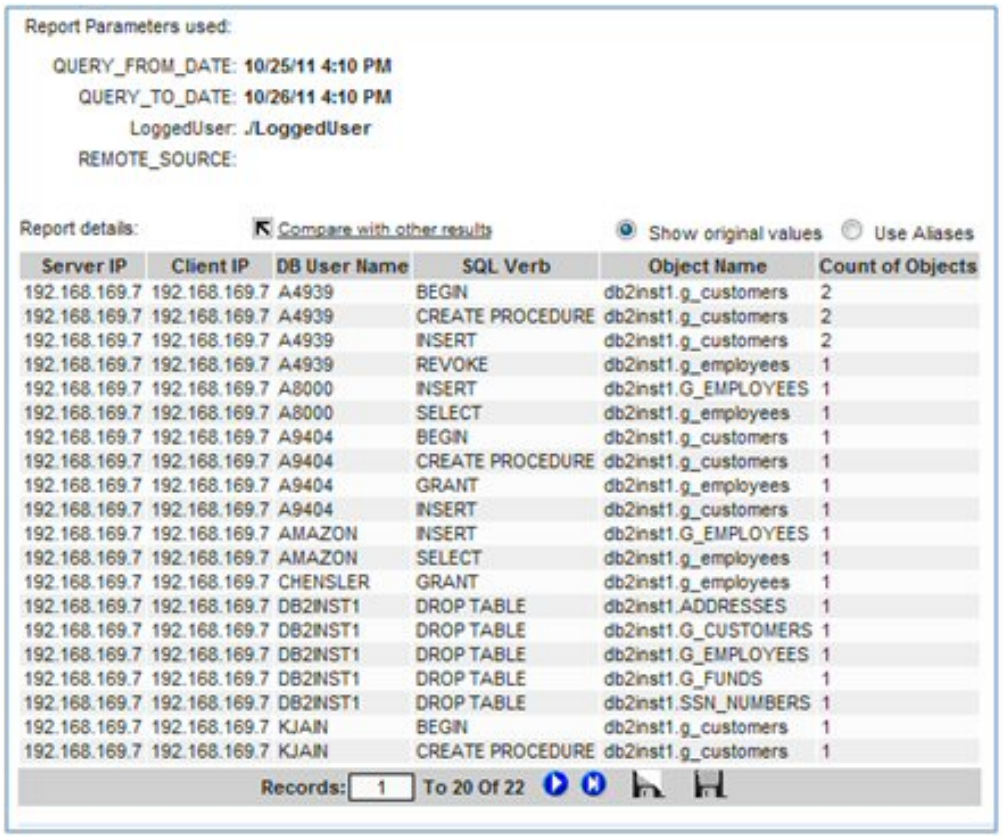
QUERY_FROM_DATE: **10/25/11 4:10 PM**
QUERY_TO_DATE: **10/26/11 4:10 PM**
LoggedUser: **./LoggedUser**
REMOTE_SOURCE:

Report details: Compare with other results — Show original values — Use Aliases

Server IP	Client IP	DB User Name	SQL Verb	Object Name	Count of Objects
192.168.169.7	192.168.169.7	A2840	CREATE VIEW	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	A2840	SELECT	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	ASEVIN	CREATE VIEW	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	ASEVIN	SELECT	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.CCN	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.CC_NUMBERS	1
192.168.169.7	192.168.169.7	KTRIMPE	SELECT	db2inst1.ccn	1
192.168.169.7	192.168.169.7	KTRIMPE	SELECT	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	SCOTT	SELECT	db2inst1.ccn	1
192.168.169.7	192.168.169.7	SCOTT	SELECT	db2inst1.cc_numbers	1

Records:1 To 10 Of 10

User02



Report Parameters used:

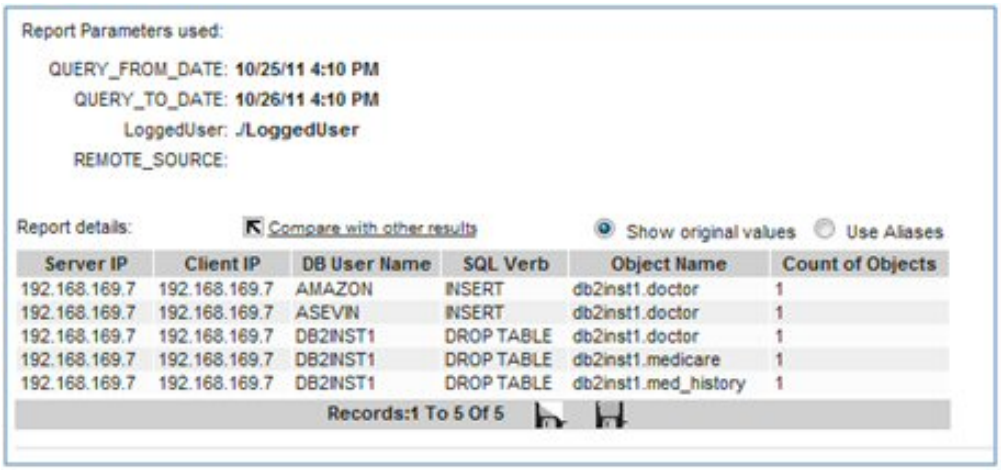
QUERY_FROM_DATE: **10/25/11 4:10 PM**
QUERY_TO_DATE: **10/26/11 4:10 PM**
LoggedUser: **./LoggedUser**
REMOTE_SOURCE:

Report details: Compare with other results — Show original values — Use Aliases

Server IP	Client IP	DB User Name	SQL Verb	Object Name	Count of Objects
192.168.169.7	192.168.169.7	A4939	BEGIN	db2inst1.g_customers	2
192.168.169.7	192.168.169.7	A4939	CREATE PROCEDURE	db2inst1.g_customers	2
192.168.169.7	192.168.169.7	A4939	INSERT	db2inst1.g_customers	2
192.168.169.7	192.168.169.7	A4939	REVOKE	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	A8000	INSERT	db2inst1.G_EMPLOYEES	1
192.168.169.7	192.168.169.7	A8000	SELECT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	A9404	BEGIN	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	A9404	CREATE PROCEDURE	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	A9404	GRANT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	A9404	INSERT	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	AMAZON	INSERT	db2inst1.G_EMPLOYEES	1
192.168.169.7	192.168.169.7	AMAZON	SELECT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	CHENSLER	GRANT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.ADDRESSES	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.G_CUSTOMERS	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.G_EMPLOYEES	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.G_FUNDS	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.SSN_NUMBERS	1
192.168.169.7	192.168.169.7	KJAIN	BEGIN	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	KJAIN	CREATE PROCEDURE	db2inst1.g_customers	1

Records: 1 To 20 Of 22

User03



親トピック: 監査プロセスの作成

監査プロセスの To-do リスト

このトピックでは、「監査プロセスの To-do リスト」と、これを開いて使用するために必要なステップについて説明します。

「監査プロセスの To-do リスト」は、以下を含むいくつかの方法で開くことができます。

- ページ・バナーの アイコンをクリックします。
- 「順守」 > 「ツールとビュー」 > 「監査プロセスの To-do リスト」にナビゲートします。
- E メール通知を受け取った場合は、「To-do リスト」リンクをクリックして To-do リストを開きます。または、「レポート」リンクをクリックして結果を開きます。 いずれの場合も、E メールには Guardium® システムにアクセス可能なロケーションからアクセスする必要があります。

以下のステップで、「監査プロセスの To-do リスト」の使用法を説明します。

1. 開く対象の To-Do リストを所有するユーザーを選択します。これは、ドロップダウン・メニューを開くか、「ユーザーの検索」をクリックすることによって行います。 リストが空の場合は通知を受けます。
2. 管理者は、任意の To-Do リスト項目にある任意のアクションを実行できます。 管理者が実行するすべてのアクションはログに記録され、管理者がユーザーの代わりにアクションを実行したことが示されます。
3. To-Do リスト項目ごとに選択可能な項目は、「表示」、「PDF 形式でダウンロード」および「表示された結果に署名」です。

   「PDF の内容」の選択項目には、「レポート」(現在の結果)、「差異」(1 つ前のレポートと新規レポートの間の差異)、 および「レポートと差異」(その両方) があります。

   注: 「PDF の内容」の選択内容は、PDF 添付ファイルと PDF エクスポート・ファイル の両方に適用されます。「差異」の結果は、このタスクの初回実行後にのみ適用されます。 前の結果がない場合に、前の結果との差異は存在しません。一度に比較可能な行の最大数は、5000 です。 結果行の数が最大数を超える場合、差異の結果にメッセージ「最初の 5000 行のみ比較」が表示されます。
4. セットの最新表示をするには、回転矢印のアイコンをクリックします。

注: 外部サーバーへのファイルの送信を、結果の To-Do リストへの追加や E メールの送信をせずに行う場合は、受信者を指定しない監査プロセスを 定義します。さらに、結果を To-Do リストに追加しないようにするために、「受信者の追加」セクションで「To-Do リスト」チェック・ボックスをクリアし、「受信者」セクションに受信者がある場合はすべて削除し、受信者の追加は行わないでください。

To-Do リストとデータ・レベル・セキュリティー

To-Do リストにはプルダウン・メニューがあり、そこから他のユーザーの To-Do リストを確認できます。 admin ロールを持つユーザーのプルダウン・メニューとは異なり、それ以外のユーザーのプルダウン・メニューには、データ・レベル・セキュリティー (DLS) 階層における、現行ユーザーの下位に属するユーザーのみが含まれます。 ユーザーが exempt ロールを持っている場合、プルダウン・メニューにはすべてのユーザーが表示されます。 admin ロールを持つユーザーのプルダウン・メニューには、すべてのユーザーが表示されます。

ユーザーが別のユーザーの結果にアクセスするとき、レポートに示されるデータは、 データ・レベル・セキュリティーおよび選択したユーザーのロールに従ってフィルターに掛けられます (例えば、 カスタム・ワークフローの場合、データは選択したユーザーのロールとそのロールに定義された状況に従ってフィルターに掛けられます)。

admin ロールを持つユーザーが階層内の下位に属するユーザーの結果にアクセスする場合、前の段落で説明したように動作します。 管理者が階層内の下位に属していないユーザーの結果にアクセスする場合、 管理者のデータ・レベル・セキュリティーを使用して結果が表示され、すべてのロールに関して表示されます。

イベントの状況の変更があったために、ユーザーの To-Do リストに今まで存在していなかった結果がそのリストに追加される場合には、ユーザーに対して E メールが送信されます。 E メールに含まれるのは通知とリンクのみであり、PDF は含まれません。

ユーザーが他のユーザーの To-Do リストに移動すると、DLS フィルタリングを決定しているユーザーを示すメッセージが表示されます。

親トピック: 監査プロセスの作成

監査およびレポート

Guardium® は、収集したデータをドメイン・セットに編成します。 各ドメインには、特定の関心領域 (データ・アクセス権、例外、ポリシー違反など) に関連する異なるタイプの情報が格納されます。

すべてのドメインおよびその内容については、付録『ドメイン、エンティティー、および属性』を参照してください。

ドメインごとに別個のクエリー・ビルダーがあり、各クエリー・ビルダーへのアクセスはセキュリティー・ロールで制御されます。ドメインに関係なく、すべての照会の作成には同じ汎用クエリー・ビルダー・ツールが使用されます。 照会の作成方法について詳しくは、『照会』を参照してください。

ユーザーは、標準のドメイン・セットに加えて、Guardium アプライアンスにアップロード可能な情報を格納するカスタム・ドメインを定義できます。 例えば、企業環境に、総称データベース・ユーザー名 (hr23455、qa4872 など) を実際の人名 (Paula Smith、John Doe など) に関連付ける表があるとします。 その表がアップロードされると、カスタム・ドメインから Guardium レポートに実名を表示できます。 カスタム・ドメインの定義方法および使用方法について詳しくは、『外部データ相関』を参照してください。

親トピック: モニターおよび監査

外部データ相関

このトピックでは、既存の Guardium® 内部データに加えて必要なエンタープライズ情報のカスタム表の作成について説明します。

多くのカスタマーがそれぞれの環境で、さまざまなデータベースに貴重な情報を所有しています。 関連情報ニーズを相互に関連付けて監査レポートを理解しやすくすることは、監査レポートに極めて有用です。 外部データ相関により、既存の Guardium 内部データに加えて、必要なエンタープライズ情報のカスタム表を Guardium アプライアンス上にユーザーが作成できるようになります。この操作は、GUI 内で手動で行うか、またはデータベース・サーバー上の既存の表に基づいて行えます。その後、この情報の照会およびレポートを、それがあたかも事前定義データであるかのように作成できます。

カスタム表、カスタム・ドメイン、およびカスタム照会に区別されます。

例えば、全社員、社員それぞれのデータベース・ユーザー名、各社員の所属部門 (例えば、開発部門、財務部門、営業部門、人事部門など) が含まれる表がデータベース・サーバーに存在するとします。 この表とそのすべてのデータをアップロードすると、この表を Guardium の内部表と相互参照し、例えば、営業部門のどの社員が財務データベースにアクセスしているか (疑わしいアクティビティーになる可能性がある) を調べることができます。

データマートのヘルプにアクセスするには、データマートをクリックします。

カスタム表

カスタム表には、Guardium アプライアンスで使用可能にする属性が 1 つ以上含まれます。 例えば、エンコードされたユーザー名を実名に関連付ける既存のデータベース表があるとします。 ネットワーク・トラフィックで見られるのは、エンコードされた名前のみです。 Guardium アプライアンスでカスタム表を定義し、その表のデータを既存の表からアップロードすることにより、コード化された名前と実名を関連付けることができるようになります。

カスタム表を定義する前に、まず、既存のデータベース上の必要なデータが、サポートされるデータ・タイプであることを確認してください。 基礎となる JDBC ドライバーが以下の SQL タイプのいずれかとして受け取るデータ・タイプがサポートされます。INTEGER、BIGINT、SMALLINT、TINYINT、BIT、BOOLEAN、DECIMAL、DOUBLE、FLOAT、NUMERIC、REAL、CHAR、VARCHAR、DATE、TIME、TIMESTAMP。次の表は、カスタム表へのアップロードがサポートされるデータ・タイプとサポートされないデータ・タイプのいくつかを要約したものです。

カスタム表でサポートされるデータ・タイプとサポートされないデータ・タイプ

次の表を使用して、特定のデータベースでどのデータ・タイプがサポートされ、どのデータ・タイプがサポートされないか確認してください。

表 1. カスタム表でサポートされるデータ・タイプとサポートされないデータ・タイプ

データベース	サポートされるデータ・タイプ	サポートされないデータ・タイプ
Oracle	float number char varchar2 date nchar nvarchar2	long clob raw nclob longraw bfile rowid urowid blob
DB2®	char varchar bigint integer smallint real double decimal date time timestamp	blob clob longvarchar datalink
Sybase	char nchar varchar nvarchar int smallint tinyint datetime smalldatetime	text binary varbinary image timestamp
MS SQL	bigint bit char datetime decimal float int money nchar numeric nvarchar real smalldatetime smallint tinyint smallmoney varchar unique identifier	text
Informix®	char nchar integer smallint decimal smallfloat float serial date money varchar nvarchar datetime	text
MY SQL	bigint decimal int mediumint smallint tinyint double float date datetime timestamp time year char binary enum set	longtext tinyblob tinytext blob text mediumblob mediumtext longblob longtext

注: 動的 SQL では blob 値 (値が 1K でも) をキャプチャーできますが、静的 SQL では同じサイズの blob 値をキャプチャーできません。

カスタム表のアーカイブおよびリストア

「カスタム表ビルダー」画面には、「パージ/アーカイブ」というボタンがあります。

「カスタム表データのパージ」画面には、「アーカイブ」用のチェック・ボックスがあります。このボックスにチェック・マークを付けると、カスタム表のデータが通常のデータ・アーカイブに組み込まれます。

このカスタム表データは、カスタム表の SQLGUARD_TIMESTAMP 列の日付に基づいてアーカイブされます。

カスタム表のデータは、コレクターまたはアグリゲーターからアーカイブ可能です。

コレクターからアーカイブされたカスタム表のデータは、ソース・コレクターと同じ中央マネージャーによって管理されているコレクターまたはアグリゲーターにリストアできます (メタデータが存在する必要があります)。

アグリゲーターからアーカイブされたカスタム表のデータは、ソース・アグリゲーターと同じ中央マネージャーによって管理されているアグリゲーターにリストアできます。

Guardium システムにリストアするアーカイブ・ファイルにメタデータがない場合、カスタム表のデータはリストアされません。

カスタム表の構造が、アーカイブ時とリストア時で、SQL エラーの原因となるような方法で変わっている場合 (列が削除されていたり、タイプが変わっていたりする場合)、統合/アーカイブ・アクティビティー・レポートに警告メッセージが表示され、データはリストアされません。

カスタム表がデフォルト・パージによってパージされるように設定されている場合、リストアされたデータは、リストア画面で指定した日数だけ保持されます。

カスタム表がアップロード時にデータを上書きするように設定されている場合、リストアされたデータは、アップロードの実行時に削除されます。

カスタム・ドメイン

カスタム・ドメインにはカスタム表が 1 つ以上含まれます。 表が複数含まれる場合は、カスタム・ドメインを定義する際に表間の関連を定義します。

カスタム照会

カスタム照会は、カスタム・ドメインに含まれるデータにアクセスします。 カスタム・ドメインに対する照会を作成するには、カスタム・クエリー・ビルダーを使用します。 その後、カスタム照会を他の照会のように使用して、レポートや監査タスクを生成したり、グループにデータを設定したり、別名を定義したりできます。

データベース・ライセンス・レポート

DB ライセンス・レポートでは、カスタム・ドメイン機能を使用して、選択したデータベース上の外部データと事前定義ライセンス・レポートの内部データとのリンクを作成します。これについては、トピック『内部データへの外部データのリンク』を参照してください。事前定義データベース・ライセンス・レポートの使用法について詳しくは、『データベース・ライセンス・レポート』を参照してください。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

カスタム表の作成

以下のいずれかにナビゲートして「カスタム表ビルダー」を開きます。

- 「順守」 > 「カスタム・レポート作成」 > 「カスタム表ビルダー」
- 「レポート」 > 「レポート構成ツール」 > 「カスタム表ビルダー」

表定義のアップロード

カスタム表の作成を行うには表定義をアップロードします。このためには、メタデータが定義されているデータベース・サーバーにあるこのメタデータにアクセスします。

注: Guardium にアップロードされたカスタム表は、プロダクト・キーで使用可能になるオプション・コンポーネントです。これらのコンポーネントが使用可能になっていなければ、カスタム表に関する選択項目は、カスタム表ビルダーの選択項目として表示されません。

1. カスタム表ビルダー を開きます。
2. 「定義のアップロード」をクリックして、「表構造のインポート」パネルを開きます。項目を選択する必要はありません。
3. 「エンティティーの記述」フィールドに表の記述を入力します。これが、カスタム照会の作成時にこの表を参照するために使用する名前になります。
4. 「表名」フィールドに、表のデータベース表名を入力します。これが、ローカル・データベースに表を作成するために使用する名前になります。
5. 「SQL ステートメント」フィールドに、表に対する有効な SQL ステートメントを入力します。この SQL ステートメントによって返される結果セットの構造は、定義したカスタム表と同じでなければなりません。 例えば、my_table という名前の表のすべての列がカスタム表に含まれる場合は、select * from my_table と入力します。
   注:

   SQL ステートメントには、改行文字を使用しないでください。すべての列に明示的に名前を付ける必要があります (必要であれば列の別名を使用)。
6. 「データ・ソースの追加」をクリックして別のウィンドウにデータ・ソース・ファインダーを開きます。 データ・ソース・ファインダーで、外部データベースの場所を定義できるほか、このプロセスで後ほど表の定義と内容を取得する際に必要となる資格情報を定義できます。
7. データ・ソース・ファインダーを使用して、表定義のアップロード元のデータベースを特定します。
8. 「取得」をクリックして表定義をアップロードします。この操作によって SQL ステートメントが実行され、表構造が取得されます。 SQL 要求は Guardium システムから外部データベースに送信されます。アップロードされるのは定義だけであることに注意してください。データは後でアップロードできます。

表定義を手動で定義する

1. カスタム表ビルダー を開きます。
2. 「手動定義」をクリックして「エンティティーの定義」パネルを開きます。
3. 「エンティティーの記述」フィールドに表の記述を入力します。これが、カスタム照会の作成時にこの表を参照するために使用する名前になります。 エンティティーの記述に特殊文字 ¥$|&;'`" は使用できません。
4. 「表名」フィールドに、表のデータベース表名を入力します。これが、ローカル・データベースに表を作成するために使用する名前になります。
5. 定義する表の列ごとに、以下のようにします。
   - 「列名」ボックスに名前を入力します。これが、データベース表の列の名前になります。
   - 「表示名」 ボックスに名前を入力します。これが、カスタム・ドメイン・ビルダーおよびカスタム・クエリー・ビルダーで属性を参照するために使用する名前になります。
   - データ・タイプ (テキスト、日付、整数、浮動小数点、またはタイム・スタンプ) を選択します。
   - テキスト属性の場合は、「サイズ」ボックスに最大文字数を入力します。(他のデータ・タイプでは「サイズ」ボックスは使用できません。)
   - 列の固有性を適用する場合は、「固有」 ボックスにチェック・マークを付けます。
   - 定義する属性はグループ・タイプと対応する場合は、そのグループ・タイプを「グループ・タイプ」 リストから選択します。
   - 「追加」をクリックして列を追加します。
6. 「エンティティー・キー」ドロップダウン・リストを使用して、エンティティー・キーとして使用する列を指定します。 エンティティー・キーは、カウントを選択するときにクエリー・ビルダーで使用されます。
7. 「追加」ボタンをクリックした後で列の削除や属性の変更などの追加変更を行った場合は、「適用」をクリックして変更を保存します。
8. 表のすべての列を追加したら、「完了」をクリックします。

表定義の変更

カスタム表の定義を変更すると、その表を使用する照会に基づいた既存のレポートが無効になる場合があります。 例えば、削除された属性やデータ・タイプが変更された属性を既存の照会が参照している場合があります。 カスタム表に変更を適用する際に、その表の属性を使用する照会が既に作成されている場合は、「照会リスト」パネルにそれらの照会が表示されます。 注:「変更」を使用して、インポートされている表構造を表示して確認することもできます。

1. カスタム表ビルダーを開きます。
2. 「エンティティー・ラベル」をクリックして強調表示することで、カスタム表を選択します。
3. 「変更」をクリックして、「エンティティーの変更」パネルを開きます。
4. 『表を手動で定義する』を参照してください。
5. カスタム表に変更を適用する際に、その表の属性に対する変更のために無効になる可能性のある照会がある場合は、「照会リスト」パネルにそれらの照会が表示されます。 「照会リスト」パネルを使用して、照会を選択して変更します。 直ちにすべての変更を行う必要はありません。いつでも戻って「無効な照会の検査」オプションを使用できます。

無効な照会

カスタム表の定義を変更すると、その表を使用する照会に基づいた既存のレポートが無効になる場合があります。 例えば、削除された属性やデータ・タイプが変更された属性を既存の照会が参照している場合があります。 表の変更処理後に無効な照会を検査することをお勧めします。

1. カスタム表ビルダーを開きます。
2. 「無効な照会」をクリックします。
3. 「照会リスト」パネルに照会が表示されます。「照会リスト」パネルを使用して、照会を選択して変更します。

カスタム表からデータをパージする

オンデマンドまたはスケジュール・ベースで、Guardium サーバー上のカスタム表からデータをパージできます。

1. カスタム表ビルダーを開きます。
2. カスタム表を、表の名前をクリックして強調表示することで選択します。
3. 「パージ」をクリックして「カスタム表データのパージ」パネルを開きます。
4. 今すぐパージするには、「すべてパージ」をクリックします。
   注:「今すぐ 1 回実行」パージは、保持データがないか RESTORED_DATA 表を調べます。「すべてパージ」は、保持データを検査することなく、削除されたすべてのレコードをパージします。
5. 「構成」パネルで、パージするデータの経過日数を、このパージ操作の日付より前の日数、週数、または月数として入力します。
6. パージのスケジュール設定操作を 1 回実行するには、「今すぐ 1 回実行」 をクリックします。
7. 「スケジュールの変更」をクリックして標準の「スケジュール定義」パネルを開き、パージ操作のスケジュールを設定します。
8. 「完了」をクリックしてパネルを閉じます。

カスタム表へのデータのアップロード

1. カスタム表ビルダーを開きます。
2. カスタム表を、表の名前をクリックして強調表示することで選択します。
3. 「データのアップロード」をクリックして「データのインポート」パネルを開きます。
4. 「SQL ステートメント」ボックスに、表に対する有効な SQL ステートメントを入力します。この SQL ステートメントによって返される結果セットの構造は、定義したカスタム表と同じでなければなりません。 例えば、my_table という名前の表のすべての列がカスタム表に含まれる場合は、`select * from my_table` と入力します。Guardium 内部の以下のフィールドを SQL ステートメントで使用できます。
   - ^FromDate?^ および ^ToDate?^。値はそれぞれ、前回のアップロード日と現在のアップロード日に相当します。
   - ^fromID^ および ^toID^。「ID 列名」と共に使用される場合に、それぞれ、前回のアップロードでの ID 列の最大値、および現在のアップロードの最大値から成ります。

   注: SQL ステートメントには、改行文字を使用しないでください。
5. 「ID 列名」の列名 (データ・ソース内で定義された表の列名) が使用されて ID によるトラッキングが可能であり、内部 Guardium フィールドの ^fromID^ および ^toID^ と共に使用されることを、必要に応じて指定します。
6. 「アップロード後の DML コマンド」ボックスに、データのアップロード後に実行する DML コマンド (update または delete SQL ステートメント) をセミコロンなしで入力します。 注: SQL ステートメントには、改行文字を使用しないでください。
7. アップロード前にカスタム表のデータをパージする場合は、「上書き」の「アップロードごと」ボックスにチェック・マークを付けます。そのデータ・ソースのデータをアップロード前にパージする場合は、「上書き」の「データ・ソースごと」にチェック・マークを付けます。
8. 「デフォルトのカスタム表パージ・ジョブ」パージ・オブジェクト (初期デフォルトの経過日数は 60 日) の一部にするには、「デフォルト・パージ」ボタン (「カスタム・データのアップロード」画面内) にチェック・マークを付けます。 この表のパージ・スケジュールを追加するには、最初の「カスタム表ビルダー」ページに移動し、「カスタム表」を選択し、「パージ」をクリックして「カスタム表データのパージ」構成画面を開きます。
9. 以前のバージョンの Guardium から表をアップロードする場合のみ、「デフォルト・スケジュールを使用」ボックスにチェック・マークを付けます。 このチェック・ボックスは、中央マネージャー・ビューにのみ表示され、定義済みのカスタム表である「CM バッファー使用状況モニター」、「エンタープライズの「トラフィックなし」、「S-TAP® 変更」、および「S-TAP 情報」に対してのみ表示されます。
10. 「データ・ソースの追加」をクリックして別のウィンドウにデータ・ソース・ファインダーを開きます。 このウィンドウを使用して、表データのアップロード元のデータベースを 1 つ以上指定します。 複数のソースからアップロードするには、複数のデータ・ソースを追加します。 注:中央マネージャーの場合、「データのインポート」ページに、「デフォルト・ソースを含める」という読み取り専用のチェック・ボックスがあります。このチェック・ボックスにチェック・マークが付いている場合は、オンラインの登録済み管理対象ユニットすべてでデータのアップロードが繰り返されます。 注: データ・ソースを追加する場合、選択したデータ・ソースのユーザー名とパスワードを指定せずに実行されるようにアプリケーションのスケジュールを設定することはできません。
11. 「検査/修復」をクリックすることにより、カスタム表のスキーマをメタデータのスキーマと比較できます。 一元管理環境の場合: 一元管理環境では、中央マネージャー上にカスタム表定義があるので、ローカル (管理対象ユニット)データベース上にカスタム表が存在するとは限りません。 カスタム表がローカルに存在するかどうかを確認し、存在しない場合はそれを作成するには、「検査/修復」ボタンをクリックします。
12. 「データ・ソースの検査」をクリックして外部データベース接続をテストします。 確認画面が表示されます。
13. 「適用」をクリックします。
14. このカスタム表にデータをアップロードするには、以下のいずれかの操作を行います。
    - データを手動でアップロードする場合は、「今すぐ 1 回実行」をクリックします。
    - スケジュールを構成する場合は、「スケジュールの変更」をクリックします。

カスタム表の保守

カスタム表の作成手順 (前述) に従い、事前定義のカスタム表を選択する場合は、「メンテナンス」をクリックして、表エンジン・タイプと表索引を管理してください。Guardium 内部データベースに保管されるデータが MYSQL ベースの場合は、すべての事前定義カスタム・データベースに関する カスタム表/ライセンスの表エンジン・タイプ (InnoDB および MyISAM) が表示されます。MySQL データベースの表ストレージ・エンジンには InnoDB と MyISAM という 2 つの主要なタイプがあります。これらの MYSQL 表エンジン・タイプの主な違いは以下のとおりです。

- InnoDB の方が複雑で、MyISAM の方が単純です。
- データ保全性は、InnoDB の方が厳格で、MyISAM の方が緩やかです。
- 挿入と更新について InnoDB は行レベルのロックを実装し、MyISAM は表レベルのロックを実装します。
- InnoDB にはトランザクションがありますが、MyISAM にはありません。
- InnoDB には外部キーと関係制約がありますが、MyISAM にはありません。

注: 表の行番号が 1M より大きい場合、エンジン・タイプを変更することは許可されていません (選択項目がぼかし表示になります)。

「カスタム表の保守」メニュー内の他の選択項目として、「表索引の管理」があります。「挿入」をクリックして「表の索引の定義」を開きます。このポップアップ画面には、 カスタム・ドメイン上で結合条件として使用される列に基づき、 索引に追加すべき表の列が提示されます。列を選択して保存します。索引が作成 (または再作成) されます。

カスタム・データのアップロードのスケジュール設定

カスタム表定義が整うと、Guardium アプライアンス上のカスタム表にスケジュール・ベースでデータをアップロードできるようになります。

注: 新規インストールでは、エンタープライズ・レポートは自動的に開始されません。アップロード・スケジュールはカスタム表ごとに 1 つあります。Guardium アプライアンス上でカスタム表のために予約されているディスク・スペース総量は 4GB です。

1. カスタム表ビルダー を開きます。
2. 「エンティティー・ラベル」をクリックして強調表示することで、カスタム表を選択します。
3. 「データのアップロード」をクリックして「データのインポート」パネルを開きます。
4. デフォルト・スケジュールを使用してこの表をアップロードするには、「デフォルト・スケジュールを使用」チェック・ボックスにマークを付けます。 それ以外の場合、このカスタム表は独自のデータ・アップロード・スケジュールを使用します。
5. 「スケジュールの変更」 をクリックして標準の「スケジュール定義」パネルを開き、スケジュールを変更します。
6. 完了したら、「完了」をクリックします。

エンタープライズにより、他のジョブと同様にカスタム・アップロードについて報告されます。これらのジョブを有効にするには、次の 2 とおりの方法があります。

- カスタム表アップロード GUI を使用する (カスタム・アップロードに関するライセンスが必要)。
- 以下のように、CLI から GuardAPI を使用する。

```
grdapi add_schedule jobName=CustomTablePurgeJob_CM_SNIFFER_BUFFER_USAGE obGroup=customTableJobGroup Enterprise S-TAPs
Changed: grdapi add_schedule jobName=customTableDataUpload_106 jobGroup=customTableJobGroup CM Buffer Usage Monitor: grdapi
add_schedule jobName=customTableDataUpload_104 jobGroup=customTableJobGroup S-TAP Info: grdapi add_schedule
jobName=customTableDataUpload_80 jobGroup=customTableJobGroup
```

カスタム・ドメインの作成

カスタム表を 1 つ以上定義した後、カスタム・データを使用して照会およびレポート作成タスクを実行できるように、カスタム・ドメインを定義します。 収集された情報はドメインに編成され、ドメインごとに特定の関心領域 (データ・アクセス、例外、ポリシー違反など) に関連する異なるタイプの情報が含まれます。ドメインごとに別々のクエリー・ビルダー・ツールがあります。 カスタム・ドメインではユーザー定義のドメインが可能であり、Guardium アプライアンスにアップロードするデータの任意の表を定義できます。 『カスタム・ドメイン』を参照してください。これらのカスタム・ライセンス (特権) ドメインを使用するということは、ライセンス・レポートを使用するということです。ライセンス・レポートには、ユーザーとしてログインした場合にアクセスできます。 これらのレポートを表示するには、「ユーザー」タブの「データベース特権」に移動します。

注: DB ライセンス・ドメインは、プロダクト・キーにより有効になるオプションのコンポーネントです。これらのコンポーネントが使用可能になっていなければ、『カスタム・ドメイン』ヘルプ・トピックで示される選択項目は、カスタム・ドメイン・ビルダーの選択項目として表示されません。

1. 以下のいずれかにナビゲートして「カスタム・ドメイン・ビルダー」を開きます。
   - 「順守」 > 「カスタム・レポート作成」 > 「カスタム・ドメイン・ビルダー」
   - 「レポート」 > 「レポート構成ツール」 > 「カスタム・ドメイン・ビルダー」
   - 「設定」 > 「ツールとビュー」 > 「カスタム・ドメイン・ビルダー」
2. 「ドメイン」をクリックして「ドメイン・ファインダー」パネルを開きます。
3. 「新規」をクリックして「カスタム表のドメイン」パネルを開きます。
4. ドメイン・ネームを入力します。ドメインに含めるカスタム表は通常 1 つなので、それと同じ名前をドメインに使用すると便利です。
5. 「使用可能エンティティー」ボックスに、定義されている (かつアクセス権限のある) カスタム表がすべてリストされます。 エンティティーを選択します。必要に応じて、(「フィルター」) ツールをクリックして「エンティティー・フィルター」を開き、リストするエンティティーのみを選択するための Like 値を入力し、「OK」をクリックします。フィルター・ウィンドウが閉じて「カスタム表のドメイン」パネルに戻ります。このパネルには、「使用可能エンティティー」ボックスにリストされた Like 値に一致するエンティティーのみが表示されます。 含めるエンティティーを選択します。
6. >> 矢印ボタンをクリックして、「使用可能エンティティー」リストで選択したエンティティーを「ドメイン・エンティティー」リストに移動します。
7. 既に表が 1 つ以上あるドメインにエンティティーを追加するには、概略手順に従います。結合条件を使用して、エンティティー間の関係を定義する必要があります。

   追加エンティティーごとに、以下のようにします。

   - 「ドメイン・エンティティー」ボックスからエンティティーを選択します。そのエンティティーのすべての属性が、「ドメイン・エンティティー」ボックスのフィールド・ドロップダウン・リストで選択可能になります。そのリストから、結合演算で使用する属性を選択します。
   - 「使用可能エンティティー」リストから追加するエンティティーを選択します。そのエンティティーのすべての属性が、「使用可能エンティティー」ボックスのフィールド・ドロップダウン・リストで選択可能になります。そのリストから、結合演算で使用する属性を選択します。
   - 結合条件を等価 (例えば domainA.attributeB = domainC.attributeD) にする場合は、「=」(等価演算子) を選択します。 選択した属性を使用して結合条件を外部結合にする場合は、外部結合を選択します。

- 「フィールド・ペアの追加」をクリックします。「フィールド・ペアの追加」を使用して、この 2 つのエンティティーの属性のペアを、さらに結合条件に追加できます。
- 追加の結合演算があれば、ステップを繰り返します。

注: データ・レベル・セキュリティーがオンになっている場合、カスタム・ドメインに追加された内部エンティティーは、フィルター・ポリシーが定義された異なるドメインに属することはできません。

8. カスタム・ドメイン・エンティティーのタイム・スタンプ属性を選択します。
   注: タイム・スタンプが設定されたエンティティーを少なくとも 1 つ使用する必要があります。カスタム・ドメインを保存するためには、タイム・スタンプが必要のためです。
9. 「適用」をクリックします。

カスタム・ドメインの変更

この目的は、外部データと内部データのリンケージを作成することです。

1. カスタム・ドメイン・ビルダー を開きます。
2. コピーを作成するカスタム・ドメインを選択します。
3. 「変更」をクリックして「カスタム表のドメイン」パネルを開きます。
4. 『カスタム・ドメイン・ビルダーを開く』 および『内部データへの外部データのリンク』を参照してください。
5. 「適用」をクリックして、変更を保存します。

カスタム・ドメインの削除

1. カスタム・ドメイン・ビルダー を開きます。
2. コピーを作成するカスタム・ドメインを選択します。
3. 「ドメイン」をクリックして「ドメイン・ファインダー」パネルを開きます。
4. 「削除」をクリックしてカスタム・ドメインを削除します。

カスタム・ドメインのコピー作成

1. カスタム・ドメイン・ビルダー を開きます。
2. コピーを作成するドメインにあるカスタム表を選択します。
3. 「ドメイン」をクリックして「ドメイン・ファインダー」パネルを開きます。
4. 「コピー」をクリックして「カスタム表のドメイン」パネルを開きます。
5. ドメイン・ネームを変更して新しいドメインを反映した名前にします。
6. 『カスタム・ドメイン・ビルダーを開く』 および『内部データへの外部データのリンク』を参照してください。
7. 「適用」をクリックして、変更を保存します。

内部データへの外部データのリンク

この目的は、外部データと内部データのリンケージを作成することです。

1. カスタム・ドメイン・ビルダー を開きます。
2. 外部データのあるカスタム表を選択します。
3. 「ドメイン」をクリックして「ドメイン・ファインダー」パネルを開きます。
4. 「変更」をクリックして「カスタム表のドメイン」パネルを開きます。
5. 「使用可能エンティティー」の横にある「フィルター」アイコンをクリックします。
6. フィルターの「カスタム」ボックスのチェック・マークを外します。必要に応じて、エンティティー名をフィルターに掛けるための「LIKE」条件を入力し、「OK」をクリックします。
7. 外部データとリンクさせるエンティティーを、「使用可能エンティティー」 から選択します。
8. データを外部データと結合するために使用するフィールドを選択します。
9. 「ドメイン・エンティティー」で、外部データが含まれる表を強調表示します。
10. データを内部データと結合するために使用するフィールドを選択します。
11. 「フィールド・ペアの追加」をクリックして関係を追加します。
12. 二重矢印 >> をクリックして内部表を「ドメイン・エンティティー」リストに追加します。
13. 「適用」をクリックして、変更を保存します。

カスタム照会の処理

このセクションでは、カスタム・クエリー・ビルダーの開き方について説明します。 照会の定義とレポートの作成については、『照会のビルド』および『レポートのビルド』を参照してください。カスタム表が 1 つ以上含まれるカスタム・ドメインのデータに対する照会を作成するには、カスタム・クエリー・ビルダーを使用します。

1. 「順守」 > 「カスタム・レポート作成」 > 「カスタム・クエリー・ビルダー」にナビゲートして「カスタム・クエリー・ビルダー」を開きます。
2. リストからカスタム・ドメインを選択します。
3. 「検索」をクリックして「照会ファインダー」を開きます。
4. 既存の照会の表示、変更、またはコピー作成を行うには、「照会名」リストから選択するか、その照会を使用するポートを「レポート・タイトル」リストから選択します。
5. 特定のカスタム表に対して定義された照会をすべて表示するには、そのカスタム表を「メイン・エンティティー」リスト (選択したカスタム・ドメインに含まれるカスタム表のみがリストされる) から選択し、「検索」ボタンをクリックします。

InfoSphere Discovery との間の双方向インターフェース

IBM Guardium と InfoSphere® Discovery にはどちらにも、社会保障番号、クレジット・カード番号などの機密データを識別し、分類する機能があります。

IBM Guardium 製品のカスタマーは、双方向インターフェースを使用して、識別された機密データ情報を一方の製品から他方の製品に転送できます。一方の InfoSphere 製品に対して既に時間を注ぎ込んでいるカスタマーは、他方の InfoSphere 製品にその機密データ情報を転送できます。

注: IBM Guardium では、分類プロセスは、定期的に実行される継続プロセスです。InfoSphere Discovery では、分類は、通常 1 回実行されるディスカバリー・プロセスの一部です。

このデータは CSV ファイルを介して転送されます。

エクスポート/インポート手順の概要を以下に示します。

- Guardium からのエクスポート - 定義済みレポートを実行し (「Discovery への機密データのエクスポート」)、CSV ファイルとしてエクスポートします。
- Guardium へのインポート - CSV データ・ソースに対してカスタム表をロードします。このデータ・ソースに対してデフォルトのレポートを定義します。

以下の手順を行います。

- Guardium からのエクスポート
- IBM Guardium から InfoSphere Discovery に分類データをエクスポート

1. Guardium アプリケーションで admin ユーザーとして、「ツール」>「レポートのビルド」>「分類結果のトラッキング」>「レポートの選択」>「Discovery への機密データのエクスポート」に移動します。
   注: このレポートを UI ペインに追加します (これはデフォルトでは行われません)。
2. 「レポート結果」画面で「カスタマイズ」アイコンをクリックし、検索条件を指定して、Discovery に転送する分類結果データをフィルターに掛けます。
3. レポートを実行し、「レコードをすべてダウンロード」をクリックします。
4. CSV として保存し、このファイルを InfoSphere Discovery の指示に従い Discovery にインポートします。

Guardium へのインポート

InfoSphere Discovery から IBM Guardium に分類データをインポート

1. InfoSphere Discovery の指示に基づき、InfoSphere Discovery から分類データを CSV としてエクスポートします。
2. 以下のいずれかにナビゲートして「カスタム表ビルダー」を開きます。
   - 「順守」 > 「カスタム・レポート作成」 > 「カスタム表ビルダー」
   - 「レポート」 > 「レポート構成ツール」 > 「カスタム表ビルダー」

   「分類データのインポート」を選択し、「データのアップロード」をクリックします。
3. 「データのアップロード」画面で、「データ・ソースの追加」をクリックし、「新規」をクリックし、新規データ・ソースとして Discovery からインポートする CSV ファイルを定義します (「データベース・タイプ」=「テキスト」)。
   注: または、Discovery データベースおよび分類結果データにアクセスする方法が判明している場合、Discovery データベースからデータを直接ロードできます。
4. データ・ソースとして CSV を定義した後、「データ・ソース・リスト」画面で 「追加」をクリックします。
5. 「データのアップロード」画面で、「データ・ソースの検査」、「適用」の順にクリックします。
6. 「今すぐ 1 回実行」をクリックして CSV からデータをロードします。
7. 「レポート・ビルダー」に移動し、分類データのインポート レポートを選択し、「ペインに追加」をクリックしてそのレポートをポータルに追加し、そのレポートに移動します。
8. レポートにアクセスし、「カスタマイズ」をクリックして開始日付/終了日付を設定し、レポートを実行します。

レポート結果には、InfoSphere Discovery からインポートされた分類データが含まれます。ダブルクリックして、このレポートに割り当てられている API を呼び出します。Discovery からインポートしたデータは以下の目的で使用できます。

- 結果セットに基づき新規データ・ソースを追加する。
- 機密データ・グループを追加/更新する。
- データ・ソースおよび機密データの詳細に基づきポリシー・ルールを追加する。
- プライバシー・セットを追加する。

CSV インターフェース・シグニチャー

以下の表に、IBM Guardium と InfoSphere Discovery の間の双方向転送で使用される CSV インターフェース・シグニチャーの例を示します。

表 2. CSV インターフェース・シグニチャー

インターフェース・シグニチャー	例
タイプ	DB2
ホスト	9.148.99.99
ポート	50001
dbName (DB2 または Oracle のスキーマ名、またはその他のデータベース名)	cis_schema
データ・ソースの URL	
表名	MK_SCHED
列名	ID_PIN
分類名	SSN
ルールの記述	InfoSphere Discovery のすぐに使用可能なアルゴリズム
HitRate	70% - Guardium バージョンではエクスポートで使用不可 8.2
使用しきい値	60% - Guardium バージョンではエクスポートで使用不可 8.2

親トピック: モニターおよび監査

プライバシー・セット

プライバシー・セットとは、特別なモニターを行うために使用できる要素の集合です。

プライバシー・セットは、1 つ以上のオブジェクト-フィールド・ペアで構成されています。 例えば、employee 表の salary フィールド、 または salary history 表の全フィールドなど。 所定の時間フレーム内のこれらの要素に対する全アクセスをレポート可能です。

プライバシー・セットの処理については、いずれかのトピックを選択してください。

プライバシー・セット・ビルダーを開く

プライバシー・セット定義にアクセスするには、Guardium® ユーザー・アカウントに、 対象のプライバシー・セット定義にも割り当てられているセキュリティー・ロールを割り当てる必要があります。 ユーザーがアクセスできないプライバシー・セットは、プライバシー・セットのリストには表示されません。

1. 以下のいずれかにナビゲートして「プライバシー・セットの識別」パネルを開きます。
   - 「順守」 > 「ツールとビュー」 > 「プライバシー・セット・ビルダー」
   - 「ディスカバー」 > 「データベース・ディスカバリー」 > 「プライバシー・セット・ビルダー」
2. 以下のいずれかを実行します。
   - 「新規」ボタンをクリックして、 新規プライバシー・セットを定義します (『プライバシー・セットの作成』を参照)。
   - リストからプライバシー・セットを選択し、以下のボタンのいずれか 1 つをクリックします。
     - コピー -『プライバシー・セットのコピー作成』を参照してください。
     - 変更 - このボタンを使用して、定義を変更したり、その定義に基づいてレポートを実行したりします。 『プライバシー・セットの変更』または 『プライバシー・セット・レポートの実行』を参照してください。
     - 削除 -『プライバシー・セットの削除』を参照してください。

プライバシー・セットの作成

1. 以下のいずれかにナビゲートして「プライバシー・セットの識別」パネルを開きます。
   - 「順守」 > 「ツールとビュー」 > 「プライバシー・セット・ビルダー」
   - 「ディスカバー」 > 「データベース・ディスカバリー」 > 「プライバシー・セット・ビルダー」
2. 「新規」をクリックして、「プライバシー・セット定義」パネルを開きます。
3. 「プライバシー・セットの記述」ボックスで、 プライバシー・セットの固有の名前を入力します。 名前にはアポストロフィ文字を含めないでください。この名前が、「プライバシー・セットの識別」パネルに表示されます。
4. 「セキュリティー分類」ドロップダウン・リストで、 このプライバシー・セットのセキュリティー分類をオプションで選択します。
5. 「このプライバシー・セットの要素」 ペインで、組み込む要素ペアごとに以下を行います。
   - 「オブジェクト」ボックスにオブジェクト名を入力します。
   - 「フィールド」ボックスにフィールド名を入力するか、 「このオブジェクトの任意のフィールド」ボックスにマークを付けて、 指定したオブジェクト (上記) に含まれるすべてのフィールドを組み込みます。
   - 「新規オブジェクト – フィールド・ペアの追加」をクリックします。
6. すべての要素の追加後、「保存」をクリックします。
7. オプションで「ロール」ボタンをクリックして、ロールを追加します。
8. オプションで「コメント」ボタンをクリックして、コメントを追加します。

プライバシー・セットの変更

1. プライバシー・セット・ビルダーで、変更するプライバシー・セットを開きます。 『プライバシー・セット・ビルダーを開く』を参照してください。
2. 必要に応じて、プライバシー・セット定義に変更を加えます。 すべてのフィールドの説明は、『プライバシー・セットの作成』で参照してください。
3. 「保存」をクリックします。
4. 完了したら、「完了」をクリックします。

プライバシー・セットのコピー作成

1. プライバシー・セット・ビルダーで、コピーを作成するプライバシー・セットを開きます。 『プライバシー・セット・ビルダーを開く』を参照してください。
2. プライバシー・セットのコピーには COPY OF 選択したプライバシー・セットという名前が付けられます。 この名前をより意味のある名前に変更することを推奨します。 名前にはアポストロフィ文字を含めないでください。
3. 必要に応じて、プライバシー・セット定義に追加の変更を加えます。 すべてのフィールドの説明は、『プライバシー・セットの作成』で参照してください。
4. 「保存」をクリックします。
5. 完了したら、「完了」をクリックします。

プライバシー・セットの削除

監査プロセスを実行中の場合は、プライバシー・セットを削除できません。監査プロセスを停止してから手順を実行し、プライバシー・セットを削除してください。

1. 「プライバシー・セットの識別」パネルで、削除するプライバシー・セットを選択します。『プライバシー・セット・ビルダーを開く』を参照してください。
2. 「削除」をクリックして、アクションを確認します。
3. 「完了」をクリックします。

プライバシー・セットの実行

ここでは、プライバシー・セット・レポートをオンデマンドで実行する手順を説明します。 プライバシー・セット・レポートをスケジュールするには、コンプライアンス・ワークフローに組み込みます (『コンプライアンス・ワークフロー自動化』を参照)。

1. プライバシー・セット・ビルダーで、レポートのプライバシー・セットを開きます。 『プライバシー・セット・ビルダーを開く』を参照してください。
2. 「実行」をクリックします。
3. 「タスク・パラメーター」で、タスクの開始時刻および終了時刻を入力します。
4. 「アクセス詳細別レポート」または「アプリケーション・ユーザー別レポート」を選択して、結果の表示方法を指定します。 最初のオプションがデフォルトであり、その場合クライアント IP、 サーバー IP、サーバー (名)、サーバー・タイプ、データベース・プロトコル、 ソース・プログラム名、およびデータベース・ユーザー名の組み合わせごとにアクセス・カウントが表示されます。 「アプリケーション・ユーザー別レポート」を選択すると、レポートには (「データベース・ユーザー名」に続けて) アプリケーション・ユーザーの名前を持つ 個別の列が組み込まれ、さらに出力がそのアプリケーション・ユーザーによって修飾されます。
5. 「今すぐ 1 回実行」をクリックします。実行後のレポートは、別ウィンドウで表示されます。

6. 「完了」をクリックします。

親トピック: モニターおよび監査

カスタム・アラート

アラート・メッセージを配布する方法として、E メール、SNMP、syslog、またはユーザー作成の Java™ クラスが可能です。この最後のオプションを「カスタム・アラート」といいます。

アラートがトリガーされると、カスタム・アラート・クラスは状況に応じて適切な任意のアクションを実行できます (例えば Web ページの更新、電話番号へのテキスト・メッセージの送信など)。

カスタム・アラート・クラスを作成するには、まず技術サポートに連絡して、必要なインターフェース・ファイルを入手してください。以下のトピックでは、インターフェースの実装方法について説明します。『カスタム・アラート・インターフェースの使用』、および例を示す『カスタム・アラート・クラスのサンプル』の各トピックを参照してください。

クラスがコンパイルされたら、Guardium® アプライアンスにアップロードする必要があります。『カスタム・クラスの管理』を参照してください。

カスタム・アラート・クラスのテストに関するガイドラインは、このトピック内の後方にある『カスタム・アラート・クラスのテスト』セクションを参照してください。

注: セキュリティー上の脆弱性のリスクを減らすために、信頼できないデータ・ソースのカスタム・コードを利用および実行しないでください。
注: 信頼できないソースのカスタム・コードを利用および実行しないでください
注: 信頼できないソースのデータを取得するカスタム・クラスを作成しないでください。

カスタム・アラート・インターフェースの使用

カスタム・アラート・クラスを com.guardium.custom パッケージの中に含めて、com.guardium.custom.alerts.CustomerDefinedAlertingIfc インターフェースを実装する必要があります (以下を参照)。

```
package com.guardium.custom
public class YourClassNameHere implements CustomerDefinedAlertingIfc {
       }
```

このインターフェースには、以下に説明する 5 つのメソッドが含まれています。

表 1. processAlert メソッド

メソッド 1	
記述	1 つのアラート・メッセージを処理します。
構文	public void processAlert (String message, Date timeStamp)
パラメーター	アラートによって生成されるメッセージを含む String。 アラート・メッセージの作成時間を示す java.util.Date。

表 2. getMessage メソッド

メソッド 2	
記述	アラート・メッセージを戻します。
構文	public String getMessage ()
パラメーター	アラート・メッセージを含む String。

表 3. getTimeStamp メソッド

メソッド 3	
記述	アラート・メッセージに関連付けられたタイム・スタンプを戻します。
構文	public Date getTimeStamp ()
パラメーター	アラート・メッセージの作成時間を示す java.util.Date。

表 4. setMessage メソッド

メソッド 4	
記述	アラート・メッセージを設定します。
構文	public void setMessage (String inMessage)
パラメーター	アラート・メッセージを含む String。

表 5. setTimeStamp メソッド

メソッド 5	
記述	アラート・メッセージに関連付けられるタイム・スタンプを設定します。
構文	public void setTimeStamp (Date inDate)
パラメーター	アラート・メッセージの作成時間を示す java.util.Date。

カスタム・アラート・クラスのサンプル

以下のサンプル・プログラムは、前のセクションで説明した 5 つのメソッドを実装しています。このプログラムの processAlert メソッドは、単にアラート・メッセージとタイム・スタンプをシステム・コンソールに書き込むだけです。

```
/*
 * Sample Custom Alerting Class
 *
 */
package com.guardium.custom;
import java.text.DateFormat;
import java.util.Date;
public class HandleAlerts implements CustomerDefinedAlertingIfc {
private String message = "";
private Date timeStamp = null;
public void processAlert(String message, Date timeStamp){
setMessage(message);
setTimeStamp(timeStamp);
System.out.println(getMessage() + " on " +
  DateFormat.getDateInstance(). format(getTimeStamp()));
}
    public void setMessage(String inMessage){
        message = inMessage;
    }
    public String getMessage(){
        return message;
    }
    public void setTimeStamp(Date inDate){
        timeStamp = inDate;
    }
    public Date getTimeStamp(){
        return timeStamp;
    }
}
```

カスタム・アラート・クラスのテスト

カスタム・アラート・クラスをコンパイルした後、以下のような手順に従ってテストします。

1. カスタム・クラスをアプライアンスにアップロードします。これは、管理者コンソールから実行する管理機能です。『カスタム・クラスの管理』を参照してください。
2. カスタム・アラート・クラスを使用する相関アラートまたはリアルタイム・アラートを定義します。どのアラート・タイプによってアラートが生成されるかに関わらず、カスタム・アラートの結果の比較対象となる 2 番目の通知タイプ (例えば E メール) を割り当てると、テストが簡単になります。
3. 以下のいずれかを行うことにより、環境を検査します。
    - 相関アラートの場合:
        - 異常検出ポーリング間隔がテストに適した設定になっていること、および異常検出が開始済みであることを確認します。ポーリング間隔が長すぎると (30 分以上)、照会の実行までの待機時間が長くなる可能性があります。
        - アラート機能のポーリング間隔がテストに適した設定になっていること、およびアラート機能が開始済みであることを確認します。
        - テスト対象のアラートにアクティブ状態のマークが付いていることを確認します。
    - リアルタイム・アラートの場合:
        - カスタム・アラート・アクション付きのルールを含むポリシーが、インストール済みポリシーであることを確認します。
        - 更新後のポリシーがインストールされた後、検査エンジンが再始動したことを確認します。
        - アラート機能のポーリング間隔がテストに適した設定になっていること、およびアラート機能が開始済みであることを確認します。
4. アラートをトリガーするために必要なアクションを実行します (例えば、多数のログイン失敗を生成します)。

親トピック: モニターおよび監査

未解析ログ処理

未解析ログ・オプションは、Guardium® アプライアンスが情報を即時に解析することなくログに記録できるようにする処理です。

こうすることで、処理リソースが節約され、より大量のトラフィックを処理できるようになります。後でコレクターまたはアグリゲーター・ユニットにおいて、そのデータを解析して Guardium の内部データベースに組み入れることができます。

注: 未解析ログに関するルールは、フィールド、オブジェクト、SQL 動詞 (コマンド)、オブジェクト/コマンド・グループ、およびオブジェクト/フィールド・グループを含んだポリシー・ルールでは機能しません。未解析ログ処理において、「未解析」とは構文ツリーが構築されていないことを意味します。 構文ツリーがない場合、フィールド、オブジェクト、および SQL 動詞は判別できません。

LOG FULL DETAILS、LOG FULL DETAILS PER SESSION、LOG FULL DETAILS VALUES、LOG FULL DETAILS VALUES PER SESSION、LOG MASKED DETAILS の各アクションは、フラット・ポリシーのルールでは機能しません。

この機能を選択するには、「設定」>「ツールとビュー」の「ポリシー・ビルダー」メニューと、「管理」>「アクティビティー・モニター」の「未解析ログ処理」メニューを操作します。

「ポリシー・ビルダー」の「ポリシー定義」画面にリストされている「未解析ログ」チェック・ボックス・オプションを選択すると、次のようになります。

- データはリアルタイムでは解析されません。
- 未解析ログは、指定された「未解析ログ・リスト」レポートで確認できます。

1. 「管理」 > 「アクティビティー・モニター」 > 「未解析ログ処理」にナビゲートします。
2. 実行するアクティビティーを以下から選択します。
    - プロセス - 未解析ログ情報を内部データベースにマージします。
    - アーカイブ/統合/パージ - 未解析ログをアーカイブまたは統合し、さらにオプションでパージします。
    - パージのみ - 未解析ログ・データをパージします。
3. 「適用」をクリックして構成を保存します。

4. プロセス・アクティビティーの場合、オプションで、以下のいずれかを実行できます。
    - 「今すぐ 1 回実行」をクリックすると、直ちに未解析ログ情報を内部データベースにマージします。
    - 「スケジュールの変更」をクリックすると、このアクティビティーのスケジュールを定義できます。開始時刻、再開の頻度、および繰り返しの頻度を選択できます。「スケジュールの基準..」フィールドで、「曜日」または「月」を選択する必要があります。スケジューリングについて詳しくは、『スケジューリング』を参照してください。

親トピック: モニターおよび監査

照会条件での式の作成

「値」、「パラメーター」、「属性」の選択項目の横にある「式の追加」アイコンを使用して、ユーザー定義文字列と数式を含む照会条件を入力します。

このフィーチャーは、属性の全体的なコンテンツそのものには基づいていないが、その属性の一部、その属性の関数、または複数の属性を組み合わせた関数に基づいた条件を追加する必要がある場合に使用します。

例: `INSTR(:attribute, '150.1') = 5`。これは、リストされる 5 つの文字に一致するクライアント IP のすべてのインスタンスを返します。文字 5 を、「式の追加」アイコンの隣の入力ボックスに入力します。`INSTR(:attribute, '150.1')` 式を、別の「式の作成」ウィンドウに入力します。「式の作成」ウィンドウで、式の妥当性をテストします。 もう 1 つの例: `LENGTH(:attribute) >= 40`。これは、40 文字を超える SQL ステートメントの長さをすべて返します。 式には、実際の属性への参照を含める (または含めない) ことが可能です。 さらに、他の属性への参照を含めることもできます。

親トピック: モニターおよび監査

データベース・ライセンス・レポート

ライセンス・レビューは、ユーザーがそれぞれの業務を行うために必要な特権のみを持っていることを検証および確認するプロセスです。

ユーザーの認証およびデータに対するロールに基づいたアクセス権の制限に加え、最も多くの特権を持つデータベース・ユーザーに対しても、定期的なライセンス・レビューを行う必要があります。このレビューは、ユーザーが自分の業務を行うのに必要な特権のみを持っていることを検証および確認するプロセスです。これは、データベース・ユーザー権限の認証レポート作成とも呼ばれます。

Guardium の事前定義データベース・ライセンス (特権) レポートを使用して、(例えば) システム特権を持つユーザーや、他のユーザーやロールにこれらの特権を付与したユーザーを確認します。データベース・ライセンス・レポートは、データベース・アクセスの変更をトラッキングしたり、使用されないまま残っているアカウントや誤って付与された特権によるセキュリティー・ホールが存在しないことを確認したりする監査員にとって重要なものです。

カスタム・データベース・ライセンス・レポートは、構成にかかる時間を減らし、Oracle、MYSQL、DB2®、SYBASE、SYBASE IQ、Informix®、MS SQL 2000/2005/2008、Netezza®、Teradata、PostgreSQL、および DB2 on z/OS の各データベースからのデータのアップロードおよびレポート作成を容易にするために作成されました。

Microsoft SQL Server データベースおよび Oracle データベースの場合、資格最適化を使用してこの情報にアクセスすることもできます。

以下の手順に従って、データベース・ユーザーおよびアクセス権の最新のスナップショットで作成された Guardium の事前定義データベース・ライセンス (特権) レポートを使用してください。

1. データ・ソース/データベースをアプライアンスに追加します (「順守」 > 「カスタム・レポート作成」 > 「カスタム・ドメイン・ビルダー」にナビゲートします)。
2. データ・ソースをライセンスに割り当てます (「順守」 > 「カスタム・レポート作成」 > 「カスタム表ビルダー」にナビゲートします)。使用するライセンスのカスタム表リストを選択します。「データのアップロード」をクリックします。「データのインポート」メニュー画面で、ライセンス・レポートにデータ・ソースを割り当てます。完了したら、「今すぐ 1 回実行」をクリックします。
3. ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

DB ライセンス・レポートでは、Guardium® のカスタム・ドメイン機能を使用して、選択したデータベース上の外部データと事前定義ライセンス・レポートの内部データとのリンクを作成します。カスタム・ドメイン・ビルダー、カスタム・クエリー・ビルダー、カスタム表ビルダーについての詳細情報は、『外部データ相関』を参照してください。

事前定義の資格レポートは、データベース・ライセンス・レポートにリストされています。

親トピック: モニターおよび監査

ユーザー識別

Guardium® には、データベース・トラフィックから実際のデータベース・ユーザーが識別できない場合に、アプリケーション・ユーザーを識別する方法がいくつか用意されています。

一部のデータベース・アプリケーションは、少数のデータベース・ユーザー・アカウントを使用または共有するように設計されています。 これらのアプリケーションでは、ユーザーがデータベース管理システムとは関係なく管理されます。 つまり、そのアプリケーションの外部からデータベース・トラフィックを監視する場合、任意の時点でデータベース接続を制御しているアプリケーション・ユーザーを判別することが困難になる可能性があります。 しかし、疑わしいデータベース・アクティビティーが発生した場合は、特定のアクションを、個人のグループが共有するアカウントではなく、特定の個人に関連付ける必要があります。 つまり、データベース・ユーザーだけではなく、アプリケーション・ユーザーを認識している必要があります。

Guardium には、データベース・トラフィックから実際のデータベース・ユーザーが識別できない場合に、アプリケーション・ユーザーを識別する方法がいくつか用意されています。

- アプリケーション・ユーザー・トランスレーションによるユーザーの識別 - 広く使用されている一部の商業アプリケーション (Oracle EBS、PeopleSoft、SAP、など) の場合、Guardium は自動的にユーザーを識別できます。
- API によるユーザーの識別 - アプリケーション・イベント API を使用すると、アプリケーション・ユーザーが接続の制御を行ったり解放したりした場合、またはその他関心のあるイベントが発生した場合に、Guardium にシグナルを通知することができます。 (これは、ユーザーの識別以外にも使用できます。)
- ストアード・プロシージャーによるユーザーの識別 - 多くのアプリケーションでは、データベースのストアード・プロシージャーがアプリケーション・ユーザーの識別に使用されます。 このような場合、ユーザー情報は、通常、ストアード・プロシージャーのパラメーターから抽出できます。

社内では、使用するアプリケーションに応じて、ユーザーの識別に複数の方法を使用する必要が生じる場合があります。

- アプリケーション・ユーザー・トランスレーションによるユーザーの識別
  一部のアプリケーションは、データベース接続のプールを管理します。 そのような 3 層アーキテクチャーでは、プールされた接続はすべて単一の機能 ID を使用してデータベースにログインし、すべてのアプリケーション・ユーザーを内部で管理します。ユーザー・セッションでそのデータベースにアクセスする必要がある場合、プールから接続を獲得し、その接続を使用した後、リリースしてプールに返します。このような状況が発生した場合、Guardium では、アプリケーションがデータベースと対話する方法は確認できますが、特定のデータベース・アクションを特定のアプリケーション・ユーザーに結びつけることはできません。
- API によるユーザーの識別
  ユーザーを内部的に管理するアプリケーションでは、アプリケーション・ユーザーをトラフィックから識別できないものがあります。 この場合に、Guardium アプリケーション・イベント API を使用できます。
- ストアード・プロシージャーによるユーザーの識別
  既存の多くのアプリケーションでは、アプリケーション・ユーザーの識別に必要なすべての情報が既存のデータベース・トラフィックから (ストアード・プロシージャー呼び出しから) 得られます。どの呼び出しを監視すべきか、どのパラメーターにユーザー名その他の必要情報が含まれるかを Guardium で認識しておくと、ユーザーを自動的に識別できます。

親トピック: モニターおよび監査

アプリケーション・ユーザー・トランスレーションによるユーザーの識別

一部のアプリケーションは、データベース接続のプールを管理します。 そのような 3 層アーキテクチャーでは、プールされた接続はすべて単一の機能 ID を使用してデータベースにログインし、すべてのアプリケーション・ユーザーを内部で管理します。ユーザー・セッションでそのデータベースにアクセスする必要がある場合、プールから接続を獲得し、その接続を使用した後、リリースしてプールに返します。このような状況が発生した場合、Guardium® では、アプリケーションがデータベースと対話する方法は確認できますが、特定のデータベース・アクションを特定のアプリケーション・ユーザーに結びつけることはできません。

Guardium には、一部の幅広く使用されるアプリケーションを対象として、アプリケーションからエンド・ユーザー情報を識別する標準装備サポートがあります。 それにより、データベース・アクティビティーをアプリケーション・エンド・ユーザーに関連付けることができます。

この機能を使用するには、以下の手順に従ってください。

1. アプリケーションのアプリケーション・ユーザー・トランスレーション構成を定義します。 『アプリケーション・ユーザー検出の構成』を参照してください。
2. そのアプリケーションに必要なすべての事前定義グループにデータを設定します。 『事前定義アプリケーション・グループへのデータの設定』を参照してください。
3. そのアプリケーションの特殊レポート用のすべてのポートレットを再生成して、そのポートレットをページに配置します。 『特殊アプリケーション・レポート・ポートレットの再生成』を参照してください。

選択的な監査証跡およびアプリケーション・ユーザー・トランスレーション

インストールしたデータ・アクセス・ポリシーで、選択的監査証跡機能を使用してログに記録されるデータ数を制限している場合、アプリケーション・ユーザー・トランスレーションに適用される 2 つの重要な考慮事項があります。

- ポリシーは、アプリケーション・ユーザー・トランスレーション・ルールに合致しない (例えば、 アプリケーション・サーバーが発信元ではない) すべてのトラフィックを無視します。
- そのセキュリティー・ポリシーのパターンに合致する SQL だけが、特殊アプリケーション・ユーザー・トランスレーション・レポートの対象になります。

アプリケーション・ユーザー検出の構成

1. 「保護」 > 「データベースの侵入検出」 > 「アプリケーション・ユーザー・トランスレーション」にナビゲートします。既存のアプリケーション・ユーザー・トランスレーション構成の詳細がページの上部に表示されます。
2. 「アプリケーション・コード」ボックスに固有のコードを入力して、新規のアプリケーション・ユーザー・トランスレーション構成の作成を開始します。
   注: 一元管理を行っている場合、管理マシンごとに異なるアプリケーション・コードを使用する必要があります。そうすることで、ユーザーごとに生成される別名が、相互に競合することを防ぎます。 (一元管理を行っている場合、すべての管理対象ユニットで共有される一式の別名セットがあります。
3. 「アプリケーション・タイプ」リストから、次のアプリケーション・タイプを選択します。
   - BO-WI - Business Objects / Web Intelligence
   - EBS - Oracle E-Business Suite
   - PeopleSoft
   - SAP Observed
   - SAP DB
   - SIEBEL Observed
   - SIEBEL DB
4. 「アプリケーション・バージョン」ボックスで、アプリケーション・バージョン番号 (例えば、11 など) を入力します。
5. 「データベース・タイプ」リストから、データベース・タイプを選択します。 選択したアプリケーション・タイプおよびバージョンで使用可能なタイプのみが表示されます。
   注: 「アプリケーション・タイプ」が EBS、SIEBEL DB、または SAP DB に設定されている場合、「データ・ソースの追加」ボタンをクリックして既存のデータ・ソースから選択するオプションがあります。データ・ソースは、構成中のアプリケーション・タイプに対してサポートされているデータベース・タイプの 1 つと一致する必要があります。
6. 「サーバー IP」ボックスで、アプリケーションがデータベースに接続するために使用する IP アドレスを入力します。
7. 「ポート」ボックスで、アプリケーションがデータベースに接続するために使用するポート番号を入力します。
8. 「インスタンス名」ボックスで、アプリケーションがデータベースに接続するために使用するインスタンス名を入力します。
9. 「データベース名」ボックスで、アプリケーションのデータベース名を入力します。 (一部のアプリケーションでのみ必須であり、それ以外では使用されません。)
10. 「アクティブ」ボックスにマークを付けて、ユーザー・トランスレーションを有効にします。 ユーザー定義の最初のインポートが完了するまで、変換は行われません。
11. データベースへのアクセス時に使用する Guardium の「ユーザー名」を入力します。データベースへのアクセス時に使用する Guardium の「パスワード」を入力します。
12. 責務 (例えば、管理など) とユーザー名を関連付ける場合は、「責務」ボックスにマークを付けます。 ユーザー名だけを記録する場合、「責務」ボックスはクリアします。 このボックスをクリアすると、ユーザーが実行したすべてのアクティビティーが、アクティビティー発生時の責務に関係なくグループ化されます。

注: アプリケーション・タイプが EBS (データベース・タイプは Oracle) である場合、「接続先サーバー IP」および「接続先ユーザー名」という 2 つの追加の選択項目が表示されます。これらに値を指定すると、システムはその IP およびユーザー名を使用して接続し、責務およびユーザー名を検索します。

13. 「追加」ボタンをクリックして、アプリケーション・ユーザー・トランスレーション定義を保存します。
14. 続いて、『事前定義アプリケーション・グループへのデータの設定』 および『特殊アプリケーション・レポート・ポートレットの再生成』の手順に進みます。
15. 前のステップが完了したら、「管理」 > 「アクティビティー・モニター」 > 「検査エンジン」にナビゲートし、「検査エンジン構成」パネルで「検査エンジンの再始動」をクリックします。
16. ステップ 16 の 2 つの手順で指定したタスクの実行後、「アプリケーション・ユーザー・トランスレーション」に戻って「今すぐ 1 回実行」をクリックし、このアプリケーション (およびその他定義されたもの) のユーザー定義をインポートします。
17. データ・インポート操作が正常に処理されたことを検証 (ステップ 20 を参照) した後で、このパネルに戻って「スケジュールの変更」ボタンをクリックし、定期的に実行されるインポート操作を定義します。 ユーザー定義データのインポートは、使用環境に適した間隔で行われるようにスケジュールする必要があります。 新規アプリケーション・ユーザー名が使用可能になるまでの最大時間は、インポート操作の実行間隔の時間です。 スケジューラーの使用方法に関する説明については、『スケジューリング』を参照してください。
18. アプリケーション・ユーザー・トランスレーションのデータ・インポートは、事前定義レポート (例えば、SAP アプリケーション・アクセス) を調べることで確認できます。 「レポート」 > 「レポート構成ツール」 > 「レポート・ビルダー」にナビゲートし、「SAP アプリケーション・アクセス」レポートを選択します。このレポートを再生成してペインに追加してから、日付範囲を比較的大きく (例えば、データについて過去 1 年間遡るなど) 設定してください。

注: アプリケーション・ユーザー・トランスレーション設定のインストール後に初めて「今すぐ 1 回実行」をクリックすると、調べている表の最終更新日付が検索されます。 その後は、新規データのみがインポートされます。この操作を行わないと、数十年分に相当するデータが不必要にインポートされて、多くの表やデータベースが満杯になる可能性があります。

事前定義アプリケーション・グループへのデータの設定

アプリケーション・ユーザー・トランスレーションが構成済みの場合、少なくとも 2 つの事前定義グループに、使用環境に固有の情報を設定する必要があります。 以下の表は、アプリケーション・タイプごとにデータを設定する必要があるグループを示しています。 グループへのデータの設定方法に関する説明については、『グループの概要』を参照してください。

アプリケーション	事前定義グループ	グループ・タイプ
EBS	EBS アプリケーション・サーバー	クライアント IP
	EBS データベース・サーバー	サーバー IP
PeopleSoft	PSFT アプリケーション・サーバー	クライアント IP
	PSFT データベース・サーバー	サーバー IP
	PeopleSoft オブジェクト	オブジェクト
Siebel	SIEBEL アプリケーション・サーバー	クライアント IP
	SIEBEL データベース・サーバー	サーバー IP
SAP	SAP アプリケーション・サーバー	クライアント IP
	SAP データベース・サーバー	サーバー IP
	SAP - PCI	オブジェクト

特殊アプリケーション・レポート・ポートレットの再生成

一部のアプリケーション・タイプについては、1 つ以上の特殊レポート・ポートレットを再生成する必要があります。 例えば、2 つの事前定義 EBS レポートと 2 つの事前定義 PeopleSoft レポートがあるとします。 これらのレポートは変更できません。 事前定義アプリケーション・グループにデータを設定したら、以下の手順に従って事前定義アプリケーション・ポートレットを再生成し、それらをページに配置します。

このセクションでは EBS ポートレットの例を示していますが、他のアプリケーション・タイプの場合でも手順は同じです。

1. 以下のいずれかを実行して、レポート・ファインダーを開きます。admin ロールを持つユーザーの場合:「ツール」-「レポートのビルド」-「レポート・ビルダー」を選択します。 その他のユーザーの場合:「モニター/監査」-「レポートのビルド」-「レポート・ビルダー」を選択します。
2. 「検索」をクリックして「レポート検索結果」パネルを開きます。
3. このアプリケーション・タイプのレポート・ポートレット (例えば、EBS アプリケーション・アクセスなど) を選択し、「ポートレットの再生成」をクリックします。ポートレットが再生成されたことが通知されます。
4. アプリケーション・レポート (例えば、EBS プロセス・データベース・アクセス、PSFT プロセス・データベース・アクセス・レポートなど) ごとに前のステップを繰り返します。ここでレイアウトにタブを追加して、そのタブに再生成された 2 つのポートレットを組み込みます。
5. 「カスタマイズ」をクリックして、「カスタマイズ」ペインを開きます。
6. 「ペインの追加」をクリックして、新規タブを定義します。
7. タブに名前 (例えば、「EBS レポート」) を入力し、「適用」をクリックします。リストの最後のタブとして、新規タブが表示されます。
8. 新規タブ名をクリックし、そのペインを編集します。
9. 「ポートレットの追加」をクリックし、必要なレポート (EBS レポートなど) が見つかるまで「次へ」をクリックし、対象となる各レポートの横にあるチェック・ボックスにマークを付けます。
10. 「適用」をクリックしてから「保存」をクリックし、新規ペインのレイアウトを保存します。タブ群の 1 行目の末尾に、新規タブが表示されます。
11. 新規タブ名をクリックし、タブを開きます。
12. 「カスタマイズ」をクリックし、ランタイム・パラメーター (日付範囲、「別名の表示」など) を設定します。

EBS アプリケーションの DB_USER パスワードを指定するのが好ましくない場合

特定の状況では、EBS トラフィックの変換に Oracle EBS の DB_USER を使用したくないユーザーも存在します。 このシナリオでは、Oracle EBS を設定して、アプリケーション・ユーザー・トランスレーションでトラフィックを変換するための以下の 2 つの選択肢があります。

- EBS が Oracle への通信に使用するユーザー名およびパスワード (多くの場合 APPS/$passwd) を指定します。

- DB_USER EBS が Oracle へのアクセスに使用するパスワードをユーザーが指定/入力したくない場合でも、アプリケーション・ユーザー・トランスレーションを行うことは可能ですが、その処理はさらに複雑になります。

1. 別名/ユーザー/責務を収集するためにデータベースにアクセスすることを許可する Oracle 用のログインを作成/選択します。 そのユーザーには、表 [APPLSYS.]FND_USER およびビュー FND_RESPONSIBILITY_VL (2 つの表 APPLSYS.FND_RESPONSIBILITY および APPLSYS.FND_RESPONSIBILITY_TL を組み合わせたもの) に対するアクセス権限が必要です。

```
(  CREATE VIEW FND_RESPONSIBILITY_VL AS SELECT /* $HEADER$ */ B.ROWID ROW_ID , B.WEB_HOST_NAME ,
B.WEB_AGENT_NAME , B.APPLICATION_ID , B.RESPONSIBILITY_ID ,
B.RESPONSIBILITY_KEY , B.LAST_UPDATE_DATE , B.LAST_UPDATED_BY ,
B.CREATION_DATE , B.CREATED_BY , B.LAST_UPDATE_LOGIN ,
B.DATA_GROUP_APPLICATION_ID , B.DATA_GROUP_ID , B.MENU_ID ,
B.START_DATE , B.END_DATE , B.GROUP_APPLICATION_ID ,
B.REQUEST_GROUP_ID , B.VERSION , T.RESPONSIBILITY_NAME ,
T.DESCRIPTION FROM FND_RESPONSIBILITY_TL T, FND_RESPONSIBILITY B
WHERE B.RESPONSIBILITY_ID = T.RESPONSIBILITY_ID
AND B.APPLICATION_ID = T.APPLICATION_ID
AND T.LANGUAGE = USERENV('LANG')  )
```

2. 次の SQL ステートメントを Guardium システムから直接実行します。select RESPONSIBILITY_ID, RESPONSIBILITY_NAME from FND_RESPONSIBILITY_VL order by RESPONSIBILITY_ID; および SELECT USER_ID, USER_NAME from FND_USER ORDER BY USER_ID;

   これら 2 つのステートメントを正常に実行するためのユーザーの設定が完了した後、2 つの異なるアプリケーション・ユーザー・トランスレーション項目が必要になります。 これらの各項目に含まれるサーバー IP、ポート、およびインスタンス名 (そしてアプリケーション・タイプおよびアプリケーション・サーバー・タイプとして選択された EBS および Oracle) は、同じでなければなりません。

   アプリケーション・コードが同じであるかどうかは関係ありません。 一方の項目には、EBS がデータベースへの接続に使用するユーザー名 (通常は APPS) が必要ですが、指定するパスワードは不正確 (ダミー) であってもかまいません。 もう一方の項目には、これらの表にアクセスするために作成されたユーザー名およびパスワードが必要です。

3. 「アクティブ」および「責務」を選択してこれら両方の項目を入力した後、「今すぐ 1 回実行」をクリックして EBS を開始または再始動します (トラフィックを調べる検査エンジン (S-TAP® またはネット) があることを想定しています)。 このようにすると、EBS トラフィックに関するデータの収集とそのデータに対する APPS ユーザー名の割り当てが行われるようになります。

Oracle EBS アプリケーション・ユーザーに必要な Oracle の特権

トランスレーション:

1. カスタム DB ユーザーに対して、以下の表における select を認可します。

   APPLSYS.FND_USER

   APPLSYS.FND_RESPONSIBILITY

   APPLSYS.FND_RESPONSIBILITY_TL

2. カスタム DB ユーザーに対して、APPLSYS.FND_USER における専用の同義語 FND_USER を作成します。
3. カスタム DB ユーザーに対して、FND_RESPONSIBILITY_VL という名のビューを作成します。 このビューは APPS ユーザーの下にあり、テンプレートとして使用できます。

SAP スタックのアプリケーション・ユーザー・トランスレーション対応の検証方法

IBM Guardium SAP アプリケーション・ユーザー・トランスレーションをサポートする場合、ABAP スタックと Java™ スタックでは方法が異なります。
注:

ABAP スタックと Java スタックではカーネルの仕様が異なります。

ABAP スタックと Java スタックのシステムでは、使用する表が異なります。

ABAP スタック

従来の ECC (Enterprise Core Components) SAP システムは ABAP コードで記述され、 主に SAP GUI を使用してアクセスしますが、Web アクセスも可能です。

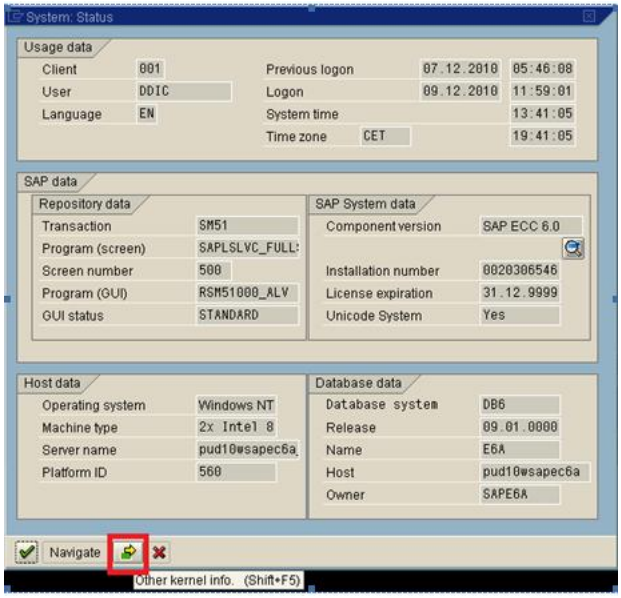
SAP ABAP システムは、従来の SAP データベースに対して直接 (読み取り/書き込み/更新) アクセスを行います。 データベースは非常に大規模で、すべての機密データが含まれます。 このような状況では、IBM Guardium が非常に役に立ちます。

SAP GUI (ABAP スタック) にアクセスすると次の画面が表示されます。

1-SAP GUI (ABAP スタック)

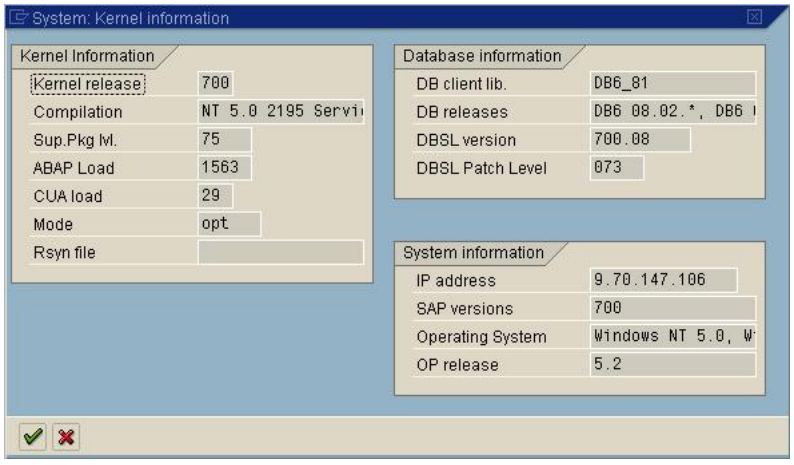
ABAP スタックの SAP カーネル・モジュールのアプリケーション・ユーザー・トランスレーション対応を検証するには、以下の手順を行います。

1. SAP にログインします。
2. 「システム」>「ステータス」に移動します。



2-システム状況 (ABAP スタック)

3. 「システム状況」画面で「その他のカーネル情報 (Other Kernel Info)」をクリックします。



3- システム・カーネル情報 (ABAP スタック)

この例では、カーネルは 700 です。

DB2® をバックエンドに持つ SAP は、SAP カーネル 640 でも使用可能ですが、ユーザーは DB6_DBSL_ACCOUNTING=1 を設定する必要があります (カーネル 700 以降では、この DB6_DBSL_ACCOUNTING 値はデフォルトで 1 です)。Oracle をバックエンドに持つ SAP では、カーネル 710 以降が必要です。

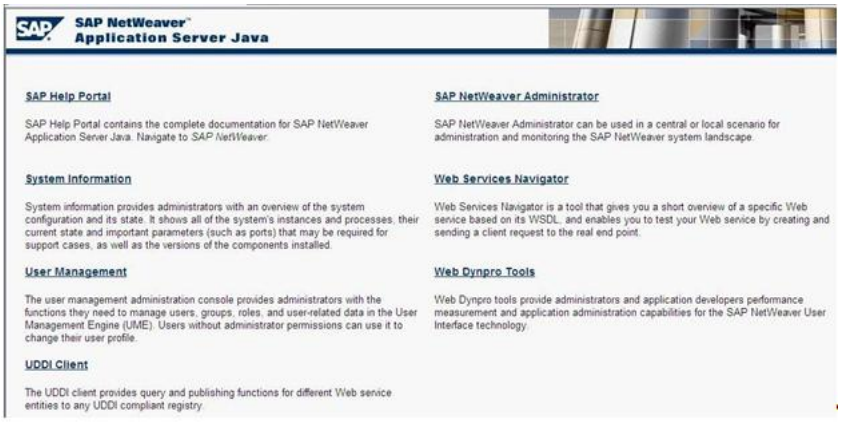
データは、アプリケーション・ユーザー・フィールドおよびアプリケーション・イベント文字列に入力されます。

Java スタック

SAP ポータル・システムは Java コードで記述されたフロントエンド Web アプリケーションで、事前に用意された照会を利用して SAP 関連の Web ページを表示します。

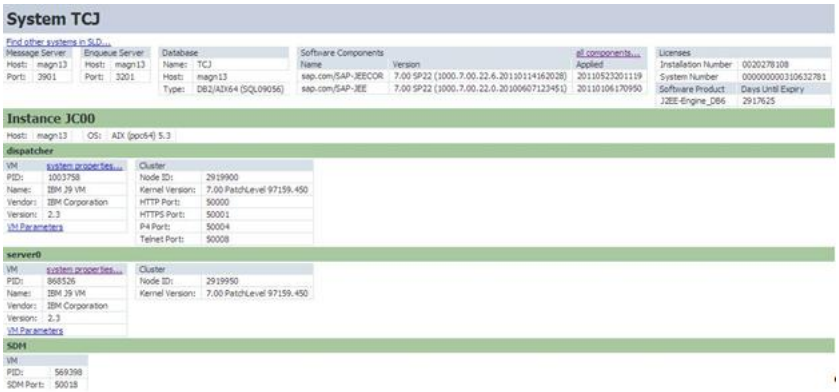
ポータル・システムは、Web ブラウザーからのみアクセス可能です。ポータル・システムのデータベースは非常に小規模であり、表領域はわずかしかありません。

SAP ポータル・システム (Java スタック) にアクセスすると次の画面が表示されます。



4-SAP ポータル・システム (Java スタック)

Java スタックの SAP カーネル・モジュールのアプリケーション・ユーザー・トランスレーション対応を検証するには、以下の手順を行います。 1.「システム情報」をクリックします。



5-システム TCJ (Java スタック)

この例では、SAP カーネル・バージョンは 7.00 です。

DB2 または Oracle 用の SAP では、7.02 以降のカーネルが必要です。

SAP は、ABAP スタックと同様に Java スタックにクライアント・プロパティーを設定します。

親トピック: ユーザー識別

API によるユーザーの識別

ユーザーを内部的に管理するアプリケーションでは、アプリケーション・ユーザーをトラフィックから識別できないものがあります。 この場合に、Guardium® アプリケーション・イベント API を使用できます。

アプリケーション・イベント API は、ユーザーが接続を獲得/リリースしたときや、他の対象とするイベントが発生した場合に、Guardium にシグナル通知するためにアプリケーション内から発行できる単純な呼び出しを用意しています。

注: Guardium セキュリティー・ポリシーで選択的な監査証跡が有効にされている場合、アプリケーション・ユーザー/アプリケーション・イベントの設定とクリアに使用したアプリケーション・イベント API コマンドはデフォルトで無視され、アプリケーション・ユーザー名/アプリケーション・イベントは記録されません。これらの項目を記録してレポートや例外で使用できるようにするには、「監査のみ」のルール・アクションを指定して、適切なコマンドを識別するためのポリシー・ルールを組み込んでください。

GuardAppUser - API によるユーザーの識別

アプリケーション・ユーザー名とアプリケーション・イベント名の両方に 2 つの事前定義トリガーを使用して、 GDM_CONSTRUCT_INSTANCE.APP_USER_NAME と GDM_APP_EVENT.* を設定します。

これらの事前定義トリガーは以下のとおりです。

- GuardAppEvent
- GuardAppUser

これらの各トリガーにより、トリガーが開始および停止されています。イベントには、Type、Username、StrValue、NumValue、および Date を設定するサブトリガーがあります。

Guardium システムは、AppUserName と AppEvent の詳細についての特殊な SELECT ステートメントを読み取ることができます。

形式は次のとおりです。

```
Select "action" [additional parameters] FROM [location].
```

表 1. アクション・オプション

構文	アクション
GuardAppUser:<username>	GDM_CONSTRUCT_INSTANCE.APP_USER_NAME を <username> に設定
GuardAppUserReleased	後続の照会のために APP_USER_NAME をクリア
GuardAppEvent:Start	GuardAppEvent を開始 (そして追加のパラメーターを検索)
GuardAppEvent:Released	GuardAppEvent を終了 (後続の照会のために情報をクリア)

表 2. 追加パラメーター (GDM_APP_EVENT の値を設定)

パラメーター	構文
GuardAppEventType: <event type string>	APP_EVENT_TYPE を <event type string> に設定
GuardAppEventUserName:<evntursname>	GDM_APP_EVENT.APP_USER_NAME を <evnturs name> に設定
GuardAppEventStrValue:<strvalue>	EVENT_VALUE_STR を <strvalue> に設定
GuardAppEventNumValue:<num>	EVENT_VALUE_NUM を <num> に設定
GuardAppEventDateValue:<date>	EVENT_DATE を <date> に設定

SELECT ステートメントの例をいくつか示します。

Select guardappuser:tiberius from dual

Select guardappuserreleased from dual

Select GuardAppEvent:Start, GuardAppEventType:Event1, GuardAppEventUserName:Tiberius, GuardAppEventStrValue:abc, GuardAppEventNumValue:123, GuardAppEventDateValue:2016-01-26 15:55:28 from dual

Select GuardAppEvent:Released from dual

ステートメントの FROM 部分は、データベース・タイプにより異なります。

Oracle の場合: from DUAL

Db2 の場合: from SYSIBM.SYSDUMMY1

Informix の場合： from SYSTABLES

MS-SQL の場合： <blank>

Sybase の場合: <blank>

MySQL の場合: <blank> または from DUAL のいずれか

Guardium によるアプリケーション・ユーザー名および名前付きテンプレートの特定

Guardium を使用して「アプリケーション・ユーザー名」を取得するにはいくつかの方法があります。 Guardium には、データが受信された方法に基づいて、APP_USER_NAME フィールド値が保管される 2 つの Turbine 表があります。

GDM_CONSTRUCT_INSTANCE

GDM_APP_EVENT

Guardium 内の名前付きテンプレートの %%AppUserName パラメーター (「グローバル・プロファイル」メニューを参照) は、Turbine 表 (GDM_CONSTRUCT_INSTANCE) にマップされます。Guardium では、名前付きテンプレートでそのパラメーターを使用するには、GDM_CONSTRUCT_INSTANCE 表内の APP_USER_NAME に「アプリケーション・ユーザー」の値を取り込む必要があります。

アプリケーションの SQL コマンドの構文を以下のように変更します。

SELECT 'GuardAppUser:<value>'

これにより値は、正しい表に挿入され、名前付きテンプレートの %%AppUserName パラメーターは正しい値に置き換わります。

例

.....

select 'GuardAppUser:Db2_User' FROM SYSIBM.SYSDUMMY1 ;

select * from AppUser_DB2;

select 'GuardAppUserReleased' FROM SYSIBM.SYSDUMMY1 ;

select * from NoMoreUser_DB2;

.....

/var/log/messages ファイルで結果を検索します。

Jan 24 12:49:41 vx64 guard_sender[28274]: LEEF:1.0|IBM|Guardium|10.0|Alert per match|ruleID=20003|ruleDesc=Alert per match|severity=INFO|devTime=2016-01-24
11:50:39|serverType=DB2|classification=|category=|dbProtocolVersion=3.0|usrName=Db2_User|sourceProgram=DB2JCC_APPLICATION|start=1448383760000|dbUser=DB2INST1|dst=9.70.144.126|dstPort=50000|src=9.70.144.126|srcPort=58781|protocol=TCP|type=SQL_LANG|violationID=20|sql=select * from AppUser_DB2 FOR READ ONLY|error=

GuardAppUser によるアプリケーション・ユーザーの設定

この呼び出しを使用して、新しいアプリケーション・ユーザーが接続の制御を取得したことを示します。 指定されたアプリケーション・ユーザー名は、アクセス期間エンティティーのアプリケーション・ユーザー属性で使用可能になります。 このセッションについてこの時点以降、Guardium は、接続におけるすべてのアクティビティーがこのアプリケーション・ユーザーによるものと見なします。これは、 Guardium が別の GuardAppUser 呼び出しまたは GuardAppUserReleased 呼び出し (アプリケーション・ユーザー名をクリアする) を受け取るまで続きます。

他のイベントの発生をシグナル通知するには (必要に応じてイベント・タイプが定義可能)、後述のセクションの GuardAppEvent 呼び出しを使用します。

構文: SELECT 'GuardAppUser:user_name' FROM location

user_name は、アプリケーション・ユーザー名を含んだ文字列です。 この文字列は、アクセス期間エンティティーのアプリケーション・ユーザー属性値として使用できます。

FROM location は、Oracle、DB2®、または Informix® の場合にのみ使用します。 (他のデータベース・タイプでは省略。) これは、 次のように正確に入力する必要があります。

- Oracle: FROM DUAL
- DB2: FROM SYSIBM.SYSDUMMY1
- Informix: FROM SYSTABLES

GuardAppUserReleased によるアプリケーション・ユーザーのクリア

GuardAppUserReleased 呼び出しを使用して、現行ユーザーが接続の制御を解放したことをシグナル通知します。 Guardium によりアプリケーション・ユーザー名がクリアされます。この名前は、 別の GuardAppUser 呼び出しを受け取るまで、その接続で空の状態にされます。

構文: SELECT 'GuardAppUserReleased' FROM location

FROM location は、Oracle、DB2、または Informix の場合にのみ使用します。 (他のデータベース・タイプでは省略。) これは、 次のように正確に入力する必要があります。

- Oracle: FROM DUAL
- DB2: FROM SYSIBM.SYSDUMMY1
- Informix: FROM SYSTABLES

GuardAppEvent によるアプリケーション・イベントの設定

この呼び出しは、アプリケーション・イベントの発生をシグナル通知するもっと汎用の方法を提供します。 独自のイベント・タイプを定義して、イベント (イベントの開始時と終了時の両方) とともに格納するテキスト、数値、または日付値を指定できます。この呼び出しは、GuardAppUser 呼び出しとともに使用できます。Guardium は、接続におけるすべてのアクティビティーがこのアプリケーション・イベントのものとみなします。これは、別の GuardAppEvent:Start コマンドか GuardAppEvent:Released コマンドを受け取るまで続きます。

構文:

SELECT 'GuardAppEvent:Start|Released',

'GuardAppEventType:type',

'GuardAppEventUserName:name',

'GuardAppEventStrValue:string',

'GuardAppEventNumValue:number',

'GuardAppEventDateValue:date' FROM location

Start | Released - キーワード Start を使用してイベントが接続の制御を取得していることを示します。 または Released を使用してイベントが接続の制御を解放したことを示します。

type はイベント・タイプを示します。 これは、Login、Logout、Credit、Debit などの任意の文字列値にできます。アプリケーション・イベント・エンティティーで、この値は「イベント・タイプ」属性 (Start 呼び出しの場合) か「イベント・リリース・タイプ」属性 (Released 呼び出しの場合) に格納されます。

name は、このイベントに設定するユーザー名の値です。 アプリケーション・イベント・エンティティーで、この値は「イベント・ユーザー名」属性 (Start 呼び出しの場合) か「イベント・リリース・ユーザー名」属性 (Released 呼び出しの場合) に格納されます。

string は、このイベントに設定する任意の文字列値です。 例えば、Login イベントの場合に、アカウント名を指定することができます。 アプリケーション・イベント・エンティティーで、この値は「イベント値 (文字列)」属性 (Start 呼び出しの場合) か「イベント・リリース値 (文字列)」属性 (Released 呼び出しの場合) に格納されます。

number は、このイベントに設定する任意の数値です。 例えば、Credit イベントの場合に、取引金額を指定することができます。 アプリケーション・イベント・エンティティーで、この値は「イベント値 (数値)」属性 (Start 呼び出しの場合) か「イベント・リリース値 (数値)」属性 (Released 呼び出しの場合) に格納されます。

date は、このイベントのユーザー指定の日付とオプションの時刻です。 形式は、yyyy-mm-dd hh:mm:ss とする必要がありますが、時刻の部分 (hh:mm:ss) はオプションです。 これは、現在の日時にすることも、トラックされているトランザクションから取得することもできます。 アプリケーション・イベント・エンティティーで、この値は「イベントの日付」属性 (Start 呼び出しの場合) か「イベント・リリース日付」属性 (Released 呼び出しの場合) に格納されます。

FROM location は、Oracle、DB2、または Informix の場合にのみ使用します。 (他のデータベース・タイプでは省略。) 以下の例を参照してください。ただし、ダミー SQL では、ダミーの表名が許可されます。

- Oracle: FROM DUAL
- DB2: FROM SYSIBM.SYSDUMMY1
- Informix: FROM SYSTABLES

GuardAppEvent 呼び出しは、アプリケーション・イベント・エンティティーにデータを設定します (付録の『エンティティーおよび属性』セクションの『アプリケーション・イベント・エンティティー』を参照)。 Guardium の照会およびレポートを作成する際、アクセスのトラッキング・ドメインまたはポリシー違反ドメインからアプリケーション・イベント・エンティティーにアクセスができます。

GuardAppEvent 呼び出しを使用してアプリケーション・イベント・エンティティーの属性が設定されていなければ、これらの値は空となります。

2 つの日付属性について:

- 「イベントの日付」は、 GuardAppEvent 呼び出しを使用して設定するか、カスタム識別の手順 (以降のセクションで説明) から設定します。
- 「タイム・スタンプ」は、 Guardium がアプリケーション・イベント・エンティティーのインスタンスを格納した時刻です。

親トピック: ユーザー識別

ストアード・プロシージャーによるユーザーの識別

既存の多くのアプリケーションでは、アプリケーション・ユーザーの識別に必要なすべての情報が既存のデータベース・トラフィックから (ストアード・プロシージャー呼び出しから) 得られます。どの呼び出しを監視すべきか、どのパラメーターにユーザー名その他の必要情報が含まれるかを Guardium® で認識しておくと、ユーザーを自動的に識別できます。

最も単純なケースとしては、多数のプロパティー値 (そのうち 1 つはユーザー名) を設定する 1 つのストアード・プロシージャーがアプリケーションに含まれるといったものを想定できます。ユーザー名を設定する呼び出しは、例えば次のようになります。

```
set_application_property('user_name', 'JohnDoe');
```

(下記で説明する) カスタム・プロシージャー・マッピングでは、以下の動作を Guardium に指示できます。

- 最初のパラメーター値が user_name である set_application_property というストアード・プロシージャーを監視する。
- アプリケーション・ユーザーを、呼び出しにおける 2 番目のパラメーターの値 (例では JohnDoe) に設定する。

1 つのアプリケーションに複数のストアード・プロシージャーが含まれる場合もあり得ます。そのうち 1 つはアプリケーション・ユーザー・セッションを開始し、1 つはセッションを終了し、それ以外のストアード・プロシージャーはそのアプリケーションに特有の主要なイベントを通知するような場合です。Guardium のカスタム識別プロシージャー・メカニズムを使用すると、任意のアプリケーション・イベントをモニター対象としてトラッキングできます。

ユーザーを識別する方法はアプリケーションごとに異なる可能性があるため、各アプリケーション用に別個のカスタム識別プロシージャー・マッピングを定義する必要が生じることがあります。これを行うには、以下に要約する手順に従います。

カスタム識別プロシージャー・マッピングの定義

1. 「保護」 > 「データベースの侵入検出」 > 「カスタム ID プロシージャー」にナビゲートします。
2. 既存のマッピングを表示するには、表示対象のマップを含む行の「詳細情報」列アイコンの上にマウス・ポインターを置きます。
3. マッピングを追加するには、「追加」をクリックします。
4. 「カスタム・マップ名」ボックスで、このマッピングに使用する名前を入力します。
5. 「プロシージャー名」ボックスでは、情報を提供するデータベース・プロシージャーの名前を入力します。
6. アクション・リストから「設定」または「クリア」を選択します。これは、プロシージャー呼び出しによってアプリケーション値の設定または消去のどちらを実行するかを指示します。 クリア・アクションが選択された場合、「イベント・タイプの位置」フィールドが特殊な方法で使用されます。
7. 既存のストアード・プロシージャー呼び出しから、1 つまたは 2 つの条件の下でのみ、アプリケーション情報が得られる場合には、
   - 条件のロケーション・ボックスを使用して、検査対象となるストアード・プロシージャー呼び出しパラメーターを指定します
   - 対応する条件の値ボックスを使用して、他の 1 つ以上のパラメーターからアプリケーション情報を設定するためにマッチさせる必要のある値を指定します。
   - 例えば、多数の値 (その 1 つはユーザー名) を設定するために set_context という名前のストアード・プロシージャーがアプリケーションで使われるとします。3 つのパラメーター (アプリケーション名、プロパティー名、および値) がプロシージャーに渡されます。標準的な 3 つの呼び出しを示します。
     - set_context('publishing_application', 'role_name', 'manager');
     - set_context('publishing_application', 'user_name', 'jsmith');
     - set_context('publishing_application', 'company', 'guardium');
   - 例では、対象となる呼び出しの形式が 2 番目のステートメントによって表されています。検査すべきパラメーターは 2 番目のパラメーター (プロパティー名) であるため、「条件 1: ロケーション」ボックスに 2 を入力して、「条件 1: 値」ボックスに user_name を入力します。
   - さらに、呼び出しの別の形式でもユーザー名を設定する場合には、「条件 2: ロケーション」および「条件 2: 値」ボックスを使用できます。例えば、以下のような形式のプロシージャー呼び出しを使ってユーザー名が設定されることがあるとします。
     - set_context('admin_application', 'admin_name', 'wjones');
   - このプロシージャーを使ってアプリケーション・ユーザー名を設定するには、「条件 2: ロケーション」ボックスに 2 を入力して、「条件 2: 値」ボックスに admin_name を入力します。
     注: 2 つの条件を使用する場合、ユーザー名、または抽出される他の情報は、両方のタイプの呼び出しにおいて同じパラメーター位置でなければなりません。

8. 「クリア」アクションの場合:
    - 「イベント・タイプの位置」および「アプリケーション・ユーザー名の位置」フィールドだけを使用します。
    - 以下のいずれかを実行します。
        - アプリケーション・イベントを消去するには、「イベント・タイプの位置」を 1 に設定し、「アプリケーション・ユーザー名の位置」を 0 に設定します。
        - アプリケーション・ユーザーを消去するには、「イベント・タイプの位置」を 0 に設定し、「アプリケーション・ユーザー名の位置」を 1 に設定します。
9. 「設定」アクションの場合、「パラメーター位置」ペインを使用して、ストアード・プロシージャー・パラメーターと Guardium アプリケーション・イベント属性の間のマッピング関係を指定します。 最初のプロシージャー・パラメーターの番号は 1 になります。呼び出しによって設定されないすべての属性に対しては 0 (ゼロ、デフォルト) を使用します。アプリケーション・ユーザー名の位置 - この時点以降 (既に説明したようにリセットの時点まで)、データベース・アクティビティーに関連付けるアプリケーション・ユーザー名のパラメーター位置を入力します。イベント文字列値の位置 - イベントの文字列値のパラメーター位置を入力します (ログインの場合、例えばユーザーまたはアカウントの名前)。イベント数値の位置 - イベントの数値のパラメーター位置を入力します (トランザクションの場合、例えばドル金額)。イベント・タイプの位置 - イベント・タイプの名前のパラメーター位置を入力します (ログイン、ログアウト、クレジット要求など)。イベント日付の位置 - イベントの日付/時刻値のパラメーター位置を入力します。形式は yyyy-mm-dd hh:mm:ss でなければなりません。時間の部分 (hh:mm:ss) はオプションであり、省略した場合は 00:00:00 に設定されます。
10. 「サーバー情報」ペインで、「サーバー・タイプ」リストから、データベース・サーバーの種類を選択します。「データベース・ユーザー名」ボックスで、データベース・ユーザー名を入力します。オプション:「データベース名」ボックスにデータベース名を入力します。省略した場合、すべてのデータベースがモニターされます。オプション: 1 つまたは複数のサーバーを指定します。サーバーを指定しない場合、すべてのサーバーがモニターされます。特定の 1 つのサーバーだけを選択するには、「サーバー IP」および「サーバー・ネットマスク」ボックスにサーバー IP アドレスとネットワーク・マスクを入力します。あるいは、複数サーバーから成るグループを選択するには、「サーバー IP グループ」リストからサーバー・グループを選択するか、「グループ」ボタンをクリックして新しいサーバー・グループを定義します。
11. 完了したら、「追加」ボタンをクリックしてマッピングをリストに追加します。

親トピック: ユーザー識別

値変更監査

値変更監査フィーチャーは、データベース表内の値の変更をトラッキングします。

値変更監査フィーチャーは、データベース表内の値の変更をトラッキングします。変更のトラッキング対象にする各表において、モニター対象にする SQL 値変更コマンド (INSERT、UPDATE、DELETE) を選択します。 モニター対象の表に対して値変更コマンドが実行されるたびに、before 値および after 値が収集されます。スケジュール・ベースで変更アクティビティーが Guardium® システムにアップロードされます。このシステムでは、すべてのレポート作成機能とアラート機能を使用できます。値変更監査フィーチャーを使用するには、以下の基本的なステップを実行します。

1. データベース・サーバー上に監査データベースを作成します。このデータベースは、値変更データを、Guardium システムにアップロードされるまで保管しておく場所です。監査データベースの作成を参照してください。
2. モニター対象にする表を指定し、それぞれの表に対して、変更を記録する値変更コマンド (INSERT、DELETE、UPDATE) を選択します。変更を記録するため、モニター対象の各表にはトリガーが作成され、そのトリガーが監査データベースに値変更データを書き込みます。監査データベースを (トリガー経由で) 更新できるようにするため、モニター対象の表に対して更新特権を持つすべてのユーザーに、監査データベースへの適切な特権が与えられます。これは、後にその表への更新特権を与えられるユーザーに影響を与えます (ステップ 4 を参照)。モニター・アクティビティーの定義方法に関する詳細な説明については、『モニター・アクティビティーの定義』を参照してください。
3. データベース・サーバーから Guardium システムへの、値変更データ転送のためのアップロードのスケジュールを設定します。『値変更アップロードのスケジュール設定』を参照してください。
4. 監査データベースへのアクセス権を保守します。 トリガーの作成後に新規のユーザーにそのトリガーのベースになっている表に対するアクセス権を与えられる場合があります。 そのユーザーがモニター対象の値変更コマンドを発行した場合、そのコマンドは失敗します。ユーザーが監査データベースを更新するための適切な特権を持っていないためです。 『特権ユーザー・リストの保守』を参照してください。
5. 管理コンソールから変更アクティビティーをモニターするか、または「値変更のトラッキング」照会ドメインを使用して、Guardium アプライアンス上にカスタム・レポートを作成します。 『値変更レポートの作成』を参照してください。

モニター・アクティビティーの定義

監査データベースを定義した後、「値変更監査ビルダー」を使用して、モニター対象にする表を特定し、記録する変更のタイプ (INSERT、UPDATE、DELETE) を選択します。

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「値変更監査ビルダー」にナビゲートして「値変更監査ビルダー」を開きます。
2. 「データ・ソースの追加」をクリックして「データ・ソース・ファインダー」パネルを開きます。
3. 監査データベースを定義したデータ・ソースを選択します。監査データベースをまだ定義していない場合は、監査データベースの作成を参照してください。
4. 「追加」をクリックして、ファインダーを閉じ、選択したデータ・ソースを「値変更監査」パネルに追加します。
5. オプションで、「スキーマ所有者」と「オブジェクト名」のどちらかまたは両方を入力すると、モニター対象にする表を選択するときに表示される表の数を制限できます。「%」(パーセント) をワイルドカード文字として使用できます。 例えば、文字「a」で始まるすべての表を表示するように制限するには、「オブジェクト名」ボックスに「a%」と入力します。
6. 「モニターする表の選択」をクリックして、「データ監査の定義」パネルを開きます。
7. モニター対象にするそれぞれの表の「選択」ボックスにチェック・マークを付けます。
   注: ユーザー定義のデータ型を 1 つ以上含む表にはトリガーを定義できません。

   「定義されたトリガー」列は、この表で既にトリガーが定義されているかどうかを示します。「挿入の監査」、「削除の監査」、および「更新の監査」のチェック・ボックスは、トリガーでそのコマンドによる変更を記録するかどうかを指定します。

   「定義されたトリガー」列にマークが付いていない場合、表の「選択」チェック・ボックスにチェック・マークを付けると、自動的に 3 つすべての監査チェック・ボックス (「挿入の監査」、「削除の監査」、および「更新の監査」) にマークが付きます。 このうちの 1 つか 2 つのコマンドのモニターを行わない場合は、該当するチェック・ボックスをクリアします。

8. 「選択の追加」をクリックして、選択した表で使用するトリガーを定義します。実行されるアクションが通知されます。
9. 「OK」をクリックしてメッセージ・ボックスを閉じ、「データ監査の定義」パネルを再表示します。選択した表は選択されたままの状態になっており、これらの表の「トリガー定義済み」列にマークが付きます。注: 表にトリガーを定義するとすぐに、トリガーはアクティブになり、選択したコマンドによる変更が監査データ

ベースに記録されるようになります。 トリガーの構成はすべて、データベース・サーバー上で実行される点が、他のほとんどの Guardium 構成と異なっています。つまり、ほとんどの構成は Guardium データベース上で定義され、その後別のタスクとしてアクティブ化/非アクティブ化されます。

10. 追加のアクションを定義するには、これらのステップを繰り返します。また、トリガーを削除するには、該当する「選択」チェック・ボックスにチェック・マークを付けて、「選択の削除」をクリックします。
11. すべての変更を完了したら、「完了」をクリックします。
    注: 「キャンセル」ボタンを使用しても、「選択の追加」ボタンまたは「選択の削除」ボタンを使用してトリガーに加えた変更は元に戻りません。

モニター・アクティビティー定義後の作業

データ・ソースに初めて値変更モニター・アクティビティーを追加した場合、このデータ・ソースのアップロードのスケジュールを設定する必要があります。これは、監査データベースは、記録されたデータを Guardium システムにアップロードした後に初めて空にされるからです。次のセクションを参照してください。

値変更アップロードのスケジュール設定

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「値変更監査ビルダー」にナビゲートして「値変更監査ビルダー」を開きます。
2. アップロードのスケジュールを設定する監査データ・ソースを選択して、「アップロードのスケジュール」pをクリックすると、汎用のタスク・スケジューラーが開きます。スケジュール設定の定義について詳しくは、共通ツール・ブックの『スケジュール』を参照してください。

特権ユーザー・リストの保守

値変更フィーチャーによってデータベース表にトリガーが追加されるときには、その時点でその表に更新権限を持つすべてのユーザーに対して、監査データベース表への更新権限が付与されます。 これが必要なのは、トリガーが監査データベースを更新して新しい値と古い値を書き込むためです。 新規のユーザーにモニター対象の表に対する更新権限を付与しても、そのユーザーが更新を試行したときに更新は許可されません。これは、そのユーザーが監査データベースを更新する権限を持っていないからです。この状況になった場合は、「値変更監査ビルダー」を使用して、監査データベースの特権ユーザー・リストを更新する必要があります。

監査データベースの特権ユーザー・リストを更新するとき、モニター対象データベースへのログインに使用するデータベース・ユーザー ID は、新規ユーザーの追加対象であるロールの作成者でなければなりません。ユーザー ID が異なっていると、そのロールのメンバーは使用できません。

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「値変更監査ビルダー」にナビゲートして「値変更監査ビルダー」を開きます。
2. 「データ・ソースの追加」をクリックして「データ・ソース・ファインダー」パネルを開き、リストから該当するデータ・ソースを選択して「追加」をクリックします。
3. 「監査表特権ユーザーの更新」をクリックします。 監査データベース表を更新するためにトリガーを実行できるすべてのユーザーのアクセス権が更新され、その操作が完了すると通知されます。
4. 「OK」をクリックしてメッセージ・ボックスを閉じます。

値変更レポートの作成

デフォルトの「変更された値」レポートから値変更データを表示できます。あるいは、「値変更のトラッキング」ドメインを使用してカスタム・レポートを作成することもできます。 デフォルトでは、「値変更のトラッキング」ドメインは、admin ロールを持つユーザーに制限されています。

「変更された値」デフォルト・レポート

「レポート」 > 「リアルタイム Guardium 運用レポート」 > 「変更された値」にナビゲートすることで、デフォルトの「変更された値」レポートを使用できます。

「変更された値」レポートの主要なエンティティーは「変更された列」エンティティーです。 ほとんどの場合、それぞれの監査アクション (INSERT、UPDATE、DELETE) に関して検出されたそれぞれの列変更ごとに、別のレポート行が表示されます。 ただし、MS SQL Server と Sybase では、モニター対象の表に主キーがない場合、1 つの変更に対して 2 つの行が表示されます。つまり、古い値と新しい値が別の行に表示されます。

親トピック: モニターおよび監査

監査データベースの作成

監査データベースを作成して値変更モニター・アクティビティーを実行します。

監査データベースを作成して値変更モニター・アクティビティーを実行するには、以下の操作を行うための適切な権限を持つユーザー・アカウントが必要です。

- サーバー上へのデータベースの作成
- サーバー上へのデータベース・ユーザー・アカウントの作成

モニター対象の各データベースへログインして、モニター対象の各データベースで表とトリガーを作成します。

Informix または Sybase で監査データベースを定義する前に行う作業

Informix® および Sybase (トリガーをサポートしていないため Sybase IQ は除外) では、データベース・サーバーが稼働するオペレーティング・システムに応じて、監査データベースを定義する前に以下の手順のいずれかを行う必要があります。

Informix の設定 - 新規データベース・スペースの配置または作成

このトピックは Informix (9.4 またはそれ以降) に適用されます。 Informix では、デフォルトのルート・データベース・スペースである root_dbs の使用を避けるよう強くお勧めします。 このスペースは、ドロップすることも、サイズを削減することもできません。

定義済みの他のデータベース・スペースを使用するか、以下のいずれかの手順 (オペレーティング・システムによって異なります) を実行してデータベース・スペースを新規作成する必要があります。

Informix - Windows Server 上での Informix データベース・スペースの作成

この手順は Guardium® GUI 外部で実行します。また、Informix バージョン 9.4 以降に適用されます。

1. データベース・サーバーがオンラインで listen 中であることを確認します。
2. guardium_dbs_dat.000 という名前のゼロ・バイトのファイルを C:¥IFMXDATA¥server-name ディレクトリーに作成します (sever-name は Informix サーバー名またはサービス名です)。 これは、空のテキスト・ファイルを保存してからそのファイルを名前変更し、接尾部の txt を 000 に置き換えることによって行えます。
3. 以下のディレクトリーを作業ディレクトリーにします。

   C:¥Program Files¥Informix¥bin

4. 以下のコマンドを実行します。

   ```
   C:¥Program Files¥Informix¥bin>onspaces
   -c -d guardium_dbs -p C:¥IFMXDATA¥server-name¥guardium_dbs_dat.000
   -o 0 -s 150000
   ```

   ファイルの作成が成功すると、以下のメッセージが表示されます。

   ```
   Verifying physical disk space, please wait ...
   Space successfully added.
   ** WARNING **  A level 0 archive of Root DBSpace will need to be done.
   ```

5. Informix サーバーを再始動し、適切なツール (例えば、Aqua Data Studio リモート・クライアント) を使用して、作成した guardium_dbs という名前のスペースへの接続と検査を行います。 最初の接続試行では、サーバーが静止モードで実行されていることに関するメッセージが表示されて失敗する場合があります。 これが発生した場合は、少なくともさらに 2 回再接続を試行します。これにより、動作するようになるはずです。
6. guardium_dbs データベース・スペースが作成されたことを検査するには、Aqua Data Studio を使用して、Storage の下を確認します。

Informix - Unix Server 上での Informix データベース・スペースの作成

この手順は Guardium GUI 外部で実行します。また、Informix バージョン 9.4 以降に適用されます。

1. コマンド行ウィンドウで以下のコマンドを実行します。

   ```
   su - informix
   cd demo/server
   vi guardium_dbs
   ```

2. テキストを追加せずに、空の guardium_dbs ファイルを保存します。
3. 以下のコマンドを入力します。

   ```
   chmod 660 guardium_dbs
   cd ../../bin
   onspaces -c -d guardium_dbs -p /home/informix10/demo/server/guardium_dbs -o 0 -s 100000
   ```

Sybase の設定 - ディスクの初期化

このトピックは Sybase サーバーのみに適用されます (Sybase IQ は該当しません。トリガーをサポートしていないからです)。 データベース・サーバーが稼働するオペレーティング・システムによって異なりますが、ディスクを初期化するために以下の手順のいずれかを行う必要があります。

Sybase - Windows Sybase Server でのディスクの初期化

1. Guardium 監査データベース guardium_audit を作成するサーバーに接続します。
2. C: ドライブに guardium_audit という名前のフォルダーを作成します。
3. データベースに接続します。
4. 以下のコマンドを実行します。

   ```
   use master
   go
   disk init name="guardium_auditdev", size=8192
   go
   disk init name="guardium_auditlog",
   physname="c:/guardium_audit/guardium_auditlog", size=8192
   go
   ```

Sybase - Unix Sybase Server でのディスクの初期化

1. データベースに接続します。
2. 以下のステートメントを実行します。

   ```
   use master
   go
   disk init name = 'guardium_auditdev', physname
    ='/home/sybase/data/guardium_auditdev' , size = 8192
   go
   disk init name = 'guardium_auditlog', physname
    ='/home/sybase/data/guardium_auditlog' , size = 8192
   go
   ```

データベースの作成

Informix または Sybase データベースの場合は、この手順を実行する前に、必ず準備タスクを実行しておいてください。

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「値変更監査データベースの作成」にナビゲートして「値変更データベース・ビルダー」を開きます。
2. 「データ・ソースの追加」をクリックして、「データ・ソース・ファインダー」パネルを開きます。「値変更監査」アプリケーションから定義したデータ・ソースには、「値のモニター」というラベルが付けられています。 他のアプリケーション用に定義されたデータ・ソースには異なるラベル (例えば、Listener、

DBanalyzer など) が付けられています。そのようなデータ・ソースには、「値変更監査」アプリケーションのための適切なデータベース・アクセス権のセットがない可能性があります。「値変更監査」アプリケーションではデータベース管理者権限を持つユーザー・アカウントが必要です。 適切なデータ・ソースが使用できない場合、「新規」ボタンをクリックして、モニター対象のデータベースに新しいデータ・ソースを定義します (データ・ソースの定義に関する詳細については、共通ツール・ブックの『データ・ソース』を参照してください。
注: このデータベース・サーバーに GUARDIUM_AUDIT データベースを既に作成済みの場合、もう 1 つ作成することはできません。新規作成する前に、GUARDIUM_AUDIT データベース/ユーザーをドロップする必要があります。

3. 管理者アカウントを使用するデータ・ソースを選択して「追加」をクリックすると、それが「値変更監査データベースの作成」パネルの「データ・ソース」ペインに追加されます。
4. 「監査データ・ソース名」に入力します。 これは、後でモニター・タスクの定義とデータのアップロードを行う際にこのデータ・ソースを識別するために使用される名前になります。 この名前と「データ・ソース」パネルにあるデータ・ソースの名前を混同しないようにしてください。
5. オプションで、「データ・ソースの共有」ボックスにマークを付けて、このデータ・ソースを他のアプリケーション (例えば、分類) と共有します。 デフォルトではデータ・ソースの共有はしません。 このタイプのデータ・ソースでは管理者特権が必要です。それで、このデータ・ソースを他のアプリケーションとは共有しないことにするかもしれません。
注: データ・ソースを他のユーザーと共有するには、そのデータ・ソースにセキュリティー・ロールを割り当てます。
6. DB2® 以外のすべてのタイプのデータベースでは、「監査構成」ペインに追加のフィールドがあります。 すべてのフィールドが必須です。以下の表を参照して、適切な値を入力してください。

表 1. 「監査構成」の追加フィールドの表

データベース・タイプ	フィールド: 説明
Informix	**データベース・スペース**: 使用する既存のデータベース・スペースの名前を入力するか、または監査データベース用に作成したデータベース・スペースの名前 (前述の例では guardium_dbs) を入力します。 これをブランクのままにした場合、デフォルトの root_dbs space が使用されます。これは推奨しません。
MS SQL Server	**監査ユーザー名**: 監査データベースにアクセスするときに使用する新しいデータベース・ユーザー名を入力します。 このユーザーには sysadmin ロールが付与されます。 **監査パスワード**: パスワードを入力します。 データ・ソースが MSSQL サーバーの場合は、「値変更監査データベースの作成」メニュー画面に追加の選択項目が表示されます。この追加の選択項目は、データ・ソースが MSSQL サーバーの場合にしか表示されません。 互換モード: 選択項目は「デフォルト」と「MSSQL 2000」です。表のモニター時に使用する互換モードをプロセッサーに指示します。 MS SQL Server の互換モードを表示するには、GuardAPI コマンド grdapi list_compatibility_modes を使用してください。
Oracle	**監査パスワード**: システム・ユーザーのパスワードを入力します。これは監査データベースへのアクセスに使用するデータベース・アカウントになります。 **デフォルト表スペース**: デフォルトの表スペースの名前を入力します。 **一時表スペース**: 一時表スペースの名前を入力します。
Sybase	**監査ユーザー名**: 監査データベースにアクセスするときに使用する新しいデータベース・ユーザー名を入力します。 このユーザーには sa_role が付与されます。 **監査パスワード**: パスワードを入力します。 **データ・デバイス名**: 監査データベースで使用するディスクを初期化する際に使用したのと同じデータ・デバイス名を入力します (前述したディスク初期化手順の場合、guardium_auditdev)。 **ログ・デバイス名**: 監査データベースで使用するディスクを初期化する際に使用したのと同じログ・デバイス名を入力します (前述したディスク初期化手順の場合、guardium_auditlog)。

7. 「監査データベースの作成」をクリックして、監査データベースを作成します。
8. 「構成と制御」タブにある「値変更監査データベースの更新とアップロード」を使用して、この表にあるアクションを選択します。

アクション	記述
削除	「データ・ソース」ペインからデータ・ソースを削除するときにクリックします。
変更	「データ・ソース定義」パネルでこのデータ・ソース定義を編集するときにクリックします。
アップロードのスケジュール	この監査データ・ソースのアップロードのスケジュールを設定するときにクリックします。

監査データベース定義後の作業

監査データベースをデータベース・サーバー上に作成すると、「値変更監査ビルダー」からそれを使用できるようになります。このビルダーは、トリガーのビルドに使用するツールです。値変更監査を参照してください。

親トピック: モニターおよび監査

モニター対象表アクセス

この機能は、Optim™ Designer データ・ライフサイクル製品との相互作用を可能にするために、「最後の評価」フィールドを関連する表に追加します。

この機能は、「表の最後の参照」とも呼びます。

この機能は、データ (事前定義外部フィード・マップ) とともに事前定義された Guardium の外部フィード、およびそれを実行する監査プロセスを使用します。

以下の手順を行います。

1. ターゲット (Optim) 表を Informix® データベースに作成します。スクリプトを使用してください。
2. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートして「監査プロセス・ビルダー」を開き、「表の最後の参照」という名前のプロセスを編集します。外部フィード・タスクにデータ・ソース (表を含む Informix データ・ソース) を追加して、サーバー・グループのランタイム・パラメーターをセットアップします。それ以外はすべて事前定義されているため、変更する必要はありません。
3. 監査プロセスを実行 (または定期的に実行するようにスケジュール) します。

注: 結果の表には、最後の実行のみ表示されます。受信者カウントは受信者の数であり、最後の実行以後の実行結果のみの数ではありません。

IBM Guardium は、データベース・オブジェクト (特に表) への外部参照を検出できます。この機能を Optim Designer とともに使用することで、非アクティブ表の廃止や、特定の保存ポリシーによるアーカイブを管理できます。

Guardium® は、最後の参照日を含む表のリストを収集して保持します。リストは Guardium でポリシーを使用して作成されます。 このポリシーには、リスト内容の更新に使用する、最後の参照の間隔と頻度が示されています。Guardium によってキャプチャーされる情報は「最後の参照」リストと呼ばれ、参照されなくなった表、および廃止の対象となる表のアクセス傾向などの情報を提供します。

アプリケーションの廃止を正確に計画できると、以下の作業に便利です。

- ハードウェアの廃止または再デプロイメントの計画
- アプリケーションをサポートするリソース (例えば、ハードウェア、DBA、アプリケーションの所有者、バックアップなどの IT 運用) の移動または廃止による、所有コストの削減。
- ほとんど、あるいはまったくアクセスされない表の認識

IBM Guardium のこの機能は、Optim Designer ユーザー・インターフェースに直接追加されました。

Guardium によって Optim に提供される情報は、表項目ごとの以下の属性で構成されています。

表 1. モニター対象表アクセスのリスト項目

リスト項目	記述
フィールド	コメント
DataSourceDesc	記述
サーバー IP	
ホスト名	
DB ベンダー	Oracle や DB2® など。
ユーザー名	例えば、Oracle の場合は、主にスキーマを定義します。
データベース名	
スキーマ	
表	
日付	最後のアクセス日

Optim 製品での Informix 表の作成スクリプト

Last_referenced_datasource

```
create table last_referenced_datasource (
    id              serial(1) not null,
    datasource_desc     varchar(100),
    server_ip         char(39),
    host_name          varchar(200),
    db_vendor         char(40),
    primary key (id) constraint last_referenced_datasource_pk
);
```

Last_referenced_table

```
create table last_referenced_table (
    id              serial(1) not null,
    datasource_id      int not null,
    user_name         char(32),
    db_name           char(128) not null,
    schema_name        char(128) not null,
    table_name        char(128) not null,
    last_reference     datetime year to second not null,
```

primary key (id) constraint last_referenced_table_pk,

foreign key (datasource_id) references last_referenced_datasource(id) constraint last_referenced_table_fk

);

親トピック: モニターおよび監査

コンプライアンス・モニターのクイック・スタート

モニター・エージェント (S-TAP) をデプロイした後、コンプライアンス・モニター・ツールを使用して、特定のセキュリティー基準および規制のモニターを設定します。

Guardium は、以下のような特定の基準および規制に対応するグループ、セキュリティー・ポリシー、およびレポートなどの、コンプライアンス・モニター・テンプレートをいくつか備えています。

- バーゼル銀行監督委員会 (BASEL II)
- 一般データ保護規則 (GDPR)
- Db2 for z/OS 用の一般データ保護規則 (Db2 for z/OS の GDPR)
- 医療保険の相互運用性と説明責任に関する法律 (HIPAA)
- クレジット・カード業界データ・セキュリティー基準 (PCI)
- 個人情報 (PII)
- サーベンス・オクスリー (SOX) 法への準拠

これらのクイック・スタート・コンプライアンス・モニター・テンプレートは、関連する基準または規制のいずれかに短期間で準拠する必要がある組織に特に役立ちます。セキュリティー・ポリシーをインストールした後、コンプライアンス・モニター・ツールは、初期セットアップやグループへの組織固有の情報 (クライアント IP アドレスや特定の特権ユーザー ID など) の取り込みについて、管理者およびコンプライアンス担当者にガイドを提供します。 さらに、コンプライアンス・モニター・ツールは、Guardium 環境を定期的に検査して、コンプライアンス・モニター・テンプレートを使用してモニターできる新規のデータベースを調べます。
コンプライアンス・モニター・テンプレートを選択し、そのコンプライアンス・タイプを適用する必要があるデータベースを示すと、コンプライアンス・モニター・ツールは以下のアクションを実行します。

- 選択されたコンプライアンス・タイプのセキュリティー・ポリシーが作成されて、インストールされます。一元管理された環境では、ポリシーはコレクターにインストールされます。
- ポリシー・インストール・スケジュールは毎日午前 10:30 に定義されます。一元管理された環境では、ポリシー・インストール・スケジュールはコレクターで実行されます。
- 選択したデータベースのサーバー IP アドレスがサーバー IP グループに取り込まれます。
- 現行ユーザーは、選択されたコンプライアンス・タイプのロールに割り当てられます。このロールにより、Guardium のメイン・ナビゲーションから関連するレポートおよびアクセラレーターへのアクセスが可能になります。
- サポートされている場合、機密データのディスカバー・シナリオが作成されます。
- 機密データのディスカバー・シナリオが作成され、選択されたデータベースの少なくとも 1 つにデータ・ソースが定義されている場合、シナリオは 1 週間に 1 回、日曜日の午前 10:30 に実行するようにスケジュールされます。一元管理された環境では、スケジュールは中央マネージャーで実行されます。

次の表に、使用可能な各コンプライアンス・タイプでサポートされる機能を要約します。

表 1. コンプライアンス・モニター・ツールによってサポートされる、コンプライアンス・タイプ別の機能の要約

	バーゼル II	GDPR	HIPAA	PCI	PII	SOX
セキュリティー・ポリシー	✓	✓	✓	✓	✓	✓
レポート	✓	✓		✓	✓	✓
機密データのディスカバー・シナリオ		✓		✓	✓	

- コンプライアンス・モニターの前提条件
  コンプライアンス・モニターを構成する前に、前提条件および制約事項を確認します。
- コンプライアンス・モニターのセットアップ
  コンプライアンス・モニターの初期構成を実行する方法について説明します。
- グループへのデータの設定
  コンプライアンス・モニターのためにグループにデータを設定する方法について説明します。
- 機密データのスキャンの有効化
  データベース資格情報を保管し、機密データのディスカバリーおよび分類を許可する方法について説明します。
- コンプライアンス・モニター・ビューの概要
  コンプライアンス・モニター・ビューの解釈および応答方法について説明します。

親トピック: モニターおよび監査
関連概念:
ポリシー
データ・ソース
関連タスク:
機密データのディスカバー
関連情報:
グループ
Guardium GDPR アクセラレーター (ビデオ)

コンプライアンス・モニターの前提条件

コンプライアンス・モニターを構成する前に、前提条件および制約事項を確認します。

コンプライアンス・モニター・ツールのクイック・スタートでは、テンプレートを使用することにより、コンプライアンス・モニターを環境内の新規のデータベース・サーバーに対して素早く設定します。これらのテンプレートは、新規の Guardium デプロイメントまたは拡張している Guardium デプロイメントでの使用に合わせて最適化されます。 始める前に、以下の前提条件を検証することにより、最も簡単な構成と最も完全な機能を確保します。

- 中央マネージャーまたはスタンドアロン・システムとして構成された Guardium V10.1.3 以降を実行している、管理特権を持つ Guardium ユーザーである。
- S-TAP が新規のデータベース・サーバーにインストールされ、作動可能になっている。
- データベース・サーバーは、コンプライアンス・モニター・テンプレートによってサポートされている。
- *「デフォルト - 不明な接続に対するデータ・アクティビティーを無視」*ポリシー以外のポリシーがインストールされていない。
  警告:

  既存のポリシーに次の「ポリシー定義」設定がある場合にのみ、既存のポリシーとともにクイック・スタート・コンプライアンス・モニター・セキュリティー・ポリシーをインストールできます。

  - 未解析ログ: 無効
  - 未解析ログに関するルール: 無効
  - 選択的な監査証跡: 有効

  既存のポリシーの設定が競合している場合、クイック・スタート・セキュリティー・ポリシーのインストールは失敗します。既存のデプロイメントで作業している場合は、クイック・スタート・ポリシーを使用する前に、既存のポリシーをアンインストールすることを検討してください。この制約事項は、新規の Guardium デプロイメントに影響を及ぼすことはありません。

以下のセクションでは、クイック・スタート・コンプライアンス・モニターの前提条件について詳しく説明します。

モニター・エージェントのデプロイ

コンプライアンス・モニターの構成を開始する前に、Guardium モニター・エージェント (S-TAP) がデータベース・サーバーにインストールされ、Guardium システムと通信するように構成されている必要があります。Guardium モニター・エージェントの迅速なインストールおよび構成については、『モニター・エージェントのデプロイ』を参照してください。

他のインストール方法を含む S-TAP の詳細については、「S-TAP 管理ガイド」を参照してください。

サポートされるデータベース

コンプライアンス・モニター・ツールは、以下の基準に基づいて、Guardium 環境でデータベースを検出します。

- Guardium システム上のアクティブ・トラフィック。
- ディスカバーされたインスタンス・レポート (「ディスカバー」 > 「レポート」 > 「ディスカバーされたインスタンス」)。

次の表に要約されているように、検出方式はサポートされるデータベース・タイプによって異なります。

表 1. サポートされるデータベース・タイプおよび検出方式の要約。

データベース	アクティブ・トラフィック	ディスカバーされたインスタンス
Db2 for Linux, UNIX, and Windows	✓	
Db2 for z/OS	✓ 重要: *「デフォルト - 不明な接続に対するデータ・アクティビティーを無視」*ポリシーでは、Db2 for z/OS データベースのトラフィックがキャプチャーされません。Db2 for z/OS データベースでコンプライアンス・モニター・ツールを使用する前に、このトピックで説明されているポリシー定義およびアクティブ・トラフィック基準を満たすポリシーをまずインストールする必要があります。	
Informix	✓	✓
Microsoft SQL Server	✓	✓
MySQL	✓	✓
Netezza	✓	
Oracle	✓	✓
PostgreSQL	✓	
Sybase	✓	✓
Teradata	✓	✓

アクティブ・トラフィックは、以下の基準を満たします。

- トラフィックでは、以下のいずれかのプロトコルが使用されます。
  - Db2 for z/OS データベース: BATCH、CALL、CICS、CTL、DRDA、PRIV、RRSAF、TRAN、TSO、または UTIL。
  - その他のすべてのデータベース: TCP。
- トラフィックはローカルではない (サーバー IP はクライアント IP と等しくない)。
- 失敗したログインは無視される。

- トラフィックは暗号化されていない。

新しいデータベースについて、アクティブ・トラフィックが毎正時 17 分後に検査されます。例えば、13:00 に設定されたデータベースからのアクティブ・トラフィックは、13:17 に検出されます。
ディスカバーされたインスタンスは、以下の基準を満たします。

- データベースでポート範囲が指定されていない。
- データベースがデータ・ソースの作成にデータベース名を必要としない。

抽出ルールおよび戻りデータの検査

クイック・スタート・コンプライアンス・モニター・ポリシーによっては、抽出ルールを使用するものがあります。抽出ルールは、要求に応答してサーバーから返されたデータを評価します。例えば、抽出ルールは、社会保障番号やクレジット・カード番号などの機密データに関連付けられた数字パターンを検査する場合があります。

抽出ルールでは、ポリシーを使用するすべての検査エンジンについて「戻りデータの検査」設定が有効になっている必要があります。次のコンプライアンス・テンプレートに含まれる抽出ルールを使用するには、返されたデータを検査エンジンが検査できるようにする必要があります。

- GDPR
- HIPAA
- PCI
- PII (データ・プライバシー)

重要: 「戻りデータの検査」を有効にすると、返された結果セットによってネットワーク・トラフィックが増大します。
「戻りデータの検査」は、「管理」 > 「アクティビティー・モニター」 > 「検査エンジン」から有効にします。「戻りデータの検査」の設定について詳しくは、ポリシーの作成および『検査エンジン構成』を参照してください。

ポリシー定義の設定

すべてのコンプライアンス・モニター・セキュリティー・ポリシーは、以下のポリシー定義設定を使用します。

- 未解析ログ: 無効
- 未解析ログに関するルール: 無効
- 選択的な監査証跡: 有効

競合する「未解決ログ」、「未解析ログに関するルール」、または「選択的な監査証跡」の設定が含まれるポリシーは、同じ Guardium 環境にインストールできません。その結果、異なる設定を使用するポリシーがインストールされている場合、クイック・スタート・コンプライアンス・モニター・テンプレートを使用できません。

新規の Guardium デプロイメントまたはユーザー定義のポリシーがないデプロイメントの場合、これらのポリシー設定との競合が発生する可能性は低くなります。既存の Guardium デプロイメントの場合、「コンプライアンス・モニターのセットアップ」ツールの使用中に「*ポリシーが競合しています (conflicting policies)*」というメッセージを受け取った場合、ポリシー定義設定を確認してください。

選択的な監査証跡について詳しくは、ルール・アクションを参照してください。
例外: インストールされているポリシーが 1 つのみの場合、*「デフォルト - 不明な接続に対するデータ・アクティビティーを無視」*ポリシーは、コンプライアンス・モニター・ポリシーのインストールによってオーバーライドされます。
親トピック: コンプライアンス・モニターのクイック・スタート

コンプライアンス・モニターのセットアップ

コンプライアンス・モニターの初期構成を実行する方法について説明します。

始める前に

前提条件および制約事項について詳しくは、コンプライアンス・モニターの前提条件を参照してください。

このタスクについて

コンプライアンス・モニターのセットアップ・ツールを使用して、データベースを 1 つ以上のコンプライアンス・テンプレートに関連付けます。この手順では、セキュリティー・ポリシー、グループ、レポート、および機密データのディスカバー・シナリオ (サポートされている場合) を迅速にインストールします。

手順

1. 「設定」 > 「クイック・スタート」 > 「コンプライアンス・モニター」にナビゲートして、コンプライアンス・モニター・ページを開きます。
2. 「コンプライアンス・モニターのセットアップ」タイルの  アイコンをクリックして、コンプライアンス・モニターのセットアップ・ツールを開きます。
3. 「コンプライアンス・タイプ」セクションで、「有効にするコンプライアンス・タイプを選択してください」メニューを使用して、構成するデータベース・モニターのタイプを選択します。 例えば、GDPR モニターを有効にするには、「一般データ保護規則 (GDPR)」を選択します。「次へ」をクリックして先に進みます。
4. 「データベース」セクションで、「使用可能なデータベース」表からデータベースを選択し、  アイコンをクリックして、そのデータベースを「選択されたデータベース」表に追加します。
   ヒント:
   - 「モニター対象データベースの除外」チェック・ボックスを使用すると、コンプライアンス・モニターが既に構成されているデータベースを非表示にできます。
   - 「Db2 for z/OS 用の一般データ保護規則 (Db2 for z/OS の GDPR)」コンプライアンス・タイプを使用する場合、Db2 for z/OS データベースのみが含まれるように使用可能なデータベースのリストがフィルタリングされます。同様に、z/OS 以外のコンプライアンス・タイプを使用する場合、Db2 for z/OS データベースは表示されません。

- 「選択されたデータベース」表からデータベースを選択し、「資格情報の指定」をクリックして、データベース資格情報を保管します。 資格情報を保管すると、一部のコンプライアンス・タイプの機密データのディスカバリーおよび分類が可能になります。自動構成がサポートされていない場合、資格情報の保管時に作成されるデータ・ソースを独自の機密データのディスカバー・シナリオで使用できます。
- データベースとコンプライアンス・タイプの関連付けを解除するには、構成を編集して、データベースを「選択されたデータベース」表から削除するか、またはコンプライアンス・タイプ・タイルから「詳細表示」 > 「データベース」にナビゲートして、データベースの横にある アイコンをクリックします。

5. モニターするデータベースの識別が完了したら、「セットアップの実行」をクリックしてポリシーをインストールし、サーバー IP グループにデータを設定して、コンプライアンス・モニター・レポートを実行します。
6. 「ページを最新表示して新しいコンテンツを表示しますか?」ダイアログで、「はい」をクリックしてページを最新表示し、セットアップを完了します。

タスクの結果

コンプライアンス・モニターをセットアップした後、構成したコンプライアンス・テンプレートに対応するコンプライアンス・モニター・ダッシュボードにタイルが表示されます。

次のタスク

コンプライアンス・モニターを構成した後、コンプライアンス・モニター・タイルにいくつかの アイコンが表示される場合があります。これらのアイコンは、追加の構成が必要であることを示しています。「グループにデータを設定する」リンクを使用して追加グループにデータを設定するか、または「データ・ソース資格情報」リンクを使用して機密データのディスカバー・シナリオ用にデータベース資格情報を指定します。

重要: コンプライアンス・モニター・セットアップ・ツールを使用してモニターを構成すると、デフォルトのサーバー IP グループが自動的に作成され、データが設定されます。ただし、いくつかの追加グループにデータを設定することによって、データベースへのアクセスを許可されるユーザーおよびアプリケーションを定義することが重要です。コンプライアンス・モニター・ページからのグループへのデータの設定については、グループへのデータの設定を参照してください。
親トピック: コンプライアンス・モニターのクイック・スタート
関連概念:
コンプライアンス・モニターの前提条件
関連情報:
モニター・エージェントのデプロイ

グループへのデータの設定

コンプライアンス・モニターのためにグループにデータを設定する方法について説明します。

始める前に

コンプライアンス・モニターのセットアップで説明されている手順に従って、コンプライアンス・モニター・テンプレートをインストールします。

このタスクについて

コンプライアンス・モニター・セットアップ・ツールを使用してモニターを構成すると、デフォルトのサーバー IP グループが自動的に作成され、データが設定されます。ただし、いくつかの追加グループにデータを設定することによって、データベースへのアクセスを許可されるユーザーおよびアプリケーションを定義することが重要です。 以下の手順では、グループに素早くデータを設定する方法について説明します。
重要:

- 空のグループはワイルドカードとして扱われず、トラフィックを収集しません。
- 階層グループおよびネストされたグループはサポートされません。

手順

1. 以下のいずれかの方法を使用して、データが設定されていないグループを識別し、「グループの編集」ダイアログを開いて開始します。
   - コンプライアンス・モニター・タイルの「モニター使用可能」セクションで、 アイコンを探して、関連付けられた「グループにデータを設定する」リンクをクリックします。
   - コンプライアンス・モニター・タイルの「詳細表示」リンクをクリックして、詳細パネルを開き、「要約」タブを選択して、グループの横にある アイコンをクリックします。
     ヒント: 詳細パネルで、データが設定されていないグループが小さい アイコンで強調表示されます。

   この時点で、詳細ビューおよび 「グループの編集」 ダイアログがコンプライアンス・モニター・ダッシュボードの上に表示されます。
2. 「グループの編集」ダイアログから、オプションでグループの「カテゴリー」および「分類」を指定します。 「アプリケーション・タイプ」フィールド、「グループ・タイプ」フィールド、および 「説明」(「グループ名」として使用される) フィールドは、前のステップで選択されたグループに基づいてデータが設定されており、編集できません。
3. 「グループの編集」ダイアログから、以下のいずれかの方法を使用して、選択したグループのデータの設定を開始します。
   - アイコンをクリックして、項目を「メンバー」表に追加し、手動でグループ・メンバーを指定します。
   - CSV ファイルからグループ・メンバーをインポートするには、「インポート」 > 「CSV から」をクリックします。
   - 同じグループ・タイプの別の Guardium グループからグループ・メンバーをインポートするには、「インポート」 > 「グループから」をクリックします。例えば、*「許可されたユーザー」*グループは、ユーザーのリストが含まれる別のグループからデータを設定することができますが、IP アドレスのリストが含まれるグループからデータを設定することはできません。
   - 外部データ・ソースからグループ・メンバーをインポートするには、「インポート」 > 「外部データ・ソースから」をクリックします。「データ・ソース」メニューには、*共有*というマークが付いているか、またはタイプが*カスタム・ドメイン*であるすべてのデータ・ソースが含まれます。詳しくは、『外部データ・ソースからのインポート』を参照してください。
4. グループへのメンバーの追加が完了したら、「OK」をクリックして、コンプライアンス・モニター・ダッシュボードに戻ります。

親トピック: コンプライアンス・モニターのクイック・スタート

機密データのスキャンの有効化

データベース資格情報を保管し、機密データのディスカバリーおよび分類を許可する方法について説明します。

始める前に

コンプライアンス・モニターのセットアップで説明されている手順に従って、コンプライアンス・モニター・テンプレートをインストールします。

このタスクについて

以下の手順では、コンプライアンス・モニター・ツールを使用してデータベース資格情報を保管することによってデータ・ソースを作成する方法について説明します。資格情報を保管して、データ・ソースを作成することにより、Guardium は機密データのディスカバリーおよび分類のためにデータベースにアクセスできます。

手順

1. 以下のいずれかの方法を使用して、データベース資格情報が必要な場所を特定します。
   - コンプライアンス・モニター・タイルの「機密データのスキャン中」セクションで、  アイコンを探して、関連付けられた「データ・ソース資格情報」リンクをクリックします。 コンプライアンス・モニター・データベース・ビューが、資格情報を必要とするデータベースのフィルター済みリストに対して開きます。
   - 「データベースの表示」リンクをクリックして、コンプライアンス・モニター・データベース・ビューを開き、「データ・ソース」列に  アイコンが表示されていないデータベースを探します。
2. コンプライアンス・モニター・データベース・ビューから、資格情報を必要とするデータベースを選択し、「データ・ソース・アクション」 > 「資格情報の指定」をクリックします。
   ヒント:
   - 複数のデータベースを選択して、「データ・ソース・アクション」 > 「資格情報の指定」をクリックすると、選択したすべてのデータベースの指定された資格情報が保存されます。複数のデータベースの資格情報を指定する際には、選択したデータベースがすべて同じ資格情報を使用していることを確認してください。 同じ資格情報を指定していない場合、異なる資格情報を使用するデータベースは接続テストに失敗します。
   - 資格情報を保管すると、一部のコンプライアンス・タイプの機密データのディスカバリーおよび分類が可能になります。自動構成がサポートされていない場合、資格情報の保管時に作成されるデータ・ソースを独自の機密データのディスカバー・シナリオで使用できます。
3. 「資格情報の指定」ダイアログで、「ユーザー名」フィールドと「パスワード」フィールドを使用して、選択したデータベースの資格情報を指定します。「OK」をクリックして、コンプライアンス・モニター・データベース・ビューに戻ります。
4. コンプライアンス・モニター・データベース・ビューから、資格情報を保管しているデータベースを選択し、「データ・ソース・アクション」 > 「接続のテスト」をクリックします。 「接続のテスト」を使用して、保管された資格情報がデータベースへのアクセスを許可していることを検証します。接続のテストが失敗した場合、機密データのディスカバリーおよび分類は機能しません。
   重要:
   - 接続のテストは時間がかかる可能性があります。一度に多数の接続をテストすることは推奨されません。
   - 接続のテストが失敗した場合は、「設定」 > 「ツールとビュー」 > 「データ・ソース定義」にナビゲートし、データ・ソースを選択して、データ・ソース定義を検証します。例えば、Db2 for z/OS データベースの正しいポートを指定するか、大/小文字混合の PostgreSQL データベース名を修正するか、あるいは使用環境に必要な他の接続プロパティーを設定することが必要な場合があります。
   - Microsoft SQL Server の接続のテストが失敗した場合は、「SQL サーバー・ブラウザー」の Windows サービスが開始されていることを確認します。

タスクの結果

機密データのスキャンを有効にした後には、スキャン結果、およびポリシーに対して行った変更 (グループおよびグループ・メンバーシップに対する変更を含む) は、ポリシーがポリシー・インストールのスケジュールに従ってインストールされた後に使用可能になります。デフォルトでは、クイック・スタート・コンプライアンス・モニター・ツールは、毎日午前 10:30 に実行されるポリシー・インストール・スケジュールを定義します。

親トピック: コンプライアンス・モニターのクイック・スタート

コンプライアンス・モニター・ビューの概要

コンプライアンス・モニター・ビューの解釈および応答方法について説明します。

ユーザー・インターフェース

「コンプライアンス・モニター」ツールは、以下のビューから構成されています。

ダッシュボード・ビュー

これはデフォルトのビューであり、コンプライアンス・タイプ別に編成された、コンプライアンス・デプロイメントの現在の状況の概要を示します。個々のタイルには、いくつかのコンプライアンス・モニター・コンポーネントの現在の構成状況が反映されます。これにより、追加構成を必要とするコンプライアンス・タイプを迅速に特定できます。

データベース・ビュー

データベース・ビューには、サポートされるコンプライアンス・モニター・テンプレートを使用して構成されているデータベースを示す表が表示されます。

コンプライアンス・モニターのセットアップ

コンプライアンス・モニターのセットアップ・ツールは、データベースとコンプライアンス・テンプレートを迅速に関連付けるため、および初期セットアップを実行するためのガイド付きインターフェースを提供します。ツールにアクセスするには、ダッシュボード・ビューの「コンプライアンス・モニターのセットアップ」タイルの  アイコンをクリックするか、データベース・ビューでデータベースを選択して、「コンプライアンス・モニターのセットアップ」ボタンをクリックします。

コンプライアンス・モニター・ビューには、コンプライアンス・モニターの設定に関連した構成タスクを完了するための相互に関連する方法がいくつか示されます。次の表に、さまざまなビューでサポートされるタスクの要約を示します。

表 1. コンプライアンス・モニター・ビューによってサポートされるタスクの要約

タスク	コンプライアンス・モニターのセットアップ	ダッシュボード・ビュー	データベース・ビュー
コンプライアンス・タイプとデータベースの関連付け	「データベース」セクションで、「使用可能なデータベース」表からデータベースを選択し、  アイコンをクリックして、そのデータベースを「選択されたデータベース」表に移動します。		
グループへのデータの設定		コンプライアンス・タイプ・タイルから、「グループにデータを設定する」リンクをクリックするか、「詳細表示」 > 「要約」にナビゲートして、グループの横の  アイコンをクリックします。	
機密データをディスカバーするためのデータ・ソースの定義	「データベース」セクションで、「選択されたデータベース」表からデータベースを選択し、「資格情報の指定」ボタンをクリックします。	コンプライアンス・タイプ・タイルから、「データ・ソース資格情報」リンクをクリックし、データベースを選択して、「データ・ソース・アクション」 > 「資格情報の指定」をクリックします。	データベースを選択して、「データ・ソース・アクション」 > 「資格情報の指定」をクリックします。

重要: コンプライアンス・モニター・テンプレートを使用して構成されると、オフラインにされたデータベースは引き続きコンプライアンス・モニター・ツールに表示されます。

ポリシー

クイック・スタート・コンプライアンス・モニター・テンプレートは、効果的で、変更せずに機能するように設計されたセキュリティー・ポリシーを提供します。これらのポリシーを使用して、コンプライアンス・モニターを素早く稼働状態にします。コンプライアンス・モニター・ダッシュボード・ビューから、「詳細表示」 > 「ポリシー」をクリックして、特定のコンプライアンス・タイプに関連付けられたポリシーを表示します。

コンプライアンス・モニターが中央マネージャーから構成されている場合、クイック・スタート・セキュリティー・ポリシーは自動的にすべてのコレクターにプッシュ・ダウンされます。デフォルトのクイック・スタート・セキュリティー・ポリシー以外のポリシーがインストールされている場合は、クイック・スタート・ポリシーが最後にインストールされます。

コンプライアンス・モニター・ポリシーを詳細に検討したい場合、「ポリシー・ファインダー」を介して確認できます。クイック・スタート・コンプライアンス・モニター・ポリシーは、「Quick Start *compliance type*」という命名規則で識別されます。例えば、デフォルトの GDPR ポリシーの名前は Quick Start GDPR です。 また、「データのポリシー・ビルダー」を使用して、コンプライアンス・モニター・セキュリティー・ポリシーを編集することもできます。
制約事項: Guardium V10.1.4 より前のバージョンでは、クイック・スタート・セキュリティー・ポリシーで使用されるルールとグループを変更すると、「コンプライアンス・モニター」ツールの構成状況が不正確になる場合があります。
コンプライアンス・モニター・ポリシーを変更した場合は、「コンプライアンス・モニター」ダッシュボード・ビューからデフォルト設定に戻します。それには、必要なコンプライアンス・タイプ・タイルで「詳細表示」をクリックし、「ポリシー」タブを選択して、「デフォルトにリセット」をクリックします。デフォルト設定を復元する前に、命名規則 Quick Start *compliance type timestamp* (*timestamp* はデフォルト設定が復元された日時を示す) を使用して、カスタマイズされたすべての設定がポリシーに保持されます。例えば、Quick Start GDPR 2017-05-01 19:17:59 のようになります。
重要: Guardium V10.1.4 より前のバージョンでは、「デフォルトにリセット」を使用した後、クイック・スタート・セキュリティー・ポリシーの再インストールが必要になる場合があります。詳しくは、『セキュリティー・ポリシーのインストール』を参照してください。

ポリシー・インストールのスケジュール

デフォルトでは、クイック・スタート・コンプライアンス・モニター・ツールは、毎日午前 10:30 に実行されるポリシー・インストール・スケジュールを定義します。

コンプライアンス・モニターがスタンドアロン・マシンから構成されている場合、ポリシー・インストール・スケジュールは、(スケジュールがアクティブか一時停止かどうかに関係なく) 既存のポリシー・インストール・スケジュールが存在しない場合に定義されます。コンプライアンス・モニターが中央マネージャーから構成されている場合、ポリシー・インストール・スケジュールは、(既存のポリシー・インストール・スケジュールが存在するかどうかに関係なく) すべてのコレクターに対して構成されます。

グループ

コンプライアンス・モニター・ツールは、各コンプライアンス・タイプに関連付けられている複数のグループに依存します。有効なコンプライアンス・モニターを設定するには、これらのグループにデータを設定する必要があります。コンプライアンス・モニター・ダッシュボード・ビューから、「詳細表示」 > 「要約」をクリックして、特定のコンプライアンス・タイプに関連付けられたグループを表示します。

制約事項:

- 階層グループおよびネストされたグループはサポートされません。
- 空のグループはワイルドカードとして扱われず、トラフィックを収集しません。
- Guardium V10.1.4 より前のバージョンでは、クイック・スタート・セキュリティー・ポリシーで使用されるルールとグループを変更すると、「コンプライアンス・モニター」ツールの構成状況が不正確になる場合があります。

データベースの数と、コンプライアンス・タイプの「詳細表示」 > 「要約」タブに示されている「サーバー IP」グループのメンバーの間に不一致がある場合があります。この不一致は、単一のデータベース・サーバー上で実行されている複数のデータベース、またはコンプライアンス・モニター・ツールの外部で更新された「サーバー IP」グループを反映しています。

レポート

クイック・スタート・コンプライアンス・モニター・テンプレートは、コンプライアンス・タイプごとにいくつかの事前定義されたレポートを提供します。コンプライアンス・モニター・ダッシュボード・ビューから、「詳細表示」 > 「レポート」をクリックして、特定のコンプライアンス・タイプに関連付けられたレポートを表示します。 これらのレポートは、Guardium のメイン・ナビゲーションの「アクセラレーター」セクションでも使用できます。このレポートのリストは、コンプライアンス・タイプごとに事前定義されており、ユーザーが定義したカスタム・レポートは反映されません。

制約事項: HIPAA コンプライアンス・モニター・テンプレートには、事前定義レポートは用意されていません。

ユーザーおよびロール

現行ユーザーは、選択されたコンプライアンス・タイプのロールに割り当てられます。このロールにより、Guardium のメイン・ナビゲーションから関連するレポートおよびアクセラレーターへのアクセスが可能になります。複数の異なる Guardium ユーザーが別々のコンプライアンス・タイプを構成する場合、個々のユーザーは、構成されたコンプライアンス・タイプに関連付けられているレポートおよびアクセラレーターにのみアクセスできます。

例えば、*user1* が *GDPR* を構成し、*user2* が *PCI* を構成する場合、*user1* は PCI レポートおよびアクセラレーターにアクセスできません。なぜなら、PCI ロールが *user1* に割り当てられていないからです。ユーザーへの特定のロールの手動割り当てについては、『アクセス管理の概要』を参照してください。

機密データ

コンプライアンス・タイプ・タイルの「一致するものが見つかりました」の値と、「詳細表示」 > 「要約」タブの関連するオブジェクト・グループの間に不一致がある場合があります。「一致するものが見つかりました」は、機密データのディスカバリー・シナリオの基準に一致した固有表名と列名のペアの数を示します。OBJECTS グループのメンバーの数は固有表名の数で、すべてのスキャンからの累積値です。

重要: タイルの「機密データのスキャン中」セクションの アイコンは、機密データのディスカバー・シナリオ用に 1 つ以上のデータ・ソースが構成されていることを示します。「データベースの表示」をクリックして、機密データのディスカバー用にデータ・ソースが定義されているデータベースを調べます。
親トピック: コンプライアンス・モニターのクイック・スタート

PCI/DSS アクセラレーターを使用して PCI コンプライアンスを実装する方法

PCI/DSS 要件を満たすために、IBM Security Guardium の PCI/DSS アクセラレーターを構成し、一連のポリシーとレポートを作成します。

PCI/DSS (Payment Card Industry/ Data Security Standard) は、カード所有者データを保護するために設計された一連の技術要件と運用要件です。

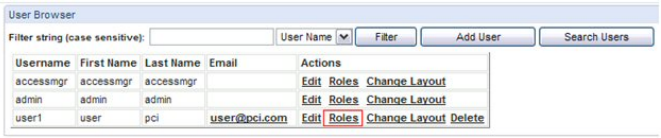
付加価値: PCI/DSS の全体的なビューをユーザーに提供し、構成にかかる時間を短縮するために定義済みのポリシーとレポートを提供します。

以下の手順を行います。

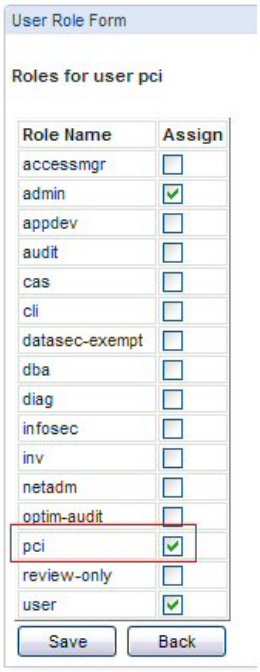
1. PCI ロールを構成します。
2. 要件を満たすレポートとポリシーを構成します。

PCI ロールの構成

1. Guardium GUI ページから「accessmgr」ユーザー・アカウントを使用してログインします。ユーザー (この場合は user1) を選択して、「ロール」をクリックします。

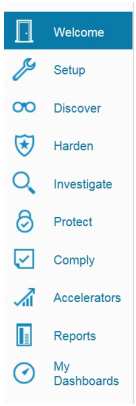


2. 「ユーザー・ロール・フォーム」で PCI を確認し、割り当てを保存します。



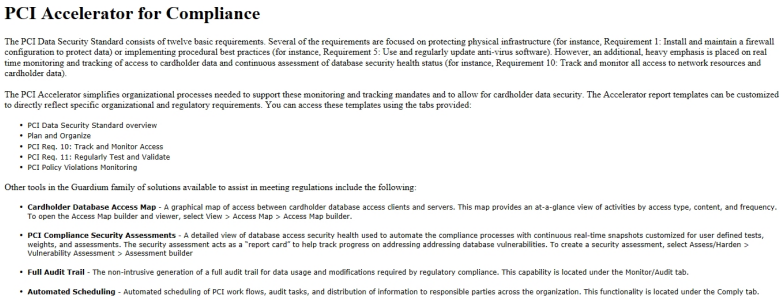
PCI アクセラレーターの実装

「user1」を使用してログオンし、「アクセラレーター」をクリックします。



概要

1. 「コンプライアンスのための PCI アクセラレーター」をクリックします。
2. 「PCI データ・セキュリティー基準」をクリックします。



PCI Accelerator for Compliance

The PCI Data Security Standard consists of twelve basic requirements. Several of the requirements are focused on protecting physical infrastructure (for instance, Requirement 1: Install and maintain a firewall configuration to protect data) or implementing procedural best practices (for instance, Requirement 5: Use and regularly update anti-virus software). However, an additional, heavy emphasis is placed on real time monitoring and tracking of access to cardholder data and continuous assessment of database security health status (for instance, Requirement 10: Track and monitor all access to network resources and cardholder data).

The PCI Accelerator simplifies organizational processes needed to support these monitoring and tracking mandates and to allow for cardholder data security. The Accelerator report templates can be customized to directly reflect specific organizational and regulatory requirements. You can access these templates using the tabs provided:

- PCI Data Security Standard overview
- Plan and Organize
- PCI Req. 10: Track and Monitor Access
- PCI Req. 11: Regularly Test and Validate
- PCI Policy Violations Monitoring

Other tools in the Guardium family of solutions available to assist in meeting regulations include the following:

- **Cardholder Database Access Map** - A graphical map of access between cardholder database access clients and servers. This map provides an at-a-glance view of activities by access type, content, and frequency. To open the Access Map builder and viewer, select View > Access Map > Access Map builder.
- **PCI Compliance Security Assessments** - A detailed view of database access security health used to automate the compliance processes with continuous real-time snapshots customized for user defined tests, weights, and assessments. The security assessment acts as a "report card" to help track progress on addressing addressing database vulnerabilities. To create a security assessment, select Assess/Harden > Vulnerability Assessment > Assessment builder
- **Full Audit Trail** - The non-intrusive generation of a full audit trail for data usage and modifications required by regulatory compliance. This capability is located under the Monitor/Audit tab.
- **Automated Scheduling** - Automated scheduling of PCI work flows, audit tasks, and distribution of information to responsible parties across the organization. This functionality is located under the Comply tab.

PCI Data Security Standard

The Payment Card Industry (PCI) Data Security Standard offers a single approach to safeguarding sensitive data for all credit card brands. This standard is the result of collaboration between Visa and MasterCard, with the objective of creating common industry security requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

The PCI Data Security Standard delivers a framework of tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. It applies to all members, merchants, and service providers that store, process, or transmit cardholder data utilizing any payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce.

PCI Compliance Validation

Separate and distinct from the mandate to comply with PCI requirements is the validation of compliance. The validation process is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained. Card vendors have prioritized and defined levels of PCI compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the systems by merchants and service providers. These include:

- Internal control
- Ongoing assessment (i.e., governance, measurement, and recordkeeping)
- Disclosure (i.e., investigation, reporting, and certification)

計画と編成

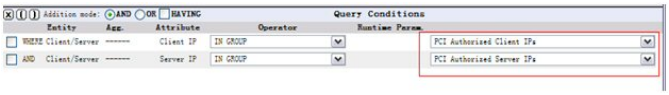
計画と編成

「概要」をクリックして、事前定義レポートがコンプライアンスにどのように準拠しているのかを示す概要を表示します。

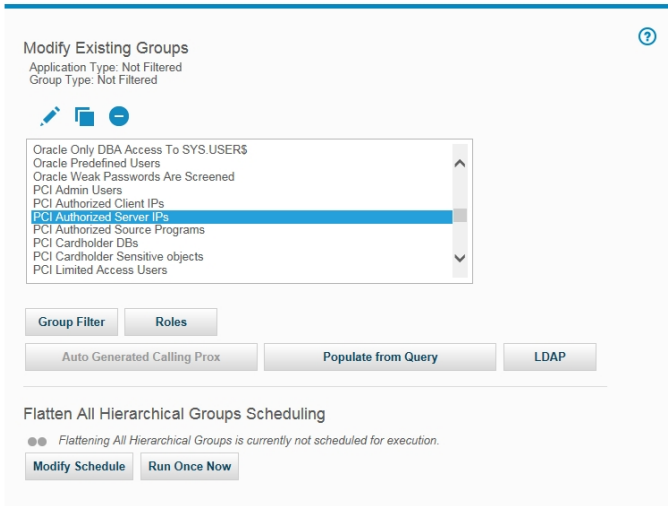
1. カード所有者サーバー IP リスト: カード所有者情報データベース・サーバーのリスト。会社の実際の状態に従って、「PCI 許可されたサーバー IP」グループの情報を設定してください。この情報により、カード所有者の情報を保管するデータベース・サーバーが指定されます。
2. カード所有者データベース: カード所有者情報データベース。「PCI カード所有者 DB: 指定済み」グループの情報を設定してください。この情報は、データベースのカード所有者情報に保管されます。
3. カード所有者オブジェクト: カード所有者情報オブジェクト。これは、PCI カード所有者の機密オブジェクトを設定する必要があります。
4. DB クライアントからサーバーへのマップ: クライアント/サーバー・マッピングの「PCI 許可されたサーバー IP」により、カード所有者情報を保管するデータベース・サーバーを指定するグループ情報が設定されます。照会を使用して、カード所有者データベースへのクライアント・アクセスを検出することができます。
5. アクティブ DB ユーザー: ユーザーのカテゴリーのほかに、カード所有者データベースにアクセスした管理者を示します。「PCI 許可されたサーバー IP」と「PCI 管理ユーザー」を設定してください。
6. カード所有者 DB 管理: カード所有者データベースの管理操作。「許可されたサーバー IP」と「PCI 管理ユーザー」を設定します。
7. 許可されたソース・プログラム: クレジット・プログラム・アクセス。「PCI 許可されたサーバー IP」と「PCI 許可されたソース・プログラム」を設定してください。クレジット・カード所有者データベース・アクセスを記録するためのプロシージャーです。
8. 無許可アプリケーション・アクセス: 非クレジット・プログラム・アクセス。「PCI 許可されたサーバー IP」と「PCI 許可されたソース・プログラム」を設定してください。カード所有者データベース・アクセスに関するクレジット・プログラムのレコードです。
9. 8.5.8 共有アカウント: コンピューターへのアクセス権限を持つ各ユーザーに固有の ID を割り当てるための、PCI の 8 番目の要件。同じデータベース・ユーザー名がカード所有者データベース IP からアクセスしようとしている回数をカウントするために、「PCI 許可されたサーバー IP」を設定します。

ステートメントで、クリックしてレポート書式を表示し、入力する必要がある特定のグループ・コンテンツを判別します。

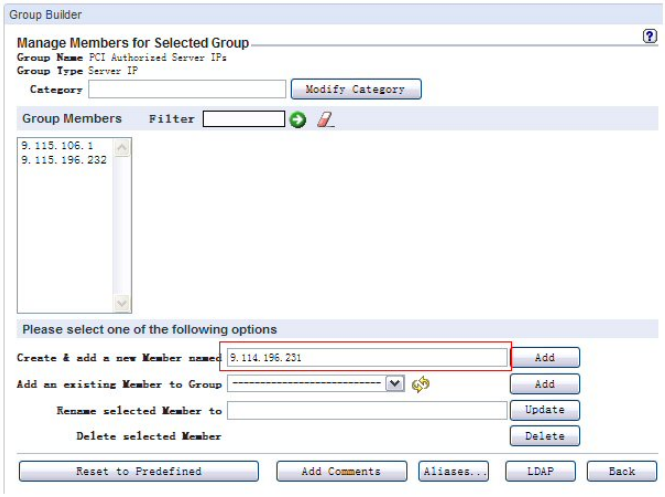
以下に実際のグループの名前を示します。



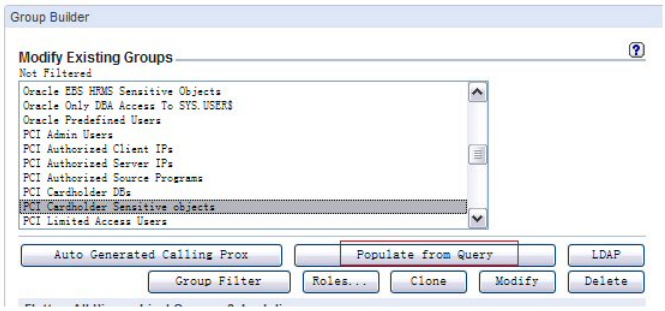
「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」にナビゲートし、「既存グループの変更」選択項目でグループ名を選択します。



「変更」(鉛筆アイコン) をクリックして、「選択したグループのメンバーの管理」ページに移動します。新規メンバーを追加します。



カスタマイズされた照会を使用してグループを入力することもできます。



PCI 要件 10 トラッキングとモニター

「概要」をクリックして、Guardium モニターと事前定義レポートがコンプライアンスにどのように準拠しているのかを示す概要を表示します。

1. 10.2 および 10.3 自動化 - オンライン・ヘルプの保護ヘルプ・ブックと順守ヘルプ・ブックを使用して、このセクションを自動化します。
2. 10.2.1 データ・アクセス - カード所有者データへの PCI アクセス。「PCI 許可されたサーバー IP」と「PCI 管理ユーザー」を設定します。
3. 10.2.2 管理アクティビティー - 管理ユーザーによる PCI アクティビティー。「PCI 許可されたサーバー IP」と「PCI 管理ユーザー」を設定します。
4. 10.2.3 監査証跡アクセス - このセクションの手順を完全に実行するには、少なくとも「SQLGuard へのログイン (Logins to SQLGuard)」、「SQLGuard サーバー上のユーザー・アクティビティーの監査証跡 (User activity audit trails on SQLGuard server)」、「スケジュールされたジョブの例外」、「ユーザー To-do リスト」の 4 種類のレポートを定義する必要があります。「設定」 > 「レポート」 > 「レポート・ビルダー」にナビゲートして、必要なレポートを作成します。
5. 10.2.4 無効なアクセス - PCI - 無効なログイン・アクセス試行: 失敗したログイン試行をデータベースに記録します。PCI - 無許可アプリケーション・アクセス: 「PCI 許可されたソース・プログラム」で定義されていないデータベース・アクセスを記録します。
6. 「10.2.6 初期化ログ」、「10.5 セキュア監査証跡」、および「10.6 アクセスの監査」の 3 つのセクションでは、組み込みオンライン・ヘルプのモニターおよび監査ヘルプ・ブックを使用することもできます。

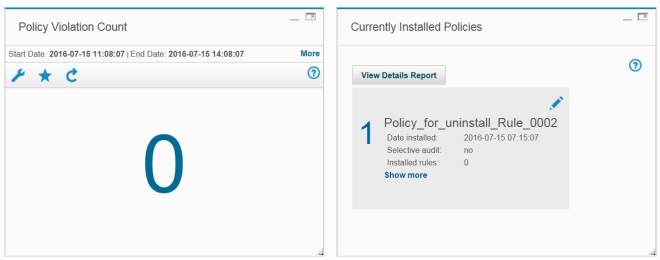
PCI 要件 11 継続的な検証

「概要」をクリックすると、脆弱性アセスメントの重要性に関する説明が表示されます。アセスメント・プロセスを作成するには、「強化」 > 「アセスメント・ビルダー」をクリックします。

PCI ポリシー・モニター

「概要」をクリックすると、ポリシーについての概要が表示されます。

1. 現在のポリシー・インストールを表示するには、「設定」 > 「ツールとビュー」 > 「ポリシー・インストール」にナビゲートし、インストールに適したポリシーを選択します。



2. ポリシー違反 - 違反操作のレコード。

ワークフロー・ビルダー

ワークフロー・ビルダーは、監査プロセスで使用する、カスタマイズされたワークフロー (ステップ、移行、およびアクション) を定義するために使用します。

追加情報は、『監査プロセスの作成』を参照してください。以下の手順に従います。

- ワークフロー・ステップを定義します (イベント状況)。
- ステップを追って移行のフローを定義します (アクション)。
- サインオフを要求するアクションを定義します。
- 各状況にロールを割り当てて、 各状況の確認を許可されるユーザーを定義します。

この機能の関連用語

イベント・タイプ - カスタム・ワークフロー

イベント状況 - ワークフローの状態/状況。

イベント・アクション - アクション/移行

注: ワークフロー・ビルダーは、プロダクト・キーによって使用可能になるオプション・コンポーネントです。

ワークフロー・プロセスの作成

1. 管理アカウントを使用して、「順守」 > 「ツールとビュー」 > 「ワークフロー・ビルダー」にナビゲートして、「ワークフロー・ビルダー」を開きます。 DataPrivacy 特権を持つユーザー・アカウントを使用して、「アクセラレーター」 > 「データ・プライバシー」 > 「トラッキングとモニター」 > 「監査証跡およびワークフローの自動化」にナビゲートして、「ワークフロー・ビルダー」を開きます。
2. 最初の画面 (「イベント・タイプ」) で、「イベント状況」をクリックして「イベント状況」構成に移動します。
3. 「イベント状況の追加」 をクリックして、新規イベント状況を定義します。複数のイベント状況が予期されています。状況の定義を入力し、 ワークフロー内で最後となるタスクについては、「 最終」チェック・ボックスにチェック・マークを付けます。
4. 「イベント・タイプ」をクリックし、「イベント・タイプ定義の追加」で「追加」をクリックして、新規イベント・タイプを定義します。
5. 定義を入力し、ワークフロー内の最初のタスクを 指定します。
6. 次に、状況項目を強調表示し、「選択可能な状況」リストと 「許可される状況」リストの間にある「>」ボタンをクリックして、「選択可能な状況 」リストから、そのワークフローの 許可される状況 をすべて選択します。
7. 終了したら、「保存」ボタンをクリックします。注: 「保存」ボタン (または「キャンセル」ボタン) は、名前、デフォルトのイベント、 または使用可能なイベントに行った変更にのみ適用されます。
8. 「イベント・タイプ」メニュー画面の「 定義済みイベント・アクション」に進みます。「定義済みイベント・アクション」では、 そのワークフローの個々のイベント・アクションの指定を行います。
9. 「新規」 ボタンをクリックします。
10. 「イベント・アクションの記述」に入力し、「前の状況」、「次の状況」、およびこのイベント・アクションでサインオフが必要かどうかを指定します。「適用」ボタンをクリックします。
11. すべてのイベント・アクションの記述と指定を行うまで、ステップ 9 と 10 を繰り返します。
12. 「イベント・タイプ」 メニュー画面の「ロール」セクションに 進みます。「ロール」では、 イベントが特定のイベント・アクションにある場合に、そのイベントを確認できる人を定義します。例えば、「検討中」のイベントを確認できる人や 「承認済み」のイベントを確認できる人です。
13. イベント・タイプ状況を選択し、 「ロール」ボタンをクリックします。
14. 「セキュリティー・ロールの割り当て」パネルで、割り当てるすべてのロールにマークを付けます (自分のアカウントに 割り当てられたロールのみが表示されます)。「適用」をクリックして、セキュリティー・ロールの 選択を保存します。「戻る」ボタンをクリックします。
15. すべてのイベント・タイプ状況でロールを 定義するまで、ステップ 13 から 14 を繰り返します。
16. ワークフロー・ビルダーからの構成が 終了しました。
17. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートして「監査プロセス・ビルダー」を開き、ワークフローをスケジュールし、ワークフロー・レポートを作成および表示します。『レポート・タスクの定義』の下にある監査プロセス・ビルダーのステップを参照してください。

付録に、使用法のシナリオ『ワークフロー・ビルダーの ワークフロー例』があります。

注: 「監査プロセス・ビルダー」のタスク・タイプが「分類プロセス」である場合は、ワークフロー・ビルダーでカスタマイズ・ワークフローを作成することはできません。

警告: ワークフロー・イベントが作成された際には、 そのイベントが使用するすべての状況にロールを割り当てることができます (つまり、 その状況にある場合、イベントはこのロールからのみ参照可能になります)。 イベントを監査プロセスに割り当てる際には、このイベントの状況に割り当てられた すべてのロールに、この監査プロセスの受信者がいることが重要です。 そうでないと、監査結果行が、この行を参照したり、状況を変更したりできる受信者が いない状況に置かれる可能性があります。

監査行がアクセス不能になった場合、admin ユーザー (ロールに関係なくすべてのイベントを表示可能) はこの行を表示し、その状況を変更できます。ただし、データ・レベル・セキュリティーがオンになっていると、 admin ユーザーがこの行を参照できない 可能性があります。admin ユーザーは、 (「グローバル・プロファイル」から) データ・レベル・セキュリティーをオフにするか、 dataset_exempt ロールを保持することが必要になります。 監査プロセスは、その監査プロセスに関連するイベントに対処する必要があるすべてのロールが受信者となるように構成することが重要です。

注: イベント状況の削除は、その状況が何らかのイベントの最初または最後の状況ではなく、アクションに 使用されていない場合にのみ許可されます。検証では、状況の削除を防止するイベント/アクションのリストが提供されます。

限定された数のレコードのみへのデフォルト・イベントの追加

監査プロセス・レポート・タスクの実行中、このプロセス・タスクの結果は、表 REPORT_RESULT_DATA_ROW に保存されます。この表は、レポートのすべての行について、1 行を持ちます。このレポート・タスクにデフォルトのイベントが 割り当てられている場合には、そのレポートのすべての行について、表 TASK_RESULT_ADDITIONAL_INFO に 行が追加されます。デフォルトのイベントが大規模な結果に対して使用される場合は、 これによってディスク・スペースの問題が発生する可能性があります。限られた数のレコードを持つ タスク結果でのみイベントを作成します。そうしないと、多数のレコードを管理することが できません。デフォルトのイベントが意図したとおりの、制限された方法で 使用される場合は、ディスク・スペースの問題もユーザビリティーの問題も発生しません。 数千個のイベントをクローズすることは容易ではありません。

- カスタマイズ・ワークフローの作成方法
  特定のカスタマー・ステップ、移行、およびアクションで構成されるカスタマイズ・ワークフローを、 監査プロセスで使用されるように定義します。
- カスタマイズしたワークフローの使用方法
  カスタマイズした顧客のワークフロー慣行に応じた監査プロセスを定義します。顧客固有の監査プロセスや手法を Guardium® ソリューションに組み入れます。

親トピック: モニターおよび監査

カスタマイズ・ワークフローの作成方法

特定のカスタマー・ステップ、移行、およびアクションで構成されるカスタマイズ・ワークフローを、 監査プロセスで使用されるように定義します。

このタスクについて

ユーザーの特定の業務に基づいてワークフローの定義および 管理を行います。

このコンポーネントの概要については、『ワークフロー・ビルダー』を 参照してください。

前提条件

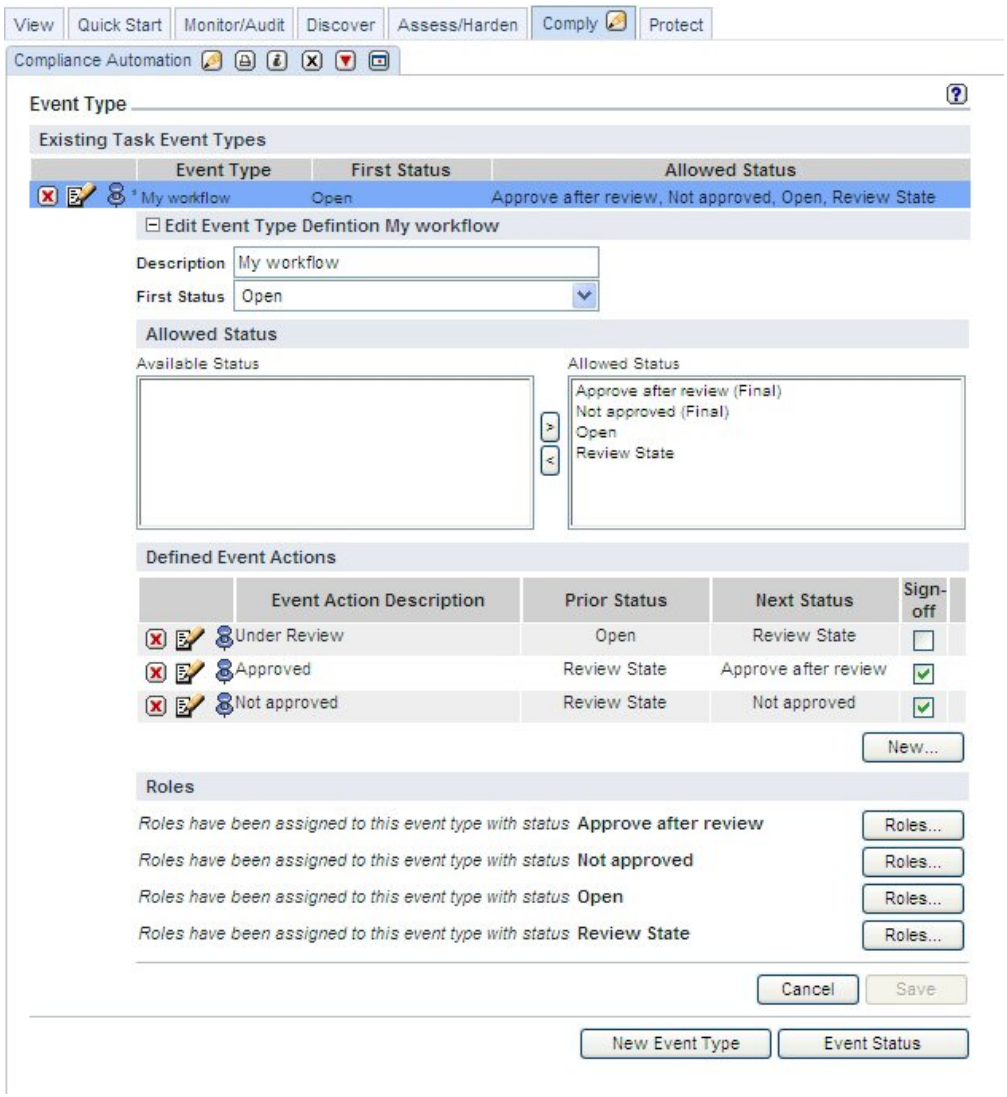
- 『監査ワークフローの作成方法』を参照してください。詳しくは、 『コンプライアンス・ワークフローの自動化』を参照してください。
- このカスタマイズ・ワークフローを作成した後、『 カスタマイズ・ワークフローと監査ワークフローの結合方法』を参照してください。

手順

1. 「順守」 > 「ツールとビュー」 > 「ワークフロー・ビルダー」にナビゲートして「ワークフロー・ビルダー」を開きます。
2. 最初の画面 (「イベント・タイプ」) で、「イベント状況」ボタンをクリックして「イベント状況」構成に移動します。
3. 「イベント状況の追加」をクリックして、新規イベント状況 を定義します。複数のイベント状況が予期されています。状況の定義を入力し、 ワークフロー内で最後となるタスクについては、「 最終」チェック・ボックスにチェック・マークを付けます。終了したら、次のステップに進みます。

   3 ステップの簡単なワークフローの例: オープン、状態の検討、承認または非承認。ワークフローの各ステップは、 個別の定義済みタスク・イベント状況です。

   例のワークフロー・タスク: オープン、 状態の検討、検討後に承認、または非承認。また、タスクがワークフロー内で 最後となる場合は、「最終」列にチェック・マークを付けます。 この例では、最後のタスクの例は「承認済み」または「非承認」です。



4. 「イベント・タイプ」ボタンをクリックし、「イベント・タイプ定義の追加」の「追加」ボタンをクリックして、新規イベント・タイプ を定義します。
5. 定義を入力し、ワークフロー内の最初のタスクを 指定します。
6. 次に、状況項目を強調表示し、「選択可能な状況」リストと 「許可される状況」リストの間にある「>」ボタンをクリックして、 「選択可能な状況」リストから、そのワークフローの許可される 状況をすべて選択します。
7. 終了したら、「保存」ボタンをクリックします。
8. 「イベント・タイプ」メニュー画面の「 定義済みイベント・アクション」に進みます。「定義済みイベント・アクション」では、 そのワークフローの個々のイベント・アクションの指定を行います。
9. 「新規」 ボタンをクリックします。

   3 ステップの簡単なワークフローの例で説明すると、 イベント・アクション「検討中」では、前の状況が「オープン」で、次の状況が「検討の状態」になります。「検討中」に続くイベント・アクションは「承認済み」で、前の状況が「検討の状態」、次の状況が「検討後に承認」になります。そうでなく、「非承認」のイベント・アクションが続く場合は、前の状況が「検討の状態」で、次の状況が「非承認」になります。また、イベント・アクションごとに指定されたレビューアーの、サインオフ機能があります (継続的または順次)。 前のスクリーン・ショットを参照してください。

10. 「イベント・アクションの記述」に入力し、「前の状況」、「次の状況」、およびこのイベント・アクションでサインオフが必要かどうかを指定します。「適用」ボタンをクリックします。
11. すべてのイベント・アクションの記述と指定を行うまで、ステップ 9 と 10 を繰り返します。
12. 「イベント・タイプ」 メニュー画面の「ロール」セクションに 進みます。「ロール」では、 イベントが特定のイベント・アクションにある場合に、そのイベントを確認できる人を定義します。例えば、「検討中」のイベントを確認できる人や 「承認済み」のイベントを確認できる人です。
13. イベント・タイプ状況を選択し、 「ロール」ボタンをクリックします。
14. 「セキュリティー・ロールの割り当て」パネルで、割り当てるすべてのロールにマークを付けます (自分のアカウントに 割り当てられたロールのみが表示されます)。「適用」をクリックして、セキュリティー・ロールの 選択を保存します。「戻る」ボタンをクリックします。
15. すべてのイベント・タイプ状況でロールを 定義するまで、ステップ 13 から 14 を繰り返します。
16. ワークフロー・ビルダーからの構成が 終了しました。
17. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートして「監査プロセス・ビルダー」を開き、ワークフローをスケジュールし、ワークフロー・レポートを作成および表示します。『レポート・タスクの定義』の下にある監査プロセス・ビルダーのステップを参照してください。

親トピック: ワークフロー・ビルダー

カスタマイズしたワークフローの使用方法

カスタマイズした顧客のワークフロー慣行に応じた監査プロセスを定義します。顧客固有の監査プロセスや手法を Guardium® ソリューションに組み入れます。

このタスクについて

Guardium 監査ワークフロー・プロセスにおけるカスタマイズ・ワークフロー

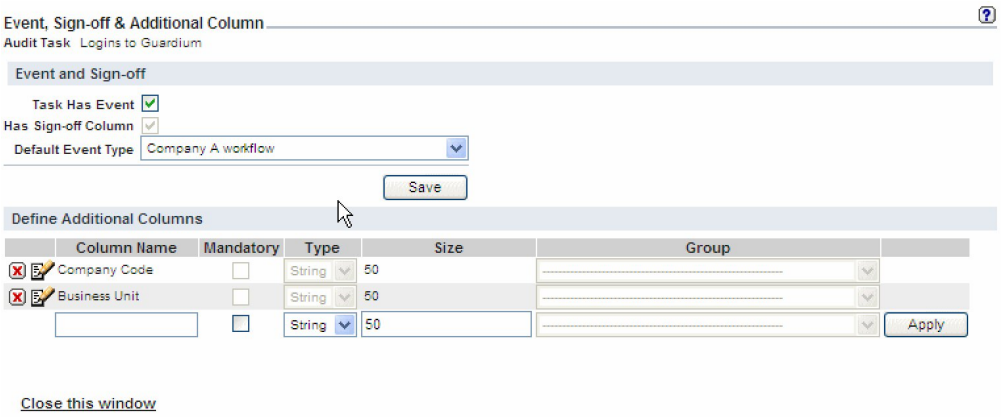
ワークフロー・ビルダーで作成されるイベント・タイプの 正式な順序の管理は、「監査タスク」ウィンドウの「イベントおよび追加列」ボタンをクリックして行います。このボタンは、監査タスクを作成して保存すると表示されます。この追加のボタンは、監査タスクを保存しないと表示されません。

前提条件

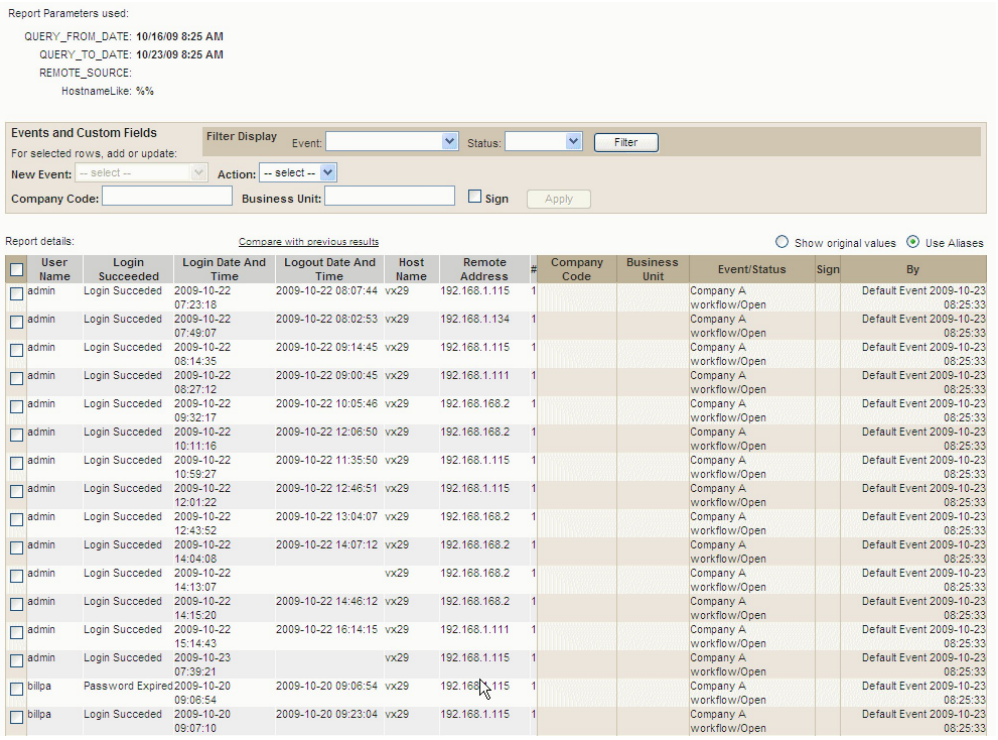
- カスタマイズしたワークフローの作成方法を参照。追加情報はワークフロー・ビルダーを参照してください。
- 『監査ワークフローの作成方法』を参照してください。詳しくは、『コンプライアンス・ワークフローの自動化』を参照してください。
- 以下の追加ステップに従い、カスタマイズした顧客のワークフロー慣行に応じた監査プロセスを定義します。

手順

1. 以下の手順で、監査タスクを追加する際にこれらのワークフロー・アクティビティーを構成します。
2. 監査タスクを作成して保存します。保存すると、追加のボタンの「イベントおよび追加列」が表示されます。
3. この追加のボタンをクリックします。



4. 次の画面で、「イベントおよびサインオフ」ボックスにチェック・マークを付けます。 ワークフロー・ビルダーで作成したワークフローが「イベントおよびサインオフ」の選択項目として表示されます。
5. この選択項目を強調表示します。選択を保存します。
6. 追加の情報 (会社コード、ビジネス・ユニット・ラベルなど) が、ワークフロー・レポートの 一部として必要である場合は、この情報を画面の「追加列」セクションに追加して、「適用」(保存) をクリックします。 完了したら、このウィンドウを閉じます。
7. 監査タスクを適用 (保存) します。監査プロセス定義全体を適用 (保存) します。 「今すぐ 1 回実行」をクリックして、レポートを作成します。「表示」をクリックすると、レポートが表示されます。
8. 「今すぐ 1 回実行」をクリックして、レポートを作成します。「表示」をクリックすると、レポートが表示されます。



この「イベントおよび追加列」ボタンは、すべての監査タスクで表示されます。

注:

監視データ・レベルでのデータ・レベル・セキュリティーが有効な場合 (「グローバル・プロファイル」設定を参照)、ユーザーに対してユーザーのデータベース情報のみが表示されるよう、監査プロセスの出力がフィルタリングされます。

「監査タスクの追加」内の「レポート」の選択項目は、「未処理のイベント」および「イベント状況の移行」の 2 つのプロシージャー型レポートです。これら 2 つのレポートを 2 つの新しい監査タスクに追加することで、すべてのワークフロー・イベントと移行の詳細を表示します。これら 2 つのレポートは、フィルター処理されません (監視データ・レベルのセキュリティー・フィルターは適用されません)。これら 2 つのレポートは、admin ユーザーおよび admin ロールを持つユーザー に対するレポート・リストでのみ、デフォルトで選択可能です。

親トピック: ワークフロー・ビルダー

脅威検出分析

Guardium には、監査済みデータをスキャンおよび分析して、さまざまなタイプのデータベース攻撃を示す可能性のある徴候を検出するための特殊な脅威検出分析が組み込まれています。

脅威検出分析では、監査済みデータをスキャンおよび分析して、SQL インジェクションまたはストアード・プロシージャーによるデータベース攻撃を示す可能性がある徴候を検出します。Guardium は、常に変化するアタック・シグニチャーのディクショナリーとの比較には依存しません。代わりに、Guardium は、長期間にわたって監査データのアクティビティー、例外、および異常値データ (Outliers Detection) を分析して、攻撃を示すパターンを探します。疑わしいイベントを一定期間にわたり追跡し、イベントを相互に関連付けることによって、Guardium は潜在的なリスクを包括的に示します。この手法はより柔軟かつ包括的であり、シグニチャーを継続的に更新する必要がありません。

脅威検出分析は、MySQL、Oracle、および Db2 でサポートされています。

- SQL インジェクション攻撃の特性
- ストアード・プロシージャー攻撃の特性
- 脅威検出分析の有効化
  このトピックでは、脅威検出分析を有効化する際の前提条件と手順について説明します。
- ケース・レポートの操作
  このトピックでは、ケース・レポートの操作について説明します。
- 脅威分析の監査プロセス・ワークフローのアクティブ化
  この手順では、Guardium の脅威診断ツールを使用するために必要な監査プロセスをスケジュールして配布する方法を説明します。
- 脅威診断ダッシュボードの操作
  「疑わしい悪意のある STP ケース」または「疑わしい SQL インジェクション攻撃」レポートの特定の脅威ケースから呼び出されるダッシュボードは、脅威診断ダッシュボードと呼ばれます。
- 脅威検出分析機能

親トピック: モニターおよび監査

SQL インジェクション攻撃の特性

SQL インジェクション攻撃は、ユーザーの入力と SQL 照会を連結することで、Web アプリケーションの脆弱性を悪用しようと試みます。これが成功すると、その攻撃で正当な Web アプリケーションの接続を使用して、悪意のある SQL コマンドを実行できるようになります。SQL インジェクション攻撃は識別が困難である場合があります。これは、攻撃の個々のステップを他のステップから独立して分析した場合、そのステップが正当であると見なされる可能性があるためです。Guardium は脅威検出分析を使用して、個々のステップを取り込み、それらのステップを 1 つの複雑な攻撃の一部として分析することで、潜在的な SQL インジェクション攻撃を識別します。

Guardium が識別する SQL インジェクション攻撃の典型的な徴候には、以下があります。

- 動的 SQL 照会の構造 (照会対象の列の数など) を識別しようとする攻撃者
- 極端に大量の新規照会 (具体的には、独特に構造化された照会、または通常とは異なる方法で構造化された照会)
- データベース構造に関する情報を格納する表へのアクセス

親トピック: 脅威検出分析

ストアード・プロシージャー攻撃の特性

悪意のあるストアード・プロシージャーとは、検出を免れ、一定の期間にわたって複雑な攻撃を実行するように設計されたコード・ブロックのことです。完全に同じ攻撃を繰り返すことも、時間とともにその特性が変化することもあります。ストアード・プロシージャーは長期間にわたって休止する場合があります。その場合、疑わしい対象として識別するのは、より困難になります。前の監査で通常とは異なるアクティビティーに気付いたとしても、次の監査が行われるまでには、以前のアクティビティーは忘れられてしまうためです。悪意のあるストアード・プロシージャーを使用することで、重要なテーブルが除去されたことを隠ぺいしたり、テーブルの内容を抽出したりすることができます。

疑わしいアクティビティーの例としては、機密オブジェクトでの DROP ステートメントを使用したストアード・プロシージャーの作成、DROP 動詞、欠落オブジェクトによる SQL 例外、長期間の休止後に変更されたプロシージャーなどが挙げられます。

Guardium は、個々のストアード・プロシージャーに関連するアクティビティーを追跡するとともに、異常値マイニング・データを使用して、各種の徴候とユーザーとを相互に関連付けます。Guardium では、この悪意のあるストアード・プロシージャー・ユース・ケースのこれらの典型的な徴候を検出できます (典型的な発生順で記載されています)。

1. データベース管理者が、顧客テーブルからデータを削除する、悪意のあるプロシージャー A を作成する。
2. 1 カ月後、データベース管理者が、プロシージャー A を呼び出すために共通して使用されているプロシージャー B を変更する。
3. 別のユーザーが変更後のプロシージャー B を呼び出し、結果としてその罪のないユーザーによって顧客テーブルのデータが削除される。

親トピック: 脅威検出分析

脅威検出分析の有効化

このトピックでは、脅威検出分析を有効化する際の前提条件と手順について説明します。

脅威検出分析を有効化するには、以下を行います。

- 検索に必要な最小限のメモリーおよびストレージ要件 (4 CPU および 24 GB RAM) を満たしていることを確認します。
- システムに、ログに記録されたアプリケーション・データがあることを確認します。具体的には、インジェクションはアプリケーションから開始されるため、SQLI にはアプリケーション・データが必要です。システムがアプリケーションを「信頼」して、Guardium でモニターしていなければ、インジェクションを識別することはできません。
- 異常値検出は、SQL インジェクションの脅威検出には必要になりませんが、疑わしいストアード・プロシージャーの検出を完全にサポートするために必要です。詳しくは、コレクターでの Outliers Detection のローカルな有効化および無効化を参照してください。
- アップグレード・パッチ・プロセスに従って Guardium V10.1 にアップグレードする際は、各コレクターでの脅威検出スキャンを有効にする必要があります。それには、Guardium API コマンド `grdapi enable_advanced_threat_scanning` を使用します。enable_advanced_threat_scanning コマンドで使用可能なパラメーターについて詳しくは、『GuardAPI 脅威検出分析機能』を参照してください。
- ケース・レポートを関連する調査ユーザーに送信するための監査プロセスをセットアップします。これはオプションですが、推奨されています。詳しくは、脅威分析の監査プロセス・ワークフローのアクティブ化を参照してください。

重要: 脅威検出は、ログに記録されたデータの分析と相関に依存します。したがって、ログに記録する前にフィルターでトラフィックを除外するルールは、脅威検出では考慮されません。「S-TAP セッションを無視」ルールの使用を慎重に検討して、コレクターの容量を最適化する代わりにこれらのセッションがログに記録されなくなるリスクを判断してください。

悪意のあるストアード・プロシージャーを分析する際の前提条件は以下のとおりです。

- 分析アルゴリズムは、部分的に機密オブジェクトのグループに依存します。 デフォルトでは、アルゴリズムはシステム定義の機密オブジェクト・グループ (グループ ID 5) のメンバーを使用します。異常値検出に別の機密オブジェクト・グループを既に指定している場合、脅威検出でもそれと同じグループが使用されます。異常値検出が有効にされていないとしても、同じ GuardAPI コマンド `set_outliers_detection_parameter parameter_name="sensitiveObjectGroupIds" parameter_value=<group ID>,<group ID>,...` を使用して独自の機密オブジェクト・グループを設定できます。
- 悪意のあるストアード・プロシージャー分析に必要なトラフィックを収集するためのポリシー・ルールをインストールする必要があります。
  推奨: ポリシー内に、以下のルールを推奨されている順で作成してください。重要な点として、これらのすべてのルールについて「次のルールに進む」チェック・ボックスにチェック・マークを付ける必要があります。
  1. アクセス・ルール: 「全詳細をロギング」(コマンド・グループ・フィルターが PROCEDURE DDL の場合)。
  2. アクセス・ルール: 「全詳細をロギング」(コマンド・グループ・フィルターが EXECUTE コマンドの場合)。使用しているデータベースが Oracle の場合は、コマンド BEGIN をルールに含めます。
  3. 例外ルール: 「ロギングのみ」(エラー・タイプ・フィルターが SQL_ERROR の場合)。

親トピック: 脅威検出分析

ケース・レポートの操作

このトピックでは、ケース・レポートの操作について説明します。

Guardium は一定期間にわたって徴候を分析し、それらを相互に関連付け、識別された潜在的な攻撃ごとにスコアを割り当てます。攻撃である可能性が高いことをスコアが示す場合、一連のイベントが 1 つのケースになり、そのケースの ID はコレクターごとに固有になります。これらのケースは、疑わしい攻撃ごとにケース・レポートで外部化されます。 ケース・レポートには、以下のいずれかの方法でアクセスします。

- 中央マネージャーの To Do リストで通知を受け取るように監査プロセスをセットアップし、関連するコレクターで直接レポートを開きます。To Do リストは 1 時間に 1 回更新されることに注意してください。
- 「調査」 > 「例外」にアクセスします。

ケース・レポートのウィンドウには、デフォルトでは、1 つのレポートで 1 行ごとに 1 件のインシデントが最大 3 件表示されます。各ケースには、1 から 3 までのリスク・スコアが含まれます (3 が最も重大です)。以下の操作が可能です。

- 攻撃の要約を表示するには、ケース ID の上にカーソルを移動します (ストアード・プロシージャーのケースのみ)。
- 詳細な徴候レポートにアクセスするには、ケース ID の上にカーソルを移動して、「徴候にリンクします」をクリックします。
- ケース固有の脅威診断ダッシュボードを開くには、ケース ID をクリックします。脅威診断ダッシュボードの操作を参照してください。

制約事項: ケース・レポートには以下の制約事項があります。

- データ・レベル・セキュリティーはありません。
- これらのレポートを複製することはできません。
- ケース・レポートの配布レポートを作成することはできますが、中央マネージャーでは、ケース・レポートから脅威診断ダッシュボードに直接リンクすることはできません。また、追加のホバー・ヘルプや徴候へのリンクもありません。

親トピック: 脅威検出分析

脅威分析の監査プロセス・ワークフローのアクティブ化

この手順では、Guardium の脅威診断ツールを使用するために必要な監査プロセスをスケジュールして配布する方法を説明します。

このタスクについて

適切なレビューアーへの脅威分析レポートの配布を制御する 2 つの監査プロセスが事前構成されています。

- 疑わしい悪意のある STP ケース
- 疑わしい SQL インジェクション・ケース

プロセスごとに 1 つの攻撃タイプに関して、疑わしいケースをプルします。これらのプロセスをカスタマイズすることも、プロセスをコピーして独自のプロセスを作成することもできます。

手順

1. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートします。オプションで、「非アクティブのみ」ラジオ・ボタンをクリックするか、「フィルター」ボックスに `Suspected` と入力することで、使用可能な監査プロセスをフィルタリングできます。

   このプロセスのデフォルトのタスクは、対応するレポート (「疑わしい悪意のある STP ケース」または「疑わしい SQL インジェクション・ケース」) です。これらのレポートのランタイム・パラメーターは変更しないでください。ただし、この同じ監査プロセスに、他のタスクを追加することはできます。例えば、両方の脅威レポートを 1 つの監査プロセスに追加できます。

   これらの監査プロセスを中央マネージャーから定義している場合、脅威データを確認する対象のコレクターごとにタスクを定義し、「リモート・データ・ソース」オプションを使用します。

2. 「結果の送信」をクリックして、監査プロセスの受信者を定義します。定義した受信者が、疑わしい悪意のあるストアード・プロシージャーに関するレポートを受け取ることになります。
3. デフォルトの受信者 (「ユーザー」) を選択してから アイコンをクリックして、組織に応じて適切な受信者 (複数可) を定義します。完了したら、「OK」をクリックします。
4. 「監査プロセスのスケジュール」」をクリックし、監査プロセスのスケジュールをレビューします。

   このプロセスを毎日、午前 12 時 30 分 (異常値検出と脅威検出の両方の通常の実行後) から 1 時間に 1 回実行することをお勧めします。このタスクには、「従属ジョブの自動実行」チェック・ボックスは適用されないことに注意してください。

   重要: 「スケジュールのアクティブ化」チェック・ボックスが選択されていることを確認します。
5. 「次へ」をクリックし、「保存」をクリックして監査プロセスの作業を完了します。

親トピック: 脅威検出分析

脅威診断ダッシュボードの操作

「疑わしい悪意のある STP ケース」または「疑わしい SQL インジェクション攻撃」レポートの特定の脅威ケースから呼び出されるダッシュボードは、脅威診断ダッシュボードと呼ばれます。

脅威診断ダッシュボードが実行する内容は他の調査ダッシュボードとほとんど同じです。ただし、異なる点として、当該ケースのダッシュボードに疑わしいイベント (データベース・ユーザー、サーバー、オブジェクトなど) のデータが取り込まれ、潜在的な攻撃を調査する際に役立つ、それらのイベントおよび周囲のイベントのさまざまなビューを提供する各種のグラフが使用されます。関連する検索および異常値データも、グラフと同じダッシュボードのページで使用できます。

多くの場合、事前定義されている脅威診断ダッシュボードの既存のフィルターは、いずれも変更する必要はありません。ただし、独自の比較分析を行う必要がある場合は、既存のフィルターを変更できます。

ダッシュボードとグラフ・フィルターの操作について詳しくは、調査ダッシュボードを参照してください。

ヒント: 脅威診断ダッシュボードは、関連する脅威レポートでケース番号をクリックすることによってのみ開くことができます。このダッシュボードや、その他すべての事前定義されたダッシュボードに変更を保存することはできません。変更した後のダッシュボードを維持して以降の調査でも使用できるようにするには、ダッシュボードをコピーし、新しい名前を付けて保存する必要があります。さらに、「フィルター」メニューをクリックし、「保存」を選択して、フィルターも保存する必要があります。

参照データとは、脅威検出分析専用に事前定義された、一連のグラフ固有のフィルターのことです。これらのフィルターにより、調査中のケースと類似するが、一般的なダッシュボード・フィルターでは含まれないデータが示されます。参照データをユーザーが変更することはできません。各グラフのフィルター・アイコンの上にカーソルを移動すると、参照データが表示されます。

疑われる SQL インジェクション攻撃の通常のシナリオでは、この攻撃で脅威診断ダッシュボードがフィルタリングされ、以下の一般的なダッシュボード・フィルターが組み込まれます。

- サーバー: 8.34.223.145
- データベース・ユーザー: USER1
- データベース: 8.4.134.213:31.5.12
- データベース・タイプ: MYSQL
- オブジェクト: stp1_name

データベース・ユーザーに関するグラフには、同様のデータベース・ユーザー (USER2、USER3、USER4 など) の参照データが含まれます。これにより、一般的なダッシュボード・フィルターではこれらの追加のユーザーが含まれないとしても、疑わしいユーザーのアクティビティーを同様のユーザーと比較することができます。

関連する参照データはすべてのフィールドに含まれるわけではありません。参照フィルターが事前定義されていないフィールドはすべて、ダッシュボードでの場合と同じようにフィルタリングされます。

一部のグラフでは、ダッシュボード全体に選択されているフィルターにかかわらず、データを比較できるよう、フィルターを非アクティブにすることができます。こうすることにより、アクティビティーの状況をより包括的に捉えることができます。

フィルター・アイコンをクリックして「グラフ・フィルターの設定」を開き、変更を行います。

- SQL インジェクションの脅威の調査

- ストアード・プロシージャーの脅威の調査

親トピック: 脅威検出分析

SQL インジェクションの脅威の調査

このタスクについて

この手順では、脅威診断ダッシュボードを使用して疑わしい SQL インジェクション攻撃を調査する方法を説明します。

手順

1. To Do リストまたは「調査」 > 「例外」から、「疑わしい SQL インジェクション・ケース」ダッシュボードを開きます。各行が 1 つのケースを表し、攻撃の確実性に対する「信頼度」評価、および攻撃のリスク・レベルが示されます。
2. 誤検出を評価するために、「表示」をクリックします。選択したケース ID の上にカーソルを移動し、「徴候 (Symptoms)」をクリックして「SQL インジェクション・ケースの徴候」ページを開きます。すべての疑われるアクションが記述され、当該 SQL 文字列が表示されます。ユーザーが文字列に加えた変更そのものを確認できます。文字列ごとに確認していくことで、前の照会から返されたエラーを使用して攻撃者がさらに多くのデータを系統的に手に入れる仕組みを観察できます。
3. ID 番号をクリックして、SQL インジェクション攻撃のデフォルト診断ダッシュボードを開きます。このダッシュボードは、インシデントの日付と、疑わしい Web アプリケーション接続の詳細でフィルタリングされています。これにより、攻撃が行われている間に発生したデータベース・トラフィックに、調査の対象を絞り込めるようになっています。フィルターを変更または除去することで、調査の範囲を広げることもできます。グラフのデータに関する詳細を調べるには、下部にあるグリッドを使用します。標準のダッシュボードに移動すると、疑われる SQL インジェクション攻撃に固有のフィルターがすべて取り消されることに注意してください。
4. グラフを調査する際は、以下のガイドラインを使用してください。
   - 時間目盛りを変更して攻撃のピーク時を見つけます。
   - セキュリティー・ポリシーの違反を見つけて、攻撃時に特定の違反が他のアクティビティーと相関しているかどうかを確認します。
5. フィルター、時間フレームなどを変更してドリルダウンし、システム全体で違いがあるかどうかを確認します。
6. ダッシュボード内の以下のグラフを評価します。

   時間およびオブジェクトごとのアクティビティー数 (Activities count per time and object)
   : このグラフには、攻撃時に最も使用されたデータベース・オブジェクトが示されます。ダッシュボードの時間フレームを拡大することで、攻撃の前後でのアクティビティーの違いを比較できます。 特定のオブジェクトをフィルタリングするには、該当するセルをクリックします。色分けによって異なるオブジェクト名が示されます。

   時間およびエラーごとのエラー数 (Error count per time and error)
   : このグラフは、Web アプリケーションで生成された SQL エラーの数を示します。SQL エラー・レートが高い場合、それは、ある種の SQL インジェクション攻撃が行われている可能性があることを意味します。色分けによって異なるエラー・タイプが示されます。

   時間および異常値の理由ごとの異常値の数 (Outlier count per time and outlier reason)
   : SQL インジェクション攻撃には、通常の照会とは構造が異なる、大量の新規照会が伴います。これらの照会により、異常値が生成されます。このグラフを使用して、問題となっている Web アプリケーションで生成された異常値の量と範囲を確認します。

   時間および違反ごとの違反数 (Violations count per time and violation)
   : SQL インジェクション攻撃が行われている間、攻撃者は、無許可のオブジェクトに対するアクセスがログに記録されるセキュリティー・ポリシーの違反を行う可能性があります。攻撃のリスクを理解するには、違反の量とタイプを比較します。

   疑わしいエラー・タイプ
   : このグラフを使用して、SQL インジェクション攻撃で脆弱性を悪用するために使用されている特定の SQL エラーを調べます。特定のセルをクリックして検索をフィルタリングし、該当するエラーを生成した SQL ステートメントを調べます。注入された SQL コードに気付く場合があります。

   疑わしいオブジェクト名 (Suspicious object names)
   : このグラフを使用して、SQL インジェクション攻撃で使用される疑わしいオブジェクトを確認します。検索の時間フレームを拡大して、攻撃が開始される前に、これらのオブジェクトが使用されたかどうかを確認します。これらのオブジェクトの使用量を比較します。

親トピック: 脅威診断ダッシュボードの操作

ストアード・プロシージャーの脅威の調査

このタスクについて

この手順では、脅威診断ダッシュボードを使用して疑わしいストアード・プロシージャー攻撃を調査する方法を説明します。

手順

1. To Do リストまたは「調査」 > 「例外」から、「疑わしい悪意のある STP ケース」ダッシュボードを開きます。各行が 1 つのケースを表し、攻撃の確実性に対する「信頼度」評価、および攻撃のリスク・レベルが示されます。
2. 誤検出を評価するために、「表示」をクリックします。
3. 選択したケース ID の上にカーソルを移動すると、ケースの詳細が表示されます。
4. 徴候をクリックして、「悪意のある STP ケースの徴候」ページを開きます。
5. ID 番号をクリックして、SQL インジェクション攻撃のデフォルト診断ダッシュボードを開きます。このダッシュボードは、インシデントの日付と、疑わしい Web アプリケーション接続の詳細でフィルタリングされています。これにより、攻撃が行われている間に発生したデータベース・トラフィックに、調査の対象を絞り込めるようになっています。フィルターを変更または除去することで、調査の範囲を広げることもできます。グラフのデータに関する詳細を調べるには、下部にあるグリッドを使用します。
6. グラフを調査する際は、以下のガイドラインを使用してください。
   - 時間目盛りを変更して攻撃のピーク時を見つけます。
   - セキュリティー・ポリシーの違反を見つけて、攻撃時に特定の違反が他のアクティビティーと相関しているかどうかを確認します。
7. フィルター、時間フレームなどを変更してドリルダウンし、システム全体で違いがあるかどうかを確認します。
8. ダッシュボード内の以下のグラフを評価します。

   さまざまなサーバーでのエラーの比較

このグラフを使用して、このサーバーとデータベース・ユーザーのエラーの数が、他のサーバーとデータベース・ユーザーと比べて異常に多いかどうかを判別します。

行動が類似する異なるデータベース・ユーザーのエラーの比較 (Compare errors from different database users with similar behavior)
このグラフを使用して、このデータベース・ユーザーのエラー・タイプと量を、類似するデータベース・ユーザーと比較します。類似するデータベース・ユーザーは、ストアード・プロシージャーを作成したすべてのユーザーです。

このデータベース・ユーザーによるストアード・プロシージャーでの類似のアクティビティー (Similar activities on stored procedures by this database user)
このグラフを使用して、特定の期間にユーザーが作成/変更したストアード・プロシージャーを確認します。 このグラフは、動詞でフィルタリングされます。このグラフを使用して、さまざまなストアード・プロシージャーでユーザーが実行したアクティビティーをドリルダウンして確認することもできます。

行動が類似するデータベース・ユーザーの違反の比較 (Compare violations from database users with similar behavior)
ストアード・プロシージャーを作成するデータベース・ユーザーの間で、違反 (ポリシー) の量とタイプを比較します

行動が類似するデータベース・ユーザーの異常値の比較 (Compare outliers from database users with similar behavior)
このグラフを使用して、このデータベース・ユーザーの異常値の量とタイプを、ストアード・プロシージャーを作成する他のデータベース・ユーザーと比較します。

このデータベース・ユーザーのデータごとの異常値 (Outliers by data on this database user)
このグラフを使用して、特定のデータベース・ユーザーの異常値の量と範囲を確認します。

親トピック: 脅威診断ダッシュボードの操作

GuardAPI 脅威検出分析機能

enable_advanced_threat_scanning

特定のデータベース攻撃 (SQL インジェクションや悪意のあるストアード・プロシージャーなど) がないか検査するスキャナー・プロセスを有効にします。

表 1. enable_advanced_threat_scanning のパラメーター

パラメーター	記述
すべて	オプション。一元管理構成に限り、すべての管理対象ユニット上のすべての脅威検出スキャナーを有効にします。指定可能な値: `true`、`false`。
schedule_start	オプション。プロセスの実行を開始する日時を指定します。許容される形式は、yyyy-mm-dd hh:mm:ss (24 時間クロック) です。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi enable_advanced_threat_scanning all=true schedule_start="2016-03-24 12:00:05”
```

異常値検出が無効になっているときに脅威分析が有効になっている場合は、以下のメッセージが表示されます。

```
Warning - Enabling advance threat scanning (AKA Eagle Eye) when Analytic anomaly detection is disabled.
Advance threat scanning (AKA Eagle Eye) enabled.
ok
```

disable_advanced_threat_scanning

コレクター上の脅威検出スキャナーを無効にします。

表 2. disable_advanced_threat_scanning のパラメーター

パラメーター	記述
すべて	一元管理構成に限り、すべての管理対象ユニット上のすべての脅威検出スキャナーを無効にします。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

get_eagle_eye_info

脅威検出パラメーターの現在の設定を表示します。

表 3. get_eagle_eye_info のパラメーター

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi get_eagle_eye_info
Eagle Eye Parameters Values:
EI_CASES_DISPLAY_LIMIT = 3
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY_CASE = 30
EI_EAGLE_EYE_ENABLED = 1
EI_PROCESSOR_TIMEOUT_SEC = 420
EI_SCANNER_PATCH_DEF = 10
EI_SCANNER_TIMEOUT_SEC = 300ok
```

set_eagle_eye_parameter

IBM 担当者の指示に従って使用してください。脅威検出の構成パラメーターを変更します。 これらのパラメーターは、以下のように、`parameter_name` および `parameter_value` を使用して明示的に設定する必要があります。

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

表 4. set_eagle_eye_parameter のパラメーター

パラメーター	記述
EI_CASES_DISPLAY LIMIT	To-do リスト・レポートに表示されるケースの数。デフォルトは 3 です。
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY CASE	To-do リスト・レポートにこのケースが既に表示されていても、そこに再表示されるようにする「信頼度」変更のパーセンテージ。Guardium が、このパーセンテージ値によって信頼度を引き上げる別の兆候を検出した場合、これが発生する可能性があります。デフォルトは 30 です。
EI_PROCESSOR_TIMEOUT_SEC	このしきい値より長い時間実行されたプロセッサーはオフになります。デフォルトは 420 秒です。
EI_SCANNER_PATCH_DEF	パッチ・インストールの結果として誤検出が発生するのを防ぐために、単一プロセス実行で作成されたストアード・プロシージャーの数がこのパラメーターを越えた場合、そのプロセスはパッチがインストールされたと想定し、兆候の分析を停止します。デフォルトでは、1 回の実行で検出されるストアード・プロシージャーの作成数は 10 です。
EI_SCANNER_TIMEOUT_SEC	このしきい値より長い時間実行されたスキャナーはオフになります。デフォルトは 300 秒です。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

get_eagle_eye_scanners_info

スキャナー設定情報を返します。

表 5. get_eagle_eye_scanners_info のパラメーター

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

返されるデータには、以下の情報が含まれます。

表 6. get_eagle_eye_scanners_info のパラメーター

フィールド	記述
ID	スキャナー ID。
Name	スキャナー名。
Status	最後の実行以降のスキャナーの状況: I: 進行中 D: 完了 K: 強制終了 E: エラーで終了
Enabled	スキャナーが有効であるかどうかを示します。 True: 有効 False: 無効
Permanent disabled	スキャナーが 24 時間で 3 回無効になった場合、そのスキャナーは永続的に無効になります。 True: 無効 False: 有効

例:

```
grdapi get_eagle_eye_scanners_info
ID=0
ID:1, Name:SQLInjectionExceptionsScanner, Status:D, Enabled:true, Permanent disabled:false
ID:2, Name:NumNewConstructScanner, Status:D, Enabled:true, Permanent disabled:false
ID:3, Name:SQLInjectionSuspiciousObjectScanner, Status:D, Enabled:true, Permanent disabled:false
ID:4, Name:SqliQueryScanner, Status:Unknown, Enabled:false, Permanent disabled:true
ID:5, Name:EagleEyeSTPCreateProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:6, Name:EagleEyeSTPCallProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:7, Name:EagleEyeSTPExceptionProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:8, Name:EagleEyePreviousStpUsageProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:9, Name:EagleEyeSTPViolationProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:10, Name:EagleEyeSTPUserOutlierScanner, Status:D, Enabled:true, Permanent disabled:false
ok
```

set_eagle_eye_scanner_parameter

IBM 担当者の指示に従って使用してください。スキャナーをアクティブ化または非アクティブ化します。これらのパラメーターは、以下のように `parameter_name` および `parameter_value` を使用して明示的に設定する必要があります。

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

表 7. set_eagle_eye_scanner_parameter のパラメーター

パラメーター	記述
scanner_id	必須。スキャナーの固有 ID。これは、get_eagle_eye_scanners_info GuardAPI コマンドから取得できます。
is_active	スキャナーを実行するかどうかを定義します。タイムアウトになったために自動的に停止されたスキャナーを開始するために使用されます。 0 : スキャナーは停止される 1: スキャナーはアクティブ化される
is_permanent_inactive	スキャナーが 24 時間で 3 回無効になった後に永続的に無効になった場合、この GuardAPI を使用することでのみ再び有効にすることができます。 1: スキャナーは永続的に停止される 0: スキャナーは有効化される
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

以下の例では、永続的に非アクティブ化されたスキャナーを再アクティブ化します。

```
set_eagle_eye_scanner_parameter scanner_id=2 parameter_name=is_permanent_inactive parameter_value=0
```

get_eagle_eye_symptom_period_hours

徴候期間パラメーターの値を時間単位で示します。徴候期間は、1 つのケースについて収集された徴候を、どのくらい前までプロセスが検索して分析するかを決定します。

表 8. get_eagle_eye_symptom_period_hours のパラメーター

パラメーター	記述
case_name	必須。ケース・タイプ。以下の値を使用できます。 STP: 悪意のあるストアード・プロシージャーのケース SQL_INJECTION: SQL インジェクションのケース
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi get_eagle_eye_symptom_period_hours case_name=STP
The symptoms period for case type: STP is: 168 in hours
ok
```

set_eagle_eye_symptom_period_hours

徴候期間パラメーターの値を時間単位で設定します。徴候期間は、1 つのケースについて収集された徴候を、どのくらい前までプロセスが検索して分析するかを決定します。

表 9. set_eagle_eye_symptom_period_hours のパラメーター

パラメーター	記述
case_name	必須。ケース・タイプ。以下の値を使用できます。 STP: 悪意のあるストアード・プロシージャーのケース SQL_INJECTION: SQL インジェクションのケース
symptom_period_hours	必須。整数。1 つのケースの兆候を分析するための過去の時間数。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi set_eagle_eye_symptom_period_hours case_name=STP symptom_period_hours=170
The symptoms period for case type: STP was changed. The old value was: 168. The new value is: 170
ok
```

get_eagle_eye_debug_level

IBM サービス担当員によって使用されます。現在のデバッグ・レベルを表示します。

- 1: オン
- 0: オフ

表 10. get_eagle_eye_debug_level のパラメーター

パラメーター	記述

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi get_eagle_eye_debug_level
ID=0
component=EAGLE_EYE level=1
ok
```

set_eagle_eye_debug_level

IBM サービス担当員によって使用されます。現在のデバッグ・レベルを表示します。

表 11. set_eagle_eye_debug_level のパラメーター

パラメーター	記述
level	整数。必須。指定可能な値: 1: オン 0: オフ
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi set_eagle_eye_debug_level level=0
ID=0
ok
```

親トピック: GuardAPI リファレンス

調査ダッシュボード

調査ダッシュボードは、Guardium 環境に存在する可能性がある問題を特定して評価するための強力なツールを提供します。これはローカルまたはシステム全体のフィルタリングされていないデータを使用し、Guardium 環境全体で、その環境内のすべての Guardium コレクターを対象としてデータを照会するための多くのフィルタリング・オプションを提供します。

調査ダッシュボードは、データ全体にわたるパターン、異常、および関係を明らかにするのに役立つ相関グラフを提供します。トポロジー、統合、またはロード・バランシング・スキームについての詳細な知識は必要ありません。これには、オリジナルの Quick Search for Enterprise の機能、およびデータを視覚化して分析するための他のツールが含まれています。

注: 調査ダッシュボードはフルスクリーン・モードで表示することをお勧めします。
制約事項: 調査ダッシュボードとデータ・レベル・セキュリティーを同時に使用可能にすることはできません。

動作モード

調査ダッシュボードは、以下の 3 つの操作モードをサポートします。

中央マネージャー専用モード

中央マネージャー上で実行依頼された照会は、検索が有効になっているすべての Guardium コレクターから企業規模の結果を返します。管理対象ユニットで実行依頼された照会は、ローカルな結果を返します。

中央マネージャー専用モードは、デフォルトの動作モードです。

全マシン・モード

企業規模の検索照会は、検索が有効になっている Guardium 環境のすべてのマシンから実行依頼されます。このモードでは、検索結果が返されるまで時間がかかる場合があります。また、環境内のすべての管理対象ユニットが接続されている必要があります。

ローカル専用モード

このモードでは、検索照会が、検索を実行依頼したローカル・コレクターに制限されます。そのため、Guardium 環境内の他のコレクターからはデータが取得されません。ローカル専用モードの CM では、データは表示されません。

検索モードの設定については、『GuardAPI Quick Search for Enterprise の機能』を参照してください。

ダッシュボードのコンポーネント

ダッシュボードは、以下の 1 つ以上の項目の集合です。

- 3 軸データ・グラフ (トリメトリック・グラフとして知られる)。これらのグラフは、カラー・マップ、棒グラフ、バブル・グラフ、折れ線グラフ、円グラフ、階段グラフ、および面グラフとして表示できます。
- アニメーション・バブル・チャート - 過去 48 時間にわたるデータ変更のアニメーション表示。
- アクティビティー・グラフ - アクティビティーおよび異常値のボリュームを表示する折れ線グラフ。これは結果表の上にあります。
- 結果表 - 元のクイック検索の検索結果と調査機能を提供します。結果表は常にダッシュボードの下部に表示されます。これは任意のダッシュボードに追加できます。
- 「場所」、「ユーザー」、「対象」、「例外」、および「タイミング」の 1 つ以上からなるファセット・リスト。これはすべてのダッシュボードの左側に表示され、削除できません。

4 つのデフォルトの DAM ビューと 2 つのデフォルトの FAM ビューがあり、それぞれ異なるグラフと表があります。ダッシュボード・メニュー からビューを選択します。デフォルトのビューは変更できません。

- 調査ダッシュボードの有効化と無効化
  このトピックでは、調査ダッシュボードを有効化および無効化する方法について説明します。
- 調査ダッシュボードでのファイル・アクティビティーの有効化
- 調査ダッシュボードへのアクセス
- データの調査ダッシュボード
  調査ダッシュボードは、事前設定されたグラフのグループと 1 つの表からなり、特定の時点でシステムに何が起こっているのかを理解するのに役立ちます。また、調査ダッシュボードをベースに、独自にカスタマイズしたダッシュボードを作成することもできます。
- ファイルの調査ダッシュボード
  調査ダッシュボードは、事前設定されたグラフのグループと 1 つの表からなり、特定の時点でシステムに何が起こっているのかを理解するのに役立ちます。また、調査ダッシュボードをベースに、独自にカスタマイズしたダッシュボードを作成することもできます。
- 調査ダッシュボードでのデータのフィルタリングおよびフィルターの保存
- 個々のグラフのフィルタリング
- 調査ダッシュボードの作成、保存、およびエクスポート
- トポロジー・ビューの使用
  トポロジー・ビューは、検索結果の Guardium アプライアンスを可視化したものです。
- ローカル検索および分散検索
- データの洞察の使用
  「データの洞察」可視化により、ユーザーは Guardium システムによって収集されたイベントのシーケンスを詳しく検査できます。特定の時間枠におけるアクティビティーを総合的に描写し、異常な動作を検出するのに役立ちます。

親トピック: モニターおよび監査
関連情報:
GuardAPI 調査ダッシュボード機能
調査ダッシュボードの CLI コマンド

調査ダッシュボードの有効化と無効化

このトピックでは、調査ダッシュボードを有効化および無効化する方法について説明します。

始める前に

調査ダッシュボードには以下の最小ハードウェア要件があります。

- 64 ビット・アーキテクチャー
- 24 GB RAM
- 4 コア CPU

制約事項: 調査ダッシュボードとデータ・レベル・セキュリティーを同時に有効化することはできません。

このタスクについて

以下に示す手順を実行すると、検索を有効化または無効化できます。

手順

1. CLI ロールを持つユーザーまたは管理者としてマシンにログインします。
2. 次の GuardAPI コマンドを使用して調査ダッシュボードを有効にします。

```
grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE
```

デフォルトでは、違反は検索結果に含まれません。違反を含めるには、次のように includeViolations パラメーターを `true` に設定します。

```
grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE includeViolations=true
```

異常値の検出を有効にするには、Outliers Detectionを参照してください。

検索索引の更新間隔など、追加のパラメーターを指定できます。パラメーターと説明の完全なリストについては、『GuardAPI 調査ダッシュボード機能』の参照情報を確認してください。

3. 次の GuardAPI コマンドを使用すると、任意のタイミングで調査ダッシュボード機能を無効にすることができます。

```
grdapi disable_quick_search
```

タスクの結果

有効になったら、調査ダッシュボードへのアクセスで詳細情報を確認し、調査ダッシュボードの使用を開始します。

重要:

- 調査ダッシュボード機能を使用すると、中央マネージャーとコレクターの両方で、ポート 8983 とポート 9983 が開きます。これらのポートは、調査ダッシュボードを有効にすると開かれ、無効にすると閉じられます。調査ダッシュボードを使用するには、ポート 8983 とポート 9983 での中央マネージャーとコレクターの間の双方向通信がファイアウォールでブロックされないようにしてください。
- 索引付き検索データは 3 日間保存されます。保存期間を変更するには、purge object Guardium CLI コマンドを使用します。例えば、「store purge object age 395」というコマンドを実行すると、データの保存期間が 5 日間に変更されます。`39` という値は、検索索引に関連付けられているデフォルトのオブジェクト識別番号であることに注意してください。詳しくは、『構成および制御 CLI コマンド』資料を参照してください。

親トピック: 調査ダッシュボード
関連情報:
GuardAPI 調査ダッシュボード機能
調査ダッシュボードの CLI コマンド

調査ダッシュボードでのファイル・アクティビティーの有効化

始める前に

- FAM バンドルをインストールして構成する必要があります。ファイルのディスカバリーおよび分類 GIM パラメーターを参照してください。
- 調査ダッシュボードを有効にする必要があります。調査ダッシュボードの有効化と無効化を参照してください。
- V10.0 Guardium システムでは、V10.1 FAM クローラーを使用しないでください。V10.1 Guardium システムでは、V10.0 FAM クローラーを使用しないでください。

このタスクについて

注: FAM は、サーバーにサーバーの IP アドレスを照会して、検出された最初のものを選択します。ホストに複数の IP アドレスがある場合、ホスト名から「適切な」IP アドレスを選択する方法はありません。 お客様は、レポートでその IP アドレスが確実に表示されるようにするには、IP アドレスを明示的に指定してください。

手順

1. コレクターの CLI プロンプトで、GuardAPI コマンドを実行します。
   `grdapi enable_fam_crawler [extraction_start] [schedule_start] [activity_schedule_interval] [activity_schedule_units] [entitlement_schedule_interval] [entitlement_schedule_units]` 例: 次のコマンドは、ディスカバリーおよび分類の更新された結果を、分類データについては 2 分ごとに、資格情報については毎日、エンタープライズ検索に送信します。
   `grdapi enable_fam_crawler activity_schedule_interval=2 activity_schedule_units=MINUTE entitlement_schedule_interval=1 entitlement_schedule_units=DAY`
   デフォルトでは、コマンドの入力時に抽出が開始され、コマンドを入力したとき (時刻) からデータが抽出されます。
2. 各コレクターで繰り返します。

親トピック: 調査ダッシュボード
関連概念:
ファイルの調査ダッシュボード
関連情報:
GuardAPI 調査ダッシュボード機能

調査ダッシュボードへのアクセス

手順

1. 「調査」 > 「データ・アクティビティーの検索」または「調査」 > 「ファイル・アクティビティーの検索」をクリックします。
2. または、検索をユーザー・インターフェースに切り替えて、調査ダッシュボードを検索します。次に、「データ・アクティビティーの検索」か「ファイル・アクティビティーの検索」のいずれかを選択します。

タスクの結果

データまたはファイルのデフォルトの調査ダッシュボードが開きます。デフォルトでは、ダッシュボード全体に適用されるフィルターのみ、過去 1 時間のデータを表示します。
親トピック: 調査ダッシュボード

データの調査ダッシュボード

調査ダッシュボードは、事前設定されたグラフのグループと 1 つの表からなり、特定の時点でシステムに何が起こっているのかを理解するのに役立ちます。また、調査ダッシュボードをベースに、独自にカスタマイズしたダッシュボードを作成することもできます。

データ・アクティビティー・モニターには 4 つのデフォルトのビューがあり、それぞれ異なるグラフと表があります。ダッシュボード・メニュー からビューを選択します。デフォルトのビューは変更できません。

デフォルトのダッシュボードには、過去 1 時間分のデータが以下の 1 つ以上のグラフと表に表示されます。

- トリメトリック・グラフ (3 軸データ・グラフ)。デフォルトのビューはカラー・マップです。追加のビューは、棒グラフ、バブル・グラフ、折れ線グラフ、円グラフ、階段グラフ、および面グラフです。
- 結果表: 元のクイック検索の検索結果と調査機能を提供します。結果表は常にダッシュボードの下部に表示されます。これは任意のダッシュボードに追加できます。以下のタブがあります。
  - アクティビティー : 「要約」タブと「詳細」タブ。「要約」タブの各行には、サーバーと DB のペアごとに記録されたアクティビティーのインスタンスの数と、データベース・タイプの数が表示されます。「詳細な概要」には、ソース・プログラムの数、データベース・ユーザー、OS ユーザー、クライアントのホスト名、クライアント IP、および日付が追加されます。「詳細」タブの各行に、1 つのアクティビティーに関する完全な詳細が示されます。
  - 異常値: 調査ダッシュボードでのデータ異常値の解釈を参照してください。
  - エラー: 「要約」タブと「詳細」タブ。「要約」タブの各行には、サーバーごとに報告されたエラーのインスタンスの数と、データベース・タイプおよびデータベース・ユーザーの数が表示されます。「詳細な概要」には、クライアント IP の数、エラー・タイプ、および日付が追加されます。「詳細」タブの各行に、1 つのエラーに関する完全な詳細が示されます。
  - 違反: 「要約」タブと「詳細」タブ。「要約」タブの各行には、サーバーと DB のペアごとに記録された違反のインスタンスの数と、データベース・タイプの数が表示されます。「詳細な概要」には、ソース・プログラムの数、データベース・ユーザー、OS ユーザー、クライアントのホスト名、クライアント IP、重大度、違反、および日付が追加されます。「詳細」タブの各行に、1 つの違反に関する完全な詳細が示されます。

追加またはオープンできる追加ビューは、以下のとおりです。

- トポロジー・ビュー 検索サーバー状況ビュー: トポロジー・ビューの使用を参照してください。
- アニメーション・バブル・チャート: 過去 48 時間にわたるデータ変更のアニメーション表示。このグラフは、24 時間の期間にわたるオブジェクトの動作を表します。 各オブジェクトは円として表され、その面積と位置 (x 軸と y 軸) がユーザー選択の 3 つの変数を表します。アニメーションは、24 時間にわたるオブジェクトの動作を表します。 「グラフの追加」ドロップダウンからアクセスします。
- アクティビティー・グラフ: 「結果表」の上にある、アクティビティーおよび異常値のボリュームを表示する折れ線グラフ。「グラフの追加」ドロップダウンからアクセスします。
- データの洞察: データ・アクティビティーの 3D 可視化。データの洞察の使用を参照してください。「グラフの追加」ドロップダウンからアクセスします。

このページのコントロールとオプションは以下のとおりです。

- 検索結果からカテゴリー化されたファセットのリスト (「場所」、「ユーザー」、「対象」、「例外」、および「タイミング」) が、すべてのダッシュボードの左側に表示されます。これは削除できません。リストを展開して、個々のファセットをクリックすることにより、特定のファセットを基準にダッシュボード全体をフィルタリングできます。
- ウィンドウの上部にある「アクティブ・フィルター」行には、現在のフィルターが表示されます。フィルターを削除するには をクリックします。
- 検索フィールド: ファセットに関係なく、すべてのフィールドの結果を同時にフィルタリングするフリー・テキスト検索。
- 分散検索: ローカル検索および分散検索を参照してください。
- 表示するデータの対象期間: 変更するには、右上隅にあるドロップダウンをクリックします。オプションは、最後の 1 時間、最後の 3 時間、最後の 1 日、最後の 3 日、ユーザーが指定する任意の期間です。デフォルトは 1 時間です。
- 「フィルター」ドロップダウン: 調査ダッシュボードでのデータのフィルタリングおよびフィルターの保存を参照してください。
- 新規ダッシュボードの追加 ダッシュボードに変更を保存 ダッシュボードを別名で保存: 調査ダッシュボードの作成、保存、およびエクスポートを参照してください。

親トピック: 調査ダッシュボード
関連概念:
調査ダッシュボードでのデータ異常値の解釈
関連タスク:
トポロジー・ビューの使用
データの洞察の使用

ファイルの調査ダッシュボード

調査ダッシュボードは、事前設定されたグラフのグループと 1 つの表からなり、特定の時点でシステムに何が起こっているのかを理解するのに役立ちます。また、調査ダッシュボードをベースに、独自にカスタマイズしたダッシュボードを作成することもできます。

デフォルトの FAM ビューは 2 つあり、それぞれ異なるグラフと表があります。ダッシュボード・メニュー からビューを選択します。デフォルトのビューは変更できません。
注: Windows でリモート・デスクトップを経由して接続する場合を除き、ダッシュボードでは、サーバー IP とクライアント IP は常に同じです。クライアント IP は、リモート・デスクトップ・セッションを使用して接続している場合のみサポートされます。
注: FAM は、サーバーにサーバーの IP アドレスを照会して、検出された最初のものを選択します。ホストに複数の IP アドレスがある場合、ホスト名から「適切な」IP アドレスを選択する方法はありません。 レポートでその IP アドレスが確実に表示されるようにするには、IP アドレスを明示的に指定してください。
デフォルトのダッシュボードには、過去 1 時間分のデータが以下の 1 つ以上のグラフと表に表示されます。

- トリメトリック・グラフ (3 軸データ・グラフ): デフォルトのビューはカラー・マップです。追加のビューは、棒グラフ、バブル・グラフ、折れ線グラフ、円グラフ、階段グラフ、および面グラフです。
- 結果表: 元のクイック検索の検索結果と調査機能を提供します。結果表は常にダッシュボードの下部に表示されます。これは、任意のダッシュボードに追加できます。以下のタブがあります。

- アクティビティー: ファイル・サーバーのポリシー・ルールに基づき、「要約」タブと「詳細」タブにモニター・データが表示されます。「要約」タブの各行には、サーバーと OS ユーザーごとに記録されたアクセス・アクティビティーのインスタンス数が示されます。「詳細」タブには、「サーバーのホスト名」、「サーバー」、「クライアントのホスト名」、「クライアント IP」、「OS ユーザー」、「ファイルの絶対パス名」、「コマンド」、「日付と時刻」が追加されます。「詳細」タブの各行に、1 つのアクティビティーに関する完全な詳細が示されます。「アクティビティー」タブに表示されるデータは、コレクターの日時と整合しています。
- 異常値: ファイル・アクティビティーの異常値の解釈を参照してください。
- エラー: 「要約」タブと「詳細」タブ。「要約」タブの各行には、サーバーとクライアント IP ごとに報告されたエラーのインスタンス数と日付が示されます。「詳細な概要」には、エラーの詳細と時刻が追加されます。「詳細」タブの各行に、1 つのエラーに関する完全な詳細が示されます。
- 違反: 「要約」タブと「詳細」タブ。「要約」タブの各行には、サーバー、ソース・プログラム、OS ユーザーの組み合わせごとに記録された違反のインスタンス数が示されます。「詳細な概要」には、クライアント IP、重大度、違反と違反の詳細、日付、時刻が追加されます。「詳細」タブの各行に、1 つの違反に関する完全な詳細が示されます。「違反」タブに表示されるデータは、ファイル・サーバーの日時と整合しています。
- 資格: 「要約」タブと「詳細」タブ。ファイル・サーバーの場合、このタブには現在の FAM 判定プランに基づく機密データが表示されます。「要約」タブの各行には、サーバーと所有者ごとに記録されたアクセス・アクティビティーのインスタンス数が示されます。「詳細」タブには、「サーバーのホスト名」、絶対パス、「タイプ」、「」、「サイズ」、「分類エンティティー」(このファイルを機密として識別する判定プラン)、「所有者」、「クライアントのホスト名」、「クライアント IP」、「OS ユーザー」、「ファイルの絶対パス名」、書き込み/読み取り/実行/削除の権限を持つユーザーとグループ、最終変更、「バージョン」(Sharepoint のみ)、作成時間、「日付」、「時刻」が追加されます。「詳細」タブの各行に、1 つのアクティビティーに関する完全な詳細が示されます。この表のデータを使用して、ファイル・サーバーのポリシー・ルールとグループを作成できます (調査ダッシュボードの「資格」タブでの FAM ポリシー・ルールの作成を参照)。

追加または開くことができる追加のビューは、以下のとおりです。

- トポロジー・ビュー 検索サーバー状況ビュー: トポロジー・ビューの使用を参照してください。
- アニメーション・バブル・チャート: 過去 48 時間にわたるデータ変更のアニメーション表示。このグラフは、24 時間の期間にわたるオブジェクトの動作を表します。 各オブジェクトは円として表され、その面積と位置 (x 軸と y 軸) がユーザー選択の 3 つの変数を表します。アニメーションは、24 時間にわたるオブジェクトの動作を表します。「グラフの追加」ドロップダウンからアクセスします。
- アクティビティー・グラフ: 「結果表」の上にある、アクティビティーおよび異常値のボリュームを表示する折れ線グラフ。「グラフの追加」ドロップダウンからアクセスします。

このページのコントロールとオプションは以下のとおりです。

- 検索結果からカテゴリー化されたファセットのリスト (「場所」、「ユーザー」、「対象」、「例外」、および「タイミング」) が、すべてのダッシュボードの左側に表示されます。これは削除できません。リストを展開して個々のファセットをクリックすることで、特定のファセットを基準にダッシュボード全体をフィルタリングできます。
- ウィンドウの上部にある「アクティブ・フィルター」行には、現在のフィルターが表示されます。フィルターを削除するには、 をクリックします。
- 検索フィールド: ファセットに関係なく、すべてのフィールドの結果を同時にフィルタリングするフリー・テキスト検索。
- 分散検索: ローカル検索および分散検索を参照してください。
- 表示するデータの対象期間: 変更するには、右上隅にあるドロップダウンをクリックします。オプションは、最後の 1 時間、最後の 3 時間、最後の 1 日、最後の 3 日、ユーザーが指定する任意の期間です。デフォルトは 1 時間です。
- 「フィルター」ドロップダウン: 調査ダッシュボードでのデータのフィルタリングおよびフィルターの保存を参照してください。
- 新規ダッシュボードの追加 ダッシュボードに変更を保存 ダッシュボードを別名で保存: 調査ダッシュボードの作成、保存、およびエクスポートを参照してください。

親トピック: 調査ダッシュボード
関連概念:
ファイル・アクティビティーの異常値の解釈
関連タスク:
トポロジー・ビューの使用

調査ダッシュボードでのデータのフィルタリングおよびフィルターの保存

このタスクについて

調査ダッシュボード全体および個々のグラフでデータをフィルタリングできます。「結果表」から関連情報にドリルダウンできます。

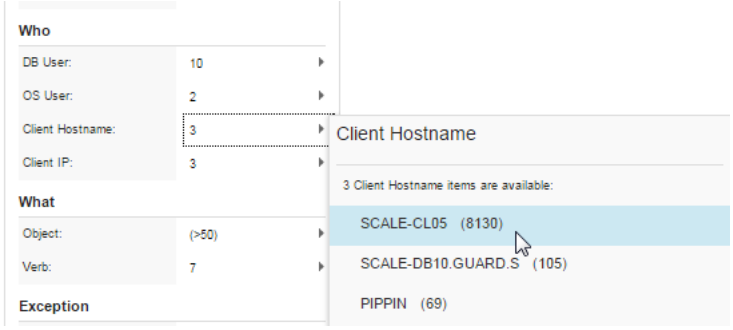
後で使用するためにフィルターを保存できます。フィルター・セットを保存するときは、フィルター・セットを共有するかどうかを選択し、それを共有するロールを選択します。

手順

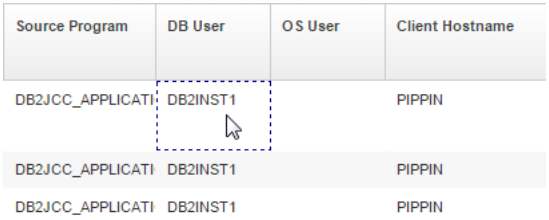
1. 以下のようにルールと構文を使用して、データをフィルタリングします。
   - ある語句と完全に一致する項目を検索するには、検索語を二重引用符で囲みます。例えば、「プロファイル・アラート・リスト」と入力すると、接続プロファイル・アラート・リストの項目は返されますが、プロファイル・リスト・アラートの項目は返されません。
   - 指定したすべての検索語と一致する項目を検索するには、検索語をスペースで区切ります。例えば、Hadoop getlisting と入力すると、語の位置や順序にかかわらず、Hadoop と getlisting の両方が含まれている項目が返されます。
   - 指定したいずれかの検索語と一致する項目を検索するには、検索語を OR または縦棒 (|) で区切ります。例えば、Hadoop OR getlisting と入力すると、語の位置にかかわらず、Hadoop か getlisting のいずれかが含まれている項目が返されます。
   - 指定した検索語が含まれない項目を検索するには、NOT またはピリオド (.) を使用します。例えば、NOT Hadoop と入力すると、語の位置にかかわらず、Hadoop が含まれている項目は返されません。
   - ワイルドカードを使用するには、文字列の先頭または末尾にアスタリスク (*) を付けます。例えば、10.10.70.* と入力すると、文字列 10.10.70. の後にさらに文字が続いている項目が返されます。
   - 検索ルールは組み合わせて使用できます。例えば、2016–5-08 (19.*|20.*) と入力すると、5 月 8 日の 19:00:00 から 20:59:59 までの時刻範囲での結果が返されます。

   フィルターを追加すると、ビューに指定された *RefFilter* に基づいて各ビューが変更されます。現在のフィルターがメニュー・バーに表示されます。X をクリックすると、それぞれをクリアできます。
2. 次のいずれかの方法で、検索結果を絞り込みます。

- 以下のようにファセット・リストに基づいて特定のフィルターを選択します。

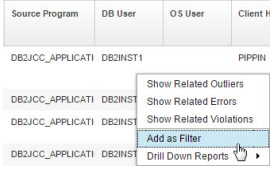


- グラフの X 軸または Y 軸のヘッダーをクリックします。
- 以下のように結果表の個別の検索結果をクリックします。



注: 1 つ以上の行を選択し、サーバー/データベース・ユーザー/クライアント IP セルのいずれかを右クリックして既存のグループに追加するか、または新規グループを作成できます。

3. 個々の結果をドリルダウンします。その方法として、特定の検索結果を右クリックして、関連する異常値、エラー、違反を調べたり、いくつかの使用可能なドリルダウン・レポートのうちの 1 つを表示したりします。



4. フィルター・セットを保存するには、「フィルター」 > 「保存」をクリックします。フィルターの名前を指定して、「プライベート」としてマークを付けるか、「共有」をクリックして、フィルターを特定のロールと共有します。 デフォルトのフィルター・セットとして保存するには (ダッシュボードは常にこれらのフィルターで開きます)、「デフォルト・フィルターとして設定」を選択します。作業が終了したら、「OK」をクリックしてフィルターを保存します。

親トピック: 調査ダッシュボード

個々のグラフのフィルタリング

このタスクについて

個々のグラフをフィルタリングできます。 アイコンは、グラフに対して一般的なダッシュボード・フィルターとは異なる特定のフィルターが設定されている場合、赤になります。アイコンの上にマウスを移動すると、そのグラフで使用されているフィルターが表示されます。

グラフではフィルターを非アクティブとして設定できます。これは、グラフ・データがそのフィールドによってフィルタリングされないことを意味します。これにより Guardium は、特定のケースに関連した項目に加え、類似しているかまたは何らかの方法で調査に関する洞察をさらに提供する可能性がある他の項目を表示できます。
例: サーバー上のアクティビティーを調査中に、グラフの 1 つを他のサーバーのデータと比較できます。これは、そのグラフに対してのみ「サーバー」フィルターを非アクティブ化することによって実行できます。 これを行うには、 アイコンをクリックし、その「サーバー」行について「非アクティブ」ラジオ・ボタンを選択します。

手順

1. アイコンをクリックします。 「グラフ・フィルターの設定」が開きます。
2. 必要に応じてラジオ・ボタンをクリックまたはクリアして、「適用」をクリックします。

親トピック: 調査ダッシュボード

調査ダッシュボードの作成、保存、およびエクスポート

このタスクについて

ダッシュボードでデータをフィルタリングするには、多くの方法があります。フィルター・セットは、専用にすることも、共有にすることもできます。例えば、環境に詳しい担当者は関連するフィルターをセットアップできます。この担当者は、特定の調査ユーザー向けのフィルターを作成してから、そのフィルターをそのロールと共有できます。 事前定義のシステム・ダッシュボードを変更して、元の名前で保存することはできません。
重要: すべての調査ダッシュボードはパブリックです。ダッシュボードが保存されると、ダッシュボードにアクセスできるすべてのユーザーは、ダッシュボード・メニューを使用して保存されたダッシュボードにもアクセスできます。さらに、ダッシュボードをデフォルト・ダッシュボードとして保存すると、すべてのユーザーにそのデフォルトが表示されます。
表示するデータに応じて、同じダッシュボードを異なるフィルター・セットで使用できます。
例: ダッシュボードに、データベース・ユーザーのアクティビティーとクライアント IP 別の明細を表示したアクティビティー・グラフが含まれています。同じデータを別のデータベース (HR や Financial など) でフィルタリングして表示することもできます。また、データベースごとに異なるコマンド・タイプを追加することもできます。

- フィルター 1: データベース HR 別、動詞 SELECT 別
- フィルター 2: データベース FINANCIAL 別、動詞 UPDATE 別

同じダッシュボードを開き、「アクティブなフィルター」リストの上の アイコンと アイコンを使用して、そのグラフに関連付けられた異なるフィルター・セットを切り替えることができます。

脅威診断を含む、すべての調査ダッシュボードを暗号化して、共有するためにエクスポートできます。フィルターではなく、ダッシュボード定義のみがエクスポートされます。

特定のインシデント・タイプの調査に適したグラフ・セットを使用して構成されたダッシュボードがある場合は、実際の攻撃データを含めたりフィルターを公開したりせずにこの知識を他の Guardium ユーザーと共有できます。

手順

1. 現在の表示を保存するには、 アイコンをクリックします。
2. 変更およびその後の使用のためにダッシュボードを別の名前で保存するには、 アイコンをクリックし、記述名およびオプションでカテゴリーを指定して保存します。また、ダッシュボードを保存する際にカテゴリーを定義することもできます。名前とカテゴリーにはスペースを含めることができます。 ダッシュボードを後で取得するには、 アイコンをクリックして、ダッシュボード・メニューを開きます。
3. 調査ダッシュボードをエクスポートするには、「管理」 > 「データ管理」 > 「定義のエクスポート」に移動します。「タイプ」メニューから、「調査ダッシュボード」を選択し、エクスポートするダッシュボード定義を選択します。次に、「エクスポート」をクリックします。

親トピック: 調査ダッシュボード

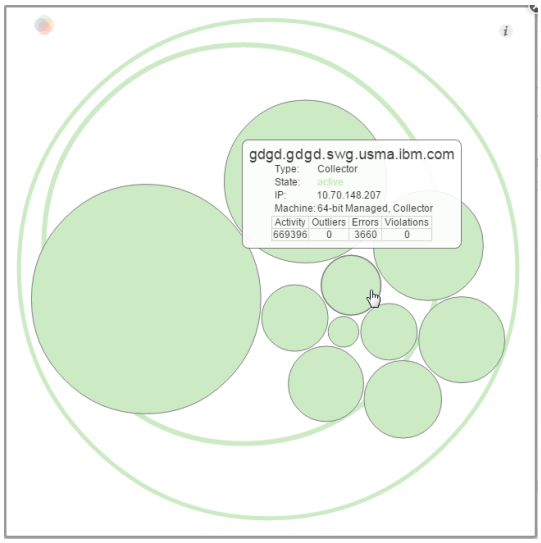
トポロジー・ビューの使用

トポロジー・ビューは、検索結果の Guardium アプライアンスを可視化したものです。

このタスクについて

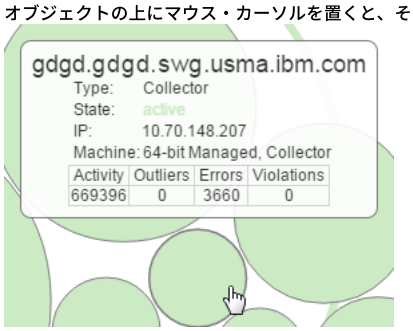
各サーバーの詳細を表示したり、フィルター基準を選択したり、検索結果を Guardium 環境全体の特定のセグメントに絞り込んだりすることができます。塗りつぶされた円はコレクターおよびアグリゲーターを表します。線のみの円は中央マネージャーを表します。円の色は、サーバーの状況を示します。中央マネージャーのアウトライン・カラーは、その状況を示します。円のサイズは、収集されたデータの相対ボリュームを示します。

トポロジー・ビューはスタンドアロン・マシンではサポートされていません。



手順

1. トポロジー・ビューを開くには、調査ダッシュボードのツールバーの「検索サーバー状況ビュー」アイコン 「検索サーバー状況ビュー」 をクリックします。
2. オブジェクトの上にマウス・カーソルを置くと、そのオブジェクトに関する詳細情報が表示されます。



3. オブジェクトを選択し、検索結果をそのオブジェクトとその子 (存在する場合) のみに絞り込みます。トポロジー・ビュー内の複数のオブジェクトを選択または選択解除するには、Ctrl キーを押しながらクリックします。
4. トポロジー・ビューを閉じるには、「閉じる」アイコン をクリックするか、トポロジー・ブラウザーの外側をクリックします。トポロジー・ビューで選択された有効範囲に基づいて、検索結果は使用可能なデータを反映するように自動更新されます。

親トピック: 調査ダッシュボード

ローカル検索および分散検索

このタスクについて

調査ダッシュボードは、ローカル・モードでも分散モードでも実行できます。ローカル・モードでは、検索はローカル・マシン (検索を実行するマシン) で使用可能なデータに制限されます。例えば、個々のコレクターから実行されたローカル検索では、そのコレクターの下にあるデータ・ソースからの結果は返されますが、環境内の他のコレクターの下にあるデータ・ソースからの結果は返されません。分散モードでは、検索を実行すると、Guardium 環境全体からのデータが返されます。結果は、検索が実行された特定のマシンによって制限されることはありません。 検索結果を Guardium 環境全体の中の特定セグメントに便宜的に絞り込むためのトポロジー・ツールが用意されています。

調査ダッシュボードは、ローカル検索モードにデフォルト設定されます。

手順

1. ローカル検索と分散検索を切り替えるには、検索ウィンドウのツールバーにある「すべてのアプライアンスの検索の有効化/無効化 (Enable / Disable search all appliance)」アイコン をクリックします。 ローカル検索または分散検索の選択に基づいて、検索結果は使用可能なデータを反映するように自動更新されます。
2. グローバル検索結果を Guardium 環境の特定セグメントでフィルタリングする方法について詳しくは、トポロジー・ビューの使用を参照してください。

親トピック: 調査ダッシュボード

データの洞察の使用

「データの洞察」可視化により、ユーザーは Guardium システムによって収集されたイベントのシーケンスを詳しく検査できます。特定の時間枠におけるアクティビティーを総合的に描写し、異常な動作を検出するのに役立ちます。

このタスクについて

データの洞察は、データ・トランザクションの全体像を把握し、予期しない動作を識別するために人間の視覚能力を使用するという革新的なパラダイムを導入します。Guardium は、監査を支援し、攻撃を検出するための堅牢な機械学習機能とデータ分析機能を既に提供しています。アルゴリズム、データ分析、およびグラフは、累積された経験と知識に基づいて設計されています。データの洞察は、人間の視覚認知の柔軟性を使用して、これまでは検出できなかった、既知の攻撃のパターンに適合しない生データの関連と移動を特定します。このツールは複雑な視覚シナリオにおけるデータのさまざまな局面を提示し、大量の複雑なデータを直接調査するためのツールを監視者に提供します。

データの洞察は、監査対象データを 3-D で可視化されたデータ・フロー (ソースから宛先まで) に時系列で変換し、発生したとおりに展開されたデータ・トランザクションを表示します。

可視化スペースには 2 つのプレーンがあり、それぞれが特定のタイプの監査ドメインのエンティティーを表します。監査データ内のすべてのエントリーは、上部プレーンのオブジェクト (例えば、クライアント IP) から下部プレーンのオブジェクト (例えば、データベース) に移動する「点滅線」として表されます。 ソースと宛先の間の点滅線は、特定のソースと宛先の間で相互作用があったことを示す証跡 (点線) を残します。それは背景へと徐々に消えていきます。証跡は、選択された期間のソースと宛先の間の相互作用の概要を示します。各ソースおよび宛先のサイズは、アクティビティーのレベルと関連しています。 ソースは、宛先の近くおよび他の類似したソースの近くにあります。この表示はさまざまな方法で変更でき、データに関する追加の情報または局面を提供します。 データの洞察は、VR ヘッドセットを使用して表示できます。

データの洞察は、常に変化するこのパラダイムに対する答えです。これは、人間の視覚認知の柔軟性を追加して、既知の攻撃タイプとは関係なく、これまでは検出できなかった生データの関連と移動を特定します。

データの洞察は、監査対象データを 3-D で可視化されたデータ・ソースおよび宛先に時系列で変換し、発生したとおりに展開されたデータ・トランザクションを表示します。可視化スペースには 2 つのプレーンがあり、それぞれが 1 つのタイプの監査ドメインのエンティティーを表します。監査データ内のすべてのエントリーは、上部プレーンのオブジェクト (クライアント IP、OS ユーザー、またはソース・プログラム) から下部プレーンのオブジェクト (データベース、オブジェクト、またはサーバー) に移動する「点滅線」として表されます。ソースと宛先の間の点滅線は、特定のソースと宛先の間で相互作用があったことを示す証跡 (点線) を残します。それは背景へと徐々に消えていきます。 点滅線には、宛先データベースと同じカラーがあります。証跡は、選択された期間のソースと宛先の間の相互作用の概要を示します。ソースは、宛先の近くおよび他の類似したソースの近くにあります。宛先エンティティーのサイズは、他の宛先エンティティーとの相対的なトランザクションの量に比例します。この表示を変更する方法は多数あります。例えば、上部エンティティーの色分け (データ・ソースの詳細が変更されると色が変わります)、データの洞察グラフのフィルタリング、調査ダッシュボードのファセットなどです。また、VR ヘッドセットを使用してデータの洞察を表示することもできます。

手順

1. 「調査ダッシュボード」ウィンドウで、「グラフの追加」 > 「データの洞察のグラフ」をクリックします。「グラフ設定」ウィンドウが開きます。
2. 「グラフ設定」ペインで、両方のプレーンに表示されるオブジェクト・タイプ、つまり両者の間のデータ・フローのタイプを変更します。オプションで、上部のプレーンのエンティティーを 2 次基準で色分けし、別のレベルの分析を実行できます。例えば、上部のプレーンのオブジェクトがクライアント IP を表す場合、ソース・プログラムの色分けを選択すると、特定の IP クライアントによるさまざまなソース・プログラムの使用法や、異なるクライアント IP による共通のソース・プログラムの使用法を表示できます。カラーが繰り返し変更されるオブジェクトは、単一のクライアント IP 内のソース・プログラムの使用法が頻繁に変更されることを示します。 「適用」をクリックします。

表 1. データの洞察グラフの設定

フィールド	説明および値
データ・フロー・ドメイン	表示されるデータ・フローのタイプ。次のいずれかです: アクティビティー、エラー、違反、異常値。

フィールド	説明および値
上部のプレーン・エンティティー	上部のプレーンに表示されるエンティティー。次のいずれかです: クライアント IP、データベース・ユーザー、OS ユーザー、ソース・プログラム。
下部のプレーン・エンティティー	下部のプレーンに表示されるエンティティー。次のいずれかです: データベース、オブジェクト、サーバー。
上部のエンティティーの色のソート基準	上部のエンティティーの追加 (オプション) の色の分類基準: なし、クライアント IP、データベース・ユーザー、OS ユーザー、ソース・プログラム。
上部のプレーン・ラベルの表示	yes、no
下部のプレーン・ラベルの表示	yes、no
上部プレーンのエンティティーの最大数	上部のプレーンに表示されるエンティティーの最大数。
下部プレーンのエンティティーの最大数	下部のプレーンに表示されるエンティティーの最大数。
上部のエンティティーの色	上部のプレーン・エンティティーの色を選択するためにカラー・パレットを開きます。上部のエンティティーの色のソートが設定されている場合は、無効になっています。
背景色	背景の色を選択するためにカラー・パレットを開きます。
プレーンの色	プレーンの色を選択するためにカラー・パレットを開きます (両方のプレーンに 1 色)。

3. 画面の変更基準:
   - フルスクリーン・モードで詳細を表示するには、拡大アイコンをクリックします
   - ビューを回転させるには、左マウス・ボタンを押したままドラッグします
   - 水平移動するには、右マウス・ボタンを押したままドラッグします
   - ズームインおよびズームアウトするには、マウス・ホイールを使用します
4. エンティティーの表示基準:
   - 凡例で詳細を表示するには、エンティティーの上にカーソルを移動します
   - エンティティーのデータ・フローのみを表示するには、そのエンティティーをクリックします (その他のエンティティーはフェードアウトします)。終了するには、背景をクリックします。
   - (ダッシュボード全体に対する) アクティブなフィルターとして使用するには、エンティティーをダブルクリックします
5. 右上隅にある情報ペインには、現在表示されているアクションのタイム・スタンプ、これまで表示されたアクションの数、および 1 秒当たりのイベントのレートの表示が示されます。この表示は、以下のように変更できます。

	データ・フローの一時停止/再開
	データ・フローを期間の最初から再開
	データ・フローの速度を上げる
	データ・フローの速度を下げる
	上部から表示 (鳥瞰)
	側面から表示 (デフォルト)

6. 必要に応じて、制御パネルの上の以下のボタンを使用します。

	データの洞察のグラフのフルスクリーン・モードをアクティブにします
	「グラフ設定」を開きます
	データの洞察のグラフを閉じます
	ポップアップ・ヘルプを開きます

親トピック: 調査ダッシュボード

Outliers Detection

2 つの簡単なステップで Outliers Detection を有効にして、Outliers Detection の監査を開始できます。これにより、Guardium が異常なサーバーの動作とユーザーの動作を識別し、考えられる攻撃を早期に検出するための処理を行えるようになります。

異常値とは、特定のデータベースまたはユーザーによるアクティビティーの「通常」の時間フレームまたは範囲から外れた特定の期間または範囲に発生した、特定のソース (DAM では、データベースまたはデータベース上の特定ユーザー。Guardium V.10.1.2 以降の FAM では、サーバーまたは OS ユーザー) による動作のことです。異常値は、アクティビティー自体が既存のセキュリティー・ポリシーに直接的に違反していなくても、セキュリティー違反の発生を示している可能性があります。

疑わしい異常値として識別されるユーザー・アクティビティーには以下があります。

- ユーザーが初めて表にアクセスする
- ユーザーが以前は選択したことのない表内の特定のデータを選択する
- エラーのボリュームが例外的に多い。例えば、アプリケーションがこれまでにない大量の SQL エラーを生成した場合です。この場合、SQL インジェクション攻撃が進行中であることを示している可能性があります。
- アクティビティー自体は珍しいものではないが、アクティビティーのボリュームが異常である
- アクティビティー自体は珍しいものではないが、アクティビティーの発生時刻が異常である。例えば、データベース管理者が特定の表にこれまでになく頻繁にアクセスしている場合です。この場合、データベース管理者がデータを少しずつ時間をかけてダウンロードしていることを示している可能性があります。

疑わしい異常値として識別されるデータベース・アクティビティーには以下があります。

- エラーのボリュームが例外的に多い

- アクティビティー自体は珍しいものではないが、アクティビティーのボリュームが異常である
- アクティビティー自体は珍しいものではないが、アクティビティーの発生時刻が異常である

異常値マイニングによる検出結果は、調査ダッシュボード (クイック検索) およびレポートで使用可能になります。

異常値マイニングは、セキュリティー・ポリシーで監査済みのデータを対象とします。異常値について評価する対象のデータが、セキュリティー・ポリシーで監査済みであることを確認してください。

Outliers Detection は、以下で実行できます。

- アグリゲーター。アグリゲーターのすべてのコレクター (Outliers Detection をローカルで実行しているコレクターを除く) からのデータを使用します.
- コレクター。コレクターが所有するデータのみを使用します。

- 異常値検出のクイック・スタート
  異常値を有効にし、いくつかの簡単なステップでアラートの受信を開始する方法について説明します。
- アグリゲーターでの Outliers Detection の有効化および無効化
  アグリゲーターのすべてのコレクターで Outliers Detection を構成するには、アグリゲーターで Outliers Detection を有効化、無効化、および構成します。
- コレクターでの Outliers Detection のローカルな有効化および無効化
  単一のコレクターで Outliers Detection を実行して、そのコレクターのデータのみを評価します。
- 調査ダッシュボードでのデータ異常値の解釈
  Guardium® には、アルゴリズムによって検出された異常値を特定し、それに応答するための便利なグラフィカル・インターフェースが用意されています。
- ファイル・アクティビティーの異常値の解釈
  調査ダッシュボードのアクティビティー・グラフと結果表でファイル・アクティビティー・モニターの異常値を確認するか (調査ダッシュボードが有効にされている必要があります)、「Analytic 異常値リスト」レポートをレビューします。
- 異常値マイニング状況のモニター
  「異常値マイニングの状況」ページを使用して、プロセスが実行される特定のユニット、および CM またはアグリゲーターのどちらかとの両方での異常値マイニング・プロセスをモニターします。
- 異常値検出で使用するユーザーとオブジェクトのグループ化
  デフォルトの異常値検出アルゴリズムにグループ (ユーザー・グループ、オブジェクト・グループなど) を追加する方法を説明します。
- 異常値検出からのイベントの除外
  特定のイベント (テスト・データからのアクティビティーなど) を、異常値検出から除外することができます。

親トピック: モニターおよび監査

異常値検出のクイック・スタート

異常値を有効にし、いくつかの簡単なステップでアラートの受信を開始する方法について説明します。

始める前に

- 異常検出が有効になっています (「設定」 > 「ツールとビュー」 > 「異常検出」)。

このタスクについて

異常値検出は、任意の数のアグリゲーターで実行可能です。ただし、1 つのアグリゲーターから開始し、構成を詳細化してから、アグリゲーターを追加して拡張することをお勧めします。開始する前に、異常値の調査に使用可能なリソースを判別します。次に、毎日報告される異常値の数を、調査可能な量に制限します。Guardium アルゴリズムでは、調査する必要がある最重要のイベント (例えば、「トップ 10」だけではない) が提供されます。

異常値検出はセキュリティー・ポリシー・ルールおよび適用とは別のプロセスであるため、異常値でリアルタイム・アラートをセットアップすることはできません。ただし、異常値データはレポートに含まれるため、相関アラートを作成することができます。相関アラートは、指定された期間をさかのぼって、アラートしきい値が満たされたかどうかを判別する照会によって起動されます。

手順

1. 異常値を有効にするには、アグリゲーターでの Outliers Detection の有効化および無効化またはコレクターでの Outliers Detection のローカルな有効化および無効化を参照してください。
2.
3. 1 日に報告される異常値の最大数を設定します。を参照してください。
4. オプションとして、異常値定義を微調整します。『異常値検出で使用するユーザーとオブジェクトのグループ化』および『異常値検出からのイベントの除外』を参照してください。
5. 照会を作成します。
   a. 「レポート」 > 「レポート構成ツール」 > 「クエリー・ビルダー」にナビゲートします。
   b. ドメイン =「分析 (analytic)」、照会名 =「Analytic 異常値リスト」または「Analytic 日付別異常値サマリー」と設定します。他のすべての設定はデフォルトのままにしておいてかまいません。
   c. 「レポートの作成」をクリックします。
6. 監査プロセスを作成します。
   a. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」にナビゲートします。
   b. プロセスに名前を付け、タスク (直前に作成したレポート) を追加します。
   c. レシーバーを定義します。必要な通知の種類を決定します。アラートをセットアップし、それを To-do リストに追加し、ユーザーが検出結果をレビューおよび正当化するように割り当てます。
   d. プロセスを日次でスケジュールし、「保存」をクリックします。
7. すぐに表示できるように、異常値レポートを「マイ・ダッシュボード」に追加します。

タスクの結果

1 週間経ってラーニング期間が完了すると、レポートにデータが含まれるようになり、アラートが送信されます。

親トピック: Outliers Detection

アグリゲーターでの Outliers Detection の有効化および無効化

アグリゲーターのすべてのコレクターで Outliers Detection を構成するには、アグリゲーターで Outliers Detection を有効化、無効化、および構成します。

始める前に

- 異常値は 24 ギガバイト以上のメモリーを備えた 64 ビット・アグリゲーターでのみ有効化にすることを強くお勧めします。

この機能は、Guardium V.10.1.2 からサポートされています。

このタスクについて

制約事項: Outliers Detection とデータ・レベル・セキュリティーを同時に有効にすることはできません。

アグリゲーターで実行すると、異常値検出データは管理対象ユニットから抽出され、アグリゲーターでラーニングおよび分析のフェーズが発生します。

異常値検出は、デフォルトでは無効になっています。指定のアグリゲーターにデータを送信するすべてのコレクター (Outliers Detection をローカルで実行中のコレクターを除く) で Outliers Detection を有効化または無効化するには、この手順を中央マネージャーで実行します。(ローカル収集について詳しくは、コレクターでの Outliers Detection のローカルな有効化および無効化を参照してください)。

コレクターをあるアグリゲーターから別のアグリゲーターに移動した場合、またはコレクターでローカルに Outliers Detection を有効化する必要がある場合は、アグリゲーターで Outliers Detection を無効化し、必要に応じて Outliers Detection をローカルで有効化してから、アグリゲーターで Outliers Detection を有効化します。アグリゲーターで Outliers Detection を有効化すると、常にそのコレクターのリストが更新されます。

手順

1. CLI ロールを持つユーザーまたは管理者として中央マネージャーにログインします。
2. Outliers Detection 機能を有効化するには、以下を入力します。

   ```
   grdapi enable_outliers_detection_agg schedule_interval=1 schedule_units=HOUR aggregator_host_name=<aggregator host name>
   DAM_FAM=DAM
   ```

   ここで:

   - aggregator_host_name パラメーターは、アグリゲーターのホスト名前です。
   - FAM_DAM は、異常値のタイプを指定するオプション・パラメーターです。デフォルトは DAM です。

3. Outliers Detection 機能を無効化するには、以下を入力します。

   ```
   grdapi disable_outliers_detection_agg aggregator_host_name=<aggregator host name>
   ```

   ここで:

   - aggregator_host_name パラメーターは、アグリゲーターの完全修飾ドメイン名です。

タスクの結果

システムが異常値データの収集を開始します。ラーニングが完了すると (14 日間)、異常値データが調査ダッシュボード (調査ダッシュボードでのデータ異常値の解釈およびファイル・アクティビティーの異常値の解釈を参照) および「異常値分析リスト」レポートで使用可能になります。

親トピック: Outliers Detection
関連概念:
調査ダッシュボード
関連情報:
GuardAPI Outliers Detection 機能

コレクターでの Outliers Detection のローカルな有効化および無効化

単一のコレクターで Outliers Detection を実行して、そのコレクターのデータのみを評価します。

始める前に

- 異常値検出は、24 ギガバイト以上のメモリーを備えた 64 ビット・コレクターでのみ有効化することを強くお勧めします。

このタスクについて

制約事項: Outliers Detection とデータ・レベル・セキュリティーを同時に有効にすることはできません。

異常値検出は、デフォルトでは無効になっています。コレクターで Outliers Detection をローカルに有効化または無効化するには、以下に説明する手順に従います。Outliers Detection がコレクターでローカルに有効化されると、そのデータはアグリゲーター上のデータと結合されません。

異常値マイニングをローカルで実行中のコレクターを識別するには、「異常値マイニングの状況」ウィンドウにアクセスし、(アグリゲーターの下ではなく) 個々のコレクターの行を調べます。列「異常値マイニングが有効/無効 (Outlier Mining Enabled/Disabled)」が緑色で表示されます。

Outliers Detection をローカルからアグリゲーターに変更するには、Outliers Detection をローカルで無効化し、アグリゲーターで異常値収集を無効化してから、アグリゲーターで Outliers Detection を再び有効化してコレクターのリストを更新します。

手順

1. CLI ロールを持つユーザーまたは管理者としてコレクターにログインします。
2. Outliers Detection 機能を有効化するには、以下を入力します。

   ```
   grdapi enable_outliers_detection schedule_interval=1 schedule_units=HOUR DAM_FAM=DAM
   ```

   ここで:

   - FAM_DAM は、異常値のタイプを指定するオプション・パラメーターです。デフォルトは DAM です。

3. Outliers Detection 機能を無効化するには、以下を入力します。

   ```
   grdapi disable_outliers_detection
   ```

タスクの結果

システムが異常値データの収集を開始します。ラーニングが完了すると (7 日間)、異常値データが調査ダッシュボード (調査ダッシュボードでのデータ異常値の解釈およびファイル・アクティビティーの異常値の解釈を参照) および「異常値分析リスト」レポートで使用可能になります。

親トピック: Outliers Detection
関連情報:
GuardAPI Outliers Detection 機能

調査ダッシュボードでのデータ異常値の解釈

Guardium® には、アルゴリズムによって検出された異常値を特定し、それに応答するための便利なグラフィカル・インターフェースが用意されています。

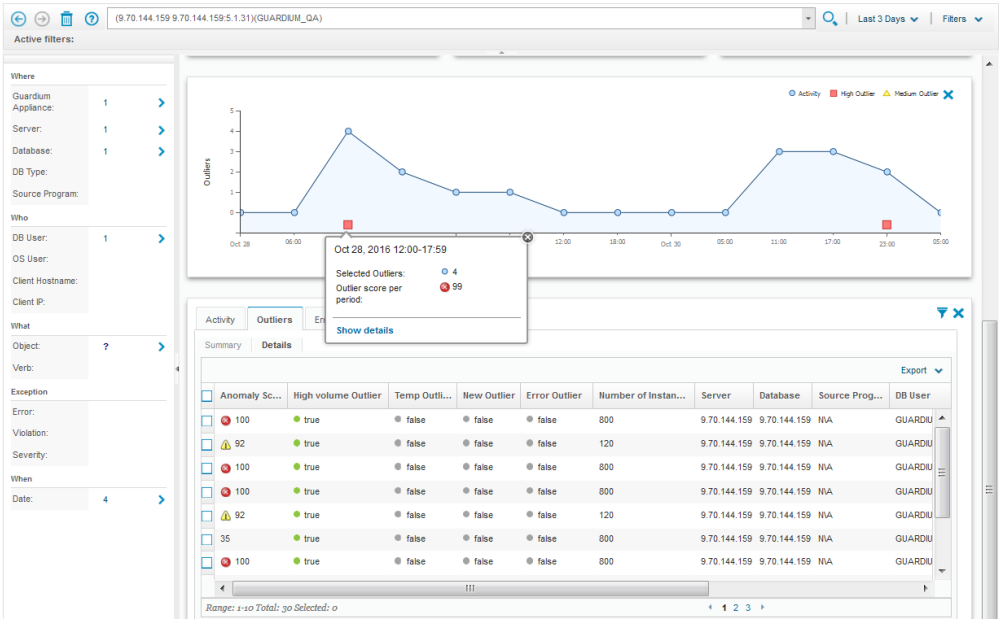
調査ダッシュボードで異常値検出データを表示するには、クイック検索を有効にする必要があります (grdapi enable_quick_search)。

アクティビティー・グラフには、選択された時間間隔の重大度や異常値スコアの合計を反映した、赤色 (高) と黄色 (中) のインディケーターが表示されます。赤色のインディケーターは、直ちに対応する必要のある異常性の高いイベントを反映しています。黄色のインディケーターは、他の調査または関連する調査の一環として注意を払う必要のある、より逸脱度の低い異常を表しています。

異常値アイコンの上にカーソルを移動すると、該当する期間に検出された異常値に関する詳細情報が表示されます。結果表をフィルタリングして、同じ期間に発生したアクティビティーまたは異常値を表示するには、「詳細を表示」をクリックします。

Guardium V.10.1.2 以降、結果表の「異常値」タブには以下の 2 つのビューがあります。

- 「要約」には、異常値が検出された 1 時間当たりのソースごとの 1 行があり、異常スコアと 1 つ以上の理由が示されます。「要約」タブに表示されるすべての異常値について、「詳細」タブにその詳細が示されるわけではないことに注意してください。
- 「詳細」は、発生したイベントのサンプルであり、イベントごとの 1 行と、その理由 (さまざまである場合を除く。表を参照) およびその他の詳細 (ソース・プログラム、オブジェクト、動詞など) があります。例えば、「大量」の場合、サンプリングはスコアが最も高いイベントを表します。「要約」タブの異常値ごとに「詳細」タブに表示するサンプル (行) の数を構成できます。



この表に、「要約」ビューと「詳細」ビューの両方に含まれる列の説明を記載します。

表 1. 結果表の「異常値」タブ内の列

列名	記述	以降のアクション

列名	記述	以降のアクション
異常スコア	「要約」タブ: 異常値の量、個々のイベントの重大度、特定の時刻における異常値の予測量などの要因に基づいて計算される集約値。例えば、通常は平日の午前 1 時に異常値が 0 個、午後 1 時に異常値が 5 から 10 個特定されるシステムで、異常値が 2 個余分に検出された場合 (午前 1 時に 2 個、または午後 1 時に 12 個) は、1 時間ごとの総数そのものよりも重要な結果 (より高く重み付けされる結果) となります。「詳細」タブ: 異常スコアは、「大量」イベントにのみ関連します。	スコアを右クリックすると、実行可能な他のアクションを選択できるメニューが開きます。「詳細」タブでは、スコアが 0 として示される場合があります。これは、個々のイベント自体は疑わしくないものの、該当する 1 時間にわたって累積されたイベントは疑わしいことを意味します。
大量の異常値	True または False。データベース・ユーザーの何らかのタイプのアクティビティーが (例えばオブジェクトに対して) 大量であることを示します。	
新規異常値	True または False。新しいオブジェクトに対するアクティビティー (例えば、管理者がいつになく多数の新しい表を作成するなど) が大量であることを示します。	
さまざまな異常値	「要約」ビューのみ。True または False。さまざまなタイプのアクティビティー (例えば、データベース・ユーザーが通常より多様なアクティビティーを行っている、またはそれらのアクティビティーを通常とは異なる時間に行っているなど) が大量であることを示します。「詳細」タブには、さまざまなイベントのサンプルが表示され、データベース・ユーザーによって識別できます。「さまざまな異常値」は「詳細」タブの列ではありませんが、それらには他の理由が割り当てられている場合もあります。 そうでない場合、理由なしで表示されます。	詳しくは、「アクティビティー」表を確認してください。
エラー異常値	True または False。エラーが大量であることを示します。	
現行の異常値	「要約」ビューのみ。True または False。過去数時間に、異常値を生成するまでではないものの、疑いを生じさせるイベントがあることを示します。	表示する必要がある特定のイベントはありません。「アクティビティー」表を表示し、ファセット・リストでデータベース別にフィルタリングして、疑わしい動作の時刻に合わせて時間間隔を変更します。
インスタンスの数	「詳細」ビューのみ。該当する 1 時間で、この特定のイベントが確認された回数。	
影響を受けるレコード	特定のイベントによって影響を受けたレコードの数。イベントが本質的にレコードに影響していない場合、負数として表示されます。	
サーバー	イベントが発生したサーバー。	
データベース	イベントが発生したデータベース。	
ソース・プログラム	「詳細」ビューのみ。イベントが発生したソース・プログラム。	
データベース・ユーザー	「詳細」ビューのみ。異常値イベントを実行したデータベース・ユーザー。	
オブジェクト	ユーザーがイベントを実行した対象のオブジェクト。	
特権ユーザー	「要約」ビューのみ。True または False。ユーザーが特権ユーザーであるかどうかを示します。	
動詞	「詳細」ビューのみ。ユーザーがイベントの実行で使用した動詞。	
日付	yyyy-mm-dd 形式で表記された、イベントが発生した日付。	
時刻	hh:mm:ss 形式で表記された、イベントが発生した時刻。	

Guardium V.10.1.2 より前のバージョンでは、異常値の理由を示す列が 1 つあり、以下の 1 つ以上の値が含まれます。

希少
: めったに見られない状態

大量
: 状態が異常に多く発生している

新規
: 最初に見られる状態

エラー
: エラー状態が異常に多く発生している

異常値の理由は、必要に応じて組み合わせて割り当てられます。例えば、めったに見られない状態が突然に何度も発生する場合は、異常値に「希少」と「大量」の両方のフラグが立てられることがあります。

注:

「影響されるレコード」結果レポートで負の結果 (「-」) が表示されている場合、ユーザーは、その負の結果をクリアするために、異常値を再有効化する必要があります。

親トピック: Outliers Detection

関連情報:

異常検出

ファイル・アクティビティーの異常値の解釈

調査ダッシュボードのアクティビティー・グラフと結果表でファイル・アクティビティー・モニターの異常値を確認するか (調査ダッシュボードが有効にされている必要があります)、「Analytic 異常値リスト」レポートをレビューします。

Guardium V.10.1.2 以降、異常値ではファイル・アクティビティー・モニターがサポートされます。

調査ダッシュボードで異常値検出データを表示するには、クイック検索を有効にする必要があります (grdapi enable_quick_search)。

調査ダッシュボードのアクティビティー・グラフと結果表で異常値を確認するか (調査ダッシュボードが有効にされている必要があります)、「Analytic 異常値リスト」レポートをレビューします。

要約グラフにアクセスするには、「データ」を選択するか、「ユーザー・インターフェース」ドロップダウンを使用し、「入力 (Enter)」をクリックします。または、検索フィールドにクイック検索を入力し、「入力 (Enter)」をクリックします。

アクティビティー・グラフには、選択された時間間隔の重大度や異常値スコアの合計を反映した、赤色 (高) と黄色 (中) のインディケーターが表示されます。赤色のインディケーターは、直ちに対応する必要のある異常性の高いイベントを反映しています。黄色のインディケーターは、他の調査または関連する調査の一環として注意を払う必要のある、より逸脱度の低い異常を表しています。

異常値アイコンの上にカーソルを移動すると、該当する期間に検出された異常値に関する詳細情報が表示されます。結果表をフィルタリングして、同じ期間に発生したアクティビティーまたは異常値を表示するには、「詳細を表示」をクリックします。

結果表の「異常値」タブには以下の 2 つのビューがあります。

- 「要約」には、異常値が検出された 1 時間当たりのソースごとの 1 行があり、異常スコアと 1 つ以上の理由が示されます。「要約」タブに表示されるすべての異常値について、「詳細」タブにその詳細が示されるわけではないことに注意してください。
- 「詳細」は、発生したイベントのサンプルであり、イベントごとの 1 行と、その理由およびその他の詳細があります。例えば、「大量」の場合、サンプリングはスコアが最も高いイベントを表します。「要約」タブの異常値ごとに「詳細」タブに表示するサンプル (行) の数を構成できます。

この表に、「要約」ビューと「詳細」ビューの両方に含まれる列の説明を記載します。

表 1. 「要約」と「詳細」の両方に定義されている列

列名	記述	以降のアクション
異常スコア	「要約」タブ: 異常値の量、個々のイベントの重大度、特定の時刻における異常値の予測量などの要因に基づいて計算される集約値。例えば、通常は平日の午前 1 時に異常値が 0 個、午後 1 時に異常値が 5 から 10 個特定されるシステムで、異常値が 2 個余分に検出された場合 (午前 1 時に 2 個、または午後 1 時に 12 個) は、1 時間ごとの総数そのものよりも重要な結果 (より高く重み付けされる結果) となります。「詳細」タブ: 異常スコアは、「大量」イベントにのみ関連します。	スコアを右クリックすると、実行可能な他のアクションを選択できるメニューが開きます。「詳細」タブでは、スコアが 0 として示される場合があります。これは、個々のイベント自体は疑わしくないものの、該当する 1 時間にわたって累積されたイベントは疑わしいことを意味します。
大量の異常値	True または False。データベース・ユーザーの何らかのタイプのアクティビティーが (例えばオブジェクトに対して) 大量であることを示します。	
新規異常値	True または False。新しいオブジェクトに対するアクティビティー (例えば、管理者がいつになく多数の新しい表を作成するなど) が大量であることを示します。	
エラー異常値	True または False。エラーが大量であることを示します。	
現行の異常値	「要約」ビューのみ。True または False。過去数時間に、異常値を生成するまでではないものの、疑いを生じさせるイベントがあることを示します。	表示する必要がある特定のイベントはありません。「アクティビティー」表を表示し、ファセット・リストでデータベース別にフィルタリングして、疑わしい動作の時刻に時間間隔を変更します。
インスタンスの数	「詳細」ビューのみ。該当する 1 時間で、この特定のイベントが確認された回数。	
サーバー	イベントが発生したサーバー。	
OS ユーザー	イベントを実行した OS ユーザー。	
特権ユーザー	True または False。ユーザーが特権ユーザーであるかどうかを示します。	
ファイルの絶対パス名	ユーザーがイベントを実行した対象のファイルの名前。	
コマンド	ユーザーがイベントの実行で使用したコマンド。	
日付	yyyy-mm-dd 形式で表記された、イベントが発生した日付。	
時刻	hh:mm:ss 形式で表記された、イベントが発生した時刻。	

親トピック: Outliers Detection
関連概念:
調査ダッシュボード
関連情報:
GuardAPI Outliers Detection 機能
異常検出

異常値マイニング状況のモニター

「異常値マイニングの状況」ページを使用して、プロセスが実行される特定のユニット、および CM またはアグリゲーターのどちらかとの両方での異常値マイニング・プロセスをモニターします。

CM で表示される「異常値マイニングの状況」ページには、すべての管理対象アグリゲーターとそれらのアグリゲーターのコレクターの詳細が表示されます。CM 内のすべてのコレクターは、それぞれのアグリゲーターの下に個別の行で表示されます。アグリゲーターで表示すると、このウィンドウには、その特定のアグリゲーターのコレクターの詳細が表示されます。コレクターから表示すると、1 つのコレクターだけが表示されます。

このページは、Guardium メニューの「管理」 > 「メンテナンス」 > 「異常値マイニングの状況」にあります。

以下の表に、このページおよび推奨されるユーザー・アクションについての説明を記載します。

表 1. 「異常値マイニングの状況」ページの列

列	記述	アクション
ユニット	ユニットの名前	NA
	このアグリゲーターにデータを送信するユニットのリストを開きます。	クリックしてユニットのリストを表示します。
ユニットのオン/オフ	ユニットがオンであるか、オフであるかを示します。	NA
異常値マイニングが有効/無効 (Outlier Mining Enabled/Disabled)	• アグリゲーター: アグリゲーターでの異常値マイニングが有効になっているかどうかを示します。無効になっている場合、この列の下にある残りの行は空になります。 • 単一のコレクターまたはスタンドアロン・ユニットの個別の行: 緑色は、異常値マイニングがローカルで有効にされていることを示します。	NA
異常値マイニングのデータを送信 (Send data for outlier mining)	コレクターのみ。コレクターは異常値マイニング・データをアグリゲーターに送信します。アグリゲーターで異常値マイニングが有効にされており、コレクターがローカルで異常値マイニングを実行していない場合、コレクターからアグリゲーターに異常値マイニングのデータが送信されます。	NA
最後の異常検出日	1 つ以上の異常 (異常値) が検出された最後の異常値マイニング実行の CM でのローカル日時。このデータは、バージョン 10.1.2 以降を実行しているユニットの場合にのみ表示されます。	NA
最後の分析日	最後の異常値マイニング実行の CM のローカル日時 (プロセス終了日時)。 このデータは、バージョン 10.1.2 以降を実行しているユニットの場合にのみ表示されます。	NA
異常値マイニングの状況	最後の異常値マイニング実行の状況。 緑色: プロセスは正常に終了しました。 黄色: プロセスは警告で終了しました。 赤色: プロセスはエラーで終了しました。 このデータは、バージョン 10.1.2 以降を実行しているユニットの場合にのみ表示されます。	エラー/警告が発生したのが 1 回だけである場合、(次の 1 時間に) プロセスをもう一度実行させて、その結果を確認します。エラーが繰り返される場合は、サポートに連絡してください。
詳細	状況は、赤色 (エラー)、黄色 (警告)、または緑色で示されます。	警告 (黄色) で終了したプロセスの場合、クリックするとポップアップが開き、警告が表示されます。 エラー (赤色) で終了したプロセスの場合、クリックするとポップアップが開き、エラーが表示されます。
ラーニング開始日	異常値マイニング・プロセスが有効化された日時。その時点から、プロセスはリソースの動作のラーニングを開始します。	NA
クイック検索のオン/オフ	管理対象ユニットで、クイック検索および Solr が有効にされているかどうかを示します。クイック検索が無効にされている場合、そのマシンのデータは調査ダッシュボードに表示されません。	調査ダッシュボードの有効化と無効化を参照してください。
最後の情報更新	この行の情報が最後に更新された日時。通常は、約 5 分間隔でデータが更新されます。	NA

表 2. 「異常値マイニングの状況」ページのボタン

ボタン	記述	アクション
リフレッシュ 	ディスプレイを最新表示します。	クリックしてディスプレイを最新表示します。
プラス記号	このボタンは、行に詳細が示されているユニットがアグリゲーターの場合にのみ表示されます。.	クリックすると、このアグリゲーターにデータを送信するユニットのリストが開きます。

親トピック: Outliers Detection

異常値検出で使用するユーザーとオブジェクトのグループ化

デフォルトの異常値検出アルゴリズムにグループ (ユーザー・グループ、オブジェクト・グループなど) を追加する方法を説明します。

このタスクについて

デフォルトでは、Guardium® の機械学習アルゴリズムで、比較的高い重み付けやスコアを付与される 2 つのユーザー・グループとオブジェクト、つまり管理ユーザーと機密オブジェクトがあります。しかし、異常値検出にも使用できる別のグループが既に作成されている場合があります。例えば、疑わしいユーザーのグループや、さまざまなアプリケーションに応じた機密オブジェクトのさまざまなグループが存在する場合があります。

手順

1. このタスクを実行するには、grdapi コマンドで使用する内部グループ ID を知っている必要があります。グループ ID を取得するには、`grdapi list_group_by_desc desc=[group name]` というコマンドを使用します。例えば、BadGuys という名前のグループがある場合は、以下のコマンドを入力することで、その内部グループ ID を取得できます。

   ```
   grdapi list_group_by_desc desc="BadGuys"
   ```

2. 目的の ID が判明したら、以下のようにランキング調整されたスコアの特権ユーザー・グループとして追加します (デフォルト・グループ 1 のスコアのランキングを調整する場合も、そのグループを含める必要があることに注意してください)。 ID 1234 のグループを追加する場合: grdapi set_outliers_detection_parameter parameter_name="privUsersGroupIds" parameter_value=1,1234
3. ID 333 および ID 156 の機密オブジェクトを追加する場合: set_outliers_detection_parameter parameter_name="sensitiveObjectGroupIds" parameter_value=5,333,156

タスクの結果

指定したグループまたは機密オブジェクトが異常値検出に追加され、アルゴリズムによって追加の重み付けが指定されます。

親トピック: Outliers Detection

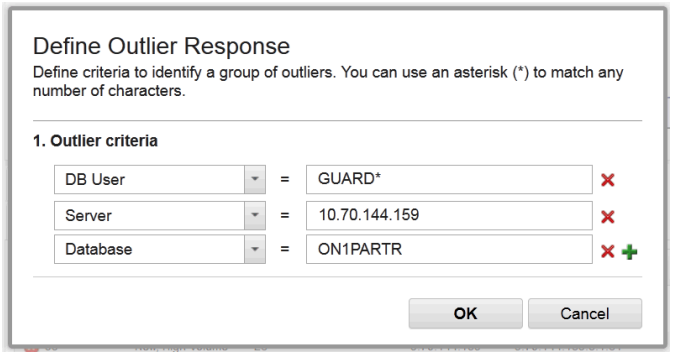
異常値検出からのイベントの除外

特定のイベント (テスト・データからのアクティビティーなど) を、異常値検出から除外することができます。

異常値応答を使用した、特定の基準に一致するイベントの除外

1. 異常値応答を除外するには、異常値インディケーターを右クリックし、「無視」を選択します。
2. 特定の値を入力するか、ワイルドカード・エントリーを使用して (* 文字を使用)、無視するイベントを定義します。
3. 該当するフィールドの ✖ アイコンをクリックして、不要なフィールドを削除します。
4. 「OK」をクリックして変更をコミットします。
5. 以前に無視したイベントを無視しないようにするには、「Analytic ユーザー・フィードバック」レポートを表示し、以前に無視したイベントをダブルクリックして、「呼び出し」 > 「delete_analytic_user_feedback」を選択します。

例えば、サーバー 10.70.144.159、データベース ON1PARTR、および名前が GUARD で始まるすべてのデータベース・ユーザーからのすべてのアクティビティーを無視する場合、ダイアログは以下のようになります。

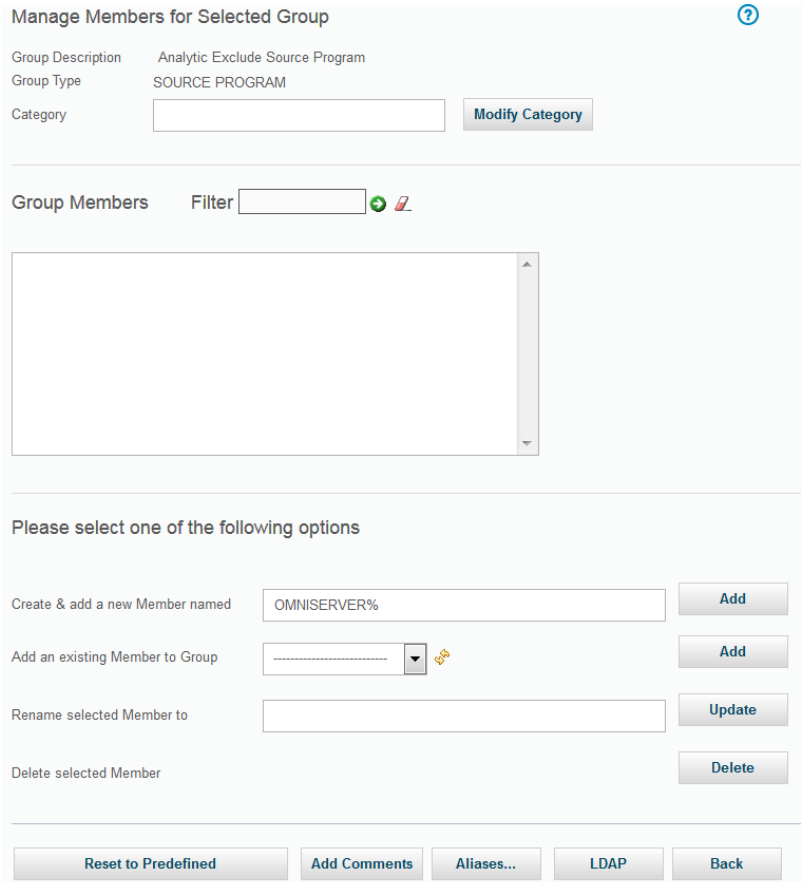


「グループ・ビルダー」を使用したイベントの除外

除外対象の項目が多数ある場合は、Guardium® の「グループ・ビルダー」を使用して、必要に応じて以下のグループのいずれかまたはすべてを設定します。

- Analytic 除外データベース・ユーザー
- Analytic 除外 OS ユーザー
- Analytic 除外サーバー IP
- Analytic 除外サービス名
- Analytic 除外ソース・プログラム

「グループ・ビルダー」には、カスタム表に対する照会から値を読み込む機能など、一括アップロードのためのオプションが用意されています。



別の方法として、GuardAPI コマンドを使用して、Analytic 除外グループを設定することもできます。例えば、「Analytic 除外ソース・プログラム」グループに OMNISERVER を追加するには、以下のコマンドを使用します。

```
grdapi create create_member_to_group_by_desc  desc="Analytic Exclude Source Program" member="OMNISERVER%"
```

親トピック: Outliers Detection

データ保護ダッシュボード

Guardium のデータ保護ダッシュボードは、上級セキュリティー担当者のためにリスクおよびコンプライアンスのデータの要約ビューを提供します。

データ保護ダッシュボードには、コンプライアンスとリスクの統計に加えて複数の図表とグラフが含まれており、大きなモニターに連続的に表示されるように設計されています。このダッシュボードを開くには、「調査」 > Guardium「データ保護ダッシュボード」にナビゲートします。

注意:
データ保護ダッシュボードを表示している間はセッションの有効期限が切れたり、ユーザーが自動的にログアウトすることはありません。 長い時間ダッシュボードを開いたままにする場合は注意してください。
情報:

- ダッシュボードは 20 分ごとに自動的に最新表示されます。
- デフォルトの検索設定は、1 日前から収集されたデータを使用した分散検索です。

図表とグラフ

いくつかの線グラフを使用すると、異なるタイプのデータを素早く比較できます。 例えば、グラフには一定期間におけるアクティビティー、エラー、および違反のボリュームを表示できます。

「異常アクティビティー」グラフには、アクティビティー全体に関する異常値の要約が表示されます。 このグラフでは、異常値の要約を示す点線が異常値の予期しないボリュームを示します。

情報: これらのグラフの Y 軸はログの軸であり、グラフの比率をゆがめる可能性があります。値やカウントはログに記録されていません。

リスクとコンプライアンスの統計

「リスク」統計には、「クリティカル」重大度で失敗したテストの数と、その失敗が発生したデータ・ソースの数が示されます。 各データ・ソースには、失敗したテストが複数含まれる可能性があります。

「モニター対象データ・ソース」には、システムがアクティビティーをログに記録しているデータ・ソースの数が示されます。この統計は、利用可能なアクセス・ドメイン・データを調べることで計算されます。

「コンプライアンス To-do リスト・タスク」には、監査プロセスの以下の要約が表示されます。当日にクローズされたプロセスの数、オープンしていたのが 3 日未満のプロセスの数、4 日以上オープンしているプロセスの数。

情報:

- ファセットおよびテキストの検索フィルターにより影響を受けないが、検索モードに影響を受ける統計。検索モードを変更するには、制御を使用して上部ペインを拡張した後、アイコンをクリックして分散検索とローカル検索を切り替えます。
- 統計コンポーネントは 1 時間に 1 回再計算されます。

親トピック: モニターおよび監査

レポート

レポートは、照会で収集したデータの表示方法を定義するものです。

デフォルトのレポートは表形式のレポートであり、照会の構造を反映して、各属性が別個の列に表示されるものになります。 表形式レポートの表示構成要素 (列見出しなど) は、すべてカスタマイズすることができます。グラフィカル・レポートはすべてレポート・ビルダーを使用して定義します。 開始日付 (照会の開始日付と照会の終了日付) のパラメーターに加え、値もすべてのレポートのページ上部と表の開始位置の間に表示できるようになりました。

レポート・ビルダーを使用する前に、クエリー・ビルダーを使用して照会を作成します。 クエリー・ビルダーの使用を参照してください。

レポートの作成と表示を最も速く行う方法は、『レポートの作成』に記載されている手順を実行し、そのレポートを「マイ・ダッシュボード」で選択する方法です。

メニュー画面間を往復して移動するには、「戻る」ボタンと「次へ」ボタンを使用してください。Web ブラウザーの戻る矢印は、Guardium® 画面間のナビゲーションでは作動しません。

レポートで使用されるアイコン

レポート・ビルダーの機能を選択するには、各種のアイコンを使用します。

表 1. レポート・アイコン

グラフィカル・アイコン	機能
	今すぐ 1 回実行する特別プロセス
	リフレッシュ
	新規ウィンドウで開くか実行
	レポートの追加
	お気に入りに追加
	このレポートの照会を変更または編集、グラフのカスタマイズ
	削除
	データマート・ビルダー
	コピー
	ランタイム・パラメーターの構成
	レポートの列の構成
<-- --> <--	レポートのカスタマイズ

編集するレポートの検索

レポートの定義にアクセスするには、レポート・ライフサイクル・アイコン  を選択して「レポート・ビルダー」をクリックします。

ドメイン、照会、またはレポート・タイトルを選択してレポートを検索します。結果は「レポート検索結果」パネルに表示されます。

- 特定のレポートを見つけるには、「レポート・タイトル」リストからレポートを選択します。選択したレポートはすぐに「レポート検索結果」パネルに表示されます。

  その他のタイプの検索をするには、1 つ以上のフィールドに入力してから「検索」ボタンをクリックします。あるいは、単に「検索」ボタンをクリックすれば、使用している Guardium アカウントで使用可能なレポートがすべてリストされます。

- 特定の照会を使用するレポートをすべてリストするには、「照会」リストから照会を選択します。
- 特定の図表タイプのレポートをすべてリストするには、「図表タイプ」リストからそのタイプを選択します。

特定のレポートを見つけるには、「レポート・タイトル」リストからレポートを選択します。選択したレポートはすぐに「レポート検索結果」パネルに表示されます。

検索によってレポートが検出されると、「レポート検索結果」パネルにそれが表示されます。次のいずれかのボタンをクリックします。

- 新規 - 『レポートの作成』を参照してください。
- コピー - 『レポートの複製』を参照してください。
- 変更 - 『レポートの変更』を参照してください。
- ロール - 『セキュリティー・ロール』を参照してください。レポート・ビルダーでレポートにロールを割り当てます。クエリー・ビルダー (トラッキング) でレポートにロールを割り当てると、レポートではなく照会のみにロールが割り当てられます。
- 削除 - 『レポートの削除』を参照してください。
- コメント - 『コメント』を参照してください。
- API 割り当て - 『API 割り当て』を参照してください。
- ドリルダウン制御 - 『レポート用のドリルダウン・レポート・メニューの変更』を参照してください。

レポートの作成

1. レポートの定義にアクセスするには、レポート・ライフサイクル・アイコン  を選択して「レポート・ビルダー」をクリックします。
2. 「新規」をクリックして「レポートの作成」パネルを開きます。
3. 「照会」リストから、レポートで使用する照会の値 (例えば、Guardium ログイン) を選択します。
4. レポート固有の名前を「レポート・タイトル」フィールドに入力します。

レポート表示のカスタマイズ

レポート表示をカスタマイズするには、以下の手順を実行します。

1. 「レポートの列の記述」パネルで次のようにします。
   - 必要に応じて「レポート・タイトル」を指定変更します。デフォルト値は、レポートの定義から取得されます。後続のほとんどのパネルでもタイトルの変更を行えます。
   - 必要に応じて「列の記述」(列見出し) を指定変更します。
2. 「次へ」をクリックして、「レポート属性」パネルを開きます。
   - 「表」ボタンまたは「グラフ」ボタンにマークを付けます。
   - 「次へ」をクリックして「レポートの実行依頼」パネルに移動します。
3. 「保存」をクリックして、作成のためにレポートを実行依頼します。

グラフィカル・レポートの作成

グラフィカル・レポートを作成するには、以下の手順を実行します。

1. 先述した『レポート表示のカスタマイズ』の手順を、「レポート列の記述」、「レポート・パラメーターの記述」、および「レポート属性」において行います。
2. 「レポートの図表タイプ」パネルで図表タイプを選択し、「次へ」をクリックします。選択肢は「面グラフ」、「棒グラフ」、「棒グラフと面グラフ」、「棒グラフと線グラフ」、「柱グラフ」、「日付面グラフ」、「日付柱グラフ」、「日付線グラフ」、「分散ラベル付き線グラフ」、「個別棒グラフ」、「個別柱グラフ」、「線グラフ」、「ピクトグラム」、「円グラフ」、「ポーラー図表」、「スピード・メーター」、および「積み重ね棒グラフ」です。円グラフ、ポーラー図表、スピード・メーター、および積み重ね棒グラフをお勧めします。1 つ選択して「次へ」をクリックします。
3. 「レポートの図表タイプ」パネルが表示されない場合はこのステップをスキップします (必要なデータはすべて入力済みです)。レポートで使用する図表のタイプを「図表タイプ」リストから選択します。
4. 「次へ」をクリックして「レポート表示パラメーター」パネルを開きます。
   - パラメーターを検討します。これは図表タイプごとに異なります。
   - 必要に応じて、選択した図表タイプのデフォルト設定を指定変更します。
5. 「次へ」をクリックして「レポートの実行依頼」パネルに進み、「レポート定義の送信」手順を実行します。
6. グラフィカル・レポートを表示するには、「マイ・ダッシュボード」に移動してグラフィカル・レポートを追加します。

注:

すべてのグラフィカル・レポートで、ヘルプ・アイコンの隣に最新表示アイコンが表示されます。

レポート定義の送信

1. 必要に応じて、コメントを追加します (『コメント』を参照)。
2. 必要に応じて、ロールを割り当てます (『セキュリティー・ロール』を参照)。
3. 「保存」をクリックします。

レポートの変更

1. 変更対象のレポートを検索します。「レポート・ビルダー」ファインダー・メニューに移動します。
2. 「変更」  をクリックして「レポートの列」パネルを開きます。
3. 続けて、『レポート表示のカスタマイズ』の手順を実行します。

レポートの複製

1. 複製対象のレポートを検索します。「レポート・ビルダー」ファインダー・メニューに移動します。
2. 「コピー」  をクリックして「レポートの列」パネルを開きます。
3. 複製するレポートの新規名を「レポート・タイトル」ボックスに入力します。この新規名は後続する任意の画面で入力できます。必要なのは、複製したレポートを保存する前に新規名を入力しておくことです。

4. 続けて、『レポート表示のカスタマイズ』の手順を実行します。

レポートの削除

事前定義レポートは削除できないことに注意してください。また、監査プロセスで使用されるレポートも削除できません。

1. 削除対象のレポートを検索します。
2. 「削除」 をクリックしてレポートを削除します。

レポートのサイズ制限

表形式のレポートの出力は 5,000 行に制限されますが、ワークフロー・プロセスに組み込まれる場合はレポート・タスクから CSV または CEF ファイルに任意の数の行をエクスポートできます。 監査プロセスの作成を参照してください。

制限

レポートを表示する際のボタン (PDF 生成、CSV 生成、および印刷可能) に対する制限は、30,000 行までです。 これはカスタマイズできません。

グループおよび別名ビルダーで「今すぐ 1 回実行」を使用して実行される「照会から取り込み」の制限は、5,000 行までです。 これはカスタマイズできません。

グループおよび別名ビルダーで「スケジューリング」を使用して実行される「照会から取り込み」の制限は、20,000 行までです。 この制限は、CLI コマンド show/store populate_from_query_maxrecs を使用してカスタマイズ可能です。

レポート用のドリルダウン・レポート・メニューの変更

デフォルトで、レポートのドリルダウン・メニューには、そのレポートの属性で提供できるランタイム・パラメーターを持つすべてのレポートが組み込まれます。ただし、通常のセキュリティー・ロール制約が課されます。あるレポートのドリルダウン・メニューを任意のレポートに対して無効または有効にするには、次のようにします。

1. レポートを見つけます。「レポート・ビルダー」ファインダー・メニューに移動します。
2. 「ドリルダウン制御」をクリックして、そのレポートの「ドリルダウン制御」パネルを開きます。
3. 無効にするレポートのチェック・ボックスにマークを付け、有効にするレポートのチェック・ボックスをクリアします。
4. 「適用」をクリックします。変更が正常に適用されたことを示すメッセージが表示されます。
5. 完了したら、「完了」をクリックします。

API 割り当て

デフォルトで、Guardium アプリケーションには多くの API 関数をレポートにリンクした設定データが添付されています。これによりユーザーには、GUI を通じてレポート・データからの API への作成済み呼び出しが提供されます。「API 割り当て」を使用して、事前定義された Guardium レポートまたはカスタム・レポートへ追加 API 関数をリンクできます。

リンクされた API 関数の使用に関する詳細については、『GuardAPI 入力の生成』にある資料を参照してください。

1. レポートを見つけます。「レポート・ビルダー」ファインダー・メニューに移動します。
2. 「API 割り当て」 ボタンをクリックして、「API 割り当て」パネルを開きます。このとき、選択したレポートに現在マップされている API 関数が表示されます。
3. 「API 関数」をクリックし、現在の API とレポートのパラメーター・マッピングを示すポップアップ・ウィンドウを表示します。ここでは API パラメーター、API パラメーターが必須かどうか、デフォルト値、そして、現在パラメーターにマップされたレポートのフィールドがあるかどうかが表示されます。

   API パラメーターにリンクされたフィールドがレポート内にない場合は、API 関数をレポートにリンクすることが不適切である場合があります。API パラメーターとレポート・フィールドのマッピングは、GUI と Guardium CLI の両方で行えます。 API パラメーターとレポート・フィールドのマッピングの追加情報については、『GuardAPI 入力の生成』セクションの『GuardAPI パラメーターのドメイン・エンティティーおよび属性へのマッピング』を参照してください。

4. 大なり記号「>」をクリックして、選択した API 関数を、このレポートに割り当てられている現在の関数リストに追加します。
5. 「適用」をクリックして、変更を保存します。

レポート・ポートレットから照会を編集用に開く

1. 編集対象の照会の基になるレポートのレポート・ポートレットを開きます。
2. ツールバーで「このレポートの照会を編集 (Edit this Report's Query)」 をクリックします。この操作には、レポートの基になっている照会を変更する権限が必要です。

- レポート・パラメーター
  パラメーターを使用して、レポートの内容や表示を制御することができます。
- ダッシュボードの作成
  1 つ以上のダッシュボードを作成し、それらにレポートを追加し、外観を構成することができます。
- レポートの表示
  レポートの表示には、ダッシュボードや UI 検索など、いくつかの方法があります。
- レポートの作成
  事前定義レポートがニーズを満たしていない場合は、独自のレポートを作成できます。
- z/OS のレポートの作成
  組み込みレポートとサンプル照会をカスタマイズすることで z/OS データ・ソース用の Guardium レポートを作成する方法について説明します。
- データマート
  データマートはデータウェアハウスのサブセットです。データウェアハウスでは、後から分析およびレポートで使用可能なように、データが汎用的な方式で集約および編成されます。データマートはユーザー定義のデータ分析を始めとして、内容、表示、使いやすさの面で、ユーザーの特定の要求に対応していることが特徴です。

- 監査およびレポート
  Guardium は、収集したデータをドメイン・セットに編成します。 各ドメインには、特定の関心領域 (データ・アクセス権、例外、ポリシー違反など) に関連する異なるタイプの情報が格納されます。
- 照会
  Guardium に付属している多数の定義済み照会の 1 つを使用して、データに関する情報を取得します。照会の作業を行うには、クエリー・ビルダーを使用します。
- ドメイン、エンティティー、および属性
  ドメインは、Guardium が保管しているデータのビューを提供します。
- 事前定義レポートを活用する方法
  カスタム・レポートを最初から作成するのではなく、Guardium アプリケーションの事前定義コンテンツを活用できます。
- データに関する質問方法
  収集したデータに関する質問の定義や変更を行うには、クエリー・ビルダーを使用します。
- 休止状態の表および列のレポート作成方法
  Guardium では、データ設計者と DBA のための機能として、現在使用されていない表やフィールドを見つける機能が提供されます。
- レポートから API 呼び出しを生成する方法
  レポート内の単一行を使用して、またはレポート全体に基づいて、レポートから Guard API 呼び出しを生成します。
- API 呼び出しで定数を使用する方法
  API 関数の呼び出し時に使用する新しいエンティティー属性を作成します。
- カスタム・レポートから API 呼び出しを使用する方法
  API 関数をレポートにリンクし、レポートの各フィールドを API 関数のパラメーターにマップします。
- オプションの外部フィード
  外部フィードを使用すると、Guardium レポート・データを外部データベースに直接送信できます。
- 外部フィードのマッピング
  外部フィードをマップして、Guardium レポート・データを外部データベースに直接送信する方法について説明します。
- 配布レポート・ビルダー
  この中央マネージャー機能により、特定の中央マネージャーに関連付けられているすべてまたは一部の Guardium 管理対象ユニットから、データを自動的に収集することができます。配布レポートは、概要ビューの提供、データ・ソース間のデータの関連付け、およびデータのビューの要約を行うように設計されています。 コレクター間での行レベル・データ収集については、引き続きアグリゲーターを使用します。
- 配布レポートの作成方法
  Guardium には、特定の Guardium 中央マネージャーに関連付けられている一部またはすべての Guardium 管理対象ユニットからデータを自動収集する機能が用意されています。

レポート・パラメーター

パラメーターを使用して、レポートの内容や表示を制御することができます。

レポート・パラメーターには 2 つのタイプがあります。

- *ランタイム・パラメーター* は、照会条件で使用される値を提供します。すべての照会にはデフォルトのランタイム・パラメーター・セットがあり、レポートで使用される照会には任意の数のランタイム・パラメーターを定義できます。
- *表示パラメーター* には、レポートの物理的特性を記述します。例えば、グラフィカル・レポートに凡例やラベルを組み込むかどうか、あるいはある要素にどの色を使用するかといったことです。すべての表示パラメーターには、レポートを定義するときの初期設定が与えられます。

レポート・パラメーターを設定するには、次のようにします。

1. レポート内の選択項目から「レポート・パラメーターの構成 (Configure Report Parameters)」をクリックします。アイコン  を参照してください。
2. パネルでは、実行するタスクでの必要性に応じて、提示されるボックスにランタイム・パラメーターと表示パラメーターを入力します。
3. 「保存」をクリックします。
4. レポートを表示するには、「マイ・ダッシュボード」に移動します。

標準ランタイム・パラメーター

すべてのレポートにおいて、以下のランタイム・パラメーターが存在します。

ランタイム・パラメーター	デフォルトと説明
QUERY_FROM_DATE	新規レポートの場合、なし。デフォルト・レポートによって異なります。どの場合でも、レポートの開始日は必須です。
QUERY_TO_DATE	新規レポートの場合、なし。デフォルト・レポートによって異なりますが、ほとんどすべてデフォルトは NOW です。これはレポートの終了日であり、どの場合でも必須です。
REMOTE_SOURCE	なし。中央マネージャー環境では、リモート・データ・ソースのリストにある Guardium® システムを選択してその管理対象ユニット上でレポートを実行できます。
SHOW_ALIASES	なし (システム共通のデフォルトが使用されることを意味します)。「オン」を選択すると常に別名が表示され、「オフ」を選択すると別名は表示されなくなります。「オン」または「オフ」 ボタンのどちらかを使用してから、デフォルト・ボタンを選択すると、システム共通のデフォルト (管理者によって制御される) に戻ります。

ランタイム・パラメーター名のリストを返す GuardAPI レポート・コマンド

GuardAPI コマンド list_parameter_names_by_report_name を使用します。この関数は、レポート名を入力パラメーターとして取り、そのレポートのランタイム・パラメーター名のリストを返します。

親トピック: レポート

ダッシュボードの作成

1 つ以上のダッシュボードを作成し、それらにレポートを追加し、外観を構成することができます。

始める前に

定期的に表示するレポートの編成方法について検討します。レポートは 1 つのダッシュボードで表示しますか、それとも複数のダッシュボードで表示しますか。レポートをグループ化し順序付ける際に、レポートの目的または重要度のいずれを基準としますか、あるいは何か別のアプローチを使用しますか。ダッシュボードの再配置や新規作成は、いつでも行うことができます。

このタスクについて

手順

1. 「マイ・ダッシュボード」 > 「新規ダッシュボードの作成」をクリックして、新規ダッシュボードを開きます。
2. 「名前」フィールドに記述名を入力します。この名前は、メニュー内のダッシュボードのリストで使用されます。
3. 「レポートの追加」  をクリックすると、使用可能なレポートのリストが表示されます。 特定のレポートをお気に入りとして指定した場合は、「お気に入り」ボックスにチェック・マークを付けると、それらのレポートのみのリストを表示できます。グラフィカル・レポートのみを表示したい場合は、「グラフのみ」ボックスにチェック・マークを付けます。
4. 「レポートの追加」ダイアログには、指定された基準を満たすすべてのレポートのリストが表示されます。レポートのリストを参照することも、「フィルター」フィールドに文字列を入力することもできます。 文字を入力するにつれて、レポートのリストが更新されます。
5. レポートのタイトルをクリックすると、そのレポートがダッシュボードに追加されます。必要な数だけレポートを追加してください。レポートを追加し終えたら、「閉じる」をクリックします。

タスクの結果

選択されたいくつかのレポートに簡単にアクセスできるダッシュボードが用意できました。

次のタスク

ダッシュボードの外観をレビューします。ダッシュボードが使いやすいか、必要な情報を簡単に検索できるかを確認してください。問題がある場合は、さらに構成することができます。
親トピック: レポート

ダッシュボードの構成

ダッシュボードができるだけ便利になるように、外観のいくつかの側面を構成することができます。

このタスクについて

レポートの使用方法について検討します。どのような配置にすると目標を達成しやすいでしょうか。いろいろ変更してみてください。

手順

1. レポートを再配置します。レポートを移動するには、レポートのタイトル・バーにカーソルを置いて、新しい場所にドラッグします。
2. 新たな列数を選択するには、「列数」エリアで「1」、「2」、または「3」をクリックします。デフォルトでは、レポートは 2 列で表示されます。各レポートにもっとスペースが必要な場合は、「1」をクリックすると、レポートをダッシュボードの最大幅にしたときの表示を確認できます。 より多くのレポートを一度に表示したい場合は、3 列を試してみてください。
3. レポートのサイズを変更します。サイズ変更アイコンをドラッグして、レポートの長さや幅を変更します。レポートの幅を調整すると、その列にあるすべてのレポートで新しい幅が採用されます。列数を変更すると、すべての列はそれぞれのデフォルト幅に戻ります。

ダッシュボードの使用

ダッシュボードにレポートを追加して、外観をカスタマイズするには、以下のステップを実行します。

このタスクについて

ダッシュボードは、「ペインに追加」および「マイ・レポートに追加 (Add to My Reports)」の代わりに使用されます。

手順

1. ナビゲーションでダッシュボード・アイコンをクリックします。
2. 次に「新規ダッシュボードの作成」をクリックします。
3. 「レポートの追加」をクリックして、アクセス可能なすべてのレポート (作成した新規レポートを含む) から、レポートを選択します。
4. フィルタリングを利用すると、関心のあるレポートを素早く見つけることができます。
5. レポート名をクリックして、ダッシュボードに追加します。単に各レポートを選択するだけで、必要な数のレポートをダッシュボードに追加できます。
6. レイアウトを選択して、ダッシュボードをカスタマイズします。デフォルトは 2 列です。1 列 - レポートではダッシュボードの幅が想定されます。2 列 - レポートではダッシュボードの半分の幅が想定されます。3 列 - レポートではダッシュボードの 3 分の 1 の幅が想定されます。
7. 画面内のレポートを移動して、ダッシュボードをカスタマイズします。グラフをカスタマイズするには、  アイコンを使用します。
8. 特定のレポートをお気に入りとして指定するには、  アイコンを選択します。レポートをダッシュボードに追加する場合は、お気に入りに基づいてフィルタリングするか、グラフに基づいてフィルタリングします。
9. 「編集」アイコンをクリックして、ダッシュボードに名前を付けます。

10. ダッシュボードを削除するには、「削除」アイコン  をクリックします。

レポートの表示

レポートの表示には、ダッシュボードや UI 検索など、いくつかの方法があります。

レポートは、以下のようにいくつかの方法で表示できます。

- レポートをダッシュボードに保存した場合は、ダッシュボードを開いてレポートを表示します。
- レポートをダッシュボードに追加できます。ダッシュボードを開き、「レポートの追加」をクリックして、リストからレポートを選択します。
- レポート・ライフサイクルのカテゴリーにいくつかのレポートがリストされます。
- 最も関連性の高いライフサイクルの下にいくつかのレポートがリストされます。
- ユーザー・インターフェース (UI) の検索機能を使用して、レポートを検索できます。バナーで、検索ボックスの横のドロップダウン・リストから「ユーザー・インターフェース」を選択します。検索ボックスにレポートの名前を入力します。数文字入力すると、結果が表示され始めます。結果のリストからレポートを選択します。

以下の選択項目 (およびアイコン) では、レポートの編集や構成が許可されます。

- このレポートの照会を編集 
- 今すぐ 1 回実行する特別プロセス - GuardAPI コマンドを呼び出す場合に使用します。 
- 新規ウィンドウで開く 
- レポートの列の構成 
- ランタイム・パラメーターの構成 - ランタイム・パラメーターは、照会条件で使用される値を提供します。すべての照会にはデフォルトのランタイム・パラメーター・セットがあり、レポートで使用される照会には任意の数のランタイム・パラメーターを定義できます。 
- お気に入りに追加 
- リフレッシュ 

列を非表示にすることができます。列アイコンをクリックして、非表示にする列のチェック・ボックスをクリアしてください。

任意の列の内容に基づいてレポート・データをソートできます。ソートの基準となる列のタイトルをクリックしてください。順序を逆にするには、タイトルをもう一度クリックします。ソートは常に実際のデータ値に対して実行されるため、定義されている別名は無視されます。

レポートの表示中に、そのレポートを印刷することができます。「エクスポート」 > 「完全印刷用レポート」をクリックすると、レポートの印刷用コピーが新規タブで開きます。 新規タブでプリンター・アイコンをクリックして、レポートを印刷します。レポートを印刷するもう一つの方法として、レポートを PDF ファイルにエクスポートし、その PDF ファイルを印刷することができます。
注: PDF テキストが小さすぎて読めない場合は、ページの幅を考えると、PDF レポートを横方向に拡大するのは物理的限界があります。PDF レポートの各行は 1 行に収まる必要があるため、データに合うように書体サイズが変更されますが、すべてのデータを表示するために非常に小さい書体サイズになる可能性があります。

グラフィカル・レポートをカスタマイズするには、「グラフのカスタマイズ」アイコンをクリックします。選択肢としては、データから線グラフへの変換、X 軸と Y 軸の方向の変更、レポートから円グラフまたは積み上げ縦棒グラフへの変換があります。

Oracle の情報を表示するレポートを表示する場合、疑問符 (?) 文字が使用されることがあります。これは、ログイン情報を使用できないことをビューアーに通知するためのものです。さらに、Oracle の情報を表示するレポートを表示する場合、数字「-1」が現れた箇所は、影響を受けたレコードの数が不明であること意味します。すべての Oracle セッションは記録されます。ログインが失敗したセッションであっても記録されます。

問題: IBM Security Guardium レポートで「OS ユーザー」フィールドが空になる

UNIX/Linux プラットフォームの場合の注記

リモート接続:「OS ユーザー」は、データベースに接続するための必須フィールドではありません。したがって、ログイン・パケットでこのフィールド値を送信するかどうかは、データベース・クライアント次第です。 OS ユーザー情報が送信されなければ、このフィールドは空になります。クライアント接続文字列にプロセス・オーナーに関する情報が含まれている場合、その情報を使用して「OS ユーザー」フィールドにデータが設定されます。

ローカル接続: ローカルで実行される接続にも同じ制限事項が適用されます。ただし、データベースへの接続がローカルで行われる場合、Guardium は、UID チェーンを有効にすることにより OS ユーザー情報を識別する方法を提供します。UID チェーンには S-TAP の追加オーバーヘッドが伴う可能性があるため、必要に応じてケース・バイ・ケースで検討する必要があります。

UID チェーンは、EXIT プロトコルによってサポートされます (Db2 出口には、特定のパッチ・レベルが必要であることに注意してください)。

MongoDB、Teradata、および Sybase ASE (実際の IP を使用) では、UID チェーンが ATAP によってサポートされます。

Windows プラットフォーム

リモート接続:「OS ユーザー」は、データベースに接続するための必須フィールドではありません。したがって、ログイン・パケットでこのフィールド値を送信するかどうかは、データベース・クライアント次第です。 OS ユーザー情報が送信されなければ、このフィールドは空になります。

ローカル接続: Windows プラットフォームは、データベースに接続したプロセスを実行している OS ユーザー (プロセス・オーナー) を常に取得します (Windows では UID チェーンは不要です)。

- レポートのリフレッシュ
  一部のレポートは、データを自動的にリフレッシュするように構成されています。 その他のレポートでは、UI を使用してデータを手動でリフレッシュできます。
- レポートのエクスポート
  レポートを PDF ファイルまたはコンマ区切り値のファイルにエクスポートできます。
- ドリルダウン・レポートの表示
  多くのレポートが、より細かいデータを提供するドリルダウン・レポートにアクセスできるようになっています。

親トピック: レポート

レポートのリフレッシュ

一部のレポートは、データを自動的にリフレッシュするように構成されています。 その他のレポートでは、UI を使用してデータを手動でリフレッシュできます。

自動的にリフレッシュするよう構成されているレポートを表示した場合、そのレポートの丸矢印リフレッシュ・アイコンの色は緑です。これはレポートが自動的にリフレッシュすることを示します。

ある時点でそのレポートへの変更がもう行われない場合は、レポートはリフレッシュを停止し、リフレッシュ・アイコンの色は緑から赤に変わります。色が変化する時点は、GUI セッションのタイムアウト時間 (これは CLI コマンド「show session timeout」を実行すると分かる) の半分に等しい時点です。

例えば、セッション・タイムアウトがデフォルトの 900 秒である場合、「リクエスト・レート」レポートの丸矢印リフレッシュ・アイコン  は、450 秒間は緑色であり、その後、赤色に変わります。

レポート・データを手動でリフレッシュするには、以下のようにいくつかの方法があります。

- ツールバーの「リフレッシュ」  をクリックします。
- 任意のツールバー・ボタンを使用して、レポートの印刷、レポート・データのダウンロード、またはレポートの PDF ファイルへの書き込みを行います。レポート・データはこれらのアクションを実行する前にリフレッシュされます。
- refreshRate パラメーター値を設定することによって、周期的なリフレッシュのための時間間隔を設定します。このタスクを実行するには次のようにします。
  - レポート・ツールバーの「カスタマイズ」  をクリックします。
  - 「構成」ダイアログで、「refreshRate」パラメーターを、次に行うレポート・データの更新までの秒数に設定します。デフォルト値のゼロは、レポート・データをスケジュール・ベースでリフレッシュしないことを表します。
  - 「OK」をクリックします。

レポートのカスタマイズ

ユーザーが「レポートのカスタマイズ (Report Customization)」を使用してレポートを編集したり変更したりする場合、ユーザーは「リフレッシュ」を手動でクリックする必要があります。 自動リフレッシュはありません。

UI のカスタマイズ - 「新しいライフサイクル (New Life Cycle)」ダイアログと「新しいグループ」ダイアログでは、グループの深度が最大で 5 レベルに制限されているため、グループ名が長くても、すべてのレベルのグループ名とノード項目テキストがナビゲーション・ペインに表示されます。

UI のカスタマイズ - 「新しいライフサイクル (New Life Cycle)」ダイアログと「新しいグループ」ダイアログのテキスト・ボックスにユーザーが「<」または「>」を入力すると、名前に特殊文字 < または > を含めることができないことを示すポップアップ・メッセージが表示され、「OK」ボタンが使用不可になります。

UI のカスタマイズ - 「新しいライフサイクル (New Life Cycle)」ダイアログと「新しいグループ」ダイアログでは、ユーザーがテキスト・ボックスに入力できる文字は最大 50 文字です。

親トピック: レポートの表示

レポートのエクスポート

レポートを PDF ファイルまたはコンマ区切り値のファイルにエクスポートできます。

レポートの内容を PDF ファイルにエクスポートし、そのファイルを保存または表示することができます。レポートのツールバーで、「エクスポート」 > 「PDF 形式でダウンロード」をクリックすると、PDF コピーが作成されます。プロンプトに従って、ファイルを保存または表示してください。

大きな PDF ファイルを生成すると、処理中に UI がタイムアウトになる可能性があります。大きな PDF ファイルを生成する予定の場合は、この処理を監査プロセスの一部として行うか、UI のタイムアウト値を大きくして、この問題を回避することを検討してください。

レポートの内容をコンマ区切り値 (csv) ファイルにエクスポートすることもできます。レポート内のすべてのレコード (レポート全体)、または表示レコードのみ (現在表示されているデータ) をエクスポートできます。

レポートのツールバーで、「エクスポート」 > 「レコードをすべてダウンロード」または「エクスポート」 > 「表示レコードのダウンロード」をクリックします。結果を保存することも、結果を表示するアプリケーションを選択することもできます。

注:

親トピック: レポートの表示

ドリルダウン・レポートの表示

多くのレポートが、より細かいデータを提供するドリルダウン・レポートにアクセスできるようになっています。

表形式レポートでドリルダウン・アクションが使用できる場合は、グリッドの行を右クリックすると、使用可能なドリルダウン・アクションを示すコンテキスト・メニューが表示されます。

ドリルダウン・レポートとして使用可能にするには、以下のようにします。

- ドリルダウン・レポートのすべてのランタイム・パラメーターは、表示されているレポートから使用できなければなりません。
- セキュリティー・ロールが割り当てられている場合、ドリルダウン・レポートへのアクセス権が必要です。

レポート用のドリルダウン・レポート・メニューの変更

デフォルトで、レポートのドリルダウン・メニューには、そのレポートの属性で提供できるランタイム・パラメーターを持つすべてのレポートが組み込まれます。ただし、通常のセキュリティー・ロール制約が課されます。あるレポートのドリルダウン・メニューを任意のレポートに対して無効または有効にするには、次のようにします。

1. レポートを見つけます。「レポート・ビルダー」ファインダー・メニューに移動します。
2. 「ドリルダウン制御」をクリックして、そのレポートの「ドリルダウン制御」パネルを開きます。
3. 無効にするレポートのチェック・ボックスにマークを付け、有効にするレポートのチェック・ボックスをクリアします。
4. 「適用」をクリックします。変更が正常に適用されたことを示すメッセージが表示されます。
5. 完了したら、「完了」をクリックします。

親トピック: レポートの表示

レポートの作成

事前定義レポートがニーズを満たしていない場合は、独自のレポートを作成できます。

始める前に

このレポートのベースとなる照会、およびその照会のドメインを選択します。新規照会を作成しなければならない場合は、その照会をベースとするレポートを作成する前に、新規照会を作成してください。照会とレポートには違いがあることに注意してください。照会は、収集したデータから取得される情報セットを記述します。レポートは、照会によって返されたデータの表示方法を記述します。照会の作成について詳しくは、クエリー・ビルダーの使用を参照してください。ドメインの処理について詳しくは、ドメイン、エンティティー、および属性を参照してください。

このタスクについて

レポートをコピーしてそれを変更する方が、最初から作成するよりも簡単であることがわかります。

手順

1. 「レポート」 > 「レポート構成ツール」 > 「レポート・ビルダー」をクリックして、「レポート・ビルダー」ファインダーまたはフィルター・メニューを開きます。この時点でドメインも照会も選択せずに「検索」を選択すると、すべての照会をリストしたメニューが表示されます。照会を選択し、アイコン (「新規レポートの追加」、「変更」、「コピー」、または「削除」) を使用して、照会を処理します。
2. 「レポート・ビルダー」ファインダー・メニューから、「新規」をクリックします。
3. 「レポートの作成」メニューが表示されます。照会を選択し、レポートに名前を付けます。「次へ」をクリックします。
4. 次の画面には、選択した照会の表の列が返されます。カスタマイズするか、そのまま使用してください。「次へ」をクリックします。
5. 「レポート属性」メニューが表示されます。 レポート・タイプとして、表またはグラフのいずれかを選択します。「次へ」をクリックします。
6. その後、「保存」をクリックして、レポートを作成のために実行依頼します。 データが正常に保存されたことを示す確認画面が表示されます。

次のタスク

このレポートをダッシュボードに組み込む場合は、ダッシュボードを開き、「レポートの追加」をクリックして、リストからこのレポートを選択します。
親トピック: レポート

z/OS のレポートの作成

組み込みレポートとサンプル照会をカスタマイズすることで z/OS データ・ソース用の Guardium レポートを作成する方法について説明します。

z/OS データ・ソースのレポートを作成するプロセスは他のデータベースでも同じですが、メインフレームの概念と Guardium のレポート・エンティティーおよび属性の間には必ずしも直接的な対応はありません。 監査員とメインフレーム担当者がコミュニケーションを取りやすいように、このセクションではメインフレーム・イベント・データと Guardium のエンティティーおよび属性とのマッピングを概説しています。カスタマイズ可能ないくつかの組み込みレポートがあり、この情報では標準的な監査シナリオに役立つ追加の照会について説明しています。

親トピック: レポート
関連概念:
ドメイン、エンティティー、および属性
クエリー・ビルダーの使用
エンティティーおよび属性

データマート

データマートはデータウェアハウスのサブセットです。データウェアハウスでは、後から分析およびレポートで使用可能なように、データが汎用的な方式で集約および編成されます。データマートはユーザー定義のデータ分析を始めとして、内容、表示、使いやすさの面で、ユーザーの特定の要求に対応していることが特徴です。

この機能により可能になる事項:

- データマートの定義と生成。
- 妥当な応答時間ですべてのユニットからの要約データと分析データを集約して概要ビューを有効にします。
- Guardium アグリゲーターのオンライン・レポートのパフォーマンスが向上します。
- パターン、トレンド、および異常値などを把握するための、対話式の分析機能を提供します。
- データのレベルの縮小および拡大を可能にします。

データマートは、Guardium のすべての事前定義レポートに対して実用的で効率的です。過負荷、完全スキャン、およびローパフォーマンスを回避するために、データを事前に準備します。

「データマート構成」アイコンは、すべての事前定義レポートで使用することができます。

利点のハイライト:

- データ分析の全ライフサイクルをサポートする Guardium 分析機能を提供します。
- 分析プロセスはクエリー・ビルダーおよびピボット・テーブル・ビルダーから開始されます。ここでは、ユーザーは自身のデータ分析についてのニーズを定義し、「データマートとして設定」します。
- データマート抽出プログラムは、指定されたスケジュールに応じてバッチで実行されます。 データは要求された間隔に応じて時間、日、週、月ごとに要約され、要約の結果は Guardium 分析データベース内の新しい表に保存されます。
- ユーザーは、標準的なレポートと監査プロセスを使用してこのデータにアクセスできるようになります。データマート抽出データは、DM ドメインで使用可能です。エンティティー名は、データマート・データに対して指定された新しい表の名前に従って設定されます。ユーザーは、標準のクエリー・ビルダーおよびレポート・ビルダーを使用して、デフォルトの照会を複製し、照会およびレポートを編集し、ポートレットを生成してペインに追加することができます。
- データの要約により、データ・ボリュームは大幅に縮小します。 正規化されておらず、かつ事前計算が行われた表にデータ分析を格納することにより、多数の表の結合を除去できます。
- 新しい Guardium 分析表用の標準の統合ユーティリティーを使用することにより、企業ビューがサポートされます。大量の詳細な行データが統合階層の上位レベルに存在する場合は、特定のモジュールの統合を可能にする選択的な統合機能を構成して、分析データのみを統合することができます。

データマート・ビルダーには、クエリー・ビルダー、レポート結果およびピボット・テーブル・ビューからアクセスすることができます。

「データマートとして設定」アイコンを選択します。このボタンが使用可能なのは、保存操作後のみです。

画面にアクセスできるのは、データマートの作成アクセス権 (ユーザー・ロール・アクセス権) を持つユーザーです。新しいデータマートとして設定ボタンは、適切なアクセス権を持つユーザーにのみ表示されます。

データマートの永続性 - オリジナルの照会、レポート、ピボット・テーブルへの変更はデータマートには影響しません。作成時に、元になる分析定義のスナップショットもデータマートと一緒に保存されるためです。

データマートがピボット・テーブルに基づいている場合、抽出プロセスでは「合計」行 (列の合計) は計算されず、「列のパーセント」もサポートされません。

「データマート定義」プロセスでは、データマート定義に加えて、以下も作成されます。

- 新規ドメインおよびエンティティー
- デフォルト照会
- デフォルトのレポートおよびポートレット
- 抽出されたデータが格納される、新しい「DATAMART」データベース内の新しいデータマート表

データマート – 照会およびレポート・ビルダー

データマート定義プロセスでは、新規ドメイン、エンティティー、デフォルトの照会およびレポートが作成されます。デフォルトの照会およびレポートには、「レポートのビルド」メニューからアクセスできます。

データマートをクリックすると、照会ファインダー GUI が開きます。「照会」、「レポート」、および「エンティティー」の各フィールドは、データマート・ドメイン (DatamartDefinition.DOMAIN_PREFIX で始まるドメイン名) のみをフィルタリングします。

レポート・ビルダー GUI: デフォルトのデータマートのレポートおよびデータマート・ドメインに関連する他のすべてのレポートが、レポート・ビルダー GUI で使用できます。

以下の手順を行います。

1. admin ユーザーとして「データマート」アイコン  を選択します。
2. 「新規」を選択して、新規データマートを作成するか、以前に作成したデータマートのリストからデータマートを選択します。
3. データマート名および表名 (デフォルトは DM) の入力を求めるフィールドに入力します。時間間隔を指定し、カレンダー・アイコンから「初始動」の時刻を選択します。「記述」の入力はオプションです。
4. スケジューラーを使用して、この機能の実行時期をスケジュールします (「今すぐ 1 回実行」)。
5. 「ロール」セクションを使用して、適切な権限を持つユーザーだけに「データマート」を制限します。
6. 構成を保存します。

   注: 元の照会/レポートを変更しても、既存のデータマートには影響しません。
   注: データマートの抽出を初めて実行する場合 (スケジュール実行または「今すぐ 1 回実行」)、時間間隔に基づいて、初始動の日付から現在時刻までのデータが抽出されます。次の期間開始が DM_EXTRACTION_STATE 表に保存されます。次回の実行時に、次の期間開始から開始されるデータが抽出されます。次の期間開始より前にデータマート抽出を実行すると、その期間は抽出によって既に処理されているため、データマート抽出は「空」として表示されます。次の期間開始より前のデータを抽出するには、古いデータをリストアしてから、データマートをもう一度実行してください。

一元管理およびデータマート

一元管理環境では、構成は、管理対象ユニットに自動的に配布されます。

管理対象ユニットでは、抽出スケジュールを指定変更できます。

中央マネージャーが複数の場合は、エクスポート/インポート機能を使用してデータマート定義をコピーすることができます。

中央マネージャーの配布画面に、データマートの抽出スケジュールを追加します。

データマート抽出

以下のデータが抽出されます。

1. エクスポート: 例外ログ - Guardium によってキャプチャーされた例外/エラーの詳細を示します。このログには、例外/エラーの説明、ユーザー名、ソース・アドレス、データベース・プロトコルなどが記録されます。
2. エクスポート: セッション・ログ - データ・ソースのセッション (ログインからログアウト) に関する詳細が記録されます。このログに記録される情報には、セッション開始とセッション終了のタイム・スタンプ、セッションの OS とデータベース・ユーザー、ソース・プログラムなどが含まれます。
3. エクスポート: 終了したセッション・ログ - セッションは長期間に及ぶ場合があります。抽出は 1 時間ごとに行われます。 このログは、開始時刻 (単位: 時) より後に終了したセッションを送信します。
4. エクスポート: アクセス・ログ - 接続情報の詳細と 1 時間ごとのアクティビティーの要約が記録されます。 このログに記録される情報には、OS およびデータベース・ユーザー、成功した SQL と失敗した SQL、クライアント IP とサーバー IP などが含まれます。
5. エクスポート: 完全な SQL - このログには、実行された SQL の詳細が記録されます。このログに記録される情報には、完全な SQL、影響されるレコード、セッション ID などが含まれます。
6. エクスポート: 異常値リスト - このログには異常値が記録されます。 このログに記録される情報には、サーバー IP、データベース・ユーザー、異常値タイプ、データベースなどが含まれます。
7. エクスポート: 異常値の概要 - このログには、1 時間ごとの異常値の概要が記録されます。このログに記録される情報には、サーバー IP、データベース・ユーザー、データベースなどが含まれます。
8. エクスポート: グループ・メンバー - すべてのグループ・メンバーのログが含まれます。 このログには、グループ・タイプ、グループの記述、グループ・メンバー、およびタプル・フラグが含まれます。
9. エクスポート: エクスポート抽出ログ – 名前が「エクスポート:」で始まるすべてのエクスポート・ファイルまたはコピー・ファイルに関連するデータのログが含まれます。
10. エクスポート: ポリシー違反 – ポリシー違反は、ポリシー・ルールが起動されるごとにログに記録されます。このログには、データベース・ユーザー、ソース・プログラム、アクセス・ルールの記述、および SQL 文字列全体などログに記録された違反に関する詳細が含まれます。
11. エクスポート: バッファー使用状況モニター - スニファーのバッファー使用状況の統計の詳細を提供します。
12. エクスポート: 脆弱性診断結果 - 脆弱性診断結果を示します。
13. エクスポート: ポリシー違反 - 詳細 – 「エクスポート抽出ログ」と同じですが、オブジェクト/動詞タプルが含まれます。いずれか一方ログだけを使用することを推奨します。
14. エクスポート: アクセス・ログ - 詳細 – アクセス・ログと同じですが、アプリケーション・イベント・エンティティーのフィールド (イベント・ユーザー名、イベント・タイプ、イベント値 (文字列)、イベント値 (数値)、イベントの日付) も含まれます。「アクセス・ログ」または「アクセス・ログ – 詳細」のいずれか一方を使用し、両方を同時に使用しないことを推奨します。
15. エクスポート: ディスカバーされたインスタンス - データベース・インスタンスをディスカバーする S-TAP ディスカバリー・アプリケーションの結果を提供します。
16. エクスポート: ディスカバーされたデータベース
17. エクスポート: 分類結果
18. エクスポート: データ・ソース
19. エクスポート: S-TAP 状況
20. エクスポート: インストール済みのパッチ
21. エクスポート: システム情報
22. エクスポート: ユーザー – ロール
23. エクスポート:分類プロセス・ログ
24. エクスポート:異常値リスト - 拡張
25. エクスポート:時間単位の異常値概要 - 拡張

データマート名	レポート・タイトル	ユニット・タイプ	データマート ID
エクスポート:アクセス・ログ	エクスポート: アクセス・ログ	コレクター	22
エクスポート:セッション・ログ	エクスポート: セッション・ログ	コレクター	23
エクスポート:終了したセッション・ログ	エクスポート: セッション・ログ	コレクター	24
エクスポート: 例外ログ	エクスポート: 例外ログ	すべて	25
エクスポート: 完全な SQL	エクスポート: 完全な SQL	コレクター	26
エクスポート:異常値リスト	Analytic 異常値リスト	すべて	27
エクスポート:時間単位の異常値概要	Analytic 異常値サマリー		
日付別	すべて	28	
エクスポート:抽出ログ	ユーザー定義抽出ログ	すべて	31
エクスポート: グループ・メンバー	エクスポート:グループ・メンバー	すべて	29
エクスポート:ポリシー違反	エクスポート:ポリシー違反	コレクター	32
エクスポート: バッファー使用状況モニター	バッファー使用状況モニター	すべて	33
エクスポート:脆弱性診断結果	セキュリティー・アセスメント・エクスポート	すべて	34
エクスポート:ポリシー違反 - 詳細	エクスポート:ポリシー違反	コレクター	38
エクスポート:アクセス・ログ - 詳細	エクスポート: アクセス・ログ	コレクター	39
エクスポート:ディスカバーされたインスタンス	ディスカバーされたインスタンス	すべて	40
エクスポート:ディスカバーされたデータベース	ディスカバーされたデータベース	すべて	41
エクスポート:分類結果	分類結果	すべて	42

データマート名	レポート・タイトル	ユニット・タイプ	データマート ID
エクスポート:データ・ソース	データ・ソース	中央マネージャー	
スタンドアロン	43		
エクスポート:STAP 状況	S-TAP 状況モニター	コレクター	44
エクスポート:インストール済みのパッチ	インストール済みのパッチ	すべて	45
エクスポート:システム情報	インストール済みのパッチ	すべて	46
エクスポート:ユーザー - ロール	ユーザー - ロール	中央マネージャー	
スタンドアロン	47		
エクスポート:分類プロセス・ログ	分類プロセス・ログ	すべて	48
エクスポート:異常値リスト - 拡張	Analytic 異常値リスト - 拡張	すべて	49
エクスポート:時間単位の異常値概要 - 拡張	Analytic 日付別異常値サマリー - 拡張	すべて	50

問題の要約

データマート・メカニズムは、定義された照会に基づいて Guardium スニッフィング・データを定期的にエクスポートします。

出力ファイルをオンデマンドで外部マシンに書き込むことができます (構成可能)。

抽出ファイルは圧縮されます。

抽出はスケジュール化することができます (デフォルトは 1 時間ごとです)。

抽出ファイルの接頭部は Global_ID とソース・マシンのホストの短縮名です。

抽出ファイルには、列見出し (属性の説明) を含めることができます。

使用法

以下に示す例はいずれも、「エクスポート:例外ログ」データマートの場合の例です。他の抽出の場合は、以下のいずれかに変更します。

"エクスポート:アクセス・ログ"

"エクスポート:セッション・ログ"

"エクスポート:終了したセッション・ログ"

"エクスポート:例外ログ"

"エクスポート:完全な SQL"

"エクスポート:異常値リスト"

"エクスポート:時間単位の異常値概要"

"エクスポート:グループ・メンバー"

"エクスポート:抽出ログ"

"エクスポート:ポリシー違反"

"エクスポート:バッファー使用状況モニター"

"エクスポート:脆弱性診断結果"

"エクスポート:分類結果"

"エクスポート:ディスカバーされたデータベース"

"エクスポート:アクセス・ログ - 詳細"

"エクスポート:ディスカバーされたインスタンス"

"エクスポート:データ・ソース"

"エクスポート:STAP 状況

"エクスポート:インストール済みのパッチ"

"エクスポート:システム情報"

"エクスポート:ユーザー - ロール"

"エクスポート:分類プロセス・ログ

"エクスポート:異常値リスト - 拡張"

"エクスポート:時間単位の異常値概要 - 拡張"

エクスポート抽出は、(データマート・メカニズムにより) システムに事前に定義されており、デフォルトでは無効になっています。エクスポート抽出 (すべてまたは個別) を有効にするには、以下に示すように、grdapi を使用してデータマートをスケジュールする必要があります。これには GUI を使用することもできます。

データマート抽出のためのジョブのスケジュール化:

grdapi schedule_job jobType=dataMartExtraction cronString=”0 1 0/1 ? * 1,2,3,4,5,6,7” objectName=”Export:Exception Log” startTime=”YYYY-MM-DD HH:MM:SS”

startTime を使用して、必要に応じて将来の開始時刻を設定します。またデータマートをすぐに開始したい場合は削除できます。

特定のエクスポート抽出を削除するには、以下を実行します。

スケジュール済みジョブの削除:

grdapi delete_schedule deleteJob="true" jobGroup="DataMartExtractionJobGroup” obname="DataMartExtractionJob_25”

jobname	**ジョブの記述/ オブジェクト名**
DataMartExtractionJob_22	エクスポート:アクセス・ログ
DataMartExtractionJob_23	エクスポート:セッション・ログ
DataMartExtractionJob_24	エクスポート:終了したセッション・ログ
DataMartExtractionJob_25	エクスポート: 例外ログ
DataMartExtractionJob_26	エクスポート: 完全な SQL
DataMartExtractionJob_27	エクスポート:異常値リスト
DataMartExtractionJob_28	エクスポート:時間単位の異常値概要
DataMartExtractionJob_29	エクスポート: グループ・メンバー
DataMartExtractionJob_31	エクスポート:抽出ログ
DataMartExtractionJob_32	エクスポート:ポリシー違反
DataMartExtractionJob_33	エクスポート: バッファー使用状況モニター
DataMartExtractionJob_34	エクスポート:脆弱性診断結果
DataMartExtractionJob_38	エクスポート:ポリシー違反 - 詳細
DataMartExtractionJob_39	エクスポート:アクセス・ログ - 詳細
DataMartExtractionJob_40	エクスポート:ディスカバーされたインスタンス
DataMartExtractionJob_41	エクスポート:ディスカバーされたデータベース
DataMartExtractionJob_42	エクスポート:分類結果
DataMartExtractionJob_43	エクスポート:データ・ソース
DataMartExtractionJob_44	エクスポート:STAP 状況
DataMartExtractionJob_45	エクスポート:インストール済みのパッチ
DataMartExtractionJob_46	エクスポート:システム情報
DataMartExtractionJob_47	エクスポート:ユーザー - ロール
DataMartExtractionJob_48	エクスポート:分類プロセス・ログ
DataMartExtractionJob_49	エクスポート:異常値リスト - 拡張
DataMartExtractionJob_50	エクスポート:時間単位の異常値概要 - 拡張

以下のコマンドを使用して、抽出を使用可能または使用不可にすることができます。

データマートをアクティブに設定:

grdapi datamart_set_active Name=”Export:Exception Log”

データマートを非アクティブに設定:

grdapi datamart_set_inactive Name=”Export:Exception Log”

データマート抽出にヘッダーを組み込み:

ヘッダー行 (列名) を出力 CSV ファイルに組み込むかどうかを決めるには、以下の grdapi を使用します。

grdapi datamart_include_file_header Name=” Export:Exception Log” includeFileHeader=”Yes”

ターゲット・ホストの詳細の設定:

エクスポート抽出のターゲット・ホストを設定するには、以下の grdapi を使用してマシンのホスト、パス、資格情報を設定する必要があります。

grdapi datamart_update_copy_file_info destinationHost=”Machine_Host” destinationPassword=”********” destinationPath=”/where/to/store/” destinationUser=”user” Name=”Export:Exception Log” transferMethod=”SCP” withCOMPLETEfile=false

withCOMPLETEfile パラメーターはオプションです。デフォルト値は true です。true に設定されていると、データ・ファイルが正常に転送された後に、COMPLETE ファイルが送信されます。詳しくは、『COMPLETE ファイル』のセクションを参照してください。

このコマンドの実行中に、ダミー・ファイルがターゲット・マシンに送信されて、接続の詳細が検証されます。これには datamart_validate_copy_file_info grdapi を使用することもできます。

ターゲット・ホストへの接続の検証:

ターゲット・ホストへの接続を検証するには、以下の grdapi を実行してください。

grdapi datamart_validate_copy_file_info destinationHost=”Machine_Host” destinationPassword=”********” destinationPath=”/where/to/store/” destinationUser=”user” transferMethod=”SCP”

事前に定義された「データマート抽出ログ」レポートを使用して抽出ログを追跡できます。 このレポートは、「レポート・ビルダー」画面で使用可能になります。このレポートをペインに追加することもできます。

「データマート抽出ログ」レポートにカスタマイズ・オプションを入力し、以下を定義します。

- Name LIKE の値を入力します: %
- 期間の開始日を入力します >=: YYYY-MM-DD HH:MM:SS (過去の日付を入力します)
- Status Like の値を入力します: %

更新をクリックすると、データマート抽出ログ・レポートはアクティブになり、最新の抽出が表示されます。

スケジューラーの推奨開始時刻

異常値データマートは毎時約 10 分過ぎにスケジュールする必要があります。その時間の前であると、データが準備されていないためです。異常値の処理は、毎時ちょうどに開始されます。

アクセス・ログ、例外ログ、完全な SQL、セッション・ログと終了したセッション・ログは、互いに少し時間を空けてスケジュールする方法が適切です。実行するたびに整合したデータを取得できるようにするためには、セッション・ログと終了したセッション・ログは最後のオブジェクトとしてスケジュールする必要があります。

推奨

ジョブの記述	推奨 cronString	毎時:
エクスポート:アクセス・ログ	0 40 0/1 ? * 1,2,3,4,5,6,7	00:40
エクスポート:セッション・ログ	0 45 0/1 ? * 1,2,3,4,5,6,7	00:45
エクスポート:終了したセッション・ログ	0 46 0/1 ? * 1,2,3,4,5,6,7	00:46
エクスポート: 例外ログ	0 25 0/1 ? * 1,2,3,4,5,6,7	00:25
エクスポート: 完全な SQL	0 30 0/1 ? * 1,2,3,4,5,6,7	00:30
エクスポート:異常値リスト	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10
エクスポート:時間単位の異常値概要	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10
エクスポート:抽出ログ	0 50 0/1 ? * 1,2,3,4,5,6,7	00:50
エクスポート: グループ・メンバー	0 15 0/1 ? * 1,2,3,4,5,6,7	00:15
エクスポート:ポリシー違反	0 5 0/1 ? * 1,2,3,4,5,6,7	00:05
エクスポート: バッファー使用状況モニター	0 12 0/1 ? * 1,2,3,4,5,6,7	00:12
エクスポート:脆弱性診断結果	0 0 2 ? * 1,2,3,4,5,6,7	毎日午前 2 時
エクスポート:ポリシー違反 - 詳細	0 5 0/1 ? * 1,2,3,4,5,6,7	00:05
エクスポート:アクセス・ログ - 詳細	0 40 0/1 ? * 1,2,3,4,5,6,7	00:40
エクスポート:ディスカバーされたインスタンス	0 20 0/1 ? * 1,2,3,4,5,6,7	00:20
エクスポート:ディスカバーされたデータベース	0 20 0/1 ? * 1,2,3,4,5,6,7	00:20
エクスポート:分類結果	0 20 0/1 ? * 1,2,3,4,5,6,7	00:20
エクスポート:データ・ソース	0 0 7 ? * 1,2,3,4,5,6,7	毎日午前 7 時
エクスポート:STAP 状況	0 0/5 0/1 ? * 1,2,3,4,5,6,7	5 分ごと
エクスポート:インストール済みのパッチ	0 0 5 ? * 1,2,3,4,5,6,7	毎日午前 5 時
エクスポート:システム情報	0 0 5 ? * 1,2,3,4,5,6,7	毎日午前 5 時
エクスポート:ユーザー - ロール	0 5 0/1 ? * 1,2,3,4,5,6,7	00:05
エクスポート:分類プロセス・ログ	0 25 0/1 ? * 1,2,3,4,5,6,7	00:25
エクスポート:異常値リスト - 拡張	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10
エクスポート:時間単位の異常値概要 - 拡張	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10

/var/exportdir のパージ

例えばターゲット・マシンのダウンなど何らかの理由でファイル転送が失敗した場合、次の実行で転送を再試行します。バックログは /var/exportdir ディレクトリーに保持されます。 パージ・プロセスにより、1 日を経過したバックログはクリーンアップされます。

COMPLETE ファイル

ファイルの準備ができたことを外部システムに伝えるため、空の COMPLETE ファイルが送信されます。

- ファイルごとに、そのファイルに加えて COMPLETE ファイルも送信されます。COMPLETE ファイル名は [file name]_COMPLETE.gz です。

1762144738_gibm32_EXP_SESSION_LOG_20151028230000_COMPLETE.gz

- このプロセスは同期的なプロセスです。例えば、最初にファイル (SESSION LOG ファイル) が生成されます。次にこのファイルがコピーされ、コピーが完了して初めて COMPLETE ファイルが生成され、コピーされます。

- COMPLETE ファイルは、送信するデータがない場合でも送信されます。

データマートの初始動の変更:

データマートの初始動時刻を変更するには、update_datamart grdapi を使用してください。

grdapi update_datamart Name="Export:Session Log" initial_start=[initial start value]

例えば、次のような場合です。

初始動を現在時刻に設定

grdapi update_datamart Name="Export:Session Log" initial_start=< >

初始動を 2016 年 10 月 1 日に設定

grdapi update_datamart Name="Export:Session Log" initial_start="2016-10-01 00:00:00"

コピー・ファイルのバンドル

複数の CSV エクスポートのデータマートをまとめてバンドルすることができます。このバンドルには、メインデータマートが設定されます。 バンドルに含まれる各データマートが、それぞれに固有のスケジュールに基づいてデータをプルします。メインデータマートはデータを抽出した後、バンドルに含まれるすべてのデータマートからのデータ・ファイルを同じ tar ファイルに含めて宛先サーバーに送信します。メインデータマートは、最新のスケジューリングを使用する必要があります。

例えば、バンドルに「エクスポート: 完全な SQL」、「エクスポート: 例外ログ」、「エクスポート: セッション・ログ」、および「エクスポート: 終了したセッション・ログ」(メインデータマート) が含まれているとします。

このバンドルに推奨されるスケジューリングは以下のとおりです。

ジョブの記述の推奨 cronString。以下に対して毎時:

エクスポート:セッション・ログ 0 45 0/1 ? * 1,2,3,4,5,6,7 00:45

エクスポート:終了したセッション・ログ 0 46 0/1 ? * 1,2,3,4,5,6,7 00:46

エクスポート:例外ログ 0 25 0/1 ? * 1,2,3,4,5,6,7 00:25

エクスポート:完全な SQL 0 30 0/1 ? * 1,2,3,4,5,6,7 00:30

バンドルを作成します。

grdapi datamart_copy_file_bundle action="create" bundle_name=[bundle name] main_datamart_name=[bundle main datamart name]

データマートをバンドルに含めます。

grdapi datamart_copy_file_bundle action="include" bundle_name=[bundle name] datamart_name=[datamart name]

バンドルからデータマートを除外します。

grdapi datamart_copy_file_bundle action="exclude" bundle_name=[bundle name] datamart_name=[datamart name]

バンドルを削除します。

grdapi datamart_copy_file_bundle action="delete" bundle_name=[bundle name]

バンドル情報を取得します。

grdapi datamart_copy_file_bundle action="info" bundle_name=[bundle name]

例:

grdapi datamart_copy_file_bundle action="create" bundle_name="SFE_BUNDLE" main_datamart_name="Export:Session Log Ended"

grdapi datamart_copy_file_bundle action="include" bundle_name="SFE_BUNDLE" datamart_name="Export:Exception Log"

grdapi datamart_copy_file_bundle action="include" bundle_name="SFE_BUNDLE" datamart_name="Export:Full SQL"

grdapi datamart_copy_file_bundle action="include" bundle_name="SFE_BUNDLE" datamart_name="Export:Session Log"

> grdapi datamart_copy_file_bundle action="info" bundle_name="SFE_BUNDLE" main_datamart_name="Export:Session Log" datamart_name=""

ID=0

==========

バンドル名: SFE_BUNDLE

==========

メインデータマート: エクスポート:終了したセッション・ログ

データマート:

エクスポート: 完全な SQL

エクスポート: 例外ログ

エクスポート:セッション・ログ

get_datamart_info grdapi

get_datamart_info grdapi は、詳細なデータマート情報を取得します。

get_datamart_info datamart_name=[Datamart Name]

例:

grdapi get_datamart_info datamart_name="Export:Export Extraction Log"

==========

データマート名: エクスポート:エクスポート抽出ログ

==========

記述:

レポートに基づく: ユーザー定義抽出ログ

ベースとなる照会: ユーザー定義抽出ログ

結果の抽出先: ファイル

初始動: 2016-04-18 09:00:00

作成日: 2016-12-28 18:01:24

時間間隔: 1 時間

アクティブ: true

ファイル名: EXP_DM_EXTRACTION_LOG

ファイルあたりの行数: 500000

ファイル・ヘッダー:「UTC オフセット」、「名前」、「期間の開始」、「期間の終了」、「実行 ID」、「開始時刻」、「終了時刻」、「状況」、「ファイル状況」、「抽出されたレコード」、「詳細」、「タイム・スタンプ」

ファイル・ヘッダーを含む: true

コピー・ファイルの情報

ホスト名: host.com

ユーザー名: admin

ディレクトリー: /local/incoming/

転送方式: SCP

バンドル名:

バンドルのメインデータマート: false

COMPLETE ファイルを送信: false

最終抽出の情報

状態:1

タイム・スタンプ: 2017-01-18 14:50:00

次の期間: 2017-01-18 14:00:00

最終抽出 ID: 0

抽出ログ

タイム・スタンプ: 2017-01-18 14:50:02

抽出状況: OK

開始時刻: 2017-01-18 14:50:00

終了時刻: 2017-01-18 14:50:00

期間の開始: 2017-01-18 13:00:00

期間の終了: 2017-01-18 14:00:00

抽出されたレコード: 26

詳細: SCP 宛先: host.com、ユーザー: admin、パス: /local/incoming/、ファイル: DMv2_gibm32_EXP_DM_EXTRACTION_LOG_20170118180000.gz

期間の最後: true

ファイル名: /var/dump/DATAMART/EXP_DM_EXTRACTION_LOG_20170118180000.csv

バンドル名:

ファイル転送状況: 完了

コメント

==========

完全な SQL データマートは、「全詳細をロギング」または「マスクされた詳細をロギング」が定義され、インストールされている場合のみ機能します。

異常値データマートは、異常値検出が有効な場合のみ機能します。

データマート・スケジューラーがしばらくの間停止しており、データを遡及的に抽出したくない場合、抽出を再実行するようにスケジュールを変更する前に、「データマート構成」画面で適切な「初始動」を設定してください。

ユーザー定義データマート

ユーザー定義データマートを使用して、データを宛先ホストに転送することもできます。データマートのタイプは「ファイル」でなければなりません。また、データマート名は「エクスポート:」で始まり、ファイル・パッチは「EXP_」で始まっていなければなりません。

依存関係

==========

パッチの適用方法:

==========

http://www-01.ibm.com/support/knowledgecenter/SSMPHH_8.2.0/com.ibm.guardium.using.doc/topics/how_to_install_patches.html?lang=en

データマート用の GuardAPI コマンド

grdapi datamart_copy_file_bundle

関数パラメーター:

action - 文字列 - 必須 - 定数値リスト

bundle_name - 文字列 - 必須

datamart_name - 文字列

main_datamart_name - 文字列

grdapi datamart_include_file_header

関数パラメーター:

includeFileHeader - 文字列 - 必須 - 定数値リスト

Name - 文字列 - 必須

grdapi datamart_set_active

関数パラメーター:

Name - 文字列 - 必須

grdapi datamart_set_inactive

関数パラメーター:

Name - 文字列 - 必須

grdapi datamart_update_copy_file_info

関数パラメーター:

destinationHost - 文字列

destinationPassword - 文字列

destinationPath - 文字列

destinationUser - 文字列

Name - 文字列 - 必須

transferMethod - 文字列 - 定数値リスト

withCOMPLETEfile - ブール値

grdapi datamart_validate_copy_file_info

関数パラメーター:

destinationHost - 文字列 - 必須

destinationPassword - 文字列 - 必須

destinationPath - 文字列 - 必須

destinationUser - 文字列 - 必須

transferMethod - 文字列 - 定数値リスト

grdapi update_datamart

関数パラメーター:

Comment - 文字列

initial_start - 日付

Name - 文字列 - 必須

grdapi get_datamart_info

関数パラメーター:

datamart_name - 文字列 - 必須

isExtended - ブール値

親トピック: レポート

監査およびレポート

Guardium® は、収集したデータをドメイン・セットに編成します。 各ドメインには、特定の関心領域 (データ・アクセス権、例外、ポリシー違反など) に関連する異なるタイプの情報が格納されます。

すべてのドメインおよびその内容については、付録『ドメイン、エンティティー、および属性』を参照してください。

ドメインごとに別個のクエリー・ビルダーがあり、各クエリー・ビルダーへのアクセスはセキュリティー・ロールで制御されます。ドメインに関係なく、すべての照会の作成には同じ汎用クエリー・ビルダー・ツールが使用されます。 照会の作成方法について詳しくは、『照会』を参照してください。

ユーザーは、標準のドメイン・セットに加えて、Guardium アプライアンスにアップロード可能な情報を格納するカスタム・ドメインを定義できます。 例えば、企業環境に、総称データベース・ユーザー名 (hr23455、qa4872 など) を実際の人名 (Paula Smith、John Doe など) に関連付ける表があるとします。 その表がアップロードされると、カスタム・ドメインから Guardium レポートに実名を表示できます。 カスタム・ドメインの定義方法および使用方法について詳しくは、『外部データ相関』を参照してください。

親トピック: レポート

照会

Guardium に付属している多数の定義済み照会の 1 つを使用して、データに関する情報を取得します。照会の作業を行うには、クエリー・ビルダーを使用します。

データについて質問する (例えば、週末の間に特定のデータベースを更新するすべてのクライアントについて尋ねる) には、照会を使用します。

照会は、レポートとは異なります。照会がデータ・セットを記述するのに対し、レポートは、照会によって返されたデータがどのように表されるかを記述します。

照会が完了したら、レポートを使用して、照会結果を表示します。レポートは通常は表形式で示されますが、レポートのレイアウトは自由にカスタマイズできます。

照会を使用するには、「順守」 > 「カスタム・レポート作成」 > 「カスタム・クエリー・ビルダー」をクリックしてクエリー・ビルダーを開きます。照会するドメインを選択し、メイン・エンティティーを選択し、さらに、必要に応じて照会を使用します。

定義済み照会を変更することはできませんが、照会のコピーを作成し、そのコピーを変更することができます。

メイン・エンティティー

照会に関して選択したメイン・エンティティーによって、以下のことが決まります。

- レポートの詳細レベル。 レポートに含まれるメイン・エンティティーのオカレンスごとに、1 行のデータがあります。エンティティー階層内でのメイン・エンティティーのロケーションは、 どの値が表示可能になるかという点で重要です。メイン・エンティティーより下にあるエンティティーの属性は、 カウント可能ですが、表示されません (各行に多数のオカレンスがある可能性があるため)。この詳細レベルを選択するには、「カウントでソート」チェック・ボックスにチェック・マークを付けます。

- 総数は、レポートの当該行に含まれるメイン・エンティティーのインスタンス数であり、レポートの最終列として追加されます。 レポートのカウント列を追加またはドロップするには、「カウントの追加」チェック・ボックスをクリックします。これにより、照会やレポートのパフォーマンスが向上する場合があります。
- レポート内で値ごとに 1 行で表示する機能を追加またはドロップする (結果的に、 照会やレポートのパフォーマンスが向上する場合がある) には、「Distinct の追加」チェック・ボックスをクリックします。 この選択により、圧縮されたレポートが生成されます。
- パーティションの最適化はデフォルトで有効にされており、パーティション化されたデータベース表での照会のパフォーマンスが向上します。Guardium V10.1.2 以降では、「パーティションの最適化」チェック・ボックスを選択解除することで、この機能を無効にできます。IBM サポートからの指示がない限り、パーティションの最適化を無効にしないでください。
- レポートの行を選択するために「期間開始」および「期間終了」ランタイム・パラメーターとの対比が行われる時間フィールド。クエリー・ビルダーは、(パラメーターの中でも特に) メイン・エンティティーを使用して、「期間開始」値および「期間終了」値の定義時に使用される時間フィールドを決定します。これは、長期実行セッションの場合 (プールされたセッションがアプリケーション・サーバーによって開かれたままである場合など) に重要になることがあります。 適用可能な場合は「アクセス期間」エンティティーの「期間の開始」/「期間の終了」が使用され、それ以外の場合はメイン・エンティティーに従って期間の値が選択されます。
  - セッション - 使用されるタイム・スタンプは、セッション・エンティティーに対する最後の更新になります。
  - セッション開始 - セッション・エンティティーの開始時刻が使用されます。
  - セッション終了 - セッション・エンティティーの終了時刻が使用されます。
  - 完全な SQL -「完全な SQL」ドメインからのタイム・スタンプ。 値にリンクされていない場合であっても、照会には「完全な SQL」ドメインからの行が含まれます (例えば、「全詳細をロギング」が設定されている場合、値はありません)。
  - 完全な SQL 値 -「完全な SQL」ドメインからのタイム・スタンプ。「完全な SQL」ドメインからの値がある場合にのみ、(それらが「フィールド」ドメインにリンクされていなくても) 照会に行が含まれます。
  - フィールド SQL 値 -「完全な SQL」ドメインからのタイム・スタンプ。「完全な SQL」ドメインからの値があり、 それらの値が「フィールド」ドメインにリンクされている場合にのみ、照会に行が含まれます。
- 「メイン・エンティティー」画面には、「2 つのステージングで実行」の選択があります。

  タイプが「レポート」の監査タスクを 2 つのステージングで実行する場合はこれを選択してください。

  これは、特定の表での照会に関するレポートにのみ該当します。この 2 つのステージングによる方式は、列および条件に対する監査プロセスとして、特定のエンティティーで照会を実行する場合にのみ適用されます。そのエンティティーとは、アクセス (クライアント/サーバー)、セッション、アクセス期間、構文 (SQL)、オブジェクト、およびセンテンス (コマンド) です。

  `Like Group` 演算子または別名に関連したいずれかの演算子 (`In Aliases Group` など) が使用された条件が照会に含まれている場合や、条件で「Having」が使用されている場合、この 2 つのステージングによる方式は使用されません。

  クエリー・ビルダーの使用に加えて、各照会を 2 つのステージングで実行するように設定できます。 デフォルトでは、照会は従来の方式で実行されます。照会を 2 つのステージングで実行するには、クエリー・ビルダーでフラグを設定する必要があります。また、この方式での照会の実行を (システム全体で) 無効にして、すべての監査タスクで従来の方式を使用することができます。そのためには、/var/log/guard/DontRunInTwoStages というファイルを作成します。 このファイルが存在するということは、2 つのステージングによる新しい方式は使用してはならないということを意味します。
  注: 本リリースでは、タプル (結合されたフィールド) を含むフィールドは、2 つのステージングによる実行ではサポートされていません。

注: 注:「メイン・エンティティー」ドロップダウン・リストに含まれるのは、1 次エンティティーだけです。 ただし、2 次エンティティー (例えば、「セッション開始」および「セッション終了」) には、対応する 1 次エンティティー (例えば、「セッション開始」および「セッション終了」の「セッション」) を通じてアクセスすることができます。

ソート

デフォルトでは、照会データは、属性値の昇順でソートされます。ソート・キーは、属性が照会に出現する順に配列されます。ソート目的のため、別名は無視されます。常に実際のデータ値がソートに使用されます。照会によって値が計算される属性 (「カウント」、「最小」、「最大」、または「平均」) は、 ソートできません。

デフォルトのソート順を変更する手順は、以下のとおりです。

1. 「順序」チェック・ボックスにチェック・マークを付けます。
2. 「ソート・ランク」に数値を入力します (最も主なソート・キーは 1 です)。
3. オプションで「降順」チェック・ボックスにチェック・マークを付けると、 その属性の値は降順でソートされます。

表形式レポートの最終列は、メイン・エンティティーのオカレンスのカウントです。このカウントについて降順でソートする (つまり、オカレンス数が最大のものを最初にリストする) には、「オカレンスでソート (Sorted by occurrences)」チェック・ボックスにマークを付けます。

タイム・スタンプ

timestamp (小文字の t) は、結合された日付と時刻の値を含んでいるデータ・タイプであり、プリントされると yyyy-mm-dd hh:mm:ss のフォーマットで表示されます (例: 2012-07-17 15:40:25)。照会の作成または編集時に、timestamp データ・タイプのほとんどの属性は、時計アイコン付きで「エンティティー・リスト」パネルに表示されます。

Timestamp (大文字の T) は多くのエンティティー・タイプに定義される属性であり、エンティティーの最終更新時刻を含みます。多くの timestamp 属性について、 追加の Timestamp 属性 (「日付」、「時刻」、「曜日」、または「年」など) を参照することにより、 日付、時刻、曜日、または年の各コンポーネントを個別にプリントできます。

- クエリー・ビルダーの使用
  照会の作成や変更を行うには、クエリー・ビルダーを使用します。照会したいドメインを指定し、メイン・エンティティーを選択してから、クエリー・ビルダーを使用して照会の定義や変更を行います。
- 照会条件
  AND、OR、および HAVING 演算子を括弧と共に使用して、照会条件を作成します。

親トピック: レポート

クエリー・ビルダーの使用

照会の作成や変更を行うには、クエリー・ビルダーを使用します。照会したいドメインを指定し、メイン・エンティティーを選択してから、クエリー・ビルダーを使用して照会の定義や変更を行います。

1. 「順守」 > 「カスタム・レポート作成」 > 「カスタム・クエリー・ビルダー」をクリックして、クエリー・ビルダーを開きます。
2. 照会するドメインを決定します。「ドメイン・ファインダー」メニューから項目を選択して「検索」をクリックするか、「新規」  をクリックしてカスタム・ドメインを作成します。
3. 「照会ファインダー」でフィルター・メニューを使用して既存の照会を選択するか、「新規」をクリックして新規照会を作成します。
4. クエリー・ビルダー画面には、以下の 3 つの主要コンポーネントがあります。
   - 「エンティティー・リスト」ペインには、ドメインに含まれるすべてのエンティティーと属性が表示されます。エンティティーはフォルダーとして、属性はフォルダーに含まれる項目として表されます。エンティティー・フォルダーをクリックするとその属性が表示され、もう一度クリックすると非表示になります。 すべてのエンティティーと属性の説明については、ドメイン、エンティティー、および属性情報の『エンティティーおよび属性』を参照してください。
   - 「照会フィールド」ペインには、アクセスするすべてのフィールド、そのフィールドについての表示内容 (値、カウント、最小、最大、または平均)、およびソート順がリストされます。 このペインの使用について詳しくは、『*照会フィールドの概要*』を参照してください。
   - 「照会条件」ペインでは、これらのフィールドを選択するための任意の条件 (例えば、 `「where VERB = UPDATE」`) を指定します。 このペインの使用について詳しくは、『*照会条件の概要*』を参照してください。

照会の作成

1. 適切なドメインについてクエリー・ビルダーを開きます。
2. 「新規」をクリックして「新規照会 - 全体詳細」パネルを開きます。
3. 「照会名」ボックスに、固有の照会名を入力します。 照会名にはアポストロフィ文字を含めないでください。
4. 「メイン・エンティティー」リストから、照会のメイン・エンティティーを選択します。 メイン・エンティティーが照会で使用可能になる詳細のレベルを制御すること、およびそのレベルは変更できないことにご注意ください。基本的に、照会によって返される各データ行は、 メイン・エンティティーの固有のインスタンスおよびそのインスタンスのオカレンス数を表します。
5. 「次へ (Next)」をクリックします。「クエリー・ビルダー」パネルで新規照会が開きます。定義を完了するには、以下のトピックのいずれかを参照してください。
   - クエリー・ビルダーの概要
   - 照会の変更

照会の変更

Guardium の定義済み照会を変更することはできませんが、照会のコピーを作成し、そのコピーを必要に応じて変更することができます。

1. ドメインとメイン・エンティティーを選択し、変更したい照会についてクエリー・ビルダーを開きます。
2. 「コピー」をクリックし、照会の新規名を入力して (アポストロフィは使用できません)、「保存」をクリックします。
3. 『クエリー・ビルダーの概要』トピックで、照会定義のコンポーネントを変更する方法を参照してください。

照会の削除

他のコンポーネントが使用している照会は削除できません。 そのような照会を削除するには、最初にその照会を使用するすべてのコンポーネント (例えば、 レポートや相関アラートなど) を削除する必要があります。照会の削除を試みると、 その照会に従属するレポートや相関アラートがリストされます。

1. ドメインと照会を選択し、削除したい照会についてクエリー・ビルダーを開きます。
2. 「削除」をクリックします。

照会フィールドの概要

「照会フィールド」ペインは、照会によって返されるデータの列をリストします。

「フィールド・モード」メニューには、そのフィールドについて表示する情報 (その値、カウント (個別の値の数)、行の最小値、最大値、平均値、または合計値) が示されます。「値」選択項目は、そのドメインのエンティティー階層で、メイン・エンティティーより大きいエンティティーの属性では使用できません。

「照会フィールド」ペインにフィールドを追加する方法は、2 とおりあります。

- ポップアップ・メニュー方式:
  1. 「エンティティー・リスト」で、追加するフィールドをクリックします。
  2. ポップアップ・メニューから「フィールドの追加」を選択します。
- ドラッグ・アンド・ドロップ方式:
  1. 「エンティティー・リスト」で、(フィールド名そのものではなく) フィールド名のアイコンをクリックし、そのアイコンをドラッグして「照会フィールド」ペインで放します。

フィールドを追加すると、そのフィールドはリストの末尾に追加されます。

「照会フィールド」ペイン内でフィールドを上下に移動するには、そのフィールドのチェック・ボックスにチェック・マークを付け、「上へ」アイコンまたは「下へ」アイコンをクリックして、フィールドを 1 行ずつ上下に移動します。

照会における「完全な SQL」属性に関する注意事項

照会で「完全な SQL」属性を使用する際には注意が必要です。これを使用すると、 属性の個別の値 (この場合、完全な SQL 照会文字列) がそれぞれ個別の行で返されるため、 過度に大容量のレポートが生成される可能性があります。

一方、「完全な SQL」の文字列を予期している場合に、レポートに全く情報が含まれない、 または多くのブランク列が含まれることがあります。Guardium は、ポリシー・ルールによって 指示された場合にのみ「完全な SQL」をキャプチャーします。そして、レポート期間中には、 ポリシー・ルールが起動されない可能性があります。

「完全な SQL」属性と、SQL にドリルダウンする機能を混同しないでください。 データ・アクセス・ドメインの照会は、SQL 要求に関して何も行いません。

属性に定義されたタイプ以外のタイプのグループ

グループ・タイプに対する検証は、多くの場合制限されています。 グループ・タイプの例については『グループの概要』を参照してください。「照会条件」、「クエリー・ビルダー」を使用する場合、グループ条件の属性に定義されたタイプ以外の タイプのグループの使用が許可されます。これらの追加の選択項目は、 IN GROUP およ

び IN DYNAMIC GROUP 演算子についてのみ使用できます。 条件に定義されたタイプ以外のタイプの選択は、表形式レポートのランタイム・パラメーターで実行されます。

1. 「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」をクリックして、グループ・ビルダーでグループを作成します。「グループ名」を指定し、「グループ・タイプ」として「オブジェクト」を選択します。
2. 「設定」 > 「レポート」 > 「レポート・ビルダー」をクリックして、レポート・ビルダーでアクセス・レポートを作成します。
3. 照会名を指定し、「エンティティー・リスト」から OBJECT フォルダーをクリックして、さらに多くの選択項目を表示します。
4. 「オブジェクト名」を強調表示して一度クリックし、「条件の追加」選択項目を取得します。「条件の追加」をクリックし、メニュー画面のメイン本文にある「照会条件」セクションに 1 行を追加します。
5. 属性「オブジェクト名」の横にあるドロップダウン選択項目に移動し、 「演算子」列で IN GROUP または IN DYNAMIC GROUP を選択します。 2 番目のドロップダウン選択項目 (「ランタイム・パラメーター」列) で、ステップ 1 で作成したグループを選択します。
6. 作業内容を保存します。 「表形式の生成」をクリックし、次に「My New Reports に追加」をクリックします。
7. 「My New Reports」タブに移動して、 作成したレポートを強調表示します。
8. レポート名の隣の「カスタマイズ」をクリックします。「ポートレットのカスタマイズ (ランタイム・パラメーター)」タブが開きます。
9. ドロップダウン選択項目を開くと、テストされているエンティティーに対応するタイプのグループがリストの最初に表示され、続いて二重破線と、さらに残りのグループが表示されます。ここで、別のグループを選択できます。
10. 「更新」をクリックして作業内容を保存します。

表 1. ボタン

ボタン	手順
削除	1. 削除する照会を選択します。 2. 「削除」をクリックします。
コピー	1. コピーを作成する照会を選択します。 2. 「コピー」ボタンをクリックします。 3. コピーした照会の新規名を入力します。
ロール	クエリー・ビルダー でレポートにロールを割り当てると、レポートではなく照会のみにロールが割り当てられます。レポート・ビルダーでレポートにロールを割り当てます。レポートを参照してください。
保存	メニュー画面で必要なすべてのタスクを完了後、「保存」をクリックしてください。
戻る	「戻る」ボタンを使用して、マルチスクリーンの Guardium タスクや機能のメニュー画面の間を後方に移動します。Web ブラウザーの「戻る」矢印は、メニュー画面間のナビゲーションとしては動作しません。
データマートとして設定	データマートはデータウェアハウスのサブセットです。 データウェアハウスでは、後から分析およびレポートで使用可能なように、データが汎用的な方式で集約および編成されます。

親トピック: 照会
関連概念:
ドメイン、エンティティー、および属性

照会条件

AND、OR、および HAVING 演算子を括弧と共に使用して、照会条件を作成します。

AND、OR、および HAVING 演算子は、クエリー・ビルダーの「照会条件」タイトル・バーにあります。

エンティティー・リストからエンティティーを選択し、演算子を使用して、照会条件を照会の一部として作成します。

AND 演算子および OR 演算子の使用:

- AND 演算子は OR 演算子より優先されます。
- 「条件の追加」メニューまたは属性アイコンのドラッグ/ドロップを使用して、条件リストの末尾または中間に AND 演算子や OR 演算子を追加します。「削除」をクリックすると、条件を選択して削除することができます。 照会を保存します。生成された SQL 照会が無効な場合、照会は保存されず、エラー・メッセージが出されます。

括弧の使用:

- すべての条件は独立しています。条件を左右の括弧で囲むことにより、グループ化します。複雑な照会条件には、大括弧を使用してください。
- 条件が選択されている場合に、左括弧ボタンを押すと、最初に選択した条件の前に左括弧条件が 1 つ追加されます。右括弧ボタンを押すと、最初に選択した条件の後に、右括弧条件が 1 つ追加されます。 選択されている条件がない場合は、括弧ボタンを押しても何も起こりません。
- 括弧を使用する照会条件を作成する場合、UI では演算子の前に括弧が表示されますが、適用されるのは演算子の後です。例えば、照会条件が「*this (AND that OR another)*」として表示されていても、実際のロジックは「*this AND (that OR another)*」になります。

円記号 (¥) 文字のエスケープ: 照会条件で使用する円記号 (¥) 文字を適切にエスケープするには、4 つの連続する円記号文字を使用します。例えば、 `domain¥user` を指定するには、`domain¥¥¥¥user` と入力します。

条件表示パネルは 2 つの部分で構成されます。1 つは WHERE 条件で始まり、もう 1 つは HAVING 条件で始まります。

HAVING 部分では、統合フィールドに「カウント」、「最小」、「最大」、および「平均」のオプションがあります。名前に ID が含まれる特定のエンティティー (「セッション ID」、「グローバル ID」、「完全な SQL ID」、「インスタンス ID」) には、オプションの「合計」も適用されます。「HAVING」ボタンがチェックされていない場合、条件は統合フィールドを空文字列として WHERE 部分に挿入されます。「HAVING」ボタンがチェックされている場合、条件は HAVING 部分に挿入され、 統合フィールドにはオプションが指定されます。条件の追加や削除が完了した後、 条件オプションが更新されます。「保存」を押すと、SQL が生成されます。SQL は保存前に検証されます。検証が (例えば、構文エラーなどで) 失敗すると、 アラート・エラー・メッセージが生成され、より詳細なエラーの記述がログに書き込まれます。条件を間違っ

た部分に追加すると (例えば、「HAVING」ボタンを設定して属性アイコンを WHERE 部分にドロップしたり、 その逆の操作を行ったりした場合)、不一致アラート・メッセージが生成されます。選択された条件が WHERE 部分内にあるが、「HAVING」ボタンが設定されている場合、設定が一致しないため、条件の追加は失敗します。

属性「アクセス合計」、「失敗した SQL」、「成功した SQL」は、(WHERE 節ではなく) HAVING 節の下にのみ追加できます。

許可される照会には、1 つのタイム・スタンプ列と、少なくとも 1 つの Mode=Count またはカウント・フラグ (あるいはその両方) が設定された列が必要です。照会によって評価される照会列は、Mode=Count またはアクセス合計列 (カウント・フラグが設定されている場合) が指定された列のいずれか 1 つでなければなりません。

照会条件の追加または削除

1. 照会条件を削除するには、対象の条件の行にあるチェック・ボックスにマークを付けて、「照会条件」タイトル・バーの「X」ボタン (マーク付き項目を削除) をクリックします。
2. 条件を追加するには、「照会条件」リストに、「エンティティー・リスト」ペインの該当するフィールドの行を作成します。

   AND 条件を追加する場合は、「照会条件」タイトル・バーの「AND」ラジオ・ボタンを選択し、次のいずれかを行います。

   - 「エンティティー・リスト」ペインからエンティティーを選択し、ポップアップ・メニューから「条件の追加」を選択します。
   - 「エンティティー・リスト」ペインからフィールド・アイコンをドラッグして、「照会条件」ペインにドロップします。

   OR 条件を追加する場合は、「照会条件」タイトル・バーの「OR」ラジオ・ボタンを選択し、次のいずれかを行います。

   - 「エンティティー・リスト」ペインからフィールド・アイコンをドラッグして、OR 条件にする条件の先頭で放します。
   - OR 条件を追加する条件のチェック・ボックスにマークを付け、「エンティティー・リスト」ペイン内のフィールドをクリックして、ポップアップ・メニューから「条件の追加」を選択します。

3. *オプション*:「統合」ドロップダウンを使用して、照会条件に使用する属性「カウント」、「最小」(最小値)、「最大」(最大値)、または「平均」(平均値) の統合を選択します。以下のような制約が適用されます。
   - OR 条件では、統合を使用できません。
   - 統合を含む条件に、OR 条件を追加できません。
4. リストから、新規条件の演算子を選択します。すべての属性タイプで、必ずしも同じ演算子セットが使用できるわけではありません。例えば、グループに関連付けることができない属性では、グループ・オプション (IN GROUP、LIKE GROUP) を指定できません。ただし、タプル (複数属性が組み合わされて形成された 1 つのグループ) を照会の条件として追加する場合、 新規条件ですべての演算子を選択可能になります。

表 1. 新規条件の演算子

演算子	記述
<	より小さい
< =	以下
< >	等しくない
=	等しい
>	より大きい
> =	以上
CATEGORIZED AS	グループ演算子が選択されている場合に表示される、 ドロップダウン・リストから選択されるカテゴリーに属するグループのメンバー。
CLASSIFIED AS	グループ演算子が選択されている場合に表示される、 ドロップダウン・リストから選択される分類に属するグループのメンバー。
IN DYNAMIC GROUP	グループ演算子が選択されている場合に表示される、 ランタイム・パラメーター列のドロップダウン・リストから選択されるグループのメンバー。
IN GROUP	グループ演算子が選択されている場合に表示される、 ランタイム・パラメーター列のドロップダウン・リストから選択されるグループのメンバー。IN GROUP または IN ALIASES GROUP は、両方同時に使用することはできません。
IN DYNAMIC ALIASES GROUP	IN DYNAMIC GROUP と同じタイプのグループに対して機能するが、 そのグループのメンバーが別名であると想定する演算子。
IN ALIASES GROUP	IN GROUP と同じタイプのグループに対して機能するが、 そのグループのメンバーが別名であることを想定する演算子。 IN GROUP 演算子はグループが実際の値を、IN ALIASES GROUP 演算子はグループが別名を含んでいることを予期します。 別名は、特定の属性タイプの保管値に代わる同義語になります。通常は、データ値を意味のある、または分かりやすい名前で表示するために使用されます。 例えば、IP アドレス 192.168.2.18 の別名として、「財務サーバー」を定義することができます。
IS NOT NULL	属性値は存在しますが、ブランクまたは印刷不能である可能性があります。
IS NULL	空の属性
IN PERIOD	タイム・スタンプについてのみ、選択された期間内にあります。
LIKE	
LIKE GROUP	ボックスに指定された like 値に一致します。like 値は、ワイルドカード文字として % 記号を使用し、値の全部または一部に一致します。 英字には大/小文字の区別がありません。例えば、%tea% は tea、TeA、tEam、steam のいずれにも一致します。 % 記号が含まれていない場合、比較演算は、等価演算 (=) になります。
NOT IN DYNAMIC GROUP	グループ演算子が選択されている場合に表示される、 ランタイム・パラメーター列のドロップダウン・リストから選択される、グループのすべてのメンバーと等しくありません。
NOT IN DYNAMIC ALIASES GROUP	NOT IN DYNAMIC GROUP と同じタイプのグループに対して機能するが、 そのグループのメンバーが別名であると想定する演算子。

演算子	記述
NOT IN GROUP	グループ演算子が選択されている場合に表示される、 ランタイム・パラメーター列のドロップダウン・リストから選択される、特定のグループのすべてのメンバーと等しくありません。
NOT IN ALIASES GROUP	NOT IN GROUP と同じタイプのグループに対して機能するが、 そのグループのメンバーが別名であることを想定する演算子。
NOT IN PERIOD	タイム・スタンプ専用。選択された期間内にありません。
NOT LIKE	指定された値と like ではありません (LIKE の説明を参照)。
NOT LIKE GROUP	LIKE GROUP に指定された値と like ではありません。
NOT REGEXP	指定された正規表現に一致しません。
REGEXP	指定された正規表現に一致します。正規表現の使用方法について詳しくは、『正規表現』を参照してください。

注: user、group、role、page の 4 つの特殊語は、パラメーター名として使用できません。

これらいずれかの語を使用するパラメーターを指定した照会を保存しようとすると、エラーが発生します。これが該当する条件として、次の 2 つのタイプがあります。

- 「=」、「<」、「LIKE」などの演算子を指定した照会条件を作成し、「パラメーター」を選択するとします。このフィールドでは特殊語は使用できません。
- DYNAMIC GROUP タイプ演算子 (IN、NOT IN、IN ALIAS など) を指定して照会条件を作成する場合、このフィールドでは特殊語を使用できなくなります。

5. グループ演算子の場合、リストからグループを選択します。

   他のほとんどの演算子については、ユーザーが条件の値を指定するか、ランタイム・パラメーター値 (感嘆符を含まない) が後で (照会の実行時に) 提供されることを指定する必要があります。このような場合、3 つのオプションを持つドロップダウンが表示されます。以下のいずれかを実行します。

   - 「値」を選択し、ボックスに正確な値を入力します。
   - 「パラメーター」を選択し、ランタイム・パラメーターの名前を入力します (名前にスペースを含めることはできません)。
   - 「属性」を選択し、 選択した属性とマッチングする別の属性を選択します (これは例えば、クライアントおよびサーバーの IP アドレスとマッチング することにより、ローカル・トラフィックをテストする場合に使用できます)。

   「値」、「パラメーター」、「属性」選択項目の隣に「式の追加」アイコンがあります。このアイコンを使用して、ユーザー定義文字列および数式を含んだ照会条件を入力します。

   このフィーチャーは、ユーザーが属性の全体的なコンテンツそのもの には基づいていないが、その属性の一部、その属性の関数、または複数の属性を組み合わせた関数 に基づいた条件を追加する必要がある場合に使用します。

   例: `INSTR(:attribute, '150.1') = 5`。これは、リストされる 5 つの文字に一致するクライアント IP のすべてのインスタンスを返します。文字 5 を、「式の追加」 アイコンの隣の入力ボックスに入力します。 `INSTR(:attribute, '150.1')` 式を、別の「式の作成」ウィンドウに入力します。「式の作成」ウィンドウで、式の妥当性をテストします。 もう 1 つの例: `LENGTH(:attribute) >= 40`。これは、40 文字を超えるすべての SQL ステートメントの長さを返します。 式には、実際の属性への参照を含める (または含めない) ことが可能です。さらに、他の属性への参照を含めることもできます。

6. すべての条件の追加が完了した後、必ず定義を保存してください。

照会条件での式の作成

「値」、「パラメーター」、「属性」選択項目の隣に「式の追加」アイコンがあります。このアイコンを使用して、ユーザー定義文字列および数式を含んだ照会条件を入力します。

このフィーチャーは、ユーザーが属性の全体的なコンテンツそのもの には基づいていないが、その属性の一部、その属性の関数、または複数の属性を組み合わせた関数 に基づいた条件を追加する必要がある場合に使用します。

例:

値 192.150.1.x. から、ストリング「150.1」の位置を返します。ここでストリング「150.1」は、値の 5 番目の文字です。ストリング「150.1」は、リストされている 5 つの文字に一致するクライアント IP のすべてのインスタンスを表します。

「式」フィールドで関数を実行する際、これは値を返し、かつその値は「入力ボックス」に入っていなければなりません。

関数 `INSTR(:attribute, '150.1')` を使用し、「式の追加」アイコンの隣にある入力ボックスに値「5」を入力すると、5 番目の位置に `150.1` があるレコードが返されます。

関数が `INSTR(:attribute, '150.1') = 5` の場合、これはブール句となり、入力ボックスに入力できる値は 0 または 1 のみです。

`INSTR(:attribute, '150.1')` 式を、別の「式の作成」ウィンドウに入力します。

「式の作成」ウィンドウで、式の妥当性をテストします。

もう 1 つの例: `LENGTH(:attribute) >= 40`。これは、40 文字を超えるすべての SQL ステートメントの長さを返します。式には、実際の属性への参照を含める (または含めない) ことが可能です。さらに、他の属性への参照を含めることもできます。

親トピック: 照会

ドメイン、エンティティー、および属性

ドメインは、Guardium® が保管しているデータのビューを提供します。

各ドメインには、特定の目的や機能 (データ・アクセス、例外、ポリシー違反など) に関連するデータ・セットが含まれます。 すべてのドメインの説明については、『ドメイン』を参照してください。

各ドメインには、1 つ以上のエンティティーが含まれます。エンティティーは、関連する属性の集合で、属性は基本的にフィールドの値です。すべてのエンティティーと属性の説明については、『エンティティーおよび属性』を参照してください。

Guardium 照会では、1 つのドメインだけからデータが返されます。 照会が定義されるときに、そのドメイン内の 1 つのエンティティーが、照会のメイン・エンティティーに指定されます。 照会により返される各データ行には、選択された属性について要求された期間で返された値に一致するメイン・エンティティーの出現数が含まれます。 これにより、1 対 1 の関係を持たないエンティティーから 2 次元のレポートの作成が可能になります。

ドメインごとに別個のクエリー・ビルダーがあり、各クエリー・ビルダーへのアクセスはセキュリティー・ロールで制御されます。したがって、各 Guardium ロールは通常、社内のそのロールの機能に応じて、ドメインのサブセットへのアクセス権限を持ちます。 Guardium admin ロール・ユーザーは通常、すべてのレポート作成ドメインへのアクセス権限を持ちます。

ドメインによっては、オプション・コンポーネント (例えば CAS や分類) がインストールされている場合のみ使用可能なものもあります。 その他のドメインは Guardium アプライアンス (例えばアーカイブ・アクティビティー) に関連する情報をレポートし、デフォルトでは Guardium admin ロール・ユーザーのみが使用可能です。

この付録に記載した属性には、admin ロールのユーザーのみが使用できるものが含まれています。これらには、「admin ロール専用に予約済み」というラベルが付けられています。

admin ロールのないユーザーは、これらの属性をクエリー・ビルダーから使用することはできません。

同様に、すべての属性をすべてのデータベース・プロトコルで使用できるわけではありません。 クエリー・ビルダーを使用する際に、この資料に記載されたエンティティーまたは属性が「エンティティー」ペインにリストされていない場合、そのエンティティーまたは属性は、選択したデータベース・タイプには使用できません。

以下のトピックを参照してください。

- ドメイン
- エンティティーおよび属性
- 照会のビルド

- ドメイン
  次の表は、Guardium システムで提供される各種のクエリー・ビルダーと関連するドメインを示しています。 お客様の会社でこのほかのカスタム・ドメインが定義されている場合があります。
- カスタム・ドメイン
  カスタム・ドメインではユーザー定義のドメインが可能であり、アプライアンスにアップロードされる任意のデータ表を定義できます。
- エンティティーおよび属性
  このトピックでは、各エンティティーに含まれる属性について説明します。
- データベース・ライセンス・レポート
  データベース・ライセンス・レポートは、ユーザーが該当するデータのみに対するアクセス権限を持っていることを確認するために使用できます。Guardium システムには、いくつかのデータベース・タイプ用の事前定義のデータベース・ライセンス・レポートが用意されています。

親トピック: レポート

ドメイン

次の表は、Guardium システムで提供される各種のクエリー・ビルダーと関連するドメインを示しています。 お客様の会社でこのほかのカスタム・ドメインが定義されている場合があります。

各ドメインには、特定の目的や機能 (データ・アクセス、例外、ポリシー違反など) に関連するデータ・セットが含まれます。 すべてのドメインの説明については、『ドメイン』を参照してください。

各ドメインには、1 つ以上のエンティティーが含まれます。エンティティーは、関連する属性の集合で、属性は基本的にフィールドの値です。すべてのエンティティーと属性の説明については、『エンティティーおよび属性』を参照してください。

Guardium® 照会では、1 つのドメインだけからデータが返されます。 照会が定義されるときに、そのドメイン内の 1 つのエンティティーが、照会のメイン・エンティティーに指定されます。 照会により返される各データ行には、選択された属性について要求された期間で返された値に一致するメイン・エンティティーの出現数が含まれます。 これにより、1 対 1 の関係を持たないエンティティーから 2 次元のレポートの作成が可能になります。

ドメインごとに別個のクエリー・ビルダーがあり、各クエリー・ビルダーへのアクセスはセキュリティー・ロールで制御されます。したがって、各 Guardium ロールは通常、社内のそのロールの機能に応じて、ドメインのサブセットへのアクセス権限を持ちます。 Guardium admin ロール・ユーザーは通常、すべてのレポート作成ドメインへのアクセス権限を持ちます。

ドメインによっては、オプション・コンポーネント (例えば CAS や分類) がインストールされている場合のみ使用可能なものもあります。 その他のドメインは Guardium アプライアンス (例えばアーカイブ・アクティビティー) に関連する情報をレポートし、デフォルトでは Guardium admin ロール・ユーザーのみが使用可能です。

この付録に記載した属性には、admin ロールのユーザーのみが使用できるものが含まれています。これらには、「admin ロール専用に予約済み」というラベルが付けられています。

admin ロールのないユーザーは、これらの属性をクエリー・ビルダーから使用することはできません。

同様に、すべての属性をすべてのデータベース・プロトコルで使用できるわけではありません。 クエリー・ビルダーを使用する際に、この資料に記載されたエンティティーまたは属性が「エンティティー」ペインにリストされていない場合、そのエンティティーまたは属性は、選択したデータベース・タイプには使用できません。

以下のトピックを参照してください。

- ドメイン
- エンティティーおよび属性
- 照会のビルド

各ドメインのクエリー・ビルダーへのアクセス権限は、セキュリティー・ロールによって制御されます。したがって通常は、ユーザー・ロールごとに別々のドメイン・セットへのアクセス権限を持ちます。 ドメインによっては、オプション・コンポーネント (例えば CAS) がインストールされている場合のみ使用可能なものもあります。

デフォルトの admin ポータルでは、「ツール」>「レポートのビルド」タブのメニューからすべてのクエリー・ビルダーを開くことができます。 デフォルトのユーザー・ポータルでは、カスタム・レポート作成アプリケーションから多数のクエリー・ビルダーを開くことができます (「モニター/監査」>「レポートのビルド」)。

「説明」列には、ドメインの簡略説明に続いて、ドメインごとに割り当てられたデフォルト・セキュリティー・ロールをリストし、デフォルト・ユーザー・ポータルからドメインにアクセスする方法を示します (使用可能な場合)。

表 1. ドメイン

クエリー・ビルダー (ドメイン)	記述
アクセス・ポリシー (アクセス・ポリシー)	このドメインを使用して、システム上の使用可能なすべてのポリシーをトラッキングします。このドメインは、システム上にインストールされているすべてのポリシーをトラッキングする際に使用される「インストール済みポリシー」ドメインに類似しています。 ロール: すべて。ユーザー・ポータル: 使用不可
アクセス (LOGGER INFO)	クライアント/サーバー、セッション、SQL、およびアクセス期間の関連データのすべて。 モニター対象サーバーに要求が送信されるたびに検査エンジンによって収集されるデータです。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「データ・アクセスのトラッキング」
統合/アーカイブ (AGGREGATION/EXPORT/IMPORT)	統合およびアーカイブ・アクティビティー。各操作 (アーカイブ、送信、パージなど) の日付、時刻、および状況が含まれます。 ロール: 管理者ユーザー・ポータル: 使用不可
アラート (ALERT)	Guardium によって生成および送信されたすべてのアラート。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「送信済みアラートのトラッキング」
アプリケーション (アプリケーション・データ)	特殊な非 Guardium アプリケーション (例えば Siebel や SAP) について記録された接続、セッション、およびアプリケーション・データ。 ロール: 管理者ユーザー・ポータル: 使用不可
監査プロセス (AUDIT TRAIL)	監査プロセスの実行と結果の配布。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「監査プロセス・ビルダー」
オートディスカバリー (AUTODETECT DB DISCOVERY)	データベース・オートディスカバリー・アクティビティー。これには実行されてホストとポートがディスカバーしたすべてのプロセスが含まれます。 ロール: すべて ユーザー・ポータル:「ディスカバー」>「データベース・ディスカバリー」>「オートディスカバリー・クエリー・ビルダー」
CAS 変更 (CAS 変更)	CAS によって検出されたすべての変更。これには記録されたすべての変更データが含まれます。 ロール: CAS ユーザー・ポータル: 使用不可
CAS 構成 (CAS 構成)	CAS インスタンスの構成。特定のホストでのテンプレートの使用を示します。 ロール: CAS ユーザー・ポータル: 使用不可
CAS ホスト履歴 (CAS ホスト履歴)	CAS エージェント・ホストに適用された CAS 変更の履歴。 ロール: CAS ユーザー・ポータル: 使用不可
CAS テンプレート (CAS テンプレート)	CAS テンプレート (モニター項目を定義) の内容についてレポートします。 ロール: CAS ユーザー・ポータル: 使用不可
分類結果 (分類プロセス)	分類プロセスの実行と結果についてレポートします。 ロール: 管理者ユーザー・ポータル: 使用不可
コメント (COMMENT)	各種 Guardium コンポーネントに関するユーザー定義のコメント。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「コメント・ビルダー」
カスタム・ドメイン・ビルダー	よく使用される表と製品のアップロード用にカスタム・ドメインが定義されています。 カスタム・ドメインにはカスタム表が 1 つ以上含まれるので、「カスタム表」を参照してください。表が複数含まれる場合は、カスタム・ドメインを定義する際に表間の関連を定義します。
カスタム・クエリー・ビルダー	Guardium アプライアンスにアップロードされるデータの表は、どのようなものでもユーザー定義のドメインで定義できます。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「カスタム・クエリー・ビルダー」
カスタム表ビルダー	カスタム表には、Guardium アプライアンスで使用可能にする属性が 1 つ以上含まれます。 例えば、エンコードされたユーザー名を実名に関連付ける既存のデータベース表があるとします。 ネットワーク・トラフィックで見られるのは、エンコードされた名前のみです。 Guardium アプライアンスでカスタム表を定義し、その表のデータを既存の表からアップロードすることにより、コード化された名前と実名を関連付けることができるようになります。

クエリー・ビルダー (ドメイン)	記述
使用可能 DB デフォルト・ユーザー	非資格情報スキャン - データベースのリストをスキャンし、デフォルト・ユーザーが使用可能になっているかどうかを検査するプロセス。 デフォルト・ユーザーと、スキャン対象サーバー・リストが、パラメーターとして API に提供されます。 それぞれのデータベース・タイプについて、インストール時にデータベースにより作成されたデフォルト・ユーザーとパスワードを含むデフォルトのグループが提供され、お客様がそのリストに追加したり削除したりできます。 グループのタイプは「データベース・ユーザー/データベース・パスワード」であり、デフォルト・グループの名前は次のとおりです。 ORACLE デフォルト・ユーザー、DB2® デフォルト・ユーザー、SYBASE デフォルト・ユーザー、MS SQL SERVER デフォルト・ユーザー、INFORMIX デフォルト・ユーザー、MYSQL デフォルト・ユーザー、TERADATA デフォルト・ユーザー、IBM® ISERIES デフォルト・ユーザー、POSTGRESQL デフォルト・ユーザー、NETEZZA デフォルト・ユーザー
ディスカバーされたインスタンス (ディスカバーされたインスタンス)	GIM によってディスカバーされたインスタンス。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「ディスカバーされたインスタンス」
エンタープライズ・バッファー使用状況	すべての管理対象ユニットからのスニファーのバッファー使用の統合を示します。 ロール: なし ユーザー・ポータル: 使用不可
例外 (表の最後にある注を参照) (LOGGER EXCEPTIONS)	例外と例外関連データのすべて。 Guardium 自体で発生した例外だけでなく、データベース・サーバーから送信されて検査エンジンによって収集された SQL 例外も含まれます。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「例外のトラッキング」
未解析ログ (未解析ログ)	未解析ログ処理アクティビティー。 ロール: なし ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「未解析ログ・ビルダー」
GIM イベント (GIM イベント)	Guardium Installation Manager ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「GIM イベント」
グループ (グループ)	Guardium グループのメンバーシップ。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「グループ・ビルダー」
Guardium アクティビティー (USER ACTIVITY AUDIT)	Guardium エンティティーに対して Guardium ユーザーが行ったすべての変更 (レポートまたは照会の定義または変更)。 ロール: 管理者ユーザー・ポータル: 使用不可
Guardium ログイン (USER LOGIN)	Guardium ユーザーのログインとログアウトに関する全情報。 ロール: 管理者ユーザー・ポータル: 使用不可
インストール済みポリシー (インストール済みポリシー)	インストール済みポリシーのポリシー・パラメーターとポリシー・ルールを示します。 「インストール済みポリシー」ドメインは、複数のポリシーと、ルール 1 つ当たり複数のアクションをサポートします。 ロール: すべて ユーザー・ポータル: 使用不可
ポリシー違反 (ACCESS RULES VIOLATIONS)	Guardium 検査エンジンまたは STAP によって検出されたポリシーのすべての違反に関するすべてのポリシー違反データ。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「ポリシー違反ビルダー」
ポリシー違反サマリー (アクセス・ルール違反)	Guardium 検査エンジンまたは STAP によって検出されたポリシーのすべての違反のサマリーに関するすべてのポリシー違反データ。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「ポリシー違反サマリー・ビルダー」
リプレイ結果	あるデータ・ソースからのデータ・ストリームを、別のデータ・ソースでリプレイします。 ロール: なし ユーザー・ポータル: 使用不可
不正な接続 (HUNTER)	共有メモリーや名前付きパイプなどの非標準手段で S-TAP® をデータベースに接続することを回避したローカル・データベース・サーバー・プロセス。 TEE モニター方式が使用される場合に Unix S-TAP にのみ適用されます。 ロール: すべて ユーザー・ポータル:「モニター/監査」>「レポートのビルド」>「不正な接続ビルダー」
セキュリティー・アセスメントの結果 (評価テスト結果モニター)	脆弱性評価プロセスの結果を記録します。 ロール: なし ユーザー・ポータル: 使用不可
スニファーのバッファー使用 (スニファーのバッファー使用のモニター)	検査エンジン統計。 ロール: なし ユーザー・ポータル: 使用不可
ユーザー/ロール/アプリケーション (ロール/ユーザー/アプリケーション)	Guardium ユーザー、ロール、およびアプリケーションを関連付けます (それにより、誰がどの Guardium アプリケーションへのアクセス権限を持っているかをレポートします)。 ロール: 管理者ユーザー・ポータル: 使用不可

クエリー・ビルダー (ドメイン)	記述
脆弱性診断テスト (評価テスト)	セキュリティー・アセスメントに使用可能なテストについてレポートします。 ロール: 管理者 ユーザー・ポータル: 使用不可
値の変更 (値変更)	トリガー・ベースの値変更アプリケーションによってトラッキングされたすべての変更。 ロール: 管理者ユーザー・ポータル: 使用不可

親トピック: ドメイン、エンティティー、および属性

カスタム・ドメイン

カスタム・ドメインではユーザー定義のドメインが可能であり、アプライアンスにアップロードされる任意のデータ表を定義できます。

これらのカスタム・ライセンス (特権) ドメインを使用するということは、ライセンス・レポートを使用するということです。ライセンス・レポートには、ユーザーとしてログインした場合にアクセスできます。 これらのレポートを表示するには、「ユーザー」タブの「データベース特権」に移動します。

いくつかのカスタム・ドメインが事前定義されています。

[カスタム] アクセス

このドメインには、標準のデータ・アクセス・ドメインと同じエンティティーがすべて含まれています。これがカスタム・ドメインとして提供されることにより、このドメインの情報と、ユーザーによって既にアップロードされた任意のカスタム表の情報を含む追加のユーザー定義ドメインを作成できます。 [カスタム] アクセス・ドメインは、コピーする必要があります。このドメインはバージョンごとに更新されるため、このドメイン上でレポートを作成することはお勧めしません。アクセス・ドメインに含まれるエンティティーについての説明は、『ドメイン』のトピックのアクセス・ドメインに関する説明を参照してください。

S-TAP 情報 (中央マネージャー)

レポート:『S-TAP® レポート』を参照。中央マネージャーでは、追加のレポート、「S-TAP 情報」が使用可能です。このレポートは、環境全体の S-TAP をモニターします。このデータのアップロードには、カスタム表ビルダーを使用します。

S-TAP 情報は、「S-TAP 情報」エンティティーが含まれている事前定義されたカスタム・ドメインであり、変更することはできません。

カスタム照会を定義する際は、アップロード・ページに移動して「検査/修復」をクリックし、CUSTOM データベースにカスタム表を作成します。そうしないと、照会を保存するときに照会が検証されません。この表は、すべてのリモート・ソースから自動的にロードします。ユーザーは、使用するリモート・ソースを選択できません。すべてのリモート・ソースから取り込まれます。

このカスタム表とカスタム・ドメインに基づく、次の 2 つのレポートがあります。

エンタープライズ S-TAP ビューは、中央マネージャーから、コレクターまたは管理対象ユニット上のアクティブな S-TAP に関する情報を表示します (同じ S-TAP エンジンに対する重複があり、一方がアクティブで、他方が非アクティブの場合、アクティブな方のみがレポートに使用されます)。

「詳細なエンタープライズ S-TAP ビュー」は、中央マネージャーから、すべてのコレクターおよび/または管理対象ユニット上のすべてのアクティブおよびパッシブな S-TAP に関する情報を表示します。

エンタープライズ S-TAP ビューと詳細なエンタープライズ S-TAP ビューが同じに見える場合は、1 つの管理対象ユニット上にあるただ 1 つの S-TAP が表示されているためです。複数の S-TAP および複数の管理対象ユニットがある場合は、詳細なエンタープライズ S-TAP ビューの表示が違ったものになります。

これらの 2 つのレポートは、スタンドアロン・システムの「TAP モニター」タブから選択可能ですが、情報は表示されません。

DB ライセンス・ドメイン

ユーザーの認証およびデータに対するロールに基づいたアクセス権の制限に加え、最も多くの特権を持つデータベース・ユーザーに対しても、定期的なライセンス・レビューを行う必要があります。このレビューは、ユーザーが自分の業務を行うのに必要な特権のみを持っていることを検証および確認するプロセスです。これは、データベース・ユーザー権限の認証レポート作成とも呼ばれます。

Guardium の事前定義データベース・ライセンス (特権) レポートを使用して、(例えば) システム特権を持つユーザーや、他のユーザーやロールにこれらの特権を付与したユーザーを確認します。データベース・ライセンス・レポートは、データベース・アクセスの変更をトラッキングしたり、使用されないまま残っているアカウントや誤って付与された特権によるセキュリティー・ホールが存在しないことを確認したりする監査員にとって重要なものです。

DB ライセンス・レポートでは、カスタム・ドメイン機能を使用して、選択したデータベース上の外部データと事前定義ライセンス・レポートの内部データとのリンクを作成します。事前定義データベース・ライセンス・レポートの使用法について詳しくは、『データベース・ライセンス・レポート』を参照してください。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

注: DB ライセンス・レポートは、プロダクト・キーにより有効になるオプションのコンポーネントです。これらのコンポーネントが有効になっていない場合、選択項目は、カスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーの選択に表示されません。

事前定義ライセンス・レポートを以下にリストします。これらは、カスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーの選択でドメイン名として表示されます。

- Oracle DB ライセンス
- MYSQL DB ライセンス
- DB2® DB ライセンス
- SYBASE DB ライセンス
- Informix® DB ライセンス
- MSSQL 2000 DB ライセンス
- MSSQL 20005/2008 DB ライセンス

- Netezza® DB ライセンス
- Teradata DB ライセンス
- PostgreSQL DB ライセンス

Oracle DB ライセンス

以下のドメインは、Oracle DB ライセンスに関するアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

Oracle

- 「ORA ALTER SYSTEM のアカウント」 - ALTER SYSTEM 特権および ALTER SESSION 特権を持つアカウント
- 「ORA BECOME USER 特権を持つアカウント」 - BECOME USER 特権を持つアカウント
- 「ORA 全システム特権および ADMIN オプション」 - ユーザーおよびロールに対するすべてのシステム特権および管理者オプションを示すレポート
- 「ORA オブジェクトおよび列特権」 - 付与されているオブジェクト特権および列特権 (GRANT オプション付きまたはなし)
- 「ORA PUBLIC によるオブジェクト・アクセス」 - PUBLIC によるオブジェクト・アクセス
- 「ORA オブジェクト特権」 - SYS 内になく、DBA ロールではないデータベース・アカウントによるオブジェクト特権
- 「ORA SYS プロシージャーに対する PUBLIC 実行特権」 - PUBLIC に割り当てられている SYS PL/SQL プロシージャーに対する実行特権
- 「ORA 権限付与されたロール」 - ユーザーおよびロールに権限付与されたロール
- 「ORA 権限付与されたシステム特権」 - 再帰的定義 (特権がロールに割り当てられ、そのロールがユーザーに割り当てられた状態) を含む、ユーザーに付与されたシステム特権を示す階層レポート
- 「ORA SYSDBA および SYSOPER アカウント」 - SYSDBA 特権および SYSOPER 特権を持つアカウント

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

grant select on sys.dba_tab_privs to sqlguard;

grant select on sys.dba_roles to sqlguard;

grant select on sys.dba_users to sqlguard;

grant select on sys.dba_role_privs to sqlguard;

grant select on sys.dba_sys_privs to sqlguard;

grant select on sys.obj$ to sqlguard;

grant select on sys.user$ to sqlguard;

grant select on sys.objauth$ to sqlguard;

grant select on sys.table_privilege_map to sqlguard;

grant select on sys.dba_objects to sqlguard;

grant select on sys.v_$pwfile_users to sqlguard;

grant select on sys.dba_col_privs to sqlguard;

MYSQL DB ライセンス

以下のドメインは、MYSQL DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

MYSQL: 末尾が_40 である照会では、最も基本的なバージョンの mysql スキーマ (MySQL 4.0 以降用) を使用します。information_schema は MySQL 5.0 で導入されてから変更されていないため、末尾が _50 の照会はありますが、末尾が _51 の照会はありません。 末尾が _50 の照会は、MySQL 5.0 および 5.1 で動作します。 また、information_schema は 6.0 でも変更される予定がないため、6.0 がリリースされた際には 6.0 でも動作します。末尾が _502 の照会 (MYSQL502) では、新しい information_schema を使用します。これにはより多くの情報が含まれ、実際のデータ・ディクショナリーにより一層類似しています。

- MYSQL データベース特権 40
- MYSQL ユーザー特権 40
- MYSQL ホスト特権 40
- MYSQL 表特権 40
- MYSQL データベース特権 500
- MYSQL ユーザー特権 500
- MYSQL ホスト特権 500
- MYSQL 表特権 500
- MYSQL データベース特権 502
- MYSQL ユーザー特権 502
- MYSQL ホスト特権 502
- MYSQL 表特権 502

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリストで、データベース表内 (またはデータベース表のビュー内) でライセンスが機能するために最小限必要な特権について説明します。

注: データをアップロードするには、必要な特権に加え、ユーザーが MYSQL データベースに接続することが必要です。

MySQL の全バージョンについて、MySQL 5.0.1 を使用したライセンス照会では、表集合 mysql.db mysql.host mysql.tables_priv mysql.user を使用します。

MySQL 5.0.2 以降の全バージョンについて、ライセンス照会では表集合 information_schema.SCHEMA_PRIVILEGES mysql.host information_schema.TABLE_PRIVILEGES information_schema.USER_PRIVILEGES を使用します。

データ・ソースに MYSQL データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての MYSQL データベースでループします。

DB2 DB ライセンス

以下のドメインは、DB2 DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

- DB2 列レベルの特権 (SELECT、UPDATE など)
- DB2 データベース・レベルの特権 (CONNECT、CREATE など)
- DB2 索引レベルの特権 (CONTROL)
- DB2 パッケージ・レベルの特権 (コード・パッケージ対象の BIND、EXECUTE など)
- DB2 表レベルの特権 (SELECT、UPDATE など)DB2 特権サマリー

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

GRANT SELECT ON SYSCAT.COLAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.INDEXAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PACKAGEAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.TABAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.SCHEMAAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PASSTHRUAUTH TO SQLGUARD;

SYBASE DB ライセンス

以下のドメインは、SYBASE DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

- GRANT オプションを含む、SYBASE ユーザーに付与されたシステム特権とロール
- GRANT オプションを含む、SYBASE ユーザーに権限付与されたロールおよびユーザーとロールに付与されたシステム特権
- SYBASE PUBLIC によるオブジェクト・アクセス
- PUBLIC に割り当てられた、プロシージャーおよび関数に対する SYBASE 実行特権
- システムまたはセキュリティー admin ロールを持つ SYBASE アカウント
- GRANT オプション付きで付与された SYBASE オブジェクト特権および列特権
- SYBASE ユーザーに権限付与されたロール

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

/* 以下は MASTER データベースでは必須です */

grant select on master.dbo.sysloginroles to sqlguard

grant select on master.dbo.syslogins to sqlguard

grant select on master.dbo.syssrvroles to sqlguard

/*以下は MASTER を含むすべてのデータベースで必須です */

grant select on sysprotects to sqlguard

grant select on sysusers to sqlguard

grant select on sysobjects to sqlguard

grant select on sysroles to sqlguard

データ・ソースに SYBASE データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての SYBASE データベースでループします。

Informix DB ライセンス

以下のドメインは、Informix DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

- データベース・アカウントによる Informix オブジェクト特権 (システム・アカウントとロールを除く)
- GRANT オプション付きでユーザーに付与された Informix データベース・レベル特権、ロール、および言語
- GRANT オプション付きでユーザーおよびロールに付与された Informix データベース・レベル特権、ロール、および言語
- Informix PUBLIC に付与されたオブジェクト権限
- PUBLIC に付与された Informix プロシージャーおよび関数に対する Informix 実行特権
- DBA 特権付きの Informix アカウント GRANT オプション付きで付与された Informix オブジェクト特権および列特権
- ユーザーおよびロールに権限付与された Informix ロール

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

システム・カタログの SELECT 特権については、すべてのユーザーが十分な特権を持っているため、どのユーザーにも特権を付与する必要はありません。Informix は、ユーザーに対してシステム・カタログを付与しないようです。通常は、権限付与が使用されます。 ただしこの場合は必要ありません。

grant select on systables to sqlguard;

grant select on systabauth to sqlguard;

grant select on sysusers to sqlguard;

grant select on sysroleauth to sqlguard;

grant select on syslangauth to sqlguard;

grant select on sysroutinelangs to sqlguard;

grant select on sysprocauth to sqlguard;

grant select on sysprocedures to sqlguard;

grant select on syscolauth to sqlguard;

データ・ソースに Informix データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての Informix データベースでループします。

MSSQL 2000 DB ライセンス

以下のドメインは、MSSQL 2000 DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「**DB ライセンス**」タブを表示します。

- MSSQL2000 デフォルトのシステム・ユーザーを除くデータベース・アカウントによるオブジェクト特権
- MSSQL2000 GRANT オプション付きでユーザーに付与されたロールおよびシステム特権
- MSSQL2000 ユーザーおよびロールに権限付与されたロール。GRANT オプション付きでユーザーおよびロールに付与されたシステム特権
- MSSQL2000 PUBLIC によるオブジェクト・アクセス
- MSSQL2000 PUBLIC に割り当てられたシステム・プロシージャーおよび関数に対する実行特権
- MSSQL2000 db_owner ロールおよび db_securityadmin ロールを持つデータベース・アカウント
- MSSQL2000 sysadmin、serveradmin、および security admin を持つサーバー・アカウント /* MASTER データベースに対してのみこのライセンスを実行します */
- MSSQL2000 GRANT オプション付きで付与されたオブジェクト特権および列特権
- MSSQL2000 ユーザーおよびロールに権限付与されたロール

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

/* 以下は MASTER データベースでは必須です */

grant select on dbo.syslogins to sqlguard

/*以下は MASTER を含むすべてのデータベースで必須です */

grant select on dbo.sysprotects to sqlguard

grant select on dbo.sysusers to sqlguard

grant select on dbo.sysobjects to sqlguard

grant select on dbo.sysmembers to sqlguard

データ・ソースに MSSQL データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての MSSQL データベースでループします。

MSSQL 20005/2008 DB ライセンス

以下のドメインは、MSSQL 2005 または MSSQL 2008 DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「**DB ライセンス**」タブを表示します。

注: リストされている MSSQL2005 のライセンス・ドメインは、MSSQL2008 でも使用できます。

- MSSQL2005/8 デフォルトのシステム・ユーザーを除くデータベース・アカウントによるオブジェクト特権
- MSSQL2005/8 ユーザーに付与されたロールおよびシステム特権
- MSSQL2005/8 GRANT オプション付きでユーザーおよびロールに付与されたロールおよびシステム特権
- MSSQL2005/8 PUBLIC によるオブジェクト・アクセス
- MSSQL2005/8 PUBLIC に割り当てられたシステム・プロシージャーおよび関数に対する実行特権
- MSSQL2005/8 db_owner ロールおよび db_securityadmin ロールのデータベース・アカウント
- MSSQL2005/8 sysadmin、serveradmin、security admin のサーバー・アカウント /* MASTER データベースに対してのみ実行します */
- MSSQL2005/8 GRANT オプション付きで付与されたオブジェクト特権および列特権
- MSSQL2005/8 ユーザーおよびロールに付与されたロール

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

/* 以下は MASTER データベースでは必須です */

grant select on sys.server_principals to sqlguard

/*以下は MASTER を含むすべてのデータベースで必須です */

grant select on sys.database_permissions to sqlguard

grant select on sys.database_principals to sqlguard

grant select on sys.all_objects to sqlguard

grant select on sys.database_role_members to sqlguard

grant select on sys.columns to sqlguard

データ・ソースに MSSQL データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての MSSQL データベースでループします。

Netezza DB ライセンス

以下のドメインは、Netezza DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、**「DB ライセンス」**タブを表示します。

注: Netezza では、データベース・エラーのテキスト変換は行われません。エラーは例外の記述に表示されます。ユーザーは、必要に応じて Netezza の例外の記述を含むレポートのコピーを作成したり、追加したりできます。

- 「Netezza オブジェクト特権 (データベース・ユーザー名別)」 - ADMIN アカウント以外のデータベース・ユーザー名により、GRANT オプション付きまたはなしで付与されたオブジェクト特権
- 「Netezza 管理者特権 (データベース・ユーザー名別)」 - ADMIN アカウント以外のデータベース・ユーザー名により、GRANT オプション付きまたはなしで付与された管理者特権
- 「Netezza ユーザーに権限付与されたグループ/ロール」 - ユーザーに権限付与されたグループ (ロール)
- 「Netezza オブジェクト特権 (グループ別)」 - PUBLIC を除くグループにより、GRANT オプション付きまたはなしで付与されたオブジェクト特権
- 「Netezza 管理者特権 (グループ別)」 - PUBLIC を除くグループにより、GRANT オプション付きまたはなしで付与された管理者特権
- 「Netezza 管理者特権 (データベース・ユーザー名グループ別)」 - ADMIN アカウントおよび PUBLIC グループを除くデータベース・ユーザー名およびグループにより、GRANT オプション付きまたはなしで付与された管理者特権
- 「Netezza 付与されたオブジェクト特権」 - GRANT オプション付きまたはなしで PUBLIC に対して付与されたオブジェクト特権
- 「Netezza 付与された管理者特権」 - GRANT オプション付きまたはなしで PUBLIC に対して付与された管理特権
- 「Netezza ユーザーおよびグループに対するグローバル管理者特権」 - ADMIN アカウントを除くユーザーおよびグループに付与されたグローバル管理者特権
- 「Netezza ユーザーおよびグループに対するグローバル・オブジェクト特権」 - ADMIN アカウントを除くユーザーおよびグループに付与されたグローバル・オブジェクト特権

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

```
/* 以下の表およびビューに対する選択特権は必須です */

/* このスクリプトは、システム・データベースから実行する必要があります */

GRANT SELECT ON SYSTEM VIEW TO sqlguard;

GRANT LIST ON DATABASE TO sqlguard;

GRANT LIST ON USER TO sqlguard;

GRANT LIST ON GROUP TO sqlguard;

GRANT SELECT ON _V_CONNECTION TO sqlguard;
```

Netezza ライセンス照会では、特にこれらのレポートを実行する予定のユーザーに対して特権を付与する際に、システム・データベースへの接続が推奨されます。特権の付与は、システム・データベースから行う必要があります。それ以外のデータベースから付与された特権は、その特定のデータベースでのみ有効になります。システム・データベースから特権の付与が行われた場合は、特殊機構により、付与された特権がすべてのデータベースで有効になります。

Teradata DB ライセンス

以下のドメインは、Teradata DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、**「DB ライセンス」**タブを表示します。

- デフォルトのシステム・ユーザーを除くデータベース・アカウントにより付与された Teradata オブジェクト特権
- GRANT オプション付きで Teradata ユーザーに付与されたシステム特権とロール
- GRANT オプション付きで Teradata ユーザーおよびロールに権限付与されたロール
- Teradata ユーザーおよびロールに権限付与されたロール。 GRANT オプション付きでユーザーおよびロールに付与されたシステム特権。
- PUBLIC に対して付与された Teradata オブジェクト特権およびシステム特権。Teradata では、PUBLIC に対してロールを権限付与できないことに注意してください。
- PUBLIC に対して付与されたシステム・データベース・オブジェクトに対する Teradata 実行特権
- ユーザーおよびロールに付与された Teradata システム管理者特権およびセキュリティー管理者特権
  注: Teradata には、システム管理者またはセキュリティー管理者というロールはありません。ユーザーは独自のロールを作成する必要があります。次のような重要なシステム特権は、通常、一般的なユーザーに付与されません: ABORT SESSION、CREATE DATABASE、CREATE PROFILE、CREATE ROLE、CREATE USER、DROP

DATABASE、DROP PROFILE、DROP ROLE、DROP USER、MONITOR RESOURCE、MONITOR SESSION、REPLICATION OVERRIDE、SET SESSION RATE、SET RESOURCE RATE。

- GRANT オプション付きでユーザーに付与された Teradata オブジェクト特権。DBC および grantee = 'All' は含みません。

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

```
/* 以下の表およびビューに対する選択特権は必須です */

GRANT SELECT ON DBC.AllRights TO sqlguard;

GRANT SELECT ON DBC.Tables TO sqlguard;

GRANT SELECT ON DBC.AllRoleRights TO sqlguard;

GRANT SELECT ON DBC.RoleMembers TO sqlguard;
```

PostgreSQL DB ライセンス

以下のドメインは、PostgreSQL DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、**「DB ライセンス」**タブを表示します。

PostgreSQL には、7 つのライセンス・カスタム・ドメイン、照会、レポートがあります。これを以下に示します (それぞれについてレポート名、説明、注記を示します)。

- 「PostgreSQL GRANT オプションあり/なしで PUBLIC ユーザー・ロールに付与されたデータベースに対する特権」。GRANT オプション付きまたはなしで、PUBLIC、ユーザーおよびロールに付与されたデータベースに対する特権です。任意のデータベース (理想的には PostgreSQL) でこれを実行します。
- 「PostgreSQL GRANT オプションあり/なしで PUBLIC ユーザー・ロールに付与された言語に対する特権」。GRANT オプション付きまたはなしで、PUBLIC、ユーザーおよびロールに対して付与された言語に対する特権です。
- 「PostgreSQL GRANT オプションあり/なしで PUBLIC ユーザー・ロールに付与されたスキーマに対する特権」。GRANT オプション付きまたはなしで、PUBLIC、ユーザーおよびロールに付与されたスキーマに対する特権です。
- 「PostgreSQL GRANT オプションあり/なしで PUBLIC ユーザー・ロールに付与された表スペースに対する特権」。GRANT オプション付きまたはなしで、PUBLIC、ユーザーおよびロールに対して付与された表スペースに対する特権です。任意のデータベース (理想的には PostgreSQL) でこれを実行します。
- 「ユーザーまたはロールに付与された PostgreSQL ロールまたはユーザー」。GRANT オプション付きでユーザーまたはロールに権限付与されたロールまたはユーザーです。任意のデータベースでこれを一度実行します。理想的には PostgreSQL で実行します。
- 「PostgreSQL ユーザーまたはロールに権限付与されたスーパーユーザー」。ユーザーまたはロールに権限付与されたスーパーユーザーです。任意のデータベースでこれを一度実行します。理想的には PostgreSQL で実行します。
- 「PostgreSQL ユーザーおよびロールに付与されたシステム特権」。ユーザーおよびロールに付与されたシステム特権です。任意のデータベースでこれを一度実行します。理想的には PostgreSQL で実行します。
- 「PostgreSQL PUBLIC に付与された表、ビュー、シーケンス、および関数特権」。PUBLIC に対して付与された、表、ビュー、シーケンス、および関数特権です。データベースごとにこれを実行します。
- 「PostgreSQL GRANT オプション付きで付与された表、ビュー、シーケンス、および関数特権」。GRANT オプションのみを付加して、ユーザーおよびロールに付与された表、ビュー、シーケンス、および関数特権です。PostgreSQL アカウントを除きます。
- 「PostgreSQL ロールに付与された表、ビュー、シーケンス、関数特権」。ロールに付与された、表、ビュー、シーケンス、および関数特権です。 PUBLIC は除きます。
- 「PostgreSQL ログインに付与された表、ビュー、シーケンス、および関数特権」。ログインに付与された、表、ビュー、シーケンス、および関数特権です。postgres システム・ユーザーを除きます。

注: バージョン 8.3.6 以降、PostgreSQL では PUBLIC に対する管理者オプションの付与をサポートしていません。関数のみで、ストアード・プロシージャーはありません。表の権限付与のみがサポートされ、列の権限付与はサポートされていません。PUBLIC はグループであり、ユーザーではありません。PUBLIC は、pg_roles には表示されません。これらのすべての照会を実行する必要がある特権は、「GRANT CONNECT ON DATABASE PostgreSQL TO username;」のみです。

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

```
/* 以下の表およびビューに対する選択特権は必須です */

/*これは POSTGRES データベースで必須です。*/
```

```
grant connect on database postgres to sqlguard;


/*以下は POSTGRES を含むすべてのデータベースで必須です (デフォルトで既に PUBLIC に付与されています) */
grant select on pg_class to sqlguard;
grant select on pg_namespace to sqlguard;
grant select on pg_roles to sqlguard;
grant select on pg_proc to sqlguard;
grant select on pg_auth_members to sqlguard;
grant select on pg_language to sqlguard;
grant select on pg_tablespace to sqlguard;
grant select on pg_database  to sqlguard;
```

データ・ソースに PostgreSQL データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての PostgreSQL データベースでループします。

親トピック: ドメイン、エンティティー、および属性

エンティティーおよび属性

このトピックでは、各エンティティーに含まれる属性について説明します。

ドメイン、エンティティー、および属性の概要については、『ドメイン、エンティティー、および属性』を参照してください。すべてのドメインの説明については、『ドメイン』を参照してください。

z/OS データ・ソース (Db2、データ・セット、および IMS) には、データ・ソース固有の属性があり、既存の属性の意味が、ここで説明する内容と異なる場合があります。z/OS データ・ソースに固有のエンティティーおよび属性について詳しくは、以下の資料を参照してください。

- データ・セットのレポート・エンティティーおよび属性
- Db2 for z/OS のレポート・エンティティーおよび属性
- IMS のレポート・エンティティーおよび属性

「アクセス・ポリシー」エンティティー

システム上で使用可能なすべてのポリシーを記述します。このエンティティーは、システム上にインストールされているすべてのポリシーに対して使用される「インストール済みポリシー」エンティティーに類似しています。

アクセス・ポリシーのエンティティー・リスト - 「アクセス・ポリシー」エンティティー、「ルール・ポリシー」エンティティー、「ルール・アクション」エンティティー、および「アラート通知」エンティティー。属性のリストについては、「ルール」エンティティーを参照してください。 属性のリストについては、「ルール・アクション」エンティティーを参照してください。属性のリストについては、「アラート通知」エンティティーを参照してください。

表 1. 「アクセス期間」エンティティー

属性	記述
ポリシー ID	アクセス・ポリシーを一意的に識別します。
ポリシーの記述	アクセス・ポリシーを記述します。
選択的な監査証跡	これが選択的な監査証跡ポリシーであるかどうかを示します (T/F)。
監査パターン	選択的な監査証跡ポリシーに使用されたテスト・パターン。
タイム・スタンプ	レコード作成のタイム・スタンプ。

「アクセス期間」エンティティー

アクセス期間はセッションに関連します。デフォルトではアクセス期間の長さは 1 時間ですが、Guardium 管理者は「検査エンジン構成」で変更することができます (「ロギング単位」に該当)。

タイムアウト値は、アナライザー・スレッドが開いたセッションの数によって異なります。 アナライザー・スレッドごとに、デフォルト値は以下のようになります。オープン・セッション数が >0 かつ < 250 の場合、タイムアウトは 60 分です。 オープン・セッション数が >= 250 かつ < 500 の場合、タイムアウトは 30 分です。 オープン・セッション数が >= 500 かつ < 750 の場合、タイムアウトは 15 分です。オープン・セッション数が >= 750 かつ < 1200 の場合、タイムアウトは 5 分です。 オープン・セッション数が >= 1200 の場合、タイムアウトは 2 分です。

表 2. 「アクセス期間」エンティティー

属性	記述
セッション ID	セッションを一意的に識別します。
インスタンス ID	構造のインスタンスを一意的に識別します。
構造 ID	コマンド構造 (例えば select a from b) を一意的に識別します。

属性	記述
アクセス合計	このアクセス期間における構造インスタンスの総数。
期間の開始日	期間開始属性の中の日付のみ。
期間の開始曜日	期間開始属性の中の曜日のみ。
期間の開始時刻	期間開始属性の中の時刻のみ。
タイム・スタンプ	初めは、アクセス期間中にクライアント/サーバー接続上で要求が初めて確認されたときに、タイム・スタンプ値が設定されます。 デフォルトではアクセス期間の長さは 1 時間ですが、Guardium 管理者は「検査エンジン構成」で変更することができます (「Guardium 管理者ガイド」を参照)。 その後は、後続の要求ごとに、その期間の平均実行時間とコマンド数が更新されるときに更新されます。
期間の終了	アクセス期間の終了の日時。
期間の終了日	期間終了属性の中の日付のみ。
期間の終了曜日	期間終了属性の中の曜日のみ。
期間の終了時刻	期間終了属性の中の時刻のみ。
アプリケーション・ユーザー	アプリケーション・ユーザー名。
平均実行時間	期間中の平均コマンド実行時間。SQL ステートメントのみが対象です。FTP および Windows ファイル共有トラフィックには適用されません。
失敗した SQL (2)	失敗した SQL 要求の数。表の最後に記載されている注を参照してください。
成功した SQL (2)	成功した SQL 要求の数。表の最後に記載されている注を参照してください。
アプリケーション・イベント ID	アプリケーション・イベント ID (API から設定された場合)。
影響を受けるレコード合計 (2)	影響を受けたレコードの総数。表の最後に記載されている注を参照してください。
影響を受けるレコードの平均 (2)	影響を受けたレコードの平均数。表の最後に記載されている注を参照してください。
影響を受けるレコード合計 (名前) (2)	「影響を受けるレコード合計」属性が数値ではなく文字列の場合、その値はここに表示されます (例えば、「大規模結果セット」や N/A)。 「影響されるレコード」- SQL ステートメントを実行するたびに影響を受けるレコードの数を示す結果セット。 注: 「影響されるレコード」オプションは、スニファーに対して、追加の応答パケットを処理し、影響を受けたデータ (バッファー・サイズを増やし、スニファー全体のパフォーマンスに悪影響を及ぼす可能性があるデータ) のロギングを延期するように要求するスニファー操作です。 大きな影響を受けるのは、非常に大きい応答からです。この操作に関連する大量のオーバーヘッドを避けるために、Guardium はデフォルトのしきい値セットを使用して、しきい値を超えたときに、処理操作をスキップすることをスニファーが決定できるようにします。 CLI コマンド store max_results_set_size、store max_result_set_packet_size、および store max_tds_response_packets を使用して、細分度のレベルを設定することができます。 結果セットの値の例は次のとおりです。 • ケース 1、「影響されるレコード」値: 正数 - これは、結果セットの正しいサイズを表します。 • ケース 2、「影響されるレコード」値: -2 - これは、レコード数が構成可能な限度 (CLI インターフェースによって調整可能) を超えたことを示します。 • ケース 3、「影響されるレコード」値: -1 - これは、Guardium によってサポートされないパケット構成のケースを示します。 • ケース 4、「影響されるレコード」値: -2 - 結果セットがストリーム・モードで送信される場合。 • ケース 5、「影響されるレコード」値: -2 - ユーザーを現在の値について更新するためのレコードのカウント中の中間結果。最終的には、レコードの合計を示す正数になります。
秒を表示	1 秒当たりのアクセス数がトラッキングされている場合、アクセス期間内 (通常は 1 時間) の秒ごとのカウントがここに含まれています。
実行確認応答時間の平均	実行確認応答時間の平均 (ミリ秒単位)。
元のタイム・ゾーン	UTC オフセット。 これは、2 つの異なるタイム・ゾーンに存在する 2 つの異なるコレクターの時間を、正しく統合するために設定する必要がある UTC オフセットを示すものです。 オフセットを設定しなかった場合、物事の発生時刻をユーザーが判別したり、正確な表記で参照したりできないという状況が存在していまいます。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「セッション ID」、「インスタンス ID」、「構造 ID」、および「アクセス合計」は、admin ロールを持つユーザーのみが使用できます。

「失敗した SQL」、「成功した SQL」、「アプリケーション・イベント ID」、「影響を受けるレコード合計」、「影響を受けるレコードの平均」、および「影響を受けるレコード合計 (名前)」は、照会のメイン・エンティティーでこのレベルの詳細が可能な場合のみ表示される属性です。「クライアント/サーバー」または「セッション」のどちらかがメイン・エンティティーである場合、これらは使用できません。

「アクセス・ルール」エンティティー

アクセス・ルールにその定義時に割り当てられた名前。アクセス・ルール違反がログに記録されているときに、所有「ポリシー・ルール違反」エンティティー (後述) からのレポート作成にのみ使用可能です。

表 3. 「アクセス・ルール」エンティティー

属性	記述
アクセス・ルールの記述	アクセス・ポリシー・ルール定義に含まれる記述。

「アクティビティー・タイプ」エンティティー

「統合/アーカイブ」ドメインからのみ使用可能。「統合/アーカイブ」ドメインは、デフォルトでは、admin ロールが割り当てられたユーザーのみが使用できます。「アクティビティー・タイプ」エンティティーは、所有する「統合/インポート/エクスポート・ログ」エンティティーからのみアクセス可能です。このエンティティーは、アクションのタイプ (統合の準備、暗号化、送信など) を示します。 .

表 4. 「アクティビティー・タイプ」エンティティー

属性	記述
アクティビティー・タイプ	統合/インポート/エクスポート・アクティビティーの記述。

「統合/アーカイブ・ログ」エンティティー

「統合/アーカイブ」ドメインからのみ使用可能。「統合/アーカイブ」ドメインは、デフォルトでは、admin ロールが割り当てられたユーザーのみが使用できます。 アクティビティーごとに「統合/インポート/エクスポート・ログ」エンティティーが 1 つ以上作成されます。 例えば、アグリゲーター・システムがデータをインポートするときに、通常は少なくとも次の 4 つのアクティビティーが表示されます。

統合の準備

重複インポートの検査 (ファイル当たり 1 つをこのアグリゲーターにエクスポート)

抽出 (ファイル当たり 1 つがマージの対象)

マージ (ファイル当たり 1 つをマージ)

表 5. 「統合/アーカイブ・ログ」エンティティー

属性	記述
タイム・スタンプ	ログに記録されるアクティビティー (アーカイブの準備、暗号化、送信など) の開始時と終了時に更新されます。 .
状況	統合/インポート/エクスポート・ログ・アクティビティーの状況。
ユーザー名	アクティビティーの開始に使用されたユーザー名。
開始時刻	アクティビティーの開始時刻。
終了時刻	アクティビティーの終了時刻。
期間の開始	対象データの開始時刻。 アーカイブまたは統合の各アクティビティーは、丸 1 日のアクティビティーを対象とします。
期間の終了	対象データの終了時刻。
ファイル名	アクティビティーに使用されたファイルの名前。アーカイブおよびエクスポート操作によって作成されるファイルには、次のような名前が付けられます。 <daysequence>-<scp_host>-w<run_datestamp>-d<data_date>.dbdump.enc 例: 732423-g1.guardium.com-w20050425.040042-d2005-04-22.dbdump.enc ファイルに含まれるデータの日付は、ファイル名の終わり近く (.dbdump.enc の直前) にある data_date (形式は yyyy-mm-dd) です。 この日付と実行日を混同しないように気を付けてください。実行日はファイル名の中の前の方にあり、データがアーカイブまたはエクスポートされた日付を示します。
コメント	アクティビティーに関する追加コメント。
Guardium ホスト名	Guardium ホストの名前。
パージされたレコード	アクティビティー・タイプが「パージ」の場合は、パージされたレコード数。 それ以外の場合は「N/A」。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「アラート通知」エンティティー

ポリシー・アラート通知について示します。

表 6. 「アラート通知」エンティティー

属性	記述

属性	記述
ALERT_NOTIFICATION_ID	アラート通知を識別します。
ALERT_ID	アラート定義を識別します。
アラート通知タイプ	ポリシー・ルール定義に含まれるアラートのタイプ。
アラート・ユーザー	アラートの受信者。
アラート宛先	アラートのタイプ (EMAIL、SNMP、SYSLOG、CUSTM)。
タイム・スタンプ	作成されたタイム・スタンプ・アラート・レコード。

ALERT_NOTIFICATION_ID および ALERT_ID は、admin ロールを持つユーザーのみが使用できます。

「アプリケーション・データ」エンティティー

SAP および Siebel レポートに使用されます。

表 7. 「アプリケーション・データ」エンティティー

属性	記述
アプリケーション・データ ID	このデータの固有 ID。
アプリケーション・コード	アプリケーション・タイプ・コード。
完全な SQL ID	完全な SQL データを識別します。
アプリケーション・タイプ	アプリケーション・タイプ。
ユーザー	アプリケーション・ユーザー名。
操作タイプ	操作のタイプ。
変更日	変更の日付。
タイム・スタンプ	このレコードのタイム・スタンプ。
項目名	影響を受けた項目の名前。
トランザクション・コード	トランザクション・コード。
システム ID	システムの固有 ID。
レコード詳細 1	項目タイプによって異なります。
レコード詳細 2	項目タイプによって異なります。
レコード詳細 3	項目タイプによって異なります。
レコード詳細 4	項目タイプによって異なります。
VBKey	VBKey 値。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「アプリケーション・イベント」エンティティー

このエンティティーは、アプリケーション・イベント API 呼び出し (これらの属性値を設定する) またはカスタム識別プロシージャーと識別されたストアード・プロシージャー呼び出し (ストアード・プロシージャー・パラメーターをこれらの属性にマップする) をシステムが確認するたびに、作成されます。

表 8. 「アプリケーション・イベント」エンティティー

属性	記述
アプリケーション・イベント ID	この「アプリケーション・イベント」エンティティーの固有 ID。
イベント・ユーザー名	ユーザー名 (GuardAppEvent:Start で設定)。
イベント・タイプ	イベントのタイプ (GuardAppEvent:Start で設定)。
イベント値 (文字列)	文字列値 (GuardAppEvent:Start で設定)。
イベント値 (数値)	数値 (GuardAppEvent:Start で設定)。
イベントの日付	日時値 (GuardAppEvent:Start で設定)。yyyy-mm-dd hh:mm:ss 形式で表示されます。 注: yyyy-mm-dd 以外の形式を使用してイベント日付を設定すると、内容はすべてゼロになります。時刻部分 (hh:mm:ss) はオプションであり、省略した場合は 00:00:00 になります。
タイム・スタンプ	イベントがログに記録されるときに 1 回だけ作成されます。この属性と「イベントの日付」属性を混同しないでください。「イベントの日付」は、API 呼び出しを使用するかストアード・プロシージャー・パラメーターから設定できる属性です。 (アプリケーション・イベント API およびカスタム識別プロシージャーの説明は、「Guardium 管理者ガイド」を参照してください。)

属性	記述
イベント・リリース・タイプ	イベントのタイプ (GuardAppEvent: Released で設定)。
イベント・リリース・ユーザー名	ユーザー名 (GuardAppEvent: Released で設定)。
イベント・リリース値 (文字列)	文字列値 (GuardAppEvent: Released で設定)。
イベント・リリース値 (数値)	数値 (GuardAppEvent: Released で設定)。
イベント・リリース日付	日時値 (GuardAppEvent: Released で設定)。yyyy-mm-dd hh:mm:ss 形式で表示されます。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「アプリケーション・イベント ID」は、admin ロールを持つユーザーのみが使用できます。

「アプリケーション・ユーザー名」エンティティー

このエンティティーは、アプリケーション・イベントが存在する場合に、アプリケーション・イベントから取得したユーザー名を表示します。 存在しない場合、構成体インスタンスから取得したユーザー名が表示されます。

表 9. 「アプリケーション・ユーザー名」エンティティー

属性	記述
アプリケーション・ユーザー名	この「アプリケーション・ユーザー名」エンティティーの固有 ID。

「評価ログ」エンティティー

このエンティティーは、評価が実行されるたびに作成されます。

表 10. 「評価ログ」エンティティー

属性	記述
アセスメント・ログ ID (Assessment Log ID)	評価を一意的に識別します。
タイム・スタンプ	評価のタイム・スタンプ。
タイム・スタンプの日付	タイム・スタンプの日付部分。
タイム・スタンプの時刻	タイム・スタンプの時刻部分。
評価ログ・タイプ	定義済みの照会またはカスタム・テスト。
評価ログ重大度	アセスメント・テスト重大度: クリティカル、メジャー、マイナー、注意、情報。これは重大度分類のレベルで順序付けされたリストです。アセスメント・テスト重大度: クリティカル、メジャー、マイナー、注意、情報。最も重大度の高いものは、このリストの最初の分類です。最も重大度の低いものは、このリストの最後の分類です。
アセスメント結果 ID1	アセスメント結果セットを識別します。
メッセージ	評価によって返されたメッセージ。
詳細	この評価の詳細。

「アセスメント・ログ ID (Assessment Log ID)」は、admin ロールを持つユーザーのみが使用できます。

「アセスメント結果データ・ソース」エンティティー

このエンティティーは、評価テストによってアクセスされたデータ・ソースを識別します。

表 11. 「アセスメント結果データ・ソース」エンティティー

属性	記述
アセスメント結果データ・ソース ID	データ・ソースの結果セットを識別します。
アセスメント結果 ID	結果を識別します。
データベース・タイプ	データベース・タイプ: Oracle、MS-SQL、DB2®、Sybase、Informix® など。
データベース名	データベース名。
バージョン・レベル	データベースのバージョン・レベル。
パッチ・レベル	データベースのパッチ・レベル。
フル・バージョン情報	データ・ソースのフル・バージョン情報。

属性	記述
データ・ソース名	データ・ソースの名前。
記述	データ・ソースの記述。
ホスト	データ・ソースのホスト名。
ポート	ホスト上のポート番号。
サービス名	データ・ソースのサービス名。
ユーザー名	データ・ソース・アクセスに使用されたユーザー名。

「アセスメント結果データ・ソース ID」および「アセスメント結果 ID」は、admin ロールを持つユーザーのみが使用できます。

「アセスメント結果ヘッダー」エンティティー

このエンティティーは、アセスメント結果セットのタスクごとに作成されます。

表 12. 「アセスメント結果ヘッダー」エンティティー

属性	記述
アセスメント結果 ID	アセスメント結果セットを識別します。
アセスメント ID	評価を識別します。
タスク ID	評価内のタスクを識別します。
パラメーター変更フラグ	最後の実行以降にパラメーターが変更されたかどうかを示します。
実行日	評価が実行された日付。
すべてで受信	これらの結果が配布リスト上のすべての受信者で受信されたかどうかを示します。
全体的なスコア	評価の全体スコア。
開始日付	評価の開始日付。
終了日付	評価の終了日付。
評価の記述	定義に含まれる評価名。
クライアント IP フィルター	選択クライアント: 厳密な IP アドレス、ワイルドカード (*) を含んだアドレス、または空 (すべて選択)
サーバー IP フィルター	選択サーバー: 厳密な IP アドレス、ワイルドカード (*) を含んだアドレス、または空 (すべて選択)
推奨	タスクに対して返された推奨。

「アセスメント結果 ID」、「アセスメント ID」、および「タスク ID」は、admin ロールを持つユーザーのみが使用できます。

「評価テスト」エンティティー

このエンティティーには、使用可能なテストの項目が含まれます。

表 13. 「評価テスト」エンティティー

属性	記述
テストの記述	テストのテキストの記述。
テスト・タイプ	評価テストのタイプ (監視、事前定義、カスタム、照会ベース、CVE)。
データ・ソース・タイプ	データ・ソースのタイプ (DB2、Informix、MYSQL、ORACLE、SYBASE など)。
しきい値	ユーザー定義のしきい値。テストの作成時に定義された値をオーバーライドします。
しきい値のデフォルト値	合格/不合格の基準を定義したデフォルトのしきい値。
重大度	評価の重大度 (クリティカル、メジャー、マイナー、注意、情報)。
カテゴリー	評価のカテゴリー (特権、認証、構成、バージョン、その他)。
タイム・スタンプ	テストが作成されたときのタイム・スタンプ。

「監査プロセス」エンティティー

このエンティティーには、監査プロセスの基本定義パラメーターが含まれます。

表 14. 「監査プロセス」エンティティー

属性	記述
プロセスの記述	監査プロセス定義に含まれる記述。
アクティブ	プロセスがアクティブかどうか (スケジュール設定できるかどうか) を示します。
結果の保持 (日数)	結果が保持される日数。
結果の保持 (数量)	保持される結果セットの数。

属性	記述

「監査プロセス・コメント」エンティティー

このエンティティーには、監査プロセス定義に付加されたコメントが含まれます。監査プロセスの結果に付加されたコメントは、「監査プロセスの結果コメント」エンティティーに含まれます。

表 15. 「監査プロセス・コメント」エンティティー

属性	記述
監査プロセス・コメント	コメントのテキスト。
監査プロセス・コメントの作成者	コメントの作成者。
監査プロセス・コメントのタイム・スタンプ	コメントのタイム・スタンプ。

「監査タスク」エンティティー

このエンティティーは、単一の監査タスク (監査プロセス内) について示します。

表 16. 「監査タスク」エンティティー

属性	記述
タスク・タイプ	数値は、タスクがレポート、セキュリティー・アセスメント、エンティティー監査証跡、プライバシー・セット、または分類プロセスのいずれであるかを示します。これらのタイプには別名が定義されるので、レポートに別名が使用され、読みやすいレポート出力になります。
タスクの記述	タスク定義に含まれるタスクの名前。

「監査プロセスの結果」エンティティー

このエンティティーには、監査プロセスの結果セットの実行日が含まれます。

表 17. 「監査プロセスの結果」エンティティー

属性	記述
実行日	監査プロセスが実行された日付。

「監査プロセスの結果コメント」エンティティー

このエンティティーには、監査プロセスの結果に付加されたコメントが含まれます。監査プロセス定義に付加されたコメントは、「監査プロセス・コメント」エンティティーに含まれます。

表 18. 「監査プロセスの結果コメント」エンティティー

属性	記述
監査プロセス・コメント	コメントのテキスト。
監査プロセス・コメントの作成者	コメントの作成者。
監査プロセス・コメントのタイム・スタンプ	コメントのタイム・スタンプ。

「オートディスカバリー・スキャン」エンティティー

このエンティティーは、いつスキャンが実行されたかを識別します。

表 19. 「オートディスカバリー・スキャン」エンティティー

属性	記述
スキャン・タイム・スタンプ	スキャンが実行された時刻。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「変更された列」エンティティー

このエンティティーは、変更された列について示します。

表 20. 「変更された列」エンティティー

属性	記述
変更された列名	データベース上の変更された列の名前。
古い値	変更前の値。
新しい値	変更後の値。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「変更後のデータ値」エンティティー

このエンティティーは、IBM InfoSphere Change Data Capture (InfoSphere CDC) レプリケーション・ソリューションとともに使用されます。このソリューションを使用すると、サポートされるデータベースとの相互レプリケーションを行うことができます。レプリケーションされたデータベースを保守することにより、処理のオーバーヘッドとネットワーク・トラフィックを低減することができます。

Database Activities Monitoring を使用する IBM Guardium ユーザーは、InfoSphere CDC にアクセスできます。

この Guardium 機能は、Java CDC ユーザー出口を使用して、値の変更情報を Guardium コレクターに送信します。

InfoSphere CDC のユーザー出口を使用すると、ユーザーは、指定された表に対してデータベース・イベントが発生する前または後に InfoSphere CDC で実行可能な一連のアクションを定義することができます。

表 21. 「変更後のデータ値」エンティティー

属性	記述
完全な SQL ID	完全な SQL の固有 ID。
表名	データベースの表名。
列名	データベースの列名。
古い値	変更前の値。
新しい値	変更後の値。
タイム・スタンプ	レコードが作成された時刻。

データベース・サーバーにインストールする必要がある 2 つのファイルは、IBM の InfoSphere Change Data Capture (InfoSphere CDC) アプリケーションとのインターフェースを取る Guardium エージェント用のファイルです。これらのファイルは、ビルドの sources/apps/GuardCDC/lib/ ディレクトリー内にあります。これらのファイルは、protobuf-java-2.4.1.jar と GuardCdc.jar です。

インストールの手順

前提条件 - InfoSphere Change Data Capture (InfoSphere CDC) アプリケーションが、データベース・サーバーに既にインストールされている必要があります。

データベース・サーバーに Guardium エージェントをインストールする手順:

1. これら 2 つのファイルを cdchome ディレクトリーの RepEngine/lib/ ディレクトリーにコピーします。絶対パスは、例えば /cdchome/cdc6.5.2/RepEngine/lib/ のようになります。
2. 各ファイルを unzip します。
3. guard_cdc_user_exit_config.mxl ファイルを編集して、Guardium_Host 名を追加します。このファイルが置かれる場所は、例えば /cdchome/cdc6.5.2/RepEngine/lib/com/guardium/cdc/userexit/ のようになります。
4. GuardiumAgent に書き込みを行うように InfoSphere CDC を構成します。CDC アプリケーションのセットアップと構成には、いくつものステップがあります。これらのステップは、IBM の InfoSphere CDC 開発/サポート・チームから入手できます。

「分類プロセスの結果」エンティティー

このエンティティーは、実行される分類プロセス・ルールごとに作成されます。

表 22. 「分類プロセスの結果」エンティティー

属性	記述
カタログ	結果セットのカタログのロケーション。
スキーマ	スキーマ名 (該当する場合)。
表名	ルール定義に含まれる表名。
列名	ルール定義に含まれる列名。
ルールの記述	分類ポリシー・ルールの記述。
コメント	このルール定義に追加されたコメント。
分類名	ルールの分類。

属性	記述
カテゴリー	ルールのカテゴリー。
データ・ソースの記述	ルールのデータ・ソース。

「分類プロセス実行」エンティティー

このエンティティーは、分類プロセスのジョブ実行について示します。

表 23. 「分類プロセス実行」エンティティー

属性	記述
プロセスの記述	プロセス定義から。
状況	ジョブの状況。
キュー日時	ジョブが分類/評価キューに実行依頼されたときのタイム・スタンプ。
開始日時	ジョブ開始時のタイム・スタンプ。
終了日時	ジョブ終了時のタイム・スタンプ。
データ・ソース	ジョブのデータ・ソース・リストを識別します。

「クライアント/サーバー」エンティティー

このエンティティーは、特定のクライアント/サーバー接続について示します。固有の属性セット (タイム・スタンプを除く) が検出されるたびにインスタンスが作成されます。

表 24. 「クライアント/サーバー」エンティティー

属性	記述
アクセス ID	このクライアント/サーバー接続の固有 ID。
タイム・スタンプ	このエンティティーのすべての属性が静的情報を持つので、このタイム・スタンプは、定義済みクライアント/サーバー接続上で Guardium が要求を初めて確認したときに、1 回だけ作成されます。
タイム・スタンプの日付	そのタイム・スタンプの日付のみ。
タイム・スタンプの時刻	そのタイム・スタンプの時刻のみ。
タイム・スタンプの曜日	そのタイム・スタンプの曜日のみ。
タイム・スタンプの年	そのタイム・スタンプの年のみ。
サーバー・タイプ	DB2、Oracle、Sybase など。
クライアント IP	クライアントの IP アドレス。
サーバー IP	サーバーの IP アドレス。
ネットワーク・プロトコル	使用されたネットワーク・プロトコル (例えば TCP、UDP など。Oracle 上の K-TAP については IPC かまたは BEQ として表示される場合があります)。
データベース・プロトコル	データベース・サーバー固有のプロトコル。
データベース・プロトコル・バージョン	データベース・プロトコルのプロトコル・バージョン。
データベース・ユーザー名	データベース・ユーザー名。データベース・ユーザー名は、ローカルまたはリモートのデータベースに接続したユーザーです。
ソース・プログラム	相互作用のソース・プログラム。
クライアント MAC	クライアントのハードウェア・アドレス。
クライアント・ホスト名	クライアント・ホスト名。
サービス名	相互作用のサービス名。場合によっては (例えば AIX® 共有メモリー接続)、別名がサービス名になり、実際のサービスが接続されるまで別名が使用されます。このような場合、実際のサービスが接続された時点で、新しいセッションが開始されます。したがって、ユーザーには単一セッションと認識されるものが 2 つのセッションとしてログに記録されることになります。 Teradata の場合、サービス名にはセッション論理ホスト ID 値が含まれます。

属性	記述
サーバー OS	サーバーのオペレーティング・システム。 Informix の場合、OS が次のように表示される場合があります。 IEEEM (Unix または JDBC を表します) IEEEI (Windows を表します) DEC (DEC Alpha を表します) Teradata の場合、クライアント/サーバー OS に関する直接情報がないので、代わりにデータ・フォーマット・タイプが使用されます。これによって、DB セッション中に整数データがどのように保管されるかが示されます。 これは使用するプラットフォームと密接な関連があり、以下のように表示される場合があります。 IBM® MAINFRAME // IBM mainframe data format HONEYWELL MAINFRAME // Honeywell mainframe data format AT&T 3B2 // AT&T 3B2 data format. INTEL 8086 // Intel 8086 data format (IBM PC or compatible) VAX // VAX data format AMDAHL // Amdahl data format
クライアント OS	クライアントのオペレーティング・システム。 Teradata の場合、クライアント/サーバー OS に関する直接情報がないので、代わりにデータ・フォーマット・タイプが使用されます。これによって、DB セッション中に整数データがどのように保管されるかが示されます。 これは使用するプラットフォームと密接な関連があり、以下のように表示される場合があります。 IBM MAINFRAME // IBM mainframe data format HONEYWELL MAINFRAME // Honeywell mainframe data format AT&T 3B2 // AT&T 3B2 data format. INTEL 8086 // Intel 8086 data format (IBM PC or compatible) VAX // VAX data format AMDAHL // Amdahl data format
OS ユーザー	相互作用の OS ユーザー・アカウント。
サーバー・ホスト名	サーバー・ホスト名。
サーバーの記述	サーバーの記述 (ある場合)。
クライアント IP/データベース・ユーザー	クライアント IP アドレスとデータベース・ユーザー名から構成されるペアの属性値。
分析されたクライアント IP	暗号化トラフィックにのみ適用されます。設定されると、クライアント IP はゼロに設定されます。 分析済みのクライアント IP には CEF ソース用のマップがあります。CEF で使用される照会内にクライアント IP が指定されておらず、分析済みのクライアント IP が指定されている場合、分析済みのクライアント IP がソースに対して使用されます。クライアント IP と分析済みのクライアント IP の両方が照会内に指定されている場合、クライアント IP が優先されます。
サーバー IP/データベース・ユーザー	サーバー IP アドレスとデータベース・ユーザー名から構成されるペアの属性値。
セッション別クライアント/サーバー	セッション別クライアント/サーバーは、メイン・エンティティーでもあります。 この「2 次エンティティー」にアクセスするには、「1 次エンティティー」である「クライアント/サーバー」をクリックします。

「アクセス ID」は、admin ロールを持つユーザーのみが使用できます。

注:「アクセスのトラッキング」の場合のみ、「クライアント/サーバー」エンティティー名は、プルダウン・メニューに 2 つの可能なエンティティー (「クライアント/サーバー」および「セッション別クライアント/サーバー」) として表示されます。

「セッション別クライアント/サーバー」は、「クライアント/サーバー」からカウントを取得し、「セッション」から日付状態を取得します。

「クライアント/サーバー」は、「クライアント/サーバー」からカウントを取得し、「クライアント/サーバー」から日付状態も取得します。

「クライアント/サーバー」を選択すると、照会には ATTRIBUTE_ID = 1 が設定されます。ユーザーが「セッション別クライアント/サーバー」を選択すると、照会には MAIN_ATTRIBUTE_ID= 0 が設定されます。

「CM バッファー使用状況モニター」エンティティー

中央マネージャー内で、アップロードされたすべての「スニファーのバッファー使用」エンティティーの統合を示します。

表 25.「CM バッファー使用状況モニター」エンティティー

属性	記述
スニファーのバッファー使用 ID	
タイム・スタンプ	レコードが作成された時刻。
スニファーの CPU PCT	スニファーによって使用された CPU のパーセンテージ。

属性	記述
スニファーのメモリー PCT	スニファーによって使用されたメモリーのパーセンテージ。
MySQL の CPU PCT	MySQL によって使用された CPU のパーセンテージ。
MySQL の MEM PCT	MySQL によって使用されたメモリーのパーセンテージ。
PID	スニファー・プロセス ID。
メモリー	スニファーによって使用されたメモリー量。
時刻	スニファーによって使用された経過時間。
空きバッファー	空きバッファー・スペース量。
アナライザー・レート	メッセージが分析される速度。
アナライザー・キュー	分析キューのサイズ。
アナライザー総計	分析されたメッセージの総数。
ロガー・キュー	ロガー・キューのサイズ。
ロガー総計	ログに記録されたメッセージの総数。
セッション・キュー	セッション・キューのサイズ。
セッション総計	セッションの総数。
ハンドラー・データ	内部スニッフィング・エンジン・データ。
補足 STR	内部スニッフィング・エンジン・データ。
使用されたスニファー接続	検査エンジンの再始動以降、現在モニターされている接続の総数。
ドロップされたスニファー・パケット	スニファーによってドロップされたパケット。
無視されたスニファー・パケット	スニファーによって無視されたパケット。
スロットルされたスニファー・パケット	検査エンジンの再始動以降、スロットルのために無視された接続の総数。
終了したスニファー接続	検査エンジンの再始動以降、モニターされて終了した接続の総数。
ロガー・セッション・カウント	ログに記録されたセッションの数。
ルールにより無視されたロガー・パケット	ポリシー・ルール・アクションにより無視されたパケット。
アナライザー逸失パケット	アナライザーによって失われたパケット。
モニターされるロガー・データベース	現在モニターされているデータベース・タイプのリスト。
Mysql 起動済み	内部データベース再始動を表すブール値インディケーター (1 = 再始動済み、0 = 未再始動)。
システム CPU 負荷	システム CPU 使用状況。
システム・アップタイム	最後の始動からの時間。
Mysql ディスク使用状況	MySQL ディスク使用状況。
システム・メモリー使用状況	システム・メモリー使用状況。
/var ディスク使用状況	/var ディスク使用状況。
システム・ルート・ディスク使用状況	システム・ルート・ディスク使用状況。
Eth0 受信	ETH 0 で受信されたメッセージ。
Eth0 送信	ETH 0 で送信されたメッセージ。
プロミスキャス受信	スニッフィング・ネットワーク・カード (非インターフェース・ポート) を介した受信パケットの率。
オープン FD	オープン・ファイル記述子。
オープン FD MySQL	データベース・オープン・ファイル記述子。
通常のセッション	通常のセッションの数。
オープンされていないセッション	スニファーによって開かれなかったセッションの数。
セッション・タイムアウト	タイムアウトになったセッションの数。
セッション無視	スニファーによって無視されたセッションの数。
セッション直接クローズ	直接閉じられたセッションの数。
セッション推測	推測されたセッション数。
SqlGuard タイム・スタンプ	カスタム表にレコードが挿入された時刻。

属性	記述
データ・ソース名	レコードのアップロードに使用されたデータ・ソースの名前。

「コマンド」エンティティー

各コマンドの親ノードとコマンド構造内でそのコマンドが現れる位置ごとに、エンティティーが作成されます。

表 26. 「コマンド」エンティティー

属性	記述
コマンド ID	コマンドを一意的に識別します。
構造 ID	構造 (例えば select a from b) を一意的に識別します。
SQL 動詞	SQL コマンド内の主動詞 (例えば select、insert、delete など)。
深さ	SQL 構文解析ツリーにおけるコマンドの深さ。
親	構文解析ツリーにおける親ノードの ID。

「コマンド ID」および「構造 ID」は、admin ロールを持つユーザーのみが使用できます。

「コメント」エンティティー

このエンティティーは、ユーザー・コメントについて示します。「コメント」ドメインでのみ使用可能です。これは、admin ユーザーに限定されています。 このドメインには、共有可能コメントのみが含まれます。共有可能コメントとは、ローカルに実行されるもの以外のすべてのコメントのことです (「ローカル・コメント」エンティティーを参照)。

表 27. 「コメント」エンティティー

属性	記述
コメント作成者	コメントを作成した Guardium ユーザー。
コメント参照	コメントが付加された要素 (例えば、照会、監査プロセスの結果、または別のコメント) を示します。
コメントの内容	完全なコメント・テキスト。
タイム・スタンプ	コメントが作成された日時。
タイム・スタンプの年	そのタイム・スタンプの年のみ。
タイム・スタンプの曜日	そのタイム・スタンプの曜日のみ。
タイム・スタンプの時刻	そのタイム・スタンプの時刻のみ。
タイム・スタンプの日付	そのタイム・スタンプの日付のみ。
オブジェクトの記述	定義されたコメントの対象となったオブジェクトの名前。 例えば、ポリシーについて定義されたコメントには、ACCESS_RULE_SET のオブジェクトの記述が含まれています。
レコード・アソシエーション	このコメントが関連付けられたレコードのリスト。

「データベース・エラー・テキスト」エンティティー

データベースの各一般的エラー・メッセージのテキストは、Guardium 内部データベースの表に格納されています。これは、所有する「例外」エンティティーから、データベース・エラーである各例外のレポートを作成する場合にのみ使用できます。例外のいくつかのタイプ (例えば S-TAP® 切断または再接続) には、データベース・エラー・テキストはありません。

表 28. 「データベース・エラー・テキスト」エンティティー

属性	記述
データベース・エラー・テキスト	データベース・エラー・コードの後に、エラーに関する短いテキストの記述が続きます。 エラー・コードは、「例外」エンティティーの「例外の記述」属性から取得されます。 エラー・コードをキーとして使用して、Guardium アプライアンス上の内部表からエラー・テキストが取得されます。この内部表には、最も一般的なエラー・メッセージ (エラー・メッセージのうち約 54,000) が含まれます。 例: ORA-00942: 表またはビューが存在しません
エラー・コード	データベース・エラー・コードを表示します。

「データ・ソース」エンティティー

このエンティティー (「CAS 構成のトラッキング」/「モニター項目詳細」エンティティーの下) は、データ・ソースを識別します。

表 29. 「データ・ソース」エンティティー

属性	記述
データ・ソース ID	データ・ソースの結果セットを識別します。
データ・ソース・タイプ	データ・ソース・タイプ - Oracle、MS-SQL、DB2、Sybase、Informix など。
データ・ソース名	データ・ソース名。

属性	記述
データ・ソースの記述	データ・ソースの記述。
ホスト	データ・ソースのホスト名。
ポート	ホスト上のポート番号。
サービス名	データ・ソースのサービス名。
ユーザー名	データ・ソース・アクセスに使用されたユーザー名。
データベース名	データベース名。
最後のコメント	最後のコメント。
共有	「はい」または「いいえ」
接続プロパティー	「接続プロパティー」ボックスに情報があるのは、このデータ・ソースとの JDBC 接続を確立するために JDBC URL に追加の接続プロパティーを含める必要がある場合のみです。

「ディスカバーされたホスト」エンティティー

このエンティティーは、ディスカバーされたホストを識別します。

表 30. 「ディスカバーされたホスト」エンティティー

属性	記述
サーバー IP	ディスカバーされたホストの IP アドレス。
サーバー・ホスト名	ディスカバーされたホストのホスト名。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「ディスカバーされたインスタンス」エンティティー

このエンティティーは、ディスカバーされたインスタンスを識別します。

表 31. 「ディスカバーされたインスタンス」エンティティー

属性	記述
タイム・スタンプ	エンティティーのこのインスタンスを Guardium が記録するときに作成されるタイム・スタンプ値 (インスタンスごとに固有のタイム・スタンプがあります)。
ホスト	このインスタンスのホスト名。
プロトコル	このインスタンスに固有のプロトコル。
ポート (最小)	ポート範囲 (検査エンジンの最小ポート番号)。
ポート (最大)	ポート範囲 (検査エンジンの最大ポート番号)。
クライアント IP	クライアントの IP アドレス/マスク。
除外クライアント IP	除外するクライアントの IP アドレス/マスク。
プロセス名	データベース実行可能プログラムの名前。
名前付きパイプ	データベースによって使用されたパイプ名。
KTAP データベース・ポート	KTAP のデータベース・ポート。
データベース・インストール・ディレクトリー	データベース・インストール・ディレクトリー。
プロセス名	プロセス名
DB2 共有メモリー調整	パケット・ヘッダー・サイズ
DB2 共有メモリー・クライアント位置	クライアント入出力域オフセット
DB2 共有メモリー・サイズ	DB2 共有メモリー・セグメント・サイズ
インスタンス名	ディスカバーされたインスタンスの名前。
Informix バージョン	Informix バージョン

「ディスカバーされたポート」エンティティー

このエンティティーは、ディスカバーされたポートを識別します。

表 32. 「ディスカバーされたポート」エンティティー

属性	記述
ポート	ディスカバーされたポート番号。
プローブ試行	サポートされるデータベース・サービスのプローブがこのポートで試行されたかどうかを示します。 T = はい、F = いいえ。
ポート・タイプ	ポート・タイプを示します (通常は TCP)。
データベース・タイプ	サポートされるデータベース・タイプがポートのプローブで検出された場合に、タイプ (DB2、Informix、MS SQL Server など) を示します。
プローブ・タイム・スタンプ	この特定のポートでプローブが行われた日時。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「例外」エンティティー

このエンティティーは、検出された例外ごとに作成されます。

表 33. 「例外」エンティティー

属性	記述
例外 ID	例外を一意的に識別します。
例外タイプ ID	例外タイプを一意的に識別します。
例外タイム・スタンプ	この「例外」エンティティーがログに記録されるときに作成された日時。
例外の日付	そのタイム・スタンプの日付のみ。
例外の時刻	そのタイム・スタンプの時刻のみ。
例外の曜日	そのタイム・スタンプの曜日のみ。
例外の年	そのタイム・スタンプの年のみ。
ソース・アドレス	例外のソース IP アドレス。
ソース・ポート	ソース・ポート番号。
宛先アドレス	宛先 IP アドレス。
宛先ポート	宛先ポート番号。
データベース・プロトコル	例外のデータベース・プロトコル。
新規 TTL 値	admin ロール専用に予約済み。
例外の記述	例外の記述。 S-TAP 再接続またはタイムアウト例外の場合、これにはデータベース・サーバーの IP アドレスまたは DNS 名が含まれます。 データベース例外の場合、これはデータベース管理システムからのエラー・コードです。 最も一般的なメッセージ (メッセージのうち約 54,000) については、「データベース・エラー・テキスト」属性で、より長いテキストの記述を使用できます。 そのテキストは、例外自体からではなく、エラー・メッセージのための内部 Guardium データベース表からのものです。
例外の原因となった SQL 文字列	例外を発生させた SQL 文字列。
ユーザー名	データベース・ユーザー名。相関が必要とされる暗号化トラフィックではこの値を使用できない場合がありますが、「クライアント/サーバー」エンティティーの「データベース・ユーザー名」属性からは常に使用可能です。
アプリケーション・ユーザー名	アプリケーション・ユーザー名。
例外についての詳細情報へのリンク 1	例外ソースによっては使用可能な場合があるオプション・リンク。
グローバル ID1	例外のグローバル ID。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「例外 ID」および「例外タイプ ID」は、admin ロールを持つユーザーのみが使用できます。

「例外タイプ」エンティティー

固定の例外タイプ・セットがあり、そのうちの 1 つが、ログに記録された各例外に関連付けられます。これらは、所有「例外」エンティティーからのレポート作成のみに使用可能です。

表 34. 「例外タイプ」エンティティー

属性	記述
例外の記述	例外タイプのテキストの記述。下記リストの中から選択されます。これらの大半は表示されることはありません。最も一般的な例外および注記については、イタリックで示された注を参照してください。 新しい構成が使用されました アラート・プロセスが例外をスローしました カスタム・アラート処理の例外 データベース・サーバーがエラーを返しました このメッセージの場合、データベース・エラー・コードは「例外」エンティティーの「例外の記述」属性に保管され、データベース・エラー・メッセージのテキスト・バージョンが、「データベース・エラー・テキスト」エンティティーの「データベース・エラー・テキスト」属性で使用可能です。 データベース・プロトコルの例外 デバッグが例外メカニズムをプリントスルーします ドロップされたデータベース要求 過剰トラフィックのためにセッション情報がドロップされました。 構成監査システム処理中にエラーが発生しました 分類処理中にエラーが発生しました 無効な照会の呼び出し ログインに失敗しました 低レベルのデータベース・プロトコルの例外 スケジュールに入れられたジョブが例外をスローしました セキュリティー・アセスメントの例外 セキュリティーの例外 このメッセージの場合、違反コードの実行 (ユーザーが Java™ API を使用して独自のアラートまたは評価を定義した場合など) がブロックされたときに、カスタム・クラス例外が発生しています。 セッションが予定より早く終了しました SQL パーサーの例外 S-TAP 接続の再接続 このメッセージの場合、データベース・サーバーの IP アドレスまたは DNS 名は、「例外」エンティティーの「例外の記述」属性で使用可能です。 S-TAP の接続のタイムアウト このメッセージの場合、データベース・サーバーの IP アドレスまたは DNS 名は、「例外」エンティティーの「例外の記述」属性で使用可能です。 TCP エラー このメッセージの場合、エラーに関する追加情報が「例外」エンティティーの「例外の記述」属性に含めれます。 Turbine クラスが例外をスローしました レポートをパージできません

「フィールド」エンティティー

Guardium は、新規フィールドを検出するたびに、フィールド・エンティティーを作成します。

表 35. 「フィールド」エンティティー

属性	記述
フィールド ID	フィールドを一意的に識別します。
構造 ID	参照された構造を一意的に識別します。
コマンド ID	参照された構造に含まれるメイン・コマンドを一意的に識別します。
オブジェクト ID	参照された構造に含まれるオブジェクトを一意的に識別します。
フィールド名	フィールドの名前。

属性	記述
List 節 Where 節 Order by 節 Having 節 Group By 節 On 節	これらの属性は、複合 SQL 照会を順序付けするのに使用します。 SQL 照会の例: Order by SELECT * FROM dept_costs WHERE dept_total > (SELECT avg FROM avg_cost) ORDER BY department Having SELECT column_name1, SUM(column_name2) FROM table_name GROUP BY column_name1 HAVING (数値関数条件) Group By SELECT column_name1, SUM(column_name2) FROM table_name GROUP BY column_name1 Where SELECT FirstName, LastName, City FROM Users WHERE City = Los Angeles

「フィールド ID」、「構造 ID」、「コマンド ID」、および「オブジェクト ID」は、admin ロールを持つユーザーのみが使用できます。

「フィールド SQL 値」エンティティー

これらのエンティティーは、値も一緒にログに記録するポリシー・ルール・アクション (例えば、「値を含む全詳細をロギング」、「値を含む全詳細をセッションごとにロギング」) によってのみ作成されます。 ログに記録されたフィールド値は、フィールド名と関連付けられる場合と、そうでない場合があります。 例えば、次のステートメントがログに記録された場合、フィールド名が使用可能です (「フィールド」エンティティー内)。

insert into t1 (foo, bar) (10, 20)

しかし、次のステートメントがログに記録された場合は、使用不可です。

insert into t2 (10, 20)

表 36. 「フィールド SQL 値」エンティティー

属性	記述
値	ログに記録された構造に含まれるフィールド値。

「未解析ログ」エンティティー

このエンティティーは、未解析ログ処理アクティビティーについて示します。

表 37. 「未解析ログ」エンティティー

属性	記述
完全な SQL	ログに記録された完全な SQL。
タイム・スタンプ	ログに記録されたときの日時スタンプ。
タイム・スタンプの日付	タイム・スタンプの日付部分。
タイム・スタンプの時刻	タイム・スタンプの時刻部分。
応答時間	要求に対する応答時間 (ミリ秒単位)。
影響を受けるレコード	要求の影響を受けたレコードの数。
成功	要求が成功したかどうかを示します (True/False)。

属性	記述
ステートメント・タイプ	SQL ステートメントのタイプ。 SQL: 単純な直接 SQL コマンド (例えば、CLI に直接入力されるコマンド) RAW: 後で実行するための SQL ステートメント PREPARE。例えば、conn.prepareStatement (select a from b where c=:value) BIND: バインドされたパラメーター値を含む、準備されたステートメントの実行 ステートメント・タイプは「完全な SQL」エンティティーの一部であり、ポリシー内でこのステートメントに対して「全詳細をロギング」を構成した場合にのみ監査されます。 ポリシー内の特定のステートメント・タイプ (例えば、監査のみの SQL および BIND ステートメント) をフィルタリングすることはできません。ただし、レポートではこれらをフィルタリングできます。
戻りデータ	返されたデータ (ある場合)。
バインド情報	要求のバインド情報。
バインド変数値	Db2/zOS の場合は、バインド変数のコンマ区切りリストが含まれます。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「完全な SQL」エンティティー

「完全な SQL」エンティティーは、ポリシー・ルール・アクションの「全詳細をロギング」、「値を含む全詳細をロギング」、「セッションごとに全詳細をロギング」、または「値を含む全詳細をセッションごとにロギング」によってのみ作成されます。

表 38. 「完全な SQL」エンティティー

属性	記述
完全な SQL	値を含む完全な SQL ステートメント。
タイム・スタンプ	タイム・スタンプは、SQL がデータベース・サーバーで実行されるときに、時刻を記録します。
応答時間	要求に対する応答時間 (ミリ秒単位)。ネットワーク・トラフィック内で要求がモニターされる場合、応答時間は要求に応答するのに要した時間を正確に反映しています (Guardium はクライアント要求とサーバー応答の両方のタイム・スタンプを設定します)。
影響を受けるレコード	影響を受けたレコードの数 (セッションごと)。この属性を使用するレポートでは、大規模結果セットや N/A などの特殊ケースが適切に表示されるように、別名をオンにすることをお勧めします。
戻りデータ	この要求に対して返されたデータ (ある場合、かつ使用可能な場合)。
完全な SQL ID	完全な SQL の固有 ID。
インスタンス ID	完全な SQL のインスタンスの固有 ID。
成功	呼び出しが成功したかどうかを示します。
影響を受けるレコード (名前)	「影響されるレコード」が数値ではなく文字列値である場合、その文字列はここに保管されます。例: 大規模結果セットまたは N/A。
アクセス・ルールの記述	使用されたポリシー・ルールの記述。
戻りデータ・カウント	ポリシー・ルールで使用された SQL ステートメントから返された行数。
自動コミット	項目が自動的に番号付けされます。
確認応答時間	確認応答時間 (ミリ秒単位)。
進入 KB カウント	要求に含まれるバイト数を記録します。
退出 KB カウント	応答に含まれるバイト数を記録します。
ステートメント・タイプ	SQL ステートメントのタイプ。 SQL: 単純な直接 SQL コマンド (例えば、CLI に直接入力されるコマンド) RAW: 後で実行するための SQL ステートメント PREPARE。例えば、conn.prepareStatement (select a from b where c=:value) BIND: バインドされたパラメーター値を含む、準備されたステートメントの実行 ステートメント・タイプは「完全な SQL」エンティティーの一部であり、ポリシー内でこのステートメントに対して「全詳細をロギング」を構成した場合にのみ監査されます。 ポリシー内の特定のステートメント・タイプ (例えば、監査のみの SQL および BIND ステートメント) をフィルタリングすることはできません。ただし、レポートではこれらをフィルタリングできます。
バインド変数値	Db2/zOS の場合は、バインド変数のコンマ区切りリストが含まれます。

属性	記述
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「完全な SQL ID」、「インスタンス ID」、および「成功」は、admin ロールを持つユーザーのみが使用できます。

「完全な SQL 値」エンティティー

これらのエンティティーは、「値を含む全詳細をロギング」および「値を含む全詳細をセッションごとにロギング」ポリシー・ルール・アクションによってのみ作成されます。

表 39. 「完全な SQL 値」エンティティー

属性	記述
値	ログに記録された構造に含まれる 1 つ以上の値。
タイム・スタンプ	「完全な SQL 値」エンティティーが作成された日時。

「GIM イベント」エンティティー

このエンティティーは、Guardium Installation Manager (GIM) を使用中に発生したイベントについて示します。

表 40. 「GIM イベント」エンティティー

属性	記述
イベント・ジェネレーター	イベントを生成したクライアント (すなわち DB サーバー) の IP アドレス。
イベントの記述	イベントの記述。
イベント時間	イベントが発生した時刻。

「グループ」エンティティー

このエンティティーは、Guardium に対して定義されたグループについて示します。

表 41. 「グループ」エンティティー

属性	記述
グループの記述	グループの名前。
グループ・サブタイプ	グループに定義されたサブタイプ (ある場合)。
タイム・スタンプ	グループ・エンティティーが作成された日時。

「グループ・メンバー」エンティティー

このエンティティーは、Guardium に対して定義されたグループのメンバーについて示します。

表 42. 「グループ・メンバー」エンティティー

属性	記述
グループ・メンバー	グループ・メンバーの名前。
タイム・スタンプ	グループ・メンバーが作成または更新された日時。
タイム・スタンプの日付	そのタイム・スタンプの日付のみ。
タイム・スタンプの時刻	そのタイム・スタンプの時刻のみ。
タイム・スタンプの年	そのタイム・スタンプの年のみ。
タイム・スタンプの曜日	そのタイム・スタンプの曜日のみ。

「グループ・タイプ」エンティティー

このエンティティーは、Guardium グループのタイプ (ユーザー、クライアント IP アドレス、コマンドなど) について示します。

表 43. 「グループ・タイプ」エンティティー

属性	記述
グループ・タイプ	グループ・タイプを識別します。
タイム・スタンプ	グループ・タイプが作成された日時。

Guardium アクティビティー・タイプ

このエンティティーは、さまざまなユーザー・アクティビティーについて示します。

表 44. Guardium アクティビティー・タイプ

属性	記述
アクティビティー・タイプの記述	アクティビティーの記述。
アクティビティー・タイプ ID	アクティビティー・タイプを一意的に識別します。

「Guardium ロール」エンティティー

このエンティティー (「ユーザー」エンティティーの下) は、Guardium ロールを識別します。

表 45. 「Guardium ロール」エンティティー

属性	記述
ロール ID	識別されたロールの ID。
ロール	Guardium ロールがリストされます。

「Guardium アプリケーション」エンティティー

このエンティティー (「ユーザー」エンティティーの下) は、Guardium アプリケーションを識別します。

表 46. 「Guardium アプリケーション」エンティティー

属性	記述
アプリケーション ID	識別されたアプリケーションの ID。
アプリケーション	Guardium アプリケーションがリストされます (例えば、クエリー・ビルダー、ポリシー・ビルダーなど)。

「Guardium アクティビティー・タイプ」エンティティー

アクティビティーのタイプごとに、内部 Guardium データベースにインスタンスが定義されます。

表 47. 「Guardium アクティビティー・タイプ」エンティティー

属性	記述
アクティビティー・タイプの記述	アクティビティーの記述。

「Guardium ユーザー・アクティビティー監査」エンティティー

このエンティティーは、Guardium ユーザー・アクティビティーごとに作成されます。

表 48. 「Guardium ユーザー・アクティビティー監査」エンティティー

属性	記述
ログイン ID	ログインに使用された ID。
ユーザー名	アクティビティーに使用された Guardium ユーザー名。
タイム・スタンプ	アクティビティーがログに記録されるときに作成されたもの。
変更エンティティー	変更された Guardium エンティティー (例えば、グループ定義)。
使用エンティティー・キー	エンティティーにアクセスするために使用されたキー。
キー値	エンティティーの新規の値。
すべての値	変更されたすべての値。
オブジェクトの記述	変更された特定のオブジェクトの名前。
グローバル ID	セッションの固有のグローバル ID。
ホスト名	ユーザーのホスト名。

「Guardium ユーザー・ログイン」エンティティー

このエンティティーは、Guardium アプライアンスにユーザーがログインするたびに作成されます。

表 49. 「Guardium ユーザー・ログイン」エンティティー

属性	記述
ログイン ID	ログインに使用された ID。
ユーザー名	Guardium ユーザーがログインまたはログアウトするときに作成されます (Guardium セッション当たり 1 つのエンティティーが存在します)。

属性	記述
ログイン日時	ユーザーがログインした日時。
ログアウト日時	ユーザーがログアウトした日時。
ログイン成功	ログインが成功したかどうかを示します。
グローバル ID	セッションの固有のグローバル ID。
ホスト名	ユーザーのホスト名。
リモート・アドレス	ユーザーのリモート・アドレス。

「ホスト」エンティティー

データベース・サーバー・ホスト上で CAS が初めて認識されたときに、CAS ホスト・エンティティーが作成されます。 オンライン/オフライン状況が変わるたびに更新されます。 「ホスト」エンティティーは、「CAS ホスト履歴」ドメインでも使用可能です。

表 50. 「ホスト」エンティティー

属性	記述
ホスト名	データベース・サーバー・ホスト名 (IP アドレスとして表示される場合があります)。
OS タイプ	オペレーティング・システム: UNIX または WIN
オンライン	レコードが書き込まれたときのオンライン状況 (はい/いいえ)。
ホスト ID	ホスト・レコードを識別します。

「ホスト構成」エンティティー

「ホスト構成」エンティティーは、CAS インスタンス内の項目ごとに作成されます。

表 51. 「ホスト構成」エンティティー

属性	記述
監査状態ラベル ID	構成項目の固有の数値 ID。
タイム・スタンプ	エンティティー作成のタイム・スタンプ。
ホスト名	データベース・サーバーのホスト名または IP アドレス。
OS タイプ	オペレーティング・システム: Unix または Windows。
データベース・タイプ	データベース・タイプ: Oracle、MS-SQL、DB2、Sybase、Informix。オペレーティング・システム・インスタンスに対する変更である場合は「N/A」。
インスタンス名	テンプレート・セット・インスタンスの名前。
タイプ	変更されたモニター項目のタイプ。 OS スクリプトまたは SQL スクリプト: モニター項目テンプレート定義に含まれる OS スクリプトによって発生した変更。 環境変数: 環境変数 (Unix のみ) レジストリー変数: レジストリー変数 (Windows のみ) ファイル: 特定のファイル。インスタンスによって使用されるテンプレート・セットで定義されたファイル・パターンを対象としたホスト構成エンティティーはありません。 代わりに、パターンに一致するファイルごとに、別々のホスト構成エンティティーがあります。
モニター項目	変更された項目の名前。記述 (入力されている場合) から取得され、それ以外の場合はタイプに応じたデフォルトの名前 (例えばファイル名) になります。

「ホスト・イベント」エンティティー

ホスト・イベント・エンティティーは、CAS によってイベント (イベント・タイプを参照) が検出されるかシグナル通知されるたびに作成されます。

表 52. 「ホスト・イベント」エンティティー

属性	記述
監査ホスト・イベント ID	ホスト・イベント・エンティティーを識別します。
イベント時間	イベントが記録された日時。

属性	記述
イベント・タイプ	記録されているイベントを識別します。以下のタイプがあります。 クライアント稼働 - データベース・サーバー・ホスト上の CAS が始動しました。 クライアント停止 - データベース・サーバー・ホスト上の CAS が停止しました。 フェイルオーバー Off - サーバーが (切断後に) 使用可能になったので、CAS データはサーバーに書き込まれます。 フェイルオーバー On - サーバーが使用不可なので、CAS データはフェイルオーバー・ファイルに書き込まれます。 サーバー停止 - データベース・サーバーが停止しました。 サーバー稼働 - データベース・サーバーが始動しました。
タイム・スタンプ	エンティティー作成のタイム・スタンプ。
監査ホスト ID	ホストを識別します。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「インシデント」エンティティー

「インシデント」エンティティーは、インシデント生成プロセスによって作成されるか、ポリシー違反をインシデントに割り当てることによって手動で作成されます。

表 53. 「インシデント」エンティティー

属性	記述
タイム・スタンプ	インシデントが作成された時刻。
カテゴリー名	インシデントに割り当てられたカテゴリー。
インシデント番号	インシデント番号 (順次割り当て)。

「インシデント重大度」エンティティー

インシデントのインシデント重大度の記述。

表 54. 「インシデント重大度」エンティティー

属性	記述
インシデント重大度の記述	重大度コードは、以下のいずれかになります。 情報、低、中、高

「インシデント状況」エンティティー

「インシデント」エンティティーの状況について示します。

表 55. 「インシデント状況」エンティティー

属性	記述
状況の記述	以下のいずれかの値になります。 オープン - インシデントはまだユーザーに割り当てられていません。 割り当て済み - インシデントは割り当てられています。 クローズ済み - インシデントは閉じられています。

「インストール済みポリシー」エンティティー

インストール済みポリシーについて示します。

表 56. 「インストール済みポリシー」エンティティー

属性	記述
ID	ポリシー・インストール・レコードを識別します。
ルール・セット ID	ルールのセットを識別します。
ポリシーの記述	ポリシー定義に含まれる記述。

属性	記述
選択的な監査証跡	これが選択的な監査証跡ポリシーであるかどうかを示します (T/F)。
監査パターン	選択的な監査証跡ポリシーに使用されたテスト・パターン。
タイム・スタンプ	レコード作成のタイム・スタンプ。
シーケンス	インストール済みポリシーが複数存在する場合にシーケンスの順序を設定します。

「インスタンス構成」エンティティー

「インスタンス構成」エンティティーは、インスタンス構成が定義されるたびに作成されます。このエンティティーは、CAS インスタンスがデータベースに接続する方法を (必要に応じて) 定義し、インスタンスの使用したテンプレート・セットを識別します。 インスタンスの現在の状況 (使用中、使用可能、使用不可) と最終リビジョンの日付を示します。

「インスタンス構成」エンティティーの属性

表 57. 「インスタンス構成」エンティティー

属性	記述
構成 ID	この構成レコードを識別します。
タイム・スタンプ	レコードが作成されたときのタイム・スタンプ。
データベース・タイプ	データベース・タイプ: Oracle、MS-SQL、DB2、Sybase、Informix。オペレーティング・システム・インスタンスの場合は「N/A」。
インスタンス	インスタンスの名前。
ユーザー	データベースへのログオンに CAS が使用するユーザー名。オペレーティング・システム・インスタンスの場合は「N/A」。
ポート	データベースへの接続に CAS が使用するポート番号。オペレーティング・システム・インスタンスの場合は空。
データベース・ホーム・ディレクトリー	データベースのホーム・ディレクトリー。オペレーティング・システム・インスタンスの場合は空。
テンプレート・セット ID	このインスタンスによって使用されたテンプレート・セットを識別します。
OS タイプ	ホストのオペレーティング・システム: UNIX または Windows

「結合」エンティティー

結合表は、多対多の関係を実装するための 1 つの方法です。結合エンティティーは、SELECT SQL ステートメントで表を結合する場合に使用します。

表 58. 「結合」エンティティー

属性	記述
結合 ID	ユニーク ID
構造 ID	結合が参照される構造を識別します。
Join SQL	結合表
Where SQL	Where 節 (結合条件)
タイム・スタンプ	「結合」エンティティーが作成された日時。

「ローカル・コメント」エンティティー

このエンティティーで、ローカル・コメントを記述します。「コメント」ドメインでのみ使用可能です。これは、admin ユーザーに限定されています。 このエンティティーには、ローカルに実行されたプロセスと結果セットに関するローカル・コメントのみが含まれます。 共有可能なコメントは、「コメント」エンティティーで定義されます。

表 59. 「ローカル・コメント」エンティティー

属性	記述
コメント作成者	コメントを作成した Guardium ユーザー。
コメント参照	コメントが付加された要素 (例えば、照会、監査プロセスの結果、または別のコメント) を示します。
コメントの内容	完全なコメント・テキスト。
タイム・スタンプ	コメントが作成された日時。
タイム・スタンプの年	そのタイム・スタンプの年のみ。
タイム・スタンプの曜日	そのタイム・スタンプの曜日のみ。
タイム・スタンプの時刻	そのタイム・スタンプの時刻のみ。
タイム・スタンプの日付	そのタイム・スタンプの日付のみ。
オブジェクトの記述	定義されたコメントの対象となったオブジェクトの名前。 例えば、インシデントについて定義されたコメントには、INCIDENT のオブジェクトの記述が含まれています。
レコード・アソシエーション	このローカル・コメントが関連付けられたレコードのリスト。

ロケーション・ビュー

アーカイブに保存されなかった日を確認する方法

変更可能な照会 (「ツール」タブ>「レポートのビルド」>「レポート・ビルダー」>「ロケーション・ビュー」照会) を使用して、アーカイブに保存されたファイルを示したレポートを作成します。このレポートには、すべてのファイルとアーカイブの日付のリストが表示されます。このレポートに組み込まれなかった日付は、アーカイブに保存されなかった日付です。必要であれば、リストに組み込まれていない日付のアーカイブを実行してください。

表 60. 「ロケーション・ビュー」エンティティー

属性	記述
開始日付	開始日
終了日付	完了日
アグリゲーター	ファイルの生成場所である Guardium システム。ただし、これはアグリゲーターだけではなく、コレクターにすることもできます。
ホスト	ホスト名
ユーザー名	ユーザーの名前
パス	ファイルへのパス名
システム・タイプ	アーカイブ中にどのプロトコルが使用されたか - プロトコルが SCP または FTP、Centera または TSM であった場合
宛先の数	アーカイブの宛先数

「ログイン相関」エンティティー

Guardium バージョン 4.0 から廃止されました。これは「アクセス・トレース・トラッキング」ドメインの唯一のエンティティーでしたが、このドメインは S-TAP バージョン 4.0 から廃止されました。 このドメインを使用する古い照会やレポートがある場合、それらはこのリリースでは機能しません。したがって、このドメインで記録されたデータベース・ログイン情報があれば、それらはどれも S-TAP バージョン 4.0 のインストールより前から存在していることになります。

「メッセージ・テキスト」エンティティー

しきい値アラートのメッセージのテキスト。

表 61. 「メッセージ・テキスト」エンティティー

属性	記述
メッセージ・テキスト ID	メッセージ・テキストを一意的に識別します。
メッセージ件名	メッセージの件名 (例えば E メール・メッセージの件名)。
メッセージ・テキスト	メッセージ・テキスト。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「送信メッセージ」エンティティー

送信されたしきい値アラート・メッセージごとの、メッセージのメッセージ・タイプ、受信者、状況、および日付。

表 62. 「送信メッセージ」エンティティー

属性	記述
メッセージ ID	メッセージを一意的に識別します。
メッセージ・タイプ	メッセージのタイプ。
送信先	1 人以上のメッセージ受信者。
メッセージ状況	メッセージの状況。以下の状況があります。 失敗 送信操作は失敗しました。 待機 メッセージはまだ送信されていません。 送信済み メッセージは送信されました。
メッセージの日付	メッセージが送信された日付。

属性	記述
メッセージ・コンテキスト	メッセージ・タイプ。以下のタイプがあります。 情報 情報メッセージ。 警告 エラー状態の可能性あり。 アラート リアルタイム・アラートまたはしきい値アラート。 エラー ソフトウェアまたはハードウェアのエラー状態。 デバッグ デバッグ・メッセージ。
メッセージ発信元	メッセージを作成するモジュール (例えば、モニターまたは GuardiumJetspeedUser)。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「値のモニター」エンティティー

「値のモニター」エンティティーは、記録された挿入、更新、または削除ごとに作成され、変更の詳細 (表名、アクション、SQL テキストなど) を含んでいます。 .

表 63. 「値のモニター」エンティティー

属性	記述
タイム・スタンプ	Guardium アプライアンスで変更が記録された日時。 このタイム・スタンプは、データ・アップロード操作時に作成されます。 監査データベースに変更が記録された時刻ではありません。 その時刻を取得するには、「監査タイム・スタンプ」エンティティーを使用します。
タイム・スタンプの日付	そのタイム・スタンプの日付のみ。
タイム・スタンプの時刻	そのタイム・スタンプの時刻のみ。
タイム・スタンプの年	そのタイム・スタンプの年のみ。
タイム・スタンプの曜日	そのタイム・スタンプの曜日のみ。
サーバー IP	データベース・サーバーの IP アドレス。
データベース・タイプ	データベース・タイプ。
サービス名	Oracle のみ。データベース・サービス名。
データベース名	DB2、Informix、Sybase、MS SQL Server のみ。データベース名。
監査 PK	Sybase および MS SQL Server のみ。新旧の値 (これらのデータベース・タイプの場合は別々にログに記録する必要がある) を関連付けるのに使用される主キー。
監査ログイン名	データ・ソースで定義されたデータベース・ユーザー名。
監査表の名前	変更された表の名前。
監査の所有者	変更された表の所有者。
監査アクション	挿入、更新、または削除。
古い値の監査	古い値のコンマ区切りリスト。形式は column-name=column_value です。
新しい値の監査	新しい値のコンマ区切りリスト。形式は column-name=column_value です。
SQL テキスト	Oracle 9 の場合のみ使用可能。値を変更する SQL ステートメント全体。
トリガーされる ID	変更に対して生成された固有 ID (この監査データベース上の固有 ID)。
監査タイム・スタンプ	トリガーが実行された日時。
監査タイム・スタンプの日付	監査タイム・スタンプの日付部分。
監査タイム・スタンプの時刻	監査タイム・スタンプの時刻部分。
監査タイム・スタンプの曜日	監査タイム・スタンプの曜日部分。
監査タイム・スタンプの年	監査タイム・スタンプの年部分。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「モニターされた変更」エンティティー

このエンティティーは、モニター項目が変更されるたびに作成されます。CAS インスタンス内のモニター項目を識別し、変更の保存データを指し示します。

表 64. 「モニターされた変更」エンティティー

属性	記述
変更 ID	変更の固有 ID。
サンプルの時刻	サンプルが取られたときのタイム・スタンプ (ホスト上の日時)。
監査構成 ID	ホスト構成を識別します。
保存データ ID	この変更に関する「保存データ」エンティティーを識別します。
監査状態ラベル ID	この変更に関する「ホスト構成」エンティティーを識別します。
タイム・スタンプ	サーバーでこの変更レコードが作成された日時 (Guardium アプライアンス・サーバーのクロック)。
MD5	MD5 アルゴリズムを使用してチェックサムを計算し、その値を前回その項目がチェックされたときに計算された値と比較することによって比較を実行するかどうかを示します。デフォルトでは、MD5 は使用しない設定になっています。MD5 を使用しても、生データのサイズが CAS ホスト用に構成された「MD5 サイズ制限」を上回る場合は、MD5 による計算と比較はスキップされます。MD5 を使用するかどうかに関わらず、項目の最終変更タイム・スタンプの現行値と項目のサイズは、前回その項目がチェックされたときに保存された値と比較されます。
所有者	Unix のみ。項目タイプがファイルの場合に、ファイル所有者。
許可	Unix のみ。項目タイプがファイルの場合に、ファイル・アクセス権。
サイズ	ファイル・サイズ。ただし、次のような特殊値があります。 -1 = ファイルは存在するが、バイト数がゼロである。 0 (ゼロ) = ファイルは存在しないが、このファイル名がモニターされている (存在しなかったか、または削除された可能性がある)。
最終変更	最終変更のタイム・スタンプ。サンプルの時刻にファイル・システムから取得されたもの。
最終変更日	最終変更の日付。
最終変更の時刻	最終変更の時刻。
最終変更の曜日	最終変更の曜日。
最終変更の年	最終変更の年。
グループ	Unix のみ。項目タイプがファイルの場合に、グループ所有者。

「モニター項目詳細」エンティティー

「モニター項目詳細」エンティティーは、CAS インスタンス内のモニター項目ごとに作成されます。

表 65. 「モニター項目詳細」エンティティー

属性	記述
監査構成 ID	ホスト構成を識別します。
タイム・スタンプ	エンティティー作成のタイム・スタンプ。
テンプレート ID	このモニター項目用の項目テンプレートを識別します。
モニター項目	監査タイプに応じて、OS スクリプトまたは SQL スクリプト、環境変数またはレジストリー変数、あるいはファイル名になります。 項目テンプレートで定義されたファイル・パターンに関して、パターンと一致するファイルごとに別々のモニター項目詳細エンティティーがありますが、ファイル・パターン自体のモニター項目詳細エンティティーはありません。 ファイル・パターンが使用された場合、ファイル・パターンは「テンプレートの内容」属性で常に使用可能です。
監査構成設定 ID	ホスト構成内のテンプレート・セットを識別します。
監査タイプ	モニター項目のタイプ。次のタイプがあります。 OS スクリプトまたは SQL スクリプト: オペレーティング・システム・スクリプトまたは SQL スクリプトの実際のテキストまたはパス。この出力が、次回の実行時に生成される出力と比較されます。 環境変数またはレジストリー変数: 環境変数または (Windows) レジストリー変数 ファイル: 特定のファイル、またはファイルのセットを識別するためのパターン。
有効	テンプレートが使用可能かどうかを示します。
同期	サーバー上のテンプレート項目定義が CAS ホスト上のテンプレート項目定義と一致するかどうかを示します。
監査頻度	項目がテストされる最大間隔。
MD5 を使用	MD5 アルゴリズムを使用してチェックサムを計算し、その値を前回その項目がチェックされたときに計算された値と比較することによって比較を実行するかどうかを示します。デフォルトでは、MD5 は使用しない設定になっています。MD5 を使用しても、生データのサイズが CAS ホスト用に構成された「MD5 サイズ制限」を上回る場合は、MD5 による計算と比較はスキップされます。MD5 を使用するかどうかに関わらず、項目の最終変更タイム・スタンプの現行値と項目のサイズは、前回その項目がチェックされたときに保存された値と比較されます。
データ保存	マークが付けられているときは、前のバージョンの項目を現行バージョンと比較できます。
記述	インスタンスの記述 (オプション)。

属性	記述
テンプレートの内容	このモニター項目の基本であるテンプレート項目。インスタンスが作成されるときに「テンプレート」エンティティーの「アクセス名」属性から設定されたものです。 通常はモニター項目と同じになりますが、テンプレートでファイル・パターンが使用された場合は、ファイル・パターンになります。

「オブジェクト」エンティティー

このエンティティーのインスタンスは、固有スキーマ内のオブジェクトごとに作成されます。

表 66. 「オブジェクト」エンティティー

属性	記述
オブジェクト ID	オブジェクトを一意的に識別します。
構造 ID	オブジェクトが参照される構造を一意的に識別します。
スキーマ	オブジェクトのデータベース・スキーマ。 注: この属性にはデータが取り込まれることが決してないため、推奨されません。
オブジェクト名	オブジェクトの名前。
アプリケーション・オブジェクト・モジュール 1	アプリケーション・オブジェクト・モジュールを一意的に識別します。

「オブジェクト ID」および「構造 ID」は、admin ロールを持つユーザーのみが使用できます。

「オブジェクト・コマンド」エンティティー

オブジェクト・コマンド・エンティティーについて示します。

表 67. 「オブジェクト・コマンド」エンティティー

属性	記述
オブジェクト/コマンド	コマンド値と結合されたオブジェクト値。

「オブジェクト・フィールド」エンティティー

オブジェクト・フィールド・エンティティーについて示します。オブジェクトが指定されていないフィールドは、オブジェクトを含んだレポートには示されないことに注意してください。

表 68. 「オブジェクト・フィールド」エンティティー

属性	記述
オブジェクト/フィールド	フィールド値と結合されたオブジェクト値。

「ポリシー・ルール違反」エンティティー

このエンティティーは、ポリシー・ルール違反がログに記録されるたびに作成されます。 すべてのポリシー・ルール違反がログに記録されるわけではありません。第 11 章『ポリシーのビルド』に記載のルール・アクションの説明を参照してください。 違反を引き起こしているアクセス・ルールは、従属する「アクセス・ルール」エンティティー (前述) で使用可能です。

表 69. 「ポリシー・ルール違反」エンティティー

属性	記述
違反ログ ID	違反エンティティーを一意的に識別します。
アプリケーション・ユーザー名	ポリシー・ルール違反を引き起こしているユーザーの名前。
SQL 文字列全体	ポリシー・ルール違反を引き起こしている SQL 文字列。
タイム・スタンプ	ポリシー・ルール違反がログに記録されるときに作成されます。すべてのポリシー・ルール違反がログに記録されるわけではありません。第 11 章『ポリシーのビルド』に記載のルール・アクションの説明を参照してください。
タイム・スタンプの日付	そのタイム・スタンプの日付のみ。
タイム・スタンプの時刻	そのタイム・スタンプの時刻のみ。
タイム・スタンプの曜日	そのタイム・スタンプの曜日のみ。
タイム・スタンプの年	そのタイム・スタンプの年のみ。
メッセージの送信	送信されたポリシー・ルール違反メッセージのテキスト。
オカレンス合計	違反を引き起こしたオカレンス数。
アプリケーション・イベント ID	アプリケーション・イベント ID (ある場合。これらはアプリケーション・イベント API を使用して設定されます)
アクセス・ルールの記述	ルールの定義に含まれるルールの記述。
カテゴリー名	ルールに対して定義されたカテゴリー。

属性	記述
重大度	ルールに対して定義された重大度 (これが割り当てられたインシデントの重大度は異なる場合があります)。
インシデント番号	インシデントに割り当てられている場合、これがインシデント番号になります。
分類名	分類プロセスの名前。
構造 ID	参照された構造を一意的に識別します。
分類プロセス実行 ID	分類プロセスのジョブ実行 ID。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「違反ログ ID」は、admin ロールを持つユーザーのみが使用できます。

「修飾オブジェクト」エンティティー

タプル では、複数の属性を組み合わせて 1 つのグループ・メンバーを形成することができます。この場合、「サーバー IP」、「サービス名」、「データベース名」、「データベース・ユーザー」、および「オブジェクト」の各フィールドがまとめて結合されます。

表 70. 「修飾オブジェクト」エンティティー

属性	記述
修飾されたオブジェクト	タプル - サーバー IP、サービス名、データベース名、データベース・ユーザー、オブジェクト

「不正接続」エンティティー

S-TAP ハンター・プロセスが認識したデータベース接続ごとにインスタンスが作成され (S-TAP 自体が認識したものについては作成されません)、この接続は S-TAP がモニターするアクセス・パスをバイパスしていることを示します。

表 71. 「不正接続」エンティティー

属性	記述
タイム・スタンプ	ハンターによって報告された不正接続を Guardium アプライアンスが記録するときに作成されたタイム・スタンプ値。
サーバー・ホスト名	データベース・サーバー・ホスト名。
ソース・プログラム	接続のソース・プログラム名。
ソース・ポート	接続のソース・ポート。
ソース PID	ソース・プロセス ID。
ターゲット・プログラム	接続のターゲット・プログラム名。
ターゲット・ポート	接続のターゲット・ポート。
ターゲット PID	ターゲット・プロセス ID。
OS ユーザー	オペレーティング・システムのユーザー・アカウント名。
IPC タイプ	接続に使用されたプロセス間通信のタイプ。次のリスト内のいずれかのタイプである可能性があります。 SHM - 共有メモリー IPv4 - インターネット・プロトコル バージョン 4 IPv5 インターネット・プロトコル バージョン 6 FIFO 名前付きパイプ PIPE 単純パイプ INET - インターネット・プロトコル (HPUX)
データベース・サーバー・タイプ	データベース・サーバー・タイプ: Oracle、DB2、Informix、または Sybase。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「ルール」エンティティー

このエンティティーは、「インストール済みポリシー・ルール」エンティティーまたは「アクセス・ポリシー・ルール」エンティティーに対して使用することができます。1 つ以上のインストール済みポリシーまたは 1 つ以上のアクセス・ポリシーのルールごとに、このエンティティーが 1 つ存在します。ID フィールド (内部データベース上のコンポーネントを一意的に識別する) は別として、これらのフィールドについてはすべて、『ポリシー』ヘルプ・トピックに記載されています。

- GDM_INSTALLED_POLICY_RULES_ID - インストール済みポリシー・ルールを識別します。
- ACCESS_RULE_ID - アクセス・ルールを識別します。
- ルールの記述 - ポリシー定義に含まれる。
- ルール位置 - ポリシー内の位置。
- ルール・タイプ - アクセス、例外、または抽出。
- LAST_ACCESSED - 前回のアクセス
- クライアント IP - ルール定義に含まれる。
- クライアント・ネットマスク - ルール定義に含まれる。
- クライアント IP グループ - ルール定義に含まれる。
- サーバー IP - ルール定義に含まれる。
- サーバー IP マスク (Server IP Mask) - ルール定義に含まれる。
- クライアント MAC - ルール定義に含まれる。
- ネット・プロトコル - ルール定義に含まれる。
- ネット・プロトコル・グループ - ルール定義に含まれる。
- フィールド - ルール定義に含まれる。
- フィールド・グループ (Field Group) - ルール定義に含まれる。
- オブジェクト - ルール定義に含まれる。
- オブジェクト・グループ - ルール定義に含まれる。
- コマンド - ルール定義に含まれる。
- コマンド・グループ - ルール定義に含まれる。
- オブジェクト・フィールド・グループ - ルール定義に含まれる。
- データベース・タイプ - ルール定義に含まれる。
- サービス名 - ルール定義に含まれる。
- サービス名グループ (Service Name Group) - ルール定義に含まれる。
- データベース名 - ルール定義に含まれる。
- データベース名グループ - ルール定義に含まれる。
- データベース・ユーザー - ルール定義に含まれる。
- データベース・ユーザー・グループ - ルール定義に含まれる。
- アプリケーション・ユーザー - ルール定義に含まれる。
- アプリケーション・ユーザー・グループ (App User Group) - ルール定義に含まれる。
- OS ユーザー - ルール定義に含まれる。
- OS ユーザー・グループ - ルール定義に含まれる。
- ソース・アプリケーション - ルール定義に含まれる。
- ソース・プログラム・グループ (Source Program Group) - ルール定義に含まれる。
- パターン / XML パターン - ルール定義に含まれる。
- 期間 - ルール定義に含まれる。
- 最小数 - ルール定義に含まれる。
- リセット間隔 - ルール定義に含まれる。
- 次のルールに進む / 取り消し - ルール定義に含まれる。
- 値を記録 - ルール定義に含まれる。
- アプリケーション・イベントの存在 - ルール定義に含まれる。
- イベント・タイプ - ルール定義に含まれる。
- アプリケーション・イベント・テキスト値 - ルール定義に含まれる。
- アプリケーション・イベント日付値 (App Event Date Value) - ルール定義に含まれる。
- イベント・ユーザー名 - ルール定義に含まれる。
- エラー・コード - ルール定義に含まれる。
- 例外タイプ - ルール定義に含まれる。
- カテゴリー名 - ルール定義に含まれる。
- 分類名 - ルール定義に含まれる。
- 重大度 - ルール定義に含まれる。
- データ・パターン - ルール定義に含まれる。
- SQL パターン - ルール定義に含まれる。
- マスキング・パターン - ルール定義に含まれる。
- クライアント IP / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- サーバー IP / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- ネットワーク・プロトコル / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- フィールド名 / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- オブジェクト名 / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- コマンド / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- サービス名 / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- データベース名 / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- アプリケーション・ユーザー / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- OS ユーザー / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- ソース・プログラム / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- エラー・コード / グループ - 単一の属性とその関連情報 (ある場合) を、レポートの単一列に表示できます。
- アプリケーション・イベント・テキスト / 数値 / 日付 - アプリケーション・イベントのテキスト属性、数値属性、および日付属性。
- カテゴリー / 分類 - ルールのカテゴリーと分類の結合。
- GDM_Installed_Policy_Header_ID - インストール済みポリシーのヘッダーを識別します。

注: GDM_INSTALLED_POLICY_RULES_ID および ACCESS_RULE_ID は、admin ロールを持つユーザーのみが使用できます。

「ルール・アクション」エンティティー

このエンティティーは、「インストール済みポリシー・ルール・アクション」エンティティーまたは「アクセス・ポリシー・ルール・アクション」エンティティーに対して使用することができます。1 つ以上のインストール済みポリシーまたは 1 つ以上のアクセス・ポリシーのルールごとに、このエンティティーが 1 つ存在します。

- シーケンス - ルール内のアクションのシーケンス。
- アクション
  - 要求のブロック -『ポリシー』に記載された『ブロッキング・アクション』を参照してください。
  - 違反またはトラフィックをロギングまたは無視 -『ポリシー』に記載された『ロギング・アクションまたは無視アクション』を参照してください。
  - アラート -『ポリシー』に記載された『アラート・アクション』を参照してください。

「保存データ」エンティティー

「保存データ」エンティティーは、モニター対象の項目に対する変更が検出されるたびに作成されます (項目テンプレート定義でその項目の「データを保持」ボックスにマークが付けられた場合)。

表 72. 「保存データ」エンティティー

属性	記述
保存データ ID	保存データ項目を一意的に識別します。
保存データ	保存されている実際のデータ。
タイム・スタンプ	保存データ・エンティティーがサーバー・データベースで記録されたときのタイム・スタンプ。
変更 ID	この保存データ・エンティティーに対応するモニターされた変更エンティティーを識別します。

「保存データ ID」は、admin ロールを持つユーザーのみが使用できます。

「サーバー IP/サーバー・ポート」エンティティー

サーバー IP/サーバー・ポート・エンティティーについて示します。

表 73. 「サーバー IP/サーバー・ポート」エンティティー

属性	記述
サーバー IP/サーバー・ポート	サーバー・ポート値と結合されたサーバー IP 値

「セッション」エンティティー

このエンティティーは、クライアント/サーバー・データベース・セッションごとに作成されます。

表 74. 「セッション」エンティティー

属性	記述
グローバル ID	セッション・アクセスを一意的に識別します。
セッション ID	セッションを一意的に識別します。
アクセス ID	アクセス期間を一意的に識別します。
タイム・スタンプ	初めは、進行中のアクティブ・セッションのないクライアント/サーバー接続上の最初の要求に対して、タイム・スタンプが作成されます。 その後、セッションが閉じられたとき、または長期間にわたってアクティビティーが監視されないために非アクティブのマークがセッションに付けられたときに、更新されます。 セッション情報をトラッキングする場合は、「タイム・スタンプ」属性よりも「セッション開始」属性と「セッション終了」属性を注目する方が適切な場合があります。
タイム・スタンプの日付	そのタイム・スタンプの日付のみ。
タイム・スタンプの時刻	そのタイム・スタンプの時刻のみ。
タイム・スタンプの曜日	そのタイム・スタンプの曜日のみ。
タイム・スタンプの年	そのタイム・スタンプの年のみ。
セッション開始	セッションが開始された日時。「セッション開始」は、メイン・エンティティーでもあります。 この 2 次エンティティーにアクセスするには、1 次エンティティーである「セッション」をクリックします。
セッション開始の日付	「セッション開始」の中の日付のみ。
セッション開始の時刻	「セッション開始」の中の時刻のみ。
セッション開始の曜日	「セッション開始」の中の曜日のみ。
セッション開始の年	「セッション開始」の中の年のみ。
クライアント・ポート	クライアント・ポート番号。
サーバー・ポート	サーバー・ポート番号。
非アクティブ・フラグ	0 (デフォルト) - オープン (SQL パッケージによって生成されたセッションの場合)。 1 - クローズ (切断/ログアウト受信)。 2 - おそらくクローズ (長時間にわたってパケットがない状態では非クローズ)。 3 - 非 SQL パケットから生成されたセッションの場合。

属性	記述
TTL	admin ロール専用に予約済み。
セッション終了	セッションが終了した日時。「セッション終了」は、メイン・エンティティーでもあります。 この 2 次エンティティーにアクセスするには、1 次エンティティーである「セッション」をクリックします。
セッション終了の日付	「セッション終了」の中の日付のみ。
セッション終了の時刻	「セッション終了」の中の時刻のみ。
セッション終了の曜日	「セッション終了」の中の曜日のみ。
セッション終了の年	「セッション終了」の中の年のみ。
データベース名	セッションの対象データベースの名前 (MSSQL または Sybase のみ)。 注: Oracle の場合、アプリケーション固有の追加情報が「データベース名」に含まれることがあります (V$SESSION ビューの MODULE 列に設定された、セッション用に現在実行中のモジュールなど)。
セッション無視	セッションの一部が (ある時点から) 無視されたかどうかを示します。
これ以降を無視	このセッションを無視し始めたときに作成されたタイム・スタンプ。
Uid チェーン	Unix S-TAP (K-Tap モードのみ) によってレポートされたセッションが対象。su ユーザーのユーザー名が異なる場合に、OS ユーザーのチェーンを示します。 ここに表示される値は、OS プラットフォームによって異なります。例えば AIX 環境では、接頭部として IBM IBM IBM という文字列が表示される場合があります。 注: Solaris ゾーンの場合は、ユーザー名の代わりにユーザー ID が「Uid チェーン」でレポートされる場合があります。
古いセッション ID	このセッションが作成されたセッションを示します。 これが接続の最初のセッションである場合は、ゼロです。
端末 ID	セッション情報を解決するために内部で使用された、接続の端末 ID。
プロセス ID	接続を開始したクライアントのプロセス ID (常に使用可能とは限らない)。
Uid チェーン圧縮	圧縮された値。「Uid」チェーンを参照してください。
期間 (秒)	セッション開始からセッション終了までの時間の長さを示します (秒単位)。
元のタイム・ゾーン	UTC オフセット。これは、特に異なるタイム・ゾーンにコレクターを持つアグリゲーターで実行されます。これにより、時間差で発生したアクティビティーが、アグリゲーターにインポートされるときに同じ時刻に発生したように表示されないようにします。 例えば、異なるタイム・ゾーンのデータを統合するアグリゲーター上で、2 つのレコード・セッションが発生したとします。1 つは元のタイム・ゾーン UTC-02:00 に対して 21:00 に開始し、もう 1 つは元のタイム・ゾーン UTC-05:00 に対して 21:00 に開始したとします。これは、これらのセッションは 3 時間違いで発生しましたが、それぞれの現地時間では同じ時刻 (21:00) に発生したことを意味します。

「グローバル ID」、「セッション ID」、および「アクセス ID」は、admin ロールを持つユーザーのみが使用できます。

「重大度」エンティティー

インシデントまたはポリシー違反のインシデント重大度。

表 75. 「重大度」エンティティー

属性	記述
重大度の記述	重大度コードは、以下のいずれかになります。 情報、低、中、高

「スニファーのバッファー使用」エンティティー

store system netfilter-buffer-size CLI コマンドで設定された間隔で (デフォルトでは 60 秒ごとに)、このエンティティーが作成されます。

表 76. 「スニファーのバッファー使用」エンティティー

属性	記述
タイム・スタンプ	レコードが作成された時刻。
スニファーの CPU 使用時間 %	スニファーによって使用された CPU のパーセンテージ。
スニファーによるメモリー使用 %	スニファーによって使用されたメモリーのパーセンテージ。
Mysql による CPU 使用時間 %	MySQL によって使用された CPU のパーセンテージ。
Mysql によるメモリー使用 %	MySQL によって使用されたメモリーのパーセンテージ。
スニファー・プロセス ID	スニファー・プロセス ID。
メモリー・スニファー	スニファーによって使用されたメモリー量。
時間スニファー	スニファーによって使用された経過時間。
空きバッファー・スペース	空きバッファー・スペース量。
アナライザー・レート	メッセージが分析される速度。
ロガー・レート	メッセージがログに記録される速度。

属性	記述
アナライザー・キューの長さ	分析キューのサイズ。
アナライザー総計	分析されたメッセージの総数。
ロガー・キューの長さ	ロガー・キューのサイズ。
ロガー総計	ログに記録されたメッセージの総数。
セッション・キューの長さ	セッション・キューのサイズ。
セッション総計	セッションの総数。
ハンドラー・データ	内部スニッフィング・エンジン・データ。
追加の情報	内部スニッフィング・エンジン・データ。
アナライザー逸失パケット	アナライザーによって失われたパケット。
Eth0 受信	ETH 0 で受信されたメッセージ。
Eth0 送信	ETH 0 で送信されたメッセージ。
モニターされるロガー・データベース	現在モニターされているデータベース・タイプのリスト。
ルールにより無視されたロガー・パケット	ポリシー・ルール・アクションにより無視されたパケット。
ロガー・セッション・カウント	ログに記録されたセッションの数。
Mysql ディスク使用状況	MySQL ディスク使用状況。
Mysql 起動済み	内部データベース再始動を表すブール値インディケーター (1 = 再始動済み、0 = 未再始動)。
プロミスキャス受信	スニッフィング・ネットワーク・カード (非インターフェース・ポート) を介した受信パケットの率。
終了したスニファー接続	検査エンジンの再始動以降、モニターされて終了した接続の総数。
使用されたスニファー接続	検査エンジンの再始動以降、現在モニターされている接続の総数。
ドロップされたスニファー・パケット	スニファーによってドロップされたパケット。
無視されたスニファー・パケット	スニファーによって無視されたパケット。
スロットルされたスニファー・パケット	検査エンジンの再始動以降、スロットルのために無視された接続の総数。
システム CPU 負荷	システム CPU 使用状況。
システム・メモリー使用状況	システム・メモリー使用状況。
システム・ルート・ディスク使用状況	システム・ルート・ディスク使用状況。
システム・アップタイム	最後の始動からの時間。
/var ディスク使用状況	/var ディスク使用状況。
通常のセッション	通常のセッションの数。
オープンされていないセッション	スニファーによって開かれなかったセッションの数。
セッション・タイムアウト	タイムアウトになったセッションの数。
セッション無視	スニファーによって無視されたセッションの数。
セッション直接クローズ	直接閉じられたセッションの数。
セッション推測	推測されたセッション数。
オープン FD	オープン・ファイル記述子。
データベース・オープン FD	データベース・オープン・ファイル記述子。
Di レート	
Di キュー長	
Di 合計	
Di 逸失パケット	
未解析ログ要求	未解析ログ要求。

SQL ベース評価定義

このエンティティーは、SQL ベースの評価定義について示します。

表 77. SQL ベース評価定義

属性	記述
バインド出力変数	オプション。SQL ステートメントに入力されたテキストが、「比較」値との比較で使用される内部 Guardium 変数にバインドされる値を返すプロシージャー型コード・ブロックであるかどうかを判別します。
比較値	比較演算子を使用して SQL ステートメントからの戻り値に対する比較に使用される比較値。
外部参照	Center for Internet Security (CIS) または Common Vulnerabilities and Exposures (CVE) への参照。
演算子	条件に使用される演算子。
推奨テキスト (不合格)	テストが不合格だったときに表示される不合格用の推奨テキスト。
推奨テキスト (合格)	テストが合格だったときに表示される合格用の推奨テキスト。
結果テキスト (不合格)	テストが不合格だったときに表示される不合格用の結果テキスト。
結果テキスト (合格)	テストが合格だったときに表示される合格用の結果テキスト。
戻りの型	SQL ステートメントから返される戻りの型。
簡略説明	評価テストの簡略説明。
詳細の SQL	詳細な SQL ステートメント。文字列のリストを取得して、Detail 接頭部と文字列リストの詳細文字列を生成する SQL ステートメントです。
SQL	テストで実行される SQL ステートメント。

「SQL」エンティティー

「SQL」エンティティー

このエンティティーは、SQL の固有文字列ごとに作成されます。値は疑問符 (?) に置き換えられ、文字列のフォーマットのみが保管されます。

表 78. 「SQL」エンティティー

属性	記述
SQL	SQL 文字列。
構造 ID	SQL が出現する構造を一意的に識別します。
バインド情報	この SQL 文字列のバインド情報。
切り捨てられた SQL	SQL が切り捨てられたかどうかを示します。値は次のとおりです。 0 - false/いいえ (切り捨てられていません) 1 - true/はい (切り捨てられました)

「タスク受信者」エンティティー

結果の受信者が必要とするアクションを示します。

表 79. 「タスク受信者」エンティティー

属性	記述
必要なアクション	署名アクションを必要とするかどうかを示します。

「タスク結果 To Do リスト」エンティティー

結果の現在の状況を示します。

表 80. 「タスク結果 To Do リスト」エンティティー

属性	記述
状況	結果の現在の状況を示します。
(エスカレーション) 必要なアクション	To Do リスト・アクションを必要とするかどうかを示します。
必要なアクション	署名アクションを必要とするかどうかを示します。

「テンプレート」エンティティー

テンプレート・セット内の項目テンプレートごとに、CAS テンプレート・エンティティーが作成されます。 項目は、特定のファイルまたはファイル・パターン、環境変数またはレジストリー変数、OS スクリプトまたは SQL スクリプトの出力、あるいはログインしたユーザーのリストです。

表 81. 「テンプレート」エンティティー

属性	記述
テンプレート ID	すべての項目テンプレートのセットにおける項目テンプレートの固有 ID。
テンプレート・セット ID	テンプレート・セットの固有 ID

属性	記述
アクセス名	監査タイプに応じて、OS スクリプトまたは SQL スクリプト、環境値またはレジストリー値、あるいはファイル名またはファイル名パターンになります。
監査タイプ	モニター項目のタイプ。
監査頻度 (分)	テスト間の最大間隔 (分単位)。
MD5 を使用	MD5 アルゴリズムを使用してチェックサムを計算し、その値を前回その項目がチェックされたときに計算された値と比較することによって比較を実行するかどうかを示します。デフォルトでは、MD5 は使用しない設定になっています。MD5 を使用しても、生データのサイズが CAS ホスト用に構成された「MD5 サイズ制限」を上回る場合は、MD5 による計算と比較はスキップされます。MD5 を使用するかどうかに関わらず、項目の最終変更タイム・スタンプの現行値と項目のサイズは、前回その項目がチェックされたときに保存された値と比較されます。
データ保存	「データを保持」チェック・ボックスにマークが付けられているかどうかを示します。 マークが付けられている場合は、前のバージョンの項目を現行バージョンと比較できます。
編集可能	このテンプレートを変更できるかどうかを示します。 デフォルト Guardium テンプレートは変更できません。 さらに、CAS インスタンスで一度使用されたテンプレート・セットは変更できません。いずれの場合も、テンプレート・セットのコピーは常に作成可能であり、そのコピー・セットに変更を加えることができます。
記述	テンプレートの記述 (オプション)。
タイム・スタンプ	このテンプレートが最後に更新された日時。

「テンプレート ID」および「テンプレート・セット ID」は、admin ロールを持つユーザーのみが使用できます。

「テンプレート・セット」エンティティー

テンプレート・セットごとに CAS テンプレート・セット・エンティティーが作成されます。テンプレート・セットとは、特定のオペレーティング・システムまたはデータベース用のテンプレート項目のセットのことです。

表 82. 「テンプレート・セット」エンティティー

属性	記述
テンプレート・セット ID	テンプレート・セットの固有 ID (連番)。
OS タイプ	オペレーティング・システム: Unix または Windows
データベース・タイプ	データベース・タイプ: Oracle、MS-SQL、DB2、Sybase、Informix。オペレーティング・システム用テンプレートの場合は「N/A」。
テンプレート・セット名	テンプレート名。
IsDefault	このテンプレートが、指定された OS タイプとデータベース・タイプの組み合わせにとってデフォルトかどうかを示します。
編集可能	このテンプレートを変更できるかどうかを示します。 デフォルト Guardium テンプレートは変更できません。 さらに、CAS インスタンスで一度使用されたテンプレート・セットは変更できません。いずれの場合も、テンプレート・セットのコピーは常に作成可能であり、そのコピー・セットに変更を加えることができます。
タイム・スタンプ	テンプレートが最後に更新された日時。

「テンプレート・セット ID」は、admin ロールを持つユーザーのみが使用できます。

「テスト結果」エンティティー

このエンティティーは、テスト結果のセットごとに作成されます。

表 83. 「テスト結果」エンティティー

属性	記述
テスト結果 ID	テスト結果を識別します。
アセスメント結果 ID	アセスメント結果セットを識別します。
テスト ID1	テストを識別します。
アセスメント・テスト ID (Assessment Test Id)	評価テスト (タスク) を識別します。
テスト・スコア	返されたテスト・スコア。
レポート結果 ID	レポート結果を識別します。
パラメーター変更フラグ	最後のテスト以降にパラメーターが変更されたかどうかを示します。
結果テキスト	テストによって返されたテキスト。
テストの記述	テスト定義に含まれる記述。
推奨	テストによって返された推奨。
スコアの記述	スコアの記述。
しきい値文字列	テストのしきい値プロンプト (例えば、1 人のユーザーに許可される異なる IP の最大数)。
重大度	テスト結果に割り当てられた重大度。
カテゴリー	テスト結果のカテゴリー。

属性	記述
アセスメント結果データ・ソース ID1	テスト結果のデータ・ソースを識別します。
結果の詳細	テストの詳細。
例外グループの記述	例外グループの説明。テストが実行される時に、データが設定されます。

「テスト結果 ID」、「アセスメント結果 ID」、および「アセスメント・テスト ID (Assessment Test ID)」は、admin ロールを持つユーザーのみが使用できます。

「しきい値アラート詳細」エンティティー

このエンティティーは、相関アラートが発生するたびに作成されます。

表 84. 「しきい値アラート詳細」エンティティー

属性	記述
アラート・ログ ID	アラート詳細エンティティーを一意的に識別します。
照会値	照会によって返された値。
基本値	統計アラートに割り当てられた値。
検査日の始まり	アラート条件による検査対象期間の開始日時。
検査日の終わり	アラート条件による検査対象期間の終了日時。
アラートしきい値	アラートに定義されたアラートしきい値。
通知の送信	送信された通知のテキスト。
タイム・スタンプ	統計アラートがログに記録されるときに 1 回だけ作成されます。
アラートの記述	アラート定義に含まれる記述。

「アラート・ログ ID」は、admin ロールを持つユーザーのみが使用できます。

ユニット使用状況レベル

「管理」 > 「レポート」 > 「ユニット使用状況」には、デフォルトで以下を含むユニット使用状況レポートがいくつか提供されています。

- ユニット使用状況: 特定の時間フレームにおける各ユニットのユニット使用状況の最大レベルが表示されます。レポートの時間フレーム内のすべての期間についてのユニットの詳細を表示するドリルダウンがあります。
- ユニット使用状況の分布: このレポートは、ユニットごとに、レポートの時間フレーム内の期間のパーセントを使用状況レベルの低、中、高で示します。
- 使用状況のしきい値: この事前定義レポートは、すべてのユニット使用状況パラメーターの下限しきい値と上限しきい値をすべて表示します。

- ユニット使用状況の日次サマリー - ユニット使用状況データの日次サマリーが表示されます。

さらに、「ユニット使用状況レベル」トラッキングを使用すると、ユーザーはカスタムの照会やレポートを作成できます。
ヒント: ユニット使用状況データを使用するすべてのカスタム・レポートおよび事前定義レポートに対して別名を有効にして、ユニット使用状況レベルが数字ではなく、意味のあるストリングとして表示されるようにします。例えば、1、2、3 ではなく「低」、「中」、「高」などです。
属性のリストには、以下が含まれます。

- ホスト名
- 期間の開始
- 再始動の数
- 再始動レベルの数
- スニファー・メモリー
- スニファー・メモリー・レベル
- MySQL メモリーの比率
- MySQL メモリーの比率のレベル
- 空きバッファー・スペース
- 空きバッファー・スペース・レベル
- アナライザー・キュー
- アナライザー・キュー・レベル
- ロガー・キュー
- ロガー・キュー・レベル
- MySQL ディスク使用状況
- MySQL ディスク使用レベル
- システム CPU 負荷
- システム CPU 負荷レベル
- システム変数ディスク使用状況
- システム変数ディスク使用状況レベル
- 全体のユニット使用状況レベル
- 要求の数
- 要求数のレベル
- 完全 SQL の数
- 完全 SQL 数のレベル
- 例外の数
- 例外数のレベル
- ポリシー違反の数

- ポリシー違反数のレベル
- 未解析ログ要求の数
- 未解析ログ要求数のレベル

注: 各パラメーターには、値と、その値およびしきい値に基づいて計算されたレベルが提供されます。

「ユーザー」エンティティー

監査プロセスの結果の受信者として定義された Guardium ユーザーを識別します。

表 85. 「ユーザー」エンティティー

属性	記述
ログイン名	Guardium ユーザー名。
ファーストネーム (名)	Guardium ユーザーのファーストネーム (名)。
ラストネーム (姓)	Guardium ユーザーのラストネーム (姓)。
E メール・アドレス	Guardium ユーザーに定義された E メール・アドレス。
最終アクティブ	このユーザーの最終アクティビティーのタイム・スタンプ。

親トピック: ドメイン、エンティティー、および属性

データベース・ライセンス・レポート

データベース・ライセンス・レポートは、ユーザーが該当するデータのみに対するアクセス権限を持っていることを確認するために使用できます。Guardium システムには、いくつかのデータベース・タイプ用の事前定義のデータベース・ライセンス・レポートが用意されています。

注: DB ライセンス・レポートは、プロダクト・キーにより有効になるオプションのコンポーネントです。これらのコンポーネントが有効になっていない場合は、カスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーの選択に、以下に示す選択項目が表示されません。

事前定義ライセンス・レポートを以下にリストします。これらは、カスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーの選択でドメイン名として表示されます。

- Oracle DB ライセンス・ドメイン
- MYSQL DB ライセンス・ドメイン
- DB2® DB ライセンス・ドメイン
- Db2 for i 6.1 および 7.1 DB ライセンス・ドメイン
- SYBASE DB ライセンス・ドメイン
- Informix® DB ライセンス・ドメイン
- MSSQL 2000 DB ライセンス・ドメイン
- MSSQL 2005 DB ライセンス・ドメイン
- Netezza® DB ライセンス・ドメイン
- Teradata DB ライセンス・ドメイン
- PostgreSQL DB ライセンス・ドメイン

資格最適化 も参照してください。

Oracle DB ライセンス

以下のドメインは、Oracle DB ライセンスに関するアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

Oracle

- 「ORA ALTER SYSTEM のアカウント」 - ALTER SYSTEM 特権および ALTER SESSION 特権を持つアカウント
- 「ORA BECOME USER 特権を持つアカウント」 - BECOME USER 特権を持つアカウント
- 「ORA 全システム特権および ADMIN オプション」 - ユーザーおよびロールに対するすべてのシステム特権および管理者オプションを示すレポート
- 「ORA オブジェクトおよび列特権」 - 付与されているオブジェクト特権および列特権 (GRANT オプション付きまたはなし)
- 「ORA PUBLIC によるオブジェクト・アクセス」 - PUBLIC によるオブジェクト・アクセス
- 「ORA オブジェクト特権」 - SYS 内になく、DBA ロールではないデータベース・アカウントによるオブジェクト特権
- 「ORA SYS プロシージャーに対する PUBLIC 実行特権」 - PUBLIC に割り当てられている SYS PL/SQL プロシージャーに対する実行特権
- 「ORA 権限付与されたロール」 - ユーザーおよびロールに権限付与されたロール
- 「ORA 権限付与されたシステム特権」 - 再帰的定義 (特権がロールに割り当てられ、そのロールがユーザーに割り当てられた状態) を含む、ユーザーに付与されたシステム特権を示す階層レポート
- 「ORA SYSDBA および SYSOPER アカウント」 - SYSDBA 特権および SYSOPER 特権を持つアカウント

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

grant select on sys.dba_tab_privs to sqlguard;

grant select on sys.dba_roles to sqlguard;

grant select on sys.dba_users to sqlguard;

grant select on sys.dba_role_privs to sqlguard;

grant select on sys.dba_sys_privs to sqlguard;

grant select on sys.obj$ to sqlguard;

grant select on sys.user$ to sqlguard;

grant select on sys.objauth$ to sqlguard;

grant select on sys.table_privilege_map to sqlguard;

grant select on sys.dba_objects to sqlguard;

grant select on sys.v_$pwfile_users to sqlguard;

grant select on sys.dba_col_privs to sqlguard;

MYSQL DB ライセンス

以下のドメインは、MYSQL DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

MYSQL: 末尾が「_40」である照会では、最も基本的なバージョンの mysql スキーマ (MySQL 4.0 以降用) を使用します。information_schema は MySQL 5.0 で導入されてから変更されていないため、末尾が _50 の照会はありますが、末尾が _51 の照会はありません。 末尾が _50 の照会は、MySQL 5.0 および 5.1 で動作します。 また、information_schema は 6.0 でも変更される予定がないため、6.0 がリリースされた際には 6.0 でも動作します。末尾が「_502」の照会 (MYSQL502) では、新しい information_schema を使用します。これにはより多くの情報が含まれ、実際のデータ・ディクショナリーにより一層類似しています。

- MYSQL データベース特権 40
- MYSQL ユーザー特権 40
- MYSQL ホスト特権 40
- MYSQL 表特権 40
- MYSQL データベース特権 500
- MYSQL ユーザー特権 500
- MYSQL ホスト特権 500
- MYSQL 表特権 500
- MYSQL データベース特権 502
- MYSQL ユーザー特権 502
- MYSQL ホスト特権 502
- MYSQL 表特権 502

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリストで、データベース表内 (またはデータベース表のビュー内) でライセンスが機能するために最小限必要な特権について説明します。

注: データをアップロードするには、必要な特権に加え、ユーザーが MYSQL データベースに接続することが必要です。

MySQL の全バージョンについて、MySQL 5.0.1 を使用したライセンス照会では、表集合 mysql.db mysql.host mysql.tables_priv mysql.user を使用します。

MySQL 5.0.2 以降の全バージョンについて、ライセンス照会では表集合 information_schema.SCHEMA_PRIVILEGES mysql.host information_schema.TABLE_PRIVILEGES information_schema.USER_PRIVILEGES を使用します。

データ・ソースに MYSQL データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての MYSQL データベースでループします。

DB2 DB ライセンス

以下のドメインは、DB2 DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

- DB2 列レベルの特権 (SELECT、UPDATE など)
- DB2 データベース・レベルの特権 (CONNECT、CREATE など)
- DB2 索引レベルの特権 (CONTROL)
- DB2 パッケージ・レベルの特権 (コード・パッケージ対象の BIND、EXECUTE など)
- DB2 表レベルの特権 (SELECT、UPDATE など)DB2 特権サマリー

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

GRANT SELECT ON SYSCAT.COLAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.INDEXAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PACKAGEAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.TABAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.SCHEMAAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PASSTHRUAUTH TO SQLGUARD;

Db2 z/OS ライセンス
以下のドメインは、DB2 for z/OS の DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。

Db2 zOS PUBLIC に付与された実行可能オブジェクト特権

Db2 zOS PUBLIC に付与されたオブジェクト特権

Db2 zOS GRANTEE に付与されたシステム特権 - V8

Db2 zOS GRANTEE に付与されたシステム特権 - V9

Db2 zOS GRANTEE に付与されたシステム特権 - V10 以降

Db2 zOS GRANTEE に付与されたデータベース特権

Db2 zOS GRANTEE に付与されたスキーマ特権 - V9 以降

Db2 zOS GRANTEE に付与されたスキーマ特権 - V8 のみ

Db2 zOS GRANTEE に付与されたデータベース・リソース

Db2 zOS GRANTEE に付与されたオブジェクト特権

Db2 zOS GRANT 付きで付与されたシステム特権 - V8

Db2 zOS GRANT 付きで付与されたシステム特権 - V9

Db2 zOS GRANT 付きで付与されたシステム特権 - V10 以降

Db2 zOS PUBLIC に付与されたデータベース・リソース

Db2 zOS PUBLIC に付与されたスキーマ特権

Db2 zOS PUBLIC に付与されたデータベース特権

Db2 zOS PUBLIC に付与されたシステム特権 - V10 以降

Db2 zOS PUBLIC に付与されたシステム特権 - V9

Db2 zOS PUBLIC に付与されたシステム特権 - V8

Db2 zOS GRANT 付きで付与されたオブジェクト特権

Db2 zOS GRANT 付きで付与されたデータベース・リソース

Db2 zOS GRANT 付きで付与されたスキーマ特権 - V8 のみ

Db2 zOS GRANT 付きで付与されたスキーマ特権 - V9 以降

Db2 zOS GRANT 付きで付与されたデータベース特権

Db2 for i 6.1 および 7.1 DB ライセンス

以下のドメインは、Db2 for i DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

スクリプト gdmmonitor-db2-IBMi.sql を使用して、データベース表内 (またはデータベース表のビュー内) でライセンスが機能するために必要な最小限の特権を詳述します。

GRANTEE に付与されたオブジェクト特権 (オブジェクト・タイプ: スキーマ、表、ビュー、パッケージ、ルーチン、シーケンス、列、グローバル変数、および XML スキーマ)

PUBLIC に付与されたオブジェクト特権 (オブジェクト・タイプ: スキーマ、表、ビュー、パッケージ、ルーチン、シーケンス、列、グローバル変数、および XML スキーマ)

PUBLIC に付与された実行可能オブジェクト特権 (オブジェクト・タイプ: パッケージおよびルーチン)

GRANT オプション付きで GRANTEE に付与されたオブジェクト特権 (オブジェクト・タイプ: スキーマ、表、ビュー、パッケージ、ルーチン、シーケンス、列、グローバル変数、および XML スキーマ)

すべてのオブジェクト特権は、事前定義された Guardium グループ「Db2 for i 除外システム・スキーマ - 資格レポート」からデフォルト・システム・スキーマを除外します。除外するスキーマはこのグループに追加してください。

SYBASE DB ライセンス

以下のドメインは、SYBASE DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

- GRANT オプションを含む、SYBASE ユーザーに付与されたシステム特権とロール
- GRANT オプションを含む、SYBASE ユーザーに権限付与されたロールおよびユーザーとロールに付与されたシステム特権
- SYBASE PUBLIC によるオブジェクト・アクセス
- PUBLIC に割り当てられた、プロシージャーおよび関数に対する SYBASE 実行特権
- システムまたはセキュリティー admin ロールを持つ SYBASE アカウント
- GRANT オプション付きで付与された SYBASE オブジェクト特権および列特権
- SYBASE ユーザーに権限付与されたロール

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

/* 以下は MASTER データベースでは必須です */

grant select on master.dbo.sysloginroles to sqlguard

grant select on master.dbo.syslogins to sqlguard

grant select on master.dbo.syssrvroles to sqlguard

/*以下は MASTER を含むすべてのデータベースで必須です */

grant select on sysprotects to sqlguard

grant select on sysusers to sqlguard

grant select on sysobjects to sqlguard

grant select on sysroles to sqlguard

データ・ソースに SYBASE データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての SYBASE データベースでループします。

SYBASE IQ ライセンス

サポートされるバージョンは sybase IQ 15 以上です。

データをアップロードするために以下のカスタム表定義が作成されます (ID は無視できます)。

139 | SybaseIQ15 オブジェクト特権 (DB ユーザー別)

140 | SybaseIQ15 オブジェクト特権 (グループ別)

141 | SybaseIQ15 ユーザーに付与されたシステム権限とグループ

142 | SybaseIQ15 ユーザーとグループに付与されたシステム権限とグループ

143 | SybaseIQ15 PUBLIC によるオブジェクト・アクセス

144 | SybaseIQ15 PUBLIC に付与されたプロシージャーと関数の実行特権

145 | SybaseIQ15 データベース管理者/アクセス権管理者などの権限を持つユーザー・グループ

146 | SybaseIQ15 GRANT 付きで付与された表、ビューの特権

147 | SybaseIQ15 ユーザーとグループに付与されたグループ

148 | SybaseIQ15 ログインが指定されたユーザー・グループのログイン・ポリシー

対応する照会およびレポートは以下のとおりです (ID は無視できます)。

597 | SybaseIQ15 オブジェクト特権 (DB ユーザー別)

598 | SybaseIQ15 オブジェクト特権 (グループ別)

599 | SybaseIQ15 ユーザーに付与されたシステム権限とグループ

600 | SybaseIQ15 ユーザーとグループの被付与者に付与されたシステム権限とグループ

601 | SybaseIQ15 PUBLIC によるオブジェクト・アクセス

602 | SybaseIQ15 PUBLIC に付与されたプロシージャーと関数に対する実行特権

603 | SybaseIQ15 データベース管理者/アクセス権管理者/ユーザー管理者/リモート・データベース管理者のデータベース権限を持つユーザー・グループ

604 | SybaseIQ15 GRANT 付きで付与された表、ビューの特権

605 | SybaseIQ15 ユーザーとグループに付与されたグループ

606 | SybaseIQ15 ログイン・オプション設定が指定されたユーザーとグループのログイン・ポリシー

これらは、他のライセンスと共に DB ライセンスの下に表示されます。

==========

それぞれについて説明します。一部のものはそれ自体が説明になっています。しかし、さらに説明が必要なものもあります。

1 /*

データベース・ユーザー別のオブジェクト特権。

オブジェクトには、表、ビュー、プロシージャーおよび関数が含まれます。

これらはユーザーにのみ付与される特権であり、グループやグループのメンバーシップは含まれていません。

*/

2. /*

グループ別のオブジェクト特権。

オブジェクトには、表、ビュー、プロシージャーおよび関数が含まれます。

これらはグループにのみ付与される特権です。

*/

3 /* ユーザーに付与されたシステム権限とグループ。

*/

4 /* ユーザーとグループの被付与者に付与されたシステム権限とグループ。

*/

5 /* PUBLIC によるオブジェクト・アクセス。

表、ビュー、関数およびプロシージャーが含まれます。

*/

6 /* PUBLIC に付与されたプロシージャーと関数に対する実行特権。

*/

7 /* データベース管理者、アクセス権管理者、ユーザー管理者、またはリモート・データベース管理者のデータベース権限を持つユーザーとグループ。

*/

8 /* GRANT オプション付きでユーザーとグループに付与された表とビューの特権。

これは Sybase IQ で唯一許可される GRANT オプション・タイプであることに注意してください。 ルーチンに GRANT オプション付きで権限を付与することはできません。

*/

9 /* ユーザーとグループに付与されたグループ。

*/

10 /* ログイン・オプション設定を指定してユーザーとグループに割り当てられたログイン・ポリシー。 */

GuardAPI を使用して Sybase IQ レポートにデータ・ソースを追加する方法

GuardAPI を使用して各 Sybase IQ レポートにデータ・ソースを追加し、それらのレポートを実行する方法です。

新しい各レポートにデータ・ソースを追加して、各レポートを実行する方法については、下記の例を参照してください。

すべての SybaseIQ 資格レポートに関するデータ・ソースを追加

grdapi create_datasource type="Sybase IQ" user=ent password=Guardium123 host=9.70.144.152 name="SybaseIQ15 entitlement6" shared=true owner=admin application=CustomDomain port=2638 dbName=sn5qpuff

すべての SybaseIQ 資格レポートに対してデータ・ソースを追加

grdapi create_datasourceRef_by_name application=CustomTables objName="SybaseIQ15 Exec priv on proc func to PUBLIC"datasourceName="SybaseIQ15 entitlement6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Group granted to user and group" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Login policy for user group with login"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Object Access By Public" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Object Privileges By DB User" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Object Privileges By Group" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 System Authority And Group Granted To User"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 System Authority And Group Granted To User And Group"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Table View priv granted with grant"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 User Group With DBA Perms Admin etc"datasourceName="SybaseIQ15 entitlement 6"

すべての SybaseIQ 資格レポートを実行

grdapi upload_custom_data tableName=SYBASEIQ15_EXEC_PRIV_ON_PROC_FUNC_TO_PUBLIC

grdapi upload_custom_data tableName=SYBASEIQ15_GROUP_GRANTED_TO_USER_AND_GROUP

grdapi upload_custom_data tableName=SYBASE_OBJ_COL_PRIVS_GRANTED_WITH_GRAN

grdapi upload_custom_data tableName=SYBASEIQ15_OBJECT_ACCESS_BY_PUBLIC

grdapi upload_custom_data tableName=SYBASEIQ15_OBJECT_PRIVS_BY_DB_USER

grdapi upload_custom_data tableName=SYBASEIQ15_OBJECT_PRIVILEGES_BY_GROUP

grdapi upload_custom_data

tableName=SYBASEIQ15_SYSTEM_AUTHORITY_AND_GROUP_GRANTED_TO_USER grdapi upload_custom_data

tableName=SYBASEIQ15_SYSTEM_AUTHORITY_AND_GROUP_GRANTED_TO_USER_AND_GROUP grdapi upload_custom_data

tableName=SYBASEIQ15_TABLE_VIEWS_PRIV_GRANTED_WITH_GRANT grdapi upload_custom_data

tableName=SYBASEIQ15_USER_GROUP_WITH_DBA_PERMS_ADMIN_ETC

Informix DB ライセンス

以下のドメインは、Informix DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「DB ライセンス」タブを表示します。

- データベース・アカウントによる Informix オブジェクト特権 (システム・アカウントとロールを除く)
- GRANT オプション付きでユーザーに付与された Informix データベース・レベル特権、ロール、および言語
- GRANT オプション付きでユーザーおよびロールに付与された Informix データベース・レベル特権、ロール、および言語
- Informix PUBLIC に付与されたオブジェクト権限
- PUBLIC に付与された Informix プロシージャーおよび関数に対する Informix 実行特権
- DBA 特権付きの Informix アカウント GRANT オプション付きで付与された Informix オブジェクト特権および列特権
- ユーザーおよびロールに権限付与された Informix ロール

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

システム・カタログの SELECT 特権については、すべてのユーザーが十分な特権を持っているため、どのユーザーにも特権を付与する必要はありません。Informix は、ユーザーに対してシステム・カタログを付与しないようです。通常は、以下の権限付与が使用されます。 ただしこの場合は必要ありません。

grant select on systables to sqlguard;

grant select on systabauth to sqlguard;

grant select on sysusers to sqlguard;

grant select on sysroleauth to sqlguard;

grant select on syslangauth to sqlguard;

grant select on sysroutinelangs to sqlguard;

grant select on sysprocauth to sqlguard;

grant select on sysprocedures to sqlguard;

grant select on syscolauth to sqlguard;

データ・ソースに Informix データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての Informix データベースでループします。

MSSQL 2000 DB ライセンス

以下のドメインは、MSSQL 2000 DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「**DB ライセンス**」タブを表示します。

- MSSQL2000 デフォルトのシステム・ユーザーを除くデータベース・アカウントによるオブジェクト特権
- MSSQL2000 GRANT オプション付きでユーザーに付与されたロールおよびシステム特権
- MSSQL2000 ユーザーおよびロールに権限付与されたロール。GRANT オプション付きでユーザーおよびロールに付与されたシステム特権
- MSSQL2000 PUBLIC によるオブジェクト・アクセス
- MSSQL2000 PUBLIC に割り当てられたシステム・プロシージャーおよび関数に対する実行特権
- MSSQL2000 db_owner ロールおよび db_securityadmin ロールを持つデータベース・アカウント
- MSSQL2000 sysadmin、serveradmin、および security admin を持つサーバー・アカウント /* MASTER データベースに対してのみこのライセンスを実行します */
- MSSQL2000 GRANT オプション付きで付与されたオブジェクト特権および列特権
- MSSQL2000 ユーザーおよびロールに権限付与されたロール

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

/* 以下は MASTER データベースでは必須です */

grant select on dbo.syslogins to sqlguard

/*以下は MASTER を含むすべてのデータベースで必須です */

grant select on dbo.sysprotects to sqlguard

grant select on dbo.sysusers to sqlguard

grant select on dbo.sysobjects to sqlguard

grant select on dbo.sysmembers to sqlguard

データ・ソースに MSSQL データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての MSSQL データベースでループします。

MSSQL 20005/2008 DB ライセンス

以下のドメインは、MSSQL 2005 または MSSQL 2008 DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「**DB ライセンス**」タブを表示します。

注: 以下に示した MSSQL2005 のライセンス・ドメインは、MSSQL2008 でも使用できます。
注: 動的照会ストリング内のオブジェクトは、xxx_DEPENDENCIES には表示されません。保管されたプログラム単位によって呼び出された EXECUTE IMMEDIATE SQL ストリング内のオブジェクトは、従属関係を表示しません。この照会は、グループ ID 202「Dependencies_exclude_schema-MSSQL」で定義されたスキーマ所有者を除外します。ユーザーは、従属関係照会を行うために、このグループのスキーマ名を追加または除去できます。

- MSSQL2005/8 デフォルトのシステム・ユーザーを除くデータベース・アカウントによるオブジェクト特権
- MSSQL2005/8 ユーザーに付与されたロールおよびシステム特権
- MSSQL2005/8 GRANT オプション付きでユーザーおよびロールに付与されたロールおよびシステム特権
- MSSQL2005/8 PUBLIC によるオブジェクト・アクセス
- MSSQL2005/8 PUBLIC に割り当てられたシステム・プロシージャーおよび関数に対する実行特権
- MSSQL2005/8 db_owner ロールおよび db_securityadmin ロールのデータベース・アカウント

- MSSQL2005/8 sysadmin、serveradmin、security admin のサーバー・アカウント /* MASTER データベースに対してのみ実行します */
- MSSQL2005/8 GRANT オプション付きで付与されたオブジェクト特権および列特権
- MSSQL2005/8 ユーザーおよびロールに付与されたロール

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

/* 以下は MASTER データベースでは必須です */

grant select on sys.server_principals to sqlguard

/*以下は MASTER を含むすべてのデータベースで必須です */

grant select on sys.database_permissions to sqlguard

grant select on sys.database_principals to sqlguard

grant select on sys.all_objects to sqlguard

grant select on sys.database_role_members to sqlguard

grant select on sys.columns to sqlguard

データ・ソースに MSSQL データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての MSSQL データベースでループします。

Netezza DB ライセンス

以下のドメインは、Netezza DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「**DB ライセンス**」タブを表示します。

注: Netezza では、データベース・エラーのテキスト変換は行われません。エラーは例外の記述に表示されます。ユーザーは、必要に応じて Netezza の例外の記述を含むレポートのコピーを作成したり、追加したりできます。

- 「Netezza オブジェクト特権 (データベース・ユーザー名別)」 - ADMIN アカウント以外のデータベース・ユーザー名により、GRANT オプション付きまたはなしで付与されたオブジェクト特権
- 「Netezza 管理者特権 (データベース・ユーザー名別)」 - ADMIN アカウント以外のデータベース・ユーザー名により、GRANT オプション付きまたはなしで付与された管理者特権
- 「Netezza ユーザーに権限付与されたグループ/ロール」 - ユーザーに権限付与されたグループ (ロール)
- 「Netezza オブジェクト特権 (グループ別)」 - PUBLIC を除くグループにより、GRANT オプション付きまたはなしで付与されたオブジェクト特権
- 「Netezza 管理者特権 (グループ別)」 - PUBLIC を除くグループにより、GRANT オプション付きまたはなしで付与された管理者特権
- 「Netezza 管理者特権 (データベース・ユーザー名グループ別)」 - ADMIN アカウントおよび PUBLIC グループを除くデータベース・ユーザー名およびグループにより、GRANT オプション付きまたはなしで付与された管理者特権
- 「Netezza 付与されたオブジェクト特権」 - GRANT オプション付きまたはなしで PUBLIC に対して付与されたオブジェクト特権
- 「Netezza 付与された管理者特権」 - GRANT オプション付きまたはなしで PUBLIC に対して付与された管理特権
- 「Netezza ユーザーおよびグループに対するグローバル管理者特権」 - ADMIN アカウントを除くユーザーおよびグループに付与されたグローバル管理者特権
- 「Netezza ユーザーおよびグループに対するグローバル・オブジェクト特権」 - ADMIN アカウントを除くユーザーおよびグループに付与されたグローバル・オブジェクト特権

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

/* このスクリプトは、システム・データベースから実行する必要があります */

GRANT SELECT ON SYSTEM VIEW TO sqlguard;

GRANT LIST ON DATABASE TO sqlguard;

GRANT LIST ON USER TO sqlguard;

GRANT LIST ON GROUP TO sqlguard;

GRANT SELECT ON _V_CONNECTION TO sqlguard;

Netezza ライセンス照会では、特にこれらのレポートを実行する予定のユーザーに対して特権を付与する際に、システム・データベースへの接続が推奨されます。特権の付与は、システム・データベースから行う必要があります。それ以外のデータベースから付与された特権は、その特定のデータベースでのみ有効になります。システム・データベースから特権の付与が行われた場合は、特殊機構により、付与された特権がすべてのデータベースで有効になります。

Teradata DB ライセンス

以下のドメインは、Teradata DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「**DB ライセンス**」タブを表示します。

- デフォルトのシステム・ユーザーを除くデータベース・アカウントにより付与された Teradata オブジェクト特権
- GRANT オプション付きで Teradata ユーザーに付与されたシステム特権とロール
- GRANT オプション付きで Teradata ユーザーおよびロールに権限付与されたロール
- Teradata ユーザーおよびロールに権限付与されたロール。 GRANT オプション付きでユーザーおよびロールに付与されたシステム特権。
- PUBLIC に対して付与された Teradata オブジェクト特権およびシステム特権。Teradata では、PUBLIC に対してロールを権限付与できないことに注意してください。
- PUBLIC に対して付与されたシステム・データベース・オブジェクトに対する Teradata 実行特権
- ユーザーおよびロールに付与された Teradata システム管理者特権およびセキュリティー管理者特権
  注: Teradata には、システム管理者またはセキュリティー管理者というロールはありません。ユーザーは独自のロールを作成する必要があります。次のような重要なシステム特権は、通常、一般的なユーザーに付与されません: ABORT SESSION、CREATE DATABASE、CREATE PROFILE、CREATE ROLE、CREATE USER、DROP DATABASE、DROP PROFILE、DROP ROLE、DROP USER、MONITOR RESOURCE、MONITOR SESSION、REPLICATION OVERRIDE、SET SESSION RATE、SET RESOURCE RATE。
- GRANT オプション付きでユーザーに付与された Teradata オブジェクト特権。DBC および grantee = 'All' は含みません。

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

/* 以下の表およびビューに対する選択特権は必須です */

GRANT SELECT ON DBC.AllRights TO sqlguard;

GRANT SELECT ON DBC.Tables TO sqlguard;

GRANT SELECT ON DBC.AllRoleRights TO sqlguard;

GRANT SELECT ON DBC.RoleMembers TO sqlguard;

PostgreSQL DB ライセンス

以下のドメインは、PostgreSQL DB ライセンスでのアップロードおよびレポート作成を容易にするために提供されています。以下の各ドメインには、同じ名前を持つ単一のエンティティーと事前定義されたレポートが 1 つあります。これらのドメインは、すべてカスタム・ドメイン・ビルダー、カスタム・ドメイン照会、カスタム表ビルダーで使用することができます。これらは、他の事前定義されたエンティティーやレポートと同様、変更はできませんが、コピーを作成してユーザー独自のドメインやレポートにカスタマイズすることができます。ライセンス・レポートを参照するには、ユーザー・ポータルにログオンし、「**DB ライセンス**」タブを表示します。

PostgreSQL には、7 つのライセンス・カスタム・ドメイン、照会、レポートがあります。これを以下に示します (それぞれについてレポート名、説明、注記を示します)。

- 「PostgreSQL GRANT オプションあり/なしで PUBLIC ユーザー・ロールに付与されたデータベースに対する特権」。GRANT オプション付きまたはなしで、PUBLIC、ユーザーおよびロールに付与されたデータベースに対する特権です。任意のデータベース (理想的には PostgreSQL) でこれを実行します。
- 「PostgreSQL GRANT オプションあり/なしで PUBLIC ユーザー・ロールに付与された言語に対する特権」。GRANT オプション付きまたはなしで、PUBLIC、ユーザーおよびロールに対して付与された言語に対する特権です。
- 「PostgreSQL GRANT オプションあり/なしで PUBLIC ユーザー・ロールに付与されたスキーマに対する特権」。GRANT オプション付きまたはなしで、PUBLIC、ユーザーおよびロールに付与されたスキーマに対する特権です。
- 「PostgreSQL GRANT オプションあり/なしで PUBLIC ユーザー・ロールに付与された表スペースに対する特権」。GRANT オプション付きまたはなしで、PUBLIC、ユーザーおよびロールに対して付与された表スペースに対する特権です。任意のデータベース (理想的には PostgreSQL) でこれを実行します。
- 「ユーザーまたはロールに付与された PostgreSQL ロールまたはユーザー」。GRANT オプション付きでユーザーまたはロールに権限付与されたロールまたはユーザーです。任意のデータベースでこれを一度実行します。理想的には PostgreSQL で実行します。
- 「PostgreSQL ユーザーまたはロールに権限付与されたスーパーユーザー」。ユーザーまたはロールに権限付与されたスーパーユーザーです。任意のデータベースでこれを一度実行します。理想的には PostgreSQL で実行します。

- 「PostgreSQL ユーザーおよびロールに付与されたシステム特権」。ユーザーおよびロールに付与されたシステム特権です。任意のデータベースでこれを一度実行します。理想的には PostgreSQL で実行します。
- 「PostgreSQL PUBLIC に付与された表、ビュー、シーケンス、および関数特権」。PUBLIC に対して付与された、表、ビュー、シーケンス、および関数特権です。データベースごとにこれを実行します。
- 「PostgreSQL GRANT オプション付きで付与された表、ビュー、シーケンス、および関数特権」。GRANT オプションのみを付加して、ユーザーおよびロールに付与された表、ビュー、シーケンス、および関数特権です。PostgreSQL アカウントを除きます。
- 「PostgreSQL ロールに付与された表、ビュー、シーケンス、関数特権」。ロールに付与された、表、ビュー、シーケンス、および関数特権です。 PUBLIC は除きます。
- 「PostgreSQL ログインに付与された表、ビュー、シーケンス、および関数特権」。ログインに付与された、表、ビュー、シーケンス、および関数特権です。postgres システム・ユーザーを除きます。

注: バージョン 8.3.6 以降、PostgreSQL では PUBLIC に対する管理者オプションの付与をサポートしていません。関数のみで、ストアード・プロシージャーはありません。表の権限付与のみがサポートされ、列の権限付与はサポートされていません。PUBLIC はグループであり、ユーザーではありません。PUBLIC は、pg_roles には表示されません。これらのすべての照会を実行する必要がある特権は、「GRANT CONNECT ON DATABASE PostgreSQL TO username;」のみです。

さまざまなデータ・ソースからデータをアップロードできるようにするライセンスの場合、通常、データベースのアクセスに使用するログインが、照会で使用される表 (すべてのライセンスに対して非表示) を読み取れる必要があります。

以下のリスト (コメント行の見出し付き) は、ライセンスを機能させるために必要な、データベース表内での (またはデータベース表のビュー内での) 最小限の特権を示します。

```
/* 以下の表およびビューに対する選択特権は必須です */

/*これは POSTGRES データベースで必須です。*/

grant connect on database postgres to sqlguard;


/*以下は POSTGRES を含むすべてのデータベースで必須です (デフォルトで既に PUBLIC に付与されています) */

grant select on pg_class to sqlguard;

grant select on pg_namespace to sqlguard;

grant select on pg_roles to sqlguard;

grant select on pg_proc to sqlguard;

grant select on pg_auth_members to sqlguard;

grant select on pg_language to sqlguard;

grant select on pg_tablespace to sqlguard;

grant select on pg_database  to sqlguard;
```

データ・ソースに PostgreSQL データベース・タイプがあるものの、データベース名がない場合 (「データ・ソース定義」を確認し、「ロケーション」の下にあるデータベース名が空である場合) は、データのアップロードが、ユーザーがアクセス権を持つすべての PostgreSQL データベースでループします。

親トピック: ドメイン、エンティティー、および属性

事前定義レポートを活用する方法

カスタム・レポートを最初から作成するのではなく、Guardium アプリケーションの事前定義コンテンツを活用できます。

Guardium アプリケーションで使用可能な事前定義レポートにアクセスすることによって、求めている情報を迅速に取得できます。 これらの事前定義レポートは、ユーザーの必要に応じて、複製してカスタマイズすることができます。

Guardium 事前定義レポートを使用することは、推奨されるベスト・プラクティスでです。これにより、組織は、不適切に公開されたオブジェクト、過度の権限を持つユーザー、および無許可の管理アクションなどのセキュリティー・リスクを迅速かつ簡単に識別できます。 多くの事前定義レポートの例として、システム特権を持つアカウント、すべてのシステム特権および管理者特権 (ユーザー別およびロール別)、ユーザー別のオブジェクト特権、および PUBLIC アクセス権限を持つすべてのオブジェクトなどがあります。

すべてのレポートに、すべてのパラメーターと値が表示されます。パラメーターと値は、任意のレポート画面で「カスタマイズ」を使用して編集できます。

レポート例をいくつか以下に示します。

Guardium へのログイン

このレポートの値はすべて、「Guardium ログイン」エンティティーから取得されます。レポート期間中、このレポートの各行には、ユーザー名、ログイン成功 (1 は成功、0 は失敗、-1 はパスワード期限切れ、-2 は異なる IP からのログイン)、ログインの日時、ログアウトの日時 (ユーザーがまだログアウトしていない場合はブランク)、ホスト名、(ユーザーの) リモート・アドレス、およびその行のログイン数がリストされます。

レポート・ロケーション:「レポート」 > 「Guardium システムのモニター」 > 「Guardium ログイン」

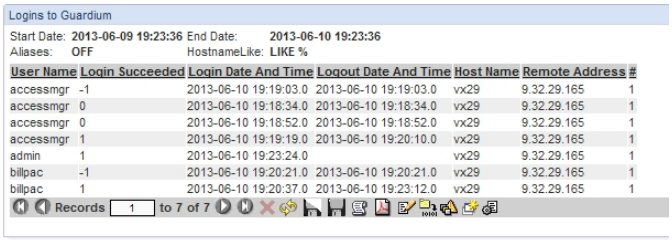


表 1. Guardium へのログイン

ドメイン	ベースとなる照会	メイン・エンティティー
Guardium ログイン	Guardium ログイン	Guardium ユーザー・ログイン
ランタイム・パラメーター	演算子	デフォルト値
ホスト名	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

バッファー使用状況モニター

バッファー使用状況の統計の詳細を表示します。

レポート・ロケーション:「レポート」 > 「Guardium 運用レポート」 > 「エンタープライズ・バッファー使用状況」

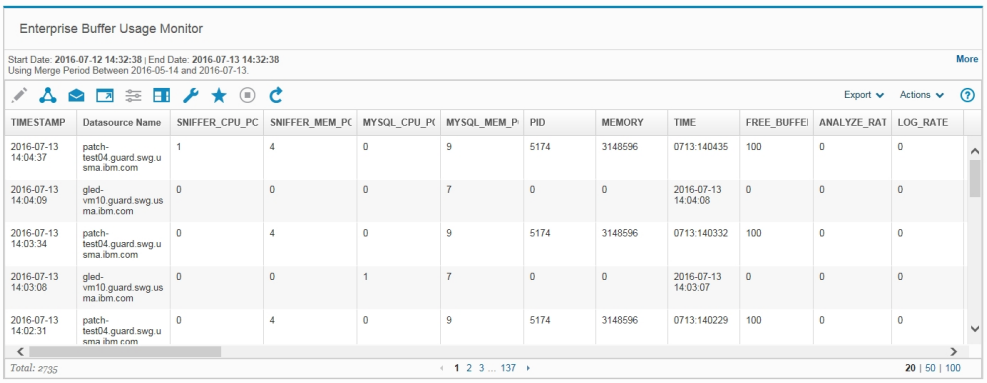


表 2. バッファー使用状況モニター

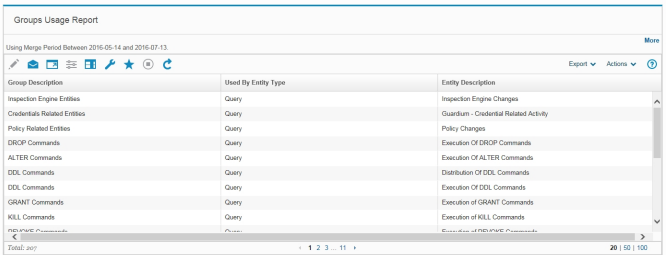
ドメイン	ベースとなる照会	メイン・エンティティー
バッファー使用状況	バッファー使用状況モニター	スニファーのバッファー使用のモニター
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

グループ使用状況レポート

このレポートは、定義済みグループと、各グループに依存するエンティティーをすべてリスト表示します。

注: このレポートには、使用可能な 328 のレコードがあります。

レポート・ロケーション:「レポート」 > 「Guardium システムのモニター」 > 「グループ使用状況レポート」



Guardium アプリケーション

Guardium アプリケーションごとに、各行には、割り当てられたセキュリティー・ロール、 または all というワード (すべてのロールが割り当てられていることを示す) がリストされます。

レポート・ロケーション: 「レポート」 > 「リアルタイム Guardium 運用レポート」 > 「すべての Guardium アプリケーション - ロール」

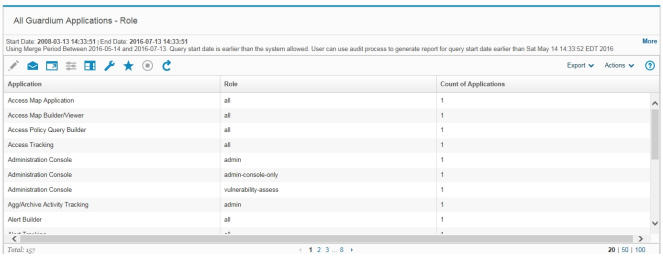


表 3. Guardium アプリケーション

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	すべての Guardium アプリケーション	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -100 Month DAY
期間終了	<=	NOW

Guardium ロール

このメニュー・ペインには、2 つのレポート (「全ロール - アプリケーション・アクセス」と 「全ロール - ユーザー」) が表示されます。

全ロール - アプリケーション・アクセス。ロールごとに、このレポートにはそのロールが割り当てられているアプリケーションの数がリストされます。

ロールが割り当てられているアプリケーションをリストするには、 そのロールをクリックして、「レコード詳細」レポートまでドリルダウンします。

レポート・ロケーション: 「レポート」 > 「Guardium システムのモニター」 > 「全ロール - アプリケーション・アクセス」

All Roles - Application Access

Start Date: **2005-02-10 11:32:45** End Date: **2013-06-10 11:32:45**
Aliases: OFF

Role	Count of Application	Count of Roles
accessmgr	27	1
admin	38	1
admin-mobile	26	1
appdev	26	1
audit	26	1
audit-delete	26	1
cas	27	1
cli	27	1
datasec-exempt	26	1
dba	26	1
diag	26	1
infosec	26	1
inv	27	1
netadm	26	1
optim-audit	26	1
review-only	26	1
security-mobile-analyst	26	1
user	27	1
vulnerability-assess	26	1

Records 1 to 19 of 19

All Roles - User

Start Date: **2005-02-10 11:32:45** End Date: **2013-06-10 11:32:45**
Aliases: OFF

Role	Users Belong	# of Roles
accessmgr	1	1
admin	1	1
admin-mobile	0	1
appdev	0	1
audit	0	1

表 4. 全ロール - アプリケーション・アクセス

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	全ロール - アプリケーション・アクセス	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -100 MONTH
期間終了	<=	NOW

全ロール - ユーザー

ロールごとに、このレポートにはそのロールが割り当てられているユーザーの数がリストされます。 ロールが割り当てられているユーザーをリストするには、そのロールをクリックして、「レコード詳細」レポートまでドリルダウンします。

表 5. 全ロール - ユーザー

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	ロール - ユーザー	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -100 MONTH
期間終了	<=	NOW

Guardium ユーザー

各ユーザー、最終アクティビティーの日付、割り当てられているロールの数をリストします。 ユーザーごとに、「レコード詳細」レポートまでドリルダウンすると、そのユーザーに割り当てられているロールを確認できます。

表 6. Guardium ユーザー

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	ユーザー・ロール	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -100 MONTH
期間終了	<=	NOW

ユニット使用状況レベル

以下のデフォルト・レポートには、ユニット使用状況データが表示されます。

- ユニット使用状況: 特定の時間フレームにおける各ユニットのユニット使用状況の最大レベルが表示されます。レポートの時間フレーム内のすべての期間についてのユニットの詳細を表示するドリルダウンがあります。
- ユニット使用状況の分布: このレポートは、ユニットごとに、レポートの時間フレーム内の期間のパーセントを使用状況レベルの低、中、高で示します。
- 使用状況のしきい値: この事前定義レポートは、すべてのユニット使用状況パラメーターの下限しきい値と上限しきい値をすべて表示します。

- ユニット使用状況の日次サマリー - ユニット使用状況データの日次サマリーが表示されます。

表 7. ユニット使用状況レベル

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	ユニット使用状況の分布	ユニット使用状況レベル
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -24 HOUR
期間終了	<=	NOW

- 定義済みレポート
  インストール時に、Guardium® アプライアンスは数多くの事前定義レポートと共に構成されています。
- 事前定義管理レポート
  このセクションでは、デフォルト管理者レイアウトでのすべての事前定義レポートについて、簡単に説明します。
- 事前定義ユーザー・レポート
  このセクションでは、デフォルト・ユーザー・レイアウトでのすべての事前定義レポートについて 簡単に説明します。
- 事前定義レポート (共通)
  このセクションでは、デフォルト・ユーザー・レイアウトとデフォルト管理者レイアウトでのすべての事前定義レポートについて、簡単に説明します。

親トピック: レポート

定義済みレポート

インストール時に、Guardium® アプライアンスは数多くの事前定義レポートと共に構成されています。

すべてのレポートに、すべてのパラメーターと値が表示されます。パラメーターと値は、 任意のレポート画面で「カスタマイズ」ボタンから編集できます。

ヘルプの検索機能を使用して、特定のレポートに直接進みます。 語句を引用符で囲むと、検索語が正確に定義されます。

事前定義レポートについては、以下のページに説明があります。

- 事前定義管理レポート (事前定義管理レポート)。これらは、admin ユーザーが使用できる事前定義レポートです。
- Accessmgr からの事前定義レポート (トピック『アクセス管理の概要』を参照): ユーザーとロールのレポート、許可されたデータ・ソース、許可されたサーバー、関連付けられていないデータベース、関連付けられていないデータ・ソース。

表形式レポートおよびグラフィカル・レポートから監査プロセスを実行する API

Guardium GUI には、GuardAPI の create_ad_hoc_audit_and_run_once を呼び出すアイコン (「今すぐ 1 回実行する特別プロセス」) があります。

これにより、以下のフィールドを示すウィンドウが開きます。

- E メール・アドレス - E メール・アドレスのコンマ区切りリスト。
- E メール受信者のコンテンツ・タイプ: PDF/CSV (ラジオ・ボタン 0 - PDF / 1 - CSV)

- ユーザーを受信者として追加 (チェック・ボックス)

このプロセスの動作は次のとおりです。

1 - 新規プロセスの場合は、 emailContentType パラメーターに示されるコンテンツ・タイプで、 リスト (存在する場合) に 1 つまたは複数の E メール受信者を作成できます。また、includeUserReceiver パラメーターが true の場合は、(API を呼び出して) ログイン・ユーザーの受信者も作成します。

2 - 既存のプロセスの場合は、すべての E メール受信者が削除され、emailContentType パラメーターに定義されているコンテンツ・タイプで、新規リスト (存在する場合) の E メールに置き換えられます。リストが空の場合は、E メール・アドレス・レシーバーがすべて削除されます。 ユーザーの受信者が既に存在する場合は (includeUserreceiver が false であっても) その受信者は削除されませんが、このパラメーターが true で、かつそのような受信者が存在しない場合は追加されます。

監査プロセスが生成されると、これは (「今すぐ 1 回実行」と同じように) 自動的に実行され、ユーザーはその監査プロセスが自分の To-Do リスト上のアイテムとなることを期待します。

特別な監査プロセスを作成する GuardAPI では、結果が 1 日ではなく 7 日間保持されます。 結果は 7 日後に削除されます。

パラメーターについて詳しくは、『GuardAPI 入力生成』ヘルプ・トピックの GuardAPI コマンド create_ad_hoc_audit_and_run_once を参照してください。

事前定義レポートのユース・ケース

データベース管理者

- SQL エラー - SQL エラーの増加は、SQL インジェクション攻撃を示している可能性があります。
- DDL (スキーマ変更の確認) - このレポートは、DDL の要求元となるクライアント IP、メイン SQL 動詞 (特定の DDL コマンド)、およびそのレコード用にアクセスされる合計オブジェクトを表示します。
- 失敗したログイン - このレポートは、期限切れのログイン資格情報を使用したデータベースへのアクセス試行を示します。

機密保護担当者

- 失敗したログイン - データベースにアクセスしようとした、適切な資格情報を持つユーザー。
- 無効なユーザー - データベースにアクセスしようとした無効なユーザー。
- ポリシー違反 - セキュリティー・ポリシーに違反しているユーザーおよび問題。

監査員

- コンプライアンス・レポート - PCI、SOX、データ・プライバシー
- コンプライアンス・ワークフロー - サインオフおよびプロシージャーの証拠を示します。

親トピック: 事前定義レポートを活用する方法

事前定義管理レポート

このセクションでは、デフォルト管理者レイアウトでのすべての事前定義レポートについて、簡単に説明します。

Guardium GUI のレポート選択には次の 5 つのセクションがあります。

- レポート構成ツール
- Guardium 運用レポート
- リアルタイム Guardium 運用レポート
- Guardium 構成項目
- Guardium システムのモニター

注: 監視データ・レベルでのデータ・レベル・セキュリティーが有効な場合 (「グローバル・プロファイル」設定を参照)、ユーザーに対してユーザーのデータベース情報のみが表示されるよう、監査プロセスの出力がフィルタリングされます。

事前定義管理レポートはアルファベット順にリストされます。

変更されたアクティブ S-TAP

このアラートは、中央マネージャー・システムでのみ実行されます。S-TAP® ホスト、S-TAP バージョン、 変更された S-TAP、タイム・スタンプ、およびカウントが表示されます。

表 1. 変更されたアクティブ S-TAP

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	変更されたアクティブ S-TAP	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	なし	なし

admin ユーザーのログイン

admin ユーザー・グループで定義したデータベース・ユーザー名によるデータベースへのログインのサマリー。 このレポートには、管理特権を持つユーザーがデータベースへのログインに使用するクライアント IP アドレス、 データベース・ユーザー名、ソース・プログラム、セッション開始日時、そのレコードのセッション総計が表示されます。

表 2. admin ユーザーのログイン

ドメイン	ベースとなる照会	メイン・エンティティー

ドメイン	ベースとなる照会	メイン・エンティティー
アクセス	admin ユーザーのログイン	セッション
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

統合/アーカイブ・ログ

このレポートでは、Guardium® の統合アクティビティーがアクティビティー・タイプ別にリストされます。 レポートの各行には、アクティビティー・タイプ、開始時刻、ファイル名、状況、 コメント、Guardium ホスト名、パージされたレコード、期間の開始、期間の終了、 およびその行のログ・レコードの数が含まれています。 「Guardium ホスト名」ランタイム・パラメーターの設定によって、 出力を制限することができます。このパラメーターは、デフォルトでは % (すべてのサーバーを選択) に設定されています。「パージされたレコード」列には、アクティビティー・タイプが「パージ」の場合にのみ、パージされたレコードの数が表示されます。

表 3. 統合/アーカイブ・ログ

ドメイン	ベースとなる照会	メイン・エンティティー
統合/エクスポート/インポート	統合/アーカイブ・ログ	統合/アーカイブ・ログ
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 WEEK
期間終了	<=	NOW
Guardium ホスト名	LIKE	%

すべての Guardium アプリケーション - ロール

このメニュー・ペインには、2 つのレポート (「全ロール - アプリケーション・アクセス」と 「全ロール - ユーザー」) が表示されます。

全ロール - アプリケーション・アクセス

ロールごとに、このレポートにはそのロールが割り当てられているアプリケーションの数がリストされます。 ロールが割り当てられているアプリケーションをリストするには、 そのロールをクリックして、「レコード詳細」レポートまでドリルダウンします。

表 4. 全ロール - アプリケーション・アクセス

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	全ロール - アプリケーション・アクセス	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -100 MONTH
期間終了	<=	NOW

全ロール - ユーザー

ロールごとに、このレポートにはそのロールが割り当てられているユーザーの数がリストされます。 ロールが割り当てられているユーザーをリストするには、 そのロールをクリックして、「レコード詳細」レポートまでドリルダウンします。

表 5. 全ロール - ユーザー

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	ロール - ユーザー	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -100 MONTH
期間終了	<=	NOW

アプライアンス設定

このレポートには、Guardium システムの構成設定が表示されます。*アプライアンス設定* レポートを使用して、Guardium 設定を迅速にレビューして確認できます。

表 6. アプライアンス設定

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	変更されたアクティブ S-TAP	使用不可
ランタイム・パラメーター	演算子	デフォルト値
別名の表示		ラジオ・ボタン (オン、オフ、デフォルト)
リモート・データ・ソース		ドロップダウン・メニュー

アプリケーション・オブジェクト・サマリー

このレポートは、Guardium アプリケーションのすべての定義のサマリーです。 例えば、「アプリケーション・オブジェクト」の「ランタイム・パラメーター」ページの「ObjectNameLike」欄に Oracle と入力すると、Oracle が使われているオブジェクト・タイプとオブジェクトの記述がすべて検出されます。

注: このレポートでは、 メタデータが提示されるため、データ・レベル・セキュリティー・メカニズムではフィルタリングされません。 このメタデータには、Oracle SID などのデータベース関連情報が含まれていることがあります。

表 7. アプリケーション・オブジェクト・サマリー

ドメイン	ベースとなる照会	メイン・エンティティー
アプリケーション・オブジェクト	アプリケーション・オブジェクト・サマリー	アプリケーション・オブジェクト
ランタイム・パラメーター	演算子	デフォルト値
ObjectNameLike	%	%
ObjectTypeNameLike	%	%

承認された TAP クライアント

特定の S-TAP のみ、Guardium アプリケーションへの接続が許可されます。このレポートは、承認されている S-TAP およびその状況を示します。

表 8. 承認された TAP クライアント

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	承認された TAP クライアント	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

監査プロセス・ログ

監査プロセス・ログ

このレポートには、すべてのタスクに関する詳細なアクティビティー・ログが、開始時刻および終了時刻も含めて示されます。 このレポートは、admin ユーザーが「Guardium モニター」タブを通じて入手可能です。監査タスクには、開始および終了時刻が示されますが、セキュリティー・アセスメントおよび分類 (キューに入れられます) の開始および終了は同じになります。

監査プロセスは、その監査プロセス全体でサインオフするユーザーだけでなく、特定行のサインオフにまで拡張されています。 サインオフされたものと、特定行の状況がリスト表示されます。

監査プロセスを停止するには、この「監査プロセス・ログ」を使用してください。タスクを停止できるのは、 そのタスクが実行されていない場合、または実行中の場合に限られます。 まだ開始されていないタスクは実行されません。 部分的な結果は送信されません。 タスクが完了している場合は、監査プロセスを停止しても、結果の送信は停止されません。 監査プロセスの停止は、「監査プロセス・ログ」レポートから、 GrdAPI コマンド invoke api によって実行されます。ユーザーには、 そのユーザーに属する行だけ (ただし、すべての詳細ではなくタスクのみ) が表示されます。 管理者ユーザーは全詳細を確認でき、任意のユーザーの実行を停止できます。 ユーザーは、自分の実行しか停止できません。

注:

監査プロセスを停止しても、リモート・ソースを使用して実行している照会は取り消されません。 リモート・ソースを使用するオンライン・レポートも同様に取り消されません。

プライバシー・セットと外部フィードに対してはサポートされません。つまり、 プライバシー・セット・タスクが開始されていたり、外付けフィードが開始されていたりした場合、 プロセスが停止してもそれは完了します (一方照会は強制終了されます)。

監査プロセス・ログ ID

ログイン名

実行 ID

タイム・スタンプ

監査プロセス ID

監査プロセスの記述

監査タスク ID

監査タスクの記述

イベント・タイプ

詳細

監査プロセス・ログの数

使用可能なパッチ

使用可能なパッチのリストを表示します。ランタイム・パラメーターはありません。 このレポート・ドメインはシステム専用です。

バッファー使用状況モニター

バッファー使用状況の統計の詳細を表示します。このレポートにリストされるフィールドについては、「スニファーのバッファー使用」エンティティーの説明を参照してください。

表 9. バッファー使用状況モニター

ドメイン	ベースとなる照会	メイン・エンティティー
バッファー使用状況	バッファー使用状況モニター	スニファーのバッファー使用のモニター
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

CAS デプロイメント

この CAS レポートでは、データベース・タイプ、OS 名、 ホスト名、および OS タイプが詳しく記述されています。

表 10. CAS デプロイメント

ドメイン	ベースとなる照会	メイン・エンティティー
CAS	CAS デプロイメント	N/A
ランタイム・パラメーター	演算子	デフォルト値
データベース・タイプ	Like	%
OS_Name	Like	%
ホスト名	Like	%
OS_Type	Like	%

変更 (CAS)

CAS 変更詳細

モニター対象の項目ごとに、所有者別に変更がリストされます。

表 11. CAS 変更詳細

ドメイン	ベースとなる照会	メイン・エンティティー
CAS 変更	CAS 変更詳細	ホスト構成
ランタイム・パラメーター	演算子	デフォルト値
DB_Type	Like	%
Host_Name	Like	%
Instance_Name	Like	%
Monitored_Item	Like	%
OS_Type	Like	%
タイプ	Like	%

CAS 保存データ

このレポートでは、検出された変更ごとに、保存されたデータがリストされます。このレポートは、ホスト名ごとにソートされ、次に最終変更時刻ごとにソートされます。

表 12. CAS 保存データ

ドメイン	ベースとなる照会	メイン・エンティティー
CAS 変更	CAS 保存データ	保存データ
ランタイム・パラメーター	演算子	デフォルト値
Host_Name	Like	%
Monitored_Item	Like	%
Saved_Data_Id	Like	%

構成 (CAS)

CAS インスタンス

このレポートは、CAS インスタンス定義 (CAS インスタンスは、特定の CAS ホストにテンプレート・セットを適用します) をリストします。 このレポートのデフォルトのソート順は、標準のソート順とは異なります。ソート・キーは、優先順位の高いものから順に、ホスト名 (昇順)、インスタンス (昇順)、最後の状況変更 (降順) です。

表 13. CAS インスタンス

ドメイン	ベースとなる照会	メイン・エンティティー
CAS 構成	CAS インスタンス	モニター項目詳細
ランタイム・パラメーター	演算子	デフォルト値
Host_Name	Like	%
OS_Type	Like	%
DB_Type	Like	%
インスタンス	Like	%

CAS インスタンス構成

このレポートは、CAS インスタンスの構成変更をリストします。このレポートのデフォルトのソート順は、標準のソート順とは異なります。ソート・キーは、優先順位の高いものから順に、ホスト名 (昇順)、インスタンス (昇順)、最後の状況変更 (降順) です。以下のランタイム・パラメーターを使用することで、出力を制限できます。これらのパラメーターは、デフォルトではすべての値を選択します。

表 14. CAS インスタンス構成

ドメイン	ベースとなる照会	メイン・エンティティー
CAS 構成	CAS インスタンス構成	モニター項目詳細
ランタイム・パラメーター	演算子	デフォルト値
Host_Name	Like	%
OS_Type	Like	%
Template_Id	Like	%

接続プロファイル・リスト

接続プロファイル・リストは、すべての許可された接続のグループです (接続プロファイル・リストは、すべての接続の詳細を示しています)。

表 15. 接続プロファイル・リスト

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	接続プロファイル・リスト	クライアント・サーバー
ランタイム・パラメーター	演算子	デフォルト値
照会の開始日付	>=	NOW -1 DAY
照会の終了日付	<=	NOW

隔離された接続

Guardium ポリシーを使用して接続の終了や隔離をリアルタイムで行うことができます。 照会をベースにしたしきい値アラートを使用します。構成の手順については、 トピック『ポリシー』の『隔離』を参照してください。

表 16. 隔離された接続

ドメイン	ベースとなる照会	メイン・エンティティー
接続隔離	隔離された接続	接続隔離
ランタイム・パラメーター	演算子	デフォルト値
サーバー IP	LIKE	%
データベース・ユーザー	LIKE	%
サーバー名	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

CPU トラッカー

S-TAP ホストと、S-TAP を実行しているマシンの CPU の数をリストします。

表 17. CPU トラッカー

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	使用不可	使用不可
ランタイム・パラメーター	演算子	デフォルト値
なし	n/a	n/a

CPU 使用量

デフォルトでは、最近 2 時間の CPU 使用量を表示します。このグラフィカル・レポートは、 最近のアクティビティーのみを表示するためのものです。「開始」および「終了」のランタイム・パラメーターを変更して対象となる時間フレームを大きくすると、データが大きすぎるというメッセージが表示される場合があります。 より大きな時間枠を表示する場合は、表形式のレポートを使用してください。

表 18. CPU 使用量

ドメイン	ベースとなる照会	メイン・エンティティー
スニファーのバッファー	CPU 使用量	スニファーのバッファー使用のモニター
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -2 HOUR
期間終了	<=	NOW

タイプ別データベース/タイプ別データベース数

モニター対象の各データベース・タイプのサーバー・タイプとクライアント・ソース。

表 19. タイプ別データベース

ドメイン	ベースとなる照会	メイン・エンティティー
アクセス	タイプ別データベース数	クライアント/サーバー
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

ディスカバーされたデータベース

このレポートは、レポート期間について、「データベース・タイプ」属性値が不明でない「ディスカバーされたポート」エンティティーごとに、プローブ・タイム・スタンプ、サーバー IP、サーバーのホスト名、データベース・タイプ、ポート、ポート・タイプ、およびその行の「ディスカバーされたポート」数をリストします。

表 20. ディスカバーされたデータベース

ドメイン	ベースとなる照会	メイン・エンティティー
オートディスカバリー	ディスカバーされたデータベース	ディスカバーされたポート
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW
PortNotLike	NOT LIKE	デフォルト値なし。

DB ユーザー・マッピング・リスト

データベース・ユーザー (違反の原因となった SQL の起動者) とリアルタイム・アラート用 E メール・アドレス間のマッピング。

表 21. DB ユーザー・マッピング・リスト

ドメイン	ベースとなる照会	メイン・エンティティー
オートディスカバリー	データベース・ユーザー・マッピング・リスト	Guardium ユーザー・ログイン
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

有効になっているデフォルト・データベース・ユーザー

このレポートでは、非資格情報スキャン API に提供されたデフォルト・ユーザーのグループとサーバー・リストに対するデータベース・スキャンの後に、有効であることが検出されたデフォルト・ユーザーの詳細を示します。 有効なユーザーがデータベース内で検出されたとき、このデータベース/ユーザーに関する検索結果は 1 回のみ報告されます。 以降のスキャンでは、データベースのタイム・スタンプおよびデータベース・バージョンが更新されます。 以降のスキャンで以前検出されていたユーザーが検出されなくなった場合、タイム・スタンプはそのまま残ります。これによって、そのユーザーがデータベース上で有効であると最後に検出された時の履歴が保持されます。 スキャンは分類リスナーの下で実行され、実行依頼されるジョブ (non_credential_scan API を使用) は、「Guardium ジョブ・キュー」レポートを使用してトラッキングできます。

表 22. 有効になっているデフォルト・データベース・ユーザー

ドメイン	ベースとなる照会	メイン・エンティティー
有効になっているデフォルト・データベース・ユーザー	有効になっているデフォルト・データベース・ユーザー	有効になっているデフォルト・データベース・ユーザー
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY

ドメイン	ベースとなる照会	メイン・エンティティー
期間終了	<=	NOW

データ・ソース

定義されているすべてのデータ・ソースをリストします。データ・ソース・タイプ、データ・ソース名、 データ・ソースの記述、ホスト、ポート、サービス名、ユーザー名、データベース名、 最後の接続、共有、接続プロパティー。

このレポートの出力は、「データ・ソース名」ランタイム・パラメーターで制限できます。 このパラメーターは、デフォルトではすべてのデータ・ソースを選択する「%」に設定されています。

表 23. データ・ソース

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	データ・ソース	使用不可
ランタイム・パラメーター	演算子	デフォルト値
データ・ソース名	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

ディスカバーされたインスタンス

この S-TAP レポートには、以下の情報の詳細が記載されています。

タイム・スタンプ、ホスト、プロトコル、ポート (最小)、ポート (最大)、KTAP データベース・ポート、 インスタンス名、クライアント、除外するクライアント、プロセス名、名前付きパイプ、 データベース・インスタンス・ディレクトリー、DB2® 共有メモリー調整、DB2 共有メモリー・クライアント位置、 DB2 共有メモリー・サイズ。

表 24. ディスカバーされたインスタンス

ドメイン	ベースとなる照会	メイン・エンティティー
例外	ディスカバーされたインスタンス	例外
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

データマート抽出ログ

データマートはデータウェアハウスのサブセットです。データウェアハウスでは、後から分析およびレポートで使用可能なように、データが汎用的な方式で集約および編成されます。データマートはユーザー定義のデータ分析を始めとして、内容、表示、使いやすさの面で、ユーザーの特定の要求に対応していることが特徴です。

データマート抽出プログラムは、指定されたスケジュールに応じてバッチで実行されます。 データは要求された間隔に応じて時間、日、週、月ごとに要約され、要約の結果は Guardium 分析データベース内の新しい表に保存されます。

ユーザーは、標準的なレポートと監査プロセスを使用してこのデータにアクセスできるようになります。データマート抽出データは、DM ドメインで使用可能です。エンティティー名は、データマート・データに対して指定された新しい表の名前に従って設定されます。ユーザーは、標準のクエリー・ビルダーおよびレポート・ビルダーを使用して、デフォルトの照会を複製し、照会およびレポートを編集し、ポートレットを生成してペインに追加することができます。

抽出ログは、データマート名、コレクター IP、サーバー IP、開始時刻、終了時刻、ID、開始された実行、終了した実行、レコードの数、状況、エラー・コードから構成されます。

定義のエクスポート/インポート・ログ

このレポートでは、Guardium のエクスポート/インポート・アクティビティーがアクティビティー・タイプ別にリストされます。 レポートの各行には、アクティビティー・タイプ、開始時刻、ファイル名、状況、 コメント、およびその行のログ・レコードの数が含まれています。

表 25. 定義のエクスポート/インポート・ログ

ドメイン	ベースとなる照会	メイン・エンティティー
統合/アーカイブ	エクスポート/インポート定義ログ	統合/アーカイブ・ログ
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

ドロップされたリクエスト

検査エンジンによってドロップされたリクエストをトラッキングします (例外の記述 = ドロップされたデータベース要求)。極めてまれですが、大量の要求がある状況で、一部の要求が失われることがあります。 その場合、「ドロップされたリクエスト」レポートに、失われた要求があるセッションがリストされます。

表 26. ドロップされたリクエスト

ドメイン	ベースとなる照会	メイン・エンティティー
例外	ドロップされたリクエスト	例外
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

例外数

レポート期間中にログに記録された例外の総数。

表 27. 例外数

ドメイン	ベースとなる照会	メイン・エンティティー
例外	例外数	例外
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

エンタープライズ S-TAP (詳細) ビュー

このレポートについては、『S-TAP 情報 (中央マネージャー)』を参照してください。

エンタープライズ S-TAP 関連履歴

エンタープライズ S-TAP 関連履歴は、ロード・バランサー環境で特定の Guardium システムに S-TAP が報告を行った期間について報告します。

エンタープライズ S-TAP ビュー

このレポートについては、『S-TAP 情報 (中央マネージャー)』を参照してください。

Discovery への機密データのエクスポート

Guardium と InfoSphere® Discovery には、機密データを分類するためのメカニズムがあります。

識別された機密データを Guardium から InfoSphere Discovery へ、および InfoSphere Discovery から Guardium へと転送するための双方向インターフェースが提供されています。

このデータは CSV ファイルを介して転送されます。詳細については、『 外部データ相関』(双方向インターフェース) を参照してください。

表 28. Discovery への機密データのエクスポート

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	Discovery への機密データのエクスポート	分類プロセスの結果
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -3 HOURS
期間終了	<=	NOW
ルールの記述	LIKE	
スキーマ	LIKE	

エンタープライズ・バッファー使用状況モニター

このレポートには、すべての管理対象ユニットからのスニファーのバッファー使用の統合が表示されます。 アップロードのスケジュールを設定する必要があります。このレポートにリストされるフィールドについては、「スニファーのバッファー使用」エンティティーの説明を参照してください。

表 29. エンタープライズ・バッファー使用状況モニター

ドメイン	ベースとなる照会	メイン・エンティティー
エンタープライズ・バッファー使用状況	エンタープライズ・バッファー使用状況	スニファーのバッファー使用
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

Guardium ジョブ・キュー

Guardium ジョブ・キューを表示します。以前は分類/アセスメントのジョブ・キューと呼ばれていました。ジョブごとに、 プロセス実行 ID、プロセス・タイプ、状況、Guardium ジョブのプロセス ID、レポート結果 ID、 Guardium ジョブの記述、監査タスクの記述、キュー時刻、開始時刻、終了時刻、 およびデータ・ソースがリストされます。

表 30. Guardium ジョブ・キュー

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	Guardium ジョブ・キュー	使用不可
ランタイム・パラメーター	演算子	デフォルト値
ジョブの記述	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

ジョブ・キュー

評価と分類は、それぞれジョブ・キューと呼ばれる個別のプロセスで実行されます。ジョブはキューに入れられ、実行を待機中のジョブを検索するためにリスナーがキューを定期的にポーリングしている間、 その状況を維持します。

停止

実行中のジョブを右クリックしてドリルダウン・メニューを表示すると、 実行中のジョブを停止し、取り消すオプションがあります。この時点ではジョブを再開することはできません。

一時停止

実行中のジョブは、ジョブ・キューが過負荷に陥る原因になるハングしたジョブの数を少なくするために、 モニターされています。30 分間非アクティブの状態が続いているジョブがあれば、リスナーの強制終了と再始動が行われ、 ジョブの操作が事実上停止されます。リスナーが再始動する前にはクリーナーと呼ばれるプロセスが実行され、 状況が RUNNING から HALTED に設定され、その後にリスナーが再始動されます。HALTED は、ジョブの実行が完了できなかったことを示します。

再実行依頼

ときには、リスナーがジョブのハング以外の理由 (例えばマシンのリブート) で再始動されることがあります。クリーナーは、実行中のジョブを一時停止する場合、そのジョブが過去 8 分以内に応答したかどうかを確認します。応答していれば、そのジョブはコピーされ、そのコピーがジョブ・キューに再実行依頼されます。一時停止した元のジョブは引き続きキューに表示され、 そのジョブが処理できた結果も入手可能です。

モニター

ジョブがアクティブ状況を維持するメカニズムは、ジョブ・キュー・レコードのタイム・スタンプにタッチすることによります。ジョブ・キュー・レコードはジョブ全体で使用されていることにご注意ください。個々の分類ルール、あるいは評価テストは、その親プロセスのタイム・スタンプと対話します。 モニターの対象になる個別のタイム・スタンプは持っていません。

分類では、すべてのルールがテストされる前、すべての SQL 操作の後にタイム・スタンプが更新されます。例えば、分類がページングをサポートするデータベース内のデータをスキャンする場合は、 データの各バッチがデータベースから戻された後にタイム・スタンプにタッチします。これは、ターゲット・データベースの状態によっては、分類が、複数の長時間実行する照会 (実行時間は 30 分に制限されます) を呼び出す可能性があるためです。

評価は、評価内の各テストが評価された後にタイム・スタンプにタッチします。ほとんどの評価テストは数秒以内に実行されます。

監視対象テスト

アセスメント・テストは比較的短時間で実行できますが、監視対象のアセスメント・テストは例外です。これらのテストは、Guardium アプライアンスで内部スニッフィング・データを使用する照会やレポートをベースにしていて、 比較的長時間実行できますが、処理中はタイム・スタンプを更新できません。 そのため、監視対象の評価テストでは、開始時にタイム・スタンプが 2 時間先に設定され、 実行が終了するまでに、基本的に 2 時間半が与えられます。このことにより、ユーザーがジョブ・キューを調べたときに、タイム・スタンプが未来の時刻に設定されているのを見て、混乱する場合があります。他の評価テストと同様、監視対象テストも終了時にタイム・スタンプにタッチします。次回のテストが監視対象のテストである場合、タイム・スタンプが再び 2 時間先の時刻に設定されます。次回のテストが監視対象のテストではない場合、タイム・スタンプは現在の時刻に設定されます。

GIM クライアント状況

GIM クライアントのリストを表示します。

表 31. GIM クライアント状況

ドメイン	ベースとなる照会	メイン・エンティティー
GIM クライアント状況	GIM クライアント状況	GIM クライアント
ランタイム・パラメーター	演算子	デフォルト値
クライアント名	%	N/A
クライアント OS	%	N/A

GIM イベント・リスト

GIM イベントのリストを表示します。

表 32. GIM イベント・リスト

ドメイン	ベースとなる照会	メイン・エンティティー
GIM イベント	GIM イベント	GIM イベント

ドメイン	ベースとなる照会	メイン・エンティティー
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

GIM インストール済みモジュール

インストール済み GIM モジュールのリストを表示します。
注: このレポートには、ホストに関連付けられているモジュールが表示されます。モジュールがホストに割り当て済みの場合、そのモジュールがスケジュールまたはインストールされていない場合でも、このレポートには割り当て済みのバージョンが表示されます。現在インストールされているモジュールを確認するには、GIM クライアント状況レポートを確認してください。

表 33. GIM インストール済みモジュール

ドメイン	ベースとなる照会	メイン・エンティティー
GIM インストール済みベース	GIM インストール済みベース	GIM インストール済み
ランタイム・パラメーター	演算子	デフォルト値
なし	適用外	適用外

グループ使用状況レポート

定義済みグループと、各グループに依存するエンティティーをすべてリスト表示します。

Guardium API 例外

すべての GuardAPI 例外のタイム・スタンプと説明を表示します。これらは、 例外タイプ ID が GUARD_API_EXCEPTION のジョブです。

表 34. Guardium API 例外

ドメイン	ベースとなる照会	メイン・エンティティー
例外	Guardium API 例外	例外
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

Guardium アプリケーション

Guardium アプリケーションごとに、各行には、割り当てられたセキュリティー・ロール、 または all というワード (すべてのロールが割り当てられていることを示す) がリストされます。

表 35. Guardium アプリケーション

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	すべての Guardium アプリケーション	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -100 Month DAY
期間終了	<=	NOW

Guardium グループの詳細

レポート期間について、このレポートの各行にはグループ・メンバーがリストされます。 列には以下の情報が入ります。グループの記述、グループ・タイプ、 グループ・サブタイプ、タイム・スタンプ (「グループ・メンバー」エンティティーから)、グループ・メンバー、 およびその行の「グループ・メンバー」エンティティーの数。タイム・スタンプの値は、 レコードの更新時に常に現在時刻に設定されます。

このレポートの出力は、ランタイム・パラメーターで制限できます。パラメーターはいずれも LIKE 演算子を指定して使用され、デフォルト値は % (すべての値を選択) です。

表 36. Guardium グループの詳細

ドメイン	ベースとなる照会	メイン・エンティティー
グループ	Guardium グループの詳細	グループ・メンバー
ランタイム・パラメーター	演算子	デフォルト値
グループの記述	LIKE	%
グループ・タイプ	LIKE	%
期間開始	>=	NOW -100 MONTH
期間終了	<=	NOW

Guardium ユーザー

各ユーザー、最終アクティビティーの日付、割り当てられているロールの数をリストします。 ユーザーごとに、「レコード詳細」レポートまでドリルダウンすると、そのユーザーに割り当てられているロールを確認できます。

表 37. Guardium ユーザー

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	ユーザー・ロール	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -100 MONTH
期間終了	<=	NOW

ホスト履歴 (CAS)

CAS ホスト履歴

このレポートは、CAS ホスト・イベントをリストします。このレポートのデフォルトのソート順は、標準のソート順とは異なります。ソート・キーは、優先順位の高いものから順に、ホスト名 (昇順)、インスタンス、イベント時間 (降順) です。

表 38. CAS ホスト履歴

ドメイン	ベースとなる照会	メイン・エンティティー
CAS ホスト履歴	CAS ホスト履歴	ホスト・イベント
ランタイム・パラメーター	演算子	デフォルト値
Host_Name	Like	%
OS_Type	Like	%
Event_Type	Like	%

非アクティブな検査エンジン

非アクティブな検査エンジンすべてをリストします。

表 39. 非アクティブな検査エンジン

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	非アクティブな検査エンジン	S-TAP 検査ヘッダー
ランタイム・パラメーター	演算子	デフォルト値
照会の開始日付	>=	NOW -3 HOUR
照会の終了日付	>=	NOW

非アクティブな S-TAP

システムで定義されている非アクティブな S-TAP をすべてリストします。これには 1 つだけ、「期間開始」というランタイム・パラメーターがあり、デフォルトでは now -1 hour に設定されています。このパラメーターを使用して、非アクティブをどのように定義するのかを制御します。このレポートには、「S-TAP 状況」レポートと同じデータの列が含まれており、レポートの各行のカウントが追加されています。

表 40. 非アクティブな S-TAP

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	非アクティブな S-TAP	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 HOUR

インストール済みのパッチ

インストール済みパッチのリストを表示します。ランタイム・パラメーターはありません。 このレポート・ドメインはシステム専用です。

表 41. インストール済みのパッチ

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	インストール済みのパッチ	使用不可
ランタイム・パラメーター	演算子	デフォルト値
なし	適用外	適用外

Guardium へのログイン

このレポートの値はすべて、「Guardium ログイン」エンティティーから取得されます。 レポート期間中、このレポートの各行には、ユーザー名、ログイン成功 (1 は成功、0 は失敗)、 ログインの日時、ログアウトの日時 (ユーザーがまだログアウトしていない場合はブランク)、 ホスト名、(ユーザーの) リモート・アドレス、およびその行のログイン数がリストされます。

表 42. Guardium へのログイン

ドメイン	ベースとなる照会	メイン・エンティティー
Guardium ログイン	Guardium ログイン	Guardium ユーザー・ログイン
ランタイム・パラメーター	演算子	デフォルト値
ホスト名	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

ログに記録される R/T アラート

レポート期間中にログに記録されたリアルタイム・アラートの総数。ルールの記述ごとにリストされます。

表 43. ログに記録される R/T アラート

ドメイン	ベースとなる照会	メイン・エンティティー
ポリシー違反	ログに記録される R/T アラート	ポリシー・ルール違反
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

ログに記録されるしきい値アラート

レポート期間中にログに記録されたしきい値アラートの総数。

表 44. ログに記録されるしきい値アラート

ドメイン	ベースとなる照会	メイン・エンティティー
アラート	ログに記録されたアラート	しきい値アラート詳細
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

コレクター・ロギング (統合ユニットからの場合のみ有効)

「ロギング・コレクター」レポートは「日次モニター」タブの下に表示され、統合ユニットでのみ有効です。このレポートでは、サーバー IP ごと、コレクターごと、 1 日ごとに、セッション数が表示されます。 例: 5 月 19 日に、アグリゲーター #1 がサーバー 192.168.x.x1 で 100 セッション、 サーバー 192.168.x.x2 で 50 セッションを収集しました。アグリゲーター #2 がサーバー 192.168.x.x3 で 30 セッション、 サーバー 192.168.x.x4 で 90 セッションを収集しました、など。

表 45. ロギング・コレクター

ドメイン	ベースとなる照会	メイン・エンティティー
例外	ロギング・コレクター	ロギング・コレクター
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

管理対象ユニット (中央マネージャー)

準備完了している管理対象ユニットを示す、中央マネージャーに関するエンタープライズ・レポート。統計アラートでこのレポートを使用して、管理対象ユニットがダウンした場合に管理者に E メールを送信します。

表 46. 管理対象ユニット (中央マネージャー)

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	管理対象ユニット	管理対象ユニット
ランタイム・パラメーター	演算子	デフォルト値
ホスト名	LIKE	%
リモート・データ・ソース		ドロップダウン・メニュー
別名の表示		ラジオ・ボタン (オン、オフ、デフォルト)

アクティブな監査プロセスの数

アクティブな Guardium 監査プロセスの数。一元管理が実施されている場合、 このレポートは、中央マネージャー上でのみデータが入り、すべての管理対象ユニットでは空になります (「要求された照会のデータが見つかりません」という標準メッセージが表示されます)。 このレポートにはランタイム・パラメーターはありません。

表 47. アクティブな監査プロセスの数

ドメイン	ベースとなる照会	メイン・エンティティー
監査プロセス	アクティブ・プロセス数	監査プロセス
ランタイム・パラメーター	演算子	デフォルト値
なし	適用外	適用外

未処理監査プロセスのレビュー

未処理の Guardium 監査プロセスの数 (Guardium ユーザー別にリスト表示)。

表 48. 未処理監査プロセスのレビュー

ドメイン	ベースとなる照会	メイン・エンティティー
監査プロセス	未処理監査プロセスのレビュー	タスク結果 To-Do リスト
ランタイム・パラメーター	演算子	デフォルト値
なし	適用外	適用外

プライマリー Guardium ホスト変更ログ

S-TAP のプライマリー・ホスト変更のログ。1 次ホストとは、 S-TAP がデータを送信する Guardium ユニットです。このレポートの各行には、 S-TAP ホスト、Guardium ホスト名、期間の開始、期間の終了がリストされます。

表 49. プライマリー Guardium ホスト変更ログ

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	プライマリー SGuard ホスト変更ログ	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

照会エンティティーと属性

このレポートでは、Guardium レポート内のすべてのエンティティーと属性がリストされます。 このレポートは、Guardium 属性間のリンケージを単純化して GuardAPI 呼び出しにするために作成されました。

このレポートは、create_constant_attribute、create_api_parameter_mapping、delete_api_parameter_mapping、または list_param_mapping_for_function を呼び出す場合にも使用します。

表 50. 照会エンティティーと属性

ドメイン	ベースとなる照会	メイン・エンティティー
任意の Guardium レポート・ドメイン	レポート・ドメインの任意のエンティティー	エンティティー内の任意の属性
ランタイム・パラメーター	演算子	デフォルト値
レポート名 LIKE <> '%' の場合は、新規パラメーターと一致するレポートで使用されるドメイン/エンティティーと属性だけが表示されます。 '%' の場合は、すべてのドメイン、照会、および属性が表示されます (どのレポートにも使用されないものも含めて)。	適用外	適用外

リプレイ統計

このレポートは、実行の開始日/実行の終了日のリプレイ統計、構成名、スケジュール・セットアップ名、ジョブ状況、統計記述、セッション ID、正常な照会、失敗した照会、合計照会、タイプ、アクティブ/待機中/完了済みの各タスクを示します。

表 51. リプレイ統計

ドメイン	ベースとなる照会	メイン・エンティティー
リプレイ結果のトラッキング	リプレイ統計	リプレイ結果統計
ランタイム・パラメーター	演算子	デフォルト値
照会の開始日付	>=	NOW -1 DAY
照会の終了日付	<=	NOW

ドメイン	ベースとなる照会	メイン・エンティティー
セッション	>=	N/A
セッション	<=	N/A

リプレイ・サマリー

レポート期間内に、どの照会が失敗または成功したかに関する測定です。「リプレイ構成」で「失敗した照会」または「成功した照会」にチェック・マークを付けておくことが必要です。

表 52. リプレイ・サマリー

ドメイン	ベースとなる照会	メイン・エンティティー
リプレイ結果	リプレイ・サマリー	リプレイ結果
ランタイム・パラメーター	演算子	デフォルト値
照会の開始日付	>=	NOW -1 DAY
照会の終了日付	<=	NOW
結果状況	%	N/A
スケジュール・セットアップ名	%	N/A

リストアされたデータ

このレポートには 2 つの列 (RESTORED_DAY と EXPIRATION_DATE) があります。 ユーザーがアーカイブからデータをリストアすると、リストアされたデータと、このデータを保持するために指定した期間に従って、この表にデータが追加されます。 パージ・プロセスはこの表を調べてパージできるデータを判別し、有効期限が切れたレコードをクリーンアップします。 RESTORED_DAY は、リストアされたデータの日付なので、過去の日付です。EXPIRATION_DATE は、このデータがパージされる日付であり、未来の日付です。

表 53. リストアされたデータ

ドメイン	ベースとなる照会	メイン・エンティティー
リストアされたデータ	リストアされたデータ	リストアされたデータ
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -10 DAY
期間終了	<=	NOW +10 DAY

リクエスト・レート

デフォルトでは、最近 2 時間のリクエスト・レートを表示します。このグラフィカル・レポートは、 最近のアクティビティーのみを表示するためのものです。ランタイム・パラメーターを変更して対象となる時間フレームを大きくすると、データが大きすぎるというメッセージが表示される場合があります。 より大きな時間枠を表示する場合は、表形式のレポートを使用してください。

表 54. リクエスト・レート

ドメイン	ベースとなる照会	メイン・エンティティー
スニファーのバッファー	リクエスト・レート	スニファーのバッファー使用のモニター
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -2 HOUR
期間終了	<=	NOW

不正な接続

このレポートは、UNIX サーバーでハンター・オプションが有効になっている場合にのみ使用できます。 ハンター・オプションが使用されるのは、TEE モニター方式が使用されている場合に限られます。 このレポートは、データベースに接続するために、 S-TAP を回避したすべてのローカル・プロセスをリストします。

表 55. 不正な接続

ドメイン	ベースとなる照会	メイン・エンティティー
不正な接続	不正な接続	不正な接続
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

スケジュールされたジョブの例外

スケジュールされたジョブ例外 (評価エラーなど) ごとに、そのタイム・スタンプと説明を表示します。これらは、 例外タイプ ID が SCHED_JOB_EXCEPTION、ASSESSMENT_EXCEPTION、ASMT_ERROR のいずれかであるジョブです。

表 56. スケジュールされたジョブの例外

ドメイン	ベースとなる照会	メイン・エンティティー
スニファーのバッファー	CPU 使用量	スニファーのバッファー使用
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -2 HOUR
期間終了	<=	NOW

スケジュールされたジョブ

現在スケジュールされているジョブのリストを表示します。

表 57. スケジュールされたジョブ

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	スケジュールされたジョブ	使用不可
ランタイム・パラメーター	演算子	デフォルト値
なし	適用外	適用外

セッション数

レポート期間中に開いた各種セッションの総数。

表 58. セッション数

ドメイン	ベースとなる照会	メイン・エンティティー
アクセス	セッション数	セッション
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

SQL 数

レポート期間中に発行されたSQL コマンドの種類の総数。

表 59. SQL 数

ドメイン	ベースとなる照会	メイン・エンティティー
アクセス	SQL 数	SQL
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

S-TAP 構成変更履歴

このレポートは、検査エンジンが追加または変更されたときだけ表示されます。 ここには S-TAP 構成変更がリストされます。個々の検査エンジンの変更は、別々の行に表示されます。 各行には、S-TAP ホスト、データベース・サーバー・タイプ、データベース・ポート (始まり)、 データベース・ポート (終わり)、データベース・クライアント IP、データベース・クライアント・マスク、 および変更のタイム・スタンプがリストされます。

表 60. S-TAP 構成変更履歴

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	構成変更履歴	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

S-TAP 状況

各 S-TAP ホストで定義されている各検査エンジンについて、状況情報を 表示します。このレポートは現在の状況をレポートするため、開始日と終了日の パラメーターはありません。このレポートの各行は、S-TAP ホスト、データベース・サーバー・タイプ、状況、最後の応答、1 次ホスト名、および属性 (KTAP (インストール済み)、TEE (インストール済み)、共有メモリー・ドライバー (インストール済み)、Db2 共有メモリー・ドライバー (インストール済み)、名前付きパイプ・ドライバー (インストール済み)、およびアプリケーション・サーバー・インストール済み) の Yes/No インディケーターをリストします。さらに、ハンター DBS をリストします。

注: Db2 共有メモリー・ドライバーは Db2 Tap フィーチャーに置き換えられました。

表 61. S-TAP 状況

ドメイン	ベースとなる照会	メイン・エンティティー

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	S-TAP 状況	使用不可
ランタイム・パラメーター	演算子	デフォルト値
なし	n/a	n/a

S-TAP 検査

S-TAP 検査のすべての結果をリストします。

表 62. S-TAP 検査

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	S-TAP 検査	S-TAP 検査ヘッダー
ランタイム・パラメーター	演算子	デフォルト値
照会の開始日付	>=	NOW -3 HOUR
照会の終了日付	>=	NOW

S-TAP イベント

S-TAP に関する情報には、このレポートを使用します (内部データベースの SOFTWARE_TAP_EVENT 表から)。

表 63. S-TAP イベント

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	S-TAP イベント	使用不可
ランタイム・パラメーター	演算子	デフォルト値
イベント・タイプ	LIKE	%
ホスト・タイプ	LIKE	%
期間開始	>=	NOW -3 DAY
期間終了	<=	NOW

S-TAP 情報 (中央マネージャー)

レポート:『S-TAP レポート』を参照。中央マネージャーでは、追加のレポート、「S-TAP 情報」が使用可能です。このレポートは、環境全体の S-TAP をモニターします。このデータのアップロードには、カスタム表ビルダーを使用します。

S-TAP 情報は、「S-TAP 情報」エンティティーが含まれる事前定義カスタム・ドメインであり、ライセンス・ドメインと違って変更できません。

カスタム照会を定義する際は、アップロード・ページに移動して「検査/修復」をクリックし、CUSTOM データベースにカスタム表を作成します。そうしないと、照会を保存するときに照会が検証されません。この表は、すべてのリモート・ソースから自動的にロードします。ユーザーは、使用するリモート・ソースを選択できません。すべてのリモート・ソースから取り込まれます。

このカスタム表とカスタム・ドメインに基づく、次の 2 つのレポートがあります。

エンタープライズ S-TAP ビューは、中央マネージャーから、コレクターまたは管理対象ユニット上のアクティブな S-TAP に関する情報を表示します (同じ S-TAP エンジンに対する重複があり、一方がアクティブで、他方が非アクティブの場合、アクティブな方のみがレポートに使用されます)。

詳細なエンタープライズ S-TAP ビューは、中央マネージャーから、すべてのコレクターまたは管理対象ユニット上のすべてのアクティブおよび非アクティブな S-TAP に関する情報を表示します。

エンタープライズ S-STAP ビューと詳細なエンタープライズ S-TAP ビューが同じに見える場合は、1 つの管理対象ユニット上にあるただ 1 つの S-TAP が表示されているためです。複数の S-TAP および複数の管理対象ユニットがある場合は、詳細なエンタープライズ S-TAP ビューの表示が違ったものになります。

これらの 2 つのレポートは、スタンドアロン・システムの「TAP モニター」タブから選択可能ですが、情報は表示されません。

アラート:『監査プロセス定義の表示』で、アラート「検査エンジンと S-TAP」(検査エンジンと S-TAP の構成に関連するすべてのアクティビティーについてアラートを出す) を参照してください。

S-TAP 最後の応答

事前定義の照会およびレポートを使用可能ですが、 パネルには追加されません。

照会/レポートには、すべての S-TAP ホストと、各 ホストから送信された最後の応答 (ハートビート) が表示されます。

この照会の目的は、 ホスト上の S-TAP が特定の期間応答しなかった場合にトリガーするアラートを定義できるようにすることです。

入力パラメーターは、「最後の応答の開始時刻」および 「最後の応答の終了時刻」です。

例えば、「最後の応答の開始時刻」に NOW -5 DAYS と指定し、「最後の応答の終了時刻」に NOW - 3 HOURS と指定して実行した場合、この 5 日間に最後の応答を送信したホストのうち、過去 3 時間以内に応答していないホストに関して、ホスト名および最後の応答時刻が表示されます。

S-TAP 状況モニター

このレポートは、この Guardium アプライアンスへの各 S-TAP レポートについて、 S-TAP ホスト、S-TAP バージョン、データベース・サーバー・タイプ、 状況 (アクティブまたは非アクティブ)、最後に受信した応答 (日時)、1 次ホスト名、 および (KTAP、TEE、MS SQL サーバー共有メモリー、DB2 共有メモリー、 ローカル TCP モニター、名前付きパイプの使用、および暗号化の) true/false インジケーターを識別します。

このレポートはランタイム・パラメーターを持たず、変更不能なシステム専用の照会をベースにしています。

STAP/Z ファイル

STAP/Z は、DB2 (z/OS® 上の) から収集した、DB2 イベント、SQL ステートメントなどを含む生データのファイルを提供します。 このレポートでは、インターフェース ID、UA ファイル名 (非正規化された監査イベント)、 UT ファイル名 (非正規化された監査イベントのテキスト)、UH ファイル名 (非正規化された監査イベントのホスト変数)、 ファイル状況、処理されたイベントの総数、失敗したイベントの数、タイム・スタンプがリストされます。 ランタイム・パラメーターは、FileName Like % と FileStatus Like % です。

このレポートでは、2 つのランタイム・パラメーター (FileName Like % と FileStatus Like %) が使用されます。 これは、変更不能なシステム専用の照会をベースにしています。

TCP 例外

レポート期間中、「例外タイプ」エンティティーの「例外の記述」が TCP/IP プロトコルの例外である例外ごとに、このレポートでは、「例外」エンティティーから以下の属性値が 1 行にリストされます。

表 64. TCP 例外

ドメイン	ベースとなる照会	メイン・エンティティー
例外	TCP 例外	例外
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

テンプレート (CAS)

CAS テンプレート

このレポートは、CAS テンプレートをリストします。デフォルトでは、すべてのテンプレート項目がリストされます。

表 65. CAS テンプレート

ドメイン	ベースとなる照会	メイン・エンティティー
CAS テンプレート	CAS テンプレート	テンプレート
ランタイム・パラメーター	演算子	デフォルト値
Access_Name	Like	%
Template_Set_Name	Like	%
Audit_Type	Like	%

テスト例外

一時的に免除されるテストとデータ・ソースのペアを示します。テスト例外の使用について詳しくは、『create_test_exception』を参照してください。

表 66. テスト例外

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	テスト例外	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -12 MONTH
期間終了	<=	NOW

スループット

レポート期間中の「アクセス期間」ごとに、各行に、期間の開始時刻、サーバー IP アドレス数、 アクセスの総数がリストされます (「アクセス期間」エンティティー)。

このレポートの出力は、「サーバー IP」ランタイム・パラメーターで制限できます。このパラメーターは、デフォルトではすべての IP アドレスを選択する % に設定されています。

表 67. スループット

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	データベース・サーバー・スループット	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY

ドメイン	ベースとなる照会	メイン・エンティティー
期間終了	<=	NOW
サーバー IP	LIKE	%

スループット (グラフィカル)

このレポートは、表形式スループット・レポートの図表バージョン「分散ラベル付き線グラフ」です。 期間の開始時刻ごとに 1 つのデータ・ポイントでレポート期間中のアクセス総数が作図されます。

このレポートの出力は、「サーバー IP」ランタイム・パラメーターで制限できます。このパラメーターは、デフォルトではすべての IP アドレスを選択する % に設定されています。

表 68. スループット (グラフィカル)

ドメイン	ベースとなる照会	メイン・エンティティー
アクセス	データベース・サーバー・スループット - グラフ	アクセス期間
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW
サーバー IP	LIKE	%

「ユーザー・アクティビティー監査証跡」レポート

「ユーザー・アクティビティー監査証跡」メニュー選択には 2 つのレポートが表示されます。 さらに、それぞれのレポートから第 3 のレポートが生成されることがあります。 以下を参照してください。

- ユーザー・アクティビティー監査証跡
- システム/セキュリティー・アクティビティー
- Guardium ユーザー・アクティビティーの詳細 (ドリルダウン)

ユーザー・アクティビティー監査証跡

レポート期間中、「Guardium ユーザー・アクティビティー監査」エンティティーに表示される個々のユーザー名で、 各行には Guardium ユーザー名、アクティビティー・タイプの記述 (「Guardium アクティビティー・タイプ」エンティティーから)、変更されたエンティティーの数の値、ホスト名、およびその行の「Guardium アクティビティー監査」エンティティーの総数が表示されます。

このレポートの任意の行から、「Guardium ユーザー・アクティビティーの詳細」レポートをドリルダウン・レポートとして選択できます。

表 69. ユーザー・アクティビティー監査証跡

ドメイン	ベースとなる照会	メイン・エンティティー
Guardium アクティビティー	ユーザー・アクティビティー監査証跡	Guardium ユーザー・アクティビティー監査
ランタイム・パラメーター	演算子	デフォルト値
ホスト名	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

システム/セキュリティー・アクティビティー

レポート期間中、「Guardium ユーザー・アクティビティー監査」エンティティーに表示される個々のユーザー名で、 各行には Guardium ユーザー名、アクティビティー・タイプの記述 (「Guardium アクティビティー・タイプ」エンティティーから)、変更されたエンティティーの数の値、ホスト名、およびその行の「Guardium アクティビティー監査」エンティティーの総数が表示されます。

このレポートの任意の行から、「Guardium ユーザー・アクティビティーの詳細」レポートをドリルダウン・レポートとして選択できます。

表 70. システム/セキュリティー・アクティビティー

ドメイン	ベースとなる照会	メイン・エンティティー
Guardium アクティビティー	ユーザー・アクティビティー監査証跡	Guardium ユーザー・アクティビティー監査
ランタイム・パラメーター	演算子	デフォルト値
ホスト名	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

Guardium ユーザー・アクティビティーの詳細 (ドリルダウン)

このレポートはメニューからは選択できませんが、「ユーザー・アクティビティー監査証跡」レポートの任意の行、または「システム/セキュリティー・アクティビティー」レポートから開くことができます。このレポートの選択した行 (「ユーザー名」と「アクティビティー・タイプの記述」をベースとしたもの) では、 このレポートで、ユーザー名、タイム・スタンプ、エンティティーの変更、オブジェクトの記述、 すべての値、およびその行の「Guardium ユーザー・アクティビティー監査」エンテ

ィティーの数といった属性値がリストされます。 属性値はすべて「Guardium ユーザー・アクティビティー監査」エンティティーから取得されますが、 「アクティビティー・タイプの記述」だけは例外で、「Guardium アクティビティー・タイプ」エンティティーから取得されます。

表 71. Guardium ユーザー・アクティビティーの詳細 (ドリルダウン)

ドメイン	ベースとなる照会	メイン・エンティティー
Guardium アクティビティー	Guardium ユーザー・アクティビティーの詳細	Guardium ユーザー・アクティビティー監査
ランタイム・パラメーター	演算子	デフォルト値
アクティビティー・タイプの記述		呼び出しレポートからの値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW
ユーザー名		呼び出しレポートからの値

警告: ユーザーは、 root ユーザーおよびその他の機密性の高いシステム・アカウントのアクティビティーがログに記録されていることを認識しておく必要があります。 これらのユーザーのアクティビティーまでドリルダウンすると、コマンド行で入力された機密のコマンドとパスワードが表示されることがあります。 したがって、ユーザーは、可能な限り、このドリルダウン・レポートに表示させたくない機密のコマンド行情報を入力しないようにしてください。

ユーザー To-do リスト

個々の Guardium 監査プロセスごとに、記述、ログイン名、必要なアクション (レビューまたは承認)、状況、 署名またはレビューしたユーザー、および指定したタスクの実行日を表示します。

表 72. ユーザー To-do リスト

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	ユーザー To-do リスト	使用不可
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

ユーザー・コメント - 共有可能

共有可能なユーザー・コメントは、検査エンジン、インストール済みポリシー、 監査プロセスの結果の各コメント以外のすべてのコメントです。 共有可能なユーザー・コメントごとに、このレポートでは、作成日、適用される項目のタイプ (例: アラート)、 コメントを作成したユーザー、およびコメントの内容がリストされます。

注: 検査エンジン、インストール済みポリシー、または監査プロセスの結果に定義されたコメントは、 個々の定義から表示できますが、レポート上には表示できません。

表 73. ユーザー・コメント - 共有可能

ドメイン	ベースとなる照会	メイン・エンティティー
コメント	定義されたコメント	コメント
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -2 MONTH
期間終了	<=	NOW

ユニット使用状況レベル

以下のデフォルト・レポートには、ユニット使用状況データが表示されます。

- ユニット使用状況: 特定の時間フレームにおける各ユニットのユニット使用状況の最大レベルが表示されます。レポートの時間フレーム内のすべての期間についてのユニットの詳細を表示するドリルダウンがあります。
- ユニット使用状況の分布: このレポートは、ユニットごとに、レポートの時間フレーム内の期間のパーセントを使用状況レベルの低、中、高で示します。
- 使用状況のしきい値: この事前定義レポートは、すべてのユニット使用状況パラメーターの下限しきい値と上限しきい値をすべて表示します。

- ユニット使用状況の日次サマリー - ユニット使用状況データの日次サマリーが表示されます。

表 74. ユニット使用状況レベル

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	ユニット使用状況の分布	ユニット使用状況レベル
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -24 HOUR
期間終了	<=	NOW

変更された値

レポート期間中、このレポートには、モニター値の変更に関する詳細情報が記録されます。 表示される属性値はすべて、「値のモニター」エンティティーから取得されます。 このレポートのベースとなる照会のソート・シーケンスは、次のように標準のソート・シーケンスとは異なっています。

- サーバー IP
- データベース・タイプ
- 監査タイム・スタンプ
- 監査表の名前
- 監査の所有者

このレポートのベースとなる照会には多数のランタイム・パラメーターがあります。 そのすべてが LIKE 演算子を使用し、デフォルト値は % (すべての値が選択されるという意味) です。

選択されたモニター値ごとに、このレポートでは、タイム・スタンプ、サーバー IP、 データベース・タイプ、サービス名、データベース名、監査ログイン名、監査タイム・スタンプ、 監査表の名前、監査の所有者、監査アクション、古い値の監査、新しい値の監査、 SQL テキスト、トリガーされる ID、およびその行の「列の変更」エンティティーの数が、1 行にリストされます。

表 75. 変更された値

ドメイン	ベースとなる照会	メイン・エンティティー
変更された値	変更された値	変更された列
ランタイム・パラメーター	演算子	デフォルト値
監査アクション	LIKE	%
監査ログイン名	LIKE	%
監査の所有者	LIKE	%
監査表の名前	LIKE	%
データベース・タイプ	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW
サーバー IP	LIKE	%

親トピック: 事前定義レポートを活用する方法

事前定義ユーザー・レポート

このセクションでは、デフォルト・ユーザー・レイアウトでのすべての事前定義レポートについて 簡単に説明します。

デフォルト管理者レイアウト上のレポートの説明については、 『事前定義管理レポート』を参照してください。

注: 監視データ・レベルでのデータ・レベル・セキュリティーが有効な場合 (「グローバル・プロファイル」設定を参照)、ユーザーに対してユーザーのデータベース情報のみが表示されるよう、監査プロセスの出力がフィルタリングされます。

インストール済みポリシーの表示

「現在インストールされているポリシー」レポートには、インストールされているポリシーの情報が 表示されます。インストール済みポリシーのリンクをクリックすると、別のウィンドウにポリシー・ルールが 表示されます。

タイプ別データベース数

モニターされる各データベース・タイプのサーバーおよびクライアントの数を 表示します (デフォルトの期間は当日です)。

リクエスト・レート

デフォルトでは、最近 2 時間のリクエスト・レートを表示します。このグラフィカル・レポートは、 最近のアクティビティーのみを表示するためのものです。「開始」および「終了」のランタイム・パラメーターを変更して対象となる時間フレームを大きくすると、データが大きすぎるというメッセージが表示される場合があります。 (より大きな時間枠を表示する場合は、表形式のレポートを使用してください。)

サーバー・タイプ別セッション

サーバー・タイプ (DB2®、Informix® など) ごとに、レポートの 1 行を使用して、 レポート期間 (デフォルトでは過去の 3 時間) にオープンされたセッションの総数が 表示されます。

機密オブジェクトに対する DML 実行

このレポートの 1 行には、「機密オブジェクト」グループのオブジェクト名を参照する「DML コマンド」グループ からの各 SQL 動詞について、アクセス期間、クライアント IP、 ソース・プログラム、およびその行で参照されるオブジェクトの総数が 表示されます。レポート・タイトルには Executions という言葉が含まれますが、 レポートされるすべてのコマンドが実際に実行されたという保証はありません。

機密オブジェクトの使用

「機密オブジェクト」グループの各オブジェクトについて、レポート期間にそのオブジェクトを参照した 各クライアント IP とソース・プログラム、およびオブジェクト参照数が 1 行に表示されます。

「機密オブジェクト」グループはインストール時には空です。企業内の誰かが、該当するメンバーのセットでグループにデータを設定する必要があります。

クライアント IP 別アクティビティー

レポート期間中に参照される各クライアント IP アドレスについて、 SQL 動詞の数、オブジェクト名、およびセッションの総数が 1 行に表示されます。

データベース・サーバー

レポートの 1 行に、レポート期間中にアクセスされる各サーバー IP アドレスについて、 サーバー・タイプ、データベース名、サービス名、 そのサーバーにアクセスするソース・プログラム数、およびその行のセッション総数が 表示されます。

IMS アクセス (z/OS)

IMS™ へのアクセスをレポートするには、これを使用します (z/OS®)。

表 1. IMS アクセス (z/OS)

ドメイン	ベースとなる照会	メイン・エンティティー
アクセス	IMS アクセス	クライアント・サーバー
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -2 HOUR
期間終了	<=	NOW

IMS オブジェクト (z/OS)

IMS に対するオブジェクトをレポートするには、これを使用します (z/OS)。

表 2. IMS オブジェクト (z/OS)

ドメイン	ベースとなる照会	メイン・エンティティー
アクセス	IMS オブジェクト	オブジェクト
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -2 HOUR
期間終了	<=	NOW

IMS イベント (z/OS)

IMS に対するイベントをレポートするには、これを使用します (z/OS)。

表 3. IMS イベント (z/OS)

ドメイン	ベースとなる照会	メイン・エンティティー
アクセス	IMS イベント	SQL
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -2 HOUR
期間終了	<=	NOW

IMS データ・アクセス詳細 (z/OS)

IMS に対するデータ・アクセス詳細をレポートするには、これを使用します (z/OS)。

表 4. IMS データ・アクセス詳細 (z/OS)

ドメイン	ベースとなる照会	メイン・エンティティー
アクセス	IMS データ・アクセス詳細	完全な SQL
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -2 HOUR
期間終了	<=	NOW
クライアント IP	LIKE	
DBUserName	LIKE	
IMS 名	LIKE	
ServerIP	LIKE	

ポリシー違反

このレポートは、レポート期間中にログに記録されるすべてのポリシー・ルール違反について、 「ポリシー・ルール違反」エンティティーからのタイム・スタンプ、 アクセス・ルールの記述、クライアント IP、サーバー IP、データベース・ユーザー名、 「ポリシー・ルール違反」エンティティーからの SQL 文字列全体、重大度の記述、およびその行の違反数を提供します。このレポートのベースとなる照会 (重大度付きポリシー違反リスト) にはアクセスできませんが、このレポートのコピーを作成することができます。

例外分布

円グラフの各扇形は、レポート期間中にログに記録された (「例外タイプ」エンティティーからの) 各「例外分布」属性値の例外の比率を 示します。

他のグラフと同様に、円グラフをドリルダウンして、そのグラフのベースとなる 表形式の照会を表示できます。 ここで利用可能な この表形式レポート (または、この表形式レポートのドリルダウン) から アクセス可能な例外レポートがいくつかありますが、これらはメニューには 含まれていません。

例外モニター

レポート期間中に記録される例外の数。ポータルでレポートをリフレッシュするたびに、 1 つのデータ・ポイントが作成されます。

失敗したユーザー・ログイン試行

レポート期間中のログイン試行の各失敗について、 ユーザー名、ソース・アドレス、宛先アドレス、およびユーザーがログインを試行するサーバーの データベース・プロトコル・タイプをリストします。

SQL エラー

レポート期間中の各 SQL エラーについて、クライアント IP アドレス、 サーバー IP アドレス、サーバー・タイプ、データベース・ユーザー名、データベース・エラー・テキスト、 およびそのレコードの合計エラー発生数を表示します。

例外数

レポート期間中にログに記録される例外の総数 (「例外」エンティティー)。

無効なユーザーのログイン

「無効なデータベース・ユーザー」グループのメンバーであるデータベース・ユーザーによる すべてのログインをリストします。各行に、データベース・ユーザー名、クライアント IP、サーバー IP、 サーバー・タイプ、ソース・プログラム、最後のログイン時 (「セッション開始」属性の最大値)、および その行のセッション数がリストされます。

「無効なデータベース・ユーザー」グループはインストール時は空です。 誰かがデータを設定する必要があります。このレポートのベースとなる照会 (無効なユーザーのログイン) は、クエリー・ビルダーから アクセスできません。

アクティブ・ユーザーの最終ログイン

「アクティブ・ユーザー」グループの各メンバーについて、 レポート期間中に記録された最後のログイン。レポート期間中にログインがない場合でも、 このグループのすべてのメンバーがリストされます。この点は、グループのメンバーに基づく 他のほとんどのレポートとは異なります。「通常」は、メンバーに対して アクティビティーが見つからない場合は、そのメンバーはリストされません。

各行に、データベース・ユーザー名、クライアント IP、サーバー IP、 サーバー・タイプ、ソース・プログラム、最後のログイン時 (「セッション開始」属性の最大値)、および その行のセッション数がリストされます。

「アクティブ・ユーザー」グループはインストール時は空です。 誰かがデータを設定する必要があります。このレポートのベースとなる照会 (アクティブ・ユーザーの最終ログイン) は、クエリー・ビルダーからはアクセスできません。

アクティビティーのないアクティブ・ユーザー

レポート期間中にアクティビティーを持たない、「アクティブ・ユーザー」グループのメンバーの リスト。レポート期間中にすべてのユーザーがアクティビティーを持つ場合、このレポートは 空になります。

「アクティブ・ユーザー」グループは事前定義されていますが、インストール時は空です。 誰かがデータを設定する必要があります。このレポートのベースとなる照会 (アクティビティーのないアクティブ・ユーザー) は、クエリー・ビルダーからはアクセスできません。

無効なユーザーによるログイン試行の失敗

「無効なデータベース・ユーザー」グループのメンバーであるデータベース・ユーザーによる ログイン試行の失敗をリストします。レポート期間中にこのグループの誰かによる ログイン試行の失敗がない場合、このレポートは空になります。

「無効なデータベース・ユーザー」グループは事前定義されていますが、インストール時は 空です。 誰かがデータを設定する必要があります。このレポートの標準装備の照会には アクセスできません。このレポートのベースとなる照会 (無効なユーザーによるログイン試行の失敗) は、クエリー・ビルダーからは アクセスできません。

期間あたりの超過エラー

エラー数/期間を表示します。例えば、同一のクライアント IP アドレス、サーバー IP アドレス、サーバー・タイプ、データベース・ユーザー名で 60 分間のエラー数が N 個より多いなど。

指定日以降に非アクティブなユーザー

アクセス・レコードがあり、最大セッション開始時刻が 90 日より前の全ユーザーについて、ユーザーおよび最後のセッションの開始時刻を示します。(非アクティブ・ユーザーは、一度もログインしたことがない場合や、古いログインがすべてパージされた場合にはなくなります。)

admin ユーザーのログイン

レポート期間中に 1 つ以上のセッションを持っていた 「admin ユーザー」グループに含まれる各データベース・ユーザー名について、各行に クライアント IP、 データベース・ユーザー名、ソース・プログラム、セッション開始の時刻、 およびその行のセッション数がリストされます。

データベース定義済みユーザー・ログイン

レポート期間中に 1 つ以上のセッションを持っていた 「データベース定義済みユーザー」グループに含まれる各データベース・ユーザー名について、 各行に、データベース・ユーザー名、クライアント IP、 サーバー IP、ソース・プログラム、データベース名、 サービス名、およびその行のセッション数がリストされます。

管理コマンドの使用状況

このレポートは、レポート期間中に表示された「管理コマンド」グループに含まれる 各 SQL 動詞について、SQL 動詞、深さ、オブジェクト名、クライアント IP、 および参照されるオブジェクト数をリストします。

管理オブジェクトの使用状況

レポート期間中に表示された「管理オブジェクト」グループに含まれる 各オブジェクト名について、各行にオブジェクト名、クライアント IP、 サーバー IP、サービス名、データベース名、ソース・プログラム、データベース・ユーザー名、 およびその行のオブジェクト数がリストされます。

管理オブジェクトに対する DML 実行

「管理オブジェクト」グループのオブジェクト名を参照する「DML コマンド」グループからの 各 SQL 動詞について、このレポートは 1 行に、データベース・ユーザー名、クライアント IP、サーバー IP、 サーバー・タイプ、サービス名、データベース名、SQL 動詞、オブジェクト名および その行で参照されるオブジェクト数を表示します。

BACKUP コマンド実行

このレポートは、レポート期間中に参照される「BACKUP コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、オブジェクト名、SQL 動詞、およびその行で参照される オブジェクト数を表示します。

RESTORE コマンド実行

このレポートは、レポート期間中に参照される「BACKUP コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、オブジェクト名、SQL 動詞、およびその行で参照される オブジェクト数を表示します。

REVOKE コマンド実行

このレポートは、レポート期間中に参照される「REVOKE コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、オブジェクト名、SQL 動詞、およびこの行で 参照されるオブジェクト数を表示します。

KILL コマンド実行

このレポートは、レポート期間中に参照される「KILL コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、オブジェクト名、SQL 動詞、およびこの行で 参照されるオブジェクト数を表示します。

DBCC コマンド実行

このレポートは、レポート期間中に参照される「DBCC コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、SQL ステートメント、およびその行で 参照されるオブジェクト数を表示します。

GRANT コマンド実行

このレポートは、レポート期間中に参照される「GRANT コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、オブジェクト名、SQL 動詞、およびその行で 参照されるオブジェクト数を表示します。

特権アカウント使用状況

admin ユーザー・グループのユーザーによる VERB の実行に関して、ユーザー、VERB、および期間のカウントを示します。

ビジネス・オブジェクトの特権ユーザー・アクセス

ビジネス・オブジェクトの選択されたグループに存在するオブジェクトによる VERB の実行および admin ユーザーに関して、ユーザー、VERB、およびオブジェクトを示します。

CREATE コマンド実行

このレポートは、レポート期間中に参照される「CREATE コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、オブジェクト名、SQL 動詞、およびその行で 参照されるオブジェクト数を表示します。

DDL コマンド

データベースに送信されるすべての DDL コマンド。このレポートは、 DDL の要求元となるクライアント IP、メイン SQL 動詞 (特定の DDL コマンド)、およびそのレコード用にアクセスされる合計オブジェクトを表示します。

このレポートは、レポート期間中に参照される「DDL コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サーバー・タイプ、SQL 動詞、およびその行で参照されるコマンド数を表示します。

ALTER コマンド実行

発行されるすべての ALTER コマンド。このレポートは、特定の行にリストされている クライアント IP/DDL コマンドの組み合わせごとに、 DDL の要求元となるクライアント IP、サーバー IP アドレス、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、オブジェクト名、およびのメイン SQL 動詞 (特定の DDL コマンド) を 表示します。

このレポートは、レポート期間中に参照される「ALTER コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、オブジェクト名、SQL 動詞、およびその行で 参照されるオブジェクト数を表示します。

DDL 分布

この棒グラフは、レポート期間中に「DDL コマンド」グループから参照される コマンドの分布を示します。参照されるコマンドごとに、単一のバーが、影響を受けるオブジェクトの総数を示します。

DROP コマンド実行

このレポートは、レポート期間中に参照される「DROP コマンド」グループからの各 SQL 動詞について、 クライアント IP、サーバー IP、サービス名、データベース・ユーザー名、 ソース・プログラム、データベース名、オブジェクト名、SQL 動詞、およびその行で 参照されるオブジェクト数を表示します。

1 ユーザー 1 IP

このレポートの各行には、レポート期間中にセッション・データが収集されたデータベース・ユーザー名ごとに、 ユーザーのログイン元となるクライアント IP アドレスの数、 およびセッションの総数が表示されます。

クライアント IP アクティビティーのサマリー

このレポートは、ランタイム・パラメーターとして指定されている、単一のクライアント IP アドレスからの レポート期間アクティビティーを表示します。レポートの各行には、 クライアント IP、ソース・プログラム、SQL 動詞、(SQL コマンド内のセンテンスの) 深さ、 オブジェクト名、およびその行のためにオブジェクトが参照された回数が表示されます。

セッション・リスト

このレポートは、レポート期間のすべてのデータベース・セッションをリストします。 各セッションについて、レポートはセッション (エンティティー) タイム・スタンプ、 セッション開始 (タイム・スタンプ)、サーバー・タイプ、クライアント IP、サーバー IP、クライアント・ポート、 サーバー・ポート、ネットワーク・プロトコル、データベース・プロトコル、データベース・プロトコル・バージョン、 データベース・ユーザー名、ソース・プログラム、およびその行のセッション数 (常に 1 でなければ なりません) を表示します。

ほとんどのレポートと同様に、ドリルダウン・レポートが利用できます。 このレポートから アクセス可能なセッション・レポートは多数ありますが、これらはメニューには 含まれていません。以下のレポートと、 選択したレポートの行からの値を使用して設定されたレポートのランタイム・パラメーター が含まれます。

表 5. セッション・リスト

レポート	ランタイム・パラメーター
クライアント IP 別セッション	サーバー IP、サーバー・タイプ
サーバー IP 別セッション	サーバー・タイプ
ソース・プログラム別セッション	サーバー・タイプ、 サーバー IP
ユーザー別セッション	サーバー・タイプ、 サーバー IP
サーバー別セッション詳細	サーバー・タイプ、 サーバー IP

コマンド・リスト

このレポートは、レポート期間中に参照されるすべての SQL 動詞をリストします。最外部レベルでは、 コマンドは正時に「アクセス期間」エンティティーからの「期間の開始」時刻によって グループ化されます (通常は 1 時間)。Guardium® 管理者は、 ログ細分度を変更することによって、アクセス期間の長さを変更することが できます (デフォルトでは 1 時間)。レポート期間の各アクセス期間について、 各行にアクセス期間の開始時刻、 SQL 動詞、SQL ステートメントの動詞の深さ、親 (所有動詞へのポインター)、 およびその行のオカレンス数がリストされます。

オブジェクト・リスト

このレポートは、レポート期間中に参照されるすべてのオブジェクトをリストします。最外部レベルでは、 オブジェクトは正時に「アクセス期間」エンティティーからの「期間の開始」時刻によって グループ化されます (通常は 1 時間)。SQL Guard 管理者は、 ログ細分度を変更することによって、アクセス期間の長さを変更することが できます (デフォルトでは 1 時間)。レポート期間中の各アクセス期間について、 各行にアクセス期間の開始時刻、オブジェクト名、および その行のオカレンス数がリストされます。

オブジェクト・アクティビティーのサマリー

このレポートは、ランタイム・パラメーターとして指定されている単一オブジェクト名についての、レポート期間アクティビティーを表示します。レポートの各行には、クライアント IP、ソース・プログラム、SQL 動詞、(SQL コマンド内のセンテンスの) 深さ、 オブジェクト名、およびその行のためにオブジェクトが参照された回数が表示されます。

アーカイブ候補

このレポートは、長期間アクセスされていないオブジェクト (データベース表またはストアード・プロシージャー など) をリストします。このレポートのベースとなる照会にアクセスすることは できません。

Windows ファイル共有アクティビティー

このレポートは、レポート期間中に参照されるすべての Windows ファイル共有 SQL アクティビティーを リストします。最外部レベルでは、SQL コマンドは正時に 「アクセス期間」エンティティーからの「期間の開始」時刻によって グループ化されます (通常は 1 時間)。Guardium 管理者は、 ログ細分度を変更することによって、アクセス期間の長さを変更することが できます (デフォルトでは 1 時間)。レポート期間の各アクセス期間について、 各行にアクセス期間の開始時刻、サービス名、クライアント IP、サーバー IP、 ソース・プログラム、SQL (SQL エンティティーから)、およびその行の オカレンス数がリストされます。このレポートのベースとなる照会にアクセスすることはできませんが、 そのレポートのコピーを作成することができます。

時間帯別アクセス詳細

このレポートは、レポート期間 (このレポートではデフォルトは 1 時間) に参照される 各データベース・ユーザー名について、非常に詳細なリストを作成します。 レポートの各行は、データベース・ユーザー名、クライアント IP、サーバー IP、 期間の開始、ソース・プログラム、SQL (SQL エンティティーから)、およびアクセス期間中のオカレンス数をリストします。

データベース・ユーザー名別の完全な SQL

このレポートは、ランタイム・パラメーターに指定されている単一データベース・ユーザー名について、ログに記録されているレポート期間の「完全な SQL」属性値を表示します。レポートの各行には、完全な SQL ID、 (「完全な SQL」エンティティーの) タイム・スタンプ、クライアント IP、データベース・ユーザー名、セッション開始、 ソース・プログラム、完全な SQL、およびその行のオカレンス数が表示されます。

クライアント IP 別の完全な SQL

このレポートは、ランタイム・パラメーターに指定されている単一クライアント IP について、ログに記録されているレポート期間の「完全な SQL」属性値を表示します。レポートの各行には、完全な SQL ID、 (「完全な SQL」エンティティーの) タイム・スタンプ、クライアント IP、データベース・ユーザー名、セッション開始、 ソース・プログラム、完全な SQL、およびその行のオカレンス数が表示されます。

未解析ログ・リスト

未解析ログ処理のタスクをリストします。

分類プロセスの結果

分類プロセスのタスクをリストします。

DW 休止オブジェクト

休止表に焦点を絞って、第 2 グループのメンバーではない、 1 つのグループの全メンバーを表示します。例えば、このレポートは、すべてのオブジェクトグループに含まれているが、選択で使用されていないオブジェクトを表示します。

DW 休止オブジェクト/フィールド

休止表および列に焦点を絞って、第 2 グループのメンバーではない、 1 つのグループの全メンバーを表示します。このインスタンスでは、 グループは 2 タプルのタイプ (値属性のペアの複合であるメンバー) です。 例えば、このレポートは、すべてのオブジェクトおよびフィールドグループに含まれているが、選択で使用されていないオブジェクトを表示します。

DW EXECUTE オブジェクト・アクセス

このレポートを使用して、実行中のストアード・プロシージャー名のセットで「DW EXECUTE オブジェクト」というグループを取り込みます。次に、 「グループ・ビルダー」/「自動生成呼び出しプロシージャー」で間接マッピングを使用して、 これらのプロシージャー内で使用されるオブジェクトをすべて生成します。

DW SELECT オブジェクト・アクセス

このレポートは、SELECT ステートメントを介してアクセスされる すべてのオブジェクト名を表示します。

DW SELECT オブジェクト/フィールド・アクセス

このレポートは、SELECT ステートメントを介してアクセスされる すべてのオブジェクト名およびフィールド名を表示します。

長時間実行されている照会

このレポートは、レポート期間について、最も長く実行されている照会と、 最も長い平均実行時間をリストします。照会ごとに、 クライアント IP、サーバー IP、SQL、 (「アクセス期間」エンティティーからの) 期間の開始、 平均実行時間、およびその行のオカレンス数がリストされます。このレポートのベースとなる照会にアクセスすることは できません。

スループット

このレポートは、レポート期間中に参照されるすべてのサーバー IP の数 および合計アクセス数を示します。最外部レベルでは、アクセスは正時に 「アクセス期間」エンティティーからの「期間の開始」時刻によって グループ化されます (通常は 1 時間)。Guardium 管理者は、 ログ細分度を変更することによって、アクセス期間の長さを変

更することが できます (デフォルトでは 1 時間)。各行には、 期間の開始時刻、参照されるサーバー IP の数、 およびその行の合計アクセス数がリストされます。

サーバー IP ランタイム・パラメーター (デフォルトではすべての IP アドレスを選択する “%” に 設定されています) を使用して、このレポートの出力を制限することができます。

スループット (グラフィカル)

このレポートは、表形式スループット・レポートの図表バージョン「分散ラベル付き線グラフ」で、期間の開始時刻ごとに 1 つのデータ・ポイントでレポート期間中のアクセス総数を作図します。

サーバー IP ランタイム・パラメーター (デフォルトではすべての IP アドレスを選択する “%” に 設定されています) を使用して、このレポートの出力を制限することができます。

アクティブなプライバシー・セット・タスクの数

1 つ以上のプライバシー・セット・タスクを含む、 アクティブな Guardium 監査プロセスの数。一元管理が使用されている場合、このレポートには中央マネージャーに関するデータのみが含まれ、 すべての管理対象ユニットに関しては空になります (「要求された照会のデータが見つかりません」という標準メッセージが表示されます)。このレポートは 標準とは異なるランタイム・パラメーターを持ちます。開始日付と終了日付のパラメーターがないため、 1 つ以上のプライバシー・セット・タスクが含まれるすべての監査プロセスが レポートされます。このレポートのベースとなる照会 (アクティブ・プライバシー・セット・プロセスの数) の コピーを作成することはできますが、デフォルト・レポートのコピー作成や再生成は できません。複製された照会には、すべての標準ランタイム・パラメーター (開始日付と終了日付 を含む) が含まれます。

Guardium ジョブ・キュー

Guardium ジョブ・キューを表示します。ジョブごとに、 プロセス実行 ID、プロセス・タイプ、状況、分類/評価プロセス ID、レポート結果 ID、 分類/評価の記述、監査タスクの記述、キュー時刻、開始時刻、終了時刻、 およびデータ・ソースがリストされます。

表 6. Guardium ジョブ・キュー

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	Guardium ジョブ・キュー	使用不可
ランタイム・パラメーター	演算子	デフォルト値
ジョブの記述	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

ディスカバーされたデータベース

このレポートは、レポート期間について、「データベース・タイプ」属性値が不明でない「ディスカバーされたポート」エンティティーごとに、プローブ・タイム・スタンプ、サーバー IP、サーバーのホスト名、データベース・タイプ、ポート、ポート・タイプ、およびその行の「ディスカバーされたポート」数をリストします。

表 7. ディスカバーされたデータベース

ドメイン	ベースとなる照会	メイン・エンティティー
オートディスカバリー	ディスカバーされたデータベース	ディスカバーされたポート
ランタイム・パラメーター	演算子	デフォルト値
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

データ・ソース

このレポートは、管理者用とユーザー用の両方のデフォルトのレイアウトに表示されます。「事前定義レポート - 共通」ページの『データ・ソース』を参照してください。

データ・ソース・バージョン履歴

このレポートは、管理者用とユーザー用の両方のデフォルトのレイアウトに表示されます。『事前定義レポート - 共通』ページの データ・ソース・バージョン履歴を参照してください。

Guardium ジョブ・キュー

Guardium ジョブ・キューを表示します。ジョブごとに、 プロセス実行 ID、プロセス・タイプ、状況、分類/評価プロセス ID、レポート結果 ID、 分類/評価の記述、監査タスクの記述、キュー時刻、開始時刻、終了時刻、 およびデータ・ソースがリストされます。

未処理監査プロセスのレビュー

このレポートは、各 Guardium ユーザー・ログイン名について、 未処理の Guardium 監査プロセスの数とタイプをリストします。未処理の監査プロセスには、「Reviewed」または「Signed」以外の状況属性値 (「タスク結果 To-Do リスト」エンティティー内) が あります。このレポートは、標準とは異なるランタイム・パラメーターを持ちます。 開始日付と終了日付がないため、未処理のタスクの結果がすべて レポートされます。このレポートのベースとなる照会のコピー (同じ名前を持つ) を 作成することができますが、デフォルト・レポートのコピー作成や再生成は できません。複製された照会には、すべての標準ランタイム・パラメーター (開始日付と終了日付 を含む) が含まれます。

アクティブな監査プロセスの数

アクティブな Guardium 監査プロセスの数。一元管理が使用されている場合、このレポートには中央マネージャーに関するデータのみが含まれ、 すべての管理対象ユニットに関しては空になります (「要求された照会のデータが見つかりません」という標準メッセージが表示されます)。このレポートは標準とは異なるランタイム・ パラメーターを持ちます。開始日付と終了日付のパラメーターがないため、すべてのアクティブな 監査プロセスがレポートされます。このレポートのベースとなる照会 (アクティブ・プロセス数) の コピーを作成することはできますが、デフォルト・レポートのコピー作成や再生成はできません。 複製された照会には、すべての標準ランタイム・パラメーター (開始日付と終了日付 を含む) が含まれます。

インストール済みポリシーの表示

この特別なレポートは、「現在インストールされているポリシー」パネルに、インストールされているポリシーに関する情報 (ポリシーの名前、それに含まれるルールの数、そのポリシー定義の設定など) を表示します。このレポートのベースとなる照会にアクセスすることは できません。

ポリシー違反数

このレポートは、レポート期間について、ログに記録されたポリシー違反の数を 表示します。

ログに記録されるしきい値アラート

このレポートは、「しきい値アラート詳細」エンティティーの「アラートの記述」属性に基づいて、ログに記録されるしきい値アラートの タイプごとに、レポート期間中にログに記録されたアラートの総数を 示すバーを表示します。

ログに記録される R/T アラート

このレポートは、「ポリシー・ルール違反」エンティティーの「アクセス・ルールの記述」属性に基づいて、ログに記録されたリアルタイム・アラートのタイプごとに、レポート期間中にログに記録されたアラートの総数を示すバーを表示します。

違反/インシデント

『インシデント管理 』トピックを参照してください。

親トピック: 事前定義レポートを活用する方法

事前定義レポート (共通)

このセクションでは、デフォルト・ユーザー・レイアウトとデフォルト管理者レイアウトでのすべての事前定義レポートについて、簡単に説明します。

共通のレポートは次のとおりです。

- データ・ソース・バージョン履歴
- データ・ソース

ステータス・モニター

「ステータス・モニター」のグラフィカル・レポートには、Guardium® アプライアンスの現在の状態 (1 秒当たりに処理するパケット数と要求数、使用されているディスク・スペースとメモリーの量など) が表示されます。次の表で、各フィールドについて説明します。

ボックスには、Linux VMSTAT コマンドの出力が表示されます。このコマンドの知識があれば、 これらの統計はおなじみのものです。

表 1. ステータス・モニター

フィールド	記述
プロセス	プロセス数: **r**: ランタイムを待機しています。 **b**: 割り込み不能なスリープ状態です (ブロックされ、別のイベントを待機中です)。
メモリー	メモリー使用量 (KB): **swpd**: 使用されている仮想メモリーの量。 **free**: 使用されていないメモリーの量。 **buff**: バッファーとして使用されている量。 **cache**: キャッシュ用に予約されている量。
スワップ	メモリーの量 (KB): **si**: ディスクからスワップインされています。 **so**: ディスクにスワップアウトされています。
入出力	入出力ブロック (KB/s): **bi**: ブロック・デバイスから受信したブロック **bo**: ブロック・デバイスに送信したブロック

フィールド	記述
システム	システム: **in**: 1 秒当たりの割り込み (クロックを含む) **cs**: 1 秒当たりのコンテキスト切り替え
CPU	次で使用する合計 CPU 時間のパーセンテージ。 **us**: 非カーネル・コードの実行に費やす時間 **sy**: カーネル・コードの実行に費やす時間 **id**: アイドル時間 (入出力待ちを含まず) **wa**: 入出力待ちに費やす時間 **st**: 仮想マシンから流用する時間
(n)pps / (m)rps	分析エンジンの横の矢印で、最近 5 分間の 2 種類の平均値が算出されます。 **n** はネットワーク・パケットの 1 秒当たりの平均数、**m** はネットワーク・データベース要求の 1 秒当たりの平均数です。
分析エンジン (q-d) ------ (p)	分析エンジンでは、 最初の行に処理のためキューに入れられているメッセージの総数 (**q**) がリストされ、その後に、バッファーがフルになる心配があったためドロップされたメッセージの数 (**d**) が続きます。2 番目の行には、 処理されたメッセージの総数 (**p**) がリストされます。 処理された数は、検査エンジンが再始動されると必ずゼロにリセットされます。
サーバー・タイプ (q) ---- (p)	各サーバー・タイプでは、処理を待つメッセージの数 (**q**) と、 処理済みのメッセージの数 (**p**) がリストされます。
空きディスク・スペース	空いているバイト数。
データベース使用率	データベースのスペース割り振りのうち、 使用されている割合。
ファイル/その他 (Files/Other)	ステータス・モニターの「ファイル/その他 (Files/Other)」部分は、nondb-sql ロガーで累積されたデータを表します。 nondb-sql ロガーは、アナライザーによって内部的にクローズされている (INACTIVE_FLAG=-1) 「無視された」セッションからアナライザーに到達したセッション・クローズ・イベントを記録します。アナライザーは、(セッションが長期間非アクティブである場合に) タイムアウトによって接続を閉じることができます。タイムアウトによってクローズされている「無視された」セッションからアナライザーにセッション・クローズ・データが到達した場合は、それが nondb-sql-logger セクションに記録されます。 アナライザーがデータベースにデータを直接記録することはありません。このセクションは、アナライザーによってロガーに送信された DB 要求 (GDM_SECURE_PARAMS への挿入など) の数や、サポートされるその他のプロトコル (FTP など) も表します。

データ・ソース・バージョン履歴

デフォルト・レイアウトのロケーション

- 管理者:「データ・ソース」レポートからドリルダウンして入手可能
- ユーザー:「ディスカバー」>「データベース・ディスカバリー」

データ・ソース

定義されているすべてのデータ・ソースをリストします。データ・ソース・タイプ、データ・ソース名、 データ・ソースの記述、ホスト、ポート、サービス名、ユーザー名、データベース名、 最後の接続、共有、接続プロパティー。

このレポートの出力は、「データ・ソース名」ランタイム・パラメーターで制限できます。 このパラメーターは、デフォルトではすべてのデータ・ソースを選択する「%」に設定されています。

表 2. データ・ソース

ドメイン	ベースとなる照会	メイン・エンティティー
内部 - 使用不可	データ・ソース	使用不可
ランタイム・パラメーター	演算子	デフォルト値
データ・ソース名	LIKE	%
期間開始	>=	NOW -1 DAY
期間終了	<=	NOW

事前定義監査プロセス

「アプライアンスのモニター」という事前定義監査プロセスがあり、これには、リストされた進行中のレポートが含まれます。この監査プロセスは、デフォルトでは非アクティブになっています。 管理者は、必要に応じてこれを活動化したり、スケジュールに入れたりすることができます。

注: この監査プロセスをスケジューリングする場合、 各レポートの FROM/TO の日付が定義済みのプロセス間隔と整合性があることを確認してください (例えば、 監査プロセスが週に一度しか実行されない場合は、レポート期間を 1 日にしても意味がありません。6 日間はアクティビティーがないことになります)。
「アプライアンスのモニター」監査プロセスには、以下のレポートが含まれます。

- Guardium への失敗したログイン
- アクティブな Guardium ユーザー
- 統合エラーまたはアーカイブ・エラー

- ポリシー関連の変更
- 検査エンジンと S-TAP® の変更
- データ・ソース変更
- CAS インスタンス構成変更
- CAS インスタンス
- CAS テンプレート
- スケジュールされたジョブの例外

親トピック: 事前定義レポートを活用する方法

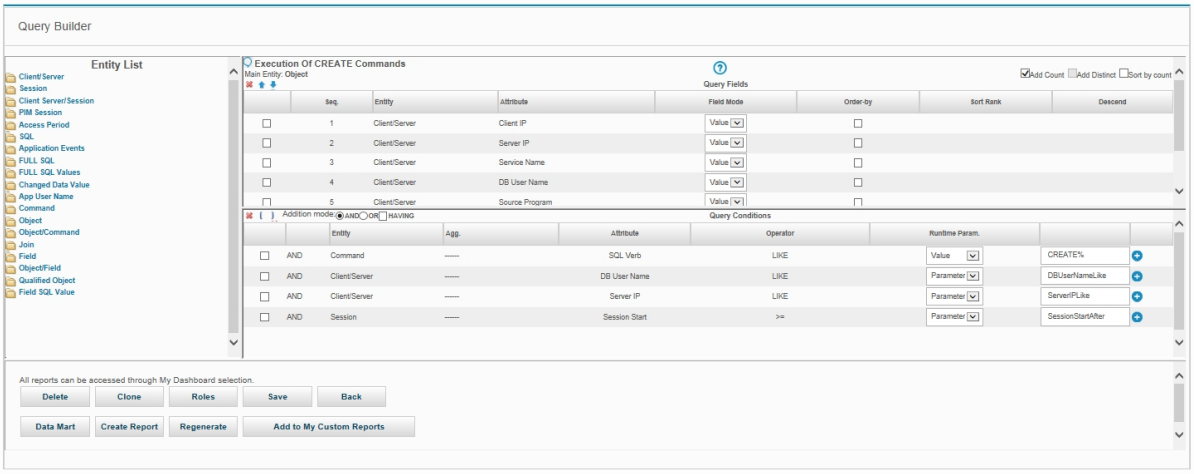
データに関する質問方法

収集したデータに関する質問の定義や変更を行うには、クエリー・ビルダーを使用します。

照会とレポートの間には、次のような違いがあります。

- 照会は、収集したデータから取得される情報セットを記述します。例えば、「週末の間に特定のデータベースを更新するすべてのクライアントを検索する」や、「機密データ (社会保障番号やクレジット・カード番号) にアクセスしようとした無許可ユーザーはだれか」などです。
- レポートは、照会によって返されたデータの表示方法を記述します。

ドメインごとに個別のクエリー・ビルダーがあり、ドメインの「照会ファインダー」から 開くことができます (『照会ファインダーを開く』を参照)。「レポート」 > 「レポート構成ツール」 > 「クエリー・ビルダー」をクリックします。



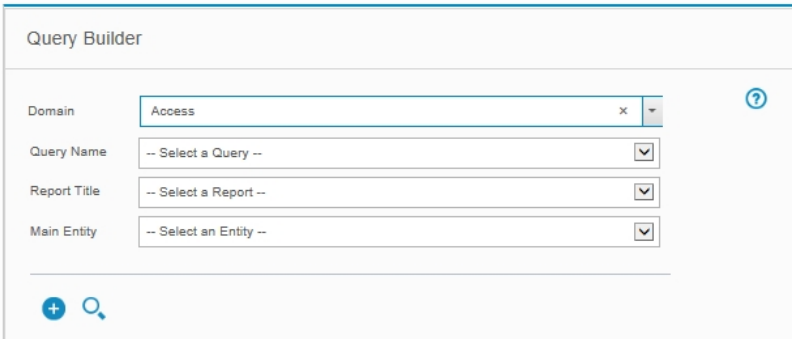
クエリー・ビルダーには、次の 3 つのペインが含まれます。

- 「エンティティー・リスト」ペインには、ドメインに含まれるすべてのエンティティーと属性が表示されます。エンティティーはフォルダーとして、属性はフォルダーに含まれる項目として表されます。 エンティティー・フォルダーをクリックするとその属性が表示され、もう一度クリックすると非表示になります。 すべてのエンティティーと属性の説明については、付録『ドメイン、エンティティー、および属性』の 『エンティティーおよび属性』を参照してください。
- 「照会フィールド」ペインには、アクセスするすべてのフィールド、そのフィールドについての表示内容 (値、カウント、最小、最大、または平均)、およびソート順がリストされます。このペインの使用について詳しくは、『照会フィールドの概要』を参照してください。
- 「照会条件」ペインでは、リストされたフィールドを選択するための条件 (例えば、「where VERB = UPDATE」) を指定します。 このペインの使用方法については、『照会』ヘルプ・トピックの『照会条件の概要』を参照してください。

詳細情報については、『照会』ヘルプ・トピックを参照してください。

照会ファインダーを開く

レポート・ドメインごとに個別のクエリー・ビルダーがあるので、正しいクエリー・ビルダーを開くことが重要になります。 そうしないと、目的の情報が表示されません。すべてのドメインについては、付録『ドメイン、エンティティー、および属性 』の 『ドメイン』のトピックで説明しています。



使用するドメインの決定後、「レポート」 > 「レポート構成ツール」 > 「クエリー・ビルダー」をクリックします。

照会の検索

クエリー・ビルダーで照会の定義を探して表示するための、いくつかのオプションがあります。

1. 照会ファインダーを使用します。『照会ファインダーの使用』を参照してください。
2. 照会に基づくレポートから、レポートのツールバーにある「このレポートの照会を編集 (Edit this Report's Query)」をクリックします。

照会ファインダーの使用

1. 適切なドメインの照会ファインダーを開きます (『照会ファインダーを開く』を参照)。
2. オプション。照会のメイン・エンティティーが判明している場合は、リストからそれを選択してください。
3. 「検索」をクリックします。

   選択されたメイン・エンティティーに 1 つの照会のみ定義されている場合、 その照会が直ちに照会定義パネルで開きます。

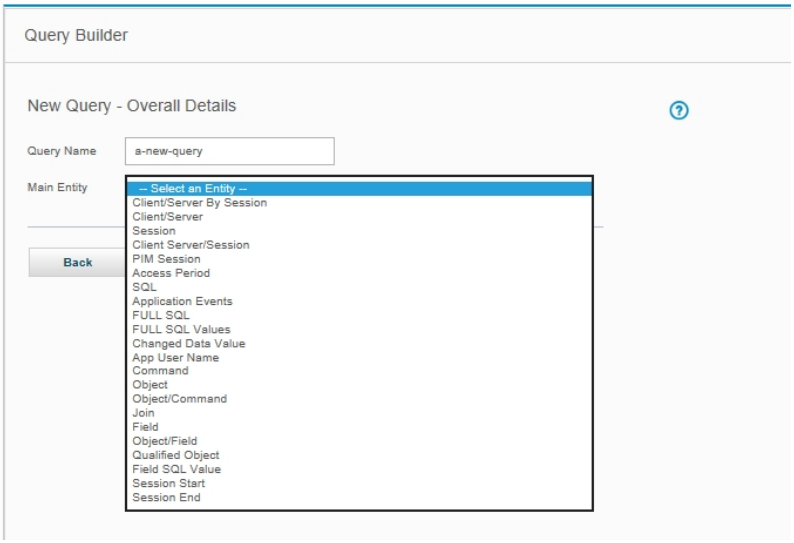
   選択したメイン・エンティティーに複数の照会が定義されている場合、 またはメイン・エンティティーが選択されなかった場合は、「照会リスト」パネルに照会のリストが表示されます。

   照会が定義されていないメイン・エンティティーを選択した場合には、通知を受けます。
4. 以下のいずれかを実行します。

   リストされた照会の「クエリー・ビルダー」パネルを開くには、対象の照会の上でクリックします。新規照会を定義するには、「新規」をクリックします。

照会の作成

1. 適切なドメインの照会ファインダーを開きます (『照会ファインダーを開く』を参照)。
2. 「新規」をクリックして「新規照会 - 全体詳細」パネルを開きます。
3. 「照会名」ボックスに、固有の照会名を入力します。 照会名にはアポストロフィ文字を含めないでください。
4. 「メイン・エンティティー」リストから、照会のメイン・エンティティーを選択します。 メイン・エンティティーが照会で使用可能な詳細のレベルを制御するため、そのレベルを変更できません。基本的に、照会によって返される各データ行は、 メイン・エンティティーの固有のインスタンスおよびそのインスタンスのオカレンス数を表します。
5. 「次へ (Next)」をクリックします。「クエリー・ビルダー」パネルで新規照会が開きます。定義を設定するには、照会フィールドに関する次のセクションを参照してください。



照会フィールドの概要

照会フィールドの概要

「照会フィールド」ペインは、基本的に、照会によって返されるデータの列をリストします。

「照会フィールド」ペインにフィールドを追加する方法は、2 とおりあります。

- ポップアップ・メニュー方式:

1. 追加するフィールドをクリックします。
2. ポップアップ・メニューから「フィールドの追加」を選択します。

- ドラッグ・アンド・ドロップ方式:

1. (フィールド名ではなく) フィールドにあるアイコンをクリックします。
2. アイコンを「照会フィールド」リストまでドラッグしてから、放します。

使用する方式に関係なく、フィールドはリストの末尾に追加されます。

「照会フィールド」ペインのフィールドを移動または削除

「照会フィールド」ペインのフィールドを移動する手順は、以下のとおりです。

1. フィールドのチェック・ボックスにマークを付けます。
2. 以下のボタンを使用して、フィールドを望ましい位置に移動します。

   「上へ」をクリックすると、フィールドが 1 行上に移動します。

   「下へ」をクリックすると、フィールドが 1 行下に移動します。

照会の変更

1. 適切なドメインの照会ファインダーを開きます (『照会ファインダーを開く』を参照)。
2. 照会ファインダーを使用して、変更する照会を開きます。
3. 『クエリー・ビルダーの概要』トピックで、照会定義のコンポーネントを変更する方法を参照してください。

レポートの作成

照会の定義が完了した後、その照会に基づく表形式レポートを、既存のメニュー・レイアウトに即時に追加するためのオプションがいくつかあります。 これらのオプションは、表形式のレポートにのみ適用されます。

1. 適切なドメインの照会ファインダーを開きます (『照会ファインダーを開く』を参照)。
2. 照会ファインダーを使用して、レポートに使用する照会を開きます。
3. 以下のいずれかを実行します。

   レポートを作成するには、「レポートの作成」をクリックします。既存の表形式レポートを再生成する場合は、 「再生成」をクリックします。

   「マイ・カスタム・レポート」タブに表形式レポートを追加するには、パネルにある「マイ・カスタム・レポートに追加」をクリックします。(その照会の表形式レポートがまだ生成されていない場合、最初に「レポートの作成」をクリックする必要があります。)

   表形式のレポートに意味のあるデータを表示するには、  をクリックしてランタイム・パラメーターにアクセスします (開始時刻および現在時刻を変更します)。

親トピック: レポート

休止状態の表および列のレポート作成方法

Guardium® では、データ設計者と DBA のための機能として、現在使用されていない表やフィールドを見つける機能が提供されます。

このタスクについて

基本的な概念は以下のとおりです。 現在、アクセスされていない表を知りたいとします。 Guardium のカスタム・ドメインとカスタム照会機能を使用して、データベースまたは構成管理データベース (CMDB) からすべての表名をアップロードします。続いて、(カスタム照会からの) レポートを使用して、オブジェクトのグループを取り込みます。

次に、モニター対象データを使用するレポートで、SELECT ステートメントに関わるすべてのオブジェクト名を表示します。 Guardium 8 ではこのために定義済みのレポートが用意されており、これらはすべて接頭部 DW (データウェアハウス) で始まります。 この出力を使用して、いずれかの定義済みグループを設定します。

最後に、最初のグループのメンバーで 2 番目のグループのメンバーでないものをすべて表示する定義済みレポートを使用します。

これらのレポートとグループには、表にフォーカスしたものと、表と列にフォーカスしたものの 2 つがあります。 唯一の違いとして、後者の場合のグループは 2 タプルのタイプ (値属性のペア (タプルと呼ばれる) の複合であるメンバー) となります。

それでは、Oracle データベースと EMP ユーザーに関連した例を通して見てみます。

以下の手順を行います。

1. 一連のシステム・カタログ表 (データベース・オブジェクトの定義) から、 すべての表名またはすべての表/列の組み合わせ (あるいは両方) をアップロードします。
2. モニター対象データを使用して、一定期間にアクセスされた表または表/列を判別します。
3. ステップ 1 の項目でステップ 2 に含まれない項目すべてについてレポートを作成します。

このタスクでは、以下の Guardium 機能を使用します。

- 表名と列名をアップロードするための外部データ相関
- 照会からのグループの取り込み
- レポート作成

手順

1. システム・カタログからすべての表をアップロードします。 これは、カスタム表を作成して行います。

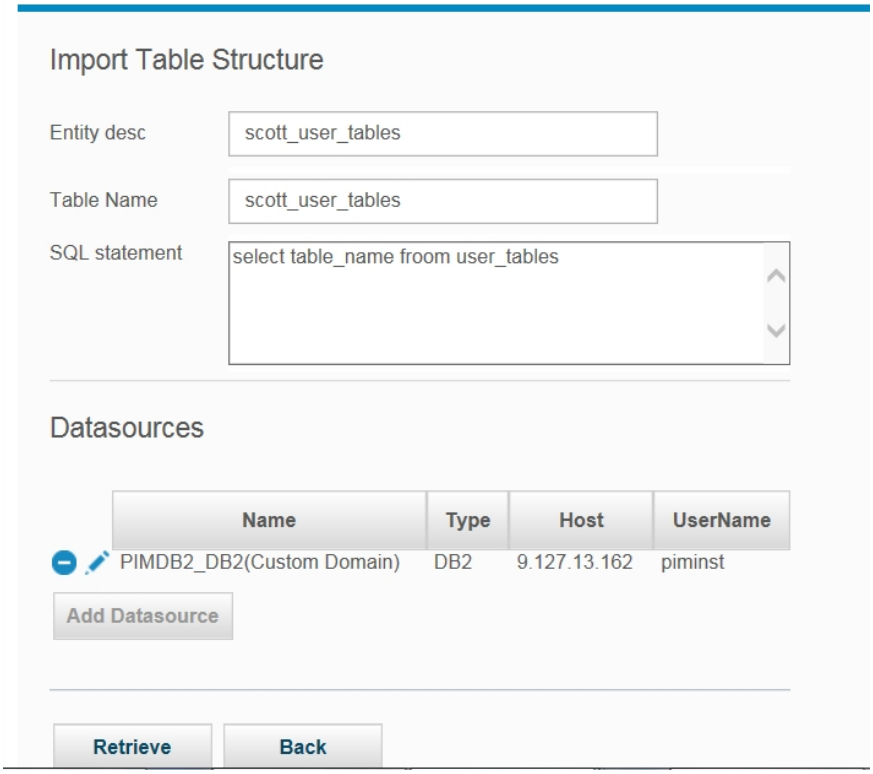
   前提条件

   a. データ・ソース/テスト・データベース接続を定義する
   b. データをアップロード (カスタム表を作成) する
   c. 新規ドメインを作成する (カスタム表に既存のレポートをマージ)

   詳しくは、『外部データ相関』を参照してください。

   以下の例は、「順守」 > 「カスタム・レポート作成」 > 「カスタム表ビルダー」 > 「定義のアップロード」 > 「表構造のインポート」から使用できます。

   構成が完了したら、「取得」ボタンをクリックします。



   構成 - 定義のアップロード、表構造のインポート

   データをアップロードして Guardium システムに (カスタム表として) 取り込み、必要に応じてこのアップロードをスケジュールします。 このデータを使用して、システムに定義されたすべての表のスーパーセットを判別します。

   システムのすべてのオブジェクト (またはオブジェクト-フィールド) のマッピング

   この例では、表名に基づく休止データを扱います。 ただし、解析には列を含むことが可能です。この場合は、アップロード・タスクを `<object,field>` のペアを返すように定義し、 タプル・グループを使用して監視対象の `object+field` のタプルと比較する必要があります。

   オブジェクト-フィールドの場合の例: 「DW 休止オブジェクト」レポートを「DW 休止オブジェクト - フィールド」レポートに置き換えます。 オブジェクト-フィールドの場合の例: 「DW SELECT オブジェクト・アクセス」レポートを「DW SELECT オブジェクト/フィールド・アクセス」レポートに置き換えます。

   アップロードが完了したら、この 1 つのカスタム表をもとにカスタム・ドメインを定義して、表名を取得するレポートを定義します。

   次に、このレポートからグループ「DW すべてのオブジェクト」を取り込み、必要に応じて「照会からのインポート」アクションをスケジュールします。 これにより、システム・カタログで定義されたすべての表を含むグループが作成されます。

   注: グループ「DW すべてのオブジェクト」へ取り込む場合、「今すぐ 1 回実行」>「すべて選択」>「インポート」ボタンをクリックして、情報を含める必要があります。 グループ名「DW SELECT がアクセスしたオブジェクト」に対しても同じことを実行してください。スケジュールされた定義すべてをインポートする必要があります。

   終了したら、「保存」ボタンをクリックします。

2. オブジェクトの直接マッピング

   モニター対象データを使用して、一定期間にアクセスされた表または表/列を判別します。

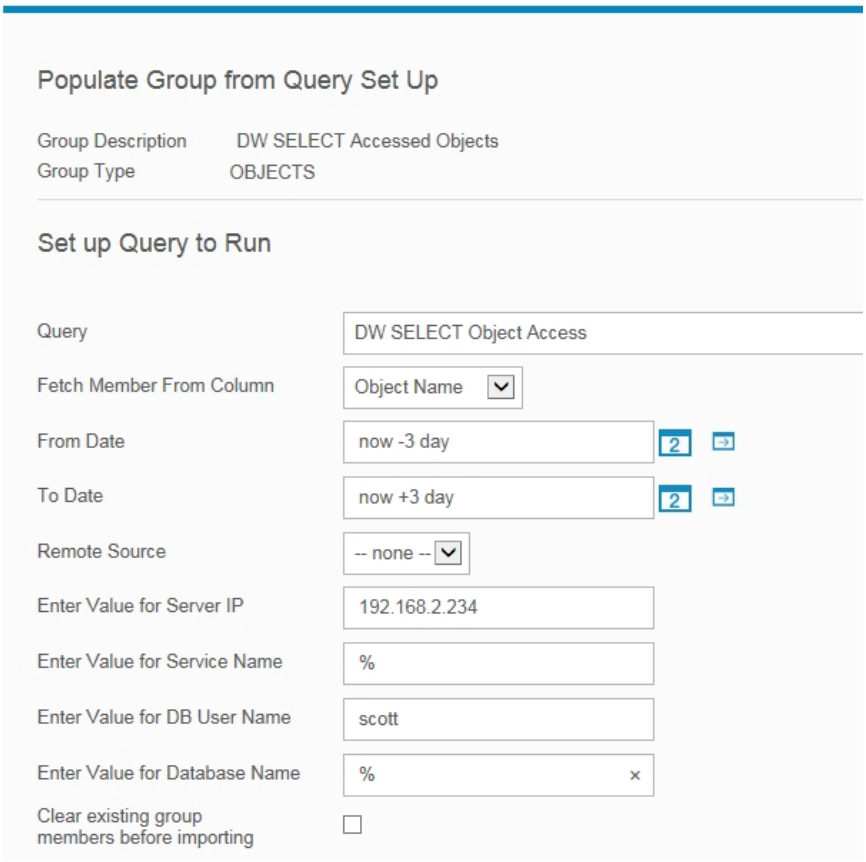
いくつか追加の定義済みレポートを見ます。「DW SELECT オブジェクト・アクセス」レポートには、SELECT ステートメントでアクセスされたすべてのオブジェクト名が表示されます。

次に、レポートから「DW SELECT がアクセスしたオブジェクト」グループを取り込み、 必要とするフィルター属性を入力します。

注: グループ「DW すべてのオブジェクト」へ取り込む場合、「今すぐ 1 回実行」>「すべて選択」>「インポート」ボタンをクリックして、情報を含める必要があります。 グループ名「DW SELECT がアクセスしたオブジェクト」に対しても同じことを実行してください。スケジュールされた定義すべてをインポートする必要があります。

以下の例は、「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」 > 「DW すべてのオブジェクト」 > 「照会から取り込み」 > 「DW SELECT オブジェクト・アクセス」から使用できます。

終了したら、「保存」ボタンをクリックします。



構成 - 照会からグループに取り込み、オブジェクト名

3. ステップ 1 の項目でステップ 2 に含まれない項目すべてについてレポートを作成します。

「DW 休止オブジェクト」レポートを使用して、「すべてのオブジェクト」グループに含まれるオブジェクトで、SELECT で使用されていないオブジェクトを表示します。

このレポートを、先の表名のレポートと比較します。 EMP は、SELECT ステートメントで使用されたため、このレポートには含まれていないことが分かります。

注: グループ・メンバーは一元管理され、中央マネージャーと管理対象ユニットとの間で同期されるため、このレポートの内容は最大で 30 分遅れる場合があります。最新の情報にアクセスする必要がある場合は、このレポートを中央マネージャーで実行するか、または Guardium 管理者に中央マネージャーから管理対象ユニットを同期するよう依頼してください。

表にアクセスするその他の方法

オブジェクトの間接的なマッピング

SELECT の直接アクセスのほか、表はストアード・プロシージャーおよび関数からアクセスされる場合があります。 この場合、Guardium でこれらの SELECT を評価できるようにするため、さらにマッピングが必要になります。

最初に、「DW EXECUTE オブジェクト・アクセス」レポートを使用して、「DW EXECUTE オブジェクト」グループに、実行されるストアード・プロシージャーの名前セットを入力します。続いて、間接マッピングを使用して、これらのプロシージャーから使用されるすべてのオブジェクトを生成します。

次のようにプロシージャーが定義されているとします。

```
create or replace procedure num_depts(deptnums out NUMBER) is
begin
    select count(*) into deptnums from dept;
end;
```

この場合、num_depts のすべての実行で DEPT の SELECT も行われます。

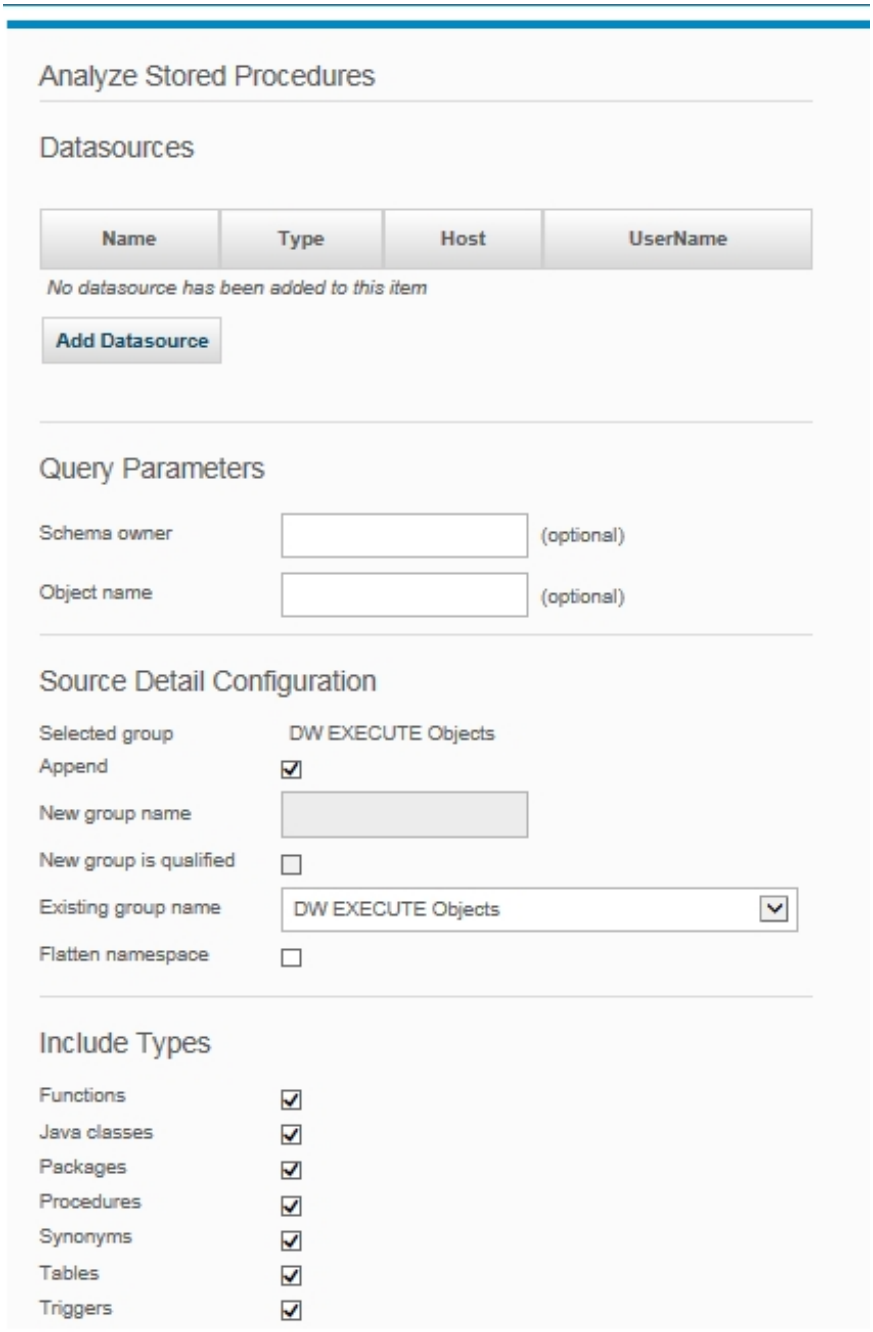
「照会からグループを取り込み」機能を使用し、「DW EXECUTE オブジェクト・アクセス」レポートの「オブジェクト名」の列を使用して「DW EXECUTE オブジェクト」グループを取り込みます。 次に、このグループを使用して「DW EXECUTE がアクセスしたオブジェクト」グループを取り込みます。

グループ・ビルダーで、リストから「DW EXECUTE オブジェクト」を選択して、「自動生成呼び出しプロシージャー」をクリックします。 「逆従属関係の使用」(Guardium 8 では Oracle についてのみサポートされています)、または「選択したオブジェクトの生成」を選択します。

従属関係を使用するよう選択した場合は、DBA_DEPENDENCIES にアクセス権のあるデータベースと、従う従属関係のタイプを選択する必要があります。

「DW EXECUTE がアクセスしたオブジェクト」グループへのメンバーの追加を選択します。

以下の例は、「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」 > 「DW EXECUTE がアクセスしたオブジェクト」 > 「自動生成呼び出しプロシージャー」 > 「逆従属関係の使用」 > 「ストアード・プロシージャーの分析」から使用できます。



構成 - 自動生成呼び出しプロシージャー、逆従属関係の使用

これにより、従属オブジェクトが「DW EXECUTE がアクセスしたオブジェクト」グループに追加されます。

親トピック: レポート

レポートから API 呼び出しを生成する方法

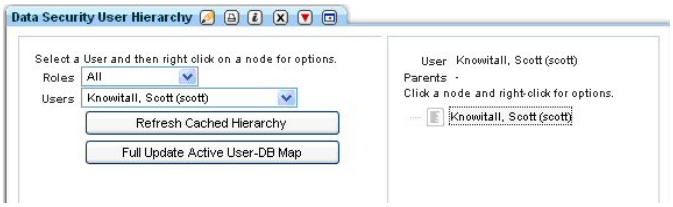
レポート内の単一行を使用して、またはレポート全体に基づいて、レポートから Guard API 呼び出しを生成します。

付加価値: レポートに表示されるシステムの既存データを API 呼び出しのパラメーターとして使用することにより、システム・レベルのコマンドを実行したり長い API 呼び出しを入力したりしなくても、GUI を使用して素早く簡単に API 呼び出しを生成しデータを設定できます。その結果、データ・ソースの作成や検査エンジンの定義、ユーザー階層の保守、あるいは S-TAP などの Guardium フィーチャーの保守などの操作を素早く実行できます。

単一行の API 呼び出し

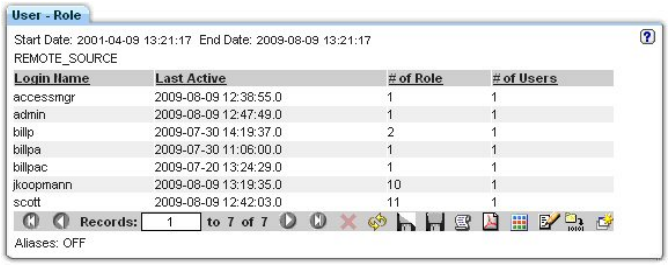
このシナリオでは、「ユーザー階層によるデータ・セキュリティー」にデータを設定するための API ファンクション・コールを生成します。

1. 最初に、ユーザー **scott** の現在の**「ユーザー階層によるデータ・セキュリティー」**

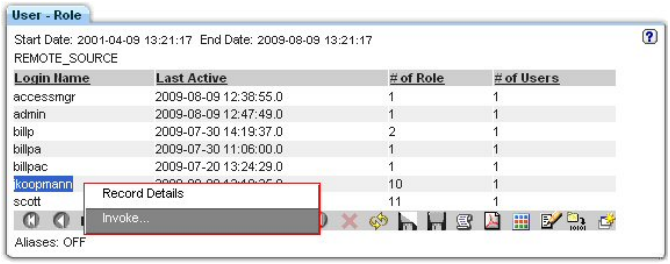


」を表示します。

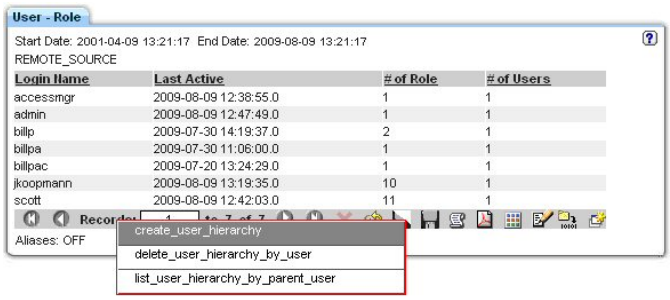
2. API 関数を呼び出すには、目的の API 関数が現在リンクされているレポートを見つける必要があります。 ユーザー階層の作成はユーザーに関連しているので、ユーザー・レポートを選択することが、よい結果をもたらします。 このシナリオでは、**「ユーザー - ロール」**レポートを選択しました。



3. **行をダブルクリック**してドリルダウンすると、 **「呼び出し...」**オプションが表示されます。

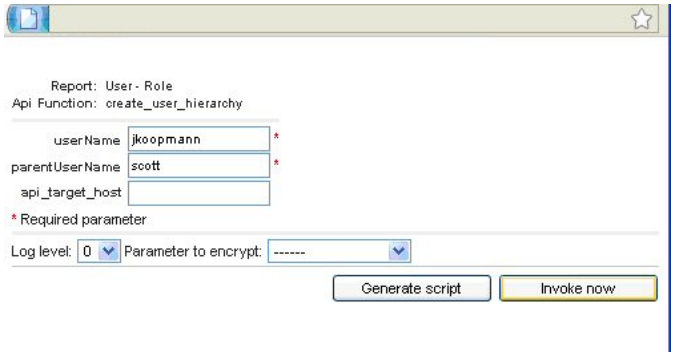


4. **「呼び出し...」**オプションをクリックして、 このレポートにマップされる API 関数のリストを表示します。



5. 呼び出す **API** をクリックします。 レポートと呼び出される API 関数の「API 呼び出しフォーム」が表示されます。

6. 選択した API 呼び出しの必須パラメーターを入力し、必須以外のパラメーターがあれば入力します。パラメーターの多くはレポートに基づいてあらかじめ入力されていますが、変更して固有の API 呼び出しを作成することもできます。必須のパラメーターと必須以外のパラメーターの入力については、 「GuardAPI リファレンス・ガイド」の個々の API 関数呼び出しを参照してください。

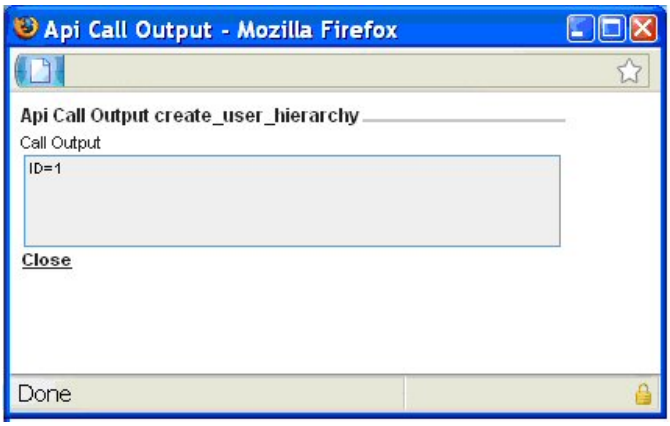


7. ドロップダウン・リストを使用して**ログ・レベル**を選択します。ログ・レベルの意味は、次のとおりです。0:「戻りコード」で定義されている ID=*identifier* と ERR=*error_code* を返します。1: 追加情報を画面に表示します。2: 情報を Guardium アプリケーション・デバッグ・ログに書き込みます。3: 両方の処理を行います。

8. ドロップダウン・リストを使用して**「暗号化するパラメーター」**を選択します。
注: パラメーター暗号化は共有パスワードを設定することによって有効になり、スクリプト生成を介して API 関数を呼び出す場合のみ該当します。

9. **「今すぐ呼び出し」**または**「スクリプトを生成」**を選択します。

   a. **「今すぐ呼び出し」**を選択すると、ただちに API 呼び出しが実行され、「API 呼び出し出力」画面に API 呼び出しの状況が表示されます。



   b. **「スクリプトを生成」**を選択した場合は、生成されたスクリプトを任意のエディターで開きます。後で編集して実行する場合は、ディスクに保存することもできます。スクリプトに空のパラメーター値 (「< >」で表記) が含まれている場合は、必要な値に置き換えてください。
   注: API 呼び出しでは、スクリプトの空のパラメーターは無視されるため、空のままにしておくこともできます。

      スクリプトの例

      # A template script for invoking guardAPI function create_user_hierarchy :

      # Usage: ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt

      # replace any < > with the required value

      #

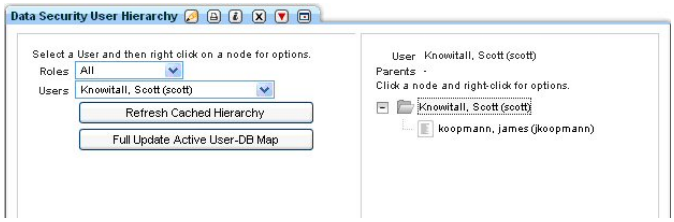
      grdapi create_user_hierarchy userName=jkoopmann parentUserName=scott

   c. CLI 関数呼び出しの実行

      呼び出しの例

      $ ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt

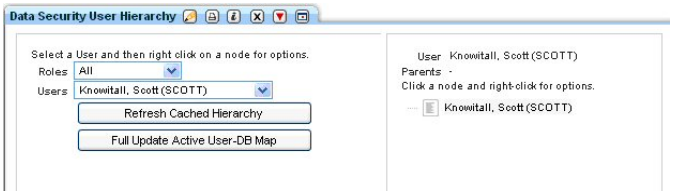
10. 検証します。このシナリオの場合は、「ユーザー階層によるデータ・セキュリティー」の再表示になります。



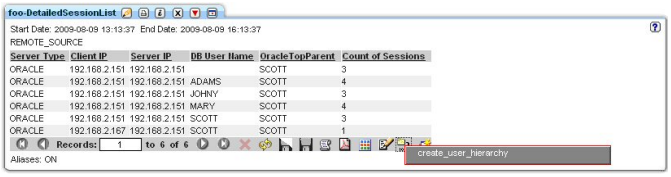
複数行の API 呼び出し

このシナリオでは、レポート・フィールドにパラメーターがマップされたカスタム・レポートを使用します。 追加情報については、このセクションで後述する追加シナリオを参照してください。

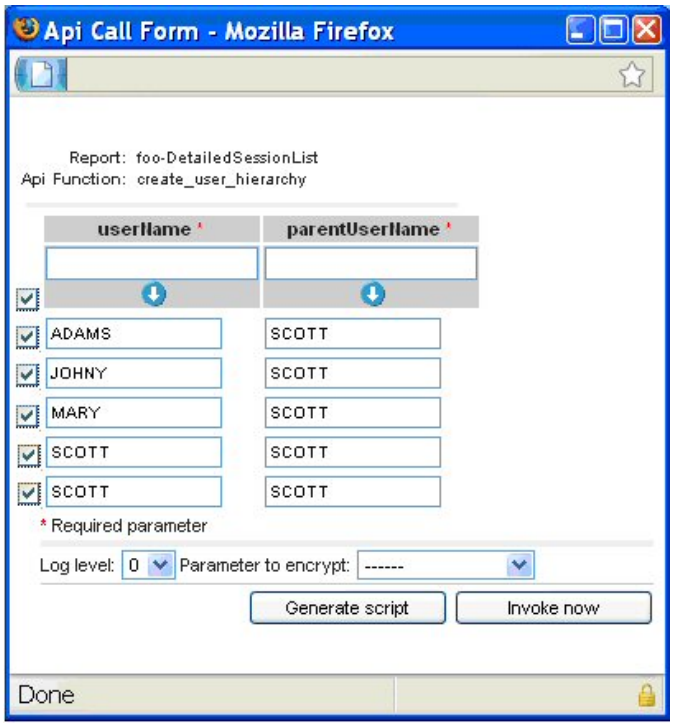
1. 始めに、ユーザー **scott** の現在の**「ユーザー階層によるデータ・セキュリティー」**を見てみましょう。



2. **「呼び出し...」**アイコンをクリックして、このレポートにマップされる API のリストを表示します。



3. 呼び出す **API** をクリックします。 レポートと呼び出される API 関数の「API 呼び出しフォーム」が表示されます。レポートから複数行を対象に API 呼び出しを起動すると「API 呼び出し形式」が生成されて表示され、画面に表示されたすべてのレコードを編集できるようになります。表示されるレコードはフェッチ・サイズによって異なり、最大で 20 です。



4. **チェック・ボックス**を使用して、API 呼び出しのターゲットになる行を選択/選択解除します。

5. 選択した API 呼び出しの**必須パラメーター**を入力し、 **必須以外のパラメーター**があれば入力します。パラメーターの多くはレポートに基づいてあらかじめ入力されていますが、変更して固有の API 呼び出しを作成することもできます。必須のパラメーターと必須以外のパラメーターの入力については、 「GuardAPI リファレンス・ガイド」の個々の API 関数呼び出しを参照してください。さらに、API 用パラメーターのセットを使用して、パラメーターの値を入力します。下矢印ボタンをクリックすると、すべてのレコードについてそのパラメーターのデータが設定されます。

6. ドロップダウン・リストを使用して**ログ・レベル**を選択します。ログ・レベルの意味は、次のとおりです。0:「戻りコード」で定義されている ID=*identifier* と ERR=*error_code* を返します。1: 追加情報を画面に表示します。2: 情報を Guardium アプリケーション・デバッグ・ログに書き込みます。3: 両方の処理を行います。

7. ドロップダウン・リストを使用して**「暗号化するパラメーター」**を選択します。
注: パラメーター暗号化は共有パスワードを設定することによって有効になり、スクリプト生成を介して API 関数を呼び出す場合のみ該当します。

8. **「今すぐ呼び出し」**または**「スクリプトを生成」**を選択します。

   a. **「今すぐ呼び出し」**を選択すると、ただちに API 呼び出しが実行され、「API 呼び出し出力」画面に API 呼び出しの状況が表示されます。階層に循環関係を持たせることができないため、このシナリオの最後の 2 つの API 呼び出しは失敗します。

   b. **「スクリプトを生成」**を選択した場合は、生成されたスクリプトを任意のエディターで開きます。後で編集して実行する場合は、ディスクに保存することもできます。スクリプトに空のパラメーター値 (「< >」で表記) が含まれている場合は、必要な値に置き換えてください。このシナリオの場合、スクリプトの最後の 2 行のために循環エラーが生じることがわかっているので、この 2 行をすぐに削除できます。
   注: API 呼び出しでは、スクリプトの空のパラメーターは無視されるため、空のままにしておくこともできます。

   スクリプトの例

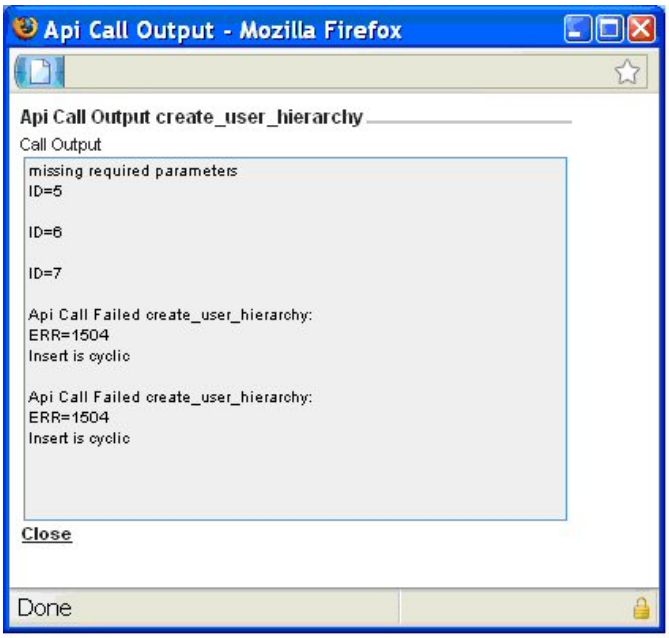
   # A template script for invoking guardAPI function create_user_hierarchy :

```
# Usage: ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt
# replace any < > with the required value
#
grdapi create_user_hierarchy userName=ADAMS parentUserName=SCOTT
grdapi create_user_hierarchy userName=JOHNY parentUserName=SCOTT
grdapi create_user_hierarchy userName=MARY  parentUserName=SCOTT
grdapi create_user_hierarchy userName=SCOTT parentUserName=SCOTT
grdapi create_user_hierarchy userName=SCOTT parentUserName=SCOTT
```

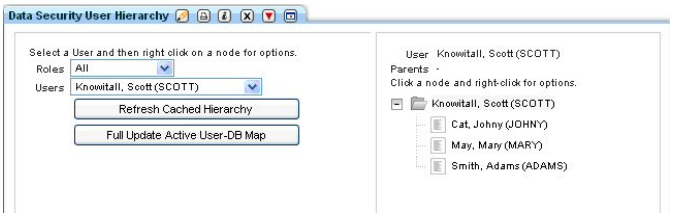
c. CLI 関数呼び出しの実行

呼び出しの例

```
$ ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt
```



9. 検証します。このシナリオの場合は、「ユーザー階層によるデータ・セキュリティー」の再表示になります。



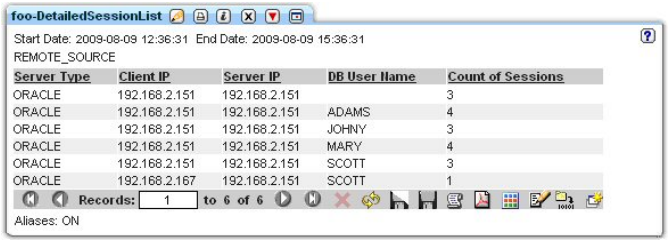
親トピック: レポート

API 呼び出しで定数を使用する方法

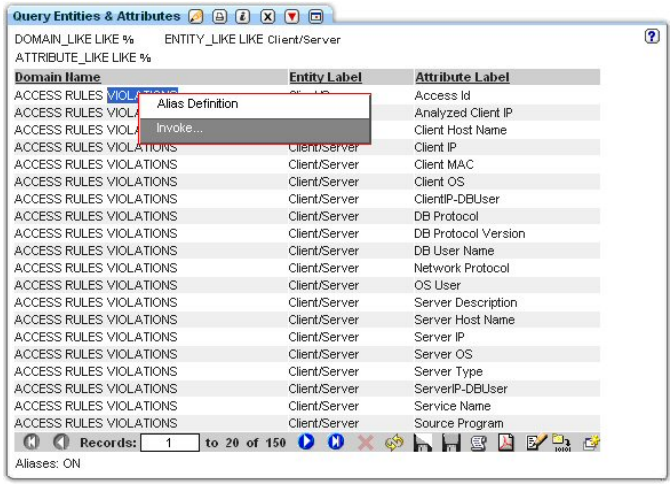
API 関数の呼び出し時に使用する新しいエンティティー属性を作成します。

付加価値: GUI を使用して、API 関数呼び出しでパラメーターの入力に使用できるユーザー定義の定数を作成します。

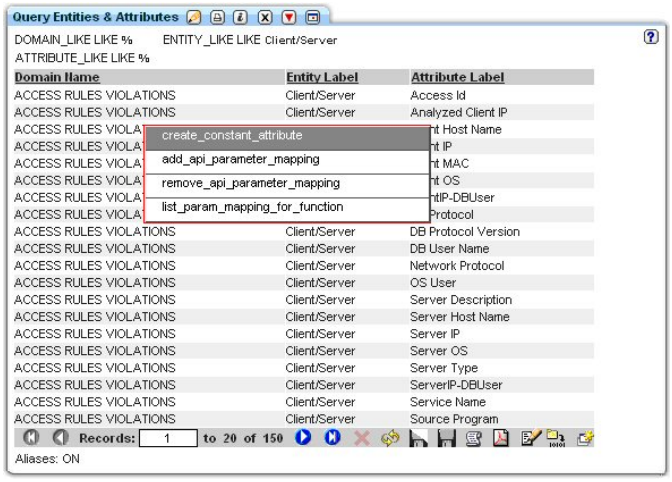
1. このレポートから、パラメーターのマッピングに使用できるフィールドを持つように、これを変更することができます。



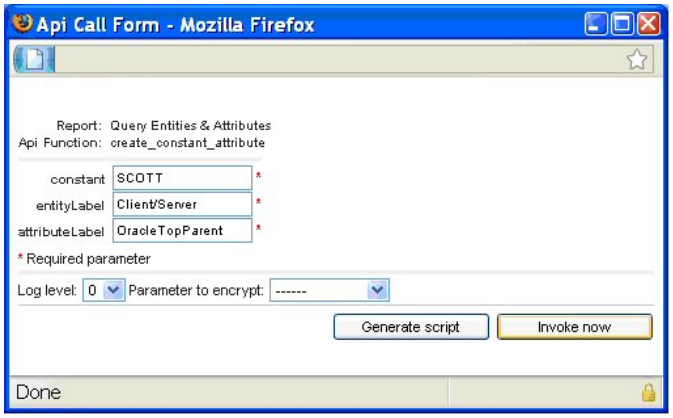
2. ACCESS RULES VIOLATIONS ドメイン内の「クライアント/サーバー」エンティティーの「照会エンティティーと属性」レポートに移動します。 行をダブルクリックして、「呼び出し...」オプションを選択します。



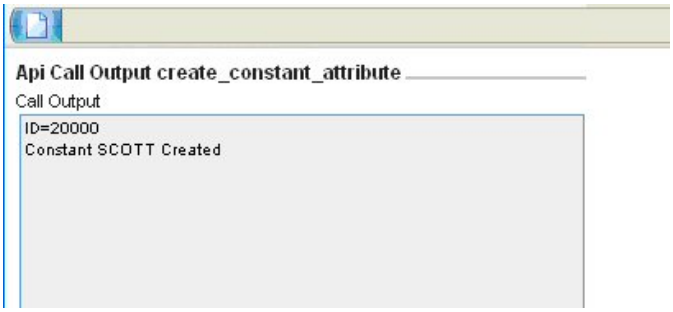
3. API 関数 create_constant_attribute を呼び出します。



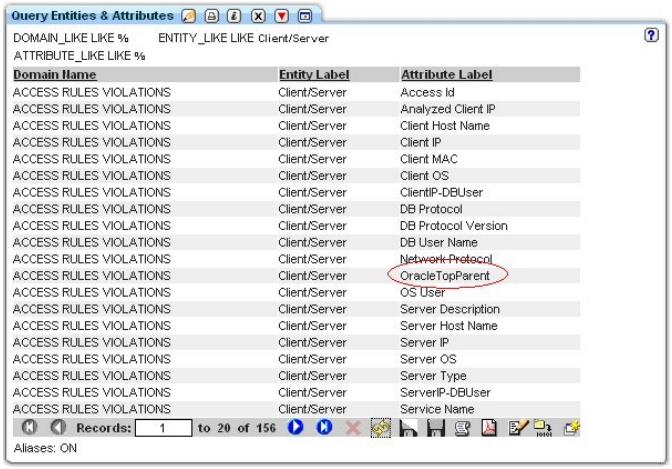
4. 使用する定数値 (「SCOTT」) を入力し、名前を付ける attributeLabel (「OracleTopParent」) を入力してから、「今すぐ呼び出し」ボタンをクリックして定数を作成します。



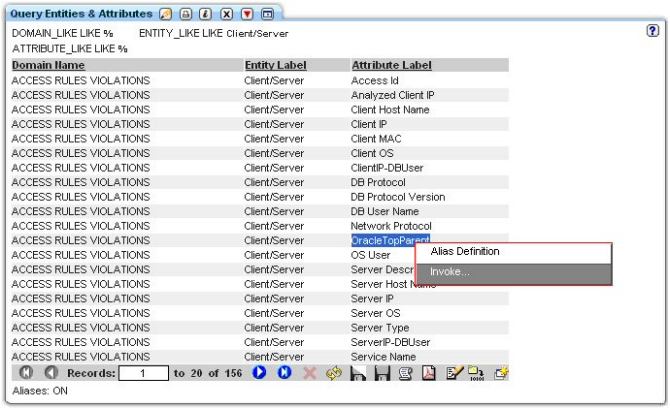
5. 「今すぐ呼び出し」ボタンをクリックすると、定数が作成されたことを示す「API 呼び出し出力」状況が生成されます。



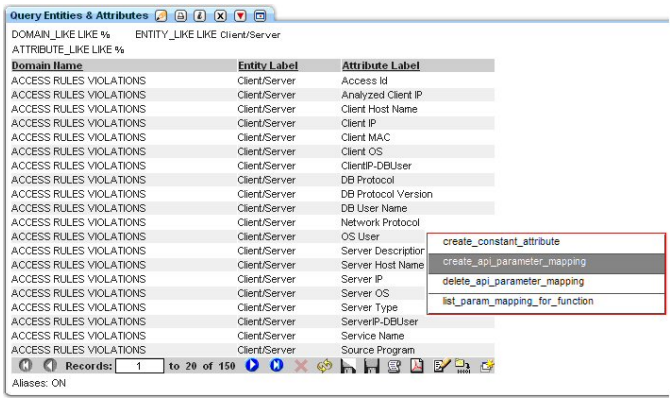
6. 「照会エンティティーと属性」レポートが再表示されて、作成された新規属性が表示されます。



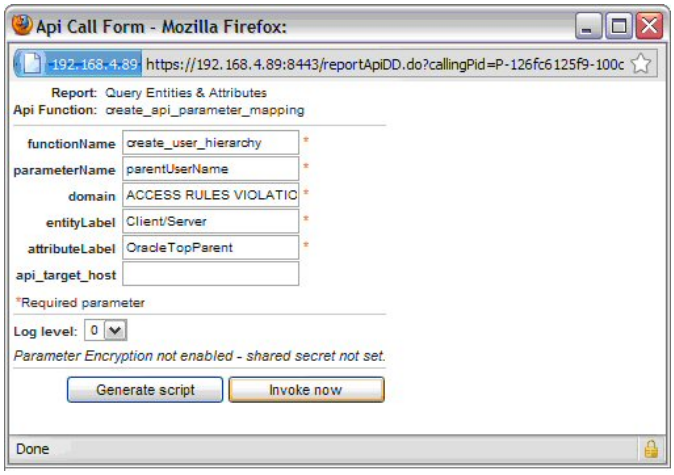
7. 次に、新規に作成された定数をレポート用にマップできます。 新規行をダブルクリックして、「呼び出し...」オプションを選択します。



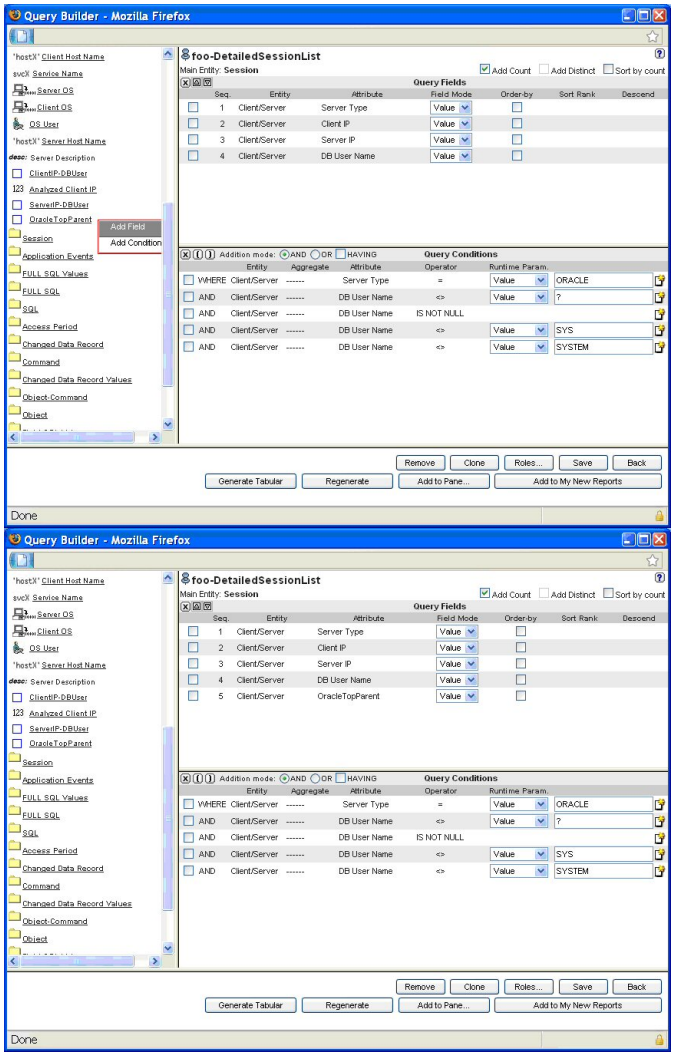
8. create_api_parameter_mapping オプションを選択します。



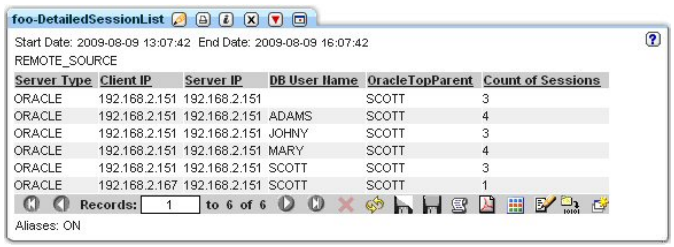
9. functionName と parameterName を入力して、「今すぐ呼び出し」ボタンをクリックします。



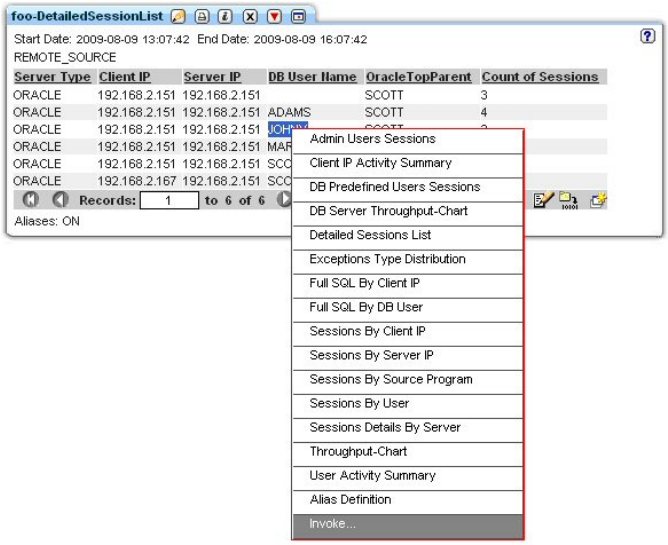
10. 新しく作成した属性はレポートに追加する必要があります。 クエリー・ビルダーを使用して照会を編集し、フィールドを追加します。



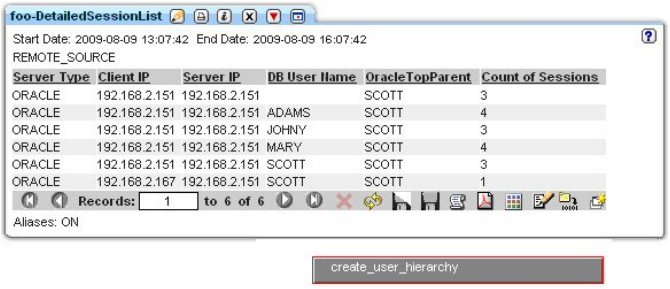
11. 次に、レポートが表示されると、新規属性が表示されます。



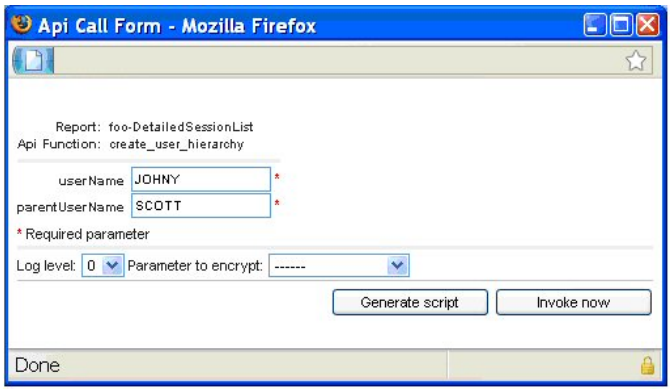
12. 新規定数の使用法を検証するには、行をダブルクリックして「呼び出し...」オプションを選択します。



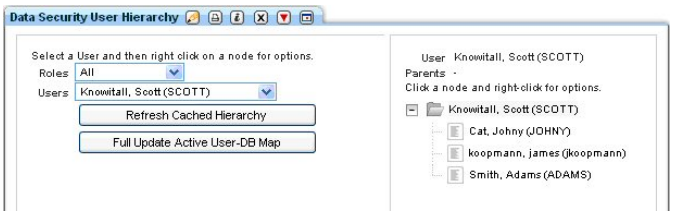
13. API 関数を選択します。



14. 次に、新規に追加した定数から parentUserName が取り込まれます。 「今すぐ呼び出し」ボタンをクリックします。



15. 新規の「データ・セキュリティー・ユーザー階層」を検証します。



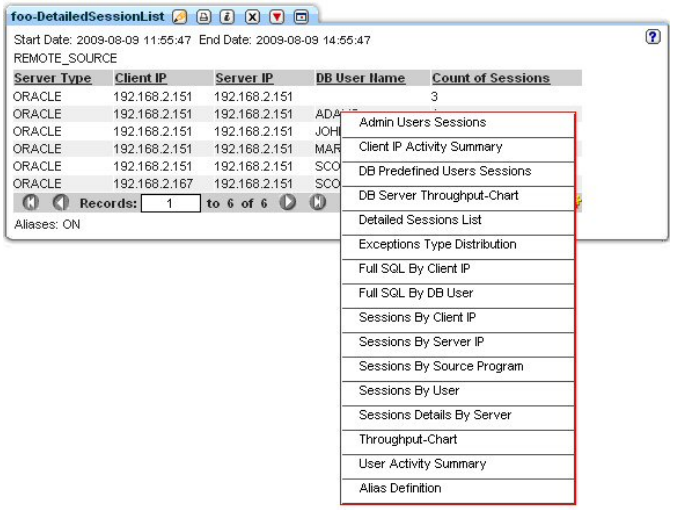
親トピック: レポート

カスタム・レポートから API 呼び出しを使用する方法

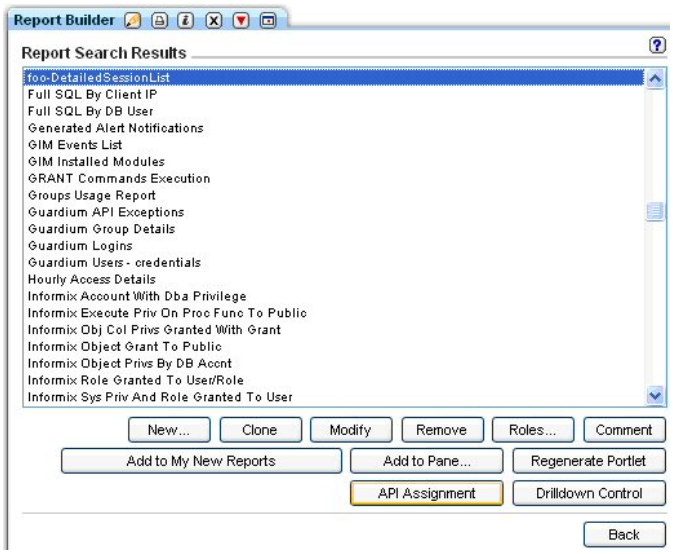
API 関数をレポートにリンクし、レポートの各フィールドを API 関数のパラメーターにマップします。

付加価値: GUI を介して、API 関数呼び出しで使用するカスタム・レポート・フィールドに API パラメーターを迅速かつ簡単にマップします

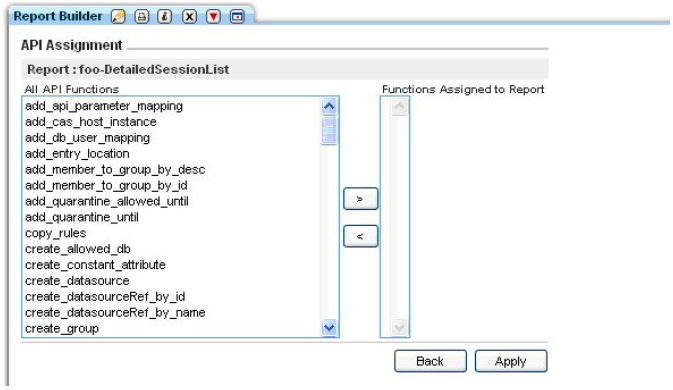
1. デフォルトでは、新しく作成したカスタム・レポートには API 関数はリンクされていません。 これは、以下のカスタム・レポートで表示できます。このレポートの行をダブルクリックすると、実行される追加のドリルダウン・レポートのリストのみが生成されますが、「呼び出し」オプションは含まれていません。



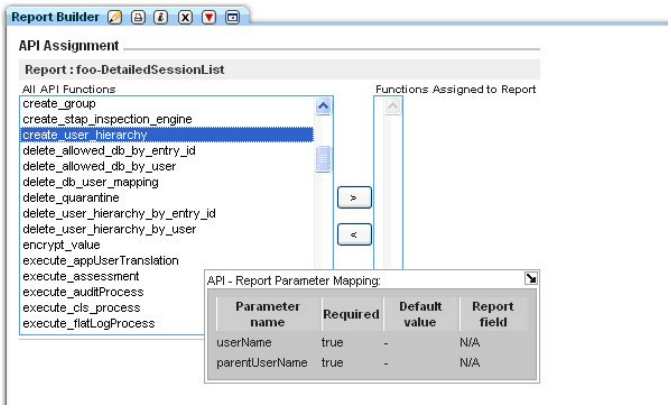
2. レポートへの API 関数のリンクは、Guardium のレポート・ビルダーから行います。レポート・ビルダーを開き、ご使用のカスタム・レポートを見つけてから、「API 割り当て」ボタンをクリックします。



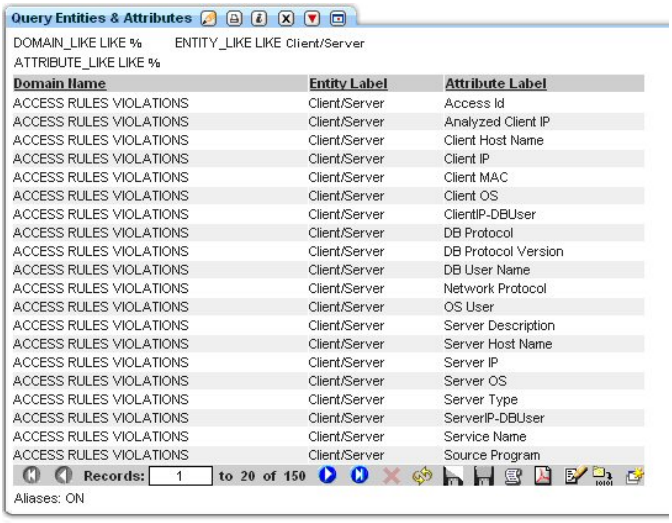
3. 「API 割り当て」パネルには、選択したレポートに割り当てられたすべての API 関数が表示されます。このシナリオでは、選択したレポートには API 関数は割り当てられていないことに注意してください。



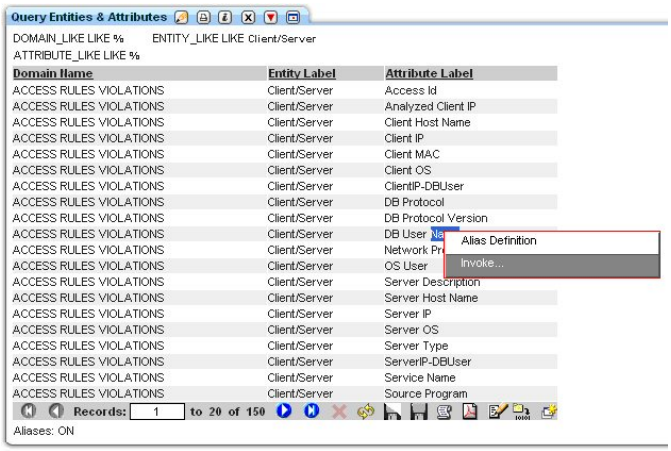
4. API 関数をレポートに割り当てるため、レポートにリンクする API を見つけ、「>」をクリックして「適用」ボタンをクリックします。 このシナリオでは、create_uer_hierarchy を選択しました。 選択すると、パラメーター・マッピング (API 関数呼び出しの際にどのレポート・フィールドが使用されるか) が表示されたポップアップ・ウィンドウが表示されます。 パラメーター名にマップされたレポート・フィールドはないことに注意してください。



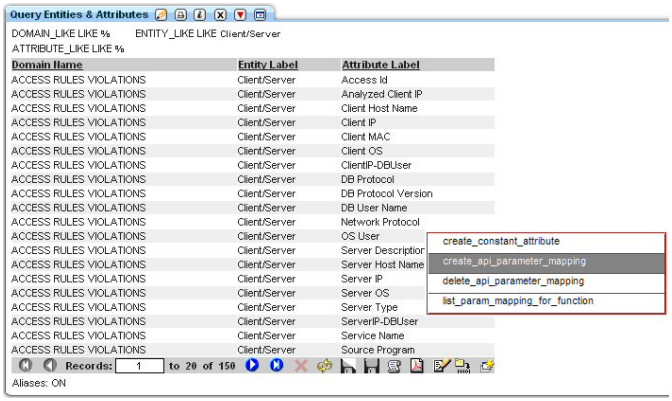
5. この時点では、どのレポート・フィールドも API パラメーターにマップされていません。 ユーザーは、「照会エンティティーと属性」レポートに移動してこれらのマッピングを作成できます。 これを行わない場合、API 呼び出しを行ったときに、どのパラメーターにも値はありません。 API パラメーター・マッピングを追加します。 「照会エンティティーと属性」レポートを開いて、マッピングを作成します。 このシナリオのレポートでは、ACCESS RULES VIOLATIONS ドメイン内では「クライアント/サーバー」エンティティーを使用するので、「カスタマイズ」ボタンを使用してレポートをフィルタリングし、「クライアント/サーバー」エンティティーのみを表示するようにレポートを変更します。



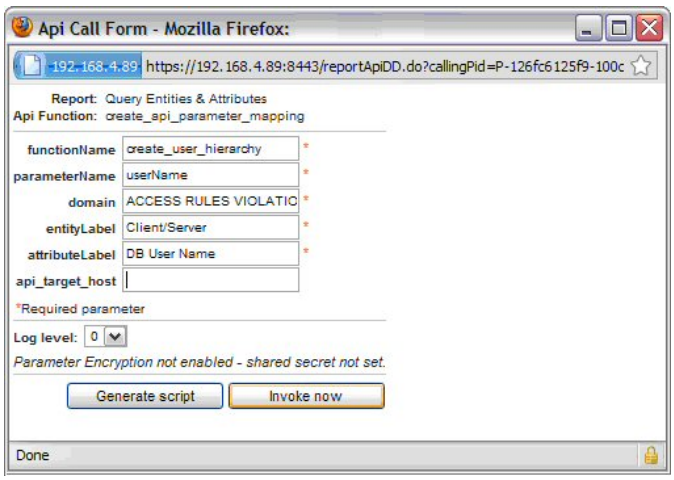
6. パラメーター名に割り当てる属性をダブルクリックして、「呼び出し...」オプションをクリックします。



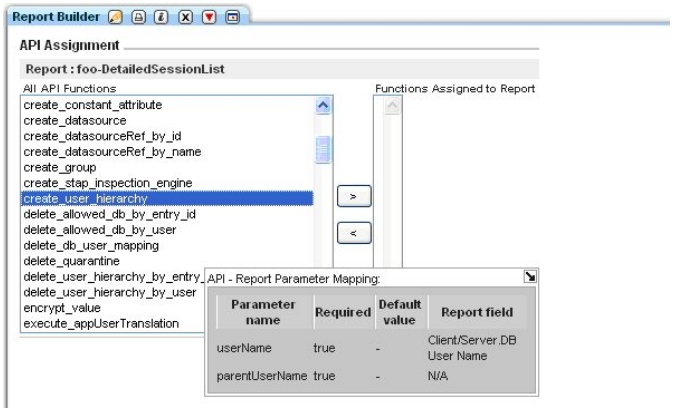
7. create_api_parameter_mapping API 関数を選択します。



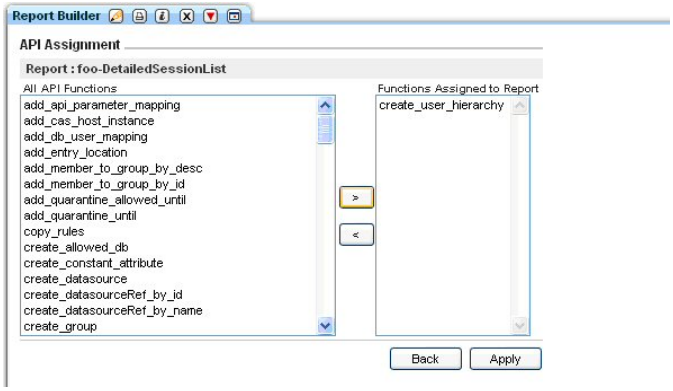
8. 「API 呼び出し形式」に functionName と parameterName を入力し、「今すぐ呼び出し」ボタンをクリックします。



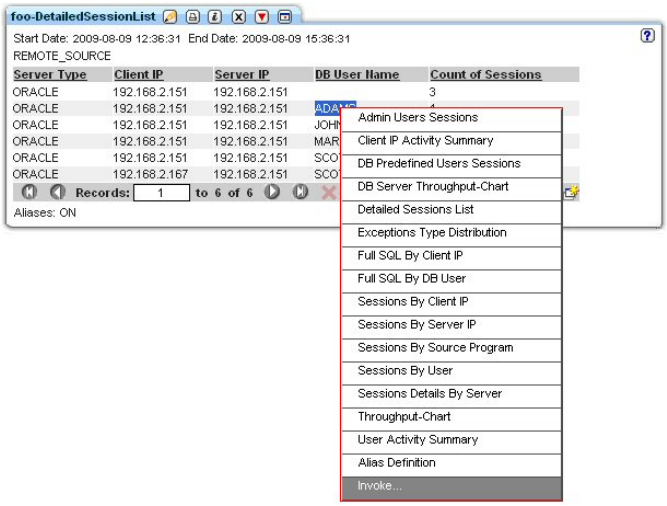
9. レポート・ビルダーの先ほどのレポートに戻って、「API 割り当て」を確認します。「create_user_hierarchy」API 関数をクリックして、レポート・マッピングを表示します。「UserName」が「クライアント/サーバー・データベース名」レポート・フィールドにマップされています。



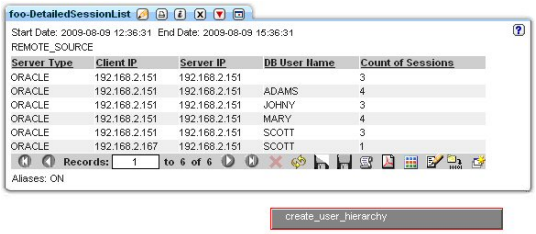
10. 「>」をクリックして「適用」ボタンをクリックします。



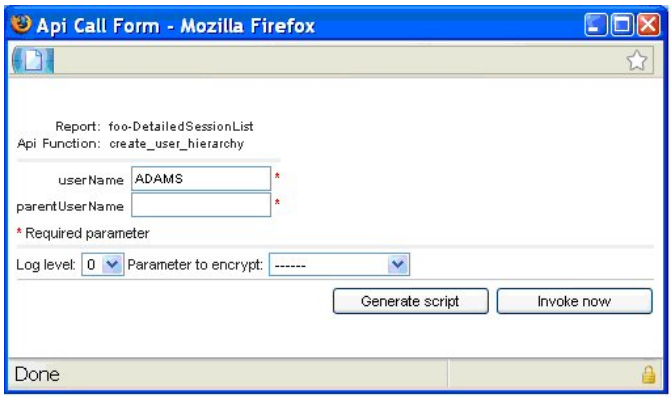
11. 次に、このレポートを介して create_user_hierarchy API 関数を呼び出すと、パラメーター userName がレポートから取り込まれます。 これを確認するには、レポートに戻って行をダブルクリックしてから、「呼び出し...」オプションをクリックします。



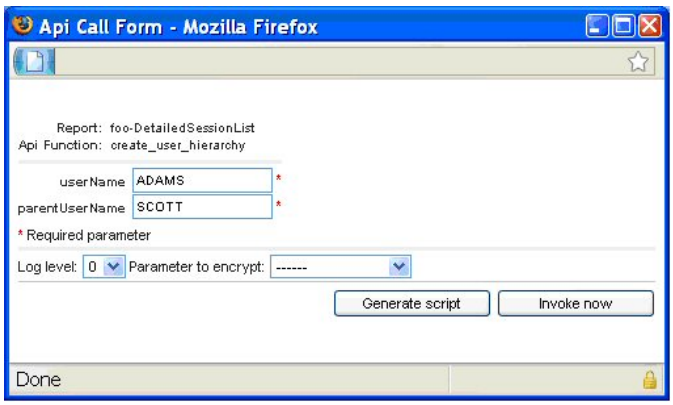
12. API 関数 (この場合は create_user_hierarchy) をクリックします。



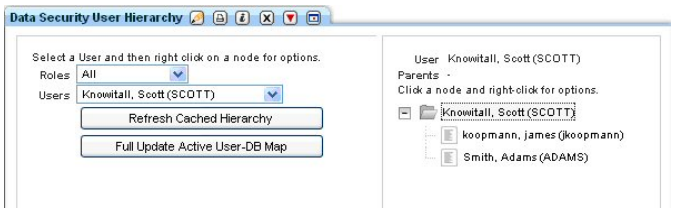
13. userName はすでにレポート・フィールドから取り込まれていることに注意してください。



14. parentUserName を入力して「今すぐ呼び出し」ボタンをクリックします。



15. 新規の「データ・セキュリティー・ユーザー階層」が追加されていることを確認してください。



親トピック: レポート

オプションの外部フィード

外部フィードを使用すると、Guardium レポート・データを外部データベースに直接送信できます。

レポート・データを外部データベースに送信することは、いくつかのシナリオで役に立ちます。例えば、Guardium データを非 Guardium データと結合または関連付ける場合や、外部レポート・ツールで Guardium データを使用する場合、あるいは、特に大規模なレポートでレコードのマシン構文解析を行う場合です。

外部フィードを使用する前に、以下の前提条件を確認してください。

- Guardium と外部データベースの間のフィードをマップします。外部フィードは、現在はリレーショナル・データベースをサポートしており、他のデータベース・タイプでは機能しない可能性があります。
- 外部フィード経由で送信するデータを定義するレポートを作成します。 事前定義レポートは、外部フィードでは動作しません。事前定義レポートを使用したい場合は、レポートのコピーを作成し、そのコピーを外部フィードに使用します。
- 外部フィードを使用する監査プロセスを定義します。

オプションの外部フィード・タスクが初めて実行されるときに、必要な監査ソースの内部表現が作成されます。 監査ソースの作成日よりも前の日付のタイム・スタンプがあるデータは保管できない、という制限が 1 つあります。 つまり、タスクが初めて実行されるとき、現在日付のデータのみがエクスポートされるという意味です。 その日付の後に続いてタスクを実行すると、その日付以降のすべてのデータをエクスポートできます。(言い換えれば、翌日は、その日のデータに加えて前日のデータもエクスポートできます。)

「オプションの外部フィードの作成」タスク

コンプライアンス・ワークフロー自動化プロセスの定義をまだ開始していない場合は、この手順を実行する前に、『ワークフロー・プロセスの作成』を参照してください。

1. 「新規タスクの追加」ペインが開いていない場合、「監査タスクの追加」をクリックします。
2. 「外部フィード」をクリックします。
3. 「フィード・タイプ」リストからフィード・タイプを選択します。(次に表示されるコントロールは、選択したフィード・タイプに応じて異なります。) 事前定義フィード・タイプの 1 つは、「最後に参照されたオブジェクト」です。
   注: この機能を使用する前に、外部フィードをマップする必要があります。
4. 「イベント・タイプ」リストから、イベント・タイプを選択します。
5. 「レポート」リストからレポートを 1 つ選択します。選択したレポートに応じて、「タスク・パラメーター」ペインに表示されるパラメーターの数が異なります。
6. 「抽出ラグ」ボックスにフィードが遅延される時間数を入力し、「継続」ボックスにマークを付けて監査タスクが実行される直前の時間までのデータを組み込みます。抽出ラグは、「継続」ボックスにマークが付いている場合のみ動作します。
7. 「データ・ソース」ペインで、外部フィードの 1 つ以上のデータ・ソースを指定します。 データ・ソースの定義または選択手順については、『データ・ソース』を参照してください。
8. 「タスク・パラメーター」ペインに、すべてのパラメーター値を入力します。 パラメーターは、選択したレポートに応じて異なります。カウント列は、外部フィードではサポートされません。
9. 「適用」をクリックします。

親トピック: レポート
関連概念:
監査プロセスの作成
関連タスク:
外部フィードのマッピング

外部フィードのマッピング

外部フィードをマップして、Guardium レポート・データを外部データベースに直接送信する方法について説明します。

始める前に

外部フィードをマップする前に、以下の前提条件を確認してください。

- フィードからデータを受信する外部データベースを特定し、そのデータベースに必要な接続情報 (IP アドレス、ポート番号、ユーザー名、パスワードなど) を収集します。外部フィードは、現在はリレーショナル・データベースをサポートしており、他のデータベース・タイプでは機能しない可能性があります。
- 外部フィードにデータを提供する Guardium レポートを特定します。
-

このタスクについて

外部フィードを使用すると、Guardium レポート情報を外部データベースに直接送信できます。レポート内に定義できるものはすべて外部フィード経由で送信できます。これらのフィードは、Guardium のレポート・メカニズムから外部データベース上の表フィールドへの DOMAIN_ID および ATTRIBUTE_ID のマッピングに依存しています。各マッピングは、4 つの表 (EF_MAP_TYPE_HDR、EF_MAP_TABLE、EF_MAP_COLUMN、および EF_MAP_GDM_TYPE) 内のレコードから成っています。grdapi_create_ef_mapping 関数を使用すると、これらの表を作成しマッピングを設定することができます。

手順

1. 外部フィードを使用して転送したいデータを含むレポートを生成します。必要なレポート・データにシステムがアクセスできる場合は、中央マネージャー、アグリゲーター、またはスタンドアロン Guardium インスタンスからこの操作を実行できます。
2. CLI から、`grdapi create_ef_mapping reportName="My report"` を実行します。grdapi_create_ef_mapping 関数は、マッピングを設定するだけでなく、後続のステップで使用される create table ステートメントのサンプルも生成します。
3. レポートが定義される Guardium システム上の /var/log/guard で、ef_sample_[my_report].sql などのファイル名を検索します。このファイルには、create table ステートメントの例が含まれています。 外部データベースの要件に合うようにこのファイル内のステートメントを変更する必要があります。ファイルを変更した後、外部データベースに対してステートメントを実行して、ターゲット表を作成します。
4. これで外部フィードは、監査プロセス・ビルダーを通して定義されたワークフロー・プロセス内で使用できます。追加情報については、オプションの外部フィードの資料を参照してください。

親トピック: レポート
関連概念:
オプションの外部フィード

配布レポート・ビルダー

この中央マネージャー機能により、特定の中央マネージャーに関連付けられているすべてまたは一部の Guardium 管理対象ユニットから、データを自動的に収集することができます。配布レポートは、概要ビューの提供、データ・ソース間のデータの関連付け、およびデータのビューの要約を行うように設計されています。 コレクター間での行レベル・データ収集については、引き続きアグリゲーターを使用します。

複雑なエンタープライズ環境では、特定のレポートで必要になるデータが存在する管理対象ユニットをユーザーが必ずしも正確に知っているわけではない場合に問題が発生する可能性がありますが、この機能により、こうした問題を軽減することができます。この問題は、ロード・バランシングなどの構成オプションに基づく Guardium のコレクターとデータベース間のリンクの時間経過に伴う変化によって発生する場合があります。この問題は、アグリゲーターとコレクターの期間やデータ保存ポリシーなどの考慮事項によってさらに複雑なものになります。

配布レポートは、簡単に作成できます。「配布レポート」画面で配布レポートを定義して任意のペインに追加するだけで、すぐに使用できるようになります。

また、この機能は、中央マネージャー上のデータマートをオプションで使用して、長期的に統合データの収集をスケジュールできるようにします。要するに、配布レポートのデータはフラット・テーブルとして中央マネージャー上に保管されるため、必要なレポートを作成する際に、複雑な結合処理を行う必要はありません。これにより、これらのエンタープライズ・レポートの応答時間が大幅に短縮されます。

配布レポートのデータは、コレクターおよびアグリゲーター、さらには中央マネージャーからも収集することができます。レポートのデフォルトの配布バージョンには、対象データを管理するユニットのホスト名が含まれます。

以下に、事前定義されている配布レポートを示します。

- エンタープライズ S-TAP 検査
- 統合/アーカイブ・ログ
- 失敗したユーザー・ログイン試行
- スケジュールされたジョブの例外

配布レポートの実行: 即時実行またはスケジュールによる実行

配布レポートを定義する際、レポートを即時に実行するか、または、レポートをバックグラウンドで実行するようにスケジュールして、中央マネージャーに結果を収集します。

- 即時: このモードでは、オンデマンド (GUI を使用して実行) でデータが収集され、関連する管理対象ユニットから結果が収集されると共に、結果が表示されます。配布レポートには、データがまだ転送中であるのか、あるいは特定の管理対象ユニットからすべてのデータを受信したのかを示す状況インディケーターが含まれます。このモードの場合、データは中央マネージャーには保存されません。レポートを閉じると同時に、データが消去されます。
- スケジュール済み: このモードでは、すぐに応答を返すことができるよう、事前にデータが収集されます。スケジューラーで指定した時間間隔に従い、指定された管理対象ユニットの関連するすべての統合データが中央マネージャー・マシン上の指定されたデータマート表に送信され、この表に対するデフォルトのレポートが作成されます。この表には、その独自のドメインとエンティティーも含まれており、クエリー・ビルダーを使用して追加のクエリーとレポートを作成することができます。これらのレポートを監査プロセスに追加して、プロセスを定期的に実行することができます。また、プロセスの結果を、レビューまたはサインオフのためにロール、ユーザー、ユーザー・グループに割り当てることができます。

配布レポートを計画する場合の考慮事項

- 32 ビットの中央マネージャーと 64 ビットの管理対象ユニットが存在する混合環境の場合、64 ビット・システムの情報は配布レポートには表示されません。この場合に情報を表示するには、中央マネージャーを 64 ビットにアップグレードする必要があります。
- 中央マネージャーに送信されるデータを調整する必要があるため、すべての管理対象ユニットのクロック時刻を、目的の管理対象ユニットが存在するタイム・ゾーンの現在時刻に設定しておくことが非常に重要です。中央マネージャーと管理対象ユニットの時間が10 分違っているだけでも、配布レポートのパフォーマンスと信頼性に影響します。
- スケジュール済み配布レポートの定義はエクスポートおよびインポートできますが、即時配布レポートの定義はエクスポートすることもインポートすることもできません。エクスポートおよびインポートされた定義には、スケジュール自体は含まれません。バックアップ用の中央マネージャーやテスト用の中央マネージャーなど、他のシステム上で再作成する必要がある場合は、定義とスケジューリングのレコードを保持することをお勧めします。システム・バックアップには、配布レポートの構成情報が含まれます。
- アグリゲーターとコレクターの両方からレポート・データを収集するように指定した場合、デフォルトの配布レポートに重複データが含まれることがあります (ただし、Guardium のホスト名は異なります)。 この場合、配布レポートの構成に対して、コレクターとアグリゲーターのいずれかのみを指定することを特にお勧めします。

- 配布レポートは、配布レポート以外の既存のレポートに基づいています。 スケジュール・モードで配布レポートを定義する際に、元の照会にランタイム・パラメーターが指定されている場合は、それらのパラメーターの値 (または、ワイルドカードの「%」) を指定するための画面が表示されます。
- 以前は使用していなかったデータベース内の中央マネージャー上のデータを使用することになるため、それを考慮して計画する必要があります。そのため、パージ、アップグレード、バックアップについて、運用方法の変更を計画する必要があります。

配布レポートの作成

配布レポートの作成は、中央マネージャーとして構成されているアプライアンスでのみ実行することができます。管理者としてログインして配布レポート・ビルダーにアクセスするには、「レポート」 > 「レポート構成ツール」 > 「配布レポート・ビルダー」に移動します。

配布レポート・ビルダーで、既存のレポートのリストからレポートを選択して構成を変更することも、レポートを任意のペインに追加することも、「新規」をクリックして新しい配布レポートを作成することもできます。通常は、中央マネージャー上の既存のレポートを即時に配布するか、スケジュールして実行することができます (あるいは、その両方)。

新しい配布レポートの作成

レポート・ビルダーで「新規」を選択し (レポート・ビルダー内の既存のデータがすべてクリアされます)、「レポートに基づく」プルダウンで、配布用に使用できる既存のレポートを 1 つ選択します。リスト内の各レポートは、「即時」と「スケジュール済み」としてそれぞれ 1 回ずつ配布することができます。 即時配布として定義されている配布レポートは、配布レポート名に「(即時)」という用語が付加されています。

配布レポートを 1 つ作成するには、既存のレポートを 1 つ選択します。

ビルダーの「データ収集元」セクションで、「すべての管理対象ユニット」(中央マネージャーで管理されているユニット) を選択するか、特定のグループまたは管理対象ユニット (あるいはその両方) を指定します。

注: 管理対象ユニット・グループは、中央マネージャーで定義できます。グループの例としては、コレクター・グループとアグリゲーター・グループ、アプリケーションに基づくグループ、責務に基づくグループ、地域に基づくグループなどがあります。

ビルダーの「動作モード」セクションで、レポートの動作モードを選択します。

- 即時: ユーザーの要求時にレポートが実行されます。このオプションを選択した場合は、考慮する追加のオプションはありません。「適用」をクリックすると、変更内容を保存できます。続いて必要に応じて「ペインに追加」をクリックすると、レポートを GUI に追加できます。
- スケジュール: 事前にデータの準備と収集を行うバッチ処理が実行されます。

スケジュールされたレポート・オプションで、以下の追加の値を指定します。

- 時間間隔: データマートをキャプチャーする時間間隔を指定します。データマート抽出は、次の時間間隔の境界で実行され、指定された時間間隔をカバーします。細分度が日数のデータマート抽出は、午前零時に開始し、X 日ごとに実行されます。細分度が時間単位のデータマート抽出は、次の時間の境界で開始し、X 時間ごとに実行されます。細分度が分単位のデータマート抽出は、次の X 分の境界で開始し、X 分ごとに実行されます。例えば、「失敗したログインの数 (Count Of Failed Logins)」レポートの「時間間隔」の値を 1 時間に指定すると、カウントは、失敗したログインの 1 時間ごとの統合に基づくことになります。
- 次の経過後にパージ: データマート内にレポート・データを保存しておく期間を指定します。この期間が経過すると、データが自動的にパージされます。
- ランタイム・パラメーター: 配布レポートのベースとなるレポートに応じて、ランタイム・パラメーターを指定する必要があります。これらのフィールドの有効な値を確認するには、元のレポートの照会を調べるか、ワイルドカードの「%」を指定します。

「適用」をクリックします。配布レポートの構成のシステムによる保存が完了すると、「スケジュールの変更」と「ロール」がアクティブになります。

スケジュールを作成するには、「スケジュールの変更」をクリックして汎用スケジューラーに移動します。

スケジュール定義は管理対象ユニットにプッシュダウンされ、統合データを中央マネージャーに送信するタイミングと頻度が各管理対象ユニットに対して指示されます。

対象の配布レポートを表示できるロールを指定するには、「ロール」をクリックします。

既存の配布レポートの変更

既存の配布レポートでは、以下の操作を行うことができます。

- 構成 (管理対象ユニット、スケジュールの詳細、ランタイム・パラメーターなど) を変更する。
- レポートをダッシュボードに追加する。
- 配布レポートを削除する。
- 既存の即時レポートをベースとするスケジュールされたレポートを作成する。このオプションでは、即時レポートが置き換えられます。既存のスケジュール済みレポートから即時レポートを作成することはできません。

既存のレポートを選択するには、テキスト検索ボックスを使用するか、既存のレポートのリストをスクロールして、変更したいレポートを選択します。

配布レポートの表示

配布レポートには、以下に示す追加の列が含まれています。

- ソース: データの収集元となった Guardium システム。
- TZ: タイム・ゾーン (Guardium システムは、中央マネージャーとは異なるタイム・ゾーンの地域に配置される可能性があるため)。
- 日付: この列には、スケジュールされたレポートの開始期間の日時が表示されます。時間/日に従って結果をグループ化することができます。「即時」モードの場合、この列には開始時刻が表示されますが、この列は有意な列ではありません。
  注: 許可されている日付フィールドの最大個数は 3 です。

編集および更新

配布レポートの場合、ベース・レポートを編集して更新し、更新後のレポート構造に基づいて配布レポートを更新します。

ベース・レポートの列を変更するか、ベース・レポートの Where 節を追加または削除してから、レポートを保存して再生成した場合、この更新後のレポートに基づいて配布レポートを更新するには、既存の配布レポートで「レポート変更の保存」をクリックします。これだけで、変更が適用されます。

既存のレポート・パラメーターを更新する場合は、最初に「レポート変更の適用」をクリックし、パラメーターの値を更新してから「レポート変更の保存」をクリックする必要があります。これで、更新が適用されます。

時刻の詳細

レポートを実行する際に、レポート・カスタマイザーを使用して、照会の絶対時間枠 (from 3-31-2014 8:00am to 3-31-2014 11:00am) または相対時間枠 (NOW -3 HOUR) を指定することができます。

絶対時間を指定した場合、各 Guardium システムは現地時間に基づいて稼働します。例えば、配布レポートが東部標準時 (EST) の Guardium システムと太平洋標準時 (PST) の Guardium システムからデータを収集する場合、各システムは現地時間に基づいて照会を実行します。この例は (午前中のピーク時間帯、深夜の時間帯、特定の絶対時間を確認する場合に便利です)、ニューヨークに存在するシステムは東部標準時の 08:00 から 11:00 までの結果を収集し、カリフォルニアに存在するシステムは、太平洋標準時の 08:00 から 11:00 までの結果を収集します。

相対時間を指定した場合、各システムは、システムの現在時刻に従って「NOW -N」を実行します。これは、リアルタイム・レポートの場合に重要になります。リアルタイム・レポートおよびリアルタイムに近いレポートの場合、絶対時間を使用することはできません。リアルタイムでモニターを行う場合は、「即時」モードを使用してください。

配布レポートの状況の確認

各配布レポートには、結果の取り込みに成功したマシンと失敗したマシンを示す状況レポートが付属しています。GUI で配布レポートにナビゲートすると、状況レポートにアクセスするためのリンクが強調表示されます。

スケジュールされたレポートの場合、状況レポートの任意の行をクリックすると、特定のユニット上でレポートを再実行するための API を実行することができます。

スケジュール・モードでの配布レポートの特定の実行でエラーが発生した場合、以下の手順により、状況レポートからレポートを再実行することができます。

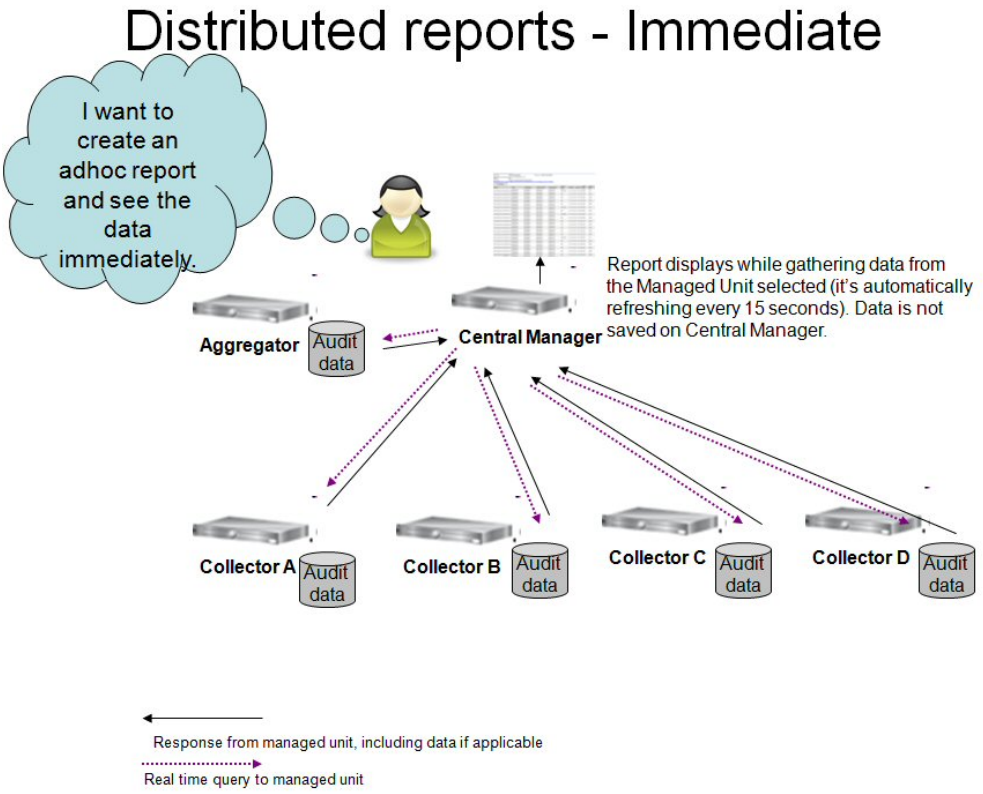
1. 状況レポートのいずれかの行をダブルクリックして「呼び出し」メニューを表示します。次に、「呼び出し」をクリックします。
2. 選択項目の「rerun_distributed_report」をクリックします。
3. これにより、特定の実行を再実行するためのポップアップ画面が開きます。レポート内の任意の行を開くことができますが、再実行できるのは「エラー」状態の行だけです。

配布レポートを再実行するための GuardAPI

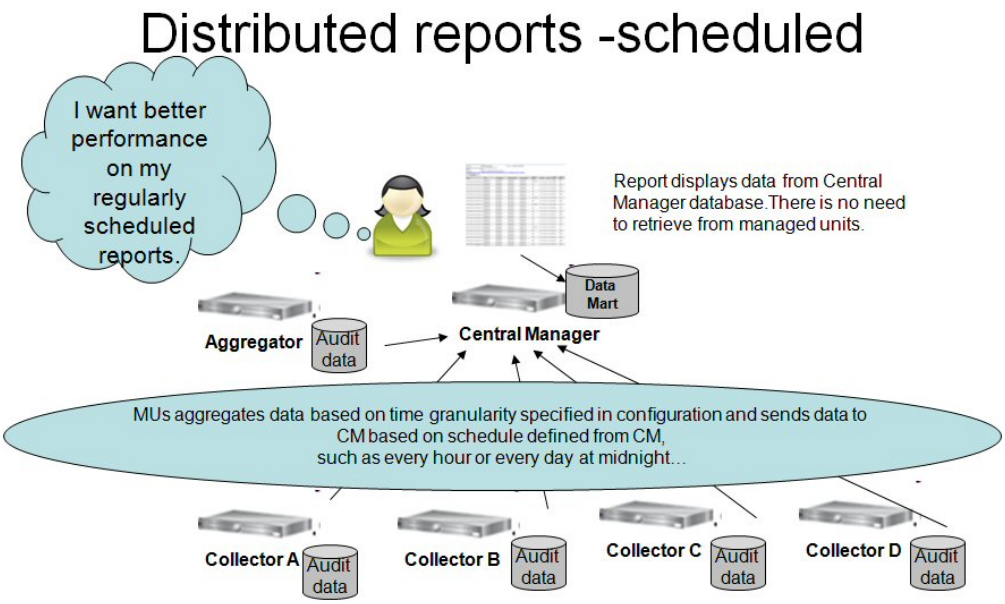
状況レポートを呼び出すための、GUI に記載された再試行コマンドには、GuardAPI コマンドを使用してアクセスすることもできます。

構文

grdapi rerun_distributed_report



この図は、即時配布レポートを実行するためのプロセスを示しています。



この図は、配布レポートをスケジュールするためのプロセスを示しています。

配布レポートの拡張: ターゲット・システムを任意の Guardium システムに設定する

配布レポートは、指定された Guardium システムに照会要求を配布します。システムはターゲット・システム内にデータを収集して結果を統合し、その統合された結果のビューを提供します。 この結果は、追加の照会の定義のためにクエリー・ビルダーで使用することができます。

配布レポート機能を使用して、ターゲット・システムを任意の Guardium システムに設定できるようになりました。以前のバージョンでは、ターゲット・システムの設定は許可されておらず、常に中央マネージャー (CM) に設定されていました。

要件の理由

多くの場合、配布レポートに関係なく CM に対する負荷が高くなります。CM はアグリゲーターとして使用されることもありますが、その場合は CM の負荷がさらに高くなります。

このような場合、ユーザーがターゲット・システムを設定できるようにした方がはるかに効率的です。

ソリューション

- ターゲット・システムは、配布レポートごとに設定することができます。CLI コマンドを使用して、オプションのターゲット・システムを設定することができます。CLI を使用して設定されたリストは、配布レポート・ビルダーの GUI に表示されます。
- 重要: この変更は、配布レポートのスケジュール・モードにのみ影響します。「即時」モードは、この変更には含まれていません。 そのため、随時の配布レポートの結果ビューアーには、CM 経由でのみアクセスすることができます。
- これまでと同様に、CM 経由でのみ配布レポートの定義を編集することができます。

GUI の変更

- 新しいフィールドである「データの送信先」が配布レポート・ビルダーの画面に追加され、配布レポートのターゲット・システム (コレクターまたはアグリゲーター) を設定できるようになりました。
- このフィールドが関係するのは、スケジュール・モードの場合だけです (それ以外の場合、このフィールドは使用不可になります)。
- デフォルトでは CM に設定されます。
- 使用可能なターゲット・システムのリストは、CLI を使用して設定されたシステムに制限されます (以下の CLI リストを参照)。
- 配布レポートの定義は、CM 経由で編集することができます。ターゲット・システム経由では、表示専用になります。
- レポートの「ペインに追加」(レポート・ビューアーをメニューに追加) は、ターゲット・システムと CM の定義画面で使用することができます。
- このオプションは、CM が対象レポートのターゲット・システムではない場合でも、CM で使用することができます。CM 上で配布レポートの状況を表示できるようにするためにこのようになっていますが、レポート自体にはデータは表示されません。

CLI コマンド (CM 経由でのみ使用可能)

1. システムをターゲット・システムとして設定:

grdapi set_distributed_report_target target_host_name=[unit host name]

2. システムのターゲット・システムとしての設定をキャンセル:

grdapi cancel_distributed_report_target target_host_name=[unit host name]

このユニットがターゲット・システムとして設定されている配布レポートがまだ存在する場合は、エラーとともにそれらのレポートのリストが返されます。

3. ターゲット・システムのリストを取得:

grdapi get_distributed_report_target_info

その他の CLI コマンド

スケジュールが設定された配布レポートの場合、ユニットごとの行の最大数の値を保管または表示します。

show scheduled_distributed

store scheduled_distributed

store コマンドには、1 つのパラメーター maximum_rows_per_unit があります。 このパラメーターの値が 15,000 より大きいか、0 と等しい (制限なし) 場合、ユーザーに次の警告メッセージが表示されます。

コレクターの数によっては、ユニット当たりの最大行数を高い値に設定すると、パフォーマンスに悪影響が及ぶ可能性があります。(Depending on number of collectors, setting maximum number of rows per unit to a high value might have negative impact on performance.)

親トピック: レポート

配布レポートの作成方法

Guardium には、特定の Guardium 中央マネージャーに関連付けられている一部またはすべての Guardium 管理対象ユニットからデータを自動収集する機能が用意されています。

このタスクについて - この例では、特定のコレクターで記録された例外 (例えば SQL エラー) について、より広範囲に表示し、相関性を把握する方法を示します。

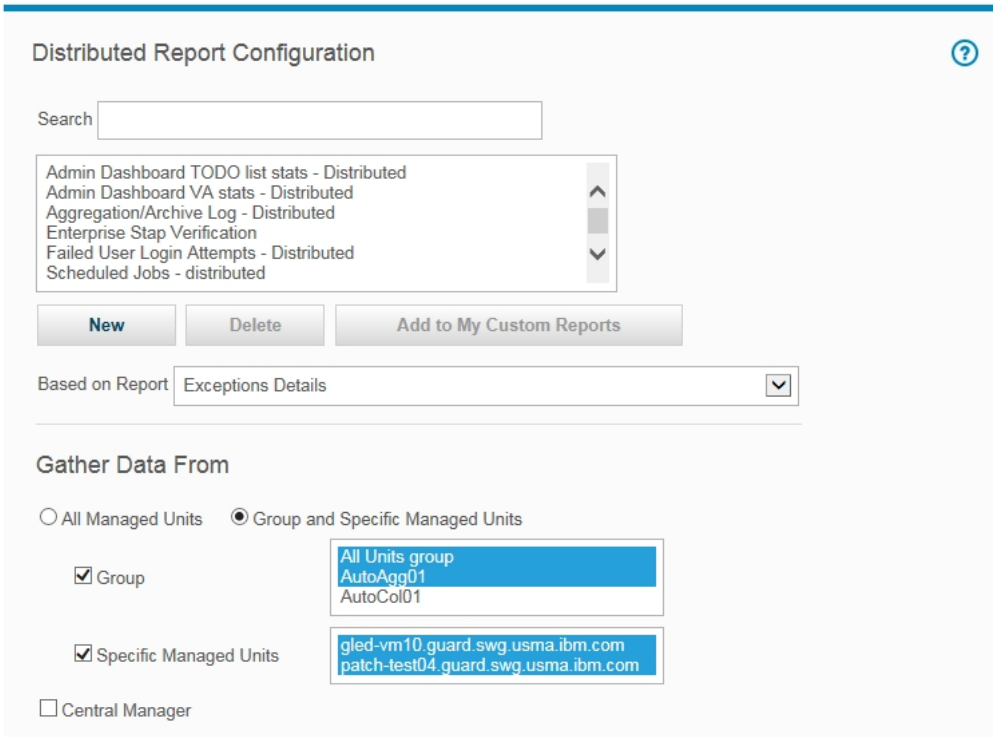
ステップの要約

前提条件 – 一元管理画面で管理対象ユニットのグループを作成します。

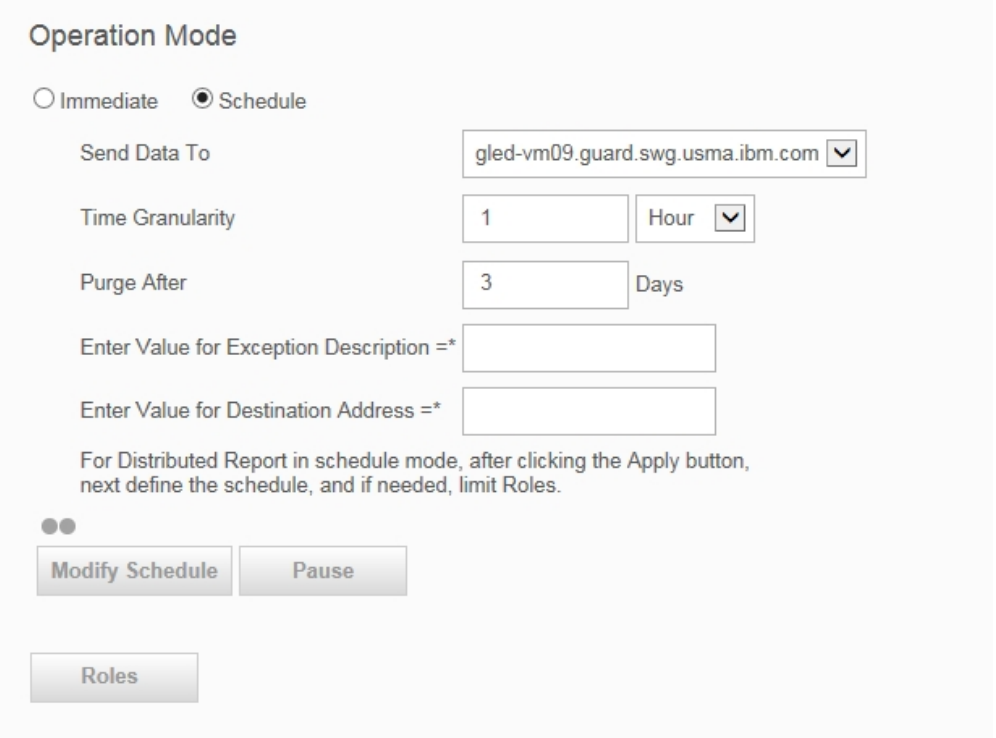
1. 配布レポートを作成します。
2. 収集したデータをレビューします。
3. 収集したデータに関する追加の要約レポートを作成します。

手順

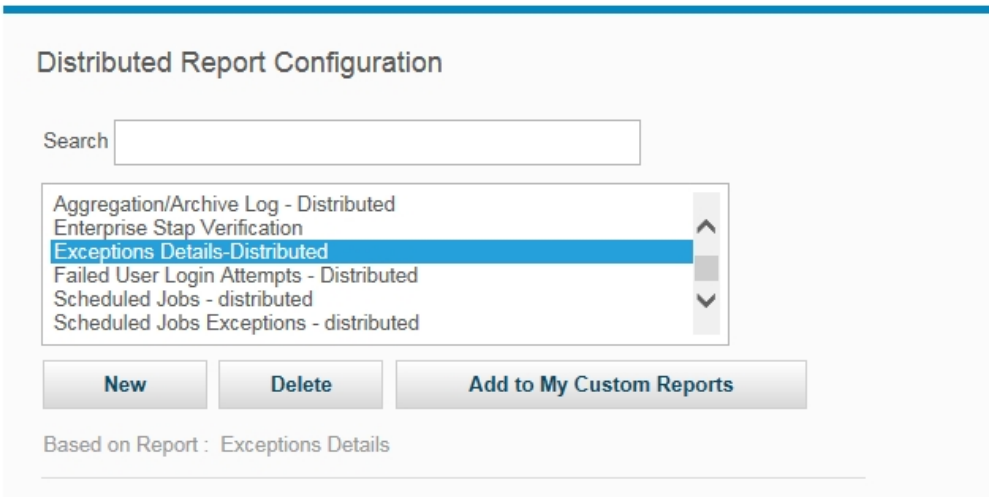
1. 「レポート」 > 「レポート構成ツール」 > 「配布レポート・ビルダー」をクリックします。
2. 「新規」をクリックします。
3. リストで「レポートに基づく」を選択します (リストにはユーザー定義レポートが表示されます)。この例の場合は、「例外の詳細」を選択します。



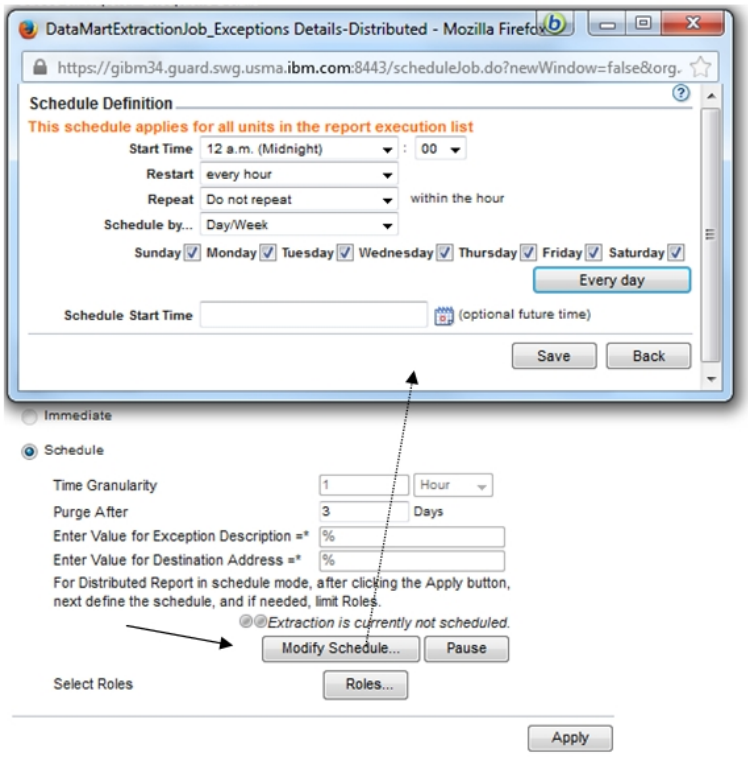
4. 画面を下方向に移動して、この配布レポートに含める管理対象ユニットを指定します。この例の場合は、グループ・リストから 2 つのグループを選択し、さらに、管理対象ユニット・リストから数個の管理対象ユニットを選択します。この例では、「中央マネージャー」のチェック・マークを外したままにします (中央マネージャーがアグリゲーターを兼ねている場合は、対象として含める必要があります)。
5. 次の画面キャプチャーは、動作モードの設定を示します。 即時モードは、主にオンライン/リアルタイム・モニター用であり、最近の失敗したログイン試行、最近の過度の例外、またはリアルタイム・アラートなどの表示に使用します。スケジュール・モードは、定義されたスケジュールに基づいて定期的に実行される継続的データ収集です。この例では、1 時間ごとに例外を要約します。「例外の記述」および「宛先アドレス」に値を取り込むための要件があります。



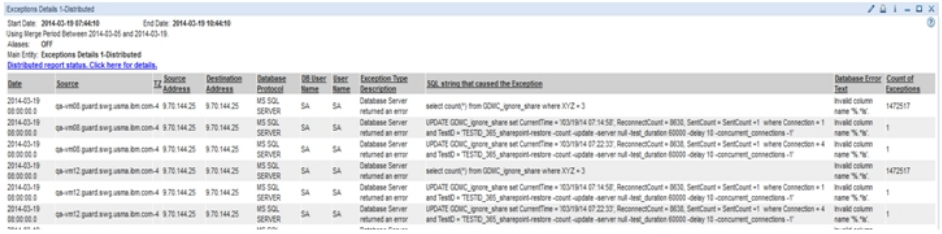
6. 「適用」をクリックして、配布レポートを作成します。
7. 適用すると、新しい配布レポートが追加され、リスト・ボックス内で強調表示されます。



8. 次に、「スケジュールの変更」をクリックして、レポートをスケジュールします (これは、プロセスをアクティブ化するためには必須です)。



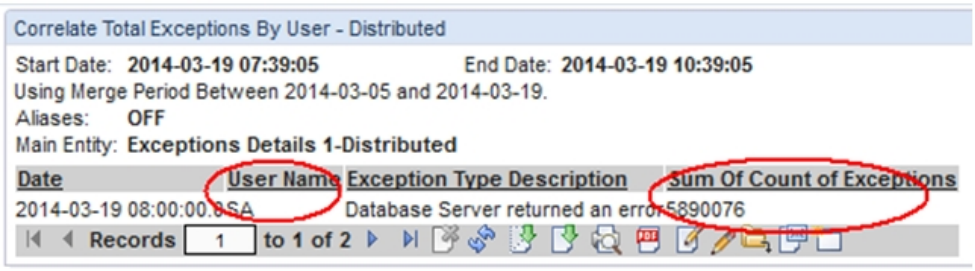
9. このレポートを特定のロールに限定することができます。そのためには、「ロール」をクリックし、適切なロールを選択します。
10. この具体例では、レポートは 1 時間ごとに実行されます。最初の結果を得るために 1 時間以上待つ必要はありません。
    注:「配布レポートの状況 - 詳細を表示するには、ここをクリックします。」の行は、データ収集の状況を示します。管理対象ユニットにデータがない場合、この行は赤色で示されます。この行をクリックすると、ユニットごとの 1 時間当たりの状況に関する詳細レポートにナビゲートします。



11. データは、指定されたすべての管理対象ユニットから収集され、指定された新規エンティティー (表) に保管されます。これで、このエンティティーは、クエリー・ビルダーおよびレポート・ビルダーを通じて、この新しい表に対する追加の照会およびレポートの作成に使用できます。追加の照会およびレポートを作成するためのオプションは、配布レポートの結果画面でも使用できます。「このレポートの照会を編集」をクリックします。

    このデフォルト・レポートは変更できません。「コピー」をクリックし、名前を付けて、すべての属性を削除し、「日付」、「ユーザー名」、「例外タイプの記述」、「例外の合計数 (Sum Of Count Of Exceptions)」をそのままにしてください。

次の画面キャプチャーは、「ユーザー別例外の合計の相関 (配布) (Correlate Total Exceptions By User (Distributed)」の例を示します。このビューには、この配布レポートで選択した Guardium 管理対象ユニットに関連付けられているすべてのデータベースからのユーザーごとの例外の合計が表示されます。同様に、システム全体における失敗したログイン試行の合計や、ソース・プログラム当たりの例外の合計を表示できます。



親トピック: レポート

評価および強化

Guardium® の「脆弱性評価」ソリューションは、IT 環境に対するセキュリティーおよびコンプライアンスのライフサイクル管理における最初のステップです。事前定義アセスメントまたはカスタム・アセスメントとプロセス・ワークフロー監査のセットを使用して、自動化方式でデータベースの脆弱性を特定および処置し、予防的に構成を改善し、インフラストラクチャーを強化することができます。

- Guardium 脆弱性評価の紹介
  Guardium 脆弱性評価では、データベース・インフラストラクチャー内のセキュリティー脆弱性を特定し、修正することができます。
- 脆弱性評価のテスト
  Guardium には、脆弱性の評価を可能にするテストのタイプがいくつか用意されています。
- 評価
  アセスメントとは、データベース・インフラストラクチャーの脆弱性をスキャンし、リアルタイム測定と履歴測定によるデータベースおよびデータ・セキュリティーの正常性評価を行う一連のテストを指します。
- 必要とされるスキーマ変更
  Guardium V9.1 では、IBM DB2 for z/OS 上での脆弱性評価テストで使用されるスキーマが変更されています。9.1 より前のリリースからアップグレードする場合、これらのテストを引き続き使用するためには、データベースを更新する必要があります。
- RACF の脆弱性の評価
  IBM DB2 for z/OS を使用する場合は、脆弱性評価テストで RACF の脆弱性を評価することができます。RACF アセスメントを使用するには、少なくともバージョン 9.1 の Guardium がインストールされている必要があります。
- 構成監査システム
  CAS はそのような変更をトラッキングして、それについて報告します。このデータは Guardium システム上で使用可能であり、レポートやアラートに使用できます。

Guardium 脆弱性評価の紹介

Guardium 脆弱性評価では、データベース・インフラストラクチャー内のセキュリティー脆弱性を特定し、修正することができます。

データベース脆弱性評価は、データベース・インフラストラクチャーで脆弱性をスキャンし、リアルタイム測定および履歴測定によるデータベースおよびデータ・セキュリティーの正常性を評価するために使用されます。

脆弱性評価では、以下の 3 タイプの成果物を使用します。

テスト
: テストでは、特定の脅威または関心面に対する脆弱性についてデータベース環境が検査されます。

アセスメント
: アセスメントとは、まとめて実行される一連のテストが含まれたジョブを指します。

データ・ソース
: データ自体のソース (データベースや XML ファイルなど)、およびデータへのアクセスに必要な接続情報。

Guardium® 脆弱性評価アプリケーションを使用すると、組織は、一貫性のある自動化された方式で、データベースの脆弱性を識別および処置することができます。Guardium の評価プロセスでは、以下を行うことによって、データベース環境の正常性を評価し、改善方法を推奨します。

- ベスト・プラクティスと対比してシステム構成を評価し、データベース・リソースに対する脆弱性または潜在的な脅威を (構成および動作上のリスクも含めて) 検出します。 例えば、無効化されていないすべてのデフォルト・アカウントを識別する、PUBLIC 特権および選択した認証方式を検査する、などです。
- セキュリティー・パッチの欠落など、IT 環境に内在する脆弱性を検出します。
- 最もクリティカルなリスクおよび脆弱性が発見された領域をベースに、アクション・プランを推奨し、優先順位付けします。 レポートおよび推奨を生成することで、コンプライアンスの変更に対応し、評価されたデータベース環境のセキュリティーを向上させる方法についてのガイドラインが提供されます。

Guardium のデータベース脆弱性評価では、2 つの中心的なテスト方式を組み合わせることにより、全範囲を網羅しています。 この方法では、複数の情報ソースを利用して、データベースとデータ環境のセキュリティー正常性の全体像を作成します。

1. エージェント・ベース - 各エンドポイント (例えば、データベース・サーバー) にインストールされたソフトウェアを使用。 これらにより、データベース・コンソールからの管理者による機密データへの直接アクセスなどの、リモートでは判別できないエンドポイントの側面を判別できます。
2. スキャン - 資格情報によるアクセスを介したネットワーク上でのエンドポイントに対する問い合わせ。

Guardium「脆弱性および脅威の管理」ソリューションには、以下が含まれています。

- データベース・オートディスカバリー - データベース環境のネットワーク・オートディスカバリーを実行し、データベースのクライアントとサーバー間の対話のグラフィカル表現を作成します。
- データベース・コンテンツ分類 - 機密データ (16 桁のクレジット・カード番号および 9 桁の社会保障番号など) を自動的に検出、分類して、問題のあるビジネスや、機密データを保管する IT プロセスを組織が迅速に識別するのに役立ちます。
- データベース脆弱性評価 - データベース・インフラストラクチャーで脆弱性をスキャンし、リアルタイムの測定および履歴測定によるデータベースおよびデータ・セキュリティーの正常性の評価を行います。
- CAS (構成監査システム) - データベース構造、セキュリティーおよびアクセス制御、重要なデータ値、データベース構成ファイルなどの項目に対して加えられたすべての変更をトラッキングします。
- コンプライアンス・ワークフロー自動化 - 評価と強化策、アクティビティー・モニターに始まり、監査レポート、レポート配布、および主要な利害関係者によるサインオフに至るまで、コンプライアンス・プロセス全体を自動化します。

CAS (構成監査システム) は、脆弱性および脅威の識別において重要な役割を果たします。Guardium の事前構成およびユーザー定義された CAS テンプレートを評価テストで使用して、ユーザーのデータベース環境の履歴ビューを起動することができます。 CAS を使用すると、Guardium はデータベースに対する脆弱性を OS レベル (ファイルのアクセス権、所有権、および環境変数など) で識別できます。 これらのテストは名前に *Assessment* というワードが含まれており、「CAS テンプレート・セット定義」パネルから参照可能です。

注: 脆弱性評価 (VA) および構成監査システム (CAS) は、英語のみでサポートされています。

Common Vulnerabilities and Exposures (CVE®) は、公に知られた機密保護の脆弱性についての共通名称 (つまり CVE ID) の辞書です。 CVE の共通 ID を使用することにより、別個のネットワーク・セキュリティー・データベースやツールの間でデータが共有しやすくなり、対象を評価するためのベースラインが提供されます。 例えば、レポートに CVE ID が組み込まれていると、ユーザーは、1 つ以上の別個の CVE 互換データベースにあるフィックス情報に素早く正確にアクセスし、問題を修正することができます。

多くの組織が、CVE ID を組み込むことにより、自社の機密保護製品およびサービスを CVE 互換にしています。Guardium は、MITRE Corporation の提供する Common Vulnerabilities and Exposures (CVE) を常にモニターしています。 関連するデータベース関連の脆弱性を調べるために、これらのテストが追加されます。

ユーザーが特定のデータベースの CVE 名を表示して、個々の脆弱性を検出する助けとして、セキュリティー・アセスメント・ビルダーを使用してテストを構成する際に、必要なデータベースの CVE ラジオ・ボタンを選択し、該当する CVE ID を選択および追加することができます。 追加情報は、MITRE Corporation が保守する CVE リストのマスター・コピーで常に検索できます。

Guardium ソリューションで CVE を最新の状態に保つため、Guardium では最新の CVE データベースをダウンロードして使用し、データベース表にすべての最新 CVE 項目および候補を取り込みます。 Guardium は、ダウンロードした CVE データと、Guardium 脆弱性評価リポジトリー内に既にある CVE データを、プログラムを使用して比較し、レビュー用に新しい CVE のリストを生成します。 次いで、Guardium データベース・セキュリティー・チームは、これらの Guardium 脆弱性知識ベースの候補を手動でレビューし、テストして、関連するものを GA Guardium 脆弱性評価知識ベースに追加します。 これらのテストには該当する CVE 番号のタグが付けられ、一度 GA リポジトリーに入れられると、Guardium 脆弱性評価アプリケーションを使用してこれらのテストを自動的に実行できるようになります。

注:

- 脆弱性評価と資格レポートのどちらについても、資格レポートの特権を付与するためのスクリプトを検索する場合は、gdmmonitor_scripts ディレクトリー内のスクリプトを使用してください。entitlement_monitor_role フォルダーは更新されなくなったため、使用しないでください。
- 有効期限が切れた製品ライセンス・キーを使用した場合、またはデータ・ソースの数が制限されているライセンスを使用した場合は、次のメッセージが表示されることがあります。「データ・ソースを追加できません。データ・ソースのライセンス許容最大数に達しています。「ライセンス有効期限」の日付および「データ・ソースの数」は、「管理者コンソール」の「システム構成」パネルで確認できます。*N* 個のデータ・ソースがある脆弱性プロセスまたは分類プロセスは、実行されるたびに *N* 個のスキャンとしてカウントされます。
- Guardium「脆弱性評価」では、評価対象データベースへのアクセス権が必要です。これを行うために、Guardium には、Guardium で使用するデータベース内にユーザーとロールを作成する一連の SQL スクリプト (データベース・タイプごとに 1 つのスクリプト) が用意されています。

  テンプレート・スクリプトが作成され、ファイル・サーバーを介してパス /log/debug-logs/gdmmonitor_scripts/ で検出およびダウンロードが可能になると、Guardium システムで使用できます。README.txt ファイルには、さらに詳しい情報が含まれています。

Guardium 脆弱性評価テストの例外

Guardium 脆弱性評価テストの例外グループには、データベースのインストール時に作成されたデフォルトのメンバー、スキーマ、オブジェクト、または特権が事前に設定されています。これらのグループを使用して、脆弱性評価の実行時の誤検出を防ぎます。評価が失敗した場合は、適切な例外グループをテストにリンクし、デフォルトのメンバーを除外して、テストを再度実行します。これでテストが違反なしで実行される場合、データベースのインストール時に作成されたデフォルトのメンバー、スキーマ、オブジェクト、または特権が初期違反の原因だったことを示します。

表 1. マッピングをテストするための脆弱性診断のグループ

グループ ID	グループ名	テスト名	テスト ID	データベース・タイプ
82	Sybase 許可された PUBLIC への特権の付与	非免除の特権が PUBLIC に付与されていない	61	SYBASE ASE
83	MS-SQL 許可された PUBLIC への特権の付与	非免除の特権が PUBLIC に付与されていない	270	MSSQL
115	Db2 許可された PUBLIC への特権の付与	オブジェクト特権が PUBLIC に付与されていない	105	Db2 LUW
144	Db2 非制限的に許可された PUBLIC への特権の付与	オブジェクト特権が PUBLIC に付与されていない	105	Db2 LUW
116	Teradata 許可された PUBLIC への特権の付与	PUBLIC に付与されているオブジェクト特権	2029	TERADATA
117	PostgreSQL 許可された PUBLIC への特権の付与	PUBLIC に付与されているオブジェクト特権	315	POSTGRESQL
118	Netezza 許可された PUBLIC への特権の付与	PUBLIC に付与されたオブジェクト特権 (Netezza)	2053	NETEZZA

グループ ID	グループ名	テスト名	テスト ID	データベース・タイプ
65	MS-SQL データベース管理者	固定サーバー・ロールに関する権限がデータベース管理者のみに付与されている	159	MSSQL
165	Oracle データベース管理者のみが SYS.USER$ にアクセスできる	データベース管理者のみが SYS.USER$ にアクセスできる	222	ORACLE
166	MS-SQL ユーザーに付与されている DDL	ユーザーに付与されている DDL	321	MSSQL
167	MS-SQL ユーザーに付与されているプロシージャー	ユーザーに付与されているプロシージャー	322	MSSQL
168	MS-SQL 個々のユーザーに特権が付与されていない	個々のユーザーに特権が付与されていない	154	MSSQL
170	PUBLIC に付与されている Sybase IQ プロシージャーおよび関数特権	プロシージャーおよび関数に対する特権が PUBLIC に付与されました。	2230	SYBASE IQ
171	Sybase IQ 個別のプロシージャー特権または関数特権がない	個別のプロシージャー特権または関数特権がありません。	2227	SYBASE IQ
172	MS-SQL レジストリー・アクセス拡張プロシージャーへのアクセス権限がない	レジストリー・アクセス拡張プロシージャーへのアクセス権限がない	215	MSSQL
173	MS-SQL ロールに付与されているロール	ロールに付与されているロール	323	MSSQL
185	サーバー・レベルの MS-SQL アクセス権限が、データベース管理者以外のユーザーに付与されました	サーバー・レベルのアクセス権限が、データベース管理者以外のユーザーに付与されました	2289	MSSQL
186	MS-SQL MSDB データベースのロール・メンバー特権	MSDB データベースのロール・メンバー特権	2296	MSSQL
48	Db2 データベース Version+Patches	バージョン: Db2	16	Db2 LUW
48	Db2 データベース Version+Patches	Db2 パッチ・レベル	54	Db2 LUW
49	Informix データベース Version+Patches	バージョン: Informix	17	INFORMIX
49	Informix データベース Version+Patches	Informix パッチ・レベル	55	INFORMIX
50	MS SQL Server データベース Version+Patches	バージョン: Microsoft SQL Server	18	MSSQL
50	MS SQL Server データベース Version+Patches	Microsoft SQL Server パッチ・レベル	56	MSSQL
51	MySql データベース Version+Patches	バージョン: MySql	19	MYSQL
51	MySql データベース Version+Patches	MySql パッチ・レベル	57	MYSQL
52	Oracle データベース Version+Patches	Oracle パッチ・レベル	58	ORACLE
52	Oracle データベース Version+Patches	バージョン: Oracle	20	ORACLE
53	Sybase データベース Version+Patches	バージョン: Sybase	21	SYBASE ASE
53	Sybase データベース Version+Patches	Sybase パッチ・レベル	59	SYBASE ASE
109	Teradata PDE Version+Patches	バージョン: Teradata PDE	284	TERADATA
109	Teradata PDE Version+Patches	Teradata PDE パッチ・レベル	286	TERADATA
110	Teradata TDBMS Version+Patches	Teradata TDBMS パッチ・レベル	287	TERADATA
110	Teradata TDBMS Version+Patches	バージョン: Teradata TDBMS	285	TERADATA
111	Teradata TDGSS Version+Patches	バージョン: Teradata TDGSS	290	TERADATA
111	Teradata TDGSS Version+Patches	Teradata TDGSS パッチ・レベル	288	TERADATA
112	Teradata TGTW Version+Patches	バージョン: Teradata TGTW	291	TERADATA
112	Teradata TGTW Version+Patches	Teradata TGTW パッチ・レベル	289	TERADATA
113	Netezza Version+Patches	Netezza バージョン・レベル	306	NETEZZA
113	Netezza Version+Patches	Netezza パッチ・レベル	307	NETEZZA
114	Postgress Version+Patches	PostGreSQL バージョン・レベル	308	POSTGRESQL

グループ ID	グループ名	テスト名	テスト ID	データベース・タイプ
114	Postgress Version+Patches	PostGreSQL パッチ・レベル	309	POSTGRESQL
169	SybaseIQ データベース Version+Patches	バージョン: Sybase IQ	377	SYBASE IQ
169	SybaseIQ データベース Version+Patches	Sybase IQ パッチ・レベル	378	SYBASE IQ

MongoDB

2007 年に開発された MongoDB は、NoSQL のドキュメント指向データベースです。MongoDB では、動的スキーマに基づく JSON ドキュメントを使用します (このフォーマットは BSON と呼ばれます)。MongoDB では、コレクションは RDBMS 表に相当し、ドキュメントは RDBMS 表内のレコードに相当します。

MongoDB は、大きく急速に成長している NoSQL データベース・システムです。Web アプリケーションでよく見られる JSON ドキュメントなどの非リレーショナル形式データはプログラミングが容易であるため、運用システムや Web アプリケーションのバックエンドとして使用される傾向にあります。

- Guardium 脆弱性評価 (VA) でサポートされる最初の NoSQL データベースです。
- 最初の非 JDBC データベース接続です。接続では Java ドライバーが使用されます。
- MongoDB データ・ソースは、SSL クライアント証明書を使用した SSL サーバーとクライアント/サーバーの接続をサポートしています。
- MongoDB クラスターの Guardium の VA ソリューションは、複数の Mongo (レプリカ・セットの 1 次ノードとすべての 2 次ノード) 上で実行することができます。
- MongoDB では資格レポートおよび照会ベース・ビルダーはサポートされません。

SSL を使用した MongoDB データ・ソース

自己署名用に別途用意したサーバー証明書をインポートできます。お客様が独自の証明書をインポートすることもできます。 さらに、証明書は中央マネージャー上で機能し、コレクターにプッシュダウンされます。

CAS for MongoDB

Mongo CAS アセスメント・テンプレートを使用すると、データ・ソース内の複数のパスを指定して、ファイル・システムのさまざまなコンポーネントをスキャンすることができます。

Teradata Aster

Aster データ

2011 年に Teradata によって買収されました。通常は、データウェアハウジングおよび分析アプリケーション (OLAP) に使用されます。Aster Data は、構造化照会言語 (SQL) を MapReduce 内で使用できるようにする SQL-MapReduce と呼ばれるフレームワークを構築しました。最もよく連想されるのは、クリック・ストリーム系のアプリケーションです。

クイーン・ノードですべてのテストを実行するには、セキュリティー・アセスメントを作成する必要があります。Aster Data 用のデータベース接続はすべて、クイーン・ノードのみを通過します。

ワーカー・ノードとローダー・ノードでテストが必要となるのは、CAS テスト (ファイル許可とファイル所有権) を実行する場合のみです。

特権テストは、所定の Aster インスタンスに含まれるすべてのデータベースをループします。

SAP HANA

SAP HANA は、SAP SE によって開発され販売されている、メモリー内の列指向型リレーショナル・データベース管理システムです。HANA のアーキテクチャーは、同一プラットフォーム上で、高いトランザクション率と複雑な照会処理の両方に対処するように設計されています。

- 脆弱性評価および分類用のデータベース特権
  Guardium は、脆弱性評価の実行に必要な最小限の特権を備えたグループや役割の作成を簡素化する一連のスクリプトを備えています。
- Db2 for i 用の VA のデプロイ
  ユーザーのグループが脆弱性評価を実行できるようにして、テストを構成して実行します。
- Cloudera での VA の使用
  Apache Hadoop の Cloudera ディストリビューションで Guardium 脆弱性評価を使用する方法を説明します。

親トピック: 評価および強化

脆弱性評価および分類用のデータベース特権

Guardium は、脆弱性評価の実行に必要な最小限の特権を備えたグループや役割の作成を簡素化する一連のスクリプトを備えています。

始める前に

このタスクでは、Guardium システムからスクリプトをダウンロードし、データベース・サーバーでそのスクリプトを実行する必要があります。Guardium システムへのアクセスに使用するマシンの IP アドレスを特定する必要があります。これは、スクリプトをデータベース・サーバーに転送する前にダウンロードする個別のワークステーションの IP アドレスにすることも、データベース・サーバー自体の IP アドレスにすることもできます。

このタスクについて

Guardium 脆弱性評価の実行および Guardium 分類の使用には、データベースに対するアクセス権限および特定のデータベース特権が必要です。Guardium は、脆弱性評価の実行に必要な最小限の特権を備えたグループや役割の作成を簡素化する一連のスクリプトを備えています。作成されたグループまたは役割は、評価を実行する必要がある任意のデータベース・ユーザーに割り当てることができます。そのユーザーを使用して Guardium データ・ソースを作成して、VA スキャンを実行します。

ほとんどのデータベース・タイプをサポートするスクリプトが用意されており、データベース・ツール自体で実行するように設計されています。各スクリプトのスクリプト・ヘッダーに、詳細な説明が含まれています。各データベース・タイプに対して付与される特権は、スクリプトで各権限付与を見ることで確認できます。
重要: スクリプトを実行する前には、データベース管理者は、スクリプト・ヘッダーに含まれている説明を読み、スクリプトで実行されるデータベース・アクションを確認する必要があります。

手順

1. Guardium システムで、fileserver CLI コマンドを使用してファイル・サーバーを有効にします。 例えば、ファイル・サーバーを 1 時間有効にし、IP アドレスが `10.0.0.1` のシステムにスクリプトをダウンロードするには、以下のコマンドを使用します。

   ```
   fileserver 10.0.0.1 3600
   ```

   正常に開始されると、ファイル・サーバーで以下のような出力が表示されます。

   ```
   Starting the file server...
   The file server is ready at https://guardium.host.com:8445
   The timeout has been set to 3600 seconds and it may timeout during the uploading.

   The upload will only be accessible from the IP you are logged in from: 10.0.0.1
   ```

   ファイル・サーバーを停止するには `ENTER` を押してください。

2. スクリプトをダウンロードするマシンで、Web ブラウザーを使用してファイル・サーバーにアクセスします。 例えば、`https://guardium.host.com:8445` で実行されている Guardium システムの場合、以下の URL で脆弱性評価および分類用のスクリプトにアクセスします。

   ```
   https://guardium.host.com:8445/log/debug-logs/gdmmonitor_scripts/
   https://guardium.host.com:8445/log/debug-logs/classification_role/
   ```

   重要: Guardium 分類のディスカバリー・プロセスでは、脆弱性評価テストで求められるよりも高いレベルのデータベース・アクセス権限が必要になります。脆弱性評価では `gdmmonitor_scripts` 内のスクリプト、分類では `classification_role` 内のスクリプトを使用することをお勧めします。スクリプトを実行する前には、データベース管理者は、スクリプト・ヘッダーに含まれている説明を読み、スクリプトで実行されるデータベース・アクションを確認する必要があります。スクリプトを実行する前には、データベース管理者は、スクリプト・ヘッダーに含まれている説明を読み、スクリプトで実行されるデータベース・アクションを確認する必要があります。
3. Web ブラウザーで[右クリック] > 「名前を付けてリンク先を保存...」アクションまたは同様の機能を使用して、必要なスクリプトをダウンロードします。
   README.txt ファイルを確認して、特定のデータベース・タイプで使用するのに適したスクリプトを特定します。
   ヒント: 以下の 3 つの Microsoft SQL Server 用のスクリプトがあります。
   - gdmmonitor-mss2000-only.sql。Microsoft SQL Server 2000 用です
   - gdmmonitor-mss.sql。Microsoft SQL Server 2005 以降用です
   - gdmmonitor-mss-SA.sql。Microsoft SQL Server 脆弱性評価テストの 6 つで必要な管理特権を付与するために使用します。該当する特権を許可しなかった場合、特権が不十分であることを示すエラーがテストで返されます。該当する 6 つのテストは、使用可能なテストのわずか 5% にすぎません。

次のタスク

データベース・サーバーで必要なスクリプトをダウンロードしたら、スクリプト・ヘッダーに含まれている説明を念入りに確認し、その説明に従ってください。

親トピック: Guardium 脆弱性評価の紹介

Db2 for i 用の VA のデプロイ

ユーザーのグループが脆弱性評価を実行できるようにして、テストを構成して実行します。

このタスクについて

デプロイメントの手順

1. Guardium システムから脆弱性評価機能がデプロイされます。
2. Guardium に付属するスクリプトをターゲット・データベースに対して実行し、適切な特権を持つロールを作成します。次に、データベースに対するデータ・ソース接続を作成します。
3. セキュリティー・アセスメントを作成し、使用するデータ・ソースと実行するテストを選択します。
4. 実行したテストが完了すると、レポートが作成されます。このレポートには、合格したテスト項目と不合格だったテスト項目のほかに、保護を強化する必要がある箇所について、詳細な推奨事項が記録されます。

IBM for i バージョン・サポート:

IBM for i 6.1、7.1、7.2 のパーティション

VA テスト範囲 (合計で 115 件のテスト):

特殊権限を持つプロファイル

データベース関数の使用権限を持つプロファイル

パスワード・ポリシー

PUBLIC に付与されているデータベース・オブジェクト特権

個々のユーザーに付与されているデータベース・オブジェクト特権

GRANT オプションが設定されているデータベース・オブジェクト特権

セキュリティーの APAR

資格レポート:

特殊権限を持つプロファイル

ユーザーに付与されているグループ

PUBLIC に付与されているデータベース・オブジェクト特権

PUBLIC に付与されているデータベース実行可能オブジェクト特権

個々のユーザーに付与されているデータベース・オブジェクト特権

GRANT オプションが設定されているデータベース・オブジェクト特権

手順

1. 「グループ・ビルダー」を使用して、VA を使用するユーザーのグループを作成します。「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」をクリックし、「グループ・ビルダー」を開きます。次のステップでは、gdmmonitor という名前のグループを対象としたスクリプトを使用しています。
2. Db2 for i システムで以下のスクリプトを実行し、VA の実行に必要な特権をこのグループに付与します。この処理は、データベースのネイティブ・クライアントを使用して、Guardium システムの外部で実行されます。

```
grant select on SYSIBMADM.FUNCTION_INFO to gdmmonitor;
grant select on SYSIBMADM.FUNCTION_USAGE to gdmmonitor;
grant select on SYSIBMADM.GROUP_PROFILE_ENTRIES to gdmmonitor;
grant select on SYSIBMADM.SYSTEM_VALUE_INFO to gdmmonitor;
grant select on SYSIBMADM.USER_STORAGE to gdmmonitor;
grant select on Qsys2.Authorizations to gdmmonitor;
grant select on SYSIBMADM.USER_INFO to gdmmonitor;
grant select on QSYS2.SYSSCHEMAAUTH to gdmmonitor;
grant select on QSYS2.SYSTABAUTH to gdmmonitor;
grant select on QSYS2.SYSPACKAGEAUTH to gdmmonitor;
grant select on QSYS2.SYSROUTINEAUTH to gdmmonitor;
grant select on QSYS2.SYSSEQUENCEAUTH to gdmmonitor;
grant select on QSYS2.SYSCOLAUTH to gdmmonitor;
```

   IBM Db2 for i v7.1 以降の場合は、以下のスクリプトも含めてください。

```
grant select on QSYS2.SYSVARIABLEAUTH to gdmmonitor;
grant select on QSYS2.SYSXSROBJECTAUTH to gdmmonitor;
```

3. Db2 for i システムへの JDBC 接続を作成します。「データ・ソース・ファインダー」を開きます。これを行うには、「設定」 > 「ツールとビュー」 > 「データ・ソース定義」をクリックし、次に「アプリケーション選択」メニューから「セキュリティー・アセスメント」をクリックします。
   a. 「新規」をクリックして適切な情報を入力します。「接続プロパティー」で、「property1=com.ibm.as400.access.AS400JDBCDriver;translate binary=true」と入力します。
4. 「アセスメント・ビルダー」を使用して、アセスメントを作成します。 「強化」 > 「脆弱性評価」 > 「アセスメント・ビルダー」をクリックし、「アセスメント・ビルダー」を開きます。
   a. アセスメントの説明を入力します。
   b. 前のステップで作成したデータ・ソースを追加します。これを行うには、「データ・ソースの追加」をクリックし、「データ・ソース・ファインダー」からデータ・ソースを選択して「追加」をクリックします。
   注: テストを構成する前に、「適用」をクリックしてアセスメントを保存する必要があります。
5. 「テストの構成」をクリックし、アセスメントにテストを追加します。「IBM for i」タブをクリックし、追加するテストを選択して「選択の追加」をクリックします。
6. 「戻る」をクリックし、「セキュリティー・アセスメント・ファインダー」に戻ります。「今すぐ 1 回実行」をクリックしてテストを実行するか、「監査プロセス・ビルダー」を使用してテストをスケジュールします。「監査プロセス・ビルダー」を開くには、「ディスカバー」 > 「分類」 > 「監査プロセス・ビルダー」をクリックします。
7. 「結果の表示」をクリックすると、実行されたすべてのテストの詳細 (スコアを改善するための推奨事項を含む) が表示されます。

タスクの結果

テストが不合格だった場合、以下の対処が可能です。

- データベースにパッチを適用する (パッチに関係する問題がある場合)
- 推奨されるベスト・プラクティスに従い、データベースのパラメーターを再構成する
- 使用しているアプリケーションでは必要ないオブジェクトやシステム特権を取り消す
- 被付与者に直接付与されているオブジェクトを取り消し、ロールまたはグループに対してオブジェクト特権を付与し、被付与者をそのロールまたはグループに割り当てる
- パスワード・ポリシー設定を変更するか、ユーザーのデフォルト・パスワードを変更する
- 例外グループを作成し、不合格だったテストにそのグループをリンクしてもう一度テストを実行する (使用しているアプリケーションで、特定の権限付与が必要になる場合)

親トピック: Guardium 脆弱性評価の紹介

Cloudera での VA の使用

Apache Hadoop の Cloudera ディストリビューションで Guardium 脆弱性評価を使用する方法を説明します。

Cloudera Manager

データ・ソースのセットアップ

Cloudera Manager データ・ソースは、接続に Cloudera Manager Java API を使用します。JDBC は使用しません。

クラスター名をデータ・ソース GUI で定義する必要があります。クラスター名は、左側の Cloudera Manager GUI でのクラスター表示名です。

Cloudera Manager の脆弱性評価テストを実行するには、ほとんどの脆弱性評価テストで、読み取り専用ロールを持つデータ・ソース・ユーザーを定義する必要があります。しかし脆弱性評価テストの中には、データ・ソース・ユーザーがテストを実行するための最小限の特権としてクラスター管理者ロールを持っている必要があるものが少数あります。

以下の脆弱性評価テストでは、データ・ソース・ユーザーがクラスター管理者ロールを持っている必要があります。

1. 認証バックエンド順序
2. 管理コンソールの HTTP ポート
3. 管理コンソールの HTTPS ポート
4. サーバーに対してエージェントの TLS 認証を使用する
5. 管理コンソールに対して TLS 暗号化を使用する
6. エージェントに対して TLS 暗号化を使用する

この情報は、Cloudera Manager gdmmonitor スクリプト (/log/var-log-guard/gdmmonitor_scripts/gdmmonitor-Cloudera-Manager.sql) でも入手できます。

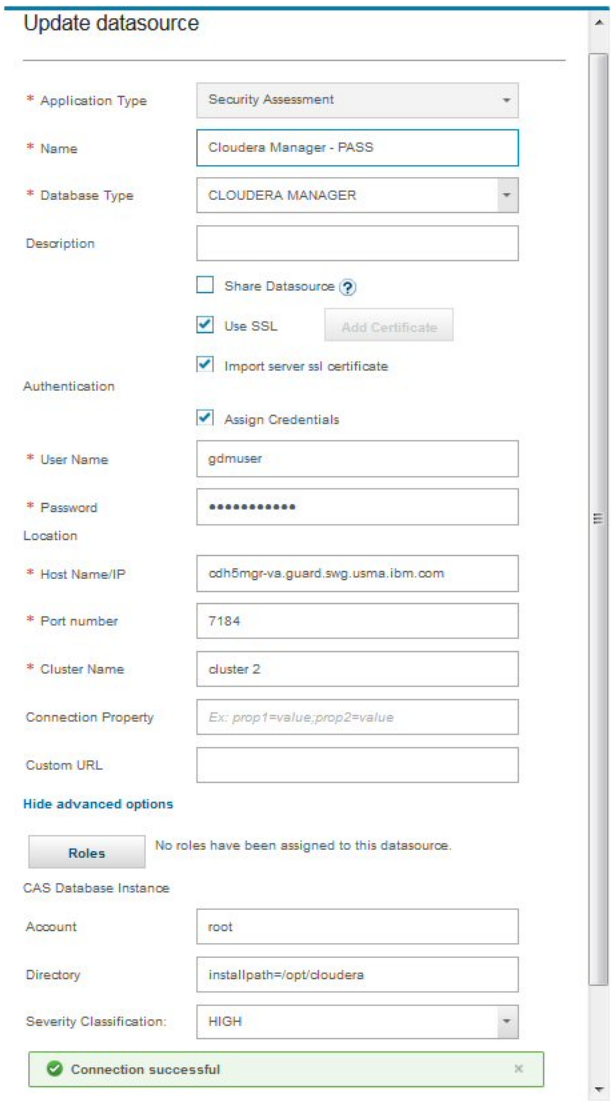
SSL が有効な場合、「SSL の使用」にチェック・マークを付け、「サーバーの SSL 証明書をインポートします」にチェック・マークを付けます。

「CAS データベース・インスタンス」の設定

アカウントは root でなければなりません。

ディレクトリーは、Cloudera Manager のインストール・パスとして定義する必要があります。例: installpath=/opt/cloudera

Cloudera Manager データ・ソースの設定の例。



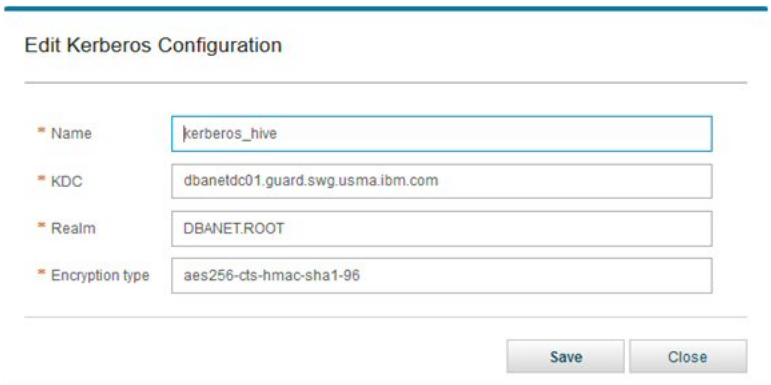
Hive

データ・ソースのセットアップ

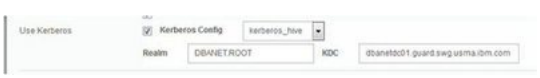
Apache Hive JDBC ドライバー 1.1.1 を使用します。

Kerberos - ユーザー名とパスワードは有効な Kerberos ユーザー ID とパスワードでなければなりません。これは CA にも使用されます。ご使用の Kerberos ユーザー ID とパスワードを Hive の beeline コマンド行へのログインに使用できることをテストして確認します。

ご使用のアプライアンスの KDC およびレルムを定義する Kerberos 構成が既に作成されていることを確認してください。Guardium GUI で、「設定」>「ツールとビュー」>「Kerberos 構成」の順に進みます。Kerberos 構成が作成されていない場合は、+ アイコンをクリックして新規の Kerberos 構成を作成します。



Kerberos 構成を作成した後、それを選択して、データ・ソースのセットアップを構成できます。



SSL が有効な場合、「SSL の使用」ボックスにチェック・マークを付け、「サーバーの SSL 証明書をインポートします」ボックスにチェック・マークを付けます。

注: Hive は LDAP/SSL または Kerberos の一方のみサポートでき、両方はサポートできません。

「CAS データベース・インスタンス」の設定

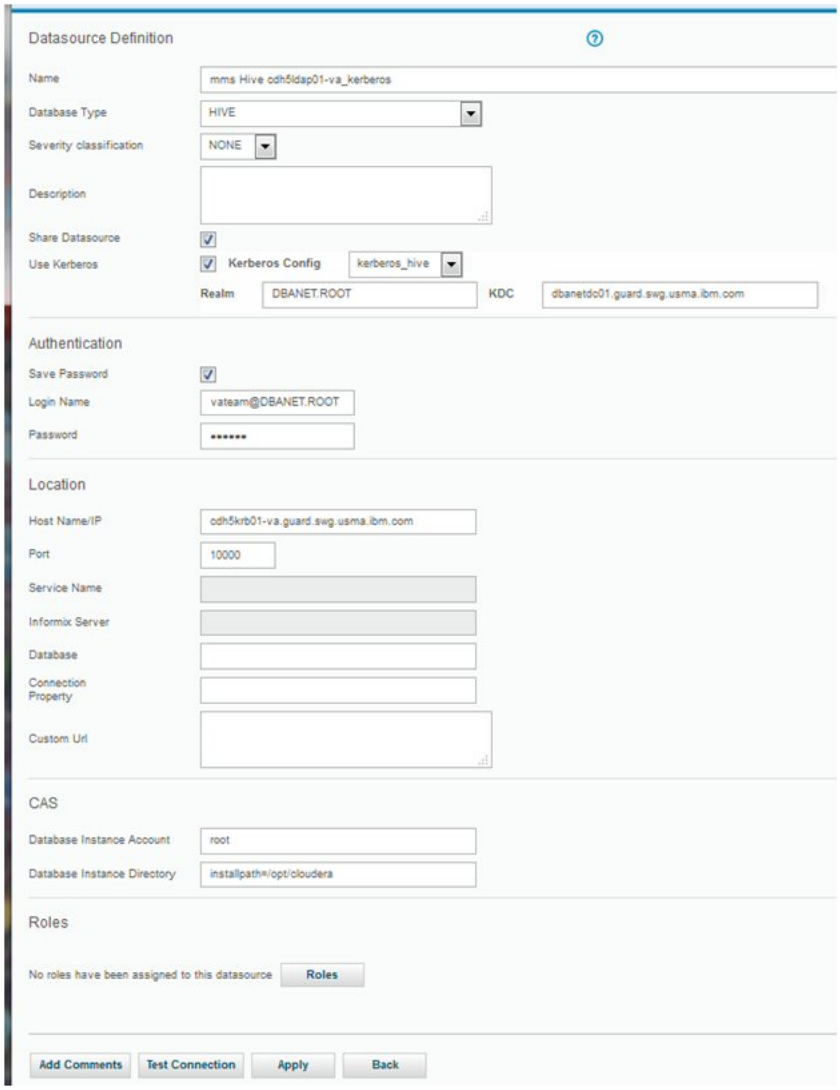
1. ディレクトリーは、Cloudera Manager のインストール・パスとして定義する必要があります。例: installpath=/opt/cloudera
2. HDFS が Kerberos に対して有効になっている場合、データ・ソース・ユーザー名とパスワードは有効な Kerberos ユーザー ID とパスワードでなければなりません。CAS スクリプトは、Kerberos チケットの取得にそれを使用します。
3. アカウントは root でなければなりません。CAS を必要とする特定のパラメーター・テストの場合、Cloudera エージェント・プロセス・ディレクトリー (/var/run/cloudera-scm-agent/process/) でリアルタイム構成にアクセスするために CAS ユーザーが root であることが重要です。

注: Guardium は構成データに何らかの変更や修正を行うことはありません。

Hive の場合

特権テストでは、データ・ソース・アカウントは Sentry Admin グループのメンバーである必要があります。Sentry Admin グループを確認する手順については、Hive gdmmonitor スクリプトを参照してください。

Hive データ・ソースのセットアップ時には、データ・ソースが Hive server2 を指しているときにのみ JDBC テスト接続を実行できます。他のすべての Hive データ・ソースについては、Cloudera サービスがインストールされているノード名を使用して、この特定のデータ・ソースのコピーを作成できます。 Hive server2 データ・ソースと同様に、コピーされたデータ・ソースにも有効なユーザー名およびパスワードがあることを確認してください。これらのデータ・ソースについては、データ・ソース・テスト接続を実行できません。しかし、Guardium は、Kerberos が有効な場合の CAS を使用した Kerberos 接続の実行は、データ・ソースからのユーザー名とパスワードの正確性に基づいて行います。



脆弱性評価のテスト

Hive 特権テストには、Sentry サービスがインストールおよび構成されている必要があります。Sentry がない場合、セキュリティーはありません。だれでも Hive に接続して、データにアクセスできます。

HDFS パラメーターの脆弱性評価 CAS テストは、Cloudera エージェント・プロセス・ディレクトリー (/var/run/cloudera-scm-agent/process/) の構成ファイルから行われます。これらのプロセス・ディレクトリー内のフォルダー名は、Cloudera エージェント・サービスが開始されるたびに変更されます。

一部の HDFS パラメーター CAS テストでは、データ・ソース・システムが特定のノード構成 (例えば、NameNode や DataNode など) である必要があります。また、一部の CAS テストでは、データ・ソース・システムに Yarn、Mapreduce、または Hive Server がインストールされている必要があります。 ご使用のデータ・ソース・システム構成に基づいて、評価のためのテストを慎重に選択してください。テストの要件が満たされない場合は、テストはエラーになり、これらのテストを適切な Cloudera サービスで実行するように推奨されます。要件はテストの説明にも記載されています。

Hive データ・ソースを作成する場合、各 Cloudera サービスに対して 1 つのデータ・ソース (NameNode、DataNode、HiveServer2、Hive メタストア、Yarn NodeManager、および Yarn ResourceManager) があることが推奨されます。

クラスター内のノードの数に関係なく、これらのすべてのサービスに対応する Guardium Hive データ・ソースがある場合は、ご使用の環境を適切にセットアップして脆弱性評価を実行してください。

例

親トピック: Guardium 脆弱性評価の紹介

脆弱性評価のテスト

Guardium には、脆弱性の評価を可能にするテストのタイプがいくつか用意されています。

脆弱性評価のテスト

Guardium® には、データベース構成のパラメーター、特権、およびその他の脆弱性などを検査するための、200 を超える事前定義テストがあります。独自のテストを定義することもできます。

1 つの脆弱性評価に、以下のタイプのテストが 1 つ以上含まれる場合があります。

事前定義テスト

事前定義テストは、データベース環境で発生する可能性のある、共通する脆弱性の問題を示す目的で設計されています。 データベース・アプリケーションの性質が非常に多様であることや、さまざまな企業またはシチュエーションに応じて許容可能な基準に違いがあることなどが原因となり、これらのテストの中には、特定のデータベースに適合しても、別のデータベース (同一企業内にあっても) にはまったく適合しないものがあります。 大部分の事前定義テストは、組織の要件を満たすようにカスタマイズ可能です。 さらに、評価に常に業界の最新のベスト・プラクティスを反映させ、新たに発見された脆弱性から保護するため、 Guardium は、データベース保護サブスクリプション・サービスの一環として新しい評価テストおよび更新を四半期ごとに配布します。 詳しくは、「Guardium 管理ガイド」を参照してください。

次のような事前定義テストがあります。

- 動作テスト
- 構成テスト

動作テスト

このテスト・セットは、データベース・トラフィックをリアルタイムで監視し、情報へのアクセスや操作に関する脆弱性を検出することにより、データベース環境のセキュリティー正常性を評価します。

例として、動作の脆弱性テストには、以下のものもあります。

- デフォルト・ユーザー・アクセス
- アクセス・ルール違反
- データベース・クライアントからの Admin コマンド、DDL コマンド、および DBCC コマンドの直接実行
- 過度のログインの失敗
- 過度の SQL エラー
- 勤務時間後のログイン
- 過度の管理者ログイン
- 拡張ストアード・プロシージャーに対する呼び出しの検査
- ユーザー ID が複数の IP アドレスからアクセスを受けていないことの検査

構成テスト

この評価セットでは、ターゲット・データベースのセキュリティー関連の構成設定を検査し、構成における脆弱性の起因となる一般的な失敗や欠陥を探します。

例として、構成の脆弱性に関するいくつかの高水準テストの現行のカテゴリーには、以下のようなものがあります。

- 特権
  - オブジェクト作成/使用権限
  - DBA および個々のユーザーに付与される特権
  - システム・レベル権限
- 認証
  - ユーザー・アカウントの使用
  - リモート・ログインの使用
  - パスワード規則

- 構成
  - データベース固有のパラメーター設定
  - システム・レベルのパラメーター設定
- バージョン
  - データベース・バージョン
  - データベース・パッチ・レベル
- オブジェクト
  - インストールしたサンプル・データベース
  - 推奨されるデータベース・レイアウト
  - データベース所有権

照会ベース・テスト

照会ベース・テストは、SQL 照会を定義または変更することで素早く簡単に作成できる事前定義またはユーザー定義のテストです。これらのテストは、データベースのデータ・ソースおよび結果に対して実行され、事前定義テスト値と比較されます。 ユーザー定義照会ベース・テストの作成に関する追加情報については、『照会ベース・テストの定義』を参照してください。

CAS ベース・テスト

CAS ベース・テストは、OS スクリプト・コマンド・タイプの CAS テンプレート項目に基づく事前定義またはユーザー定義のテストで、CAS 収集データを使用します。

ユーザーは、テンプレート項目を指定して CAS 結果の内容に対するテストを実行できます。 OS スクリプト・タイプの CAS テンプレートの作成については、『新規テンプレート・セット項目の作成』を参照してください。

Guardium には、CAS ベース・テストの作成に使用可能な、事前構成された OS スクリプト・タイプの CAS テンプレート項目もあります。 これらのテストは名前に「*Assessment*」という語が含まれており、「CAS テンプレート・セット定義」パネルから参照可能です。例えば、Unix/Oracle 用評価セットの名前は、Guardium Unix/Oracle Assessment になります。さらに、ファイル・アクセス権が関係する追加テンプレートも、アクセス権および所有権の検査に使用されます。 これらのテンプレート・セットを表示し、これらの OS スクリプト・タイプの項目を参照する方法については、『テンプレート・セット項目の変更』を参照してください。

Guardium で事前構成されたものを使用する場合であっても、独自に定義する場合であっても、定義されたテストは、CAS ベース・テストの作成または変更の際に選択項目として表示されます。 追加情報について、『CAS ベース・テストの定義』を参照してください。

CVE テスト

Guardium は、MITRE Corporation の提供する Common Vulnerabilities and Exposures (CVE) を常にモニターしています。 関連するデータベース関連の脆弱性を調べるために、これらのテストが追加されます。

- 照会ベース・テストの定義
  SQL ステートメントを実行する照会に基づいてテストを作成します。
- CAS ベース・テストの定義
  脆弱性評価では、CAS メカニズムを使用して、データベース・サーバーに対して OS レベルのテストを実行し、脆弱性を識別します。

親トピック: 評価および強化

照会ベース・テストの定義

SQL ステートメントを実行する照会に基づいてテストを作成します。

このタスクについて

以下のいずれかの方法で、新規照会ベース・テストを作成できます。

新規
: 作成を最初から開始してすべてのフィールドを定義します。

コピー
: 既存の照会ベース・テストをコピーします。

変更
: 既存の照会ベース・テストに変更を加えます。

手順

1. 「強化」 > 「脆弱性評価」 > 「アセスメント・ビルダー」をクリックし、「アセスメント・ビルダー」を開きます。
2. 「ユーザー定義テスト」から、「照会ベース・テスト」をクリックします。
3. 「新規」、「コピー」、「変更」のいずれかをクリックし、「照会ベース・テスト・ビルダー」を開きます。
4. 固有の「テスト名」を入力します。
5. 「データベース・タイプ」を選択します。
6. 「カテゴリー」を選択します。
7. 「重大度」を選択します。
8. オプション: テストの「簡略記述」を入力します。
9. オプション: テストの「外部参照」を入力します。
10. テストに合格したときに表示される「合格の結果テキスト」を入力します。
11. テストに不合格だったときに表示される「不合格の結果テキスト」を入力します。
12. テストで実行される「SQL ステートメント」を入力します。

    SQL ステートメント内でグループ・メンバーを追加および参照するには、以下の規則に従います。

例:

グループ MyUsersGroup に定義されたユーザーのグループを参照し、それを実際に使用されるグループ・メンバーで置き換えるには、次のようにします。

```
 Select ... from DBA_GRANTS where ... AND USER in (~~G~MyUsersGroup~~) and ...
```

この結果、以下のような SQL ステートメントが得られます。ここで、U1、U2 などは MyUsersGroup グループのメンバーです。

```
Select ... from DBA_GRANTS where ... AND USER in ('U1','U2','U3',...) and ...
```

グループにメンバーが存在しない場合、データベースはエラーを返します。 この場合、参照は、次のような一組の引用符に置き換えられます。

```
Select ... from DBA_GRANTS where ... AND USER in ('') and ...
```

以下の規則に従って、(特定のグループ・タイプの) 特定の別名への参照を実際の別名に置き換えます。

例:

Select ... from USER_OBJECTS where ... AND OBJECT_TYPE = '~~A~GroupType~TYPE~~'

グループ・タイプ GroupType の TYPE に別名がある場合、文字列がそれに置換されて、結果として以下のような SQL が得られます。

Select ... from USER_OBJECTS where ... AND OBJECT_TYPE = 'TYPE'

ここで、TYPE は実際の別名です。

13. オプション: 「詳細な SQL ステートメント」を入力します。この SQL ステートメントは、文字列のリストを取得して、「詳細の接頭部」+ 文字列リストから成る詳細文字列を生成するものです。「詳細の接頭部」の例を参照してください。
    注: 生成される詳細は、照会ベース・テストが失敗した時しか表示されません。これにより、ユーザーは、テストの失敗の原因になった情報を取得する SQL ステートメントを入力し、失敗の原因の特定に役立てることができます。
    注: 詳細文字列は、アセスメント・テスト名をクリックすることにより「セキュリティー・アセスメント結果」で確認できます。また、「テスト結果」エンティティーの「結果の詳細」属性により照会することもできます。
14. オプション: 「テスト前検査 SQL ステートメント」を入力します。このステートメントは、テストの実行前に実行されます。 このステートメントで 0 が返されると、テストは実行されません。 このテストで 1 またはエラーが返されると、テストが実行されます。
15. オプション: 「テスト前失敗メッセージ」を入力します。SQL ステートメントで 0 が返されたためにテストが実行されない場合は、このメッセージがアセスメント結果に挿入されます。
16. オプション: 「ループ・データベース」に、テストがループする必要があるデータベースのリストを入力します。 テストでは、指定したすべてのデータベースから返された結果の和集合または合計が返されます。 この関数は、テストで整数値が返され、かつ、データベース・タイプが Informix、SQL Server、Sybase SE、PostgreSQL および MySQL である場合にのみ使用できます。 ループは、「DB ループ・フラグ」ボックスにチェックマークが付いている場合に実行されます。 テストの実行時に、指定された 1 つ以上のデータベースが使用できないことがあります。 このような場合、テストでは、そのデータベースがスキップされて続行されるか、テストが停止して失敗メッセージが発行されます。これは、「エラーの場合はスキップ」ボックスにチェックマークが付いているかどうかによって異なります。
17. オプション: 詳細文字列の先頭に現れる「詳細の接頭部」を入力します。

```
「詳細な SQL ステートメント」および「詳細の接頭部」の例:
特定の権限を付与されたオブジェクトを検査するテスト。
詳細の接頭部: "Objects found with certain GRANT:"
詳細な SQL ステートメント: SELECT object FROM....--returning 4 records:
      Obj1
      Obj2
      Obj3
      Obj4
==> Details: Objects found with certain GRANT: Obj1, Obj2, Obj3, Obj4
```

18. オプション: SQL ステートメントに入力したテキストが、「比較値」との比較で使用される内部 Guardium® 変数にバインドされる値を返すプロシージャー型コード・ブロックである場合は、「出力変数のバインド」チェック・ボックスにチェック・マークを付けます。

```
例 (Oracle):
declare
    retval integer := 0;
    strval varchar2(255) := '';
    nver number;
    sver varchar2(255) := '';
begin
    select VERSION
    into sver
    from V$INSTANCE;
    nver := to_number(substr(sver,1,(instr(sver,'.',1,2) - 1)));
    if nver >= 11.1 then
        select VALUE
        into strval
        from V$PARAMETER
        where NAME = 'sec_case_sensitive_logon';
    end if;
    if (nver < 11.1 or strval = 'TRUE') then
        retval := 0;
    else
        retval := 1;
    end if;
    ? := retval;
end;
```

19. SQL ステートメントから返される「戻りの型」を選択します。
20. 条件に使用する「演算子」を選択します。
21. 「比較値」を入力します。この値は、比較演算子を使用して SQL ステートメントからの戻り値と比較するために使用されます。この比較によって、テストの合格/不合格が判定されます。 さらに、「RE」(regex) をクリックして、比較値を正規表現で定義することもできます。
22. 以下のいずれかを実行します。

- 「戻る」をクリックし、変更をキャンセルして前の画面に戻ります。
- 「適用」をクリックして、照会ベース・テストを保存します。

タスクの結果

この新規作成された照会ベース・テストをアセスメントに追加できます。

次のタスク

親トピック: 脆弱性評価のテスト

CAS ベース・テストの定義

脆弱性評価では、CAS メカニズムを使用して、データベース・サーバーに対して OS レベルのテストを実行し、脆弱性を識別します。

始める前に

このタスクについて

既存の CAS ベース・テストに変更を加えるか、作成を最初から開始してすべてのフィールドを定義することにより、新規 CAS ベース・テストを作成することができます。

手順

1. 「強化」 > 「脆弱性評価」 > 「アセスメント・ビルダー」をクリックし、「アセスメント・ビルダー」を開きます。
2. 「ユーザー定義テスト」から、「CAS ベース・テスト」をクリックして「CAS ベース・テスト・ファインダー」パネルを開きます。
3. 「新規」または「変更」をクリックして、新規テストを作成します。
4. 固有の「テスト名」を入力します。
5. 「データベース・タイプ」メニューからデータベースを選択します。
6. 「カテゴリー」メニューからカテゴリーを選択します。
7. 「重大度」メニューからカテゴリーを選択します。
8. オプション: テストの「簡略記述」を入力します。
9. オプション: テストの「外部参照」を入力します。
10. テストに合格したときに表示される「合格の結果テキスト」を入力します。
11. テストに不合格だったときに表示される「不合格の結果テキスト」を入力します。
12. テストに合格したときに表示される「合格の推奨テキスト」を入力します。
13. テストに不合格だったときに表示される「不合格の推奨テキスト」を入力します。不合格の推奨テキスト: クロスサイト・ハッキングを防止するため、「不合格の推奨テキスト」テキスト・ボックス内で expression、function、javascript、script、alert、eval、<img、ContentType のいずれかの名前が使用されている場合、その名前は書き直されます。
14. 「CAS テンプレート」メニューから、使用するテンプレートを選択します。
15. 「演算子」メニューから、使用する演算子を選択します。
16. 「検索文字列」に、CAS テンプレートから返される内容を比較するために演算子とともに使用する検索文字列を入力します。この比較によって、このテストの合格/不合格が判定されます。「RE」アイコンをクリックして、検索文字列に対して正規表現を定義することも可能です。
17. オプション: 検索文字列との一致があればテストを不合格にする場合は、「一致した場合に不合格」チェック・ボックスにチェック・マークを付けます。
18. 「適用」をクリックし、CAS ベース・テストを保存します。

タスクの結果

この新規作成された CAS ベース・テストをアセスメントに追加できます。
親トピック: 脆弱性評価のテスト

評価

アセスメントとは、データベース・インフラストラクチャーの脆弱性をスキャンし、リアルタイム測定と履歴測定によるデータベースおよびデータ・セキュリティーの正常性評価を行う一連のテストを指します。

- アセスメントの作成
  アセスメントの作成、既存のアセスメントの変更またはコピーを行います。
- 脆弱性評価テストの例外の作成
  セキュリティー・アセスメントからグループの特定メンバーを除外するには、テスト例外を使用します。例外グループに対してセキュリティー・アセスメントを実行すると、グループの特定メンバーがアセスメント結果に影響を及ぼしているかどうかを確認できます。これは、グループ設定を変更したくない場合や、変更が許可されていない場合に便利です。
- セキュリティー・アセスメントの作成方法
  選択したデータ・ソースに対してセキュリティー・アセスメントを実行することで、事前に脆弱性を特定および処置し、構成を改善し、インフラストラクチャーを強化します。
- アセスメントの実行
  アセスメントの結果を得るには、アセスメントを作成後に実行する必要があります。
- アセスメント結果の表示
  アセスメント結果の表示中に、さまざまなアクションを実行できます。
- VA サマリー
  以下の表に、 VA サマリー表に表示される各テストの情報およびデータベース・キーをリストします。ユニーク ID ごとのテスト結果、不合格になってからの累積経過日数、最初に不合格になった日付/ 最後に不合格になった日付、最後に合格した日付、および最後にスキャンされた日付などが示されます。この情報はトラッキングされ、ユーザーはこの情報に基づいてレポートを作成できます。

親トピック: 評価および強化

アセスメントの作成

アセスメントの作成、既存のアセスメントの変更またはコピーを行います。

始める前に

「強化」 > 「脆弱性評価」 > 「アセスメント・ビルダー」をクリックし、「アセスメント・ビルダー」を開きます。

このタスクについて

手順

1. 完全に新規のアセスメントを作成するには、「セキュリティー・アセスメント・ファインダー」パネルで「新規」をクリックします。 既存のアセスメントで作業をするには、「コピー」または「変更」をクリックします。 これらのいずれのボタンをクリックしても、「セキュリティー・アセスメント・ビルダー」パネルが開きます。 完全に新規のアセスメントを作成する場合は、以下のステップをすべて実行します。既存のアセスメントをコピーまたは変更する場合は、新規の記述を入力した後、変更したいフィールドのみを変更します。
2. そのアセスメントに固有の「記述」を入力します。
3. 「データ・ソースの追加」をクリックし、必要な情報を入力して「追加」をクリックすることにより、データ・ソースを追加します。
4. 「テストの構成」をクリックし、アセスメントにテストを追加します。
   a. 「追加できるテスト」ペインから、以前に追加したデータ・ソースの該当するタブを選択します。
   b. 必要なテストを選択し、「選択の追加」をクリックしてそれらをアセスメントに追加します。追加した選択内容は、「アセスメント・テスト選択」ペインに表示されます。
   c. 「アセスメント・テスト選択」を使用して、アセスメントのテストを管理します。選択したテストを削除したり、任意のテストに対して「このテストのチューニングを調整」をクリックし、そのテストのパラメーターをカスタマイズしたりすることができます。
5. アセスメントにロールを追加します。
   注: アセスメントには、そのベースのデータ・ソースにロールを割り当てるまでは、ロールを割り当てることができません。
6. 「適用」をクリックして、アセスメントを保存します。

   「CAS サポート」をクリックし、アセスメントに関する適切なデータを指定します。

   任意のアセスメントに対して「コメントの追加」を使用して、アセスメントに対して加えた変更の内容や理由を文書化および記録することもできます。

タスクの結果

これで新規のアセスメントを実行する準備ができました。
親トピック: 評価

脆弱性評価テストの例外の作成

セキュリティー・アセスメントからグループの特定メンバーを除外するには、テスト例外を使用します。例外グループに対してセキュリティー・アセスメントを実行すると、グループの特定メンバーがアセスメント結果に影響を及ぼしているかどうかを確認できます。これは、グループ設定を変更したくない場合や、変更が許可されていない場合に便利です。

手順

1. 「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」をクリックし、「グループ・ビルダー」を開きます。
2. 「グループ・タイプ」メニューから「脆弱性診断テストの例外」を選択し、事前定義された例外グループのリストを表示します。
3. 「既存グループの変更」メニューからグループを選択し、「変更」をクリックします。
4. 脆弱性評価テストから除外するグループ・メンバーを追加します。
5. 「強化」 > 「脆弱性評価」 > 「アセスメント・ビルダー」をクリックし、「アセスメント・ビルダー」を開きます。「セキュリティー・アセスメント・ファインダー」からアセスメントを選択し、「テストの構成」をクリックします。
6. 例外を追加したいテストを見つけ、「チューニング」列からそのテストの「このテストのチューニングを調整」ボタンをクリックします。
7. メニューから例外グループを選択し、「保存」をクリックします。アセスメントを再実行し、例外グループがテスト結果に影響を及ぼしているかどうかを確認します。
   注: デフォルトでは、Guardium には IBM iSeries プロファイル・ユーザー例外という例外グループが含まれています。このグループをコピーし、必要に応じて変更を加えることができます。

   すべてのデータベース・オブジェクト特権テストでは、Guardium グループからデフォルトのシステム・スキーマが除外されます。

親トピック: 評価

セキュリティー・アセスメントの作成方法

選択したデータ・ソースに対してセキュリティー・アセスメントを実行することで、事前に脆弱性を特定および処置し、構成を改善し、インフラストラクチャーを強化します。

このタスクについて

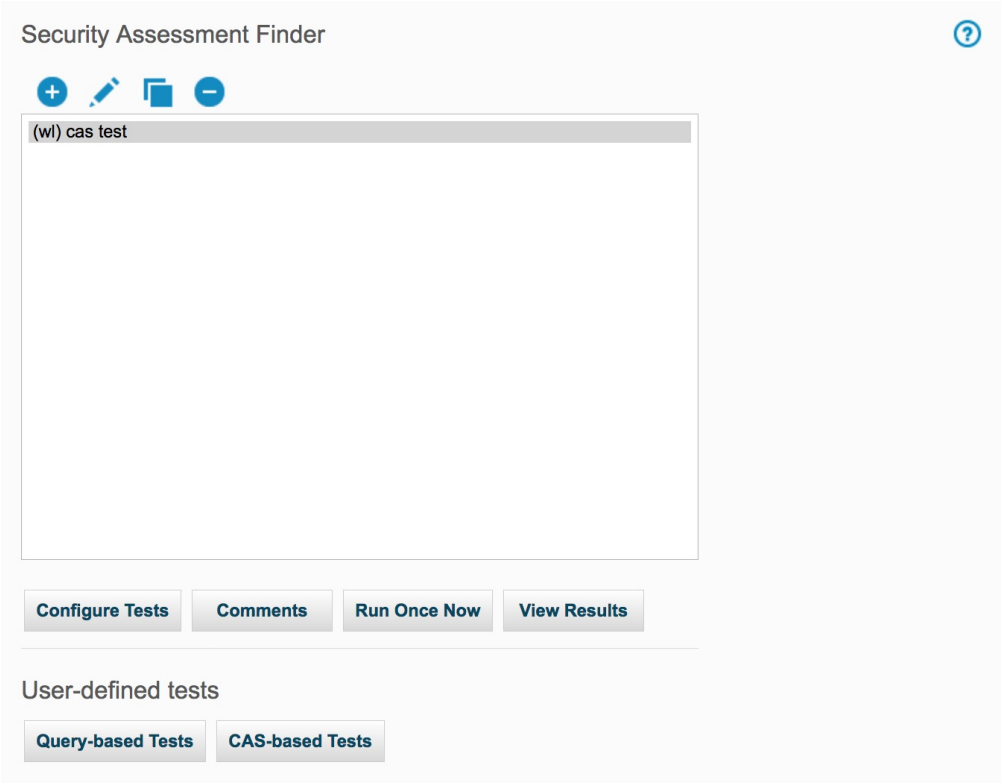
セキュリティー・アセスメントを作成するための基本的なステップは、以下のとおりです。

1. アセスメントの作成

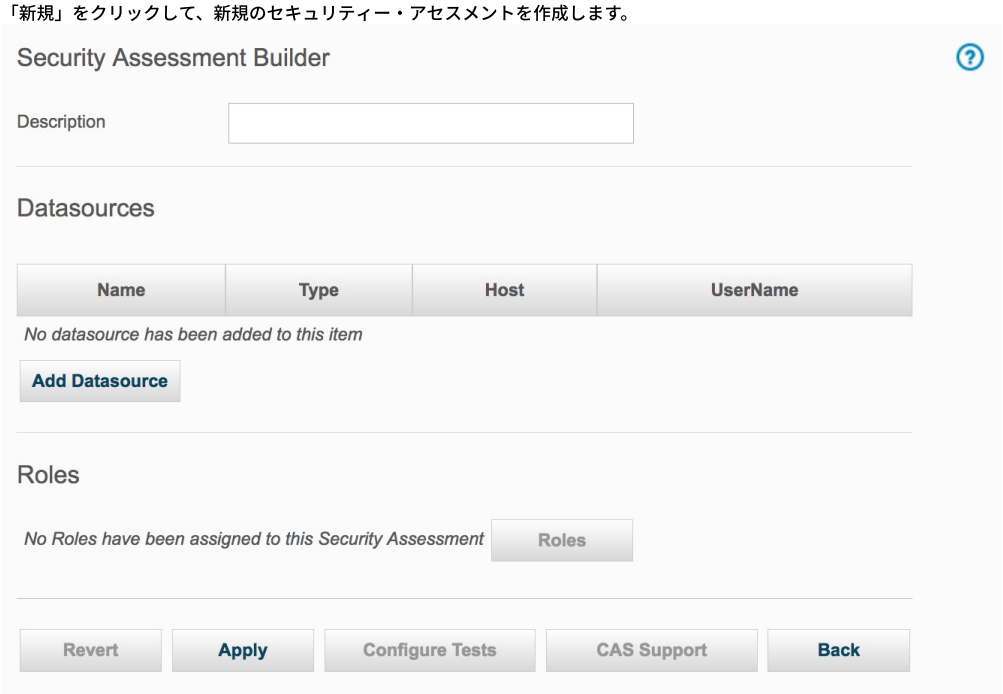
2. アセスメントへのデータ・ソースの追加
3. アセスメントへのテストの追加

手順

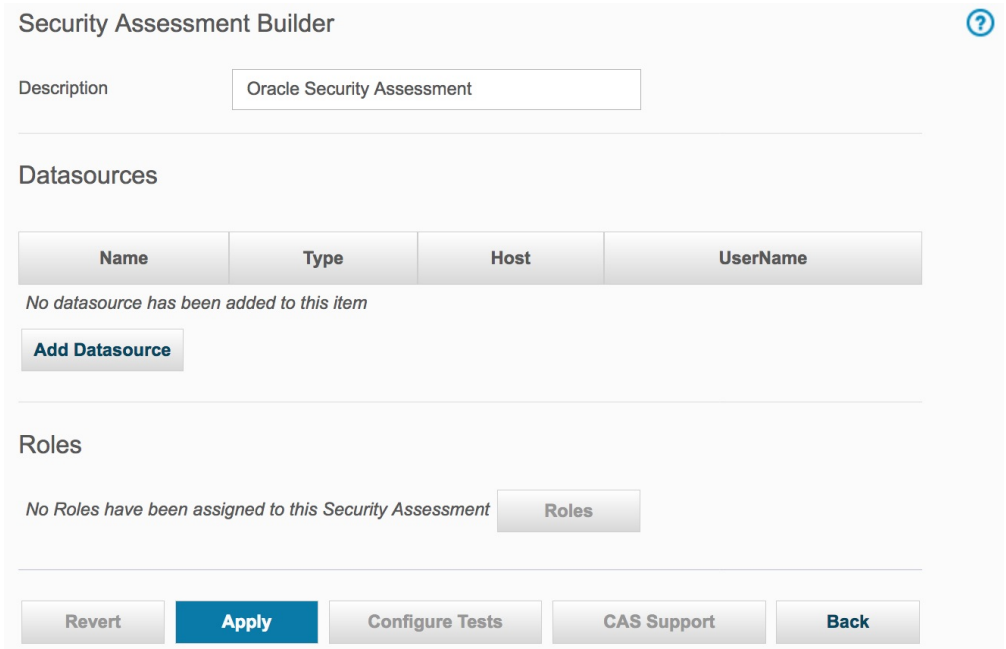
1. 「アセスメント・ビルダー」を開いて、アセスメントを作成または変更します。「強化」 > 「脆弱性評価」 > 「アセスメント・ビルダー」をクリックし、「アセスメント・ビルダー」を開きます。



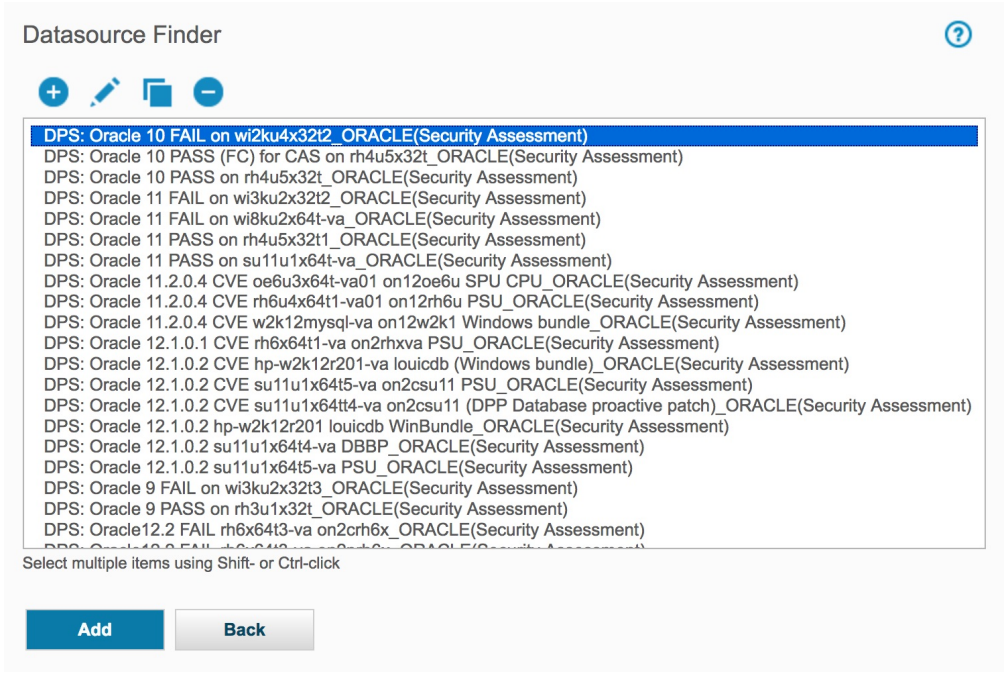
2. 「新規」をクリックして、新規のセキュリティー・アセスメントを作成します。



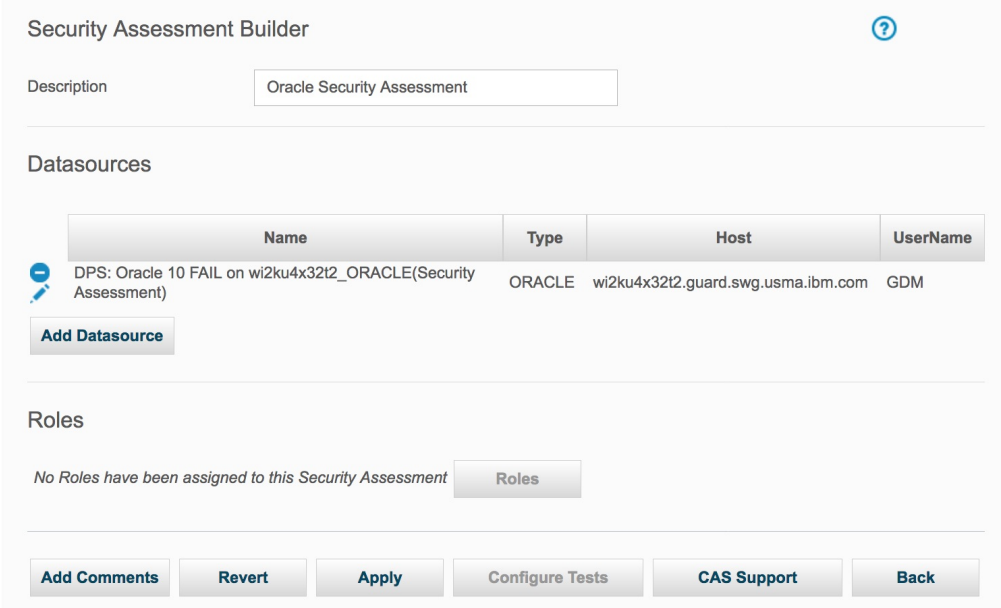
3. 「記述」にアセスメントの固有の名前を入力し、「適用」をクリックしてアセスメントを保存します。



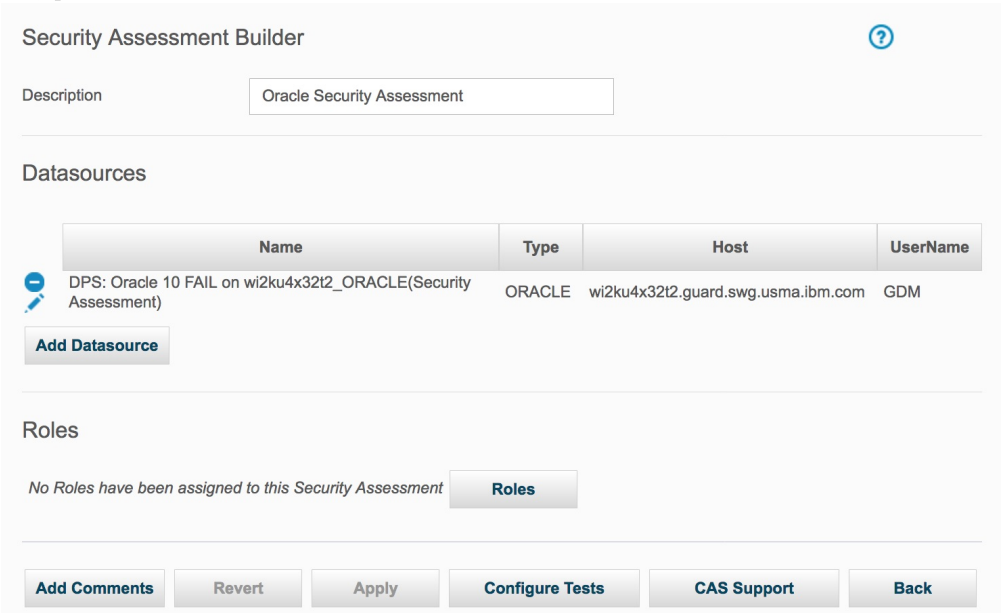
4. 「データ・ソースの追加」をクリックし、アセスメントにデータ・ソースを追加します。「データ・ソース・ファインダー」からデータ・ソースを選択し、「追加」をクリックします。新規データ・ソースを追加するには、 をクリックし、「データベース定義」ウィンドウで情報を入力して、「適用」をクリックします。 詳しくは、『データ・ソース』を参照してください。



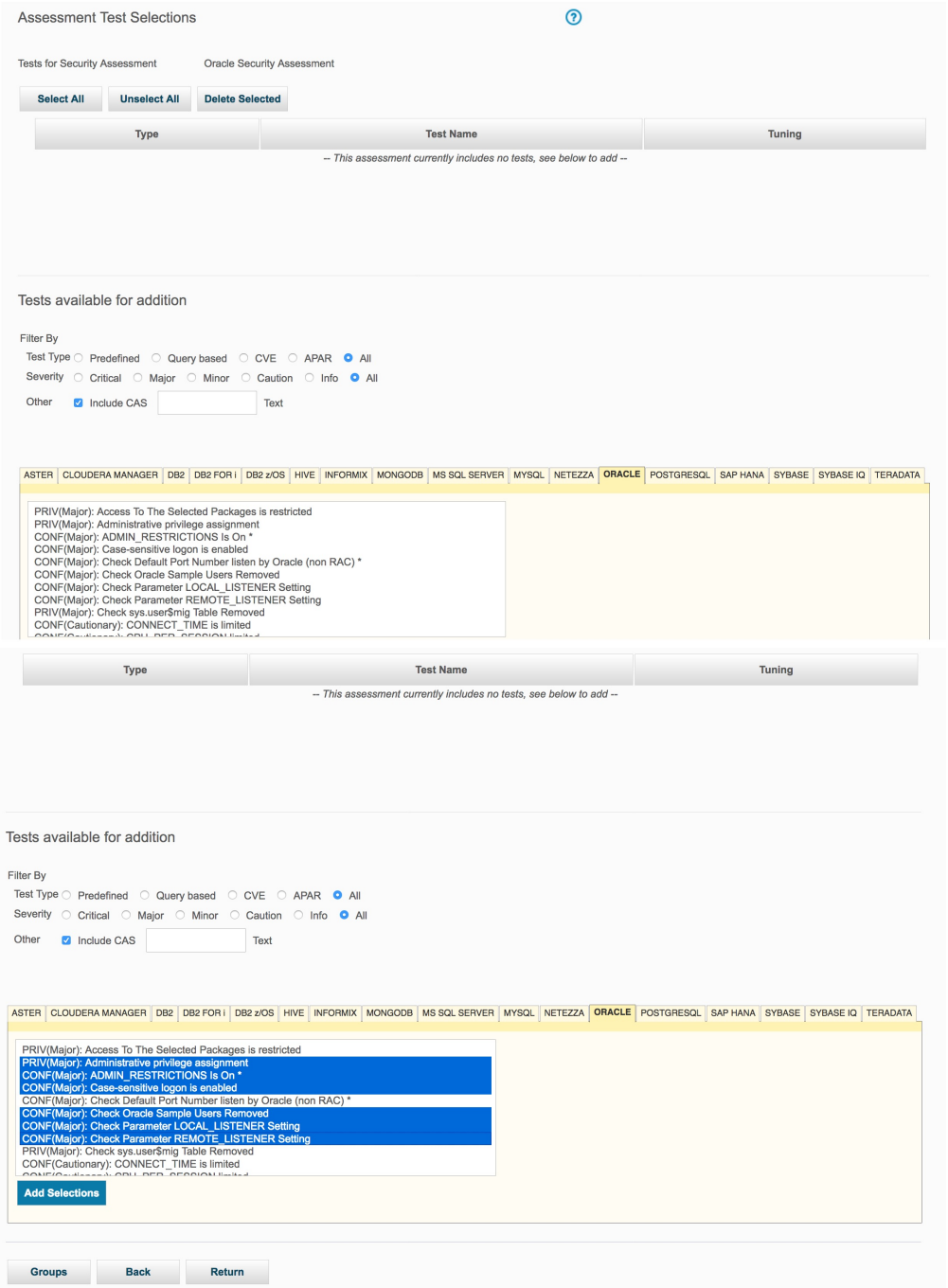
「追加」ボタンをクリックすると、セキュリティー・アセスメント・ビルダーの「データ・ソース」セクションにデータ・ソースが表示されます。

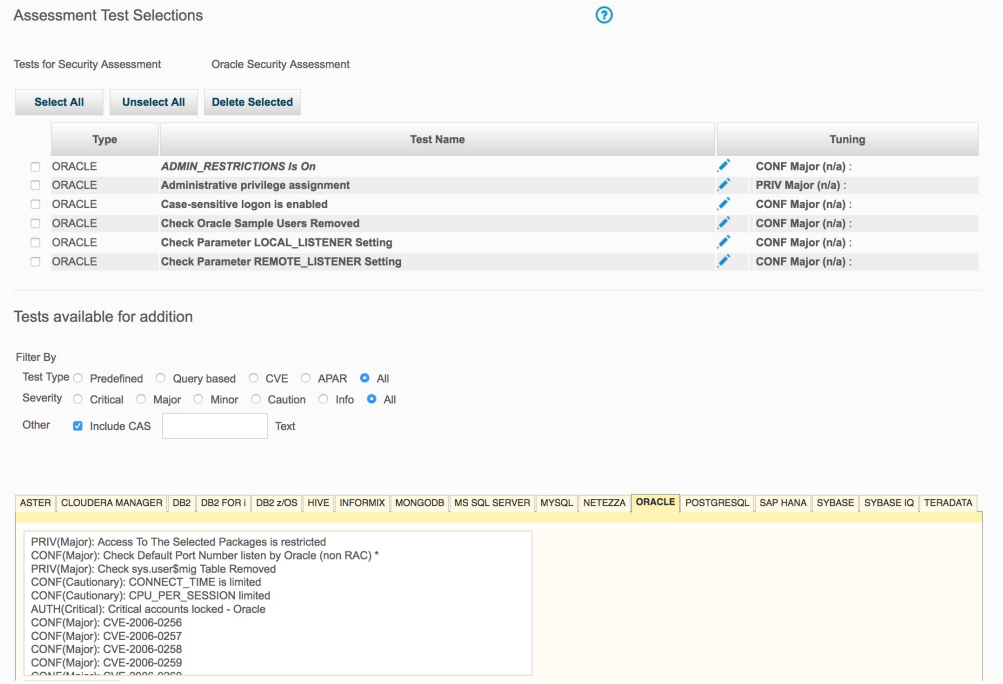


5. 「適用」をクリックして、アセスメントを保存します。



6. 「テストの構成」をクリックして、評価にテストを追加します。 「追加できるテスト」パネルで、作成した適切なデータ・ソースを示すタブをクリックし、アセスメントに追加するテストを選択して、「選択の追加」をクリックします。追加するテストをフィルタリングするには、ラジオ・ボタンを使用します。詳しくは、『事前定義テスト』、『照会ベース・テスト』、『CVE テスト』、または『APAR テスト (APAR Tests)』を参照してください。


Assessment Test Selections
Tests for Security Assessment
Oracle Security Assessment
Select All
Unselect All
Delete Selected
Type
Test Name
Tuning
-- This assessment currently includes no tests, see below to add --
Tests available for addition
Filter By
Test Type Predefined Query based CVE APAR All
Severity Critical Major Minor Caution Info All
Other Include CAS Text
ASTER CLOUDERA MANAGER DB2 DB2 FOR i DB2 z/OS HIVE INFORMIX MONGODB MS SQL SERVER MYSQL NETEZZA ORACLE POSTGRESQL SAP HANA SYBASE SYBASE IQ TERADATA
PRIV(Major): Access To The Selected Packages is restricted
PRIV(Major): Administrative privilege assignment
CONF(Major): ADMIN_RESTRICTIONS Is On *
CONF(Major): Case-sensitive logon is enabled
CONF(Major): Check Default Port Number listen by Oracle (non RAC) *
CONF(Major): Check Oracle Sample Users Removed
CONF(Major): Check Parameter LOCAL_LISTENER Setting
CONF(Major): Check Parameter REMOTE_LISTENER Setting
PRIV(Major): Check sys.user$mig Table Removed
CONF(Cautionary): CONNECT_TIME is limited
Type
Test Name
Tuning
-- This assessment currently includes no tests, see below to add --
Tests available for addition
Filter By
Test Type Predefined Query based CVE APAR All
Severity Critical Major Minor Caution Info All
Other Include CAS Text
ASTER CLOUDERA MANAGER DB2 DB2 FOR i DB2 z/OS HIVE INFORMIX MONGODB MS SQL SERVER MYSQL NETEZZA ORACLE POSTGRESQL SAP HANA SYBASE SYBASE IQ TERADATA
PRIV(Major): Access To The Selected Packages is restricted
PRIV(Major): Administrative privilege assignment
CONF(Major): ADMIN_RESTRICTIONS Is On *
CONF(Major): Case-sensitive logon is enabled
CONF(Major): Check Default Port Number listen by Oracle (non RAC) *
CONF(Major): Check Oracle Sample Users Removed
CONF(Major): Check Parameter LOCAL_LISTENER Setting
CONF(Major): Check Parameter REMOTE_LISTENER Setting
PRIV(Major): Check sys.user$mig Table Removed
CONF(Cautionary): CONNECT_TIME is limited
Add Selections
Groups
Back
Return



7. 「戻る」をクリックしてセキュリティー・アセスメント・ビルダーに戻り、「ロール」をクリックして、アセスメントにロールを追加します。
   注: アセスメントには、そのベースのデータ・ソースにロールを割り当てるまでは、ロールを割り当てることができません。
8. 「適用」をクリックしてアセスメントを保存します。これで、選択したデータ・ソースに対して、このアセスメントを実行することができます。

親トピック: 評価

アセスメントの実行

アセスメントの結果を得るには、アセスメントを作成後に実行する必要があります。

アセスメントは、シリアライズ・モードで 1 つずつ順番に実行されます。複数のアセスメントの実行をスケジュールに入れる場合、キューに入れる必要があります。 このキューは、Guardium のジョブ・キュー・レポートで表示できます。

「今すぐ 1 回実行」ボタンをクリックすると、そのアセスメントがキューに入れられ、直ちに実行されます。短時間で、ジョブが実行されて表示可能になります。アセスメントの結果について詳しくは、『アセスメント結果の表示』を参照してください。

オプションで、アセスメント定義の実行の自動化プロセスを定義し、スケジュールに入れることができます。 「監査プロセス・ファインダー」パネルから操作を開始して、監査プロセス・スケジュールの作成や変更を行います。 アセスメントを自動的に実行するスケジュールを作成するには、「監査プロセス・ファインダー」パネルに移動します。 監査プロセスの定義について詳しくは、『コンプライアンス・ワークフロー自動化』を参照してください。

親トピック: 評価

アセスメント結果の表示

アセスメント結果の表示中に、さまざまなアクションを実行できます。

アセスメント結果の表示

「レポート・ビルダー」でアセスメントの結果を表示します。「強化」 > 「レポート」 > 「レポート・ビルダー」をクリックして「レポート・ビルダー」を開き、フィルターを使用して必要なレポートを見つけます。

アセスメント結果の解釈

アセスメントでは、複数のレポートに基づいて複数のテストを評価します。結果全体は、「セキュリティー・アセスメントの結果」というタイトルが付いた別個のブラウザー・ウィンドウに表示されます。そのウィンドウには以下のセクションがあります。

アセスメント ID

アセスメント結果には、以下の情報が示されます。

- アセスメント名
- アセスメントを実行した日時
- アセスメントの期間
- クライアントおよびサーバーの IP アドレスまたはサブネット

アセスメントの選択

ドロップダウン・メニューを使用して、アセスメントの過去の結果を選択して表示します。デフォルトでは最新の結果が表示されます。

アセスメント結果履歴

「アセスメント結果履歴」にはある期間にわたるテストの合格率が表示されます。テストの合格率をさらに改善するための推奨事項が「アセスメント・テスト結果」セクションの下に表示されます。

ログの表示

これをクリックすると、新しいウィンドウに、アセスメント・テストのランタイム実行を示す「実行ログ」が表示されます。イベントとメッセージのタイム・スタンプは、特定のテストが不合格になった原因と考えられる問題をデバッグするときに役立ちます。

結果のサマリー

表形式のグラフにより、このアセスメントで実行されたすべてのテストの要約が示されます。x 軸はテストの重大度 (クリティカル、メジャー、マイナー、注意、または情報) を表します。y 軸はテストのタイプ (特権、認証、構成、バージョン、またはその他) を表します。 グリッド内に、テストの実行試行時に合格、不合格、あるいはエラーとなったテストの回数がそれぞれ示されます。 これらの数値は、「アセスメント・テスト結果」セクションの下に示されるアセスメント・テストの詳細に直接関連しています。

現在適用されているフィルタリング

フィルタリングを現在の適用内容から変更したい場合は、以下の 2 つのオプションを使用し、必要に応じて結果をフィルターに掛けます。

フィルタリングのリセット -「フィルター/ソート制御」オプションで選択されたフィルタリング・オプションをすべて削除します。

フィルター/ソート制御 - これを使用して、レポートのフィルター/ ソート・オプションを開きます。オプションを使用すると、「重大度」、データ・ソース重大度分類 (「DS 重大度分類」)、「スコア」(合格、不合格、またはエラー)、および「テスト・タイプ」(監視/データベース・タイプ) ごとにフィルター操作ができます。ソート・オプションを使用すると、重大度、スコア、およびデータ・ソースを組み合わせたソートを実行できます。選択したフィルター/ソート・オプションを有効にするには、「適用」をクリックします。

アセスメント・テスト結果

「アセスメント・テスト結果」セクションでは、実行したテストの詳細な説明、ターゲット・データ・ソースとデータ・ソース重大度分類に関する情報、およびテストの合格/不合格状況、重大度、外部参照、および現在状況の理由が示されます。各テスト名はクリックできるようになっていて、その特定のテストについての関連情報以外のすべての情報をレポートからフィルター除去することができます。 「理由」フィールドには吹き出しヘルプ機能があり、不合格またはエラーになったテストに対する改善策に役立つ推奨事項が表示されます。

アセスメント結果には、以下の各カテゴリー内のテスト数と合格したテスト数のカウントが含まれます。

- CIS テスト
- CVE テスト
- STIG テスト

これらの値は、アセスメント結果ビューアーに表示され、VA 結果ドメインの一部としてレポートの作成に使用できます。

データ・ソース詳細

「データ・ソース詳細」セクションを展開すると、このアセスメントで参照されているすべてのデータ・ソースが表示され、それと共にデータ・ソース固有の環境情報が示されます。

CVE および CVSS 情報

アセスメント・テスト結果ビューアーには、CVE レコードおよび CVSS 情報が表示されます。

参照リンクはクリックできます (新しいウィンドウが開きます)。対応するレコードが結果に含まれていない場合は、いずれのセクションも表示されません。

重要な CVSS フィールドは以下のとおりです。

- CVSS スコア
- アクセスの複雑性
- 可用性への影響
- 機密性への影響
- 保全性への影響
- 認証
- アクセス・ベンダー
- ソース
- 生成日時

不合格だったテストの処理

アセスメントで一部のテストに不合格状況が表示される場合、以下のいずれかのアクションを実行できます。

テストの例外を追加する
: このアクションを実行すると、一定期間、テストは必ず合格になります。 例えば、最新の使用可能なサービス更新が適用されていることを確認するテストで不合格となるサーバーのグループがあるとします。 週末のメンテナンス・ウィンドウまで、更新を適用することはできません。 それまでテストで不合格となり続けるのは望ましくありません。 結果パネル内の「不合格」という単語を右クリックすると、「テスト例外の追加」ポップアップ・メニューが表示されます。 例外の終了日時を指定し、オプションでコメントを指定します。 テストがこのアセスメントから実行されるか、あるいは別のアセスメントの一部として実行されるかに関係なく、例外の期限切れ前にテストが実行されるたびに、すべてのデータ・ソースでテストは合格となります。

不合格の要素を例外グループに追加する

テストで不合格となった場合、テストの名前をクリックすると、さらに情報を表示できます。 新規パネルに、「詳細」というタイトルのエリアが含まれます。このヘッダーの下に、不合格となったテストの要素が表示されます。要素が表示された場合は、それらをこのテストの例外グループに追加できます。 これを行うには、ヘッダー「詳細:」をクリックして新規ダイアログを開きます。 このダイアログに不合格の要素が表示され、各要素に 1 つのチェック・ボックスがあります。 例外グループに追加する要素のチェック・ボックスにチェック・マークを付け、他のチェック・ボックスのチェック・マークを外します。 次に、グループを選択します。このテストにデフォルトの例外グループが定義されている場合は、それがダイアログに表示され、事前選択されています。 ドロップダウン・リストには、定義されている他のすべてのタイプ VA テスト例外のグループが表示されます。 リストからグループを選択するには、リストの横のラジオ・ボタンをクリックし、リストからグループを選択します。 「保存」をクリックして、選択項目を実装します。 残りの要素を別のグループに追加するには、再度「詳細」をクリックします。

PDF へのエクスポート、あるいは SCAP または AXIS XML へのエクスポート

「PDF のダウンロード」をクリックすると、アセスメント結果の PDF バージョンを生成できます。

「XML のダウンロード」ボタンを使用して、2 つのメニュー選択項目 (「SCAP xml としてダウンロード」と「AXIS xml としてダウンロード」) を開きます。 それらの選択項目のいずれかを選んで、表示されているアセスメント結果を表す XML ファイルをワークステーションにダウンロードします。 このファイルは、Security Content Automation Protocol (SCAP) XML または QRadar で使用される Apache EXtensible Interaction System (AXIS) XML 用にフォーマットされます。

親トピック: 評価

VA サマリー

以下の表に、 VA サマリー表に表示される各テストの情報およびデータベース・キーをリストします。ユニーク ID ごとのテスト結果、不合格になってからの累積経過日数、最初に不合格になった日付/ 最後に不合格になった日付、最後に合格した日付、および最後にスキャンされた日付などが示されます。この情報はトラッキングされ、ユーザーはこの情報に基づいてレポートを作成できます。

VA サマリー

キーには、3 つのオリジナル要素に加えて、データ・ソース名が含まれる場合があります。デフォルトは、ホスト、ポート、およびインスタンス名です。

クエリー・ビルダーで VA サマリー・トラッキングを使用して、 照会およびレポートを定義します。

この表はエクスポート/インポートできます。インポート・データは、 Guardium システムの既存データをオーバーライドします (キーごと)。

表 1. VA サマリー

表の列	タイプ	記述
VA_SUMMARY_ID	Int	自動増加 - 主キー
DATA_SOURCE_HASH	Varchar(40)	キーのハッシュ
DB_TYPE	Varchar	データベース・タイプ
SERVICE_NAME	Varchar	データベース・インスタンス名 (キーの一部である場合、そうでない場合は「N/A」)
DB_PORT	Varchar	データベース・ポート (キーの一部である場合、そうでない場合は「N/A」)
DB_HOST	Varchar	ホスト/IP (キーの一部である場合、そうでない場合は「N/A」)
TEST_ID	Int	テストの ID
FIRST_EXECUTION	DateTime	テストが最初に実行された時
LAST_EXECUTION	DateTime	テストが最後に実行された時
FIRST_FAIL	DateTime	この DB に関してテストが最初に不合格になった時
LAST_FAIL	DateTime	この DB に関してテストが最後に不合格になった時
FIRST_PASS	DateTime	この DB に関してテストが最初に合格した時
LAST_PASS	DateTime	この DB に関してテストが最後に合格した時
CURRENT_SCORE	varchar	合格 / 不合格 / エラー
CURRENT_SCORE_SINCE	Datetime	テストが現行の状況になった日付
CUMULATIVE_FAIL_AGE	Int	不合格になってからの累積経過日数
CUMULATIVE_PASS_AGE	Int	合格してからの累積経過日数

CLI コマンドは、store va_test_show_query および show va_test_show_query です。export va_summary は、この情報をエクスポートするときに使用します。

キーを変更または表示する GuardAPI コマンドは、 grdapi modify_va_summary_key および grdapi reset_va_summary_by_key です。 合格および不合格の両方に関する累積経過日数をリセットする GuardAPI コマンドは、 grdapi reset_va_summary_by_id です。この情報をエクスポートするときには grdapi export_va_summary を使用します。

grdapi reset_va_summary_by_ke および grdapi modify_va_summary_key に、追加のパラメーター datasourceName が追加されました。

VA サマリーのエンティティーは追加の属性 Datasource Name を持ちます。Datasource Name にデータが設定されるのは、データソース名がキーの一部である場合のみです。

注: GrdAPI コマンド modify_va_summary_key の 4 つのパラメーター (useHost、usePort、useServiceName、useDatasourceName) のすべてに false を指定して呼び出すと、キーを空にすることができます。この場合、キーが空になると、VA サマリーの計算は無効になります (サマリー・データの計算、更新、保存は行われません)。

親トピック: 評価

必要とされるスキーマ変更

Guardium V9.1 では、IBM DB2 for z/OS 上での脆弱性評価テストで使用されるスキーマが変更されています。9.1 より前のリリースからアップグレードする場合、これらのテストを引き続き使用するためには、データベースを更新する必要があります。

このタスクについて

ご使用の Guardium システムをバージョン 10.x にアップグレードする場合は、データベース・サーバー上に新しいデータベース表を作成する必要があります。 これらの表により、新しいテスト・セットに対するサポートが追加されますが、新しいテストを使用するかどうかにかかわらず、これらの表を作成する必要があります。
前のリリースでは、次の表は gdmmonitor スキーマで作成され、データが設定されました。

- GDMMONITOR.OS_GROUP
- GDMMONITOR.OS_USER

これらの表は、次の CKADBVA スキーマの表に置き換えられます。

- CKADBVA.CKA_OS_GROUP
- CKADBVA.CKA_OS_USER

手順

1. Install Guardium 10.x
2. ご使用の Guardiumシステムの /var/log/guard/gdmmonitor_scripts ディレクトリーから、create_CKADBVA-schema_tables_zOS.sql を データベース・サーバーにコピーします。 データベース・サーバー上で、fileserver コマンドを実行して、このファイルを取得します。
3. スクリプトには、スクリプトの実行の前後に実行すべきステップを説明した指示が含まれています。これらの指示をよく読んで、スクリプトを実行します。
4. 新しい表に、元の表に格納されていたデータと同様のデータを設定します。

タスクの結果

これで、現行の脆弱性評価テストを使用するようにシステムが構成されました。

次のタスク

親トピック: 評価および強化

RACF の脆弱性の評価

IBM DB2 for z/OS を使用する場合は、脆弱性評価テストで RACF の脆弱性を評価することができます。RACF アセスメントを使用するには、少なくともバージョン 9.1 の Guardium がインストールされている必要があります。

このタスクについて

リソース・アクセス管理機能 (RACF) 特権がデータベース内で付与されたのかデータベース外で付与されたのかを評価します。 RACF 脆弱性評価を構成するこのテストでは、オブジェクト特権、データベース特権、およびシステム特権のアクセス制御が識別されます。

これらのテストを使用するためには、IBM Security zSecure Audit バージョン 2.1 を入手し、インストールする必要があります。 この製品は、これらのテストで RACF との対話に使用されるコマンドを使用可能にします。

資格を検査するテストでは、合格/不合格のグレードは返されません。資格を持つユーザーのリストが返されます。 これらのレポートのサンプルには、被付与者に付与された表特権およびビュー特権と、被付与者に付与されたパッケージ特権が含まれています。非常に多数のユーザーやアプリケーションが含まれている大規模な環境では、これらのレポートによって膨大な量のデータが生成されます。このような大規模な環境でこれらのレポートを実行すると、プロセスが長い時間実行され、大量のリソースが消費される可能性があり、最終的にタイムアウトになることがあります。

手順

1. データベース・サーバー上で脆弱性評価をサポートするために使用されるデータベース・スキーマをアップグレードします。
2. データベース・サーバーに zSecure Audit をインストールします。 zSecure Audit に付属している説明とツールを使用して、新しい zSecure テストをサポートするために、CKADBVA スキーマの およそ 24 個の表にデータを設定する方法を確認します。
3. zSecure チームは、zSecure Audit と Guardium 脆弱性評価との連携を可能にする PTF を発行します。この PTF を入手し、付属している説明に従って PTF を適用します。

タスクの結果

これでシステムが、新しい zSecure テストを活用するように構成されます。

次のタスク

実行する新しいテストを選択して、RACF の脆弱性を評価します。テストを構成し、実行します。

親トピック: 評価および強化

構成監査システム

CAS はそのような変更をトラッキングして、それについて報告します。このデータは Guardium システム上で使用可能であり、レポートやアラートに使用できます。

構成監査システムの概要

データベースはサーバー環境の変更によって影響を受ける場合があります。例えば、構成ファイル、環境変数やレジストリー変数、他のデータベース・コンポーネントやオペレーティング・システムのコンポーネント (データベース管理システムやオペレーティング・システムが使用する実行可能ファイルやスクリプトを含む) の変更があります。CAS はそのような変更をトラッキングして、それについて報告します。このデータは Guardium システム上で使用可能であり、レポートやアラートに使用できます。

注: 脆弱性評価 (VA) および構成監査システム (CAS) は、英語のみでサポートされています。

CAS エージェント

CAS はデータベース・サーバー上にインストールされたエージェントであり、モニター対象のエンティティーの内容、所有権、またはアクセス権に変更が加えられるたびに、Guardium システムに報告します。CAS クライアントは、S-TAP® のインストールで使用するのと同じユーティリティーを使用して、データベース・サーバー・システム上にインストールします。CAS と S-TAP は互いに独立して実行されますが、構成情報はコンポーネント間で共有します。 CAS クライアントをホスト上にインストールした後、実際の変更監査機能を Guardium® ポータルで構成します。

CAS サーバー

CAS サーバーは、Guardium のコンポーネントであり、Guardium システム上で稼働します。これは、Tomcat アプリケーション・サーバーとは関係なく、スタンドアロン・プロセスとして実行されます。 また、inittab ファイルを介して制御されます。

CAS サーバーは、Guardium システム上の少数の使用可能なプロセッサーを使用するように構成されています。CAS で使用されるプロセッサーの数は、*divide_num_of_processors_by* パラメーターを使用して決定されます。 このパラメーターは cas.server.config.properties ファイルに保管されます。そのデフォルト値は 2 です。Guardium システム上で使用可能なプロセッサーの数がこの値で除算されます。これにより、割り振られたプロセッサー上で CAS によって CPU が 100% 使用されている場合でも、残りのプロセッサーを他のアプリケーションで使用できるようになります。

CAS サーバー認証

Guardium は、SSL で提供される基本セキュリティーに加え、データベース・サーバー上で実行される CAS クライアント上での CAS サーバー認証をサポートします。 これは、CAS クライアントが Guardium の CAS サーバーとのみ通信することを保証するものとなります。 非認証接続および共通名 (CN) の不一致は CAS ログ・ファイルで報告されます。

この構成を行うと、CAS サーバー始動時には、署名済み証明書が秘密鍵とともにそこにロードされ、接続を受け入れるサーバー・ソケットにそれらが割り当てられます。データベース・サーバー側にある CAS クライアントは、以下の接続モードをサポートします。

1. 非セキュア接続 (use_tls='0')
2. 認証なしのセキュア接続 (use_tls ='1', guardium_ca_path=NULL)。このモードでは、CAS サーバーとの通信手段として SSL の使用が強制されます (つまり、サーバー認証なしの SSL の使用)。
3. サーバー認証付きセキュア接続 (use_tls ='1', guardium_ca_path=<public key location>)。CAS クライアントは CAS サーバーを認証するために公開鍵を使用します。この公開鍵 (ca.cert.pem) は <install_dir>/etc/pki/certs/trusted の下に配置されます。

   ca.cert.pem はルート認証局証明書 (自己署名されたもの) を格納したファイルです。これは、ブラウザーにおけるトラステッド CA 証明書 (VeriSign の証明書など) に相当します。

   すべての gmachine 証明書はルート認証局によって発行/署名されます。このようにして、証明書は検証され、トラスト・チェーンが確立されます。

   guardium_ca_path には、実際の公開鍵ファイル名を示す絶対パスを設定することもできますし、単にディレクトリー名 (<install_dir>/etc/pki/certs/trusted) を設定することもできます。ディレクトリー名の場合、そのディレクトリーの中にあるすべての公開鍵がサーバーの認証に使用されます。 公開鍵が存在しないファイルまたはディレクトリーを guardium_ca_path に設定すると、接続を試行しても失敗します。

4. サーバー認証付きセキュア接続と共通名検証。 このモードには追加検査があり、サーバーからの証明書 CN はパラメーター sqlguard_cert_cn で設定された CN と比較されます。 sqlguard_cert_cn が NULL または空である場合、この検査は使用不可になります。 それ以外の場合、Guardium の自己署名証明書が持つのと同じ CN ('gmachine') が設定されていることが必要です。

注: ここに記載されているパラメーターはすべて guard_tap.ini ファイルに含まれています。

CAS での SSL の使用

CAS エージェントは、CAS サーバーにデータを送信する際に Secure Sockets Layer (SSL) 接続を使用するように構成できます。 バージョン 10.1 でインストールされた CAS サーバーは、米国連邦情報処理標準 140-2 (FIPS 140-2) の要件に準拠しています。SSL を使用してこの CAS サーバーと通信できるのは、FIPS 準拠の CAS エージェントだけです。 このアプローチを使用する場合は、ご使用の CAS エージェントをこのパッチとともに配布されたバージョンにアップグレードする必要があります。 また、CAS エージェントが実行されているサーバーに IBM Java がインストール済みでなければなりません。さらに、CAS エージェントがそれを使用するように構成されている必要があります。 FIPS 通信を使用するためには、証明書ベースの認証を使用している必要があります。

古い CAS エージェントで、SSL を使用して、更新済みの CAS サーバーと通信しようとすると、CAS エージェント・システム上のログ・ファイルに次のメッセージが表示されます。

```
javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure
```

Guardium システム上の CAS ログ・ファイルに次のメッセージが表示されることもあります。

```
javax.net.ssl.SSLHandshakeException: Client requested protocol SSLv3 not
enabled or not supported
```

CAS エージェントと CAS サーバーの間で非 SSL 接続を使用する場合は、引き続き既存の CAS エージェントを使用できます。

テンプレート・セット

CAS テンプレート・セットには、一緒に組み込まれている項目テンプレートのリストが含まれていて、特定のタイプのデータベース (UNIX 上の Oracle など) のモニターなどの共通の目的を共有しています。このセットは次の 2 つのタイプのいずれかです。

- オペレーティング・システムのみ (UNIX または Windows)
- データベース (UNIX-Oracle、Windows-Oracle、UNIX-Db2、Windows-Db2 など)

データベース・テンプレート・セットは、データベース・タイプとオペレーティング・システム・タイプのどちらの場合も常に固有のものです。

CAS テンプレート項目

単一のモニター対象エンティティーに対するモニター・タスクの定義または属性セット。ユーザーは、新規の CAS テンプレートを作成して新しい CAS テストを定義することも、変更可能な事前定義 CAS テンプレートを使用することもできます。

テンプレート項目は、特定のファイルまたはファイル・パターン、環境変数またはレジストリー変数、OS スクリプトまたは SQL スクリプトの出力、あるいはログインしたユーザーのリストです。 これらの項目すべての状態は、生データ、つまりファイルの内容やレジストリー変数の値などによって影響を受けます。 CAS は、生データのサイズを検査するか、または生データのチェックサムを計算することによって、変更を検出します。 ファイルの場合は、ファイルの所有権、アクセス許可、パスなどの CAS はシステム・レベルの変更も検査します。

すべてのユニット (コレクターとアグリゲーター) が 1 つのマネージャーによって管理されるフェデレーテッド環境では、すべてのテンプレートはコレクターとアグリゲーターの両方で共有され、CAS データはレポート作成や脆弱性評価に使用できます。 コレクターとアグリゲーター (またはアーカイブされるデータがリストアされるホスト) が同一管理クラスターの一部ではない場合、テンプレートは共有されません。それで、CAS データは、たとえデータが存在していたとしても脆弱性評価には使用できなくなります。これを改善するには、定義のエクスポート/インポートを使用してテンプレートをコレクターからアグリゲーター (またはリストア・ターゲット) にコピーします。

注: クライアントあたり、10,000 を超えるファイルをモニターするように CAS に要求しないでください。
注: 処理するモニター対象のファイル数が、1 時間あたり 1,000 以下になるように、 CAS を構成することをお勧めします。

モニター対象エンティティー

モニター対象にできる実際のエンティティーとしては、1 つのファイル (その内容とプロパティー)、環境変数の値または Windows レジストリーの値、さらに OS のコマンドやスクリプトと SQL ステートメントからの出力が挙げられます。

CAS インスタンス

特定のホスト (そのテンプレート・セットのインスタンスの作成と特定のホスト上への適用を行うホスト) への CAS テンプレート・セットの適用

CAS 構成

CAS 構成によって 1 つ以上の CAS インスタンスが定義されます。各インスタンスは、ホスト上のセットになった項目をモニターするために使用されるテンプレート・セットを識別します。

デフォルトのテンプレート・セット

Guardium は、サポートされる各オペレーティング・システム・タイプおよびデータベース・タイプに対して、事前構成されたデフォルトのテンプレート・セットを提供しています。これは UNIX または Windows プラットフォーム上のさまざまなデータベースをモニターするためのものです。 デフォルトのテンプレート・セットから操作を開始して、特定のテンプレート・セット・タイプ用に定義された新規のテンプレート・セットを使用できます。 テンプレート・セット・タイプは、 オペレーティング・システムのみ (Unix または Windows)、またはデータベース管理システム (DB2®、Informix®、Oracle など) のどちらかです。データベース管理システムは常にオペレーティング・システム・タイプで修飾されます。 例えば、UNIX-Oracle、あるいは Windows-Oracle というようになります。多くの事前構成されたデフォルトのテンプレート・セットは、Guardium の脆弱性評価で使用され、例えば、既知のパラメーター、ファイルのロケーション、ファイル・アクセス権などを検査することができます。

Guardium デフォルト・テンプレート・セットを変更することはできませんが、そのコピーを作成してコピーとして作成したバージョンを変更することはできます。各 Guardium デフォルト・テンプレート・セットは、一連のモニター対象項目を定義します。デフォルト・テンプレート・セットでモニターされる項目それぞれの機能と使用法をよく把握して、実際の環境に合ったものを使用してください。独自のテンプレート・セットを定義した場合、そのテンプレート・セットを、そのテンプレート・セットが対象とするタイプにおけるデフォルトとして指定することができます。 そのようにすれば、独自の新しいデフォルト・テンプレート・セットから操作を開始して、特定のオペレーティング・システムとデータベース・タイプ用の新規のテンプレート・セットを定義できます。 そのタイプにおける Guardium デフォルト・テンプレート・セットは削除されません。定義は残りますが、デフォルトとしてのマークは付かなくなります。

テンプレート・セット作成を特定のデータベース構成に合わせるための理論的根拠

Guardium は事前定義 CAS テンプレート・セットを各データベース・タイプ用に提供していますが、データベース構成の種類は多彩であるため、実稼働環境のすべての要件に合わせるには、事前定義テンプレート・セットを微調整するか、またはテンプレート・セットを新規作成しなければならない場合もあります。とりわけ、データベース・ソフトウェアとデータ・ファイルのロケーションに関してはこれが当てはまります。 CAS を使用してデータベース・ファイルの所有権、アクセス許可、そして変更内容をモニターする場合は、追加のテンプレートの作成を計画する必要があります。

例えば、Oracle 用の事前定義 CAS テンプレート・セットにはいくつかのテンプレートが含まれていますが、その中に次のものがあります。

- $ORACLE_HOME/oradata/../.*dbf
- $ORACLE_HOME/oradata/../.*ctl
- $ORACLE_HOME/oradata/../.*log
- $ORACLE_HOME/../init.*.ora

見てわかるとおり、これらのファイル・パターン・テンプレートは、すべて同じルート $ORACLE_HOME で始まります (注: これは、必ずしもご使用のデータベース・サーバーで必ずしも定義されている $ORACLE_HOME 環境変数であるわけではありません。設定によっては、CAS はデータ・ソースのフィールド「データベース・インスタンス・ディレクトリー」を $ORACLE_HOME の値として使用します)。

実稼働環境で、Oracle のデータ・ファイルがログ・ファイルと同一のディレクトリー・ツリーに存在しないか、場合によっては同一のデバイス上にさえ存在しない可能性があります。また、Oracle 構成ファイルもさらに別のロケーションにある可能性もあります。

CAS で 以下のような Oracle のファイルすべてを検出してモニターできるような、絶対パスを使用する追加の CAS テンプレートを作成することもできます。

- /u01/oradata/mydb/*.dbf
- /u02/oradata/mydb/*.dbf
- /u03/oradata/mydb/*.dbf
- /u01/oradata/mydb/*.ctl
- /u02/oradata/mydb/*.ctl
- /u03/oradata/mydb/*.ctl
- /home/oracle11/admin/mydb/bdump/*.log
- /home/oracle11/product/11.1/db_1/dbs/init*.ora

さらには、Oracle インスタンス・アカウントで定義した追加の環境変数を使用することもできます。 例えば変数を、$ORA_DATA1、$ORA_DATA2 および $ORA_SOFT として定義した場合、次のように指定できます。

- $ORA_DATA1/mydb/*.dbf
- $ORA_DATA2/mydb/*.dbf
- $ORA_DATA1/mydb/*.ctl
- $ORA_DATA2/mydb/*.ctl
- $ORA_SOFT/admin/mydb/bdump/*.log
- $ORA_SOFT/product/11.1/db_1/dbs/init*.ora

別のロケーションからのファイルのソーシング

CAS テンプレートでは、ユーザー・プロファイルなどの特定のファイルが特定のロケーションにあることを前提としています。 CAS は、正規表現を使用して指定した他のロケーションで、これらのファイルを検索するように構成できます。 この機能を使用するには、user_profile_files パラメーターを config ディレクトリー内の cas.client.config.properties ファイルに追加します。 各項目の形式は、次のとおりです。

```
identifying_string=comma-separated list of files
```

例えば、いずれかの Db2 ユーザーのホーム・ディレクトリーで .profile ファイルを検索するとします。 この例では、これらすべてのホーム・ディレクトリーの名前に「db2」という文字列が含まれていることを前提としています。 プロパティー・ファイルに次の行を追加します。

```
user_profile_files=.*db2.*=.profile
```

複数のパターンを指定する必要がある場合は、縦線記号 (|) を使用してパターンを区切ります。 mysql ユーザーのプロファイルを前の項目に追加する場合は、前述の例を以下のものに置き換えます。

```
user_profile_files=.*db2.*=.profile|.*mysql.*=.profile
```

- CAS の始動とフェイルオーバー
  フェイルオーバーと接続の種々のパラメーターは『S-TAP 制御の変更監査』で変更できます。
- CAS テンプレート
  Guardium には、データ・リポジトリーのタイプごとに CAS テンプレートのセットが 1 つ用意されています。
- CAS テンプレートの処理
  このセクションでは、CAS テンプレートの維持方法について説明します。
- CAS ホスト
  構成監査システム (CAS) のホスト構成では、1 つ以上の CAS インスタンスが定義されます。
- CAS レポート
  このセクションでは、構成監査システム (CAS) のレポート作成について説明します。
- CAS 状況
  「管理」 > 「変更モニター」 > 「CAS 状況」をクリックして、「構成監査システム状況」を開きます。

親トピック: 評価および強化

CAS の始動とフェイルオーバー

フェイルオーバーと接続の種々のパラメーターは『S-TAP® 制御の変更監査』で変更できます。

CAS クライアントは、ホスト上で始動するときに、以前にシステムに書き込んだチェックポイント・ファイルがあるかどうかを検索します。 CAS は、このファイルから前回実行時に行った処理を知ることができます。 それから、CAS は Guardium システムに接続します。チェックポイント・ファイルが検出された場合は、CAS は、そのモニター割り当てのバージョンを、Guardium® データベースに保管されているバージョンと比較して検証するように、Guardium システムに要求します。CAS クライアントと Guardium システムが切断されていた間に、割り当てに変更があった可能性があります。差異があった場合そのすべてが解決されると、CAS はモニターを再開します。チェックポイント・ファイルが検出されなかった場合、CAS は、Guardium システムにどのような処理を行うかを尋ねます。Guardium システムがそのデータベースで CAS ホストを検出した場合、関連するテンプレート・セットが CAS クライアントに送信され、モニター項目に展開され、モニターが開始されます。Guardium システムがデータベースで CAS ホストを検出できなかった場合は、その CAS ホストをデータベースに追加し、CAS ホストのオペレーティング・システム用のデフォルト・テンプレート・セットを送信します。

CAS クライアントと Guardium システムの間の接続が失われると、1 次 Guardium システムとの連絡が失われたことを CAS クライアントと Guardium システムが検出するまでに、最大 5 分 (CAS クライアントが Guardium システムからのメッセージを待機する時間) かかります。通信エラーが検出された場合にはこれより早い場合もあります。

CAS クライアントが Guardium システムとの接続を失った場合、または初期接続ができなかった場合、CAS クライアントはフェイルオーバー・ファイルを開いて、Guardium システムに送信するはずだったメッセージをフェイルオーバー・ファイルに書き込み始めます。このフェイルオーバー・ファイルのパスは、guard_tap.ini の中に、cas_fail_over_file という名前で保管されています。通信が再確立されると、CAS クライアントはシャットダウンと再始動を行い、フェイルオーバー・ファイルに保管したすべてのメッセージを Guardium システムに送信し、そのファイルを削除します。CAS クライアントが初期接続できなかった場合は、チェックポイント・ファイルを使用してモニター対象を判別し、通信障害の前に行っていた作業を続行します。

通信が失われると、クライアントはスレッドも開始します。このスレッドは周期的に 1 次 Guardium システムとの再接続を試行します。CAS が再接続を試行する回数と、再接続試行の平均時間間隔は、構成可能なパラメーターになっています。 クライアントは、guard_tap.ini の cas_server_failover_delay という名前で設定された期間、再接続を試行します。その時間が過ぎると、クライアントは guard_tap.ini で指定される 2 次サーバーへの接続も試行します。2 次サーバーへの試行は、guard_tap.ini の

SQL_Guard セクションにリストされた「primary」属性値の順序で行われます。primary が 1 でない場合は 2 次になります。クライアントが 2 次サーバーに接続している間も、1 次サーバーへの再接続の試行を継続します。

再接続の試行限度に達すると、CAS クライアントは再接続の試行を停止しますが、フェイルオーバー・ファイルへのデータの書き込みは継続します。 データベース・サーバー上のディスク・スペース所要量を一定以下にするため、実際には 2 つのフェイルオーバー・ファイルが存在します。 CAS はフェイルオーバー・ファイルの最大サイズ (これは構成可能) に達するまで 1 つのファイルに書き込みます。それからもう一方に切り替え、そのファイルにあった以前のデータに上書きします。 デフォルトのフェイルオーバー・ファイルのサイズは、50MB (ファイルごと) です。

CAS クライアントを構成する際には、1 つ以上の 2 次 Guardium システムを指定できます。フェイルオーバー・モードでは、CAS は guard_tap.ini の cas_server_failover_delay で指定された時間を超えるまでは、1 次サーバーへの再接続のみを試行します。その時間になると、CAS は、1 次サーバーに試行すると同時に 2 次サーバーへの接続試行も開始します (再接続試行中に最初に接続を試行するのは常に 1 次サーバーです)。 CAS は、2 次サーバーに接続している間も、1 次サーバーへの再接続の試行を続行します。

CAS クライアントの構成変更は、1 次サーバーからのみ行うことができ、ホストがオンラインのときにのみ実行できます。 Guardium システムがスタンドアロン構成になっている場合、1 次サーバー上で CAS クライアントの構成が変更されるたびに、ホスト上にエクスポート・ファイルが保存されます。CAS クライアントが 2 次サーバーに接続すると、保存されたエクスポート・ファイルはホストから 2 次サーバーにインポートされます。

1 次サーバーと 2 次サーバーの両方で構成を別個に維持する必要はありません。ただし、1 次サーバー上で個々のモニター対象項目のパラメーターがテンプレート定義から変更された場合、その変更は 2 次サーバーに転送されることはありません。 例えば、特定のファイルに対するテスト間隔がテンプレートのデフォルトである 1 時間から 10 分に変更された場合でも、2 次サーバーでのテスト間隔は元の 1 時間のままです。基本的には、モニター対象項目はインポートされた構成のテンプレートから再生成されます。 2 次サーバーの検索を開始するまでの遅延は時間に直接基づいており、フェイルオーバー・ファイルのサイズは関係ありません。 遅延は guard_tap.ini の cas_server_failover_delay パラメーターで設定され、デフォルトは 60 分です。

フェイルオーバーと接続の種々のパラメーターは『S-TAP 制御の変更監査』で変更できます。

S-TAP の場合と同様、CAS 接続に障害があると Guardiumシステム上に例外が作成されるため、障害を検出すると即座にアラートを出すことができます。

2 次サーバーの設定と保守

データベース・サーバー・システム上の S-TAP/CAS 構成ファイルには、1 つ以上の 2 次 Guardium サーバーを定義できます。1 次 Guardium サーバーが使用不可になった場合、そのデータベース・サーバー・システム上の CAS は 2 次 Guardium システムに接続します (前述のとおりです。『始動とフェイルオーバー』を参照してください)。

フェイルオーバーのルール

ルール #	Guardium システム	フェイルオーバー先	有効
1	スタンドアロン	スタンドアロン	はい
2	管理対象	管理対象 (マネージャーが同一)	はい
3	管理対象	管理対象 (マネージャーが異なる)	いいえ
4	管理対象	スタンドアロン	いいえ
5	スタンドアロン	管理対象	いいえ

CAS フェイルオーバーの制限

1. CAS インスタンスは、ソース Guardium システムが管理対象ユニットであり、ターゲット Guardium システムが以下のいずれかである場合には、フェイルオーバー Guardium システムへ再配置されません。
   - スタンドアロン Guardium システム
   - 異なるマネージャーが管理している管理対象ユニット
2. CAS インポート/エクスポート・オプションは、マネージャーとスタンドアロン・マシンのみに制限されます。

CAS ホストのエクスポート

1. 「管理」 > 「統合/アーカイブ」 > 「エクスポート」をクリックし、「定義のエクスポート」パネルを開きます。「タイプ」メニューから「CAS ホスト」を選択し、エクスポートする定義を「エクスポートする定義」メニューから選択し、「エクスポート」をクリックします。
2. exp_<date>_<time>.sql という名前のファイルがシステムに保存されます。このファイルには、選択したすべての CAS ホストの定義と、それらの CAS ホストが使用するすべてのテンプレート・セットの定義が格納されます。

CAS ホストのインポート

1. 「管理」 > 「統合/アーカイブ」 > 「インポート」をクリックし、「定義のインポート」パネルを開きます。
2. 「参照」ボタンと「アップロード」ボタンを使用してファイルを選択してアップロードした後、「アップロード済み定義のインポート」ペインから定義を選択します。
3. 「この定義セットをインポート」をクリックして定義をインポートします。
4. 選択したアクションを (行うか行わないかを) 確認します。
   注: インポート操作では、既存の定義に上書きされません。既存の定義と同じ名前の定義をインポートしようとすると、その項目は置き換えられなかったことが通知されます。 インポートされた定義で既存の定義を上書きする場合は、インポート操作を実行する前に、既存の定義を削除する必要があります。

CAS ホストの 2 次サーバーの保守

CAS 構成は、エクスポートとインポート操作を使用して保守することもできます。 インポート操作では既存の定義は置換されないため、それぞれの 2 次サーバーで、古い CAS ホスト定義を削除してから新しいものをインポートする必要があります。

この手順を実行するのは、必ず、選択した CAS ホストが 1 次サーバーに接続されているときのみにしてください。

1. CAS ホストの定義をエクスポートします (前のセクションを参照)。

2. それぞれの 2 次サーバーで以下の操作を行います。
    - 置換の対象になる古い CAS ホスト定義を削除します。
    - 1 次サーバーからエクスポートした定義をインポートします (前述の『CAS ホストのインポート』を参照)。

CAS クライアントのインストール

CAS クライアント・エージェントは、一般に S-TAP エージェントと共にインストールされます。 これは後でインストールすることもできます。Windows ではインストール DVD から、UNIX ではインストール・スクリプト install_cas.sh を実行することによって行います。インストール・スクリプトは S-TAP のインストール・ディレクトリーに配置されており、デフォルトでは /usr/local/guardium/guard_stap です。

CAS クライアントの変更の無視アラート

CAS クライアント・エージェントは、事前定義設定に基づいて、変更通知が CAS サーバーに送信されないようにすることができます。

CAS クライアント・エージェントは、CAS クライアント・エージェントの cas.client.config.properties 構成ファイル内で新しいパラメーター ignore_change_alerts を探します。

このパラメーターが見つからないか設定されていない場合、CAS クライアントは変更なしで動作し、「変更の無視アラート」機能は有効になりません (例えば、CAS クライアントはファイル変更時にアラートを出します)。

新規パラメーターが設定されている場合、CAS クライアント・エージェントは、パラメーター値に指定された変更タイプに基づいて、変更通知の送信を無視します。

使用可能な変更タイプは次のとおりです。

PERMISSION、SIZE、OWNER、GROUP、TIMESTAMP

複数の変更タイプを無視する場合は、指定した複数の変更タイプを「+」で区切って連結して設定できます。

例:

OWNER と GROUP の変更時に変更通知が送信されないようにするには、以下のようにパラメーターを設定します。

ignore_change_alerts=OWNER+GROUP

注: 初期インストール時または新規テンプレートの定義時に、ファイルの最初のスキャンが実行され、これらのファイルは、「変更の無視アラート」の設定に関係なく、「CAS 変更」レポートに表示されます。

無効な非 IP ホスト名の修正

ユーザーが無効な tap_ip (guard_tap.ini パラメーター) または CAS_TAP_IP (GIM パラメーター) を指定して CAS エージェントをインストールすると、そのホストに関して定義された Windows データ・ソースが使用できなくなる可能性があります (リモート・データベースへのアクセスを必要とするアクティビティーについて使用された場合)。

このような状況が起きた場合は、データ・ソースを削除し、tap_ip パラメーターを正しいデータベース・サーバー・ホスト名/IP に変更する必要があります。

親トピック: 構成監査システム

CAS テンプレート

Guardium には、データ・リポジトリーのタイプごとに CAS テンプレートのセットが 1 つ用意されています。

CAS テンプレート - DB2

OS スクリプト

実行する OS スクリプトを指定します。CAS ホーム・ディレクトリーの下のスクリプト・ディレクトリーを示す変数 $SCRIPTS で始まり、実行するスクリプト (例えば、`$HOME/ db2_spm_log_path_group_test.sh`") を示している必要があります。スクリプト自体も CAS $SCRIPTS ディレクトリーにある必要があります。 スクリプトからの出力は、Guardium® データベースに格納され、セキュリティー・アセスメントに使用されます。 これは、実行可能なシェル・スクリプトまたはバッチ・スクリプトか、あるいはコマンド行に入力できるコマンドのセットのいずれかです。 Java の構文解析は変更される可能性が高いため、最も単純な種類のコマンド以外については直接実行するのではなく、スクリプトに配置することを推奨します。 UNIX では、スクリプトは指定した OS ユーザーの環境で実行されます。 ユーザーがスクリプトを記述するために使用できる実行環境用に、3 つの環境変数が定義されます。$UCAS はデータベース・ユーザー名、$PCAS はデータベース・パスワード、$ICAS はデータベース・インスタンス名です。 Windows の場合、これらの 3 つの値はバッチ・ファイル実行時に最後の 3 つの引数として付加されます。 例えば、OS スクリプト・テンプレート `%SCRIPTS%¥MyScript.bat my-arg1 my-arg2` を使う場合、%3、%4、および %5 はそれぞれ DB ユーザー名、パスワード、およびインスタンス名になります。

ファイル

セキュリティー・アセスメントでトラッキングおよびモニターの対象にするファイルを指定します。 ファイルのパスは、絶対パスまたは $INSTHOME 変数を基準とする相対パスにすることができます。「データ・ソース定義」パネルの「データベース・インスタンス・ディレクトリー」で、$INSTHOME 変数の値を設定します。 これは単一のファイルの名前と見なされます。OS ユーザー環境の環境変数をファイル名の中で使うことができ、展開して使用されます。例えば、$HOME/START.sh は DB2® ユーザーのホーム・ディレクトリーにある始動スクリプトの名前です。

ファイル・パターン

セキュリティー・アセスメントでトラッキングおよびモニターの対象にするファイルのグループを指定します。 ファイルのパスは、絶対パスまたは $INSTHOME 変数を基準とする相対パスにすることができます。 「データ・ソース定義」パネルの「データベース・インスタンス・ディレクトリー」で、$INSTHOME 変数の値を設定します。 パスの中で指定する「..」は、その前のパス部分とその後のパス部分の間に 1 つ以上のディレクトリーがあることを示します。パスの中で指定する「.+」は、その前のパス部分とその後のパス部分の間に 1 つだけディレクトリーがあることを示します。 例えば、`$INSTHOME/sqllib/../db2.*` という指定は、1 つの単一識別文字列 (ディレクトリー内のすべてのファイルに一致するファイル・パターン) から多くの単一ファイル識別文字列を作成するための簡略表記になります。ファイル・パターンは、「/」で分離した一連の正規表現と見なせます。ファイルの絶対パスの各要素が順番どおりにその正規表現の 1 つと一致すれば、そのファイルが一致したということ

になります。 パターンの要素が環境変数である場合、突き合わせの前に環境変数が展開されます。 パターンのいずれかの要素が「..」である場合、ゼロ個以上のディレクトリー・レベルと一致することになります。 例えば、/usr/local/../foo は、/usr/local/foo や /usr/local/gunk/junk/bunk/foo と一致します。 1 つのファイル・パターンに複数の「..」要素を使用する必要はありませんし、使用すべきではありません。そのようにすると、パターンを展開するのに非常に時間がかかってしまうからです。混乱を避けるため、正規表現では Windows で使用される可能性のある区切り文字として ¥ を使用することはできません。

さらに、「Guardium Unix/DB2 のアセスメント: UNIX - DB2 for Unix」セットには、以下のテンプレートが含まれています。

Db2govd SETUID ビット未設定

このテストは、DB2GOVD の SETUID ビットが無効になっているかどうかをモニターします。

Db2start SETUID ビット未設定

このテストは、DB2START の SETUID ビットが無効になっているかどうかをモニターします。

Db2stop SETUID ビット未設定

このテストは、DB2STOP の SETUID ビットが無効になっているかどうかをモニターします。

ファイル所有権

このテストは、DB2 ファイルのファイル所有権およびその変更をモニターします。

ファイルの許可

このテストは、Db2 ファイルのファイル・アクセス許可およびその変更をモニターします。

CAS テンプレート - Informix

OS スクリプト

実行する OS スクリプトを指定します。CAS ホーム・ディレクトリーの下のスクリプト・ディレクトリーを示す変数 $SCRIPTS で始まり、実行するスクリプト (例えば、`$HOME/ informix_rootpath_owner.sh`") を示している必要があります。スクリプト自体も CAS $SCRIPTS ディレクトリーにある必要があります。 スクリプトからの出力は、Guardium データベースに格納され、セキュリティー・アセスメントに使用されます。 これは、実行可能なシェル・スクリプトまたはバッチ・スクリプトか、あるいはコマンド行に入力できるコマンドのセットのいずれかです。 Java の構文解析は変更される可能性が高いため、最も単純な種類のコマンド以外については直接実行するのではなく、スクリプトに配置することを推奨します。 UNIX では、スクリプトは指定した OS ユーザーの環境で実行されます。 ユーザーがスクリプトを記述するために使用できる実行環境用に、3 つの環境変数が定義されます。$UCAS はデータベース・ユーザー名、$PCAS はデータベース・パスワード、$ICAS はデータベース・インスタンス名です。 Windows の場合、これらの 3 つの値はバッチ・ファイル実行時に最後の 3 つの引数として付加されます。 例えば、OS スクリプト・テンプレート `%SCRIPTS%¥MyScript.bat my-arg1 my-arg2` を使う場合、%3、%4、および %5 はそれぞれ DB ユーザー名、パスワード、およびインスタンス名になります。

ファイル

セキュリティー・アセスメントでトラッキングとモニターの対象にするファイルを指定します。 ファイルのパスは、絶対パスまたは $ INFORMIXDIR 変数を基準とする相対パスにすることができます。「データ・ソース定義」パネルの「データベース・インスタンス・ディレクトリー」で、$INFORMIXDIR 変数の値を設定します。 これは単一のファイルの名前と見なされます。OS ユーザー環境の環境変数をファイル名の中で使うことができ、展開して使用されます。例えば、$HOME/START.sh は Informix® ユーザーのホーム・ディレクトリーにある始動スクリプトの名前です。

さらに、UNIX 用の「Guardium Unix/Informix のアセスメント」セットには、以下のテンプレートが含まれています。

ログ・ファイルに対するエラーのスキャン

このテストは、online.log ファイルにエラーがあるかどうかをモニターします。

ファイル所有権

このテストは、Informix ファイルのファイル所有権およびその変更をモニターします。

ファイルの許可

このテストは、Informix ファイルのファイル・アクセス許可およびその変更をモニターします。

CAS テンプレート - Oracle

OS スクリプト

実行する OS スクリプトを指定します。CAS ホーム・ディレクトリーの下のスクリプト・ディレクトリーを示す変数 $SCRIPTS で始まり、実行するスクリプト (例えば、$SCRIPTS/oracle_user.sh) を示している必要があります。スクリプト自体も CAS $SCRIPTS ディレクトリーにある必要があります。 スクリプトからの出力は、Guardium データベースに格納され、セキュリティー・アセスメントに使用されます。(これは、実行可能なシェル・スクリプトまたはバッチ・スクリプトか、あるいはコマンド行に入力できるコマンドのセットのいずれかです。 Java の構文解析は変更される可能性が高いため、最も単純な種類のコマンド以外については直接実行するのではなく、スクリプトに配置することを推奨します。 UNIX では、スクリプトは指定した OS ユーザーの環境で実行されます。 ユーザーがスクリプトを記述するために使用できる実行環境用に、3 つの環境変数が定義されます。$UCAS はデータベース・ユーザー名、$PCAS はデータベース・パスワード、$ICAS はデータベース・インスタンス名です。 Windows の場合、これらの 3 つの値はバッチ・ファイル実行時に最後の 3 つの引数として付加されます。 例えば、OS スクリプト・テンプレート $SCRIPTS/mysql_mysqld_user.sh を使用する場合、%3、%4、および %5 はそれぞれ DB ユーザー名、パスワード、およびインスタンス名になります。)

ファイル

トラッキングとモニターの対象にするファイルを指定します。 ファイルのパスは、絶対パスまたは $ORACLE_HOME 変数を基準とする相対パスにすることができます。 $ORACLE_HOME 変数の値は「データ・ソース定義」パネルの「データベース・インスタンス・ディレクトリー」フィールドで設定した値です。(これは単一のファイルの名前と見なされます。OS ユーザー環境の環境変数をファイル名の中で使うことができ、展開して使用されます。例えば、$HOME/START.sh は Oracle ユーザーのホーム・ディレクトリーにある始動スクリプトの名前です。)

ファイル・パターン

トラッキングとモニターの対象にするファイルのグループを指定します。ファイルのパスは、絶対パスまたは $ORACLE_HOME 変数を基準とする相対パスにすることができます。「データ・ソース定義」パネルの「データベース・インスタンス・ディレクトリー」で、$ORACLE_HOME 変数の値を設定します。 パスの中で指定する「..」は、その前のパス部分とその後のパス部分の間に 1 つ以上のディレクトリーがあることを示します。パスの中で指定する「.+」は、その前のパス部分とその後のパス部分の間に 1 つだけディレクトリーがあることを示します。 例えば、$ORACLE_HOME/oradata/../*.dbf とします。これは、1 つの単一ファイル識別文字列であるファイル・パターンから多くの単一ファイル識別文字列を作成するための簡略表記になります。ファイル・パターンは、「/」で分離した一連の正規表現と見なせます。ファイルの絶対パスの各要素が順番どおりにその正規表現の 1 つと一致すれば、そのファイルが一致したということになります。 パターンの要素が環境変数である場合、突き合わせの前に環境変数が展開されます。 パターンのいずれかの要素が「..」である場合、ゼロ個以上のディレクトリー・レベルと一致することになります。 例えば、/usr/local/../foo は、/usr/local/foo や /usr/local/gunk/junk/bunk/foo と一致します。 1 つのファイル・パターンに複数の「..」要素を使用する必要はありませんし、使用すべきではありません。そのようにすると、パターンを展開するのに非常に時間がかかってしまうからです。混乱を避けるため、正規表現では Windows で使用される可能性のある区切り文字として ¥ を使用することはできません。前述のファイル・パターンは正しくありません。*.dbf は有効な正規表現ではないからです。この場合は .*dbf とする必要があります。

さらに、デフォルトの Guardium Unix/Oracle テンプレート・セットには、以下のテンプレートが含まれています。

ADMIN_RESTRICTIONS がオン

このテストは、listener.ora パラメーター ADMIN_RESTRICTIONS が適切に設定されているかどうかをモニターします。

ファイル所有権

このテストは、Oracle データ・ファイル、ログ、実行可能ファイルなどのファイル所有権およびその変更をモニターします。

ファイルの許可

このテストは、Oracle データ・ファイル、ログ、実行可能ファイルなどのファイル・アクセス許可およびその変更をモニターします。

ログ・ファイルに対するエラーのスキャン

このテストは、Oracle ログ・ファイルにエラー文字列が出現するかどうかをスキャンします。

SPOOLMAIN.LOG が存在しない

このテストは、Oracle SPOOLMAIN.LOG が存在するかどうか検査します。

CAS テンプレート - MongoDB

MongoDB は、非リレーショナル形式のデータ (JSON 文書など) のプログラミングが容易であるため、運用システムや Web アプリケーションのバックエンドとして使用されることが一般的です。

Unix/MongoDB テンプレートを使用すると、データ・ソースに複数のパスや複数のディレクトリーを指定して、MongoDB データ・ソース定義で指定された各種コンポーネントをスキャンすることができます。

ファイル・パターンをスキャンするには、「$」で始まるテンプレート項目を選択します。

$SCRIPTS/mongodb_unmask_value.sh 項目は選択しないでください。これは Guardium の予約項目です。

テンプレート項目が MongoDB データ・ソース定義で「データベース・インスタンス・ディレクトリー」の一部として指定されていない場合は、この項目はスキップオーバーされ、スキャンされません。

注: CAS スクリプトが機能するためには、Mongo DB サーバー上で MongoDB アカウントのログインを有効にする必要があります。ログインを有効にするには、root としてログインし、chsh mongod コマンドを実行し、新しいシェルを求めるプロンプトが出されたら `/bin/bash` と入力します。
注: 複数のファイル・パスを使用して、任意のタイプのデータ・ソースのテンプレートを独自に作成することができます。独自のテンプレートを作成する際には、Unix/MongoDB を参考にすることをお勧めします。MongoDB データ・ソースの新規テンプレートを作成する場合は、Unix/MongoDB テンプレートをコピーし、それに変更を加えることができます。
注: MongoDB データ・ソースは、SSL クライアント証明書を使用した SSL サーバーとクライアント/サーバーの接続をサポートしています。MongoDB 接続では、JDBC データベース接続ではなく Java ドライバーを使用します。
注: MongoDB クラスターの VA ソリューションは、複数の Mongo (レプリカ・セットの 1 次ノードとすべての 2 次ノード) 上で実行することができます。

CAS テンプレート - Netezza®

ファイル所有権

このテストは、CAS テンプレートの定義に従って、ファイルが正しいグループに所有され、所属しているかどうかを検査します。

ファイルの許可

このテストは、CAS テンプレートの定義に従って、ファイル・アクセス権が適切に設定されているかどうかを検査します。

ログ・ファイルに対するエラーのスキャン

このテストは、以下の 2 つのログ・ファイルに対してイベント (FATAL、ERROR、DEBUG、ABORT、および PANIC) があるかどうかを検査します。/nz/kit/log/postgres/pg.log および /nz/kit/log/startupsvr/startupsvr.log

CAS テンプレート - Oracle

OS スクリプト

実行する OS スクリプトを指定します。CAS ホーム・ディレクトリーの下のスクリプト・ディレクトリーを示す変数 $SCRIPTS で始まり、実行するスクリプト (例えば、$SCRIPTS/oracle_user.sh) を示している必要があります。スクリプト自体も CAS $SCRIPTS ディレクトリーにある必要があります。 スクリプトからの出力は、Guardium データベースに格納され、セキュリティー・アセスメントに使用されます。(これは、実行可能なシェル・スクリプトまたはバッチ・スクリプトか、あるいはコマンド行に入力できるコマンドのセットのいずれかです。 Java の構文解析は変更される可能性が高いため、最も単純な種類のコマンド以外については直接実行するのではなく、ス

クリプトに配置することを推奨します。 UNIX では、スクリプトは指定した OS ユーザーの環境で実行されます。 ユーザーがスクリプトを記述するために使用できる実行環境用に、3 つの環境変数が定義されます。$UCAS はデータベース・ユーザー名、$PCAS はデータベース・パスワード、$ICAS はデータベース・インスタンス名です。Windows の場合、これらの 3 つの値はバッチ・ファイル実行時に最後の 3 つの引数として付加されます。 例えば、OS スクリプト・テンプレート $SCRIPTS/mysql_mysqld_user.sh を使用する場合、%3、%4、および %5 はそれぞれ DB ユーザー名、パスワード、およびインスタンス名になります。)

ファイル

トラッキングとモニターの対象にするファイルを指定します。 ファイルのパスは、絶対パスまたは $ORACLE_HOME 変数を基準とする相対パスにすることができます。$ORACLE_HOME 変数の値は「データ・ソース定義」パネルの「データベース・インスタンス・ディレクトリー」フィールドで設定した値です。(これは単一のファイルの名前と見なされます。OS ユーザー環境の環境変数をファイル名の中で使うことができ、展開して使用されます。例えば、$HOME/START.sh は Oracle ユーザーのホーム・ディレクトリーにある始動スクリプトの名前です。)

ファイル・パターン

トラッキングとモニターの対象にするファイルのグループを指定します。ファイルのパスは、絶対パスまたは $ORACLE_HOME 変数を基準とする相対パスにすることができます。「データ・ソース定義」パネルの「データベース・インスタンス・ディレクトリー」で、$ORACLE_HOME 変数の値を設定します。 パスの中で指定する「..」は、その前のパス部分とその後のパス部分の間に 1 つ以上のディレクトリーがあることを示します。パスの中で指定する「.+」は、その前のパス部分とその後のパス部分の間に 1 つだけディレクトリーがあることを示します。 例えば、$ORACLE_HOME/oradata/../*.dbf とします。これは、1 つの単一ファイル識別文字列であるファイル・パターンから多くの単一ファイル識別文字列を作成するための簡略表記になります。ファイル・パターンは、「/」で分離した一連の正規表現と見なせます。ファイルの絶対パスの各要素が順番どおりにその正規表現の 1 つと一致すれば、そのファイルが一致したということになります。 パターンの要素が環境変数である場合、突き合わせの前に環境変数が展開されます。 パターンのいずれかの要素が「..」である場合、ゼロ個以上のディレクトリー・レベルと一致することになります。 例えば、/usr/local/../foo は、/usr/local/foo や /usr/local/gunk/junk/bunk/foo と一致します。 1 つのファイル・パターンに複数の「..」要素を使用する必要はありませんし、使用すべきではありません。そのようにすると、パターンを展開するのに非常に時間がかかってしまうからです。混乱を避けるため、正規表現では Windows で使用される可能性のある区切り文字として ¥ を使用することはできません。前述のファイル・パターンは正しくありません。*.dbf は有効な正規表現ではないからです。この場合は .*dbf とする必要があります。

さらに、デフォルトの Guardium Unix/Oracle テンプレート・セットには、以下のテンプレートが含まれています。

ADMIN_RESTRICTIONS がオン

このテストは、listener.ora パラメーター ADMIN_RESTRICTIONS が適切に設定されているかどうかをモニターします。

ファイル所有権

このテストは、Oracle データ・ファイル、ログ、実行可能ファイルなどのファイル所有権およびその変更をモニターします。

ファイルの許可

このテストは、Oracle データ・ファイル、ログ、実行可能ファイルなどのファイル・アクセス許可およびその変更をモニターします。

ログ・ファイルに対するエラーのスキャン

このテストは、Oracle ログ・ファイルにエラー文字列が出現するかどうかをスキャンします。

SPOOLMAIN.LOG が存在しない

このテストは、Oracle SPOOLMAIN.LOG が存在するかどうか検査します。

Oracle RAC システムの場合の構成

Oracle RAC システムの場合に必要な構成は以下のとおりです。
S-TAP でインストールされた、各ノード上の guard_tap.ini を以下のように変更します。
unix_domain_socket_marker=<key>
<key> 値は IPC プロトコル定義内の listener.ora に見つかります。
例 1:
listener.ora 内の記述が以下のようになっている場合、
LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=ORCL))))
以下のパラメーターをそれに従って変更します。
unix_domain_socket_marker=ORCL
例 2:
listener.ora 内に複数の IPC 行がある場合、すべてのキーの共通項を使用します。LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER)))) LISTENER_SCAN1=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN1)))) LISTENER_SCAN2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN2)))) LISTENER_SCAN3=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN3))))
Guardium はパスで文字列検索を使用するので、「LISTENER」を指定すれば、 上記の 4 つすべてに有効です。この場合、以下のように使用します。
unix_domain_socket_marker=LISTENER

CAS テンプレート - PostgreSQL

注: PostgreSQL_BIN および PostgreSQL_DATA 環境変数が正しく定義されていることは非常に重要です。設定が無効である場合、他の CAS 評価テストが正しく作動しなくなるか、まったく作動しなくなります。

ファイル所有権

このテストは、CAS テンプレートの定義に従って、ファイルが正しいグループに所有され、所属しているかどうかを検査します。

ファイルの許可

このテストは、CAS テンプレートの定義に従って、ファイル・アクセス権が適切に設定されているかどうかを検査します。

PostgreSQL_BIN 環境変数が定義済み

このテストは、データベース・サーバーで $PostgreSQL_BIN 環境変数が定義されているかどうかを検査します。この変数は、Unix/Linux の root アカウントの下に定義する必要があります。あるいは、root ログイン用の .profile に追加することができます。Windows OS の場合は、管理者ログインに対してこれを定義する必要があります。Red Hat Linux の場合、PostgreSQL BIN フォルダーは通常は /usr/bin 内にあります。Solaris の場合、通常これは /data/postgres/postgres/8.3-community/bin/64 などのようになります。この環境変数の設定は非常に重要です。他の評価テストはこのフォルダーのロケーションに依存するためです。

PostgreSQL_DATA 環境変数が定義済み

このテストは、データベース・サーバーで $PostgreSQL_DATA 環境変数が定義されているかどうかを検査します。この変数は、Unix/Linux の root アカウントの下に定義する必要があります。あるいは、root ログイン用の .profile に追加することができます。Windows OS の場合は、管理者ログインに対してこれを定義する必要があります。Red Hat Linux の場合、DATA フォルダーのデフォルトは通常は /var/lib/pgsql/data 内にあります。 Solaris の場合、一定のロケーションはありません。 この環境変数の設定は非常に重要です。他の評価テストは、正しい構成ファイルを検出するためにこのフォルダーのロケーションに依存するためです。

CAS テンプレート - SQL Server

OS スクリプト

実行する OS スクリプトを指定します。 スクリプトからの出力は、Guardium データベースに格納されます。 これは、実行可能なシェル・スクリプトまたはバッチ・スクリプトか、あるいはコマンドに入力できるコマンドのセットのいずれかです。

レジストリー変数

セキュリティー・アセスメント・テストで必要な特定のキー値を Windows レジストリーから検索します。

CAS テンプレート - Sybase

OS スクリプト

実行する OS スクリプトを指定します。CAS ホーム・ディレクトリーの下のスクリプト・ディレクトリーを示す変数 $SCRIPTS で始まり、実行するスクリプト (例えば、$HOME/sybase_sysdevice_type_test.sh) を示している必要があります。スクリプト自体も CAS $SCRIPTS ディレクトリーにある必要があります。 スクリプトからの出力は、Guardium データベースに格納され、セキュリティー・アセスメントに使用されます。 これは、実行可能なシェル・スクリプトまたはバッチ・スクリプトか、あるいはコマンド行に入力できるコマンドのセットのいずれかです。 Java の構文解析は変更される可能性が高いため、最も単純な種類のコマンド以外については直接実行するのではなく、スクリプトに配置することを推奨します。 UNIX では、スクリプトは指定した OS ユーザーの環境で実行されます。 ユーザーがスクリプトを記述するために使用できる実行環境用に、3 つの環境変数が定義されます。$UCAS はデータベース・ユーザー名、$PCAS はデータベース・パスワード、$ICAS はデータベース・インスタンス名です。 Windows の場合、これらの 3 つの値はバッチ・ファイル実行時に最後の 3 つの引数として付加されます。 例えば、OS スクリプト・テンプレート「%SCRIPTS%¥MyScript.bat my-arg1 my-arg2」を使う場合、%3、%4、および %5 はそれぞれ DB ユーザー名、パスワード、およびインスタンス名になります。

ファイル

セキュリティー・アセスメントでトラッキングとモニターの対象にするファイルを指定します。 ファイルのパスは、絶対パスまたは $SYBASE 変数を基準とする相対パスにすることができます。 $SYBASE 変数の値は「データ・ソース定義」パネルの「データベース・インスタンス・ディレクトリー」フィールドで設定した値です。 これは単一のファイルの名前と見なされます。OS ユーザー環境の環境変数をファイル名の中で使うことができ、展開して使用されます。例えば、$HOME/START.sh は Sybase ユーザーのホーム・ディレクトリーにある始動スクリプトの名前です。

ファイル・パターン

セキュリティー・アセスメントでトラッキングとモニターの対象にするファイルのグループを指定します。 ファイルのパスは、絶対パスまたは $SYBASE 変数を基準とする相対パスにすることができます。 $SYBASE 変数の値は「データ・ソース定義」パネルの「データベース・インスタンス・ディレクトリー」フィールドで設定した値です。パスの中で指定する「..」は、その前のパス部分とその後のパス部分の間に 1 つ以上のディレクトリーがあることを示します。パスの中で指定する「.+」は、その前のパス部分とその後のパス部分の間に 1 つだけディレクトリーがあることを示します。 例えば、「$SYBASE/../.*dat」という指定は、1 つの単一ファイル識別文字列であるファイル・パターンから多くの単一ファイル識別文字列を作成するための簡略表記になります。ファイル・パターンは、「/」で分離した一連の正規表現と見なせます。ファイルの絶対パスの各要素が順番どおりにその正規表現の 1 つと一致すれば、そのファイルが一致したということになります。 パターンの要素が環境変数である場合、突き合わせの前に環境変数が展開されます。 パターンのいずれかの要素が「..」である場合、ゼロ個以上のディレクトリー・レベルと一致することになります。 例えば、/usr/local/../foo は、/usr/local/foo や /usr/local/gunk/junk/bunk/foo と一致します。 1 つのファイル・パターンに複数の「..」要素を使用する必要はありませんし、使用すべきではありません。そのようにすると、パターンを展開するのに非常に時間がかかってしまうからです。混乱を避けるため、正規表現では Windows で使用される可能性のある区切り文字として ¥ を使用することはできません。

さらに、「Guardium Unix/Sybase のアセスメント: UNIX - SYBASE」セットには、以下のテンプレートが含まれています。

ログ・ファイルに対するエラーのスキャン

このテストは、Sybase ログ・ファイルにエラーがあるかどうかをモニターします。

sysdevice 所有者が sysbase

このテストは、sysdevice の所有権をモニターします。

ファイル所有権

このテストは、Sybase ファイルのファイル所有権およびその変更をモニターします。

ファイルの許可

このテストは、Sybase ファイルのファイル・アクセス許可およびその変更をモニターします。

CAS テンプレート - Teradata

ファイル所有権

このテストは、CAS テンプレートの定義に従って、ファイルが正しいグループに所有され、所属しているかどうかを検査します。

ファイルの許可

このテストは、CAS テンプレートの定義に従って、ファイル・アクセス権が適切に設定されているかどうかを検査します。

Aster データ

Aster Data は 2011 年に Teradata によって買収されました。Aster Data は一般的に、データウェアハウジングおよび分析アプリケーション (OLAP) に使用されます。Aster Data は、構造化照会言語 (SQL) を MapReduce 内で使用できるようにする SQL-MapReduce と呼ばれるフレームワークを構築しました。Aster Data で最もよく連想されるのは、クリック・ストリーム系のアプリケーションです。

Aster nCluster には、クイーン・ノード・グループ、ワーカー・ノード・グループ、およびローダー・ノード・グループが含まれています。CAS エージェントは、3 つすべてのノード・グループにインストールされます。

クイーン・ノードですべてのテストを実行するには、セキュリティー・アセスメントを作成する必要があります。Aster Data 用のデータベース接続はすべて、クイーン・ノードのみを通過します。

ワーカー・ノードとローダー・ノードでテストが必要となるのは、CAS テスト (ファイル許可とファイル所有権) を実行する場合のみです。

特権テストは、所定のインスタンスに含まれるすべてのデータベースをループします。

CAS アクセスを必要とする脆弱性評価テストを実行し、CAS データ・ソース構成の選択を入力する際には、データベース・インスタンス・アカウントで Aster のインストールに使用したユーザー名を指定してください。このユーザー名は通常、beehive と呼ばれます。

データベース・インスタンス・ディレクトリーでは、これが beehive ユーザーのホーム・ディレクトリーとなります。デフォルトは通常、/home/beehive です。

CAS を使用しない脆弱性評価テストを実行する場合は、ユーザーがクラスター内のクイーン・ノードを指定して、独自のデータ・ソースを作成する必要があります。

CAS に依存する脆弱性評価テストを実行する際に、テスト対象ノードがワーカーのいずれかである場合は、クイーン・ノードを指すようにデータ・ソース内の「カスタム URL」を設定する必要があります (これは listen 方法を示します)。

例

ホスト名/IP = Worker.guard.xxx.xxx..com または 1xx.1xx.111.111 (ワーカーがこれを listen していない場合でも、これが実際のワーカー・ホストになります。CAS はこのワーカーのノードからデータを送受信できるため、これが必要となります。)

ポート = 2046 または使用される任意のポート

データベース = beehive

カスタム URL = jdbc:ncluster://aster6q:2406/beehive (この JDBC の例は、実際にはポート 2406 および beehive データベース上のクイーン・ノードである aster6q に接続することを示しています。)

データベース・インスタンス・アカウント = beehive

データベース・インスタンス・ディレクトリー = /home/beehive

親トピック: 構成監査システム

CAS テンプレートの処理

このセクションでは、CAS テンプレートの維持方法について説明します。

テンプレート/テンプレート・セットの定義

- 新しいテンプレート・セットの作成
- テンプレート・セットの変更
- テンプレート・セットのコピー作成
- テンプレート・セットの削除

新しいテンプレート・セットの作成

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS テンプレート・セットの構成」をクリックして、「CAS 構成ナビゲーター」を開きます。
2. 「新規」をクリックして、「モニター項目テンプレート定義」パネルを開きます。
3. OS タイプを選択します。
4. データベース・タイプを選択します。特定のデータベース・タイプがテンプレート・セットで必要とされない場合は、「データベース・タイプ」として N_A を選択します。
5. テンプレート・セット名として固有の名前を入力します。
   注: 128 文字を超えるテンプレート・セット名は切り捨てられます。
6. 「適用」をクリックして、CAS テンプレート・セット定義を保存します。
7. 新しいテンプレート・セットに項目を追加するには、「セットに追加」をクリックします。『テンプレート・セット項目の定義』を参照してください。

Guardium® CAS パネルを見つける

デフォルトでは、CAS 構成機能へのアクセス権限は admin ユーザー、および CAS ロールを割り当てられたユーザーに限定されます。

「強化」をクリックします。CAS 機能のリストは「構成変更制御 (CAS アプリケーション)」ヘッダー内に表示されます。

CAS 構成ナビゲーターを開く

「CAS 構成ナビゲーター」パネルから操作を開始して、CAS テンプレート・セットを作成または変更することができます。

「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS テンプレート・セットの構成」をクリックして、「CAS 構成ナビゲーター」パネルを開きます。

リストは OS タイプやデータベース・タイプでフィルタリングすることができます。

テンプレート・セットの変更

既存の CAS テンプレート・セットを変更するには、「CAS 構成ナビゲーター」パネルを使用します。いずれかの CAS ホストでテンプレート・セットが既に使用中の場合、そのテンプレート・セットで変更できる点は限られています。定義のいくつかの要素を少し変更することはできますが、テンプレートの追加/削除はできません。

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS テンプレート・セットの構成」をクリックして、「CAS 構成ナビゲーター」パネルを開きます。
2. テンプレート・セット・リストを OS タイプまたはデータベース・タイプでフィルターに掛けます。
3. 変更するテンプレート・セットを選択して「変更」をクリックすると、「CAS テンプレート・セット定義」パネルが開きます。
4. 必要な変更を加え、「適用」をクリックして変更内容を保存します。

テンプレート・セットのコピー作成

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS テンプレート・セットの構成」をクリックして、「CAS 構成ナビゲーター」パネルを開きます。
2. テンプレート・セット・リストを OS タイプまたはデータベース・タイプでフィルターに掛けます。
3. コピーするテンプレート・セットを選択して「コピー」をクリックすると、「CAS テンプレート・セット定義」パネルが開きます。
4. コピーが作成されたら、必要に応じてコピーに変更を加えます。

注: 事前定義テンプレートは編集できません。これには CAS ホストで使用されているものと同じ制約事項があります。お客様が変更を加える場合は、そのコピーを作成し、作成したコピーを編集する必要があります。

テンプレート・セットの削除

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS テンプレート・セットの構成」をクリックして、「CAS 構成ナビゲーター」パネルを開きます。
2. テンプレート・セット・リストを OS タイプまたはデータベース・タイプでフィルターに掛けます。
3. 削除するテンプレート・セットを選択して、「削除」をクリックします。

テンプレート・セット項目の定義

いずれかの CAS ホストでテンプレート・セットが既に使用中の場合、そのテンプレート・セットで変更できる点は限られています。定義のいくつかの要素を少し変更することはできますが、テンプレートの追加/削除はできません。

- 新しいテンプレート・セット項目の作成
- テンプレート・セット項目の変更
- テンプレート・セット項目の削除

新しいテンプレート・セット項目の作成

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS テンプレート・セットの構成」をクリックして、「CAS 構成ナビゲーター」パネルを開きます。
2. 「新規」をクリックして、「モニター項目テンプレート定義」パネルを開きます。
3. テンプレート・セット名を入力し、OS タイプとデータベース・タイプを選択して、「適用」をクリックします。
4. 「セットに追加」をクリックし、新規項目を作成します。

テンプレート・セット項目の変更

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS テンプレート・セットの構成」をクリックして、「CAS 構成ナビゲーター」パネルを開きます。
2. テンプレート・セット・リストを OS タイプまたはデータベース・タイプでフィルターに掛けます。
3. 変更するテンプレート・セットを選択して「変更」をクリックすると、「CAS テンプレート・セット定義」パネルが開きます。
4. 変更する項目を選択し、「選択したものを編集」をクリックします。必要な変更を加え、「適用」をクリックして変更内容を保存します。

テンプレート・セット項目の削除

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS テンプレート・セットの構成」をクリックして、「CAS 構成ナビゲーター」パネルを開きます。
2. テンプレート・セット・リストを OS タイプまたはデータベース・タイプでフィルターに掛けます。
3. 変更するテンプレート・セットを選択して「変更」をクリックすると、「CAS テンプレート・セット定義」パネルが開きます。
4. 削除する項目を選択し、「選択したものを削除」をクリックします。

CAS アイテム・テンプレート定義パネル

コンポーネント	記述
OS タイプ	オペレーティング・システムの種類 (Windows または Unix)。 テンプレート・セットが空の場合にはこの選択を変更できますが、テンプレート・セットに 1 つ以上の項目が含まれる場合は変更できません。
データベース・タイプ	データベースの種類 (Oracle、MS-Sql、DB2®、Sybase、Informix® など)、またはオペレーティング・システム・テンプレート・セットの場合は N/A。テンプレート・セットが空の場合にはこの選択を変更できますが、テンプレート・セットに 1 つ以上の項目が含まれる場合は変更できません。

記述	レポートで使われる、項目を示すオプションの名前。他の CAS パネル (例えば「CAS テンプレート・セット定義」) の中で項目を識別します。省略した場合、項目名のデフォルトとして、(タイプに応じて) ファイル名またはパターン、変数名、またはスクリプトが使用されます。
タイプ	以下のいずれか 1 つ: SQL 照会、OS スクリプト、環境変数、レジストリー変数、レジストリー変数パターン、ファイル、ファイル・パターン 詳しくは『テンプレートと監査のタイプ』を参照してください。 注: CAS に基づく評価テストと共に使われる場合は、OS スクリプト・タイプでなければなりません。
内容	モニターする特定の項目を定義するタイプ依存テキストや、それを生成する方法。 詳しくは『テンプレートと監査のタイプ』を参照してください。 注: OS スクリプトの場合、CAS はスクリプトが完了するのを待ちます。OS スクリプトの実行時間を制限し、CAS がスクリプトを強制終了できるようにするには、cas_command_wait という guard_tap.ini ファイル中のパラメーターを使用します。デフォルトの待機時間は 300 秒つまり 5 分です。このパラメーターを変更するとき、CAS を再始動する必要はありません。
アクセス権の制限	ファイルおよびファイル・パターン・タイプのみ。 Unix のみで使用 - このファイルに関して、超過してはならないアクセス権 (許可) の数
ファイル所有者	ファイルおよびファイル・パターン・タイプのみ。ファイルの所有者。
ファイル・グループ	ファイルおよびファイル・パターン・タイプのみ。ファイルのグループ所有者。
期間	各テスト実行間の最大間隔。分数 (m)、時間数 (h)、または日数 (d) で指定します。最初の期間が始まった後、次の期間が始まるまで、データが使用可能になります。
データを保持	選択した場合、実データのコピーがそれぞれの変更点と共に保存されます。例えばファイル項目の場合、そのファイルのコピーが保存されます。選択した場合でも、項目の生データのサイズが (この CAS ホストについて構成された)「生データ制限」を超えると、データは保存されません。
MD5 を使用	MD5 アルゴリズムを使って生データのチェックサムを計算することにより、追加的な比較を行うかどうかを示します。大きな文字オブジェクトの場合、MD5 チェックサムの計算にかなり時間がかかります。しかし、これは変更の標識として、単なるサイズよりも優れています。デフォルトでは MD5 が使用されません。MD5 を使用しても、生データのサイズが CAS ホスト用に構成された 「MD5 サイズ制限」を上回る場合は、MD5 による計算と比較はスキップされます。
有効	デフォルトで選択済みです。項目の変更を検査するかどうかを示します。

テンプレートと監査のタイプ

タイプ	記述
SQL 照会	内容は有効な SQL ステートメントでなければなりません。ステートメントによって戻される結果は、前回の照会実行で戻された結果と比較されます。使用されるデータ・ソースで指定されたパラメーターを使って照会が実行されます (ユーザー名、パスワード、データベース・ポートなど)。照会の結果を戻せないという障害を防ぐために、データ・ソースでこれらのパラメーターを設定するときには注意が必要です。
OS スクリプト	内容として、有効なコマンド行エントリー、または OS 実行可能スクリプトが入っているファイル名が可能です。スクリプトは、データ・ソース定義の「データベース・インスタンス・アカウント」フィールドで指定されている OS ユーザーの環境で実行されます。
環境変数	内容は、データ・ソース定義の「データベース・インスタンス・アカウント」フィールドで指定されている OS ユーザーのコンテキストで定義された、環境変数を指定する必要があります。
レジストリー変数	内容は、ホストの Windows レジストリー内の変数のパスとして解釈されます。そのパスで検出される値は、前回のパスのトレースで検出された値と比較されます。
レジストリー変数パターン	内容は、Windows レジストリーのパスの構成要素と突き合わせるために使用される一連の正規表現です。パターンは、(前述の説明のように扱われる) レジストリー変数タイプのモニター項目を作成するために使用されます。 複数の正規表現は / によって結合され、1 つのレジストリー・パスに似たパターンとなります。より一般的な ¥ 文字は Java™ 正規表現の構文における特殊文字であるため、使用できません。いずれかの正規表現の中で / を使用する必要がある場合は ¥ を使用してエスケープしなければなりません (例えば U/235 に一致させるには U¥/235 を使用します)。 パターン .. を使用すると、パス内のゼロ個以上の構成要素に一致させることができます。例えば、HKLM/Software/../buzz は HKLM¥Software¥buzz と HKLM¥Software¥one¥two¥three¥buzz のどちらとも一致します。 このタイプのパターンは処理負荷の高いレジストリー検索になる可能性があるため、慎重に使用してください。 これらの例外を除いて、正規表現は Java 正規表現の構文に従います。
ファイル	内容は、ホスト上の絶対ファイル・パスとして解釈されます。このパスで検出されるファイルの特性は、パスが最後にトレースされたときに検出された特性と比較されます。環境変数をパスに含めることができます。環境変数は、データ・ソースで指定されている OS ユーザーのコンテキストで展開されます。また、("$SYBASE_HOME" のような) 置換変数をパスの先頭で使用することもできます。置換変数は、データ・ソース定義の「データベース・インスタンス・ディレクトリー」フィールドで入力された値に置換されます。

ファイル・パターン	内容は一連の正規表現です。これは、ファイル・パスの構成要素と突き合わせて、ファイル・タイプのモニター項目を生成するために使用されます。複数の正規表現は / によって結合され、実際のファイル・パスに似たパターンとなります。正規表現の構文のために、レジストリー・パターンの場合と同様、Windows ファイルには ¥ を使用できません。パターンが *?:* で始まる場合、Windows マシンでは、複数ドライブ・マシンの各ドライブでパターン・マッチングが開始されます。レジストリー・パターンで説明された「..」構造は、ファイル・パターンでも (慎重に) 使用することができます。OS ユーザーのコンテキストからの環境変数をファイル・パターンで使用できます。環境変数は、正規表現の展開の前に展開されます。

GuardAPI コマンド

create_cas_template_set

create_cas_template

create_datasource

create_cas_host_instance

親トピック: 構成監査システム

CAS ホスト

構成監査システム (CAS) のホスト構成では、1 つ以上の CAS インスタンスが定義されます。

1 つ以上の CAS テンプレート・セットを定義して CAS をデータベース・サーバーにインストールすると、CAS をそのホスト上で構成する準備ができた状態になります。CAS ホスト構成は 1 つ以上の CAS インスタンスを定義します。各 CAS インスタンスは 1 つの CAS テンプレート・セットを指定し、データベースへの接続に必要なパラメーターをすべて定義します。CAS がインストールされているデータベース・サーバーごとに 1 つの CAS ホスト構成があり、通常は複数の CAS インスタンスがそこに含まれます (例えばオペレーティング・システム項目をモニターする 1 つの CAS インスタンスと、個々のデータベース・インスタンスをモニターする追加的な複数の CAS インスタンス)。

- CAS インスタンスの定義
- CAS インスタンスの変更
- CAS インスタンスの削除
- CAS インスタンスの無効化

CAS インスタンスの定義

1. 「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS ホスト構成」をクリックして、「CAS 構成ナビゲーター」を開きます。

   メニューには、CAS がインストールされているすべてのデータベース・サーバーがリストされ、このホストが Guardiumに接続済みです。

2. リストのフィルタリングを使用して、OS タイプまたはデータベース・タイプでフィルターに掛け、処理したいホストを見つけることができます。
3. 変更するホストを強調表示し、「変更」をクリックします。
4. メニューからテンプレート・セットを選択します。
   注: CAS インスタンスは、ホストがオフライン状態である場合、またはホストの 2 次 Guardium システムである場合には、定義することはできません。
5. 「データ・ソースの追加」をクリックして「データ・ソース・ファインダー」パネルを開きます。
   注: このホストで、このテンプレート・セット用の互換データ・ソースが存在しない場合は、「新規」をクリックして「データ・ソース定義」パネルを開き、データ・ソースを追加することができます。
6. テンプレート・セットに追加するデータ・ソースを選択し、「追加」をクリックしてテンプレート・セットに追加します。

Guardium® CAS パネルを見つける

CAS 構成機能へのアクセス権限は admin ユーザー、および CAS ロールを割り当てられたユーザーに限定されます。

「強化」をクリックします。CAS 機能はすべて「構成変更制御 (CAS アプリケーション)」ヘッダー内にリストされます。

CAS 構成ナビゲーターを開く

「CAS 構成ナビゲーター」パネルから操作を開始して、CAS ホストを作成または変更することができます。

「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「CAS ホスト構成」をクリックして、「CAS 構成ナビゲーター」パネルを開きます。

CAS インスタンスの変更

1. CAS 構成ナビゲーターを開きます。
2. リストのフィルタリングを使用して、OS タイプまたはデータベース・タイプでフィルターに掛け、処理したいインスタンスを見つけることができます。
3. 変更するホストを強調表示し、「変更」をクリックします。

   選択したホストに関連付けられた定義済み CAS インスタンスがリストされて、それと共に以下の情報と編集オプションが表示されます。

表 1. CAS インスタンスの変更

コンポーネント	記述
「インスタンスの無効化/有効化」アイコン	「インスタンスの無効化」アイコンをクリックすると、CAS インスタンスが無効/有効になります
「インスタンスの削除」アイコン	「インスタンスの削除」アイコンをクリックすると、CAS インスタンスが削除されます
データ・ソース	インスタンスによって使われるデータ・ソースを識別します。「**データ・ソース**」をクリックすると「データ・ソース定義」パネルが開いて、データ・ソース定義を編集できます

コンポーネント	記述
テンプレート・セット	インスタンスによって使われる CAS テンプレート・セットを識別します。このリンクをクリックすると「モニター項目テンプレート定義」パネルが開いて、テンプレート・セット定義を表示または変更できます。 詳しくは、CAS テンプレートの処理を参照してください
モニター項目	インスタンスによって現在モニターされている項目の数。このリンクをクリックすると「モニター項目定義」パネルが開いて、現在モニターされている全項目のリストが表示されます 詳しくは、『モニター項目リストの表示』を参照してください。 注: 定義されたモニター項目の数にかかわらず、デフォルトでは 10,000 個のモニター項目をレポートで表示可能です。モニター項目の数がこの制限に近づいた場合には、複数のインスタンスを定義することをお勧めします。

CAS インスタンスの削除

1. CAS 構成ナビゲーターを開きます。
2. リストのフィルタリングを使用して、OS タイプまたはデータベース・タイプでフィルターに掛け、処理したいインスタンスを見つけることができます。
3. 「インスタンスの削除」をクリックして、CAS インスタンスを削除します。収集されたすべての変更データも削除されます。

CAS インスタンスの無効化

1. CAS 構成ナビゲーターを開きます。
2. リストのフィルタリングを使用して、OS タイプまたはデータベース・タイプでフィルターに掛け、処理したいインスタンスを見つけることができます。
3. 変更するホストを強調表示して「変更」をクリックするか、ダブルクリックすると、「ホスト・インスタンス定義」パネルが開きます。
4. 「インスタンスの無効化」アイコンをクリックすると、CAS インスタンスが無効になります。このアイコンを再びクリックしてインスタンスを有効にするまでは、変更データは収集されません。

モニター項目リストの表示

「ホスト・インスタンス定義」パネルで「モニター項目」リンクをクリックすると、モニターされる項目の詳細リストが「モニター項目定義」パネルに表示されます。以下の表では、このホスト構成に関する「モニター項目定義」パネルに表示されるコンポーネントについて説明します。

モニターされるすべての項目は、生データ、ホスト上の文字オブジェクト、SQL 照会の結果、OS スクリプトの出力、またはファイルの内容を参照します。その文字オブジェクトのサイズが計算されます。項目がファイルである場合、許可、所有者、グループ、最終変更時間もまた検査されます。項目が最後に検査された時点と比べて、これらのいずれかが変更されている場合には、変更が記録されます。

表 2. モニター 項目リストの表示

コンポーネント	記述
選択ボックス	モニター項目を個々に、またはグループとして編集するには、選択ボックスにチェック・マークを付けます。 いずれかのモニター項目をダブルクリックすると、その項目を編集できます。
項目	「CAS アイテム・テンプレート定義」パネルに記述されたモニター項目の名前
タイプ	OS スクリプト、SQL 照会、ファイル、環境変数、またはレジストリー変数のいずれか 1 つ OS スクリプトまたは SQL スクリプト: オペレーティング・システム・スクリプトまたは SQL スクリプトの実際のテキストまたはパス。この出力が、次回の実行時に生成される出力と比較されます。 ファイルまたはファイル・パターン: 1 つの特定のファイル、または複数ファイルのセットを識別するためのパターン 環境変数またはレジストリー変数: 環境変数または (Windows) レジストリー変数
期間	テスト実行の平均間隔。秒数、分数、時間数、または日数で指定します。
データを保持	マークを付けた場合、実データのコピーがそれぞれの変更点と共に保存されます。例えばファイル項目の場合、そのファイルのコピーが保存されます。マークを付けた場合でも、項目の生データのサイズが (この CAS ホストに関して構成された)「生データ制限」を超えると、データは保存されません。
MD5 を使用	MD5 アルゴリズムを使って生データのチェックサムを計算して比較を行うかどうかを示します。大きな文字オブジェクトの場合、MD5 チェックサムの計算にかなり時間がかかります。しかし、これは変更の標識として、単なるサイズよりも優れています。デフォルトでは MD5 が使用されません。MD5 を使用しても、生データのサイズが CAS ホスト用に構成された「MD5 サイズ制限」を上回る場合は、MD5 による計算と比較はスキップされます。

GuardAPI コマンド

delete_cas_host

list_cas_hosts

create_cas_host_instance

delete_cas_host_instance

list_cas_host_instances

update_cas_host_instance

親トピック: 構成監査システム

CAS レポート

このセクションでは、構成監査システム (CAS) のレポート作成について説明します。

admin ユーザーは、すべてのクエリー・ビルダーおよびデフォルト・レポートに対するアクセス権限を持ちます。 admin ロールでは、デフォルト CAS レポートにアクセス可能ですが、 CAS クエリー・ビルダーにはアクセスできません。 CAS ロールでは、デフォルト CAS レポートとクエリー・ビルダーの両方にアクセス可能です。

- CAS クエリー・ビルダーへのアクセス
- デフォルト CAS レポートへのアクセス
- CAS レポート・ドメイン

CAS クエリー・ビルダーへのアクセス

このセクションでは、管理者およびユーザーのポータルから、CAS クエリー・ビルダーにアクセスする方法について説明します。 クエリー・ビルダーやレポート・ビルダーの使用方法については、『照会』または『レポート』を参照してください。

UI を使用する場合:

1. 「調査」 > 「レポート・ビルダー」をクリックして、「レポート・ビルダー」を開きます。
2. 「新規」をクリックし、メニューから「照会」を選択し、レポート・タイトルを指定して「次へ」をクリックします。「レポート・ビルダー」の残りは、必要に応じて入力します。

デフォルト CAS レポートへのアクセス

CAS 関連のデフォルト・レポートを表示するには、「強化」 > 「レポート」をクリックします。

CAS レポート・ドメイン

ドメイン	記述
CAS テンプレート	CAS テンプレート定義をトラッキングします。 テンプレートは、変更をモニターされる項目を識別します。 モニター項目は、ファイル、環境またはレジストリー変数、OS または SQL スクリプト出力セット、 またはログオン・ユーザー・セットのいずれであってもかまいません。
CAS 構成	CAS ホスト構成をトラッキングします。 ここで、構成とは、特定のデータベース・サーバー・ホストに 対する、1 つ以上のテンプレート・セットのアプリケーションです。 構成インスタンスから、 テンプレート・セット内で使用可能または使用不可になっている項目や、 ファイル名パターン・テンプレートによって選択されモニターされている (またはされていない) 正確なファイルを 確認することができます。
CAS ホスト履歴	CAS ホスト・イベント (サーバーまたはクライアントのサービス開始やサービス休止など) を追跡します。
CAS 変更	モニター項目 (ファイル、レジストリー変数など) に対する変更をトラッキングします。

CAS テンプレート・ドメイン

エンティティー	記述
テンプレート・セット	テンプレート・セット定義を記述します。
テンプレート	テンプレート・セット内のテンプレート項目を記述します。

「テンプレート・セット」エンティティー

属性	記述
テンプレート・セット ID	テンプレート・セットの固有 ID (連番)。
OS タイプ	オペレーティング・システム: Unix または Windows
データベース・タイプ	データベース・タイプ (Oracle、MS-SQL、DB2®、Sybase、Informix® など) またはオペレーティング・システム・テンプレートの場合は「N/A」。
テンプレート・セット名	テンプレート名。
IsDefault	このテンプレートが、指定された OS タイプとデータベース・タイプの組み合わせにとってデフォルトかどうかを示します。
編集可能	このテンプレートを変更できるかどうかを示します。 デフォルト Guardium® テンプレートは変更できません。 さらに、CAS インスタンスで一度使用されたテンプレート・セットは変更できません。ただし、テンプレート・セットのコピーは常に作成可能であり、そのコピー・セットに変更を加えることができます。
タイム・スタンプ	テンプレートが最後に更新された日時。

「テンプレート」エンティティー

属性	記述
テンプレート ID	テンプレート・セットの固有 ID (連番)。
アクセス名	監査タイプに応じて、OS スクリプトまたは SQL スクリプト、環境値またはレジストリー値、あるいはファイル名またはファイル名パターンになります。
監査タイプ	モニター項目のタイプ。
監査頻度 (分)	テスト間の最大間隔 (分単位)。
MD5 を使用	MD5 アルゴリズムを使用してチェックサムを計算し、その値を前回その項目がチェックされたときに計算された値と比較することによって比較を実行するかどうかを示します。デフォルトでは、MD5 は使用しない設定になっています。MD5 を使用しても、生データのサイズが CAS ホスト用に構成された「MD5 サイズ制限」を上回る場合は、MD5 による計算と比較はスキップされます。MD5 を使用するかどうかに関わらず、項目の最終変更タイム・スタンプの現行値と項目のサイズは、前回その項目がチェックされたときに保存された値と比較されます。
データ保存	「データを保持」チェック・ボックスにマークが付けられているかどうかを示します。マークが付けられている場合は、前のバージョンの項目を現行バージョンと比較できます。
記述	テンプレートの記述 (オプション)。
タイム・スタンプ	テンプレートが最後に更新された日時。

CAS テンプレート・ドメインのデフォルト・レポート

デフォルト・レポート	記述
CAS テンプレート・レポート	CAS テンプレートをリストします。

CAS テンプレート・レポート

エンティティー	属性	演算子	デフォルト値
テンプレート	Access_Name	Like	%
テンプレート・セット	Template_Set_Name	Like	%
テンプレート	Audit_Type	Like	%

CAS 構成ドメイン

エンティティー	記述
ホスト	CAS ホスト (データベース・サーバー) および CAS の現行の状況 (オンライン/オフライン) を識別します。このエンティティーは、「CAS ホスト履歴」ドメインでも使用可能です。

インスタンス構成	インスタンス構成項目は、ホストごとに、 データベース接続パラメーターを (必要に応じて) 含む CAS インスタンスについて記述し、 そのインスタンスが使用するテンプレート・セットを識別します。 インスタンスの現在の状況 (使用中、使用可能、使用不可) と最終リビジョンの日付を示します。
モニター項目詳細	CAS インスタンスがモニターする項目 (例えば、ファイルまたは環境変数など) を識別します。項目定義を含み、項目が使用可能であるかどうかを示します。

「ホスト」エンティティー

エンティティー	記述
ホスト名	データベース・サーバー・ホスト名 (IP アドレスとして表示される場合があります)。
OS タイプ	オペレーティング・システム: UNIX または WIN
オンライン	レコードが書き込まれたときのオンライン状況 (「はい」 または「いいえ」)

「インスタンス構成」エンティティー

属性	記述
データベース・タイプ	データベース・タイプ (Oracle、MS-SQL、DB2、Sybase、Informix など) またはオペレーティング・システム・インスタンスの場合は「N/A」。
インスタンス	インスタンスの名前。
ユーザー	データベースへのログオンに CAS が使用するユーザー名。オペレーティング・システム・インスタンスの場合は「N/A」。
ポート	データベースへの接続に CAS が使用するポート番号。オペレーティング・システム・インスタンスの場合は空。
データベース・ホーム・ディレクトリー	データベースのホーム・ディレクトリー。オペレーティング・システム・インスタンスの場合は空。
テンプレート・セット ID	このインスタンスによって使用されたテンプレート・セットを識別します。

「モニター項目詳細」エンティティー

属性	記述
テンプレート ID	データベース・タイプ (Oracle、MS-SQL、DB2、Sybase、Informix など) またはオペレーティング・システム・インスタンスの場合は「N/A」。
モニター項目	インスタンスの名前。
監査タイプ	データベースへのログオンに CAS が使用するユーザー名。オペレーティング・システム・インスタンスの場合は「N/A」。
有効	データベースへの接続に CAS が使用するポート番号。オペレーティング・システム・インスタンスの場合は空。
同期	データベースのホーム・ディレクトリー。オペレーティング・システム・インスタンスの場合は空。
監査頻度	このインスタンスによって使用されたテンプレート・セットを識別します。
MD5 を使用	MD5 アルゴリズムを使用してチェックサムを計算し、その値を前回その項目がチェックされたときに計算された値と比較することによって比較を実行するかどうかを示します。デフォルトでは、MD5 は使用しない設定になっています。MD5 を使用しても、生データのサイズが CAS ホスト用に構成された「MD5 サイズ制限」を上回る場合は、MD5 による計算と比較はスキップされます。MD5 を使用するかどうかに関わらず、項目の最終変更タイム・スタンプの現行値と項目のサイズは、前回その項目がチェックされたときに保存された値と比較されます。
データ保存	マークが付けられているときは、前のバージョンの項目を現行バージョンと比較できます。
記述	インスタンスの記述 (オプション)。
テンプレートの内容	このモニター項目の基本であるテンプレート項目。インスタンスが作成されるときに「テンプレート」エンティティーの「アクセス名」属性から設定されたものです。 通常はモニター項目と同じになりますが、テンプレートでファイル・パターンが使用された場合は、ファイル・パターンになります。

CAS 構成ドメインのデフォルト・レポート

デフォルト・レポート	記述
CAS インスタンス	CAS インスタンスをリストします。
CAS インスタンス構成	CAS インスタンスの構成変更をリストします。

CAS インスタンス・レポート

エンティティー	属性	演算子	デフォルト値
ホスト	Host_Name	Like	%
ホスト	OS_Type	Like	%
インスタンス構成	DB_Type	Like	%
インスタンス構成	インスタンス	Like	%

CAS インスタンス構成レポート

エンティティー	属性	演算子	デフォルト値
ホスト	Host_Name	Like	%
ホスト	OS_Type	Like	%
モニター項目詳細	Template_Id	Like	%

ドリルダウン・レポート

レポート	記述
レポートの詳細	モニター項目列のカウントに含まれるモニター項目を表示します。

CAS ホスト履歴ドメイン

エンティティー・リスト	ドメインの説明
ホスト	CAS ホスト (データベース・サーバー) および CAS の現行の状況 (オンライン/オフライン) を識別します。このエンティティーは、「CAS 構成」ドメインでも使用可能です。
ホスト・イベント	CAS クライアント/サーバー関係におけるイベントの日時は、クライアントまたはサーバーのサービス開始やサービス休止を示します。

「ホスト」エンティティー

属性	記述
ホスト名	データベース・サーバー・ホスト名
OS タイプ	オペレーティング・システム: Unix または Windows
オンライン	現在のオンライン状況 (はい/いいえ)

ホスト・イベント

属性	記述
イベント時間	イベントが記録された日時。
イベント・タイプ	記録されているイベントを識別します。以下のタイプがあります。 "クライアント停止": データベース・サーバー・ホスト上の CAS が停止しました。 "クライアント稼働": データベース・サーバー・ホスト上の CAS が始動しました。 "フェイルオーバー Off": サーバーが (切断後に) 使用可能になったので、CAS データはサーバーに書き込まれます。 "フェイルオーバー On": サーバーが使用不可なので、CAS データはフェイルオーバー・ファイルに書き込まれます。 "サーバー停止": データベース・サーバーが停止しました。 "サーバー稼働": データベース・サーバーが始動しました。

CAS ホスト履歴ドメインのデフォルト・レポート

デフォルト・レポート	記述
CAS ホスト履歴レポート	各 CAS ホストの CAS イベントをリストします。

CAS ホスト履歴レポート

エンティティー	属性	演算子	デフォルト値
ホスト	Host_Name	Like	%
ホスト	OS_Type	Like	%

ホスト・イベント	Event_Type	Like	%

CAS 変更ドメイン

エンティティー	記述
モニターされた変更	モニター項目が変更されるたびに作成されます。
ホスト構成	モニター項目が変更されるたびに作成されます。
保存データ	変更の保存データを含みます。

「モニターされた変更」エンティティー

属性	記述
変更 ID	変更の固有 ID。
サンプルの時刻	サンプルが取られたときのタイム・スタンプ (ホスト上の日時)。
保存データ ID	この変更に関する「保存データ」エンティティーを識別します。
監査状態ラベル ID	この変更に関する「ホスト構成」エンティティーを識別します。
タイム・スタンプ	サーバーでこの変更レコードが作成された日時 (Guardium アプライアンス・サーバーのクロック)。
所有者	UNIX のみ。項目タイプがファイルの場合に、ファイル所有者。
許可	UNIX のみ。項目タイプがファイルの場合に、ファイル・アクセス権。
サイズ	ファイル・サイズ。ただし、次のような特殊値があります。 -1。ファイルは存在するが、バイト数がゼロである。 0。ファイルは存在しないが、このファイル名がモニターされている (まったく存在しなかったか、削除された可能性がある)。
最終変更	最終変更のタイム・スタンプ。サンプルの時刻にファイル・システムから取得されたもの。
最終変更日	最終変更の日付。
最終変更の曜日	最終変更の曜日。
最終変更の年	最終変更の年。
グループ	UNIX のみ。項目タイプがファイルの場合に、グループ所有者。

「ホスト構成」エンティティー

属性	記述
監査状態ラベル ID	構成項目の固有の数値 ID。
ホスト名	データベース・サーバーのホスト名または IP アドレス。
OS タイプ	オペレーティング・システム: Unix または Windows
データベース・タイプ	データベース・タイプ (Oracle、MS-SQL、DB2、Sybase、Informix など) またはオペレーティング・システム・インスタンスに対する変更である場合は「N/A」。
インスタンス名	テンプレート・セット・インスタンスの名前。
タイプ	変更されたモニター項目のタイプ。 OS スクリプトまたは SQL スクリプト: モニター項目テンプレート定義に含まれる OS スクリプトによって発生した変更。 環境変数: 環境変数 (Unix のみ) レジストリー変数: レジストリー変数 (Windows のみ) ファイル: 特定のファイル。インスタンスによって使用されるテンプレート・セットで定義されたファイル・パターンを対象としたホスト構成エンティティーはありません。 代わりに、パターンに一致するファイルごとに、別々のホスト構成エンティティーがあります。
モニター項目	変更された項目の名前。記述 (入力されている場合) から取得され、それ以外の場合はタイプに応じたデフォルトの名前 (例えばファイル名) になります。

「保存データ」エンティティー

属性	記述
保存データ ID	保存データ項目の固有の数値 ID。
保存データ	保存されている実際のデータ。
タイム・スタンプ	保存データ・エンティティーがサーバー・データベースで記録されたときのタイム・スタンプ。
変更 ID	この保存データ・エンティティーに対応するモニターされた変更エンティティーを識別します。

CAS 変更ドメインのデフォルト・レポート

デフォルト・レポート	記述
CAS 変更詳細	モニター項目ごとに、所有者による変更をリストします。このレポートには、ファイルのプロパティー (所有者やアクセス許可など) に対する変更がリストされます。ファイルの内容に対する変更はリストされません。
CAS 保存データ	オプションの「データを保持」ボックスがチェックされたモニター項目の場合、検出された変更ごとにデータをリストします。このレポートには、ファイルのプロパティーに対する変更ではなく、ファイルの内容に対する変更がリストされます。

CAS 変更のトラッキング

エンティティー	属性	演算子	デフォルト値
ホスト構成	DB_Type	Like	%
ホスト構成	Host_Name	Like	%
ホスト構成	Instance_Name	Like	%
ホスト構成	Monitored_Item	Like	%
ホスト構成	OS_Type	Like	%
ホスト構成	タイプ	Like	%

ドリルダウン・レポート

レポート	記述
レコード詳細	「保存データの数」列に組み込まれる保存データを表示します。

CAS 保存データ

エンティティー	属性	演算子	デフォルト値
ホスト構成	Host_Name	Like	%
ホスト構成	Monitored_Item	Like	%
モニターされた変更	Saved_Data_Id	Like	%

ドリルダウン・レポート

レポート	記述
差異の表示	選択したデータと以前のバージョンとの差異を表示します。

親トピック: 構成監査システム

CAS 状況

「管理」 > 「変更モニター」 > 「CAS 状況」をクリックして、「構成監査システム状況」を開きます。

CAS がインストールされ、実行されており、かつ、この Guardium システムがアクティブな Guardium® ホストとして構成されているデータベース・サーバーごとに、このパネルに CAS 状況と、そのデータベース・サーバーに構成されている各 CAS インスタンスの状況が表示されます。

状況標識ライトの色を区別できない場合は、状況ライト上にマウスを移動すると、テキスト・ボックスに現在の状況が表示されます。

コンポーネント	記述
CAS システム状況標識ライト	このパネルに表示されるライトは、CAS が Guardium システム上でアクティブに稼働しているかどうかを示します。 赤: CAS はこの Guardium システムで実行されていません。 緑: この Guardium システム上の CAS はアクティブです。
CAS エージェント状況標識ライト	これらの状況ライトは、個々の CAS エージェントが Guardium システムに接続されているかどうかを示します。各 CAS エージェントを特定するには、状況標識ライトの行の前に表示される IP アドレスを参照します。 **赤**: ホストおよび/または CAS エージェントはオフラインか到達不能です。 **緑**: ホストおよび CAS エージェントはオンラインです。 **黄色:** Guardium システムは 2 次 CAS ホストです。
リセット	このモニター対象システム上の CAS エージェントをリセットします。これにより、データベース・サーバー上の CAS エージェントが停止し、再始動します。 注: これによりチェックポイント・ファイルもリセットされるため、最初からやり直すことができ、ファイルは最初から再スキャンされます。
削除 (X)	このモニター対象システムを CAS から削除し、また、CAS クライアントに関連付けられていた Guardium システム上のデータも削除します。

	このボタンは、このシステム上で CAS エージェントが実行中の場合は無効になっています。 削除するには、CAS エージェントを停止する必要があります。詳しくは、『CAS エージェントの停止および始動』を参照してください。
赤/黄/緑のライト	各ライト・セットはモニター対象システムの 1 つの CAS インスタンスの状況を示します。 所有するモニター対象システムの状況が赤 (CAS エージェントがオフラインであることを示す) である場合は、この状況ライト・セットは無視してください。 **赤**: インスタンスは使用不可です。 **緑**: インスタンスは使用可能でオンラインです。また、その構成は Guardium システムの構成と同期されています。 **黄色**: インスタンスは使用可能ですが、Guardium システム上のインスタンス構成がモニター対象システム上のインスタンス構成と一致しません (インスタンスは Guardium システム上で更新されたが、その更新がモニター対象システムに適用されていない)。
リフレッシュ	「リフレッシュ」をクリックすると、リスト内のすべてのサーバーの状況が再確認されます。このボタンはデータベース・サーバー上の CAS を停止および/または再始動するためのものではありません。Guardium システム上の CAS と各データベース・サーバー上の CAS との間の接続を検査するだけです。

注: guard_tap.ini ファイルへの TAP_IP 入力が必要です。TAP_IP が欠落していると CAS は始動せず、CAS クライアントのログ・ファイルにエラー・メッセージが記録されます。

CAS エージェントの停止および始動

ある種の状況においては、モニター対象システム上で CAS エージェントを停止または始動しなければならない場合があります。
注: CAS エージェントを停止して再始動する場合は、「管理」 > 「変更モニター」 > 「CAS 状況」をクリックします。

UNIX ホスト上での CAS の停止

1. /etc/inittab ファイルを編集します。
2. CAS の respawn 行を見つけます。

```
cas:2345:respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
```

3. 先頭文字の位置に「#」を挿入して、この行をコメント化します。
4. ファイルを保存します。
5. コマンド init -q を入力します。
6. コマンド ps -er | grep cas を入力します。
7. リストされているそれぞれのプロセスの PID をメモします。
8. リストされているプロセスごとに、コマンド kill -9 <pid> を実行します。
9. Guardium 管理者ポータルの「構成監査システム状況」パネルで、この CAS ホストの状況ライトが赤になっている必要があり、また、「削除」ボタンが有効になっている必要があります。これにより、Guardium システムの内部データベースのこの CAS ホストからデータを削除できます。

UNIX ホスト上での CAS の始動

CAS が、前述のように /etc/inittab ファイルを編集して停止された場合にのみ、次の手順に従って CAS エージェントを再始動します。

1. /etc/inittab ファイルを編集します。
2. 次の行を見つけます。

```
#cas:2345:respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
```

3. 例 (ステップ 2.) で、先頭文字の位置の # を削除して、この行をアンコメントします。オペレーティング・システムによって、コメント文字は異なる場合があります。
4. ファイルを保存します。
5. コマンド init -q を入力して CAS エージェントを再始動します。

Windows ホスト上での CAS の始動および停止

Windows では CAS はシステム・サービスとして実行されます。

1. 「サービス」パネルで、構成監査システムのクライアント項目を強調表示します。
2. 「操作」メニューから「始動」 または「停止」を選択します。

親トピック: 構成監査システム

Guardium システムの構成

ビジネス目標を効果的かつ効率的に達成できるようにするために、Guardium システムのいくつかの側面を構成できます。

- システム構成
  「システム構成」パネル上のほとんどの情報は、インストール時に CLI を使用して設定されます。
- 検査エンジン構成
  検査エンジンは 1 つ以上のサーバーからなるサーバー・セットと、1 つ以上のクライアントからなるクライアント・セットとの間の、特定のデータベース・プロトコル (Oracle や Sybase など) を使用したトラフィックをモニターします。
- ポータル構成
  Guardium® アプライアンスの Web サーバーは、デフォルト・ポート (8443) のままにしておくことも、ポータルを再設定することもできます。デフォルト・ポートのご使用を強くお勧めします。
- 新規レイアウトの生成
- 認証の構成
  デフォルトでは、Guardium ユーザー・ログインは他のアプリケーションから独立して Guardium によって認証されます。
- グローバル・プロファイル
  「グローバル・プロファイル」パネルでは、すべてのユーザーに適用されるデフォルトを定義します。

- アラート機能の構成
  アラート機能を構成してアクティブ化するまでは、E メール・メッセージ、SNMP トラップ、アラート関連 Syslog メッセージはまったく送信されません。
- 異常検出
  異常検出プロセスは、アラートの照会に基づいて相関アラート通知を作成して保存する (ただし送信はしない) ためにポーリング間隔ごとに実行されます。
- セッション推論
  セッション推論は、指定された期間にわたって非アクティブ状態が続いている開いたセッションがあるかどうか検査し、それらにクローズ済みのマークを付けます。
- IP からホスト名への別名割り当て
  IP からホスト名への別名割り当て機能は、ドメイン・ネーム・システム (DNS) サーバーにアクセスして、クライアントおよびサーバーの IP アドレスのホスト名別名を定義します。
- システム・バックアップ
  システム・バックアップ機能を使用すると、オンデマンドまたはスケジュールに基づいて実行可能なバックアップ操作を定義できます。パッチ・バックアップ機能を使用して、バックアップ・プロファイル設定を作成します。
- パッチ・バックアップの構成
  この機能は、バックアップ・プロファイル情報を保管するために使用します。
- ソケット接続権限の構成
  このトピックは、カスタム・アラート・クラスに適用されます。

システム構成

「システム構成」パネル上のほとんどの情報は、インストール時に CLI を使用して設定されます。

システムを構成する方法、またはその他のシステム構成設定を変更する方法については、『システム構成の変更』を参照してください。

アプライアンス内の各種機能を使用するためには、有効なライセンスがなければなりません。システムが始動してからライセンスを入力した場合、GUI を再始動する必要があります。

システム共有パスワードについて

Guardium® 管理者は、「システム構成」でシステム共有パスワードを定義します。システム共有パスワードには、以下の 2 つの一般的な用途があります。

- アーカイブ/エクスポート・アクティビティーによってアプライアンスからエクスポートされたファイルを暗号化する
- 中央マネージャーと管理対象ユニットの間のセキュア通信を確立する

「一元管理」または「統合」(あるいはその両方) を使用している場合、関連するすべてのシステムの「システム共有パスワード」を同じ値に設定する必要があります。

システム共有パスワードの値は、インストール時は NULL です。 企業のセキュリティー・プラクティスに応じて、システム共有パスワードを定期的に変更する必要が生じることがあります。 各アプライアンスは、そのアプライアンスで定義されているすべての共有パスワードの履歴レコードが入っている共有パスワード・ファイルを保守します。 したがって、同じシステムが後日、そのシステムで暗号化された情報を暗号化解除する場合に問題が発生することはありません。

あるシステムから情報がエクスポートまたはアーカイブされ、別のシステムにインポートまたはリストアされた場合、後者のシステムは、前者のシステムで使用された共有パスワードへのアクセス権限を持っている必要があります。 このような場合のために、ある Guardium システムからシステム共有パスワードをエクスポートし、それらを別のシステムにインポートする目的で使用できる CLI コマンドがあります。

CLI 付録で以下のコマンドを参照してください。

- aggregator backup keys file
- aggregator restore keys file

システム構成の変更

1. 「設定」 > 「ツールとビュー」 > 「システム」をクリックして、「システム構成」を開きます。
2. 変更を加えます。
3. 「適用」をクリックして、更新されたシステム構成を保存します。

注: 適用した変更は、Guardium システムを再始動するまで有効になりません。構成変更を適用した後で、「再始動」をクリックし、システムを停止してから再始動します。

表 1. システム構成パネル・リファレンス

フィールドまたはコントロール	記述
固有グローバル ID	この値は、データの照合と統合に使用します。 デフォルト値は、マシンの MAC アドレスから派生した固有値です。 この値は、システムがモニター操作を開始した後は変更しないでください。

フィールドまたはコントロール	記述
システム共有パスワード	ここで入力した値は表示されません。 入力した文字はマスクされます。 システム共有パスワードはアーカイブ/リストア操作、および一元管理/統合操作で使用されます。これを使用する場合、互いに通信するすべてのユニットの間でその値が同じでなければなりません。インストール時にはこの値は NULL で、時間の経過とともに変化する可能性があります。 システム共有パスワードは次のような場合に使用されます。 • 中央マネージャーと管理対象ユニットの間でセキュア接続が確立されるとき。 • 統合されるユニットが、アグリゲーターにエクスポートされるデータに署名して暗号化するとき。 • いずれかのユニットが、アーカイブ用のデータに署名して暗号化するとき。 • アグリゲーターが、統合されるユニットからデータをインポートするとき。 • いずれかのユニットがアーカイブ・データをリストアするとき。 企業のセキュリティー・プラクティスに応じて、システム共有パスワードを時々変更する必要が生じることがあります。共有パスワードは変更される可能性があるため、各システムは、そのシステムで定義されているすべての共有パスワードの履歴レコードが入っている共有パスワード・ファイルを保守します。これにより、古い共有パスワードを使ってシステムからエクスポート (またはアーカイブ) されたファイルを、新しく置換された同じ共有パスワードを持つシステムでインポート (またはリストア) することができます。 **注意**: 使用する場合は、必ず共有パスワードの値を安全なロケーションに保存するようにしてください。 この値が失われると、アーカイブされたデータにアクセスできなくなります。
パスワードの再入力	システム共有パスワードを入力または変更する場合は、新しい値を再入力します。ここで入力した値は表示されません。入力した文字は、すべてアスタリスクで表示されます。
ライセンス・キー	ライセンス・キーは、インストール時に構成に挿入されます。このフィールドは、技術サポートからの指示がある場合を除き、変更しないでください。 オプションのコンポーネントを追加する場合は、新規プロダクト・キーをここに貼り付けなければならないことがあります。 一元管理ユニットで新規プロダクト・キーをインストールする場合は、「適用」をクリックすると、「警告: 一元管理ユニットのライセンスを変更するには、すべての管理対象ユニットの情報をリフレッシュする必要があります。」という警告メッセージを受け取ります。新規プロダクト・キーをインストールするには、「OK」をクリックしてメッセージ・ウィンドウを閉じた後で、「適用」を再度クリックする必要があります。データは正常に保存されました。というメッセージを受け取ることによって、新規ライセンスがインストールされたことを確認できます。 新規プロダクト・キーを一元管理ユニットにインストールする場合に、CM に適用されたライセンスをその管理対象ユニット上でリフレッシュする必要があるという警告を受け取ることがあります。 この場合は、中央マネージャーからリフレッシュを実行する必要があります。それには、中央マネージャーから、リストされている各コレクターのリフレッシュ・アイコンを押します。 ライセンスは、製品およびそれに対応する機能へのアクセス権をユーザーに付与します。 ライセンスは、追加することもオーバーライドすることもできます。 アクティブ・ライセンスは、ADMINCONSOLE_PARAMETER の LICENSE_KEY に格納されます。 製品タイプ: DAM、FAM、VA 製品タイプのエディション: Express、Standard、Advanced
データ・ソースの数	制限付きライセンスが適用されている場合、データ・ソース・ライセンスごとに許容されるデータ・ソースの最大数が表示されます。
残計量スキャン数	制限付きライセンスが適用されている場合、計量ライセンスごとに許容される脆弱性評価スキャンの数 (データ・ソース計量) が表示されます。脆弱性評価がトリガーされるたびに、このスキャン・カウンターが 1 つずつ減少します。
ライセンス有効期限:	制限付きライセンスが適用されている場合、ライセンスが無効になることが確定している日付が表示されます。
ライセンスの数	この値は、残っているライセンスの数を示します。
注: ネットワーク・アドレス、2 次管理インターフェース、およびルーティングの設定は、CLI を使用して構成します。	これらの設定は、GUI を使用して構成することはできないため、「システム構成」ユーザー・インターフェースではグレー化して表示されます。
システム・ホスト名	Guardium システムの解決可能なホスト名。この名前は、1 次システム IP アドレスの DNS ホスト名に一致している必要があります。
ドメイン	Guardium システムがある DNS ドメインの名前。
システム IP アドレス	ユーザーと S-TAP® または CAS エージェントが Guardium システムへの接続に使用する 1 次 IP アドレス。これは、ETH0 というラベルの付いたネットワーク・インターフェースに割り当てられます。
サブネット・マスク	1 次システム IP アドレスのサブネット・マスク。
ハードウェア (MAC) アドレス	1 次ネットワーク・インターフェースの MAC アドレス。

フィールドまたはコントロール	記述

システム IP アドレス (2 次)	オプション: 高可用性フェイルオーバー IP チーミングを提供するために、1 つのポートを 1 次インターフェースと組み合わせて構成することもできます。
	
	または、デバイス上のポートを 2 次管理インターフェースとして、1 次とは異なる IP アドレス、ネットワーク・マスク、およびゲートウェイを使用して構成することもできます。
	
	これら 2 つのオプションを同時に使用することはできません。
	
	2 次管理接続の種類には、次の 2 つがあります。これらは同時には使用できません。どちらも同じ CLI コマンドに対するオプションによって制御されます。
	
	結合 (チーム化)
	eth0 と、もう 1 つの指定されたネットワーク・インターフェース・カード (NIC) を、スタンバイ・フェイルオーバー機能を備えた結合ペアとします。このオプションを実装するには、store network interface high-availability on <nic> という CLI コマンドを使用します。ここで nic は、使用可能な NIC です。
	2 次インターフェース
	Guardium システム内の別の NIC から、GUI および CLI にアクセスできるようにします。このオプションを実行するには、store network interface secondary on <nic> <ip> <mask> <gateway> という CLI コマンドを使用して、2 次 NIC、その IP アドレス、およびネットワーク・マスクを指定し、必要に応じてゲートウェイを指定します。
	
	物理および VM システムの両方で同じ機能が提供されます。 この機能は、Guardium システムまたは VM に取り付けられている NIC の数によって異なります。
	
	ユニットにインストールされているネットワーク・インターフェースを表示するには、**show network interface inventory** CLI コマンドを使用します。 例:
	
	`show network interface inventory`
	`Current network card configuration:`
	`Device  | Mac Address  |Member of`
	`----------`
	`eth0  |  00:50:56:3b:c3:73  |`
	`eth1  |  00:50:56:8a:0d:fa  |`
	`eth2  |  00:50:56:8a:0d:fb  |`
	`eth3  |  00:50:56:8a:00:c1  |`
	
	注: 「Member of」は、結合が存在する場合に、どの NIC が結合ペアであるかを示します。
	
	アプライアンス上の eth コネクターを見つけるには、**show network interface port** CLI コマンドを使用します。 これにより、そのポート上でオレンジ色のライトが 20 回明滅します。 例:
	
	guard14.xyz.com> sho net int port 3
	
	これで、オレンジ色のライトがポート eth5 上で 20 回明滅します。
	
	注: 2 次 IP アドレスとそれに関連付けられたポートは、1 次接続の IP チーム化を介してフェイルオーバー・サポートを提供する高可用性フィーチャーとは無関係です。 高可用性オプションについて詳しくは、CLI 付録の『**store network interface** コマンド』を参照してください。

サブネット・マスク (2 次)	オプション。2 次システム IP アドレスのサブネット・マスク。
デフォルト経路 / 2 次経路	システムのデフォルト・ルーターの IP アドレス / 2 次ルーターの IP アドレス
1 次リゾルバー 2 次リゾルバー 3 次リゾルバー	1 次リゾルバーの IP アドレス (DNS) は必須です。 2 次と 3 次はオプションです。
接続のテスト	対応する DNS (ドメイン・ネーム・システム) サーバーへの接続をテストするには、「接続のテスト」をクリックします。これは単に、指定されたホストのポート 53 (DNS) にアクセスできることを検査するだけです。 機能している DNS サーバーであることの検証はしません。 DNS サーバーが応答したかどうかを示すメッセージ・ボックスを受け取ります。
停止	システムをシャットダウンするには、「停止」をクリックします。
再始動	システムを停止してから再始動するには、「再始動」をクリックします。アクションの確認を求めるプロンプトが出されます。
適用	変更内容を保存するには、「適用」をクリックします。変更内容は、次回にシステムを再始動したときに適用されます。

親トピック: Guardium システムの構成

検査エンジン構成

検査エンジンは 1 つ以上のサーバーからなるサーバー・セットと、1 つ以上のクライアントからなるクライアント・セットとの間の、特定のデータベース・プロトコル (Oracle や Sybase など) を使用したトラフィックをモニターします。

検査エンジンはネットワーク・パケットから SQL を抜き出し、センテンス、要求、コマンド、オブジェクト、およびフィールドを識別する構文解析ツリーをコンパイルして、そのトラフィックについての詳細情報を内部データベースに記録します。

Guardium® アプライアンス上で複数の検査エンジンを構成し、開始したり停止したりすることができます。

検査エンジンは中央マネージャー・ユニット上で定義したり実行したりすることはできません。 ただし、管理対象ユニット上の検査エンジンを、中央マネージャー制御パネルから開始および停止することができます。

また、検査エンジンは S-TAP® 上でも定義されます。S-TAP がこの Guardium アプライアンスにレポートを送る場合は、アプライアンスが S-TAP と同じトラフィックをモニターしないように気をつけてください。 そのような状況が発生すると、分析エンジンが重複するパケットを受け取り、メッセージを再構成できず、そのトラフィックを無視することになります。

IP アドレスの選択

各検査エンジンは 1 つ以上のクライアントおよびサーバーの IP アドレス間のトラフィックをモニターします。 検査エンジンの定義において、これらは IP アドレスおよびマスクを使用して定義されます。IP アドレスを単一のロケーションと考え、マスクを一定範囲の IP アドレスを定義できるワイルドカードの手段と考えることができます。

IP アドレスの形式は n.n.n.n で、それぞれの n は 0 から 255 の範囲の 8 ビットの数字 (オクテットと呼ぶ) です。

例えば、ご使用の PC の IP アドレスが 192.168.1.3 だとします。このアドレスは例で使用されます。これらは 2 進数なので、最後のオクテット (3) は 00000011 と表記されます。

マスクは IP アドレスと同じ形式 (n.n.n.n) で指定されます。 マスクの任意のビット位置にあるゼロは、ワイルドカードの意味になります。したがって、マスク 255.255.255.240 と IP アドレス 192.168.1.3 を組み合わせると、最後のオクテットが 0 から 15 のすべての値に一致します。これは、値 240 は 2 進数で 11110000 だからです。しかし最初の 3 つのオクテットでは値 192.168.1 にのみ一致します。これは 255 は 2 進数で表すとすべて 1 である (つまり、最初の 3 つのオクテットにはワイルドカードが適用されない) からです。

2 進数によるマスクの指定は多少紛らわしいかもしれません。しかし便宜上、IP アドレスは通常、階層的にグループ化されており、あるカテゴリー (デスクトップ・コンピューターなど) のすべてのアドレスは最後の 2 つのオクテットのいずれかでグループ化されます。したがって、実際にマスクで最もよく目にする数字は 255 (ワイルドカードなし) または 0 (すべて) となります。

このように、マスク 255.255.255.255 (ゼロ・ビットを持たない) は、IP アドレスにより指定される単一のアドレス (例では 192.168.1.3) のみを識別します。

または、マスク 255.255.255.0 を同じ IP アドレスと組み合わせると、192.168.1 で始まるすべての IP アドレスが一致します。

すべてのアドレスの選択

すべての IP アドレスを示すのにしばしば利用される IP アドレスの 0.0.0.0 は、Guardium では許可されません。IP アドレスとマスクの組み合わせですべての IP アドレスを選択するには、任意のゼロ以外の IP アドレスにすべてがゼロのマスクを続けます (例えば 1.1.1.1/0.0.0.0 となります)。ただし、 0.0.0.0/0.0.0.0 は有効な組み合わせです。

すべての検査エンジンに適用される設定の構成

1. 「管理」 > 「アクティビティー・モニター」 > 「検査エンジン」をクリックして、「検査エンジン構成」を開きます。
2. 表を参照して、必要な変更を行います。
3. 変更が終わったら「適用」をクリックして、更新したシステム構成を保存します。
4. 必要に応じて、検査エンジンにコメントを追加します。
5. 「検査エンジンの再始動」をクリックします。

注: 適用された変更は、検査エンジンが再始動するまで有効になりません。検査エンジンの構成変更を適用した後、「再始動」ボタンをクリックしてシステムを停止し、(新しい構成設定を使用して) 再始動します。
注: HTTP サポートについては、検査エンジン構成に制限があります。 次の検査エンジン設定は HTTP ではサポートされません: 「デフォルトで値をキャプチャー」、「デフォルトで自動コミットをマーク」、「順序付けをロギング」、「例外 SQL 文字列をロギング」、「影響を受けるレコードをロギング」、「平均応答時間を計算」、「戻りデータの検査」、「空セッションを記録」。

表 1. すべての検査エンジンに適用される設定

コントロール	記述
デフォルトで値をキャプチャー	デフォルト値は false です。リプレイ関数によって、トランザクションとキャプチャー値を区別するために使用されます。準備済みステートメントがある場合は、割り当てられた値がキャプチャーおよびリプレイされます。キャプチャーされた準備済みステートメントを準備済みステートメントとしてリプレイする場合は、キャプチャーされたデータのチェック・ボックスにチェック・マークが付いている必要があります。
デフォルトで自動コミットをマーク	デフォルト値は true です。さまざまなデータベースには各種の自動コミット・モデルがあるため、この値は、当該トランザクションと各コマンドの後の自動コミットに明示的にマークを付けるためにリプレイ関数により使用されます。 注: チェック・ボックスにチェック・マークが付いている場合、コミットとロールバックは無視されます。現在サポートされているデータベースには、DB2®、Informix®、Oracle などがあります。
順序付けをロギング	マークが付いている場合、直前の SQL ステートメントと現在の SQL ステートメントのレコードが作成されます (ただし、前回の構成が十分短期間内に発生していることが条件となります)。
例外 SQL 文字列をロギング	マークが付いている場合、例外が記録されるときに、SQL ステートメント全体が記録されます。

コントロール	記述
影響を受けるレコードをロギング	「影響されるレコード」- SQL ステートメントを実行するたびに影響を受けるレコードの数を示す結果セット。 マークが付いている場合は、各 SQL ステートメント (該当する場合) で影響を受けるレコードの数が記録されます。「影響を受けるレコードをロギング」のデフォルト値は、FALSE (0) です。 注: JDBC を使用している場合、Oracle バインド変数トラフィックを正しくロギングするためにはこれに必ずマークを付ける必要があります。 注: 「影響されるレコード」オプションは、スニファーに対して、追加の応答パケットを処理し、影響を受けたデータ (バッファー・サイズを増やし、スニファー全体のパフォーマンスに悪影響を及ぼす可能性があるデータ) のロギングを延期するように要求するスニファー操作です。 大きな影響を受けるのは、非常に大きい応答からです。この操作に関連する大量のオーバーヘッドを避けるために、Guardium はデフォルトのしきい値セットを使用して、しきい値を超えたときに、処理操作をスキップすることをスニファーが決定できるようにします。 注: 通常、「影響されるレコード」は、ユーザーが「影響を受けるレコードをロギング」をオンにしたときに (「検査エンジン」 > 「影響を受けるレコードをロギング」)、正しく設定されます。ただし、ストアード・プロシージャーを通じて MS-SQL を使用する場合は、「影響されるレコード」が -1 に設定されます。 細分度のレベルを設定するには、構成および制御 CLI コマンドで store max_results_set_size、store max_result_set_packet_size、および store max_tds_response_packets について参照してください。 結果セットの値の例は次のとおりです。 • ケース 1、「影響されるレコード」値: 正数 - これは、結果セットの正しいサイズを表します。 • ケース 2、「影響されるレコード」値: -2 - これは、レコード数が構成可能な限度 (CLI コマンドによって調整可能) を超えたことを示します。 • ケース 3、「影響されるレコード」値: -1 - これは、Guardium によってサポートされないパケット構成のケースを示します。 • ケース 4、「影響されるレコード」値: -2 - 結果セットがストリーム・モードで送信される場合。 • ケース 5、「影響されるレコード」値: -2 - ユーザーを現在の値について更新するためのレコードのカウント中の中間結果。最終的には、レコードの合計を示す正数になります。 注: 「影響されるレコード」機能は、ストリーム・モードを使用して結果を送信する場合は、Db2 ではサポートされません。
平均応答時間を計算	これをマークすると、ロギングされる各 SQL 構文について平均応答時間が計算されます。
戻りデータの検査	マークを付けると、SQL 要求から返されるデータが検査され、Ingress 数と Egress 数が更新されます。 セキュリティー・ポリシーでルールが使用される場合は、このチェック・ボックスにマークを付ける必要があります。
空セッションを記録	これをマークすると、SQL ステートメントを含まないセッションが記録されます。マークを付けないと、これらのセッションは無視されます。
XML の構文解析	検査エンジンは通常、XML トラフィックの構文解析を実行しません。このチェック・ボックスにマークを付けると、XML トラフィックの構文解析が実行されるようになります。
ロギング単位	ログ単位の分数 (1、2、5、10、15、30、または 60)。 レポートで要求される場合、Guardium は要求データをこの細分度で要約します。 例えば、ログ細分度が 60 の場合、ある要求が指定した 1 時間に n 回発生したことになります。 チェック・ボックスがマークされていない場合、その時間内でコマンドが起こった正確な時間は記録されません。しかし、ポリシーのルールが要求によってトリガーされると、リアルタイム・アラートにより、正確な時刻を示すことができます。 ポリシーの例外ルールを定義するときに、それらのルールはログ単位にも適用されます。 例えば、1 時間に 5 回のログイン失敗を無視させるが、6 回目のログイン失敗時にアラートを送信させる場合などが考えられます。
戻りデータ当たりの最大ヒット数	戻りデータが検査されるときに、いくつのヒット (ポリシー・ルール違反) が記録されるかを示します。
無視ポート・リスト	無視するポートのリストです。 データベース・サーバーが非データベース・プロトコルを処理しており、Guardium に非データベース・トラフィックの分析でサイクルを無駄にさせたくない場合は、このリストに値を追加します。例えば、データベースのあるホストがポート 80 で HTTP サーバーも実行していることがわかっている場合は、無視ポート・リストに 80 を追加して、Guardium がこれらのストリームを処理しないようにすることができます。 値を複数入れる場合にはコンマで区切り、ポートの範囲をその値も含めて指定する場合は、値をハイフンでつなぎます。 例: 101、105、110-223
バッファー・フリー: n %	表示のみ。 **n** は、検査エンジンの処理に使用できるバッファー・スペースの空きのパーセントです。 この値は、ウィンドウが最新表示されるたびに更新されます。すべての検査エンジンを駆動する単一の検査エンジン・プロセスがあります。 これは、その処理で使用されるバッファーです。
検査エンジンの再始動	「検査エンジンの再始動」をクリックして、すべての検査エンジンを停止して再始動します。
コメントの追加	「コメント」をクリックして、検査エンジン構成にコメントを追加します。
適用	「適用」をクリックして、構成を保存します。 注: 行ったすべての一括変更 (かつ「適用」ボタンを使用して保存したもの) は、検査エンジンを再開するまで有効になりません。ただし、個々の検査エンジンの属性 (除外、シーケンスの配列など) は直ちに有効になります。

検査エンジンの作成

1. 「管理」 > 「アクティビティー・モニター」 > 「検査エンジン」をクリックして、「検査エンジン」を開きます。
2. 「検査エンジンの追加」をクリックして、パネルを展開します。
3. 「名前」ボックスに名前を入力します。 この名前はアプライアンスで固有でなければなりません。名前には文字と数字のみを使用することをお勧めします。特殊文字を使うと、CLI を介してこの検査エンジンを操作できなくなるからです。

4. 「プロトコル」ボックスから、モニター対象のプロトコル (Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share) またはキーワード「IE を除外」のいずれかを選択します。指定したクライアントとサーバー間のすべてのトラフィックを無視する場合は、IE を除外を選択します。
   注: 「IE を除外」はポートに対してのみ作動します。IP には関係しません。無視するポートの範囲を入力します。このポートで特定の IP を除外する場合は、作成した検査エンジンで「除外データベース・クライアント IP」を使用できます。特定のポート範囲についてパケットを選出する必要がない場合、タイプ「IE を除外」(IGNORE) の別個の検査エンジンを定義します。このエンジンで定義する必要がある値は、PORT_RANGE_START と PORT_RANGE_END のみです。例えば、ポート範囲 1024-65535 を使用して包括的なすべての Oracle 検査エンジンが定義されている状況で、特定のポートを除外する必要がある場合、この種類の除外処理が必要になります。Oracle for Windows を使用する場合は、ポート範囲を 1000 から 65535 に拡大してください。
   注: GreenPlum データベースから IPC トラフィックを送信した場合、これは Guardium システムで PostgresSQL トラフィックとしてログに記録されます。GreenPlum データベースから TCP トラフィックを送信した場合、これは検査エンジンで GreenPlum データベースとしてログに記録されます。TCP トラフィックの場合、Guardium はポートによって (GreenPlum のポートは、ポート 5432) データベースを判別します。Guardium システムは、IPC トラフィックについては名前付きパイプを使用し、GreenPlum データベースについては、PostgresSQL をデータベースの名前として使用します。PostgresSQL と Greenplum データベースの両方が同じシステム上にあるとき、それぞれの IPC トラフィックは、guard_tap.ini ファイルに設定されている最初の PostgresSQL または Greenplum データベース IE に応じて、DB_PROTOCOL に記録されます。
5. 「データベース・クライアント IP/マスク」ボックスに、モニター対象のクライアントのリスト (データベース接続が開始されたクライアント・ホスト) を入力します (または、「除外データベース・クライアント IP」がマークされている場合は、除外するクライアントのリストを入力します)。各クライアントは IP アドレスおよびサブネット・マスクで識別されます。概要には、これらのフィールドの使用法に関する詳しい説明があります。

   正符号をクリックして、追加の IP アドレスおよびサブネット・マスクを追加します。負符号をクリックすると、最後の IP アドレスとサブネット・マスクが削除されます。

6. 「データベース・サーバー IP/マスク」ボックスに、モニター対象のデータベース・サーバー (データベースがある場所) のリストを入力します。各サーバーは IP アドレスおよびサブネット・マスクで識別されます。 概要には、これらのフィールドの使用法に関する詳しい説明があります。

   正符号をクリックして、追加の IP アドレスおよびサブネット・マスクを追加します。負符号をクリックすると、最後の IP アドレスとサブネット・マスクが削除されます。

7. 「ポート」ボックスに、指定したクライアントとデータベース・サーバー間のトラフィックをモニターするのに使用する単一ポートまたはポートの範囲を入力します。 たいていの場合、これは単一ポートです。

   警告: 広いポート範囲を入力しないでください。適正なポートのみを含めるようにしてください。データベース・トラフィックを送信しないポート上のトラフィックや環境に関係ないトラフィックの分析を試行することにより、検査エンジンの速度が低下することがあります。

8. 開始時にこの検査エンジンを自動的に始動させる場合は、「始動時にアクティブ」ボックスにマークを付けます。
9. 「データベース・クライアント IP/マスク」リストにリストされたクライアントを除くすべてのクライアントのトラフィックを検査エンジンにモニターさせる場合は、「除外データベース・クライアント IP」ボックスにマークを付けます。このオプションと「無視」プロトコルの選択との違いを正しく理解してください。このオプションでは、IP アドレスからのトラフィックを除くすべてのトラフィックが含まれます。その他のすべてのクライアントを含めずに、特定のクライアントのセットを無視するには、それらのクライアント用に別の検査エンジンを定義し、「無視」プロトコルを使用します。
10. 「追加」をクリックして、定義を保存します。
11. 必要に応じて、検査エンジン・リストの検査エンジンの位置を変更します。 検査エンジンで定義したフィルター処理機構が、順番に実行されます。 必要な場合は、定義の枠にある「Up」ボタンまたは「Down」ボタンを使用して、新しい検査エンジン構成の位置や、既存の構成の位置を変更します。
12. 必要に応じて、「開始」をクリックして、ここで構成した検査エンジンを開始します。 検査エンジンが開始されると、「始動」ボタンが「停止」ボタンに置き換わります。
13. 注: TAP_IDENTIFIER の値を指定したときに、その値にスペースが含まれている場合は、Guardium によってそのスペースが自動的にハイフンに置き換えられます。例えば、"Sample description" という値は "Sample-description" になります。

検査エンジンの開始または停止

「管理」 > 「アクティビティー・モニター」 > 「検査エンジン」をクリックして、「検査エンジン」を開きます。検査エンジンを開始するには、「開始」をクリックします。 検査エンジンを停止するには、「停止」をクリックします。

検査エンジンの削除

検査エンジンを使用しなくなった場合は、検査エンジンを誤って再開しないように、定義を削除することをお勧めします。

1. 「管理」 > 「アクティビティー・モニター」 > 「検査エンジン」をクリックして、「検査エンジン」を開きます。
2. 削除する検査エンジンが停止していない場合は「停止」をクリックします。
3. 検査エンジンを削除するには、「削除」をクリックします。

親トピック: Guardium システムの構成

ポータル構成

Guardium® アプライアンスの Web サーバーは、デフォルト・ポート (8443) のままにしておくことも、ポータルを再設定することもできます。デフォルト・ポートのご使用を強くお勧めします。

1. 「設定」 > 「ツールとビュー」 > 「ポータル」をクリックして、「ポータル」を開きます。
2. 「始動時にアクティブ」チェック・ボックスがマークされていない場合はマークを付けます (このチェック・ボックスは無効にしないでください)。
3. 「HTTPS ポート」を 1025 から 65535 までの整数値に設定します。
4. 「適用」をクリックして、値を保存します。(Guardium セキュリティー・ポータルは、再始動するまではこのポートでの listen を開始しません。)あるいは「元に戻す」をクリックして、最後の「適用」操作で保管した値をリストアします。
5. 変更を保存したら、「再始動」をクリックして、Guardium Web サーバーを再始動します。これで、新しく割り当てたポート上のユニットに接続できます。
   注: 新しいポート番号で再始動したユニットに再接続するには、ブラウザーで Guardium ログイン・ページを開く際に使用する URL を変更する必要があります。

Guardium アプライアンスにログインするときにユーザー・パスワードが認証される方法を定義するには、Guardium ポータル構成を使用します。 3 つの選択肢があります。

それらの選択肢は、ローカル (Guardium のデフォルト)、RADIUS、LDAP です。

「設定」 > 「ツールとビュー」 > 「ポータル」の下のポータル構成画面は、以下の用途で使用されます。

1. ユーザー・パスワードを認証するための最善の方法を定義する。
2. 認証タイプをリセットするために GUI を再始動する。

ローカル接続は、特定のユーザーのパスワードがログインから定義される場合に機能します。 ログインは accessmgr ロールを使って定義されます。 デフォルトでは、accessmgr ロールを持つ **accessmgr** アカウントにログインします。 このロールによりユーザーは、ユーザー・アカウントを追加またはアップロードし、パスワードを作成することが可能になります。

accessmgr ロール・タイプを使ってユーザー名とパスワードを定義すると、Guardium アプライアンスにログインする際、ユーザーごとに定義済みのパスワードが使用されます。

RADIUS 接続では、Radius サーバーを通じたログイン認証が可能になります。パスワードと SecurID トークン番号の両方を使って Radius/RSA サーバーを定義できます。SecurID トークンの数値パスワードは、ハードウェア・トークンを介して表示されます。

Radius/RSA サーバーは Windows サーバー上で定義されます。また、セキュリティー RSA SecurID トークンが Radius サーバー上に定義され、保管されます。Radius ポータルを機能させるためにそれをダウンロードする必要はありません。

さらに、Unix プラットフォームを使って Radius サーバー接続を定義することができます。Radius は FreeRadius としても定義されます。 ユーザー・アカウントとパスワードが Radius サーバー上で定義されており、それらのダウンロードは必要ありません。 FreeRadius を使用するために、クライアント (Guardium サーバー)、ユーザー名、およびパスワードが FreeRadius Unix サーバー上で定義され、Radius ポータル接続の定義時に使用されます。

デフォルトのポータルは「ローカル」に設定されます。

LDAP 接続は、特定の LDAP サーバーでパスワードが定義され、保管されている場合に機能します。 ユーザーが LDAP ポータルを使ってログインするためには、まず **LDAP サーバー**からユーザー・アカウント名がインポートされる必要があります。accessmgr アカウントから使用可能な「ユーザー LDAP インポート」機能を使用して、LDAP ロケーションを定義した後、LDAP ユーザーをインポートします。パスワードをアップロードする必要はありません。

親トピック: Guardium システムの構成

新規レイアウトの生成

ユーザー・レイアウトに基づいてロールの新規レイアウトを生成

Guardium® 管理者またはアクセス・マネージャーは、CLI を使用してロールのデフォルトのレイアウトを生成できます。レイアウトを生成すると、そのロールを割り当てられた新規ユーザーの初回ログイン後に、そのレイアウトが使用されます。

注: ユーザーおよびロールのデフォルトの .psml 構造は、admin ユーザーが GUI で定義できます。 詳しくは、『ポートレット・エディター』を参照してください。

generate-role-layout CLI コマンドを使用することにより、指定したユーザーのレイアウトによって既存のロール用の新規レイアウトを生成できます。 新規のロール用レイアウトが定義されると、そのロールを初めてのログイン前に割り当てられたユーザーは、そのロール用のレイアウトを受け取ります。

generate-role-layout

構文 generate-role-layout <user> <role>

注: ユーザー (ログイン名) とロールには大/小文字の区別がありません。

パラメーター

次のパラメーターのいずれかがスペースを含む場合 (ユーザーの John Doe またはロールの DBA Managers)、スペース文字を下線文字に置き換えてください。

例:

generate-role-layout John_Doe DBA_Managers

user - レイアウトがロール用レイアウトのモデルとして使用されるユーザーの名前。 ユーザーが存在しない場合は、「次のユーザーは存在しません: `<user> (No such user '<user>')`」というメッセージが表示されます。

role - 新規レイアウトの付加先のロール。

親トピック: Guardium システムの構成

認証の構成

デフォルトでは、Guardium® ユーザー・ログインは他のアプリケーションから独立して Guardium によって認証されます。

Guardium admin ユーザー・アカウントのログインは、常に Guardium だけによって認証されます。他のすべての Guardium ユーザー・アカウントの場合、RADIUS または LDAP を使用するよう認証を構成することができます。これら 2 つの場合、認証サーバーと接続するための追加的な構成情報が必要になります。
注: FreeRadius クライアント・ソフトウェアがサポートされます。

代替的な認証方式を使用する場合であっても、すべての Guardium ユーザーを Guardium アプライアンス上でユーザーとして定義する必要があります。他のアプリケーションによって実行されるのは認証だけです。

ユーザー・アカウントとロールは accessmgr ユーザーによって管理されますが、使用される認証方式は admin ユーザーによって管理されます。これは、職掌分散のための標準的なベスト・プラクティスです。

認証を構成する方法については、次のトピックを参照してください。

Guardium 認証の構成

1. 「設定」 > 「ツールとビュー」 > 「ポータル」をクリックして、「認証構成」を開きます。
2. 「認証構成」パネルで「Guardium」ラジオ・ボタンを選択します。
3. 「適用」をクリックします。

RADIUS 認証の構成

1. 「設定」 > 「ツールとビュー」 > 「ポータル」をクリックして、「認証構成」を開きます。
2. 「認証構成」パネルで「RADIUS」ラジオ・ボタンを選択します。追加のフィールドがパネルに表示されます。
3. 「プライマリー・サーバー」ボックスで、1 次 RADIUS サーバーのホスト名または IP アドレスを入力します。
4. オプションで、2 次および 3 次 RADIUS サーバーのホスト名または IP アドレスを入力します。
5. RADIUS によって使用される UDP ポート (1812 または 1645) を入力します。
6. RADIUS サーバーの「共有パスワード」を 2 度入力します。
7. 「タイムアウト秒数」を入力します (デフォルトは 120)。
8. 「認証タイプ」を次のように選択します。
   - PAP - パスワード認証プロトコル
   - CHAP - チャレンジ・ハンドシェーク認証プロトコル
   - MS-CHAPv2 - Microsoft チャレンジ・ハンドシェーク認証プロトコル (バージョン 2)
9. オプションで、「テスト」をクリックして構成を検証します。テストの結果が通知されます。なお、変更内容を保存するために「適用」ボタンをクリックしたときにも、常に構成がテストされます。
10. 「適用」をクリックします。Guardium はテスト・ユーザーの認証を試み、その結果を通知します。

LDAP 認証の構成

1. 「設定」 > 「ツールとビュー」 > 「ポータル」をクリックして、「認証構成」を開きます。
2. 「認証構成」で「LDAP」ラジオ・ボタンを選択します。
3. 「サーバー」ボックスで、LDAP サーバーのホスト名または IP アドレスを入力します。
4. 「ポート」番号を入力します (LDAP over SSL のデフォルトは 636 です)。
5. 「ユーザー RDN タイプ」(相対識別名タイプ) を入力します。デフォルトでは uid です。
   注:

   この属性は LDAP 認証用にユーザーを識別します。Access Manager が LDAP ユーザー・インポート操作を実行するため、ここで使われる属性を Access Manager に認識させる必要があります。LDAP ユーザーのインポートについて、詳しくは『LDAP ユーザー・インポート』ヘルプ・リンクをクリックしてください。

   RDN 値として SamAccountName を使用する場合、フルネームで a =search または =[domain name] のいずれかを使用する必要があります。

   例: SamAccountName=search、SamAccountName=dom

6. 「ユーザー基本 DN」(識別名) を入力します。
7. LDAP サーバーの必要に応じて「SSL を使用」チェック・ボックスにマークを付けるか、クリアします。
8. オプション。1 つ以上のトラステッド証明書を検査するには、「トラステッド証明書」をクリックして、パネルの指示に従います。
9. オプション。トラステッド証明書を追加するには、「トラステッド証明書の追加」をクリックして、パネルの指示に従います。
10. オプション。「テスト」をクリックして、構成を検証します。テストの結果が通知されます。なお、変更内容を保存するために「適用」をクリックしたときにも、常に構成がテストされます。
11. 「適用」をクリックします。Guardium はテスト・ユーザーの認証を試み、その結果を通知します。

親トピック: Guardium システムの構成

グローバル・プロファイル

「グローバル・プロファイル」パネルでは、すべてのユーザーに適用されるデフォルトを定義します。

デフォルト別名設定のオーバーライド

デフォルトでは、どの新規レポートにも、およびデフォルト・レイアウトに含まれるどのレポートにも、別名は使用されません。

別名は、特定の属性タイプの保管値に代わる同義語になります。通常は、データ値を意味のある、または分かりやすい名前で表示するために使用されます。 例えば、IP アドレス 192.168.2.18 の別名として、「財務サーバー」を定義することができます。

デフォルトで別名を表示させるには、次のようにして、すべてのレポートのデフォルト別名設定を変更できます。

- 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
- 「特に指定されない限りレポートで別名を使用」チェック・ボックスにマークを付けます。
- 「適用」をクリックします。

PDF ページ・フッターのカスタマイズ

さまざまな Guardium® コンポーネント (監査タスクなど) によって作成される PDF ファイルには、標準のページ・フッターがあります。このフッターをカスタマイズするには、次のようにします。

1. 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
2. 「PDF フッター・テキスト」フィールドで、各ページの下部に出力されるテキストを入力します。
   注: PDF フッター・テキストは、中央マネージャー/アグリゲーターから管理対象ユニットに配布されません。
3. 「適用」をクリックします。

アラート・メッセージ・テンプレートの編集

アラートの生成に使われるメッセージ・テンプレートをカスタマイズするには、次のようにします。

1. 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
2. 「メッセージ・テンプレート」テキスト・ボックスで、アラート・テンプレート・テキストを編集します。

   「折り返しなし」チェック・ボックスにマークを付けると、メッセージ内の改行の位置を表示できます。

3. 完了したら、「適用」をクリックします。
4. 検査エンジンが再始動するまで、変更内容は有効になりません。これを直ちに有効にするには、「管理」 > 「アクティビティー・モニター」 > 「検査エンジン」をクリックして、「検査エンジン」を開きます。「検査エンジンの再始動」をクリックします。

表 1. アラート・メッセージ・テンプレートの変数

変数	記述
%%addBaselineConstruct	ベースラインに追加 重要: 「ベースライン・ビルダー」と関連機能は、Guardium V10.1.4 から非推奨になりました。
%%AppUserName	アプリケーション・ユーザー名
%%AuthorizationCode	許可コード
%%category	ルール定義でのカテゴリー
%%classification	ルール定義での分類
%%clientHostname	クライアント・ホスト名
%%clientIP	クライアントの IP アドレス
%%clientPort	クライアント・ポート番号
%%DBName	データベース名。
%%DBProtocol	データベース・プロトコル
%%DBProtocolVersion	データベース・プロトコル・バージョン
%%DBUser	データベース・ユーザー名
%%lastError	最後のエラーの記述 (例外ルールを起動する SQL エラー要求に、最後のエラーの記述フィールドが含まれる場合にのみ使用可能)
%%netProtocol	ネットワーク・プロトコル (Oracle 上の K-TAP では IPC または BEQ として表示されます)
%%OSUser	セッション情報 (GDM_ACCESS での OS_USER)
%%receiptTime	アラートの発生時間を表すタイム・スタンプ
%%receiptTimeMills	アラートの発生時間を表す数値 (固定日 1900 年 1 月 1 日からのミリ秒数)
%%requestType	要求タイプ
%%ruleDescription	ポリシー・ルール定義でのルールの記述
%%ruleID	ルール定義でのルール番号
%%serverHostname	サーバー・ホスト名
%%serverIP	サーバーの IP アドレス
%%serverPort	サーバー・ポート番号
%%serverType	データベース・サーバー・タイプ
%%serviceName	サービス名
%%DBName	データベース名。
%%sessionStart	セッション開始時間 (ログイン時間)
%%sessionStartMills	アラートが発生したセッションの開始時間を表す数値 (固定日 1900 年 1 月 1 日からのミリ秒数)
%%severity	ルール定義での重大度
%%SourceProgram	ソース・プログラム名
%%SQLNoValue	マスクされた値を含む SQL 文字列。SYSLOG 内で SQL の値が ? に置き換えられます。
%%SQLString	SQL 文字列 (存在する場合)
%%SQLTimestamp	パケット/要求の時間 (GDM_CONSTRUCT_TEXT での TIMESTAMP)
%%Subject[ ]	この変数がメッセージ・テンプレートで使用されている場合、[ ] の間に表示されるものすべて (例えば、ファイル名、E メール送信者、説明) は、ユーザーに送信される E メールの件名行になります。
%%violationID	GDM_POLICY_VIOLATION_LOG でのこのアラートの POLICY_VIOLATION_LOG_ID を表す数値 (これはポリシー違反/インシデント管理レポートの「違反ログ ID」と同じです)

名前付きテンプレート

メッセージ・テンプレートを使用してアラートが生成されます。

この機能は、複数のメッセージ・テンプレートを定義し、異なるルールに対して異なるテンプレートを使用できるようにします。これまでは、すべてのルール、すべての受信者タイプなどに対してただ 1 つのメッセージ・テンプレートしか使用できませんでした。

名前付きメッセージ・テンプレートを追加、変更、および削除するには、「編集」をクリックします。新しい名前付きテンプレートを作成するとき、文字列には最初、グローバル・プロファイルのメッセージ・テンプレートで現在設定されている内容のコピーが入っています。可能な重大度のレベルは「R/T アラート」のみです。

SIEM ソリューション (ArcSight、EnVision および QRadar) 用に事前定義メッセージ・テンプレートが作成されています。Guardium システムには、この 2 つの SIEM ソリューションと統合するための 2 つの認定済み (合意済み) テンプレートがプリロードされています。

名前付きテンプレートのビルダーは、 2 つのテンプレート・タイプ (リアルタイム・アラートおよび 監査プロセス・レポート) から選択できます。

監査プロセス・レポートは、プロセス・タスクを監査するときに使用します。

「名前付きテンプレートの編集」をクリックします。「SIEM」を選択し、「変更」をクリックします。「リアルタイム・アラート」または「監査プロセス・レポート」を選択します。

編集した後、複数のメッセージ・テンプレートを「ポリシー・ビルダー」メニューの中から選択できます。ポリシーを参照してください。

QRadar テンプレートを追加すると、(QRadar のフォーマットである) LEEF フォーマットを使用して、QRadar にリアルタイム・アラートまたは監査プロセス・レポートを送信できます。

ステップに従って、リアルタイム・アラートまたは監査プロセスの結果を QRadar SIEM に送信します。

リアルタイム・アラート (Guardium から QRadar へ)

1. リアルタイム・アラートを作成します。
2. syslog に書き込みます。
3. テンプレート型 (読み取り時間アラート) を選択します。
4. (LEEF マッピング / 事前定義メッセージ・テンプレートを介して) Q1 Labs QRadar SIEM に転送します - グローバル・プロファイルから QRadar 名前付きテンプレートを選択します。
5. CLI から、CLI コマンド「store remotelog」を実行して、syslog メッセージを QRadar に転送します。

監査プロセス・レポート (Guardium から QRadar へ)

「強化」 > 「脆弱性評価」 > 「監査プロセス・ビルダー」をクリックして、「監査プロセス・ビルダー」を開きます。

1. 監査プロセス・レポートを作成します (監査プロセス・ビルダー)。
2. syslog に書き込みます。
3. テンプレート型 (監査プロセス・レポート) を選択します。
4. (LEEF マッピング / 事前定義メッセージ・テンプレートを介して) Q1 Labs QRadar SIEM に転送します - グローバル・プロファイルから QRadar 名前付きテンプレートを選択します。
5. CLI から、CLI コマンド「store remotelog」を実行して、syslog メッセージを QRadar に転送します。

例として、「ディスカバーされたデータベース」レポート用のデフォルト LEEF テンプレートを以下に示します。

```
LEEF:0|IBM|Guardium|9.0|Databases Discovered|Time Probed=${1}|Server IP=${2}|Server Host Name=${3}|DB
Type=${4}|Port=${5}|Port Type=${6}
```

テンプレートにマップされるレポートの列を以下に示します。

プローブ時間　　サーバー IP
サーバー・ホスト名　　データベース・タイプ　　ポート　　ポート・タイプ

1. 「CSV ファイルへのエクスポート」と「Syslog に書き込む」にチェック・マークを付けます。
2. 名前付きテンプレート LEEF Discovered Databases を選択します。
3. store remotelog コマンドを使用して、リモート Syslog を構成します。例:

   ```
   store remotelog add user.info 9.70.145.68 udp
   ```

   これにより、監査プロセスからすべてのレコードが、指定された IP アドレスにプッシュされます。

送信者のエンコード

出力メッセージ (E メールおよび SNMP トラップ) を、UTF8 以外のエンコード・スキーマでエンコードするには、CLI コマンド store sender_encoding を使用します。

1 タイプのテンプレートのフィルター操作
すべてのリアルタイム・アラートまたは監査プロセス・レポートを選択するためのフィルター・メカニズムがあります。各選択項目にチェック・マークを付けるか、外します。

Envision 2 メッセージ・テンプレート
GUARDIUM_ALERT:
rule-id=%%ruleID^^category=%%category^^classification=%%classification^^severity=%%severity^^session-start-time=%%sessionStart^^client-hostname=%%clientHostname^^client-ip=%%clientIP^^server-type=%%serverType^^server-ip=%%serverIP^^src-program=%%SourceProgram^^os-user=%%OSUser^^db-user=%%DBUser^^app-user=%%AppUserName^^service-name=%%serviceName^^req-type=%%requestType^^rule-desc=%%ruleDescription^^sql=%%SQLNoValue

しきい値のデフォルトのテンプレート

リアルタイム・アラートの場合と同様に、しきい値に到達したときに送信されるメッセージのテンプレートを選択できます。このテンプレートでは、特定のアラート用に適切な値に置換される変数の定義済みリストが使用されます。

これらの変数は、以下のとおりです。

%%alertName - アラート名

%%description - アラートの記述

%%alertQueryValue - アラートの原因となった照会値

%%alertThreshold - アラートのしきい値

%%alertQueryFromDate - 照会期間の開始

%%alertQueryToDate - 照会期間の終了

%alertBaseQueryValue - アラートの基本照会値

%%classification - アラートの分類

%%category - アラートのカテゴリー

%%severity - アラートの重大度

%%recommendation - アラートに対する推奨アクション

%%Subject[] - メッセージの件名

しきい値アラートのデフォルトのテンプレートは、以下のとおりです (コピーと編集が可能)。

%%Subject[Guardium アラート。 重大度: (%%severity)、アラート名: %%alertName]

アラート名: %%alertName。 アラートの記述: %%description。

現行値: %%alertQueryValue

基本照会値: %%alertBaseQueryValue

しきい値: %%alertThreshold

照会期間: %%alertQueryFromDate - %%alertQueryToDate

アラートの分類: %%classification

カテゴリー: %%category

重大度: %%severity

推奨アクション: %%recommendation

リアルタイム・アラートと E メールのカスタマイズ
E メールの件名に Guardium アプライアンス名を含む接頭部を表示するかどうかを制御します。
E メール本文に E メールの件名を表示するかどうかを制御します。
Guardium ユーザーが、名前付きテンプレート (件名または本文のいずれか) にアプライアンスのホスト名を追加できるように、命名テンプレート・パラメーター %%applianceHostName を追加します。
これを行うには、ADMINCONSOLE_PARAMETERS 表の以下の 2 つのフィールドを使用します。
APPEND_APPLIANCENAME_SUBJECT
APPEND_SUBJECT_IN_BODY
これら 2 つのフィールドの内容を制御するには、以下の CLI コマンドを使用します。
show alerter email append_name_subject
store alerter email append_name_subject
E メールの件名にアプライアンス名を付加するためのフラグを表示または保管します
show alerter email append_subject_body
store alerter email append_subject_body は、E メール本文の先頭に E メールの件名を付加するためのフラグを表示または保管します
CLI 内の値が変更されるたびに、送信される E メールに直ちに反映されます。

CSV 区切り文字

監査プロセスで使われる区切り文字を定義するには、次のようにします。

1. 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
2. コンマ、セミコロン、タブのいずれかを選択するか、または、使用される CSV 区切り文字を「その他」ボックスで独自に定義します。
3. 「適用」をクリックします。

Guardium ウィンドウへの他の HTML コンテンツの追加

他の HTML コンテンツを Guardium ウィンドウに追加するには、次のようにします。

1. 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
2. 「HTML - 左」および「HTML - 右」テキスト・ボックスで、ウィンドウ上に含めるテキストまたは他の項目を表す HTML を入力します。
3. オプションで、プレビュー・ボタンをクリックして、HTML が予期したとおりに表示されるかどうかを確認します。
4. 「適用」をクリックします。

ログイン・メッセージの追加または無効化

ユーザー・ログイン時にメッセージ・ボックスに毎回表示されるメッセージを追加するには、次のようにします。

1. 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
2. 「ログイン・メッセージ」テキスト・ボックスで、各ユーザーのログイン時に表示するテキストを入力します。

3. 「ログイン・メッセージを表示」ボックスにマークを付けると、ログイン・メッセージの表示が有効になります (ボックスをクリアすると表示が無効になります)。
4. 「適用」をクリックします。

同じユーザーによる複数の同時ログインの有効化/無効化

デフォルトでは、同じ Guardium ユーザーが複数の IP アドレスからアプライアンスにログインできます。同じユーザーからの複数の同時ログインを無効にすることができます。無効化した場合、各 Guardium ユーザーは同時に 1 つの IP アドレスからのみログインできます。ユーザーがログアウトせずにブラウザーを閉じた場合、非アクティブ状態のため接続がタイムアウトになります。したがってユーザー・アカウントが長時間にわたってブロックされることはありません。

この設定を変更するには、次のようにします。

1. 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
2. フィールド「異なる IP からの同時ログイン」を探します。
3. 現在の状況に応じて、「有効化」または「無効化」をクリックして、設定を変更します。
   注: この機能が無効になっている場合は、「有効化」ボタンの横に「アンロック」ボタンが表示されます。「アンロック」をクリックすると、別のユーザーがこのユーザー・アカウントを使って別の IP アドレスからログインできるようになります。これはサポートを目的として備えられています。

監視データ・レベルにおけるデータ・レベル・セキュリティーの有効化

この機能では、特定の Guardium ユーザーが特定のデータベースを担当することを想定します。そのため、システム全体に渡って結果をフィルタリングするメカニズムが存在し、各ユーザーは自分が担当するデータベースの情報だけを表示できるようになっています。

制約事項: データ・レベル・セキュリティーと調査ダッシュボードは同時に有効化できません。

この設定を変更するには、次のようにします。

1. 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
2. 「データ・レベル・セキュリティーのフィルタリング」オプションの「有効化」または「無効化」ボタンをクリックします
   注: データ・レベル・セキュリティーが有効で、datasec-exempt ロールがユーザーに割り当てられている場合、datasec-exempt ロールがアクティブになります。
3. 追加の選択項目には、以下のものがあります。
   - すべて表示 - 行がどのユーザーに属するかにかかわらず、ログイン済みのビューアーで結果のすべての行を表示できるようにします。Datasec-exempt ロールと併用すると、データ・レベル・セキュリティーのフィルタリングをオーバーライドできます。
   - 間接レコードを含める - ログインしたビューアーでは、ログイン済みユーザーに属する行を表示できることに加えて、ユーザー階層でログイン済みユーザーの下位にあるユーザーに属するすべての行を表示できます。

注: 監視データ・レベルでのデータ・レベル・セキュリティーが有効になっている場合、監査プロセスのエスカレーションはユーザー階層の上位レベルのユーザーに対してのみ許可されます。

デフォルトのフィルタリング

オンライン・ビューアーおよび監査プロセスの結果配布のデフォルト設定。

「すべて表示」- デフォルト設定は、無効になっています。

結果をすべてのユーザーにエスカレートする

「結果をすべてのユーザーにエスカレート」 - このチェック・ボックスにチェック・マークを付けると、監視データ・レベルでのデータ・レベル・セキュリティーが有効になっている場合であっても、監査プロセスの結果 (および PDF バージョン) がすべてのユーザーにエスカレートされます。 デフォルト設定では有効になっています。このチェック・ボックスが無効になっている (チェック・ボックスにチェック・マークが付けられていない) 場合、監査プロセスのエスカレーションはユーザー階層の上位レベルのユーザーおよび datasec-exempt ロールを持つユーザーに対してのみ許可されます。チェック・ボックスが無効になっており、ユーザー階層がない場合、エスカレーションは許可されません。

カスタム・データベース表の最大サイズ

カスタム・データベース表のサイズを MB 単位で設定します。 デフォルト値は 4000 MB です。

この時点で、「グローバル・プロファイル」メニューに、現在の使用量を確認するためのボタンが表示されます。 「現在の使用量」ボタンをクリックすると、INNODB、MYISAM および合計について値が表示されます。

注: カスタム・サイズ制限は、データのインポートの前にテストされます。 インポートによって最大サイズ制限を超える可能性があります。 制限を超えた場合、その次のインポートが回避されます。

異なるポートを介するファイルの SCP および FTP 送信

SCP および FTP を介するファイル送信に使用できるポートに変更します。

グローバル・プロファイルの場合 - エクスポートおよびパッチ・バックアップを変更できます。 ssh/scp/sftp のデフォルトのポートは 22 です。FTP のデフォルトのポートは 21 です。
注: Guardium GUI にポートとして「0」が表示される場合、デフォルト・ポートが使用されており、変更の必要がないことを示します。

Guardium ウィンドウへのロゴの追加

企業のロゴ・グラフィックを Guardium ウィンドウに追加するか、または他の HTML コンテンツを Guardium ウィンドウに追加するには、次のようにします。

1. 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
2. ポータル・ウィンドウにロゴ・イメージを含めるには、「ロゴ・イメージのアップロード」でイメージ・ファイル名を入力するか、「参照」をクリックして Guardium アプライアンスにアップロードするファイルを選択した後、「アップロード」をクリックします。

3. ブラウザー・ウィンドウをリフレッシュします。新しいロゴが表示されます。

注: アップロードするロゴ・ファイルの名前に、単一引用符、二重引用符、「より小」記号、または「より大」記号を含めることはできません。

Must Gather の暗号化

「Must Gather の暗号化 (Encrypt Must Gather)」が、「グローバル・プロファイル」に追加されました。デフォルトでは、クリアされています (暗号化しない)。これがクリアされている場合、Must Gather 出力は圧縮されるだけで、暗号化されません。このチェック・ボックスにチェック・マークを付けると、以降のすべての Must Gather 出力は暗号化されます。暗号化は、store encrypt_must_gather on CLI コマンドを使用してオンに設定したり、store encrypt_must_gather off を使用してオフに設定したりすることもできます。

Guardium の更新の確認

チェック・マークを追加すると、お客様がダウンロードできる、関連する随時の Guardium パッチ、GPU/CFP/バンドル、Sniffer パッチ、およびセキュリティー・パッチが表示されます。パッチは、インストールされると、リストに表示されなくなります。

データ・ソース接続タイムアウト

データ・ソース接続タイムアウトを分単位で設定します。デフォルトは 60 秒間です。

この値を更新するための対応する GrdAPI コマンドは、grdapi update_datasource_connection_timeout timeoutInSecond=80 です。

親トピック: Guardium システムの構成

アラート機能の構成

アラート機能を構成してアクティブ化するまでは、E メール・メッセージ、SNMP トラップ、アラート関連 Syslog メッセージはまったく送信されません。

アラート機能用のメッセージは他のコンポーネントによって作成され、キューに入れられます。アラート機能は、構成済みのポーリング間隔に基づいてメッセージを検査し、送信します。

個々の相関アラートを構成、有効化、または無効化するには、相関アラートを参照してください。相関アラートおよびアプライアンス・アラートが生成されるためには、異常検出も開始済みでなければなりません。 リアルタイム・アラートが生成されるためには、セキュリティー・ポリシーがインストール済みでなければなりません。

メール/SNMP/SYSLOG メッセージは、優先度に従って送出されます。

始動時のアラート機能の自動アクティブ化

1. 「設定」 > 「ツールとビュー」 > 「アラート機能」をクリックして「アラート機能」を開くか、「保護」 > 「データベースの侵入検出」 > 「アラート機能」をクリックして「アラート機能」を開きます。
2. 「始動時にアクティブ」チェック・ボックスにマークを付けます。アプライアンスが再始動するたびに、アラート機能が自動的にアクティブ化されます。
3. 「適用」をクリックします。
4. アラート機能が実行中でない場合、これを開始するには「再始動」をクリックします。

アラート機能によるメッセージ検査/送信の頻度の設定

1. 「設定」 > 「ツールとビュー」 > 「アラート機能」をクリックして「アラート機能」を開くか、「保護」 > 「データベースの侵入検出」 > 「アラート機能」をクリックして「アラート機能」を開きます。
2. 「ポーリング間隔」(秒) を入力します。
3. 「適用」をクリックします。

SMTP (E メール) メッセージを送信するようアラート機能を構成する

1. 「設定」 > 「ツールとビュー」 > 「アラート機能」をクリックして「アラート機能」を開くか、「保護」 > 「データベースの侵入検出」 > 「アラート機能」をクリックして「アラート機能」を開きます。
   注: このトピックの残りの項目はすべて、「アラート機能」パネルの「SMTP」セクションに含まれています。
2. 「IP アドレス」ボックスに SMTP ゲートウェイの IP アドレスを入力します。
3. 「ポート」ボックスに SMTP ポート番号を入力します (ほとんどの場合、25 です)。
4. オプションで、「接続のテスト」ハイパーテキスト・リンクをクリックして SMTP アドレスとポートを検証します。これは単に、指定されたホストとポートにアクセスできることを検査するだけです。機能している SMTP サーバーであることを検証するものではありません。この操作の成功または失敗を通知するダイアログ・ボックスが表示されます。
   注: この SMTP サーバーが認証を使用する場合、以下の 2 つのフィールドで、そのメール・サーバーの有効なユーザー名とパスワードを提供する必要があります。そうでない場合は、これらのフィールドをブランクにすることができます。
5. SMTP サーバーが認証を使用する場合、メール・サーバーの有効なユーザー名を「ユーザー名」ボックスに入力します。
6. SMTP サーバーが認証を使用する場合、ユーザーのパスワードを「パスワード」ボックスに入力します。「パスワードの再入力」ボックスにそれを再び入力します。
7. 「送信先 E メールアドレス」ボックスに、システムから送られる E メールの送信先アドレスを入力します。 通常、このアドレスは、頻繁にチェックされる管理アカウントです。
8. SMTP サーバーが認証を使用する場合、「認証方式」で 「認証」 を選択します。そうでない場合は、「なし」を選択します。「認証」を選択した場合、認証で使われるユーザー名とパスワードを指定する必要があります。
9. 「適用」をクリックして、構成を保存します。
   注: アラート機能が再始動するまでは、新しい構成は使用されません。
10. 「再始動」をクリックすると、新しい構成を使ってアラート機能が再始動します。

SNMP トラップを送信するようアラート機能を構成する

1. 「設定」 > 「ツールとビュー」 > 「アラート機能」をクリックして「アラート機能」を開くか、「保護」 > 「データベースの侵入検出」 > 「アラート機能」をクリックして「アラート機能」を開きます。
   注: このトピックの残りの項目はすべて、「アラート機能」パネルの「SMTP」セクションに含まれています。
2. 「IP アドレス」ボックスで、SNMP トラップの送信先となる IP アドレスを入力します。
3. オプションで、「接続のテスト」ハイパーテキスト・リンクをクリックして SNMP アドレスとポート (162) を検証します。これは単に、指定されたホストとポートにアクセスできることを検査するだけです。機能している SNMP サーバーであることを検証するものではありません。この操作の成功または失敗を通知するダイアログ・ボックスが表示されます。
4. 「「トラップ」コミュニティー」ボックスに、トラップのコミュニティー名を入力します。「コミュニティーの再入力」ボックスにコミュニティーを再入力します。
5. 「適用」をクリックして、構成を保存します。
   注: アラート機能が再始動するまでは、新しい構成は使用されません。
6. 「再始動」をクリックすると、新しい構成を使ってアラート機能が再始動します。

親トピック: Guardium システムの構成

異常検出

異常検出プロセスは、アラートの照会に基づいて相関アラート通知を作成して保存する (ただし送信はしない) ためにポーリング間隔ごとに実行されます。

この通知は、各アラートに対して定義されたスケジュールに従って実行されます。 通知の送信について詳しくは、アラート機能の構成を参照してください。

異常検出プロセスは、指定された期間をさかのぼって調査する相関アラートの照会の結果と、 相関アラートのしきい値を使用して、条件 (例えば過剰なログイン失敗数) が満たされたかどうかを判別します。詳しくは、相関アラートを参照してください。

中央マネージャー環境では、各 Guardium システムの「異常検出」パネルを使用して、その特定の Guardium システムに適さない相関アラートをオフにすることができます。一元管理下では、すべての相関アラートは、どのシステムで作成や更新が行われたかに関係なく、中央マネージャーで定義されます。これらの相関アラートは、すべての Guardium システムに対して同じになり、アクティブ化されるときには、デフォルトですべての Guardium システムに対してアクティブ化されます。

注: 保存したアラート・メッセージを SYSLOG、E メール、または SNMP トラップに送信するには、アラート機能コンポーネントを構成して開始する必要があります。
注: 異常検出は、(セキュリティー・ポリシーによって生成される) リアルタイム・アラートの生成には関与しません。

始動時の異常検出の自動アクティブ化

1. 「設定」 > 「ツールとビュー」 > 「異常検出」をクリックして、「異常検出」を開きます。
2. 「始動時にアクティブ」チェック・ボックスにマークを付けます。Guardium システムが再始動するたびに、異常検出が自動的にアクティブ化されます。
3. 「適用」をクリックします。

異常検出によってアプライアンスの問題を検査する頻度の設定

1. 「設定」 > 「ツールとビュー」 > 「異常検出」をクリックして、「異常検出」を開きます。
2. 「ポーリング間隔」(分) を入力します。
3. 「適用」をクリックします。

アクティブ・アラートの有効化/無効化

中央マネージャー環境でアラートをグローバルに無効化するには、「アラートの変更」パネルの「アクティブ」チェック・ボックスをクリアするのが簡単な方法です。

一元管理環境で 1 つの Guardium システムのアラートを有効または無効にするには、以下の手順に従ってください。

1. 1 つ以上のアラートを無効にする対象の Guardium システムの UI にログインします。
2. 「設定」 > 「ツールとビュー」 > 「異常検出」をクリックして、「異常検出」を開きます。
3. いずれかのアラートを無効にするには、「アクティブ・アラート」ボックスでそれを選択して「無効化」をクリックします。
4. いずれかのアラートを有効にするには、「ローカルでは無効なアラート」ボックスでそれを選択して「有効化」をクリックします。

異常検出の停止/再始動

1. 「設定」 > 「ツールとビュー」 > 「異常検出」をクリックして、「異常検出」を開きます。
2. 異常検出を停止するには「停止」をクリックし、再始動するには「再始動」をクリックします。

親トピック: Guardium システムの構成

セッション推論

セッション推論は、指定された期間にわたって非アクティブ状態が続いている開いたセッションがあるかどうか検査し、それらにクローズ済みのマークを付けます。

セッション推論オプションを構成するには、次のようにします。

1. 「設定」 > 「セッション推論」をクリックして、「セッション推論」を開きます。
2. Guardium® システムの開始時にセッション推論を開始するには、「始動時にアクティブ」ボックスにマークを付けます。
3. 「ポーリング間隔」ボックスに、セッション推論により開いたセッションがないか検査する頻度 (分数) を入力します。デフォルトは 120 (分) です。
4. 「最大非アクティブ期間」ボックスに、セッションにクローズ済みのマークを付けるまでの、非アクティブ状態の分数を入力します。デフォルトは 720 (分) です。
5. 「適用」をクリックすると、構成データベースに値が保管されます。セッション推論が再始動するまでは、新しい構成は使用されません。
6. 「再始動」をクリックすると、新しい構成を使ってセッション推論が再始動します。

セッション推論を停止するには、「セッション推論」パネルを開いて「停止」をクリックします。

親トピック: Guardium システムの構成

IP からホスト名への別名割り当て

IP からホスト名への別名割り当て機能は、ドメイン・ネーム・システム (DNS) サーバーにアクセスして、クライアントおよびサーバーの IP アドレスのホスト名別名を定義します。

それぞれクライアント用、およびサーバー用に別個の IP アドレス・セットが 2 つあります。IP からホスト名への別名割り当てが有効になっている場合、適切な場合に Guardium® 内で IP アドレスが別名に置き換えられます。

1. 「保護」 > 「データベースの侵入検出」 > 「IP からホスト名への別名割り当て」をクリックして、「IP からホスト名への別名割り当て」を開きます。
2. 「クライアント IP とサーバー IP のホスト名別名の生成 (使用可能な場合)」チェック・ボックスにマークを付け、ホスト名の別名を有効にします。

   2 番目のチェック・ボックスにアクセスできるようになります。このチェック・ボックスの名前は「既存のホスト名別名の更新 (再発見された場合)」です。

3. このチェック・ボックスにマークを付け、以前に定義された、現在の DNS ホスト名に一致しない別名 (通常、その IP アドレスのホスト名が変更されたことを示す) を更新します。いくつかの別名を手操作で既に割り当てた場合は、このような動作が不適切であることがあります。例えば、ある IP アドレスの DNS ホスト名が dbserver204.guardium.com で、そのサーバーの通称が QA Sybase Server であるとします。その IP アドレスの別名として QA Sybase Server が手動で定義されており、かつ「既存のホスト名別名の更新 (再発見された場合)」のチェック・ボックスにマークが付けられている場合、その別名は DNS ホスト名により上書きされます。
4. 「適用」をクリックして、IP からホスト名への別名割り当て構成を保存します。
5. 以下のいずれかを実行します。
   - 「今すぐ 1 回実行」をクリックすると、別名が直ちに生成されます。
   - 「スケジュールの定義」をクリックすると、このタスク実行のスケジュールを定義できます。詳しくは、スケジューリングを参照してください。

定義した別名を表示するには、『別名』を参照してください。

親トピック: Guardium システムの構成

システム・バックアップ

システム・バックアップ機能を使用すると、オンデマンドまたはスケジュールに基づいて実行可能なバックアップ操作を定義できます。パッチ・バックアップ機能を使用して、バックアップ・プロファイル設定を作成します。

システム・バックアップ

ハードウェア破損が生じた場合にサーバーを復元する目的で、必要なすべてのデータと構成値をバックアップして保管するために、システム・バックアップを使用します。

すべての構成情報とデータが 1 つの暗号化ファイルに書き込まれ、このアプライアンスのバックアップ用に構成された転送方式を使用して、指定の宛先に送信されます。

バックアップされたシステム情報をリストアするには、restore system CLI コマンドを使用します。また、特定のユーザーのロールとして diag が定義されている場合には、CLI コマンド diag を使用できます。

システム・バックアップは、以下の方式をサポートしています。

- SCP - デフォルトで定義され、CLI および GUI を介してアクセス可能
- FTP - デフォルトで定義され、CLI および GUI を介してアクセス可能
- Centera - CLI にログインし、次のコマンドを実行して GUI に追加可能: store storage centera backup on
- TSM - 追加できます。そのためには CLI にログインし、次のコマンドを実行します: store storage tsm backup on
- AMAZON S3 - デフォルトで定義され、CLI および GUI を介してアクセス可能。CLI からアクセスできるのは、GUI で定義されている場合です。
- Softlayer - Softlayer のクラウド・バックアップ
- Cleversafe - CleverSafe 機能。Amazon S3 に類似する方法でバックアップを保管します。使用可能なバケットのリストが GUI に直接抽出されます。最初にリストされている名前は、データベースに保存したバケットの名前です。注: (Guardium UI/CLI から) 新しいバケットを作成することも、バケットを削除することもできません。

注: システム・リストアは、システム・バックアップと同じパッチ・レベルに対して実行する必要があります。例えばバージョン 7.0 パッチ 7 の時点でアプライアンスをバックアップした後、新しく構築したアプライアンスにこのバックアップをリストアするには、まずバージョン 7.0 のパッチ 1 から 7 までをアプライアンスにインストールした後で、ファイルをリストアする必要があります。

システム情報をバックアップするには、次のようにします。

1. 「管理」 > 「データ管理」 > 「システム・バックアップ」をクリックして、「システム・バックアップ」を開きます。
2. リストから、ストレージ方式のラジオ・ボタンを選択します。Guardium システムの構成方法によっては、これらのボタンの 1 つ以上が選択できない場合があります。アーカイブおよびバックアップのストレージ方式の構成方法については、構成および制御 CLI コマンドで show storage-system コマンドと store storage-system コマンドの説明を参照してください。
   - EMC CENTERA
   - TSM
   - SCP
   - FTP
   - AMAZON S3
   - Softlayer
   - Cleversafe
3. 選択したストレージ方式に応じて、適切な手順を実行します。
   - SCP または FTP アーカイブまたはバックアップの構成
   - EMC Centera アーカイブまたはバックアップの構成
   - TSM アーカイブまたはバックアップの構成
   - AMAZON S3 アーカイブまたはバックアップの構成
   - Softlayer オブジェクト・ストレージ・クラウド・バックアップの構成
   - Cleversafe - 入力> 有効なエンドポイント、有効なバケット名、有効なアクセス・キー、有効な共有パスワード

4. 「バックアップ」の次のチェック・ボックスのいずれかまたは両方にマークを付けます。
   - 「構成」チェック・ボックスにマークを付けると、すべての定義がバックアップされます。
   - 「データ」チェック・ボックスにマークを付けると、すべてのデータがバックアップされます。(データを定期的にアーカイブしている場合は、これは不要です。)
5. 「スケジューリング」セクションを使用して、この操作を定期的に実行するためのスケジュールを定義できます。
6. 「保存」」をクリックすると、構成の変更が検証されて、保存されます。システムはそのロケーションにテスト・データ・ファイルを送信することにより、構成の検証を試みます。
   - 操作が失敗すると、エラー・メッセージが表示され、構成は保存されません。
   - 操作が成功すると、構成が保存されます。
7. 「今すぐ 1 回実行」をクリックして、操作を 1 回実行します。

注: SCP/FTP/TSM/Centera/AMAZON S3/Softlayer ファイル転送中にバックアップ・ファイルの転送が失敗した場合、(システム・バックアップ、構成バックアップ、アーカイブ、CSV アーカイブなど) バックアップ/アーカイブ・ファイルの各セットの最後のファイルが diag/current フォルダーに保存されます。その後、バックアップ・ファイルの宛先が再びオンラインになったときに、diag/current フォルダーから宛先に手操作でバックアップ・ファイルを転送できます。 バックアップ/アーカイブ・ファイルのセットが diag/current フォルダーに保存されるのは、ファイル転送が失敗した場合だけです。 別のバックアップ・ファイル転送中にファイルの転送が失敗した場合、バックアップ/アーカイブ・ファイルのセットが diag/current フォルダーに再び保存されます。ただし、保存されるファイルが多くなりすぎてディスク・スペースが不足するのを防ぐために、それぞれの種類の最新のファイルだけが保存されます。それより前のバックアップ・ファイルは上書きされます。
注: システム・バックアップを実行し、GIM を定義してあるサーバーから別のサーバーにリストアするときは、 リストア・サーバーに対する GIM フェイルオーバーを構成する必要があります。この GIM 構成は、 バックアップ中央マネージャーまたはシステム・バックアップおよびリストアに適用されます。

異なるポートを介するファイルの SCP および FTP 送信

SCP および FTP を介するファイル送信に使用できるポートに変更します。

システム・バックアップまたはパッチ・バックアップの場合 - プロトコル (SCP または FTP) を設定し、ホスト、ディレクトリー、およびポートを指定します。
ssh/scp/sftp のデフォルトのポートは 22 です。FTP のデフォルトのポートは 21 です。

バックアップ/アーカイブのスクリプトによる /var 容量の使い尽くしの防止

バックアップ・プロセスは、実行前に /var の空き容量をチェックして失敗を防止します。 このプロセスは、バックアップ用のスペースが十分にない場合にも、 ユーザーに警告を出します。

アーカイブ・プロセスは、 静的表のサイズをチェックし、アーカイブを作成できる空き容量が /var にあることを 確認します。

バックアップが 50% を超えると、 ログ・ファイルおよび GUI にエラーが記録されるようになっています。例:

```
ERROR: /var backup space is at 60% used. Insufficient disk space for backup.
```

Guardium での Amazon S3 へのアーカイブおよびバックアップ

Guardium から、Amazon S3 へのデータのアーカイブとバックアップを行う場合に、この機能を使用します。

Amazon S3 (Amazon Simple Storage Service) は、いつでも、Web 上のどこからでも容量に関係なく、データを格納/取得できるシンプルな Web サービス・インターフェースを提供します。これによって、Amazon が Web サイトの稼働に使用しているものと同じ、拡張性と信頼性が高く、安全でありながら安価なインフラストラクチャーを、あらゆる開発者が利用することが可能になります。

前提条件

1. Amazon アカウント
2. S3 サービスの登録
3. Amazon S3 にアクセスするためには、Amazon S3 の認証情報が必要です。 必要な認証情報は次のとおりです。
   - Access Key ID (アクセス・キー ID): ユーザーをサービス要求の担当者として識別します。各要求にこの ID が含まれている必要があります。これは機密ではなく、暗号化する必要はありません (20 文字の英数字から成るシーケンス)。
   - Secret Access Key (シークレット・アクセス・キー): Secret Access Key は Access Key ID に関連付けられ、要求に含まれているデジタル署名を計算します。Secret Access Key は機密事項であり、ユーザーと AWS のみが保持する必要があります (40 文字から成るシーケンス)。このキーは、ファイルではなく、単なる長い文字列であり、この文字列を使用して、要求内に含まれている必要があるデジタル署名を計算します。

「管理コンソール」メニューの「データ管理」セクションでは、次の 2 つのアーカイブ操作を選択可能です。

- 「データ・アーカイブ」は、アプライアンスによって所定の期間内にキャプチャーされたデータをバックアップします。
- 「結果アーカイブ」は、監査タスクの結果 (レポート、アセスメント・テスト、エンティティー監査証跡、プライバシー・セット、および分類プロセス) のほか、表示およびサインオフの証跡、ワークフロー・プロセスからの調整コメントをバックアップします。

Guardium データがアーカイブされると、日ごとに別のデータ・ファイルができます。

アーカイブ・データ・ファイルの名前は、次の形式になります。

```
<time>-<hostname.domain>-w<run_datestamp>-d<data_date>.dbdump.enc
```

アーカイブ機能は、不正に開封できない、署名付きの暗号化ファイルを作成します。 生成されたアーカイブ・ファイルの名前を変更することはできません。 アーカイブ操作は、アーカイブ処理中に作成されるファイル名に依存します。

ハードウェア破損が生じた場合にサーバーを復元する目的で、必要なすべてのデータと構成値をバックアップして保管するために、システム・バックアップを使用します。

すべての構成情報とデータが 1 つの暗号化ファイルに書き込まれ、このアプライアンスのバックアップ用に構成された転送方式を使用して、指定の宛先に送信されます。

バックアップ・システム・ファイルの形式は、次のとおりです。

```
<data_date>-<time>-<hostname.domain>-SQLGUARD_CONFIG-9.0.tgz
<data_date>-<time>-<hostname.domain>-SQLGUARD_DATA-9.0.tgz
```

「統合/アーカイブ・ログ」レポートを使用して、操作が正常に完了したことを確認できます。各アーカイブ操作には、複数のアクティビティーがリストされていなければなりません。 また、各アクティビティーの状況は成功でなければなりません。

Guardium カタログは、アーカイブ・データの宛先に関係なくすべてのアーカイブ・ファイルの送信場所を記録するため、以降のどの時点においても、最小限の労力でシステムでアーカイブ・ファイルを取得およびリストアすることができます。

アプライアンスごとに個別のカタログが保守され、アプライアンスがデータや結果をアーカイブするたびにカタログに新しいレコードが追加されます。

カタログ・エントリーは、以下のいずれかの方法により、アプライアンス間で転送することができます。

- 統合 - カタログ表は統合されます。つまり、アグリゲーターが、そのすべてのコレクターのカタログをマージしたものを保持することになります。
- カタログのエクスポート/インポート - これらの機能は、コレクター間でカタログ・エントリーを転送したり、将来のリストアのためにカタログをバックアップしたりするために使用できます。
- データのリストア - 各データ・リストア操作には、アーカイブした日のデータ (その日のカタログも含む) が含まれます。 したがって、データのリストア時には、カタログも更新されます。

カタログ・エントリーは、別のシステムからインポートされたときには、そのシステムによって暗号化されたファイルをポイントします。 そのようなファイルをリストアまたはインポートする前に、そのファイルを暗号化したシステムのシステム共有パスワードが、インポート側のシステムで使用できなければなりません。

Guardium CLI からの Amazon S3 の有効化

Amazon S3 のアーカイブ/バックアップ・オプションは、デフォルトでは Guardium GUI で有効になっています。Guardium CLI から Amazon S3 を有効にするには、次の CLI コマンドを実行します。

```
store storage-system amazon_s3 archive on
store storage-system amazon_s3 backup on
```

Amazon S3 では、Guardium システムのクロック時刻が正確であること (15 分以内) が求められます。 そうでない場合、Amazon のエラーとなります。要求の時刻と現在の時刻の差が大きすぎると、要求は受け入れられません。

Guardium のシステム時刻が正確でない場合は、次の CLI コマンドを使用して正しい時刻を設定してください。

```
show system ntp server
store system ntp server (An example is ntp server: ntp.swg.usma.ibm.com)
store system ntp state on
```

ユーザー・インターフェース

バックアップを構成するには、「システム・バックアップ」画面 (「管理」 > 「データ管理」 > 「システム・バックアップ」) を使用します。CLI コマンドを使用して Amazon S3 を有効にすると、プロトコルのリストに「Amazon S3」が表示されます。

以下のユーザー入力が必要です。

- S3 Bucket Name (S3 バケット名)。Amazon S3 に保管されるすべてのオブジェクトは、バケット内に格納されます。バケットは、Amazon S3 に保管されるオブジェクトの名前空間をパーティション化します。1 つのバケット内では、保管するオブジェクトに任意の名前を使用できますが、バケット名は Amazon S3 内の全バケットの中で一意である必要があります。
- Access Key ID
- Secret Access Key

バケット名が存在しない場合は、作成されます。

Secret Access Key は、データベースに保存されるときに暗号化されます。

Amazon S3 にファイルがアップロードされたことの確認

1. AWS マネジメント・コンソールに、E メール・アドレスとパスワードを使用してログオンします。

http://aws.amazon.com/console/

1. 「S3」をクリックします。
2. Guardium UI で指定したバケットをクリックします。

Softlayer オブジェクト・ストレージ

SoftLayer オブジェクト・ストレージは、冗長かつハイ・スケーラブルなクラウド・ストレージ・サービスです。 このサービスを使用すると、インターネット上でデータを簡単に保管、検索、取得できます。 これは OpenStack Swift プラットフォームに基づくサービスであり、RESTful API および Web ポータルを使用してアクセスできます。

事前に必要な情報:

- 認証エンドポイント - 認証要求は、ご使用のオブジェクト・ストレージ・アカウントに関連付けられたエンドポイントに送信する必要があります。 https://dal05.objectstorage.softlayer.net/auth/v1.0
- コンテナー - オブジェクト・ストレージ内のすべてのデータの基本ストレージ・ユニットはコンテナーです。ここにはデータ/ファイルが保管され、オブジェクト・ストレージ・アカウントに関連付けられている必要があります。
- X-Auth-User - 認証するユーザー名 (テナント値:ユーザー名)

- X-Auth-Key - 認証する API キー (パスワード)

アカウント資格情報は https://control.softlayer.com/ にログオンすると取得できます。

GUI からの Softlayer によるシステム・バックアップ

1. 「管理」 > 「データ管理」 > 「システム・バックアップ」、「管理」 > 「データ管理」 > 「データ・アーカイブ」、または「管理」 > 「データ管理」 > 「結果アーカイブ」をクリックします。
2. Softlayer プロトコルを選択します。
3. 認証エンドポイント URL を入力します (例: https://dal05.objectstorage.softlayer.net/auth/v1.0)。
4. オブジェクト・ストレージ・コンテナー名を指定します (例: yourname_Container)
5. X-Auth-User (テナント値: ユーザー名) を指定します (例: username)
6. X-Auth Key を入力します (例: password)
7. バックアップ対象 (構成またはデータ) を指定します。
8. 「スケジュールの変更」または「今すぐ 1 回実行」を選択します。

CLI によるシステム・バックアップ (構成)

CLI にアクセスします。

CLI> backup system

1. DATA

2. CONFIGURATION

Please enter the number of your choice: (q to quit) 1

1. SCP

2. CONFIGURED DESTINATION

Please enter the number of your choice: (q to quit) 2

Make sure destination is configured in the GUI under the <System Backup> option

Please wait, this may take some time.

Performing a DEFAULT backup, config=

システム・バックアップおよびシステム・リストア

CLI にアクセスします。

CLI> restore system

1. SCP

2. FTP

3. TSM

4. CENTERA

5. AMAZONS3

7. SOFTLAYER

8. SFTP

Please enter the number of your choice: (q to quit) 7

Enter the SoftLayer Authentication Endpoint URL:

Enter Softlayer Object Storage Container name:

Enter Softlayer X-Auth-User:

Enter X-Auth-Key:

Enter a file name from list:

Authenticate success!

Download file success!

Select your recovery type, for most cases, use the normal option:

1. normal

2. upgrade

システム・バックアップ > Cleversafe

前提条件

Guardium サーバーを正しい現地時間に設定する必要があります。必要に応じて NTPserver サーバーを使用して変更します。

システム・バックアップの選択:

認証エンドポイント URL

(AWS) アクセス・キー

(AWS) 秘密アクセス・キー

バケット名

証明書のすべての質問に対して yes と応答します。

親トピック: Guardium システムの構成

パッチ・バックアップの構成

この機能は、バックアップ・プロファイル情報を保管するために使用します。

手順

1. 「設定」 > 「パッチ・バックアップ」をクリックして、「パッチ・バックアップ」パネルを開きます。
2. ファイル転送の方式を選択します。
3. ホスト名と、情報の保管先ディレクトリーを入力します。
4. 宛先ホストでファイルの所有者となるユーザー名とパスワードを入力します。
5. 操作が完了したら、「適用」をクリックします。

親トピック: Guardium システムの構成

ソケット接続権限の構成

このトピックは、カスタム・アラート・クラスに適用されます。

カスタム・クラスによって使われるすべてのソケット接続の権限を構成するには、この手順に従ってください。

1. 「設定」 > 「評価」 > 「通信の許可」をクリックして、「通信の許可」を開きます。
2. 「ソケット接続権限の追加」 をクリックして、そのペインを拡張します。
3. ホストの IP アドレスまたはホスト名を入力します。
4. ソケット接続のポート番号を入力します。
5. 説明を入力します。
6. 「保存」をクリックします。

親トピック: Guardium システムの構成

アクセス管理の概要

アクセス管理は、アカウントの管理、保守、モニター、および取り消しの 4 つのタスクで構成されています。

アクセス管理は、システム管理の職務とは別個のものです。

Guardium® アプライアンスには、accessmgr および admin という 2 つの事前定義ユーザーがあります。

- *accessmgr* は、アクセス・マネージャーに割り当てられるユーザー名です。デフォルトでは、アクセス・マネージャー が、ユーザー・アカウントおよびセキュリティー・ロールの管理権限を持つ唯一のユーザーになります。
- *admin* は、(1 次) Guardium 管理者に割り当てられるユーザー名です。デフォルトでは、管理者には、ユーザー・アカウントやセキュリティー・ロールを管理する権限がありません。 admin ユーザーは、より広範な一連の特権を持ちます。

注:

admin および accessmgr ロールを、同一ユーザーに割り当てることはできません。既存の状態やアップグレードの結果として、同一ユーザーがこれら両方のロールを持つ場合があります。ただし、現行の使用では、これらの 2 つのロールを同一ユーザーに割り当てることはできません。

以前は、ユニットをアップグレードすると、accessmgr ロールが admin ユーザーに割り当てられ、accessmgr ユーザーが無効にされていました。このアップグレード状態では、 まず admin としてログインして accessmgr ユーザーを有効にした後、 accessmgr としてログインして (初期パスワード「accessmgr」を使用すると、システムから変更を求めるプロンプトがユーザーに出されます)、admin ユーザーから accessmgr ロールを削除する必要がありました。

アクセス管理の選択

- 「ユーザー・ブラウザー」 - ユーザーの管理
- 「ロール・ブラウザー」 - アクセス権の管理およびロールのレイアウトのカスタマイズ
- 「ロール権限」 - アプリケーションの権限の管理
- 「LDAP ユーザーのインポート」 - LDAP からのユーザーのインポート

データ・セキュリティーの選択

- 関連付けられたデータ・ソース
- 関連付けられていないデータ・ソース
- 関連付けられたサーバー
- 関連付けられていないサーバー
- ユーザー階層
- ユーザー - データベース関連付け

Accessmgr からの事前定義レポート

Accessmgr ユーザーは以下の事前定義レポートを使用できます。

ユーザーとロールのレポート

ユーザーの定義と変更 (『ユーザーの管理』を参照) では、 Guardium システムを使用するユーザーと、そのユーザーに割り当てるロール (『ロールの管理』を参照) の両方を決める必要があります。 ロールとは、そこに属するユーザー全員に同じアクセス権限が割り当てられる、ユーザーのグループです。

ユーザーとロールのレポートには、次のレポートが含まれています。

- ユーザー - ロール -- ユーザーが所属しているロールの数を、ユーザー別に表示するレポート。
- 全ロール - ユーザー -- ロールに属するユーザーの数を、 ロール別に表示するレポート。

注: admin と access manager は既存ですが、その他のロールは access manager によって作成されます。

以下のレポートは、中央マネージャーまたはスタンドアロン・ユニットで使用できます。管理対象マシンで使用しようとすると、エラー・メッセージが表示されます。「関連付けられていないサーバー」では、中央マネージャーのシステム内にあるすべての管理対象ユニットのサーバーが表示されます。

関連付けられたデータ・ソース

このレポートでは、データ・ソース名、ホスト、サービス名、ログイン名、関連付けのタイプが識別されます。 この情報は、「ユーザーとデータベース間の関連」アクティビティーで行った選択から取得されます。ヘルプ・トピック『データ・ユーザー・セキュリティー - 階層および関連付け』を参照してください。

関連付けられていないデータ・ソース

このレポートは、どのユーザーとも関連付けられていないデータ・ソースのリストです。 このレポートでは、データ・ソース名、データ・ソース・タイプ、ホスト、およびサービス名が識別されます。 この情報は、「ユーザーとデータベース間の関連」アクティビティーで行った選択から取得されます。ヘルプ・トピック『データ・ユーザー・セキュリティー - 階層および関連付け』を参照してください。

関連付けられたサーバー

このレポートでは、サーバー IP、サービス名、ログイン名、および関連付けのタイプが識別されます。 この情報は、「ユーザーとデータベース間の関連」アクティビティーで行った選択から取得されます。ヘルプ・トピック『データ・ユーザー・セキュリティー - 階層および関連付け』を参照してください。

関連付けられていないサーバー

このレポートは、どのユーザーとも関連付けられていないサーバーのリストです。 このレポートでは、サーバー IP とサービス名が識別されます。 この情報は、「ユーザーとデータベース間の関連」アクティビティーで行った選択から取得されます。ヘルプ・トピック『データ・ユーザー・セキュリティー - 階層および関連付け』を参照してください。

- ロールについて
  Guardium ユーザーにロールを割り当てて、特定のアクセス権を付与します。ロールの例として、CLI、admin、accessmgr、CAS、および user が挙げられます。
- ロールと権限の管理
  ロールおよびアクセス権により、ユーザーの職務に基づいた各種アクセス・レベルがユーザーに提供されます。
- 最小限のアクセス権しか持たないロールの作成方法
  このトピックでは、最小限のアクセス権しか持たない新規ロール (例えば、監査プロセスの To-do リストへのアクセスおよび特定のレポートの表示のみが可能な監査員ロール) を作成する方法について説明します。
- ユーザーの管理
  ユーザー・アカウントの追加、ユーザー・アカウントの有効化または無効化、LDAP からのメンバーのインポート、またはユーザー権限の編集を行うには、ユーザー名 *accessmgr* が割り当てられたアクセス・マネージャーを使用します。「アクセス」 > 「アクセス管理」 > 「ユーザー・ブラウザー」をクリックして、「ユーザー・ブラウザー」を開き、ユーザー・アカウントを参照します。
- CLI への適切なログイン資格を持つユーザーの作成方法
  このタスクは、CLI を使用して GuardAPI コマンドを実行するための適切なロールとライセンスを持つユーザーを作成するときに使用します。
- LDAP からのユーザーのインポート
  Guardium ユーザー定義を LDAP サーバーからインポートすることができます。これには、該当するユーザーを取得するインポート操作の構成をします。
- 「データ・セキュリティー」- ユーザー階層およびデータベースの関連付け
  データ・セキュリティー機能を使用して、ユーザーの階層を作成し、ユーザーを特定のデータベースおよびサーバーに関連付けることができます。Guardium のデータ・セキュリティー機能は、どのユーザーがどの情報にアクセスしたかを報告し、確実に特定のユーザーのみが自分の担当している情報を表示できるようにします。
- ユーザー階層の定義方法
  アクセス・マネージャー・アカウントから UI を使用すると、容易にユーザー階層を定義できます。
- スマート・カードを使用した Guardium UI へのログイン
  Guardium のスマート・カード・サポートは、すべてのベンダーがユーザー・アクセスで多要素認証をサポートする必要があるという米国政府の義務付けを満たしています。スマート・カード認証がサポートされるのは、Web ベースの Guardium ユーザー・インターフェース (UI) へのアクセスのみです。

ロールについて

Guardium ユーザーにロールを割り当てて、特定のアクセス権を付与します。ロールの例として、CLI、admin、accessmgr、CAS、および user が挙げられます。

アクセス・マネージャーはロールを定義し、それをユーザーおよびアプリケーションに割り当てます。 ロールがアプリケーションまたは項目の定義 (特定の照会など) に割り当てられると、そのロールを割り当てられた Guardium ユーザーのみがそのコンポーネントにアクセスできます。

ユーザー定義が LDAP サーバーからインポートされるときに、その定義が属するグループは、オプションでロールとして定義できます。 詳しくは、LDAP からのユーザーのインポートを参照してください。

注: ユーザーにロールを割り当てるときに、admin ロールとアクセス・マネージャー・ロールを同一ユーザーに割り当てることはできません。
注: カスタム作成のロールを、デフォルトで提供されるロール (例: user、admin、accessmgr、cli、inv、datasec-exempt、review-only) と組み合わせて使用することはできません。
注: admin ロールおよびオブジェクトの所有者は、デフォルトですべてのオブジェクトにアクセスできます。
注: 基本ロールを選択して (ナビゲーション項目を追加して) カスタマイズした後、 そのカスタマイズしたロールをコピーした場合、カスタマイズまたはコピーしたロールをデフォルトにリセットすると、 カスタマイズ内容が失われます。

デフォルトのロール

Guardium システムは、管理者、ユーザー、アクセス・マネージャー、および調査という、大きく 4 つのデフォルトのロールに分類されるユーザーをサポートするために事前構成されています。 Guardium アクセス・マネージャーは新しいロールを作成することもできます。
注: 注: 監視データ・レベルにおいてデータ・レベル・セキュリティーが有効になっている場合 (「グローバル・プロファイル」設定を参照)、監査プロセスのエスカレーションはデータ階層の上位レベルのユーザーに対してのみ許可されます (『アクセス・マネージャー』を参照)。Datasec-exempt ユーザーは誰に対してでも、無制限にエスカレーションできます。

表 1. デフォルトのロール

デフォルトのロール	記述
user	すべての一般ユーザーにデフォルトのレイアウトとアクセス権限を提供します。このロールは削除できません。
admin	Guardium 管理者のデフォルトのレイアウトとアクセス権限を提供します。admin ロールと admin ユーザー を混同しないでください。後者は admin ロールを持つ特別のユーザー・アカウントですが、admin ユーザー・アカウントのみに用意されている追加の権限も持っています。このロールは削除できません。
accessmgr	アクセス・マネージャーのデフォルトのレイアウトおよびアクセス権限を提供します。このロールは削除できません。
cli	CLI へのアクセスを提供します。admin ユーザーは CLI に対してデフォルトのアクセス権限を持っています。その他のユーザーは、アクセス・マネージャーにより作成され、ロールが指定されたときにアクセス権を付与される必要があります。 アクセス・マネージャーはシステム内で同じ数だけのユーザーを定義し、そのユーザーに CLI ロールを付与することができます。 これらのユーザーは CLI に対するアクセス権を持ち、そのユーザーの CLI セッションのすべてのアクティビティーはこのユーザーに関連付けられます。 admin 権限を持っていないユーザーが GrdAPI コマンドまたは CLI コマンドを実行するには、ユーザー・ロール・アクセス権の選択で、「管理コンソール」に対して「CLI」ロールをクリックします。 diag ロールの管理方法については、トピック『diag CLI コマンド』を参照してください。
inv	調査ユーザーのデフォルトのレイアウトとアクセス権限を提供します。 調査ユーザーはそのユーザー定義の姓として、リストア先データベース名である INV_1、INV_2、または INV_3 を持つ必要があります。これは GUI で強制されませんが、調査アプリケーションが正しく機能するために必要です。 名前が割り当てられるときに、ユーザー・ロールも割り当てられる必要があります。 このロールは削除できません。 注:「今すぐ 1 回実行する特別プロセス」ボタンは、調査 (INV) ユーザーを除くすべてのユーザーが、すべてのレポート画面で使用できます。
datasec-exempt	データ・セキュリティー - 免除。このロールは、データ・レベルのセキュリティーが有効にされ (管理コンソールの「グローバル・プロファイル」を参照)、datasec-exempt ロールが割り当てられたときに活動化します。ユーザーがこのロールを持っている場合には、「すべて表示」チェック・ボックスがすべてのレポートに表示されます。チェック・マークを付けると、検出されたすべてのデータ記録が表示されます (フィルター処理は一切行われません)。このロールは ロール・ブラウザーでは削除できません。
review-only	このロールで指定されたユーザーは、各種結果 (監査、評価、分類)、監査結果、および To Do リストのみを表示できます。このロールは ロール・ブラウザーでは削除できません。 このロールを持つユーザーは、監査プロセス・ビューアーでコメントを入力できます (行単位のワークフローやコメント/データではなく、処理/結果レベルのコメント)。 このロールを持つユーザーは、ワークフロー自動化結果 (エスカレート、再割り当てなど) に対して、いかなる変更/アクションを実行することもできません。

サンプル・ロール

デフォルトのロールに加えて、一連のロールのサンプルも定義されています。

表 2. サンプル・ロール

サンプル・ロール	記述
dba	セキュリティーでデータベースを中心とした監視を行うユーザー。データベース関連のレポートにアクセスでき、データベース・オブジェクトのトラッキングを行います。
infosec	機密保護に重点的に関与するユーザー。データベースへのアクセスのトラッキング、ネットワーク要求、監査、およびフォレンジックの処理などを行います。
netadm	ネットワークを中心とした監視を行うユーザー。データベース要求の IP 送信元などを監視します。
appdev	アプリケーション開発者、アーキテクト、および QA 担当者。アプリケーションを中心とした監視を行い、アプリケーションにより生成された SQL ストリームのトラッキングとそれに関するレポートを行います。

サンプル・ロール	記述
audit	監査レポートを表示する必要がある監査員およびその他のユーザー。 注: このロールをコピーしようとすると、このロールのすべての側面をコピーできるわけではないことを示す組み込みメッセージが表示されます。メッセージは以下のとおりです。「"audit" ロールのレイアウトおよびアクセス権を使用して新しいロールを作成します。"audit" ロールに関連付けられた特権および特別なアクションはコピーされません。」
audit-delete	監査プロセスの結果が削除されている場合、このロールを使用して、トラッキングまたはロギングが実行されます。audit-delete ロールを所有するユーザーは、レポートを削除できます。管理ユーザーも、レポートを削除することができます。トラッキングは、ユーザー・アクティビティー監査証跡レポートを使用して実行されます。
admin-console-only	このロールで指定されたユーザーは、管理コンソール・タブにのみアクセスできます。
cas	構成監査システム (CAS)
vulnerability-assess	このロールで指定されたユーザーは、脆弱性結果のみを表示できます。
diag	このロールで指定されたユーザーは、CLI で diag コマンドにアクセスして実行することができます。
workload-replay-admin	このロールで指定されたユーザーは、ワークロード・リプレイ機能を定義および変更することができます。
workload-replay-user	このロールで指定されたユーザーは、ワークロード・リプレイ機能を実行できます。
fam	このロールで指定されたユーザーは、ファイル・アクティビティー・モニター機能を定義および変更することができます。
BaselII	アクセラレーター - Basel II。このロールは削除できません。 バーゼル II の第 2 部のセクション 4 とセクション 5 の要件では、金融機関が財務情報をもとに証券化の枠組みを定義し、それに伴う運営上のリスクを推定しなければならないことが定められています。
DataPrivacy	アクセラレーター - データ・プライバシー。このロールは削除できません。 データ・プライバシー・アクセラレーターは、特に ID の盗用に対して保護を施し、業界のベスト・プラクティスに基づく、事前に定義したポリシー、リアルタイム・アラート、および監査レポートのポートフォリオを提供しています。データ・プライバシー・アクセラレーターを使用すると、セキュリティー管理者、プライバシー保護担当者、およびデータベース管理者は、データ要素 (「プライバシー・セット」という) の組み合わせを定義することから作業を開始できます。これらに対するアクセスは、内部ユーザーによるハッキングまたは不適切なアクティビティーを示している可能性があります。
GDPR	アクセラレーター - GDPR。このロールは削除できません。 Guardium GDPR アクセラレーターは、GDPR のグループおよびポリシーに基づく事前定義レポートを提供します。GDPR アクセラレーターの処理を開始するには、GDPR ロールを Guardium ユーザーに割り当て、そのユーザーのアカウントを使用して「アクセラレーター」 > 「GDPR」にナビゲートします。
pci	アクセラレーター - PCI。このロールは削除できません。 PCI DSS は、カード所有者データを保護するために設計された一連の技術要件と運用要件であり、カード所有者データの保管、処理、使用、または送信を行うすべての組織に適用されます。この要件に準拠できない場合、特権の喪失や厳しい罰金のほか、データ・ブリーチの発生時にはブランドやサービスに関する消費者の信頼感の著しい低下が伴う可能性があります。IBM Guardium アクセラレーターは、事前定義ポリシー、レポート、グループ定義などを使用して、この規格の各部分に準拠するプロセスを実施する上で役立ちます。
sox	アクセラレーター - SOX。このロールは削除できません。 SOX 法の第 404 条では、財務報告について会社ごとに適切な内部統制機構と手続きを確立し、維持していくことが求められています。

中央マネージャー環境のロール

中央マネージャー環境では、すべてのユーザー・アカウント、ロール、およびアクセス権が中央マネージャーによって制御されます。 これらの定義のいずれかを管理するには、中央マネージャーにログインしている必要があります (管理対象ユニットにではなく)。

ロールの作成

1. accessmgr としてログインし、「アクセス」 > 「アクセス管理」 > 「ロール・ブラウザー」をクリックして、「ユーザー・ロール・ブラウザー」を開きます。
2. 「ロールの追加」をクリックして、「ロール・フォーム」パネルを開きます。
3. 「ロール名」に固有の名前を入力して、「ロールの追加」をクリックします。

ロールの削除

1. 「アクセス」 > 「アクセス管理」 > 「ロール・ブラウザー」をクリックして、「ユーザー・ロール・ブラウザー」を開きます。
2. いずれかのロールの「削除」をクリックします (一部のロールは削除できません。そのようなロールには、「削除」オプションはありません)。 すると、そのロールの「ロール・フォーム」が開きます。
3. 「削除の確認」をクリックします。そのロールへのすべての参照が削除されることを通知するメッセージが表示され、操作を確認するよう求められます。
4. 削除を確認するには「OK」を、操作を中止するには「キャンセル」をクリックします。

親トピック: アクセス管理の概要

ロールと権限の管理

ロールおよびアクセス権により、ユーザーの職務に基づいた各種アクセス・レベルがユーザーに提供されます。

ロールには user、admin、audit などがあります。ロールを使用すると、ユーザー・グループ全体に対するアクセス権を容易に定義できます。新規ロールを作成したりそのロールにユーザーを割り当てたりすることができるのは、アクセス・マネージャーのみです。アクセス・マネージャーは、ロール作成の一環として、そのロールのナビ

ゲーション・メニューおよびアクセス権をカスタマイズすることもできます。

カスタマイズしたロールを作成するには、以下のような、いくつかの処理が必要です。

- 新規ロールを作成する
- ロールのアクセス権を管理し、ユーザーがアクセスできる対象を制限する
- オプションで、ロールのナビゲーション・メニューをカスタマイズし、ユーザーが表示可能な内容をさらに制限する
- ユーザーをロールに追加する

特定のアプリケーションへのアクセスを制限するには、以下の 2 つの方法があります。

アプリケーションからのアクセスの制限

アプリケーションからのアクセスを制限するには、「ロール権限」 > 「アプリケーション・ロール権限の編集」画面で「すべてのロール」チェック・ボックスを選択解除します。次に、アプリケーションにアクセスする必要がある個々のロールを選択します。

この処理は、「すべてのロール」チェック・ボックスが既に選択解除されている場合も同じです。 単に、アプリケーションへのアクセス権を付与するか取り消すロールを個別に選択または選択解除します。

特定のアプリケーションに対して「すべてのロール」が選択されている場合は、現在定義されているすべてのロールがそのアプリケーションにアクセスできます。

ロールからのアクセスの制限

ロールからのアクセスを制限するには、 「ロール・ブラウザー」 > 「権限の管理」画面にナビゲートし、 アプリケーションを個別に「アクセス可能なアプリケーション (Accessible applications)」リストから「アクセス不能なアプリケーション (Inaccessible applications)」リストに移動します。

アクセス権を管理したり新規ロールのナビゲーション・メニューをカスタマイズしたりすると、 「アクセス可能なアプリケーション (Accessible applications)」リストに表示されるデフォルトに、 「ロール権限」 > 「アプリケーション・ロール権限の編集」画面で 「すべてのロール」チェック・ボックスを選択したアプリケーションが反映されます。

ロールおよびアクセス権を操作するときにアプリケーションのアクセス権を削除すると、新規ロールのデフォルト・アクセス権も変化します。つまり、アプリケーションのアクセス権を削除すると、その後に作成するすべてのロールでもそのアプリケーションに対するアクセス権が欠落します。デフォルトで「アクセス可能なアプリケーション (Accessible applications)」リストに表示されなくなったアプリケーションのアクセス権を新規ロールに付与する場合は、その新規ロールに対して必要なアプリケーションを「アクセス不能なアプリケーション (Inaccessible applications)」リストから「アクセス可能なアプリケーション (Accessible applications)」リストに移動する必要があります。

「ロール・ブラウザー」 > 「ナビゲーション・メニューのカスタマイズ (Customize Navigation Menu)」ツールを使用してメニュー項目を非表示にすることで、アクセス権を特定のツールに制限することもできます。この方法では、デフォルトのアプリケーション・アクセス権を変更せずにアクセスが制限されますが、アクセス権ベースの方法より安全性が低くなる場合があります。

ベスト・プラクティス:

- ロールのアクセス権を編集した後、 「ロール・ブラウザー」 > 「ナビゲーション・メニューのカスタマイズ (Customize Navigation Menu)」画面に表示される、そのロールのナビゲーション・レイアウトを確認します。必要に応じて「ナビゲーション・メニュー (Navigation Menu)」リストの項目を追加または削除して、ロールに適したレイアウトを作成します。
- 事前定義のロールをコピーしてから編集し、必要なアクセス権およびナビゲーション・メニューを設定します。この方法を行えば、 必要に応じて元のロールに戻すことができます。

親トピック: アクセス管理の概要
関連タスク:
最小限のアクセス権しか持たないロールの作成方法
関連情報:
ユーザー・インターフェースのカスタマイズ (Customizing the user interface)
ユーザー、ロール、および Guardium システムの管理 (ビデオ)

最小限のアクセス権しか持たないロールの作成方法

このトピックでは、最小限のアクセス権しか持たない新規ロール (例えば、監査プロセスの To-do リストへのアクセスおよび特定のレポートの表示のみが可能な監査員ロール) を作成する方法について説明します。

手順

1. 新規ロールを作成します。
   a. *accessmgr* としてログインし、 「アクセス」 > 「アクセス管理」にナビゲートして、「ロール・ブラウザー」を選択します。
   b. 「ロールの追加」ボタンをクリックし、ロールに名前を指定して 「ロールの追加」ボタンをクリックし、新規ロールを作成します。
2. 新規ロールが「監査プロセスの To-do リスト」および「レポート・ビルダー」 (レポートを表示するために必要です) のみにアクセスできるように、アクセス権を管理します。
   a. 「ロール・ブラウザー」で、新規ロールの「権限の管理」リンクをクリックします。
   b. 「アクセス可能な項目」リストのヘッダーにあるチェック・ボックスを選択し、 矢印を使用してすべての項目を「アクセス不能な項目」リストに移動します。 制限の厳しいロールを作成するときは、まずアクセス権を削除するほうが簡単です。
   c. 「アクセス不能な項目」リストで 「監査プロセスの To-do リスト」および「レポート・ビルダー」を選択し、矢印を使用して「アクセス可能な項目」リストに戻します。 これで、新規ロールがこれら 2 つのアプリケーションのみにアクセスできるようになりました。
   d. 「OK」ボタンをクリックして、変更内容を確定します。
3. メニューおよびナビゲーションをカスタマイズするために、新規ロールで使用できるレポートおよびアプリケーションを定義します。
   a. 「ロール・ブラウザー」で、新規ロールの「ナビゲーション・メニューのカスタマイズ (Customize Navigation Menu)」リンクをクリックします。
   b. 「ナビゲーション・メニュー (Navigation Menu)」リストで、 「レポート」グループを選択します (強調表示されます)。 選択したグループが、以降のステップで追加するメニュー項目の宛先となります。
   c. 「使用可能なツールとレポート (Available Tools and Reports)」リストで、 「レポート」セクションを展開するか「フィルター」を使用して特定のレポートを探し、 新規ロールで使用可能にする必要がある項目それぞれの横にあるチェック・ボックスを選択した後、 矢印を使用して、その項目を「ナビゲーショ

ン・メニュー (Navigation Menu)」リストに追加します。「ナビゲーション・メニュー (Navigation Menu)」リストに移動した項目が、このロールに割り当てられたユーザーに表示されるようになります。
   d. 「ナビゲーション・メニュー (Navigation Menu)」リストで、「レポート」 > 「レポート構成ツール」および「調査」グループの横にある アイコンをクリックして、「レポート・ビルダー」へのアクセス権を削除します。これにより、このロールのメニュー構造が簡素化され、「レポート・ビルダー」ツールへのアクセス権が削除されますが、レポートにアクセスする必要があるアプリケーション・アクセス権は削除されません。
   e. 「OK」ボタンをクリックして、変更内容を確定します。これで、ユーザーへの割り当てが可能なごく最小限の特権を持つ新規ロールが作成されました。
4. オプションで、新規ロールのカスタム・ホーム・ページを指定します。
   a. 「ロール・ブラウザー」で、新規ロールの「ナビゲーション・メニューのカスタマイズ (Customize Navigation Menu)」リンクをクリックします。
   b. 「ナビゲーション・メニュー (Navigation Menu)」リストで、「順守」 > 「ツールとビュー」 > 「監査プロセスの To-do リスト」を選択してから、ツールバーの アイコンをクリックし、新しいデフォルト・ホーム・ページを指定します。このロールに割り当てられたユーザーがログインすると、デフォルト画面として「監査プロセスの To-do リスト」が表示されるようになります。
   c. 「OK」ボタンをクリックして、変更内容を確定します。
5. 新規ユーザーを作成し、そのユーザーをこの新規ロールに追加します。
   a. 「アクセス」 > 「アクセス管理」にナビゲートして「ユーザー・ブラウザー」を選択します。
   b. 「ユーザーの追加」をクリックし、必要な情報を指定して、「ユーザーの追加」をクリックし、新規ユーザーを作成します。作成したユーザーが「ユーザー・ブラウザー」にリストされます。

      新規ユーザーを作成したとき、アカウントはデフォルトで無効になっています。ユーザーがアカウントに即時アクセスできるようにする場合は、「無効」チェック・ボックスを選択解除します。

   c. 「ユーザー・ブラウザー」で新規ユーザーの「ロール」リンクをクリックすると、使用可能なロールのリストが表示されます。
   d. 以前に作成したカスタム・ロールの横にある「割り当て」チェック・ボックスを選択します。これにより、新規ロールにユーザーが割り当てられます。
   e. *user* ロールの横にある「割り当て」チェック・ボックスを選択解除します。*user* ロールを選択解除すると、新規ユーザーがデフォルトの *user* アクセス権および許可を継承できなくなります。
   f. 「保存」をクリックして、変更内容を確定します。

親トピック: アクセス管理の概要
関連概念:
ロールと権限の管理

ユーザーの管理

ユーザー・アカウントの追加、ユーザー・アカウントの有効化または無効化、LDAP からのメンバーのインポート、またはユーザー権限の編集を行うには、ユーザー名 *accessmgr* が割り当てられたアクセス・マネージャーを使用します。「アクセス」 > 「アクセス管理」 > 「ユーザー・ブラウザー」をクリックして、「ユーザー・ブラウザー」を開き、ユーザー・アカウントを参照します。

ユーザーの定義と変更には、Guardium® システムを誰が使用するのか、およびその人たちにどのロールを割り当てるかの両方を決定する作業が含まれます。ユーザーのグループは、すべて同じロールと同じアクセス権を持つことができます (そのように選択する場合)。ロールについて詳しくは、ロールについてを参照してください。

注: ロールにデフォルトのレイアウトを定義して、そのロールを割り当てられたすべての新規ユーザーがそのレイアウトを持つようにすることができます。「CLI リファレンス」の『新規レイアウトの生成』を参照してください。

ユーザー定義は LDAP サーバーからオンデマンドで、またはスケジュールに従ってインポートできます。

ユーザーがどのように Guardium システムに定義されているかに関係なく、Guardium 管理者は Guardium、LDAP、または Radius を介してユーザーを認証するようにシステムを構成できます。

Guardium システムを開始する際の初期の重要なタスクは、そのシステムを使用するのはどのユーザー・グループで、そのグループの機能は何かを確認することです。例えば、情報セキュリティー・グループはアラートおよびトラブルシューティングのために Guardium を使用し、データベース管理者グループはレポートとモニターのために Guardium を使用します。Guardium システムにアクセスするユーザーを決定するときには、会社の機密データがこのシステムによって取り出される可能性があることを念頭においてください。したがって、そのデータに誰がアクセスできるかには十分に注意を払ってください。

どのユーザー・グループが Guardium システムを使用するか (そして何の目的で使用するか) を決定したら、それぞれのユーザーについて次の情報を収集します。

- ユーザーの氏名
- ユーザーのアカウント名 (ログインに使用する名前)
- ユーザーの E メール・アドレス
- Guardium におけるユーザーの機能/ロール

ユーザー・アカウントのセキュリティー

ユーザー・アカウントに対して追加のセキュリティーを提供するために、いくつかの設定を変更できます。これらの設定は CLI コマンドの show および store password を使用して有効または無効にできます (「CLI リファレンス」の『ユーザー・アカウント、パスワード、および認証 CLI コマンド』を参照)。

- デフォルトで、パスワードの検証は有効になっています。これは、パスワードには最低 8 文字が必要で、次のそれぞれの種類の文字が少なくとも 1 文字含まれていなければならないことを意味します。
  - A から Z の英大文字
  - a から z の英小文字
  - 0 から 9 の数字
  - 特殊文字: @#$%^&.;!-+=_

  注: パスワード検証が無効になっている場合はすべての文字を使用できます。
- デフォルトでは、パスワードの有効期限は有効になっています。指定した日数が経過したら有効期限が切れるようにパスワードを構成できます。
- デフォルトでは、ログイン試行の失敗が指定された回数に達したときのアカウントのロックアウトは有効になっています。一定時間内の試行回数が一定数に達した後、またはアカウントが存続する期間中の試行回数の累計が一定数に達した後でロックアウトが発生するように構成できます。

ロックされたアカウント

1. 「アクセス」 > 「アクセス管理」をクリックして、「ユーザー・ブラウザー」を開き、ユーザーのリストを表示します。
2. 任意のユーザーの「編集」をクリックして、「無効」チェック・ボックスをクリアし、「ユーザーの更新」をクリックして、変更内容を保存します。
   注: admin ユーザー・アカウントがロックされた場合は、unlock admin CLI コマンドを使用してこれをアンロックします (「CLI リファレンス」の『構成および制御 CLI コマンド』を参照してください)。

ユーザー・アカウントの作成

1. 「ユーザー・ブラウザー」を開き、「ユーザーの追加」をクリックして、「ユーザー・フォーム」パネルを開きます。
2. 「ユーザー名」に固有の名前を入力します。名前にはアポストロフィ文字を含めないでください。ユーザー名には大/小文字の区別がありません。
   注: 「ユーザーの追加」パネルまたは「ユーザー LDAP インポート」のいずれかから手動でユーザーを追加するときに、ファーストネームとラストネームのどちらかまたは両方がない場合は、ログイン名が使用されます。
3. パスワードを入力して、「パスワード (確認)」ボックスにもう一度入力して確認します。割り当てたパスワードは一時的なもので、ユーザーは最初のログインの後、これを変更するよう要求されます。
   注: パスワードは大/小文字の区別があります。 パスワード検証が有効 (デフォルト) になっている場合、パスワードは 8 文字以上の長さでなければならず、さらに、英大文字 (A-Z)、英小文字 (a-z)、数字 (0-9)、および特殊文字 (@$%^&.;!-+=_) を、それぞれ 1 つ以上含んでいる必要があります。
   注: ユーザー名での非ラテン文字 (中国語や日本語など) の使用はサポートされていません。
4. ユーザーのファーストネームとラストネームをそれぞれのフィールドに入力します。
   注: 調査データ・リストアのロール (inv) を割り当てられているユーザーのラストネームには、制限が適用されます。ユーザーにこの調査ロールを割り当てる場合、そのユーザーのラストネームは INV_1、INV_2、INV_3 でなければなりません。UI では、このフィールドに別の名前を入力することを制限しませんが、前述のラストネームが入力されなければ、アプリケーションは適切に機能しなくなります。また、調査ユーザーにその他のロールを割り当てることはできません。inv のみでなければなりません。これは、user ロールまたは admin ロールが必要とされない唯一の場合です。
5. (オプション) ユーザーの E メール・アドレスを入力します。
6. (注意) 「無効」チェック・ボックスには、デフォルトでチェック・マークが付けられています。チェック・ボックスをクリアし、アカウントを有効にするのは、一連の正しいロールがユーザーに対して割り当てられた後まで待つようお勧めします。

   ユーザーが初回にログインしたときにそのレイアウトにすべてのコンポーネントが含まれるよう、最初にロールを割り当てておく方がずっと簡単です。 ユーザーが初回にログインするときに、そのレイアウトはその時点で割り当てられているすべてのロールを使用して作成されます。後でロールが追加された場合、ユーザーはそのロールで使用可能なすべての対象にアクセスできますが、そのロールに固有のレポートまたはアプリケーションを手動で追加しなければなりません。
7. 「ユーザーの追加」をクリックして新しいユーザー・アカウント定義を保存し、パネルを閉じます。

これでユーザーの定義は完了です。初回ログインのパスワードをユーザーに通知する前に、ユーザーのために適切なロールを追加することをお勧めします。詳細については、ロールについてを参照してください。

複数のユーザーの有効化/無効化

「ユーザー・ブラウザー」を開いて「ユーザーの検索」をクリックすると、ユーザーをロール別に簡単にフィルタリングできます。ユーザーの選択時には、ユーザーを有効または無効にするオプションがあります。ユーザーはデフォルトで無効になっているため、このメニューは、複数のユーザーの状況を容易に変更するのに非常に便利です。

ユーザー・アカウントの更新

1. 「ユーザー・ブラウザー」を開き、変更を加えるユーザーの「編集」をクリックします。
2. 「ユーザー・フォーム」パネルの任意の値を置き換えます。
3. 「ユーザーの更新」をクリックして、変更内容を保存します。

注: ユーザーのパスワードを変更するには、そのユーザーが次回にログインした後に自身でパスワードを変更する必要があります。

無効なユーザー・アカウントを有効にする

1. 「ユーザー・ブラウザー」を開き、有効にするユーザーの「編集」をクリックします。
2. 「無効」チェック・ボックスをクリアします。
3. ユーザーがパスワードを忘れてしまった場合は、新規パスワードを「パスワード」と「パスワード (確認)」の両方のボックスに入力します。
4. 「ユーザーの更新」をクリックします。

ユーザー・アカウントの削除

1. 「アクセス」 > 「アクセス管理」をクリックして、「ユーザー・ブラウザー」を開きます。
2. 削除するユーザーの「削除」をクリックします。
3. 「削除の確認」をクリックします。

注: 削除されたユーザーに送信されていたアラートは、今度は管理者に送信されるようになります。ただし、これはアクセス・ポリシーが再インストールされるまで有効になりません。

データ・セキュリティー・ユーザー階層を定義する

1. 「データ・セキュリティー」 > 「ユーザー階層」をクリックします。
2. 「ユーザー」メニューからユーザーを選択して画面を最新表示し、選択したユーザーの現在の階層をユーザー・ペインに表示します。
3. ユーザー・ノードを右クリックして、以下のオプションを表示します。
   - ユーザーの追加 - 「ユーザーの追加」をクリックすると、「ユーザーの追加」ダイアログが表示されます。検索するか、ロール別にフィルタリングして、選択したユーザーの子孫としてユーザーを追加します。

     こうして、ある階層の親には特定のサーバーおよびデータベースの表示を許可し、その階層の子には許可しないことで、データ・レベルのセキュリティー軽量のための手段を作成できます。 構成によっては、子のデータ・レベル・セキュリティーを親が継承するという継承を行うこともできます。

     注: ユーザーが複数の親を持つことができ、かつ、親が複数のユーザーを持つことができる、「多対多」の関係が許可されます。

- 親からユーザーをリンク解除 - 子孫を親から切り離します。
- すべての子孫を削除 - すべての子孫を親から切り離します。

4. 「キャッシュ階層のリフレッシュ」をクリックして、最近の変更内容をユーザー階層マップに適用します。
5. 「アクティブなユーザー - DB マップの全更新」をクリックして、最近の変更内容を、アクティブなユーザー - DB 関連付けマップにすべて適用します。
   注: ベスト・プラクティスではユーザー階層の変更後に「アクティブな「ユーザー - DB」マップの全更新」を行います。

   階層またはデータベースへの関連付けに (UI または GuardAPI を介して) 変更を加えたとき、その変更内容は自動的には有効になりません。「定期更新」が実行されたのが「初めて」でない限り、「定期更新」はこの変更内容をピックアップしません。 それ以外の場合、変更内容を有効にするには、ユーザーは「全更新」をクリックするか、Full Update GuardAPI コマンドを実行する必要があります。

   ユーザー階層の定期更新は、10 分ごとに自動的に実行されます。 手動では実行できません。これはインクリメンタル更新です。つまり、最後に定期更新が実行されたとき以降に検出された新しいサーバー IP またはサービス名のみを検査しているということです。 既存の階層および関連付けを新しい IP/サービス名と比較し、どのユーザーがこれらの IP/サービス名へのアクセス権限を持つ必要があるかを特定します。

   ユーザー階層の全更新は自動的には実行されません。 UI または GuardAPI 関数を介して行われる場合にのみ、実行されます。これは、すべての IP/サービス名を既存の階層および関連付けと比較し、誰が何に対するアクセス権限を持つかを特定します。

データ・セキュリティー・ユーザーとデータベースの関連付けを定義する

「ユーザーとデータベースの関連付けによるデータ・セキュリティー」を使用して、ユーザーの検索、使用可能なサーバーおよびサービス名 (データベース) へのユーザーの割り当て、およびそれらからのユーザーの削除を行います。

1. 「データ・セキュリティー」 > 「ユーザー - データベース関連付け」をクリックして、「ユーザー - データベース関連付け」パネルを開きます。
2. 「サーバーおよびサービス名の推奨」のチェック・ボックスを選択して、ユーザーに関連付けるデータベースとサービス名を見つけます。次のような選択肢があります。
   - 監視対象アクセス - Guardium 内部データベース表「GDM_Access」からの監視対象トラフィック。
   - データ・ソース定義 - データ・ソースの名前、データベース・タイプ、認証情報、およびロケーションなどの既存のデータ・ソース定義情報。
   - S-TAP® 定義 - データベース・サーバーの IP アドレスや、S-TAP からデータを受け取る Guardium ホストの IP アドレスなどの既存の S-TAP 定義情報。
   - 自動検出されたホスト - Guardium オートディスカバリー・プロセスによって検出され、以前は認識されていなかったホスト。Guardium のオートディスカバリー・アプリケーションは、ネットワークをプローブして、データベースを検索し、 ディスカバーしたすべてのデータベースについてレポートを作成するように構成できます。
   - Guardium Install Manager (GIM) が検出したシステム - GIM によって検出され、以前は認識されていなかったホスト。
3. 「移動」をクリックし、使用可能なサーバー、サービス名、および現在関連付けられているユーザーを見つけて表示します。
   注: ノード・ツリーをトラバースする際に、各サーバーおよびサービス名の横に数値標識が表示され、直接関連付けられたユーザーおよび関連付けられた子孫ユーザーの数が示されます。この標識は直接関連付けの場合は [nn] の形式をとり、子孫の関連付け (例えば、現在のサーバー内のサーバーまたはサービス名にユーザーが関連付けられている) の場合は (mm) の形式をとります。同様に、サーバーまたはサービス名に関連付けられているユーザーを表示するとき、ツリーのより上位レベルのノードに関連付けられているユーザーがいる場合は、そのユーザーが表示されます。
4. サーバーまたはサービス名のノードをクリックして、関連付けられているユーザーを表示します。 任意のノードを選択して、以下のいずれかを実行できます。
   - ユーザーとデータベースの関連付けを新規に追加するには、「ユーザーの追加」をクリックし、追加する任意のユーザー (複数可) をクリックしてから、「追加」をクリックします。
   - グループとデータベースの関連付けを新規に追加するには、「グループの追加」をクリックします。「グループの追加」を選択すると、「グループ・ビルダー」を使用してグループ・タイプ「Guardium ユーザー」として作成されたグループが表示されます。追加するグループを選択して、「追加」をクリックします。
   - サーバーまたはサービス名のノードを右クリックして、以下のいずれかを実行します。
5. サーバーまたはサービス名のノードを右クリックすると、以下のいずれかを実行するためのオプションが表示されます。
   - サーバーを強調表示する。
   - サーバーを展開または縮小する。
   - サーバーを検索する。
   - サーバー、サービス名、または無名サービスを追加する。
   - サーバーを削除する。
6. ツリー構造の前にある「IP」フィールドと「サービス名」フィールドを使用して、IP または IP/サービス名のペアを追加します。
   注: 「検索」ボタンを使用して、IP/サービス名ツリー構造を検索することができます。IP 文字列は部分的に入力したり、ワイルドカード * を含めることができます。例えば、「192.168」と「192.168.**」はどちらも有効です。ただし、ワイルドカードの後ろに数値を入れることはできず、数値とワイルドカードでオクテットを形成することはできません。サービス名には任意の場所にワイルドカード「%」を含めることができます。
7. 「アクティブなユーザー - DB マップの全更新」をクリックして、最近の変更内容を、アクティブなユーザー - DB 関連付けマップにすべて適用します。
   注: 「ユーザー - データベース関連付け」を変更してから、「アクティブなユーザー - DB マップの全更新」を行うのがベスト・プラクティスです。

   ユーザー階層の全更新は自動的には実行されません。 「アクティブなユーザー - DB マップの全更新」ボタンまたは GuardAPI 関数を介して行われる場合にのみ、実行されます。これは、すべての IP/サービス名を既存の階層および関連付けと比較し、誰が何に対するアクセス権限を持つかを特定します。

   ユーザー階層の定期更新は、10 分ごとに自動的に実行されます (手動では実行できません)。この更新は、最後に定期更新が実行されたとき以降に検出された新しいサーバー IP またはサービス名のみを検査します。既存の階層および関連付けを新しい IP/サービス名と比較し、どのユーザーがこれらの IP/サービス名へのアクセス権限を持つ必要があるかを特定します。

   データベースの関連付けに (UI または GuardAPI を介して) 変更を加えたとき、その変更内容は自動的には有効になりません。「定期更新」が実行されたのが「初めて」でない限り、「定期更新」はこの変更内容をピックアップしません。それ以外の場合、変更内容を有効にするには、「アクティブなユーザー - DB マップの全更新」ボタンをクリックするか、full update GuardAPI コマンドを実行する必要があります。

親トピック: アクセス管理の概要

CLI への適切なログイン資格を持つユーザーの作成方法

このタスクは、CLI を使用して GuardAPI コマンドを実行するための適切なロールとライセンスを持つユーザーを作成するときに使用します。

このタスクについて

次の理由から、この how-to トピックは重要です。 (1) GuardAPI コマンドは CLI からしか実行できません。 (2) ほとんどの GuardAPI コマンドは特定のアプリケーションとそのロールに関連付けられているため、適切なロールを持たない 標準の CLI ユーザー (ハードコーディングされた「admin」ロールを持つユーザー) では実行できない GuardAPI コマンドが多数あります。

手順

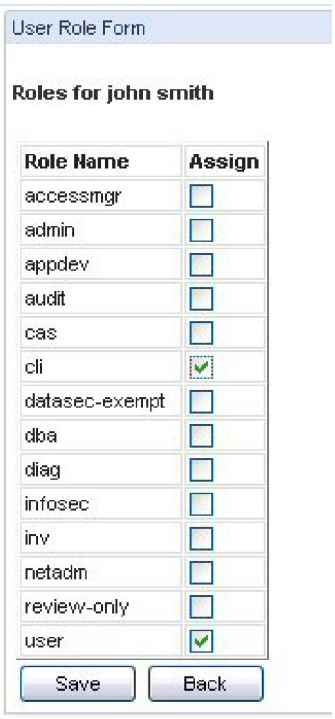
1. accessmgr としてログインし、「アクセス」 > 「アクセス管理」 > 「ユーザー・ブラウザー」をクリックして、「ユーザー・ブラウザー」を開きます。
2. 「ユーザー・ブラウザー」パネルで、「ユーザーの追加」をクリックします。

3. 「ユーザー・フォーム」に入力し、「無効」チェック・ボックスをクリアして作成時にユーザーを有効にするようにしてから、「ユーザーの追加」をクリックします。

ユーザーを作成した初期状態では、CLI にログインする特権がなく、GuardAPI コマンドはいずれも実行できません。例えば、新しく作成したユーザーの CLI アカウント (guardcli1 から guardcli5) を使用すると、 すぐに切断されて、必要なロールが定義されていないことが示されます。

```
$ ssh -l guardcli1 192.168.1.89  guardcli1@192.168.1.89's password:
Last login: Tue Aug 10 18:37:25 2010 from 192.168.1.14
Welcome guardcli1 - your last login was Tue Aug 10 18:37:26 2010
Please enter your GUI login (one with ADMIN or CLI role defined):johnsmith
No such user or user does not have the necessary role defined.
Connection to 192.168.1.89 closed.
```

4. 「ユーザー・ブラウザー」パネルで、任意のユーザーの「ロール」をクリックして、「ユーザー・ロール・フォーム」パネルを表示します。
5. 「CLI」チェック・ボックスにチェックマークを付けて、「保存」をクリックすると、ユーザーに CLI アクセス権が付与されます。



これで、新しく作成したユーザーの CLI アカウント (guardcli1 から guardcli5) の使用を試みると、パスワードが要求されて、CLI へのアクセスが許可されます。

```
$ ssh -l guardcli1 192.168.1.89
guardcli1@192.168.1.89's password:
Last login: Tue Aug 10 18:39:01 2012 from 192.168.1.14
Welcome guardcli1 - your last login was Tue Aug 10 18:39:02 2011
The 'set guiuser' command must be run (successfully) before any other commands will work
set guiuser admin
Enter current password
192.168.1.89>
```

6. 必要に応じて追加のロールを付与し、GuardAPI 関数を実行するためのアクセス権限をユーザーに許可します。

   例えば、ユーザー johnsmith で次の GuardAPI コマンドを実行すると、実行できる API コマンドがないことが分かります。

   ```
   192.168.1.89 >grdapi commands user
   ID=0
   Matching API Function list:
   ok
   ```

   しかし、johnsmith に accessmgr ロールを付与 (上記のステップ 5) した場合は、同じ GuardAPI コマンドを使用すると、次の API コマンドが使用可能であることが分かります。

   ```
   192.168.1.89> grdapi commands user
   ID=0  Matching API Function list :
   create_db_user_mapping
   create_user_hierarchy
   delete_allowed_db_by_user
   delete_db_user_mapping
   delete_user_hierarchy_by_entry_id
   delete_user_hierarchy_by_user
   execute_ldap_user_import
   list_allowed_db_by_user
   list_db_user_mapping
   list_user_hierarchy_by parent_user
   update_user_db
   ok
   ```

親トピック: アクセス管理の概要

LDAP からのユーザーのインポート

Guardium® ユーザー定義を LDAP サーバーからインポートすることができます。これには、該当するユーザーを取得するインポート操作の構成をします。

インポート操作は、オンデマンドで実行するか、または定期的に実行するようにスケジュールすることが可能です。 新規ユーザーのみをインポートするか、または既存のユーザー定義を置換するかを選択することができます。どちらの場合も、LDAP グループは Guardium のロールとしてインポートできます。

LDAP ユーザーをインポートする場合:

- Guardium の admin ユーザー定義は、いかなる形でも変更されません。
- 既存のユーザーは削除されません (つまり、ユーザー・セット全体が LDAP からインポートされるセットで置き換えられるわけではありません)。
- Guardium パスワードは変更されません。
- Guardium に追加される新規ユーザー:
  - デフォルトで非アクティブのマークが付けられる

- ブランク・パスワードを持つ
- ユーザー・ロールを割り当てられる

注:

ユーザー名の特殊文字はサポートされません。

アクセス管理を介して (「ユーザーの追加」または「LDAP ユーザーのインポート」から) 手動でユーザーを追加するときに、姓名のどちらかまたは両方がない場合は、ログイン名が使用されます。

この LDAP 構成メニュー画面では、いくつかのメニュー項目でヒントが表示されます。カーソルをメニュー項目 (「ユーザーのオブジェクト・クラス」など) に移動すると、 短い説明が表示されます。

CLI ユーザーの特権は分離されないため、Guardium CLI ユーザーは LDAP 環境で認証できません。

LDAP ユーザー・インポートの構成

ユーザーの識別に使用する属性は、Guardium 管理者により、「LDAP 認証の構成」パネルの「ユーザー RDN タイプ」ボックスで定義されています。詳しくは、『LDAP 認証の構成』を参照してください。 デフォルトは uid ですが、Guardium 管理者と相談して使用する値を決めてください。RDN 値として SamAccountName を使用する場合、フルネームで a=search または =[domain name] のいずれかを使用する必要があります。例: SamAccountName=search、SamAccountName=dom

注: LDAP ユーザー・インポートを構成する accessmgr ユーザーには、グループ・ビルダーの実行特権が必要です。 特定の状態において、ロール特権に変更が加えられた場合、accessmgr のグループ・ビルダーに対する特権が取り消される可能性があります。 その結果、LDAP ユーザー・インポートを正常に保存することも実行することもできなくなります。 アクセス管理ポータルに移動して、選択項目から「ロール権限」を選択してください。グループ・ビルダー・アプリケーションを選択し、「すべてのロール」ボックスまたは「accessmgr」ボックスにチェック・マークが付けられていることを確認します。

1. 「アクセス」 > 「アクセス管理」 > 「LDAP ユーザーのインポート」をクリックして、「LDAP ユーザーのインポート」パネルを開きます。

   必須情報の入力については、このヘルプ・トピックの最後にある『Tivoli® LDAP 構成の例』を参照してください。

2. 「LDAP ホスト名」に、アクセス先の LDAP サーバーの IP アドレスまたはホスト名を入力します。
3. 「ポート」に、LDAP サーバーへの接続に使用するポート番号を入力します。
4. 「サーバー・タイプ」メニューから、LDAP サーバー・タイプを選択します。
5. Guardium から LDAP サーバーに SSL (Secure Sockets Layer) 接続を使用して接続する場合は、「SSL 接続を使用」チェック・ボックスにチェック・マークを付けます。
6. 「基本 DN」に、検索を開始する、ツリー内のノードを指定します。例えば、企業ツリーは DC=encore,DC=corp,DC=root のように開始されることがあります。
7. 「インポートする属性」に、ユーザーのインポートに使用する属性 (例えば、cn) を入力します。各属性は名前を持ち、objectClass に属します。
8. インポートする前にすべての既存のグループ・メンバーを削除する場合は、「インポートする前に既存のグループ・メンバーをクリアする」チェック・ボックスにチェック・マークを付けます。
9. 「ログイン・ユーザー」および「パスワード」に、Guardium サーバーに接続するユーザー・アカウントの情報を入力します。
10. 「検索フィルターの有効範囲」に、基本レベルにのみ検索を適用する場合は「1 レベル」を、基本レベルの下のレベルに検索を適用する場合は「サブツリー」を選択します。
11. 「制限」に、返される項目の最大数を入力します。過剰な数のメンバーを意図せずロードしてしまうことを防ぐため、このフィールドを 使用して、新規照会や、既存の照会への変更をテストすることをお勧めします。
12. **オプション:** 「検索フィルター」に、基本 DN、有効範囲、および検索フィルターを定義します。通常、インポートは LDAP グループのメンバーシップに基づいているため、memberOF キーワードを使用します。 例えば、「memberOf=CN=syyTestGroup,DC=encore,DC=corp,DC=root」を使用します。
13. 「適用」をクリックして、構成設定を保存します。
    注: 「構成 - 一般」セクションの「状況」標識が「*このグループの LDAP インポートは現在、次のように設定されています*」に変わり、「スケジュールの変更」ボタンと「今すぐ 1 回実行」ボタンが有効になります。これで、LDAP サーバーからインポートすることができます。

LDAP ユーザー・インポートのスケジュール

LDAP インポートがまだ構成されていない場合は、この手順を実行する前に、LDAP ユーザー・インポートの構成を実行する必要があります。

1. 「アクセス」 > 「アクセス管理」 > 「LDAP ユーザーのインポート」をクリックして、「LDAP ユーザーのインポート」パネルを開きます。

LDAP ユーザー・インポートの実行

LDAP ユーザー・インポートをオンデマンドで実行する際には、照会によって返される各ユーザーを受け入れるまたは拒否する機会が与えられます。 これは特に、テストを目的とする場合に便利です。LDAP インポートがまだ構成されていない場合は、この手順を実行する前に、LDAP ユーザー・インポートの構成を実行する必要があります。

1. 「アクセス」 > 「アクセス管理」 > 「LDAP ユーザーのインポート」をクリックして、「LDAP ユーザーのインポート」パネルを開きます。
2. 「今すぐ 1 回実行」をクリックします。タスクの完了後、ユーザーの選択基準を満たすメンバー・セットが「LDAP 照会結果」パネルに表示されます。
3. 「LDAP 照会結果」パネルで、追加する各ユーザーのチェック・ボックスにマークを付けて、「インポート」をクリックします (または「キャンセル」をクリックして、ユーザーをインポートせずに戻ります)。
4. 追加されたユーザーを表示するには、「アクセス」 > 「アクセス管理」 > 「ユーザー・ブラウザー」をクリックして、「ユーザー・ブラウザー」を開きます。 正しいユーザー・アカウントが追加されていることを確認します。

Tivoli LDAP 構成の例

表 1. Tivoli LDAP 構成の例

LDAP ホスト名	**値**
ポート	389
サーバー・タイプ	Tivoli Directory
SSL 接続を使用	

LDAP ホスト名	値
基本 DN	cn=sample realm,o=sample
インポート・モード	「既存の属性をオーバーライド」を選択
インポート・リストにないユーザーは無効にする	
新しくインポートされたユーザーを有効にする	
ログイン・ユーザー	cn=root
パスワード	
検索フィルターの有効範囲	サブツリー
制限	
ユーザー・ログインとしてインポートする属性	cn (ポータルを介して構成可能)
検索フィルター	
ユーザーのオブジェクト・クラス	デフォルト値で埋める - |(objectClass=organizationalPerson)(objectClass=inetOrgPerson)(objectClass=person)
ロールのインポート	チェック・マークを追加
ロールとしてインポートする属性	cn
ロール検索の基本 DB	デフォルト値で埋める - cn=sample realm,0=sample
ロール・フィルター	
ロールのオブジェクト・クラス	デフォルト値で埋める - |(objectClass=groupOfNames)(objectClass=group)(objectClass=groupOfUniqueNames)
ロールを関連付けるユーザーの属性	デフォルト値で埋める - memberOf
ユーザーを関連付けるロールの属性	デフォルト値で埋める - member

親トピック: アクセス管理の概要

「データ・セキュリティー」- ユーザー階層およびデータベースの関連付け

データ・セキュリティー機能を使用して、ユーザーの階層を作成し、ユーザーを特定のデータベースおよびサーバーに関連付けることができます。Guardium® のデータ・セキュリティー機能は、どのユーザーがどの情報にアクセスしたかを報告し、確実に特定のユーザーのみが自分の担当している情報を表示できるようにします。

Guardium のデータ・セキュリティー機能を有効にして使用するには、以下の手順を実行します。

1. データ・セキュリティーの有効化
2. ユーザー階層の作成
3. ユーザーとデータベースの関連付けの作成
4. 結果のフィルタリング

データ・セキュリティー機能を分類機能 (データベースの複数の場所にある機密データをディスカバーおよび分類する機能) と併用すると、データ・レベル・セキュリティーは、指定されたユーザーが指定されたデータ・ソース (データ・ソース定義) からの分類結果を表示できないようにします。また、タスク・タイプが「分類」の場合、データ・レベル・セキュリティーを使用すると、指定されたユーザーが監査タスク結果を表示できないようにすることも可能です。

データ・セキュリティーの有効化

制約事項: データ・レベル・セキュリティーと調査ダッシュボードは同時に有効化できません。

1. admin ユーザーとしてログインし、「設定」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。
2. データ・レベル・セキュリティーのフィルタリングの「有効化」をクリックします。

   注: データ・レベル・セキュリティーのフィルタリングの状況標識アイコンが  として表示されます。

   「サービス状況 (Services Status)」パネル (「設定」 > 「サービス状況 (Services Status)」) を参照することによって、データ・レベル・セキュリティーのフィルタリングが有効になっていることを確認できます。

- データ・レベル・セキュリティーのフィルタリングが有効になっている状態で、accessmgr としてログインし、「ユーザー階層」機能と「ユーザー - データベース関連付け」機能を使用します。

ユーザー階層の作成

「ユーザー階層」には、すべてのユーザー間の親子関係が表示されます。ユーザー階層は、関係の親には特定のサーバーおよびデータベースの表示を許可しますが、子には許可しません。

accessmgr としてログインし、「データ・セキュリティー」 > 「ユーザー階層」をクリックして、「ユーザー階層」を開きます。

以下のいずれかを実行します。

- 「アクティブなユーザー - DB マップの全更新」をクリックして、ユーザーの階層全体を表示します。
- 「ロール」フィルターと「ユーザー」フィルターを使用して、特定のユーザーまたはロールの階層を表示します。ツリーを展開または縮小したり、特定の階層にユーザーを追加したりするには、階層内のノードを右クリックします。
- 「キャッシュ階層のリフレッシュ」をクリックして、階層を更新します。

注: 構成によっては、子のデータ・レベル・セキュリティーを親が継承するという、継承を行うこともできます。

ユーザーとデータベースの関連付けの作成

「ユーザー - データベース関連付け」機能は、ユーザーを特定のデータベースにマップして、ユーザーが、表示を許可されているデータしか表示できないようにします。

accessmgr としてログインし、「データ・セキュリティー」 > 「ユーザー - データベース関連付け」をクリックして、「ユーザー - データベース関連付け」を開きます。

以下のいずれかを実行します。

1. 「アクティブなユーザー - DB マップの全更新」をクリックして、データベースへのユーザーの現在のマッピングを表示します。
2. 「サーバーおよびサービス名の推奨」リストからオプションを選択して、「移動」をクリックし、新規の「ユーザー - DB 関連付け」マップを作成します。
   注: マップが完全に更新された後、すべてのサーバーをリストしたツリーが表示されます。ツリー内の任意のノードをクリックすると、そのノードに現在関連付けられているユーザーが表示されます。

   デュアル・スタック構成を使用している場合は、ルート・ノード、およびアドレスの 2 つのツリー (選択可) が表示されます。1 つのツリーは IPv4 アドレスを示し、長い方のツリーは IPv6 アドレスを示します。

   ユーザーまたはグループをノードに追加するには、ノードを選択して、「ユーザーの追加」または「グループの追加」をクリックします。

一元管理

一元管理アプライアンスでは、「ユーザー - データベース関連付け」画面に、管理対象ノードのデータに基づいてデータベースの関連付けを作成できるようにするためのボックスも表示されます。リモート・ソースの選択は、一元管理アプライアンスに表示されるボックスからのみ行います。また、すべての管理対象ノードからデータを取得するチェック・ボックスも表示されます。

結果のフィルタリング

監視データ・レベルにおけるデータ・レベル・セキュリティーには、特定のユーザーおよびそのユーザーが担当する特定のデータベースに対するデータのフィルタリングが必要です。

システム・レベルでのフィルタリングは「ユーザー階層」および「ユーザー - データベース関連付け」に基づいて行われます。そのため、Guardium システム内のさまざまなレポート、監査プロセス、セキュリティー・アセスメントなどでは、ユーザーに割り当てられているデータベースの情報のみがユーザーに表示されます。

admin ユーザーとしてログインし、「グローバル・プロファイル」を使用して、結果をフィルタリングします。「設定」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。

- デフォルトのフィルタリング
  - すべて表示 - このオプションを使用できるのは、ログインしているユーザーに特殊なロール *datasec-exempt* が定義されている場合だけです。このロールにより、データ・レベル・セキュリティーがない場合と同様に、すべてのデータを表示できるようになります。
  - 間接レコードを含める - このチェック・ボックスは、ログインしたユーザーに属する行だけでなく、その階層におけるその他のユーザーに属する行もすべてビューアーに表示します。
- 監査プロセスのエスカレーション: このタイプのタスクに対するエスカレーションは、datasec-exempt ロールを持つユーザーに対してのみ許可されます。 datasec-exmpt ロールを持たないユーザーは、エスカレーション・リストに表示されません。

  「結果をすべてのユーザーにエスカレート」- このチェック・ボックスにチェック・マークを付けると、監視データ・レベルでのデータ・レベル・セキュリティーが有効になっている場合であっても、監査プロセスの結果 (および PDF バージョン) がすべてのユーザーにエスカレートされます。デフォルト設定では有効になっています。このチェック・ボックスが無効になっている (チェック・ボックスにチェック・マークが付けられていない) 場合、監査プロセスのエスカレーションはユーザー階層の上位レベルのユーザーおよび datasec-exempt ロールを持つユーザーに対してのみ許可されます。チェック・ボックスが無効になっており、ユーザー階層がない場合、 エスカレーションは許可されません。

- 結果の (E メールの添付書類による) 配布用の PDF および CSV の生成では、「管理コンソール」パラメーターで設定されているデフォルトのグローバル・プロファイル値が使用されます。
- ビューアーから生成された PDF および CSV では、画面上で使用されるものと同じフィルタリングが使用されます。

注:

ユーザーとデータベースの関連付けによるデータ・セキュリティーでは、Access、Exception、および Policy Violations の各ドメイン (およびこれらのドメインまたはこれらのドメインの表を使用するカスタム・ドメイン) からのレポートのみをフィルタリングします。その他のすべてのドメイン (レポート) は、ユーザーとデータベースの関連付けによるデータ・セキュリティーによりフィルタリングされません。

admin ロールを持つユーザーは、すべてのロールのイベント・タイプを表示できます (ただし情報は、監視データ・レベルのセキュリティー・パラメーターに基づいてフィルタリングされます)。

データ・レベル・セキュリティーが有効になっている場合、データ・レベル・セキュリティーのフィルタリングが正しく機能するように、カスタム・ドメインに追加された事前定義エンティティーが、その同じドメイン内にある必要があります。

データ・レベル・セキュリティーが有効な場合に、2 つの事前定義エンティティー・サブジェクトが、フィルタリング・ポリシーを使用している (カスタム・ドメイン以外の) 2 つのドメインからデータを送信しようとする場合、2 つの事前定義エンティティー・サブジェクトの送信は許可されません。データ・レベル・セキュリティーは、1 種類のフィルタリング・ポリシーしか実施できません (例えば、server_ip/service_name に応じた 1 つのポリシーおよびデータ・ソースに応じた 1 つのポリシーのみ)。

親トピック: アクセス管理の概要

ユーザー階層の定義方法

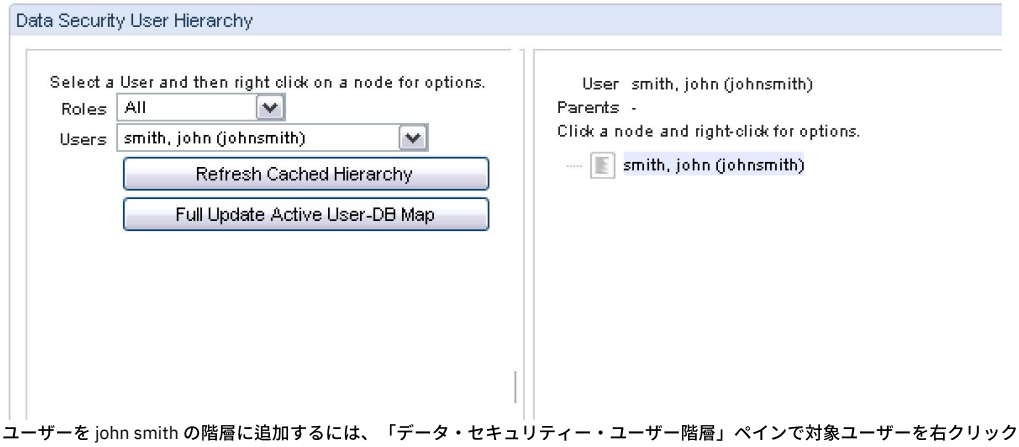
アクセス・マネージャー・アカウントから UI を使用すると、容易にユーザー階層を定義できます。

このタスクについて

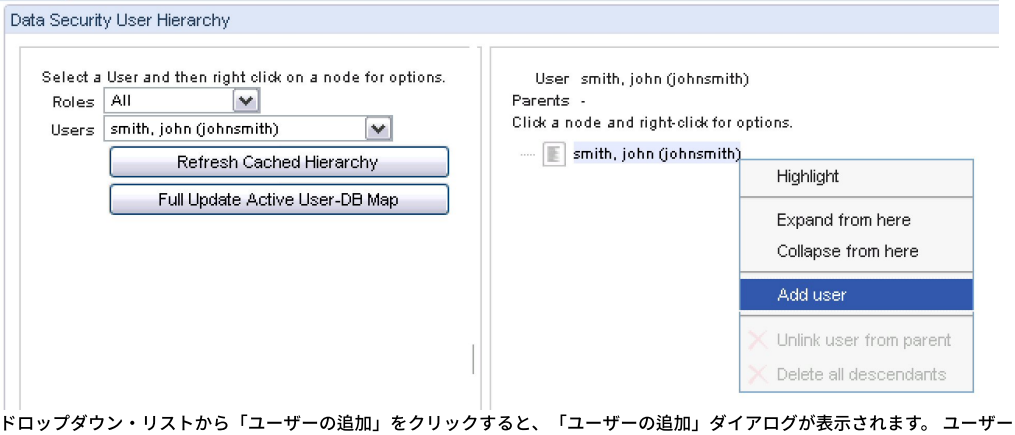
ユーザー階層によるデータ・セキュリティーは、ユーザー間の親子関係を表します。これにより、ある階層の親には特定のサーバーおよびデータベースの表示を許可し、その階層の子には許可しないことで、データ・レベルのセキュリティーを作成および適用できます。構成によっては、子のデータ・レベル・セキュリティーを親が継承するという継承を行うこともできます。

手順

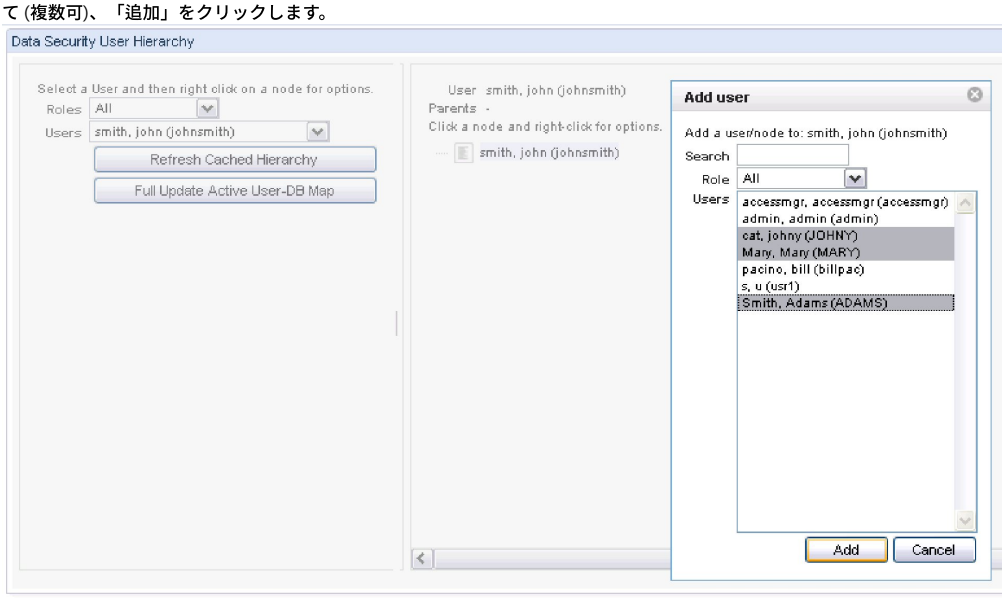
1. accessmgr としてログインし、「データ・セキュリティー」 > 「ユーザー階層」をクリックします。
2. 「ユーザー」ドロップダウン・メニューからユーザーを選択し、そのユーザーを「データ・セキュリティー・ユーザー階層」ペイン内に表示させます。この例では、john smith をユーザーとして使用します。



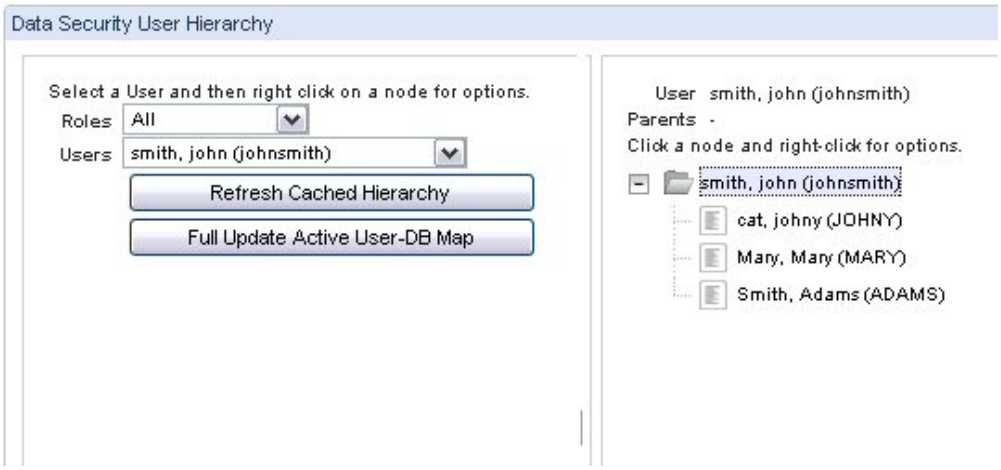
3. ユーザーを john smith の階層に追加するには、「データ・セキュリティー・ユーザー階層」ペインで対象ユーザーを右クリックし、ドロップダウン・メニューから「ユーザーの追加」を選択します。



4. ドロップダウン・リストから「ユーザーの追加」をクリックすると、「ユーザーの追加」ダイアログが表示されます。 ユーザーの階層に追加するユーザーを選択して (複数可)、「追加」をクリックします。



5. ユーザーを階層に追加すると、「データ・セキュリティー・ユーザー階層」パネルがリフレッシュされ、新しい階層をドリルダウンしたり、表示したりできます。



6. この手順を繰り返して、必要なユーザー全員をデータ・セキュリティーのユーザー階層に定義します。

親トピック: アクセス管理の概要

スマート・カードを使用した Guardium UI へのログイン

Guardium のスマート・カード・サポートは、すべてのベンダーがユーザー・アクセスで多要素認証をサポートする必要があるという米国政府の義務付けを満たしています。スマート・カード認証がサポートされるのは、Web ベースの Guardium ユーザー・インターフェース (UI) へのアクセスのみです。

始める前に

多要素認証の要件の詳細は、「Security and Privacy Controls for Federal Information Systems and Organizations」 (NIST Special Publication 800-53) 文書の『Identification and Authentication (Organizational Users) (IA-2)』セクションに記載されています。NIST 800-53 は、NIST の Web サイト (https://www.nist.gov) から入手できます。

政府系アプリケーションでは、Personal Identity Verification (PIV) カードを参照します。民間のアプリケーションでは、Common Access Card (CAC) カードを参照します。PIV カードと CAC カードでは認証局が異なりますが、それ以外の点ではこれらのカードは同じです。

Guardium のスマート・カード・サポートは、「Personal Identity Verification (PIV) of Federal Employees and Contractors」(FIPS Publication 201-2) 文書の『PIV Cardholder Authentication (6)』セクションに記載されている PIV 保証レベルで高信頼度を満たしています。FIPS 201-2 は、NIST の次の Web サイト (https://www.nist.gov) から入手できます。

前提条件

デバイスが必要とするのは次のとおりです。

- Web ブラウザー経由での、スマート・カード証明書にアクセスできる Guardium UI へのアクセス
- スマート・カード・リーダー
- 有効な PIV/CAC カード

このタスクについて

このタスクでは、スマート・カード上の情報を Guardium ユーザーと正しく関連付ける方法について説明します。

スマート・カードと関連付ける Guardium ユーザーを作成します。既存のユーザーをスマート・カードと関連付ける場合、新しいユーザーを作成する必要はありません。ユーザーの作成とアクセス管理について詳しくは、『アクセス管理の概要』を参照してください。

1. 管理ユーザーとして Guardium UI にログインします。
2. 「セットアップ」 > 「ツールとビュー」 > 「ポータル」に移動します。
3. 「認証構成」セクションの下で、「スマート・カード」オプションを選択します。「スマート・カード」オプションがない場合は、スマート・カード・パッチがインストールされていることを確認してください。
4. 「正規表現一致パターン」フィールドで、スマート・カード上のユーザー情報と一致する正規表現 (regex) を指定します。

例

ユーザーの作成

Guardium アプリケーションには、ユーザーを作成するさまざまな方法が用意されています。ユーザーの作成方法に関係なく、認証にスマート・カードを使用するように Web を構成すると、スマート・カードの資格情報のみを使用して SSL/TLS 通信を確立します (Guardium サイトは https を使用します)。

ユーザーを手動で作成する方法の例を次に示します。

1. Accessmgr として CM にログインします。
2. 「アクセス」「ユーザー・ブラウザー」を選択します。
3. 「追加」をクリックします。
4. ユーザー名「Test Cardholder X」を追加します。
5. パスワードを 2 回追加します。
6. ユーザーと同じファーストネーム (名) とラストネーム (姓) を入力します。

7. 「追加」をクリックします。

これで、マッピングを構成できるため、スマート・カードが存在するときは、スマート・カード上の情報がシステム内のユーザーに正しくマップされます。

1. CM から、またはスタンドアロンで Admin としてログインします。
2. ログイン後、「セットアップ」 > 「ツールとビュー」 > 「ポータル」に移動します。

「認証構成」というタイトルのメニュー画面が表示された場合は、スマート・カード・サポート・パッチがインストールされています。

ここで、「正規表現一致パターン」で正規表現を使用して、スマート・カード上のユーザー情報を照合します。正規表現一致パターンの例を次に示します。

CN ?= ?(.*?), ?OU ?= ?Test Agency, ?OU ?= ?Test Department, ?O ?= ?Test Government, ?C ?= ?US

これは、HTTPS を確立するために Web サーバーに送信するように選択したクライアント証明書を持つスマート・カードと連携して動作します。選択したスマート・カード上で、このクライアント証明書は Web サーバーが要求したときにその内容を Web サーバーに提供します。これは、この機能が有効なときに発生する厳密な動作です。例えば、クライアント証明書は、バージョン、シリアル番号、署名アルゴリズム、署名ハッシュ・アルゴリズム、発行者、有効日の始まり、有効日の終わり、所有者などの詳細情報を持ちます。

この例では、次のいずれかのパターンを使用できます。両方ともマッピングと照合されます。 パターン 1 はより厳密です。パターン 2 は、目的に応じて、ニーズに合う独自のパターンを記述できます。効率の良いマッピング・パターンを記述するには、スマート・カード上のデータに詳しいユーザーと協力する必要があります。

パターン 1:

CN ?= ?(.*?), ?OU ?= ?Test Agency, ?OU ?= ?Test Department, ?O ?= ?Test Government, ?C ?= ?US

パターン 2:

CN ?= ?(.*?)

例は両方とも、証明書所有者の CN 属性の値を取得します。これは、ブラウザーで証明書の詳細を調べることで確認できます。この場合は、「Test Cardholder X」です。このパターンを正しく構成することは、スマート・カードの認証を確実に成功させるために最も重要な部分であると考えられます。

他のモジュールで現在使用できる正規表現検証ツールは、この目的では使用できないことに注意してください。(『トラブルシューティングまたはリカバリー・シナリオ』セクションの項目 2 と 3 を参照)。

ここで保存します。まだ完了していないことと、CLI から有効にする必要があることに注意してください。有効化の一部は、GUI が存在しない、サーバーのシャットダウン後に実行する必要があるためです。

CLI での実行部分のために GUI から移動する前に、ルート CA 証明書をトラストストアにアップロードする必要があります。

Web サーバーのトラストストアへのルート CA 証明書のアップロード

この部分では、GUI が使用するトラストストアにルート CA の証明書をアップロードする方法について説明します。「Guardium ポータル」画面と「認証構成」画面の「証明書のインポート」選択肢を使用します。

スマート・カード上の証明書に署名した CA のルート証明書がない場合、CA が署名したユーザー証明書、またはユーザー証明書が含まれているスマート・カードからルート証明書をエクスポートできます。

顧客から授与されたか、certMgr.exe などの認証管理ツールまたはオープン SSL などのツールを使用してスマート・カードからエクスポートすることで、取得した証明書を持っていると想定します。

トラステッド CA のパブリック・ルート証明書。これが、スマート・カード・インフラストラクチャーと、スマート・カードの配布と認証に対する標準的な方法を既に持つ環境では最も一般的なルート証明書のソースです。

スマート・カード認証に使用する証明書を選択します。署名チェーンは、一連の署名認証局をリストします。選択に最適な証明書は、通常、ユーザー証明書の上の中間認証局の証明書です。

CLI からの機能の有効化 (CLI でのみ実行可)

状況を確認するために、次の CLI コマンドを使用します。

```
show system websmartcard
```

この CLI コマンドをオンにするために、次を使用します。

```
store system websmartcard on
```

この CLI コマンドをオフにするために、次を使用します。

```
store system websmartcard off
```

この機能をオフにすると、ローカル認証を使用するシステムとともに GUI が自動的に再開されます。これは、システムの初回デプロイ時に、設定した正規表現が正しくなくてエラーが表示されるときにも役立ちます。

注: 認証にはしが使用されますが、アクセス制御 (ユーザーがアクセス権を持つモジュール、ユーザーがアクセスできるナビゲーションなど) は、引き続きスマート・カード認証がない場合と同様に行われます。

この機能の有効化後

機能を有効にすると、サイトにアクセスできる方法は有効なスマート・カード (PIV、CAC など) 経由のみになります。

これで、GUI サイトにアクセスすると、証明書の選択を求める認証プロンプトが表示されるようになります。

上記の詳細は、管理者がセットアップします。正しく設定されている場合、エンド・ユーザーに必要なのはカードの挿入のみで、直接サイトのコンテンツに移動できます。

有効なスマート・カードを持つユーザーが Web サイトをロードすると、スマート・カードの PIN を求めるプロンプトがブラウザーに表示されます。この PIN により、要求されたときにカード上のクライアント証明書にアクセスできるようになります。

PIN の指定後は、ユーザー・フィールドにスマート・カードから抽出したログイン情報が事前入力された通常の Guardium ログイン・ページが表示されます。ここではパスワードが使用されないことに注意してください。ユーザー・フィールドに表示されるのは、マッピングのために抽出されたユーザーのプレースホルダーのみです。

例えば、証明書が有効で、「Test Cardholder X」に対するスマート・カード発行者のルート CA が Guardium の Web サーバーにロードされた場合 (実行方法についてはセクション『Web サーバーのトラストストアへのルート CA 証明書のアップロード』を参照)、ユーザー・フィールドには「Test Cardholder X」が事前入力され、スマート・カードの PIN を求めるプロンプトが表示されます。これは、スマート・カード上のクライアント証明書にアクセスするためです。クライアント証明書はスマート・カード上に留まり、ファイルにエクスポートすることはできません。プロンプトが 2 回表示される場合がありますが、単に PIN を指定してください。

次のタスク

トラブルシューティングまたはリカバリー・シナリオ

この機能を有効にした後、Guardium の URL をロードしたときに、エラー・ページが表示されます。

診断: 照合する正規表現の構成が正しくないか、カード上に有効な証明書がない可能性が高いと思われます。

照合する正規表現を作成したが、機能しているように見えません。Guardium には正規表現検証ツールがあったことを思い出し、ツールで機能する場合は有効な正規表現であると考えてそのツールを使用しました。 残念ながら、そのツールでテストに成功しても、スマート・カード構成では正規表現パターンが動作しません。

診断: そのツールは、テキスト段落内に正規表現が見つかるかどうかを検出するためのものです。そのため、このケースでは機能しません。この構成は、証明書の詳細に表示される所有者に表示される証明書テキストからテキストの一部を抽出するためのものです。

証明書を選択するためのプロンプトがブラウザーに表示されません。

診断: PC/ラップトップはカード・リーダーとスマート・カードをインストールできます。スマート・カードにある証明書のコピーが Windows OS の certmgr にコピーされます。ただし、サイトにアクセスするときに、ブラウザー (IE、Firefox、または Chrome) が証明書を読み取りません。つまり、この 3 つのブラウザーはすべて、証明書を読み取ることができないため、証明書を選択するためのプロンプトが表示されません。

この現象は、テストしたいくつかのラップトップ上で、すべてのブラウザーについて認められました。この場合、Guardium サイトでのみ発生するわけではありません。スマート・カードの動作を必要とする他のサイトでも、この現象が発生します。これはまれな現象です。

解決策: スマート・カードを管理する部門に連絡してください。

親トピック: アクセス管理の概要

統合および一元管理

統合を使用すると、複数の Guardium システムから取得したデータを 1 つにまとめて表示することができます。一元管理を使用すると、複数の Guardium システム間で整合性を維持することができます。

- 統合
  複数の Guardium® ユニットから情報を収集して 1 つの Guardium 統合アプライアンスにマージすることにより、データベースの使用状況に関するエンタープライズ全般のビューを表示できるようにします。
- 一元管理
  一元管理構成では、1 つの Guardium ユニットが中央マネージャーとして指定されます。 このユニットは、他の Guardium ユニット (管理対象ユニットと呼ばれる) をモニターして制御するために使用できます。 管理対象外のユニットはスタンドアロン・ユニットと呼ばれます。
- 調査センター
  調査センターは統合サーバーの拡張機能です。 調査ユーザーは (一度定義されると) 選択した履歴日付のデータおよび結果をリストアし、フォレンジック調査を実行できます。 日にち (日付) をリストアしたら、調査ユーザーは標準の Guardium UI を使用して、調査対象日付の範囲だけのレポートを定義し、表示できます。

統合

複数の Guardium® ユニットから情報を収集して 1 つの Guardium 統合アプライアンスにマージすることにより、データベースの使用状況に関するエンタープライズ全般のビューを表示できるようにします。

統合プロセス

- ソース・アプライアンスからアグリゲーターに日次ベースでデータをエクスポート (すなわち、日次エクスポート・ファイルをアグリゲーターにコピー) することによって実施されます。
- その後に、アグリゲーターはアップロードされたファイルを調べ、各ファイルを抽出して、アグリゲーター上の内部リポジトリーにマージします。

例えば、エンタープライズ・デプロイメントで Guardium を実行している場合、複数の異なる環境 (例えばさまざまな地理的位置、業務単位など) をモニターする複数の Guardium サーバーが存在することがあります。すべてのデータを中心的なロケーションに集めることができれば、エンタープライズ全体のデータベース使用状況を確認するうえで役立つでしょう。統合アプライアンスとして (初期インストール手順で) 構成された 1 つのサーバーに別の多数のサーバーからデータをエクスポートして、このことを達成できます。このようなデプロイメントでは、通常、すべてのレポート、アセスメント、監査プロセスなどを統合アプライアンスで実行することによって、必ずしもエンタープライズ全般のビューではないにしても、幅広いビューを生成できます。ただし、アグリゲーターでデータを収集するわけではありません。コレクターから取り込んだデータを表示するときに、アグリゲーターを使用します。

事前定義された統合レポートは、「Guardium モニター」タブの「エンタープライズ・バッファー使用状況モニター」、「日次モニター」タブの「ロギング・コレクター」にあります。

アプライアンス・タイプ

コレクター

これを使用して、データベース・アクティビティーを収集し、そのアクティビティーをリアルタイムで分析し、内部リポジトリーに記録して、さらに詳しく分析するか、(アラート送信やブロッキングなどの) 対応をリアルタイムで行うか、あるいはこの両方を行います。 .
このユニットは、データベース・アクティビティーをリアルタイムでキャプチャーおよび分析するために使用します。

アグリゲーター (注 1、2 を参照)
これを使用して、複数のアプライアンス (コレクターおよび他のアグリゲーター) から情報を収集してマージし、環境全体の総括的なビューを作成し、エンタープライズ・レベルのレポートを生成します。 アグリゲーターはデータそのものを収集するのではなく、複数のソースからのデータを統合するだけです。

中央マネージャー (注 1、3、4 を参照)
このアプライアンスを使用して、複数の Guardium アプライアンスを管理および制御します。
中央マネージャー (CM) を使用して、Guardium のデプロイメント全体 (すなわち、すべてのコレクターおよびアグリゲーター) を単一のコンソール (CM コンソール) から管理します。
管理内容として、パッチ・インストール、ソフトウェア更新、および照会、レポート、グループ、ユーザー、ポリシーなどの管理と構成があります。

注:

多くの環境では、中央マネージャーはアグリゲーターでもあります。 中央マネージャーとアグリゲーターは同じアプライアンスにインストールできます。

Guardium アプライアンスは、中央マネージャーにプロモートできるように、インストール時にアグリゲーターとして構成する必要があります。

フェデレーテッド環境ごとの中央マネージャーの数は 1 つです。

中央マネージャー/アグリゲーターの制約
v9.5 (v9.0 パッチ 500) 以降、アプリケーションには、中央マネージャーがアグリゲーター・タイプのアプライアンスでなければならないという制約があります。 つまり、v9.5 以降では、アグリゲーター・タイプのアプライアンスのみを中央マネージャー・アプライアンスにプロモートできます。v9.5 より前の既存の CM アプライアンスは、この変更の対象ではありません。

アップグレード後にダウンと表示されるユニットについての解決策

問題: 検索モードが CM_only モードまたは Local_only モードのアグリゲーターをアップグレードすると、アップグレード後に検索でこのユニットがダウンとして表示される。また、アップグレード後にユーザーが検索モードを all_machines に変更することを選択すると、アグリゲーターから検索を使用できなくなる。

解決策: アグリゲーター・ユニットをアップグレードした後、検索のツールチップでそのアグリゲーター・ユニットがダウンと表示されないようにする場合、ユーザーは以下の 2 つのコマンドを実行できます。

1. grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE
2. restart network

注: 環境が以前 cm_only モードまたは local_only モードであった場合、または今後 cm_only モードまたは local_only モードにする場合、この手順ではアグリゲーターからの検索は有効にならず、アグリゲーターがダウンと表示されなくなるだけです。

用語

表 1.

用語	記述
Guardium アプライアンス	物理的または仮想的な Guardium ボックス。「コレクター」または「アグリゲーター」のいずれかです (一元管理を実施する場合としない場合がある)。
Guardium ユニット	Guardium アプライアンスを参照
マネージャー・ユニット	中央マネージャーとして構成されたアプライアンス
管理対象ユニット	中央マネージャーによって管理されるアプライアンス
スタンドアロン・ユニット	中央マネージャー環境に含まれないアプライアンス
パージ	最適なパフォーマンスを得るために、不要なデータをすべてパージします。パージによって、ディスク・スペースを解放します。
アーカイブ	1 日のデータを圧縮して暗号化されたファイルに入れ、アグリゲーターに送信します。

階層的な統合

Guardium では階層的な統合もサポートされます。これは、複数の統合アプライアンスを上位レベルの中心的な統合アプライアンスにマージすることです。複数レベルのビューを提供するには、これが役立ちます。例えば、複数のユニットを統合する北アメリカ地域用の統合アプライアンスを 1 つ、複数のユニットを統合するアジア地域用の別の統合アプライアンスを 1 つそれぞれ配置し、北米とアジアの統合アプライアンスの内容をマージして単一の企業ビューを提供する中心的なグローバル統合アプライアンスを配置できます。データを集計するために、統合されているすべての Guardium サーバーはスケジュールに基づいてデータを統合アプライアンスにエクスポートします。統合アプライアンスはそのデータを統合アプライアンス上の単一のデータベースの中にインポートします。これにより、統合アプライアンスに対して実行されるレポートは、統合されるすべての Guardium サーバーから集計されたデータに基づくようになります。

システム共有パスワードについて

Guardium 管理者は「システム構成」パネルでシステム共有パスワードを定義します。以下のセクションでは、これについて説明します。システム共有パスワードはアーカイブ/リストア操作、および一元管理/統合操作で使用されます。これを使用する場合、互いに通信するすべてのユニットの間でその値が同じでなければなりません。インストール時にはこの値は NULL で、時間の経過とともに変化する可能性があります。

システム共有パスワードは次のような場合に使用されます。

- 中央マネージャーと管理対象ユニットの間でセキュア接続が確立されるとき。
- 統合される装置が、アグリゲーターにエクスポートされるデータに署名して暗号化するとき。

- いずれかの装置が、アーカイブ用のデータに署名して暗号化するとき。
- アグリゲーターが、統合される装置からデータをインポートするとき。
- いずれかのユニットがアーカイブ・データをリストアするとき。

企業のセキュリティー・プラクティスに応じて、システム共有パスワードを時々変更する必要が生じることがあります。共有パスワードは変更される可能性があるため、各システムは、そのシステムで定義されているすべての共有パスワードの履歴レコードが入っている共有パスワード鍵ファイルを保守します。これにより、古い共有パスワードを使ってシステムからエクスポート (またはアーカイブ) されたファイルを、新しく置換された同じ共有パスワードを持つシステムでインポート (またはリストア) することができます。CLI を使って (現在および過去の) 共有パスワードを 1 つのアプライアンスからエクスポートして、別のアプライアンスにインポートできます。

統合が機能するためには、アグリゲーターおよび統合されるすべてのコレクターで共有パスワードを設定する (それらの間で同じに設定する) 必要があります。

統合、アーカイブ、およびパージ操作

スケジュールされたエクスポート操作により、Guardium コレクター・ユニットから Guardium 統合アプライアンスにデータが送信されます。統合アプライアンスは、独自のスケジュールでインポート操作を実行し、統合処理を完了します。 この一方または両方のユニットにおいて、アーカイブ操作とパージ操作がスケジュールされ、それにより (スペースを解放し、内部データベースのアクセス操作を高速化する目的で) データは定期的にバックアップおよびパージされます。エクスポート、アーカイブ、パージの各機能では、同じデータを処理できますが、同じ日付範囲を処理することはできません。例えば 1 日より古いすべての情報をエクスポートおよびアーカイブし、1 カ月より古いすべての情報をパージすることで、常に 1 カ月分のデータを送信側装置上に残しておくことができます。

注:

アグリゲーターでインポートのスケジュールを設定するときには、すべてのコレクターでエクスポートが完了してからインポートを実行するように計画してください。

CAS データも統合とアーカイブの対象になります。

注: アグリゲーター・サーバーでは No Traffic アラートが非アクティブです。

アグリゲーターでのデータの管理

- データのエクスポート
  - エクスポートの停止
- データのインポート
  - インポートの停止
- アーカイブとパージ
- アーカイブとパージの停止
- アーカイブおよびパージ処理の検証
- 統合およびアーカイブ・アクティビティーに関するレポート
- リストア

データのエクスポート

表 2. データのエクスポート

項目	記述
機能	1 日 (午前零時から次の日の午前零時まで。通常は「昨日」)のデータを圧縮して暗号化されたファイルに入れ、アグリゲーター (またはアーカイブ上の外部リポジトリー) に送信します。
スケジュール	日次ベースで実行されます。 1 日のデータをすべて含めるように、午前零時直後 (00:10)に開始されます。 完了までに要する時間は最大 2 時間 (平均値 - データ量によって異なる) と想定されます。
プロセスの概要	一時データベースを作成します。 関連するデータ (昨日のアクティビティー) を一時データベースにロードします。 一時データベースの自動増分 ID を更新して、その固有性を確保します。 一時データベースの圧縮された暗号化エクスポート・ファイルを作成します。 そのエクスポート・ファイルをアグリゲーター (またはアーカイブ上の外部リポジトリー) にコピーします。

統合アプライアンスにデータをエクスポートするには、手順に従います。各 Guardium ユニットに対して 1 つのエクスポート構成を定義できます。

1. 「管理」 > 「データ管理」 > 「データ・エクスポート」をクリックして、「データ・エクスポート」を開きます。
2. 「エクスポート」ボックスを選択します。これにより、データ・エクスポートの追加オプションが開きます。
3. 「次の期間を経過したデータをエクスポート」に続くボックスで、エクスポート操作の対象となる開始日を、当日 (0 日) よりさかのぼった日数、週数、または月数として指定します。 これらはカレンダーによる計測であり、今日が 4 月 24 日である場合、4 月 23 日にキャプチャーした全データは、操作が実行された時刻に関係なく 1 日古いデータということになります。 昨日のデータからデータ・アーカイブを開始するには、値 1 を入力します。
4. オプションで、「次の期間を経過したデータを無視」に続くボックスを使用して、何日分のデータをアーカイブするかを制御します。 ここで指定する値は「次の期間を経過したデータをエクスポート」の値より大きくする必要があります。つまり、常に少なくとも 2 日分のデータがエクスポートされます。 「次の期間を経過したデータを無視」をブランクのままにした場合、「次の期間を経過したデータをエクスポート」行で指定された値よりも古いすべての日のデータがエクスポートされます。「次の期間を経過したデータを無視」の値を常に設定することをお勧めします。そうしないと、まったく同じ日のデータを何度もエクスポートすることになり、(無視される) 重複データのためにネットワークやアグリゲーターに過負荷が発生します。
5. デフォルトでは「値のエクスポート」ボックスが選択されます。データ・エクスポートが禁止されている国にコレクターが配置され、別の国に統合アプライアンスが配置されているような場合、「値のエクスポート」チェック・ボックスのチェック・マークをクリアすることができます。これにより、データベース値を含んでいるすべてのフィールドがマスクされます。
6. 「ホスト」ボックスに、このシステムの暗号化データ・ファイルの送信先となる統合アプライアンスの IP アドレスまたは DNS ホスト名を入力します。複数のアグリゲーターのエクスポート・データのために 2 次統合を使用可能にするオプションもあります。「ホスト」ボックスは 2 つ使用可能であり、 1 つ目のホストは必須

ですが、2 次ホストはオプションです。 このユニットと、データ送信先の統合アプライアンスとの間では、システム共有パスワードが同じでなければなりません。そうでない場合、エクスポート操作は可能ですが、データを受け取る側の統合アプライアンスはエクスポート・ファイルを暗号化解除できず、インポートが失敗します。詳しくは、システム構成のシステム共有パスワードの説明を参照してください。共有パスワードは、エクスポート・システムと受信システムとで同じでなければなりません。 この理由は、同じ共有パスワードを持っていないと、 エクスポート・システムの構成が設定されず、 受信システムに送信できないというメッセージがテスト・ファイルに関して出力されるからです。

7. 「スケジューリング」セクションを使用して、この操作を定期的に実行するためのスケジュールを定義できます。
8. この装置のエクスポート/パージ構成を保存するには「保存」ボタンをクリックします。「適用」ボタンをクリックすると、システムは、指定されたアグリゲーター・ホストがこのユニットからのデータを受け入れるかどうか確認しようとします。この操作が失敗した場合、「テスト・データ・ファイルをこのホストに送信できませんでした」というメッセージが表示されて、構成は保存されません。ホスト名または IP アドレスが正しく入力されていること、およびホストがオンラインであることを確認してください。
9. 「今すぐ 1 回実行」をクリックして、操作を 1 回実行します。

エクスポートの停止

統合アプライアンスへのデータ・エクスポートを停止するには、次のようにします。

1. 「管理」 > 「データ管理」 > 「データ・エクスポート」をクリックして、「データ・エクスポート」を開きます。
2. 「エクスポート」チェック・ボックスをクリアします。
3. 「保存」をクリックします。

注:「今すぐ 1 回実行」ボタンをクリックした後でエクスポートを停止することはできません。

データのインポート

Guardium コレクター・ユニットは、統合アプライアンスとして構成された別の Guardium アプライアンスに、暗号化されたデータ・ファイルをエクスポートします。統合アプライアンスがインポート操作を実行し、すべてのデータを暗号化解除して独自の内部データベースにマージするまで、暗号化データ・ファイルは統合アプライアンス上の特別なロケーションに保管されます。

注: まだ完全に着信し終わっていないファイルをインポートしてしまうのを防ぐために、統合アプライアンスは最近 2 分間に変更されたファイルをインポートしません。

表 3. データのインポート

項目	記述
機能	データをインポートし、インポートしたデータをアグリゲーターの内部データベースにマージします。
スケジュール	日次ベースで実行されます。 02:00 (またはエクスポートの終了後) に開始されます。 完了に要する時間は最大 3 時間と想定されます。
プロセスの概要 (パージする各日ごと)	パージする各表ごとに delete コマンドを構成します (表とパージ条件は AGG_TABLES で定義されます)。 各表ごとに delete コマンドを実行します。

統合アプライアンス上でデータ・インポート操作を定義するには、以下の手順に従います。各ユニットに対して、データ・インポート構成を 1 つだけ定義できます。

1. 「管理」 > 「データ管理」 > 「インポート」をクリックして、「インポート」を開きます。
2. 「インポート」チェック・ボックスを選択します。すると、インポートされるデータ・ファイルのロケーションを示す変更不能な追加のフィールドが表示されます。
3. 「適用」をクリックして、構成を保存します。「適用」ボタンは、「データのインポート元」チェック・ボックスのオン/オフを切り替えたときにのみ、使用可能になります。
4. 「今すぐ 1 回実行」をクリックして、操作を 1 回実行します。
5. 「スケジュールの変更」をクリックすると、汎用のタスク・スケジューラーが開いて、定期的に実行するよう操作をスケジュールできます。この統合アプライアンスと、これにデータをエクスポートするすべてのユニットの間で、システム共有パスワードが同じでなければなりません。そうでない場合、エクスポート操作は正常に行われますが、統合アプライアンスはエクスポートされたデータ・ファイルを暗号化解除できません。

インポートの停止

他の Guardium ユニットから送られるデータのインポートを停止するには、次のようにします。

1. 「管理」 > 「データ管理」 > 「インポート」をクリックして、「インポート」を開きます。
2. 「データのインポート (Import data)」ボックスをクリアします。
3. 「適用」をクリックして、構成を保存します。インポートを停止しても、他の Guardium ユニットからこのシステムへのデータ・エクスポートは停止しません。それを停止するには、送信側の各ユニットにおいてエクスポート操作を停止する必要があります。

注:「今すぐ 1 回実行」ボタンをクリックした後でインポートを停止することはできません。

アーカイブとパージ

Guardium システムを正常に稼働させるには、定期的にデータをアーカイブおよびパージすることが重要です。最適なパフォーマンスを得るために、不要なデータをすべてアーカイブしてパージすることを強くお勧めします。パージを実行して、ディスク・スペースを解放することは重要です。例えば 3 カ月分のデータだけを Guardium アプライアンス上に残しておく必要がある場合、90 日より古いすべてのデータをアーカイブしてパージします。

アーカイブ/パージ処理により、スペースが解放され、将来の使用に備えて情報が保存されます。スタンドアロン・ユニットおよび統合ユニットから定期的にデータをアーカイブ/パージするのが適切です。Guardium のアーカイブ機能は、不正開封できない、署名付きの暗号化ファイルを作成します。アーカイブ・ファイルは、ファイル・サーバーやストレージ・システムなどの外部システムに転送され格納されます。

注:

アーカイブとパージが両方ともスケジュールされている場合、アーカイブの後にパージが実行されます。

コレクターでアーカイブしたデータは、別のコレクターまたはアグリゲーター・サーバーでリストアできます。アグリゲーターでアーカイブしたデータをコレクター・マシンでリストアすることはサポートされていません。

アグリゲーター・システム上のデータのアーカイブ - 月の最初の日にすべての静的表がアーカイブされます。それ以外の日は、 アーカイブ・データに追加されたデータのみがアーカイブされます。 この方法は、コレクターで使用される方法と同じです。静的表を 通常のパージ・プロセスに追加すると、 オーファンの存在が排除され、ディスク・スペースが解放されるため、レポートのパフォーマンスが改善されます。

アグリゲーター上の静的表のアーカイブとエクスポートにおいて、 すべての静的データが対象に含められるのは、アーカイブの場合は月の最初の日に限られます。 エクスポートの場合は、エクスポート構成が変更されたときです。CLI コマンド store archive_table_by_date [enable | disable] または show archive_table_by_date を使用してください。 他に関連する CLI コマンドとしては、store aggregator clean orphans や show aggregator clean orphans があります。

データ管理タスクのスケジューリング - ユニットの作成時には、デフォルトのスケジュール時刻が提供されます。その時刻を状況に応じて修正することができます。データ管理タスクは、夜間などのビジーでないときにスケジュールする必要があります。データ管理タスクはタスク同士が重なることがないように (例えば、1 つのタスクが開始して終了する前に、別のタスクを開始することはできません)、一定の間隔を置いてスケジュールする必要があります。

データ・インポートとデータ・アーカイブを実行するアグリゲーター/中央マネージャーを扱うときのアグリゲーターのデータ・アーカイブ。デフォルトまたは一般的な設定は、データ・アーカイブで、1 日を経過したデータのアーカイブを実行し、2 日を経過したデータを無視することです。他のコレクター/アグリゲーターからのデータ・インポートの前にデータ・アーカイブの実行がスケジュールされていると、アーカイブにその日のアーカイブ用のインポートが含まれません。次のスケジュールがあるとします: 午前 0 時 30 分にデータ・アーカイブを実行し、午前 6 時に 1 日を経過したデータを対象にデータ・インポートを実行する (このとき、2 日を経過したデータは対象としない)。 アーカイブの発生時に、「昨日」に相当するデータはアーカイブされません。その日のデータ用のインポートがまだ行われていないためです。この例では、データ・アーカイブを、データ・インポートが終了した後に発生するように、スケジュール変更する必要があります。このようにすると、アーカイブに正しく昨日のデータが含まれるようになります。

表 4. データのアーカイブとパージ

項目	記述
パージ機能	アプライアンスから古いレコード (通常、60 日を超えたもの) を削除して、スペースを解放し、内部データベースへのアクセス操作を迅速化します。 パージは日付に基づいて行われます (すなわち、終日分のデータが削除されます) が、引き続き「使用中」(オープン・セッションなど) のレコードは削除されません。
スケジュール	デフォルト・パージ・アクティビティーは、毎日午前 5:00 にスケジュールされます。 コレクター (エクスポート/アーカイブ後) アグリゲーター (インポート後) 完了に要する時間は最大 2 時間と想定されます。
プロセスの概要 (パージする各日ごと)	パージ構成は、データ・アーカイブとデータ・エクスポートの両方で使用されます。 「次の期間を経過したデータをパージ」フィールドを使用して、パージ操作の開始日を、当日 (0 日) よりさかのぼった日数、週数、または月数として指定します。
デフォルト・パージ	パージのデフォルト値は 60 日です。 デフォルト・パージ・アクティビティーは、毎日午前 5:00 にスケジュールされます。 新規インストールでは、デフォルトの値とアクティビティーに基づくデフォルト・パージ・スケジュールがインストールされます。 ユニット・タイプをマネージャー管理に変更したり、スタンドアロンに戻したりするときに、デフォルト・パージ・スケジュールが適用されます。パージ・スケジュールは、アップグレード中は影響を受けません。

特定の時点で、このデータに関するレポートまたは調査を実行する必要が生じることがあります。例えば一部の規制環境では、24 時間以内に照会できる形式でこの情報を 3 年、5 年、または 7 年にわたって保持する必要があります。この作業は、アーカイブ・データをユニットに復元する Guardium リストア機能によってサポートされます。

以下のセクションでは、アーカイブを定義してスケジュールする方法、およびアーカイブからリストアする方法について説明します。

注: アーカイブ操作とリストア操作は、アーカイブ処理時に生成されるファイル名に依存します。アーカイブ・ファイルの名前を決して変更しないでください。

アーカイブ・データ・ファイルをネットワーク上の SCP または FTP ホストに送信したり、EMC Centera または TSM ストレージ・システム (構成されている場合) に送信したりすることができます。各ユニットに対して 1 つのアーカイブ構成を定義できます。ネットワーク上の別のホストにデータをアーカイブして、(オプションで) ユニットのデータをパージするには、手順に従います。

1. 「管理」 > 「データ管理」 > 「データ・アーカイブ」をクリックして、「データ・アーカイブ」を開きます。
2. 「アーカイブ」チェック・ボックスを選択すると、アーカイブ処理に関する追加のフィールドが表示されます。
3. 「次の期間を経過したデータをアーカイブ」に続くボックスに、アーカイブ操作の開始日を、当日 (0 日) よりさかのぼった日数、週数、または月数として指定します。 これらはカレンダーによる計測であり、今日が 4 月 24 日である場合、4 月 23 日にキャプチャーした全データは、操作が実行された時刻に関係なく 1 日古いデータということになります。 昨日のデータからデータ・アーカイブを開始するには、値 1 を入力します。
4. オプションで、「次の期間を経過したデータを無視」に続くボックスを使用して、何日分のデータをアーカイブするかを制御します。 ここに指定する値は、「次の期間を経過したデータをアーカイブ」フィールドの値よりも大きくなければなりません。 「次の期間を経過したデータを無視」行をブランクのままにすると、「次の期間を経過したデータをアーカイブ」行で指定した値より古いすべての日のデータがアーカイブされます。つまり、毎日アーカイブを行い、30 日より古いデータをパージする場合には、(31 日目にパージされるまで) 日次データを 30 回アーカイブすることになります。(CLI コマンド store storage-system を使って) システムで構成されたアーカイブ・オプションに応じて、EMC Centera または TSM オプションがパネルに含まれることがあります。このいずれかのアーカイブ宛先を選択する場合は、以下の該当するトピックを参照してください。
    a. EMC Centera のアーカイブとバックアップ
    b. TSM のアーカイブとバックアップ
5. アーカイブ・データを受信するホストの名前を、IP アドレスまたは DNS で「ホスト」に入力します。

6. 「ディレクトリー」ボックスで、データの格納先ディレクトリーを指定します。FTP または SCP のどちらのファイル転送方式を使用するかに応じて、指定方法が異なります。FTP の場合、FTP アカウントのホーム・ディレクトリーを基準にした相対パスでディレクトリーを指定します。SCP の場合、絶対パスとしてディレクトリーを指定します。
7. 「ユーザー名」ボックスで、ホスト・マシンへのログオンに使用するユーザー名を入力します。このユーザーは、「ディレクトリー」ボックスで指定したディレクトリーに対する書き込み/実行権限を保持していなければなりません。
8. ユーザーのパスワードを「パスワード」ボックスに入力した後、「パスワードの再入力」ボックスに再入力します。
9. データ・パージ
10. アーカイブされるかどうかに関わらずデータをパージするには、「パージ」チェック・ボックスを選択します。このボックスにチェック・マークを付けると、「次の期間を経過したデータをパージ」フィールドが表示されます。 重要: パージ構成は、データ・アーカイブとデータ・エクスポートの両方で使用されることに注意してください。ここで行った変更は、すべてのデータ・エクスポートの実行に適用されます。データ・アーカイブの場合も同様です。パージがアクティブになっていて、データ・エクスポートとデータ・アーカイブの両方が同じ日に実行される場合には、最初に実行された操作が古いデータをすべてパージした後に 2 番目の操作が実行されます。そのため、データ・エクスポートとデータ・アーカイブが共に構成されているときは常に、エクスポート基準経過日数とアーカイブ基準経過日数の両方よりもパージ基準経過日数の方が大きくなければなりません。
11. データをパージする場合は、「次の期間を経過したデータをパージ」フィールドを使用して、パージ操作の対象となる開始日を、当日 (0 日) よりさかのぼった日数、週数、または月数として指定します。指定した日、およびそれより古いすべての日のデータは、注に示す例外を除いてすべてパージされます。パージ開始日に指定する値は、「次の期間を経過したデータをアーカイブ」に指定した値よりも大きくなければなりません。さらに、データ・エクスポートがアクティブである場合 (統合アプライアンスへの「データのエクスポート」を参照)、ここに指定するパージ開始日は、「次の期間を経過したデータをエクスポート」の値よりも大きくなければなりません。 それ以前の操作によってまだアーカイブ/エクスポートされていないデータをパージする際には、警告は出されません。パージ操作では、リストア操作で指定される「リストアしたデータをパージしない」時間枠の範囲内に経過日数が入っているリストア・データはパージされません。詳しくは、アーカイブ・データの「リストア」を参照してください。
12. 「スケジューリング」セクションを使用して、この操作を定期的に実行するためのスケジュールを定義できます。
13. 「保存」」をクリックすると、構成の変更が検証されて、保存されます。「保存」ボタンをクリックすると、システムは指定された「ホスト」、「ディレクトリー」、「ユーザー名」、「パスワード」を検証しようとします (テスト・データ・ファイルをそのロケーションに送信することにより)。
14. 「今すぐ 1 回実行」をクリックして、操作を 1 回実行します。

アグリゲーターでのオーファン・クリーンアップ

リストアされたデータがアグリゲーターに含まれる場合、そのリストアされたデータに関連するオーファン・クリーンアップは、データが最初にリストアされたときに設定された有効期限に従って実行されるように設定されます。

GuardAPI コマンドを使用して有効期限に関連する変更を行っても、リストアされたデータがオーファン・クリーンアップの対象となる日付には影響しません。

例えば、ユーザーがデータをリストアし、そのデータを 7 日間保持したいとします。したがって、このデータの有効期限は、本日から、このデータがオーファン・クリーンアップの対象になる 7 日後までの 7 日間です。

有効期限を変更しても、コンピューターに残されているデータは、最初に設計されたとおりにオーファン・クリーンアップの対象になります (データをより短い/より長い期間保持するように設定しても、そのデータがオーファン・クリーンアップの対象となる日付には影響しません。ユーザーは、特に有効期間をより長い期間に変更する場合、データを失わないようにするために、この点に特に注意する必要があります)。

EMC Centera のアーカイブとバックアップ

EMC Centera を使用するには、

1. 「管理」 > 「データ管理」 > 「データ・アーカイブ」をクリックして、「データ・エクスポート」を開きます。
2. 「データ管理」セクションで、「データ・アーカイブ」または「システム・バックアップ」をクリックします。初期状態では、「ネットワーク」ラジオ・ボタンがデフォルトで選択され、ネットワーク・バックアップ・パラメーターが表示されています。
3. 「EMC Centera」ラジオ・ボタンを選択します。EMC Centera パラメーターがパネルに表示されます。
4. 「保持」ボックスに、データを保持する日数を入力します。 最大値は 24855 (68 年) です。それより長く保存する場合には、後ほどデータをリストアして再び保存します。
5. 「Centera プール・アドレス」ボックスに、Centera プール接続文字列を入力します (例えば `10.2.3.4,10.6.7.8/var/centera/profile1_rwe.pea`)
6. 「PEA ファイルのアップロード」をクリックして、接続文字列に使用する Centera PEA ファイルをアップロードします。
7. 「保存」をクリックして構成を保存します。システムは、指定された接続文字列を使用してプールを開くことにより、Centera アドレスの検証を試みます。操作が失敗すると、通知メッセージが表示され、構成は保存されません。

TSM のアーカイブとバックアップ

アーカイブまたはバックアップの宛先として TSM を選択した場合、アーカイブ構成パネルまたはバックアップ構成パネルの TSM 部分が拡張されます。TSM をアーカイブ/バックアップの宛先として設定する前に、Guardium システムをクライアント・ノードとして TSM サーバーに登録しておく必要があります。TSM クライアント・システム・オプション・ファイル (dsm.sys) を (例えばご使用の PC 上に) 作成して、Guardium にアップロードする必要があります。さらに、そのファイルが定義される方法によっては、dsm.opt ファイルもまたアップロードする必要があります。 Guardium で使用するために dsm.sys ファイルを作成する方法については、所属する組織の TSM 管理者に問い合わせてください。TSM 構成ファイルをアップロードするには、CLI コマンド import tsm config を使用します。

TSM (または Spectrum Protect クライアント) ライフサイクルは、Spectrum Protect 製品用語で定義されます。

TSM を使用するには、

1. 「管理」 > 「データ管理」 > 「データ・アーカイブ」をクリックして、「データ・アーカイブ」を開きます。
2. 「TSM」ラジオ・ボタンを選択します。TSM パラメーターがパネルに表示されます。
3. 「パスワード」ボックスで、TSM サービスを要求するためにこの Guardium ユニットが使用する TSM パスワードを入力して、「パスワードの再入力」ボックスに再び入力します。
4. オプションで、dsm.sys ファイルの servername 項目と一致するように、「サーバー名」を入力します。
5. オプションで、「ホスト」に名前を指定します。
6. 「保存」をクリックして構成を保存します。「適用」ボタンをクリックすると、システムは dsmc アーカイブ・コマンドを使用してサーバーにテスト・ファイルを送信することにより、TSM 宛先の検証を試みます。操作が失敗すると、通知メッセージが表示され、構成は保存されません。

アーカイブとパージの停止

1. 「管理」 > 「データ管理」 > 「データ・アーカイブ」をクリックして、「データ・アーカイブ」を開きます。
2. 「アーカイブ」または「パージ」ボックスをクリアします。
3. 「保存」をクリックします。

アーカイブおよびパージ処理の検証

1. 「レポート」 > 「Guardium 運用レポート」 > 「統合/アーカイブ・ログ」 をクリックして、「統合/アーカイブ・ログ」を開きます。
2. それぞれのアーカイブ/パージ操作の状況が「成功」になっていることを確認します。

統合およびアーカイブ・アクティビティーに関するレポート

1. 「管理」 > 「レポート」 > 「データ管理」 > 「統合/アーカイブ・ログ」にナビゲートして、「統合/アーカイブ・ログ」を開きます。
2. 照会を定義してレポートを作成します。

リストア

前述したように、アーカイブは SCP ホストまたは FTP ホストに、あるいは Centera ストレージ・システムまたは TSM ストレージ・システムに書き込まれます。アーカイブをリストアするには、データのリストア先となる Guardium システムに 1 つ以上の適切なファイルをコピーする必要があります。各日のデータに対して 1 つの別個のファイルがあります。 アーカイブ/パージ操作の構成方法によっては、同じ日に対して、アーカイブ・データの複数コピーが存在する場合があります。アーカイブとエクスポートのデータ・ファイル名は同じ形式です (<daysequence>-<hostname.domain>-w<run> datestamp>-d<data_date>.dbdump/TAR ファイル)。バックアップ・システムではなく、アーカイブ済みデータのファイルをリストアするには、「カタログ・アーカイブ」という GUI 画面を使用する必要があります。アーカイブ操作とリストア操作は、アーカイブ処理時に生成されるファイル名に依存します。アーカイブ・ファイルの名前を決して変更しないでください。生成済みのファイル名が変更された場合、リストア操作は正常に機能しません。

例えば 732423-g1.guardium.com-w20050425.040042-d2009-04-22.dbdump/TAR ファイルとなります。

その月に作成された最初のアーカイブからデータをリストアする場合を除いて、複数日のデータをリストアする必要があります。その理由は、Guardium がデータをリストアする際、リストア対象のデータがアーカイブされたときのすべての情報が必要になるためです。アーカイブが作成された後、そのような情報の一部は、使われないため既にパージされた可能性があります。各月にデータが初めてアーカイブされるとき、リストア操作に必要なすべての情報が自動的にアーカイブされます。したがって、データをリストアする場合、月の第 1 日をリストアして、それ以降、目的の日までのすべての日をリストアするか、目的の日をリストアしてから、以降の月の第 1 日をリストアできます。

例えば 6 月 28 日をリストアするには、6 月 1 日から 6 月 28 日までをリストアするか、あるいは 6 月 28 日と 7 月 1 日をリストアします。

バックアップ・システムではなく、アーカイブ済みデータのファイルをリストアするには、「カタログ・アーカイブ」という GUI 画面を使用する必要があります。アーカイブ操作とリストア操作は、アーカイブ処理時に生成されるファイル名に依存します。アーカイブ・ファイルの名前を決して変更しないでください。生成済みのファイル名が変更された場合、リストア操作は正常に機能しません。

1. 「管理」 > 「データ管理」 > 「データのリストア」をクリックして、「データのリストア」を開きます。
2. 「開始」ボックスに日付を入力し、データを必要とする最も古い日付を指定します。
3. 「終了」ボックスに日付を入力し、データを必要とする最も新しい日付を指定します。
4. 「ホスト名」 ボックスに、アーカイブの起点となる Guardium アプライアンスの名前をオプションで入力します。
5. 「検索」をクリックします。
6. 「検索結果」パネルで、リストアする各アーカイブの「選択」ボックスにマークを付けます。
7. 「リストアしたデータを少なくとも次の期間パージしない」ボックスに、リストアしたデータをアプライアンスに保持する日数を入力します。
8. 「復元」をクリックします。
9. 完了したら、「完了」をクリックします。

トラブルシューティング

技術サポートへのエスカレーションを行うときには、問題発生時からの詳細なログを提供してください。「管理」 > 「レポート」 > 「データ管理」 > 「統合/アーカイブ・ログ」にナビゲートし、該当する期間のレポートを定義します。

アグリゲーター当たりのコレクター最大数の計算

Guardium システムが .ISO から作成される場合、アグリゲーター当たりのコレクター最大数にはデフォルト値 10 が設定されます。

お客様が Guardium システムをアップグレードすると、システムは、以下のロジックを使用してコレクターの最大数を計算します。

1. 内部の Guardium 表のデータにしたがって、コレクターの数を取得します。デフォルト値は 10 です。
2. ステップ 1 の結果が 0 (コレクターが見つからない) である場合、システムはこの値を 10 に設定します。
3. 異なる数のコレクターが見つかった場合、システムは、ステップ 2 で判別される数に 20 % を追加します。
4. 例えば、ステップ 1 でコレクターが見つからなかった場合、ステップ 2 で値 10 を設定してから、ステップ 3 で 20% を追加して 12 にします。
5. 別の例では、ステップ 1 でシステムはアグリゲーターにエクスポートする 5 つのコレクターを検出しました。この場合、値は 5 に設定されます。結果が 5 であり、0 でなかったので、ステップ 2 は該当しません。ステップ 3 は、5 に 20% を追加し、この値を 6 に設定します。

親トピック: 統合および一元管理

一元管理

一元管理構成では、1 つの Guardium® ユニットが中央マネージャーとして指定されます。 このユニットは、他の Guardium ユニット (管理対象ユニットと呼ばれる) をモニターして制御するために使用できます。 管理対象外のユニットはスタンドアロン・ユニットと呼ばれます。

ローカル・マシンという概念は一元管理システム内の任意のマシンを指します。アプリケーションによっては (監査プロセス、照会、ポートレットなど)、管理対象ユニットと中央マネージャーの両方で実行できるものがあります。 どちらの場合も、定義は中央マネージャーから、データはローカル・マシンから来ます (ローカル・マシンが中央マネージャーの場合もある)。

一元管理システムが設定されると、お客様は中央マネージャーと管理対象ユニットのどちらかを使用して、大部分の定義の作成または変更を行うことができます。 実際の編集をどのマシンで行っているかには関わらず、定義のほとんどは中央マネージャー上にあることに留意してください。

注:

- リモート・ソース機能を使用すると、マネージャー上のユーザーは (正しいロール特権を保持していれば) 任意のレポートを管理対象ユニット上で実行でき、また、その管理対象ユニットのデータと情報を表示できます。
- CAS テンプレート定義は他のすべての定義 (レポート、ポリシー、アラートなど) と同様に、フェデレーテッド環境内のすべてのユニット間で共有されます。
- ユーザーによる CAS レポートの実行は、マネージャー上で行うことを推奨します。特に、CAS 構成、ホスト、およびテンプレートと関連する CAS レポートについてはそのようにしてください。
- 「カスタム・ドメイン・ビルダー」を使用してリモート表 (中央マネージャー環境内のマネージャー上にある表。「データ・ソース」や「コメント」など) の一部またはすべてを使用するレポートを作成している場合、そのレポートは管理対象ノード上では動作しません。データは戻されません。
- マネージャーの「一元管理」ページでは、特定の時間間隔に基づく自動的なリフレッシュは行わなくなりました。このページは、システムの GUI タイムアウトに基づいてタイムアウトになります。
- 一定期間アクティビティーがない場合、システムは自動的にユーザーをログアウトし、再度サインインするよう求めます。GUI タイムアウトの長さは CLI コマンド show/store session timeout を使用して設定できます (デフォルトは 900 秒)。セッションがアクティブな間は、状況ライトが 5 分ごとにリフレッシュされます。
- ユーザーがデータを中央マネージャーから管理対象ノードに同期またはアップロードしようとしている場合、そのようなタイプのアクティビティーに関係するすべてのノードでは、Guardium のバージョンが同一でなければなりません。
- 予備の一元管理の移行では、その一元管理環境で定義されているユニット数によって、ユニット・タイプの同期化の実行に最大 5 分かかる場合があります。

- Guardium コンポーネント・サービス
  一元管理環境内の Guardium コンポーネントと、その取得元ロケーションを識別します。
- 一元管理の実装
  特定のマシンを中央マネージャーにして、他のマシンを一元管理システムに接続し、管理対象ユニットを登録して中央マネージャーと通信できるようにします。
- 一元管理機能の使用
  一元管理機能を使用すると、ポータル・ユーザー・アカウントの同期化、管理対象ユニットのモニター、および管理対象ユニットへのセキュリティー・ポリシーのインストールを行うことができます。

親トピック: 統合および一元管理

Guardium コンポーネント・サービス

一元管理環境内の Guardium コンポーネントと、その取得元ロケーションを識別します。

この装置は、他の Guardium 装置 (管理対象装置と呼ばれる) をモニターして制御するために使用できます。 管理対象外のユニットはスタンドアロン・ユニットと呼ばれます。

表 1. Guardium コンポーネント・サービス

コンポーネント	記述
ユーザー、ロール、およびアクセス権	中央マネージャーは、すべての管理対象システムのユーザー、ロール、グループ、およびデータマート表の各定義を制御します。中央マネージャーは、すべてのユーザー、セキュリティー・ロール、グループ、およびデータマート表の定義を含むセットを、スケジュールに基づいて、またはオンデマンドでエクスポートします。管理対象ユニットは、内部データベースを 1 時間ごとに更新します。その結果、中央マネージャー上でユーザー、ロール、アクセス権、またはデータマート表が追加または変更された時刻と、管理対象ユニットでそれらの更新が適用される時刻との間に、最大 1 時間の遅延が生じる可能性があります。 注: Guardium® ユーザーまたはセキュリティー・ロールを、一元管理に登録する予定の既存のスタンドアロン・ユニット上で定義した場合、そのユーザーとセキュリティー・ロールを中央マネージャー上でも定義しない限り、それらの定義はそのシステムが登録された後に使用可能になりません。 管理対象ユニット上でユーザーやセキュリティー・ロールの管理を行うことはできません。そのような定義は中央マネージャーにログオンしたときにのみ管理できます。あるユニットが一元管理に未登録の場合、追加されたすべてのユーザーとセキュリティー・ロールは、デフォルト・ユーザー (admin、accessmgr) 以外はすべて削除されます。アクセラレーター・アドイン製品 (PCI、SOX など) を中央マネージャー環境にインストールする場合は、最初に中央マネージャーにインストールしてから、管理対象ユニット上にインストールします。アクセラレーターで必要なすべてのロールとユーザーは、中央マネージャー上で追加します (そこから管理対象ユニットに同期されます)。アクセラレーターの資料は、アクセラレーター・モジュールに含まれています。このコンポーネント・サービス表の最後に記載されている PCI アクセラレーターの概要を参照してください。
別名とグループ	自動的に別名またはグループを生成するすべてのプロセス (LDAP からのユーザー・グループのインポート、照会によるグループ生成、照会による別名生成、分類など) において、(同一マネージャーが管理する) 複数の管理対象マシンに同一のグループまたは別名が自動生成される場合、既存のグループまたは別名との間に競合が発生する可能性があります。この場合、既存のグループが置換されることはありません。
監査プロセス	監査プロセス自体の定義とそれに対応するタスクすべての定義は、中央マネージャーに保存され、すべての管理対象ユニットでそれらを使用できます。 しかし、スケジュール、結果、および To-Do リストはローカル・マシンに保存されます。 このことは、同一の監査プロセス・タスクがすべての管理対象ユニット上、および中央マネージャー上で実行できることを意味します。しかし監査プロセス・タスクは、異なる時間に異なるマシン上で実行することもできます。これは、管理対象ユニットの負荷期間のピークが異なる場合に役立ちます。 各マシンは、そのマシンが収集したデータに基づき、それぞれ独自の結果セットを保持します。また、各マシンはすべてのユーザーの To-Do リストの独自のセットを保持します。監査プロセス定義は中央マネージャーから管理対象ユニットにユーザー同期プロセスの一部としてエクスポートされます (『ポータル・ユーザー・アカウントの同期』を参照)。 監査プロセスの結果が作成されると、ユーザーはその結果を使用できるようになります。しかし、管理対象ユニット上では、「未処理監査プロセスのレビュー」などのレポートまたはモニターが更新されるまでに最大 1 時間の遅延が生じる場合があります。
照会	各照会では、単一のマシンからデータベース情報のみを取得することができます。中央マネージャーの定義と管理対象ユニットのデータの両方を含む、アクセス情報を必要とする照会では、データが表示されないか、データが欠落します。

コンポーネント	記述
ポリシー	ポリシー定義は中央マネージャーに保存されます。ただし、管理対象ユニットにポリシーをインストールすると、ローカル・コピーが作成されて管理対象ユニットに保存されます。これは、なんらかの理由で中央マネージャーが使用できない場合でも、管理対象ユニットでデータベース・アクティビティーをモニターしてポリシーを使用し続ける必要があるためです。 注: ポリシーを管理対象ノード上にインストールしても、中央マネージャー上の「リフレッシュ」をクリックするまでは、このポリシーは中央マネージャーにアップロードされません。ポリシーをインストールする際には、中央マネージャーと管理対象ユニットのバージョンが同じでなければなりません。異なる場合は、ポリシーはインストールされずエラーが生成されます。
レポート	レポート定義は中央マネージャーに保存されます。 中央マネージャー上でポートレットの再生成が呼び出されると、すべての管理対象ユニットに対してもポートレットの再生成 (レポート ID 付き) の管理要求 (HTTPS) が送信されます。再生成が管理対象ユニット上で呼び出されるとき、それが画面から (管理要求ではなく) 呼び出された場合は、ポートレットのリフレッシュを行うようにマネージャーに対して管理要求が送信されます (これはすべてのユニットにも送信されます)。 あるユニットが停止した場合に備え、管理要求には持続性メカニズムがあります。このトピック内の登録とポリシーのインストールに関するセクションを参照してください。 中央マネージャーでは、レポートと監査プロセスで管理対象ユニットからのデータを使用できますが、管理対象アグリゲーターからのものは使用できません。 管理対象ユニットは、ランタイム・パラメーターとして選択され、リモート・データ・ソースとして参照され、さらに管理対象ユニットのみを含むフィルタリングされたドロップダウン選択リストとして表示されます。 監査プロセスがリモート・データ・ソースを参照するとき、監査プロセスは中央マネージャーからのみ実行できます。そのため、これは管理対象ユニット上に表示される監査プロセスのリストには出現しません。 注: ドメイン「スニファーのバッファー使用」(例えば、リクエスト・レート、CPU 使用量、バッファー使用状況モニターなど) の、中央マネージャー上にある特定のレポートでは、データがまったく表示されません。レポートは空になります。
セキュリティー・アセスメント	監査プロセスと同様、セキュリティー・アセスメントの定義自体は中央マネージャーに保存されます。しかし、結果はローカル・マシンに保存されます。 このことは、同一のセキュリティー・アセスメントを、すべての管理対象ユニット上および中央マネージャー上で実行できることを意味します。
ベースライン	ベースラインは常に中央マネージャーに保存されます。しかし、ベースラインは生成されるマシンにローカルなログに記録されたデータを使用して生成されます。それで、すべての管理対象ユニットからの構成を含める場合は、すべての管理対象ユニット上でベースラインを再生成して、新規の結果を既存のベースラインにマージする必要があります。 重要: 「ベースライン・ビルダー」と関連機能は、Guardium V10.1.4 から非推奨になりました。
コメント	コメントは、そのコメントが関連付けられている対象に応じて、ローカル・マシンと中央マネージャーのいずれかに保存できます。コメントが中央マネージャーにある定義に関連付けられている場合、コメントも Central Manager に保存されます。コメントがローカル・マシンにある結果、または管理対象ユニット固有のもの (検査エンジンなど) に関連付けられている場合、コメントもローカル・マシンに保存されます。
スケジュール	スケジュールは常にローカル・マシンに保存されます。これは、定義が中央マネージャーに保存されている場合でもそうです。
非中央マネージャー・タスク	サーバーが中央マネージャーとして構成されると、あるタスクはそのユニット上で実行できず、他の (非 Central Manager) ユニット上で実行する必要があることに注意してください。 検査エンジンは中央マネージャー上では定義できず、管理対象ユニット上でのみ作成可能です。 しかし、検査エンジンを中央マネージャーで表示することはできます。
アップグレードの考慮事項	中央マネージャーと管理対象ユニットは同じバージョンにすることを推奨します。中央マネージャーを最初にアップグレードし、管理対象ユニットはその後にアップグレードする必要があります。 マネージャーのバージョンが管理対象ユニットのバージョンと異なる状況は、一時的なものにしてください。すべての管理対象ユニットは、マネージャーと同じバージョンにアップグレードすることを強く推奨します。アップグレード後には、同期 (リフレッシュ) をすべての管理対象ノード上で実行することにより、これらの管理対象ノードが適切なソフトウェア・バージョンを認識するようにします。
コンプライアンスのための PCI アクセラレーター	PCI データ・セキュリティー基準は、12 の基本的な要件から構成されています。このうちの多くの要件は、物理的なインフラストラクチャーの保護 (例えば、要件 1: データを保護するためのファイアウォール構成のインストールと保守) や、手続き上のベスト・プラクティスの実施 (例えば、要件 5: アンチウィルス・ソフトウェアの使用と定期的な更新) に焦点を当てています。ただし、そのほかに、カード所有者データへのアクセスのリアルタイムでのモニターとトラッキング、およびデータベース・セキュリティーの正常性状況の連続的なアセスメント (例えば、要件 10: ネットワーク・リソースおよびカード所有者データへのすべてのアクセスのトラッキングおよびモニター) についても、非常に強調されています。 Guardium のデータベース・コンプライアンス用の PCI アクセラレーターは、これらのモニターとトラッキングの要件をサポートし、カード所有者データのセキュリティーを確保するために必要な組織内のプロセスを簡素化するように設計されています。アクセラレーター・レポートのテンプレートは、特定の組織要件と法的要件を直接反映するようカスタマイズすることができます。これらのテンプレートにアクセスするには、用意されている以下のタブを使用します。 • PCI データ・セキュリティー基準の概要 • 計画と編成 • PCI 要件 10: アクセスのトラッキングとモニター • PCI 要件 11: 定期的なテストと検証 • PCI ポリシー違反のモニター 法規制を満たすのに役立つ Guardium ソリューション・ファミリーのその他のツールには、以下のようなものがあります。 • PCI コンプライアンス・レポート・カード - カード所有者データベース・アクセスのセキュリティーの正常性を示す詳細なビュー。ユーザー定義のテスト、重み付け、アセスメントに合わせてカスタマイズされた、連続するリアルタイムのスナップショットをこのビューで使用することにより、コンプライアンス・プロセスが自動化されます。レポート・カードは、セキュリティー・アセスメントを使用して生成することができます。 • 完全な監査証跡 - 法規制へのコンプライアンスのために必要なデータの使用状況と変更内容に関する完全な監査証跡を、ユーザーに負担がかからない方法で生成します。 • 自動化されたスケジューリング - 組織全体における PCI ワークフロー、監査タスク、担当者への情報の通知について、自動的にスケジューリングを行います。

以下の表は、一元管理環境でどのコンポーネントがどのロケーションから取られるかを識別するのに役立ちます。

表 2. 中央マネージャー環境内のコンポーネントおよびロケーション

中央マネージャー	管理対象ユニット
ユーザー	システム構成
セキュリティー・ロール	検査エンジン
アプリケーション・ロールの権限	アラート機能 (構成)
照会	異常検出
レポート	セッション推論
期間	IP からホスト名への別名割り当て
アラート	システム・バックアップ
セキュリティー・アセスメント	統合/アーカイブ
監査プロセス定義	カスタム・アラート
プライバシー・セット	カスタム識別プロシージャー
ベースライン 重要: 「ベースライン・ビルダー」と関連機能は、Guardium V10.1.4 から非推奨になりました。	csv エクスポート出力
ポリシー	スケジュール
グループ	DB オートディスカバリー構成
別名	監査プロセスの結果

ユーザー、セキュリティー・ロール、監査プロセスの各定義、およびグループは、後で説明するように、中央マネージャーからすべての管理対象ユニットへ、スケジュールに基づいてエクスポートされます。

中央マネージャーから、管理者は以下のことを実行できます。

- 管理対象として Guardium ユニットを登録する
- 管理対象ユニットをモニターする (ユニットの使用可能性、検査エンジンの状況など)
- 管理対象ユニットのシステム・ログ・ファイル (syslogs) を表示する
- 管理対象ユニット上のデータを使用してレポートを表示する
- 管理対象ユニットの主な統計を表示する
- Guardium セキュリティー・ポリシーを管理対象ユニットにインストールする
- 管理対象ユニットを再始動する
- 管理対象ユニット上で Guardium 検査エンジンを管理する
- すべての管理対象システム上で使用されるユーザー、セキュリティー・ロール、グループ、およびアプリケーション・ロール権限の完全なセットを保守する
- パッチ配布
- アップロードした JAR ファイルの配布
- パッチ・バックアップ設定の配布
- 認証構成の配布
- 構成の配布

注: 管理者は、アプリケーション・ロール権限を任意の管理対象ユニットから変更できます。これを行うと、権限はすべての管理対象ユニットで変更されます。
親トピック: 一元管理

一元管理の実装

特定のマシンを中央マネージャーにして、他のマシンを一元管理システムに接続し、管理対象ユニットを登録して中央マネージャーと通信できるようにします。

- 新規インストールでの一元管理の実装
- 既存インストールでの一元管理の実装
- 一元管理ユニットが使用不可の場合

- 新規インストールでの一元管理の実装
  1 台のマシンを中央マネージャーにして、同じ共有パスワードを使用し、ユニットを登録して、管理対象ユニットをグループ化します。
- 既存インストールでの一元管理の実装
  既存の Guardium 環境に一元管理を実装し、アクティブ・インスタンスを持つ CAS コレクターを管理対象にマイグレーションします。

親トピック: 一元管理

新規インストールでの一元管理の実装

1 台のマシンを中央マネージャーにして、同じ共有パスワードを使用し、ユニットを登録して、管理対象ユニットをグループ化します。

1 台のマシンを中央マネージャーにする作業

まず、1 台のマシンを中央マネージャーにします。マシンを選択します。次に、以下の手順を実行します。

1. 中央マネージャーにするマシンの CLI にログインします。
2. store unit type manager と入力します。このステップによって、マシンは中央マネージャーになります。ただし、まだ何も管理していません。

同じ共有パスワードの使用

中央マネージャーを用意したら、他のマシンを一元管理システムに接続する必要があります。セキュリティー上の理由で、マシン間の通信は、同じ共有パスワードを使用して暗号化することが要件になっています。このステップを実行するには、以下のアクション項目を実行します。

1. 「設定」 > 「ツールとビュー」 > 「システム」をクリックして、「システム」を開きます。
2. すべてのシステムで、共有パスワードを同じ文字列に設定します。

- ユニットの登録
  管理対象ユニットを登録して、中央マネージャーと通信できるようにします。
- 管理対象ユニットの登録抹消
  ユニットが登録抹消されたときは、必ず中央マネージャーからそのユニットを登録抹消してください。このメソッドは、中央マネージャーで管理対象ユニットの数を減らす唯一の方法です。
- ポータル・ユーザー・アカウントの同期
  中央マネージャーを使用して、ポータル・ユーザーの同期を管理します。

親トピック: 一元管理の実装

ユニットの登録

管理対象ユニットを登録して、中央マネージャーと通信できるようにします。

一元管理への Guardium 装置の登録は、Central Manager からでも、その装置自体からでも行えます。登録をどのように行った場合でも、中央マネージャーとすべての管理対象ユニットは同じシステム共有パスワードを持つ必要があります。管理対象にするユニットが別のマネージャーの一元管理に既に登録されている場合、その中央マネージャーからユニットを登録抹消してから、新規マネージャーに登録します。一元管理に登録および登録抹消したときにそのユニットに対して実行される処理を必ず正確に把握するようにしてください。

注: 管理対象ユニットにログインしているユーザーが中央マネージャーに存在しない場合は、セッションが無効になります。そのユニットが中央マネージャーに登録されるまで、セッションは無効な状態のままです。

登録時に実行される処理

登録時には、以下のアクションが実行されます。

- ユニット・タイプが管理対象に設定され、マネージャー IP が保管されます。
- マネージャーのプロダクト・キーが適用されます。(ライセンス・キーは、ping またはユーザー同期では伝搬しません。登録時、またはシステムのリフレッシュ時に送信されます。)
- すべてのジョブ・スケジューリングがデフォルトにリセットされます。
- すべての psml ファイル (ポータル GUI カスタマイズ) が削除されます。
- すべてのローカル・ユーザーとロールが削除されます。
- 評価されない、しきい値アラートのリストがリセットされます。
- ユーザー・ロール、マネージャーからのアクセス権がロードされます。
- カスタム・クラス、ユーザーがアップロードした JAR、マネージャーからの LDAP トラストストアがアップロードされます。
- 管理対象からマネージャーへのデータベース接続が有効になります。
- マネージャーから管理対象へのデータベース接続が有効になります。
- 必要に応じて、CAS リスナーが始動します。

登録の後、レポート、照会、グループ、ポリシー、監査などのすべての定義が中央マネージャーから取得されます。

登録したユニットの状況がオフラインのままである場合

登録したユニットがオンラインになっており、中央マネージャーからアクセス可能であるにもかかわらず、状況がオフラインのままである場合は、以下の手順を実行します。

- 管理対象にする装置がオンラインで、アクセス可能なおかつ作動可能であるかどうか検査します。これは、ブラウザー・ウィンドウを使用して、その装置の Guardium システムにログインして行います。
- そのユニットの「リフレッシュ」をクリックします。
- ユニットの IP アドレスの入力が正しいことを確認します。
- ユニットが中央マネージャーと同じ共有パスワードを持っていることを確認します。

注: ユニットの登録がオフラインの場合は、登録要求が保持されます。この要求は、ユニットが登録されるまで、指定された IP/ポートに、設定された間隔で再送されます。正常に実行されない登録要求は、7 日後に有効期限切れとなります。

管理対象ユニットからの登録

管理対象ユニット上で GUI を使用して、ユニットを中央マネージャーに登録できます。あるいは、CLI の register コマンドを使用することもできます。これについては、『CLI を使用した管理対象ユニットの登録』で説明します。

1. 「設定」 > 「一元管理」 > 「登録およびロード・バランシング」をクリックして「一元管理登録」を開きます。
2. 「ホスト IP」に、中央マネージャーの IP アドレスを入力します。
3. 「ポート」に、中央マネージャーの https ポート (通常は 8443) を入力します。
4. 「登録」をクリックします。

管理対象ユニット上で登録を行うとすぐに中央マネージャーとの通信が開始され、これ以上の操作は必要ありません。

注: 一元管理で登録を行うとき、一元管理ユニットはオンラインで、このユニットからアクセス可能でなければなりません。これとは対照的に、一元管理ユニットからユニットを管理対象として登録するときは、現在アクセス可能ではないユニットの登録ができます。

CLI を使用した管理対象ユニットの登録

1. 管理対象ユニットで、CLI にログインします。
2. `register management <Manager IP> <Manager Port>` と入力します。

管理対象ユニット上で登録を行うとすぐに中央マネージャーとの通信が開始され、これ以上の操作は必要ありません。

中央マネージャーからのユニットの登録

現在アクセスできないユニットを登録できます。

1. 「管理」 > 「一元管理」 > 「一元管理」にナビゲートして「一元管理」を開きます。
2. 「新規登録」をクリックします。「ユニット登録」ページが開きます。
3. ユニットの IP およびポートを入力し、「保存」をクリックします。「一元管理」ページがリフレッシュされ、新しいユニットが表示されます。

親トピック: 新規インストールでの一元管理の実装

管理対象ユニットの登録抹消

ユニットが登録抹消されたときは、必ず中央マネージャーからそのユニットを登録抹消してください。このメソッドは、中央マネージャーで管理対象ユニットの数を減らす唯一の方法です。

管理対象ユニットからユニットを登録抹消しても、そのユニットが中央マネージャー上で登録抹消されることはありません。中央マネージャーは、ライセンス交付の目的で引き続きそのユニットを管理対象ユニットとしてカウントし、そのユニットを管理対象として扱います。これにより、別のユニットを中央マネージャーに登録できなくなる可能性があります。管理対象ユニット上の登録抹消機能は、緊急時の使用のみを目的として組み込まれています。Manager がサービスを提供しなくなった場合、ユニットは、登録抹消してからでなければ別のマネージャーに登録できません。

管理対象ユニットからユニットを登録抹消しても、そのユニットは引き続き中央マネージャー画面に表示されます。そのユニットの「リフレッシュ」ボタンを押すと、そのユニットが再登録されます。そのユニットの他の操作ボタンを押すと、そのユニットが管理対象ではなくなったことを示すメッセージが表示され、マネージャーからユニットが削除されます。

管理対象ユニット上で GUI を使用して、ユニットを中央マネージャーから登録抹消できます。また、CLI の unregister コマンドを使用することもできます。これについては、『CLI を使用した管理対象ユニットの登録抹消』で説明します。

1. 管理対象ユニットの Guardium UI に admin としてログインします。
2. 「設定」 > 「一元管理」 > 「登録およびロード・バランシング」をクリックして「一元管理登録」を開きます。
3. 「登録抹消」をクリックします。

登録抹消時に実行される処理

登録抹消時には、以下のアクションが実行されます。

- ユニット・タイプがスタンドアロンに設定されます。
- マネージャーの IP がクリアされます。
- プロダクト・キーがクリアされます (新規マネージャーに登録するかライセンスを手動でロードするまではライセンスは NULL です)。
- 評価されない、しきい値アラートのリストがリセットされます。
- すべてのジョブ・スケジューリングがデフォルトにリセットされます。
- Psml ファイルが削除されます。
- デフォルト・ユーザー (admin、accessmgr) 以外のすべてのユーザーが削除されます。
- 管理対象からマネージャーへのデータベース接続が無効になります。
- GUI が再始動されます。

登録抹消の後、レポート、照会、グループ、ポリシー、監査などのすべての定義はローカル・データベースから取得されます。中央マネージャーに保管された定義にはアクセスできなくなります。

確認方法が分からない場合は、ユニットを登録抹消する前に Guardium サポートに連絡してください。

中央マネージャーからのユニットの登録抹消

1. 中央マネージャーに admin としてログインします。
2. 「管理」 > 「一元管理」 > 「一元管理」をクリックして、「登録」を開きます。
3. 登録抹消を行う管理対象ユニットに対応するチェック・ボックスにマークを付けます。
4. 「登録抹消」をクリックします。

管理対象ユニットを中央マネージャー画面から登録抹消すると、管理対象ユニットのリストからそのユニットが削除され、スタンドアロン・ユニットに設定されます。

注: そのユニットのプロダクト・キーは削除され、ユニットを別のマネージャーに登録しない限り、そのプロダクト・キーは手動で設定されることになります。

管理対象ユニットからの登録抹消

管理対象ユニットで UI を使用して、ユニットを中央マネージャーから登録抹消できます。また、CLI の unregister コマンドを使用することもできます。これについては、『CLI を使用した管理対象ユニットの登録抹消』で説明します。

1. 管理対象ユニットに admin としてログインします。
2. 「設定」 > 「一元管理」 > 「登録およびロード・バランシング」をクリックして「登録」を開きます。

3. 「登録抹消」をクリックします。

CLI を使用して管理対象ユニットを登録抹消するには、以下の手順を実行します。

1. 管理対象ユニットで、CLI にログインします。
2. 「`unregister management`」と入力します。

管理対象ユニットから登録抹消した後、中央マネージャーとの通信が切断され、これ以上の操作は必要ありません。

親トピック: 新規インストールでの一元管理の実装

ポータル・ユーザー・アカウントの同期

中央マネージャーを使用して、ポータル・ユーザーの同期を管理します。

このタスクについて

前述したように、中央マネージャーはすべての管理対象ユニットのユーザー、セキュリティー・ロール、グループ、およびデータマート表の各定義を制御します。中央マネージャーは、すべてのユーザー・ロールとセキュリティー・ロールのセットの、暗号化された署名付きのコピーを作成します。また、中央マネージャーは、その情報をすべての管理対象ユニットに送信します。さらに、ローカル処理で必要な他の一部の定義 (グループとグループ・メンバー、監査プロセス、別名など) もコピーされます。管理対象ユニットは、その後、内部データベースを 1 時間ごとに更新します。このプロセスは、ロールまたはデータマート表の使用において最大 1 時間の遅延が生じる可能性があることを意味します。

ユーザー同期の全サイクルが実行されるのは、登録時、または一元管理画面で「リフレッシュ」をクリックしたときです。どちらの場合も、同期情報がマネージャーから送信され、管理対象ユニットにただちにロードされます。

注: スケジュールを設定するときは、他のスケジュール済みジョブ (インポートなど) を妨げないように注意してください。そのジョブを開始できなくなる可能性があります。

手順

ポータル・ユーザーの同期を管理するには、「管理」 > 「一元管理」 > 「ポータル・ユーザー同期」をクリックします。

a. 「スケジュールの変更」 をクリックして、標準のタスク・スケジューラーを使用してユーザー同期タスクのスケジュールを変更します。
b. タスクがアクティブにスケジュールされている場合、「一時停止」をクリックすると、それ以後のスケジュールされた実行を停止します。
c. タスクが一時停止している場合、「再開」をクリックすると、タスクの実行を (定義済みのスケジュールに従って) 再度開始します。
d. 「今すぐ 1 回実行」をクリックすると、同期タスクがただちに実行されます。
   注: スケジュールされているタスクまたは「今すぐ 1 回実行」されるタスクとは、データの収集と管理対象ユニットへのそのデータの送信のみを指します。管理対象ユニットは、データを受信してから最大 1 時間後まで、そのデータを使用したユーザー表の更新をしない場合があります。

親トピック: 新規インストールでの一元管理の実装

既存インストールでの一元管理の実装

既存の Guardium 環境に一元管理を実装し、アクティブ・インスタンスを持つ CAS コレクターを管理対象にマイグレーションします。

既存の Guardium 環境では、概略を示す手順を参照して、一元管理の実装計画を作成します。既存の Guardium ユニットを中央マネージャーに変換する場合は、中央マネージャーがネットワーク・トラフィックをモニターできないことに留意してください。例えば、検査エンジンを中央マネージャー上で定義することはできません。

1. 中央マネージャーおよびすべての管理対象ユニットで使用するシステム共有パスワードを選択します。詳しくは、『システム構成』のシステム共有パスワードに関するトピックを参照してください。
2. 中央マネージャー・ユニットをインストールするか、既存システムの 1 つを Central Manager として指定します。どちらの場合でも、store unit type コマンドを使用して、中央マネージャーにマネージャー属性を設定します。
3. スタンドアロン・ユニットからの定義で一元管理環境で使用可能にするものはすべて、そのスタンドアロン・ユニットを管理対象として登録する前にエクスポートしておく必要があります。後で、それらの定義は中央マネージャーにインポートされます。定義をエクスポートまたはインポートする前に、管理対象ユニットとなるスタンドアロン・ユニットごとに、ここで示す手順を実行してください。『定義のエクスポート/インポート』の概要情報を参照してください。
   - システムが管理対象ユニットになった後に使用できるようにするスタンドアロン・システムの定義を決定します。スタンドアロン・システム上のコンポーネントのうち、使用可能にしないものについては無視してください。
   - スタンドアロン・ユニット上で定義されていたセキュリティー・ロールとグループを中央マネージャー上で定義されているものとを比較します。一元管理下では、これらの定義の単一のバージョンをすべてのユニットに適用します。同じ名前のセキュリティー・ロールが両方のシステムに存在し、異なる目的で使用されている場合、中央マネージャーにロールを新規追加し、定義のインポート後に該当する定義にその新規ロールを割り当てます。
   - 同じグループ名がスタンドアロン・ユニットと中央マネージャーに存在し、そのメンバーが異なっている場合、スタンドアロン・システム上に複写したグループを新規作成します。このとき、中央マネージャー上に存在しないグループ名を選択するよう注意してください。エクスポートする対象の定義すべてにおいて、古いグループ名への参照を新規グループ名への参照に変更します。
   - すべての定義に割り当てられたセキュリティー・ロールは、すべてスタンドアロン・システムからエクスポートされます。定義をインポートするときは、ロールなしでインポートされます。そのため、ロールは手動で追加する必要があります。
   - 各システムのアプリケーション・ロール権限を確認します。スタンドアロン・ユニット上のアプリケーションに割り当てられたセキュリティー・ロールのいずれかが中央マネージャーで欠落している場合は、それを中央マネージャーに追加します。
   - システムが管理対象ユニットになった後に使用できるようにするすべてのスタンドアロン・システムの定義をエクスポートします。(『定義のエクスポート/インポート』参照)。ユーザーとセキュリティー・ロールはエクスポートしないでください。ある定義についてインポートするか不明である場合は、それを別個のエクスポート操作でエクスポートしておけば、その定義を中央マネージャーにインポートするかどうかを後で決定できます。 一元管理に登録すると、スタンドアロン・ユニットにあった古い定義はいずれも使用できなくなります。
   - スタンドアロン・ユニット上で、監査プロセスの結果の PDF バージョンを作成し、適切なロケーションに保管しておきます。 一元管理下では、一元管理下で作成された監査結果のみが使用可能です。
   - すべてのユーザーに対して、スタンドアロン・ユニット上で、カスタム・レポートを含むすべてのポートレットを削除するように、そして一元管理への変換が完了するまで新規のレポートは作成しないように指示します。

- 中央マネージャー上で、スタンドアロン・ユニットにあったすべてのユーザーを手動で追加します。
- スタンドアロン・ユニット上で、admin ユーザーを除くすべてのユーザー定義を削除します (admin は削除できません)。
- スタンドアロン・ユニットを一元管理に登録します。『一元管理へのユニットの登録』を参照してください。
- 中央マネージャー上で、スタンドアロン・システムからエクスポートしたすべての定義をインポートします。組み込んだ項目への参照 (例えば、アラート通知の受信者など) が正しいかどうか確認します。セキュリティー・ロールを、必要に応じてすべてのインポート定義に再度割り当てます。
- レイアウトに表示するカスタム・レポート用にポートレットを再生成するには、「レポート・ビルダー」アプリケーションを使用する必要があることを管理対象ユニットのユーザーに知らせます。

スタンドアロン CAS コレクターの管理対象へのマイグレーション

アクティブ・インスタンスを持つ CAS コレクターを管理対象にマイグレーションするときには、以下の手順を使用します。

1. CAS ホスト定義をスタンドアロン・コレクターからエクスポートします。
2. スタンドアロン・コレクターを管理対象にします。
3. 管理対象になったコレクターの GUI から CAS ホストを再始動します。
4. CAS ホスト定義をマネージャーにインポートします。
5. 管理対象コレクターの GUI から CAS ホストを再度再始動します。

これらのステップを実行すると、CAS コレクターはスタンドアロンだったときと同じインスタンスを保持し、同じファイルをモニターします。

注: スタンドアロンだったときに収集された CAS データは削除されます。ファイルに変更がなければ、収集される CAS データはありません。
親トピック: 一元管理の実装

一元管理機能の使用

一元管理機能を使用すると、ポータル・ユーザー・アカウントの同期化、管理対象ユニットのモニター、および管理対象ユニットへのセキュリティー・ポリシーのインストールを行うことができます。

- 「適用状態」ビュー
  「適用状態」のビューでは、Guardium 環境全体に関する情報が収集され、強力で簡単に取り込まれるグラフィカル・ビューに表示されます。
- デプロイメント・インベントリー
  「インベントリー (inventory)」ビューには、すべてのデータベース・サーバーとインストール済みの S-TAP クライアントまたは GIM クライアントの一元管理ビューが表示されます。
- 「リソース・デプロイメント」ビュー
  「リソース・デプロイメント」ビューには、すべてのデータベース・サーバーと、関連するコレクター、アグリゲーター、および中央マネージャーの一元管理ビューが表示されます。
- 管理対象ユニット・グループの作成
  管理対象ユニットをグループに編成してから、それらのグループにアクションを実行します。
- 管理対象ユニットのモニター
  一元管理を使用して管理対象ユニットをモニターします。
- 管理対象ユニットへのセキュリティー・ポリシーのインストール
  管理対象ユニットにセキュリティー・ポリシーをインストールします。
- 一元化パッチ管理
  パッチのインストール、状況、および履歴を表示可能にし、制御します。
- 構成プロファイルの処理
  構成プロファイルにより、中央マネージャーから構成設定およびスケジューリング設定を定義して、中央マネージャー自体の構成を変更することなく、それらの設定を管理対象ユニット・グループに配布することができます。
- 構成の配布
  構成、ならびにそのスケジュールは、全体またはその一部を、中央マネージャーと管理対象ユニットの間で配布することができます。
- 認証構成の配布
  各アプライアンスで別個に認証を構成する代わりに、中央マネージャー上で一元管理認証 (認証の構成) を 1 回構成し、それからすべての管理対象ユニットに配布することができます。このようにすると、情報の入力を 1 回行うことで、その情報を一部またはすべてのユニットに適用することができます。一部のユニットで異なるタイプの認証を使用することもできます。
- 予備の中央マネージャー
  予備の中央マネージャーまたはバックアップ中央マネージャー (CM) を使用して、プライマリー CM が使用不可になった場合に備えてセカンダリー CM またはバックアップ CM を構成します。

親トピック: 一元管理

「適用状態」ビュー

「適用状態」のビューでは、Guardium 環境全体に関する情報が収集され、強力で簡単に取り込まれるグラフィカル・ビューに表示されます。

「適用状態」のビューを使用すると、システムの使用傾向を調査すること、および不安定なシステムやダウンしているシステムを素早く特定することができます。これらのビューにより、対応時間が削減され、Guardium デプロイメント内の問題によるリスクが軽減されます。「適用状態」のビューは、異なる複数の情報ソースを固有の関連ビューに統合することで連携して動作するように設計されています。

「適用状態トポロジー」ビューおよび「適用状態表」ビュー

「適用状態トポロジー」ビューおよび「適用状態表」ビューには、環境内のシステム間のデータ・フロー関係が表示されます。これらのビューにより容易に、問題のあるシステムを識別し、根本的な問題を調査できます。

トポロジー・ビューにアクセスするには、「管理」 > 「システム・ビュー」 > 「適用状態トポロジー」にナビゲートします。表ビューにアクセスするには、「管理」 > 「システム・ビュー」 > 「適用状態表」にナビゲートします。

適用状態ダッシュボード

「適用状態ダッシュボード」では、Guardium デプロイメントで検出された問題の概要を一目で確認できます。このダッシュボードは、問題が特定された個々のシステムを調査する前に、正常性データでパターンと傾向を特定するのに特に便利です。

このダッシュボードにアクセスするには、「管理」 > 「システム・ビュー」 > 「適用状態ダッシュボード」にナビゲートします。

以下の表に、「適用状態」の各ビューで使用できるデータのタイプをまとめます。

表 1. 「適用状態」のビューの概要

	ダッシュボード	トポロジー	表
ユニット使用状況	✔	✔	✔
相関アラート	✔		
自己モニター	✔		
システム要件	✔		
統合		✔	✔
検査エンジン (S-TAP 検査データ)		✔	
接続		✔	✔
S-TAP 接続		✔	

重要: 「適用状態」のビューには、Guardium 環境全体から収集されたデータが表示されます。これらのビューは、中央マネージャーからのみ使用できます。

- 「適用状態」のビューのための中央マネージャーの構成
  「適用状態」のビューを使用するには、ユニット使用状況データの収集を有効にし、相関アラートを構成し、環境のデータ・インポートおよびエクスポートを構成します。
- 「適用状態トポロジー」ビューおよび「適用状態表」ビュー
  「適用状態トポロジー」ビューおよび「適用状態表」ビューで、Guardium 環境の構成とそのデータがどのように表示されるかについて詳しく説明します。
- 適用状態ダッシュボード
  Guardium デプロイメント全体からのデータが適用状態ダッシュボードにどのように表示されるかについて詳しく説明します。
- シナリオ:「適用状態トポロジー」ビューを使用した過負荷システムのトラブルシューティング
  このトピックでは、「適用状態トポロジー」ビューを使用して、環境内の過負荷システムを特定し、修正する方法について説明します。

親トピック: 一元管理機能の使用

「適用状態」のビューのための中央マネージャーの構成

「適用状態」のビューを使用するには、ユニット使用状況データの収集を有効にし、相関アラートを構成し、環境のデータ・インポートおよびエクスポートを構成します。

このタスクについて

中央マネージャーの「適用状態」のビューには、Guardium 環境全体からのデータが表示されます。デプロイメント全体に関するデータを表示できるようにするために、ユニット使用状況データの収集、相関アラートの構成が必要であり、またデータのインポート、エクスポート、および S-TAP 検査を正しく構成する必要があります。「適用状態」のビューに表示されるデータの概要については、「適用状態」ビューを参照してください。

デプロイメントは、「適用状態」のビューをサポートするように既に構成されている場合が多いです。いずれかの「適用状態」のビューで以下のいずれかの問題を見つけた場合、この手順で説明されている構成ステップを確認してください。

- CM バッファー使用状況レポートはスケジュールに入っていません
- ユニット使用状況レポートはスケジュールに入っていません
- エクスポートはスケジュールに入っていません
- インポートはスケジュールに入っていません
- 問題は見つかりませんでした
- 状況不明

手順

1. 中央マネージャーからのユニット使用状況データの収集と処理を構成します。 詳しくは、『ユニット使用状況データ処理の構成』を参照してください。
2. 「適用状態ダッシュボード」への相関アラートの組み込みを有効にします。
   a. 「保護」 > 「データベース侵入保護 (Database Intrusion Protection)」 > 「アラート・ビルダー」を開きます。
   b. 既存のアラートを選択し、 アイコンをクリックします。または、 アイコンをクリックして新規アラートを作成します。
   c. アラートの「カテゴリー」を指定します。 カテゴリーが指定されていないアラートは「カテゴリーなし」として表示されます。
   d. ダッシュボードにアラートを組み込むために、「適用状態ダッシュボードに表示」チェック・ボックスを選択します。
   重要: 適用状態ダッシュボードにアラートを組み込むために、「重大度」を「低」、「中」、または「高」に設定する必要があります。
   アラートの定義について詳しくは、アラートの作成を参照してください。
3. 中央マネージャーからのデータのインポートとエクスポートを構成します。 詳しくは、統合を参照してください。
   ヒント: 「構成プロファイルの配布」ツールを使用して、Guardium デプロイメントのデータ・インポートおよびエクスポートを構成するプロセスを簡素化します。詳しくは、構成プロファイルの処理を参照してください。
4. サポートされるすべての S-TAP のために S-TAP 検査を構成します。 詳しくは、S-TAP 状況モニターおよびS-TAP 検査結果の確認を参照してください。

タスクの結果

構成手順を完了し、データを更新できるようにした後、「適用状態トポロジー」および「適用状態表」ビューに、 状況が主に表示されます (ただし、システムに既存の正常性の問題がある場合は除きます)。「適用状態ダッシュボード」には、既存のユニット使用状況の問題が含まれ、新しい相関アラートの状態の表示が開始されます。

ユニット使用状況、またはデータのインポートおよびエクスポートのスケジュールについてアラートがある場合、最大 1 時間待機し、「適用状態」ビューを新しい情報で更新できるようにします。新しい相関アラート・データを使用できるかどうかは、アラートに対して指定されている通知頻度によって決まります。

親トピック: 「適用状態」ビュー
関連概念:
統合
関連タスク:
ユニット使用状況データ処理の構成
構成プロファイルの処理
関連情報:
相関アラート

「適用状態トポロジー」ビューおよび「適用状態表」ビュー

「適用状態トポロジー」ビューおよび「適用状態表」ビューで、Guardium 環境の構成とそのデータがどのように表示されるかについて詳しく説明します。

「適用状態トポロジー」ビューは、中央マネージャーからアクセス可能であり、その中央マネージャーに接続されている Guardium 環境全体の概要を可視化します。 「適用状態トポロジー」ビューには、環境内のノード間の関係の表示に加えて、接続されているすべてのアグリゲーター、コレクター、および S-TAPs に関する適用状態の情報も示されます。環境で検出された正常性の問題に素早く対処できるようにするために、「適用状態トポロジー」ビューから複数の調査および解決アクションを直接使用できます。

デフォルトの「適用状態トポロジー」ビューは、アグリゲーターと管理対象ユニット間のデータのインポートとエクスポートの関係を示すデータ・フロー・ビューです。「適用状態トポロジー」ビューは、「管理」 > 「システム・ビュー」 > 「適用状態トポロジー」で開きます。

また、「管理」 > 「システム・ビュー」 > 「適用状態表」で、適用状態データのソート可能な表ビューも使用できます。

データ可用性

いくつかの要因が、システム・データの可用性、およびそのデータの「適用状態トポロジー」ビューと「適用状態表」ビューでの表示に影響します。「適用状態」ビューを使用するようにシステムを構成する方法については、「適用状態」のビューのための中央マネージャーの構成を参照してください。

データのタイプ

正しく構成されている場合、「適用状態トポロジー」ビューおよび「適用状態表」ビューには、複数の異なるソースから収集されたデータが表示されます。表示されるデータのタイプはユニット・タイプによって決まります。これについて、以下のセクションで概説します。

接続

接続カテゴリーは、Guardium 環境内のシステムが通信できるかどうかを示します。

- 適用対象: 中央マネージャー、アグリゲーター、コレクター、および S-TAPs
- 例:「ユニットは応答しません」、「S-TAP は応答しません」など

ユニット使用状況

ユニット使用状況カテゴリーは、Guardium システムがどの程度ロードされているかに関する情報を示します。

- 適用対象: 中央マネージャー、アグリゲーター、およびコレクター
- 例:「CPU ロード」、「空きバッファー・スペース」、「MySQL ディスク使用状況」など
- 詳しくは、ユニット使用状況レベルを参照してください。

統合

統合カテゴリーは、Guardium システム間のデータのインポートおよびエクスポートのフローに関する情報を示します。

- 適用対象: 中央マネージャー (アグリゲーターとして構成されている場合)、アグリゲーター、およびコレクター
- 例:「インポートに失敗しました」、「エクスポートに失敗しました」、「エクスポートはスケジュールに入っていません」など
- 詳細については、事前定義管理レポートおよび 統合 を参照してください。

検査エンジン

検査エンジン・カテゴリーは、S-TAP 検査情報を提供します。

- 適用対象: S-TAPs
- 例:「S-TAP 検査が失敗しました」など
- 詳細については、Configuring the S-TAP verification schedule および Viewing S-TAP verification results を参照してください。

アイコンをクリックすると、「設定のカスタマイズ」ダイアログが開きます。ここで、「適用状態トポロジー」ビューおよび「適用状態表」ビューに表示するデータのタイプを定義できます。

データ待ち時間

事前設定およびユーザー定義の複数のスケジュールによって、「適用状態トポロジー」ビューに表示されるデータの待ち時間が決まります。これらのスケジュールについて、以下の表にまとめます。

表 1. 「適用状態トポロジー」ビューのデータ待ち時間

正常性カテゴリー	ノード・タイプ	待ち時間
接続	アグリゲーターまたはコレクター	15 分未満
接続	S-TAP	エンタープライズ・ロード・バランシングが使用可能の場合、15 分未満 エンタープライズ・ロード・バランシングが使用不可の場合、1 時間未満
統合	中央マネージャー、アグリゲーター、またはコレクター	1 時間未満
検査	S-TAP	1 時間未満
ユニット使用状況	中央マネージャー、アグリゲーター、またはコレクター	推奨構成に基づき 1 から 2 時間。詳しくは、ユニット使用状況データ処理の構成を参照してください。

特定の環境変更および構成変更について、以下の待ち時間を監視します。

- 新しく登録されたアグリゲーターまたはコレクターは、15 分以内に「適用状態」ビューで使用できるようになります。
- コレクターからデータ・エクスポート・スケジュールまたはデータ・エクスポート構成を削除した場合、2 時間以内に「適用状態」ビューに反映されます。

データ表示

正常性状況

「適用状態トポロジー」ビューには、Guardium システムに関する 3 つのカテゴリーの正常性情報 (「接続」、「ユニット使用状況」、および「統合」) が表示されます。これらのカテゴリーのメトリックには、次のいずれかの正常性状況が割り当てられます:「状況不明」(重大度最小)、「正常性の問題はありません」、「重大度低 (low severity)」、「重大度中」、「重大度高」(重大度最大)。全体状況は、表示される正常性カテゴリーに含まれる個々のメトリックの最も重大な状況によって決まります。「設定のカスタマイズ」ダイアログを使用して除外したデータは、システムの全体状況を決定するのに使用されません。

例えば、「ユニット使用状況」カテゴリーの「再始動」メトリックに「重大度高」状況が割り当てられているが、別のカテゴリーに正常性の問題が存在しない場合、そのシステムの「全体状況」は「重大度高」になります。この動作により、最も重大な状態をシステムの全体状況としていつでも一目で確認できます。

「管理」 > 「システム・ビュー」 > 「適用状態トポロジー」ビューには、重大度が低、中、または高の問題が少なくとも 1 つ検出された場合に限り、使用可能な正常性カテゴリーの詳細な状況が表示されます。

「管理」 > 「システム・ビュー」 > 「適用状態表」ビューには、使用可能な正常性カテゴリーの詳細な状況が常に表示されます。

正常性状況のロールアップ

「適用状態トポロジー」ビューには、Guardium 環境全体の正常性情報を効率よく表示するために、正常性状況のロールアップ方針が実装されています。この方針を使用すると、子ノードは親ノードの下に縮小され、子の正常性状況は親にロールアップされます。ロールアップされた状況は、親ノードに付加された小さいアイコンとして表されます。

重要: 状況を親コレクターにロールアップする S-TAP ノードに対してのみ、正常性状況のロールアップがサポートされます。

例えば、  は、正常性の問題がないコレクターを示していますが、小さい赤色の円は、そのコレクターに関連する 1 つ以上の S-TAPs に、重大度が高の問題があることを示します。そのコレクターをクリックすると、ノードが展開され、関連した S-TAPs とそれらの正常性状況が表示されます。例えば、

は、コレクターに関連する 4 つの S-TAPs のうち、2 つの S-TAPs に重大度が高の正常性の問題があり、別の 2 つの S-TAPs に重大度が低の正常性の問題があることを示します。

子ノードが縮小されているときに、子ノードから親ノードにロールアップされるのは、最も重大な状況のみです。上記の例では、親ノードは小さい赤色の円を示しています。これは、その 1 つ以上の子に重大度が高の問題があるためです。ただし、1 つ以上の子ノードに重大度が低の問題がある一方で、他のすべての子ノードには正常性の問題がない場合、親ノードには小さい黄色い円が表示されます。

デプロイメントの表示

「適用状態トポロジー」ビューには、予期しないデプロイメント構成が表示されることがあります。これらの構成シナリオのいくつかについて、以下のセクションで説明します。

Guardium V10.1.3 より前の管理対象ユニット

Guardium V10.1.3 より前の管理対象ユニットがバージョン V10.1.3 以後の中央マネージャーに接続している場合、これらの管理対象ユニットでは、不正確または不整合なユニット使用状況データが表示されることがあります。この問題を解決するには、中央マネージャーの CLI にログインし、管理対象ユニットごとに次のコマンドを実行します。

```
grdapi change_tracker_reset host=[managed unit host name or IP address]
```

ベスト・プラクティス: 管理対象環境では、すべてのユニットが同じ Guardium バージョン・レベルで作動するようにお勧めします。

Guardium V10.1 より前の管理対象ユニット

Guardium V10.1 より前の管理対象ユニットを「適用状態トポロジー」ページまたは「適用状態表」から表示した場合、これらの管理対象ユニットでは、「統合」正常性セクションで「状況不明」が表示されます。

ベスト・プラクティス: 管理対象環境では、すべてのユニットが同じ Guardium バージョン・レベルで作動するようにお勧めします。

サポート対象外の S-TAP

「適用状態トポロジー」ビューには、S-TAP 検査用に構成されている S-TAP、およびエンタープライズ・ロード・バランシングに参加している S-TAP が表示されます。S-TAP を、S-TAP 検査用に構成できない場合、またはエンタープライズ・ロード・バランシングに参加するように構成できない場合、S-TAP は表示されません。

S-TAP ロード・バランシング

S-TAP ロード・バランシングが participate_in_load_balancing パラメーターを使用して構成され、S-TAP が、複数のコレクター間でトラフィックのバランスを取るように構成されている場合、「適用状態トポロジー」ビューには、その S-TAP が各コレクターの子ノードとして表示されます。例えば、*S-TAP 1* が *コレクター A* と *コレクター B* でロード・バランシングされる場合、*コレクター A* と *コレクター B* の両方が、「適用状態トポロジー」ビューで *S-TAP 1* を子として表示します。

非管理対象ユニット

コレクターが中央マネージャーまたは中央マネージャーとして構成されているアグリゲーターにデータをエクスポートする一方で、そのコレクターがその一元管理クラスターの管理対象ユニットとして指定されていない場合、「適用状態トポロジー」ビューでは、コレクターの「全体状況」が「正常性状況が利用できません」として表示されます。コレクターが中央マネージャーの管理対象ユニットとして指定されている場合を除いて、コレクターに関する追加情報は「適用状態トポロジー」ビューでは利用できません。

1 次ホストおよび 2 次ホストにデータをエクスポートするコレクター

1 次ホストと 2 次ホストの両方にデータをエクスポートするようにコレクターが構成されている場合、「適用状態トポロジー」ビューでは 1 次ホストのみ使用されます。

親トピック: 「適用状態」ビュー
関連タスク:
「適用状態」のビューのための中央マネージャーの構成

適用状態ダッシュボード

Guardium デプロイメント全体からのデータが適用状態ダッシュボードにどのように表示されるかについて詳しく説明します。

データ可用性

複数の要因が正常性データの可用性および待ち時間に影響し、またそのデータが適用状態ダッシュボードにどのように表示されるかにも影響します。以下の表に、ダッシュボードに含まれるデータ、トリガー基準、データ待ち時間、およびパージについての情報をまとめます。

表 1. 適用状態ダッシュボードのデータの概要

データ・ソース	情報タイプ	トリガー基準	データ待ち時間	データ・パージ間隔
システム・リソース	システム構成 (CPU コア、システム・メモリー、/var ディスク容量など)	システムが最小要件を満たしていない	ユーザー・インターフェース・サーバーが始動または再始動すると常に更新される	適用外
ユニット使用状況	ユニット使用状況データ (スニファー再始動、MySQL ディスク使用状況、CPU 負荷など)	値がユニット使用状況のしきい値を超える	推奨構成に基づき 1 から 2 時間以内に更新される。詳しくは、ユニット使用状況データ処理の構成を参照してください。	ユニット使用状況データは 60 日後にパージされる スニファーのバッファー使用状況データは 14 日後にパージされる
システム自己モニター	MySQL ディスク使用状況およびシステム・ディスク使用状況	使用量がデフォルトのしきい値以上になる (重大度が「高」では 75%、重大度が「クリティカル」では 90%)	5 から 10 分ごとに更新される 重大度が「高」では、15 分の期間内に同じイベントが複数回発生した場合、最新の発生を反映するようにタイム・スタンプが更新されます。15 分の間隔後に同じイベントが発生した場合、最新のタイム・スタンプを使用して新しいエントリーが作成されます。 「クリティカル」な問題では、イベントが発生するたびに固有のタイム・スタンプを使用してエントリーが作成されます。	重大度が「高」の問題は 7 日後にパージされる 「クリティカル」な問題はパージされない
相関アラート	トリガーされた相関アラート	アラートしきい値に到達する	アラート通知の頻度に基づき更新される。詳しくは、相関アラートを参照してください。	データは 7 日後にパージされる

重要:

- Guardium V10.1.2 以降を実行するシステムからのデータのみが適用状態ダッシュボードに表示されます。
- システムのホスト名を変更すると、元のホスト名に関連付けられている既存のデータは適用状態ダッシュボードに表示されなくなります。
- フェイルオーバー・シナリオ中にプライマリー中央マネージャーがバックアップ中央マネージャーにデータを転送しているとき、最大 30 分、適用状態ダッシュボードでデータが使用不可になります。

データ表示

適用状態ダッシュボードでは、各種タイルまたは小さなウィンドウに類似するコンテナーを通じてデータがフォーマット設定され、表示されます。以下の表に、各ダッシュボード・タイルに表示されるデータをまとめます。

表 2. 適用状態ダッシュボードのタイルの概要

	タイル名

データ・ソース	リソース要件	ユニット使用状況の問題	ユニット使用状況のタイム・チャート	アラート (カテゴリー、名前、重大度、またはシステムによる)	イベント	重大度高	クリティカル
システム・リソース	✔					✔	
ユニット使用状況		✔	✔		✔	✔	
システム自己モニター					✔	✔ (使用量がしきい値である 75% 以上になった場合)	✔ (使用量がしきい値である 90% 以上になった場合)
相関アラート				✔	✔	✔	
次のタイルはデフォルトで表示されます: 「*名前別のアラート*」、「*クリティカルな問題*」、「*イベント・タイムライン*」、「*重大度の高い問題*」、および「*ユニット使用状況の問題*」。							

ダッシュボード・フィルター

ダッシュボード・フィルターを使用すると、Guardium システム、問題の重大度、および期間に基づきデータを素早くフィルタリングできます。フィルター設定は、特に注記がない限り、ダッシュボードのどの部分に表示されるデータにも影響します。

Guardium システム・フィルターを使用すると、ユニット・タイプにより、または「管理」 > 「一元管理」 > 「管理対象ユニット・グループ」で定義されているグループにより、ダッシュボードをフィルタリングできます。

デフォルトでは、ダッシュボードには、発生したすべての問題 (「低」、「中」、「高」、および「クリティカル」) が表示されます。「重大度」メニューを使用すると、ダッシュボードで重大度によりデータをフィルタリングできます。「高」を選択すると、ダッシュボード全体がフィルタリングされ、重大度が高の問題のみが表示されます。「クリティカル」を選択すると、ダッシュボード全体がフィルタリングされ、クリティカルな問題のみが表示されます。「高」と「クリティカル」の両方の問題を選択することもできます。この場合、これらよりも重大度が低いすべてのデータがフィルターにより除外されます。
注意:

- 未処理または未解決のクリティカルな問題は、「重大度」フィルターの設定に関係なく、ダッシュボードに表示されます。
- 「*ユニット使用状況の問題*」タイルでは、ダッシュボードの「重大度」フィルターは、ユニット使用状況の重大度全体に基づきます。ユニット使用状況の重大度が割り当てられる方法について詳しくは、ユニット使用状況の問題を参照してください。

時間フィルターにより、ダッシュボードに表示されるデータの範囲が決まります。デフォルトの設定では、1 時間から 3 週間までの期間を使用できますが、カスタム期間もサポートされています。時間フィルターは、クリティカルな問題には適用されません。クリティカルな問題は、時間フィルターの設定に関係なく常に表示されます。

「グラフの追加」メニューを使用すると、ダッシュボードにタイルを追加することや、以前削除したデフォルトのタイルを元の場所に戻すことができます。

ダッシュボード・サマリー (Dashboard summary)

「ダッシュボード・サマリー (dashboard summary)」には、Guardium デプロイメントで検出された正常性の問題の全体数が表示されます。「問題のあるコレクター」および「問題のあるアグリゲーター」の数は、正常性の問題が検出されたシステム (コレクターおよびアグリゲーター) の数を示します。「クリティカル」および「高」の数は、ダッシュボードに含まれるすべてのシステムで検出された問題の数を示します。
注:

- ダッシュボードに対してタイルを追加または削除しても、「クリティカル」および「高」の数は影響を受けません。
- 「ダッシュボード・サマリー (dashboard summary)」バー上の数は、ダッシュボード・フィルターの設定を反映します。

カテゴリー、名前、重大度、またはシステムによるアラート

適用状態ダッシュボードは、Guardium 相関アラート (「*カテゴリー別のアラート*」、「*名前別のアラート*」、「*重大度別のアラート*」、および「*システム別のアラート*」) に基づく複数のタイルをサポートしています。ダッシュボードに相関アラート・タイルを追加するには、「グラフの追加」メニューを使用します。

相関アラートは、適用状態ダッシュボードに含めるかどうか明示的に構成する必要があります。ダッシュボードのアラートの構成については、「適用状態」のビューのための中央マネージャーの構成を参照してください。

リソース要件

「*リソース要件*」タイルは、Guardium デプロイメント内のシステムが、CPU、メモリー、および /var ディスク容量に関する最小ハードウェア要件を満たしているかどうかを示します。最小要件を満たしていないシステム・リソースは、重大度が高の問題として示され、「*リソース要件*」タイルと「*重大度の高い問題*」タイルの両方に表示されます。

タイルの詳細ビューの「正常なシステムを含める」チェック・ボックスを使用すると、ダッシュボードのフィルター・バーで示されているシステムおよび時間フレームに対して使用できるすべてのデータを含めることができます。「正常なシステムを含める」チェック・ボックスは、ダッシュボード・フィルター全体の「重大度」設定よりも優先され、使用可能なすべてのデータが組み込まれます。正常性の問題が検出されなかったシステムは、デフォルトでは除外されます。

Guardium デプロイメントのリソース要件のうち満たされているものと満たされていないものをすべて表示する表は、「管理」 > 「一元管理」 > 「システム・リソース」でも表示できます。
注:

- システム・リソースの問題は、特定のタイム・スタンプに関連付けられていないため、「*イベント*」タイムラインには表示されません。

ユニット使用状況の問題

「*ユニット使用状況の問題*」タイルには、ユニット使用状況のしきい値に基づいて問題が表示されます。このタイルに表示される問題は、各しきい値を超えた個々のメトリックを表します。指定の期間内に個々のシステムに対して使用可能なすべてのメトリックで検出された問題のうち、最も重大度の高い問題に基づき、全体的な重大度が割り当てられます。ユニット使用状況のしきい値について詳しくは、ユニット使用状況レベルを参照してください。

「*ユニット使用状況の問題*」タイルの詳細ビューには、「期間の開始」時刻と「タイム・スタンプ」の両方が含まれます。

- 「期間の開始」時刻は、「*CM バッファー使用状況モニター*」のデータが時間単位の期間 (例えば、13:00、12:00、および 11:00 に開始される期間) にロールアップされたことを示します。
- 「タイム・スタンプ」は、ユニット使用状況レベルのデータが適用状態ダッシュボードにいつ追加されたかを示します。この追加は、ユニット使用状況レベルのスケジュールに基づき、または「*今すぐ 1 回実行*」を使用することで行われます。

詳しくは、ユニット使用状況データ処理の構成を参照してください。
ユニット使用状況データが適用状態ダッシュボードに初めて追加された時点では、すべてのユニット使用状況データで、「*タイム・スタンプ*」が同じになりますが、「*期間の開始*」時刻は異なります。時間が経過すると、タイム・スタンプはユニット使用状況レベルのスケジュールに基づいた間隔を置いて表示されます。例えば、ユニット使用状況レベルのデータが、正時の 1 時間 40 分後に収集される場合、「*期間の開始*」時刻と「*タイム・スタンプ*」の値は以下のようになります。

表 3. ユニット使用状況の「期間の開始」時刻と「タイム・スタンプ」値の例

期間の開始	タイム・スタンプ
13:00	14:40
12:00	13:40
11:00	12:40

タイルの詳細ビューの「正常なシステムを含める」チェック・ボックスを使用すると、ダッシュボードのフィルター・バーで示されているシステムおよび時間フレームに対して使用できるすべてのデータを含めることができます。「正常なシステムを含める」チェック・ボックスは、ダッシュボード・フィルター全体の「重大度」設定よりも優先され、使用可能なすべてのデータが組み込まれます。正常性の問題が検出されなかったシステムは、デフォルトでは除外されます。

ユニット使用状況のタイム・チャート

「*ユニット使用状況のタイム・チャート*」を使用すると、時間の経過に伴うユニット使用状況データの傾向を監視できます。「*ユニット使用状況のタイム・チャート*」は、単一の Guardium システムに対して複数のユニット使用状況メトリックを表示するように構成したり、複数の Guardium システムに対して単一のユニット使用状況メトリックを表示するように構成したりできます。

「*ユニット使用状況のタイム・チャート*」は、以下の基準に基づいて構造化されます。

- X 軸は、「*期間の開始*」時刻を表します。
- 複数のメトリックがグラフ化され、メトリックの値が同じ範囲内にある場合、Y 軸が 1 つ描画されます。例えば、「*MySQL ディスク使用状況*」と「*/var ディスク使用状況*」はどちらもパーセンテージで表され、同じ Y 軸を使用して描画されます。
- 複数のメトリックがグラフ化され、メトリックの値が類似していない場合、Y 軸が 2 つ描画されます。例えば、「*MySQL ディスク使用状況*」はパーセンテージで表され、「*未解析ログ要求*」は整数で表されるため、2 つの Y 軸 (一方はパーセンテージを表示し、もう一方は整数を表示する) が描画されます。
- メトリックの値が Y 軸の範囲外になった場合、その値はグラフの下部に表示されます。この動作により、類似する単位を使用して異なるメトリックを表す一方で、値が大幅に異なるシナリオ (例えば、千単位の範囲の整数と 100 万単位の範囲の整数) にも対応できます。
  ヒント: 値が大幅に異なる範囲にある場合は、複数のタイム・チャートを作成してください。

注: ダッシュボードのフィルター・バーで指定されている時間フレーム内に、システムに関するユニット使用状況データが存在しない場合、そのシステムは「タイム・チャートの設定」 > 「ホスト名」メニューには含まれません。
親トピック: 「適用状態」ビュー
関連タスク:
「適用状態」のビューのための中央マネージャーの構成
ユニット使用状況データ処理の構成

シナリオ:「適用状態トポロジー」ビューを使用した過負荷システムのトラブルシューティング

このトピックでは、「適用状態トポロジー」ビューを使用して、環境内の過負荷システムを特定し、修正する方法について説明します。

このタスクについて

このシナリオでは、「適用状態トポロジー」ビューから正常性の問題を特定し、根本原因を評価し、さらにその評価と追加データを関連付けた後で、問題を解決し、修正を検証します。ここで説明する例では、過負荷のコレクターを取り上げますが、このプロセスは他のケースにも適用できます。

手順

1. 中央マネージャーで、「管理」 > 「システム・ビュー」 > 「適用状態トポロジー」にナビゲートします。
2. 適用状態トポロジーを確認し、環境内のシステムの全体的な正常性を評価します。 大まかには、アイコンにより、正常なシステムが示され、一方 アイコンおよび アイコンにより、正常性に問題があるシステムが示されます。
3. 状況アイコンまたは 状況アイコンがあるシステムを見つけた場合、そのノードをクリックすると、追加の正常性情報を含むオーバーレイが表示されます。
4. ノードのオーバーレイに表示される情報を使用して、正常性の問題の診断を開始します。例えば、「変数ディスク使用状況」、「再始動」、「アナライザー・キュー」、および「ロガー・キュー」の重大度状況が高または中のコレクターは過負荷となっています。
5. 「適用状態トポロジー」ビューから正常性の問題を最初に評価した後、見つけた内容と追加データの関連付けを試行します。例えば、システムが過負荷となっている疑いがある場合、そのシステムのトラフィックのモニターを開始します。

6. 正常性の根本問題の診断が確定した場合、修正アクションを実行します。この過負荷システムの例では、エンタープライズ・ロード・バランシングを確立することや、S-TAPs を別のコレクターに再割り当てすることができます。 エンタープライズ・ロード・バランシングが既に構成され、使用されている場合、この一連の症状は通常発生しません。
7. 修正アクションを実行した後、ユニット使用状況および中央マネージャーのバッファー使用モニター・データの次回更新に続いて、「適用状態トポロジー」ビューでノードの状況が更新されます。この更新間隔は、ユニット使用状況データの処理のスケジュールによって決まります。

親トピック: 「適用状態」ビュー

デプロイメント・インベントリー

「インベントリー (inventory)」ビューには、すべてのデータベース・サーバーとインストール済みの S-TAP クライアントまたは GIM クライアントの一元管理ビューが表示されます。

親トピック: 一元管理機能の使用

「リソース・デプロイメント」ビュー

「リソース・デプロイメント」ビューには、すべてのデータベース・サーバーと、関連するコレクター、アグリゲーター、および中央マネージャーの一元管理ビューが表示されます。

親トピック: 一元管理機能の使用

管理対象ユニット・グループの作成

管理対象ユニットをグループに編成してから、それらのグループにアクションを実行します。

このタスクについて

管理対象ユニット・グループを使用すると、管理対象ユニットを分かりやすいグループに編成してから、それらのグループにアクションを実行することができます。例えば、特定のユニット・タイプ、地理的位置、または業務別の管理対象ユニット・グループを作成できます。実行するアクションには、管理対象ユニットのグループへのポリシーのインストール、またはパッチもしくは構成の配布などがあります。

手順

1. 「管理」 > 「一元管理」 > 「管理対象ユニット・グループ」にナビゲートします。
2. 「管理対象ユニット・グループ」ページで、  をクリックして新規管理対象ユニット・グループを作成するか、  をクリックして既存のグループを編集します。
3. 「新規管理対象ユニット・グループの作成」ダイアログで、「グループ名」フィールドにグループの名前を入力します。
   推奨: 他の Guardium コンポーネントとの互換性を維持するために、グループ名でスペースや特殊文字は使用しないでください。
4.  アイコンを使用して、グループに組み込む管理対象ユニットを選択します。
5. グループに組み込む管理対象ユニットの選択が完了したら、「保存」ボタンをクリックします。 新しい管理対象ユニット・グループが保存され、「管理対象ユニット・グループ」ページに表示されます。
6. オプションとして、「管理対象ユニット・グループ」ページで、アイコンをクリックして、グループを展開し、その管理対象ユニットを表示します。

タスクの結果

定義後、管理対象ユニット・グループは、「管理」 > 「一元管理」 > 「一元管理」ページから、「管理」 > 「一元管理」 > 「構成プロファイルの配布」ページから、「管理」 > 「一元管理」 > 「エンタープライズ・ロード・バランシング」 > 「S-TAP と管理対象ユニットの関連付け」ツール内の管理対象ユニット・グループとして、および管理対象ユニット・グループが使用されるその他の場所で利用できます。

親トピック: 一元管理機能の使用

管理対象ユニットのモニター

一元管理を使用して管理対象ユニットをモニターします。

管理対象装置をモニターするには次のようにします。

1. admin ユーザーとして、管理対象ユニットの「Guardium® GUI」にログインします。
2. 「レポート」 > 「Guardium 運用レポート」 > 「管理対象ユニット」をクリックして、「管理対象ユニット」を開きます。

「一元管理」ペインの各コンポーネントの説明を、以下の表に示します。

表 1. 管理対象ユニットのモニター

コントロール	記述
「すべて選択」チェック・ボックス	列 1 の陰影付きのエリアにあるこのボックスにマークを付けると、すべての管理対象ユニットが選択されます。
選択をすべて解除	すべての管理対象ユニットをクリアします。
チェック・ボックス	このボックスにマークを付けると、操作対象にするユニットが選択されます。
ユニット情報のリフレッシュ	ユニットの展開ビューに表示されているすべての情報をリフレッシュし、そのユニットに新規要求を発行します。このアクションによって、フル・ユーザー同期サイクルも発生します。

コントロール	記述
ユニットのリブート	ユニットをオペレーティング・システム・レベルでリブートします。デフォルトでは、Guardium ポータルは始動時に開始します。
ユニット・ポータルの再始動	管理対象ユニット上で Guardium アプリケーション・ポータルを再始動します。その後、そのユニットにログインして、Guardium タスク (検査エンジンの定義または削除など) を実行できます。
ユニット SNMP 属性の表示	「SNMP ビューアー 」ペインを別のウィンドウで開きます。「SNMP ビューアー」ペインのリフレッシュ・アイコンをクリックすると、ウィンドウのデータがリフレッシュされます。
ユニット syslog の表示	「syslog ビューアー」を別のウィンドウで開きます。syslog メッセージの最新 64 KB が表示されます。「syslog ビューアー」ペインの「リフレッシュ」アイコンをクリックすると、ウィンドウのデータがリフレッシュされます。
ユニット・ポータルへのショートカット	管理対象ユニット用の Guardium ログイン・ページを、別のブラウザー・ウィンドウで開きます。
ユニット名	管理対象ユニットのホスト名。マウス・ポインターをユニット名の上に置くと、ツールチップに IP アドレスが表示されます。 ユニット上でホスト名が変更された場合、オンライン状況の自動リフレッシュが行われると、中央マネージャーがそのユニットを認識しなくなります。ホスト名が変更された可能性がある場合は、ツールバーの「リフレッシュ」を使用してください。変更されたホスト名を取得し、そのユニットについて表示される現在のオンライン状況とその他の情報を更新します。
オンライン	ユニットがオンラインかどうかを示します。緑のインディケーターが点灯している場合、ユニットはオンラインです。赤いインディケーターが点灯している場合、ユニットはオフラインです。 中央マネージャーは、一元管理構成で指定されたリフレッシュ間隔 (デフォルトは 1 分) でこの状況をリフレッシュします。ユニットへの接続でエラーが発生した場合、ツールチップにエラーの記述が表示されます。管理表のそのユニットのレコードの上にマウス・ポインターを移動してください。
検査エンジン	・アイコンをクリックすると、検査エンジンのリストが展開され、・アイコンをクリックすると、検査エンジンのリストが非表示になります。 ここから、状況に応じて検査エンジンを停止または開始できます。 各検査エンジンについて表示される情報は次のようになります (この情報は、「リフレッシュ」が押されるときに管理対象ユニットから取り出されます。ping のたびに取り出されるのではありません)。 名前 - 検査エンジンの名前 プロトコル- 検査エンジンがモニター対象にするプロトコル: Oracle、MSSQL、Sybase、Informix®、または DB2® 始動時にアクティブ - システムの始動時に検査エンジンが開始するかどうかを示します。 送信元 IP の除外 - 送信元 IP アドレスのリストを除外する (調査しない) かどうかを示します。 送信元 IP/マスク - クライアントの IP アドレスとサブネット・マスクのリスト。検査エンジンがモニターするのは、このクライアントにおける「送信先 IP/マスク」アドレスへのデータベース・トラフィックです。 ポート - データベース・クライアントとサーバーが通信に使用するポート。単一ポート、ポートのリスト、またはポートの範囲の場合があります。 送信先 IP/マスク - サーバーの IP アドレスとサブネット・マスクのリスト。モニター対象となるのは、対応するクライアント・マシン (「送信元 IP/マスク」) からこのサーバーへのトラフィックです。
インストール済みセキュリティー・ポリシー	管理対象ユニット上にインストールされたセキュリティー・ポリシーの名前。このフィールドは ping のたびに更新されます。
モデル	管理対象ユニットの Guardium モデル番号。
バージョン	管理対象ユニットの Guardium バージョン番号。
最終パッチ	最後にインストールされたパッチ。
最終 ping 時刻	中央マネージャーが管理対象ユニットのオンライン/オフライン状況を判断するために、最後にこのユニットが ping された時刻。
選択済みユニット	
グループ・セットアップ	「グループ・セットアップ」を使用すると、グループの保守 (新規グループの作成、グループの削除、および管理対象ユニットのグループへの関連付け) をユーザーが行えるようにする新規ウィンドウが開きます。
登録抹消	選択されたすべてのユニットを登録抹消します。
再始動	
リブート	選択されたユニットをリブートします。
ポータルの再始動	選択されたポータルを再始動します。
検査エンジンの再始動	選択されたユニットの検査エンジンを再始動します。
配布	
リフレッシュ	選択されたユニットをリフレッシュします。
ポリシーのインストール	ポリシー名は、ポリシーの詳細を示す新規ウィンドウを開くリンクになっています。
パッチ配布	「パッチ配布」を押すと新しい画面が開き、使用可能なパッチのリストが従属関係とともに表示されます。さらにそこからパッチを選択し、選択したすべてのユニットにインストールできます。最大 1 年先までのパッチのスケジュールを設定します。

コントロール	記述
アップロードした JAR ファイルの配布	「強化」 > 「脆弱性評価」 > 「カスタム・アップロード」をクリックします。次に、アップロードするファイルの名前を入力します。または、「参照」クリックしてそのファイルを探し、選択します。ドライバーは、1 つずつアップロードしてください。 「アップロード」をクリックします。操作完了時には通知があり、アップロードしたファイルが表示されます。 このアクションによって、アップロードされたファイルが中央マネージャーに移動します。 これらの JAR ファイルの配布対象となる管理対象ユニットのチェック・ボックスを選択します。「アップロードした JAR ファイルの配布」をクリックします。
パッチ・バックアップ設定の配布	この設定により、選択したユニットに以下が配布されます。 PATCH_BACKUP_FLAG; PATCH_AUTOMATIC_RECOVERY_FLAG; PATCH_BACKUP_DEST_HOST; PATCH_BACKUP_DEST_DIR; PATCH_BACKUP_DEST_USER; PATCH_BACKUP_DEST_PASS
認証構成の配布	一元管理認証の配布を受信する管理対象ユニットを選択します。 「認証構成の配布」 をクリックすると、選択したすべての管理対象ユニットに認証構成が配布されます。
構成の配布	以下の構成が配布され、中央マネージャーと管理対象ユニット間でパラメーターが同期します。 • 異常検出 - 始動時にアクティブ、ポーリング間隔 • アラート機能 - すべてのフィールド • データ・アーカイブ - すべてのフィールド • グローバル・プロファイル - 同時ログイン、データ・レベル・セキュリティー、名前付きテンプレート (既に同期済み) 以外のすべてのフィールド、PDF フッター・テキスト、およびロゴ・イメージ • IP からホスト名への別名割り当て - 両方のチェック・ボックス • 結果アーカイブ - すべてのフィールド • 結果エクスポート - すべてのフィールド • セッション推論 - すべてのフィールド • システム・バックアップ - すべてのフィールド • データ・エクスポート - すべてのフィールド 上記の構成のうち一部 (「異常検出」、「セッション推論」) は、ポータルが再始動されるまで有効になりません。「アラート機能」などの他のプロセスは、管理対象ユニットの「管理」ポータルを介して直接再始動するか、または関係のあるすべての管理対象ユニットをマネージャーからリブートすることによって再始動する必要があります。 「構成の配布」 では、管理対象ユニットは再始動しません。再始動する管理対象ユニットごとに別個のアイコンがあります。 「ポータルの再始動」では、選択したすべてのユニットが再始動されます。 配布後に、管理対象ユニットですべての構成を有効にするため、管理対象ユニットを再始動する必要があることを示すメッセージが表示されます。 スケジュール設定が付いている各パラメーターには、第 2 のチェック・ボックスがあります。この第 2 のボックスにチェック・マークを付けると、このパラメーターのスケジュール設定が配布されます。 構成を選択して配布する方法については、『構成の配布』を参照してください。 ポータルのリブートと再始動の比較 アラート機能 「始動時にアクティブ」チェック・ボックス。アプライアンスが再始動するたびに、アラート機能が自動的にアクティブ化されます。 GUI 再始動では「始動時にアクティブ」値は有効になりません。 中央マネージャーから管理対象ユニットへの構成の配布を完全に有効にするため、管理対象ユニットのリブートが必要です。 アラート機能については、admin ポータルを使用して管理対象ユニット上で手動で再始動します (「管理コンソール」/「アラート機能」)。この再始動は Central Manager からはできないので、同じ効果を得るため、「管理コンソール」から管理対象装置を再始動します。 異常検出 「始動時にアクティブ」チェック・ボックス。アプライアンスが再始動するたびに、異常検出が自動的にアクティブ化されます。 GUI 再始動で「始動時にアクティブ」値が有効になります。 中央マネージャーから管理対象ユニットへの構成の配布を完全に有効にするため、管理対象ユニットでポータルの再始動が必要です。 セッション推論

コントロール	記述
	「始動時にアクティブ」チェック・ボックスを使用して、Guardium アプライアンスの開始時にセッション推論を開始します。 GUI 再始動で「始動時にアクティブ」値が有効になります。 中央マネージャーから管理対象ユニットへの構成の配布を完全に有効にするため、管理対象ユニットでポータルの再始動が必要です。 結果エクスポート/システム・バックアップ/データ・アーカイブ/結果アーカイブ/データ・エクスポート 中央マネージャーから管理対象ユニットへの構成の配布を有効にするために、管理対象ユニットでポータルの再始動をする必要ありません。 グローバル・プロファイル 中央マネージャーから管理対象ユニットへの構成の配布を有効にするために、管理対象ユニットでポータルの再始動をする必要はありません (ただし、異なる名前付きテンプレートの使用は、ポリシーがインストールされたときにのみ適用されます)。
新規登録	「ユニット登録」ペインを開いて、管理対象にするユニットを新規登録します。
パッチ・インストール状況	「パッチ・インストール状況」画面には、各ユニットごとの、失敗したインストールと矛盾が表示されます。例えば、あるパッチが、他のユニットでインストールに失敗したか、インストールされなかったかにかかわらず、一部のユニットにのみインストールされている状況です。

中央マネージャーを使用した、個々の管理対象ユニットまたは管理対象ユニット・グループへの相関アラートの割り当て

この新機能は、管理対象環境に対するものです。

中央マネージャーが、個々の管理対象ユニットまたは管理対象ユニット・グループに相関アラートを割り当てることができるようにします。ユニットまたはグループに割り当てるか、ユニットまたはグループから除外することができます。また、中央マネージャー自体で実行するかどうかも指定する必要があります。使用されるグループは管理対象ユニット・グループであり、中央マネージャーのページで使用されるのと同じタイプのグループです。

管理対象環境の中央マネージャーで、アラート・ビルダーには、「管理対象ユニット」用の新しいセクションがあります。このセクションで、アラートに組み込むか、アラートから除外する単一のユニットまたは管理対象ユニットのグループのどちらかを指定します。また、その中央マネージャー自体が組み込まれるか、除外されるかも、チェック・ボックスで指定します。デフォルトの動作は既存の動作と一致します。すなわち、アラートはどこでも実行されます。アラートがどこでも実行されないことを指定する場合、指定する場所でアラートが実行されることを確認してください。UI には、単一ユニットまたはグループの組み込み/除外のための 4 つのオプションが含まれています。また、管理グループのリストから選択し、必要に応じて新規管理グループを作成するか、または既存の管理対象ユニット・グループを編集するためのダイアログも含まれています。

個々の管理対象ユニットで、アラート・ビルダーは管理対象ユニットのセクションを表示しません。中央マネージャーだけがユニットとグループにアラートを割り当てることができます。

所定の管理対象ユニットで「アラート」表にエントリーがある場合、そのユニットの除外元のアラートごとにそのユニットを除外するために、システム生成グループが自動的に作成されます。これが行われるのは、アラートがその管理対象ユニットで開始する場合です。

アラートをローカルで有効/無効にするために、管理コンソールで異常検出ページのアラート・ペインが使用されました。この機能の場合、アラート・ペインは中央マネージャーにのみ表示されます。

管理対象ユニットには、アクティブ・アラートおよびそれらのアクティブ・アラートが有効であるかどうかを示す表示が表示されます。

親トピック: 一元管理機能の使用

管理対象ユニットへのセキュリティー・ポリシーのインストール

管理対象ユニットにセキュリティー・ポリシーをインストールします。

このタスクについて

管理対象ユニットへのセキュリティー・ポリシーのインストール

手順

1. 「設定」 > 「ツールとビュー」 > 「ポリシー・インストール」をクリックして、「現在インストールされているポリシー」と「ポリシー・インストーラー」を開きます。
2. 「ポリシー」リストから、インストールするポリシーを選択します。
3. リストからインストール・アクションの選択をします。インストール・アクションを選択した後、各ポリシーのインストールの成功 (または失敗) が通知されます。選択したユニットを使用できない場合 (オフラインの場合やリンクが停止している場合)、中央マネージャーからそのことが通知されます。最長で 7 日間 (そのユニットが一元管理に登録されている間)、引き続き新しいポリシーのインストールが試みられます。
4. 「ポリシー」リストから、インストールするポリシーを選択します。
5. 使用可能なインストール・アクションには、以下の項目があります。
    a. 「インストールおよびオーバーライド」 - インストール済みのポリシーすべてを削除し、代わりに選択したものをインストールします。
    b. 「最後のインストール」 - 選択したポリシーをシーケンスの最後のものとしてインストールします。すなわち、現在インストールされているすべてのポリシーの後にこのポリシーをインストールし、優先度は最も低いです。

c. 「最初のインストール」- 選択したポリシーをシーケンスの最初のものとしてインストールします。現在インストールされているすべてのポリシーより前に、このポリシーをインストールします。

注: 中央マネージャーからポリシーをインストールする場合、「今すぐ 1 回実行」 (およびスケジューラー) を選択すると、インストール済みポリシー内の既存のグループが更新されます。

ルールの変更 (グループの追加と削除を含む) をロードするには、次のいずれかを行う必要があります。

a. コレクターからのポリシーの初期インストール
b. コレクターまたは中央マネージャーからのポリシーの再インストール

親トピック: 一元管理機能の使用

一元化パッチ管理

パッチのインストール、状況、および履歴を表示可能にし、制御します。

このタスクについて

パッチのインストール、状況、および履歴を表示可能にし、制御します。一元管理クラスターは、Central Manager から管理対象装置にパッチをインストールする機能を備えています。

パッチをインストールするときには、パッチをインストールする時期を示す日時要求を指定できます。日時を入力しない場合、または「now」が入力された場合、インストール要求時間は「今すぐ」です。

注: 正常にインストールされているパッチを再インストールできます。これは、バッチ処理の対象となるパッチに対して重要です。パッチが既にインストールされている場合は、警告で通知されます。

管理者ユーザーとして、管理対象ユニットの「Guardium® GUI」にログインします。

手順

1. 「管理」 > 「一元管理」 > 「一元管理」をクリックします。
2. パッチが必要なユニットを選択し、「パッチ配布」をクリックします。
3. 「パッチ配布」画面から、配布するパッチを選択し、「今すぐパッチをインストール」または「パッチのスケジュールを設定」をクリックします。
4. インストールの状況を確認するには、「管理」 > 「一元管理」 > 「一元管理」をクリックし、ユニットを選択し、「パッチ・インストール状況」をクリックします。「パッチ・インストール状況」画面には、各ユニットごとの、失敗したインストールと矛盾が表示されます。例えば、あるパッチが、他のユニットでインストールに失敗したか、インストールされなかったかにかかわらず、一部のユニットにのみインストールされている状況です。「パッチ配布」画面からパッチを削除するには、パッチの横の削除アイコン (赤色の x) をクリックします。これにより、アプライアンスのパッチ配布ディレクトリーからはパッチは削除されませんが、表示からは削除されます。

親トピック: 一元管理機能の使用

構成プロファイルの処理

構成プロファイルにより、中央マネージャーから構成設定およびスケジューリング設定を定義して、中央マネージャー自体の構成を変更することなく、それらの設定を管理対象ユニット・グループに配布することができます。

始める前に

構成プロファイルを作成し、配布する前に、以下の前提条件を確認してください。

- 中央マネージャーとその管理対象ユニット間のポート 8447 を介した通信を許可します
- 中央マネージャーと、構成を受け取る管理対象ユニットは、Guardium V10.1 以上でなければなりません

このタスクについて

構成プロファイルには、構成設定とスケジューリング設定の 1 つ以上のセットと、構成設定とスケジューリング設定で更新される管理対象ユニット・グループのリストという 2 つのタイプの情報が含まれています。構成プロファイルは、定義した後、保管および変更して、構成設定とスケジューリング設定の特定のセットを特定の管理対象ユニット・グループに配布するために再使用することができます。

構成プロファイルは、中央マネージャーのローカル設定とは無関係に定義されます。 そのため、中央マネージャーの構成を中断したり、管理対象ユニットを個別に構成する必要なしに、構成設定を素早く定義し、その設定を管理対象ユニット・グループにデプロイすることができます。

この作業では、構成プロファイルの作成、配布、および保存の方法を説明します。

手順

1. 「管理」 > 「一元管理」 > 「構成プロファイルの配布」にナビゲートします。
2. をクリックするか、既存のプロファイルを選択して、構成プロファイルの処理を開始します。
3. 「名前および記述」パネルで、プロファイルの名前、およびオプションで記述を指定します。「次へ」をクリックして先に進みます。
   オプション: 「ロール」ボタンをクリックして、構成プロファイルを使用できるセキュリティー・ロールを指定します。
4. 「配布対象」パネルで、をクリックして新規構成を定義するか、既存の構成を選択し、をクリックして編集します。
   a. 「構成タイプ」メニューで、構成タイプを選択してプロファイルを追加します。
   b. 選択した構成タイプの構成とスケジューリングの詳細を指定します。 構成設定について詳しくは、定義している構成タイプの製品資料を参照してください。

制約事項: データ・エクスポート構成設定をアグリゲーターに配布しても、パージ設定は配布されません。アグリゲーター上の既存のパージ設定が保持されます。保存期間を含めて、パージ設定は、コレクターに配布され、コレクター上の既存のパージ設定を置き換えます。

c. 「保存」をクリックして、構成詳細の編集を終了します。

必要に応じて、構成の追加または編集を続行します。「次へ」をクリックして先に進みます。

5. 「配布場所」パネルで、「管理対象ユニット・グループ」表からグループを選択して、  アイコンを使用して、グループを「選択されたグループ」表に追加します。「次へ」をクリックして先に進みます。

注:  をクリックして新規管理対象ユニット・グループを作成するか、  をクリックして既存のグループを編集します。「管理」 > 「一元管理」 > 「管理対象ユニット・グループ」を選択して、管理対象ユニット・グループを定義および編集することもできます。

6. 「構成の配布」パネルで、「今すぐ実行する」をクリックして、選択したグループに構成プロファイルを配布します。 配布が完了したことを状況が示している場合、「次へ」をクリックして続行します。
7. 「結果のレビュー」パネルで、配布プロセスとその結果の概要を確認します。
   オプション: 配布プロセスの詳しいログを参照する場合は、「実行ログ」をクリックします。
8. 再使用するために構成プロファイルを保存する場合は、「保存」をクリックします。

次のタスク

構成プロファイルを中央マネージャー間で移動する必要がある場合は、「管理」 > 「データ管理」 > 「定義のエクスポート」および「管理」 > 「データ管理」 > 「定義のインポート」を使用して、「タイプ」メニューから「構成プロファイル」を選択します。

親トピック: 一元管理機能の使用

関連概念:

統合

アラート機能の構成

定義のエクスポート/インポート

IP からホスト名への別名割り当て

スケジューリング

構成の配布

構成、ならびにそのスケジュールは、全体またはその一部を、中央マネージャーと管理対象ユニットの間で配布することができます。

手順

1. 構成を受け取る管理対象ユニットを「選択」します。
2. 「構成の配布」をクリックして、「構成の配布」ウィンドウを表示します。
3. 配布する「構成」に対応するボックスにチェック・マークを付けます。 ヘッダーにあるチェック・ボックスを使用すれば、すべての構成が選択されます。
4. 配布する「スケジュール」に対応するボックスにチェック・マークを付けます。 ヘッダーにあるチェック・ボックスを使用すれば、すべてのスケジュールが選択されます。構成がスケジュールされていない場合は、チェック・ボックスが表示されず、代わりに「適用外」が表示されます。
5. 「配布」をクリックし、構成とスケジュールを配布します。
6. オプション: 配布を中止するには、「キャンセル」をクリックします。

タスクの結果

コマンドを使用する場合は、「一元管理」 > 「構成の配布」 > 「グローバル・プロファイル」をクリックすると、以下の値が配布されます。

- ACTIVATE_ALIASES
- CUSTOM_DB_MAX_SIZE
- CHECK_CONCURRENT_LOGIN
- HTML_BOTTOM_RIGHT
- HTML_BOTTOM_LEFT
- DISPLAY_LOGIN_MESSAGE
- LOGIN_MESSAGE
- CSV_DELIMETER
- FILTERING_ENABLED
- INCLUDE_CHILDREN_ON_FILTER
- SHOW_ALL_RECORDS
- ACCORDION_DISABLED
- SCHEDULER_RESTART_INTERVAL
- SCHEDULER_RESTART_WAIT_SHUTDOWN
- ESCALATE_TO_ALL
- MESSAGE_TEMPLATE

親トピック: 一元管理機能の使用

認証構成の配布

各アプライアンスで別個に認証を構成する代わりに、中央マネージャー上で一元管理認証 (認証の構成) を 1 回構成し、それからすべての管理対象ユニットに配布することができます。このようにすると、情報の入力を 1 回行うことで、その情報を一部またはすべてのユニットに適用することができます。一部のユニットで異なるタイプの認証を使用することもできます。

手順

1. 認証 (認証の構成) を中央マネージャーと管理対象ユニットの両方で確実に実行します。LDAP 認証を使用している場合、LDAP が中央マネージャー上と管理対象ユニットの両方で構成されていることを確認します。
2. 一元管理認証の配布を受信する管理対象ユニットを選択します。

3. 「認証構成の配布」 をクリックすると、選択したすべての管理対象ユニットに認証構成が配布されます。

親トピック: 一元管理機能の使用

予備の中央マネージャー

予備の中央マネージャーまたはバックアップ中央マネージャー (CM) を使用して、プライマリー CM が使用不可になった場合に備えてセカンダリー CM またはバックアップ CM を構成します。

予備の中央マネージャーでは、以下の機能がサポートされています。

1. バックアップ中央マネージャー - プライマリー中央マネージャーの接続が切断されると、「プライマリー CM に設定」リンクが使用可能になります。
2. ユーザー・レイアウトが保持されます。
3. ユーザーおよびロールは同期バックアップに含まれており、ポータル・ユーザー同期に依存しません。
4. ユーザー・グループのロール・データが保持されます。
5. GuardAPI 関数 make_primary_cm が追加され、中央マネージャーへの切り替えを CLI から実行できるようになっています。
6. プライマリー中央マネージャーからバックアップ中央マネージャーへの切り替え後に、監査プロセス・ビルダーのプロセスからのデータが保持されます。
7. 一元管理バックアップには、以前と同様、すべての定義 (レポート、照会、アラート、ポリシー、監査プロセスなど)、ユーザー、およびロールが含まれます。
8. バックアップ対象に、エンタープライズ・レポート、配布レポート、および LDAP のスケジュールが含まれます。
9. バックアップ対象に、すべての監査プロセスのスケジュール、およびデータ管理プロセス (アーカイブ、エクスポート、バックアップ、インポートなど) のスケジュールと設定が含まれます。
10. バックアップ対象に、アラート機能および送信者の設定が含まれます。
11. ユーザーの GUI カスタマイズ、カスタム・クラス、およびアップロードされた JDBC ドライバーが含まれます。

注: データ (収集されたデータ、監査結果のデータ、およびカスタム表のデータなど) は含まれません。
注:

バックアップ CM 上の cm_sync_file の状況をリストするには、CLI コマンド show local_cm_sync_file を使用します。各管理対象ユニットのバックアップ CM IP の値をリストするには、GuardAPI コマンド grdapi show_backup_cm_ip を使用します (この API コマンドを実行できるのは、中央マネージャー上のみです)。

注: 中央マネージャーのロード・バランシングを伴うフェイルオーバー - フェイルオーバー後に新しい管理対象ユニットが接続してすぐに切断すると、フェイルオーバー・メッセージが受信されるまで、正しい DB_USER が送信されません。

開発サーバーまたはセカンダリー・サーバーで以下の手順を実行して、テストを行ってください。正常に動作した場合は、プライマリー (稼働中の) Guardium サーバーで以下の手順を実行してください。

中央マネージャーへのパッチのインストール

1. 現在のプライマリー CM から、CLI としてログインします。
2. CLI コマンド store system patch install scp を使用して、パッチをインストールします。
3. この CLI コマンドにより、Guardium サーバーにファイルがコピーされ、これらのファイルをインストールできるようになります。
4. CLI コマンド show system patch install を使用して、これらのパッチのインストール状況を監視します。
5. 両方のパッチのパッチ状況が「DONE: Patch installation Succeeded.」と表示されるまで待機します。

バックアップ CM へのパッチのインストール

1. 現在のプライマリー CM GUI に admin としてログインします。
2. 「設定」>「ツールとビュー」を選択し、次に「中央マネージャー」を選択します。
3. 中央マネージャー上にあるバックアップ CM 管理対象ユニットのチェック・ボックスをクリックします。
4. 「パッチ配布」をクリックし、前の手順でプライマリー CM にインストールしたすべてのパッチをインストールします。

パッチのインストールの例

1. 「パッチ配布」をクリックします。
2. 「今すぐパッチをインストール」をクリックします。
3. パッチがすべての管理対象サーバーに確実にインストールされるまで、約 15 分間、待機します。
4. 確認のために、バックアップ CM に CLI としてログインし、バックアップ CM サーバーから CLI コマンド show system patch install を実行します。

その他すべての管理対象サーバーへのパッチのインストール (オプションの手順)

1. 上記の手順を繰り返して、すべての管理対象サーバーにパッチをインストールします。
2. 次の手順に進む前に、すべてのパッチがインストールされていることを確認します。

すべてのパッチが CM および管理対象サーバーにインストールされた後の手順

1. 現在のプライマリー CM に admin としてログインします。
2. 「設定」>「ツールとビュー」を選択し、次に「中央マネージャー」を選択します。「バックアップ CM の指定」をクリックします。
3. 返された適格なバックアップ CM 候補のリストから、バックアップ CM サーバーを選択します。
4. 「適用」をクリックします。
5. バックアップ CM が同期化されて、新規バックアップ CM ファイルが作成され、バックアップ CM にコピーされるまで、約 2 分間、待機します。
6. 2 つのバックアップ CM 同期ファイルについて、バックアップのすべての処理が 2 回完了するまで (約 1 時間) 待機します。これらのファイルは、バックアップ CM にコピーされ、「Guardium モニター」タブの「統合/アーカイブ・ログ」レポートに表示されます。
7. バックアップ CM 同期ファイルの作成の進行状況を表示するには、「Guardium モニター」を選択し、「統合/アーカイブ・ログ」レポートを選択します。
8. アクティビティー・バックアップが開始され、「統合/アーカイブ・ログ」レポートから cm_sync_file.tgz ファイルが作成されたことを確認します。
    a. GUI から管理者としてログインします。
    b. 「Guardium モニター」タブを選択します。
    c. 「統合/アーカイブ」レポートを選択します。
    d. バックアップ・タイプを探します。
9. 完了すると、以下の状態になります。
    a. パッチが CM にインストールされています。
    b. パッチがバックアップ CM にインストールされています。
    c. オプション: パッチが他のすべての管理対象ユニットにインストールされています。
    d. 2 つのバックアップ CM 同期ファイルが作成されています (「Guardium モニター」タブの「統合/アーカイブ・ログ」ファイルを参照)。
    e. 以下の手順では、現在のプライマリー CM とその管理対象ノードをバックアップ CM に変換するプロセスの概要を示します。

注:

- 重要: バックアップ CM をサポートする 2 つのバックアップ CM 同期ファイルの処理が確実に完了するまで、約 1 時間、待機してください。
- バックアップ CM 同期ファイルのバックアップ・スケジュールは、約 30 分ごとです。
- バックアップ CM ファイルを作成し、そのファイルをバックアップ CM 上のディレクトリーにコピーするためのプロセスが、CM で実行されます。

2 つの同期ファイルの処理が完了した後のバックアップ CM プロセスの開始

プライマリー CM Guardium サーバーをシャットダウンします。

プライマリー CM をシャットダウンするためのアクセス権限がない場合は、バックアップ CM に直接移動して、admin としてログインし (「設定」>「ツールとビュー」を選択し、次に「一元管理」を選択)、「プライマリー CM に設定」をクリックします。本資料のセクション『バックアップ CM をプライマリー CM にするための構成を開始するための手順』にスキップします。

1. 約 5 分間待機し、バックアップ CM の GUI に admin として再度ログインします。
2. プライマリー CM が完全にシャットダウンされたら、次のステップに進むことができます。

注:

プライマリー CM にログインしているときに、そのプライマリー CM がシャットダウンされた場合は、接続がタイムアウトになったことを示すメッセージが表示されます。

バックアップ CM をプライマリー CM にするための構成を開始するための手順

セカンダリー CM は、約 5 分間、応答できない状態になります。5 分後にログインすると、「プライマリー CM に設定」リンクが使用可能になります。このリンクは、admin としてログインし、「設定」>「ツールとビュー」>「一元管理」を選択すると使用可能になります。

1. プライマリー・サーバーがシャットダウンされると、バックアップ CM に「リモート・マネージャーに接続できません。(バックアップ CM の名前) への切り替えを検討してください」というメッセージが表示されます。
2. 切り替えを行う場合は、以下の手順を実行します。
    a. 管理者としてログインします
    b. 「設定」>「ツールとビュー」を選択します。
    c. 「プライマリー CM に設定」をクリックします (「プライマリー CM に設定」リンクは複数回クリックしないでください。また、このプロセスの実行中は、この画面から移動せず、他のオプションを選択しないでください。このプロセスの進行状況と完了を確認できるログ・ファイルが作成されます)。このプロセスの完了にはしばらく時間がかかります。安全防護策として、このボタンを複数回クリックしてしまっても、現在のプロセスには変更が加えられないようになっています。
    d. 数秒後に、「このユニットをプライマリー CM にしてよろしいですか?」というメッセージが表示されます。「OK」をクリックします。
    e. さらに数秒後に、「数分の時間がかかる場合があります」というメッセージが表示されます。バックアップ CM がプライマリー CM になるために要する時間は、バックアップ CM 同期ファイルからバックアップされるデータの量、およびプライマリー CM になるバックアップ CM への切り替えを行う管理対象ノードの総数によって異なります。「OK」をクリックします。

「OK」をクリックすると、load_secondary_cm_sync_file.log というログ・ファイルが直ちに作成されます。このファイルを使用すると、切り替えの進行状況から、バックアップ CM への切り替えプロセスの完了に至るまでを確認できます。このファイルは GUI から表示できます。以降の手順では、このログ・ファイルを表示するための方法を示します。

f. 最後のメッセージが画面に表示されるまでには、しばらく時間がかかります。これが、バックアップ CM への切り替えが完了する前の最後のメッセージになります。そのメッセージは、「GUI は今すぐ再始動されます。数分後に再度ログインすると、バックアップ CM がプライマリー CM になります」です。「OK」をクリックします。

バックアップ CM がプライマリーになり、すべての管理対象ノードが新規プライマリー CM への切り替えを完了するまで、数分間待機します。

CM バックアップ・プロセスの実行中 – 進行状況ログ・ファイルの表示

「プライマリー CM に設定」プロセスの実行中に、バックアップ CM から以下の手順を実行して、バックアップ CM がプライマリー CM になるまでの進行状況を確認することができます。

前提条件: ログ・ファイルを表示するには、接続先サーバーの IP が必要です。

1. バックアップ CM サーバーで Putty.exe セッションから CLI としてログインします。
2. CLI から、「Fileserver <IP> (IP 番号を入力) 3600」を実行します (例: fileserver 9.70.32.122 3600)。
3. GUI から、値 http://yourserver.x.x.x.com を入力します (コマンドの入力後に CLI 画面に表示されます)。例: http://joe.server.guardium.com (サーバー名はバックアップ CM サーバー)

   UI で、ファイルを選択するためのファイル・サーバー・ウィンドウが開きます。Sqlguard ログを選択します。
4. ファイル load_secondary_cm_sync_file.log を選択します (このファイルは、ステップ 3 のファイル・リストに表示されます)。これにより、バックアップ CM がプライマリー CM になるまでの進行状況を確認できるようになります。

   表示するログ・ファイルを探します。

   load_secondary_cm_sync_file.log に以下の行が表示されたら、CM バックアップ・プロセスは完了です。

   Import CM sync info - DONE
5. すべての管理対象ユニットが新規プライマリー CM から使用可能になるまで、約 10 分間待機します。

バックアップ CM がプライマリーになり、すべての管理対象ノードがバックアップ CM サーバーによって管理されるようになった後の手順

これで、以前の CM サーバーを起動できるようになります。以前のサーバーを稼働させたら、以下の手順を実行して、このサーバーをバックアップ CM サーバーとして追加します。

1. 以前のプライマリー CM をリブートします。
2. サーバーが起動したら、CLI としてログインします。
3. マネージャー・ユニット・タイプを削除します。delete unit type manager と入力します。
4. 完了すると、CLI から OK メッセージが表示されます。
5. 非常に重要: deleted unit type で成功メッセージと GUI 再始動メッセージが表示された後も、GUI が完全に再始動するまで約 5 分間待機してください。
6. 5 分経過したら、新規プライマリー CM にログインして、以前の CM を管理対象ユニットとして登録します。
7. 新規プライマリー CM に admin としてログインします。
8. 「設定」>「ツールとビュー」>「一元管理」を選択します。
9. 「新規登録」をクリックします。
10. 前のステップでリブートした以前のプライマリー CM の IP を入力します。
11. ポートとして 8443 と入力します。
12. 「保存」をクリックします。(重要: このボタンを 2 回クリックしないように注意してください。)
13. 以前のプライマリー CM が登録されるまで、しばらく待機します。
14. 以前のプライマリー CM を新規バックアップ CM に設定します。
15. 「バックアップ CM の指定」をクリックします。
16. 以前のプライマリー CM サーバーをクリックします。
17. 「適用」をクリックします。
18. これで、以前のプライマリー CM サーバーが新規バックアップ CM サーバーに設定されました。
19. 「一元管理」画面をリフレッシュすると、新規ユニット・タイプの「バックアップ CM」が定義されていることを確認できます。
20. これで、このタスクは完了です。

バックアップ CM プロセスの完了後のレポート・データ

バックアップ CM プロセスの完了後に以下のデータが欠落します。これは、プライマリー CM からセカンダリー CM への「初回」の切り替えにのみ関連します。

欠落データ:

1. 監査プロセスの結果
2. カスタム表データ
3. カスタム・レポート・データ
4. VA 結果
5. 分類結果
6. DSD 結果
7. CAS 結果
8. データマート・データ
9. 収集済みデータ
10. 資格データ

新規プライマリー CM でこれらのレポートを再実行した後、レポートにデータが再追加されます。旧プライマリー CM に切り替えると、これらのレポートのデータが表示されます。

親トピック: 一元管理機能の使用

調査センター

調査センターは統合サーバーの拡張機能です。 調査ユーザーは (一度定義されると) 選択した履歴日付のデータおよび結果をリストアし、フォレンジック調査を実行できます。 日にち (日付) をリストアしたら、調査ユーザーは標準の Guardium® UI を使用して、調査対象日付の範囲だけのレポートを定義し、表示できます。

各 Guardium アプライアンスは、アーカイブされたすべてのデータおよび結果のカタログを保持します。 このカタログにはアーカイブ、アーカイブのロケーション、およびそれらにアクセスするための資格情報についての情報が含まれています。 統合プロセスの一環として、カタログはコレクターからエクスポートされ、統合サーバーの完全なカタログにマージされます。 カタログが整っていれば、調査ユーザーはリストアのために希望する日付を選択することができ、これらの日付は自動的に調査センターにアップロードされてその調査ユーザーのビューにマージされます。 統合サーバーを通じてコレクターのカタログをマージするほかに、「設定」>「ツールとビュー」からカタログをエクスポートおよびインポートすることもできます。

ユーザーおよびロール

Guardium 統合サーバーには特別の調査ロール (inv) があります。inv ロールを持つユーザーは、履歴データに対してフォレンジック調査を実行することができます。

調査ユーザーは、大部分において、他のユーザーが使用するのと同じ照会定義およびレポート定義を利用します。 最大の違いは、調査ユーザーは自分の調査データベース用に選択したデータのみを表示することです (1 つの INV データベースを共用するように複数の調査機能を構成できます)。選択したデータはアーカイブからリストアできます。または、まだパージされていないデータの場合は現在のデータベースから表示できます。 調査ユーザーは、アーカイブされた監査プロセスの結果もリストア、および表示できます。

注意: ロール inv は、ユーザーを別の調査専用内部データベースに接続できる特別のロールです。 これはロール user と組み合わせる必要があり、一般に他のすべてのロールとは両立しません。

注: 調査ユーザーを正しく構成するには、ユーザーの姓を 3 つの調査データベース (「INV_1」、「INV_2」、または「INV_3」) のいずれかの名前に設定する必要があります (大/小文字の区別あり)。

調査ユーザーを作成するとき、使用する調査データベースにユーザー名が対応するよう、または使用する調査データベースを表す表記がユーザー名に含まれるようにすることをお勧めします。例えば、ユーザーが INV_1 データベースを使用する場合、ユーザー名を「john1」や「inv1」のようにします。

注: 「随時監査プロセスを実行」ボタンは、調査 (INV) ユーザーを除くすべてのユーザーが、すべてのレポート画面で使用できます。

監査プロセスおよび INV ロール

ユーザーが INV の場合は、監査プロセス・ファインダーがロールと所有権に従って監査プロセスを表示しますが、INV に所有されていないすべての監査プロセスについては、「コピー」または「新規」のみが許可されます。

ユーザーが INV の場合、監査プロセス定義メニュー画面では次のことが許可されます。

- 調査ユーザーおよび/または特定の E メール・アドレスのみが受信者として許可されます (INV 以外の通常ユーザー、グループ、ロールは受信者として許可されません)。
- 保存されたレポート監査タスク内の「イベントおよび追加列」ボタンは常に使用不可に設定されます。 いずれの API 自動化も指定できません。
- スケジュールは指定できません。INV データに対する監査プロセスは、「今すぐ実行する」ボタンを使用して手動でのみ実行できます。
- タイプが「レポート」の監査タスクのみ許可されます。
- 「アクティブ」は使用できません。「日数の保持」および「実行の保持」フィールドも使用できません。

ユーザーが INV でない場合、監査プロセス・ファインダーは (割り当てられたロールにかかわらず) 調査ユーザーが所有するどの監査プロセスも表示しません。

監査プロセスが INV のデータに対して実行されるときには、結果のタイトルの後ろに「Executed on Investigation center by」という言葉と INV ユーザーの名前が付きます。

結果には、実行時に調査データベースにデータがマウントされた日付とマウントされたデータのソース・ホストを指定したコメントが付けられます。

この結果は監査プロセス・ビルダーから、または結果のナビゲーション・リストで表示できます。

調査センターに対して実行された監査の結果はアーカイブできず、結果は調査データが破棄されるときに破棄されます。

調査コンテキスト

Guardium の調査センターは、並行して 1 から 3 つの調査期間 (INV_1、INV_2、および INV_3 と呼ばれる) をサポートします。これらはそれぞれ別々の履歴データを保持することができ、その期間のフォレンジック調査の手段を提供します。調査ユーザーを作成する際に、そのユーザーを調査データベースの 1 つと関連付けるためには、ユーザーの姓を INV_1、INV_2、または INV_3 のいずれかにする必要があります。 調査ユーザーの 1 人を使用して調査センターにログインすると、選択した調査期間がラベルに示されます。

GUI

調査ロールを持つユーザーには、調査センター固有の 2 つの追加のタブが表示されます。

- 「監査」タブでは、リストアされた監査プロセスの結果にアクセスできます。
- 「ボリューム管理」タブでは、ユーザーが調査期間を設定または変更したり、リストアする監査プロセスの結果を選択したり、調査の終了時にデータを破棄することができます。

調査センターの処理

- 調査期間のリストア
- 監査結果のリストア
- リストア・ログの表示
- リストアされた監査結果の表示

調査期間のリストア

inv ロールを持つユーザーとして Guardium インターフェースにログインした後で、以下を行います。

1. 「管理」 > 「データ管理」 > 「データのリストア」をクリックして、「データのリストアの検索条件 (Data Restore Search Criteria)」を開きます。
2. C
3. 「データのリストア」をクリックして、「リストアされたデータ」パネルを開きます。前にリストアを実行していた場合は、現在マウントされている、使用中のデータ期間がこのパネルに表示されます。 この時点で、「データの破棄」をクリックすると、以前にマウントされたすべてのデータ期間をアンマウントできます。
4. 「調査期間の再選択」をクリックして、「データのリストア検索基準」パネルを開きます。
5. 検索する開始期間について、開始日を「開始日:」ボックスに入力します。
6. 検索する終了期間について、終了日を「終了日:」ボックスに入力します。
7. 結果セットをホスト名でフィルター処理できるように、オプションで「ホスト名」を入力します。
8. 「検索」をクリックして、結果セットを表示します。これにより、検索基準に一致するすべてのアーカイブのカタログが検索されます。
9. 生成された結果セットから、リストアする期間の「選択」ボックスにチェック・マークを付けます。選択処理を速めるために、「すべて選択」または「選択をすべて解除」をクリックすることもできます。
10. 選択した期間を復元するには、「復元」をクリックします。リストアする期間の数、およびデータ・セットがシステムに対してローカルであるかどうかによって、リストア・プロセスに時間がかかることがあります。
11. リストア・プロセスの進行状況は「リストア・ログの表示」パネルでチェックできます。

注: 調査センターへリストアされた任意の日付のデータで、それがマージ期間に入っている場合、そのデータは Guardium アプリケーション・データベースにもマージされ、inv ユーザー以外のユーザーにも見ることができます。

監査結果のリストア

「監査プロセス・ビルダー」チェック・ボックスで、プロセスの結果をアーカイブするかどうかを指定できます。 すべての署名者によって署名されており、アーカイブのチェック・マークが付けられたプロセスの結果のみがアーカイブされます。 特定の実行の結果は圧縮され、zip されて保管され、ロケーションはカタログに記録され、監査結果のリストアで選択とリストアの際に使用されます。 Guardium 監査プロセスからアーカイブされた結果は、調査センターへリストアされますが、これには結果、ビュー、サインオフ証跡とならんで、これらの結果に関連付けられたコメントが含まれます。

inv ロールを持つユーザーとして Guardium インターフェースにログインした後で、以下を行います。

1. 「ボリューム管理」タブをクリックします。
2. 「監査結果のリストア」をクリックして、「リストアされた結果」パネルを開きます。前にリストアを実行していた場合は、現在リストアされている、使用中の結果がこのパネルに表示されます。 この時点で、「データの破棄」をクリックすると、以前にマウントされたすべての結果をアンマウントできます。
3. 「監査結果のリストア」をクリックして、「結果リストアの検索条件 (Results Restore Search Criteria)」パネルを開きます。
4. 検索する開始期間について、開始日を「開始日:」ボックスに入力します。
5. 検索する終了期間について、終了日を「終了日:」ボックスに入力します。
6. 結果セットをフィルター処理できるように、オプションで「ホスト名」、「監査プロセス」、または「実行番号」を入力します。
7. 「検索」をクリックし、結果セットを表示します。
8. 作成された結果セットから、リストアする結果の「選択」ボックスにチェック・マークを付けます。 選択処理を速めるために、「すべて選択」または「選択をすべて解除」をクリックすることもできます。
9. 選択した結果を復元するには、「復元」をクリックします。リストアする結果の数、およびデータ・セットがシステムに対してローカルであるかどうかによって、リストア・プロセスに時間がかかることがあります。
10. リストア・プロセスの進行状況は「リストア・ログの表示」でチェックできます。

リストア・ログの表示

リストア・ログは、過去のアーカイブ/リストアと、現在ログインしているユーザーの現在のリストアの試行およびフィルター処理を表示します。 このログにより、ユーザーはデータと監査結果の両方について、正常にリストアが行われたかどうかを確認できます。

inv ロールを持つユーザーとして Guardium インターフェースにログインした後で、「リストアのログ」をクリックして「マイ・リストア・ログ」を開きます。このパネルから、すべてのリストアの試行の状態を見ることができます。

リストアされた監査結果の表示

inv ロールを持つユーザーとして Guardium インターフェースにログインした後で、以下を行います。

1. 「監査」タブをクリックします。
2. 「結果のナビゲーション」リンクをクリックして、「監査プロセス・ファインダー」パネルを開きます。
3. 監査プロセスがある場合は、ドロップダウン・リストからプロセスを選択します。
4. 「表示」をクリックして、別のウィンドウを開き、使用可能なレポートを表示して監査結果を確認します。

親トピック: 統合および一元管理

Guardium システムの管理

管理タスクには、システムの正常性のモニターや、グループ、ドメイン、通知などの成果物の管理が含まれます。

- Guardium の管理
  Guardium® 管理者は、各種の管理およびメンテナンス・タスクを行います。
- 証明書
  機能が失われないように、証明書を定期的に確認してください。 新しい証明書を入手してインストールするには、CLI コマンドを使用します。
- ユニット使用状況レベル
  Guardium 環境内の頻繁に使用されているシステムとあまり使用されていないシステムを特定するには、ユニット使用状況レポートを使用します。
- カスタム・アップロード
  データベース・アクティビティー・モニター・コンテンツ・サブスクリプション (旧称は、データベース保護サブスクリプション・サービス)は、事前定義アセスメント・テスト、SQL ベースのテスト、CVE、APAR、およびグループ (データベース・バージョンやパッチなど) の保守をサポートしています。
- 「サービス状況 (Services Status)」パネル
  「サービス状況 (Services Status)」パネルは、CAS やアラート機能などのサービスの状況を確認して、必要な場合には各サービスをさらに調査するための、一元管理された場所です。「設定」 > 「ツールとビュー」 > 「サービス状況 (Services Status)」をクリックして、「サービス状況 (Services Status)」パネルを開きます。「サービス状況 (Services Status)」パネルが開かれるたびに、各サービスの状況が最新表示されます。
- アーカイブ、パージおよびリストア
  アーカイブおよびパージ操作は、スケジュールに基づいて実行する必要があります。 キャプチャーされた情報を監査のために保管するには、「データ・アーカイブ」と「結果アーカイブ」を使用します。このトピックの終わりで、Guardium での Amazon S3 へのアーカイブおよびバックアップについても説明しています。
- Guardium カタログ
  Guardium システムからデータをアーカイブすると、Guardium カタログは、すべてのアーカイブ・ファイルの送信先を追跡して、そのファイルを取得およびリストアできるようにします。
- バックアップとアーカイブの管理方法
  データを保持する方法を確立し、アクティビティー・ボリュームの制御を行い、データのアーカイブとパージのスケジューリングと、毎月のバックアップのスケジューリングを管理します。
- 結果のエクスポート (CSV、CEF、PDF)
  CSV、CEF、および PDF ファイルをワークフロー・プロセスで作成できます。この機能で、Guardium システム上に存在するこれらのファイルをすべてエクスポートします。
- 定義のエクスポート/インポート
  要件が同じまたは同じようなシステムが複数あり、一元管理を使用していない場合は、これらのシステムのソフトウェア・リリース・レベルが同じであれば、必要なコンポーネントを 1 つのシステムで定義し、その定義を他のシステムにエクスポートできます。
- 分散インターフェース
  この構成画面は、分散インターフェースを定義し、プロトコル・バッファー (.proto) ファイルを DIST_INT データベースにアップロードするために使用します。
- カスタム・クラスの管理
  アラートまたは評価で使用されるカスタム・クラスをアップロードして保守します。 カスタム・クラスを管理するには、「設定」 > 「カスタム・クラス」をクリックします。
- 鍵ファイルのアップロード
  まれなケースですが、暗号化 SQL Server トラフィックをモニターするために、Microsoft SQL Server の鍵ファイルを Guardium システムにアップロードしなければならない場合があります。
- SSH 公開鍵
  この情報を使用して、SSH 公開鍵を作成、変更、または削除します。
- ブラウザーの SSL 証明書チャレンジを回避するためのアプライアンス証明書のインストール方法
  IBM Security Guardium CLI コマンドを使用して、証明書署名要求 (CSR) の作成、および Guardium システム上へのサーバー証明書、認証局 (CA) 証明書またはトラステッド・パス証明書のインストールを行います。
- 自己モニター
  Guardium ソリューションは、自己モニターを行って、中断を最小限に抑え、可能な場合は常に問題を自動的に修正します。
- グループ
  グループを使用すると、分類、ポリシー、照会の各定義を簡単に作成および管理できるほか、更新を S-TAP クライアントおよび GIM クライアントに展開することができます。アクセス・ポリシーのデータ・オブジェクトのグループを繰り返し定義するのではなく、オブジェクトをグループに入れると、簡単に管理できます。
- セキュリティー・ロール
  セキュリティー・ロールは、データ (グループ、照会、レポートなど) へのアクセスを 許可したり、アプリケーション (「グループ・ビルダー」、「レポート・ビルダー」、「ポリシー・ビルダー」、 「CAS」、「セキュリティー・アセスメント」など) へのアクセスを許可するために使用します。
- 通知
  通知を作成するには、「アラート機能」および「アラート・ビルダー」を使用します。アラート・アクションに E メールまたはその他の通知が必要な場合は、以下の手順に従って、各タイプの通知について定義してください。
- リアルタイム・アラートの作成方法
  同じユーザーによるログインの失敗が 5 分以内で 3 回を超えた場合に、 データベース管理者にリアルタイム・アラートを送ります。
- カスタム・アラート・クラスの管理
  カスタムの受信者にアラートを送信するには、カスタム・アラート・クラスを使用します。 カスタム・クラスをアップロードしてから、「アラート・ビルダー」を使用して、アラート通知受信者としてカスタム・クラスを指定します。
- 事前定義アラート
  表で、「アラート・ビルダー」にある事前定義アラートについて説明します。
- スケジューリング
  汎用スケジューラーは、さまざまなタイプのタスク (アーカイブ、統合、 ワークフロー・オートメーションなど) をスケジュールに入れるために使用します。

- 別名
  レポートまたは照会で使用されるデータ値またはデータ・オブジェクトのシノニムを作成します。
- 日付とタイム・スタンプ
  カレンダー・ツールを使用して絶対日付を選択し、相対日付ピッカーを使用して現在時刻からの相対的な日付を選択します。
- 期間
  ポリシー・ルールや照会条件に使用できる期間を作成するには、「期間ビルダー」を使用します。
- 期間
  ポリシー・ルールおよび照会条件によって、ユーザー定義の期間内にイベントが発生したかどうかをテストできます。
- コメント
  コメントは、定義とワークフロー・プロセス結果に適用されます。
- パッチのインストール方法
  1 つのパッチ、または複数のパッチをバックグラウンド・プロセスとしてインストールします。
- サポート・メンテナンス
  サポート・メンテナンス・フィーチャーは、パスワードで保護されており、技術サポートから指示があった場合にのみ使用できます。詳しくは、技術サポートにお問い合わせください。

Guardium の管理

Guardium® 管理者は、各種の管理およびメンテナンス・タスクを行います。

admin ロールが割り当てられたユーザーは、Guardium 管理者と呼ばれます。これは、admin ユーザー・アカウントとは明らかに異なります。

admin ロール特権

Guardium admin ロールは、そのロールに明示的に割り当てられていない特権があります。例えば、admin ロールを持つユーザーがプライバシー設定定義のリストを表示すると、Guardium システムに定義されているプライバシー・セットがすべて表示され、これらの定義をどれでも表示、変更、または削除できます。admin ロールのないユーザーがプライバシー・セットのリストにアクセスすると、自身の (すなわち自身が作成した) プライバシー・セットのみ表示されます。他にそのユーザーにも割り当てられている、セキュリティー・ロールが割り当てられたすべてのプライバシー・セットも表示されます。

CLI diag コマンド・アクセス

diag CLI コマンドを使用するには、追加のパスワードが必要です。これには admin ロールを持つどのユーザーのパスワードも使用できます。

自動アカウント・ロックアウトが有効な場合 (指定されている回数ユーザー・アカウントへのログインに失敗すると、そのアカウントをロックする機能)、admin ユーザー・アカウントで何度かログインに失敗すると、ロックされる場合があります。これが発生した場合は、unlock admin CLI コマンドを使用してこれをアンロックしてください。

注: アクセス・マネージャー (accessmgr) は、「ユーザー・ブラウザー」からアカウントをアンロックできます。「アクセス」 > 「アクセス管理」 > 「ユーザー・ブラウザー」をクリックして、「ユーザー・ブラウザー」を開きます。

admin ユーザー特権

admin ユーザーは、次のように admin ロールに付与されない追加の特権を持ちます。

- すべてのユーザーの To-Do リストへのアクセス
- インポートされた定義の所有者
- アクセス管理機能

admin ユーザーの To-Do リストに対する権限

To-do リストとは、監査プロセスの結果のユーザーへの配布を制御するワークフロー自動化機能です。admin ユーザーには、この領域で特殊な特権および責務があります。ユーザー・アカウントが無効化されると、そのユーザーに対するすべての監査プロセスの結果が admin ユーザーに自動的に再割り当てされます。ユーザーがその他の何らかの理由で使用不可の場合、監査プロセスの結果をそのユーザーの To-Do リストにインストールする (すなわち、結果を次の受信者にリリースする前にサインオフを待つ) ことができます。admin ユーザーは、あらゆるユーザーの To-Do リストを開き、そのユーザーが使用できるすべてのアクションを実行できます。 admin ユーザーが別のユーザーの To-Do リスト上のアクションを実行すると、その事実が監査プロセスのアクティビティー・ログに記録されます。例えば、「admin ユーザーがユーザー x の代わりに結果に署名した」。

インポートされる定義所有権

定義がエクスポートされると、すべてのロールが削除され、所有者が admin ユーザーに変更されます。これは、インポート側システムで定義の使用方法を制御する唯一の方法です。

アクセス管理と管理者

セキュリティー上の目的で、アクセス・マネージャーと管理者の職務は分離されています。管理ユーザーはアクセス・マネージャーの特権を持つことができず、逆もまた同様です。

次に admin ユーザーがログインすると、アクセス・マネージャーの機能が使用可能になります。これは、admin ユーザーのみに可能です (admin ロールを持つ他のユーザーには使用可能になりません)。

注:

既存の状態やアップグレードの結果として、同一ユーザーがこれら両方のロールを持つ場合があります。ただし、現行の使用では、これらの 2 つのロールを同一ユーザーに割り当てることはできません。

以前は、ユニットをアップグレードすると、accessmgr ロールが admin ユーザーに割り当てられ、accessmgr ユーザーが無効にされていました。

この状況では、accessmgr および admin を構成するには、admin としてログインして、accessmgr ユーザーを有効にしてから、accessmgr としてログインして (デフォルトの初期パスワードは guardium)、admin ユーザーから accessmgr ロールを削除します。

親トピック: Guardium システムの管理

証明書

機能が失われないように、証明書を定期的に確認してください。 新しい証明書を入手してインストールするには、CLI コマンドを使用します。

証明書の有効期限

証明書の有効期限が切れると、機能が失われます。show certificate warn_expire コマンドを定期的に実行して、期限が切れた証明書がないか確認してください。このコマンドは、6 カ月以内に有効期限が切れる証明書と、既に有効期限が切れた証明書を表示します。ユーザー・インターフェースでも、有効期限が切れる証明について通知されます。すべての証明書の概要を表示するには、コマンド show certificate summary を実行します。

詳しくは、証明書 CLI コマンドの完全なリストを参照してください。

新しい証明書

新しい証明書を入手するには、証明書署名要求 (CSR) を生成して、VeriSign や Entrust などのサード・パーティー認証局 (CA) に連絡します。Guardium は、CA サービスを提供しません。また、デフォルトでインストールされているもの以外の証明書をシステムに添付することもありません。証明書の形式は、PEM でなければならず、BEGIN および END の区切り文字を含んでいる必要があります。証明書は、コンソールから貼り付けるか、標準インポート・プロトコルのいずれかを介してインポートすることができます。

以下のいずれかのコマンドを使用して、証明書署名要求 (CSR) を生成できます。

- create csr alias - このコマンドは、別名を持つ証明書要求を作成します。
- create csr gui - このコマンドは、Tomcat 用の証明書要求を作成します。
- create csr sniffer - このコマンドは、スニファー用の証明書要求を作成します。

注: このアクションは、システム・ネットワーク構成パラメーターの設定が終了するまで実行しないでください。
コマンド行インターフェースを使用して新しい証明書をインストールするには、以下のいずれかのコマンドを使用します。

- store certificate gim - このコマンドは、GIM 証明書を鍵ストアに保管します。
- store certificate gui - このコマンドは、Tomcat 証明書を鍵ストアに保管します。
- store certificate keystore - このコマンドは、証明書を一意的に識別するための 1 単語の別名を要求して、それを鍵ストアに保管します。
- store certificate mysql - このコマンドは、MySQL クライアントおよび MySQL サーバーの証明書を保管します。
- store certificate stap - このコマンドは、S-TAP 証明書を保管します。
- store certificate sniffer - このコマンドは、スニファー証明書を保管します。

コマンド行インターフェースを使用して新しい証明書鍵をインストールするには、以下のいずれかのコマンドを使用します。

- store cert_key mysql - このコマンドは、MySQL クライアントおよび MySQL サーバーの証明鍵を保管します。
- store cert_key sniffer - このコマンドは、スニファー証明鍵を保管します。

バックアップ・オプションとデフォルト・オプション

backup パラメーターまたは default パラメーターを使用して、証明書と証明書鍵のリストアを選択することができます。 証明書を最後に保存された証明書にリストアするには、backup パラメーターを使用します。証明書を Guardium が提供する元の証明書にリストアするには、default パラメーターを使用します。

コマンドの変更点

一部の証明書コマンドが変更されました。

- csr は create csr gui になりました。
- create system csr は create csr sniffer になりました。
- restore keystore は restore certificate keystore backup になりました。
- restore system-certificate は restore certificate sniffer default になりました。
- show system certificate は show certificate sniffer になりました。
- store system certificate は store certificate sniffer になりました。
- store trusted certificate は store certificate keystore になりました。
- store certificate console は store certificate gui になりました。

新規コマンド

以下のコマンドを使用できるようになりました。

- create csr alias
- restore certificate keystore default
- restore certificate sniffer backup
- show certificate all
- show certificate gim
- show certificate gui
- show certificate keystore alias
- show certificate keystore all
- show certificate mysql client
- show certificate mysql server

- show certificate summary
- show certificate warn_expired

推奨されないコマンド

以下のコマンドは推奨されなくなりました。

- csr
- store certificate console
- store system key
- show system key
- store system certificate
- show system certificate

コマンドの完全なリスト

証明書の作成、リストア、表示、または保管には、以下のコマンドを使用します。

- create csr gui
- create csr alias
- create csr sniffer
- restore certificate keystore default
- restore certificate keystore backup
- restore certificate sniffer backup
- restore certificate sniffer default
- show certificate all
- show certificate gim
- show certificate gui
- show certificate keystore alias
- show certificate keystore all
- show certificate mysql client
- show certificate mysql server
- show certificate sniffer
- show certificate summary
- show certificate warn_expired
- store certificate sniffer
- store certificate gui

親トピック: Guardium システムの管理

ユニット使用状況レベル

Guardium 環境内の頻繁に使用されているシステムとあまり使用されていないシステムを特定するには、ユニット使用状況レポートを使用します。

「管理」 > 「レポート」 > 「ユニット使用状況」をクリックし、いずれかのレポートを選択して、ユニット使用状況レポートを開きます。

デフォルトのユニット使用状況レポートには、以下が含まれます。

- バッファー使用状況モニター
- CPU トラッカー
- エンタープライズ・バッファー使用状況モニター
- ユニット使用状況

使用状況パラメーター

ほとんどのパラメーターは、特定のユニットの、特定の時刻範囲における平均値です。「再始動の数」は、さまざまな PID に基づく、特定の時刻範囲におけるスニファーの再始動回数です。

サポートされるパラメーターは次のとおりです。

- 再始動の数
- スニファー・メモリー
- MySQL メモリーの比率
- 空きバッファー・スペース
- アナライザー・キュー
- ロガー・キュー
  制約事項: ロガー・キューの SQL 数は 500 に制限されています。500 を超える SQL を同時にこのキューに入れようとすると、キュー制限を超えた余分な SQL により `RA=-1` がログに記録されます。
- MySQL ディスク使用状況
- システム CPU 負荷
- システム変数ディスク使用状況
- 要求の数
- 完全な SQL の数
- 例外の数
- ポリシー違反の数
- ディスク使用量のクイック検索
- ドキュメントの数のクイック検索
- 未解析ログ要求

しきい値

パラメーターごとに 2 つのしきい値が定義されています。これらのしきい値が、3 つの使用状況レベル (低、中、および高) の区切りとなります。

使用状況レベルは以下のとおりです。

- 低: 値がしきい値 1 を下回っている場合
- 中: 値がしきい値 1 を上回り、しきい値 2 を下回っている場合
- 高: 値がしきい値 2 を上回っている場合

各ユニットの全体的な使用状況レベルもあります。各期間について、このレベルが、その期間におけるすべてのレベルの最高レベルとなります。

レポート作成

使用可能なユニット使用状況レポートを表示するには、「管理」 > 「レポート」 > 「ユニット使用状況」をクリックします。

「ユニット使用状況レベル」トラッキング・オプションを使用すると、カスタムの照会やレポートを作成できます。

カスタム・レポートおよび事前定義レポートでユニット使用状況データを使用するときは、別名を使用することをお勧めします。そうしなければ、使用状況レベルが「低」、「中」、「高」ではなく、数字 (1、2、3) で表示されます。

属性のリストには、以下が含まれます。

- ホスト名
- 期間の開始
- 再始動の数
- 再始動レベルの数
- スニファー・メモリー
- スニファー・メモリー・レベル
- MySQL メモリーの比率
- MySQL メモリーの比率のレベル
- 空きバッファー・スペース
- 空きバッファー・スペース・レベル
- アナライザー・キュー
- アナライザー・キュー・レベル
- ロガー・キュー
- ロガー・キュー・レベル
- MySQL ディスク使用状況
- MySQL ディスク使用レベル
- システム CPU 負荷
- システム CPU 負荷レベル
- システム変数ディスク使用状況
- システム変数ディスク使用状況レベル
- 全体のユニット使用状況レベル
- 要求の数
- 要求数のレベル
- 完全 SQL の数
- 完全 SQL 数のレベル
- 例外の数
- 例外数のレベル
- ポリシー違反の数
- ポリシー違反数のレベル
- 未解析ログ要求数
- 未解析ログ要求数のレベル

注: 各パラメーターには、値があり、さらに値およびしきい値に基づいて計算されるレベルがあります。

ユニット使用状況で使用可能なスループット情報

スループット・データは、コレクター・ユニットごとに収集されます。CM は、すべてのスループット・データを統合して、企業のカスタム表を作成します。この表は、事前定義の使用状況レポートに追加されます。

収集されるスループット情報は、以下のとおりです。

- (その期間における) 要求の数 (構造インスタンスから)
- (その期間における) 完全 SQL の数 (構造テキストから)
- 例外の数
- ポリシー違反の数

デフォルトでは、スループット情報は 1 時間ごとに収集されます。

ユニット使用状況を使用するための GuardAPI コマンドと CLI コマンド

Guard API:

- listUtilizationThresholds

  updateUtilizationThresholds

reset_unit_utilization

CLI コマンド:

- store monitor gdm_statistics
- show monitor gdm_statistics

- ユニット使用状況データ処理の構成
  この手順では、ユニット使用状況データを処理して表示するための Guardium システムの構成方法を説明します。

親トピック: Guardium システムの管理

ユニット使用状況データ処理の構成

この手順では、ユニット使用状況データを処理して表示するための Guardium システムの構成方法を説明します。

このタスクについて

一元管理される環境の場合、ユニット使用状況情報の表示には、中央マネージャーでの 2 つのプロセスのスケジュールが必要です。すなわち、中央マネージャー・バッファー使用状況モニター用のデータのアップロード、およびユニット使用状況データの処理です。

スタンドアロン・システムの場合、ユニット使用状況情報の表示には、ユニット使用状況データの処理のスケジュールのみが必要です。スタンドアロン・システムを使用する場合、中央マネージャー・バッファー使用状況モニター用のデータ・アップロードをスケジュールする必要はありません。

手順

1. 一元管理される環境の場合、中央マネージャー・バッファー使用状況モニター・データをアップロードするためのスケジュールを中央マネージャーで定義します。
   a. 「レポート」 > 「レポート構成ツール」 > 「カスタム表ビルダー」にナビゲートします。
   b. 「カスタム表」画面で、「CM バッファー使用状況モニター」を選択し、「データのアップロード」をクリックして次に進みます。
   c. 「データのアップロード」画面で、「スケジュールの変更」をクリックして、中央マネージャー・バッファー使用状況モニター・データをアップロードするためのスケジュールを定義します。スケジュールの定義後、「保存」をクリックしてから、「先頭に戻る」をクリックして「データのアップロード」画面に戻ります。 1 時間に 1 回プロセスを実行するようにスケジュールするのが、最初は多くのデプロイメントで妥当な方法ですが、使用可能なリソースまたはデータの現行性のニーズに合わせて間隔を調整できます。
   重要: ユニット使用状況レポートで最新のデータを使用できるようにするには、ユニット使用状況データを処理する前に、バッファー使用状況モニター・データを処理するスケジュールを定義します。また、バッファー使用状況モニター・データは、特定時間に正確に実行されるようにスケジュールしないでください。
   ベスト・プラクティス: 正時の 10 分後にバッファー使用状況モニター・データを処理し、正時の 40 分後にユニット使用状況データを処理するスケジュールを定義します。
   d. 「データのアップロード」画面で、オプションとして「今すぐ 1 回実行」をクリックして即時にデータをアップロードします。
2. 一元管理される環境またはスタンドアロン・システムの場合、ユニット使用状況データを処理するためのスケジュールを定義します。 一元管理される環境では、中央マネージャーでユニット使用状況スケジュールを定義するだけで済みます。
   a. 「管理」 > 「ユニット使用状況」 > 「ユニット使用状況レベル」にナビゲートします。
   b. 「ユニット使用状況レベル」画面で、「スケジュールの変更」をクリックして、ユニット使用状況データを処理するためのスケジュールを定義します。スケジュールの定義後、「保存」をクリックしてから、「先頭に戻る」をクリックして「ユニット使用状況レベル」画面に戻ります。 1 時間に 1 回プロセスを実行するようにスケジュールするのが、最初は多くのデプロイメントで妥当な方法ですが、使用可能なリソースまたはデータの現行性のニーズに合わせて間隔を調整できます。
   重要: ユニット使用状況レポートで最新のデータを使用できるようにするには、バッファー使用状況モニター・データを処理した後にユニット使用状況データを処理するスケジュールを定義します。
   ベスト・プラクティス: 正時の 10 分後にバッファー使用状況モニター・データを処理し、正時の 40 分後にユニット使用状況データを処理するスケジュールを定義します。
   c. 「ユニット使用状況レベル」画面で、オプションとして「今すぐ 1 回実行」をクリックして即時にデータを処理します。

タスクの結果

上記のステップの完了後、「管理」 > 「レポート」 > 「ユニット使用状況」にナビゲートしてユニット使用状況レポートを表示します。集中管理される環境では、中央マネージャーとその管理対象ユニットのデータが利用可能です。スタンドアロン・システムの場合、その個別システムのデータのみが使用可能です。スケジュールを定義する際に「今すぐ 1 回実行」オプションを使用しなかった場合、ユニット使用状況レポートが最新データで更新される前に、それらのプロセスが実行されるまで待つ必要があります。

親トピック: ユニット使用状況レベル

カスタム・アップロード

データベース・アクティビティー・モニター・コンテンツ・サブスクリプション (旧称は、データベース保護サブスクリプション・サービス)は、事前定義アセスメント・テスト、SQL ベースのテスト、CVE、APAR、およびグループ (データベース・バージョンやパッチなど) の保守をサポートしています。

アップロードは、情報を常に最新の状態に維持し、業界のベスト・プラクティスにおいて、新たに発見された脆弱性から保護するために使用されます。 更新の配布は、四半期ごとに行われます。

カスタム・アップロードを使用して、以下のものをアップロードします。 DPS 更新ファイル、Oracle JDBC ドライバー、MS SQL Server JDBC ドライバー、および DB2 for z/OS ライセンス jar。

注: 事前定義された Guardium® グループと同じ名前のカスタム・グループが存在する場合、アップロード・プロセスによって、事前定義グループの名前の前に「Guardium」が追加されます。

1. 「強化」 > 「脆弱性評価」 > 「カスタム・アップロード」をクリックして「カスタム・アップロード」を開きます。
2. 「DPS のアップロード」で、「参照」をクリックして、アップロードするファイルを見つけ、選択します。

注: どのファイルがアップロードされたかを確認するには、「DPS のインポート」ペインを参照してください。

3. 「DB2 z/OS ライセンス jar のアップロード」で、「参照」をクリックして、ファイルを見つけ、選択します。
4. 「Oracle JDBC ドライバーのアップロード」または「MS SQL Server JDBC ドライバーのアップロード」を使用して、オープン・ソース・ドライバーをアップロードします。 アップロードの後、「データ・ソース・ファインダー」にデータベースが追加されています。ドライバーは、1 つずつアップロードしてください。
   注: Oracle データ・ダイレクト・ドライバーまたは MS SQL データ・ダイレクト・ドライバーよりもオープン・ソース・ドライバーを使用することが推奨される場合が 2 種類あります。
   a. Windows Authentication for MS SQL Server をサポートする場合。その他のすべての用法では、Guardium アプライアンスにプリロードされたデータ・ダイレクト・ドライバーを使用することで十分です。
   b. Oracle バージョン 10 以上で「値変更のトラッキング」アプリケーションを使用する場合。トリガーの代わりにストリームの使用をサポートするには、オープン・ソース・ドライバーが推奨されます。

   キーワードを使用して、オープン・ソース JDBC ドライバーを検索してダウンロードします (例: *open source JDBC driver for MS SQL*)。

5. 中央マネージャーを使用して、.jar ファイルを管理対象ユニットに配布します。ファイルのアップロードが成功したら、中央マネージャーと管理対象ユニットで GUI を再始動する必要があります。

注:

ユニット間で相互に定義をエクスポートしたり、インポートしたりする場合は、サブスクライブしたグループがエクスポートされないように注意してください。 サブスクライブしたグループを参照する定義をエクスポートする場合、ユーザーは参照されるサブスクライブしたグループをすべて、インポート側ユニット (フェデレーテッド環境では中央マネージャー) にインストールしておく必要があります。

DB2® z/OS® ライセンス JAR ファイルをアップロードする場合、ライセンスは GUI を再始動した後に有効になります。

注: 何らかの理由 (例えば、サーバーの再始動や GUI の再始動など) で DPS が停止した場合、30 分間待ってから DPS アップロード・プロセスを再開することを推奨しています。

最新の Oracle DataDirect ドライバーを使用して、Oracle サーバーで ASO を有効にする

最新の Oracle DataDirect ドライバーを使用して Oracle サーバーで ASO を有効にする場合、以下を参照してください。

SQLNET.CRYPTO_CHECKSUM_SERVER = 必須

SQLNET.ENCRYPTION_SERVER = 必須

SQLNET.ENCRYPTION_TYPES_SERVER = (AES256, AES192, AES128)

#SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA256)

SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA1)

Oracle JDBC ドライバーは動作し、接続プロパティーの指定は不要です。

ただし、最新の Oracle JDBC ドライバーを Oracle からダウンロードする必要があります。ファイル名は ojdbc7.jar です。キーワードを使用して、オープン・ソース JDBC ドライバーを検索してダウンロードします (例: open source JDBC driver for Oracle)。次に、Guardium カスタム・アップロード機能を使用して、そのドライバーをアプライアンスにアップロードします。

Oracle DataDirect ドライバーを引き続き使用する場合、データ・ソースに対する接続プロパティーを指定する必要があります。

Oracle DataDirect ドライバーの接続プロパティーを定義する場合、以下を使用します。

DataIntegrityLevel=required;EncryptionLevel=required;DataIntegrityTypes=(MD5、SHA1)

注: 現在の Oracle DataDirect ドライバーは SHA-256 をサポートしていません。このため、SHA-1 を使用する必要があります。これが、sqlnet.ora 参照 (#SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA256)) をコメント化する必要があった理由です。ただし、Guardium カスタマーが SHA-256 を使用して接続する必要がある場合、代わりに Oracle JDBC ドライバーを使用する必要があります。

データ・ダイレクトのリファレンス:

https://www.progress.com/documentation/datadirect-connectors

一連のコマンドのリファレンスとして、Oracle データベースの JDBC のユーザー・ガイド (PDF) をダウンロードしてください。

「カスタム・アップロード」機能を使用してデータ・ソース・アップロード・ファイルを作成および保存するときのタブ区切りファイル (.TXT) の使用

コンマ区切りファイル構造 (.CSV) を使用する場合、いずれかの列値にコンマが含まれていると、意図したとおりに動作しません。

以下の手順を行います。

1. EXCEL を使用している場合、タブ区切り (.TXT) ファイルとしてファイルを保存します。
2. OpenOffice または Libre Office を使用している場合、タブ区切り文字付きの (.CSV) ファイルとして保存します。
3. admin としてログインし、「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「カスタム・アップロード」をクリックして、「カスタム・アップロード」を開きます。
4. 「CSV をアップロードしてデータ・ソースを作成/更新」で、「参照...」をクリックして、タブ区切りファイルを選択します。

CSV のアップロード・メニューにより CSV をアップロードしてデータ・ソースを作成する

データ・ソース情報を格納するタブ区切り .TXT 形式ファイルを作成するには、以下の手順を行います。これにより、このタブ区切り .TXT ファイルは、Guardium アプリケーション内の「カスタム・アップロード」機能によって多くのデータ・ソース・タイプに使用できます。

データ・ソースをインポートする機能の使用は、必ずしもすべての Guardium ソフトウェア・リリースで互換性があるわけではありませんでした。この手順によって、あらゆるデータ・ソースのアップロードが可能になります。

以下のリストは、.TXT 形式のタブ区切りデータ・ソース・アップロード・ファイルを作成するときに Excel スプレッドシートに追加する必要があるヘッダー列です。

列の値 (.CSV データ・ソース・アップロード・ファイルで受け入れられる)

表 1. create_datasource

パラメーター	記述
application	必須。 データ・ソースの定義対象となるアプリケーションを指定します。 次のいずれかでなければなりません。 ChangeAuditSystem Access_policy MonitorValues DatabaseAnalyzer AuditDatabase CustomDomain Classifier AuditTask SecurityAssessment Replay Stap_Verification
compatibilityMode	互換モード: 選択項目は「デフォルト」と「MSSQL 2000」です。表のモニター時に使用する互換モードをプロセッサーに指示します。
conProperty	オプション。 このデータ・ソースとの JDBC 接続を確立するために JDBC URL に追加の接続プロパティーを含める必要がある場合にのみ使用します。 使用するフォーマットは、「property=value」である必要があります。このとき、プロパティーと値の各ペアはコンマで区切ります。 Roman8 をデフォルトの文字セットとする Sybase データベースの場合、次のプロパティーを入力します。charSet=utf8
customURL	オプション。 データ・ソースに対する接続文字列。これを入力しない場合は、前回入力したフィールドのホスト、ポート、インスタンス、プロパティーなどを使用して接続が行われます。 これは、例えば Oracle Internet Directory (OID) の接続を作成するときに便利です。
dbInstanceAccount	オプション。 CAS によって使用されるデータベース・アカウント・ログイン名 (ソフトウェア所有者)
dbInstanceDirectory	オプション。 CAS によって使用される、データベース・ソフトウェアがインストールされたディレクトリー
dbName	オプション。 DB2 または Oracle データ・ソースの場合、スキーマ名を入力します。他の場合は、データベース名を入力します。
description	オプション。データ・ソースの詳細説明。
host	必須。 ホスト名または IP アドレスを入力できます。
name	必須。 システム上のデータ・ソースに固有の名前を付けます。
owner	必須。 データ・ソースを所有する Guardium ユーザー・アカウントを指定します。
password	オプション。所有者のパスワード。使用する場合、ユーザーも使用する必要があります。
port	オプション (整数)。ポート番号。
serviceName	Oracle、Informix®、DB2、および IBM® ISeries の場合は必須。DB2 データ・ソースではデータベース名を入力します。それ以外ではサービス名を入力します。
severity	オプション。データ・ソースの重大度分類 (あるいは影響レベル)。
shared	オプション (ブール値)。他のアプリケーションと共有する場合は **true** に設定します。データ・ソースを他のユーザーと共有する場合は、GUI からロールを割り当てる必要があります。

パラメーター	記述
type	必須。 データ・ソース・タイプを指定します。次のいずれかでなければなりません。 DB2 DB2 for i Db2 for z/OS Informix MS SQL Server MS SQL サーバー (DataDirect) MySQL NA Netezza Oracle (DataDirect) Oracle (サービス名) Oracle (SID) PostgreSQL Sybase Sybase IQ Teradata アプリケーションが CustomDomain または Classifier である場合、以下も使用できます。 TEXT TEXT:FTP TEXT:HTTP TEXT:HTTPS TEXT:SAMBA
user	オプション。データ・ソースのユーザー。使用する場合、パスワードも使用する必要があります。
environmentTitle	クラウド・データベース・サービスの保護に必要。アカウント名。
region	クラウド・データベース・サービスの保護に必要。AWS 領域。
objectLimit	クラウド・データベース・サービスの保護に必要。分類プロセスで検出され、監査対象オブジェクトのリストに自動的に追加されるオブジェクトの最大数。クラウド・データベース・サービス保護を参照してください。
primaryCollector	クラウド・データベース・サービスの保護に関連。クラウド・データベースから監査データを抽出するコレクター。

注:

1. 各列名は、タブ区切り形式 (.TXT) ファイルとして保存される Excel スプレッドシートに含める必要があります。
2. 作成されるデータ・ソース名 (データ・ソースを検索するときに表示されるもの) は、名前列とタイプ列の両方で構成されます。
3. アップロード・ファイルは、列タブ区切り形式のファイル・タイプとして保存される必要があります。

txt ファイルを CSV テキスト形式で作成およびアップロードしてデータ・ソースのデータを追加するステップ

1. データ・ソース・インポート機能をサポートする以下のヘッダーおよびデータ・ソースのデータを使用して、Excel スプレッドシート・ファイルを作成してタブ区切り .TXT ファイルとして保存します。
2. Guardium アプリケーションへのアップロード用の PC または UNIX/Linux デバイスに対して .txt ファイルを作成して保存します。
3. admin としてログインし、「強化」 > 「構成変更制御 (CAS アプリケーション)」 > 「カスタム・アップロード」をクリックして、「カスタム・アップロード」を開きます。
4. 「CSV をアップロードしてデータ・ソースを作成/更新」で、「参照」 をクリックして、タブで区切られたデータ・ソース情報を格納している .txt ファイルを選択します。
5. 「アップロード」をクリックします。

.txt ファイルからアップロードされた値を示すメッセージが表示されます。

1. **「新規」**: ファイルをアップロードするたびに (ファイルを保存して新規データ・ソース・メンバーを追加した場合)、これらのメンバーは「新規」状況になります。
2. **「更新」**: 同じデータ・ソースに変更を加えてアップロードすると、「更新」の状況が付与されます。
3. **「不合格」**: 失敗したデータ・ソースまたはエラーが表示されます

親トピック: Guardium システムの管理

「サービス状況 (Services Status)」パネル

「サービス状況 (Services Status)」パネルは、CAS やアラート機能などのサービスの状況を確認して、必要な場合には各サービスをさらに調査するための、一元管理された場所です。「設定」 > 「ツールとビュー」 > 「サービス状況 (Services Status)」をクリックして、「サービス状況 (Services Status)」パネルを開きます。 「サービス状況 (Services Status)」パネルが開かれるたびに、各サービスの状況が最新表示されます。

例えば、5 分間でログインの失敗が 3 回を超えた場合に常にリアルタイム・アラートを送信するポリシーを設定するとします。この潜在的な侵入から保護するために、ポリシーがインストールされていて、アラート機能がオンになっていることを確認する必要があります。

「サービス状況 (Services Status)」 パネルを使用して、これらのサービスの両方が適切に構成されていることを確認します。

いずれかのサービスをクリックすると、その構成ページに移動します。そのページで、サービスのオンとオフの切り替え、サービスの再始動、サービスの構成など関連する操作を実行できます。

何らかの理由でポリシーが正しくインストールされていなかった場合は、「設定」 > 「ツールとビュー」 > 「ポリシー・インストール」をクリックして、「ポリシー・インストーラー」に進み、現在インストールされているポリシーを表示して、必要な変更を加えます。

それぞれのサービスに、以下のいずれかのアイコンが表示されます。

- サービスが実行中/スケジュール済みの場合:
- サービスが一時停止している場合:
- サービスがオフの場合:

親トピック: Guardium システムの管理

アーカイブ、パージおよびリストア

アーカイブおよびパージ操作は、スケジュールに基づいて実行する必要があります。 キャプチャーされた情報を監査のために保管するには、「データ・アーカイブ」と「結果アーカイブ」を使用します。このトピックの終わりで、Guardium での Amazon S3 へのアーカイブおよびバックアップについても説明しています。

「データ・アーカイブ」および「結果アーカイブ」は、「管理」 > 「データ管理」をクリックすると見つかります。

- 「データ・アーカイブ」は、Guardium システムによって一定期間内にキャプチャーされたデータをバックアップします。データ・アーカイブを構成する際には、パージ操作も構成できます。 通常、データは毎日、1 日の終わりにアーカイブされます。こうすることで、災害発生時に失われるのはその当日のデータだけになります。データのパージは、アプリケーションごとに異なり、ビジネス要件や監査要件によってかなり大きな違いがあります。 ほとんどの場合、データは Guardium システム上に 6 カ月以上保持することができます。
- 「結果アーカイブ」は、監査タスクの結果 (レポート、アセスメント・テスト、エンティティー監査証跡、プライバシー・セット、および分類プロセス) のほか、表示およびサインオフの証跡、ワークフロー・プロセスからの調整コメントをバックアップします。 結果セットは、ワークフロー・プロセスの定義に従ってシステムからパージされます。

統合環境では、データはコレクター、アグリゲーター、またはその両方のロケーションからアーカイブできます。 データは、一度だけアーカイブするのが最も一般的です。 アーカイブ元となるロケーションは、ユーザーの要件に応じて異なります。

スケジュールされたエクスポート操作により、Guardium® コレクター・ユニットから Guardium 統合サーバーにデータが送信されます。統合サーバーは、独自のスケジュールでインポート操作を実行し、統合プロセスを完了します。 この一方または両方のユニットにおいて、アーカイブ操作とパージ操作がスケジュールされます。これらの操作は (スペースを解放し、内部データベースのアクセス操作を高速化する目的で) 定期的にデータをバックアップしてパージします。

アーカイブ・ファイルは、SCP または FTP プロトコルを使用して送信することもできますし、EMC Centera や TSM ストレージ・システムが構成されている場合には、そこに送信することもできます。 各 Guardium システムには、単一のアーカイブ構成を定義できます。

Guardium のアーカイブ機能では、改ざんできない、署名付きの暗号化ファイルが作成されます。 生成されたアーカイブ・ファイルの名前を変更しないでください。 アーカイブ操作およびリストア操作は、アーカイブ処理中に作成されるファイル名に依存します。

アーカイブおよびエクスポートの各アクティビティーでは、システム共有パスワードを使用して暗号化データ・ファイルが作成されます。 あるシステムで暗号化した情報を、別のシステムでリストア可能にするには、アーカイブ側の システムでそのファイルを作成したときに使用した共有パスワードが、リストア側のシステムに必要です。

データをアーカイブする際には、必ず操作が正常に完了したことを確認してください。 これを行うには、「管理」 > 「レポート」 > 「データ管理」 > 「統合/アーカイブ・ログ」をクリックして、「統合/アーカイブ・ログ」を開きます。アーカイブ操作ごとに複数のアクティビティーがリストされていて、各アクティビティーの状況は完了になっているはずです。

「管理」 > 「データ管理」 > 「システム・バックアップ」をクリックして、システム・バックアップ・タスクを実行します。CLI からバックアップ・タスクを実行することもできます。詳しくは、ファイル処理 CLI コマンドを参照してください。

デフォルト・パージ

- パージのデフォルト値は 60 日です。
- デフォルト・パージ・アクティビティーは、毎日午前 5:00 にスケジュールされます。
- 新規インストールでは、デフォルトの値とアクティビティーに基づくデフォルト・パージ・スケジュールがインストールされます。
- ユニット・タイプを「管理対象ユニット」に変更するか、「スタンドアロン・ユニット」に戻すと、デフォルト・パージ・スケジュールが適用されます
- パージ・スケジュールは、アップグレード中は影響を受けません
- 多数のレコード (1000 万件以上) をパージするときは、バッチ・サイズを大きく (500k から 1M) 設定するのが最も有効な方法です。 小さめのバッチ・サイズまたは NULL を使用すると、パージに要する時間が何時間も余計にかかります。 小規模のパージは短時間で終了するため、バッチ・サイズを大きく設定する方法はパージが大規模である場合にのみ該当します。

注: バッチ・サイズの設定は、UI では実行できません。GuardAPI コマンド grdapi set_purge_batch_size batchSize を使用して、バッチ・サイズを設定します。

アーカイブに保存されなかった日を確認する方法

「レポート・ビルダー」を使用して、アーカイブの日付を示す全ファイルのリストを表示します。「管理」 > 「レポート」 > 「レポート・ビルダー」をクリックして、「レポート・ビルダー」を開きます。「照会」メニューから、「ロケーション・ビュー」を選択します。このレポートに組み込まれなかった日付は、アーカイブに保存されなかった日付です。必要であれば、リストに組み込まれていない日付のアーカイブを実行してください。

データ・アーカイブおよびパージの構成

1. 「管理」 > 「データ管理」 > 「データ・アーカイブ」をクリックして、「データ・アーカイブ」を開きます。
2. アーカイブするには、「アーカイブ」チェック・ボックスにチェック・マークを付けます。 「構成」パネルに、追加のフィールドが表示されます。
3. 「次の期間を経過したデータをアーカイブ」で、値を入力して、メニューから時間の単位を選択します。前日のデータからデータのアーカイブを開始するには、値 1 を入力し、メニューから「日」を選択します。
4. 何日分のデータをアーカイブするかを制御するには、「次の期間を経過したデータを無視」を使用します。ここに指定する値は、「次の期間を経過したデータをアーカイブ」」の値よりも大きくなければなりません。
   注: このフィールドをブランクのままにすると、「次の期間を経過したデータをアーカイブ」で指定した値より古いすべての日のデータがアーカイブされます。 つまり、毎日アーカイブを行い、30 日より古いデータをパージする場合には、(31 日目にパージされるまで) 日次データを 30 回アーカイブすることになります。
5. SQL 文字列からの値をアーカイブ・データに含めるには、「値のアーカイブ」チェック・ボックスにチェック・マークを付けます。このボックスをクリアすると、値はアーカイブでは疑問符文字に置き換えられます (したがって、リストア操作以後、これらの値を使用できなくなります)。
6. 「プロトコル」オプションを選択して、適切な情報を入力します。Guardium システムの構成方法によっては、これらのボタンの 1 つ以上が選択できない場合があります。 アーカイブおよびバックアップのストレージ方式の構成方法については、show storage-system および store storage-system コマンドの説明を参照してください。
7. 選択したストレージ方式に応じて、適切な手順を実行します。
   - SCP または FTP アーカイブまたはバックアップの構成
   - EMC Centera アーカイブまたはバックアップの構成
   - TSM アーカイブまたはバックアップの構成
8. 「パージ」チェック・ボックスにチェック・マークを付けて、パージ操作を定義します。

   重要: このパージ構成は、データ・アーカイブとデータ・エクスポートの両方で使用されます。 ここで行った変更は、すべてのデータ・エクスポートの実行に適用されます。逆もまた同様です。パージがアクティブになっていて、データ・エクスポートとデータ・アーカイブの両方が同じ日に実行される場合には、最初に実行された操作が古いデータをすべてパージした後に 2 番目の操作が実行されます。

   そのため、データ・エクスポートとデータ・アーカイブが共に構成されているときは常に、エクスポート基準経過日数とアーカイブ基準経過日数の両方よりもパージ基準経過日数の方が大きくなければなりません。

9. データをパージする場合は、「次の期間を経過したデータをパージ」フィールドを使用して、パージ操作の対象となる開始日を、当日 (0 日) よりさかのぼった日数、週数、または月数として指定します。指定した日、およびそれより古いすべての日のデータは、注に示す例外を除いてすべてパージされます。パージ開始日に指定する値は、「次の期間を経過したデータをアーカイブ」に指定した値よりも大きくなければなりません。 また、データ・エクスポートがアクティブになっている場合、ここに指定するパージ開始日は、「次の期間を経過したデータをエクスポート」の値よりも大きくなければなりません。『重要』の注を参照してください。
   注:

   それ以前の操作によってまだアーカイブ/エクスポートされていないデータをパージする際には、警告は出されません。

   パージ操作では、リストア操作で指定される「リストアしたデータをパージしない」時間枠の範囲内に経過日数が入っているリストア・データはパージされません。

10. 「スケジューリング」セクションを使用して、この操作を定期的に実行するためのスケジュールを定義できます。
11. 「保存」をクリックして、構成の変更を保存します。システムはそのロケーションにテスト・データ・ファイルを送信することにより、構成の検証を試みます。
    - 操作が失敗すると、エラー・メッセージが表示され、構成は保存されません。
    - 操作が成功すると、構成が保存されます。
12. 「今すぐ 1 回実行」をクリックして、操作を 1 回実行します。

SCP または FTP アーカイブまたはバックアップの構成

アーカイブまたはバックアップの構成パネルで SCP または FTP を選択した後、以下の情報を指定する必要があります。

1. 「ホスト」に、アーカイブ・データを受信するホストの IP アドレスまたはホスト名を入力します。
2. 「ディレクトリー」に、データの格納先ディレクトリーを指定します。FTP または SCP のどちらのファイル転送方式を使用するかに応じて、指定方法が異なります。
   - FTP の場合: FTP アカウントのホーム・ディレクトリーに対する相対パスでディレクトリーを指定します。
   - SCP の場合: 絶対パスとしてディレクトリーを指定します。
3. 「ポート」に、SCP および FTP を介したファイル送信に使用できるポートを指定します。ssh/scp/sftp のデフォルトのポートは 22 です。FTP のデフォルトのポートは 21 です。
   注: ポートにゼロ (0) が表示される場合、デフォルト・ポートが使用されていて、変更の必要がないことを示します。
4. 「ユーザー名」および「パスワード」に、SCP サーバーまたは FTP サーバーにログオンするユーザーの資格情報を入力します。 このユーザーは、「ディレクトリー」で指定したディレクトリーに対する書き込み権限/実行権限を保持していなければなりません。

   Windows の場合、ドメイン・ユーザーは domain¥user の形式にしてください。

5. 「保存」をクリックして構成を保存します。

EMC Centera アーカイブまたはバックアップの構成

このバックアップまたはアーカイブ・タスクでは、ファイルがオフサイトの EMC Centera ストレージ・システムにコピーされます。 EMC からのライセンスのほか、ユーザー名およびパスワードが必要です。 このタスクでは、次の 4 つのメイン・アクションが必要です。

1. ネットワーク上で EMC Centera でのアカウントを確立する (IP アドレスおよび ClipID が必要)。

2. Guardium システムからデータまたは構成ファイルのいずれかまたは両方を構成する。
3. ライブラリーを定義およびエクスポートする。
4. ファイルが EMC Centera ストレージ・システムに格納されていることを確認する。

CLI アクション

CLI から以下のコマンドを実行します。

```
store storage-system centera backup ON
show storage-system
```

Centera アーカイブまたはバックアップの構成

「管理」 > 「データ管理」 > 「システム・バックアップ」をクリックして、「システム・バックアップ」を開きます。「EMC Centera」を選択します。以下の情報を指定する必要があります。

1. 「保持」に、データを保持する日数を入力します。最大値は 24855 (68 年) です。それより長くデータを保存する場合は、後ほどデータをリストアして再度保存します。
2. 「Centera プール・アドレス」に、Centera プール接続文字列を入力します (例: 10.2.3.4,10.6.7.8?/var/centera/us1_profile1_rwe.pea txt)。
   注: この IP アドレスおよび .PEA ファイルは、EMC Centera から取得します。 パスを構成する際には、疑問符が必須です。 「.../var/centera/...」を含むパス名でなければバックアップが失敗するため、このパス名は重要です。 .PEA ファイルは、Centera バックアップ要求ごとにアクセス権、ユーザー名、およびパスワード認証を提供します。
3. 「PEA ファイルのアップロード」をクリックして、接続文字列に使用される Centera PEA ファイルをアップロードします。この場合にも「Centera プール・アドレス」が必要です。
   注: 「このアドレスのプールを開くことができません」というメッセージが表示される場合、Guardium システムのホスト名のサイズを確認してください。Centera では、長さが 4 文字未満のホスト名の使用時に、タイムアウト問題が報告されています。
4. 「保存」をクリックして構成を保存します。システムは、指定された接続文字列を使用してプールを開くことにより、Centera アドレスの検証を試みます。操作が失敗すると、通知メッセージが表示され、構成は保存されません。
5. 「今すぐ 1 回実行」をクリックし、ダウンロードした .PEA ファイルを使用してバックアップを実行します。

ファイルが EMC Centera にコピーされていることを確認します。このタスクでは、対象のファイルの名前と ClipID が必須です。

TSM アーカイブまたはバックアップの構成

TSM サーバーへアーカイブする前には、CLI を使用して Guardium システムに dsm.sys 構成ファイルをアップロードする必要があります。 import tsm config CLI コマンドを使用します。 アーカイブまたはバックアップの構成パネルで TSM を選択した後、以下の情報を指定します。

1. 「パスワード」に、TSM サービスを要求するためにこの Guardium システムが使用する TSM パスワードを入力し、「パスワードの再入力」ボックスに再び入力します。
2. オプションで、dsm.sys ファイルの servername 項目と一致するように、「サーバー名」を入力します。
3. オプションで、「ホスト」名を指定します。
4. 「保存」をクリックして構成を保存します。「保存」ボタンをクリックすると、システムは dsmc アーカイブ・コマンドを使用してサーバーにテスト・ファイルを送信することにより、TSM 宛先の検証を試みます。操作が失敗すると、通知メッセージが表示され、構成は保存されません。
5. アーカイブまたはバックアップ手順に戻って、構成を完了します。

結果アーカイブの構成

1. 「管理」 > 「データ管理」 > 「結果アーカイブ (監査)」をクリックして、「結果アーカイブ」を開きます。
2. 「次の期間を経過した結果をアーカイブ」に続くファイルに、アーカイブ操作の開始日を、当日 (0 日) よりさかのぼった日数、週数、または月数として指定します。前日のデータから結果のアーカイブを開始するには、値 1 を入力し、リストから「日」を選択します。
3. オプションで、「次の期間を経過した結果を無視」に続くフィールドを使用して、何日分の結果をアーカイブするかを制御します。 ここに指定する値は、「次の期間を経過した結果をアーカイブ」の値よりも大きくなければなりません。
4. ラジオ・ボタンでストレージ方式を選択します。Guardium システムの構成方法によっては、これらのボタンの 1 つ以上が選択できない場合があります。アーカイブおよびバックアップのストレージ方式の構成方法については、構成および制御 CLI コマンドで show storage-system コマンドと store storage-system コマンドの説明を参照してください。
   - EMC CENTERA
   - TSM
   - SCP
   - FTP
5. 選択したストレージ方式に応じて、適切な手順を実行します。
   - SCP または FTP アーカイブまたはバックアップの構成
   - EMC Centera アーカイブまたはバックアップの構成
   - TSM アーカイブまたはバックアップの構成
   - Guardium での Amazon S3 へのアーカイブおよびバックアップ
6. 「スケジューリング」セクションを使用して、この操作を定期的に実行するためのスケジュールを定義できます。
7. 「保存」」をクリックすると、構成の変更が検証されて、保存されます。システムはそのロケーションにテスト・データ・ファイルを送信することにより、構成の検証を試みます。
   - 操作が失敗すると、エラー・メッセージが表示され、構成は保存されません。
   - 操作が成功すると、構成が保存されます。
8. 「今すぐ 1 回実行」をクリックして、操作を 1 回実行します。

データのリストア

このシステムが、リストアするアーカイブを生成したシステムではない場合、カタログ・アーカイブを使用してカタログでロケーション・エントリーを作成し、「追加」(参照:「Guardium カタログ」) または「GuardAPI」(参照:「CLI および API」 > 「GuardAPI リファレンス」 > 「GuardAPI カタログ・エントリー関数」) をクリックする必要があります。データのリストアが開始されると、この情報を使用してファイルがシステムに転送され、その後データが処理されます。

データをリストアする前に

- TSM からリストアする前には、CLI を使用して Guardium システムに dsm.sys 構成ファイルをアップロードする必要があります。import tsm config CLI コマンドを使用します。
- EMC Centera からリストアする前には、「データ・アーカイブ」パネルを使用して Guardium システムに PEA ファイルをアップロードする必要があります。
- 別の Guardium システムが暗号化したファイルをリストアまたはインポートする前に、そのシステムがファイルの暗号化に使用したシステム共有パスワードが、こちらのシステムでも使用可能であることを確認してください (使用可能でない場合、ファイルを暗号化解除できません)。システム構成の『システム共有パスワードについて』を参照してください。
- Guardium コレクターでリストアする前には、CLI コマンド stop inspection-core を実行して、inspection-core プロセスを停止してください。
  注: そのデータは、リストア処理の間はキャプチャーできません。

データのリストア手順は、以下のとおりです。

1. 「管理」 > 「データ管理」 > 「データのリストア」をクリックして、「データのリストア」を開きます。
2. 「開始」に日付を入力し、データを必要とする最も古い日付を指定します。
3. 「終了」に日付を入力し、データを必要とする最も新しい日付を指定します。
4. 「ホスト名」に、アーカイブが行われた Guardium システムの名前をオプションで入力します。
5. 「検索」をクリックします。
6. 「検索結果」パネルで、リストアする各アーカイブの「選択」チェック・ボックスにチェック・マークを付けます。
7. 「リストアしたデータを少なくとも次の期間パージしない」フィールドに、リストアしたデータをシステムに保持する日数を入力します。
8. 「復元」をクリックします。
9. 完了したら、「完了」をクリックします。

注: コレクターからアーカイブしたデータのリストアは、 同じコレクターへのリストア、アグリゲーターへのリストア、 または統合クラスターに属さない調査専用の別のコレクターへのリストアのみにしてください。コレクターが異常終了した場合は、 システム・バックアップを新規のクリーンなコレクターにリストアできます。

Guardium での Amazon S3 へのアーカイブおよびバックアップ

Guardium から、Amazon S3 へのデータのアーカイブとバックアップを行う場合に、この機能を使用します。

Amazon S3 (Amazon Simple Storage Service) は、いつでも、Web 上のどこからでも容量に関係なく、データを格納/取得できるシンプルな Web サービス・インターフェースを提供します。これによって、Amazon が Web サイトの稼働に使用しているものと同じ、拡張性と信頼性が高く、安全でありながら安価なインフラストラクチャーを、あらゆる開発者が利用することが可能になります。

前提条件

1. Amazon アカウント
2. S3 サービスの登録
3. Amazon S3 にアクセスするためには、Amazon S3 の認証情報が必要です。 必要な認証情報は次のとおりです。
   - Access Key ID (アクセス・キー ID): ユーザーをサービス要求の担当者として識別します。各要求にこの ID が含まれている必要があります。これは機密ではなく、暗号化する必要はありません (20 文字の英数字から成るシーケンス)。
   - Secret Access Key (シークレット・アクセス・キー): Secret Access Key は Access Key ID に関連付けられ、要求に含まれているデジタル署名を計算します。Secret Access Key は機密事項であり、ユーザーと AWS のみが保持する必要があります (40 文字から成るシーケンス)。このキーは、ファイルではなく、単なる長い文字列であり、この文字列を使用して、要求内に含まれている必要があるデジタル署名を計算します。

- 「データ・アーカイブ」は、システムによって所定の期間内にキャプチャーされたデータをバックアップします。
- 「結果アーカイブ」は、監査タスクの結果 (レポート、アセスメント・テスト、エンティティー監査証跡、プライバシー・セット、および分類プロセス) のほか、表示およびサインオフの証跡、ワークフロー・プロセスからの調整コメントをバックアップします。

Guardium データがアーカイブされると、日ごとに別のデータ・ファイルができます。

アーカイブ・データ・ファイルの名前は、次の形式になります。

```
<time>-<hostname.domain>-w<run_datestamp>-d<data_date>.dbdump.enc
```

Guardium のアーカイブ機能では、改ざんできない、署名付きの暗号化ファイルが作成されます。生成されたアーカイブ・ファイルの名前を変更することはできません。アーカイブ操作は、アーカイブ処理中に作成されるファイル名に依存します。

ハードウェア破損が生じた場合にサーバーを復元する目的で、必要なすべてのデータと構成値をバックアップして保管するために、システム・バックアップを使用します。

すべての構成情報とデータが 1 つの暗号化ファイルに書き込まれ、このシステムのバックアップ用に構成された転送方式を使用して、指定の宛先に送信されます。

バックアップ・システム・ファイルの形式は、次のとおりです。

```
<data_date>-<time>-<hostname.domain>-SQLGUARD_CONFIG-9.0.tgz
<data_date>-<time>-<hostname.domain>-SQLGUARD_DATA-9.0.tgz
```

Guardium の「統合/アーカイブ・ログ」レポートを使用して、操作が正常に完了したことを確認してください。「管理」 > 「レポート」 > 「データ管理」 > 「統合/アーカイブ・ログ」をクリックして、「統合/アーカイブ・ログ」を開きます。各アーカイブ操作には、複数のアクティビティーがリストされていなければなりません。 また、各アクティビティーの状況は「*成功*」でなければなりません。

Guardium カタログは、アーカイブ・データの宛先に関係なくすべてのアーカイブ・ファイルの送信場所を記録するため、以降のどの時点においても、最小限の労力でシステムでアーカイブ・ファイルを取得およびリストアすることができます。

システムごとに個別のカタログが保守され、システムがデータや結果をアーカイブするたびにカタログに新しいレコードが追加されます。

カタログ・エントリーは、以下のいずれかの方法により、アプライアンス間で転送することができます。

- 統合 - カタログ表は統合されます。つまり、アグリゲーターが、そのすべてのコレクターのカタログをマージしたものを保持することになります。

- カタログのエクスポート/インポート - これらの機能は、コレクター間でカタログ・エントリーを転送したり、将来のリストアのためにカタログをバックアップしたりするために使用できます。
- データのリストア - 各データ・リストア操作には、アーカイブした日のデータ (その日のカタログも含む) が含まれます。 したがって、データのリストア時には、カタログも更新されます。

カタログ・エントリーは、別のシステムからインポートされたときには、そのシステムによって暗号化されたファイルをポイントします。 そのようなファイルをリストアまたはインポートする前に、そのファイルを暗号化したシステムのシステム共有パスワードが、インポート側のシステムで使用できなければなりません。

Guardium CLI からの Amazon S3 の有効化

Amazon S3 のアーカイブ/バックアップ・オプションは、デフォルトでは Guardium GUI で有効になっていません。Guardium CLI から Amazon S3 を有効にするには、次の CLI コマンドを実行します。

```
store storage-system amazon_s3 archive on
store storage-system amazon_s3 backup on
```

Amazon S3 では、Guardium システムのクロック時刻が正確であること (15 分以内) が求められます。 そうでない場合、Amazon のエラーとなります。要求の時刻と現在の時刻の差が大きすぎると、要求は受け入れられません。

Guardium のシステム時刻が正確でない場合は、次の CLI コマンドを使用して正しい時刻を設定してください。

```
show system ntp server
store system ntp server (An example is ntp server: ntp.swg.usma.ibm.com)
store system ntp state on
```

ユーザー・インターフェース

バックアップを構成するには、「システム・バックアップ」を使用します。「管理」 > 「データ管理」 > 「システム・バックアップ」をクリックして、「システム・バックアップ」を開きます。

以下のユーザー入力が必要です。

- S3 Bucket Name (S3 バケット名)。Amazon S3 に保管されるすべてのオブジェクトは、バケット内に格納されます。バケットは、Amazon S3 に保管されるオブジェクトの名前空間をパーティション化します。1 つのバケット内では、保管するオブジェクトに任意の名前を使用できますが、バケット名は Amazon S3 内の全バケットの中で一意である必要があります。
- Access Key ID
- Secret Access Key

バケット名が存在しない場合は、作成されます。

Secret Access Key は、データベースに保存されるときに暗号化されます。

Amazon S3 にファイルがアップロードされたことの確認

1. AWS マネジメント・コンソールに、E メール・アドレスとパスワードを使用してログオンします。

http://aws.amazon.com/console/

1. 「S3」をクリックします。
2. Guardium UI で指定したバケットをクリックします。

Guardium アプライアンスからデータをパージする方法

Guardium アプライアンスでは、次の 2 つの領域が満杯になる可能性があり、それが原因で GUI が停止する場合があります。

- 内部データベース
- ファイル・システム自体 (通常 /var パーティション)

ユーザー CLI として、次の CLI コマンドを使用してデータベースが満杯かどうか確認します。

support show db-status free %

これで 10% 以下という結果が返ってきた場合、データベースは 90% 以上が埋まっています。

/var パーティション (ファイル・システム) が 90% 以上埋まっているかどうか確認するために、CLI から must gather コマンドを実行します。

support must_gather system_db_info

ファイル・サーバーで表示できる system_output.txt ファイル内の df -k 出力を、ファイル・サーバーを使用して確認できます。

must_gather/system_logs/system_output.txt

または、このファイルは、system.<datetime>.tgz ファイルをダウンロードした後にそこから取り出します。

system_output.txt ファイル内で、詳細を確認できます。

以下では、/var パーティションが 65% 埋まっています。

==========2016-11-30 08:36:09 ... Output of df command:==========

Filesystem 1024-blocks Used Available Capacity Mounted on

/dev/sda3 10154020 2272668 7357232 24% /

/dev/sda2 28571320 17384504 9712052 65% /var

/dev/sda1 505604 33476 446024 7% /boot

tmpfs 6169768 0 6169768 0% /dev/shm

より新しい Guardium バージョンには、安全なキャッチ/機能が備わっており、これにより、データベースまたはファイル・システムが特定のレベルに到達すると、メイン・プロセスはそれ以上のデータを収集するのを停止します。

デフォルトでは、データベース、ファイル・システム、またはこれらの両方が 90% 埋まったらプロセスは停止します (この例は v10.1 の資料に基づきます)。CLI を使用して、安全なキャッチの現行値を確認できます。

CLI> show auto_stop_services_when_full

注: auto_stop_services_when_full がオフの場合、アプライアンスでは、システムが 100% 満杯になる可能性があり、それによりシステムにまったくアクセスできなります。

以下の回答で説明されている特定の状況で一時的に使用される場合を除き、auto_stop_services_when_full をオフにする必要はありません。以下の特定の状況では、説明に従ってオフにし、スペースの問題を解決した後にオンに戻す必要があります。

注: auto_stop をオフに切り替える前に inspection-core を停止する必要があります。これにより、システムはそれ以上満杯にならなくなります。

この場合、ファイル・システムまたはデータベースが 90% 満杯のときには、システムにより inspection-core およびその他のプロセスが自動的に停止されます。これには、GUI インターフェースが含まれます。このため、その時点で GUI に接続できなくなります。

次のコマンドを使用して、停止したサービスを再始動しようとすると、システム (および GUI インターフェース) は 5 分後に同じ理由で再び停止する可能性があります。
restart stopped_services

注: このコマンドは、スペースがリカバリーされたことを確認した後でのみ使用する必要があります。

データベースまたはファイル・システムが満杯で「自動停止」レベルになる前に、システム・ログ (メッセージ・ファイル) で警告を受け取るはずです。

自動停止がトリガーされる前に、スペースの問題に関する E メールが送信されるようにアラートを設定できます。Guardium のデータベースが満杯になったときのアラートを参照してください。

must_gather コマンドを実行し、作成された圧縮ファイル内を調べて、最新のメッセージ・ファイルが含まれているか確認できます。

support must_gather system_db_info

>>>GUI がダウンした場合、内部データベースからデータをパージする

自動停止がトリガーされた場合、GUI などのサービスが停止します。これにより、「今すぐ 1 回実行」パージ・オプションを使用したデータの緊急パージも実行できなくなります。

この緊急パージを実行するには、以下を行います。

- アプライアンスにデータがこれ以上フラッディングしないようにするために、コレクターで inspection-core をオフにする必要があります。

stop inspection-core

- show processlist を除くデータベース・コマンドが実行されていないことを確認します (必要な場合は、次のステップの前に、実行中のコマンドを終了してかまいません)。

support show db-processlist running

『What can I do if I see my Guardium Appliance getting full?』で説明されているように、GUI にアクセスしてパージを実行するために、単純に restart gui を実行できるようにする必要があります。

GUI が 5 分ごとにダウンするという問題が発生した場合、GUI を再始動し、一部のデータをパージできるようにするために、auto_stop_services_when_full を「一時的」にオフに切り替えることを検討してください。この方法で GUI を再始動した場合、5 分間だけ GUI が実行されます。十分なデータがパージされる前、またはパージの継続を設定する前に、メインの Nanny プロセスによってサービスが再び停止される場合があります。

注: auto_stop_services_when_full がオフの場合、アプライアンスでは、システムが 100% 満杯になる可能性があり、それによりシステムにまったくアクセスできなります。

ここで説明されている特定の状況で一時的に使用される場合を除き、auto_stop_services_when_full をオフにする必要はありません。特定の状況では、説明に従ってオフにし、スペースの問題を解決した後にオンに戻す必要があります。

auto_stop をオフに切り替える前に inspection-core を停止する必要があります。これにより、システムはそれ以上満杯にならなくなります。

CLI> store auto_stop_services_when_full off

CLI> show auto_stop_services_when_full [off | restart | gui]

これで、GUI にアクセスし、その後「データ管理アーカイブ (Data Management Archive)」にアクセスし、一部のデータを消去するためにパージの実行を設定できます。

データベースが満杯かどうか引き続き確認します。パージ・プロセスが終了すると統合アーカイブ・ログが表示されます。

プロセスが終了し、システムにスペースができた後、auto_stop を再びオンに設定し、停止しているサービスを再始動する必要があります。

store auto_stop_services_when_full on

restart stopped services

必要に応じて、inspection-core を開始します。

これで、データの収集が再び開始されるはずです。

システムが満杯になったとき、多くの場合、非常に多くのアクティビティーが記録されています。

親トピック: Guardium システムの管理
関連情報:
高度な Guardium システム管理および構成 (ビデオ)
Guardium データベースが満杯になる問題の予防および対処 (ビデオ)

Guardium カタログ

Guardium システムからデータをアーカイブすると、Guardium カタログは、すべてのアーカイブ・ファイルの送信先を追跡して、そのファイルを取得およびリストアできるようにします。

このタスクについて

Guardium システムごとに個別のカタログが保守され、データまたは結果をアーカイブするたびにカタログに新しいレコードが追加されます。カタログ・エントリーは、以下のいずれかの方法により、アプライアンス間で転送することができます。

- 統合: カタログ表は統合されます。つまり、アグリゲーターが、そのすべてのコレクターのカタログをマージしています。
- カタログのエクスポート/インポート: これらの機能は、コレクター間でカタログ・エントリーを転送したり、将来のリストアのためにカタログをバックアップしたりするために使用できます。
- データのリストア - 各データ・リストア操作には、アーカイブした日のデータ (その日のカタログも含む) が含まれます。データのリストア時には、カタログも更新されます。

カタログをアーカイブしたり、カタログを外部ストレージにエクスポートしたり、保管されているカタログをインポートしたりすることができます。

カタログ・エントリーは、別のシステムからインポートされると、そのシステムによって暗号化されたファイルをポイントします。そのようなファイルをリストアまたはインポートする前に、そのファイルを暗号化したシステムのシステム共有パスワードが、インポート側のシステムで使用できなければなりません。aggregator backup keys file CLI コマンドおよび aggregator restore keys file CLI コマンドを使用して、ある Guardium システムから別のシステムに共有パスワードをコピーすることができます。

親トピック: Guardium システムの管理

カタログのアーカイブ

手順

1. 「管理」 > 「データ管理」 > 「カタログ・アーカイブ」をクリックします。
2. 日付範囲を指定して選択可能なカタログ・エントリーを表示するか、カタログ・エントリーを追加することができます。 カタログ・エントリーを表示する場合:
   a. 「開始」に日付を入力し、データを必要とする最も古い日付を指定します。
   b. 「終了」に日付を入力し、データを必要とする最も新しい日付を指定します。
   c. オプション: 「ホスト名」に、アーカイブが行われた Guardium® システムの名前を入力します。
   d. 「検索」をクリックします。

   カタログ・エントリーを追加する場合:
   a. 「追加」をクリックします。
   b. 「ファイル名」を入力します。
   c. 「ホスト名」を入力します。
   d. ファイルの「パス」を入力します。
      注:

      FTP の場合、FTP アカウントのホーム・ディレクトリーを基準にした相対パスでディレクトリーを指定します。

      SCP の場合: 絶対パスとしてディレクトリーを指定します。

      TSM の場合: 元のロケーションの絶対パスとしてディレクトリーを指定します。

   e. このロケーションにアクセスするための「ユーザー名」および「パスワード」を入力します。
   f. 「保持」フィールドに、この項目をカタログ内に保持する日数 (デフォルト値は 365) を入力します。
   g. 「ストレージ・システム」メニューから、ファイルを格納するためのオプションを選択します。
   h. 「保存」をクリックします。
3. カタログ・エントリーを削除するには、カタログを開き、エントリーを選択して、「選択したものを削除 (Remove Selected)」をクリックします。
4. 完了したら、「完了」をクリックします。

カタログのエクスポート

手順

1. 「管理」 > 「データ管理」 > 「カタログ・エクスポート」をクリックします。
2. 「タイプ」ドロップダウン・リストから定義タイプを選択します。 「エクスポートする定義」リストに、選択したタイプの定義が設定されます。
3. このタイプの定義でエクスポートするものをすべて選択して、「エクスポート」をクリックします。 ご使用のブラウザーのセキュリティー設定に応じて、ファイルを保存するか開くかを訪ねるメッセージが表示される場合があります。
4. エクスポート・ファイルを保存するためのロケーションを選択します。

カタログのインポート

手順

1. 「管理」 > 「データ管理」 > 「カタログ・インポート」をクリックします。
2. 「参照」をクリックしてファイルを見つけ、選択します。
3. 「アップロード」をクリックします。操作完了時には通知が出され、ファイルに含まれる定義が表示されます。さらにファイルをアップロードするには、手順を繰り返します。
4. アップロード・ファイルをインポートする場合は「インポート」をクリックします。または、内容をインポートせずにアップロード・ファイルを削除する場合は「インポートなしで削除 (Remove without Importing)」をクリックします。

バックアップとアーカイブの管理方法

データを保持する方法を確立し、アクティビティー・ボリュームの制御を行い、データのアーカイブとパージのスケジューリングと、毎月のバックアップのスケジューリングを管理します。

付加価値: ベスト・プラクティス。データが損失しないように、データを保護してください。監査のために、いつでもデータにアクセスできるようにしてください。

システム・バックアップ機能を使用すると、オンデマンドまたはスケジュールに基づいて実行可能なバックアップ操作を定義できます。

ハードウェア破損が生じた場合にサーバーを復元する目的で、必要なすべてのデータと構成値をバックアップして保管するために、システム・バックアップを使用します。

使用可能なアーカイブ操作は 2 つあります。「管理」 > 「データ管理」に移動して、「データ・アーカイブ」機能または「結果アーカイブ」機能を選択します。

- 「*データ・アーカイブ*」は、Guardium システムによって所定の期間内にキャプチャーされたデータをバックアップします。データ・アーカイブを構成する際には、パージ操作も構成できます。 通常、データは、キャプチャーされた日の終わりにアーカイブされます。 こうすることで、災害発生時に失われるのはその当日のデータだけになります。 データのパージは、アプリケーションごとに異なり、ビジネス要件や監査要件によってかなり大きな違いがあります。 ほとんどの場合、データはマシン上に 6 カ月以上保持することができます。
- 「*結果アーカイブ*」は、監査タスクの結果 (レポート、アセスメント・テスト、エンティティー監査証跡、プライバシー・セット、および分類プロセス) のほか、表示およびサインオフの証跡、ワークフロー・プロセスからの調整コメントをバックアップします。結果セットは、ワークフロー・プロセスの定義に従ってシステムからパージされます。

統合環境では、データはコレクター、アグリゲーター、またはその両方のロケーションからアーカイブできます。 データは、一度だけアーカイブするのが最も一般的です。 アーカイブ元となるロケーションは、ユーザーの要件に応じて異なります。

データをアーカイブする際には、必ず操作が正常に完了したことを確認してください。 これを確認するには、管理者ユーザーとしてログインし、「管理」 > 「レポート」 > 「データ管理」 > 「統合/アーカイブ・ログ」をクリックして、「統合/アーカイブ・ログ」を開きます。各アーカイブ操作には、複数のアクティビティーがリストされていなければなりません。また、各アクティビティーの状況は「*成功*」でなければなりません。

データ・バックアップ

推奨されるデータ・バックアップのタイプは、以下の 3 つです。

1. フルバックアップ/システム・バックアップ
    a. 中央マネージャー・ユニットの週次または日次のフルバックアップ (スタンドアロンの中央マネージャーの場合)。
    b. アグリゲーターまたはコレクターについてオフピーク時に実行する月次のバックアップ。
2. アグリゲーターまたはコレクター用の日次アーカイブ。これらのアーカイブは、増分バックアップと考えることができます。アグリゲーターのアーカイブ・ファイルは、コレクターのアーカイブ・ファイルよりも大幅に大きくなります。例えば、1 つのアグリゲーターに対して 10 個のコレクターがデータを送信する場合、アーカイブ・ファイルの最初のサイズは、これら 10 個のコレクターのアーカイブ・ファイル全体と同じサイズになります。ただし、アグリゲーターのアーカイブ・ファイルには、毎日コレクターから送信されるのとは別のデータが含まれるため、このファイルのサイズは、コレクターのアーカイブ・ファイルをすべて組み合わせたサイズよりも大幅に大きくなります。
3. アグリゲーター用の結果アーカイブ (これは、日次バックアップとフルバックアップのデータの特殊なサブセットです)。結果アーカイブを使用する代わりに、すべてのユーザーがレビュー・プロセスを完了した後で、「監査プロセス」から PDF ファイルの保存操作を実行することもできます。

データの保持

データのバックアップとアーカイブ・ファイルは、災害からの復旧と、履歴調査または監査の目的で役立ちます。

以下の推奨事項は、社内のデータ保持ポリシーに基づいて変更することができます。例えば、組織によっては、すべてのバックアップを 18 カ月間保持しなければならない場合があります。

災害からの復旧目的でのデータ保持

- 各ユニットのフルバックアップを 3 カ月分ごとに循環して保持します。
- 管理対象コレクターの日次アーカイブを 2 週間ごとに循環して保持します。

注: スタンドアロンのコレクターを使用している場合、日次アーカイブは、データ保持ポリシーに従って保存してください。

履歴調査または監査目的でのデータ保持

- アグリゲーターのすべての日次アーカイブを、監査ポリシーまたは会社のデータ保持ポリシーで定義されている期間だけ保持します。

記憶容量

以下に示すサイズは、補助ストレージ容量を計画するためのバックアップとアーカイブ・ファイルのサイズの見積もりまたは範囲にすぎません。

実際のサイズは、(1) Guardium コレクターに記録されるデータベース・アクティビティーのボリュームおよび細分度と、(2) バックアップ・ファイルの保存期間に応じて異なります。

日次アーカイブ

コレクター: 約 40 MB (特権ユーザー・モニターの場合) から 1 GB (すべてのトラフィックについてすべての詳細を記録する広範なモニターの場合) まで。

アグリゲーター: コレクターの数のおおよその倍数。例えば、コレクターの数に 40 MB を掛けた値。

月次システム・バックアップ: Dell R610 または IBM xSeries 3550 M4 (600 GB ディスク) で、データベースが 50% 使用されていることを想定

注: このバックアップでは、バックアップ・ファイルの圧縮比率は約 1:8 になります。

コレクター: 7 GB から 10 GB まで

アグリゲーター: 16 GB から 20 GB まで

中央マネージャー (集約なし): << 1 GB

結果アーカイブ

実装された監査プロセスの数と頻度によって異なります。

アクティビティー・ボリュームの制御

データベース・サーバーでモニターされるアクティビティーと、コレクターに記録されるアクティビティーのボリュームを制御すると、ネットワーク使用率の削減、Guardium システムのデータベース・ディスク使用量の削減、IBM Security Guardium インフラストラクチャーの全体的な性能とパフォーマンスの改善に役立ちます。

この制御は、主に、検査エンジン構成を介してポリシー・ルールで行われます。

一般的なガイドラインを以下に示します。

- 検査エンジンで、ポート範囲は使用しないでください。
- 信頼できるアプリケーションとバッチ・プログラムをすべて特定してください。通常、これらのプログラムによって大量のデータベース・アクティビティーが生成されるため、可能であれば、「S-TAP セッションを無視」アクションまたは「ロギングをスキップ」アクションを使用して、これらのアクティビティーを無視またはスキップしてください。
- 必要である場合を除き、「全詳細をロギング」アクションは使用しないでください。
- 可能であれば、選択的な監査ポリシーを「S-TAP セッションを無視」ルールとともに使用して、ネットワーク・トラフィックを最小化してください。
- 例えば、抽出ルールを使用しない場合、結果セットは検査されません。結果セットが Guardium システムに送信されないように、「セッションごとに応答を無視」アクションを使用することを検討してください。
- 新しいデータベースとアプリケーションに対応するために、ポリシー・ルール (グループを含む) のレビューと更新を定期的に実行するプロセスを確立してください。
- SQL エラーを定期的にモニターし、DBA とアプリケーションの開発チームが修復を行うためのプロセスを確立してください。

スケジューリング

以下の表に、Guardium システムで構成する必要がある主なスケジュールの要約を示します。この表の下に、各プロセスの簡単な説明があります。

「統合/アーカイブ・ログ」を使用すると、各プロセスの時刻と状況が記録されるため、スケジューリング時刻の調整に役立ちます。

以下の表に、コレクターとしてデプロイされる、Guardium システムのタスクのスケジュールをリストします。

機能	スケジュール
データ・エクスポート (アグリゲーターへのエクスポート)	日次*: 12:30 AM
データのアーカイブとパージ	日次: 01:30 AM、15 日分をパージ
監査/ワークフローのジョブ	日次: 03:00 AM (スタンドアロンの場合)
SCP/FTP サーバーへの CSV/CEF のエクスポート	日次: 05:00 AM、監査ジョブ内で構成されていて、かつその監査ジョブが完了している場合。
ホスト名の別名割り当て	日次: 10:00 PM
ポリシーの再インストール	日次: 11:00 PM
システム・バックアップ	月次: 毎月第 1 日曜日の 6:00 AM

以下の表に、アグリゲーターとしてデプロイされる、Guardium システムのタスクのスケジュールをリストします。

機能	スケジュール
データのアーカイブとパージ	日次: 4:00 AM、30 日分をパージ
データ・インポート (コレクターからのインポート)	日次 1:15 AM
監査/ワークフローのジョブ	日次: 03:30 AM
SCP/FTP サーバーへの CSV/CEF のエクスポート	日次: 05:15 AM、監査ジョブ内で構成されていて、かつその監査ジョブが完了している場合。
ホスト名の別名割り当て	日次: 10:00 PM

システム・バックアップ	月次: 毎月第 1 日曜日の 7:00 AM

注: 各 Guardium システムにおける内部の始業時処理と競合することを避けるため、12:15 AM よりも前の時刻にはスケジューリングしないでください。

日次データ・アーカイブを設定する場合は、1 日以上経過したデータをアーカイブし、2 日以上経過したデータについては無視するように設定してください。 初回の実行では、すべてのデータがデータベースにアーカイブされ、それ以降の処理では、前日のデータだけがアーカイブされます。

オンラインで保持されるデータの量は各 Guardium システムのデータベースのサイズによって制限されるため、パージ処理は、オンラインで保持されるデータ量の管理に役立ちます。パージ処理は、日次アーカイブと連携して機能します。データベースがいっぱいになるのを避け、データベースのパフォーマンスを改善するために、必要最小限の量のデータだけを保持することをお勧めします。

コレクターの場合、コレクター用に 15 日分、アグリゲーター用に 30 日分のデータを保持することをお勧めします。ただし、実際の期間は、記録されるデータの量 (S-TAP の数、ポリシー・ルールの数、コレクターの数など) によって異なります。

データのエクスポートとインポート

前日に記録されたアクティビティーは、コレクターから、そのコレクターに割り当てられたアグリゲーターへ、統合レポート用に毎日エクスポートされます (プッシュ処理)。 このアクティビティーは、アグリゲーターでの「データ・インポート」に対応しています。

注: 利便性を考慮して、「アーカイブ」設定画面でも「エクスポート」設定画面でもパージを構成できるようになっています。

データ・インポート処理は、アグリゲーター上でのみスケジュールされます。この処理では、コレクターからエクスポートされた前日のデータがインポートされて処理されます。

月次バックアップ

既に説明したように、システム・バックアップはフルバックアップであり、災害からの復旧目的で使用されます。以下に、毎月第 1 日曜日の 6:00 AM に開始される月次スケジュールの例を示します。

親トピック: Guardium システムの管理

結果のエクスポート (CSV、CEF、PDF)

CSV、CEF、および PDF ファイルをワークフロー・プロセスで作成できます。この機能で、Guardium システム上に存在するこれらのファイルをすべてエクスポートします。

ワークフロー・プロセスによって作成される CEF/CSV ファイルを syslog に書き込むこともできます。この処理が行われた場合、それらのファイルはここで説明する方法でエクスポートすることはできません。 それらのファイルは、他の方法で syslog からアクセスする必要があります。

CSV、CEF、および PDF ファイルをエクスポートするには、以下のようにします。

1. 「管理」 > 「データ管理」 > 「結果エクスポート (ファイル)」をクリックして、「結果エクスポート (ファイル)」を開きます。
2. 「プロトコル」ラジオ・ボタンから、オプション (SCP、FTP、Amazon S3、または Softlayer) を選択します。
3. 「ホスト」に、ファイルを受信するホストの IP アドレスまたは DNS ホスト名を入力します。
4. 「ディレクトリー」に、データの格納先ディレクトリーを指定します。このディレクトリーの指定方法は、選択したプロトコルによって異なります。
   - FTP の場合: FTP アカウントのホーム・ディレクトリーに対する相対パスでディレクトリーを指定します。
   - SCP の場合: 絶対パスとしてディレクトリーを指定します。
5. SCP および FTP を介するファイル送信に使用できるポートに変更します。SSH、FTP、および SFTP のデフォルトのポートは 22 です。FTP のデフォルトのポートは 21 です。
6. 「ユーザー名」および「パスワード」に、ホスト・マシンにログインするユーザーの資格情報を入力します。 このユーザーは、「ディレクトリー」フィールドで指定したディレクトリーに対する書き込み権限/実行権限を保持していなければなりません。
7. 「スケジューリング」セクションを使用して、この操作を定期的に実行するためのスケジュールを定義できます。
8. 「保存」をクリックして構成を保存します。システムはそのロケーションにテスト・データ・ファイルを送信することにより、構成の検証を試みます。この操作が失敗した場合は、エラー・メッセージが表示されます。
9. 「今すぐ 1 回実行」をクリックして、操作を 1 回実行します。
10. ファイルがエクスポートされたことを検証するには、「統合/アーカイブ・ログ」にチェック・マークを付けます。エクスポートした CSV または CEF ファイルのそれぞれに、「送信」アクティビティーがなければなりません。

デフォルトの区切り文字を定義するには、「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックして、「グローバル・プロファイル」を開きます。

すべてのファイル名に含めるラベルを入力するには、「ツール」 > 「監査プロセス・ビルダー」に移動します。
注:

Syslog メッセージの最大サイズは 4000 です。CSV 結果は、この制限を超えると切り捨てられます。

.CSV ファイルを読み取るために使用するアプリケーションが何であっても、エンコードは UTF-8 に設定します。Excel では、異なる文字セットがデフォルトではされるため、.CSV ファイルが破損する可能性があります。Excel を使用する場合、単にファイルを開くのではなく、またはファイルの関連付けに基づいて Excel を起動するのではなく、.CSV ファイルをインポートし、UTF-8 エンコードを選択します。

親トピック: Guardium システムの管理

定義のエクスポート/インポート

要件が同じまたは同じようなシステムが複数あり、一元管理を使用していない場合は、これらのシステムのソフトウェア・リリース・レベルが同じであれば、必要なコンポーネントを 1 つのシステムで定義し、その定義を他のシステムにエクスポートできます。

一度にエクスポートできる定義のタイプ (例えばレポート) は 1 つです。 要素のエクスポートごとに、参照される他の定義もエクスポートされます。 例えば、レポートは常に照会に基づいており、IP アドレス・グループや期間などの他の項目も参照することがあります。 参照される定義はすべて (セキュリティー・ロールを除く)、レポート定義と共にエクスポートされます。 ただし、その定義が複数のエクスポート項目で参照される場合は、1 つの定義のコピーのみがエクスポートされます。 ポリシーまた

は照会のエクスポートでは、エクスポートされるポリシーまたは照会が参照するグループのみがエクスポートされます。 これまでは、ポリシーまたは照会をエクスポートすると、すべてのグループがエクスポートされていました。

定義のエクスポート/インポート
定義のエクスポートおよびインポートを使用して、特定の Guardium システムから機能データを保存した後、復元します。 例えば、この機能により、1 つの Guardium システム上でレポートを作成し、次に同じ Guardium のバージョンがインストールされている別のサーバー上にその同じレポートをインポートすることができます。
注: この機能は、サーバーのフルバックアップと同じではありません。この機能を使用していても、定期的に、または手動により、バックアップを定義して実行する必要があります。
定義のエクスポート - これは、レポート/照会、CAS データ、分類データなど、定義されている機能値を保存して共有するために使用されます。エクスポート・タイプは PC 上に .sql ファイル・タイプとして保存されます。
定義のインポート - この機能は、同じ Guardium ソフトウェア・バージョンを使用しているサーバー上に、エクスポート済み定義をインポートするために使用されます。例えば、Guardium V10 システムから定義をエクスポートする場合は、別の V10 システムにのみ、それらの定義をインポートできます。

注:

- グラフィカル・レポートをエクスポートする場合、表示パラメーター設定 (色、フォント、タイトルなど) はエクスポートされません。これらのレポートをインポートすると、インポート側システムのデフォルトの表示パラメーター設定が使用されます。
- サブスクライブしたグループはエクスポートされません。 サブスクライブしたグループを参照する定義をエクスポートする場合は、参照されるサブスクライブしたグループをすべて、インポート側アプライアンス (フェデレーテッド環境では中央マネージャー) にインストールしておく必要があります。
- エクスポート/インポート定義のログの保存期間は、モニターされるデータベースのアクティビティー・ログと同じです。
- コメントはエクスポートに含まれません。
- 実行がスケジュール設定 (スケジュール時刻を含む) された監査プロセス定義を別のシステムにエクスポートした場合、「監査プロセス・ビルダー」の「アクティブ」チェック・ボックスにチェック・マークは付けられません (非アクティブ)。
- 1 つのアプライアンスで定義されて別の (無関係の) アプライアンスにエクスポートされた監査プロセスの「開始時刻のスケジュール設定」- 元の「開始時刻のスケジュール設定」が定義されている場合は、保持されます。 元の「開始時刻のスケジュール設定」が定義されていない場合 (空の場合)、インポートされた「開始時刻のスケジュール設定」は、それがインポートされた時刻に設定されます。
- オープン・ソース・ドライバーを使用するデータ・ソースをエクスポートする場合、オープン・ソース・ドライバーはエクスポートに含まれません。オープン・ソース・ドライバーを使用して作成されたデータ・ソース定義をインポートする前に、まずそのオープン・ソース・ドライバーを新しいシステムにアップロードしておく必要があります。そうしないと、データ・ダイレクト・ドライバーがインポートされると、それがオープン・ソース・ドライバーの代わりに使用されるようになります。
- 大規模で複雑なインポートでは、かなり時間がかかることがあり、ユーザーのセッションの長さを超える場合があります。 この状況になってセッションがタイムアウトになっても、インポートは完了するまでバックグラウンドで実行され続けます。
- 分類ポリシーの定義をエクスポートする場合、ポリシーに関連付けられているカスタム評価クラスは定義と共にエクスポートされません。インポート済みポリシーを動作させるには、カスタム評価クラスを個別にアップロードする必要があります。
- 異なる言語間での定義のエクスポート/インポートは機能しません。例えば、中国語 (簡体字) の Guardium® システムからファイルをエクスポートし、英語の Guardium システムにそのファイルをインポートしようとしても成功しません。

XACML プロトコルへのエクスポート

Guardium は、XACML ファイルへのポリシー・ルールのエクスポート、および別の Guardium システムへの XACML ファイルのインポートをサポートしています。

XACML (eXtensible Access Control Markup Language) は、XML 内に実装される宣言アクセス制御ポリシー言語で、ポリシーの解釈方法を記述する処理モデルでもあります。

標準的な XACML のエクスポート/インポートが双方向のインターフェースとして使用され、Optim Designer と Guardium の間でポリシー・ルールが転送されます。

Optim Designer は、さまざまな目的で、さまざまな手段によってデータ値を変換できます。コア Optim ランタイム (z/OS および Distributed) において、列マップ内で宣言されたデータ・プライバシー関数を呼び出すことにより、この操作が行われます。 Optim Privacy では、これは属性に対するデータ・プライバシー・ポリシーの適用としてユーザーにより指定され、データ・アクセス・プラン内のエンティティーによって参照されます。

Optim Privacy と Guardium の両方を購入したお客様は、一方の製品からポリシーとプライバシーの情報を XACML にエクスポートし、他方の製品にインポートすることができます。

注: 以前のバージョンの Guardium からの XACML インポートはサポートされていません。
Guardium のポリシーを XACML にエクスポートするには、以下の手順を実行します。

1. 「管理」 > 「データ管理」 > 「エクスポート」をクリックします。
2. 「タイプ」メニューから「ポリシー」を選択します。
3. 「XACML ファイルへのエクスポート」チェック・ボックスにチェック・マークを付けます。
4. 「エクスポートする定義」メニューから定義を選択します。
5. 「エクスポート」をクリックします。

別の Guardium システムまたは Optim Privacy から XACML ファイルをインポートするには、「管理」 > 「データ管理」 > 「インポート」をクリックして、「定義のインポート」を開きます。

グループのインポート

既に存在するグループをインポートする場合、メンバーが追加される場合がありますが、メンバーが削除されることはありません。

別名のインポート

別名をインポートする場合、新しい別名が追加される場合がありますが、別名が削除されることはありません。

インポートされた定義の所有権

定義が作成されると、それを作成したユーザーが、その定義の所有者として保存されます。 この意味は、その定義にセキュリティー・ロールが割り当てられていなければ、それへのアクセス権限があるのは、所有者と admin ユーザーのみであるということです。

定義がインポートされると、所有者は常に admin ユーザーに変更されます。

インポートされた定義のロール

セキュリティー・ロールの参照は、エクスポートされた定義から削除されます。 したがって、インポートされた定義には、ロールが割り当てられていません。

インポートされた定義のユーザー

エクスポートされる定義内にユーザーの参照があると、そのユーザー定義がエクスポートされます。 定義がインポートされるとき、参照されるユーザー定義がインポートされるのは、インポート側システムにそのユーザー定義が存在しない場合のみです。つまり、既存のユーザー定義に上書きされることはありません。『ロールおよびユーザーの重複に関する考慮点』に記載されているように、これにはいくつかの考慮点があります。

なお、インポートされたユーザー定義は使用不可に設定されます。つまり、インポートされたユーザーは、インポート側システムから送信された E メール通知を受信できますが、管理者がそのアカウントを使用可能に設定するまで、そのシステムにログインできないことになります。

グループおよびユーザーの重複に関する考慮点

エクスポートされた定義によって参照されるグループがインポート側システムに存在する場合、エクスポート側システムからのそのグループの定義はインポートされません。そのために、両方のシステムでグループが同じ目的に使用されていない場合は、何らかの混乱が生じる可能性があります。

インポート側システムにユーザー定義が存在する場合、エクスポート側システムで定義されたその同じ個人のユーザー定義ではない可能性があります。例えば、エクスポート側システムでは、E メール・アドレスが john_doe@aaa.com のユーザー jdoe は、エクスポートされたアラートからの出力の受信者であるとします。 一方、インポート側システムでは、E メール・アドレスが jane_doe@zzz.com のユーザー jdoe が既に存在するとします。 エクスポートされたユーザー定義はインポートされません。インポートされたアラートが起動すると、E メールは jane_doe@zzz.com アドレスに送信されます。いずれにしても、セキュリティー・ロールまたはユーザー定義がインポートされないときは、両方のシステムでの定義を確認して、違いがないか調べてください。 違いがある場合は、それらの定義に対して適切な調整を行ってください。

エクスポートの定義タイプ

表 1. エクスポートの定義タイプ

エクスポート可能	エクスポート不可
アラート	カスタム・アラート・クラス 「定義のエクスポート」画面には、グループ・メンバーの除外を行うチェック・ボックスがあります。 グループ明細項目の説明を参照してください。
別名	カスタム評価テスト
監査プロセス	カスタム識別プロシージャー
オートディスカバリー・プロセス	
CAS ホスト	
CAS テンプレート・セット	
分類プロセス	アクセス・ルール
分類ポリシー	
カスタム・クラス接続の許可	
カスタム・ドメイン	
カスタム表	
データ・ソース	
イベント・タイプ	
グループ	「定義のエクスポート」画面には、グループ・メンバーの除外を行うチェック・ボックスがあります。 このチェック・ボックスは、エクスポート階層のいずれかの場所にグループが存在するデータ・セットの場合にのみ表示されます (例えば、アラートのエクスポートにはアラートの照会も含まれ、照会に照会条件内のグループが含まれることがあります)。データ・ソースのエクスポートにグループが含まれていない場合は、このチェック・ボックスは表示されません。 このチェック・ボックスが設定されている場合、エクスポート・ファイルにはグループが含まれています (グループがエクスポートされた定義にリンクされている場合) が、グループのメンバーはエクスポートされません。 このチェック・ボックスはデフォルトでは設定されず、その状態は永続的ではありません。また、現在のエクスポートにのみ適用されます。
名前付きテンプレート	
期間	
ポリシー (組み込まれたベースラインではない)	
プライバシー・セット	
照会	
Replay	
レポート	「定義のエクスポート」画面には、グループ・メンバーの除外を行うチェック・ボックスがあります。 グループ明細項目の説明を参照してください。
ロール	

エクスポート可能	エクスポート不可
セキュリティー・アセスメント	
ユーザー	
ユーザー・データベース・マッピング	
ユーザー・データベース・アクセス権	
ユーザー階層	

エクスポート定義

1. 「管理」 > 「データ管理」 > 「エクスポート」をクリックして、「定義のエクスポート」ペインを開きます。
2. 「タイプ」メニューからオプションを選択します。「エクスポートする定義」ボックスに、選択したタイプの定義が設定されます。
3. このタイプのすべての定義をエクスポートすることを選択します。
   注: 名前に引用文字が 1 つ以上含まれるポリシー定義はエクスポートしないでください。こうした定義はエクスポートできますが、インポートできません。 このような定義をエクスポートするには、そのコピーを作成し、引用文字を使用しない名前を付けた後にエクスポートします。
4. 「エクスポート」をクリックします。ご使用のブラウザーのセキュリティー設定に応じて、ファイルを保存するか、それともエディターを使用して開くかを尋ねる警告メッセージが表示される場合があります。
5. エクスポート・ファイルを適切な場所に保存します。

インポート定義

1. 「管理」 > 「データ管理」 > 「インポート」をクリックして、「定義のインポート」ペインを開きます。
2. 「参照」をクリックしてファイルを見つけ、選択します。
3. 「アップロード」をクリックします。操作完了時には通知が出され、ファイルに含まれる定義が表示されます。追加のファイルをアップロードするには、手順を繰り返します。
4. 直接インポートされた、または照会やポリシーなどの他のデータ・セットを通じてインポートされた新規グループ・メンバーの追加方法の動作を設定するには、「グループ・メンバーを完全に同期」チェック・ボックスを使用します。 このチェック・ボックスをオフにすると、インポートされた新規メンバーは追加され、一方でインポートされなかったメンバーは削除されません。このチェック・ボックスをオンにすると、インポートされなかったグループ・メンバーは削除されます。チェック・ボックスの設定を保存するには、チェック・ボックスの横にある「デフォルトとして設定」ボタンを使用します。
5. 「この定義セットをインポート」をクリックすると、定義セットがインポートされます。または「この定義セットをインポートなしで削除」をクリックすると、定義をインポートせずに、アップロード・ファイルが削除されます。
6. いずれのアクションの場合も、確認を求めるプロンプトが出されます。
   注: インポート操作では、既存の定義に上書きされません。既存の定義と同じ名前の定義をインポートしようとすると、その項目は置き換えられなかったことが通知されます。 インポートされた定義で既存の定義を上書きする場合は、インポート操作を実行する前に、既存の定義を削除する必要があります。

親トピック: Guardium システムの管理

分散インターフェース

この構成画面は、分散インターフェースを定義し、プロトコル・バッファー (.proto) ファイルを DIST_INT データベースにアップロードするために使用します。

このデータベースから、照会ドメイン・メタデータが自動的に作成されます。 メタデータの作成後、ユーザーは「カスタム・ドメイン・ビルダー」に移動して、データを変更したり、コピー作成したりして、カスタム・レポートを作成することができます。分散インターフェース・データは、プロトコル・バッファーを使用します。 プロトコル・バッファーは、構造化データをシリアライズするための、柔軟、効率的、かつ自動化されたメカニズムです。

Universal Feed タイプ 3 の場合、「管理」 > 「データ管理」 > 「分散インターフェース」をクリックして、DIST_INT データベースの構成用のプロトコル定義ファイルをアップロードします。

注: 表エンジン・タイプと表索引を管理する場合は、「メンテナンス」をクリックします。Guardium 内部データベースに保管されるデータが MYSQL ベースのため、Universal Feed 表の表エンジン・タイプ (InnoDB および MyISAM) が、すべての Universal Feed 表に対して表示されます。 InnoDB および MyISAM の保守について詳しくは、外部データ相関を参照してください。

分散インターフェースの構成

1. 「管理」 > 「データ管理」 > 「分散インターフェース」をクリックして、「分散インターフェース・ファインダー」を開きます。
2. 「新規」をクリックして、新しい分散インターフェースを作成するか、「分散インターフェース・ファインダー」から既存の分散インターフェースを選択して、「変更」または「削除」をクリックします。
3. 「ベンダー ID」に、ベンダーの ID (例えば、20000) を入力します。
4. 「ドメイン・ネーム」に、カスタム・ドメイン・ビルダーから選択可能になるドメインの名前を入力します。
5. 「統合に包含」にチェック・マークを付けます。
6. 「ファイル名」で、「参照」をクリックしてファイルを選択します。
7. 「適用」をクリックして、この構成を保存します。
8. 「カスタム・ドメイン・ビルダー」でカスタム・レポートを作成します。 「設定」 > 「ツールとビュー」 > 「カスタム・ドメイン・ビルダー」をクリックして、「カスタム・ドメイン・ビルダー」を開きます。

.proto ファイルの例

```
package bim;
option java_package = "com.ibm.infosphere.bim.proto";
option java_outer_classname = "BimEvent";
// NOTE: AssetID and Property_type (== Property name!) are strings.
// For AssetID , it is safest to use a UUID since it provides world-wide unique ID.
// This will be the key to the table of current metrics and property values.
// per each asset, per each property , there will be one value (recent, or min, or max,etc)
message EventTypeID {
```

```
    required string eventType                   = 1; //e.g. Schema change
}
message AssetID {
    required string assetId                     = 1;
}
message InfoPropertyID {
    required string assetId                     = 1;
    required string propertyName                = 2;
}
message MetricPropertyID {
    required string assetId                     = 1;
    required string propertyName                = 2;
}
message AssetRelationID {
    // These are asset "native" ids
    required string sourceAssetId               = 1;
    required string targetAssetId               = 2;
}
message RelationPropertyID {
    required string assetRelationId             = 1;
    required string propertyName                = 2;
}
message Event {
    optional InnerEvent innerEvent              = 1;
}
message InnerEvent {
    // Common for all events
    optional EventTypeID eventTypeId                = 1;
    optional string description                     = 2;
    optional string time                            = 3;
    optional string agentId                         = 4;
    // Event can be for asset info, or metric property
    optional AssetInfoEvent assetInfoEvent          = 5;
    optional MetricPropertyEvent metricPropertyEvent  = 6;
    optional AssetRelationEvent  relationEvent      = 7;
    optional RuleEvent ruleEvent                    = 8;
}
message AssetInfoEvent {
    optional AssetID unique_key__               = 1;
    optional string assetType                   = 2;
    optional string assetName                   = 3;
    optional string gdm_server_ip               = 4;
    optional string gdm_service_name            = 5;
    repeated InfoProperty property              = 6;
}
message InfoProperty {
    optional InfoPropertyID unique_key__        = 1;
    optional string value                       = 2;
}
message MetricPropertyEvent {
    optional AssetID assetId                    = 1;
    repeated MetricProperty property            = 2;
}
message MetricProperty {
    optional MetricPropertyID unique_key__      = 1;
    optional AssetID assetId                    = 2;
    optional string stringValue                 = 3;
    optional double doubleValue                 = 4;

    enum Data_type {
        DOUBLE                                      = 1;
        LONG                                        = 2;
        INT                                         = 3;
        FLOAT                                       = 4;
        DATE                                        = 5;
        BOOLEAN                                     = 6; // convention is to store it
as 0 and 1 in the double_value
        STRING                                      = 7; // stored in string_value
    }
        optional Data_type dataType                 = 5;
    optional string unit                        = 6; // unit for the value
}
message AssetRelationEvent {
    optional AssetRelationID unique_key__       = 1;
    required string relationshipType            = 2;
    repeated RelationshipProperty property      = 3;
    optional bool deleted                       = 4;
}
message RelationshipProperty {
    optional RelationPropertyID unique_key__    = 1;
    optional string value                       = 2;
}
message RuleEvent {
    optional string ruleName                    = 1;
    optional bool enabled                       = 2;
}
// --- Metadata --- All unique identifier must be defined here
message Identifier {
    optional InfoPropertyID infoPropertyId              = 1;
    optional MetricPropertyID metricPropertyId          = 2;
    optional AssetID assetId                            = 3;
    optional AssetRelationID assetRelationId            = 4;
    optional RelationPropertyID relationshipPropertyId  = 5;
}
```

親トピック: Guardium システムの管理

カスタム・クラスの管理

アラートまたは評価で使用されるカスタム・クラスをアップロードして保守します。 カスタム・クラスを管理するには、「設定」 > 「カスタム・クラス」をクリックします。

クラスをコンパイルした後、これを Guardium® システムにアップロードする必要があります。

カスタム・クラスのアップロード

1. アラートまたは評価のためのカスタム・クラスをアップロードできます。「設定」 > 「カスタム・クラス」をクリックしてから、「アラート」 > 「アップロード」または「評価」 > 「アップロード」のいずれかをクリックして、カスタム・クラスをアップロードします。
2. カスタム・クラスの説明を入力します。
3. 「参照」をクリックし、アップロードするクラス・ファイルを見つけ、選択します。
4. 「適用」をクリックします。

カスタム・クラスのアップデート

1. 「設定」 > 「カスタム・クラス」を選択してから、「アラート」 > 「更新」または「評価」 > 「更新」のいずれかを選択します。
2. 更新するクラスの「説明」を選択します。
3. 「参照」をクリックして、更新に使用するクラス・ファイルを見つけ、選択します。
4. 「適用」をクリックします。

カスタム・クラスの削除

1. 「設定」を選択してから、「アラート」 > 「削除」または「評価」 > 「削除」のいずれかを選択します。
2. 削除するクラスの「説明」を選択します。
   注: 他のコンポーネントで使用中のクラスは削除できません (インストールされたポリシーなど)。
3. 「削除」をクリックします。

親トピック: Guardium システムの管理

鍵ファイルのアップロード

まれなケースですが、暗号化 SQL Server トラフィックをモニターするために、Microsoft SQL Server の鍵ファイルを Guardium® システムにアップロードしなければならない場合があります。

S-TAP® が SQL Server にインストールされていて、暗号化を処理するように構成されている場合、鍵ファイルは必要ありません。 これは、MS SQL Server 用の S-TAP エージェントを構成する場合に推奨される方法であり、最も一般的な方法です。 S-TAP が暗号化 MS SQL Server トラフィックを処理するように構成されているかどうかを判別するには、以下のようにします。

1. 「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」をクリックして、「S-TAP 制御」を開きます。
2. MS SQL Server ホスト上の S-TAP エージェントの「詳細」ペインを展開します。
3. 「*SQL Server TAP 暗号化解除*」プロパティーが「SSL のみ」または「Kerberos および SSL」のいずれかに設定されていることを確認します。
4. 「*SQL Server TAP 暗号化解除*」プロパティーが「なし」に設定されている場合は、この設定値を「SSL のみ」または「Kerberos および SSL」のいずれかに変更することをお勧めします。Windows S-TAP の構成について詳しくは、GUI からの S-TAP の構成を参照してください。
   注: 「*SQL Server TAP 暗号化解除*」プロパティーを変更した後は、変更内容を有効にするために、S-TAP と MSSQL モニター・サービスを再始動する必要があります。

   何らかの理由で「SQL Server TAP 暗号化解除」の設定を変更することを許可されていない場合は、この手順を使用して、サーバーから鍵ファイルをアップロードしてください。

S-TAP がインストールされていない場合、またはインストールされていても暗号化 SQL Server トラフィックを処理するように構成されていない場合、以下の条件下で SQL Server トラフィックをモニターするためには鍵ファイルが必要です。

- 「プロトコルを強制的に暗号化する」オプションを使用してサーバーが構成されている場合。
- SQL Server 2005 環境内のサーバーが、SQL Server 混合認証による暗号化ログイン・セッションを使用している場合。

単一の Guardium システムが複数の SQL Server インスタンスをモニターしている場合があるため、複数の鍵ファイルをアップロードする必要が生じることがあります。Guardium システムに鍵ファイルをアップロードするには、以下のようにします。

1. 「設定」 > 「ツールとビュー」 > 「鍵ファイルのアップロード」をクリックします。
2. 「参照」をクリックして、アップロードする鍵ファイルを見つけます。
   注: 鍵ファイル名は、SQL Server の完全修飾ドメイン名でなければなりません。 クラス・ファイルの名前は変更できないため、この名前で作成する必要があります。
3. 「鍵ファイルのアップロード」をクリックします。操作の結果が通知されます。

親トピック: Guardium システムの管理

SSH 公開鍵

この情報を使用して、SSH 公開鍵を作成、変更、または削除します。

1. 「管理」 > 「アクティビティー・モニター」 > 「SSH 公開鍵管理」をクリックして、以下のいずれかを実行します。
   - 鍵を作成するには、「新規」をクリックします。

- 鍵を生成するには、「生成」をクリックします。
- 鍵を変更するには、リストからその鍵を選択し、「変更」をクリックします。
- 鍵を削除するには、リストからその鍵を選択し、「削除」をクリックします。

2. 「SSH 公開鍵編集」パネルで適切な情報を入力し、「適用」をクリックして保存します。

親トピック: Guardium システムの管理

ブラウザーの SSL 証明書チャレンジを回避するためのアプライアンス証明書のインストール方法

IBM Security Guardium CLI コマンドを使用して、証明書署名要求 (CSR) の作成、および Guardium® システム上へのサーバー証明書、認証局 (CA) 証明書またはトラステッド・パス証明書のインストールを行います。

このタスクについて

以下のような証明書エラーの警告画面が表示されなくなります。

```
There is a problem with this website's security certificate.  The security certificate presented by this website was issued  for a different website's address. Security certificate problems may indicate an attempt to fool  you or intercept any data you send to the server.
```

すべての証明書コマンドの詳細については、『証明書 CLI コマンド』を参照してください。

注: 1 つの前提条件は、証明書の署名のために使用する CA (Verisign、Thwate、Geotrust、GoDaddy、Comodo、within-your-company など) からの公開証明書を用意しておくことです。
注: Guardium は、CA サービスは提供しません。また、デフォルトでインストールされているもの以外の証明書をシステムに添付することもありません。独自の証明書を希望するお客様は、サード・パーティー CA にお問い合わせください。
注: 証明書に自己署名がない場合、最低レベルのパブリック証明書 (例えば、自己署名がある証明書) を署名者ごとに取得する必要もあります。openssl x509 -in t.pem -text -noout コマンドを使用すると、x509 証明書の内容を表示できます。

手順

1. 証明書の署名のために使用する CA (認証局) (Verisign、Thwate、Geotrust、GoDaddy、Comodo、自社内など) から取得した公開証明書を使用できる状態にします。
2. 署名付きの証明書を配置する個々の Guardium システムで CLI にログインします。

   コマンドを実行する前に、該当する証明書 (バイナリー形式ではなく PEM 形式) を CA から取得し、その証明書 (Begin 行と End 行を含む) をクリップボードにコピーします。

3. コマンド store certificate keystore を入力します。次のプロンプトが表示されます。

   ```
   What is a one-word alias we can use to uniquely identify this certificate?
   ```

   証明書に付ける 1 単語の名前を入力し、Enter を押します。

   次の指示が表示されます。

   ```
   Please paste your CA certificate, in PEM format. Include the BEGIN and END lines, and then press CTRL-D.
   ```

   PEM 形式の証明書をコマンド行に貼り付けた後、CRTL-D を押します。保管操作の成功または失敗が通知されます。

   署名のために使用する CA が Guardium システムで信頼できる CA として設定されます。

4. 次に、CLI コマンド・プロンプトで `create csr gui` と入力します。

   要求された情報を入力します。証明書の CN (共通名) がボックスの hostname.domain に設定されていないと、ブラウザーから証明書エラーが生成されます。

   パラメーターはありませんが、部門 (OU)、国別コード (C)、などを提供するようプロンプトが出されます。この情報は必ず正確に入力してください。最後のプロンプトは次のようなものです。

   ```
   What encryption algorithm should be used (1=DSA or 2=RSA)?
   ```

   DSA (デジタル署名アルゴリズム) は、デジタル署名に関する連邦情報処理標準 (FIPS) です。RSA は、鍵の生成、暗号化、および暗号化解除を行う公開鍵暗号方式です。デフォルトの暗号化アルゴリズムは RSA です。

   最後のプロンプトに応えた後、要求の説明とそれに続いて要求そのもの、さらに続いて追加の説明がシステムに表示されます。 例:

   ```
   This is the generated CSR: Certificate Request: Data: Version: 0 (0x0) Subject: C=US, ST=MA, L=Littleton, O=XYZCorp,
   OU=Accounting, CN=g2.xyz.com -----BEGIN NEW CERTIFICATE REQUEST-----
   MIICWjCCAhcCAQAwVDELMAkGA1UEBhMCVVMxEDAOBgNVBAgTB1dhbHRoYW0xETAPBgNVBAoTCEd1
   YXJkaXVtMRUwEwYDVQQLEwxndWFyZGl1bS5jb20xCTAHBgNVBAMTADCCAbgwggEsBgcqhkjOOAQB
   MIIBHwKBgQD9f1OBHXUSKVLfSpwu7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2
   y5tVbNeBO4AdNG/yZmC3a5lQpaSfn+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQT
   WhaRMvZ1864rYdcq7/IiAxmd0UgBxwIVAJdgUI8VIwvMspK5gqLrhAvwWBz1AoGBAPfhoIXWmz3e
   y7yrXDa4V7l5lK+7+jrqgvlXTAs9B4JnUVlXjrrUWU/mcQcQgYC0SRZxI+hMKBYTt88JMozIpuE8
   FnqLVHyNKOCjrh4rs6Z1kW6jfwv6ITVi8ftiegEkO8yk8b6oUZCJqIPf4VrlnwaSi2ZegHtVJWQB
   TDv+z0kqA4GFAAKBgQCONsEB4g4/limbHkuZ5YnLn9CGM3a2evEnqjXZts4itxeTYwPQvdkjdSmQ
   kaQlBxmNUsZOJZrq5nC5Cg3X9spa+BzFr+PgR/5zka17nHcxKXCjVjLk451L67KllXv61TUfv/bU
   PKmiaGKDttsP2ktG4dBFXQdICJEGo0aNFCYn6qAAMAsGByqGSM44BAMFAAMwADAtAhUAhHTY5z9X NiBAuyAC9PS4GzleYakCFF2kcfxfjX1BFy5I228XWMAU0N95
   -----END NEW CERTIFICATE REQUEST-----
   ```

   注: 共通名では、FQDN (完全修飾ドメイン名) 形式のホスト名を使用します。ただし、FDQN (system1.us.ibm.com など) の代わりに短縮ホスト名 (system1 など) を使用して GUI に通常接続すると、「アドレスが一致しません (Address Mismatch)」という証明書エラーを受け取るため、証明書を使用するために CN=system1 を変更するか、https://system1.us.ibm.com:8443/sqlguard を使用して接続する必要があります。
   注: 国別コードは 2 文字でなければなりません。
   注: 鍵サイズとして 1024 または 2048 を使用できます。

5. 生成されたハッシュを ---Begin CSR---- から ---End CSR--- までコピーして、テキスト文書に貼り付けます。この文書を CA に送信して、署名付きの鍵を送り返してもらいます。

   続行する前に「件名」行を調べて、会社の情報を正しく入力していることを確認します。 ここから先は、サーバー証明書を CA から取得する際に通常使用する手順に従います。

   注: 要求を CA に送信する場合、証明書を PKCS#7 PEM 形式にするように要求する必要があります。
6. CA が CSR に署名して、署名付きの鍵を送り返します。
7. Guardium システムの CLI プロンプトに戻って、CA から送られてきた署名付きの鍵を配置します。以下を入力します: store certificate gui。

   表示どおり正確にコマンドを入力します。下記の情報が表示され、プロンプトが出されます。

   Please paste your new server certificate, in PEM format.

   Include the BEGIN and END lines, and then press CTRL-D.

   PEM 形式の証明書をコマンド行に貼り付けた後、CRTL-D を押します。保管操作の成功または失敗が通知されます。

```
-----BEGIN CERTIFICATE----- MIIDvTCCAqegAwIBAgIBATALBgkqhkiG9w0BAQUwcjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xDzANBgNVBAcTBllha2ltYTEMMAoGA1UEChMDSUJN
MRUwEwYDVQQLEwxHdWFyZGl1bURlbW8xGDAWBgNVBAMTD0d1YXJkaXVtRGVtb19D
QTAeFw0xMTAzMjUxNTM1MTRaFw02OTEyMzEyMzU5NTlaMHIxCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpXYXNoaW5ndG9uMQ8wDQYDVQQHEwZZYWtpbWExDDAKBgNVBAoT
A0lCTTEVMBMGA1UECxMMR3VhcmRpdW1EZW1vMRgwFgYDVQQDEw9HdWFyZGl1bURl
bW9fQ0EwggEgMAsGCSqGSIb3DQEBAQOCAQ8AMIIBCgKCAQEAw08aZVJNdnC69LR6
YtvHO+KbsqA89vCezLw7xmEa7F6+io0NofIFX7b7FvSkxzx1SO4eStaQSTDBxOGk
mqK2vk3VeJk9+lItofUuQXl1CZ1R4wQPMRfaWgELt+t94XB3YlzmI68vwfr1fB32
u3Yjpt4aq27sTMrjEqZIyDqQ7hQ1tpMtoBUqNi54wN+OJjhtpNYDAkCHs+3NPqXE
6HeL7W5X6PJ+YCyyZiXeqQ+T8qdpH0KDVJGJLGX1YC+0WnQz/S2kaaRfxe6Nhe6q
YeYaD09tlWkVrZQm8a76SDULjzjrQ4wNoTJu17JQk7Uc835RE/bF5WMsaN5HGs3s
9zP3uwIDAQABo2QwYjAPBgNVHRMBAf8EBTADAQH/MA8GA1UdDwEB/wQFAwMHBgAw
HQYDVR0OBBYEFINmKThm8tA+Z8cyFC7MOZ7v398SMB8GA1UdIwQYMBaAFINmKThm
8tA+Z8cyFC7MOZ7v398SMAsGCSqGSIb3DQEBBQOCAQEAcXttcJwy1aowq9wtJksK
q6n6laEFR38i+pLJ6kArjoJGP5WxFdaYcDQr5cAw2Q6YFZvQGaYAqiSS6ezF20PT
3BrrP+Mg/SK8jgPvM0ekodmpr385iQqSDneTTwPPrIaQBrrtb2510wHSEyiVcRRI
4vn3ktVahjiSMD92bfmZilPYQ51pD0jFgGFFRvekulPWGWv7iuCT+alCM99/76xR
uWrRc7cxypfxK1yymptizZVrxLHS47VVoXzmZ7yO3kfhhdZbBmoXg1MDM82rVdnp
WVQdlSasn8deHaVG//RsCrWx4PxN8TVIDGbfh0nWRYU4zPORvWst3fa+h9B2W55z /A== -----END CERTIFICATE-----
```

8. 最後のステップとして、コマンド restart gui を使用して UI を再始動します。

   1 つの Guardium ユニットに 1 つの証明書を正常にインストールできました。オンサイトのすべての Guardium システムで手順を繰り返してください。

親トピック: Guardium システムの管理

自己モニター

Guardium ソリューションは、自己モニターを行って、中断を最小限に抑え、可能な場合は常に問題を自動的に修正します。

Guardium ソリューションが使用可能で、正常に機能しており、改ざんされておらず、問題がある場合はユーザーに警告することを保証するために、以下の三方面からのアプローチが使用されます。

- レポート - 文字ベースの場合も、グラフィック・ベースの場合もありますが、レポートは Guardium® ソリューションの中核です。ユーザーは、Guardium のクエリー・ビルダーおよびレポート・ビルダーを使用することにより、関連付けられたドメインおよびエンティティーを通して収集された任意の自己モニター・データに関するレポートを効率的に作成できます。定義済みレポートの多くは、より詳細に指定することにより、より高い細分度を提供できるように改善できます。セキュリティーの評価に使用できるテストに関するレポートを作成するための特別なクエリー・ビルダー (VA Test Tracking) が作成されました。
- アラート - ユーザーは、レポートの作成に加え、定義したしきい値を使用して、それらのレポートに基づくアラートを定義できます。アラートは、例外やポリシー・ルール違反を示します。アラートの生成はリアルタイムか、または履歴分析により決定されます。次に、これらのアラートにより、SMTP、SNMP、syslog、カスタム Java™ クラスを使用したユーザーへの通知をトリガーすることができます。
- 自己モニター・ユーティリティー - Guardium では、内蔵の自己モニター・デーモン (常時稼働) サービス・ユーティリティーが、コレクターとアグリゲーターに実装されます。これらのユーティリティーは 5 分ごとに目覚めて、システム・スキャンを実行し、コンポーネントが最適に構成されているか、あるいは効率的に作動しているかをチェックして、必要に応じて修復します。例えば、Web サーバーがダウンしていることをユーティリティーが検出すると、まずサービスが完全にシャットダウンしているかどうかが検証され、サービスが再開されてから、管理ユーザーにアラートが送られます。

モニター対象のコンポーネント

表 1. モニター対象のコンポーネント

コンポーネント	アクセス方法
システム ディスク・スペース (使用量%)	「管理」>「システム・ビュー」>「システム・モニター」 アラート:「スニファーのバッファー」ドメイン および「スニファーのバッファー使用」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。

コンポーネント	アクセス方法
CPU 負荷 アップタイムおよびリブート メモリー使用状況 モニター・エンジン (スニファー) - 状況: 作動中/ダウン/スタック/過負荷 CPU 使用量 メモリー使用状況 過負荷および遅延 (キュー)	「レポート」>「Guardium 運用レポート」>「バッファー使用状況モニター」 アラート:「スニファーのバッファー」ドメイン および「スニファーのバッファー使用」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。
失敗したログイン	「管理」>「システム・ビュー」>「システム・モニター」。 アラート:「Guardium ログイン」ドメインおよび「Guardium ユーザー・ログイン」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。
失われた要求	「管理」>「レポート」>「アクティビティー・モニター」>「ドロップされたリクエスト」 アラート:「例外」ドメインおよび「例外」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。
データ・パターンの変更	「レポート」>「リアルタイム運用レポート」>「変更された値」 アラート:『監査プロセス定義の表示』で、アラート「データ・ソースの変更」(すべてのデータ・ソースの変更にアラートを出す) を参照。
パケット・レート リクエスト・レート 無視されたデータ	「レポート」>「Guardium 運用レポート」>「バッファー使用状況モニター」 アラート:「スニファーのバッファー」ドメイン および「スニファーのバッファー使用」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。
スケジュールされたジョブの例外	「レポート」>「Guardium 運用レポート」>「スケジュールされたジョブの例外」、または『事前定義管理レポート』を参照。 アラート:「例外」ドメインおよび「例外タイプ」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。
監査プロセスの状況	「レポート」>「Guardium 運用レポート」>「アクティブな監査プロセスの数」、または『事前定義管理レポート』を参照。 アラート:「監査プロセス」ドメインおよび「監査プロセス」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。
検査エンジンの変更	「レポート」>「アクティビティー・モニター」>「S-TAP 構成変更履歴」 アラート:『監査プロセス定義の表示』で、アラート「検査エンジンと S-TAP」(検査エンジンと S-TAP の構成に関連するすべてのアクティビティーについてアラートを出す) を参照。
Guardium ユーザー・アクティビティー - ログイン/ログアウト	「レポート」>「Guardium 運用レポート」>「Guardium へのログイン」、または『事前定義管理レポート』を参照。 アラート:「Guardium ログイン」ドメインおよび「SQL Guard ログイン」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。
失敗したログイン	「レポート」>「Guardium 運用レポート」>「Guardium へのログイン」、または『事前定義管理レポート』を参照。 アラート:『監査プロセス定義の表示』で、アラート「Guardium への失敗したログイン」(最近の 11 分間でログインの失敗が 5 回を超えるとアラートを出す) を参照。または「ツール」>「レポートのビルド」>「レポート・タイトル」ドロップダウンで、「Guardium ログイン」を選択。詳細について、『レポート』を参照。
ユーザー・アクティビティー監査証跡	「レポート」>「Guardium 運用レポート」>「ユーザー・アクティビティー監査証跡」、または『事前定義管理レポート』を参照。 アラート:「Guardium アクティビティー」ドメインおよび「SQL Guard ユーザー・アクティビティー監査」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。 注: ユーザー・アクティビティーには、ユーザーがルート・シェルに変更する場合も含まれるため、ルートのアクティビティーのログが提供されます。
ユーザー/ロールの作成/削除	「レポート」>「Guardium 運用レポート」>「ユーザー・アクティビティー監査証跡」、または『事前定義管理レポート』を参照。 アラート:『監査プロセス定義の表示』で、アラート「Guardium - ユーザーの追加/削除」(Guardium ユーザーのすべての追加または削除にアラートを出す) を参照。

コンポーネント	アクセス方法
許可のモニター	「レポート」>「Guardium 運用レポート」>「Guardium ユーザー」、「Guardium のロール」、または「Guardium アプリケーション」 アラート:「アプリケーション」ドメインおよび「アプリケーション・データ」エンティティーを利用して、照会および相関アラートを使用することにより、アラートを作成できます。
S-TAP® 情報 (中央マネージャー)	レポート:『S-TAP レポート』を参照。中央マネージャーでは、追加のレポート、「S-TAP 情報」が使用可能です。このレポートは、環境全体の S-TAP をモニターします。このデータのアップロードには、カスタム表ビルダーを使用します。このレポートは、リモート・ソースを使用してデータを中央マネージャーにアップロードし、そのデータを使用して S-TAP の統合ビューを表示した結果です。 S-TAP 情報は、「S-TAP 情報」エンティティーが含まれる事前定義カスタム・ドメインであり、ライセンス・ドメインと違って変更できません。

Guardium Nanny プロセス

Guardium Nanny は、システムのクリティカル・リソースをモニターし、潜在的な問題が発生する際にアラートを出す内部プロセスです。Nanny のアラートは syslog に送られ、そこから転送されたり、E メールとして管理者に送信したりできます。場合により、修正処置がとられます。

Nanny は Guardium システム内のキー・コンポーネントおよびクリティカル・リソースを監視し、それらの可用性と信頼性を保証します。リソースおよびコンポーネントには以下が含まれます。

- Web サービスのモニター - サービス・ポート (デフォルトで 8443) が応答していない、または tomcat サービスが起動していない。
  - syslog メッセージ
  - 管理者にメール送信
  - Web サービス再始動の実行
- 検査エンジン・アクティビティー - スニフの過負荷、応答なし、または失敗。
  - syslog メッセージ
  - 管理者にメール送信
  - Guardium サポートにメール送信 (オプション)
  - 条件により、スニフを再始動して修正を試行
  - プロセスが停止した場合にスニフの respawn を試行
- ディスク・スペース使用状況 - 重要なパーティションで 75% 以上になった場合にアラートを出す。
  - syslog メッセージ
  - 管理者にアラート送信
  - 95% を超える場合に一時ファイルをクリーニングし、予防処置を実行
- アプライアンスへのログイン (ssh) の失敗 - 失敗した ssh ログイン試行に関する ssh デーモンのメッセージおよびアラートを確認する。
  - 管理者にメール送信 (既に syslog 内にある)
- 内部データベース (TURBINE) のモニター - サービスが開始されていること、状況、および容量使用状況モニターの検証。
  - syslog メッセージ
  - 管理者にメール送信
  - サービスの再始動
- ファイル・システムの使用状況 - Nanny.pl が 5 分ごとに /var のファイル・システムを検査して、/var ディレクトリーの使用率が 75% を超えるとアラートで警告し、/var ディレクトリーの使用率が 90% を超えるとクリティカル・アラートで警告してサービスを停止する。
  - syslog メッセージ
  - 管理者にアラート送信
  - 管理者がクリーンアップする必要がある (使用する CLI コマンドは show filesystem usage、clear filesystem dir、および restart stopped_services)

- アラートを介して Guardium システムをモニターする方法
  組み込み相関アラートとカスタム相関アラートを組み合わせて使用して、IBM Security Guardium システムのキャパシティー、パフォーマンス、可用性をモニターします。
- SNMP によるモニター
  Guardium システムには SNMP エージェントがインストールされており、guardiumsnmp という名前の SNMP コミュニティーを使用して読み取り専用アクセス権限が提供されています。
- 実行照会モニター
  「実行照会モニター」にはアクティブ・ユーザー照会の状況が表示され、これによってすべてのレポート/モニター照会のタイムアウト値を設定することができます。

親トピック: Guardium システムの管理

アラートを介して Guardium システムをモニターする方法

組み込み相関アラートとカスタム相関アラートを組み合わせて使用して、IBM Security Guardium システムのキャパシティー、パフォーマンス、可用性をモニターします。

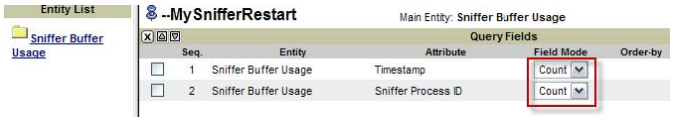
CPU 使用率、データベースのディスク・スペース、非アクティブ STAP、および「トラフィックなし」の各状態など、システムのパフォーマンスに影響を与える可能性のある問題についてユーザーに警告します。

「スニファーのバッファー使用」ドメインは、以下に示すアラートの大部分の基礎になっています。

スニファー再始動アラート

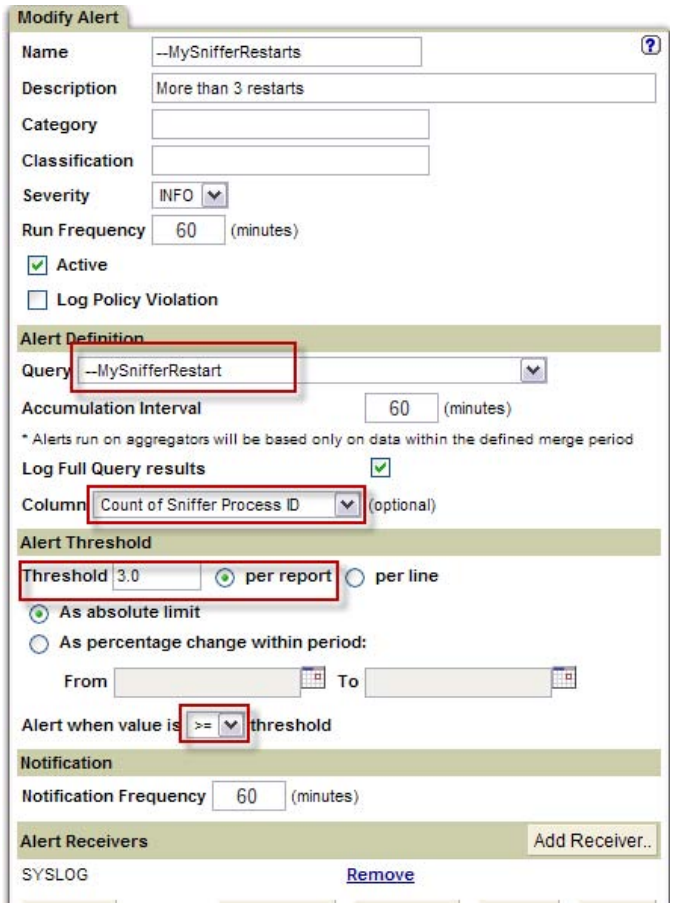
コレクター上のスニファーが 1 時間に 3 回以上再始動した場合にアラートが送信されます。

「スニファーのバッファー使用」ドメインを使用して、以下の列とフィールドを持つ照会を作成します。条件はありません。



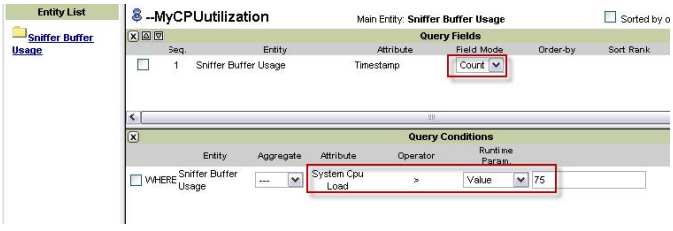
この照会の出力例を以下に示します。

次に、アラートを定義します。



高 CPU 使用率

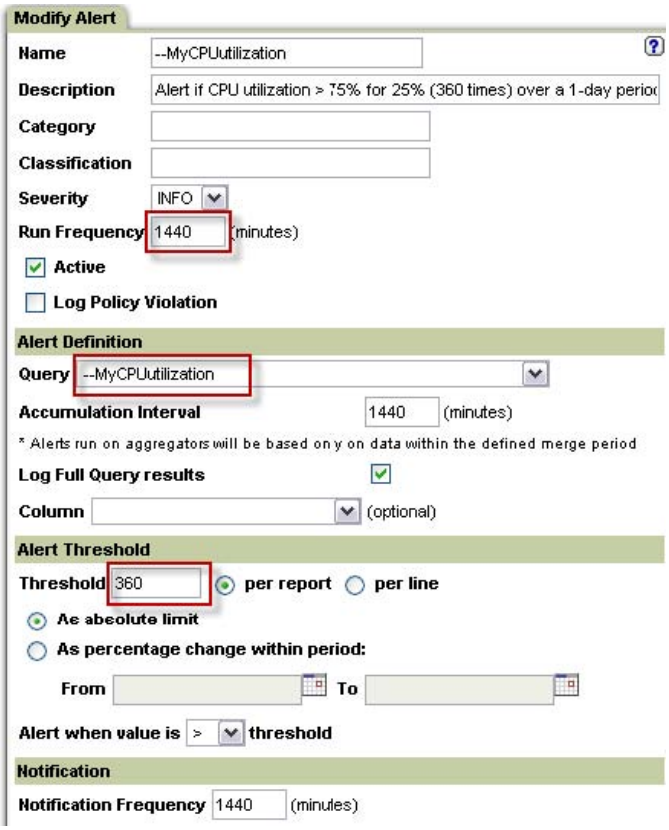
「エンタープライズ・バッファー使用状況」ドメインを使用して、システムの CPU 使用率をモニターするアラートを作成します。CPU 使用率が 75% を超える照会例を以下に示します。



このアラートは、75% の使用率を 24 時間で 360 回 (例えば、1 日の 25%) 超えた場合にのみ起動するように設定されます。

注: 「スニファーのバッファー使用」ドメインには 1 分ごとにデータが取り込まれるため、24 時間で 1440 項目が生成されます。

アラートを定義するには、「保護」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックします。

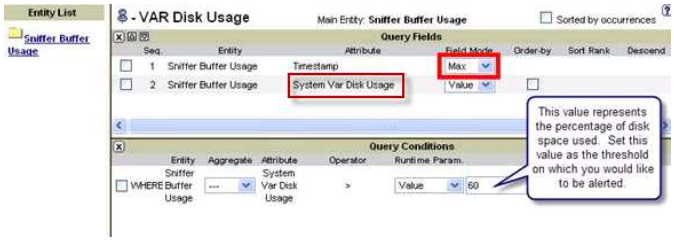


データベース・ディスク・スペースのアラート

クエリー・ビルダーを使用して類似した 2 つのレポートと 2 つのアラートを作成します。アラートの 1 つはコレクター用で、もう 1 つはアグリゲーター用です。これは、データベース・サイズはコレクターでは固定されていますが、アグリゲーターでは動的であるためです (最大で VAR パーティションのサイズまで)。

アグリゲーター・ディスク・スペースのアラート

1. メイン・エンティティーとして「スニファーのバッファー使用」を持つ新しい照会を作成します。
2. 以下のようにフィールドと条件を構成します。

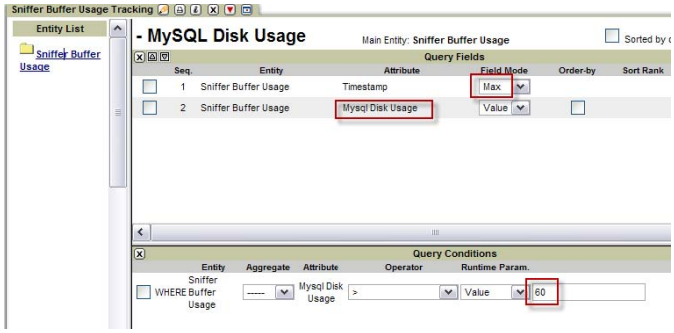


1. 「アラート・ビルダー」で新規アラートを設定します。 「保護」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックして、「アラート・ビルダー」を開きます。

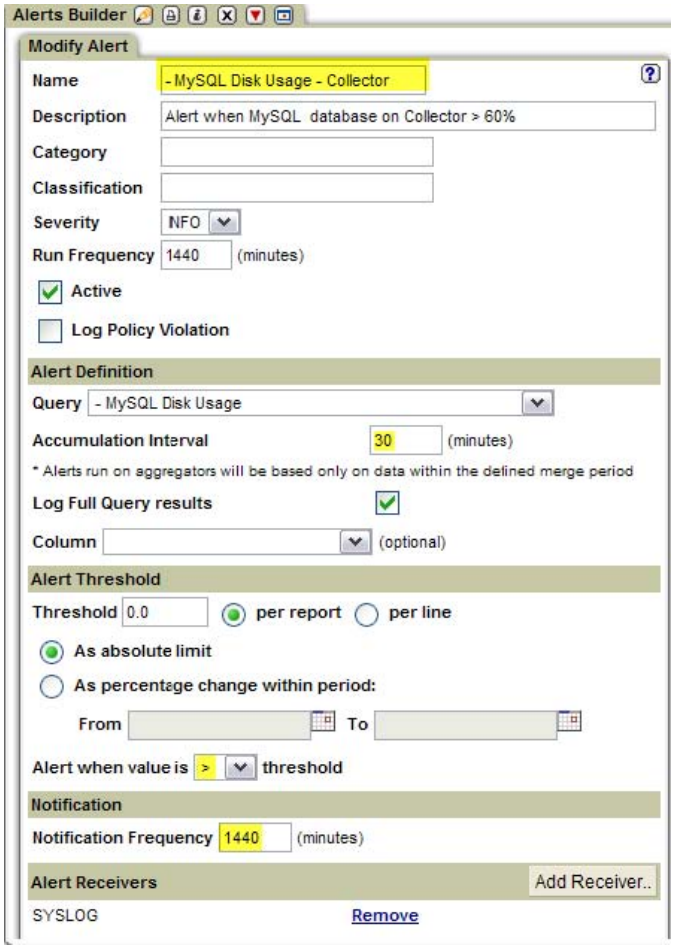
コレクター・ディスク・スペースのアラート

前のステップを繰り返して、コレクターのディスク・スペースをモニターするためのアラートを作成します。

1. 照会を作成します。



1. 「アラート・ビルダー」を使用して、以下のように新しいアラートを設定します。



データ・インポート、マージ (統合)、アーカイブ、または障害バックアップのアラート

これは組み込みアラートであり、アクティブ化してスケジューリングする必要があります。

非アクティブ S-TAP アラート

これは組み込みアラートであり、アクティブ化してスケジューリングする必要があります。

1 次コレクターと 2 次コレクターで構成された STAP では、ネットワークの問題などが原因で STAP が 1 次コレクターと通信できない場合、2 次コレクターにフェイルオーバーします。元の 1 次コレクターが STAP を ping できない場合、非アクティブな STAP アラートが生成されます。

注: 構成が正しくない場合、クラスター構成内の STAP によって誤ったアラートが生成されることがあります。

「トラフィックなし」アラート

これは組み込みアラートであり、アクティブ化してスケジューリングする必要があります。

このアラートは、以前にコレクターがトラフィックを受信していたアクティブな検査エンジンからのトラフィックがあるかどうかを検査し、さらに、ポリシーによって処理されるトラフィックがあるかどうかを検査します。両方の条件が 48 時間以内に満たされない場合、アラートが生成されます。

随時レポートを介したアプリケーション・モニター

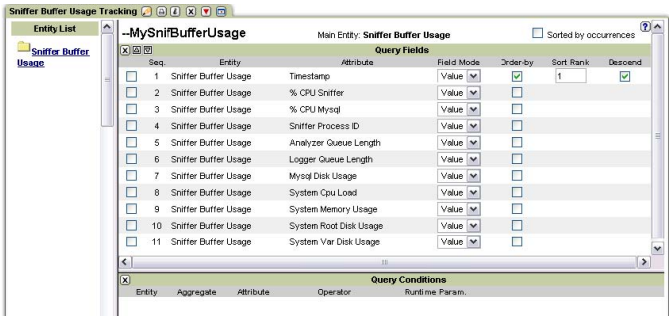
一般的なルールとして、1 時間を超える随時照会または随時レポートをコレクターで呼び出すことは避けてください。大規模な照会や、実行に長時間を要する照会は、アグリゲーターで呼び出す必要があります。監査プロセスを使用すると、最適なスケジュールを設定することができます。

以下の 2 つのレポートについて、各コレクターで毎週実行されるように、中央マネージャーからスケジューリングする必要があります。

注: また、これらのレポートは、それぞれのアグリゲーターで個別にスケジューリングする必要があります。

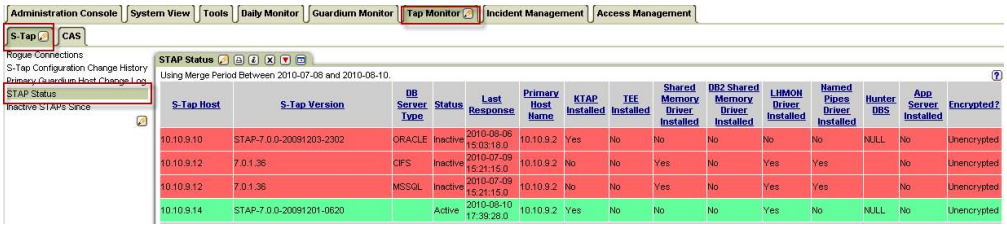
カスタムの「スニファーのバッファー使用」レポート

「スニファーのバッファー使用」ドメインを使用して、以下のフィールドを持つレポートを作成します。



STAP 状況レポート

このレポートには、特定のコレクターに関するすべての STAP と検査エンジンの主要なパラメーターが表示されます。 このレポートを変更することはできませんが、各コレクターで実行したり、各コレクターを指す中央マネージャーから実行したり、各コレクターの監査プロセスを介してスケジューリングしたりすることができます。



親トピック: 自己モニター

SNMP によるモニター

Guardium® システムには SNMP エージェントがインストールされており、guardiumsnmp という名前の SNMP コミュニティーを使用して読み取り専用アクセス権限が提供されています。

照会を行う際に、値 -1 (マイナス 1) は、データベースで NULL を示します。 このセクションの最後にある表に、使用可能な SNMP OID がリストされています。

SNMP の例

UNIX セッションから、snmpget または snmpwalk コマンドを使用して SQL Guard SNMP 情報を表示できます。 (コマンド構文を表示するには、snmpget -h または snmpwalk -h を使用します。) SNMP 情報を表示するために、さまざまな UI ベースのソフトウェア・パッケージを使用できます。これらの代替手段についてはここでは説明しません。

表 1. SNMP の例

SNMP の例
使用されている、および使用可能なディスク・スペース
> snmpget -v 2c -c guardiumsnmp a1.corp.com UCD-SNMP-MIB::dskAvail.1
UCD-SNMP-MIB::dskAvail.1 = INTEGER: 1043856
> snmpget -v 2c -c guardiumsnmp a1.corp.com UCD-SNMP-MIB::dskUsed.1
UCD-SNMP-MIB::dskUsed.1 = INTEGER: 914856
合計メモリーおよび使用されているメモリーをリストする場合
> snmpget -v 2c -c guardiumsnmp a1.corp.com
HOST-RESOURCES-MIB::hrStorageSize.101
HOST-RESOURCES-MIB::hrStorageSize.101 = INTEGER: 2067352
> snmpget -v 2c -c guardiumsnmp a1.corp.com HOST-RESOURCES-MIB::hrStorageUsed.101
HOST-RESOURCES-MIB::hrStorageUsed.101 = INTEGER: 1017548
使用可能メモリーをリストする場合
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com memAvailReal
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 1049564
CPU 使用量に関連した値をリストする場合
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawUser
UCD-SNMP-MIB::ssCpuRawUser.0 = Counter32: 89240
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawSystem

SNMP の例
UCD-SNMP-MIB::ssCpuRawSystem.0 = Counter32: 195310
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawNice
UCD-SNMP-MIB::ssCpuRawNice.0 = Counter32: 11
注: RawUser、RawSystem、および RawNice 番号を追加すると、CPU 総使用量に近い概算を得ることができます。
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawIdle
UCD-SNMP-MIB::ssCpuRawIdle.0 = Counter32: 26734332

Guardium SNMP OID

表 2. Guardium SNMP OID

SNMP OID	記述
.1.3.6.1.4.1.2021.9.1.7.1 UCD-SNMP-MIB::dskAvail.1	/ ディレクトリーで使用可能なディスク・スペース
.1.3.6.1.4.1.2021.9.1.7.2 UCD-SNMP-MIB::dskAvail.2	/var ディレクトリーで使用可能なディスク・スペース
.1.3.6.1.4.1.2021.9.1.8.1 UCD-SNMP-MIB::dskUsed.1	/ ディレクトリーで使用されているディスク・スペース
.1.3.6.1.4.1.2021.9.1.8.2 UCD-SNMP-MIB::dskUsed.2	/var ディレクトリーで使用されているディスク・スペース
.1.3.6.1.2.1.25.2.3.1.5.1 HOST-RESOURCES-MIB::hrStorageSize.1	使用可能な合計メモリー
.1.3.6.1.2.1.25.2.3.1.6.1 HOST-RESOURCES-MIB::hrStorageUsed.1	使用されているメモリー
.1.3.6.1.4.1.2021.8.1.101.1 UCD-SNMP-MIB::extOutput.1	オープンしているモニター対象セッション数
.1.3.6.1.4.1.2021.8.1.101.2 UCD-SNMP-MIB::extOutput.2	現在のスニファー・プロセスにより記録された要求 (再始動ごとにゼロに設定する)
.1.3.6.1.4.1.2021.8.1.101.3 UCD-SNMP-MIB::extOutput.3	最終セッションのタイム・スタンプ
.1.3.6.1.4.1.2021.8.1.101.4 UCD-SNMP-MIB::extOutput.4	最終構成のタイム・スタンプ
.1.3.6.1.4.1.2021.8.1.101.5 UCD-SNMP-MIB::extOutput.5	スニファー・プロセスにより使用されているメモリー
.1.3.6.1.4.1.2021.8.1.101.7 UCD-SNMP-MIB::extOutput.7	ETH1 への到着パケット数/ETH2 からの送信パケット数。通常、SPAN ポートまたは TAP ポートが使用されるときには 1 つの数値だけ (到着) です。
.1.3.6.1.4.1.2021.8.1.101.8 UCD-SNMP-MIB::extOutput.8	ETH3 への到着パケット数/ETH4 からの送信パケット数。通常、SPAN ポートまたは TAP ポートが使用されるときには 1 つの数値だけ (到着) です。
.1.3.6.1.4.1.2021.8.1.101.9 UCD-SNMP-MIB::extOutput.9	ETH5 への到着パケット数/ETH6 からの送信パケット数。通常、SPAN ポートまたは TAP ポートが使用されるときには 1 つの数値だけ (到着) です。

マシンでアクセス可能な他の MIB は SNMPv2-MIB、IF-MIB、RFC1213-MIB、および HOST-RESOURCES-MIB です。

親トピック: 自己モニター

実行照会モニター

「実行照会モニター」にはアクティブ・ユーザー照会の状況が表示され、これによってすべてのレポート/モニター照会のタイムアウト値を設定することができます。

「管理」 > 「アクティビティー・モニター」 > 「実行照会モニター」をクリックして、「実行照会モニター」を開きます。

「実行照会モニター」から以下のことを実行できます。

- ポートレットで稼働中のすべてのレポートおよびモニターの照会タイムアウトを設定します。ポリシー・シミュレーション、監査プロセス、内部処理などの、他の照会処理は、このタイムアウト値の影響を受けません。デフォルトは 180 秒 (3 分) です。
- 現在実行中のユーザー照会を強制終了します。監査プロセスなど、このパネルにリストされている一部の照会は、指定した照会タイムアウトを超えている可能性があります。このようなことが予想されるのは、レポート/モニター照会タイムアウトがポートレットで実行中のレポートおよびモニターにのみ適用されるためです。

照会タイムアウトをデフォルト設定 (180 秒) を超えて長時間にわたって設定することはお勧めしません。この制限を超えて設定すると、特別なレポート・アクティビティーによってシステムに過負荷がかかる可能性が高くなります。

タイムアウト設定を変更するには、「レポート/モニター照会タイムアウト (秒)」に秒数を入力して、「更新」をクリックします。 更新が完了したことが通知されます。

親トピック: 自己モニター

グループ

グループを使用すると、分類、ポリシー、照会の各定義を簡単に作成および管理できるほか、更新を S-TAP クライアントおよび GIM クライアントに展開することができます。アクセス・ポリシーのデータ・オブジェクトのグループを繰り返し定義するのではなく、オブジェクトをグループに入れると、簡単に管理できます。

- グループの概要
  類似のデータ・オブジェクトをグループ化して、照会、ポリシー、および分類の各定義の作成に使用します。事前定義された多数のグループのうちの 1 つを使用するか、「グループ・ビルダー」を使用して独自のグループを作成します。
- グループ・ビルダーの使用
  グループ・ビルダーはグループ・メンバーシップとグループの使用について一目で確認できる情報を提供します。また、グループにデータを取り込むための便利な方法がいくつか用意されています。
- グループ・ビルダー (レガシー)の使用
- 照会およびポリシーでのグループの使用
  照会の条件演算子、およびポリシーでグループを使用する場所についての簡単な概要
- 例: グループを使用したルールとポリシーの作成
  グループを使用して、ポリシーのルール条件を素早く指定します。
- 事前定義グループ
  このセクションでは、Guardium® の事前定義グループについて詳しく説明します。

親トピック: Guardium システムの管理

グループの概要

類似のデータ・オブジェクトをグループ化して、照会、ポリシー、および分類の各定義の作成に使用します。事前定義された多数のグループのうちの 1 つを使用するか、「グループ・ビルダー」を使用して独自のグループを作成します。

グループの使用が役立つ状況は多くあります。類似のデータ・オブジェクトをグループ化することにより、複数のデータ・オブジェクトを個別に選択する必要なしに、ポリシー、分類、照会、およびレポートでオブジェクトのセット全体を使用できます。

照会またはポリシーに変更を加える必要がある場合、変更内容を各オブジェクトに個別に適用するのではなく、グループに適用できます。

S-TAP および GIM も、複数の管理対象サーバーにまたがって更新を容易に展開できるようにするために、グループを使用します。

グループ・ビルダー

「グループ・ビルダー」では、ユーザー・インターフェースから、新規グループを作成したり、既存のグループに変更を加えたりすることができます。

「設定」 > 「グループ・ビルダー」をクリックして、「グループ・ビルダー」を開きます。

「グループ・フィルター」画面では、アプリケーション・タイプ、グループ・タイプ、説明、またはカテゴリーに基づいてグループを簡単にソートできます。

グループのタイプ

「グループ・タイプ」フィールドは、一緒にグループ化されるデータのタイプを指します。 例えば、「*サーバー IP*」では、IP アドレスとして配列されたデータが予期され、「*ユーザー*」では、アプリケーションのユーザーの名前が示されることが予期されます。

タプル・グループ

タプル・グループでは、複数の属性を組み合わせて 1 つの複合グループ・メンバーを形成することができます。3 つの順序付き値セットは、3 タプルと呼ばれます。 n 個の値属性セットがあるものを n タプルと呼びます。 これにより、レポートおよびポリシー・ルールの条件の指定が簡略化されます。

以下にタプル・グループの例を示します。

- タプル・グループ - オブジェクト/コマンド、オブジェクト/フィールド、クライアント IP/データベース・ユーザー、サーバー IP/データベース・ユーザー
- 3 タプル・グループ - クライアント IP/ソース・プログラム/データベース・ユーザー、データベース・ユーザー/オブジェクト/特権
- 5 タプル・グループ - クライアント IP/ソース・プログラム/データベース・ユーザー/サーバー IP/サービス・インスタンス
- 7 タプル・グループ - クライアント IP/ソース・アプリケーション/データベース・ユーザー/サーバー IP/サービス名/OS ユーザー/データベース名

タプルには、1 つのスラッシュおよび 1 つのワイルドカード文字 (%) を使用できます。ダブルスラッシュ (//) の使用はサポートされません。
注: タプル・クエリー - ユーザーが LIKE GROUP 条件を使用しようとし、データ内に「¥」がある場合、結果は正しくない場合があります。データ内に「¥」がある場合、ユーザーは代わりに IN GROUP を使用する必要があります。

事前定義グループ

Guardium には、いくつもの事前定義されたグループが含まれています。「グループ・フィルター」および「グループ・タイプ」メニューを使用して、グループのリストを表示し、ニーズに最も適したグループを見つけます。

グループ・タイプ「*データベース・ユーザー/データベース・パスワード*」は、デフォルトで admin ユーザーのみが使用可能です。このデフォルト設定を変更する場合は、グループのロールを変更してください。

重複するグループ・メンバーシップ

グループ・メンバーを複数のグループに入れることができます。

例えば、2 つの事前定義グループ「*Create コマンド*」および「*DDL コマンド*」がいずれも「CREATE TABLE」という名前のメンバーを持つとします。いずれかの一方のグループを照会する場合、レポート期間のすべての CREATE TABLE メンバーがそのグループでカウントされます。

各メンバーが 1 つのグループにのみ属するようにグループ・セットを定義する場合があります。例えば、レポート目的で、データベース・ユーザーを「従業員」または「コンサルタント」の 2 つのグループのいずれかにグループ化する必要があるとします。 これらの各グループを同じサブグループ・タイプ (「雇用者の身分」など) で定義します。 サブグループが使用される場合、メンバーが同じサブグループ・タイプの別のグループに既に追加されていると、システムは、そのメンバーをサブグループに追加することを許可しません。

メンバー内のワイルドカード

グループが照会条件やポリシー・ルールで使用される場合に、グループ・メンバーにワイルドカード (%) 文字を含めることができます。

表 1. メンバー内のワイルドカード

メンバー	一致	不一致
aaa%	aaa aaazzz	zzzaaa aaz
%bbb	bbb,zzbbb	bb bbbzzz
%ccc%	ccc ccczz zzzccczzz	cc zzzcczzz

管理対象ユニット・グループ

ポリシーの作成および管理を簡素化するために、およびレポート表示を明確にするために要素をグループ化しますが、この要素のグループ化に使用される管理対象ユニット・グループとグループ・ビルダーを介して作成されたグループには明確な違いがあります。管理対象ユニット・グループについて詳しくは、管理対象ユニット・グループの作成を参照してください。

親トピック: グループ

グループ・ビルダーの使用

グループ・ビルダーはグループ・メンバーシップとグループの使用について一目で確認できる情報を提供します。また、グループにデータを取り込むための便利な方法がいくつか用意されています。

グループ・ビルダーを使用して、グループを作成し、CSV ファイル、外部データ・ソース、および既存のグループを含むさまざまなソースからグループにデータを取り込みます。さらに、グループ・ビルダーは、グループ・メンバーシップについて、またグループがセキュリティー・ポリシー、分類ポリシー、照会、およびレポートのどこで使用されているかについて、一目で確認できる情報を提供します。

ヒント:

Guardium V10.1.4 では、新しいグループ・ビルダー・インターフェースが導入されており、これについてはここで説明します。新しいグループ・ビルダーには、「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」でアクセスできます。

元のグループ・ビルダーには、「設定」 > 「ツールとビュー」 > 「グループ・ビルダー (レガシー)でアクセスできます (グループ・ビルダー (レガシー)の使用を参照)。

- グループの作成および編集
  グループの作成方法と編集方法について説明します。
- グループ・メンバーシップおよびグループの使用場所の表示
  グループ・メンバーシップの表示方法およびグループが使用されているポリシー、レポート、照会の識別方法について説明します。
- グループへの取り込み
  グループ・ビルダーでは、メンバーをグループへ追加するための複数の方法がサポートされています。

親トピック: グループ

グループの作成および編集

グループの作成方法と編集方法について説明します。

親トピック: グループ・ビルダーの使用

グループの作成

手順

1. 「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」にナビゲートして、グループ・ビルダーを開きます。
2. 「グループ・ビルダー」表で  アイコンをクリックします。
3. 「新規グループの作成」ダイアログを使用して、新規グループを定義します。 グループの説明を入力し、「アプリケーション・タイプ」メニューと「グループ・タイプ」メニューを使用してグループを定義します。
4. 新規グループを定義したら、「メンバー」タブを使用してグループにデータを取り込みます。 グループへのデータの取り込みについては、グループへの取り込みを参照してください。
5. 「保存」をクリックして、新規グループの定義を終了します。

グループの編集

手順

1. 「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」にナビゲートして、グループ・ビルダーを開きます。
2. 「グループ・ビルダー」表からグループを選択し、  アイコンをクリックします。
3. 「グループの編集」ダイアログを使用してグループの設定を変更します。 グループへのメンバーの追加またはグループ・メンバーシップの変更を行うには、「メンバー」タブを使用します。グループへのデータの取り込みについては、グループへの取り込みを参照してください。
4. 「保存」をクリックしてグループの編集を終了します。

グループ・メンバーシップおよびグループの使用場所の表示

グループ・メンバーシップの表示方法およびグループが使用されているポリシー、レポート、照会の識別方法について説明します。

親トピック: グループ・ビルダーの使用

グループ・メンバーシップの表示

このタスクについて

「グループ・ビルダー」表の「メンバー」列と「データ設定元」列は、グループ内のメンバー数およびグループへのデータの取り込み方法を示します。以下の手順では、グループ・メンバーシップと、グループへのデータの取り込み方法についての詳細情報を取得する方法について説明します。

手順

1. 「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」にナビゲートして、グループ・ビルダーを開きます。
2. 「グループ・ビルダー」表からグループを選択し、  アイコンをクリックすることで、「グループの編集」ダイアログを開きます。
3. 「グループの編集」ダイアログで「メンバー」タブをクリックして、グループ・メンバーシップを表示します。

グループの使用場所の識別

このタスクについて

「グループ・ビルダー」表の「分類で使用」、「ポリシーで使用」、および「照会で使用」の各列は、グループが Guardium のどこで使用されているかについての概要を示します。以下の手順では、グループが使用されているポリシー、照会、およびレポートの詳細情報を取得する方法を説明します。

手順

1. 「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」にナビゲートして、グループ・ビルダーを開きます。
2. 「グループ・ビルダー」表からグループを選択して「アクション」 > 「詳細表示」をクリックすることで、詳細パネルを開きます。
3. 詳細パネルの「ポリシー」タブと「照会」タブを使用して、選択したグループがセキュリティー・ポリシー、分類ポリシー、照会、およびレポートのどこで使用されているかを表示します。

グループへの取り込み

グループ・ビルダーでは、メンバーをグループへ追加するための複数の方法がサポートされています。

手順

1.  アイコンをクリックして新規グループを作成するか、「グループ・ビルダー」表からグループを選択し、  アイコンをクリックして既存のグループを編集します。
2. 「新規グループの作成」ダイアログまたは「グループの編集」ダイアログの「メンバー」タブを選択します。
3. 以下のいずれかの方法を使用して、グループにデータを取り込みます。
   -  アイコンを使用して、グループ・メンバーを手動で定義します。
   - 「インポート」メニューを使用して、以下のいずれかの方法を使用してグループ・メンバーを追加します。
     - CSV から
     - グループから
     - 外部データ・ソースから
     - 照会から
     - LDAP から

ヒント: 構成されると、スケジュール可能なインポート・アクションが「新規グループの作成」ダイアログまたは「グループの編集」ダイアログにタブとして表示されます。「CSV からインポート」などの一回限りのアクションはスケジュールできないため、ダイアログ上に新しいタブは表示されません。

- 一部のグループ・タイプでは、グループへデータを取り込むための方法として、以下の拡張された方法もサポートされています。
  - データ・ソースに対するストアード・プロシージャー分析の使用
  - データベース従属関係の使用
  - 逆従属関係の使用
  - 監視対象プロシージャーの使用
  - 選択したオブジェクトの生成

重要: Guradium V10.1.4 で導入されたグループ・ビルダーを使用すると、拡張インポート・アクションはターゲット・グループに対して呼び出されます。ターゲット・グループには、ユーザー選択の入力グループに対して実行される分析の結果に基づいてデータが取り込まれます。これは、レガシー・グループ・ビルダーからの動作の変更を意味します。レガシー・グループ・ビルダーでは、拡張アクションは分析対象の入力を含むソース・グループに対して呼び出され、ユーザー選択のグループに分析結果がインポートされました。

- 外部データ・ソースからのインポート
  Guardium グループに独自データベースのデータを素早く追加し、それらのグループとデータの同期を保つ方法について説明します。

親トピック: グループ・ビルダーの使用

外部データ・ソースからのインポート

Guardium グループに独自データベースのデータを素早く追加し、それらのグループとデータの同期を保つ方法について説明します。

このタスクについて

「インポート」 > 「外部データ・ソースから」を使用すると、独自データ・ソースのデータを Guardium グループに追加するためのカスタム表、ドメイン、および照会の作成が自動化されます。これらの成果物は、作成後、Guardium とデータの間の永続的な接続を表します。データを更新すると、関連する Guardium グループに反映されます。

手順

1. 「インポート」 > 「外部データ・ソースから」を選択して「外部データ・ソースからインポート」ダイアログにアクセスします。
2. 「データ・ソース」メニューを使用して、データ・ソースからデータをインポートします。 アイコンをクリックして新規データ・ソースを定義するか、 アイコンをクリックして既存のデータ・ソースを編集します。
3. 「表名」フィールドおよび「列名」フィールドを使用して、データ・ソースからインポートするデータの場所を指定します。
4. 「OK」をクリックして先に進みます。

タスクの結果

「外部データ・ソースからインポート」ダイアログでの入力を完了すると、以下の Guardium 成果物が自動的に作成または更新されます。

- カスタム表
- カスタム・データ・ソース
- カスタム・ドメイン
- カスタム・クエリー
- グループ

これらの成果物は、次の表で説明されている命名規則を使用して、標準 Guardium ツールを通じて使用できます。この表の *[table name]* と *[column name]* は、「外部データ・ソースからインポート」ダイアログの「表名」フィールドと「列名」フィールドから取得されます。

表 1. 外部データ・ソースからインポート: 作成される成果物の概要

成果物	Guardium ツール	命名規則	例	スケジュール済み
カスタム表	「カスタム表ビルダー」 > 「データの編集」	*[table name]_[column name]_[datasource ID]*	`USERS_ADMIN_12345`	
カスタム・データ・ソース	「カスタム表ビルダー」 > 「データのアップロード」	*[datasource name]_[datasource type](カスタム・ドメイン)*	`user_repository`(カスタム・ドメイン)	✓
カスタム・ドメイン	「カスタム・ドメイン・ビルダー」	*[group type]_[table name]_[column name]_[datasource ID]*	`USERS_USERS_ADMIN_12345`	
カスタム・クエリー	「カスタム・クエリー・ビルダー」	*[group type]_[table name]_[column name]_[datasource ID]*	`USERS_USERS_ADMIN_12345`	
グループ	「グループ・ビルダー」 > 「照会から取り込み」		PCI 管理ユーザー	✓

重要: インポートされた名前は、64 文字より後が切り捨てられます。

親トピック: グループへの取り込み

グループ・ビルダー (レガシー)の使用

- 新規グループの作成
  データ・オブジェクトのグループを手動で作成するには、グループ・ビルダーを使用します。
- グループの変更
  メンバーの追加や、グループのカテゴリーの変更など、グループに変更を加えます。変更はその他のユーザーやポリシーに影響を与える可能性があるため、グルー

プの変更や削除を行う際には注意してください。

- グループへの取り込み
  グループを作成するか、処理するグループを見つけた後、グループにメンバーを取り込みます。「グループ・ビルダー (レガシー)」を使用して手動でメンバーをグループに追加するか、自動化されたいくつかのインポート方法を使用します。

親トピック: グループ

新規グループの作成

データ・オブジェクトのグループを手動で作成するには、グループ・ビルダーを使用します。

手順

1. 「設定」 > 「グループ・ビルダー (レガシー)」をクリックして、「グループ・ビルダー」を開きます。
2. 「次へ」をクリックして、フィルターをバイパスし、新しいグループを作成します。
3. 「新規グループの作成」パネルで、「アプリケーション・タイプ」メニューから、グループで使用するアプリケーションを決定するためのオプションを選択します。
4. 新しいグループのための固有の「グループの記述」を入力します。このフィールドには、アポストロフィ文字を含めないでください。
5. 「グループ・タイプの記述」を選択して、グループ化するデータのタイプを選択します。
6. 「カテゴリー」を入力します。これはオプションのラベルであり、フィルター条件として使用し、ポリシー違反やレポートの項目をフィルター処理して、グループ化することができます。
7. 「分類」を入力します。これはもう 1 つのオプションのラベルであり、フィルター条件として使用し、ポリシー違反やレポートの項目をフィルター処理して、グループ化することができます。
8. 「階層」を選択して、階層グループのグループを作成します。このグループでは、admin ユーザーがアクセス権を持ち、階層グループのグループ内のユーザーにアクセス権を渡します。
9. 「追加」をクリックして、グループを追加します。

親トピック: グループ・ビルダー (レガシー)の使用

グループの変更

メンバーの追加や、グループのカテゴリーの変更など、グループに変更を加えます。変更はその他のユーザーやポリシーに影響を与える可能性があるため、グループの変更や削除を行う際には注意してください。

手順

1. 「設定」 > 「グループ・ビルダー (レガシー)」をクリックして、「グループ・ビルダー (レガシー)」を開きます。
2. 「グループ・フィルター」を使用して、変更するグループを見つけるか、フィルターを空のままにして「次へ」をクリックし、グループの完全なリストを表示します。
3. グループを変更する際、グループのコピーを作成して  、新しいグループとして保存してから、そのコピーに変更を加えるようにして、Guardium システムの他の部分に好ましくない影響が発生するのを避けることがベスト・プラクティスです。

   「既存グループの変更」ペインでは、以下を実行できます。

   - 任意のグループの変更、コピーの作成、または削除
   - ロールの割り当てまたは変更
   - 照会または LDAP サーバーから、あるいは「自動生成呼び出しプロシージャー」機能を使用した、グループへのデータの取り込み
4. いずれかのグループが選択された状態で、「変更」  をクリックすると、以下を実行できます。
   - グループのカテゴリーの変更
   - グループへの新規メンバーの追加
   - グループ・メンバーの名前変更
   - 事前定義メンバーへのグループのメンバーシップのリセット
   - コメントの追加
   - グループの別名の作成
   - LDAP からグループに取り込み

親トピック: グループ・ビルダー (レガシー)の使用

グループ・カテゴリーの変更

手順

「グループ・メンバー」リストからグループを選択して、「カテゴリー」フィールドに新しいカテゴリー名を入力し、「カテゴリーの変更」をクリックして、変更内容を保存します。

グループ・メンバーの追加

新規メンバーを作成してグループに追加するか、既存メンバーをグループに追加します。

手順

グループに追加する新規メンバーがある場合、「次の名前の新規メンバーを作成および追加」フィールドにメンバーの名前を入力して、「追加」をクリックします。
注: オブジェクト・グループに追加する場合、 有効なメンバー名は object_name、schema.object_name、ワイルドカードを使用した %object_name のような名前、またはそれら 3 つすべての組み合わせで構成されます。

これで、新規メンバーは「グループ・メンバー」リストに追加されました。

グループ・メンバーの名前変更

手順

1. 「グループ・メンバー」リストから、名前変更するグループ・メンバーを選択します。これにより、「選択したメンバーを次の名前に変更」に現在のグループ・メンバーも表示されます。
2. 「選択したメンバーを次の名前に変更」フィールドでグループ・メンバーの名前を変更して、「更新」をクリックします。

事前定義グループ・メンバーシップへのリセット

任意のグループの「事前定義にリセット」をクリックして、現行のグループ・メンバーを事前定義グループ・メンバー・セットに置き換えます。

グループにコメントを追加

任意のグループの「コメントの追加」をクリックして、将来の参照のためにコメントを追加します。

グループの別名の作成

手順

1. 「別名」をクリックして、「別名クイック定義」ウィンドウを開きます。
2. 別名を作成する対象となるグループ・メンバーごとに、「別名」列に値を入力して、「適用」をクリックします。

グループへの取り込み

グループを作成するか、処理するグループを見つけた後、グループにメンバーを取り込みます。「グループ・ビルダー (レガシー)」を使用して手動でメンバーをグループに追加するか、自動化されたいくつかのインポート方法を使用します。

- LDAP からのグループの設定方法
  Guardium® グループで使用するデータを LDAP サーバーからインポートする方法。
- 照会を使用したグループへの取り込み
  照会を作成し、その結果を使用してグループにデータを取り込みます。 このグループへの取り込みオプションは、外部データ相関によってカスタム表が Guardium システムにアップロードされた後に使用すると最も効果的です。
- ストアード・プロシージャーを使用したグループへの取り込み
  ストアード・プロシージャーからコマンド・グループまたはオブジェクト・グループにデータを取り込む方法はいくつかあります。「グループ・ビルダー」の自動生成呼び出しプロシージャー機能では、特定のグループ・メンバーのコマンド・グループまたはオブジェクト・グループを分析して、それらのメンバーを新規グループに追加することができます。

親トピック: グループ・ビルダー (レガシー)の使用
関連情報:
Guardium のグループおよびポリシー (ビデオ)

LDAP からのグループの設定方法

Guardium® グループで使用するデータを LDAP サーバーからインポートする方法。

このタスクについて

LDAP サーバーを使用する Guardium を構成したら、オンデマンドでインポートするか、将来のインポートをスケジュールします。

LDAP ユーザーをインポートする場合:

- Guardium の admin ユーザー・アカウントは、いかなる形でも変更されません。
- インポート前にグループから既存のメンバーをクリアするオプションがあります。
- 既存のユーザー・パスワードは変更されません。
- デフォルトでは、新規ユーザーは追加時に無効になっていて、ブランク・パスワードを持っており、ユーザー・ロールが割り当てられます。

注:

ユーザー名での特殊文字の使用はサポートされていません。

インポートをスケジュールすると、既存のスケジュール済みインポートの動作に影響を与えるため、その時点で可能性のある他のすべてのスケジュール済みのインポートを考慮してください。

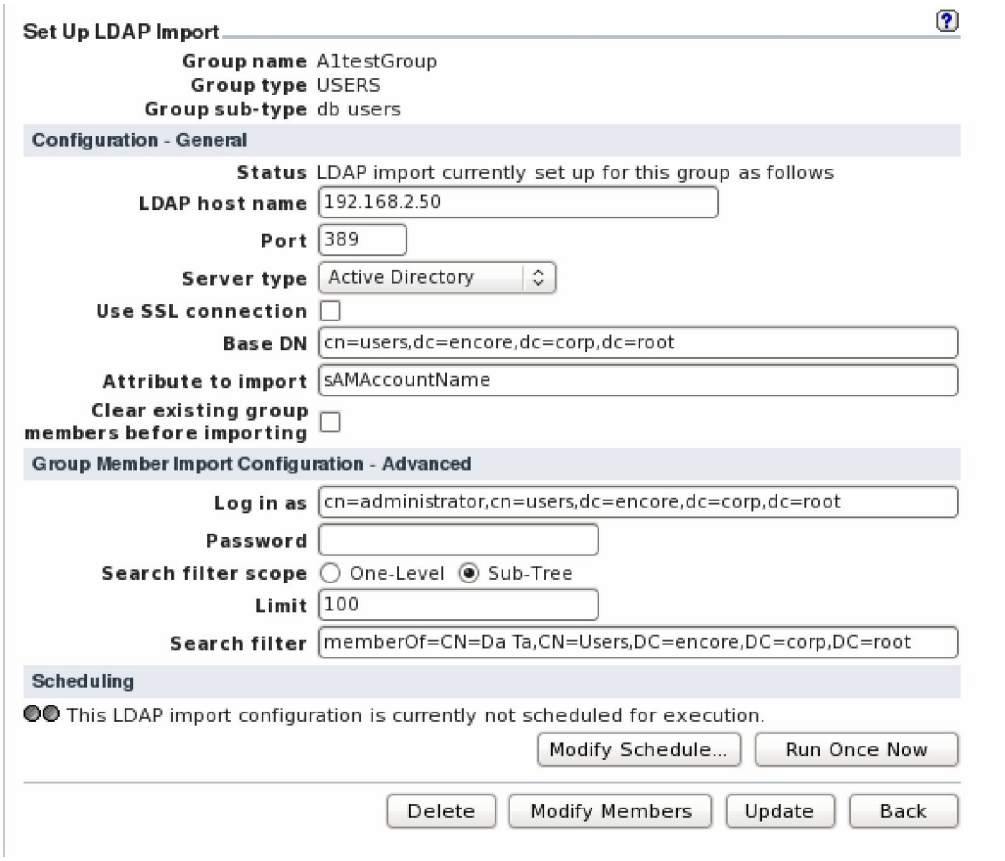
手順

Guardium システムで LDAP サーバーを構成します。「設定」 > 「グループ・ビルダー (レガシー)」をクリックして「グループ・ビルダー」を開き、必須情報を入力します。

a. 「LDAP ホスト名」に、アクセス先の LDAP サーバーの IP アドレスまたはホスト名を入力します。
b. 「ポート」に、LDAP サーバーへの接続に使用するポート番号を入力します。
c. 「サーバー・タイプ」メニューから、LDAP サーバー・タイプを選択します。

d. Guardium から LDAP サーバーに SSL (Secure Sockets Layer) 接続を使用して接続する場合は、「SSL 接続を使用」チェック・ボックスにチェック・マークを付けます。
e. 「基本 DN」に、検索を開始する、ツリー内のノードを指定します。例えば、企業ツリーは DC=encore,DC=corp,DC=root のように開始されることがあります。
f. 「インポートする属性」に、ユーザーのインポートに使用する属性 (例えば、cn) を入力します。各属性は名前を持ち、objectClass に属します。
g. インポートする前にすべての既存のグループ・メンバーを削除する場合は、「インポートする前に既存のグループ・メンバーをクリアする」チェック・ボックスにチェック・マークを付けます。
h. 「ログイン・ユーザー」および「パスワード」に、Guardium サーバーに接続するユーザー・アカウントの情報を入力します。
i. 「検索フィルターの有効範囲」に、基本レベルにのみ検索を適用する場合は「1 レベル」を、基本レベルの下のレベルに検索を適用する場合は「サブツリー」を選択します。
j. 「制限」に、返される項目の最大数を入力します。過剰な数のメンバーを意図せずロードしてしまうことを防ぐため、このフィールドを 使用して、新規照会や、既存の照会への変更をテストすることをお勧めします。
k. オプション: 「検索フィルター」に、基本 DN、有効範囲、および検索フィルターを定義します。通常、インポートは LDAP グループのメンバーシップに基づいているため、memberOF キーワードを使用します。 例えば、 「memberOf=CN=syyTestGroup,DC=encore,DC=corp,DC=root」を使用します。
l. 「適用」をクリックして、構成設定を保存します。

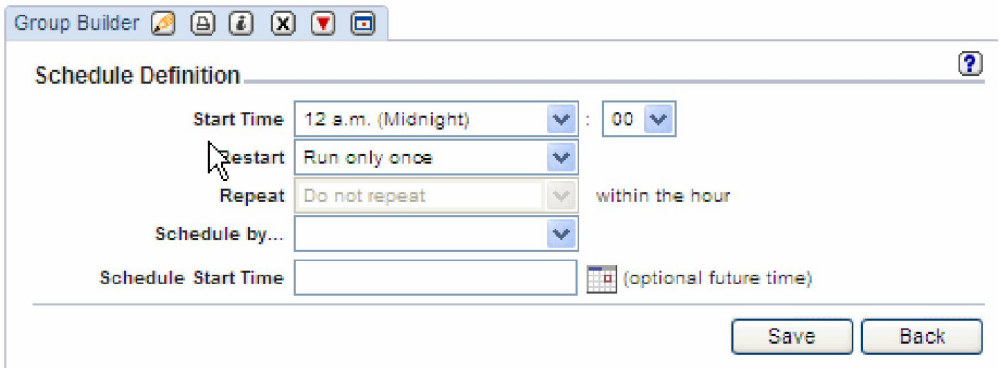
「構成 - 一般」セクションの「状況」標識が「*このグループの LDAP インポートは現在、次のように設定されています*」に変わり、「スケジュールの変更」ボタンと「今すぐ 1 回実行」ボタンが有効になります。これで、LDAP サーバーからインポートすることができます。



次のタスク

インポートを実行またはスケジュールします。

- LDAP インポートをスケジュールするには、「スケジュールの変更」をクリックし、スケジュールの情報を入力してから、「保存」をクリックします。



- オンデマンドでインポートを実行するには、「今すぐ 1 回実行」をクリックします。 タスクの完了後、ユーザーの選択基準を満たすメンバー・セットが「LDAP 照会結果」パネルに表示されます。

注:

オンデマンドでインポートする際には、LDAP サーバーから返される各エントリーを受け入れるか拒否する機会が与えられます。

LDAP インポートをスケジュールする際には、ユーザーの検索基準を満たす LDAP エントリーがすべてインポートされます。

「グループ・ビルダー」でグループを選択し、次に、「変更」  をクリックしてグループのメンバーシップを確認することで、メンバーがそのグループに追加されていることを検証します。

大規模なグループの場合は、Guardium グループの詳細レポート (「レポート」 > 「Guardium グループの詳細」) を使用すると、メンバーをより簡単に検証できる場合があります。

親トピック: グループへの取り込み

照会を使用したグループへの取り込み

照会を作成し、その結果を使用してグループにデータを取り込みます。 このグループへの取り込みオプションは、外部データ相関によってカスタム表が Guardium システムにアップロードされた後に使用すると最も効果的です。

手順

1. 「設定」 > 「グループ・ビルダー (レガシー)」をクリックして、「グループ・ビルダー」を開きます。データの取り込み先グループをフィルターを使用して見つけるか、「次へ」をクリックしてすべてのグループのリストから見つけます。
2. グループが選択された状態で、「照会から取り込み」ボタンをクリックして、「照会からグループに取り込みの設定」パネルを開きます。
3. 「照会」リストから、実行する照会を選択します。
    a. データの取り込み先グループのタイプによって、表示されるフィールドは異なります。ほとんどのグループ・タイプでは、「列からメンバーをフェッチ」メニューが表示されます。
    b. ペアの属性グループ (オブジェクト/コマンド、オブジェクト/フィールド、またはクライアント IP/DB ユーザー) の場合、「属性 1 の列の選択」および「属性 2 の列の選択」の 2 つのメニューが表示されます。
    c. グループへのデータの取り込みに使用する列 (複数可)、および照会で使用する追加のパラメーターを選択してください。すると、照会のランタイム・パラメーターがペインに追加されます。
4. 新規メンバーをインポートする前に既存のグループの内容を削除するには、「インポートする前に既存のグループ・メンバーをクリアする」ボックスを選択します。
5. オプション: リモート・ソースを選択します (中央マネージャーからのみ選択可能)。
6. 「保存」をクリックして定義を保存します。
7. 「今すぐ 1 回実行」をクリックして照会をすぐに実行することも、「スケジュールの変更」をクリックして将来の照会のスケジュールを設定することもできます。

親トピック: グループへの取り込み

ストアード・プロシージャーを使用したグループへの取り込み

ストアード・プロシージャーからコマンド・グループまたはオブジェクト・グループにデータを取り込む方法はいくつかあります。「グループ・ビルダー」の自動生成呼び出しプロシージャー機能では、特定のグループ・メンバーのコマンド・グループまたはオブジェクト・グループを分析して、それらのメンバーを新規グループに追加することができます。

このタスクについて

「グループ・ビルダー (レガシー)」は、以下の 2 つの方法で、コマンド・グループ・タイプまたはオブジェクト・グループ・タイプにデータを自動的に取り込むことができます。

- ストアード・プロシージャーのソース・コードを分析する方法。 このオプションを使用するには、ストアード・プロシージャーが定義されているデータベース に Guardium® がアクセスする必要があります。また、ストアード・プロシージャーは、 暗号化フォーマットで格納されていてはなりません。
- Guardium がモニターおよびロギングしているデータベース・トラフィックで、 ストアード・プロシージャーを分析する方法。 このオプションを使用するには、Guardium アプライアンスが (例えば、「セッションを無視」アクションや「ロギングをスキップ」アクションを使用するのではなく) 適切なデータベース・ストリームを検査しており、その情報をロギングしていること、 分析タスクが (アーカイブ/パージ操作の後で実行するのではなく) データがまだユニット上にある間に実行されることが必要です。

ストアード・プロシージャーからグループへの取り込みには、次の 2 つのグループが関与します。

- 受信グループ。メンバーの追加先となります。
- 開始グループ。分析の対象になります。このグループは、既存のコマンド・グループまたはオブジェクト・グループでなければなりません。この検索および追加プロセスは再帰的です。 例えば、受信グループに prox_one という名前のストアード・プロシージャーが追加され、prox_one が prox_two で参照されている場合、prox_two も受信グループに追加されます。

注: ストアード・プロシージャーのグループ・メンバー・フィールドではワイルドカードはサポートされていません。

手順

1. 「設定」 > 「グループ・ビルダー (レガシー)」をクリックして、「グループ・ビルダー」を開きます。
2. コマンド・グループ・タイプまたはオブジェクト・グループ・タイプのいずれかの開始グループを分析対象として選択します。
3. 開始グループが選択された状態で、「自動生成呼び出しプロシージャー」をクリックします。次の 5 つのオプションがあります。
    a. データベース・ソースの使用: 1 つ以上のデータベースからストアード・プロシージャー定義を分析することにより、グループにデータを取り込みます。
    b. データベース従属関係の使用 - 関数、Java クラス、パッケージ、プロシージャー、同義語、表、トリガー、および/またはビューを分析することにより、オブジェクトのグループまたは修飾されたオブジェクトのグループにデータを取り込みます。
    c. 逆従属関係の使用: オブジェクト・セットから開始する場合に使用されるオブジェクト・セットを計算することにより、グループにデータを取り込みます。
    注: 「逆従属関係の使用」オプションは、Oracle でのみ使用可能です。

d. 監視対象プロシージャーの使用: CREATE PROCEDURE コマンドおよび ALTER PROCEDURE コマンドを (データベース・トラフィックで監視されるにつれて) 分析することにより、グループにデータを取り込みます。
e. 選択したオブジェクトの生成: 監視対象ストアード・プロシージャーをリバース分析することにより、グループにデータを取り込みます。ストアード・プロシージャー・セットから開始する場合、これらのプロシージャーが (直接的または間接的に) 使用する すべての表を計算します。
注: 「選択したオブジェクトの生成」オプションは、オブジェクト・グループ・タイプでのみ使用できます。

- データベース・ソースを使用したグループへの取り込み
- データベース従属関係を使用したグループへの取り込み
  このオプションを使用して、関数、Java クラス、パッケージ、プロシージャー、同義語、表、トリガー、および/またはビューなどの、データベース従属関係に基づいてグループにデータを取り込みます。**このオプションは、Oracle データベースの場合のオブジェクト・グループ・タイプに対してのみ機能にします。**このオプションは、*コマンド・グループ・タイプ*では機能しません。これは、データベース内の従属関係情報がオブジェクトにしか関連していないためです。
- 逆従属関係を使用したグループへの取り込み
  「選択したオブジェクトの生成」は、監視対象ストアード・プロシージャーをリバース分析することにより、グループにデータを取り込みます。
- 監視対象プロシージャーを使用したグループへの取り込み
  Guardium は、ストアード・プロシージャーに対するすべての変更または追加を検査することにより、グループにデータを取り込みます。これにより、ストアード・プロシージャーに対する変更の継続的な分析を通じて、 マッピング情報が最新の状態に保たれます。
- 選択したオブジェクトの生成を使用したグループへの取り込み
  「選択したオブジェクトの生成」オプションは、自動生成呼び出しプロシージャー機能の一部であり、監視対象ストアード・プロシージャーをリバース分析することにより、オブジェクト・グループ・タイプにデータを取り込みます。

親トピック: グループへの取り込み

データベース・ソースを使用したグループへの取り込み

始める前に

このオプションの使用手順は、以下のとおりです。

- 対象のストアード・プロシージャーが定義されている場所を認識している必要があります。
- ソースは、暗号化フォーマットで格納されていてはなりません。
- これらのデータベース上のストアード・プロシージャー・ソースに対するアクセス権を保持している必要があります。

このタスクについて

Guardium は、1 つ以上のデータベース・サーバー上で、ストアード・プロシージャー・ソース・コードを分析します。 グループを選択して自動生成呼び出しプロシージャープロセスを実行し、ストアード・プロシージャーをスキャンします。 このプロセスでは、選択したグループを検査して、そのグループ内の任意のオブジェクトがアクセス可能であるかどうかや、 そのグループ内の任意のコマンドが実行可能であるかどうかを調べます。 一致があればすべて新規グループに追加されます。データベース・ソースを使用してグループに取り込む場合

手順

1. 「設定」 > 「グループ・ビルダー (レガシー)」をクリックして、「グループ・ビルダー」を開きます。データの取り込み先グループをフィルターを使用して見つけるか、「次へ」をクリックしてすべてのグループのリストから見つけます。
   注: このオプションは、コマンド・グループ・タイプまたはオブジェクト・グループ・タイプでのみ使用できます。
2. グループが選択された状態で、「自動生成呼び出しプロシージャー」をクリックして、「データベース・ソースの使用」オプションを選択します。 すると、「ストアード・プロシージャーの分析」パネルが開きます。
3. 「データ・ソースの追加」をクリックして、「データ・ソース・ファインダー」からデータ・ソースを選択します。選択されたデータ・ソースが「データ・ソース」ペインに表示されます。
4. オプション: 「照会パラメーター」を入力します。 一部のフィールドは、特定のデータベースだけに適用されます。
   - **Sybase、MS SQL Server、および Informix の場合、**操作が制限されるデータベースの名前を入力します。ブランクの場合、マスター・データベース内のすべてのストアード・プロシージャーが分析されます。
   - **MySQL、Oracle、または Db2 の場合のみ、**操作が制限されるデータベースを所有するスキーマの名前を入力します。MySQL の場合のみ、「スキーマ所有者」の形式は user_name@host になります。 ここで、host には特定の IP を入力することも、 % を入力してすべてのホストを指定することもできます。 すべてのホストを取得するには、スキーマ名に続けて % を入力してください。
   - **MySQL、Oracle、または Db2 の場合のみ、**「オブジェクト名」にストアード・プロシージャー名を入力します。ワイルドカード文字を使用できます。例えば、文字 ABC で始まるプロシージャーのみを対象とする場合、「オブジェクト名」 ボックスに ABC% と入力します。
5. 「ソース詳細構成」セクションで、以下のいずれかを実行します。
   - 「追加」チェック・ボックスにチェック・マークを付け、次に「既存のグループ名」メニューからグループを選択して、既存のグループにメンバーを追加します。
   - 「新規グループ名」に新規グループ名を入力して、新規グループにメンバーを追加します。
     注: グループ名にはアポストロフィ文字を含めないでください。
6. 「名前空間のフラット化」を選択し、ワイルドカード文字を使用してメンバー名を作成し、グループを LIKE GROUP 比較で使用できるようにします。例えば、sp_1 がディスカバーされると、 メンバー %sp_1% がグループに追加され、 LIKE GROUP 比較において値 sp_101、 sp_102、sss_sp_103 などがすべて一致することになります。
7. 「データベースの分析」をクリックして、グループへのデータの取り込みを開始します。この操作が完了するまでしばらく時間がかかることがあります。

親トピック: ストアード・プロシージャーを使用したグループへの取り込み

データベース従属関係を使用したグループへの取り込み

このオプションを使用して、関数、Java クラス、パッケージ、プロシージャー、同義語、表、トリガー、および/またはビューなどの、データベース従属関係に基づいてグループにデータを取り込みます。**このオプションは、Oracle データベースの場合のオブジェクト・グループ・タイプに対してのみ機能にします。**このオプションは、*コマンド・グループ・タイプ*では機能しません。これは、データベース内の従属関係情報がオブジェクトにしか関連していないためです。

このタスクについて

グループ・タイプを指定する際、*オブジェクト* または *修飾されたオブジェクト* のグループ・タイプのみがこのオプションで使用できることを覚えておいてください。修飾されたオブジェクトでは、サーバー IP、インスタンス、データベース名、所有者、およびオブジェクトの 5 つの値属性が必要です。 このオブジェクトは、5 タプル・オブジェクトとも呼ばれます。

「修飾されたオブジェクト」グループ・メンバーの表示例は、 「192.168.1.0+guardium+oracle+admin+fininacial object」のようになります。

手順

1. 「設定」 > 「グループ・ビルダー (レガシー)」をクリックして、「グループ・ビルダー」を開きます。データの取り込み先グループをフィルターを使用して見つけるか、「次へ」をクリックしてすべてのグループのリストから見つけます。
2. オブジェクト・グループまたは修飾されたオブジェクト・グループが選択された状態で、「自動生成呼び出しプロシージャー」をクリックして、「データベース従属関係の使用」オプションを選択します。すると、「ストアード・プロシージャーの分析」パネルが開きます。
3. 「データ・ソースの追加」をクリックして、「データ・ソース・ファインダー」からデータ・ソースを選択します。選択されたデータ・ソースが「データ・ソース」ペインに表示されます。
4. オプション: 「照会パラメーター」を入力します。
5. 「ソース詳細構成」セクションで、以下のいずれかを実行します。
   - 「追加」ボックスにチェック・マークを付け、次に「既存のグループ名」メニューからグループを選択して、既存のグループにメンバーを追加します。
   - 「新規グループ名」に新規グループ名を入力して、新規グループにメンバーを追加します。
     注: グループ名にアポストロフィ文字を含めないでください。また、新規グループが完全に修飾されていること (サーバー IP、インスタンス、データベース名、所有者、およびオブジェクトの 5 つの値属性が指定されていること) を確認してください。
6. 「名前空間のフラット化」を選択し、ワイルドカード文字を使用してメンバー名を作成し、グループを LIKE GROUP 比較で使用できるようにします。 例えば、sp_1 がディスカバーされると、 メンバー %sp_1% がグループに追加され、 LIKE GROUP 比較において値 sp_101、 sp_102、sss_sp_103 などがすべて一致することになります。
7. 「インクルード・タイプ」セクションで、データベース従属関係 (関数、Java クラス、パッケージ、プロシージャー、同義語、表、トリガー、および/またはビュー) を選択します。
8. 「データベースの分析」をクリックして、 グループにデータを取り込みます。結果が通知されます。

親トピック: ストアード・プロシージャーを使用したグループへの取り込み

逆従属関係を使用したグループへの取り込み

「選択したオブジェクトの生成」は、監視対象ストアード・プロシージャーをリバース分析することにより、グループにデータを取り込みます。

このタスクについて

グループ自動取り込みメニューのこれらのオプションは、オブジェクト・セットから開始する場合に使用されるオブジェクト・セットを計算します。 例えば、ストアード・プロシージャー・セットから開始する場合、これらのプロシージャーが (直接的または間接的に) 使用する すべての表を計算します。

手順

1. 「設定」 > 「グループ・ビルダー (レガシー)」をクリックして、「グループ・ビルダー」を開きます。データの取り込み先グループをフィルターを使用して見つけるか、「次へ」をクリックしてすべてのグループのリストから見つけます。
   注: 「逆従属関係」オプションは Oracle の場合にのみ使用可能です。
2. グループが選択された状態で、「自動生成呼び出しプロシージャー」をクリックして、「逆従属関係の使用」オプションを選択します。すると、「ストアード・プロシージャーの分析」パネルが開きます。
3. 「データ・ソースの追加」をクリックして、「データ・ソース・ファインダー」からデータ・ソースを選択します。選択されたデータ・ソースが「データ・ソース」ペインに表示されます。
4. オプション: 「照会パラメーター」を入力します。
5. 「ソース詳細構成」セクションで、以下のいずれかを実行します。
   - 既存のグループにメンバーを追加するには、「追加」を選択し、次に「既存のグループ名」リストからグループを選択します。
   - 新規グループにメンバーを追加するには、「新規グループ名」に新規グループ名を入力します。
     注: グループ名にはアポストロフィ文字を含めないでください。
6. 「名前空間のフラット化」を選択し、ワイルドカード文字を使用してメンバー名を作成し、グループを LIKE GROUP 比較で使用できるようにします。 例えば、sp_1 がディスカバーされると、 メンバー %sp_1% がグループに追加され、 LIKE GROUP 比較において値 sp_101、 sp_102、sss_sp_103 などがすべて一致することになります。
7. 「インクルード・タイプ」セクションで、データベース従属関係 (関数、Java クラス、パッケージ、プロシージャー、同義語、表、トリガー、および/またはビュー) を選択します。
8. 「データベースの分析」をクリックして、 グループにデータを取り込みます。結果が通知されます。

親トピック: ストアード・プロシージャーを使用したグループへの取り込み

監視対象プロシージャーを使用したグループへの取り込み

Guardium は、ストアード・プロシージャーに対するすべての変更または追加を検査することにより、グループにデータを取り込みます。これにより、ストアード・プロシージャーに対する変更の継続的な分析を通じて、 マッピング情報が最新の状態に保たれます。

手順

1. 「設定」 > 「グループ・ビルダー (レガシー)」をクリックして、「グループ・ビルダー」を開きます。データの取り込み先グループをフィルターを使用して見つけるか、「次へ」をクリックしてすべてのグループのリストから見つけます。
2. 開始グループが選択された状態で、「自動生成呼び出しプロシージャー」をクリックして、「監視対象プロシージャーの使用」オプションを選択します。すると、「監視ストアード・プロシージャーの分析」パネルが開きます。

3. 既存の構成を編集する場合、「ソース詳細」リストからその構成を選択します。新しい構成を作成するには、「*新規*」をクリックします。
4. 「アクセス情報」セクションで、分析するデータベース・サーバーをすべて選択します。チェック・ボックスは、どの組み合わせでも選択できます。
5. 「ソース詳細構成」セクションで、以下のいずれかを実行します。
   - 「追加」ボックスにチェック・マークを付け、次に「既存のグループ名」メニューからグループを選択して、既存のグループにメンバーを追加します。
   - 「新規グループ名」に新規グループ名を入力して、新規グループにメンバーを追加します。
     注: グループ名にはアポストロフィ文字を含めないでください。
6. 「名前空間のフラット化」を選択し、ワイルドカード文字を使用してメンバー名を作成し、グループを LIKE GROUP 比較で使用できるようにします。 例えば、sp_1 がディスカバーされると、 メンバー %sp_1% がグループに追加され、 LIKE GROUP 比較において値 sp_101、 sp_102、sss_sp_103 などがすべて一致することになります。
7. 「保存」をクリックして構成を保存します。
8. 以下のいずれかを行うことによって、グループのスケジュールを設定します。
   - 照会を即時に実行して結果をすぐに得るには、「今すぐ 1 回実行」をクリックします。
   - 操作のスケジュールを定義するには、「スケジュールの変更」をクリックします。

親トピック: ストアード・プロシージャーを使用したグループへの取り込み

選択したオブジェクトの生成を使用したグループへの取り込み

「選択したオブジェクトの生成」オプションは、自動生成呼び出しプロシージャー機能の一部であり、監視対象ストアード・プロシージャーをリバース分析することにより、オブジェクト・グループ・タイプにデータを取り込みます。

このタスクについて

Guardium は、ストアード・プロシージャーに対するすべての変更または追加を検査することにより、グループにデータを取り込みます。 これにより、ストアード・プロシージャーに対する変更の継続的な分析を通じて、 マッピング情報が最新の状態に保たれます。

手順

1. 「設定」 > 「グループ・ビルダー (レガシー)」をクリックして、「グループ・ビルダー」を開きます。データの取り込み先グループをフィルターを使用して見つけるか、「次へ」をクリックしてすべてのグループのリストから見つけます。
2. 開始グループが選択された状態で、「自動生成呼び出しプロシージャー」をクリックして、「選択したオブジェクトの生成」オプションを選択します。すると、「監視ストアード・プロシージャーの分析」パネルが開きます。
3. 既存の構成を編集する場合、「ソース詳細」メニューからその構成を選択します。新しい構成を作成するには、*「新規」*をクリックします。
4. 「アクセス情報」セクションで、分析するデータベース・サーバーをすべて選択します。チェック・ボックスは、どの組み合わせでも選択できます。
5. 「ソース詳細構成」セクションで、名前を入力して、「verb」メニューからオプションを選択します。
6. 以下のいずれかを実行します。
   - 「追加」ボックスにチェック・マークを付け、次に「既存のグループ名」メニューからグループを選択して、既存のグループにメンバーを追加します。
   - 「新規グループ名」に新規グループ名を入力して、新規グループにメンバーを追加します。
     注: グループ名にはアポストロフィ文字を含めないでください。
7. 「名前空間のフラット化」を選択し、ワイルドカード文字を使用してメンバー名を作成し、グループを LIKE GROUP 比較で使用できるようにします。 例えば、sp_1 がディスカバーされると、 メンバー %sp_1% がグループに追加され、 LIKE GROUP 比較において値 sp_101、 sp_102、sss_sp_103 などがすべて一致することになります。
8.
9. 「保存」をクリックして構成を保存します。
10. 以下のいずれかを行うことによって、グループのスケジュールを設定します。
    - 照会を即時に実行して結果をすぐに得るには、「今すぐ 1 回実行」をクリックします。
    - 操作のスケジュールを定義するには、「スケジュールの変更」をクリックします。

親トピック: ストアード・プロシージャーを使用したグループへの取り込み

照会およびポリシーでのグループの使用

照会の条件演算子、およびポリシーでグループを使用する場所についての簡単な概要

照会

照会では、条件演算子とグループが使用されます。以下に、各条件演算子の例を示します。

- IN GROUP - 値が、選択したグループの任意のメンバーと一致する場合、 条件は真になります。IN ALIASES GROUP 演算子は、IN GROUP と同じタイプのグループに対して機能しますが、 そのグループのメンバーが別名であると想定します。 IN GROUP 演算子はグループが実際の値を、IN ALIASES GROUP 演算子はグループが別名を含んでいることを予期します。 クエリー・ビルダーは、グループ内の別名値に一致するデータベース値のレコードを探します。
- NOT IN GROUP - 値が、選択したグループのどのメンバーとも一致しない場合、 条件は真になります。NOT IN ALIASES GROUP は、NOT IN GROUP と同じタイプのグループに対して機能しますが、そのグループのメンバーが別名であると想定します。
- IN DYNAMIC GROUP - 値が、ランタイム・パラメーターとして指定された任意のグループのメンバーと一致する場合、条件は真になります。 IN DYNAMIC ALIASES GROUP は、IN DYNAMIC GROUP と同じタイプのグループに対して機能しますが、 そのグループのメンバーが別名であると想定します。
- NOT IN DYNAMIC GROUP - 値が、ランタイム・パラメーターとして指定されるグループの任意のメンバーに一致しない場合、 条件は真になります。NOT IN DYNAMIC ALIASES GROUP は、NOT IN DYNAMIC GROUP と同じタイプのグループに対して機能しますが、 そのグループのメンバーが別名であると想定します。
  注: グループには、使用する演算子 (IN GROUP または IN ALIASES GROUP) に応じて、別名が含まれる場合も実値が含まれる場合もありますが、これらの演算子を同時に使用することはできません。
- LIKE GROUP - 値が、選択したグループのいずれかのメンバーと類似している場合、条件は真になります。この条件では、グループ・メンバー名にワイルドカード (%) 文字を使用できます。
  注: LIKE メンバー値では、値の全部または一部に一致する 1 つ以上のワイルドカード (%) 文字が使用されます。 LIKE 比較では、英字に大/小文字の区別はありません。 例えば、%tea% は tea、 TeA、tEam、または steam と一致します。

ポリシーおよびルール

ポリシーの一部としてルールを作成する場合は、グループを使用することで、目的のパラメーターを指定するプロセスを簡略化できます。

「ルール定義」ペインの「グループ」ドロップダウン・メニューがある場所で、グループを選択できます。

さらに、グループを急いで作成または変更する必要が生じた場合は、「グループ」アイコン  をクリックして「グループ定義」ウィンドウを開き、必要な変更を加えます。

例: 実動サーバー上で発生しているアクティビティーをキャプチャーする場合は、完全 IP アドレスを毎回入力する代わりに、*「実動サーバー」* というグループを作成して、これを使用できます。

親トピック: グループ

例: グループを使用したルールとポリシーの作成

グループを使用して、ポリシーのルール条件を素早く指定します。

このタスクについて

各ポリシーは、1 つ以上のルールで構成されています。ルールを規定する条件を指定し、そのルールがトリガーされたときに実行するアクションを 1 つ以上選択します。この例では、グループを使用して無許可ユーザーを識別し、機密オブジェクトのグループへのそれらのユーザーのアクセスの詳細をログに記録し、アクセスが発生したことを示すアラートを送信する方法を説明します。

手順

1. Guardium システムにログインし、「設定」 > 「ツールとビュー」 > 「データのポリシー・ビルダー」をクリックして、「ポリシー・ビルダー」を開きます。
2.  アイコンをクリックして、「ポリシー定義」ウィンドウを開き、新規ポリシーを作成します。
3. ポリシー定義を定義し、「適用」をクリックしてポリシーを保存します。
4. 「ルールの編集」をクリックして「ポリシー・ルール」ウィンドウを開き、ポリシーへのルールの追加を開始します。
5. 「ルールの追加」 > 「アクセス・ルールの追加」をクリックして、ポリシーに新しいルールを追加します。
6. 最初にルールの「記述」を指定します。オプションで、「カテゴリー」ラベルおよび「分類」ラベルを指定します。
7. データの検索場所を指定します。「サーバー IP」行で、「(パブリック) PCI 許可されたサーバー IP」グループを選択します。 ルールは、すべての PCI サーバーからのすべてのアクティビティーに適用されます。
   注:「グループ・ビルダー」に移動して、任意のグループのメンバーを表示したり、任意のグループを変更したりすることができます。
8. 無許可ユーザーを指定します。「データベース・ユーザー」行で「Not」チェック・ボックスにマークを付け、「(パブリック) 許可されたユーザー」グループを選択します。「*(パブリック) 許可されたユーザー*」グループに所属しないすべてのユーザーにルールが適用されます。
9. 機密オブジェクトを指定します。「オブジェクト」行で、「(パブリック) PCI カード所有者の機密オブジェクト」を選択します。 これで、ルールは、PCI 機密オブジェクトにアクセスしようとしている PCI サーバー上のすべての無許可ユーザーに適用されます。
10. 「アクションの追加」をクリックし、メニューから「アクション」 > 「全詳細をロギング」を選択して、ルールにアクションを追加します。「適用」をクリックしてルールを保存します。 このアクションにより、アクセスの正確なタイム・スタンプなど、アクセスの詳細がログに記録されます。
11. 「アクションの追加」をクリックし、メニューから「アクション」 > 「セッションごとに 1 回アラート」を選択して、ルールに別のアクションを追加します。アラートの宛先を指定し、「適用」をクリックしてルールを保存します。 このアクションにより、ルールがトリガーされたことを示すアラートが送信されるか、ログに記録されます。
12. 「保存」をクリックして、ルールを保存します。
13. ポリシーをインストールします。
    a. 作成したポリシーを検索します。「戻る」を 2 回クリックするか、「ポリシー・ビルダー」をクリックして「ポリシー・ファインダー」に移動し、ポリシーのリストを参照します。
    b. ポリシーを選択した状態で、インストール・アクション・メニューから「インストールおよびオーバーライド」を選択します。
    c. 「OK」をクリックして、ポリシーのインストールを確認してから、「最近のログと違反」にチェック・マークを付けて、ポリシーがインストールされたことを確認します。

    これで、ポリシーはインストールされてアクティブになっています。「*(パブリック) 許可されたユーザー*」グループに属していないいずれかのユーザーが「*(パブリック) PCI カード所有者の機密オブジェクト*」グループ内のオブジェクトにアクセスしようとすると、そのセッションがログに記録され、アクセスを示すアラートがトリガーされます。

親トピック: グループ

事前定義グループ

このセクションでは、Guardium® の事前定義グループについて詳しく説明します。

次の表では、Guardium システムに含まれている事前定義グループについて説明しています。すべてのグループのリストを表示するには、「設定」 > 「グループ・ビルダー」をクリックして、「グループ・ビルダー」を開きます。「アプリケーション」メニューから「*SQL_APP_NAME*」を選択して、「次へ」をクリックします。次の画面の「選択されたグループ」から、メンバーの管理を行います。*グループ・タイプ*という用語は、ラベルによって示されるデータ・タイプの予期を指します。 例えば、グループ・タイプ「*サーバー IP*」では、IP アドレスとして配列されたデータ (192.168.1.0) が予期され、グループ・タイプ「*ユーザー*」では、アプリケーションのユーザーの名前が示されることが予期されます。

事前定義グループは定期的に追加され、この追加の事前定義グループについてはここに説明されていない場合があります。 「グループ・ビルダー」を開き、すべての既存のグループを表示します。

グループ・タイプ「データベース・ユーザー/データベース・パスワード」の事前定義グループは、admin のロールを持つユーザーにしか許可されていません。 ユーザーは好みに応じて他のロールを追加できます。さらには、グループに対してすべてのロールを許可することもできます。

表 1. 事前定義グループ

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
DB2® zOS グループ	zOS 監査動的 SQL	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査照会	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査のアップデート	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査の削除	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査の挿入	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査ユーティリティー	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査オブジェクト・メンテナンス	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査ユーザー・メンテナンス	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査のユーザー許可の変更	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査 DB2 コマンド	DB2 コマンドのグループ・タイプ
DB2 zOS グループ	zOS 監査計画/パッケージ・メンテナンス	DB2 コマンドのグループ・タイプ
IMS™ zOS グループ	zOS IMS 監査照会	IMS コマンドのグループ・タイプ
IMS zOS グループ	zOS IMS 監査のアップデート	IMS コマンドのグループ・タイプ
IMS zOS グループ	zOS IMS 監査の削除	IMS コマンドのグループ・タイプ
IMS zOS グループ	zOS IMS 監査の挿入	IMS コマンドのグループ・タイプ
IMS zOS グループ	zOS IMS 監査データベース・コマンド	IMS コマンドのグループ・タイプ
ポリシー・ビルダー	カード所有者オブジェクト	グループ・タイプ、オブジェクト
ポリシー・ビルダー	財務オブジェクト	グループ・タイプ、オブジェクト
ポリシー・ビルダー	PHI オブジェクト	グループ・タイプ、オブジェクト
ポリシー・ビルダー	許可されたクライアント IP	グループ・タイプ、クライアント IP
ポリシー・ビルダー	実動ユーザー	グループ・タイプ、ユーザー
ポリシー・ビルダー	PII オブジェクト	グループ・タイプ、オブジェクト
ポリシー・ビルダー	実動サーバー	グループ・タイプ、サーバー IP
ポリシー・ビルダー	財務サーバー	グループ・タイプ、サーバー IP
ポリシー・ビルダー	機能ユーザー	グループ・タイプ、ユーザー
ポリシー・ビルダー	Sharepoint サーバー	グループ・タイプ、サーバー IP
セキュリティー・アセスメント・ビルダー	DB2 データベース Version+Patches Informix® データベース Version+Patches MS SQL Server データベース Version+Patches MySql データベース Version+Patches Netezza® Version+Patches Oracle データベース Version+Patches Postgress Version+Patches Sybase データベース Version+Patches Teradata PDE Version+Patches Teradata TDBMS Version+Patches Teradata TDGSS Version+Patches Teradata TGTW Version+Patches	(特定の) データベース・バージョンおよびパッチ・レベルのテストに使用

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
セキュリティー・アセスメント・ビルダー	DB2 許可された PUBLIC への特権の付与 Informix 許可された PUBLIC への特権の付与 MS-SQL 許可された PUBLIC への特権の付与 MYSQL 許可された PUBLIC への特権の付与 Netezza 許可された PUBLIC への特権の付与 Oracle 許可された PUBLIC への特権の付与 Postgres 許可された PUBLIC への特権の付与 Teradata 許可された PUBLIC への特権の付与	TUPLE、 オブジェクト/コマンド・アプリケーション 8 (セキュリティー・アセスメント) パブリックへの特権の付与が許可されているオブジェクト/コマンドのリスト これらのオブジェクトは、パブリックへの特権付与をチェックする MS-SQL および Sybase のテストではスキップされます。 注: 例外グループには、正規表現を含めることも、メンバーだけを含めることもできます。 正規表現の場合、グループ・メンバーは (R) (大/小文字の区別あり) で始める必要があり、(R) の後ろに正規表現としてチェックされる詳細なレコードが続きます。 例えば、次のようなグループ・メンバーがあるとします。 (R)SYSTEM.[a-z]+ この場合、各レコードの詳細はパターン SYSTEM.[a-z]+ を使用してチェックされます。 メンバーが (R) で始まらない場合、レコード詳細はそのグループ・メンバーと等しい場合のみ例外と見なされます。 グループには正規表現と特定の例外を混用できることに注意してください。
セキュリティー・アセスメント・ビルダー	MS-SQL 許可された拡張プロシージャー	グループ・タイプはオブジェクト
セキュリティー・アセスメント・ビルダー	MS-SQL データベース管理者	グループ・タイプはユーザー
セキュリティー・アセスメント・ビルダー	Teradata プロファイル	グループ・タイプはオブジェクト
パブリック	アカウント管理コマンド	アカウント (ユーザー、ロール、アクセス権) の保守に使用されるコマンド。例: REVOKE、GRANT、ALTER/CREATE/DROP USER
パブリック	アカウント管理プロシージャー	アカウント (ユーザー、ロール、アクセス権) の保守に使用されるアカウント管理オブジェクト、ストアード・プロシージャー
パブリック	アクティブ・ユーザー	グループ・タイプはユーザー
パブリック	管理者ユーザー	デフォルトの管理ユーザー (DBA および SysAdmin)
パブリック	管理オブジェクト	特権オブジェクト。DBA アカウントまたは Sys アカウントのみがアクセスできるオブジェクト。これらのアカウントは、デフォルトでは「パブリック」に対してロックされています。
パブリック	管理コマンド	特権コマンド。 特権コマンドは、DBA だけが実行できるコマンドです。例: GRANT、BACKUP、DDL の各コマンド
パブリック	管理プログラム	データベースに同梱されているデータベース・ユーティリティー (クライアント) で、通常はデータベース・サーバーに置かれ、サーバー自体で使用できます。
パブリック	ALTER コマンド	例: alter database、alter procedure、alter profile、alter session、 alter user
パブリック	アプリケーション特権コマンド	「パブリック」から取り消す必要があるが、アプリケーションによって使用されているために取り消しできないパブリック特権コマンド。
パブリック	アプリケーション特権プロシージャー	アプリケーション特権オブジェクト。 「パブリック」から取り消す必要があるが、アプリケーションが使用しているために取り消しできないパブリック特権プロシージャー。
パブリック	アプリケーション・スキーマ・ユーザー	アプリケーション・ユーザー。 アプリケーションがアプリケーション表の保守/使用に使用するデータベース・ユーザー。
パブリック	アーカイブ候補	グループ・タイプはオブジェクト
パブリック	許可されたソース・プログラム	グループ・タイプはソース・プログラム
パブリック	許可されたユーザー	グループ・タイプはユーザー
パブリック	接続プロファイル・リスト	グループ・タイプは、クライアント IP/ソース・アプリケーション/DB ユーザー/サーバー IP/SVC です。 名前 許可される接続のリスト
パブリック	CREATE コマンド	例: create context、create database link、create function、create statistics、create type、create user

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
パブリック	資格情報関連エンティティー	Guardium 監査タイプ、 自己モニター。例: allowed_role、LDAP_config、Turbine_user_group_role
パブリック	データ転送コマンド	バックアップ・コマンド。 データベース・データのバックアップ/リストアを処理するコマンド
パブリック	データ転送プロシージャー	データ転送オブジェクト。 データベース・データ (主に MSS および SYB 上にある) のバックアップ/リストアを処理するプロシージャー
パブリック	データベース定義済みユーザー	非 admin の定義済みユーザー、または管理ユーザーを含むすべての定義済みユーザー
パブリック	DBCC コマンド	グループ・タイプはコマンド
パブリック	DDL コマンド	データ定義言語、 スキーマ特権コマンド。例: ALTER、CREATE、DROP
パブリック	DML コマンド	DML コマンド。 例: insert、truncate、update
パブリック	DROP コマンド	例: drop_context、drop_event_monitor、drop_procedure、drop_role
パブリック	DW すべてのオブジェクト・フィールド DW すべてのオブジェクト DW EXECUTE がアクセスしたオブジェクト DW SELECT がアクセスしたオブジェクト DW SELECT がアクセスしたオブジェクト/フィールド	モニター対象データを使用してオブジェクト名を表示する事前定義レポートが 5 つ あります。これらのレポートはすべて接頭部 DW (Data Warehouse) で始まります。これらの 事前定義レポートの使用法について詳しくは、ヘルプ・トピック『休止表/列のレポート方法』を参照してください。
パブリック	EBS アプリケーション・サーバー	グループ・タイプはクライアント IP
パブリック	EBS データベース・サーバー	グループ・タイプはサーバー IP
パブリック	EXECUTE コマンド	例: call、execute、execute function
パブリック	GRANT コマンド	例: grant、grant objectives、grant system privileges
パブリック	Guardium 詳細報告書用監査カテゴリー	Guardium パッチ。 TURBINE_USER_GROUP_ROLE
パブリック	ICM アプリケーション・サーバー	グループ・タイプはクライアント IP
パブリック	ICM データベース・サーバー	グループ・タイプはサーバー IP
パブリック	ImportLDAPUser	グループ・タイプはオブジェクト
パブリック	ImportLDAPUser_bindValues	グループ・タイプはオブジェクト
パブリック	検査エンジン・エンティティー	例: adminconsole_sniffer、software_tap_db_client、software_tap_db_server
パブリック	Java™ コマンド	例: alter java、create java、drop java
パブリック	KILL コマンド	例: kill
パブリック	Masked_SP_Executions_MS_SQL_SERVER	MS SQL Server では、ストアード・プロシージャー (SP) 名のコレクションを含むグループ。 含まれるプロシージャーが実行される場合、それが引用符で囲まれていても、すべてにマスクが掛けられます。 これは、空として事前定義されています。
パブリック	Masked_SP_Executions_Sybase	Sybase では、ストアード・プロシージャー (SP) 名のコレクションを含むグループ。 含まれるプロシージャーが実行される場合、それが引用符で囲まれていても、すべてにマスクが掛けられます。 これは、空として事前定義されています。
パブリック	MongoDB スキップ・コマンド	グループ・タイプはコマンド
パブリック	MS-SQL レプリケーション・プロシージャー	グループ・タイプはオブジェクト
パブリック	MS-SQL セキュリティー・システム・プロシージャー	グループ・タイプはオブジェクト
パブリック	MS-SQL システム・プロシージャー	グループ・タイプはオブジェクト
パブリック	Oracle EBS HRMS 機密オブジェクト	グループ・タイプはオブジェクト
パブリック	Oracle EBS-PCI	グループ・タイプはオブジェクト
パブリック	Oracle EBS-SOX	グループ・タイプはオブジェクト
パブリック	Oracle 定義済みユーザー	グループ・タイプはユーザー
パブリック	ピア関連コマンド	データのリンク/レプリケーション、例、リンク、配送記録、レプリケーション、スナップショットを処理するコマンド
パブリック	ピア関連プロシージャー	ピア関連オブジェクト、 データのリンク/レプリケーションを処理するプロシージャー 例: リンク、配送記録、レプリケーション、スナップショット
パブリック	PeopleSoft オブジェクト	グループ・タイプはオブジェクト
パブリック	PeopleSoft 機密オブジェクト	グループ・タイプはオブジェクト

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
パブリック	パフォーマンス・コマンド	例: analyze、create statistics、update all statistics
パブリック	Policy 関連エンティティー	例: access_rule、gdm_install_policy_header
パブリック	潜在的なオーバーフロー・オブジェクト	グループ・タイプはオブジェクト
パブリック	プロシージャー・コマンド	例: begin、call、execute、exit、repeat、set
パブリック	PROCEDURE DDL	例: alter procedure、create procedure、drop procedure
パブリック	PSFT アプリケーション・サーバー	グループ・タイプはクライアント IP
パブリック	PSFT データベース・サーバー	グループ・タイプはサーバー IP
パブリック	パブリック実行可能プロシージャー	実行専用オブジェクト。 デフォルトでパブリックへのアクセス権を付与されているプロシージャー/関数/パッケージ
パブリック	パブリック選択可能オブジェクト	選択専用オブジェクト。デフォルトでパブリックへのアクセス権を付与されている表
パブリック	RESTORE コマンド	例: restore database、restore log
パブリック	REVOKE コマンド	例: revoke object privileges、revoke system privileges
パブリック	リスク表示エラー・メッセージ	セキュリティーに関連した SQL エラー
パブリック	Sharepoint サーバー	
パブリック	SAP-PCI	グループ・タイプはオブジェクト
パブリック	SAP アプリケーション・サーバー	グループ・タイプはクライアント IP
パブリック	SAP データベース・サーバー	グループ・タイプはサーバー IP
パブリック	SAP HR 機密オブジェクト	グループ・タイプはオブジェクト
パブリック	SELECT コマンド	例: select、select list
パブリック	機密オブジェクト	例: activity、sales
パブリック	SIEBEL アプリケーション・サーバー	グループ・タイプはクライアント IP
パブリック	SIEBEL データベース・サーバー	グループ・タイプはサーバー IP
パブリック	Siebel SIA 機密オブジェクト	グループ・タイプはオブジェクト
パブリック	SPECIAL CASE ソース・プログラム	グループ・タイプはソース・プログラム
パブリック	疑わしいオブジェクト	グループ・タイプはオブジェクト
パブリック	疑わしいユーザー	グループ・タイプはユーザー
パブリック	システム構成コマンド	データベース構成コマンド (管理コマンドのサブセット) 例: ALTER DATABASE、ALTER SYSTEM
パブリック	システム構成プロシージャー	システム構成オブジェクト (「管理オブジェクト」のサブセット)
パブリック	無効なデータベース・ユーザー	グループ・タイプはユーザー
パブリック	脆弱なオブジェクト (ワイルドカード使用)	脆弱性が報告されているデータベース・オブジェクト
パブリック	Windows ファイル共有コマンド	グループ・タイプはコマンド
パブリック	Db2 デフォルト・ユーザー IBM iSeries デフォルト・ユーザー Informix デフォルト・ユーザー MS-SQL Server デフォルト・ユーザー MYSQL デフォルト・ユーザー Netezza デフォルト・ユーザー Oracle デフォルト・ユーザー PostgreSQL デフォルト・ユーザー Sybase デフォルト・ユーザー Teradata デフォルト・ユーザー	グループ・タイプはデータベース・ユーザー/データベース・パスワード
パブリック	Hadoop スキップ・コマンド Hadoop スキップ・オブジェクト Hadoop 以外のサーバー	グループ・タイプはコマンド グループ・タイプはオブジェクト グループ・タイプはサーバー IP
パブリック	リプレイ - 比較対象から除外する リプレイ - 比較対象に含める	グループ・タイプはオブジェクト
監査プロセス・ビルダー		これは、空として事前定義されています。

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
ベースライン・ビルダー		これは、空として事前定義されています。 重要: 「ベースライン・ビルダー」と関連機能は、Guardium V10.1.4 から非推奨になりました。
Classifier		これは、空として事前定義されています。
エクスプレス・セキュリティー		これは、空として事前定義されています。

親トピック: グループ

セキュリティー・ロール

セキュリティー・ロールは、データ (グループ、照会、レポートなど) へのアクセスを 許可したり、アプリケーション (「グループ・ビルダー」、「レポート・ビルダー」、「ポリシー・ビルダー」、 「CAS」、「セキュリティー・アセスメント」など) へのアクセスを許可するために使用します。

デフォルトでは、 コンポーネントが最初に定義されるときに、owner (定義を行った人) と admin ユーザー (特別な特権を持つ) がそのコンポーネントへのアクセスおよび変更を 許可されます。

セキュリティー・ロールを割り当てることによって、定義したコンポーネントに他のユーザーが アクセスできるようにすることができます。例えば、DBA という名前のセキュリティー・ロールを 監査プロセスに割り当てると、DBA ロールに割り当てられたすべてのユーザーが、その監査プロセスにアクセスできます。

注: LDAP ユーザー・インポートを構成する accessmgr ユーザーには、グループ・ビルダーの実行特権が必要です。 特定の状態において、ロール特権に変更が加えられた場合、accessmgr のグループ・ビルダーに対する特権が取り消される可能性があります。 その結果、LDAP ユーザー・インポートを正常に保存することも実行することもできなくなります。 アクセス管理ポータルに移動して、「ロール権限」を選択してください。グループ・ビルダー・アプリケーションを選択し、「すべてのロール」ボックスまたは「accessmgr」ボックスにチェック・マークが付けられていることを確認します。

セキュリティー・ロールの割り当て

1. 1 つ以上のセキュリティー・ロール (ポリシー定義またはレポート定義など) を割り当てる項目を開くか、選択します。
2. 「ロール」をクリックします。
3. 「セキュリティー・ロールの割り当て」リストから、割り当てるすべてのロールにチェック・マークを付けます。自分のアカウントに割り当てられているロールのみを割り当てることができます。
4. 「適用」をクリックします。

新規セキュリティー・ロールの定義

デフォルトでは、特別な accessmgr ユーザー のみが、セキュリティー・ロールの作成または削除を許可されています。

1. accessmgr としてログインし、「アクセス」 > 「アクセス管理」 > 「ユーザー・ロール・ブラウザー」をクリックして、「ユーザー・ロール・ブラウザー」を開きます。
2. ロール・ブラウザーの最後にある「ロールの追加」をクリックします。
3. 「ロール・フォーム」パネルで、新しい「ロール名」を入力して、「ロールの追加」をクリックします。

セキュリティー・ロールの削除

デフォルトでは、特別な accessmgr ユーザー のみが、セキュリティー・ロールの作成または削除を許可されています。コンポーネントに割り当てられたロールを削除するには、コンポーネントへのセキュリティー・ロールの割り当てを参照してください。

1. accessmgr としてログインし、「アクセス」 > 「アクセス管理」 > 「ユーザー・ロール・ブラウザー」をクリックして、「ユーザー・ロール・ブラウザー」を開きます。
2. ロールの「削除」をクリックしてから、「削除の確認」をクリックします。

親トピック: Guardium システムの管理

通知

通知を作成するには、「アラート機能」および「アラート・ビルダー」を使用します。アラート・アクションに E メールまたはその他の通知が必要な場合は、以下の手順に従って、各タイプの通知について定義してください。

アラート機能の構成

1. アラート・アクションを選択する前に、「アラート機能」で E メールの SMTP 設定を構成する必要があります。
2. 「保護」 > 「データベースの侵入検出」 > 「アラート機能」をクリックして、「アラート機能」を開きます。
3. SMTP または SNMP (あるいは両方) の情報を入力します。
4. 各セクションに入力した後、「接続のテスト」をクリックして、接続が機能していることを確認します。接続が機能していない場合は、接続が到達不能であるというメッセージを受け取ります。
5. 「適用」をクリックして、構成を保存します。
6. 最低でも IP アドレス/ホスト名、ポート、および送信先 E メールアドレスを指定しなければなりません。
7. 「通知タイプ」メニューから「*メール*」を選択します。メッセージの重大度が「*高*」の場合、緊急フラグが設定されます。
8. 「アラート受信者」リストからユーザー (個人またはグループ) を選択します。リアルタイム E メール通知の追加の受信者は、「起動者」(ポリシー起動の原因となった実際の SQL コマンドを開始したユーザー) と「所有者」(データベースの所有者) です。起動者と所有者は、Guardium® API を使用して構成されたユーザー ID (IP ベース) を取得することによって識別されます。
9. 「追加」をクリックします。

アラートの作成

1. 「アラート機能」を構成した後、「保護」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックして、「アラート・ビルダー」を開きます。
2. 「設定」、「アラート定義」、「アラートしきい値」、および「通知」の各セクションに情報を入力して、「適用」をクリックします。
3. 「受信者の追加..」をクリックしてユーザーを選択することで、通知を受け取るユーザーを選択します。

親トピック: Guardium システムの管理

リアルタイム・アラートの作成方法

同じユーザーによるログインの失敗が 5 分以内で 3 回を超えた場合に、 データベース管理者にリアルタイム・アラートを送ります。

このタスクについて

疑わしいアクティビティーが検出された場合や、アクセス・ポリシーに違反があった場合に、リアルタイムのセキュリティー・アラートを生成します。

以下の手順を行います。

1. ポリシーの作成
2. ポリシーへのルールの追加
3. ポリシーのインストール
4. ポリシー起動時のリアルタイム・アラートのセットアップ

前提条件

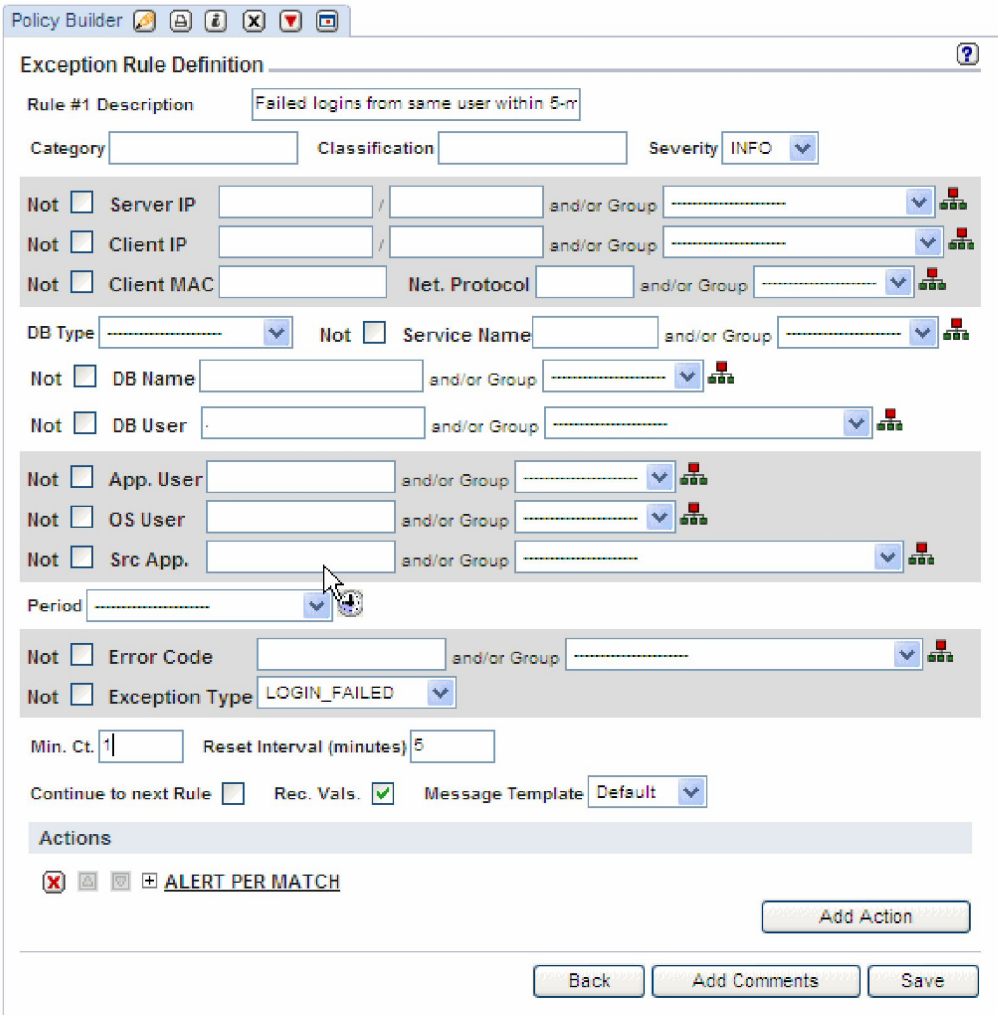
「アラート機能」での SMTP の構成。 「保護」 > 「データベースの侵入検出」 > 「アラート機能」をクリックして、「アラート機能」を開いて、SMTP 情報を入力します。

注: ポリシー違反は、インシデント管理でレポートとして表示することも可能です。詳しくは、『ポリシー』を参照してください。

手順

1. ポリシーを作成します。
   a. 「設定」 > 「ツールとビュー」 > 「データまたはアプリケーションのポリシー・ビルダー」をクリックして「ポリシー・ビルダー」を開きます。
   b. 「新規」をクリックするか、「ポリシー・ファインダー」でポリシーを選択して「変更」をクリックすることで、既存のポリシーを変更します。
   c. 必須情報を入力して、「適用」をクリックし、ポリシーを保存します。
2. ポリシーにルールを追加します。
   a. ポリシーを保存したら、「ルールの編集」をクリックして既存のポリシー・ルールを表示します。
   b. 「ルールの追加...」をクリックすると、5 つのルール・オプションが表示されます。
   c. 「例外ルールの追加」を選択して必須情報を入力します。

      「例外ルール定義」画面には、最初に以下の項目が表示されます:



- 記述 - ルールの簡潔な記述名を入力します。
- カテゴリー - カテゴリーは違反とともにログに記録され、グループ化およびレポート目的で使用されます。何も入力しないと、ポリシーのデフォルトが使用されます。
- 分類 - (オプション) 「分類」ボックスに分類を入力します。カテゴリー同様、これらは例外とともにログに記録され、グループ化およびレポート目的で使用されます。
- 重大度 - メニューから重大度コード (「情報」、「低」、「なし」、「中」、または「高」) を選択します (デフォルトは「情報」です)。

d. 他のフィールドを使用してルールの突き合わせ方法 (検索する場所、検索対象、検索対象ユーザー、検索するタイミング) を指定します。
e. 個々の値を別々にカウントするには、「データベース・ユーザー」フィールドにピリオド「.」を入力します。
f. 「例外タイプ (Excpt. Type)」 (例外タイプ) メニューから、「LOGIN_FAILED」を選択します。
g. 「最小数」を使用して、ルールが何回一致したらアクションを起動するかの最小回数を設定します。この例では 1 を選択します。 ルールが成立した回数は、アクションが起動されるごとに、またはリセット間隔が満了になるとリセットされます。
h. 「リセット間隔」を使用して、ルール・カウンターをゼロにリセットするまでの時間を分数で設定します。カウンターはまた、ルール・アクションが起動するごとにゼロにリセットされます。この例では、「5」を選択してください。
i. 「次のルールに進む」チェック・ボックスにチェック・マークを付け、このルールが成立してルールのアクションが起動された後にルールのテストを続行するようにします。これが選択されていない場合は、このルールが成立した際に、追加のルールはテストされません。
j. 「値を記録」チェック・ボックスにチェック・マークを付けると、ルールのアクションが起動されたときに、そのイベントの原因となる SQL ステートメント全体がログに記録され、ポリシー違反レポートで参照できるようになることを意味します。マークを付けない場合、SQL 文字列属性は空になります。

3. ルールが起動したときのアクションを追加します。
   a. 「例外ルール定義」画面のアクション・セクションから、「アクションの追加」をクリックします。
   b. 「アクション」メニューからオプションを選択して、「適用」をクリックします。この例では、*ALERT PER MATCH* が選択され、ルールが起動するたびに通知を受け取るようにしています。
   c. 「通知タイプ」メニューからオプションを選択します。 メール通知タイプまたは SNMP 通知タイプの「アラート機能」を構成する必要があります。
   d. アラート受信者を追加し、「適用」をクリックしてアクションを保存します。
4. ポリシーをインストールします。
   a. 「設定」 > 「ツールとビュー」 > 「ポリシー・インストール」をクリックします。
   b. 「ポリシー・インストーラー」メニューからポリシーを探し、インストール・アクションを選択して、「スケジュールの変更」または「今すぐ 1 回実行」をクリックします。 これで、ポリシーがインストールされました。アラート受信者は、ポリシー・ルールの起動時にリアルタイム通知を受信します。

親トピック: Guardium システムの管理

カスタム・アラート・クラスの管理

カスタムの受信者にアラートを送信するには、カスタム・アラート・クラスを使用します。 カスタム・クラスをアップロードしてから、「アラート・ビルダー」を使用して、アラート通知受信者としてカスタム・クラスを指定します。

- カスタム・クラスを使用するには、事前に Guardium システムにアップロードしておく必要があります。「セットアップ」 > 「カスタム・クラス」 > 「アラート」 > 「アラート・クラスのアップロード」をクリックして、カスタム・アラート・クラスをアップロードします。「参照」をクリックしてファイルを選択し、「適用」をクリックして保存します。
- カスタム・クラスをアップロードした後、「アラート・ビルダー」を使用し、そのカスタム・クラスをアラートで使用します。「管理」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックして、「アラート・ビルダー」を開きます。必須情報を入力して、「通知タイプ」メニューから「*CUSTM*」を選択し、「保存」をクリックします。

親トピック: Guardium システムの管理

事前定義アラート

表で、「アラート・ビルダー」にある事前定義アラートについて説明します。

Guardium は、「アラート・ビルダー」で見つかる一連の事前定義アラートを備えています。「保護」 > 「データベースの侵入検出」 > 「アラート・ビルダー」をクリックして、「アラート・ビルダー」を開きます。「アラート・ビルダー」を開くと、「アラート・ファインダー」にすべての既存のアラートのリストが表示されます。ファインダーからアラートを選択して、「変更」をクリックし、編集します。

「アラートの変更」画面で、受信者やしきい値など、アラートの任意の部分を変更します。

アラートの基準となっているデフォルトの照会は変更できません。照会を変更する場合、照会の「この照会を編集」アイコン をクリックして、「クエリー・ビルダー」を開きます。ビルダーで照会のコピーを作成した後、ニーズに合わせてこれを変更します。

アラートに変更を加えた後、「適用」をクリックして保存します。

次の表に、すべての事前定義アラートを示します。

表 1. 事前定義アラート

アラート	記述
変更されたアクティブ S-TAP	最後の集計間隔中にアクティブ S-TAP® 検査エンジンに加えられた変更をチェックします。 この期間中に変更された検査エンジンが少なくとも 1 つあれば、このアラートが起動します。 デフォルトでは、このアラートは 30 分ごとに最後の 1 時間をチェックします。
統合エラーまたはアーカイブ・エラー	正常に完了しなかったすべての統合タスクまたはアーカイブ・タスクについて、1 日に一度アラートを出します。
接続プロファイル・アラート	アラートは 60 分間隔で実行され、通知が事前定義グループ (許可された接続の接続プロファイル・リスト - 名前リスト） に送信されます。
CAS インスタンス構成変更	CAS インスタンス構成変更で 1 日に一度アラートを出します。
CAS テンプレート変更	CAS テンプレート構成変更で 1 日に一度アラートを出します。
データ・ソース変更	データ・ソース定義の変更で 1 日に一度アラートを出します。
データベースのディスク・スペース	内部データベースの満杯率が 80% を超えた場合に、10 分ごとにアラートを出します。ディスク・スペース (満杯率) と Guardium® Nanny プロセスの詳細については、『自己モニター』ヘルプ・トピックを参照してください。
エンタープライズの「トラフィックなし」	エンタープライズの「トラフィックなし」アラートは、 中央マネージャー・システムでのみ実行されます。これは、「トラフィックなし」アラートでの照会と同様の照会を基にして、タイム・スタンプが X と Y の間にあるレコードを検索します。この場合、X は照会パラメーター、Y は集計間隔を基にしたアラート・メカニズムが生成する日付からの照会です (既存の「トラフィックなし」アラートの場合と同じ方法)。
変更されたエンタープライズ S-TAP	このアラートは、中央マネージャー・システムでのみ実行されます。
Guardium への失敗したログイン	Guardium アプライアンスへのログイン試行の失敗が 5 回を超えた場合、10 分ごとにアラートを出します。
Guardium - ユーザーの追加/削除	Guardium ユーザーが追加または削除された場合、 1 日に一度アラートを出します。
Guardium - 資格情報アクティビティー	Guardium 資格情報が変更された場合 (LDAP 構成の変更など)、1 日に一度アラートを出します。
非アクティブ管理対象ユニット	アラートは、30 分間隔で実行され、通知は 1 日に 1 回、「管理対象ユニット・アラート」という事前定義グループに送信されます。
非アクティブな S-TAP	非アクティブなすべての S-TAP について、 1 時間に一度アラートを出します。
検査エンジンと S-TAP	検査エンジンと S-TAP 構成に関連したアクティビティーについて、1 日に一度アラートを出します。
トラフィックなし	特定のデータベース・サーバーからのトラフィックがないかどうかを示すアラート。 このアラートは、Guardium システムのトラフィック収集元であるサーバーから、過去 48 時間のいずれかの時点で収集されるトラフィックがない場合にアラートを出します。 このアラートは、集計間隔に定義されている期間内にトラフィックがない場合に起動します。 例えば、集計間隔が 60 分だとすると、特定のデータベース・サーバーから過去 1 時間内にはトラフィックがなかったが、48 時間以内には何らかのトラフィックがあったという場合に、このアラートは E メールを送信します。 このアラートは、(デフォルトでは) 24 時間ごとにしか E メールを送信しません。集計間隔、通知インターバル、実行頻度などのパラメーターは、カスタマイズできます。 しきい値、「行当たり」、演算子、照会などのパラメーターは変更しないでください。これらのパラメーターを変更すると、アラートが正常に機能しなくなります。「トラフィックなし」照会のコピーを作成しないようにご注意ください。

アラート	記述
サーバー/プロトコルによるトラフィックなし	通常の「トラフィックなし」アラートと似ていますが、以下の点が異なります。 このアラートはサービス名/ネット・プロトコルごとに出され、行ごとに報告されます。 新しい追加パラメーター「アクティブ・トラフィック・インターバル」により、各サーバーからの最後の要求をいつ受信したかがわかります。 このアラートは、以下の条件で起動します。各サーバー/ネット・プロトコルからのアラート間隔中にはトラフィックがなかったが、その組み合わせのアクティブ・トラフィック・インターバル以降にトラフィックがあった場合。 アラート間隔中にはトラフィックがなかったが、その直前の 48 時間以内にサーバー IP 当たりのトラフィックがあった場合に起動する通常の「トラフィックなし」アラートとは違います。
ポリシー変更アラート	セキュリティー・ポリシーの変更があった場合に、 1 日に一度アラートを出します。
長時間実行の照会	照会の実行が 900 秒を超える場合に通知します。
スケジュールされたジョブの例外	スケジュールされたジョブの例外 (アセスメント・ジョブを含む) で、10 分ごとにアラートを出します。

親トピック: Guardium システムの管理

スケジューリング

汎用スケジューラーは、さまざまなタイプのタスク (アーカイブ、統合、 ワークフロー・オートメーションなど) をスケジュールに入れるために使用します。

実行中の タスクのタイプにより、ここで説明するすべての機能が使用可能であるとは限りません。 例えば、タスク・タイプのスケジュールは一時停止できるものと、 できないものがあります (停止または開始のみ可能)。

注: 夏時間の期間中にタスクをスケジュールに入れると、スケジュール異常が発生する可能性がある ことに注意してください。

スケジュールの定義または変更

1. タスク (「監査プロセス・ビルダー」など) で、「スケジュールの定義」または「スケジュールの変更」をクリックして、「スケジュール定義」パネルを開きます。
2. 「開始時刻 」に入力します。デフォルトは 12 a.m. (午前零時) です。
3. オプションで、タスクを 1 日に複数回実行するには、以下のようにします。
   - 「再始動」リストから値を 選択します (毎時から最大 12 時間ごと)。デフォルトは「1 回だけ実行 」で、タスクが同じ日に再始動されないことを意味します。
   - 「繰り返し」リストから値を 選択します (毎分から最大 59 分ごと)。デフォルトは「繰り返しなし」です。
4. 「スケジュールの基準 」リストから、以下のいずれかを選択します。
   - 「曜日」 1 つ以上の曜日 (月曜日、火曜日、水曜日など) に基づくスケジュールを 定義します。
   - 「月」 毎月または特定の月で、その月の 1 日以上の日に基づいてスケジュールを 定義します。

   「スケジュールの基準」リストから 「曜日」を選択した場合、タスクを実行する各曜日に マークを付けるか、「毎日」をクリックしてすべての日を選択します (既にすべての日が選択されている場合は、 すべてクリアされます)。

   または

   「スケジュールの基準」リストから 「月」を選択した場合、以下のいずれかを実行します。

   - 日付 (例えば 15 日) を選択するには、次のようにします。
     - 「日」ボタンを選択します。
     - 選択した月に応じて、日付を 1 から 31 から 選択します。
     - 「毎月 」、または 1 つ以上の特定の月を選択します。
   - その月内の曜日オカレンス (例えば、第 1 月曜日) を選択するには、 次のようにします。
     - ボタンを選択します。
     - 月初めからの相対的な週 (第 1、第 2、第 3 など) を 選択します。
     - 曜日 (日曜日、 月曜日、火曜日など) を 選択します。
     - 「毎月」または 1 つ以上の特定の月を選択します。
5. 「開始時刻のスケジュール設定 」リストから、タスクを実行する時分を選択します。 NOW より前の時刻が選択されている場合、スケジューラーの開始時刻は NOW に戻ります。
6. 「適用」をクリックします。

スケジュールの一時停止

注: スケジュールに入れられたすべてのタイプのタスクが一時停止オプションを提供するわけではない、ということに注意してください。

1. 「一時停止」をクリックします。
2. アクションを確認します。

スケジュールの削除

スケジュールの定義が完了した後、「スケジュール定義」パネルに 「削除」ボタンが表示されます。

1. 「スケジュールの定義」または「スケジュールの変更」をクリックして、「スケジュール定義」パネルを開きます。
2. 「削除」ボタンをクリックします。

親トピック: Guardium システムの管理

別名

レポートまたは照会で使用されるデータ値またはデータ・オブジェクトのシノニムを作成します。

別名の概要

別名は、データ値を意味のある、または分かりやすい名前で表示するために使用されます。

例えば、IP アドレス 192.168.2.18 の別名として、「*財務サーバー*」を定義することができます。別名を定義すると、ユーザーはデータ値の代わりに別名を使用してレポート結果を表示し、 照会を形成し、パラメーター値を入力することができるようになります。

別名を定義する方法は、何とおりかあります。

- 「IP からホスト名への別名割り当て」ツール - 検出されたクライアント IP とサーバー IP に対して別名を生成するには、このツールを使用します。

  「保護」 > 「データベースの侵入検出」 > 「IP からホスト名への別名割り当て」をクリックして、「IP からホスト名への別名割り当て」ツールを開きます。

- 「別名ビルダー」 – 別名を手動で定義する場合、この方法を使用します。

  「順守」 > 「ツールとビュー」 > 「別名ビルダー」をクリックして、「別名ビルダー」を開きます。

- 照会
- 「別名クイック定義」 (「グループ・ビルダー」使用時)
-

注: 中央マネージャーまたは管理対象ユニットでの別名変更を他のシステム・ユニットで有効にするには、 GUI を再起動するか、そのシステム・ユニットの GUI を使用して別名変更を行う必要があります。

IP からホスト名への別名割り当て

別名の一般的な応用方法の 1 つは、IP アドレスのシノニムとして使用することです。 このツールを使用して、クライアント IP とサーバー IP のディスカバリーのスケジュールを設定し、それらの別名を生成します。

1. 「保護」 > 「データベースの侵入検出」 > 「IP からホスト名への別名割り当て」をクリックして、「IP からホスト名への別名割り当て」ツールを開きます。
2. 「クライアント IP とサーバー IP のホスト名別名の生成 (使用可能な場合)」チェック・ボックスにチェック・マークを付けます。
3. ツールがホスト名別名を継続的に探して更新するようにする場合は、「既存のホスト名別名の更新 (再発見された場合)」チェック・ボックスにチェック・マークを付けます。
4.
5. 「適用」をクリックして構成を保存した後、操作のスケジュールを設定します。
   - 「今すぐ 1 回実行」をクリックすると、ツールが直ちに開始されます。
   - 今後のツールのスケジュールを設定するには、「スケジュールの定義...」をクリックします。
   - クライアント IP とサーバー IP の別名の生成を一時停止するには、「一時停止」をクリックします。

別名ビルダー

別名を手動で作成するには、この方法を使用します。

1. 「設定」 > 「ツールとビュー」 > 「別名ビルダー」をクリックして、「別名ビルダー」を開きます。
2. 別名を定義する属性タイプを選択します。
3. 「値」フィールドと「別名」フィールドを使用して、その属性タイプで検索をフィルタリングし、「検索」をクリックします。
4. いずれかの結果が検索と一致すると、値と別名の表に表示されます。検索結果の「適用」をクリックするか、「値」および「別名」の名前を指定してから「追加」をクリックして新規別名を追加します。
5. 「項目のコメント」アイコン をクリックして、別名にコメントを追加します。これは、将来、別名の参照先を素早く見つける上で役立ちます。

照会を使用した別名定義

このメソッドは、照会から別名を作成する場合に使用します。カスタム表が Guardium® にアップロードされると、その表を使用して別名を特定の値にマップすることができます。

1. 「設定」 > 「ツールとビュー」 > 「別名ビルダー」をクリックして、「別名ビルダー」を開きます。
2. 別名を定義する属性タイプを「別名ファインダー」から選択して、「照会から取り込み」をクリックして、「照会からの別名ビルダーの設定」パネルを開きます。
3. 必須情報を入力して、「保存」をクリックし、別名を保存します。
   - 「照会」メニューから、実行する照会を選択します。
   - 「値の列の選択」と「別名の列の選択」の両方の値を選択します。
   - 列の値を選択した後、その他のフィールド (「開始日付」、「終了日付」、「リモート・ソース」、および選択した照会に関する追加のパラメーター) が表示され、これらのフィールドに入力する必要があります。
   - 照会から取り込む前にグループの既存の内容を削除するには、「インポートする前に既存のグループ・メンバーをクリアする」チェック・ボックスにチェック・マークを付けます。
   - 「保存」をクリックして、保存します。
   - 照会が保存されると、「スケジューリング」ボタンがアクティブになります。「スケジュールの変更」をクリックして照会を将来に実行することも、「今すぐ 1 回実行」をクリックして照会をすぐに実行することもできます。

グループ・ビルダーからの別名クイック定義

グループの作成時または取り込み時にすぐにグループの別名を作成するには、この方法を使用します。

1. 「設定」 > 「グループ・ビルダー」をクリックして、「グループ・ビルダー」を開きます。リストから任意のグループを選択して、「変更」をクリックします。
2. 「別名...」をクリックして、「別名クイック定義」ウィンドウを開きます。グループ (複数可) の別名を入力して、「適用」をクリックし、別名を保存します。

別名用の GuardAPI

これらの GuardAPI コマンドは、別名機能の作成、更新および削除に使用します。

- grdapi create_alias
- grdapi update_alias
- grdapi delete_alias

親トピック: Guardium システムの管理
関連情報:
高度な Guardium システム管理および構成 (ビデオ)

日付とタイム・スタンプ

カレンダー・ツールを使用して絶対日付を選択し、相対日付ピッカーを使用して現在時刻からの相対的な日付を選択します。

日付フィールドにデータを追加するために使用する 2 つのツールがあります。1 つは絶対日付を選択するためのカレンダー・ツール、もう 1 つは現在時刻からの相対的な日付 (例えば、now -1 day) を選択する相対日付ピッカーです。さらに、絶対日付または相対日付を手動で入力することもできます。

日付を選択または入力する際には、ブラウザーを実行しているシステム上の日付が、接続先の Guardium® アプライアンス上の日付とは異なる場合があることに注意してください。

照会内のタイム・スタンプ

タイム・スタンプを照会に含める場合は、注意が必要です。

まず、timestamp (小文字の「t」) および Timestamp (大文字の「T」) の区別に注意してください。

- timestamp (小文字の t) は、結合された日付と時刻の値を含んでいるデータ・タイプであり、印刷時には yyyy-mm-dd hh:mm:ss のフォーマットで示されます (例: 2005-07-17 15:40:25)。照会の作成または編集時に、timestamp データ・タイプのほとんどの属性は、時計アイコン付きで「エンティティー・リスト」パネルに表示されます。
- Timestamp (大文字の T) は多くのエンティティー・タイプに定義される属性です。これには通常、そのエンティティーの最終更新時刻が含まれます。

Timestamp 属性値を照会に含めると、Timestamp 値ごとに行が作成されます。これにより、過剰な出力が行われる場合があります。この問題を回避するには、照会に Timestamp を含める際に count アグリゲーターを使用し、レポート行にドリルダウンを行い、その行のみに含まれる項目の個別の Timestamp 値をドリルダウン・レポートに表示します。「照会」の『フィールドの統合』を参照してください。

複数のエンティティーの Timestamp 属性を含む照会で Timestamp 値を表示する場合は、そのレポートに適切なエンティティー・タイプの Timestamp 属性を選択するよう注意してください。例えば、「セッション」をメイン・エンティティーに選択して、照会で「クライアント/サーバー」エンティティーおよび「セッション」エンティティーの両方の情報を表示する場合は、1 つまたは両方のエンティティーの Timestamp 属性を表示できます。「クライアント/サーバー」の Timestamp を含める場合は、特定のクライアント/サーバー接続のすべてのセッションで同じ値が出力されます。この値は常に、特定のクライアント/サーバーが最後に更新された時刻です。セッションの Timestamp 属性を含めると、リストされている各セッションが最後に更新された時刻が表示されます。

ヒント: レポートに異なる時刻が表示されると予期される場合に、すべて同じ時刻が表示されるときには、エンティティー階層内での位置が、レポートに必要な詳細レベルに対して高すぎるエンティティーの Timestamp 属性が含まれている可能性があります。

カレンダーから絶対日付を選択する

カレンダー・ウィンドウを使用して絶対日付を選択するには、次のようにします。

1. 日付を挿入するフィールドの「カレンダー」ボタンをクリックします。これにより、別のウィンドウにカレンダーが開きます。
   - 矢印ボタンをクリックすると、カレンダー・ウィンドウに前月または翌月が表示されます。
2. 日付をクリックして選択します。カレンダー・ウィンドウが閉じ、クリックしたカレンダー・ツールの隣にある「日付」フィールドに選択した日付が挿入されます。
   注: カレンダーを使用して選択した日付のデフォルトの時刻は常に 00:00:00 (その日の始め) です。他の時刻を指定するには、24 時間フォーマット (hh:mm:ss) で希望の時刻を入力し、この値を上書きします。ここで hh は時間 (0-23)、mm および ss はそれぞれ分および秒 (いずれも 0-59) です。

絶対日付を手動で入力する

1. 日付を入力するフィールドをクリックし、yyyy-mm-dd フォーマットで日付を入力します。
   - yyyy はオプションであり、任意の正整数値を使用できます。省略した場合、yyyy にはデフォルトで現在の年が使用されます。1 桁または 2 桁の年が入力された場合、日付の世紀の部分にはデフォルトで 19 が使用されます。
   - mm は、月 (1-12) です。
   - dd は、その月の日 (月に応じて 1 から 28、29、30、または 31) です。
2. 時刻が入力されない場合、時刻にはデフォルトの 00:00:00 (その日の始め) が使用されます。他の時刻を指定するには、24 時間フォーマット (hh:mm:ss) で希望の時刻を入力し、この値を上書きします。ここで hh は時間 (0-23)、mm および ss はそれぞれ分および秒 (いずれも 0-59) です。

日付ピッカーから相対日付を選択する

絶対日付を指定するよりも、現在の日付 (now) やその他の日付 (例えば、first Monday) のいずれかに対する相対日付を指定するほうが便利であることがよくあります。例えば、常に過去 7 日間の情報を照会に含める場合は、相対日付 (例えば、start = now minus seven days および end = now) を定義する方が便利です。「相対日付ピッカー」ツールを使用して、多くのタイプのタスクで相対日付を選択できます。

1. 相対日付が使用可能なフィールドの横にある「相対日付ピッカー」ボタンをクリックします。これにより、「相対日付ピッカー」ウィンドウが開きます。
2. リストから「Now」、「Start」、または「End」を選択します。選択内容にかかわらず、表示が変更され、さらに選択項目が表示されます。
3. 中央のリストから、「this」、「last」、または「previous」を選択します。これは、特定の単位 (次のリストで選択される「日」、「週」、「月」、または「曜日」) に対する相対的なものです。
   - 「This」は、現在の単位です。
   - 「Last」は、現在の単位から 1 を引いたものです。
   - 「Previous」は、現在の単位から 2 を引いたものです。
4. 「日」、「週」、「月」、または特定の曜日 (月曜日から金曜日) を選択します。

5. 完了したら、「OK」ボタンをクリックします。クリックした「相対日付ピッカー」ボタンの隣にあるフィールドに、相対日付が挿入されます。
6.

相対日付を手動で入力する

相対日付を手動で入力するには、いずれかのステップに従います。キーワードには大/小文字の区別はありませんが、各コンポーネントを 1 つ以上のスペースで区切る必要があります。

相対日付を入力する際に使用できる一般的なフォーマットには、以下の 3 つがあります。

NOW に続けて指定した負の数と、minute、hour、day、week、month

または

Start of または End of に続けて、this、last、または previous と day、week、または month

または

Last または Previous に続けて曜日 (Sunday、Monday、Tuesday など)

NOW に対する相対日付

1. 相対日付を入力するフィールド内をクリックします。
2. キーワード「NOW」を入力します。
3. 相対的な時間数、日数、週数、または月数を指定する負の整数を入力します (負符号 (-) と整数の間にスペースを入れることはできません)。
4. 使用する単位のキーワード (HOUR、DAY、WEEK、または MONTH) を入力します。複数形 (hours、days など) は使用できないことに注意してください。例: now -14 day

日、週、または月に対する相対日付

1. 相対日付を入力するフィールド内をクリックします。
2. キーワード「START OF」または「END OF」を入力します。
3. 「THIS」、「LAST」または「PREVIOUS」に続けて、「DAY」、「WEEK」、または「MONTH」を入力します。例: end of last week

曜日に対する相対日付

1. 相対日付を入力するフィールド内をクリックします。
2. キーワード「START OF」または「END OF」を入力します。
3. 「LAST」または「PREVIOUS」に続けて、「SUNDAY」、「MONDAY」、「TUESDAY」、「WEDNESDAY」、「THURSDAY」、「FRIDAY」、または「SATURDAY」を入力します。例: start of previous Tuesday

親トピック: Guardium システムの管理

期間

ポリシー・ルールや照会条件に使用できる期間を作成するには、「期間ビルダー」を使用します。

データベースのアクティビティーをモニターするときは、期間を使用して、モニターを行う時期を指定します。新規期間の作成や既存の期間の変更は、「期間ビルダー」を使用して行います。

期間の追加

1. 「設定」 > 「ツールとビュー」 > 「期間ビルダー」をクリックして、「期間ビルダー」にナビゲートします。
2. 「+」ボタンをクリックして、「期間の追加」ペインを展開します。
3. 情報を入力し、「追加」をクリックして、期間を追加します。
   - 「期間の説明」には、アポストロフィ文字を使用しないでください。
   - 「連続」チェック・ボックスにチェック・マークを付けて、複数の日にまたがる単一の期間を定義します。出勤週は連続として定義されていますが、出勤日は不連続として定義されています。

期間の削除

1. 「設定」 > 「ツールとビュー」 > 「期間ビルダー」をクリックして、「期間ビルダー」にナビゲートします。
2. 削除する期間のチェック・ボックスにチェック・マークを付けて、「削除」をクリックします。

親トピック: Guardium システムの管理

期間

ポリシー・ルールおよび照会条件によって、ユーザー定義の期間内にイベントが発生したかどうかをテストできます。

事前定義の期間のセット (7x24、残業、早出、夜間、出勤日、土曜日、日曜日、週末) が用意されており、ユーザーが独自の期間を定義することもできます。

期間の追加

1. 「期間」パネルにナビゲートします。
   - 「セットアップ」>「ツールとビュー」>「期間ビルダー」

2. 「+」ボタンをクリックして、「期間の追加」ペインを展開します。
3. 「期間の説明」ボックスに、期間に固有の説明を入力します。記述にはアポストロフィ文字を含めないでください。
4. オプションで、「連続」ボックスにマークを付けて複数の日にまたがる単一の期間を定義することもできます。1 日以上の範囲に固定の時間枠を定義する場合はこのボックスをクリアしたままにします。

   例: 連続期間と非連続期間の比較

   以下の 2 つの期間は両方とも月曜日 09:00 に始まり、金曜日 17:00 に終わります。
   - 「出勤週」は連続として定義されています。
   - 「出勤日」は非連続として定義されています。

   1 番目の期間「出勤週」は、月曜日午前 9 時から金曜日午後 5 時までの 164 時間から成る期間を 1 つ定義しています。 一方、2 番目の期間「出勤日」は、 連続した 5 つの日 (月曜日から金曜日まで) に対して 8 時間から成る期間 (午前 9 時から午後 5 時まで) を個別に 5 つ定義しています。

5. 「開始時刻」ボックスに、開始時刻の時 (00 から 24) および分 (00 から 59) を入力します。
6. 「終了時刻」ボックスに、終了時刻の時 (00 から 24) および分 (00 から 59) を入力します。
7. 「開始曜日」ボックスで、開始する曜日を選択します。
8. 「終了曜日」ボックスで、終了する曜日を選択します。
9. オプションで、「コメント」ボタンをクリックしてコメントを追加します (『コメント』を参照)。
10. 「追加」ボタンをクリックします。

期間の削除

1. 「期間」パネルにナビゲートします。
   - 「セットアップ」>「ツールとビュー」>「期間ビルダー」
2. 削除する期間の「選択」チェック・ボックスにマークを付けます。
3. 「削除」ボタンをクリックします。削除の確認を求めるプロンプトが出されます。既存のポリシー・ルールで使用されている期間は削除できないことに注意してください。

親トピック: Guardium システムの管理

コメント

コメントは、定義とワークフロー・プロセス結果に適用されます。

コメントは、UI 全体のいくつかの場所で追加または表示できます。コメントは、参照の目的でグループまたは別名に追加したり、監査要件を軽減するためにレポートに追加したりすることができます。例えば、特定の日付に構成変更が行われた理由を、監査員が確認する場合です。変更を加えた理由を簡単に参照できるように、コメントを使用します。

コメントは定義 (グループ、別名、レポート、ポリシー) およびワークフロー・プロセス結果に適用されます。1 つのコンポーネントに複数のコメントを追加でき、コメントにもコメントを追加できます。ただし、既存のコメントの変更や削除はできません。

以下のとおり、2 つの異なる種類のコメントがあります。

- **「コメント」エンティティー** - 中央マネージャー上に保管されます。その一元管理環境内で使用可能であり、ロールとアクセス権について通常の制約が課されます。
- **「ローカル・コメント」エンティティー** - 単一のユニットに対して定義され、そのユニットのローカルでの使用にとどまります。スタンドアロン・ユニットまたは管理対象ユニットのローカル・コメントは、中央マネージャーには保管されません。

コメントの追加または表示

1. コメントを表示するには、「順守」 > 「レポート」 > 「ユーザー・コメント」をクリックして、「ユーザー・コメント」ウィンドウを開きます。
2. UI 全体で、コメントをエンティティーまたはレポートに追加するための各種の方法があります。
   - グループにコメントを追加するには、グループを変更して、「選択したグループのメンバーの管理」画面で「コメントの追加」をクリックします。
   - 別名にコメントを追加するには、「別名ビルダー」を開き、「項目のコメント」アイコン をクリックします。「設定」 > 「ツールとビュー」 > 「別名ビルダー」をクリックして、「別名ビルダー」を開きます。

レポート・コメント

すべてのユーザー・コメントのレポートを表示するには、「順守」 > 「レポート」 > 「ユーザー・コメント」をクリックします。

- 「ローカル・コメント」エンティティーは、中央マネージャー環境でのみ使用されます。ローカル・コメントは、そのコメントが定義されたシステムのローカルでの使用にとどまり、中央マネージャーには保管されません。
- 「コメント」エンティティーには、中央マネージャーに保管されているコメントが入っています。

親トピック: Guardium システムの管理

パッチのインストール方法

1 つのパッチ、または複数のパッチをバックグラウンド・プロセスとしてインストールします。

このタスクについて

このトピックでは、パッチのインストール、状況、および履歴を表示可能にし、制御する方法について説明します。

詳しくは、『一元管理』を参照してください。

この How-to トピックでは、最新の Guardium パッチのインストールに役立つ CLI のコマンドと GUI の選択項目を組み合わせて使用しています。Guardium システムは、パッチのインストール後にリブートする必要があります。

重要: ZIP 形式でダウンロードしたパッチは、アップロードおよびインストールの前に Guardium システム外部で unzip しておく必要があります。データベース構造の変更を伴うパッチについて以下の制約事項に注意してください。

- 負荷の高いレポート、監査プロセス、バックアップ、インポートなどの長期実行プロセスとの競合を避けるために、パッチのインストールは Guardium システムの負荷が低い時間に実行またはスケジュールしてください。
- パッチ・インストールの正確な所要時間は、データベース使用状況、データ分布などの考慮事項によって異なります。
- パッチのインストールはトップダウン方式、つまり最初に中央マネージャーにパッチを適用してから、アグリゲーターに適用し、最後にコレクターに適用してください。

以下の手順では、中央マネージャーとして指定および構成されている Guardium システムからステップを実行します。

1. CLI コマンド store backup profile を使用して、システム・プロファイルをバックアップします。
2. CLI コマンド store system patch install を入力して、ネットワーク・ロケーションから 1 つのパッチ、または複数のパッチを中央マネージャーにインストールします。
3. 「設定」 > 「ツールとビュー」 > 「パッチ配布」をクリックして、パッチを CM から管理対象ユニットに移動します。

手順

システム・プロファイルのバックアップ

1. SSH クライアントを使用して、CLI ユーザーとして IBM Security Guardium 中央マネージャーにログインします。
2. コマンド store backup profile を入力します。
3. 次のダイアログが表示されます。

```
Do you want to setup for automatic recovery? (Y/n)
Enter the patch backup destination host:
Enter the patch backup destination directory:
Enter the patch backup destination user:
Enter the patch backup destination port if you have a special port for SCP operation, or press ENTER to use the default port:
Enter the patch backup destination password:
```

4. パッチのインストールが失敗した場合、パッチを元に戻せなかった場合、および自動復元が失敗した場合 (あるいはこれが無効であった場合)、次の CLI コマンドを使用します。次のコマンドは、pre-patch backup ファイルを取得し、システムでそれを復元します。pre-patch backup ファイルがシステム上に現在ある場合、ファイル名を入力してください。それ以外の場合、pre-patch backup プロファイル情報を使用してファイルを取得します。

```
CLI>show backup profile patch backup flag is 1 patch backup automatic recovery flag is 1 patch backup dest host is
patch backup dest dir is patch backup dest user is patch backup dest port is patch backup dest pass is CLI>restore pre-patch
backup
```

中央マネージャーへのパッチのインストール

注: 圧縮された 1 つのパッチ・ファイルに複数のパッチが含まれることがありますが、一度にインストールできるパッチは 1 つのみです。複数のパッチをインストールするには、インストールする必要があるすべてのパッチをコンマで区切って選択します。CLI は内部的に、リストの各パッチに関する要求を (ユーザーによって指定された順序で) 実行依頼しますが、その際、最初のパッチはユーザーによって指定された要求時間に行われ、後続の各パッチは前のパッチの 3 分後になります。さらに CLI は、指定された (1 つまたは複数の) パッチが既に要求されているかどうか確認し、重複要求を許可しません。

5. 次のコマンドを入力します。

```
store system patch install <type> <date> <time>
```

ここで、`<type>` は `sys`、`ftp`、`scp`、または `cd` で、`<date>` と `<time>` は、YYYY-mm-dd および hh:mm:ss という形式のパッチ・インストール要求の日付と時刻です。日付と時刻を入力しない場合、または「now」を入力した場合、インストール要求時刻は「今すぐ」です。

表 1. パッチ・インストール・タイプの説明およびパラメーター

名前	記述
`sys`	`sys` オプションは、このコマンドを以前使用して Guardium システムにコピーされた圧縮ファイルに含まれる 2 番目 (またはそれ以降) のパッチをインストールする場合に使用します。以前の store system patch 実行により IBM® Guardium® システムに既にコピーされたパッチ・ファイルに含まれる、2 番目 (またはそれ以降) のパッチを適用するには、このオプションを使用します。 /var/log/guard/patches からインストールします。

名前	記述
ftp または scp	ftp および scp オプションは、圧縮されたパッチ・ファイルをネットワーク上のロケーションから Guardium システムにコピーします。ネットワーク上のいずれかの場所にある圧縮パッチ・ファイルからパッチをインストールするには、ftp または scp オプションを使用して、以下に示すプロンプトに応答します。 重要: ZIP 形式でダウンロードしたパッチは、アップロードおよびインストールの前に Guardium システム外部で unzip しておく必要があります。データベース構造の変更を伴うパッチについて以下の制約事項に注意してください。 ○ 負荷の高いレポート、監査プロセス、バックアップ、インポートなどの長期実行プロセスとの競合を避けるために、パッチのインストールは Guardium システムの負荷が低い時間に実行またはスケジュールしてください。 ○ パッチ・インストールの正確な所要時間は、データベース使用状況、データ分布などの考慮事項によって異なります。 ○ パッチのインストールはトップダウン方式、つまり最初に中央マネージャーにパッチを適用してから、アグリゲーターに適用し、最後にコレクターに適用してください。 Please enter the following information for file transfer: Host to import patch from: User on (host name): Full path to the patch, including name (file name may use wildcard *): (LDAP password) Password: Enter the scp/ftp port if you need to use a special port, else just press Enter key to continue: The file transfer process can take a while to complete. Leave the terminal open and do not answer any questions until the transfer is complete. Starting transfer, please wait. The file transfer is complete. The backup profile is not set for saving the backup file when patch installation failed. If you want to save the backup file, please answer NO to the question and run CLI command store backup profile to set up the parameters. Do you want to continue (yes or no)? はい List the files in the patches directory: 1. (name of file) Please choose patches to install (1-1, or multiple numbers separated by ",", or q to quit): 1 Install item 1 Patch has been submitted, and will be installed according to the request time, please check installed patches report or CLI (show system patch installed). Please don't forget to remove your media if necessary.
cd	cd オプションは、DVD ディスクからパッチをインストールするときに使用します。適用済みのパッチの全リストを表示するには、管理者ポータルの Guardium モニター・タブの「インストール済みのパッチ」レポートを参照してください。この同じ「Guardium モニター」タブには、「使用可能なパッチ」レポートもあります。パッチを DVD からインストールするには、このコマンドを実行する前に IBM Guardium DVD-ROM ドライブに DVD を挿入してください。DVD に含まれるパッチのリストが表示されます。

- パッチ・インストール要求を削除するには、CLI コマンド delete scheduled-patch を使用します。
- パッチは、インストール後、中央マネージャーにのみ残ります。スタンドアロンまたは管理対象ユニットのパッチ・ファイルは、インストール後に削除されます。
- 使用可能なパッチを表示するには、以下を使用します: show system patch available
- 既にインストールされているパッチ、およびインストールされるようスケジュールされているパッチを表示するには、以下を使用します。日時とインストール状況が示されます: show system patch installed
- Guardium アプライアンスで稼働する HTTPS ベースのファイル・サーバーを始動するには、fileserver コマンドを使用します。このファシリティーは、ユニットへのパッチのアップロード、またはユニットからのデバッグ情報のダウンロードを容易に実行できるようにすることを目的としています。 このファシリティーは開始のたびに、パッチのアップロード先のディレクトリーに含まれるすべてのファイルを削除します。
  注: ファイル・サーバーがアクセスすることになるファイルを生成する操作は、ファイル・サーバーの開始前に完了する必要があります (ファイルをファイル・サーバーが使用できるようにするため)。
  a. ファイル・サーバーを開始するには、fileserver コマンド fileserver を入力します。
  b. ファイル・サーバーを開始しています。これは https://(ユニットの名前) にあります。
  c. ファイル・サーバーを停止するには ENTER を押してください。
  d. ブラウザー・ウィンドウでファイル・サーバーを開き、以下のいずれかを実行します。
     - パッチをアップロードするには、「Upload a patch」をクリックし、指示に従います。
     - ログ・データをダウンロードするには、まず「Sqlguard logs」をクリックします。次に、目的のファイルに移動してそれを右クリックし、他のファイルの場合と同様にダウンロードします。
  e. 完了した後で CLI セッションに戻り、**Enter** を押してセッションを終了します。

UI を使用した中央マネージャーから管理対象ユニットへのパッチの移動

6. 「設定」 > 「ツールとビュー」 > 「パッチ配布」をクリックします。

   「パッチ配布」ボタンを押すと新しい画面が開き、使用可能なパッチのリストが従属関係とともに表示されます。さらにそこからパッチを選択し、選択したすべてのユニットにインストールできます。使用可能なパッチのリストは、使用可能なパッチのうち、選択したユニットごとに現在インストール済みのパッチを使用可能なパッチの従属関係リストとともに評価されたもので構成されます。 使用可能でもインストール可能ではないパッチ (依存するパッチが欠落している) は、リスト中でグレー化して表示され、選択できなくなっています。 インストールするパッチの選択は単一選択です。一度に 1 つのパッチしかをインストールできません。いったんパッチを選択して「インストール」ボタンを押すと、選択したユニットすべてにパッチをインストールするコマンドが送信されます。このパッチ・インストール処理はバックグラウンドで行われます。

7. 「一元管理」 > 「一元管理」 > 「パッチ配布」にナビゲートします。
8. 「パッチ・インストール状況」をクリックします。「パッチ・インストール状況」画面には、各ユニットに対して、失敗したインストールと不一致が表示されます。不一致とは、1 つのパッチが一部のユニットのみにインストールされているような状況であり、他のユニットでのインストールが失敗したのか、インストールしなかったのかには関係ありません。

タスクの結果

これで、パッチを適用したシステムを使用できるようになりました。ただし、パッチをインストールした後、Guardium システムをリブートする必要があります。

親トピック: Guardium システムの管理
関連情報:
Guardium パッチをダウンロードし、インストールする方法 (ビデオ)

サポート・メンテナンス

サポート・メンテナンス・フィーチャーは、パスワードで保護されており、技術サポートから指示があった場合にのみ使用できます。詳しくは、技術サポートにお問い合わせください。

親トピック: Guardium システムの管理

製品の統合

IBM Guardium を他の製品と統合できます。

- Guardium システムと通信するように BIG-IP アプリケーション・セキュリティー・マネージャー (ASM) を構成する
  (F5 Networks が提供する) Big-IP ASM を Guardium のリアルタイム・データベース・アクティビティー・モニターと併用して、Web アプリケーション層とデータベース・アプリケーション・サーバー層との間の ID 伝搬の問題を解決します。
- Hadoop 統合
  このトピックでは、Guardium で Hadoop データをモニターするための基本概念およびプロセスについて説明します。
- Guardium DAM と PIM の統合
  Privileged Information Management (PIM) の支援により、組織は、共有特権 ID の使用を自動化および追跡でき、さらにそれらの共有特権 ID の使用をモニターできます。
- QRadar と Guardium の統合
  QRadar と Guardium は両方向の情報フローで連係して動作して、Guardium データ保護ポリシーを自動的に更新し、また QRadar からのセキュリティー・インテリジェンス・イベントにほぼリアルタイムで応答することができます。
- OPTIM から Guardium へのインターフェース
  OPTIM から Guardium へのインターフェースは、Protobuf (汎用フィード・エージェント) を使用して Optim アクティビティー・ログを Guardium に送信します。
- リアルタイム・アラートおよび相関分析と SIEM 製品との統合
  データベースのアクティビティー・パターン、構造、およびプロトコルのコンテキスト・ナレッジを、SIEM システムのサード・パーティー・データベースに直接配布します。
- InfoSphere Discovery に機密データを転送する方法
  IBM Security Guardium で識別および分類された機密データ情報を取得し、その情報を InfoSphere® Discovery に転送します。
- CEF マッピング
  ArcSight の CEF 標準は、一連の必須フィールドと、一連のオプション・フィールドを定義しています。
- LEEF マッピング
  QRadar からの Log Event Extended Format (LEEF)

Guardium システムと通信するように BIG-IP アプリケーション・セキュリティー・マネージャー (ASM) を構成する

(F5 Networks が提供する) Big-IP ASM を Guardium のリアルタイム・データベース・アクティビティー・モニターと併用して、Web アプリケーション層とデータベース・アプリケーション・サーバー層との間の ID 伝搬の問題を解決します。

このソリューションでは、BIG-IP ASM と Guardium® システムとの間のワイヤー・フォーマットとして、Google のプロトコル・バッファー (.protobuf) を使用します。

Big-IP ASM と Guardium リアルタイム・データベース・アクティビティー・モニターの間の統合の構成に関する情報は、F5 の Web サイト (http://www.f5.com/pdf/deployment-guides/ibm-guardium-asm-dg.pdf) で提供されています。

親トピック: 製品の統合

Hadoop 統合

このトピックでは、Guardium で Hadoop データをモニターするための基本概念およびプロセスについて説明します。

キャパシティー・プランニング

以下のサイズ決定ガイドラインは、監査対象トラフィックが平均的な量であることを前提としています。監査対象トラフィックの量が多い場合、追加のリソースが必要になることがあります。

- コレクターごとに 10 個の管理ノードまたはサーバー・ノード
- データ・ノードに対して S-TAP が必要な場合 (すべてのコンポーネントに対しては S-TAP が必要ない場合)、コレクターごとに 20 個以上のデータ・ノード
- 物理アプライアンスを使用するとき、場合によりコレクターごとに追加ノード

ノードのプロセッサー・バリュー・ユニット (PVU) によってサイズ決定することもできますが、少ない量のトラフィックを監査する場合、この方法ではサイズが大きくなりすぎることがあります。キャパシティー・サイズ決定ガイドラインは、コレクターごとに 4000 PVU です。

統合のシナリオ

Cloudera で SSL 暗号化を使用する場合、Cloudera Navigator を使用した Hadoop 統合を参照してください。

Hortonworks Hadoop クラスターで SSL 暗号化を使用する場合、Hortonworks および Apache Ranger を使用した Hadoop 統合を参照してください。
注: Hive を使用した戻りデータの編集はサポートされていません。Hive を使用したデータ編集が必要な場合、標準 Guardium S-TAP を使用した Hadoop 統合を参照してください。

Hadoop クラスターで SSL 暗号化が必要ない場合、標準 Guardium S-TAP を使用した Hadoop 統合を参照してください。

- 標準 Guardium S-TAP を使用した Hadoop 統合
  HDFS および MapReduce モニターのために標準 Guardium S-TAP を使用して Hadoop を統合する方法について説明します。
- Cloudera Navigator を使用した Hadoop 統合
  Cloudera のネイティブ・データ・ガバナンス・ソリューションである Cloudera Navigator を使用して Haddop を統合する方法について説明します。
- Hortonworks および Apache Ranger を使用した Hadoop 統合
  Hortonworks Data Platform に含まれる Apache Ranger を使用すると、ポリシーにより、Hive、HBASE、HDFS などの Hadoop コンポーネントに対して詳細なアクセス制御および監査を実行できます。

親トピック: 製品の統合
関連情報:
Hadoop 用の S-TAP 構成パラメーター

標準 Guardium S-TAP を使用した Hadoop 統合

HDFS および MapReduce モニターのために標準 Guardium S-TAP を使用して Hadoop を統合する方法について説明します。

Hadoop デプロイメントには、以下の 2 つの基本コンポーネントが含まれます。

- Hadoop 分散ファイル・システム (HDFS)。これにはデータが保管されます。
- MapReduce または MapReduce 2。これらは、データにアクセスし、分析するためのフレームワークを提供します。

管理コンソール・トラフィックを除くすべてのデータが HDFS を経由するため、これらの 2 つのコンポーネントでのキャプチャー・アクティビティーでは、基本監査要件が対象になります。

HDFS アクティビティーは、監査では扱いにくいので注意してください。これは、リレーショナル・データベースでのファイル・アクセスのモニターにやや類似しているためです。Hive、Big SQL、Impala など、環境で使用されている他のコンポーネントからのアクティビティーのモニターを検討してください。これらのコンポーネントは、データベース・アクセスとかなり類似するモニターをサポートしています。

編集ポリシーおよびブロック・ポリシー

Guardium は、Hive および Impala について抽出ルールを使用した編集、および S-GATE ターミネートを使用したブロックをサポートしています。V9.x では、S-TAP 使用時に BigSQL 用のブロックがサポートされていました。

Hadoop での編集およびブロック・ポリシーの使用について詳しくは、「IBM Security Guardium Deployment Guide for Hadoop Systems」を参照してください。

Kerberos

Guardium は、Kerberos セキュア・クラスターの使用をいくつかの制限付きでサポートしています。Kerberos ユーザー ID を暗号化解除するために、Guardium では、キータブ・ファイルを生成し、特定の場所に配置する必要があります。詳しくは、「IBM Security Guardium Deployment Guide for Hadoop Systems」を参照してください。

重要: HBase または Hive を使用する場合に限り、Kerberos 構成が必要になることがあります。

- 推奨事項と制限事項
  Guardium と Hadoop を統合する場合、以下の推奨事項が参考になります。
- Hadoop での S-TAP および検査エンジン
  Guardium S-TAP をデプロイし、Hadoop で使用する検査エンジンを構成します。
- Hadoop に関する Guardium ポリシーおよびルール
  Hadoop アクティビティーをモニターするための Guardium ポリシーおよびルールの作成を開始します。
- Hadoop を使用した Guardium レポート
  Hadoop 用の組み込み Guardium レポートを使用することや、Hadoop オブジェクトおよびコマンドを使用してカスタム・レポートを定義することができます。

親トピック: Hadoop 統合

推奨事項と制限事項

Guardium と Hadoop を統合する場合、以下の推奨事項が参考になります。

デプロイメントの推奨事項

コレクターのフラッディングを回避するために、および問題の診断を簡素化するために、Guardium コレクターが処理するトラフィックの量およびタイプを削減するための以下の方針を検討します。

- ネットワークを介してアプライアンスにフローする必要があるデータを制限するために、構成する検査エンジンの数を制限します。
- コレクターでログに記録されるデータの量を制限するために、ポリシーで条件を設定します。

1 つの戦略として、検査エンジンを追加し、HDFS などの追加の高ボリューム・トラフィックに対してポリシーを開く前に、Hive コマンド行照会を構成し、テストを行う場合があります。

新しい検査エンジンを構成するたびに、S-TAP を再始動する必要があります。

多くのサービスでトラフィックが生成されるため、Guardium システムは必ずモニターしてください。Guardium デプロイメントのレッドブックに、システムをモニターする方法、およびコレクターに対するトラフィックが多すぎないか確認する方法についての詳細が含まれます。

制限

標準 Guardium S-TAP を使用して Hadoop をモニターする場合、以下の制限が適用されます。

- SSL 暗号化はサポートされません (ただし、Ranger で Hortonworks を使用した場合、または Cloudera Manager で Cloudera を使用した場合は除きます)。Ranger と Cloudera Manager の統合は、この情報の個別セクションで扱います。
- UID チェーンはサポートされません。
- ブロックと編集は、Big SQL、Hive、および Impala に対してのみサポートされます。
- 構成監査システムおよび機密データ・ディスカバリーは現時点ではサポートされていません。
- Guardium は、現時点では、例えば、サービスの開始や停止を監査する管理コマンドはサポートしていません。
- Kerberos を使用した場合、Gardium のロード・バランシングおよびフェイルオーバー・オプションはサポートされません。ただし、仮想 IP アドレスが使用される F5 またはその他のロード・バランシングはオプションとして使用できます。

IBM InfoSphere BigInsights および Big SQL の考慮事項

他のほとんどの Hadoop ディストリビューションと異なり、GPFS および Big SQL での Hadoop には以下の制限が適用されます。

PGFS での Hadoop (IBM Spectrum Scale)
: BigInsights の GPFS デプロイメントには、HDFS Transparency Connector が必要です。

Big SQL
: Big SQL エンジンがインストールされているすべてのノードに S-TAP をインストールする必要があります。Big SQL のサポートは包括的であり、Guardium が Db2 に対して既にサポートしている内容と類似しています。

  Kerberos または GPFS を使用する場合、Big SQL ノードごとに特別な通信出口を構成する必要があります。Guardium は、Big SQL と対話する、動的にロードされる共有ライブラリーを提供しています。実行時に Big SQL により、SQL 要求およびユーティリティー要求が実行されると、そのライブラリー内の関数が呼び出されます。
  制約事項: モニターおよび監査は、Big SQL の出口手法を使用した場合にのみサポートされます。編集およびブロックは、S-TAP を使用した場合にのみサポートされる拡張機能です。

親トピック: 標準 Guardium S-TAP を使用した Hadoop 統合

Hadoop での S-TAP および検査エンジン

Guardium S-TAP をデプロイし、Hadoop で使用する検査エンジンを構成します。

S-TAP および GIM クライアントのデプロイ

Guardium は、Hadoop 用の CAS およびデータベース・ディスカバリーをまだサポートしていないため、S-TAP および GIM クライアントのみ必要になります。S-TAP デプロイメントでは、ご使用のオペレーティング・システムおよびカーネル・レベルに対応する正しい S-TAP をダウンロードしてください。

重要: エッジ・ノードに対しては S-TAP をお勧めします (特に、データのランディング・ゾーンとしてエッジ・ノードを使用する場合)。

検査エンジンの構成

S-TAP のデプロイ後、Guardium アプライアンスから適切な検査エンジンを定義する必要があります。検査エンジンで、特定の S-TAP ホストからモニターするトラフィックを指定します。例えば、特定の S-TAP ホストにおいて、ポート 8032 および 60000 からのトラフィックを Guardium でモニターするように検査エンジンで示す場合があります。検査エンジンでは、Hadoop、HTTP など、モニターするプロトコルも指定します。

検査エンジンを構成する前に、Hadoop 管理者と協力して、モニターする各 Hadoop ノードに関する以下の情報を収集します。

- モニターする Hadoop ノードおよびサービス
- サービスのポート番号
- サーバーの IP アドレス (例えば、S-TAP ホストの IP アドレス)

検査エンジン・プロトコルは、次の表に示されているように Hadoop ノード・タイプおよびサービスに基づいて決定します。

表 1. Hadoop ノードおよびサービスのための検査エンジン・プロトコル

Hadoop ノード	Hadoop サービス	検査エンジン・プロトコル
ネームノード	HDFS ノード名	Hadoop
ネームノード	WebHDFS の HTTP ポート	WEBHDFS
ネームノード	YARN のリソース・マネージャー	Hadoop
ジョブ・トラッカー 注: このノードは、MapReduce1 に対してのみ必要です。	MapReduce ジョブ・トラッカー	Hadoop
HBase マスター	HBase マスター	Hadoop
HBase リージョン	HBase リージョン	Hadoop
hiveserver2	Thrift プロトコル・メッセージ	HIVE
Hive メタストア	Hue から Impala および Hive データベース・ユーザーを取得するために使用される Thrift プロトコル・メッセージ。 注: 計算された属性を使用する必要があります。	HADOOP
Impala デーモン	Impala	IMPALA
Impala	Hue からの Impala	HIVE 注: Hue からの Impala では hiveserver2 が使用されます。

Hadoop ノード	Hadoop サービス	検査エンジン・プロトコル
管理ノード	BigSQL サーバー	Db2
計算ノード	BiGSQL サーバー	Db2
Hue ノード	Oracle、MySQL、または PGSQL バックエンドでの Hue ユーザー・インターフェース	HUE
Solr 検索ノード	Solr 検索	HTTP

例えば、HDFS ネーム・ノードは、ポート `8020`、`Hadoop` プロトコルを使用し、ホスト・アドレスとして `10.0.0.21` を使用する場合があります。
Guardium ユーザー・インターフェースで「管理」 > 「アクティビティー」 > 「モニター」 > 「S-TAP 制御」にナビゲートして、または Guardium API コマンドを使用して、この情報を指定することで、検査エンジンを構成できます。Guardium API コマンドは、例えば、以下のようになります。

```
grdapi create_stap_inspection_engine client=0.0.0.0/0.0.0.0 protocol=HADOOP
    ktapDbPort=8020 portMax=8020 portMin=8020 connectToIp=127.0.0.0 stapHost=10.0.0.21
```

制限:

- Hive CLI は、Hadoop ディストリビューションでは非推奨で、Guardium ではサポートされていません。
- Impala では、Impala デーモンを実行するすべてのノードに対して検査エンジンを構成する必要があります。
- HBase では、マスター・ノードを含むすべてのデータ・ノードで S-TAP が必要です。
- Kerberos または GPFS を備えた Big SQL を使用する場合、DB2_Exit のある S-TAP を構成する必要があります。これは、Big SQL/DB2 暗号化トラフィック、GPFS、またはこの両方をキャプチャーするための安全で効率的な方法です。ただし、このシナリオではブロックおよび編集はサポートされません。Big SQL サポートについての追加情報は、Guardium に関する IBM developerWorks で入手できます。

その他の例および詳しい説明については、「IBM Security Guardium Deployment Guide for Hadoop Systems」を参照してください。
親トピック: 標準 Guardium S-TAP を使用した Hadoop 統合

Hadoop に関する Guardium ポリシーおよびルール

Hadoop アクティビティーをモニターするための Guardium ポリシーおよびルールの作成を開始します。

モニターを目的にする場合、ユーザー、モニター対象のデータ・オブジェクト、および実行するアクションまたはコマンドの観点から考えることは有用です。Guardium の用語では、これらはそれぞれ、*DB ユーザー*、*オブジェクト*、および*動詞* または*コマンド* になります。これらのエンティティーは、リアルタイム・アラートなど、特定のアクションをトリガーするためのポリシー・ルールで使用できます。

Guardium ポリシー・ルール・アクションを使用すると、ポリシー違反のログ記録やアラートに加えて、パフォーマンスのためにトラフィックをフィルタリングできるようになります。Hadoop トラフィックでは、「*S-TAP セッションを無視*」など、セッション・レベルのフィルタリング・アクションは使用できません。これは、Hadoop がリレーショナル・データベースと同じ方法でセッション管理を行わないためです。リレーショナル・データベースでは、データベースにログインするとセッションが確立され、ログアウトするまでそのセッション内で SQL トラフィックが生成されます。Hadoop では、各コマンドがそれ独自のセッションであり、クラスター全体に処理が分散されると、各コマンドにより多数のセッションが作成されることがあります。

Guardium は、コマンド行コンポーネントの失敗したログインを Hue および IBM BigSQL から表示できます。しかし、通常はこれらの失敗したログインをキャッチすることはできません。

ファイル・システム・レベルでアクセス権の例外を受け取るため、例外ドメインを使用してそれらをレポートします。

トラフィックがキャプチャーされるようにするために、標準装備の Hadoop ポリシーからポリシーの作成を開始します。トラフィックが少ないテスト環境でデフォルト・ポリシーをテストすることをお勧めします。また、表示されるノイズの量を削減するために、Hive など単一のサーバー・タイプにトラフィックを制限するアクセス・ルールをもう 1 つ追加できます。コレクターへのトラフィックのフローに問題がなければ、デフォルト・ポリシーを複製して、セキュリティーおよびコンプライアンスの要件に合致したポリシーを作成できます。

実動 Hadoop 環境のためのポリシーの詳しい説明および例については、「IBM Security Guardium Deployment Guide for Hadoop Systems」を参照してください。

親トピック: 標準 Guardium S-TAP を使用した Hadoop 統合

Hadoop を使用した Guardium レポート

Hadoop 用の組み込み Guardium レポートを使用することや、Hadoop オブジェクトおよびコマンドを使用してカスタム・レポートを定義することができます。

Guardium には、Hadoop 用の組み込みレポートがいくつか含まれます。使用可能なレポートのリストを表示するには、「マイ・ダッシュボード」 > 「新規ダッシュボードの作成 (Create a new dashboard)」にナビゲートし、「レポートの追加」をクリックします。「レポートの追加」ウィンドウで、検索フィールドに `hadoop` と入力し、使用可能な Hadoop レポートのリストを表示します。

一部の組み込みレポートでは、コンポーネント・ベースのレポートが提供されます。このレポートは、構成を検証する場合や、コンポーネントからトラフィックを正常にキャッチしているか検証する場合に便利です。「*Hadoop - 許可レポート*」、「*Hadoop - 機密オブジェクトにアクセスする特権ユーザー*」、「*Hadoop - 例外レポート*」、「*Hadoop - ユーザー・ログイン*」など、その他のレポートは、セキュリティーおよびコンプライアンスに焦点を当てています。

このセクションには、Hadoop で使用されるオブジェクトとコマンドまたは動詞のリストが含まれています。グループ・ビルダー・ツールを使用して、Guardium のグループにコマンドをカット・アンド・ペーストできます。また、ご使用の環境に基づいてユーザーおよびオブジェクトのグループを作成する必要があります。

Hadoop オブジェクト

- HDFS ファイル/ディレクトリー
- MapReduce 2 ジョブ名

  MapReduce 2 より前、MapReduce ジョブ名は個別オブジェクトとしてログに記録されませんでした。ただし、組み込み MapReduce レポートとその計算済み属性を使用して完全メッセージからジョブ名を取得することで MapReduce ジョブ名を取得できました。

- IBM Big SQL、Impala、Hive、HBase の表およびビューの名前

HDFS コマンド
HDFS の読み取りコマンド:

- getFileInfo
- getBlockLocations
- getFileLocation
- getListing

HDFS の書き込みコマンド:

- addBlock
- complete
- create
- delete
- mkdirs
- rename

HBase コマンド
HBase の読み取りコマンド:

- list
- scan

HBase の書き込みコマンド:

- createTable
- disableTable
- deleteTable
- multi

  通常、これは insert/update コマンドです。Ranger 統合デプロイメント・オプションでは、これは put コマンドです。

- drop

Big SQL、Hive、および Impala のオブジェクトおよびコマンド
Big SQL、Hive、および Impala の照会言語は、SQL に類似しており、Guardium の他のほとんどのリレーショナル・データベースで使用される通常の解析およびロギング・ルールをサポートしています。ALTER コマンド、CREATE コマンド、管理コマンドなど、これらのコマンドの多くは Guardium コマンド・グループに既に含まれています。SQL 構文のサポート範囲は、これらのディストリビューション間で大きく異なり、Big SQL が最も幅広くサポートしています。

親トピック: 標準 Guardium S-TAP を使用した Hadoop 統合

Cloudera Navigator を使用した Hadoop 統合

Cloudera のネイティブ・データ・ガバナンス・ソリューションである Cloudera Navigator を使用して Haddop を統合する方法について説明します。

Guardium は、標準 S-TAP を使用した Cloudera Hadoop の監査をサポートしています。詳しくは、標準 Guardium S-TAP を使用した Hadoop 統合を参照してください。

Cloudera Navigator でロギングの代替宛先として Kafka が構成されている場合、Guardium では監査イベントにサブスクライブする機能も使用できます。監査対象アクティビティーは Kafka クラスターに送信され、そこで Guardium S-TAP はイベントを取り込み、それらを解析およびログ記録のために Guardium コレクター・アプライアンスに送信します。データが Guardium に取り込まれた後、そのデータは十分に保護され、リアルタイム・アラート、SIEM との統合、レポートとワークフロー、分析など、通常の Guardium 機能をすべて使用できます。

標準の Guardium S-TAP を使用した統合と比較すると、Cloudera Navigator 統合では、Hadoop データにアクセスするクライアントのために SSL 暗号化がサポートされます。Cloudera Navigator 統合を使用した場合、データは、Guardium アプライアンスが受信する前に暗号化解除されます。

制約事項: Cloudera Navigator 統合を使用した場合、Hadoop コンポーネントに対して Guardium ベースのブロックはサポートされません。

前提条件

Cloudera Navigator と Guardium の統合では、以下の最小ソフトウェア・リリース・レベルが必要です。

- V10.1.2 以降の IBM Security Guardium および S-TAP
- CDH 5.7、Cloudera Manager 5.8、およびこれらのリリースに含まれるバージョンの Kafka

アーキテクチャーとデータ・フロー

S-TAP が Hadoop サーバーに常駐するのではなく、Cloudera Manager エージェントが監査イベントを Hadoop コンポーネント・ログから Cloudera Navigator 監査サーバーに送信します。この時点で、Cloudera Navigator は監査イベントをその監査データベースに書き込みます。Guardium と統合するには、追加ロガーとして Kafka を設定します。これにより、Guardium は Kafka からイベント・レコードを収集します。

Hadoop クラスター内のノードまたは Hadoop クラスターの外部の個別サーバーに S-TAP をインストールできるという点で、構成は非常に柔軟です。ただし、そのサーバーが Kafka クラスターおよび Guardium アプライアンスとネットワーク接続できる必要があります。Kafka クラスターごとに 1 つの S-TAP しか指定できませんが、その S-TAP は、標準的な高可用性またはロード・バランシング技法を使用して複数の Guardium システムにトラフィックを送信できます。

この構成では、Cloudera Navigator が Hadoop コンポーネントごとにログ・イベントを生成し、S-TAP がそれらのイベントを取り込みます。Guardium ユーザー・インターフェースを使用して、Cloudera Navigator が使用するメッセージ・トピック ID を指定します。これにより、Guardium S-TAP は、ピックアップする予定のイベントを認識します。

推奨: 監査イベントを確実に保護するために、セキュア Kafka クラスターを使用してください。

- Cloudera Navigator との統合の計画
  統合を構成する前に、このトピックのタスクを実行し、確認します。

親トピック: Hadoop 統合
関連情報:
Hadoop 用の S-TAP 構成パラメーター

Cloudera Navigator との統合の計画

統合を構成する前に、このトピックのタスクを実行し、確認します。

Cloudera Navigator と統合するには、Guardium を担当するデータ・セキュリティー・チームから情報を入手するだけでなく、Cloudera および Kafka を担当する管理者から情報を入手する必要があります。開始する前に、次の情報を収集します。

- Kafka ブートストラップ・サーバーのホストおよびポート。
- Kafka クラスターで TLS および Kerberos が使用されているかどうか。
- S-TAP がインストールされているサーバーのホストおよびポート。このサーバーと Kafka クラスターのネットワーク接続、およびこのサーバーと Guardium システムのネットワーク接続があることを確認します。
- S-TAP ホストで使用されているオペレーティング・システムとそのバージョン。これは、正しい S-TAP をダウンロードし、インストールできるようにするためです。
- Guardium システムのホスト。これは、S-TAP をインストールおよび構成するために必要です。

1. モニター用のソリューションの構成
   このセクションでは、モニター用のソリューションを構成する方法について説明します。
2. Guardium と Cloudera Navigator の通信の構成
   Kafka クラスターを使用して Guardium システムと Cloudera Navigator の間の通信を確立する方法について説明します。

親トピック: Cloudera Navigator を使用した Hadoop 統合

モニター用のソリューションの構成

このセクションでは、モニター用のソリューションを構成する方法について説明します。

手順

1. Cloudera Navigator 監査コンポーネントを構成します。

   詳しくは、Cloudera の資料およびIBM Security Guardium Activity Monitoring for Cloudera Hadoop Using Navigator Integration を参照してください。

2. Kafka 用に TLS/SSL が正しく構成されていることを確認します。

   Cloudera 監査イベントを生成するために使用する Kafka クラスターを、SSL クライアント認証を要求するように構成しないでください。詳しくは、IBM Security Guardium Activity Monitoring for Cloudera Hadoop Using Navigator Integration を参照してください。

3. Guardium S-TAP をサーバーにインストールします。

   使用可能な任意の方法を使用して、Hadoop クラスターの内部または外部にある指定サーバーに S-TAP をインストールします。Guardium で、「管理」 > 「システム・ビュー」 > 「S-TAP 状況モニター」にナビゲートして、S-TAP と Guardium システムの間の接続を確認します。

   Hadoop 関連の S-TAP 構成パラメーターのリファレンスについては、Hadoop 用の S-TAP 構成パラメーターを参照してください。

4. Kafka への Cloudera Navigator 監査イベントの発行を構成します。

   Navigator 管理者またはフル管理者は、Cloudera Manager からこのタスクを実行する必要があります。詳しくは、IBM Security Guardium Activity Monitoring for Cloudera Hadoop Using Navigator Integration を参照してください。

5. Guardium と Cloudera Navigator の通信の構成
6. 構成を検証します。

   ソリューションを構成した後、「管理」 > 「システム・ビュー」 > 「S-TAP 状況モニター」に戻り、S-TAP 状況がまだ緑色であることを確認します。検査エンジンの検査は、Hadoop ソースに対してはサポートされておらず、「*未検査*」状況が常に示されます。

7. Guardium および Cloudera Navigator のポリシーをインストールします。

   モニターおよび監査の場合、Hadoop 用の標準 S-TAP モニターを使用するのではなく Cloudera Navigator 統合を使用する場合もポリシー・ルールに実質的に違いはありません。最初に Guardium ポリシーをインストールするか、デフォルト・ポリシーを使用し、Cloudera クラスターで HDFS または Hive コマンドを実行し、Guardium レポートでトラフィックを確認できるか検査します。詳しくは、IBM Security Guardium Activity Monitoring for Cloudera Hadoop Using Navigator Integration を参照してください。

親トピック: Cloudera Navigator との統合の計画
次のトピック: Guardium と Cloudera Navigator の通信の構成

Guardium と Cloudera Navigator の通信の構成

Kafka クラスターを使用して Guardium システムと Cloudera Navigator の間の通信を確立する方法について説明します。

このタスクについて

「セットアップ」>「ツールとビュー」>「Hadoop モニター」に移動し、**「クラスター情報の追加」**タイルでプラス・アイコンを選択します。

手順

1. 「セットアップ」 > 「ツールとビュー」 > 「Hadoop モニター」にナビゲートし、「クラスター情報の追加」タイルでプラス・アイコンをクリックします。
2. 「S-TAP ホスト名」メニューを使用して、Guardium システムに接続する S-TAP を選択します。
3. Kafka クラスターの「トピック名」を指定します。

   Kafka クラスターの構成設定でこれが変更されていない限り、`NavigatorAuditEvents` (デフォルト値) を使用してください。

4. 「ブートストラップ・サーバー」セクションを使用して、Guardium S-TAP からの初回接続を取得する Kafka ノードを 1 つ以上指定します。

   トピックのパーティションのリーダーであるノードは、コンシューマー要求を処理します。初回接続では、いずれかのブートストラップ・サーバーがダウンした場合にフェイルオーバーを実行できるようにするために、複数のサーバーを指定するのが最も適切です。

5. Kafka クラスターを TLS で構成する場合、「TLS の有効化」チェック・ボックスにチェック・マークを付けます。
   制約事項: Guardium は、SSL クライアント認証を要求するように構成された Kafka クラスターはサポートしません。
6. Kafka クラスターで Kerberos 認証を要求する場合、「Kerberos を使用」チェック・ボックスにチェック・マークを付けます。
   a. 「プリンシパル」フィールドを使用して、S-TAP の Kerberos プリンシパル名を指定します。

      例えば、`guardium/FullyQualifiedDomainName@kerberosDomain` などです。

   b. 「キータブ・ファイルへのパス」フィールドに、S-TAP サーバー上の Kerberos キータブ・ファイルの絶対パスを入力します。

      例えば、`/etc/krb.keytab` などです。キータブを S-TAP ユーザーおよびグループが所有していることを確認し、さらにユーザーがキータブの読み取りのみ可能であることを確認します。

7. 「保存」をクリックします。

   結果のタイルでは、Hadoop モニターが構成済みであることが示され、S-TAP 状況が緑色になります。

親トピック: Cloudera Navigator との統合の計画
前のトピック: モニター用のソリューションの構成

Hortonworks および Apache Ranger を使用した Hadoop 統合

Hortonworks Data Platform に含まれる Apache Ranger を使用すると、ポリシーにより、Hive、HBASE、HDFS などの Hadoop コンポーネントに対して詳細なアクセス制御および監査を実行できます。

監査データは HDFS と Solr (推奨) の両方に書き込まれます。以下の 2 つの方法で Ranger と Guardium を統合できます。

- 監査では、Guardium は、Ranger Auditing のもう 1 つのロガー・ソースとして動作します。監査対象のアクティビティーは Guardium コレクターに送信され、そこで解析され、ログに記録されます。データが Guardium に取り込まれた後、そのデータは強固なアプライアンスで十分に保護され、リアルタイム・アラート、SIEM との統合、レポートとワークフロー、分析など、通常の Guardium 機能をすべて使用できます。
- ブロックの場合、Guardium は、Ranger では動的ポリシーとして知られるものを使用して、Ranger のアクセス制御ポリシーを拡張します。

モニターおよびブロックに関して標準 Guardium S-TAP に依存する Hadoop 統合と異なり、Ranger との統合では、クライアントと Hadoop データの間での SSL 暗号化がサポートされます。Ranger 統合では、データは暗号化解除された後に、監査のために Guardium システムに送信されます。動的ポリシーを使用する Ranger 統合では、SSL のサポートに加えて、標準 S-TAP の使用でサポートされるコンポーネントよりも多くのコンポーネントに対してブロックをサポートできます。

同じクラスター内で検査エンジンと Ranger 統合の両方を使用できますが、両方の方法を同時に使用することはほとんどありません。統合パスの選択について詳しくは、Hadoop 統合を参照してください。

前提条件

Ranger との統合では、以下が必要です。

- IBM Security Guardium 10.1 (S-TAP およびアプライアンス)
- Ranger を含む Hortonworks 2.3

アーキテクチャーとデータ・フロー

このアーキテクチャーでの重要な相違点は、S-TAP が Hadoop コンポーネントから監査データを直接収集しないことです。むしろ、このアーキテクチャーでは Ranger プラグインが監査メッセージを log4j に書き込みます。これらのメッセージは S-TAP に転送され、S-TAP はそれらのメッセージを、ロギング、アラート、レポート、および分析のために Guardium コレクターに送信します。

Ranger 統合をオンにするには、log4j_reader_enabled=1 を指定して S-TAP を構成する必要があります。

S-TAP を複数のノードにインストールできるという点で、構成は非常に柔軟です。例えば、すべてのコンポーネント・トラフィックが 1 つの S-TAP に送信されるように Ranger を構成することや、すべての HBase トラフィックが 1 つの S-TAP に送信され、Hive および HDFS が別の S-TAP に送信されるように指定することができます。

ブロックは、Guardium アプライアンスで指定されているブロック・ポリシー・ルールに対応するように Ranger アクセス制御ポリシーを拡張することで実装します。ブロックの実際の実装は、Ranger からのアクセス否認として実行されます。ブロックをアーキテクチャーおよびデータ・フローに適合させる方法について、およびブロックを実装するためのガイダンスについて詳しくは、IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration を参照してください。

- Hortonworks および Apache Ranger との統合の計画
  統合を構成する前に、このトピックのタスクを実行し、確認します。
- モニター用のソリューションの構成
  このセクションでは、モニター用のソリューションを構成する方法について説明します。

親トピック: Hadoop 統合
関連情報:
Hadoop 用の S-TAP 構成パラメーター

Hortonworks および Apache Ranger との統合の計画

統合を構成する前に、このトピックのタスクを実行し、確認します。

S-TAP およびコレクターのトポロジー

必要なトポロジーを決定します。

- 必要なコレクターの数
- 各 S-TAP でモニターするコンポーネント

一部のカスタマーは、コンポーネントごとに 1 つの S-TAP を使用しています。最低でも、HBase のために 1 つの S-TAP、他のすべてのために 1 つの S-TAP を使用することをお勧めします。
ヒント: S-TAP は、特定のコンポーネントと同じノードに配置する必要はありません。S-TAP 専用の Linux ボックスを設定できますが、Hadoop HA をサポートする場合はこれをお勧めします。
1 つの S-TAP に対する接続の数を構成する場合、次の経験則を使用してください。

- HBase: リージョン・サーバーの数 + 1
- その他のすべて: モニター対象のコンポーネントごとに 1 つ + 1

重要:

- ブロックの場合、すべての HBase リージョン・サーバーへのアクセスを確認します。これは、Guardium プラグインの JAR ファイルをこれらのリージョン・サーバーそれぞれにコピーする必要があるためです。

  高可用性フェイルオーバー・シナリオを構成する場合、フェイルオーバー・ノードの IP アドレスまたはホスト名を記録します。

高可用性およびフェイルオーバー

Hadoop では、1 次ノードで障害が発生した場合、高可用性対応の 2 次ノードを使用してデータ要求が処理されます。フェイルオーバー・シナリオで監査データを継続して収集できるようにするために、S-TAP デプロイメントには複数のオプションがあります。

S-TAP をインストールし、Hadoop クラスターに属さないシステムでそれをセットアップする
: これにより、コンポーネントのフェイルオーバー時に、新しいノードがリモート・ロガーとして S-TAP を自動的に使用する簡素な構成が実現します。S-TAP の構成に対する変更は不要です。

HDFS および Hive S-TAP に対して `localhost` を使用し、HBase に対して別個のシステムを使用する
: S-TAP ホスト・フィールドで `localhost` を使用して HDFS および Hive 用の S-TAP をインストールし、その後、HBase 用のエッジ・ノードとして別個のシステムを使用します。S-TAP をすべてのノードおよびリージョン・サーバーにインストールする代わりに、この方法を使用できます。この方法を使用することをお勧めします。

クラスター内のノードに S-TAP をインストールする
: このモデルでは、各コンポーネント用の 1 次ノードおよびスタンバイ・ノードに S-TAP をインストールします。

  S-TAP ホスト・フィールドで `localhost` を使用して、クラスター内のすべてのノード、および HBASE のすべてのリージョン・サーバーに S-TAP をインストールします。この方法は推奨されていません。

Guardium ロード・バランシング

Ranger 統合を有効にすると、Guardium S-TAP およびエンタープライズ・ロード・バランシング・オプションがサポートされます。

Ambari および Ranger 情報の収集

セットアップの重要な部分は、Hadoop 管理インターフェースである Ambari を使用して行います。構成を実行するには、以下の情報が必要です。

Ambari

- サービス管理者アカウントなど、*log4j* 構成を更新および保存する特権を持つユーザーの ID およびパスワード。簡潔にするために、これを管理アカウントおよび管理パスワードと呼びます。
- ポートと IP アドレスまたはホスト名。
- クラスター名。

Ranger
: ブロックを構成する場合に限り、以下の情報が必要です。ブロックの構成について詳しくは、IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration を参照してください。

- *log4j* 構成を更新および保存できるサービス管理者アカウント。
- ポートと IP アドレスまたはホスト名。

必要なポートを開く

以下のポートが開いているか確認します (デフォルト・ポートの使用を想定しています)。

- モニターのために、S-TAP があるノードと Ranger サーバーとの間のポート 5555 を開きます。
- ブロックのために、ポート 5556 を開き、S-TAP と Guardium プラグインがあるクラスター内のすべてのノードとの間で通信を実行できるようにします。

親トピック: Hortonworks および Apache Ranger を使用した Hadoop 統合

モニター用のソリューションの構成

このセクションでは、モニター用のソリューションを構成する方法について説明します。

始める前に

Ranger と Guardium の通信の構成を開始する前に、Ambari を使用して Ranger プラグインを構成します。詳しくは、「IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration」ガイドまたは Hortonworks の資料を参照してください。

1. Guardium と Ranger の通信の構成
   Guardium システムと Ranger の間で通信を確立する方法について説明します。
2. S-TAP のインストールおよび構成
   Ranger 統合のために S-TAP をインストールし、構成します。
3. Hadoop サービスのモニターの有効化
   特定の Hadoop コンポーネントに対してモニターを有効にします。

次のタスク

これらのセットアップ・ステップを完了した後、Guardium および Ranger のポリシーをインストールします。モニターおよび監査の場合、Hadoop 用の標準 S-TAP モニターを使用するのではなく Ranger を使用する場合も、ポリシー・ルールに実質的に違いはありません。詳しくは、「IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration」を参照してください。
親トピック: Hortonworks および Apache Ranger を使用した Hadoop 統合

Guardium と Ranger の通信の構成

Guardium システムと Ranger の間で通信を確立する方法について説明します。

このタスクについて

このタスクでは、Guardium システムと Ranger の間で通信を確立する方法について説明します。

手順

1. 「設定」 > 「ツールとビュー」 > 「Hadoop モニター」にアクセスします。
2. 「クラスター情報の追加」セクションで  をクリックして、新しい構成の定義を開始します。
3. 「名前」フィールドに、構成の名前を入力します。
4. 「Hadoop ディストリビューション」メニューから `Hortonworks` を選択します。
5. 「ホスト名/IP」フィールドに、Ambari サーバーのホスト名または IP アドレスを入力します。
6. 「ポート番号」フィールドに、Ambari サーバーのポート番号を入力します。 このフィールドを空白のままにすると、構成ではデフォルト・ポートの 8080 が使用されます。
7. 「クラスター名」フィールドに、Hadoop クラスターの名前を入力します。
8. 「ユーザー名」フィールドに、Ambari 管理者のユーザー名を入力します。
9. 「パスワード」フィールドに、Ambari 管理者アカウントのパスワードを入力します。
10. 「接続のテスト」ボタンをクリックして、構成を検証します。
11. 「保存」をクリックして構成を保存します。

タスクの結果

「Hadoop モニター」ページから新しい構成を使用できます。
親トピック: モニター用のソリューションの構成
次のトピック: S-TAP のインストールおよび構成

S-TAP のインストールおよび構成

Ranger 統合のために S-TAP をインストールし、構成します。

始める前に

S-TAP の要件およびデプロイメント・オプションについて詳しくは、Hortonworks および Apache Ranger との統合の計画を参照してください。

手順

1. S-TAP をインストールし、Ranger 統合のために有効にします。 トラフィックを処理するために複数の S-TAP が必要になる場合があります。例えば、HDFS、Hive、および Kafka トラフィックのためにネーム・ノードで S-TAP を 1 つ構成し、すべての HBase トラフィックのために HBASE マスター・ノードで S-TAP を 1 つ構成します。

2. 監査のために guard_tap.ini を構成します。
   a. guard_tap.ini をテキスト・エディターで開きます。 これらの設定では UI および GIM はサポートされていないため、ファイルを直接編集する必要があります。
   b. 以下にリストされているパラメーターを追加します。 ご使用の環境に合わせて値を更新します。

```
; Settings for log4j
logging log4j_reader_enabled=1
log4j_port=5555
log4j_listen_address=0.0.0.0
; Maximum number of connections to support from the log4j service
log4j_num_connections=50
```

   c. 設定を更新した後、S-TAP を再始動します。

親トピック: モニター用のソリューションの構成
前のトピック: Guardium と Ranger の通信の構成
次のトピック: Hadoop サービスのモニターの有効化
関連情報:
Hadoop 用の S-TAP 構成パラメーター

Hadoop サービスのモニターの有効化

特定の Hadoop コンポーネントに対してモニターを有効にします。

このタスクについて

このタスクでは、Guardium によるモニターをどの Hadoop コンポーネントに対して有効にするか定義する方法について説明します。

手順

1. 「設定」 > 「ツールとビュー」 > 「Hadoop モニター」にアクセスします。
2. サービスの構成を開始するために、Hadoop クラスターの ⊕ をクリックします。
3. 「サービス」メニューを使用して、モニターを有効にする Hadoop コンポーネントを選択します。
4. 「S-TAP ホスト名/IP」メニューを使用して、Ranger から監査イベントを収集する S-TAP を選択します。
5. 「ポート番号」フィールドに、リスナーのポート番号を入力します。 このフィールドを空白のままにすると、サービスはデフォルト・ポートの 5555 を使用します。
6. 「モニターをただちにアクティブ化 (Activate monitoring immediately)」を選択して、選択したサービスのモニターを有効にします。
7. 「保存」ボタンをクリックして、サービスの構成を保存します。
   重要: Hadoop 管理者は、サービス構成に行った変更を有効にするために、Hadoop サービスを再始動する必要があります。

タスクの結果

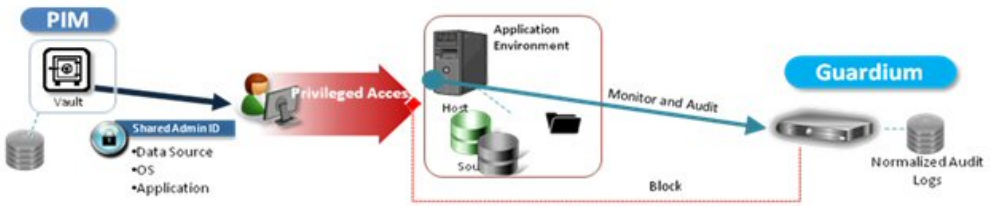
「Hadoop モニター」ページから、有効化したサービスに緑色のチェック・マーク・アイコンが付いていることを確認します。
親トピック: モニター用のソリューションの構成
前のトピック: S-TAP のインストールおよび構成

Guardium DAM と PIM の統合

Privileged Information Management (PIM) の支援により、組織は、共有特権 ID の使用を自動化および追跡でき、さらにそれらの共有特権 ID の使用をモニターできます。

ここでは、データベースにログインしている実際のユーザー (人) を可視化できるようにするために、PIM アクティビティー・データを Guardium DAM データと統合します。

次の図は統合を表しています。



この統合の主な目的は、以下のとおりです。

- PIM データ (PIM によって管理されるリース履歴 (誰が共有アカウントを使用したか)、資格情報、データベースなど) を、Guardium アプライアンスで可視化する。
- PIM 情報と相関関係のある DAM 情報を提供する。例えば、Guardium で、本日のデータベース・ユーザー、および特定ユーザーが発行した実際の要求を表示できるようになります。この統合により、データベース・ユーザーおよび共有 ID をリースした実際の PIM ユーザーの両方を使用できるようになります。

インストール

Guardium パッチ (v10.1p103) を使用すると、PIM 統合機能をインストールできます。PIM 統合は、スタンドアロンの Guardium システムおよびフェデレーテッド環境で使用できます。

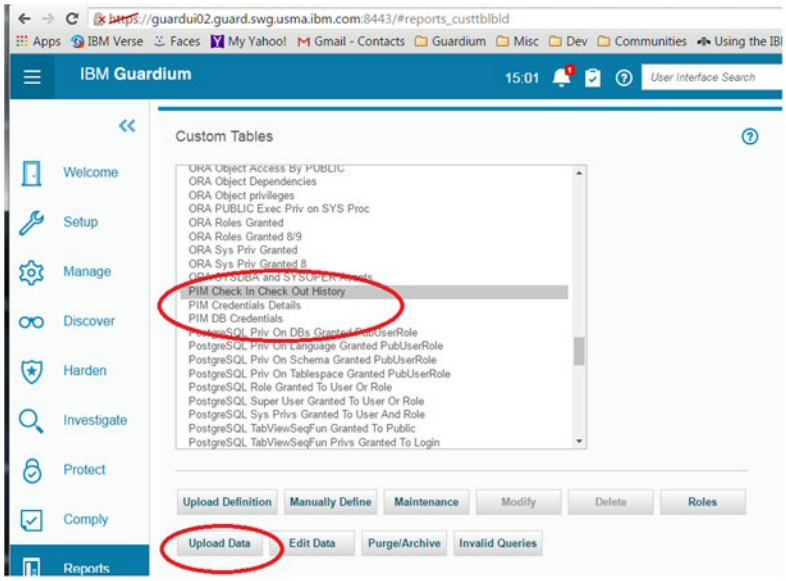
注: PIM アクティビティー・データが既に実装済みであることを前提とします。

以下の手順を行います。

1. Guardium システムにデータを取り込みます。

   データ・ソースを選択し、Guardium UI で「レポート」 > 「レポート構成ツール」 > 「カスタム表ビルダー」を選択します。

   3 つの PIM 事前定義表を見つけ、選択し、表ごとに自動データ・アップロードをスケジュールします。



   Guardium システムへの PIM 表のアップロード

   Guardium 中央マネージャーを使用する場合、Guardium UI で「管理」 > 「中央マネージャー」 > 「PIM データ配布」を選択します。これを行うことで、中央マネージャーからすべての管理対象ユニットへのデータ配布をスケジュールします。

2. データが管理対象ユニットに取り込まれた後、CLI コマンドの store pim_correlation_mode を使用して、PIM データと Guardium セッション・データの相関関係を有効にします。

   CLI コマンド

   store pim_correlation_mode

   使用法: store pim_correlation <state>

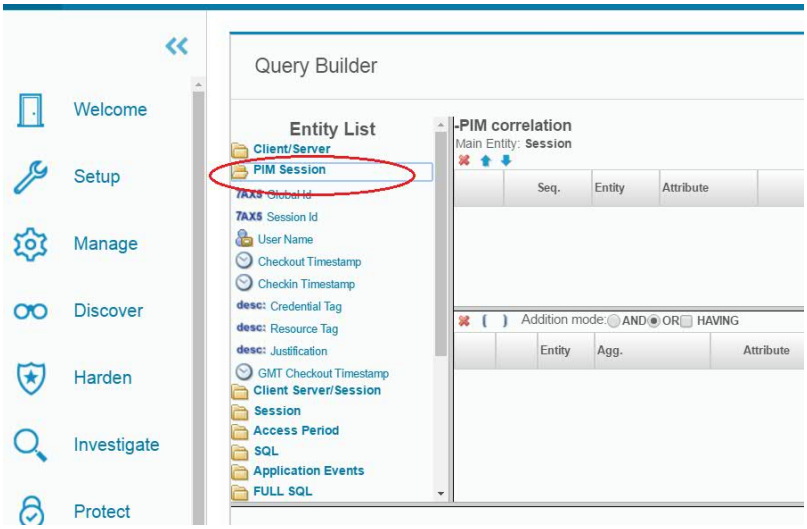
   where state is on/off. on で有効になり、off で無効になります。

   表示コマンド

   show pim_correlation_mode

3. 相関を実行するには、Guardium GUI で「順守」 > 「カスタム・レポート作成」 > 「PIM データ相関」を選択します。

   アクセス・ドメインのレポートを通じて、相関関係のあるデータを確認できます。



   アクセス・ドメインの PIM セッション

親トピック: 製品の統合

QRadar と Guardium の統合

QRadar と Guardium は両方向の情報フローで連係して動作して、Guardium データ保護ポリシーを自動的に更新し、また QRadar からのセキュリティー・インテリジェンス・イベントにほぼリアルタイムで応答することができます。

IBM QRadar は、セキュリティー・インテリジェンス・ツールであり、セキュリティー情報とイベントのモニター、異常を検出するためのカスタマイズ可能ルールの使用、およびインシデント・フォレンジックと脆弱性管理のためのツールの提供によって脅威からの保護を実現します。

IBM Guardium は、サーバーに保管されるデータの保全性の実現を支援する、データ・セキュリティーおよびデータ・プライバシーのためのソリューションです。Guardium では、ポリシーおよび包含/除外リスト (Guardium グループと呼ばれます) を使用してデータへのアクセスが制御されます。

QRadar および Guardium ソリューションでは、QRadar セキュリティー・イベントに応じてアクションをトリガーするための QRTrigger フレームワークが活用されます。構成設定に応じて、QRadar イベントにより、そのイベント自体がもたらす情報に基づき、Guardium グループに新しいメンバーが追加されます。さらに、メンバーシップの変更をただちに有効にするために、グループに関連する Guardium ポリシーが自動的に再インストールされます。

QRadar および Guardium ソリューションを使用すると、単一の Guardium コレクター、または Guardium 中央マネージャー (CM) によって制御される Guardium コレクターのグループを更新できます。

QRadar と Guardium の連携

従来の QRadar と Guardium の統合は、片方向の情報フローで、Guardium がアラートと脆弱性評価 (VA) レポートを QRadar に送信していました。

データベースの一般的なアラート・ユース・ケース:

- 失敗したログイン
- 無許可アクセス
- SQL エラー・コード (例えば、SQL インジェクション攻撃)
- ユーザーによる特権のエスカレート試行
- ユーザーによる機密データに間接アクセスするためのトリガーおよびビューの作成

現在、QRadar と Guardium は、両方向の情報フローで連係して動作できます。

その他のユース・ケース:

- 暗号漏えいしたマシンからのアクセスをブロックする
- 疑わしい対象になったユーザー ID によるアクセスに対する監査レベルを上げる
- Privileged Identity Management (PIM) システムに登録された特権共有ユーザー ID によるアクセスに対する監査レベルを上げる

QRadar イベントに基づく Guardium ポリシーの更新

QRadar および Guardium ソリューションのデプロイ手順を以下に示します。

1. ソリューション・ファイルをインストールします。
2. Guardium でクライアント ID およびパスワードを設定します。
3. QRadar で転送先を構成します。
4. QRadar イベントをソリューションに送信するルールを構成します。
5. 必要に応じて、統合のために Guardium のグループおよびポリシーを定義します。

Guardium バージョン 10.1 以降には、この統合をサポートすることを目的とした、以下の 3 つの事前定義グループがあります。

- QRadarBlockingConnection
- QRadarAlertingConnection
- QRadarLogConnection

これらの各グループには、次のタプル構造があります。

<クライアント IP>、<ソース・アプリケーション>、<DB ユーザー>、<サーバー IP>、<サービス名>、<OS ユーザー>、<DB 名>

3 つのルール (ブロック・ルール、アラート・ルール、およびロギング・ルール) を含む「QRadarPolicy」という名前の事前定義 Guardium ポリシーがあります。各ルールは、上記のリストの各グループに関連付けられています。

QRadar および Guardium ソリューションのインストール方法

QRadar および Guardium ソリューションのインストールに関する詳細な指示については、次の IBM Developerworks の記事を参照してください。

https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W746177d414b9_4c5f_9095_5b8657ff8e9d/page/QRGuardium

Guardium のセットアップ

QRadar および Guardium ソリューションを Guardium REST API に対して認証できるようにするには、クライアント ID を Guardium に登録し、関連するクライアント・パスワードを取得する必要があります。

クライアント ID の登録は、Guardium の grdapi コマンド行ユーティリティーを使用して行います。この操作は、1 回のみ実行します。クライアント ID を登録すると、クライアント・パスワードなど、新しいクライアントの詳細を含む JSON エントリーが作成されます。

```
> grdapi register_oauth_client client_id=qrguardium
ID=0
{"client_id":"qrguardium","client_secret":"3ac89782-ce55-
4f24-b795-b6c76ecc4045",
"grant_types":"password","scope":"read,write","redirect_uri"
:"https://joeApp"}
ok
```

トラブルシューティング・ログ

QRadar および Guardium ソリューションは、操作の管理およびトラブルシューティングを支援する多数のログ・ファイルを提供します。これらのログ・ファイルには以下が含まれます。

表 1. ログ・ファイル

パラメーター名	記述
guardiumEvents_audit.log	これは、QRadar イベントに基づいて Guardium に対して行われるすべての変更の監査ログです。各行は JSON オブジェクトで、処理されたイベントの ID、タイム・スタンプ、および詳細が含まれます。
QRListener.log	QRadar から転送されたイベント・データを受信するリスナー・プロセスのログ出力。
HANDLER_<イベント名>.log	特定イベントの専用ハンドラー AL のログ出力。
RESPONSE_<イベント名>.log	カスタム応答 AL のログ出力 (この AL がその AssemblyLine 名に基づくロギングを実装している場合)。例えば、これは、次の Javascript を使用して Log Appender File Path パラメーターが計算されるように設定することで実行できます。 return “logs/” + task.getShortName() + “.log”;

親トピック: 製品の統合
関連情報:
ディレクトリー・インテグレーター統合 (ビデオ)

OPTIM から Guardium へのインターフェース

OPTIM から Guardium へのインターフェースは、Protobuf (汎用フィード・エージェント) を使用して Optim アクティビティー・ログを Guardium に送信します。

このインターフェースの目的は、OPTIM アクティビティーに対して Guardium 監査機能を使用することです。この監査機能には、 レポート・ツール (ユーザー定義の照会とレポート)、監査プロセス (ロール/ユーザー/グループ、ユーザー定義の状況フロー・プロセス、 エスカレーション、エクスポートなどに 1 つのタスクを割り当てることを可能にするワークフローの自動化機能)、およびしきい値アラートが含まれます。

Optim 監査アクティビティー情報には、アクセスの詳細、セッション番号、アクティビティー・タイプ (verb)、表 (オブジェクト)、詳細 (フィールド)、実行時間 (応答時間)、エラーの数 (影響を受けたレコードの数) が含まれます。

データは Guardium 標準オブジェクト・モデルにマップされます。

OPTIM の監査を有効にするには、OPTIM による有効化処理と、Guardium での次のステップが必要です。 (1) ユーザーを Optim 監査ロールにリンクする (2) 事前定義レポートを該当するペインに追加する (3) スニファーを有効にする (4) ポリシー・アクションを「値を含むデータをログに記録する (Log Data With Values)」に設定する。

このインターフェースには、optim-audit ロール、optim-audit ロールのデフォルトのレイアウト (psml ファイル)、7 つの事前定義レポートが含まれています。

これらのレポートは以下のとおりです。

- Optim - Optim サーバー当たりの失敗した要求の要約
- Optim - ユーザー当たりの要求の実行
- Optim - Optim サーバー - 表の使用状況の詳細
- Optim - 要求ログ
- Optim - 表の使用状況の要約
- Optim - 要求の要約

注: 「optim-audit」ロールおよびユーザーを作成すると、OPTIM 監査という 1 つのタブのみ表示されます。ユーザーが生成できるカスタム・レイアウトを持つロールと同様に、このロールのレイアウトは単独で使用するためのものです (optim-audit ユーザーには他のユーザー・ロール・タブは不要です)。ただし、ユーザー・ロールは必須であるため、ユーザーが optim-audit ロールを持った時点でレイアウトのマージがオフになり、optim の対象項目のみ取得できるようになります。同じように動作する他のロールに「review-only」と「inv」があります。
注: optim-audit ロールを作成して保存した後に、「ユーザー・ブラウザー」メニュー内の「レイアウトの生成」選択項目をクリックし、「リセット」をクリックして、そのロールに関連付けられているレイアウトを取得してください。「ユーザー・ブラウザー」内でロールを変更した場合は、この作業を再度行ってください。

親トピック: 製品の統合

リアルタイム・アラートおよび相関分析と SIEM 製品との統合

データベースのアクティビティー・パターン、構造、およびプロトコルのコンテキスト・ナレッジを、SIEM システムのサード・パーティー・データベースに直接配布します。

このタスクについて

Guardium® は、大量のデータベース・トラフィックを前処理し、重要な情報を抽出します。抽出した後は、圧縮した要約を外部の SIEM (Security Incident Event Manager) システム (ArcSight、Envision、QRadar など) に送信します。 したがって、SIEM 製品が大量のトラフィック・ストリームを処理する必要がなくなります。むしろ、すべてのアクティビティーの相関付け、無許可の動作や疑わしい動作に対するアラート、イベント・ログに関する規制コンプライアンス要件への対応に集中することが可能になります。

この Guardium SIEM (Security Incident Event Manager) 統合は、以下のいずれかの方法で実施できます。

- Syslog 転送 (アラートおよびイベントの最も一般的な方法)
- CLI コマンド store remotelog を使用して、機能/優先度およびホスト (宛先) への Syslog 転送を指定する。
- ArcSight、Envision、および QRadar 用の Guardium テンプレートの使用
- SCP/FTP (CSV または CEF ファイルは外部リポジトリーに送られ、SIEM システムはこの外部リポジトリーからアップロードして解析する必要があります。)

Guardium は、データベースのアクティビティー・パターン、構造、およびプロトコルのコンテキスト・ナレッジを、SIEM システムのサード・パーティー・データベースに直接配布します (Guardium は SIEM システムの資格情報を持ち、SIEM データベースへの SIEM スキーマによる直接書き込みが可能です)。Guardium のエンティティーをサード・パーティー・スキーマにマップする必要があるため、Guardium サポートにお問い合わせください。

注: SIEM システムもリモート・ロギングを有効にして、syslog 内に定義された適切な機能/優先度を listen できるようにする必要があります。

Guardium のリアルタイム・セキュリティー・アラートと相関解析を、SIEM およびログ管理製品と組み合わせることによって、企業は以下の能力を高めることができます。

- 外部からの攻撃、信頼された内部関係者、コンプライアンス違反によるリスクを事前に識別して緩和する。
- Sarbanes-Oxley (SOX)、PCI-DSS (クレジット・カード業界のデータ・セキュリティー基準)、 データ・プライバシー規制に応じた自動制御を実施する。
- 企業データベースやアプリケーションといったデータ・センターのコアにあるクリティカル・ログ/イベントと合わせて、システムおよびネットワークのイベントを管理し、会社全体の相関付け、法務、インシデントの優先付け、レポート作成を行う。

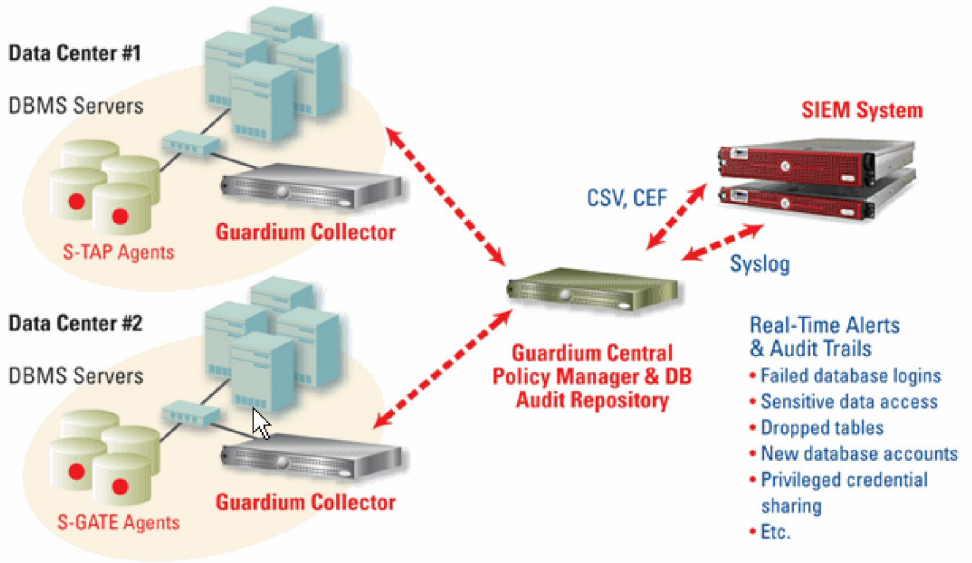
Security Information and Event Management (SIEM) ソリューション (Security Event Management (SEM) ソリューションとも呼ばれる) は、QRadar、ArcSight、CA、Cisco MARS、LogLogic、RSA enVision および SenSage の各社より提供されています。SIEM 製品は、Guardium のデータベース・アクティビティー・モニター・ソリューションを補完する製品です。これらの製品は、Guardium によるデータベース・イベントのフィルター処理および前処理機能を使用して、SOX、PCI-DSS、およびデータ・プライバシーに応じた 100% の可視性とデータベース分析も行うことができます。

SIEM テクノロジーは、ネットワーク・ハードウェアおよびアプリケーションで生成されたセキュリティー・アラートをリアルタイムで分析します。これにより、企業はネットワーク攻撃に対してより迅速に対処したり、毎日生成される大量のログ・データを整理したりすることができるようになります。SIEM ソリューションは、ログ・ベースの相関エンジンです。

SIEM ソリューションは、監査ではなく、主に検出とセキュリティーを重点的に扱います。 他のログのデータを組み合わせることで、ハイレベルの分析を行います。 さらに多くのデータ (IP アドレスやルーターなど) の相関付けをしますが、データベースの可視性はあまり得られません。法務基準、デジタル署名、監査モニター機能には対応していないため、 即座に情報を得るのには使用できますが、履歴を証拠として扱うためには使用できません。

Security Information and Event Management (SIEM) のユーザーは、内部の DBMS ユーティリティーで生成された未加工のログをインポートする必要があります。DBMS ロギング・ユーティリティーのパフォーマンス、このユーティリティーによって生成される未フィルター情報、および必要な細分化された情報がないことにより、不都合が生じます。

Guardium のユーザー・インターフェースを使用することにより、各種の SIEM ツールと統合するための Guardium の構成が簡単に行えます。



注: SIEM との統合において、Guardium システムではレポートおよびポリシーに変更はありません。既存のポリシーおよびレポートの継続使用、アラートのトリガー、および SIEM システムへのレポートの送信を行うことができます。

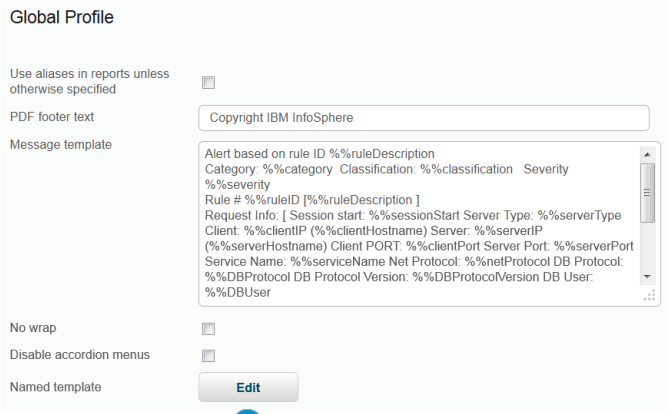
SIEM と Guardium の統合では、QRadar、Envision、および ArcSight 用の事前定義テンプレートがあるため、それらを定義する必要がありません。ルール・アクションにおける適切なメッセージ・テンプレートを選択できます。

デフォルトのメッセージ・テンプレートの変更、syslog 転送に関するパラメーターの指定、およびエクスポートする CSV ファイルまたは CEF ファイルの作成を行うことができます。

注: CEF を使用できるのは、ArcSight の場合のみです。その他の SIEM 製品は別の形式を使用し、CEF を使用しません。

SIEM 製品が送信された情報を認識できるようにするため、「グローバル・プロファイル」を介してメッセージ・テンプレートを変更する必要があります。これは、SIEM ソリューションと Guardium の間で合意された形式であり、SIEM 製品は着信メッセージを解析して、そのデータベースを新しいイベント/データで更新することが可能になります。

1. 「グローバル・プロファイル」を開くには、「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」をクリックします。
2. 「名前付きテンプレート」の「編集」をクリックします。



3. テンプレートを選択するか、 アイコンで新規のテンプレートを作成します。

Guardium アプライアンスは、syslog メッセージをリモート・システムに送信するよう構成できます。特定のタイプの syslog メッセージを特定のホストに送信できます。syslog メッセージのタイプは、メッセージの機能-優先度から判別されます。

機能の例として、all、auth、authpriv、cron、daemon、ftp、kern、local0、local1、local2、local3、local4、local5、local6、local7、lpr、mail、mark、news、security、syslog、user、uucp があります。優先度の例として、alert、all、crit、debug、emerg、err、info、notice、warning があります。

他のアプリケーションが使用可能な情報を含んだレポート、または大量のデータを含んだレポートを、CSV ファイル形式でエクスポートすることができます。 レポート、エンティティー監査証跡、およびプライバシー・セット・タスクの出力は、CSV (区切り文字区切り値) ファイルにエクスポート可能です。 また、CSV ファイル出力を syslog に書き込むことができます。 リモート syslog 機能を使用する場合、出力 CSV ファイルがリモート syslog ロケーションに送信されます。

CSV ファイルや CEF ファイルの各レコードは、レポートの 1 行を表しています。エクスポートする CSV ファイルの再フォーマット可能なツールについては、Guardium サポートまでお問い合わせください。

Guardium アプライアンスは、store remotelog CLI コマンドを使用して syslog メッセージをリモート・システムに送信するよう構成できます。特定のタイプの syslog メッセージを特定のホストに送信できます。 syslog メッセージのタイプは、メッセージの機能-優先度から判別されます。

機能の例として、all、auth、authpriv、cron、daemon、ftp、kern、local0、local1、local2、local3、local4、local5、local6、local7、lpr、mail、mark、news、security、syslog、user、uucp があります。優先度の例として、alert、all、crit、debug、emerg、err、info、notice、warning があります。

他のアプリケーションが使用可能な情報を含んだレポート、または 大量のデータを含んだレポートを、CSV ファイル形式でエクスポートすることができます。 レポート、エンティティー監査証跡、およびプライバシー・セット・タスクの出力は、CSV (区切り文字区切り値) ファイルにエクスポート可能です。 また、CSV ファイル出力を syslog に書き込むことができます。 リモート syslog 機能を使用する場合、出力 CSV ファイルがリモート syslog ロケーションに直ちに送信されます。

CSV ファイルや CEF ファイルの各レコードは、レポートの 1 行を表しています。

CSV ファイルへの syslog メッセージの送信およびレポートのエクスポートを行うには、以下の手順を実行します。
注: 監査プロセス定義内のファイルは、SIEM ベンダーが正しく解析できるようにするために、zip しないでください。

1. 監査プロセス・ファインダーを開くには、「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」をクリックします。
2. アイコンをクリックしてプロセスを追加するか、ドロップダウン・リストから既存のプロセスを選択します。
3. 「監査タスク」にある「新規監査タスク (New Audit Task)」をクリックします。
4. 説明を入力し、「レポート」を選択します。
5. ドロップダウン・リストからレポートを選択して、「CSV/CEF ファイル・ラベル」に入力します。
6. 「CSV ファイルへのエクスポート」と「Syslog に書き込む」を選択します。名前付きテンプレートをドロップダウンリストから選択します。
7. タスク・パラメーターの下で、カレンダー・アイコンを使用して「期間の開始日を入力>=」と「期間の終了日を入力<=」を選択します。
8. 「適用」をクリックします。

CSV/CEF ファイルもスケジュールに基づいて SIEM ホストにエクスポートできます。監査タスクを変更するか追加します。

1. 「順守」 > 「ツールとビュー」 > 「監査プロセス・ビルダー」をクリックして監査プロセス・ファインダーを開き、監査タスクを変更するか追加します。
2. 「CSV ファイルへのエクスポート」または「CEF ファイルのエクスポート」を選択します。
   注: アクセス・レポートは CEF 形式または LEEF 形式で保存して送信できますが、その他のレポート (Guardium ログイン、統合アクティビティー・ログ、CAS イベントなど) は CEF または LEEF にマップできません。
3. 「Syslog に書き込む」のチェック・マークを外します。そうしないと、ファイルでなく syslog メッセージが生成されます。
4. 「管理」 > 「データ管理」 > 「結果エクスポート (ファイル)」をクリックして、CSV/CEF のエクスポート・メニューを開きます。
5. 「SCP」プロトコルまたは「FTP」プロトコルを選択します。 次に、「ホスト」、「ディレクトリー」、「ユーザー名」、「ポート」、および「SCP/FTP パスワード」に入力します。
6. 「スケジューリング」セクションで、「開始時刻」、「再始動」頻度、「繰り返し」頻度、「スケジュールの基準」 (日、週、または月単位)、「開始時刻のスケジュール設定」を定義します。ボックスにチェック・マークを付けて、従属ジョブを自動実行します。
7. 「保存」をクリックして変更をコミットするか、「リセット」をクリックしてフィールドをクリアします。

ポリシーのアラートが syslog に送られるようにするため、syslog への通知の送信をトリガーするように、例外ルール、アクセス・ルール、および抽出ルールを変更しなければなりません。このアクションは、「ポリシー・ビルダー」に移動することで行うことができます。ポリシー・ルールは、E メールで送信、または syslog に送信して転送することが可能です。

1. 「設定」 > 「ツールとビュー」 > 「ポリシー・ビルダー」をクリックして、ポリシー・ビルダーを開きます。
2. 目的のポリシーを選択して、「ルールの編集」をクリックします。
3. 「ルールの追加...」 > 「例外ルールの追加」をクリックします。
4. 「記述」、「カテゴリー」、「分類」に入力し、ドロップダウン・リストから「重大度」レベルを選択します。

「ポリシー違反」レポートは、レポート期間中にログに記録されるすべてのポリシー・ルール違反について、 「ポリシー・ルール違反」エンティティーからのタイム・スタンプ、 アクセス・ルールの記述、クライアント IP、サーバー IP、データベース・ユーザー名、 「ポリシー・ルール違反」エンティティーからの SQL 文字列全体、重大度の記述、 およびその行の違反数を提供します。このレポートを使用することで、違反をグループにしてインシデントを作成し、各違反の重大度を設定して、インシデントをユーザーに割り当てることができます。

親トピック: 製品の統合

InfoSphere Discovery に機密データを転送する方法

IBM Security Guardium で識別および分類された機密データ情報を取得し、その情報を InfoSphere® Discovery に転送します。

IBM Guardium と InfoSphere Discovery にはどちらにも、社会保障番号、クレジット・カード番号などの機密データを識別し、分類する機能があります。

IBM Guardium 製品のカスタマーは、双方向インターフェースを使用して、識別された機密データ情報を一方の製品から他方の製品に転送できます。

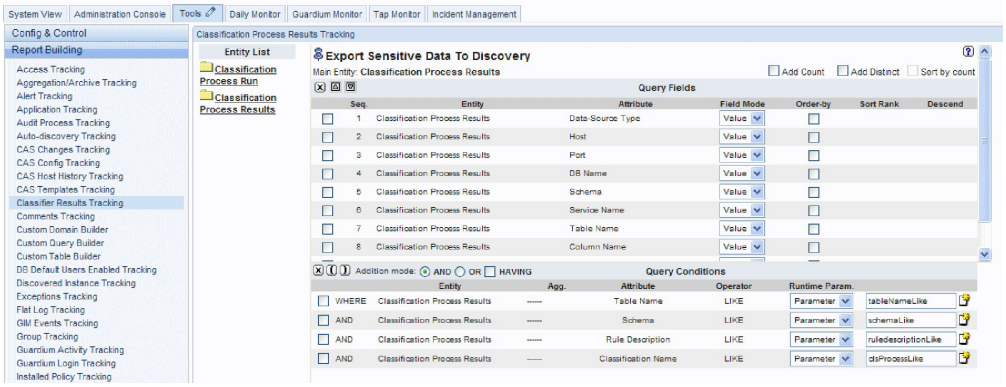
注: IBM Guardium では、分類プロセスは、定期的に実行される継続プロセスです。InfoSphere Discovery では、分類は、通常 1 回実行されるディスカバリー・プロセスの一部です。
注: このデータは CSV ファイルを介して転送されます。

エクスポート/インポート手順の概要を以下に示します。

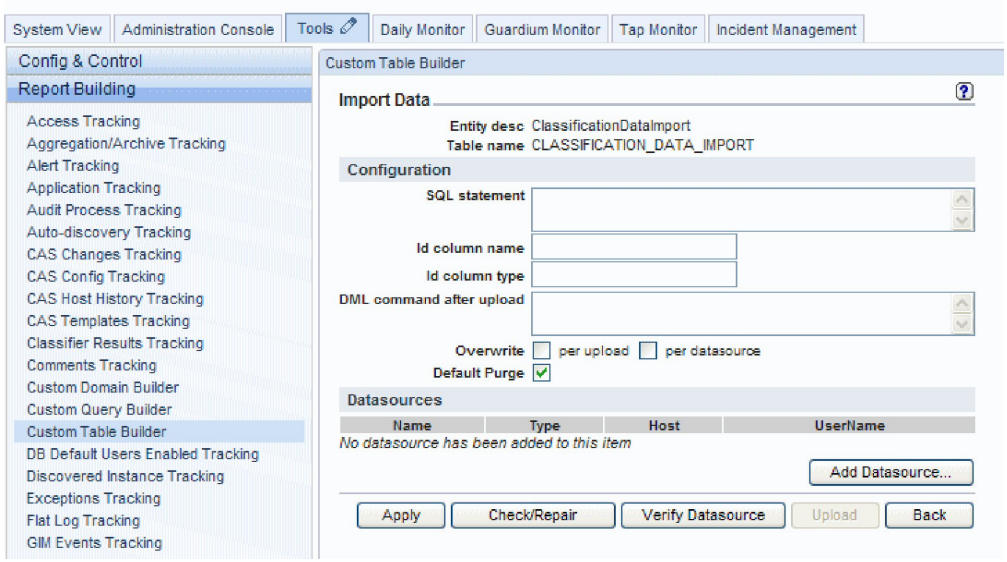
- Guardium からのエクスポート - 定義済みレポートを実行し (「Discovery への機密データのエクスポート」)、CSV ファイルとしてエクスポートします。
- Guardium へのインポート - CSV データ・ソースに対してカスタム表をロードします。このデータ・ソースに対してデフォルト・レポートを定義します。

以下の手順を行います。

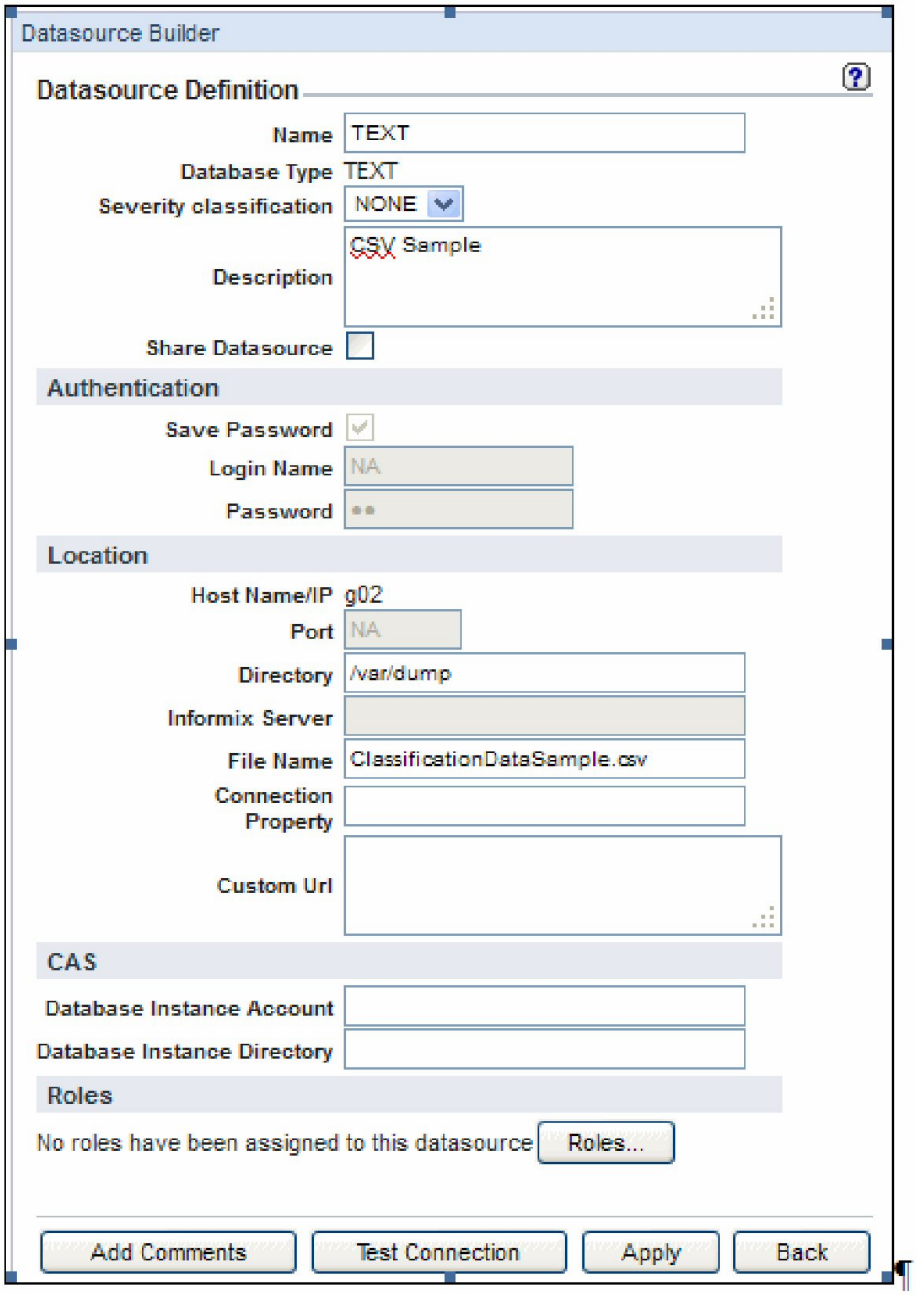
1. Guardium からのエクスポート - IBM Guardium から InfoSphere Discovery に分類データをエクスポートします。
2. Guardium® アプリケーションで admin ユーザーとして、「ツール」 > 「レポートのビルド」 > 「分類結果のトラッキング」 > 「レポートの選択」 > 「Discovery への機密データのエクスポート」に移動します (スクリーン・ショットを参照)。
   注: このレポートを UI ペインに追加します (これはデフォルトでは行われません)。



3. 「レポート結果」画面で「カスタマイズ」アイコンをクリックし、検索条件を指定して、Discovery に転送する分類結果データをフィルターに掛けます。
4. レポートを実行し、「レコードをすべてダウンロード」アイコンをクリックします。
5. CSV として保存し、このファイルを InfoSphere Discovery の指示に従い Discovery にインポートします。
6. Guardium にインポート- InfoSphere Discovery から IBM Guardium に分類データをインポートします。
7. InfoSphere Discovery の指示に基づき、InfoSphere Discovery から分類データを CSV としてエクスポートします。
8. Guardium アプリケーションで admin ユーザーとして、「ツール」 > 「レポートのビルド」 > 「カスタム表」画面に移動し、「分類データのインポート」を選択し、「データのアップロード」ボタンをクリックします。(スクリーン・ショットを参照)。



9. 「データのアップロード」画面で、「データ・ソースの追加」をクリックし、「新規作成」ボタンをクリックし、新規データ・ソースとして Discovery からインポートする CSV ファイルを定義します (「データベース・タイプ」=「テキスト」)。CSV データ・ソース定義の次のスクリーン・ショットを参照してください。



注: または、Discovery データベースおよび分類結果データにアクセスする方法が判明している場合、Discovery データベースからデータを直接ロードできます。

10. データ・ソースとして CSV を定義した後、「データ・ソース・リスト」画面で「追加」ボタンをクリックします。
11. 「データのアップロード」画面で、「データ・ソースの検査」、「適用」の順にクリックします。
12. 「今すぐ 1 回実行」ボタンをクリックして CSV からデータをロードします。
13. 「レポート・ビルダー」に移動し、「分類データのインポート」レポートを選択し、「ペインに追加」をクリックしてそのレポートをポータルに追加し、そのレポートに移動します。
14. レポートにアクセスし、「カスタマイズ」をクリックして開始日付/終了日付を設定し、レポートを実行します。

レポート結果には、InfoSphere Discovery からインポートされた分類データが含まれます。ダブルクリックして、このレポートに割り当てられている API を呼び出します。Discovery からインポートしたデータは以下の目的で使用できます。

- 結果セットに基づき新規データ・ソースを追加する。
- 機密データ・グループを追加/更新する。
- データ・ソースおよび機密データの詳細に基づきポリシー・ルールを追加する。
- プライバシー・セットを追加する。

表 1. CSV インターフェース・シグニチャー

インターフェース・シグニチャー	例
タイプ	DB2®
ホスト	9.148.99.99
ポート	50001

インターフェース・シグニチャー	例
dbName (DB2 または Oracle のスキーマ名、またはその他のデータベース名)	cis_schema
データ・ソースの URL	
表名	MK_SCHED
列名	ID_PIN
分類名	SSN
ルールの記述	InfoSphere Discovery のすぐに使用可能なアルゴリズム
HitRate	70% - Guardium バージョン 8.2 ではエクスポートで使用不可
使用しきい値	60% - Guardium バージョン 8.2 ではエクスポートで使用不可

親トピック: 製品の統合

CEF マッピング

ArcSight の CEF 標準は、一連の必須フィールドと、一連のオプション・フィールドを定義しています。

後者は CEF 標準では、拡張と呼ばれます。 データは、Guardium® 構成情報およびレポートからこれらのフィールドにマップされます。すべての Guardium フィールドが CEF フィールドにマップされるわけではないため、印刷レポートの行とそのレポートから作成した CEF ファイルの間では 1 対 1 の関係にならない可能性があることに注意してください。 またこの機能の意図としては、データ・アクセス・ドメイン (例えば、データ・アクセス、例外、ポリシー違反など) のデータをマップすることであって、Guardium 自己モニター・ドメイン (統合/アーカイブ、監査プロセス、Guardium ログインなど) のデータのマップではないことにも注意してください。

注: 分析済みのクライアント IP には CEF ソース用のマップがあります。CEF で使用される照会内にクライアント IP が指定されておらず、分析済みのクライアント IP が指定されている場合、分析済みのクライアント IP がソースに対して使用されます。クライアント IP と分析済みのクライアント IP の両方が照会内に指定されている場合、クライアント IP が優先されます。

下記の表に示す CEF フィールドは常に存在します。

表 1. 必須の CEF フィールドのマッピング

CEF フィールド	Guardium マッピング
バージョン	0 (ゼロ)。現在 CEF フォーマットの唯一のバージョン
Device Vendor	Guardium
Device Product	Guardium
Device Version	Guardium ソフトウェアのバージョン番号
Signature ID	ReportID
名前	レポート・タイトル
重大度	0 から 10 までの範囲の数値の重大度コード。10 が最重要なイベントです。 レポートで再設定されていなければ 0 (このゼロは、Guardium では情報に変換されます)。

CEF 拡張フィールドはオプションであり、マッピングが適用される場合にのみ存在します。 例えば、レポートにアクセス・ルールの記述が含まれていない場合、act フィールド (最初の拡張フィールド) は存在しません。 Guardium のエンティティーと属性について詳しくは、該当するエンティティー・リファレンスのトピックを参照してください。

表 2. CEF マッピング、Guardium バージョン 8.2

CEF フィールド	エンティティー	属性
severity	ポリシー・ルール違反	重大度
act	ポリシー・ルール違反	アクセス・ルールの記述
app	クライアント/サーバー	データベース・プロトコル
app	例外	データベース・プロトコル
dst	クライアント/サーバー	サーバー IP
dst	例外	宛先アドレス
dhost	クライアント/サーバー	サーバー・ホスト名
dpt	セッション	サーバー・ポート
dpt	例外	宛先ポート
dproc	クライアント/サーバー	ソース・プログラム
duid	クライアント/サーバー	OS ユーザー
duser	クライアント/サーバー	データベース・ユーザー名
duser	例外	ユーザー名
end	例外	例外タイム・スタンプ
end	ポリシー・ルール違反	タイム・スタンプ
end	アクセス期間	期間の終了

CEF フィールド	エンティティー	属性
end	セッション	セッション終了
msg	例外	例外の記述
msg	メッセージ・テキスト	メッセージ・テキスト
msg	メッセージ・テキスト	メッセージ件名
src	クライアント/サーバー	クライアント IP
src	クライアント/サーバー	分析されたクライアント IP
src	例外	ソース・アドレス
shost	クライアント/サーバー	クライアント・ホスト名
smac	クライアント/サーバー	クライアント MAC
spt	セッション	クライアント・ポート
spt	例外	ソース・ポート
start	例外	例外タイム・スタンプ
start	ポリシー・ルール違反	タイム・スタンプ
start	アクセス期間	期間の開始
start	セッション	セッション開始
proto	クライアント/サーバー	ネットワーク・プロトコル
request	完全な SQL	完全な SQL
request	SQL	SQL
cs1	セッション	Uid チェーン
cs2	セッション	Uid チェーン圧縮

表 3. CEF マッピング、Guardium バージョン 9.0

CEF フィールド	エンティティー	属性
severity	ポリシー・ルール違反	重大度
act	ポリシー・ルール違反	アクセス・ルールの記述
app	クライアント/サーバー	データベース・プロトコル
app	例外	データベース・プロトコル
dst	クライアント/サーバー	サーバー IP
dst	例外	宛先アドレス
dhost	クライアント/サーバー	サーバー・ホスト名
dpt	セッション	サーバー・ポート
dpt	例外	宛先ポート
dproc	クライアント/サーバー	ソース・プログラム
duid	クライアント/サーバー	OS ユーザー
duser	クライアント/サーバー	データベース・ユーザー名
duser	例外	ユーザー名
end	例外	例外タイム・スタンプ
end	ポリシー・ルール違反	タイム・スタンプ
end	アクセス期間	期間の終了
end	セッション	セッション終了
msg	例外	例外の記述
msg	メッセージ・テキスト	メッセージ・テキスト
msg	メッセージ・テキスト	メッセージ件名
src	クライアント/サーバー	クライアント IP
src	クライアント/サーバー	分析されたクライアント IP
src	例外	ソース・アドレス
shost	クライアント/サーバー	クライアント・ホスト名
smac	クライアント/サーバー	クライアント MAC
spt	セッション	クライアント・ポート
spt	例外	ソース・ポート
start	例外	例外タイム・スタンプ

CEF フィールド	エンティティー	属性
start	ポリシー・ルール違反	タイム・スタンプ
start	アクセス期間	期間の開始
start	セッション	セッション開始
proto	クライアント/サーバー	ネットワーク・プロトコル
request	完全な SQL	完全な SQL
request	SQL	SQL
cs1	セッション	Uid チェーン
cs2	セッション	Uid チェーン圧縮

CEF に関する詳細については、Web で Common Event Format: Event Interoperability Standard を検索するか、ArcSight の Web サイト www.arcsight.com にアクセスしてください。

親トピック: 製品の統合

LEEF マッピング

QRadar からの Log Event Extended Format (LEEF)

LEEF フォーマットは、オプションの syslog ヘッダー、LEEF ヘッダー、およびそのイベントについて記述した属性のコレクションで構成されます。

Syslog_Header (オプション) LEEF_Header|Event_Attributes

LEEF ヘッダーは、パイプ (「|」) で区切られ、属性はタブで区切られます。

例

Jan 18 11:07:53 host LEEF:Version|Vendor|Product|Version|EventID|Key1=Value1<tab>Key2=Value2<tab>Key3=Value3<tab>...<tab>KeyN=ValueN

表 1. LEEF パラメーター

パラメーター	記述
LEEF: バージョン	そのログ・メッセージに使用された LEEF のバージョンを識別する、バージョンの整数。
ベンダー	イベント・ログを送信したデバイスまたはアプリケーションのベンダーを識別するストリング。
製品	そのイベント・ログを送信した製品を識別する製品ストリング。注: ベンダーと製品の組み合わせは固有のものでなければなりません。
バージョン	イベント・ログを送信したデバイスまたはアプリケーションのバージョンを識別するストリング。
イベント ID	イベントを一意的に識別する ID。
属性 1..N	タブ文字で区切られた、イベントのキー値ペア属性のセット。順序は強制されません。 事前定義のキーのセットを定義し、使用できるときに使用する必要があります。 LEEF フォーマットは拡張可能です。また、イベント・ログに追加のキー値ペアを追加することができます。 キーにスペースまたは等号を含めることはできません。 値にタブを含めることはできません。

例:

```
Jan 18 11:07:53 192.168.1.1 LEEF:1.0|QRadar|QRM|1.0|NEW_PORT_DISCOVERD|src=172.5.6.67 dst=172.50.123.1 sev=5 cat=anomaly msg=there are spaces in this message
```

文字エンコード

UTF8

定義済みの属性

表 2. 定義済みの属性

キー名	データ・タイプ	最大長	記述
Cat	ストリング		イベント・カテゴリー
devTime	日付		デバイスまたはアプリケーションがイベントを発行した時間
devTimeFormat	ストリング		Java SimpleDateFormat によって定義されます。これは、カスタマイズした日付形式を使用している場合のみ必須です。詳しくは、日付形式のセクションを参照してください。
proto	整数		トランスポート・プロトコル
sev	整数 (1 から 10)		このイベントの重大度
src	IPv4 または IPv6 アドレス		ソース・アドレス

キー名	データ・タイプ	最大長	記述
dst	IPv4 または IPv6 アドレス		宛先アドレス
VSrc	IPv4 または IPv6 アドレス		バーチャル・ソース・アドレス
srcPort	整数		ソース・ポート。有効なポート番号は 0 から 65535 までです。
dstPort	整数		宛先ポート。有効なポート番号は 0 から 65535 までです。
srcPreNat	IPv4 または IPv6 アドレス		ネットワーク・アドレス変換 (NAT) が発生する前のメッセージのソース・アドレス。
dstPreNat	IPv4 または IPv6 アドレス		ネットワーク・アドレス変換 (NAT) が発生する前のメッセージの宛先アドレス。
srcPostNat	IPv4 または IPv6 アドレス		ネットワーク・アドレス変換 (NAT) が発生した後のメッセージのソース・アドレス。
dstPostNat	IPv4 または IPv6 アドレス		ネットワーク・アドレス変換 (NAT) が発生した後のメッセージの宛先アドレス。
usrName	ストリング	255	イベントに関連付けられたユーザー名。
srcMAC	MAC アドレス		コロンで区切られた 6 つの 16 進数。 例: `1:2D:67:BF:1A:71`
dstMAC	MAC アドレス		コロンで区切られた 6 つの 16 進数。 例: `11:2D:67:BF:1A:71`
srcPreNATPort	整数		ソース・ポート。有効なポート番号は 0 から 65535 までです。
dstPreNATPort	整数		宛先ポート。有効なポート番号は 0 から 65535 までです。
srcPostNATPort	整数		ソース・ポート。有効なポート番号は 0 から 65535 までです。
dstPostNATPort	整数		宛先ポート。有効なポート番号は 0 から 65535 までです。
identSRC	IPv4 または IPv6 アドレス		
identHostName	ストリング	255	イベントに関連したホスト名。通常、このパラメーターは、ID イベントにのみ関連します。
identNetBios	ストリング	255	イベントに関連した NetBIOS 名。通常、このパラメーターは、ID イベントにのみ関連します。
identGrpName	ストリング	255	レコードに関連したイベント名。通常、このパラメーターは、ID イベントにのみ関連します。

カスタム属性

一部のケースでは、生成中のイベントに関する詳細を識別するために、カスタム属性が必要になる可能性があります。これらのケースでは、ベンダーが独自のカスタム属性を定義し、それらのカスタム属性をイベント・ログに組み込む場合があります。カスタム属性フィールドは、定義済みのフィールドへの受け入れ可能なマッピングが存在しない場合にのみ使用してください。

カスタム属性キーは以下のようになっている必要があります。

- スペースのない単一ワード
- 英数字
- 明快かつ簡潔
- 定義済みの属性キーと同じ名前を付けることはできない

カスタム属性は、カスタム・プロパティーを作成することによって、QRadar イベント・ビューアーでの表示に使用される可能性があります。

カスタム属性は、顧客プロパティーを作成することで、QRadar レポート・エンジンによって使用される可能性があります。

カスタム属性をイベント相関に使用することはできません。

注: MS-SQL データベース名を取り込むには、databaseName=%%DBname を LEEF テンプレートに追加します。既存の LEEF テンプレートを更新するか、クローン作成によって新規テンプレートを作成します。

日付形式

以下の事前定義形式のいずれかを使用できます。

1. 1970 年 1 月 1 日からのミリ秒 (整数)
2. MMM dd yyyy HH:mm:ss (例えば Jun 06 2012 16:07:36)
3. MMM dd yyyy HH:mm:ss.SSS (例えば Jun 06 2012 16:07:36.300)
4. MMM dd yyyy HH:mm:ss.SSS zzz (例えば Jun 06 2012 02:07:36.300 GMT)

これらの形式が適さない場合は、dTimeFormat キーを使用して日付形式を指定することで、dTime フィールドでカスタム日付形式を定義することができます。

日付形式の指定について詳しくは、SimpleDateFormat のページ (http://java.sun.com/javase/6/docs/api/java/text/SimpleDateFormat.html) を参照してください。

親トピック: 製品の統合

問題のトラブルシューティング

IBM 製品の問題を切り分けて解決するために、トラブルシューティングとサポートの情報を使用することができます。 この情報には、IBM Guardium を含む IBM 製品に付属する問題判別リソースの使用方法が掲載されています。

- 問題のトラブルシューティング手法
  *トラブルシューティング*は、問題解決のための系統的なアプローチです。 トラブルシューティングの目的は、ある部分が予期したとおりに機能しない理由および問題を解決する方法を判別することです。確立されている一般的な手法でタスクのトラブルシューティングを行うことができます。
- 問題および解決策
  このトピックで、発生した問題の解決策を検索してください。

問題のトラブルシューティング手法

*トラブルシューティング*は、問題解決のための系統的なアプローチです。 トラブルシューティングの目的は、ある部分が予期したとおりに機能しない理由および問題を解決する方法を判別することです。確立されている一般的な手法でタスクのトラブルシューティングを行うことができます。

トラブルシューティング・プロセスの最初のステップは、問題を完全に記述することです。問題を記述することで、ユーザーと IBM 技術サポート担当者が、問題の原因をどこから探し始めるか認識しやすくなります。このステップでは、次の基本的な質問をご自身で検討します。

- 問題の症状はどのようなものか。
- 問題が発生する場所はどこか
- 問題が発生したのはいつか。
- どのような条件下で問題が発生するか
- 問題を再現できるか。

通常は、これらの質問に回答することで問題が適切に記述され、問題解決につながります。

問題の症状はどのようなものか。

問題は何か。この質問は単純なように思われますが、これをいくつかのさらに絞り込んだ質問に分解し、問題をさらに具体的に記述することができます。次のような質問が考えられます。

- 誰が、または何が問題を報告しているか。
- どのようなエラー・コードまたはメッセージが出ているか。
- どのような障害がシステムに起こったか。例えば、ループ、ハング、異常終了、性能低下、結果が正しくない、など。

問題が発生する場所はどこか

問題がどこで発生しているかの判断は、簡単にできるとは限りませんが、問題解決のための最も重要なステップの 1 つです。問題を報告しているコンポーネントと障害が起こっているコンポーネントの間には、多数のテクノロジー層が存在することがあります。問題を調査するときは、ネットワーク、ディスク、ドライバーを始めとして多くのコンポーネントを考慮する必要があります。

問題が発生している部分に焦点を当てて問題となっているレイヤーを切り分ける上で、次の質問が役立ちます。

- 問題は 1 つのプラットフォームまたはオペレーティング・システムに固有か、それとも複数のプラットフォームまたはオペレーティング・システムに共通か。
- 現在の環境および構成がサポートされているか。
- ユーザー全員に問題が発生しているか。
- (マルチサイト・インストール済み環境の場合。)すべてのサイトに問題が発生しているか。

ある層で問題が報告されたとしても、必ずしもその層内で問題が発生しているとは限りません。問題がどこで発生したかを突き止めるには、問題が存在する環境を理解することが不可欠です。しばらく時間を割いて、問題の環境を完全に記述してください。これにはオペレーティング・システムとそのバージョン、対応するすべてのソフトウェアとそのバージョン、およびハードウェア情報を含める必要があります。サポートされている構成の環境で実行していることを確認してください。問題の多くは、ソフトウェアのレベルが非互換 (一緒に実行することが意図されていないソフトウェアまたはその組み合わせでのテストが完全になされていないソフトウェア) であることが原因で生じている可能性があります。

問題が発生したのはいつか。

障害に至るまでのイベント (特に発生が 1 回限りのイベント) の詳しい時系列表を作成してください。最も簡単に時系列表を作成する方法は、逆方向にたどることです。エラーが報告された時点 (ミリ秒単位に至るまで可能な限り精密に) から開始して、使用可能なログと情報を通じて逆方向にたどります。通常、確認する必要があるのは、診断ログで見つけた最初の疑わしいイベントまでの部分のみです。

イベントの詳細な時刻表を作成するには、以下の質問に答えてください。

- 問題が発生するのは、日中または夜間の特定の時刻のみか。
- 問題が発生する頻度はどの程度か。
- 問題が報告された時刻までにイベントがどのような順序で発生したか
- 問題が発生したのは環境変更 (ソフトウェアまたはハードウェアのアップグレードまたはインストールなど) の後か。

このような質問に回答することで、問題を調査するための基準枠を設定できます。

どのような条件下で問題が発生するか

問題が発生したときに実行中だったシステムおよびアプリケーションがどれかを知ることは、トラブルシューティングの重要部分です。お客様の環境に関する以下の質問は、問題の根本原因を識別するために役立ちます。

- 問題は同じタスクの実行中に常に起こるか
- 特定の一連のイベントが発生した場合にのみ、その問題が発生するか
- ほかのアプリケーションにも同時に障害が起こるか。

これらのタイプの質問に回答することは、問題が発生している環境を説明し、依存関係の相関付けをするのに役立ちます。ほぼ同時に複数の問題が発生したとしても、それらの間に関連があるとは限らないことに注意してください。

問題を再現できるか。

トラブルシューティングの観点からすると、理想的な問題とは、再現できる問題であるということです。通常、問題を再現できる場合は、調査に役立てるために自由に使用できるツールまたは手順の数が多くなります。そのため、再現できる問題は多くの場合、デバッグや解決がより容易です。

しかし、問題を再現できることが、デメリットになることもあります。問題がビジネスに大きな影響を及ぼす場合は、問題が再発するのは望ましくありません。可能な場合は、テスト環境または開発環境で問題を再現してください。通常、そのような環境では、より柔軟で制御の利いた調査ができます。

- 問題をテスト・システムで再現することができるか。
- 複数のユーザーまたはアプリケーションで、同じタイプの問題が検出されているか。
- 1 つのコマンド、一連のコマンド、または特定のアプリケーションを実行することで、問題を再現できるか。

- Fix Central からのフィックスの入手
  Fix Central を使用して、Guardium を含むさまざまな製品について、IBM サポートが推奨するフィックスを見つけることができます。Fix Central では、ご使用のシステム用のフィックスを検索、選択、注文、およびダウンロードすることができ、その際に配信オプションを選択できます。以下は英語のみの対応となります。 お客様の問題の解決に、プロダクトのフィックスが有効な場合があります。
- IBM サポートへの問い合わせ
  IBM サポートでは、製品の問題に関する支援や、よくある質問への回答、製品の問題のユーザーによる解決のための支援を提供します。
- IBM サポートのための基本情報
  IBM サポートに連絡する前に、IBM Guardium (コレクター、アグリゲーター、中央マネージャー、UNIX/Linux S-TAP、Windows S-TAP) に関する基本情報を収集します。
- IBM との情報の交換
  問題を診断または特定するために、システムのデータおよび情報を IBM サポートに提供する必要がある場合があります。問題判別に使用するツールまたはユーティリティーを IBM サポートから提供される場合もあります。
- サポート更新のサブスクライブ
  使用する IBM 製品に関する重要な情報を常に入手するために、更新にサブスクライブできます。

親トピック: 問題のトラブルシューティング

Fix Central からのフィックスの入手

Fix Central を使用して、Guardium を含むさまざまな製品について、IBM サポートが推奨するフィックスを見つけることができます。Fix Central では、ご使用のシステム用のフィックスを検索、選択、注文、およびダウンロードすることができ、その際に配信オプションを選択できます。以下は英語のみの対応となります。 お客様の問題の解決に、プロダクトのフィックスが有効な場合があります。

このタスクについて

手順

フィックスを見つけてインストールするには、次のようにします。

1. フィックスを入手するために必要なツールを取得します。インストールされていない場合は、 製品の更新インストーラーを入手します。このインストーラーは、Fix Central からダウンロードできます。 このサイトには、更新インストーラーのダウンロード、インストール、および構成の手順が示されています。
2. 製品として Guardium を選択し、 解決する問題に関連したチェック・ボックスを 1 つ以上選択します。
3. 必要なフィックスを特定して選択します。
4. フィックスをダウンロードします。
   a. ダウンロード・マニュアルを開き、Download package セクション内のリンクに従います。
   b. ファイルをダウンロードするときに、メンテナンス・ファイルの名前が変更されていないことを確認してください。 この変更は意図的である場合や、特定の Web ブラウザーやダウンロード・ユーティリティーに起因する意図しない変更である場合があります。
5. フィックスを適用します。
   a. ダウンロード資料の『Installation Instructions』セクションに記載されている説明に従ってください。
   b. 詳しくは、製品資料のトピック『更新インストーラーを使用したフィックスのインストール』を参照してください。
6. オプション: フィックスおよびその他の IBM サポートの更新に関する電子メール通知を毎週受信するようにサブスクライブします。

親トピック: 問題のトラブルシューティング手法

IBM サポートへの問い合わせ

IBM サポートでは、製品の問題に関する支援や、よくある質問への回答、製品の問題のユーザーによる解決のための支援を提供します。

始める前に

技術情報などのその他の自己解決型の選択肢を使用して答えまたは解決策を見つけようとした後に、IBM サポートに問い合わせることができます。 IBM サポートにお問い合わせいただくには、会社または組織が有効な IBM *保守契約名*を保持し、お問い合わせいただくユーザーが IBM に問題を送信する権限を持っている必要があります。利用できるサポートの種類については、「"*Software Support Handbook*"」の『Support portfolio』トピックを参照してください。

手順

問題について IBM サポートに問い合わせるための手順は以下のとおりです。

1. 問題を明確にし、バックグラウンド情報を収集して、問題の重大度を判別します。 詳細については、「*Software Support Handbook*」の『Getting IBM support』のトピックを参照してください。

2. 診断情報を収集します。
3. 以下のいずれかの方法で、IBM サポートに問題を報告します。
   - IBM サポート・ポータルからオンラインで報告:「サービス・リクエスト」ページの「サービス・リクエスト」ポートレットから、お客様のすべてのサービス要求を開いて更新、表示することができます。
   - 電話: お客様の地域の連絡先電話番号については、Directory of worldwide contacts の Web ページを参照してください。

タスクの結果

ユーザーが提出した問題が、ソフトウェア障害または資料の不正確や欠落が原因である場合、IBMサポートがプログラム診断依頼書 (APAR) を作成します。 APAR では問題を詳細に記述します。 IBM Support は、APAR が解決されてフィックスが 配信されるまで、ユーザーが実施できる次善策を可能な限り提供します。 IBM は、解決された APAR を IBM サポート Web サイトに毎日公開し、同じ問題を経験した他のユーザーが、同じ解決方法を利用できるようにしています。

親トピック: 問題のトラブルシューティング手法

関連情報:

サポート・チケット (PMR) にデータをアップロードする方法 (ビデオ)

Guardium のトラブルシューティングおよびサポート (ビデオ)

IBM サポートのための基本情報

IBM サポートに連絡する前に、IBM Guardium (コレクター、アグリゲーター、中央マネージャー、UNIX/Linux S-TAP、Windows S-TAP) に関する基本情報を収集します。

support must_gather commands を使用します。これを CLI を通じて実行すると、任意の Guardium システムの状態に関する特定の情報を生成することができます。この情報は、Guardium GUI を介して収集することもできます。

この情報は、問題管理レポート (PMR) が記録されているときであればいつでも、Guardium システムからアップロードして IBM サポートに送信できます。

サポート情報の結果の収集

サポート情報を収集するには、「管理」 > 「メンテナンス」 > 「サポート情報の結果」をクリックします。以下のセクションの内容を実行します。

1. サポート情報収集セッションを記述します。
2. PMR 番号を入力します。
3. E メール・アドレスに結果を送信するには、「E メール:」を指定し、E メール・アドレスを入力します。
4. カレンダー・アイコンをクリックして、開始時刻をスケジュールします。
5. 以下のカテゴリーに関連する Must Gather ログ情報をチェックします。
   - 統合
   - ユーザー・インターフェース
   - backup
   - データベース・ユーザー
   - Scheduler
   - システム DB
   - ネットワーク
   - 適用状態
   - アラート
   - 監査
   - 中央マネージャー
   - パージ
   - スニファー
   - パッチ・インストール
   - 高度な脅威スキャン
   - 資格最適化
6. 情報を収集する対象となる特定の期間を示す値 (分) を入力します。デフォルト値は 10 分です。この値は、ログが収集される期間です。E メールを指定した場合、プロセスを開始した時刻から 10 分間ログが収集され、その後 E メールが送信されます。問題のトラブルシューティングに必要なデバッグ情報が、ログに含まれるようにするために、問題を再現し、指定された期間中のログ情報を生成する必要があります。
7. 結果ログ・ファイルに表示される最大行数を入力します。
8. 構成が終了したら、「開始」をクリックします。
9. 「サポート情報の結果」に移動して、結果を表示します。.tgz ファイルを開くか、または保存することができます。

CLI を使用した Guardium アプライアンスの Must Gather

IBM Guardium のコレクター、アグリゲーター、中央マネージャー

must_gather コマンドは、ユーザーが CLI を通じていつでも実行できます。以下の手順を実行します。

1. 問題のコレクター、アグリゲーターまたは中央マネージャーに対して Putty セッション (または同様のセッション) を開きます。
2. ユーザー `cli` でログインします。
3. 問題のタイプに応じて、適切な must_gather コマンドを CLI プロンプトに貼り付けます。問題を診断するために、複数の must_gather コマンドが必要となる場合があります。コマンドを、以下のリストに説明と共に示します。
   - support must_gather agg_issues (統合プロセス)
   - support must_gather alert_issues (アラート)
   - support must_gather app_issues (アプリケーション)
   - support must_gather audit_issues (監査プロセス)
   - support must_gather backup_issues (バックアップ・プロセス)
   - support must_gather cm_issues (中央マネージャー)
   - support must_gather datamining_issues (データ・マイニング)
   - support must_gather miss_dbuser_prog_issues (システム・データベース・ユーザー)

- support must_gather en (資格最適化)
- support must_gather network_issues (ネットワーク体系)
- support must_gather ocr_issues
- support must_gather patch_install_issues (パッチのインストールおよびアップグレード)
- support must_gather purge_issues (パージ・プロセス)
- support must_gather scheduler_issues (スケジューラー機能)
- support must_gather sniffer_issues (スニファー機能)
- support must_gather system_db_info (Guardium システムのデータベース・パフォーマンスまたは操作スペース・パフォーマンス)

出力は、以下の例のようなファイル名で must_gather ディレクトリーに書き込まれます。

must_gather/system_logs/.tgz

4. 結果の出力を IBM サポートに送信してください。

fileserver <ip address> を使用すると、.tgz ファイルをアップロードして、IBM サポートに送信できます。

E メールでファイルを送信するか、標準的なデータ・アップロードを使用して ECUREP にアップロードします。PMR 番号と、アップロードするファイルを指定します。

UNIX/Linux S-TAP の must gather

guard_diag スクリプトは、Guardium の診断に役立つ統計をサーバー上で作成します。

guard_diag の説明:

診断スクリプト (guard_diag)

概要:

GUI で S-TAP ロギングのレベルを 7 に設定すると /usr/local/guardium/guard_stap/guard_diag から実行される診断スクリプト (guard_diag) が付属するようになりました。S-TAP を実行しているマシンにこのスクリプトを転送することも可能です。

使用法: ./guard_diag output_dir

スクリプトが S-TAP のインストール場所を自動的に判別できない場合は、場所を尋ねるプロンプトが出されます。実行時間は約 1.5 分です。出力ディレクトリーを指定しない場合、スクリプトは、生成される .tar ファイルを /tmp に格納します。スクリプトが GUI からロギングを実行し、有効化する場合、.tar ファイルは /var/tmp に入れられます。

収集される一般システム・データ:

- Uname -a
- インストールされているカーネル・モジュールのリスト
- 1 つのサイクルの出力
- アップタイム
- プロセッサーの番号とタイプ
- 最新の syslog のダンプ
- Netstat 出力
- IPC リスト
- ディスクの空きの統計
- /etc/services のコピー
- /etc のディレクトリー・リスト
- さまざまなプラットフォーム固有の情報
- /etc/inittab の内容

収集される S-TAP データ:

- S-TAP バージョン
- guard_tap.ini の内容
- K-TAP デバイス・ノードでの ls -l
- S-TAP の 30 秒のトレース
- K-TAP 統計
- インストール・ディレクトリー内のすべてのファイルのリスト
- K-TAP khash
- K-TAP (2) および S-TAP (4) の詳細デバッグ・ログ

既知の問題:

- Tusc がすべての HP-UX オペレーティング・システムにインストールされているわけではないため、S-TAP PID をトレースできません。
- システムに gzip が必ずインストールされているとは限りません。圧縮 (最終的な拡張子は .tar.Z) することを試みますが、失敗した場合は .tar ファイルが出力ディレクトリーに格納されます。
- AIX での Topas 出力には制御コードが含まれており、エディターで開くとほとんど理解できなくなるため、端末で解釈するのが最善です。
- 非 root S-TAP には、診断スクリプトに関するいくつかの問題があります。
- Linux では、/var/log/messages は、root のみが読み取り可能です。
- 一部の Solaris オペレーティング・システムは、正しく構成されていない可能性があり、そのために netstat がエラーを表示します。
- 非 root ユーザーのパスはかなり基本的なものであり、その結果、一部のコマンドはまったく実行されない可能性があります。特に HP-UX の gzip で、この既知の問題が発生します。

サポートされているプラットフォーム:

- Linux

- HP-UX
- AIX
- Solaris

STAP に関する要件: なし

Linux に関する要件: なし

AIX に関する要件: topas

Solaris に関する要件: top、prtdiag、psrinfo

HP-UX に関する要件: tusc

Windows S-TAP の must gather

このスクリプトを実行すると、current ディレクトリー内に以下のテキスト・ファイルが生成されます。

- stap.txt
- tasks.txt
- system.txt
- evtlog.txt または evtlog2008.txt
- reg.txt

注:

1. この診断スクリプトは、どの S-TAP バージョンでも実行できます。
2. 診断スクリプトの名前を diag.bat に変更して、S-TAP のインストール・ディレクトリーの下に配置してください これにより、そのスクリプトを手動で実行できるようになります。診断情報を含むテキスト・ファイルが生成されます。
3. 結果を Guardium L3 Support または Research & Development に送信してください。

このスクリプトは以下のデータを収集します。

- %system%guard_tap.ini の内容
- Guardium S-TAP インストール・ログ
- すべての実行中のタスク
- インストールされている全カーネル・ドライバーのリスト
- システム情報ユーティリティーから収集される OS 情報
- ipconfig /all
- netstat -nao
- データベース・サーバーから Guardium システムへの ping と trace の結果
- guardium_stapr の CPU 使用量
- 全体のシステム CPU 使用量
- guardium_stapr のプロセス・ハンドル・カウントとメモリー使用状況
- S-TAP によって生成されるイベント・ログ・メッセージ
- システム・イベント・ログ・メッセージ
- 以下のレジストリー項目:
  - HKLMSOFTWAREMicrosoftWindowsCurrentVersionUninstall
  - HKLMSYSTEMCurrentControlSetServices
  - HKLMSYSTEMCurrentControlSetControlGroupOrderList
  - HKEY_LOCAL_MACHINESOFTWAREMicrosoftMSSQLServer

Must Gather の暗号化

「Must Gather の暗号化 (Encrypt Must Gather)」が、「グローバル・プロファイル」画面に追加されました。「グローバル・プロファイル」画面に移動するには、「設定」 > 「グローバル・プロファイル」をクリックします。デフォルトでは、クリアされています (暗号化しない)。これがクリアされている場合、Must Gather 出力は圧縮され、暗号化されません (現行の機能)。チェック・ボックスにチェック・マークが付けられている場合、以降のすべての Must Gather 出力は暗号化されます。暗号化は、store encrypt_must_gather on CLI コマンドによって設定したり、store encrypt_must_gather off コマンドによってクリアしたりすることもできます。

GuardAPI の must gather

GuardAPI コマンドを使用して、スクリプトから GuardAPI Must Gather 情報収集を実行します。

grdapi must_gather --help=true。

以下の関数パラメーターがリストされます。

```
ID=0
function parameters :
commandsList - String -required - Constant values list
description - String
email - String
maxLogLength - Integer - Constant values list
pmrNumber - String
runDuration - Integer - Constant values list
startRun - Date
To get a Constant values list for a parameter, call the function with --get_param_values=<param-name>
```

--commandsList には文字列が必要です。--description も、必須の文字列です。--runDuration は、must_gather がどれだけの期間実行されるかを示します。must_gather レポートを送信する E メール・アドレスを入力します。--maxLogLength パラメーターは、ログ・レポートの最大長を設定する必須の整数です。--pmrNumber は、IBM サポートが顧客のレポートを追跡して解決するために使用する問題管理レポート番号です。--startRun は、必須の日付 (now など) です。grdapi must_gather --get_param_values=<param-name> 関数を呼び出すことによって、パラメーターごとの値のリストを取得することができます。

親トピック: 問題のトラブルシューティング手法
関連情報:
Guardium のトラブルシューティングおよびサポート (ビデオ)

IBM との情報の交換

問題を診断または特定するために、システムのデータおよび情報を IBM サポートに提供する必要がある場合があります。問題判別に使用するツールまたはユーティリティーを IBM サポートから提供される場合もあります。
親トピック: 問題のトラブルシューティング手法

IBM サポートへの情報の送信

問題解決に必要な時間を短縮するために、トレースおよび診断情報を IBM サポートに送信することができます。

手順

診断情報を IBM サポートに送信するには、次のようにします。

1. 問題管理レコード (PMR) を開きます。
2. 必要な診断データを収集します。診断データは、PMR を解決するまでの時間を短縮するのに役立ちます。診断データは、次のように手動でも自動でも収集できます。
   - データを手動で収集する。
   - データを自動的に収集する。
3. ファイルを .zip または .tar ファイル形式を使用して圧縮します。
4. ファイルを IBM に転送します。 以下のいずれかの方法を使用して、ファイルを IBM に転送できます。
   - サービス・リクエスト・ツール
   - 標準的なデータのアップロード方法: FTP、HTTP
   - セキュアなデータ・アップロード方法: FTPS、SFTP、HTTPS
   - E メール

   これらすべてのデータ交換方法については、IBM サポートの Web サイトで説明されています。

IBM サポートからの情報の受信

IBM 技術サポート担当者から、診断ツールやその他のファイルのダウンロードをお願いする場合があります。これらのファイルは FTP を使用してダウンロードできます。

始める前に

IBM 技術サポート担当者から、ファイルのダウンロードに使用する推奨サーバー、およびアクセスするディレクトリーとファイルの正確な名前について、必ず指定を受けてください。

手順

IBM サポートからファイルをダウンロードするには、次のようにします。

1. FTP を使用して、IBM 技術サポート担当者が指定したサイトに接続し、`anonymous` としてログインします。電子メール・アドレスをパスワードとして使用します。
2. 次のようにして、適切なディレクトリーに移動します。
   a. /fromibm ディレクトリーに移動します。

      ```
      cd fromibm
      ```

   b. IBM 技術サポート担当者が指定したディレクトリーに移動します。

      ```
      cd nameofdirectory
      ```

3. セッションでバイナリー・モードを有効にします。

   ```
   binary
   ```

4. get コマンドを使用して、IBM 技術サポート担当者が指定したファイルをダウンロードします。

   ```
   get filename.extension
   ```

5. FTP セッションを終了します。

   ```
   quit
   ```

サポート更新のサブスクライブ

使用する IBM 製品に関する重要な情報を常に入手するために、更新にサブスクライブできます。

このタスクについて

Guardium に関する更新を受け取るようにサブスクライブすることで、特定の IBM サポート・ツールおよびリソースに関する重要な技術情報と更新を受け取ることができます。次の 2 つの方法のうちいずれかを使用して、更新にサブスクライブできます。

RSS フィードとソーシャル・メディアのサブスクリプション

Guardium については、次の RSS フィードとソーシャル・メディアのサブスクリプションを利用できます。

- *RSS feed 1*
- *RSS feed 2*
- *RSS feed 3*

RSS に関する一般情報 (RSS を使用するための設定の手順や、RSS に対応した IBM Web ページのリストなど) については、IBM Software Support RSS feeds の Web サイトを参照してください。

My Notifications
「My Notifications」を使用すると、任意の IBM 製品のサポート更新にサブスクライブすることができます。(「My Notifications」は、これまでにご利用いただいた可能性のある類似のツール「My Support」に代わるものです。)「My Notifications」を利用すると、電子メールによる告知を毎日または毎週受け取るように指定できます。 また、受信する情報のタイプ (資料、ヒント、製品フラッシュ (アラートとも呼ばれる)、ダウンロード、およびドライバーなど) を指定できます。「My Notifications」を利用して、情報を受け取りたい製品やニーズに最適な配信方法を、カスタマイズしたりカテゴリー化したりすることができます。

手順

サポート更新にサブスクライブするには、以下の手順に従ってください。

1. Guardium RSS フィードをサブスクライブします。
2. IBM® サポート・ポータルにアクセスし、「通知」ポートレットの「My Notifications」をクリックすることによって、「My Notifications」にサブスクライブします。
3. IBM ID およびパスワードを使用してサインインし、「送信」をクリックします。
4. 更新を受け取る対象と方法を指定します。
    a. 「サブスクライブ」タブをクリックします。
    b. 該当するソフトウェア・ブランドまたはハードウェアのタイプを選択します。
    c. 1 つ以上の製品名を選択して、「続行」をクリックします。
    d. 更新を受け取る方法 (電子メールで受信、指定したフォルダーにオンライン受信、RSS または Atom フィードとして受信) の設定を選択します。
    e. 例えば、製品ダウンロードについての新しい情報とディスカッション・グループのコメントなど、受け取る資料の更新のタイプを選択します。
    f. 「送信」をクリックします。

タスクの結果

RSS フィードと My Notifications の設定を変更するまで、要求した更新情報に関する通知を受け取ることになります。設定は必要に応じて (ある製品の使用を中止して、別の製品の使用を開始する場合など) 変更できます。
親トピック: 問題のトラブルシューティング手法
関連情報
IBM Software Support RSS feeds
Subscribe to My Notifications support content updates
My Notifications for IBM technical support
My Notifications for IBM technical support overview

問題および解決策

このトピックで、発生した問題の解決策を検索してください。

- ユーザー・インターフェース
- ポリシー
- レポート
- 評価および強化
- Guardium システムの構成
- アクセス管理
- 統合
- 一元管理
- S-TAP およびその他のエージェント
- GIM
- ファイル・アクティビティーのトラブルシューティング
- Guardium システムのインストール

親トピック: 問題のトラブルシューティング

ユーザー・インターフェース

- 検査エンジンの追加時に変更内容が保存されない
  検査エンジンの追加時に変更内容が保存されない場合は、パラメーターが有効であることを確認します。
- HTTP エラー 403
  HTTP エラー 403 を受け取った場合は、Cross-Site Request Forgery (CSRF) 保護機構を無効にすると、このエラーを回避できます。
- Java.lang.IllegalStateException
  java.lang.IllegalStateException エラーを受け取った場合は、Java サーブレットをクリーンアップします。
- ページが正しくロードされない
  ページが正しくロードされない場合は、GUI を再始動するか、別のブラウザーを使用します。

親トピック: 問題および解決策

検査エンジンの追加時に変更内容が保存されない

検査エンジンの追加時に変更内容が保存されない場合は、パラメーターが有効であることを確認します。

症状

検査エンジンを追加したときに、新規の設定が数分間だけ残り、その後消失します。

原因

S-TAP 構成ファイル guard_tap.ini 内で、新規検査エンジンまたは別の検査エンジンの 1 つ以上のパラメーター値にエラーがあります。

環境

Guardium コレクター・ユーザー・インターフェースが影響を受けます。

問題の解決

検査エンジンに設定する必要のあるすべてのパラメーターに、有効な値が設定されていることを確認してください。例えば、一部のデータベース・タイプでは、db_install_dir を、サーバー上のインストール・ディレクトリーのパスに設定する必要があります。ただし、その他のデータベース・タイプでは、このパラメーターを設定してはならないか、または NULL に設定する必要があります。ご使用のデータベース・タイプに固有の要件を S-TAP ヘルプ・ブックでチェックし、すべてのパラメーターが正しく設定されていることを確認してください。

親トピック: ユーザー・インターフェース

HTTP エラー 403

HTTP エラー 403 を受け取った場合は、Cross-Site Request Forgery (CSRF) 保護機構を無効にすると、このエラーを回避できます。

症状

システムのメインページから IBM Security Guardium GUI をリフレッシュすると、以下のエラーを受け取ります。

```
HTTP Status 403-
type Status report
message
description Access to the specified resource () has been forbidden
```

原因

これは、Cross-Site Request Forgery (CSRF) を回避するように設計されている Guardium の機能が原因です。CSRF 保護は、デフォルトで有効になっています。

環境

すべての Guardium 構成 (コレクター、アグリゲーター、中央マネージャー) が影響を受けます。

問題の解決

この機能を無効にするには、CLI コマンド store gui csrf_status off を使用します。

注: CSRF 保護をオフにすると、Guardium システムのセキュリティー・レベルは低下します。

以下のコマンドによって、Cross-Site Request Forgery に対する保護が有効になります。デフォルトでは有効になっています。store gui csrf_status on

状況を確認するには、CLI コマンド show gui csrf_status を実行します。

親トピック: ユーザー・インターフェース

Java.lang.IllegalStateException

java.lang.IllegalStateException エラーを受け取った場合は、Java サーブレットをクリーンアップします。

症状

以下のエラー・メッセージを受け取ります。

エラーが発生しました。 システム管理者に連絡してください
(java.lang.IllegalStateException)

原因

このエラーが発生するのは、メソッドが呼び出され、Java VM がそのメソッドと不整合な状態である場合です。また、デッドロックが原因で Java サーブレットが破損している場合もあります。

環境

Guardium システムが影響を受けます。

問題の解決

数分待ってからやり直してください。エラーが続く場合は、ユーザー cli としてログインした後、コマンド restart GUI を実行して GUI を再始動します。

Java サーブレットをクリーンアップするには、コマンド support clean sevlets を実行します。

問題が解決しない場合は、以下の tomcat ログを収集し、IBM Security Guardium 技術サポートにお問い合わせください。

```
tomcat_log/localhost.<date_stamp>.log
tomcat_log/catalina.<date_stamp>.log
```

親トピック: ユーザー・インターフェース

ページが正しくロードされない

ページが正しくロードされない場合は、GUI を再始動するか、別のブラウザーを使用します。

症状

空白画面または別のエラーが表示されることがあります。この問題は特定のシステム上の特定のブラウザーで発生しますが、他では発生しません。

原因

この原因は、ローカライズされたブラウザーに限定されるか、Java 仮想マシンに問題がある可能性があります。

環境

コレクター、アグリゲーター、および中央マネージャーが影響を受けます。

問題の解決

問題を解決するには、Guardium システムで CLI プロンプトから restart GUI を実行します。それでも解決しない場合は、以下のアクションを試してください。

- システムを再始動します。
- Java 仮想マシンをアンインストールし、再インストールします。
- ブラウザーをアンインストールしてから、再インストールします。
- 異なるブラウザーを使用します。

親トピック: ユーザー・インターフェース

ポリシー

- 相関アラート定義内に照会が表示されない
  相関アラート定義内に照会が表示されない場合は、カウント・フィールドにチェック・マークを付けて、タイム・スタンプでソートします。
- ルールがトリガーされない
  ポリシー・コマンド・フィールドに値を持つルールが予期されるようにトリガーされない場合は、ルールを再構成します。
- 編集機能によって結果が過度にマスクされる
  編集機能によって結果が過度にマスクされる場合は、正規表現 [¥x0c]{1}[0-9]{8}([0-9]{4}) を使用します。
- Oracle データベースにログインする SSH セッションおよび自動化 CRON ジョブが失敗したログインとして表示される
  Oracle データベースにログインする SSH セッションおよび自動化 CRON ジョブが失敗したログインとして表示される場合は、ポリシーを修正します。
- Guardium 内部データベースがいっぱいになる
  Guardium 内部データベースがいっぱいになった場合は、手動で、または通常のパージ戦略の一環としてパージすることができます。

親トピック: 問題および解決策

相関アラート定義内に照会が表示されない

相関アラート定義内に照会が表示されない場合は、カウント・フィールドにチェック・マークを付けて、タイム・スタンプでソートします。

症状

相関アラートを作成するために、アクセス照会を作成しました。しかし、相関アラート定義内で、この照会はドロップダウン・リストに表示されません。

原因

レポートでの相関アラート検索は、タイム・スタンプに基づいています。

環境

コレクターおよびアグリゲーターが影響を受けます。

問題の解決

「カウントの追加」チェック・ボックスにマークを付け、タイム・スタンプでソートします。

親トピック: ポリシー

ルールがトリガーされない

ポリシー・コマンド・フィールドに値を持つルールが予期されるようにトリガーされない場合は、ルールを再構成します。

症状

ポリシーの「コマンド」フィールドに値を持つルールが予期されるようにトリガーされません。

原因

この原因は、コマンド・フィールドの構成の誤りです。 Guardium パーサーは、コマンド修飾子をコマンドの一部と見なしません。

環境

Guardium コレクター - ワイルドカード (%) を使用する場合、ポリシー・ルール内のコマンド・フィールドも影響を受けます。

問題の解決

ルールの「コマンド」フィールド内の値は、SQL 動詞に表示される値と正確に一致する必要があり、必要に応じてワイルドカード (%) が追加されます。正しい例は次のとおりです。

```
GRANT
GRANT%
```

この例は正しくありません。

```
GRANT% TO PUBLIC
%GRANT% ADMIN OPTION%
```

ADMIN OPTION と TO PUBLIC は一致せず、ルールをトリガーできません。これは、Guardium パーサーがこれらをコマンドの一部と認識しないためです。一般に、パーサーはコマンド修飾子をコマンドの一部と見なしません。 代わりに、ポリシーがモニターするトラフィックを調べるためのレポートを作成し、そのレポートにコマンド・エンティティーからの「SQL 動詞」フィールドを組み込みます。 「SQL 動詞」フィールドにリストされたものはすべてパーサーに認識され、ポリシー・ルールの「コマンド」フィールドに使用できます。複数のコマンドをグループに追加して、そのグループをルール内で単一コマンドの代わりに使用することができます。この場合、各グループ・メンバーは SQL 動詞内のエントリーに一致する必要があります。Guardium には、ユーザーが使用したりコピーを作成したりできるコマンド・グループがいくつかあります。
親トピック: ポリシー
親トピック: レポート

編集機能によって結果が過度にマスクされる

編集機能によって結果が過度にマスクされる場合は、正規表現 [¥x0c]{1}[0-9]{8}([0-9]{4}) を使用します。

症状

編集機能によって結果が過度にマスクされるか、Oracle トラフィックに ORA-03106 エラーが発生します。

原因

Guardium ポリシー・ルールの編集機能は、結果セットとのパターン・マッチングを行います。これには、一致した文字列をユーザーが指定した文字に置き換える機能があります。

環境

Guardium コレクターが影響を受けます。

問題の解決

正規表現 `[¥x0c]{1}[0-9]{8}([0-9]{4})` を使用します。 この正規表現では、結果が列の長さで始まり、その後に 12 桁が続くようになり、最後の 4 桁が置き換えられます。

親トピック: ポリシー

Oracle データベースにログインする SSH セッションおよび自動化 CRON ジョブが失敗したログインとして表示される

Oracle データベースにログインする SSH セッションおよび自動化 CRON ジョブが失敗したログインとして表示される場合は、ポリシーを修正します。

症状

`/as sysdba` を指定して SQLPLUS および RMAN から Oracle データベースにログインする SSH セッションおよび自動化 CRON ジョブが、失敗したログインとして表示されます。

原因

画面に表示されない場合でも、Oracle はこうしたログインの試みに対して以下のエラーで応答します。

```
ORA-01-17: invalid username/password; logon denied.
```

このエラーによって、失敗したログインのアラートがトリガーされます。例えば、データベース・ユーザー WRONGLOGIN が DBA グループのメンバーであり、`sqlplus WRONGLOGIN as sysdba` としてログインした場合、WRONGLOGIN のデータベース認証が失敗します。この失敗によって ORA-01-17 エラー・アラートがトリガーされ、Guardium ログに反映されます。ただし、sysdba 特権を持つユーザーはデータベース認証なしでもデータベースに接続できるため、セッションの続行が許可されます。どちらのイベントもキャプチャーされ、記録されます。

環境

Guardium コレクターが影響を受けます。

問題の解決

失敗したログインについてアラートするルールの前に許可アクションを組み込むように、ポリシーを修正することができます。以下の条件を使用して、ポリシー内に例外ルールを作成します。

```
Client IP=<Server IP>
Source program = SQLPLUS
DB user in trusted group
OS user in group of Oracle DBAs
Net protocol = BEQUEATH (if local BEQUEATH, not TCP)
```

このルールにより、ORA-01-17 エラーが原因のログイン失敗アラートはスキップされます (ただしログには記録されます)。ログイン失敗アラートをレポートからフィルターに掛けて除外するには、条件リストの最後に以下の条件を追加します。

```
AND
        (
    client IP<>server IP OR
    src prg <> SQLPLUS OR
    db user NOT IN group of trusted OR
    os user NOT IN group of oracle DBAs OR
    net protocol <>BEQUEATH (if this is local BEQUEATH, not TCP )
   )
```

親トピック: ポリシー

Guardium 内部データベースがいっぱいになる

Guardium 内部データベースがいっぱいになった場合は、手動で、または通常のパージ戦略の一環としてパージすることができます。

症状

Guardium 内部データベースがいっぱいになり、データのほとんどが GDM_POLICY_VIOLATIONS_LOG 表内にある。

原因

ポリシーへの変更によって、ポリシー違反ルールが頻繁にトリガーされる場合があります。データのほとんどが GDM_POLICY_VIOLATIONS_LOG 表内に見つかります。

環境

Guardium コレクターが影響を受けます。

問題の診断

CLI コマンド support show db-top-tables all を実行します。

問題の解決

「ポリシー違反 / インシデント管理」レポートにチェック・マークを付けて、常にトリガーされるポリシー・ルールを識別します。次に、ポリシー・ルールがそれほど頻繁にトリガーされないように調整します。

GDM_POLICY_VIOLATIONS_LOG 表内の余分なデータは、通常のパージ戦略の一環としてパージされます。ただし、GDM_POLICY_VIOLATIONS_LOG 表からデータを手動で消去する場合は、コマンド support clean DAM_data policy_violations<start_date><end_date> を使用できます。

親トピック: ポリシー

レポート

- 少なくとも 1 回監査プロセスが実行された後に監査プロセスの受信者の表を変更できない
  監査プロセスの受信者の表を変更できない場合は、監査プロセスをコピーし、元の監査プロセスを置き換えます。
- マルチバイト文字が表示されない
  PDF にエクスポートした Guardium レポートの文字が正しくない場合は、PDF フォント構成を切り替えます。
- ファイル・システムがほとんどいっぱいである
  Guardium ファイル・システムがほとんどいっぱいである場合は、ログ・ローテーション戦略を変更します。

- Guardium 監査レポートを Microsoft Excel で表示すると予期しない文字を含む行が表示される
  監査レポートを .csv 形式で表示したときに予期しない文字を含む行が表示される場合は、別の .csv ビューアーを使用するか、.pdf ファイルとして表示します。
- レポートに IP アドレスが 0.0.0.0 と表示される
- 「要求が中断されたか、割り当て量を超えました」エラー・メッセージ
  レポートの実行時に、要求が中断されたか、割り当て量を超えたことを示すエラー・メッセージを受け取る場合は、より短いレポート間隔にレポートを分割します。
- ルールがトリガーされない
  ポリシー・コマンド・フィールドに値を持つルールが予期されるようにトリガーされない場合は、ルールを再構成します。
- 5 分おきのスケジュールされたジョブの例外
  スケジュールされたジョブの例外を 5 分おきに受け取る場合は、「異常検出」ページからのアラートを非アクティブ化します。
- スケジュール済みジョブ例外: マージが必要です。プロセスの実行を延期してください (merge required, delay executing process)
  マージが必要であるというエラー・メッセージを受け取った場合は、プロセスの実行を延期し、監査プロセスのスケジュールを変更します。
- Teradata のモニター時に Guardium レポートにデータベース・ユーザーが正しく表示されない
  Teradata のモニター時に、Guardium レポートにデータベース・ユーザーが正しく表示されない場合は、Teradata Database を構成します。
- 埋め込みコマンドによる Guardium レポートが予期しない結果になる
  予期しない結果の Guardium レポートを受け取った場合は、タプルを使用して深さを処理するようにポリシー・ルールを構成します。

親トピック: 問題および解決策

少なくとも 1 回監査プロセスが実行された後に監査プロセスの受信者の表を変更できない

監査プロセスの受信者の表を変更できない場合は、監査プロセスをコピーし、元の監査プロセスを置き換えます。

症状

監査プロセスを少なくとも 1 回実行した後には、受信者を削除することも追加することもできなくなります。また、受信者の以下のプロパティーを変更することもできません。

- 必要なアクション
- 続行
- 空の場合は承認

原因

監査プロセスが少なくとも 1 回実行されると、受信者の表はロックされ、ほとんどのプロパティーを変更できなくなります。

環境

すべての Guardium 構成 (コレクター、アグリゲーター、中央マネージャー) が影響を受けます。

問題の解決

以下の手順によって、受信者の表を変更できます。

1. 監査プロセスをコピーします。
2. コピーされた監査プロセスに変更を加えます。
3. 元の監査プロセスを削除します。ただし、監査プロセスの履歴を残したい場合は、その監査プロセスの名前を変更することができます。
4. コピーされた監査プロセスの名前を、元の監査プロセスの名前に変更します。

親トピック: レポート

マルチバイト文字が表示されない

PDF にエクスポートした Guardium レポートの文字が正しくない場合は、PDF フォント構成を切り替えます。

症状

GUI ではレポートを表示できます。しかし、レポートを PDF にエクスポートすると、文字が正しく表示されないか、欠落します。 PDF レポートで、文字が疑問符 (?) またはその他の記号で表示されます。

原因

Guardium PDF エクスポートのデフォルトのフォントでは、マルチバイト文字が正しく表示されません。例えば、ギリシャ語、キリル文字、中国語の文字は正しく表示されません。

環境

コレクター、アグリゲーター、および中央マネージャーが影響を受けます。

問題の解決

バージョン 9 以降では、PDF フォント構成を切り替えて問題を解決します。

1. CLI のユーザーとしてログインします。

2. コマンド store pdf-config multilanguage_support を実行します。
3. 2 Multi-language. を選択します。

親トピック: レポート

ファイル・システムがほとんどいっぱいである

Guardium ファイル・システムがほとんどいっぱいである場合は、ログ・ローテーション戦略を変更します。

症状

ファイル・システムがいっぱいになりつつあり、100% に達しようとしています。

原因

syslog に送信されるアラートとレポートによって、ファイル・システムがいっぱいになる場合があります。

環境

コレクターまたはアグリゲーターが影響を受ける場合があります。

問題の解決

デフォルトでは、ログ・ファイルは毎週循環され、5 つのファイルが保持されます。ただし、ログ・ファイルのログ・ローテーション戦略を変更することができます。以下のコマンドを使用して、システム内のメッセージをより少なく保持するようにします。

```
store logrotate [agg|message] [daily|weekly|monthly] [# of rotations]
```

親トピック: レポート

Guardium 監査レポートを Microsoft Excel で表示すると予期しない文字を含む行が表示される

監査レポートを .csv 形式で表示したときに予期しない文字を含む行が表示される場合は、別の .csv ビューアーを使用するか、.pdf ファイルとして表示します。

症状

Microsoft Excel で監査レポート (.csv 形式) を表示すると、特定の行に予期しない文字が含まれていることに気付きます。 これらの文字は、完全な SQL 列内で見られる文字に似ています。この問題は、.pdf レポートまたは GUI レポートでは発生しません。

原因

Microsoft Excel では、セルに含めることができる文字数の制限は 32,767 文字です。キャプチャーした SQL がこの制限を超える場合は、次の行にまたがります。

環境

コレクター、アグリゲーター、および中央マネージャーが影響を受けます。

問題の解決

セルあたりの文字数の制限がより大きい、別の .csv ビューアーを使用するか、.pdf ファイルとして監査レポートを表示します。

親トピック: レポート

レポートに IP アドレスが 0.0.0.0 と表示される

症状

Guardium で IP アドレスが 0.0.0.0 と表示されます。

原因

Guardium がトラフィックを暗号化解除するとき、IP アドレスは最初は 0.0.0.0 として記録されます。これは、スニファーが実際の IP アドレスを認識していないことが原因です。暗号化解除が完了すると、別のスレッドによって正しい IP アドレスがセッション・テーブルに再設定されます。

環境

データベース・トラフィックを暗号化するすべてのデータベースが影響を受けます。

問題の解決

数分後に同じレポートを実行します。より新しいトラフィックの正しいクライアント IP を表示するには、クライアント/サーバー・ドメインのフィールド「分析済みのクライアント IP」をレポートに追加します。 一部の行では、「分析済みのクライアント IP」がブランクになる可能性があります。 ブランクの場合、その部分のトラフィッ

クの暗号化解除は完了していません。

親トピック: レポート

「要求が中断されたか、割り当て量を超えました」エラー・メッセージ

レポートの実行時に、要求が中断されたか、割り当て量を超えたことを示すエラー・メッセージを受け取る場合は、より短いレポート間隔にレポートを分割します。

症状

Guardium でレポートを実行すると、「要求が中断されたか、割り当て量を超えました」というエラー・メッセージを受け取ります。

原因

エラー・メッセージ「要求が中断されたか、割り当て量を超えました」が表示されるのは、対話式レポートが 3 分の時間制限内に完了しない場合です。基になる原因は、一般的にレポートのサイズです。

環境

コレクターおよびアグリゲーターが影響を受けます。

問題の解決

この問題を解決するには、以下のオプションのいずれかを実行します。

- レポートを、より短いレポート間隔に分割します。 このアクションは、最も推奨される方式です。レポートが 4 GB を超える場合、MYSQL 表データのポインター・サイズがなくなる原因になります。
- 照会タイムアウト値を大きい値にします。「管理」 > 「アクティビティー・モニター」 > 「実行照会モニター」をクリックして、「実行照会モニター」を開きます。
- ブラウザーをアンインストールしてから、再インストールします。「レポート/モニター照会タイムアウト」ボックスに秒数を入力し、「更新」をクリックします。
- バックグラウンドでレポートを実行します。バックグラウンドで実行されるレポートは、照会タイムアウトの影響を受けません。
- 監査プロセスとしてレポートを実行します。

親トピック: レポート

ルールがトリガーされない

ポリシー・コマンド・フィールドに値を持つルールが予期されるようにトリガーされない場合は、ルールを再構成します。

症状

ポリシーの「コマンド」フィールドに値を持つルールが予期されるようにトリガーされません。

原因

この原因は、コマンド・フィールドの構成の誤りです。 Guardium パーサーは、コマンド修飾子をコマンドの一部と見なしません。

環境

Guardium コレクター - ワイルドカード (%) を使用する場合、ポリシー・ルール内のコマンド・フィールドも影響を受けます。

問題の解決

ルールの「コマンド」フィールド内の値は、SQL 動詞に表示される値と正確に一致する必要があり、必要に応じてワイルドカード (%) が追加されます。正しい例は次のとおりです。

```
GRANT
GRANT%
```

この例は正しくありません。

```
GRANT% TO PUBLIC
%GRANT% ADMIN OPTION%
```

ADMIN OPTION と TO PUBLIC は一致せず、ルールをトリガーできません。これは、Guardium パーサーがこれらをコマンドの一部と認識しないためです。一般に、パーサーはコマンド修飾子をコマンドの一部と見なしません。 代わりに、ポリシーがモニターするトラフィックを調べるためのレポートを作成し、そのレポートにコマンド・エンティティーからの「SQL 動詞」フィールドを組み込みます。 「SQL 動詞」フィールドにリストされたものはすべてパーサーに認識され、ポリシー・ルールの「コマンド」フィールドに使用できます。複数のコマンドをグループに追加して、そのグループをルール内で単一コマンドの代わりに使用することができます。この場合、各グループ・メンバーは SQL 動詞内のエントリーに一致する必要があります。Guardium には、ユーザーが使用したりコピーを作成したりできるコマンド・グループがいくつかあります。
親トピック: ポリシー
親トピック: レポート

5 分おきのスケジュールされたジョブの例外

スケジュールされたジョブの例外を 5 分おきに受け取る場合は、「異常検出」ページからのアラートを非アクティブ化します。

症状

定期的な短い間隔 (通常 5 分おき) で、スケジュール済みジョブ例外レポート内に同じメッセージを受け取ります。 この間隔は、異常検出が実行されるポーリング間隔と同じです。

スケジュール済みジョブ例外レポートの例は以下のとおりです。

```
Timestamp            Exception Description                              Count of Exceptions
2013-12-05 15:51:22.0 java.lang.NumberFormatException: empty String        1
```

同じ例外が 5 分おきに発生します。

原因

アクティブ・アラートのいずれかがエラーの原因です。

環境

Guardium のコレクターおよびアグリゲーターが影響を受けます。

問題の診断

ポーリング間隔とアクティブ・アラートは、「異常検出」ページで確認できます。「保護」 > 「データベースの侵入検出」 > 「異常検出」をクリックして、「異常検出」ページを開きます。

問題の解決

問題の原因になっているアラートを正確に特定し、非アクティブ化します。

1. 「異常検出」ページで 1 つのアラートを非アクティブ化します。
2. ポーリング間隔が経過するまで待ちます。
3. そのアラートを非アクティブ化したことによってエラーがなくなったかどうかを確認します。
4. エラーが続く場合は、そのアラートを再アクティブ化して、別のアラートを非アクティブ化します。
5. ステップ 2 から 5 を繰り返して、すべてのアラートを試します。

問題の原因になっているアラートが見つかり、そのエラーを把握して停止するために支援が必要な場合は、IBM Guardium 技術サポートに問い合わせて、以下のアイテムを提供してください。

1. 正確なエラー・テキストおよび画面キャプチャー。
2. 以下の CLI コマンドの出力。要求された場合、1 ポーリング間隔の長さを指定します。

   support must_gather app_issues

   support must_gather alert_issues

親トピック: レポート

スケジュール済みジョブ例外: マージが必要です。プロセスの実行を延期してください (merge required, delay executing process)

マージが必要であるというエラー・メッセージを受け取った場合は、プロセスの実行を延期し、監査プロセスのスケジュールを変更します。

症状

以下のメッセージを受け取ります。「マージが必要です。プロセスの実行を延期してください `(merge required, delay executing process)`」。短期間でこのようなメッセージをいくつか受信する可能性があります。

原因

監査プロセスが実行されるためには、その前にマージ・プロセスが終了している必要があります。

環境

アグリゲーターが影響を受けます。

問題の診断

「レポート」 > 「Guardium 運用レポート」 > 「統合/アーカイブ・ログ」をクリックして、「統合/アーカイブ・ログ」を開きます。agg_progress.log で問題を診断することもできます。

問題の解決

監査プロセスが、マージ・プロセス後に少なくとも 10 分経過してから実行されるようにスケジュールを変更します。

親トピック: レポート

Teradata のモニター時に Guardium レポートにデータベース・ユーザーが正しく表示されない

Teradata のモニター時に、Guardium レポートにデータベース・ユーザーが正しく表示されない場合は、Teradata Database を構成します。

症状

Guardium レポートで、モニター対象の Teradata Database からのレコードを表示すると、データベース・ユーザー名のフィールドが予期されるとおりに表示されません。ユーザー名が切り捨てられるか、欠落します。

原因

Teradata Database では、完全なユーザー名を返すことができません。

環境

Teradata Database からデータをキャプチャーするすべての Guardium コレクターが影響を受けます。

問題の解決

以下のコマンドを使用して、Teradata Database が完全なユーザー名を正しい文字セットでモニター・アプリケーションに返すことができるようにします。他のアプリケーションは影響を受けません。

gtwcontrol -u yes -d

-d コマンドによって、更新された GDO 設定が表示されます。

注: この設定では、ユーザー名が暗号化されない形式で返されます。暗号化が有効になっている場合は、システムからエラー・メッセージが返されます。
親トピック: レポート

埋め込みコマンドによる Guardium レポートが予期しない結果になる

予期しない結果の Guardium レポートを受け取った場合は、タプルを使用して深さを処理するようにポリシー・ルールを構成します。

症状

レポートの結果が、予期しないものであるか、ポリシーによってフィルターに掛ける必要があると思われます。逆に、キャプチャーしようとしていたステートメントがキャプチャーされません。

原因

通常、SQL には複数のオブジェクトおよびコマンドがステートメント内に埋め込まれています。ポリシー定義またはレポート定義が、異なる深さのオブジェクトまたはコマンドを処理するように構成されていません。

環境

Guardium コレクターが影響を受けます。

問題の解決

条件が正しいオブジェクト名と一致していることを確認します。正しいメイン・エンティティーを使用して、異なる深さのオブジェクトまたは SQL 動詞を表示します。それでも予期しない動作が見られる場合は、グループ・ビルダーを使用して、ポリシー内で使用するタプルのグループを定義します。タプルでは、複数の属性を組み合わせて 1 つのグループ・メンバーを形成することができます。

注: タプルには、1 つのスラッシュおよび 1 つのワイルドカード文字 (%) を使用できます。 ダブルスラッシュは使用できません。
親トピック: レポート

評価および強化

- Windows で CAS が Java 1.7 と連携しない
  Windows 上で Guardium 変更監査システムが Java バージョン 1.7 と連携しない場合、msvcr100.dll を CAS の bin フォルダーにコピーします。
- 失敗したテストに脆弱性評価の例外グループ・メンバーが表示される
  失敗した脆弱性評価テストにテスト例外グループのメンバーが表示される場合は、円記号 (¥) にエスケープ・シーケンスを使用します。

親トピック: 問題および解決策

Windows で CAS が Java 1.7 と連携しない

Windows 上で Guardium 変更監査システムが Java バージョン 1.7 と連携しない場合、msvcr100.dll を CAS の bin フォルダーにコピーします。

症状

Guardium CAS は、古いバージョンの Java とは連携しますが、Java 1.7 とは連携しません。

原因

<GUARDIUM STAP directory>¥cas¥bin¥ に、msvcr100.dll がありません。

環境

Windows 上の Guardium CAS が影響を受けます。

問題の解決

この問題を解決するには、以下の手順を実行します。

1. ご使用のシステムで Java 1.7 がインストールされたパス (C:¥Program Files (x86)¥Java¥jre7¥bin など) を見つけます。
2. 前のステップで見つけた Java パス内で、ライブラリー jvm.dll のロケーションを見つけます。
3. <CAS directory>¥conf ディレクトリー内の cas.cfg ファイルを編集します。例えば、C:¥Program Files (x86)¥GUARDIUM_STAP¥cas¥conf¥cas.cfg が標準的なファイル・パスです。
4. JVM に対応する行 (;JVM=c:¥program files¥java¥jre1_2_3¥bin¥client¥jvm.dll など) を見つけます。
5. 行の先頭からセミコロンを削除します。次に、JVM を、ステップ 2 のライブラリー jvm.dll のパスに設定します。`JVM=C:¥Program Files (x86)¥Java¥jre7¥bin¥server¥jvm.dll`
6. msvcr100.dll を、Java 7 インストール・ディレクトリー内の bin フォルダーから、<CAS directory>¥bin フォルダーにコピーします。例えば、C:¥Program Files (x86)¥Java¥jre7¥bin¥msvcr100.dll を C:¥Program Files (x86)¥Guardium¥GUARDIUM_STAP¥cas¥bin¥msvcr100.dll にコピーします。
7. 変更監査システムを再始動します。

注: これは、Java バージョン 1.7 の場合のみ必要です。Java のそれより古いバージョンでは、このステップは必要ありません。
親トピック: 評価および強化

失敗したテストに脆弱性評価の例外グループ・メンバーが表示される

失敗した脆弱性評価テストにテスト例外グループのメンバーが表示される場合は、円記号 (¥) にエスケープ・シーケンスを使用します。

症状

脆弱性評価を実行すると、詳細フィールドにテスト例外グループの一部のメンバーが表示されます。このグループには、円記号 (¥) と REGEX タグを持つメンバーが含まれています (例: `(R)US¥John Doe`)。

原因

Guardium による例外グループの解析時に、特殊文字によってエラーがトリガーされる場合があります。

環境

Guardium コレクターが影響を受けます。

問題の解決

円記号 (¥) にエスケープ・シーケンスを使用すること、および REGEX タグを使用しないようにします (完全一致を使用します)。以下の例はどちらも機能します。

```
US¥John Doe
```

```
(R)US¥¥John Doe
```

REGEX タグ (R) は、詳細フィールドの正規表現検索をトリガーするために使用され、正規表現に一致するすべての文字列が削除されます。 正規表現において意味を持つ円記号 (¥) やその他の文字は、構文解析エラーを回避するために円記号 (¥)のエスケープ・シーケンスが必要です。(R) タグを使用しない場合、Guardium がマッチングを行う際には、グループ・メンバーは詳細フィールド内の行全体と完全に一致する必要があります。脆弱性テストを通過するには、テストの詳細フィールドを空にする必要があります。

親トピック: 評価および強化

Guardium システムの構成

- アップグレード後に STAP を構成できない
  S-TAP をアップグレードした後に Guardium 内で S-TAP を構成します。
- Guardium がネットワーク・デバイス VMXNET x を認識できない
  Guardium がネットワーク・デバイス VMXNET x を認識できない場合は、Guardium を仮想マシンにインストールし、ネットワーク・アダプターを追加します。
- システム・ボードの交換後に Guardium ネットワーク・インターフェース・エラーが発生する
  ハードウェアの修理後にエラー・メッセージを受け取った場合は、ネットワーク・パラメーターをリセットします。
- ネットワークから Guardium 仮想マシンにアクセスできない
  ネットワークから Guardium 仮想マシンにアクセスできない場合は、store network interface inventory コマンドを実行し、システムを再始動します。

- SSLv3 が有効になっている
  `SSLv3 is enabled` という警告を受け取った場合は、SSLv3 を無効にして POODLE 攻撃を防止します。

親トピック: 問題および解決策

アップグレード後に STAP を構成できない

S-TAP をアップグレードした後に Guardium 内で S-TAP を構成します。

症状

Guardium Installation Manager (GIM) を使用して S-TAP をアップグレードした後に、モジュールのインストール結果で正常に完了したと表示されたにも関わらず、Guardium 内の検査エンジンでデータベース・パス・パラメーターを構成できません。

原因

新規 S-TAP がまったく新しいモジュールとしてインストールされた場合、K-TAP は正しくアップグレードされません。古い K-TAP モジュールが削除されないため、古い K-TAP モジュールと新しい S-TAP の間にプロトコルの不一致が生じます。

環境

AIX、HP-UX、Linux、および Solaris などの UNIX および Linux にインストールされた S-TAP。

問題の診断

問題を診断するには、guard_diag ユーティリティーを実行して、Guardium S-TAP の Must Gather データを収集します。

以下の行が syslog ファイル内にあります。

```
STAP and KTAP Protocol Version Mismatch,
Exit!!!!!: No such file or directory
Tap_controller::init failed
GUARD-01: Error Initializing STap
```

モジュールのログ・ファイルには、古い K-TAP がリストされます。例: `ktap_24276 338760 0`

問題の解決

この問題を解決するには、GIM モジュール・インストール・ペインで以下の手順を実行します。

1. K-TAP Live Update を Y に設定します。
2. K-TAP_ENABLED を Y に設定し、新規 S-TAP を再インストールします。

親トピック: Guardium システムの構成

Guardium がネットワーク・デバイス VMXNET x を認識できない

Guardium がネットワーク・デバイス VMXNET x を認識できない場合は、Guardium を仮想マシンにインストールし、ネットワーク・アダプターを追加します。

症状

VMware でのインストール中に、Guardium がネットワーク・デバイス VMXNET x を認識できません。ゲストとして VMware で Guardium をインストールすると、「`eth0: unknown interface: No such device`」というエラーを受けとります。システムの再始動後にこのエラー・メッセージが表示されます。

原因

VMXNET x 仮想ネットワーク・アダプターは、VMware ツールのみに含まれる特定のドライバーを必要とします。どのオペレーティング・システムにもそのドライバーはありません。Guardium が Linux で実行されており、インストーラーには VMXNET x 用のドライバーは含まれていません。

環境

Guardium システムが影響を受けます。

問題の解決

以下の手順を実行して、この問題を解決します。

1. E1000 または Flexible などのデフォルトのネットワーク・アダプターを使用して、VMware 上に仮想マシンを作成します。
2. 仮想マシンに Guardium をインストールします。
3. Guardium 用の現行の GPU 累積パッチをインストールします。
4. インストール後に、CLI コンソールにログオンし、setup vmware_tools install コマンドを実行して、VMware ツールをインストールします。
5. CLI コンソールから stop system コマンドを使用して Guardium システムをシャットダウンします。
6. VMware Infrastructure Client などの VMware クライアント・ツールを使用して仮想マシン設定を編集します。現行のネットワーク・アダプターを選択し、それを削除します。
7. VMXNET というネットワーク・アダプターを追加します。

8. Guardium システムを再始動します。

親トピック: Guardium システムの構成

システム・ボードの交換後に Guardium ネットワーク・インターフェース・エラーが発生する

ハードウェアの修理後にエラー・メッセージを受け取った場合は、ネットワーク・パラメーターをリセットします。

症状

Guardium アプライアンスでシステム・ボードの交換などのハードウェアの修理を行った後に、ネットワーク接続が失われます。アプライアンスのリブート時に、ネットワーク・インターフェースごとに以下のエラー・メッセージが出されます。

```
rtnetlink answers: no such device
```

原因

システム・ボードを交換すると、MAC アドレスが変わります。アドレスが変わることで、実際の MAC アドレスと、インターフェース構成ファイルに保管されているアドレスが一致しなくなります。

環境

システム・ボードが交換された Guardium アプライアンス (コレクター、アグリゲーター、または中央マネージャー) と、すべての Guardium バージョンが影響を受けます。

問題の解決

ユーザー CLI としてコンソールからアプライアンスにログインし、以下のコマンドを実行してネットワーク・パラメーターをリセットしてください。

```
store network interface inventory
restart network
store network interface ip<IP_address>
store network interface mask<netmask>
store network routes defaultroute<gateway_address>
restart network
```

それでも問題が解決されない場合は、Guardium サポートに連絡して、手動操作を依頼してください。

親トピック: Guardium システムの構成

ネットワークから Guardium 仮想マシンにアクセスできない

ネットワークから Guardium 仮想マシンにアクセスできない場合は、store network interface inventory コマンドを実行し、システムを再始動します。

症状

新規 Guardium システムを仮想マシンとして実装し、すべての必要な初期ネットワーク構成を実行しました。しかし、IP アドレスを使用してシステムを ping することができず、ネットワーク内でそのシステムにアクセスできません。

原因

仮想環境によって仮想マシンに割り当てられた MAC アドレスが、Guardium での MAC アドレスと一致していません。

環境

コレクター、アグリゲーター、および中央マネージャーが影響を受けます。

問題の診断

この問題を診断するには、ネットワークで IP アドレスを ping します。 ping<appliance's ip address> コマンドを使用します。失敗した場合は、システムの MAC アドレスを表示します。

1. ユーザー "cli" でログインします。
2. show network macs コマンドを実行して、Guardium 構成に保管されている MAC アドレスを表示します。
3. ご使用の仮想環境の管理ユーティリティーから、仮想マシンの MAC アドレスを確認します。
    a. VMware Workstation を開きます。
    b. 仮想マシンを右クリックし、「設定 (Settings)」または「プロパティー (Properties)」を選択して「仮想マシンの設定 (Virtual Machine Settings)」を開きます。
    c. 「ハードウェア (Hardware)」の下で「ネットワーク・アダプター (Network Adapter)」を選択します。
    d. 「拡張 (Advanced)」をクリックして、「ネットワーク・アダプター拡張設定 (Network Adapter Advanced Settings)」を開きます。
    e. ステップ 2 と 3 の MAC アドレスを比較します。

問題の解決

この問題を解決するには、以下の手順を実行します。

1. ユーザー "cli" として Guardium システムにログインします。
2. store network interface inventory コマンドを実行します。
3. `y` と入力して、NIC をリセットします。
4. restart system コマンドを使用して、システムを再始動します。

親トピック: Guardium システムの構成

SSLv3 が有効になっている

`SSLv3 is enabled` という警告を受け取った場合は、SSLv3 を無効にして POODLE 攻撃を防止します。

症状

以下の警告を受け取ります: `SSLv3 is enabled`。

原因

SSLv3 には、Padding Oracle On Downgraded Legacy Encryption (POODLE) と呼ばれるプロトコル脆弱性が存在します。システムで SSLv3 が有効になっている場合、この脆弱性によりアタッカーは SSL/TLS を強制的に SSLv3 にフォールバックさせ、暗号を解除して、ネットワーク・トラフィックをプレーン・テキストで傍受することが可能となります。この脆弱性の詳細は、National Vulnerability Database の CVE-2014-3566 で説明されています。

Guardium® では、POODLE 攻撃を防止するためにすべてのシステムで SSLv3 を無効にすることを推奨しており、新しい Guardium システムではデフォルトで SSLv3 が無効になっています。ただし、古いシステムや一部のアップグレード・シナリオでは SSLv3 が有効なままになっている場合があります。

このトピックでは、SSLv3 の状況を確認し、必要な場合に無効にする方法について説明します。

重要: SSLv3 を無効にすると、Guardium v10 中央マネージャーと GPU 500 より前の Guardium v9 を実行する管理対象ユニットの一部との間の接続が切れる可能性があります。GPU 500 より前の Guardium v9 を実行する管理対象ユニットが存在する混合環境を使用している場合、SSLv3 を無効にする前に、管理対象ユニットを GPU 500 にアップグレードするか、またはパッチ 9501 を適用してください。

問題の解決

1. CLI コマンド `show sslv3` を使用して SSLv3 の状況を確認します。
   - 出力が `SSL setting is disabled` の場合、SSLv3 は無効です。SSLv3 を無効にするための追加手順は不要です。
   - 出力が `SSL setting is enabled` の場合、SSLv3 は有効です。SSLv3 を無効にするための手順を続けてください。
2. CLI コマンド `store sslv3 off` を使用して SSLv3 を無効にします。コマンド出力は、以下のようになります。

```
Current SSL setting is enabled.  Will change to disabled.
Restarting
gui (GUI を再始動しています)
Changing to port 8443 (ポート 8443 に変更しています)
From port 8443
Stopping..... (停止しています.....)
ok
```

3. `show sslv3` と入力して SSLv3 が無効になったことを確認します。出力は `SSL setting is disabled` となるはずです。

親トピック: Guardium システムの構成

アクセス管理

- admin または accessmgr 以外で Guardium にログインできない
  admin または accessmgr としてログインする場合を除いて Guardium GUI にログインできない場合は、認証構成設定を確認します。
- Guardium accessmgr のパスワードのリセット
  accessmgr パスワードが分からなくなり、ログインできない場合は、Guardium サポートに連絡してください。

親トピック: 問題および解決策

admin または accessmgr 以外で Guardium にログインできない

admin または accessmgr としてログインする場合を除いて Guardium GUI にログインできない場合は、認証構成設定を確認します。

症状

admin または accessmgr 以外のユーザーで Guardium にログインすることができません。accessmgr が定義した正しいユーザーおよびパスワードを使用しているにも関わらず、ユーザー名またはパスワードが無効であるというエラーが表示されます。 以下のエラー・メッセージを受け取ります。ユーザー名/パスワードのいずれか （または両方） が無効です。資格情報を再入力してください。

原因

認証設定がローカルとして構成されていません。

環境

コレクター、アグリゲーター、および中央マネージャーが影響を受けます。

問題の解決

問題を解決するには、認証設定をローカルに変更します。このアクションにより、accessmgr によって定義されたどのユーザーとしてもログインできます。

親トピック: アクセス管理

Guardium accessmgr のパスワードのリセット

accessmgr パスワードが分からなくなり、ログインできない場合は、Guardium サポートに連絡してください。

症状

Guardium accessmgr のパスワードが分からなくなり、GUI にログインできません。連続してログイン試行に失敗すると、アカウントのロックも行われます。

原因

Guardium では、複数回のログイン試行の失敗を許容しません。

環境

コレクター、アグリゲーター、および中央マネージャーが影響を受けます。

問題の解決

CLI にログインし、support reset-password accessmgr<N>|random というコマンドを実行します。

<N> または random を使用できます。<N> は、10000000 から 99999999 までの範囲内の数値です。random と指定すると10000000 から 99999999 までの範囲内の数値が自動的に生成されます。IBM Guardium サポートを利用し、PMR を開いて、以下の出力を送信します。

```
G10.ibm.com> support reset-password accessmgr random
Password for accessmgr account have been successfully reset using keyword:<passkey>
Please provide these number to Guardium Customer Service to receive actual account password.
ok
```

新しいパスワードを受け取ったら、アカウントをアンロックします。

1. アカウントをアンロックするには、以下のコマンドを使用します。unlock accessmgr。
2. accessmgr としてログインし、accessmgr の詳細を編集して、一時的なパスワードを入力します。
3. 一時的なパスワードを使用して再度ログインします。
4. プロンプトが出されたら、新規パスワードを入力します。

親トピック: アクセス管理

統合

親トピック: 問題および解決策

Guardium コレクターをアグリゲーターに変換できない

Guardium コレクターを中央マネージャー・アグリゲーターに変換できない場合は、Guardium を再インストールし、インストール時にアグリゲーターを選択してください。

症状

store unit type manager aggregator というコマンドを使用して、Guardium コレクターをアグリゲーターに変換しようとします。

しかし、以下のコマンドで、ユニット・タイプがまだマネージャーとしてリストされます。

```
> show unit type
Manager
```

原因

CLI コマンドを使用してコレクターをアグリゲーターに変換することはできません。

環境

Guardium コレクターが影響を受けます。

問題の解決

コレクターをアグリゲーターに変換するには、Guardium 製品を再インストールし、インストール時にユニット・タイプとしてアグリゲーターを選択します。アグリゲーターのインストール後に、コマンド store unit type manager を使用して、アグリゲーターを中央マネージャー・アグリゲーターに変換できます。

中央マネージャー/アグリゲーターの制約
v9.5 (v9.0 パッチ 500) 以降、アプリケーションには、中央マネージャーがアグリゲーター・タイプのアプライアンスでなければならないという制約があります。つまり、v9.5 以降では、アグリゲーター・タイプのアプライアンスのみを中央マネージャー・アプライアンスにプロモートできます。v9.5 より前の既存の CM アプライアンスは、この変更の対象ではありません。

親トピック: 統合

Guardium 管理対象システムの GUI からのデータ・エクスポートの構成変更がエラーのため失敗する

データ・エクスポートの構成変更が失敗した場合は、コレクターとアグリゲーターで共有パスワードが同一になるようにしてください。

症状

データ・エクスポートの新規の設定を保存しようとして、構成を保存するために「適用」をクリックしたときに、エラーが発生します。

以下のエラーを修正したうえで再試行してください:
指定されたパラメーターを使用してテスト・データ・ファイルをこのホストに送信することができませんでした。　ホスト名または IP アドレスが正しく入力されていること、ホストがオンラインであること、ターゲット・ディレクトリーが存在し指定したユーザーが書き込めること、そのユーザーのパスワードが正しく指定されていることを確認してください。

原因

Guardium は、データ・エクスポート構成で指定されたユーザーおよびパスワードを使用して、ターゲット・ホストに scp によってログインしようとします。次に、Guardium はテスト・ファイルをターゲット・ディレクトリーにコピーしようとします。このシステム上の共有パスワードは、このシステムからのエクスポート先として設定しようとしているアグリゲーター上の共有パスワードと一致しません。

環境

Guardium 構成: コレクターとアグリゲーターが影響を受けます。

問題の解決

必ず、コレクターとアグリゲーターで共有パスワードが同一になるようにしてください。以下のいずれかの方式を使用できます。

1. アグリゲーター上の共有パスワードを知っている場合は、コレクター上の共有パスワードを同じ値に設定します。以下のいずれかの方式を使用できます。
   - CLI から store system shared secret コマンドを使用して、共有パスワードを設定します。
   - GUI から、「設定」 > 「システム」 > 「システム構成」で共有パスワードを設定します。
2. アグリゲーター上の現在の共有パスワードをバックアップし、コレクターにリストアします。
   - アグリゲーターで、CLI コマンドを実行します。

     ```
     aggregator backup keys file <user@host:/path/filename>
     パラメーター
     user@host:/path/filename
     ```

     ファイル転送操作において、バックアップ鍵ファイルのユーザー、ホスト、および絶対パス名を指定します。 指定するユーザーには、指定したディレクトリーに対する書き込み権限が必要です。
   - コレクターで、次のコマンドを使用して、共用パスワードをリストアします。

     ```
     aggregator restore keys file<user@host:/path/filename>
     ```
3. 両方のアプライアンスの共有パスワードを、同一になるようにリセットします。
   注: アグリゲーターの共有パスワードを変更した場合、アグリゲーターをエクスポート先とする他のすべての Guardium システムの共有パスワードをリセットする必要があります。

親トピック: 統合

監査プロセスの結果とレポートの違い

監査プロセスの結果とレポートの間に違いがある場合は、すべてのアプライアンスが同じタイム・ゾーンに設定されていることを確認してください。

症状

時間パラメーター (例えば「最終日の始め (Start of Last Day)」および「最終日の終わり (End of Last Day)」など) を使用して監査プロセスの一部としてアグリゲーターで実行されるように、レポートを設定します。 そのレポートの結果を調べると、最初のタイム・スタンプは常に、00.00 よりも後の規定の時刻 (例えば 02.00) になります。さ

らに、最後のタイム・スタンプは、常に 23.59 よりも前の規定の時刻 (例えば 21.59) になります。ただし、レポートを対話式に実行すると、タイム・スタンプは予期したとおりに表示されます。

原因

コレクターとアグリゲーターのタイム・ゾーンが同一の設定になっていない可能性があります。

環境

アグリゲーターが影響を受けます。

問題の診断

すべてのアプライアンスが同じタイム・ゾーンに設定されていることを確認してください。次のコマンドを使用します。`show system clock timezone.`

問題の解決

コレクターとアグリゲーターが同じタイム・ゾーンで設定されていない場合は、CLI を使用してアプライアンスのタイム・ゾーンを構成してください。

```
store system clock timezone list
store system clock timezone <timezone>
```

以下のコマンドを使用して、アプライアンスでの時刻が正しいことを確認します。

```
show system clock datetime
store system clock datetime
```

日時は、以下のコマンドによって NTP サーバーを使用して同期化することもできます。

```
show system ntp all
store system ntp state
store system ntp server
```

親トピック: 統合

アグリゲーターで構成を復元した後に HY000 エラーが発生する

アグリゲーターで構成をリストアした後に HY000 エラーを受け取った場合は、ダミー・インポートを実行します。

症状

アグリゲーターまたは中央マネージャーの構成をリストアしたときに、以下のメッセージのいずれかまたは両方を受け取ります。

```
ERROR 1031 (HY000) at line 1: Table storage engine for 'GUARD_USER_ACTIVITY_AUDIT' doesn't have this option
ERROR 1031 (HY000) at line 1: Table storage engine for 'AGGREGATOR_ACTIVITY_LOG' doesn't have this option
```

原因

このエラー条件は、内部データベースで一時的な不一致がある場合に発生することがあります。

環境

コレクターおよびアグリゲーターが影響を受けます。

問題の解決

この問題を解決するには、ダミー・インポートを実行します。

親トピック: 統合

一元管理

- ユーザーが Guardium 管理対象ユニットで無効になっているが中央マネージャーで有効として表示される
  あるユーザーが、Guardium 管理対象ユニットで無効になっているが、中央マネージャーで有効として表示される場合は、ポータル・ユーザー同期を実行します。
- アップグレードされたユニットの新規バージョンを中央マネージャーが認識しない
  中央マネージャーが、アップグレードされたユニットの新規バージョンを認識しない場合は、アップグレードされたユニットを選択し、ページをリフレッシュします。
- スケジュールされたタスクが予定の時刻に起動しない
  スケジュールされたタスクが予定の時刻に起動しない場合は、ポータル・ユーザー同期の後に実行されるように、インポートの時刻をスケジュールします。
- GUI の「一元管理」ビューでのトルク例外
  「一元管理」でトルク例外が発生した場合は、カスタム・グループを削除して新規グループを作成します。

親トピック: 問題および解決策

ユーザーが Guardium 管理対象ユニットで無効になっているが中央マネージャーで有効として表示される

あるユーザーが、Guardium 管理対象ユニットで無効になっているが、中央マネージャーで有効として表示される場合は、ポータル・ユーザー同期を実行します。

症状

あるユーザーが管理対象ユニットで無効になっています。そのユーザーのアカウントが中央マネージャーで再有効化されましたが、管理対象ユニットでは引き続き無効として表示されています。そのユーザーのアカウントは、中央マネージャーでは有効であるものとして表示されます。

原因

中央マネージャー内のユーザーのアカウントが、管理対象ユニットと同期化されていません。

環境

中央マネージャー、コレクター、またはアグリゲーターの組み合わせが影響を受ける可能性があります。

問題の解決

中央マネージャーと管理対象ユニットの間で現在のユーザー状況を同期化するには、ポータル・ユーザー同期を実行します。

1. admin ユーザーとして中央マネージャーにログインします。
2. 「管理」 > 「一元管理」 > 「ポータル・ユーザー同期」をクリックして、「ポータル・ユーザー同期 (Portal User Synchronization)」を開きます。
3. 「今すぐ 1 回実行」をクリックします。

このようにしても、管理対象ユニットと中央マネージャーの間でユーザーのアカウントが同期化されない場合は、IBM Guardium 技術サポートにお問い合わせください。

親トピック: 一元管理

アップグレードされたユニットの新規バージョンを中央マネージャーが認識しない

中央マネージャーが、アップグレードされたユニットの新規バージョンを認識しない場合は、アップグレードされたユニットを選択し、ページをリフレッシュします。

症状

中央マネージャーは、管理対象の、アップグレードされたアグリゲーターまたはコレクターの新規バージョンを、直ちに認識しない場合があります。中央マネージャーから、新規バージョンを必要とするパッチをプッシュすると、ユニットがまだ以前のバージョンであることを示すエラーが出される可能性があります。

管理対象ユニットの古いバージョンが、引き続き GUI の「一元管理」ビューに表示されます。そのビュー内のユニットの ping 時間は、中央マネージャーと管理対象ユニットの間の通信が良好であることを示しています。

原因

新規バージョンの情報をプルするには、GUI をリフレッシュする必要があります。

環境

Guardium 中央マネージャーが影響を受けます。

問題の解決

GUI の「一元管理」ビューで、アップグレードされたユニットを選択し、「リフレッシュ」を押します。このアクションによって、ユニットから新規バージョンの情報がプルされます。

親トピック: 一元管理

スケジュールされたタスクが予定の時刻に起動しない

スケジュールされたタスクが予定の時刻に起動しない場合は、ポータル・ユーザー同期の後に実行されるように、インポートの時刻をスケジュールします。

症状

インポートが失敗し、agg_progress.log で以下のメッセージを受け取ります。

```
* 05/20 04:00:01 --- Import cannot start
(guard_agg|turbine_backup.sh|restore_from_file.pl already running)
* 05/20 20:00:46 --- Merge cannot start - aggregation still active
```

原因

中央マネージャーのポータル・ユーザー同期との競合があります。

環境

アグリゲーターが影響を受けます。

問題の診断

バックグラウンドで実行されているタスクを見つけます。「レポート」 > 「Guardium 運用レポート」 > 「統合/アーカイブ・ログ」をクリックして、「統合/アーカイブ・ログ」を開きます。

問題の解決

問題を解決するには、ポータル・ユーザー同期の後に実行されるように、インポートの時刻をスケジュールします。ポータル・ユーザー同期を 1 時間ごとに実行し、インポートの時刻を、その時刻の 30 分後にします。

親トピック: 一元管理

GUI の「一元管理」ビューでのトルク例外

「一元管理」でトルク例外が発生した場合は、カスタム・グループを削除して新規グループを作成します。

症状

Guardium GUI の「一元管理」ビューで特定のカスタム・グループを選択すると、グループ内の管理対象ユニットではなく、エラーが表示されます。

```
org.apache.torque.TorqueException: Failed to select one and only one row.
```

例外の発生後に、「一元管理」タブの下のどのグループまたはビューにもその例外が表示されます。GUI からログアウトして再度ログインするまで、その例外は以前に作業していたグループに対しても表示されます。

原因

このトルク例外は、グループ内の管理対象ユニットのうちの 1 つが、中央マネージャーではなく管理対象ユニットから登録抹消された場合に、発生する可能性があります。

環境

Guardium 中央マネージャーが影響を受けます。

問題の解決

カスタム・グループを削除して、同じメンバーを含む新規グループを作成します。

親トピック: 一元管理

S-TAP およびその他のエージェント

- IBM Security Guardium S-TAP のインストール時またはアップグレード時に AIX 6.1 で障害が発生する
  AIX 6.1 上で Guardium S-TAP をインストールまたはアップグレードするときにオペレーティング・システムで障害が発生する場合は、フィックスパック AIX 6.1 を適用します。
- Guardium COMM_EXIT_LIST for DB2 の構成時に共有メモリー領域を開くとエラーが発生する
  Guardium COMM_EXIT_LIST の構成時にエラー・メッセージを受け取った場合は、guardctl コマンドを使用して Db2 インスタンス所有者を許可します。
- Guardium が Informix から共有メモリー・トラフィックを収集できない
  Guardium が Informix から共有メモリー・トラフィックを収集できない場合は、検査エンジン構成を確認します。
- Guardium STAP ホスト内で CPU および I/O 使用量が高い
  CPU または I/O 使用量が高い場合は、すべての検査エンジンの構成を確認します。
- ログイン・パケットからの情報の欠落
  ログイン・パケットからの情報が欠落している場合は、S-TAP デバッグ・トレースおよび slon トレースを収集します。
- Nanny プロセスによってスニファーが強制終了される
  Nanny プロセスによってスニファーが強制終了される場合、着信するトラフィックが多すぎる可能性があります。
- スニファーが UNIX S-TAP に接続できない
- S-TAP を開始できない
  S-TAP を開始できない場合は、バッファー・サイズが大きすぎる可能性があります。
- Linux 上で S-TAP が自動的に開始されない
  Linux 上で Db2 または Oracle 向けの S-TAP エージェントが自動的に開始されない場合は、/etc/event.d/ ディレクトリーを確認します。
- S-TAP からの戻りが FIPS 140-2 準拠ではない
  FIPS 140-2 に関するエラーを受け取った場合は、「S-TAP 制御」ページで構成を変更します。
- S-TAP のアンインストール後も K-TAP カーネル・モジュールが存在している
  S-TAP のアンインストール後も K-TAP カーネル・モジュールが存在する場合は、手動で削除します。
- UNIX S-TAP が 16 を超える検査エンジンを読み取れない
  UNIX S-TAP が 16 を超える検査エンジンを読み取れない場合は、listen ポートのパラメーターを変更するか、PCAP を使用します。
- Windows S-TAP サービスが始動時にクラッシュする (エラー ID 1000)
  エラー ID 1000 により S-TAP がクラッシュする場合は、guard_tap_ini 構成ファイル内の SOFTWARE_TAP_IP パラメーターを確認します。
- Guardium システム上で z/OS S-TAP がアクティブと表示されない
  Guardium システム上で z/OS S-TAP がアクティブと表示されない場合は inspection-core を再始動します。

IBM Security Guardium S-TAP のインストール時またはアップグレード時に AIX 6.1 で障害が発生する

AIX 6.1 上で Guardium S-TAP をインストールまたはアップグレードするときにオペレーティング・システムで障害が発生する場合は、フィックスパック AIX 6.1 を適用します。

症状

AIX 6.1 上で Guardium S-TAP をインストールまたはアップグレードするときに、オペレーティング・システムで障害が発生します。AIX クラッシュ・メモリー・ダンプに、以下のスタック・トレースが表示されます。

```
Error ID: DD11B4AF Resource Name: SYSPROC
Detail Data: 00007FFFFFFFD080 0000000000473260
0000000000020000 8000000000029032

Symptom Information:
Crash Location: [0000000000473260] execvex_common+1880
Component: COMP Exception Type: 131

Stack Trace:
[0000000000473260] execvex_common+1880
[000000000047744C] execve+A8
[F1000000C083E84C] my_execve+424
```

原因

このクラッシュは、AIX バージョン 6.1 の既知の問題であり、execvex_common コード・パスでのシステム・クラッシュが原因で発生します。

環境

AIX 6.1 オペレーティング・システムにインストールされるすべての S-TAP が影響を受けます。

問題の解決

フィックスパック AIX 6.1 6100-08-04 を適用して問題を解決するには、http://www-01.ibm.com/support/docview.wss?uid=isg1IV50179 を参照してください。

Guardium COMM_EXIT_LIST for DB2 の構成時に共有メモリー領域を開くとエラーが発生する

Guardium COMM_EXIT_LIST の構成時にエラー・メッセージを受け取った場合は、guardctl コマンドを使用して Db2 インスタンス所有者を許可します。

症状

Guardium libguard を使用するように DB2 COMM_EXIT_LIST を構成して Db2 サーバーを再始動した後、Db2 diag ログで以下のエラーを受け取ります。

```
2013-06-28-11.41.12.306169-300 E870950E486 LEVEL: Severe
PID : 15764 TID : 139905833363200 PROC : db2sysc 0
INSTANCE: db2001 NODE : 000
APPHDL : 0-16
HOSTNAME: dbhost1
EDUID : 54 EDUNAME: db2agent () 0
FUNCTION: DB2 UDB, DRDA Communication Manager, sqljcCommexitLogMessage,
probe:234
DATA #1 : String with size, 91 bytes
WARNING: Shmem_access /.guard_writer0 failed Error opening shared memory area errno=2 err=8
```

原因

以下のメッセージは、Guardium ライブラリーが必要な共有メモリー・デバイスを作成できなかったことを示しています。

```
Shmem_access /.guard_writer0 failed
Error opening shared memory area
errno=2
err=8
```

guardctl コマンドを使用して、Db2 インスタンス所有者を許可されたユーザーとして追加する必要があります。

環境

Db2 Exit (バージョン 10) と S-TAP の統合を使用する Guardium コレクターが影響を受けます。

問題の解決

guardctl コマンドを使用して、Db2 インスタンス所有者を許可されたユーザーとして追加する必要があります。

1. Db2 インスタンスを停止します。

2. Db2 インスタンス所有者を許可します。
3. Db2 インスタンスを開始します。

Guardium Installation Manager (GIM) がインストールされていない場合は、以下のコマンドを使用して Db2 インスタンス所有者を許可します。

```
<guardium_installdir>/bin/guardctl authorize-user<db2 instance owner>
```

Guardium Installation Manager (GIM) がインストールされている場合は、以下のコマンドを使用して Db2 インスタンス所有者を許可します。

```
<guardium_installdir>/modules/ATAP/current/files/bin/guardctl authorize-user<db2 instance owner>
```

例えば、Db2 インスタンス所有者が db2001 であり、GIM が /usr/local/guardium にインストールされている場合、コマンドは `/usr/local/gim/modules/ATAP/current/files/bin/guardctl authorize-user db2001` です。

親トピック: S-TAP およびその他のエージェント

Guardium が Informix から共有メモリー・トラフィックを収集できない

Guardium が Informix から共有メモリー・トラフィックを収集できない場合は、検査エンジン構成を確認します。

症状

Guardium S-TAP が Informix から共有メモリー・トラフィックを収集できません。

原因

検査エンジンが正しく構成されていません。

環境

Informix システムからの S-TAP 収集がすべて影響を受ける可能性があります。

問題の解決

「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」で、検査エンジン構成を確認します。「プロセス名」フィールドの値が、データベース・サーバーでの以下のコマンドの結果と一致することを確認します。

```
ls -lrt /INFORMIXTMP/.inf.*
```

Informix: /INFORMIXTMP/.inf.sqlexec は、すべての Informix プラットフォームに適用します (Linux を除く)。Linux での Informix の例: /home/informix11/bin/oninit

このコマンドが値を返すためには、Informix が実行されていることが必要です。

Linux サーバーの場合は、共有メモリー・トラフィックを収集するように A-TAP が構成されている必要があります。 A-TAP 構成内の --db-info パラメーターと同じ値に設定してから、A-TAP をアクティブ化します。

親トピック: S-TAP およびその他のエージェント

Guardium STAP ホスト内で CPU および I/O 使用量が高い

CPU または I/O 使用量が高い場合は、すべての検査エンジンの構成を確認します。

症状

Guardium S-TAP プロセスによる CPU または I/O 使用量が高くなっています。

原因

以下の項目が一般的な原因です。

1. いずれかの検査エンジンの構成エラー。 検査エンジンにエラーがある場合は、S-TAP プロセスが頻繁に再始動するか、検査エンジンに繰り返し再接続しようとします。
2. S-TAP の K-TAP 部分が、S-TAP への確認要求とともに接続情報を送信している。このステップが遅延の原因となっています。
3. ORACLE RAC が使用されているが、量が多い可能性がある Oracle RAC トラフィックをモニターしないようにするための unix_domain_socket_marker パラメーターが、S-TAP 構成ファイル内に設定されていない。
4. ユーザー ID チェーン (UID チェーン) 機能が有効になっている (例えば、S-TAP 構成ファイル内のパラメーター hunter_trace=1)。ハンター・トレースは UID チェーンで使用され、S-TAP に対してかなり CPU を使用する場合があります。
5. ファイアウォールが有効になっている (firewall_installed=1)。 このファイアウォールによって、監視対象の新規セッションごとに判定が要求されるため、S-TAP のパフォーマンスが低下する可能性があります。

環境

AIX にインストールされている S-TAP

問題の解決

原因に応じて、対応するアクションを実行します。

1. すべての検査エンジンの構成を確認し、どのパラメーターにもエラーがないようにします。例えば、データベース・インストール・ディレクトリー、実行可能ファイル、ポート、および検査エンジンに使用可能なその他のパラメーターが、つづりや値の誤りがなく正しく設定されていることを確認します。
2. Set S-TAP 構成パラメーター ktap_fast_tcp_verdict を 1 に設定し (guard_tap.ini 構成ファイルで ktap_fast_tcp_verdict = 1 を設定)、S-TAP を再始動します。以下に使用可能な設定を示します。

   ktap_fast_tcp_verdict=0: KTAP は、ポートと IP をチェックして、セッションが検査エンジンによって構成されたデータベース接続であることを確認します。

   ktap_fast_tcp_verdict=1: KTAP は、セッションのポートが範囲内にある間は S-TAP に要求を送信しません。

3. UID チェーン機能が不要な場合は、hunter_trace=0 を設定し、S-TAP を再始動することによって無効にします。
4. SGATE が不要な場合は、firewall_installed=0 を設定し、S-TAP を再始動します。

親トピック: S-TAP およびその他のエージェント

ログイン・パケットからの情報の欠落

ログイン・パケットからの情報が欠落している場合は、S-TAP デバッグ・トレースおよび slon トレースを収集します。

症状

Guardium で、ログイン・パケットからの情報 (データベース・ユーザー名、ソース・プログラム、データベース名など) の欠落に関する問題が発生します。

原因

セッションが短すぎる場合、ログイン・パケットの情報が欠落することがあります。

環境

Guardium コレクターが影響を受けます。

問題の解決

Guardium S-TAP がインストールされているデータベース・サーバーから S-TAP デバッグ・トレースを収集し、コレクターから slon トレースを収集します。

これらのトレースの収集について詳しくは、『関連 URL』セクションの『技術情報』を参照してください。

1. 両方のトレースを同時に実行します。
2. 両方のトレースの実行中に、問題を再現する新規データベース・セッションを生成します。ログイン・パケットが送信されるのは、データベース接続が開いているときのみです。
3. 既存のレポートに、セッション開始、クライアント・ポート、およびサーバー・ポートを追加します。新規接続を使用して問題を再現したら、レポートをリフレッシュします。
4. セッション開始をチェックして、セッション中にトレースが実行されていることを確認します。
5. セッションを 5 分以上開いたままにして、スニファーがログイン・パケットを分析できるようにします。
6. フィールドが欠落しているセッションを送信します。セッションの生成に使用したアプリケーション名、データベース名、接続 DB ユーザー、接続タイプ、SQL ステートメント、およびその他の関連する詳細を明らかにします。
7. データベース・サーバーから S-TAP デバッグ・トレース・ファイルを収集し、Guardium コレクターから slon トレースを収集します。また、現在のスニファー関連の「Must Gather」サポート情報を収集します。

親トピック: S-TAP およびその他のエージェント

Nanny プロセスによってスニファーが強制終了される

Nanny プロセスによってスニファーが強制終了される場合、着信するトラフィックが多すぎる可能性があります。

症状

Guardium システム・ログ (メッセージ) またはアラートに、以下のようなメッセージが 1 回以上報告されます。

`Nanny プロセスのエラー状態。(Nanny process error condition.) Nanny プロセスによってスニファーが強制終了されました。(The nanny process killed the sniffer.) VmData は number であり、制限を超えました。(VmData was number and was over the limit.)`

原因

スニファー・メモリー使用量が使用可能メモリーの 90% を超えたため、Nanny プロセスがスニファーを再始動しました。これは製品の予期される動作です。

環境

Guardium コレクター

問題の解決

このメッセージが頻繁に表示される場合、Guardium システムに着信するトラフィックが多すぎます。このメッセージが表示されないようにするには、この Guardium システムへのトラフィックを減らします。例えば、一部の STAP を負荷が少ないコレクターに移動したり、ポリシー内で一部のトラフィックを無視したり、ロード・バラン

シングを実装してトラフィックを複数のコレクターに広げたりします。

メッセージがめったに表示されない場合は、トラフィックが一時的にスパイク状態であると考えられます。 メッセージが表示されないようにするには、スパイクの原因を特定し、トリガーを回避します。例えば、その時点で実行されていたプロセスを確認し、より多くのトラフィックを生成するものを識別します。このメッセージが常に特定のプロセスの実行と同時に表示される場合は、その時点の同時トラフィックを減らします。例えば、最も負荷が大きいプロセスを移動して別の時刻に実行することも、ポリシーを通じてこのトラフィックの一部を無視することもできます。

親トピック: S-TAP およびその他のエージェント

スニファーが UNIX S-TAP に接続できない

症状

別のスレッド数を指定すると (例えば、コマンド snif -t 20 を使用して 20 を指定する)、スニファーは UNIX S-TAP に接続できなくなります。GUI コンソールで、S-TAP の状況は非アクティブになっています。

原因

デフォルトでは、スニファーは 6 つのスレッドで開始されます。スレッドの数が制限を超えると、動作が未定義であるため、スニファーは UNIX S-TAP に接続できません。

環境

UNIX S-TAP が影響を受けます。

問題の解決

スレッドの数を減らして、接続を正常に確立できるようにします。

親トピック: S-TAP およびその他のエージェント

S-TAP を開始できない

S-TAP を開始できない場合は、バッファー・サイズが大きすぎる可能性があります。

症状

S-TAP を開始できず、以下のメッセージが表示されます。

```
mmap: 十分なスペースがありません (Not enough space)
初期化できません (Can't initialize): バッファー・ファイル /tmp/stapbuf/192.168.100.107.0.buf を mmap できません (Can't mmap buffer file /tmp/stapbuf/192.168.100.107.0.buf)
初期化エラー (Error Initializing): Stap は SQLGuard キューを初期化できません (Stap cannot initialize SQLGuard queue)
```

原因

S-TAP が、バッファー・ファイルに合う十分なメモリーを割り振ることができません。

問題の解決

S-TAP のバッファー・ファイル・サイズを小さくします。 サイズは、guard_tap.ini ファイルの buffer_file_size パラメーターで指定します。

親トピック: S-TAP およびその他のエージェント

Linux 上で S-TAP が自動的に開始されない

Linux 上で Db2 または Oracle 向けの S-TAP エージェントが自動的に開始されない場合は、/etc/event.d/ ディレクトリーを確認します。

症状

/etc/inittab ファイルに正しい U-TAP エントリーが表示されているにもかかわらず、Linux 上で S-TAP プロセスが自動的に開始されません。

原因

RedHat 6 などの各種 Linux ディストリビューションでは、etc/inittab ファイルを使用する従来の init デーモンの使用は非推奨になりました。 それらのディストリビューションでは、代わりに upstart と呼ばれる init プロセスを使用するようになりました。Upstart では、U-TAP などのプロセスの自動開始、停止、および respawn に /etc/event.d ディレクトリーと /etc/init ディレクトリーを使用します。

S-TAP インストーラーは、/etc/event.d ディレクトリーが存在するかどうかを検査するようになりました。 存在する場合は、upstart で使用するために /etc/init 内にエントリーが作成されます。存在しない場合は、従来の init デーモンで使用するために /etc/inittab 内にエントリーが作成されます。

upstart を持つシステムに何らかの理由で /etc/event.d がない場合は、代わりに inittab ファイルにデータが設定されます。S-TAP プロセスは、必要な場合に始動も respawn も行いません。

環境

Linux で稼働している S-TAP が影響を受けます。

問題の解決

/etc/event.d ディレクトリーが存在するかどうかを確認します。

/etc/event.d/ ディレクトリーが存在しない場合は、以下の手順を実行して状態を解決します。

1. 既存の S-TAP インストール済み環境をアンインストールします。
2. ユーザー root として /etc/event.d ディレクトリーを作成します (mkdir /etc/event.d)。
3. S-TAP をインストールします。

親トピック: S-TAP およびその他のエージェント

S-TAP からの戻りが FIPS 140-2 準拠ではない

FIPS 140-2 に関するエラーを受け取った場合は、「S-TAP 制御」ページで構成を変更します。

症状

サポート対象: - Solaris X86 - Linux x86/64 - Linux x86/32 - Linux S390X - Linux IA64 Not Supported: - Solaris SPARC - AIX PowerPC - HPUX RISC - HPUX IA64 - Linux PowerPC

S-TAP イベント・ログに以下のメッセージが表示されます。

```
LOG_ERR: Not FIPS 140-2 compliant - use_tls=0 failover_tls=1.
```

原因

FIPS 140-2 は、暗号モジュールに関する米国政府のセキュリティー基準です。このメッセージが表示される場合は、S-TAP 構成が政府の要件を満たしていないことを示しています。

注: このメッセージは、S-TAP にエラーが発生していることを示すわけではありません。

環境

Guardium S-TAP が影響を受けます。

サポート対象: Solaris X86; Linux x86/64; Linux x86/32; Linux S390X; Linux IA64

非サポート対象: Solaris SPARC; AIX PowerPC; HPUX RISC; HPUX IA64; Linux PowerPC

問題の解決

FIPS 準拠を有効にするには、guard_tap.ini ファイルに以下を設定する必要があります。

```
use_tls=1
failover_tls=0
```

その他の組み合わせでは FIPS モードがオフになり、エラー・メッセージが表示されます。

以下のいずれかの方法を使用して、構成を変更できます。

1. 「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」をクリックします。
2. 関連する S-TAP の詳細セクションを変更し、TLS チェック・ボックスを使用します。
3. S-TAP を再始動します。

DB サーバー上で guard_tap.ini ファイルを直接編集して、S-TAP を再始動することもできます。

親トピック: S-TAP およびその他のエージェント

S-TAP のアンインストール後も K-TAP カーネル・モジュールが存在している

S-TAP のアンインストール後も K-TAP カーネル・モジュールが存在する場合は、手動で削除します。

症状

Solaris サーバーから S-TAP をアンインストールした後も、K-TAP カーネル・モジュールが存在しています。

原因

Solaris サーバーから K-TAP カーネル・モジュールを削除するために、サーバーが正しく再始動されませんでした。

環境

S-TAP をアンインストールした後の Solaris サーバーが影響を受けます。

問題の診断

modinfo | grep ktap および ls -al /dev/*tap* の両方を実行して、Solaris サーバーで確認します。

問題の解決

以下の手順を実行して、K-TAP カーネルを手動で削除します。

1. /etc/init.d/upguard が削除されていることを確認します。
2. /kernel/drv/sparcv9/ktap* および /kernel/drv/ktap* を削除します。
3. modinfo | grep ktap を実行して、ロードされたドライバーの名前を取得します。
4. 次に、rem_drv<loaded driver> を実行します。例: `rem_drv ktap_36821`。
5. /dev/ktap* および `/dev/guard_ktap` を削除します。
6. サーバーを再始動します。
7. modinfo | grep ktap を実行して、以降はドライバーがロードされないようにします。
8. /etc/inittab から GIM および gsvr のエントリーを削除します (GIM のみを使用している場合)。
9. /usr/local/guardium 内に残っているファイルを手動でクリーンアップします。

親トピック: S-TAP およびその他のエージェント

UNIX S-TAP が 16 を超える検査エンジンを読み取れない

UNIX S-TAP が 16 を超える検査エンジンを読み取れない場合は、listen ポートのパラメーターを変更するか、PCAP を使用します。

症状

UNIX S-TAP が、検査エンジン設定内の最初の 16 個の `port_range` 定義しか読み取りません。

原因

設計上、K-TAP が読み取れる `port_range` 定義は 16 個のみです。

環境

K-TAP を使用し、16 を超える検査エンジンを定義する UNIX S-TAP が影響を受けます。

問題の解決

パラメーター `port_range_start` および `port_range_end` を使用して、必要なすべてのポートを最初の検査エンジン定義に組み込みます。このアクションによって、指定したポート範囲からのすべてのトラフィックがインターセプトされます。範囲内の一部のポートを無視する必要がある場合は、不要なサーバー・ポートを無視するようにポリシーを定義できます。

以下の例では、モニター対象のターゲット・ポートとして 50000 から 50020 の listen ポートを定義しています。

```
[DB_0]
port_range_end=50020
port_range_start=50000
```

あるいは、`ktap_local_tcp=1` および `devices=<device_name>` を設定して、TCP 接続に PCAP を使用します。

```
[TAP]
ktap_local_tcp=1
devices=<Network Device Name>
```

親トピック: S-TAP およびその他のエージェント

Windows S-TAP サービスが始動時にクラッシュする (エラー ID 1000)

エラー ID 1000 により S-TAP がクラッシュする場合は、guard_tap_ini 構成ファイル内の SOFTWARE_TAP_IP パラメーターを確認します。

症状

Windows サーバー上の S-TAP が始動しません。Windows イベント・ログに、Guardium S-TAP からのイベント ID 1000 で示されたエラーが表示されます。

```
Log Name:      Application
Source:        Application Error
Event ID:      1000
Task Category: (100)
Level:         Error
Keywords:      Classic
記述:
Faulting application name: guardium_stapr.exe, version: 9.0.0.0
Exception code: 0x40000015
```

原因

guard_tap.ini ファイルに誤った SOFTWARE_TAP_IP が指定されていることが原因で、S-TAP は Windows システムに接続できません。

環境

Windows でのすべての Guardium S-TAP が影響を受けます。

問題の解決

guard_tap.ini 構成ファイル内の `SOFTWARE_TAP_IP` パラメーターが、Windows サーバーの正しい IP アドレスと一致することを確認します。このパラメーターは、インストール CLI パラメーターまたは IBM Guardium Installation Manager (GIM) パラメーターで渡されます。

親トピック: S-TAP およびその他のエージェント

Guardium システム上で z/OS S-TAP がアクティブと表示されない

Guardium システム上で z/OS S-TAP がアクティブと表示されない場合は inspection-core を再始動します。

症状

Guardium システム上で z/OS S-TAP を初めて始動した後、z/OS S-TAP がアクティブと表示されません。ポリシーは、Db2 または IMS コレクション・プロファイルを使用して正しく構成され、インストールされています。z/OS S-TAP は、ポート 16022 を使用するように適切に構成されています。メインフレーム上のすべてのメッセージは接続を示しています。

原因

コレクターが、作成および構成されて以降コレクターとしてアクティブに使用されていない場合は、スニファーがポート 16022 でタイムアウトするようです。

環境

z/OS が影響を受けます。

問題の解決

CLI コマンド restart inspection-core を使用して、inspection-core を再始動します。

親トピック: S-TAP およびその他のエージェント

GIM

親トピック: 問題および解決策

Guardium Installation Manager (GIM) のインストール時にエラーが発生する

GIM が正しくインストールされない場合は、ディレクトリーを手動で作成します。

症状

Guardium Installation Manager (GIM) を RHEL6 にインストールしようとしたときに、以下のエラー・メッセージが表示されます。

```
cp: cannot stat `/usr/local/GIM/modules/central_logger.log': No such file or directory Installation failed
```

原因

RedHat 6 などの各種 Linux ディストリビューションでは、etc/inittab ファイルを使用する従来の init デーモンの使用は非推奨になりました。それらのディストリビューションでは、代わりに Upstart と呼ばれる init プロセスを使用するようになりました。Upstart は、プロセスを自動的に開始、停止、および respawn するために、/etc/event.d ディレクトリーおよび /etc/init ディレクトリーを使用します。

環境

Guardium Installation Manager (GIM) が影響を受けます。

問題の解決

この問題を修正するには、以下の手順を実行します。

- 部分的な GIM インストールを削除します。
- mkdir /etc/event.d コマンドによって手動で /etc/event.d ディレクトリーを作成します。

- GIM インストーラーを実行します。

親トピック: GIM

Windows で Guardium Installation Manager (GIM) サービスが開始しない

Windows で Guardium Installation Manager (GIM) サービスが開始しない場合は、32 ビット・アプリケーション用に予約されているフォルダーに GIM を再インストールします。

症状

Guardium Installation Manager (GIM) を Windows に正常にインストールした後で、サービスが実行されていないことに気付きます。

原因

GIM は 32 ビット・アプリケーションです。64 ビットの Windows を使用している場合、Program Files(x86) ではなく Program Files に GIM がインストールされている可能性があります。

環境

GIM が影響を受けます。

問題の解決

GIM を Program Files(x86) にインストールしてください。これが 32 ビット・アプリケーション用に予約された Windows フォルダーです。

親トピック: GIM

ファイル・アクティビティー

- ファイル・アクティビティーが調査ダッシュボードにもレポートにも記録されない
- 取り外し可能ディスクのファイル・アクティビティーが調査ダッシュボードのログに記録されない
- ファイル・アクティビティーがレポートで表示されるが、調査ダッシュボードで表示されない
- 分類結果で一部のファイルが欠落する
- レポートおよび調査ダッシュボードにファイル・ディスカバリー (資格) 結果が一部しか表示されない
  レポートおよび調査ダッシュボードにディスカバリー (資格) 結果が一部しか表示されない。
- レポートおよび調査ダッシュボードでファイル分類結果が欠落する
- FAM バンドルをインストールできない
  GIM クライアントをインストールした後に FAM バンドルのインストールが失敗する。

親トピック: 問題および解決策

ファイル・アクティビティーが調査ダッシュボードにもレポートにも記録されない

症状

調査ダッシュボードおよび事前定義レポート (「ファイル・アクティビティー」、「ファイル・ライセンス」、「ファイル: クライアントあたりのアクティビティー数」、「ファイル: サーバーあたりのアクティビティー数」、「ファイル: ユーザーあたりのアクティビティー数」、「ファイル: 特権」など) にファイル・アクティビティーが記録されない。

問題の解決

以下を確認します。

- FAM ライセンスがインストールされているか、および S-TAP がアクティブか確認します。
- アクティビティーのファイル・サーバーに root としてログインしていないことを確認します。root (UID0) からのアクティビティーは、デフォルトではログに記録されません。
- Linux/AIX では、ポリシー・ルールで指定されているファイル・パスを確認します。例えば、/testdir/ は、testdir という名前のディレクトリー内のファイルではなくて、testdir という名前のファイルをモニターします。/testdir/* を指定して、testdir ディレクトリー内のファイルをモニターします。
- Windows では、ドメインを使用し、ポリシー・ルールでユーザーを指定する場合、ドメインが指定されていることを確認します。例えば、Maryjane のみではなく svldev¥Maryjane を使用します。

親トピック: ファイル・アクティビティーのトラブルシューティング

取り外し可能ディスクのファイル・アクティビティーが調査ダッシュボードのログに記録されない

症状

取り外し可能ディスクのファイル・アクティビティーが調査ダッシュボードのログに記録されない

環境

FAM_SCAN_EXCLUDE_REMOTE_DIRECTORIES が true に設定されています

問題の解決

取り外し可能ディスクをマウントする*前に*、ファイル・アクティビティー・モニター・ポリシーをインストールしてください。
親トピック: ファイル・アクティビティーのトラブルシューティング

ファイル・アクティビティーがレポートで表示されるが、調査ダッシュボードで表示されない

症状

ファイル・アクティビティーが事前定義レポートには表示されるが、調査ダッシュボードには表示されない。

問題の解決

Guard API を使用して構成を検査します。

- クイック検索にクロール・データを送信するには、以下を使用します: grdapi enable_fam_crawler activity_schedule_interval=2 activity_schedule_units=MINUTE entitlement_schedule_interval=10 entitlement_schedule_units=MINUTE
- (違反も含めるオプションを指定して) クイック検索を有効にするには、以下を使用します: grdapi enable_quick_search includeViolations=true schedule_interval=2 schedule_units=MINUTE

親トピック: ファイル・アクティビティーのトラブルシューティング

分類結果で一部のファイルが欠落する

症状

分類結果で一部のファイルが欠落する。

原因

以下は、分類でサポート*されない*ファイル・タイプです: DAT、JPG、JPEG、GIF、TIF、TIFF、BMP、WAV、MOV、MP3、MP4、AVI、MPG、WMA、WMV、P7S、XFDL、XFD、FRM、JAR。

親トピック: ファイル・アクティビティーのトラブルシューティング

レポートおよび調査ダッシュボードにファイル・ディスカバリー (資格) 結果が一部しか表示されない

レポートおよび調査ダッシュボードにディスカバリー (資格) 結果が一部しか表示されない。

症状

レポートおよび調査ダッシュボードに表示されるディスカバリー (資格) 結果が不完全である。一部のファイルの結果が表示されない。

問題の解決

ディスカバリー用の GIM 構成に、文書のタイプおよびロケーションが含まれていることを確認します。以下の GIM 構成パラメーターを確認します。

- FAM_SCAN_EXCLUDE_FILES
- FAM_SCAN_EXCLUDE_DIRECTORIES
- FAM_SCAN_EXCLUDE_EXTENSIONS
- FAM_SCAN_EXCLUDE_FILES
- FAM_SCAN_MAX_DEPTH

親トピック: ファイル・アクティビティーのトラブルシューティング

レポートおよび調査ダッシュボードでファイル分類結果が欠落する

症状

レポートおよび調査ダッシュボードでファイル分類結果が欠落する。

原因

分類は、メタデータ・ディスカバリーの後に実行される追加プロセスです。

問題の解決

分類に使用される IBM Content Classification エンジン (http://www-01.ibm.com/support/docview.wss?uid=swg27020838) のソフトウェア要件が満たされていると仮定した場合、以下の GIM 構成を確認します。

- GIM パラメーターの FAM_IS_DEEP_ANALYSIS が TRUE であることを確認します。
- FAM_ICM_CLASS_DECISION_PLANS 設定で判定プラン名が正しいこと、および判定プランのリストがセミコロンで区切られていることを確認します。
- リストされているすべての判定プラン (.dpn) ファイルが、ファイル・サーバーの次の場所に存在することを確認します: %FAM_HOME%¥conf¥ContentClassification

ユーザーの処置: オプション。特定のユーザーが実行する特定のアクションがある場合は、1 つ以上の ts*Response エレメントを使用します。

親トピック: ファイル・アクティビティーのトラブルシューティング

FAM バンドルをインストールできない

GIM クライアントをインストールした後に FAM バンドルのインストールが失敗する。

症状

FAM バンドルをインストールしようとすると、システムが次のようなメッセージで応答する。

```
-1、GIM - 障害点 : dependancy_violation (従属関係違反 (FAM) : 必須の従属関係が欠落しています - GIM.pm 行 3176 の STAP、<MYFILE> 行 20。
(-1,GIM - Failure point : dependancy_violation (Dependancy violation (FAM) : Missing mandatory dependency - STAP at GIM.pm line
3176, <MYFILE> line 20.)
```

原因

FAM バンドルをインストールする前に S-TAP バンドルをインストールする必要があります。

問題の解決

FAM バンドルをインストールしてください。ファイル・アクティビティー・モニター・コンポーネントのインストールおよびアクティブ化を参照してください。
親トピック: ファイル・アクティビティーのトラブルシューティング

Guardium システムのインストール

- S-TAP のインストール中にチェックサム・エラーが発生する
  チェックサム・エラーを受け取った場合は、FTP クライアントで転送モードをバイナリーに設定します。
- Guardium S-TAP が cp: illegal option - f のエラー・メッセージを返す
  S-TAP のインストールが cp: illegal option - f で失敗した場合は、which cp コマンドを実行し、ファイル・パスを変更します。
- 新規 Guardium パッチのインストールが完了しない
  新規 Guardium パッチのインストールを完了できない場合は、プロセスへの介入を停止し、パッチを再インストールします。
- 新規 Guardium S-TAP のインストール後にファイルまたはディレクトリーが欠落している
- Guardium のインストール時にパーティション・エラーが発生する
  パーティション・エラーを受け取った場合は、「カスタム」インストールを選択し、ディスクのロケーションとサイズを明示的に指定します。
- パッチ・インストールが失敗する: No such file or directory
  パッチ・インストールが失敗した場合は、ファイルが、ダウンロードされたパッチの MD5SUM と一致することを確認します。

親トピック: 問題および解決策

S-TAP のインストール中にチェックサム・エラーが発生する

チェックサム・エラーを受け取った場合は、FTP クライアントで転送モードをバイナリーに設定します。

症状

UNIX または Linux で Guardium S-TAP をインストールするために S-TAP インストーラーを実行したときに、以下のようなエラーを受け取ります。

```
./guard-stap-v81_r26808_1-aix-6.1-aix-powerpc.sh
Verifying archive integrity...Error in checksums: 2082112805 is
different from 3728267449
```

原因

インストーラー・ファイルが破損しています。ファイルがデータベース・サーバーに転送されたとき、または製品がダウンロードされたときに、ファイルが破損しました。

環境

UNIX または Linux 上の S-TAP が影響を受けます。

問題の解決

この問題を解決するには、FTP クライアントで転送モードがバイナリーに設定されていることを確認してください。次に、再度データベースへの転送を試みてください。プロセスが失敗する場合は、製品を再度ダウンロードしてください。

親トピック: Guardium システムのインストール

Guardium S-TAP が cp: illegal option - f のエラー・メッセージを返す

S-TAP のインストールが cp: illegal option - f で失敗した場合は、which cp コマンドを実行し、ファイル・パスを変更します。

症状

S-TAP のインストールが失敗し、以下のエラー・メッセージが表示されます。

```
A directory called 'guardium' containing Guardium software needs to be created under a path provided.
Enter the path prefix [/usr/local]? /opt/guardium
Directory /opt/guardium/guardium/guard_stap does not exist, would you like to create it [Y/n]? Y
Run STAP as root, or as user 'guardium' [R/u]? R
Please be patient... This might take more than a minute.
Copying installation files...
cp: illegal option -- f
UX:vxfs cp: INFO: V-3-21462: Usage: cp [-i] [-p] f1 f2
cp [-i] [-p] f1 ... fn d1
cp [-i] [-p] [-r|-R] [-e { force | ignore | warn}] d1 d2
```

原因

/usr/bin/cp へのパスが、インストーラーが予期していたパスとは異なります。

環境

UNIX/Linux データベース・サーバーが影響を受けます。

問題の解決

which cp コマンドを実行します。

which cp を実行して /usr/bin/cp 以外の値が返された場合は、export PATH=/usr/sbin:/usr/bin:$PATH コマンドを実行します。

which cp コマンドを再実行して、パスが /usr/bin/cp になっていることを確認してください。

親トピック: Guardium システムのインストール

新規 Guardium パッチのインストールが完了しない

新規 Guardium パッチのインストールを完了できない場合は、プロセスへの介入を停止し、パッチを再インストールします。

症状

新規パッチのインストール時に、インストールが完了しません。CLI コマンド show system patch installed の状況列に、以下のいずれかのメッセージが表示されます。

```
STEP: Setting “java” off
STEP: Setting “amei” off
STEP: Setting “sqlw” off
```

原因

マシン上の Tomcat、検査コア、または別のプロセスが、パッチ・インストールに干渉します。

環境

コレクター、アグリゲーター、および中央マネージャーが影響を受けます。

問題の解決

新規 Guardium パッチをインストールするには、すべてのプロセスがインストールに干渉しないようにします。

1. delete scheduled-patch コマンドを使用して、正常にインストールできなかったパッチを削除します。
2. restart system コマンドを使用して、システムを再始動します。
3. システムの再始動後に、stop gui コマンドと stop inspection-core コマンドを使用して、GUI および検査コアを停止します。
4. パッチを再インストールし、restart gui コマンドおよび start inspection-core コマンドを使用して、GUI および検査コアを再始動します。

親トピック: Guardium システムのインストール

新規 Guardium S-TAP のインストール後にファイルまたはディレクトリーが欠落している

症状

S-TAP をインストールしようとしたときに、以下のエラー・メッセージを受け取ります。

```
Tap_controller::init failed Opening pseudo device /dev/guard_ktap No such file or directory
```

さらに、/dev/*ktap* が存在しません。

原因

K-TAP デバイス作成の失敗については、多数の理由が考えられます。最も一般的な原因を以下に示します。

- Linux カーネル用の K-TAP モジュールを含め、モジュール・ファイルを使用しなかった。
- モジュール・ファイルから K-TAP モジュールをロードするための Flex Loading オプションを指定しなかった。
- 古いインストール済み環境の以前の K-TAP モジュールが、引き続き実行されているかインストールされている。

環境

IBM Guardium S-TAP 製品をインストールできるすべての Linux および UNIX オペレーティング・システムが影響を受けます。

問題の解決

この問題を解決するには、以下の手順を実行します。

1. これらのコマンドは、root として実行してください。

   ```
   <STAP directory>/KTAP/guard_ktap_loader stop
   <STAP directory>/KTAP/guard_ktap_loader uninstall
   <STAP directory>/KTAP/guard_ktap_loader install
   <STAP directory>/KTAP/guard_ktap_loader start
   ```

2. ls /dev/*ktap* コマンドによって、K-TAP デバイスが作成されたかどうかを確認します。作成された場合、問題は解決しています。作成されていない場合は、次のステップに進みます。
3. S-TAP プロセス guard_stap が実行されている場合は、これを停止します。ps -ef | grep guard_stap コマンドを使用して、このプロセスが実行されているかどうかを確認できます。
4. ps -ef | grep guard_stap コマンドを使用して、S-TAP プロセスが実行されていないことを確認します。
5. S-TAP をアンインストールします。
6. S-TAP ディレクトリーがなくなっていることを確認します。
7. 古いインストール済み環境の K-TAP モジュールがまだ実行されているかどうかを確認します。ご使用のオペレーティング・システムに該当するコマンドを使用してください。

   ```
   Linux    : lsmod | grep ktap
   Solaris  : modinfo | grep  tap
   HP-UX    : lsdev | grep tap
   AIX      : genkex | grep tap
   ```

   ktap_<release> などのデバイスがリストされている場合、K-TAP モジュールが実行されています。
8. 前のステップで、K-TAP モジュールが実行されていることが分かった場合、以下のステップを実行して、K-TAP モジュールを停止し、アンインストールします。

   ```
   <STAP directory>/KTAP/guard_ktap_loader stop
   <STAP directory>/KTAP/guard_ktap_loader uninstall
   ```

   サーバーを再始動します。
9. Guardium Installation Manager (GIM) を使用する場合、「管理」 > 「モジュール・インストール」 > 「クライアント別の設定 (レガシー)」に移動し、クライアントを選択して「クライアントのリセット」をクリックします。サーバーが GIM GUI のクライアント・リストに再度表示されるまで待機します (通常は数分間)。
10. S-TAP を再インストールします。GIM を使用して S-TAP をインストールする場合は、GIM および以下のコマンドを使用して S-TAP バンドルを再インストールしてください。

    ```
    KTAP-ALLOW_COMBOS=Y
    KTAP_LIVE_UPDATE=Y
    KTAP_ENABLED=Y
    ```

親トピック: Guardium システムのインストール

Guardium のインストール時にパーティション・エラーが発生する

パーティション・エラーを受け取った場合は、「カスタム」インストールを選択し、ディスクのロケーションとサイズを明示的に指定します。

症状

VMWare で Guardium アプライアンスをインストールすると、以下のエラーを受け取ります。

```
Error Partitioning
Could not allocate requested partitions:
Partitioning failed: Could not allocate partitions as primary partitions.
Not enough space left to create partition for /boot.
```

原因

VMWare で Guardium システムをインストールするときに「標準 (Typical)」を選択した場合、VMWare は、VMWare で OS タイプに対して事前定義された構成パラメーターを使用します。これらの構成パラメーターは、このインストールには適さない場合があります。

環境

すべての Guardium 構成 (コレクター、アグリゲーター、中央マネージャー) が影響を受けます。

問題の解決

「カスタム」インストールを選択し、ディスクのロケーションとサイズを明示的に指定します。モニターおよび監査のニーズを満たすために十分な大きさのディスク・サイズを指定します。これが構成された後には、Guardium で、システムにディスク・スペースを追加する操作はサポートされなくなります。

親トピック: Guardium システムのインストール

パッチ・インストールが失敗する: No such file or directory

パッチ・インストールが失敗した場合は、ファイルが、ダウンロードされたパッチの MD5SUM と一致することを確認します。

症状

Guardium でのパッチ・インストールが失敗し、「`patch.reg: No such file or directory`」というエラーが表示されます。

原因

以下のケースでは、パッチ・インストールが失敗する可能性があります。

- パッチがバイナリー・モードでダウンロードされず、ファイルが破損した。
- 圧縮ファイル自体が Guardium システムにアップロードされた。
- Guardium サポートからパッチを受け取り、パッチのファイル名の接頭部として PMR 番号が付加されている。
- パッチが Windows FTP サーバーから Guardium にアップロードされた。

環境

コレクター、アグリゲーター、および中央マネージャーが影響を受けます。

問題の解決

ファイルの内容が、ダウンロードされたパッチの MD5SUM と一致することを確認します。圧縮ファイルを解凍できないか、MD5SUM が一致しない場合は、ファイルをバイナリー・モードでダウンロードしてください。

圧縮ファイル自体が Guardium システムにアップロードされた場合は、圧縮ファイルを解凍し、パッチのみをアップロードしてください。

ファイル名の接頭部として PMR 番号が付加されている場合は、その番号を削除してから、パッチを Guardium システムにアップロードしてください。

パッチが Windows FTP サーバーからアップロードされる場合は、大/小文字を正しく区別して正確なファイル名を指定してください。

親トピック: Guardium システムのインストール

S-TAPs およびその他のエージェント

Guardium の S-TAPs は、データベース・サーバー・システムまたはファイル・サーバー・システムにインストールされる、単純なソフトウェア・エージェントです。S-TAPs は、データベースやファイルのトラフィックをモニターし、そのトラフィックに関する情報を Guardium システムに転送します。K-TAPs や A-TAPs などのその他のエージェントによって、補足的な機能が実行されます。

- S-TAP のインストール
  S-TAP は、モニター対象のデータベース・システムまたはファイル・システムが含まれているサーバーにインストールできます。S-TAP のインストールには、いくつかのオプションがあります。
- エンタープライズ・ロード・バランシング
  エンタープライズ・ロード・バランサーは、管理対象ユニットをシステムの負荷と利用可能性に基づいて動的に S-TAP エージェントに割り当てます。
- Kerberos 認証データベース・トラフィック
- 出口ライブラリーの使用
  出口ライブラリーは、出口メカニズムを使用して Guardium ライブラリーをデータベースに組み込みます。出口ライブラリー、つまり出口モジュールは、Guardium S-TAP と直接通信してデータベース・トラフィックを転送します。
- 特別な環境での構成 (Linux、Solaris、HP-UX、AIX)
  ゾーン、RAC、WPAR、クラスターがあるシステムでは、以下の該当する手順を使用してください。
- S-TAP 管理ガイド
  Guardium の S-TAP® は、データベース・サーバー・システムにインストールされる、単純なソフトウェア・エージェントです。
- S-TAP を管理するための Guardium システムの構成
  Guardium GUI から S-TAP を管理するには、事前に Guardium システムを構成し、検査エンジンを再始動します。
- S-TAP 認証
  この機能を使用して、無許可の S-TAP が Guardium システムに接続することをブロックします。
- SSL 証明書を使用する S-TAP 認証のセットアップ
  S-TAP サーバーと Guardium システムの間の認証をセットアップします。
- S-TAP スループットの増加
  複数の Guardium システムに報告する S-TAP を構成すると、データのスループットを増やすことができます。
- UNIX S-TAP
  UNIX S-TAP をインストールして構成します。
- Windows S-TAP
  このセクションは、Windows S-TAP の構成に関する情報を得るために利用してください。
- S-TAP のディスカバリー
  S-TAP が定期的にデータベース・インスタンスを検出し、現在のアクティブな S-TAP システムにその結果を送信できるようにします。
- A-TAP の管理
  A-TAP は application-level tapping の省略形です。A-TAP はアプリケーション層に配置され、暗号化されたデータベース・トラフィックのモニターをサポートします。このモニターは、K-TAP によってカーネルで実行することはできません。

- Tee
  Tee は非推奨になりました。この情報は、参照用としてのみ記載しています。
- GUI からの S-TAP の構成
  S-TAP エージェントをデータベース・サーバーにインストールした後、GUI から S-TAP の構成を実行できます。
- S-TAP 構成パラメーターの編集
  S-TAP をインストールしてからその構成を変更するにはいくつかの方法があります。
- 遅延クラスター・ディスク・マウントの構成
  このトピックは、Oracle、Informix®、および DB2® の各データベース・サーバーにのみ適用されます。
- S-TAP 状況モニター
  S-TAP 状況モニターを使用すると、ご使用の S-TAP の現在の状況を表示したり、問題を調査したりすることができます。
- S-TAP 検査結果の確認
  S-TAP 検査プロセスはいくつかの構成パラメーターを確認し、検査エンジンに接続しようとします。結果は S-TAP 状況モニター・ページに表示されます。
- S-TAP 検査スケジュールの構成
  S-TAP 検査を実行するためのスケジュールを構成できます。
- Linux プラットフォームでの S-TAP の問題のトラブルシューティング
  「システム・ビュー」の「S-TAP 状況モニター」タブを使用して、問題の調査を行うことができます。 他のツールを使用しなければならない場合があります。特に、検査エンジンを検査できないデータベースをモニターしている場合です。
- S-TAP 動作のモニター
  S-TAP モニター (guard_monitor) は、S-TAP のパフォーマンスと反応性をモニターするために設計されたプロセスです。さまざまなしきい値に基づいて、特定のアクションを実行できます。
- 「S-TAP イベント」パネル
  「S-TAP イベント」パネルを使用して、S-TAP によって出力されるイベント・メッセージを表示することができます。
- S-TAP レポート
  デフォルトでは、このトピックで説明するレポートが「レポート」パネルに表示されます。
- S-TAP エラー・メッセージ
  以下のリストは、S-TAP が生成するエラー・メッセージをアルファベット順に説明します。
- S-TAP 付録
  このセクションでは、Informix のあるバージョンから別のバージョンへの移行について詳述します。
- コマンド行からの CAS のインストール、始動、停止
  以下のコマンドを使用して、CAS をインストール、始動、および停止します。
- IMS 定義
  IMS 定義により、Guardium システムから監査対象の IMS 環境への接続が確立されます。
- Db2 for i S-TAP
  Guardium Db2 for i S-TAP を使用して、IBM i 上のあらゆるデータベース・アクセスをモニターおよびレポートすることができます。これには、ネイティブのデータベース入出力操作または SQL アクセスを使用するあらゆるプログラム (RPG など) が含まれます。
- IBM Security Guardium S-TAP for z/OS
  IBM Security Guardium S-TAP for z/OS® ソリューションは、DB2 on z/OS、Data Sets on z/OS、または IMS™ on z/OS のデータ・アクセス情報を収集し、相互に関連付けて、監査員がビジネス・アクティビティーを包括的に把握できるようにするツールです。

S-TAP のインストール

S-TAP は、モニター対象のデータベース・システムまたはファイル・システムが含まれているサーバーにインストールできます。 S-TAP のインストールには、いくつかのオプションがあります。

S-TAP のインストールの概要

S-TAP をデータベース・サーバーにインストールする場合は、S-TAP からデータを受信する Guardium システムの IP アドレスまたは完全修飾ホスト名を指定する必要があります。 S-TAP が Guardium システムに接続されていると、残りの S-TAP 構成パラメーターは、すべて Guardium システムの「管理コンソール」から設定できます。

注: インストール中に S-TAP インストーラーは、カーネルのバージョンに合った K-TAP を使用できるかどうか検査します。K-TAP をインストールできない場合や、K-TAP が開始されない場合、ユーザーはインストールを続行するかどうかの確認を求められます。

S-TAP 用のインストール・ディレクトリーは、存在しないか、または空である必要があります。既にファイルが格納されているディレクトリーに、S-TAP をインストールすることはできません。

S-TAP をインストールする前に、IBM Security Guardium バージョン 10.1 のシステム要件を調べて、ご使用のデータベースおよびオペレーティング・システムのバージョンがサポートされていることを確認してください。

S-TAP をインストールして使用を開始するには、2 つの重要なタスクを実行する必要があります。

1. データベース・サーバーに S-TAP をインストールします。
2. 適切なトラフィックをモニターするように、S-TAP を構成します。

これらのタスクについては、本セクションと後続のセクションで説明します。

インストール方式

データベース・サーバーに S-TAP および他のエージェントをインストールするための推奨される方式は、Guardium Installation Manager (GIM) を使用する方式です。GIM を使用すると、個別サーバーまたはサーバーのグループ上でエージェントをインストール、アップグレード、および管理することができます。また、GIM は、GIM の制御下でインストールされたプロセスもモニターします。 GIM を使用すると、パラメーターの変更や他の管理タスクの実行が可能です。 GIM の詳細については、Guardium Installation Manager のセクションを参照してください。

場合によっては、S-TAP をローカルにインストールすることもできます。 これを行うには、対話式インストーラーまたはコマンド行を使用することができます。 このセクションでは、これらの方法について説明します。

S-TAP を UNIX サーバーにインストールする場合、インストール・プログラムによって Guardium グループが存在するかどうかが確認されます。 このグループが存在しない場合は、インストール・プログラムによって作成されます。A-TAP や Db2 出口などの特定のコンポーネントや機能を使用する場合は、適切に機能するように、ユーザー

をこのグループに追加する必要があります。 これらの要件については、この情報の関連セクションで説明します。

S-TAP のインストール前提条件

以下の表に、S-TAP をサポートするために特定のリリースまたはパッチ・レベルでインストールするか、あるいは構成する必要がある、データベース・コンポーネントをリストします。

表 1. データベース・コンポーネント

コンポーネント	前提条件
HP-UX での CAS	Java™ 1.5 以上
その他の UNIX での CAS	Java 1.4.2 以上
Windows での CAS	CAS で MS SQL サーバーのイベント・ログをモニターする場合、Microsoft Windows リソース・キットに含まれる dumpel.exe プログラムを、データベース・サーバーにインストールする必要があります。このプログラムが c:¥Program Files¥Resource Kit¥ ディレクトリー内にあることを確認します。存在しない場合は、Microsoft からダウンロードできます。
S-TAP® (すべての UNIX)	TEE モニター方式とハンター・コンポーネントと使用する場合は、Perl 5.8.0 以降
Red Hat Linux V4 上の S-TAP	MAKE バージョン 3.81 以降。MAKE ユーティリティーのバージョンを確認するには、`make -v` コマンドを発行します。
Oracle ASO、SSL AIX® - すべて	AIX 5.3 の場合は、LDR_PRELOAD をサポートするためにテクノロジー・レベル 5 以降が必要です。 AIX 6 と 7 には、このサポートが含まれています。
Oracle ASO、HP-UX 11.11	LD_PRELOAD のインストールが必須。パッチ PHSS_28436 以降でインストールされる。
TLS	UNIX サーバー上の S-TAP では、/dev/random または /dev/urandom がサーバー上にあること。 UNIX サーバーと Windows サーバーの場合は、『Guardium® のポート要件』を参照して、TLS ポートの要件を確認してください。

注: Java 1.6.0 のインストール中、またはアップグレード中に JVM から、DLL が見つからない、ダイナミック・リンク・ライブラリー MSVCR71.dll が指定されたパスで見つからないというエラーが生成される場合があります。このエラーは、次の 2 つの回避策のいずれかによって修正できます。1) 異なる (別のリリースの) JVM を使用する (その JVM が対象のシステムで使用可能な場合)、または、2) Microsoft からこの DLL をダウンロードして、Windows のシステム・ディレクトリーに配置する。
注:

GIM または S-TAP をインストールする場合、ユーザーおよびグループの作成および削除を行うために、root ユーザーである必要があります。

表 2. プラットフォームごとの要件のタイプ

要件タイプ	HP-UX	Solaris	AIX	Linux
ファイルが存在する	/bin/sh	/bin/sh	/bin/sh	/bin/sh
ファイルが存在する	/bin/sed または /usr/bin/sed	/bin/sed または /usr/bin/sed	/bin/sed または /usr/bin/sed	/bin/sed または /usr/bin/sed
ファイルが存在する	tar、awk、grep、tr	tar、awk、grep、tr	tar、awk、grep、tr	tar、awk、grep、tr
ファイルが存在する	prealloc	dd および /dev/zero	dd および /dev/zero	dd および /dev/zero
ファイルが存在する	uudecode が /usr/bin または /tmp にあるか、Perl が存在する	uudecode が /usr/bin または /tmp にあるか、Perl が存在する	uudecode が /usr/bin または /tmp にあるか、Perl が存在する	uudecode が /usr/bin または /tmp にあるか、Perl が存在する

S-TAP および CAS - ディスク・スペース要件

表 3. ディスク・スペース要件

ディスク・スペース	記述
S-TAP プログラム・ファイル	GIM 以外のインストールの場合、AIX: 300 MB HP-UX: 400 MB Linux: 350 MB Solaris: 300 MB Windows: 180 MB です。 GIM インストールの場合、AIX: 400 MB HP-UX: 500 MB Linux: 450 MB Solaris: 400 MB Windows: 300 MB です。 UNIX の FAM プログラム・ファイル - 最小で 600 MB
CAS プログラム・ファイル (Java を含む)	AIX: 309 MB HP-UX: 630 MB Linux: 405 MB Solaris: 390 MB Windows: 277 MB
バッファー・ファイル	デフォルトでは、S-TAP は、匿名メモリーを使用して、Guardium システムに送信するためにデータをステージングします。 バッファー・ファイルを使用するように S-TAP を構成する場合、サイズはデフォルトで 100 MB に設定されます。 サイズは、buffer_file_size 構成ファイル・パラメーターにより制御されます。

ディスク・スペース	記述
Java	CAS を使用する場合は、Java が必要。UNIX サーバーでは、お客様自身で Java を取得およびインストールしていただく必要があります (ライセンス交付の制約により)。Java をインストールするには、一定量のディスク・スペースが必要になります。
Perl	UNIX のみ。TEE データ収集メカニズム、およびオプションのハンター・コンポーネントを使用する場合、Perl 5.8.0 が必須です。まだインストールされていない場合は、Perl を入手して、インストールしていただく必要があります。スペース所要量、または Perl のダウンロードについては、perl.org を参照してください。

各コンポーネントのインストール・プロセスによって、ログ・ファイルが作成されます。 ロケーションには、/var/tmp およびコンポーネントのインストール・ディレクトリーが含まれます。

インストール・プロセスによって、inittab、upstart、および rc の各スクリプトが更新されます。

Guardium のポート要件

Guardium のコンポーネント間 (例えば、Guardium システムと S-TAP またはデータベース・サーバー上の CAS エージェント) にファイアウォールがある場合、それらのコンポーネント間の接続に使用されるポートがブロックされていないことを確認する必要があります。表 4 を参照しながら、ご使用のファイアウォール管理ユーティリティーで、適切なポートをチェック (および、場合によりオープン) してください。

表 4. UNIX サーバーのポート要件

ポート	プロトコル	Guardium システムの接続先
16016	TCP	クリアな (ポートをオープン) UNIX S-TAP
16017	TCP	クリアな (ポートをオープン) UNIX CAS
16018	TLS	暗号化された UNIX S-TAP
16019	TLS	暗号化された UNIX CAS
16020-16021		プールされた接続に使用します。
16022		フィード・プロトコル

表 5. Windows サーバーのポート要件

ポート	プロトコル	Guardium システムの接続先
8075	UDP	Windows S-TAP ハートビート・シグナル 注: Unix S-TAP エージェントは、ハートビート・シグナルに UDP を使用しないため、この機能に対応する Unix のポートはありません。
9500	TCP	クリアな (ポートをオープン) Windows S-TAP
9501	TLS	暗号化された Windows S-TAP
16017	TCP	クリアな (ポートをオープン) Windows CAS
16019	TLS	暗号化された Windows CAS

S-TAP エージェントまたは CAS エージェントをデータベース・サーバーにインストールする場合は、そのサーバーと Guardium システムとの間に接続が存在することを検査することは有用です。 UNIX システムでは、nmap コマンドで以下のオプションを使用して、接続を検査できます。

```
nmap -p <port> <ip_address>
```

例えば、ポート 16018 (Guardium で TLS に使用されるポート) が IP アドレス 192.168.3.104 に到達可能であることを検査するには、次のコマンドを入力します。

```
nmap -p 16018  192.168.3.104 Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port       State
Service 16018/tcp  open        unknown
```

- S-TAP の Windows サーバーへのインストール
  Guardium Installation Manager (GIM)、対話式インストーラー、またはコマンド行インストーラーを使用して、S-TAP を Windows にインストールします。
- S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール
  Guardium Installation Manager (GIM)、RPM、シェル・インストーラー、またはネイティブ・インストーラーのうち、ニーズに最も適したものを使用して、S-TAP クライアントを、Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーにインストールします。
- S-TAP のインストール後またはアップグレード後にデータベースを再始動またはリブートするタイミング
  このトピックでは、S-TAP をインストールした後に、データベース・サーバーまたはデータベース・インスタンスを再始動する必要がある場合、およびリブートする必要がある場合の具体例を詳しく説明します。Windows 上の S-TAP と UNIX/Linux 上の S-TAP の両方について説明します。 v9.0/9.1/9.5 と v10.0/10.1 の両方について説明します。 再始動およびリブートの要件は、GIM による実装と GIM を使用しない実装のどちらの場合も同じです。

親トピック: S-TAPs およびその他のエージェント

S-TAP の Windows サーバーへのインストール

Guardium Installation Manager (GIM)、対話式インストーラー、またはコマンド行インストーラーを使用して、S-TAP を Windows にインストールします。

ライセンス・キーによっては、ファイルとデータベースの両方のアクティビティー・モニターに同じ S-TAP エージェントを使用できます。FAM の固有パラメーターはありません。

S-TAP を Windows システムにインストールする場合、以下に示す 4 つの方法があります。

デプロイ・モニター・エージェント・ツール

Guardium V.10.1.3 から、GIM クライアントのアクティブ化、S-TAP のインストール、およびデータベース・トラフィックのモニター開始を自動的に行えます。モニター・エージェントをデプロイするためのクイック・スタートを参照してください。

Guardium Installation Manager

サーバーに S-TAPs をインストールする場合は、GIM を使用することをお勧めします。GIM を使用すると、個別のサーバーまたはサーバーのグループに対して、エージェントのインストール、アップグレード、管理を行うことができます。これには、その制御下でインストールされた各種プロセスのモニター、エージェント・パラメーターの変更、その他の管理タスクの実行が含まれます。詳しくは、Guardium Installation Manager を使用して Windows S-TAP をインストールするを参照してください。

対話式インストーラー

小規模なデプロイメントの場合や、ガイドに従い手順を追ってインストールを行う必要がある場合は、対話式インストーラーを使用すると便利です。対話式インストーラーを使用すると、ステップごとに検証処理が実行されるため、エラーが発生しにくくなります。詳しくは、対話式インストーラーを使用して Windows S-TAP をインストールするを参照してください。

注: Windows S-TAP パラメーターは、アップグレード中に対話式インストーラーを使用して変更することはできません。ユーザーは、アップグレードの後に GUI を使用して Windows S-TAP パラメーターを変更することができます。

コマンド行インストーラー

Windows で S-TAP のコマンド行インストーラーを使用すると、スクリプト可能ソリューションが提供されます。このソリューションは、大規模なデプロイメント環境を管理する場合に特に便利です。詳しくは、コマンド行インターフェースを使用して Windows S-TAP をインストールするを参照してください。

注: Windows S-TAP インストールでは、インストール用に新規または空のフォルダーが必要です。
注: S-TAP のインストールには、Base Filtering Engine (BFE) サービスが実行されている必要があります。サービスが存在しているが実行されていない場合、Guardium はそれを開始しようとします。
注: V10.0 および V10.1 の S-TAP には .NET Framework 4.5 以上が必要です。.NET 4.5 以上の環境が存在しない場合、S-TAP は .NET 4.5.2 をインストールします。
注:

非 ASCII 環境 (例えば、日本語) に Windows S-TAP をインストールする際、ユーザーは、その言語パックが含まれているサーバーを使用するか、システム・ロケールをその場所 (日本) に設定する必要があります。

データベースのオートディスカバリー

S-TAP を Windows にインストールする際に、データベースのオートディスカバリーを指定するオプションと、ディスカバーされたデータベースの検査エンジンを作成するオプションを選択することができます。オートディスカバリー・プロセスは、S-TAP のインストール時に 1 回だけ実行されます。自動的に繰り返し実行されることはありません。

アップグレードを実行すると、オートディスカバリーにより、新しくディスカバーされたすべてのデータベースに対して検査エンジンが作成され、既存のすべての検査エンジンが調整されます。そのため、存在しないデータベースに対して検査エンジンを追加した場合や、機能しないポートを指定した場合は、アップグレード時にオートディスカバリー・プロセスによってその検査エンジンが調整されることになります。

S-TAP のインストールにおいてインストール時またはアップグレード時にデータベースのオートディスカバリーを実行したくない場合は、それぞれの Windows S-TAP インストーラーに対して記述されている手順を実行すると、S-TAP のインストール・プロセスでデータベースのオートディスカバリーが実行されなくなります。

エンタープライズ・ロード・バランシング

S-TAP を Windows にインストールする際に、エンタープライズ・ロード・バランシング機能を使用するように S-TAP を構成することができます。詳しくは、エンタープライズ・ロード・バランシングを参照してください。

- Guardium Installation Manager を使用して Windows S-TAP をインストールする
  S-TAPs をデータベース・サーバーにインストールする場合は、Guardium Installation Manager (GIM) を使用することをお勧めします。
- 対話式インストーラーを使用して Windows S-TAP をインストールする
  小規模なデプロイメントの場合や、ガイドに従い手順を追ってインストールを行う必要がある場合は、対話式インストーラーを使用すると便利です。
- コマンド行インターフェースを使用して Windows S-TAP をインストールする
  コマンド行インストーラーを使用すると、スクリプト可能ソリューションが提供されます。このソリューションは、大規模なデプロイメント環境を管理する場合に特に便利です。
- コマンド行を使用して Windows S-TAP をインストールする場合のリファレンス情報
  コマンド行インストーラーを使用すると、大規模なデプロイメント環境を管理する場合に特に便利なスクリプトを作成することができます。このリファレンス情報では、スクリプト内で使用できるパラメーターについて説明します。それぞれのパラメーターには、短い説明が付いています。
- Windows 上での S-TAP のアップグレードと削除
  ここでは、Windows 上で S-TAP のアップグレードと削除を行う方法について説明します。

親トピック: S-TAP のインストール
関連概念:
S-TAP のインストール
Guardium Installation Manager
エンタープライズ・ロード・バランシング

Guardium Installation Manager を使用して Windows S-TAP をインストールする

S-TAPs をデータベース・サーバーにインストールする場合は、Guardium Installation Manager (GIM) を使用することをお勧めします。

始める前に

インストールを開始する前に、以下の点を確認してください。

- S-TAP のインストールに記載されている Windows S-TAP のインストール要件を確認します。
  - サポート対象のデータベース・サーバーとオペレーティング・システムを使用していることを確認します。

    - S-TAP と Guardium システム間の通信に必要なポートを特定します。
- S-TAP と Guardium システム間の通信に使用されるファイアウォール・ポートを開きます。
- 予定している S-TAP のインストール・ディレクトリーが空になっているか存在しないことを確認します。
- GIM クライアントは、S-TAP をインストールするデータベース・サーバーにインストールされます。
- データベース・サーバー上の GIM クライアントは、Guardium システムと通信を行います。

このタスクについて

GIM クライアントをデータベース・サーバーにインストールすると、S-TAP for Windows などのモジュールのインストールが Guardium システムによってスケジュールされます。

手順

1. インストールする Windows S-TAP モジュールをアップロードします。
    a. Guardium システムで、「管理」 > 「モジュール・インストール」 > 「モジュールのアップロード」にナビゲートします。
    b. 「ファイルの選択 (Choose File)」をクリックし、インストールする S-TAP モジュールを選択します。
    c. 「アップロード」をクリックして、モジュールを Guardium システムにアップロードします。 アップロードが完了すると、「アップロード済みモジュールのインポート」表にモジュールが表示されます。
    d. 「アップロード済みモジュールのインポート」表で、インストールする S-TAP モジュールの横にあるチェック・ボックスをクリックします。 モジュールがインポートされ、インストール可能な状態になります。モジュールのインポートが完了すると、「モジュールのアップロード」ページがリセットされ、「アップロード済みモジュールのインポート」表が空になります。
2. S-TAP のインストール先となるクライアント・システムを選択します。
    a. 「管理」 > 「モジュール・インストール」 > 「クライアント別の設定 (レガシー)」にナビゲートします。
    b. 「クライアント検索条件」画面で、S-TAP のインストール先となるクライアントの検索条件を指定し、「検索」をクリックして操作を続行します。 以下の検索条件を自由に組み合わせて検索することができます。
        - クライアント・グループを選択する。
        - クライアントのホスト名、IP アドレス、またはオペレーティング・システムで検索する。
        - すべての検索条件フィールドを空白のままにして、使用可能なすべてのクライアントのリストが返されるようにする。
    c. 「クライアント」画面で、S-TAP のインストール先となるクライアントの横にあるチェック・ボックスをクリックし、「次へ」をクリックして操作を続行します。
3. クライアント・システムにインストールする前に、S-TAP モジュールを選択して構成します。
    a. 「共通モジュール」画面の「モジュール」表で、インストールする S-TAP モジュールを選択し、「次へ」をクリックして操作を続行します。
        - 「最新バージョンの表示」チェック・ボックスと「バンドルのみ表示 (Display Bundles Only)」チェック・ボックスを使用して、使用可能なモジュールのリストをフィルタリングします。
        - 「モジュール状況」表を使用して、ターゲット・クライアント上の選択済みモジュールに関する情報を確認します。
    b. 「クライアント用モジュール・パラメーター」画面で、S-TAP のインストール・パラメーターを指定します。
        - 同じパラメーターを複数のクライアントに適用するには、「共通モジュール・パラメーター」フィールドでインストール・パラメーターを指定し、「クライアント用モジュール・パラメーター」表にリストされているクライアントの横にあるチェック・ボックスをクリックして、「選択したものに適用」をクリックします。
        - 固有のパラメーターを個別のクライアントに適用するには、「クライアント用モジュール・パラメーター」表でインストール・パラメーターを直接指定します。

    重要:
        - ほとんどのインストールではデフォルトのパラメーターを適用できますが、WINSTAP_INSTALL_DIR 値は指定する必要があります。このデフォルト値は C:/Program Files/IBM/Windows S-TAP です。
        - WINSTAP_TAP_IP (コマンド行パラメーターの -taphost と同じ) を指定しなかった場合、GIM_CLIENT_IP 値が使用されます。
        - WINSTAP_SQLGUARD_IP (コマンド行パラメーターの -appliance と同じ) を指定しなかった場合、GIM_URL 値が使用されます。
    c. S-TAP のインストール・パラメーターを指定したら、「クライアントに適用」をクリックすることにより、選択したクライアントにそれらのパラメーターを適用します。
4. 最後に、選択したクライアントに S-TAP をインストールします。
    a. 「クライアント用モジュール・パラメーター」画面で「インストール/更新」をクリックします。
    b. 「スケジュール日」ダイアログで、インストールを開始する日付または時刻を指定して「適用」をクリックします。 インストールをすぐに開始する場合は、「スケジュール日」フィールドで「`now`」の値を使用します。

次のタスク

「共通モジュール」画面の「モジュール状況」表を使用して、S-TAP モジュールのインストール状況をモニターします。「管理」 > 「レポート」 > 「インストール管理」 > 「GIM クライアント状況」でレポートを表示して、モジュールのインストール状況を確認することもできます。

S-TAP が Guardium システムと通信していることを確認します。これを行うには、「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」にナビゲートし、S-TAPs の状況と構成を確認します。

親トピック: S-TAP の Windows サーバーへのインストール
関連概念:
Guardium Installation Manager

対話式インストーラーを使用して Windows S-TAP をインストールする

小規模なデプロイメントの場合や、ガイドに従い手順を追ってインストールを行う必要がある場合は、対話式インストーラーを使用すると便利です。

始める前に

インストールを開始する前に、以下の点を確認してください。

- S-TAP のインストールに記載されている Windows S-TAP のインストール要件を確認します。
    - サポート対象のデータベース・サーバーとオペレーティング・システムを使用していることを確認します。

    - S-TAP と Guardium システム間の通信に必要なポートを特定します。
- S-TAP と Guardium システム間の通信に使用されるファイアウォール・ポートを開きます。
- S-TAP のインストール先となるデータベース・サーバーまたはドメイン・コントローラーの IP アドレスを特定します (仮想 IP アドレスを含む)。
- S-TAP を制御する Guardium システムの IP アドレスを特定します。
- 予定している S-TAP のインストール・ディレクトリーが空になっているか存在しないことを確認します。

このタスクについて

データベース・サーバーに S-TAP をインストールする場合は、S-TAP からデータを受信する Guardium システムの IP アドレスまたはホスト名を指定する必要があります。S-TAP が Guardium システムに接続されたら、「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」ページにナビゲートして S-TAP を構成します。

手順

1. システム管理者のアカウントを使用して、データベース・サーバーにログオンします。
2. 「Guardium Windows S-TAP インストール・ウィザード (Guardium Windows S-TAP Install Wizard)」 を探して起動します。
   重要: S-TAP を Windows 2012 以降にインストールする場合は、管理者特権を使用する必要があります。その場合は、インストーラーを右クリックして「管理者として実行」を選択します。
3. 「Guardium ライセンス (Guardium License)」画面で使用条件を確認します。インストールを続行する場合は、「使用条件の条項に同意します」を選択して「次へ」をクリックします。
4. 必要な情報を「お客様情報 (Customer Information)」画面で入力し、「次へ」をクリックして操作を続行します。ほとんどのインストールでは、デフォルト値が適しています。
5. 以下に示すいずれかのインストール・タイプを選択し、「次へ」をクリックして操作を続行します。
   - 標準 (Typical): 標準インストールは、ほとんどのユーザーに適しています。
   - 簡易 (Compact): 簡易インストールでは、エンタープライズ・ロード・バランシングなどの追加機能が必要ないことが想定されます。
   - カスタム: カスタム・インストールを選択すると、追加の S-TAP インストール・オプション (ソフトウェアの選択、インストール・ディレクトリーの指定、Windows S-TAP プロセスを実行するユーザー・アカウントの指定など) を変更することができます。
6. 必要に応じて、「ロード・バランシング・オプション (Load Balancing Options)」画面の「ロード・バランシングを有効にする (Enable Load Balancing)」チェック・ボックスを選択してエンタープライズ・ロード・バランシングを有効にします。「次へ」をクリックして先に進みます。
   a. エンタープライズ・ロード・バランシングを有効にする場合は、「ロード・バランサーのホスト・アドレス (Load Balancer Host Address)」フィールドで、ロード・バランサーの IP アドレスを指定します。
   b. 「拡張オプション (Advanced Options)」ボタンをクリックし、追加のエンタープライズ・ロード・バランシング・オプションを指定します。 詳しくは、エンタープライズ・ロード・バランシングを参照してください。
7. 「ネットワーク・アドレス」画面で、「S-Tap ホスト・アドレス (Software Tap Host Address)」を確認して「アプライアンス・アドレス (Appliance Address(es))」を指定し、「次へ」をクリックして操作を続行します。
   - S-Tap ホストのアドレスにより、S-TAP のインストール先となるローカル・マシンのアドレスが指定されます。
   - アプライアンスのアドレスにより、S-TAP を制御する Guardium システムのアドレスが指定されます。S-TAP のフェイルオーバー・システムを設定する場合や、participate_in_load_balancing パラメーターを使用して S-TAP のロード・バランシングを構成する場合は、複数のアドレス (通常は 3 つ以内) を個別の行に指定します。

   重要: インストール後に S-TAP サービスを有効にしたくない場合は、「S-Tap サービスの開始 (Start S-Tap Service)」 チェック・ボックスの選択を解除します。 「S-Tap サービスの開始 (Start S-Tap Service)」チェック・ボックスの選択を解除すると、データベースのオートディスカバリーと検査エンジンの作成も無効になります。
8. インストールが正常に完了すると、「インストール・ウィザードの完了 (Install Wizard Completed)」画面が表示されます。「完了」をクリックして、インストーラーを閉じます。

次のタスク

S-TAP が Guardium システムと通信していることを確認します。これを行うには、「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」にナビゲートし、S-TAPs の状況と構成を確認します。

親トピック: S-TAP の Windows サーバーへのインストール
関連概念:
エンタープライズ・ロード・バランシング

コマンド行インターフェースを使用して Windows S-TAP をインストールする

コマンド行インストーラーを使用すると、スクリプト可能ソリューションが提供されます。このソリューションは、大規模なデプロイメント環境を管理する場合に特に便利です。

始める前に

インストールを開始する前に、以下の点を確認してください。

- S-TAP のインストールに記載されている Windows S-TAP のインストール要件を確認します。
    - サポート対象のデータベース・サーバーとオペレーティング・システムを使用していることを確認します。
    - S-TAP と Guardium システム間の通信に必要なポートを特定します。
- S-TAP と Guardium システム間の通信に使用されるファイアウォール・ポートを開きます。
- S-TAP のインストール先となるデータベース・サーバーまたはドメイン・コントローラーの IP アドレスを特定します (仮想 IP アドレスを含む)。
- S-TAP を制御する Guardium システムの IP アドレスを特定します。
- 予定している S-TAP のインストール・ディレクトリーが空になっているか存在しないことを確認します。

手順

1. システム管理者のアカウントを使用して、データベース・サーバーにログオンします。
2. Windows の「コマンド プロンプト」で、Windows S-TAP のインストーラー・ディレクトリーにナビゲートします。 例えば、以下のように入力します。

```
cd c:¥Windows-V10-r79771
```

このインストーラー・ディレクトリーに setup.exe 実行可能ファイルが格納されています。

3. setup.exe 実行可能ファイルで適切なパラメーターを指定して、S-TAP をインストールします。 例えば、以下のように入力します。

```
setup.exe -UNATTENDED -APPLIANCE 10.0.147.234 -TAPHOST 10.0.145.41
```

- -UNATTENDED: これは、コマンド行インストーラーを起動するための必須パラメーターです。
- -APPLIANCE: これは、S-TAP を制御する Guardium システムの IP アドレスを指定するためのパラメーターです。
- -TAPHOST: これは、S-TAP のインストール先となるクライアントの IP アドレスを指定するための必須パラメーターです。

setup.exe 実行可能ファイルとそのパラメーターの詳細な説明については、コマンド行を使用して Windows S-TAP をインストールする場合のリファレンス情報を参照してください。

次のタスク

S-TAP が Guardium システムと通信していることを確認します。これを行うには、「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」にナビゲートし、S-TAPs の状況と構成を確認します。

親トピック: S-TAP の Windows サーバーへのインストール
関連資料:
コマンド行を使用して Windows S-TAP をインストールする場合のリファレンス情報

コマンド行を使用して Windows S-TAP をインストールする場合のリファレンス情報

コマンド行インストーラーを使用すると、大規模なデプロイメント環境を管理する場合に特に便利なスクリプトを作成することができます。このリファレンス情報では、スクリプト内で使用できるパラメーターについて説明します。それぞれのパラメーターには、短い説明が付いています。

CLI インストールでは、適切なパラメーターを指定した setup.exe 実行可能ファイルを使用して、S-TAP をインストールします。これは、以下の形式で指定します。

Setup.exe -PARAMETER value

値をパラメーターに割り当てる場合、「=」記号は使用しないでください。「=」を使用するのは、コマンド行でパラメーターを入力するように、guard_tap.ini ファイルの TAP セクションにパラメーターを直接追加する場合だけです。

ここに指定されていないパラメーターを guard_tap.ini ファイルに追加する必要がある場合は、以下のように、「=」記号を使用してそのパラメーターと値を指定することにより、[TAP] セクションを追加できます。

setup.exe -UNATTENDED -INSTALLPATH "C:/Program Files/IBM/Windows S-TAP" -APPLIANCE 10.0.148.160 -TAPHOST 10.0.146.160 QRW_INSTALLED=0 QRW_DEFAULT_STATE=0

重要: UNATTENDED と TAPHOST は必須属性です。

表 1. すべての .NET インストーラーに適用可能なパラメーター

パラメーター	記述
-UNATTENDED	サイレント・インストールを実行します (値は必要ありません)。
-INSTALLPATH	これはインストール・ディレクトリーです。デフォルトのインストール・パスは「C:/Program Files/IBM/Windows S-TAP」です。
-ENABLEGAM	このパラメーターは、Guardium Agent Monitor (GAM) サービスを有効にします。
-UNINSTALL	アンインストールします。値は不要です。
-CUSTOMER	カスタマー名を変更する場合に使用します。
-COMPANY	会社名を変更する場合に使用します。
-SERVICEUSER	サービスを実行するユーザーを指定する場合に使用します。
-SERVICEPASSWORD	ユーザーのパスワードを指定します。

表 2. 適用可能な値「ON」を持つ S-TAP パラメーター. 以下のパラメーターの値は、デフォルトで「ON」に設定されており、有効になっています。特に記載がない限り、これらのパラメーターを「ON」以外の値に設定すると、そのパラメーターが無効になります。

パラメーター	記述
-TCP	TCP_DRIVER_INSTALLED=1
-NMP	NAMED_PIPE_DRIVER_INSTALLED=1
-DB2SHMEM	DB2_TAP_INSTALLED=1
-DB2EXIT	DB2_EXIT_DRIVER_INSTALLED=1
-FAM	FSM_DRIVER_INSTALLED=1
-ORACLEPLUGIN	ORA_DRIVER_INSALLED=1
-MSPLUGIN	KRB_MSSQL_DRIVER_INSTALLED=2 (最初は 0 に設定されていた場合、または新規インストールを実行する場合のみ)

表 3. その他の S-TAP パラメーター

パラメーター	記述
-NOAUTODISCOVERY	インストール時にオートディスカバリーを実行したくない場合に使用します。値は不要です。

パラメーター	記述
-ENABLEGAM	このパラメーターは、Guardium Agent Monitor (GAM) サービスを有効にします。
-START	インストール時にサービスを起動する場合に使用します。 重要: このパラメーターは、デフォルトで有効になっています。このパラメーターは、値を 0 に設定することでのみ無効にできます。0 以外の値を設定すると、このパラメーターは有効になります。
-TAPHOST	これは、ローカル IP またはクライアント IP です。無人インストールの場合、このパラメーターは必須です。
-APPLIANCE	これは、SQLGUARD の IP です。新しい値を複数回使用してこのパラメーターを指定するだけで、複数のアプライアンスを設定することができます。
-LOAD-BALANCER-IP	これは、ロード・バランサーを有効にするための CM の IP です。
-LB-APP-GROUP	この STAP が属するエンタープライズ・ロード・バランシング用のアプリケーション・グループ名を指定します。 重要: スペースまたは特殊文字を含むグループ名はサポートされません。
-LB-MU-GROUP	エンタープライズ・ロード・バランシング用の MU グループ名を指定します。 重要: スペースまたは特殊文字を含むグループ名はサポートされません。
-LB-NUM-MUS	割り当てる管理対象ユニットの数を指定する場合に使用します。

親トピック: S-TAP の Windows サーバーへのインストール

Windows 上での S-TAP のアップグレードと削除

ここでは、Windows 上で S-TAP のアップグレードと削除を行う方法について説明します。

親トピック: S-TAP の Windows サーバーへのインストール

コマンド行を使用して Windows S-TAP をアップグレードする

このタスクについて

旧バージョンの Windows S-TAP がインストールされている場合は、設定プログラムを使用して、コマンド行からアップグレードを実行することができます。

手順

1. システム管理者のアカウントを使用して、データベース・サーバー・システムにログオンします。
2. S-TAP® 設定プログラムが入っているディレクトリーに移動します。
3. オプション setup -UNATTENDED を使用して、設定プログラムを実行します。
   重要: 以前のリリースの一部のファイルは、次回にスケジュールされているリブートが実行されるまで、完全には削除されません。

「プログラムの追加と削除」を使用して Windows S-TAP を削除する

このタスクについて

この手順では、構成ファイルを将来使用できるように確実に保存し、インストールされている S-TAP を削除します。

手順

1. システム管理者のアカウントを使用して、データベース・サーバー・システムにログオンします。
2. 現在の S-TAP 構成ファイルを安全なロケーション (Guardium 以外のディレクトリー) にコピーします。このファイルは C:Program Files (x86)¥IBM¥Windows S-TAP¥Bin¥guard_tap.ini で見つけてください。
3. 「プログラムの追加と削除 」制御パネルから、「GUARDIUM_STAP」を削除します。
   重要: 一部のファイルは、次回にスケジュールされているリブートが実行されるまで、完全には削除されません。

コマンド行を使用して Windows S-TAP を削除する

このタスクについて

この手順では、構成ファイルを将来使用できるように確実に保存し、インストールされている S-TAP を削除します。

手順

1. システム管理者のアカウントを使用して、データベース・サーバー・システムにログオンします。
2. 現在の S-TAP 構成ファイルを安全なロケーション (Guardium 以外のディレクトリー) にコピーします。このファイルは C:Program Files (x86)¥IBM¥Windows S-TAP¥Bin¥guard_tap.ini で見つけてください。
3. S-TAP の設定プログラムが格納されているディレクトリーに移動します。
4. setup -UNINSTALL オプションを指定して設定プログラムを実行します。
   重要: 一部のファイルは、次回にスケジュールされているリブートが実行されるまで、完全には削除されません。

S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール

Guardium Installation Manager (GIM)、RPM、シェル・インストーラー、またはネイティブ・インストーラーのうち、ニーズに最も適したものを使用して、S-TAP クライアントを、Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーにインストールします。

Guardium V.10.1.3 以降は、以下にリストされている方法に加えて、GIM クライアントのアクティブ化、S-TAP のインストール、およびデータベース・トラフィックのモニター開始を自動的に行えます。モニター・エージェントをデプロイするためのクイック・スタートを参照してください。

S-TAP クライアントをインストールする場合、インストール・プログラムによって Guardium グループが存在するかどうかが確認されます。 このグループが存在しない場合は、インストール・プログラムによって作成されます。A-TAP や Db2 出口などの特定のコンポーネントや機能を使用する場合は、適切に機能するように、ユーザーをこのグループに追加する必要があります。これらの要件については、関連セクションで説明します。

S-TAP は /usr/local/guardium にインストールされます。

まれに、S-TAP を Guardium として (root ではなく) 実行する必要があります。これは他の問題を引き起こす可能性があるため、必要な場合にのみ使用してください。Guardium ユーザーとして S-TAP を実行すると、許可レベルが原因で、一部のデータベースまたはプロトコルが機能しなくなる場合があります。データベース・パスまたは exec ファイルに、Guardium ユーザーに読み取りを許可する権限が付与されていることを確認します。ご使用の環境に応じて、代表的な制限事項は以下のようになります。

- ディスカバリーは、機能が限定されています。
- wait_for_db_exec が機能しない可能性があります。そのため、クラスターの場合、データベース・パスまたは実行ファイルで、Guardium ユーザーによる読み取りが許可されているかどうか確認してください。
- AIX® WPAR および Solaris Zones のデータベースが機能しない可能性があります。インストール・パスまたは実行ファイルへのアクセス権限を確認してください。
- Oracle BEQ の場合は、データベースの始動後、または再始動後に S-TAP を再始動してください。
- Informix® 共有メモリーの場合は、データベースの始動後、または再始動後に S-TAP を再始動してください。
- Db2 共有メモリーの場合
  - ktap_fast_shmem が 0 に設定されていると、許可の問題が原因で shmctl が失敗した場合、ほとんどの場合に S-TAP が root として実行されるように変更する必要があります。
  - ktap_fast_shmem が 1 に設定されていて、グループによる読み取りが共有メモリー・セグメントで許可されている場合は、Db2 インスタンスがユーザー (Guardium) グループに追加されていることを確認してください。ただし依然として、サーバーごとに、Db2® の構成は 1 セットのみサポートされます。
  - Db2 ユーザーによる読み取りのみが共有メモリー・セグメントで許可されている場合は、S-TAP を root として実行する必要があります。(Db2 共有メモリー・セッションを開き、コマンド ipcs -ma を実行し、出力で MODE を確認します)

- 使用する S-TAP セットアップの選択
  モニターまたはブロックするデータに応じて、使用する S-TAP セットアップを選択します。出口ライブラリーは、他のすべてのモニター・メカニズムよりも優先されます。出口ライブラリーを使用できない場合、次に選択されるのは K-TAP です。
- GIM による S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール
  Guardium Installation Manager を使用して、スタンドアロン Guardium アプライアンスまたは中央マネージャーから S-TAP エージェントをインストールして、1 つ以上のデータベースでのインストールのスケジュールを設定します。インストール後、すべてのパラメーターを管理し、その制御下でインストールされたプロセスをモニターできます。他のいずれかのインストール方法を使用してインストールすると、GIM を使用して変更できるエージェント・パラメーターの数が少なくなります。
- RPM を使用した Linux サーバー、Solaris サーバー、 AIX サーバー、HP-UX サーバーでの S-TAP のインストールと更新
  RPM を使用して、Linux サーバーで S-TAP をインストール、アンインストール、および更新できます。RPM によるインストールの利点は、データベース・サーバー上の他のすべてのソフトウェアを管理するとの同じ方法で STAP をインストールおよび管理する点です。
- シェル・インストーラーを使用した Linux、Solaris、AIX、HP-UX S-TAP のインストール
  シェル・インストーラーを使用して、対話モードまたは非対話モードのいずれかで、Linux、Solaris、HPUX、AIX の各データベース・サーバーに S-TAP クライアントをインストールします。
- ネイティブ・インストーラーを使用した Linux、Solaris、AIX、HP-UX S-TAP のインストールとアンインストール
  ネイティブ・インストーラーは、シェル・インストーラーにシェルを提供します。唯一の利点は、S-TAP がオペレーティング・システムの資産リポジトリーに確実に登録されることです。この登録は、Guardium で S-TAP をインストールする場合の要件ではありませんが、企業の要件になっている場合があります。ネイティブ・インストーラーは、必要な場合にのみ使用してください。
- S-TAP のアンインストール
  古い構成ファイルを保存する必要がある場合、S-TAP® の新規バージョンをインストールする前にこの手順を実行します。
- K-TAP の処理
- Java または Perl の情報の取得
  データ・サーバーで使用されている Java または Perl のバージョンをチェックしなければならない場合があります。

親トピック: S-TAP のインストール

使用する S-TAP セットアップの選択

モニターまたはブロックするデータに応じて、使用する S-TAP セットアップを選択します。出口ライブラリーは、他のすべてのモニター・メカニズムよりも優先されます。出口ライブラリーを使用できない場合、次に選択されるのは K-TAP です。

以下の表を使用して、OS および DB ごとに、必要な操作を実行可能なモニター・メカニズムを判別してください。例えば、以下の項目の 1 つ以上をトラッキングする必要が生じる場合があります。

- ローカル・トラフィックのみ
- ローカル・トラフィックおよびネットワーク・トラフィック
- 共有メモリー
- 暗号化されたデータ
- モニターおよびブロック
- モニターのみ

以下の表では、Guardium のモニター・メカニズムによってサポートされる、最も一般的なプラットフォーム、データベース・タイプ、およびプロトコルを取り上げています。この表は一般ガイドラインを示しています。ここには示されていない他のサポート対象の組み合わせが存在する場合があります。ここに示されているサポート対象のセットアップの一部は、特定の構成に依存する場合があります。特定のニーズに最も適したセットアップを確認するには、お客様サポートにお問い合わせください。空のセルは、その組み合わせがサポートされないことを示しています。

OS	データベース	ネットワーク・トラフィック	ローカル・トラフィック	暗号化されたトラフィック	共有メモリー	Kerberos	ブロッキング	編集	UID チェーン
AIX	Oracle	K-TAP	K-TAP	A-TAP (ASO、SSL)		K-TAP	K-TAP、A-TAP	K-TAP	K-TAP
AIX	Sybase ASE	K-TAP	K-TAP	A-TAP (SSL)		K-TAP	K-TAP、A-TAP	K-TAP	K-TAP、A-TAP (実際の IP に対して構成されている場合は ATAP のみ)
AIX	Sybase IQ	K-TAP	K-TAP	A-TAP (ログイン・パケットの暗号化解除のみ。TLS サポートなし)	A-TAP		K-TAP、A-TAP	K-TAP	K-TAP
AIX	Db2	Db2 出口、K-TAP	Db2 出口、K-TAP	Db2 出口	Db2 出口、K-TAP	K-TAP	Db2 出口、K-TAP	K-TAP	Db2 出口、K-TAP
AIX	Informix	Informix 出口、K-TAP	Informix 出口、K-TAP	Informix 出口	Informix 出口、K-TAP		Informix 出口、K-TAP	Informix 出口、K-TAP	Informix 出口、K-TAP
HP-UX	Oracle	K-TAP	K-TAP	A-TAP (ASO、SSL)		K-TAP	K-TAP、A-TAP	K-TAP	K-TAP
HP-UX	Sybase ASE	K-TAP	K-TAP	A-TAP (Sybase 15 のみ)			K-TAP、A-TAP	K-TAP	K-TAP、A-TAP (実際の IP に対して構成されている場合は ATAP のみ)
HP-UX	Sybase IQ	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
HP-UX	Db2	Db2 出口、K-TAP	Db2 出口、K-TAP	Db2 出口	Db2 出口、K-TAP	K-TAP	Db2 出口、K-TAP	K-TAP	Db2 出口、K-TAP
HP-UX	Informix	Informix 出口、K-TAP	Informix 出口、K-TAP	Informix 出口	Informix 出口、K-TAP		Informix 出口、K-TAP	Informix 出口、K-TAP	Informix 出口、K-TAP
Linux	Db2	Db2 出口、K-TAP		Db2 出口	Db2 出口、A-TAP	K-TAP	Db2 出口、K-TAP、A-TAP (Linux 2.6.36 以降の ATAP のみ)	K-TAP	Db2 出口、K-TAP
Linux	Informix	Informix 出口、K-TAP	Informix 出口、K-TAP	Informix 出口	Informix 出口、A-TAP		Informix 出口、K-TAP、A-TAP (Linux 2.6.36 以降の ATAP のみ)	Informix 出口、K-TAP	Informix 出口、K-TAP
Linux	Oracle	K-TAP	K-TAP	A-TAP (ASO、SSL)		K-TAP	K-TAP、A-TAP (Linux 2.6.36 以降の ATAP のみ)	K-TAP	K-TAP
Linux	Postgres	K-TAP	K-TAP	A-TAP			K-TAP、A-TAP (Linux 2.6.36 以降の ATAP のみ)	K-TAP	K-TAP、A-TAP (実際の IP に対して構成されている場合は ATAP のみ)
Linux	Sybase IQ	K-TAP		A-TAP (x86_64 のみ)	A-TAP		K-TAP、A-TAP (Linux 2.6.36 以降の ATAP のみ)	K-TAP	K-TAP、A-TAP (実際の IP に対して構成されている場合は ATAP のみ)
Linux	Sybase ASE	K-TAP	K-TAP	A-TAP			K-TAP、A-TAP (Linux 2.6.36 以降の ATAP のみ)	K-TAP	K-TAP、A-TAP (実際の IP に対して構成されている場合は ATAP のみ)
Linux	MongoDB	K-TAP	K-TAP	A-TAP			K-TAP、A-TAP (Linux 2.6.36 以降の ATAP のみ)	K-TAP	K-TAP、A-TAP (実際の IP に対して構成されている場合は ATAP のみ)

OS	データベース	ネットワーク・トラフィック	ローカル・トラフィック	暗号化されたトラフィック	共有メモリー	Kerberos	ブロッキング	編集	UID チェーン
Linux	Teradata	Teradata 出口、K-TAP		Teradata 出口、A-TAP			Teradata 出口、K-TAP、A-TAP (Linux 2.6.36 以降の ATAP のみ)	K-TAP	K-TAP、A-TAP (実際の IP に対して構成されている場合は ATAP のみ)
Linux	Netezza	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Cassandra	K-TAP					K-TAP	K-TAP	K-TAP
Linux	SAP HANA	K-TAP					K-TAP	K-TAP	K-TAP
Linux	MySQL	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	MemSQL	K-TAP	K-TAP	K-TAP			K-TAP	K-TAP	K-TAP
Linux	Vertica	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	Hadoop (Cloudera/Hortonworks)	K-TAP、Cloudera Navigator、Hortonworks および Apache Ranger		Cloudera Navigator、Hortonworks および Apache Ranger			Hortonworks および Apache Ranger		K-TAP
Linux	Greenplum	K-TAP	K-TAP	A-TAP			K-TAP、A-TAP (Linux 2.6.36 以降のみ)	K-TAP	K-TAP
Linux	MariaDB	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	Aster	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	Couch	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Hive	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Accumulo	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Impala	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Hue	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	WebHDFS	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Solar	K-TAP					K-TAP	K-TAP	K-TAP
Solaris	Oracle	K-TAP	K-TAP	A-TAP (ASO、SSL)		K-TAP	K-TAP、A-TAP	K-TAP	K-TAP
Solaris	Sybase ASE	K-TAP	K-TAP	A-TAP (Sparc のみ)		K-TAP	K-TAP、A-TAP	K-TAP	K-TAP、A-TAP (実際の IP に対して構成されている場合は ATAP のみ)
Solaris	Postgres	K-TAP	K-TAP	A-TAP (9.3 以上)			K-TAP、A-TAP	K-TAP	K-TAP、A-TAP (実際の IP に対して構成されている場合は ATAP のみ)
Solaris	Sybase IQ	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Solaris	Db2	Db2 出口、K-TAP	Db2 出口、K-TAP	Db2 出口	Db2 出口、K-TAP	K-TAP	Db2 出口、K-TAP	K-TAP	Db2 出口、K-TAP
Solaris	Informix	Informix 出口、出口、K-TAP	Informix 出口、K-TAP	Informix 出口	Informix 出口、K-TAP		Informix 出口、K-TAP	Informix 出口、K-TAP	Informix 出口、K-TAP

親トピック: S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール

GIM による S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール

Guardium Installation Manager を使用して、スタンドアロン Guardium アプライアンスまたは中央マネージャーから S-TAP エージェントをインストールして、1 つ以上のデータベースでのインストールのスケジュールを設定します。インストール後、すべてのパラメーターを管理し、その制御下でインストールされたプロセスをモニターできます。他のいずれかのインストール方法を使用してインストールすると、GIM を使用して変更できるエージェント・パラメーターの数が少なくなります。

このタスクについて

手順

1. S-TAP のインストール先となっているデータベース・サーバーの IP アドレスを取得します。仮想 IP を使用する場合は、これらもメモしてください (これらは、構成を完了するときに、後で構成する必要があります)。
2. 中央マネージャーでインストールする場合、この S-TAP を制御するコレクターであり、かつ S-TAP が報告を行う先のコレクターの IP アドレスを特定します。
3. データベース・サーバーとコレクターの間の接続を確認します。データベースで、nmap -p <port> <ip_address> を入力します。例えば、ポート 16018 (Guardium® で TLS に使用されるポート) に IP アドレス 192.168.3.104 で到達できるか検査するには、次のコマンドを入力します。
   nmap -p 16018 192.168.3.104
   通常の出力は、以下のとおりです。
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. GIM クライアントがデータベース・サーバーにインストールされていることを確認します。UNIX サーバーへの GIM クライアントのインストールを参照してください。
5. 正しい S-TAP インストーラー・スクリプトを取得します。スクリプト名によって、データベース・サーバーのオペレーティング・システムが識別されます。
6. 適切な S-TAP モジュールを Guardium Installation Manager アプライアンスにアップロードします。
   a. 「管理」 > 「モジュール・インストール」 > 「モジュールのアップロード」に移動します。
   b. 「ファイルの選択 (Choose File)」をクリックし、インストールする S-TAP モジュールを選択します。
   c. 「アップロード」をクリックして、モジュールをアプライアンスにアップロードします。 モジュールが「アップロード済みモジュールのインポート」表に表示されます。
   d. 「アップロード済みモジュールのインポート」表で、インストールする S-TAP モジュールの横にあるチェック・ボックスをクリックします。 モジュールがインポートされ、インストール可能な状態になります。「モジュールのアップロード」ページがリセットされ、「アップロード済みモジュールのインポート」表が空になります。
7. S-TAP のインストール先となるデータベースを 1 つ以上選択します。
   a. 「管理」 > 「モジュール・インストール」 > 「クライアント別の設定 (レガシー)」に移動します。
   b. 「クライアント検索条件」ページで、S-TAP のインストール先となるデータベースの検索条件を指定し、「検索」をクリックします。 以下の検索条件を自由に組み合わせてデータベースを検索します。
      - クライアント・グループを選択する。
      - クライアントのホスト名、IP アドレス、またはオペレーティング・システムで検索する。
      - すべての検索条件フィールドを空白のままにして、「検索」をクリックし、使用可能なすべてのクライアントのリストが返されるようにする。
   c. 「クライアント」ページで、S-TAP のインストール先となるクライアントの横にあるチェック・ボックスを選択し、「次へ」をクリックします。
8. クライアント・システムにインストールする前に、S-TAP パラメーターを選択して構成します。
   a. 「共通モジュール」ページの「モジュール」表で、インストールする S-TAP モジュールを選択します。
      - 「最新バージョンの表示」チェック・ボックスと「バンドルのみ表示 (Display Bundles Only)」チェック・ボックスを使用して、使用可能なモジュールのリストをフィルタリングします。
      - 「モジュール状況」表を使用して、ターゲット・クライアント上の選択済みモジュールに関する情報を確認します。
   b. 「次へ」をクリックします。
   c. 「クライアント用モジュール・パラメーター」ページで、データベース・グループのパラメーターを指定でき、個別データベースのパラメーターも指定できます。
      - 同じパラメーター値を複数のデータベースに適用します。「共通モジュール・パラメーター」フィールドで値を指定し、「クライアント用モジュール・パラメーター」表内のデータベースの横にあるチェック・ボックスをクリックして、「選択したものに適用」をクリックします。
      - 固有のパラメーターを個別のクライアントに適用するには、「クライアント用モジュール・パラメーター」表で値を指定し、「選択したものに適用」をクリックします。

      重要:

      以下のパラメーターは必須です。

      - KTAP_LIVE_UPDATE: サーバー・リブートの必要なしに KTAP 更新を有効にするには、「Y」と入力します。
      - STAP_TAP_IP: STAP がインストールされているデータベース・サーバーまたはノードの IP アドレスまたは FQDN (-taphost コマンド行パラメーターと同じ)。指定されていない場合、GIM_CLIENT_IP 値が使用されます。
      - STAP_SQLGUARD_IP: この STAP の通信先である 1 次コレクターの IP アドレスまたは FQDN (-appliance コマンド行パラメーターと同じ)。指定されていない場合、GIM_URL 値が使用されます。
      - Linux のみ: KTAP_ALLOW_MODULE_COMBOS。「Y」と入力します (デフォルト は N です)。バンドルに完全一致のカーネルがない場合、最も一致率が高いカーネルがインストールされます。K-TAP をインストールできない場合や、K-TAP が開始されない場合、ユーザーはインストールを続行するかどうかの確認を求められます。
   d. 「クライアントに適用」をクリックして、選択したクライアントにパラメーターを適用します。
9. S-TAP をインストールします。
   a. 「クライアント用モジュール・パラメーター」表でデータベースが選択されていることを確認します。
   b. ウィンドウの下部にある「インストール/更新」をクリックします。
   c. 中央マネージャーの「スケジュール日」領域で、インストールを開始する日付または時刻を指定し、「適用」をクリックします。 インストールをすぐに開始する場合は、「スケジュール日」フィールドで「now」の値を使用します。

次のタスク

S-TAP 状況を確認します。

- 「管理」 > 「レポート」 > 「インストール管理」 > 「GIM クライアント状況」のレポートで、モジュール・インストール状況を確認します。
- 「管理」 > 「モジュール・インストール」 > 「クライアント別の設定 (レガシー)」にナビゲートして、Guardium クライアントのインストール状況をモニターします。「検索」をクリックし、S-TAP の横にある をクリックします。
- 「モニター」 > 「保守」 > 「S-TAP ログ」 > 「S-TAP 状況」で、S-TAP の行の状況 (最初の列) が緑色であることを確認します。

親トピック: S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール
関連概念:
Guardium Installation Manager

RPM を使用した Linux サーバー、Solaris サーバー、 AIX サーバー、HP-UX サーバーでの S-TAP® のインストールと更新

RPM を使用して、Linux サーバーで S-TAP をインストール、アンインストール、および更新できます。RPM によるインストールの利点は、データベース・サーバー上の他のすべてのソフトウェアを管理するとの同じ方法で STAP をインストールおよび管理する点です。

このタスクについて

RPM 名のフォーマットは、guard-stap-10.1.0.89165-1-rhel-6-linux-x86_64.x86_64.rpm です。ここで、最初の 3 つの番号は STAP のリリース番号 (10.1.0、10.1.2 など) であり、4 番目の番号はコード改訂 (89165) です。その直後に続く番号はパッケージの世代を表し、RPM に KTAP モジュールが追加される場合に増加されます。

32 ビット S-TAP の RPM は 1 つですが、64 ビット S-TAP の RPM は 2 つあるため、32 ビット出口ライブラリーが必要でなければ、64 ビット S-TAP が 32 ビット・ライブラリーに依存することはありません。追加の RPM は guard-stap-32bit-exit-libs-10.1.0.89165-1-rhel-6-linux-x86_64.x86_64.rpm のような名前であり、メインの RPM に依存します。

デフォルトでは、インストール・プロセスは、Linux カーネルをチェックして、そのカーネルで処理を実行するための K-TAP モジュールが作成済みかどうかを判別します。モジュールが存在する場合、それがインストールを行います (ktap_installed = 1 が設定されます)。モジュールがない場合、ローダー柔軟性を有効にしない限り、K-TAP はインストールを行いません。ローダー柔軟性は、完全一致が存在しない場合に、現在作成されているモジュールのインストールに役立ちます。ローダー柔軟性が有効になっている場合、Linux カーネルに対応する K-TAP の作成が試行されます。

RPM は S-TAP を /opt/guardium にインストールします。この場所は変更できません。tap_ip は自動的にシステムのホスト名に設定されます。sqlguard_ip は、目的の構成のプレースホルダーとして 127.0.0.1 に設定されます。以下の手順で説明されているように、インストール後に構成を完了します。

手順

1. S-TAP のインストール先となっているデータベース・サーバーの IP アドレスを取得します。仮想 IP を使用する場合は、これらもメモしてください (これらは、構成を完了するときに、後で構成する必要があります)。
2. この S-TAP を制御するコレクターであり、かつ S-TAP が報告を行う先のコレクターの IP アドレスを特定します。
3. データベース・サーバーとコレクターの間の接続を確認します。データベースで、nmap -p <port> <ip_address> を入力します。例えば、ポート 16018 (Guardium® で TLS に使用されるポート) に IP アドレス 192.168.3.104 で到達できるか検査するには、次のコマンドを入力します。
   nmap -p 16018 192.168.3.104
   通常の出力は、以下のとおりです。
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. 正しい S-TAP インストーラー・スクリプトを取得します。スクリプト名によって、データベース・サーバーのオペレーティング・システムが識別されます。
5. パッケージを unzip し、データベース・サーバーの /tmp に RPM をコピーします。
6. ローダー柔軟性を有効にするために、Linux 環境変数 `NI_ALLOW_MODULE_COMBOS="Y"` を設定します。
7. RPM をインストールします。
   a. コマンド `rpm -i <RPM_NAME>` を実行します。

      S-TAP がインストールされます。

   b. 9 で説明されているパラメーターを使用したスクリプト `guard-config-update` を実行して、構成を完了します。
   RPM が既にインストールされている場合、S-TAP シェル・インストーラーはインストールを行いません (二重インストールを防ぎます)。
8. アップグレードするには、RPM パッケージを /opt/guardium にコピーし、コマンド `rpm -U <RPM_NAME>` を実行します。
9. 構成または更新するには、`root` としてシステムにログインし、ディレクトリーを /opt/guardium に変更し、以下のリストの該当する [option] と [action] を使用して、スクリプト `guard-config-update` を実行します。
   注: コマンドの先頭に presets を配置する必要があります。コマンドの末尾に presets を配置すると、インストールが失敗します。引数にファイルを指定して presets を使用することは正常に機能します。

[--stap-dir]	デフォルトでない場合の STAP インストール・ディレクトリー (デフォルト: /usr/local/guardium)
[--set-tap-ip [IP またはホスト名]]	STAP 構成ファイル /usr/local/guardium/guard_stap/guard_tap.ini の tap_ip を設定します (デフォルト: rh5u9x64t.guard.swg.usma.ibm.com)
[--set-sqlguard-ip [IP またはホスト名]]	STAP 構成ファイル /usr/local/guardium/guard_stap/guard_tap.ini の SQLGuard_0 セクションの sqlguard_ip を設定します (デフォルト: 127.0.0.1)
[--add-sqlguard [ID] [IP またはホスト名]] (Guardium v10.1.4 以上)	STAP 構成ファイル /usr/local/guardium/guard_stap/guard_tap.ini へ SQLGuard_ID セクションを追加します
[--remove-sqlguard [ID]] (Guardium v10.1.4 以上)	STAP 構成ファイル /usr/local/guardium/guard_stap/guard_tap.ini から SQLGuard_ID セクションを削除します
[--modify-sqlguard [ID] [parameter] [value]] (Guardium v10.1.4 以上)	STAP 構成ファイル /usr/local/guardium/guard_stap/guard_tap.ini の SQLGuard_ID セクションのパラメーターを設定します。パラメーター: sqlguard_ip SQLGuard ユニットの IP アドレスまたはホスト名 sqlguard_port SQLGuard ユニットへの接続に使用されるポート (デフォルト: 16016) primary 優先順位 (1 が最も優先) num_main_thread SQLGuard で使用するメイン接続の数。participate_in_load_balancing = { 1、4 } (デフォルト: 1) と併用 connection_pool_size SQLGuard ユニットへのメイン接続ごとのデータ接続の (デフォルト: 0)
[--modify-tap [parameter] [value]]	STAP 構成ファイル /usr/local/guardium/guard_stap/guard_tap.ini の TAP セクションのパラメーターを設定します。パラ

(Guardium v10.1.4 で更新されました)	メーター: tap_debug_output_level デバッグ・レベルを設定します (0 以上の整数にする必要がありますが、2 または 3 にはできません) participate_in_load_balancing ロード・バランシングへの参加を設定します (0 以上かつ 4 以下の整数にする必要があります) use_tls TLS を有効にします [0、1] failover_tls 非 TLS への TLS 接続のフェイルオーバー [0、1] hunter_trace UID チェーン・レポートを有効にします [0、1] buffer_file_size バッファー・ファイル・サイズ (MB) alternate_ips STAP 用の代替 IP/ホスト名のコンマ区切りリスト firewall_installed ファイアウォールを有効にします [0、1] firewall_fail_close 判断がないとき (SQLGuard に到達不能な場合やタイムアウトに達した場合など) に実行するアクション [0: 何もしない、1: 接続をブロック] firewall_default_state デフォルトの状態を設定します [0: 監視しない、1: 監視する] firewall_timeout ファイアウォール・タイムアウトを秒単位で設定します firewall_force_watch firewall_default_state=0 の場合でも監視する IP/マスクのコンマ区切りリスト firewall_force_unwatch firewall_default_state=1 の場合でも監視しない IP/マスクのコンマ区切りリスト
[--help-config [option]]	使用可能な場合、ini 内のオプションに関する情報を表示します (オプションが何も指定されない場合、使用可能なすべてを表示します)。
[--set-flexload [0 または 1]]	KTAP フレックス・ロードを有効または無効にします
[--retry-ktap-load]	KTAP ロードを再試行します (STAP が自動的に再始動される、dev パッケージのインストール、KTAP 要求による更新、または flexload の変更の後に役立ちます。)
[--discover-ies]	ディスカバリーを実行し、すべての検査エンジンをディスカバーされたものと置換し
[--stop [service]]	サービス (stap、tee、または monitor) を一時的に停止します (Solaris サービスおよび inittab はこれを永久無効として処理し、再度有効にするまでは起動時に自動始動しません)
[--start [service]]	サービス (stap、tee、または monitor) がまだ実行されていない場合、それを開始します (有効化を意味します)
[--restart [service]]	サービス (stap、tee、または monitor) が既に実行されている場合、それを再始動します
[--disable [service]]	サービス (stap、tee、または monitor) が再実行されないようにします
[--enable [service]]	サービス (stap、tee、または monitor) に自動始動を設定します
[--status]	開始されているサービスと、自動的に開始するように設定されているかどうかを表示します

10. アンインストールするには、以下のようにします。
    a. RPM 名を取得するために、`rpm -qa | grep guard_stap` を実行します。
    b. `rpm -e <RPM_NAME>` を実行します。

アンインストール後も、/opt/guardium ディレクトリーは引き続き存在しますが、/opt/guardium/guard_stap/guard_tap.ini.rpmsave と /opt/guardium/rpm_logs のみが含まれます。

次のタスク

S-TAP 状況を確認します。

- 「モニター」 > 「保守」 > 「S-TAP ログ」 > 「S-TAP 状況」 で、S-TAP の行の状況 (最初の列) が緑色であることを確認します。
- データベースから、STAP が実行されていること、および KTAP がロードされていること (KTAP をインストールした場合) を確認します。

親トピック: S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール

シェル・インストーラーを使用した Linux、Solaris、AIX、HP-UX S-TAP のインストール

シェル・インストーラーを使用して、対話モードまたは非対話モードのいずれかで、Linux、Solaris、HPUX、AIX の各データベース・サーバーに S-TAP クライアントをインストールします。

このタスクについて

インストールとアンインストールを行うには、対話モードが簡単な方法ですが、システムごとに個別に実行する必要があります。対話式インストーラーを使用すると、ステップごとに検証処理が実行されるため、エラーが発生しにくくなります。小規模なデプロイメントの場合や、ガイドに従い手順を追ってインストールを行う必要がある場合は、対話式インストーラーを使用すると便利です。非対話モードでは、1 つのスクリプトで複数の S-TAP をインストールできるため、大規模なデプロイメントを管理する場合は特に便利です。

いずれかの段階でインストールが失敗した場合は、その時点までのすべてのステップを取り消します。 S-TAP を部分的にインストールしたまま放置しないでください。

S-TAP パッケージ名のフォーマットは、guard-stap-guard-10.0.0_r79927_1-rhel-5-linux-x86_64.sh です。ここで、10.0.0 はリリース番号であり、r79927 はリビジョン番号です。

個々の S-TAP のインストールには、対話モードをお勧めします。システムにより、基本構成を尋ねるプロンプトが出され、ユーザーの入力がすぐに検証されるので、エラーは発生しません。デフォルトでは、S-TAP インストール時に K-TAP が自動的にインストールされます。S-TAP インストーラーは、カーネルのバージョンに合った K-TAP を使用できるかどうか検査します。インストール・プロセスは、対応する K-TAP を検出できない場合、当該 Linux カーネルに対応する K-TAP の作成を試みます。K-TAP をインストールできない場合や、K-TAP が開始されない場合、ユーザーはインストールを続行するかどうかの確認を求められます。

単一コマンドを実行し、tapfile パラメーター --tapfile <path to ini file> と、データベースおよびその詳細を指定する関連構成ファイルを使用して、複数データベース、複数システムにインストールする場合は、非対話モードを使用します。非対話モードの代わりに GIM を使用することを検討してください。

手順

1. S-TAP のインストール先となっているデータベース・サーバーの IP アドレスを取得します。仮想 IP を使用する場合は、これらもメモしてください (これらは、構成を完了するときに、後で構成する必要があります)。
2. この S-TAP を制御するコレクターであり、かつ S-TAP が報告を行う先のコレクターの IP アドレスを特定します。
3. データベース・サーバーとコレクターの間の接続を確認します。データベースで、nmap -p <port> <ip_address> を入力します。例えば、ポート 16018 (Guardium® で TLS に使用されるポート) に IP アドレス 192.168.3.104 で到達できるか検査するには、次のコマンドを入力します。
   nmap -p 16018 192.168.3.104
   通常の出力は、以下のとおりです。
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. 正しい S-TAP インストーラー・スクリプトを取得します。スクリプト名によって、データベース・サーバーのオペレーティング・システムが識別されます。
5. `root` アカウントを使用して、データベース・サーバーにログオンします。
6. インストール・ディレクトリーを指定し、そこに十分なディスク・スペース (合計で、約 400 MB から 500 MB) があることを確認します。
7. S-TAP .tgz をデータベース・サーバー上のローカル・ディスク (通常は /tmp) にコピーします。
8. 非対話モードによる標準インストールの場合は、以下を入力します。

   ```
   ./guard-stap-guard-<release number>_<revision number>_1-rhel-5-linux-x86_64.sh -- --ni -k --dir
   <guardium_installation_directory>   --ktap_allow_module_combos   --tapip <tap_ip or host_name>  --sqlguardip < sqlguard_ip or
   host_name>
   ```

   注: S-TAP インストーラーには、さまざまな Linux カーネルに固有の、考えられるすべてのモジュールが含まれています。まれに、S-TAP パッケージに、該当する K-TAP モジュールが含まれていない場合があります。この場合は、以下のコマンドを使用して、K-TAP モジュールを /tmp にコピーします。K-TAP モジュール・ファイルは、インストール時に S-TAP インストール・ディレクトリーにコピーされます。

   ```
   ./guard-stap-guard-10.0.0_r79927_1-rhel-5-linux-x86_64.sh --
   --modules /tmp/modules-guard-10.0.0_r79927_1.tgz"
   ```

9. 対話モードの場合
   a. `./guard-stap-guard-<release number>_<revision number>_1-rhel-5-linux-x86_64.sh` を入力します。
   b. インストーラーの指示に従って、特記事項およびその他のプロンプトに応答します。提供されたデフォルトをすべて受け入れることをお勧めします。
   c. Guardium システムの IP アドレスを尋ねるプロンプトでは、この S-TAP が通信するアプライアンスの IP を入力します。
   d. tap ホストの IP アドレスを尋ねるプロンプトでは、データベースの IP を入力します。
   e. ユーザー名 (root または guardium) を尋ねるインストーラーのプロンプトでは、`root` を選択します。まれに、S-TAP を Guardium として実行する必要があります。これは他の問題を引き起こす可能性があるため、本当に必要な場合にのみ使用してください。
   f. インストーラーにより、パラメーター・ファイルの変更についてのプロンプトが出されます。他のパラメーターの値は Guardium ユーザー・インターフェースから設定できるため、通常、このファイルは必ずしも編集する必要はありません。構成ファイルを編集することを選択した場合は、:wq コマンドを使用してファイルを保存し、終了します。インストール・プログラムによって、設定したパラメーター値が検査されます。正常であれば、続いて次のプロンプトが出されます。そうでない場合は、問題のあるパラメーターを修正してからファイルを再度保存してください。
   g. AIX® の場合のみ: データベース・サービスとリスナーを再始動してください。 その他すべての場合は、このステップをスキップできます。
10. UI から S-TAP 構成を完了します。GUI からの S-TAP の構成を参照してください。
11. A-TAP によるモニターが必要なデータベース・インスタンス用に S-TAP® がインストールされたら、Guardium グループにデータベース・ユーザーを追加します。このグループは S-TAP インストーラーによって作成されますが、システム管理者は usermod ユーティリティーを使用してユーザーを追加することができます。以下の例では、Oracle は Oracle データベースの OS ユーザーのユーザー ID、sybase15 は Sybase 15 データベースの OS ユーザーのユーザー ID です。

    ```
    usermod -a -G guardium oracle
    usermod -a -G guardium sybase15
    ```

次のタスク

S-TAP 状況を確認します。

- 「管理」 > 「レポート」 > 「インストール管理」 > 「GIM クライアント状況」のレポートで、モジュール・インストール状況を確認します。
- 「共通モジュール」画面の「モジュール状況」表で S-TAP のインストール状況をモニターします。
- 「モニター」 > 「保守」 > 「S-TAP ログ」 > 「S-TAP 状況」で、S-TAP の行の状況 (最初の列) が緑色であることを確認します。
- データベースから、STAP が実行されていること、および KTAP がロードされていること (KTAP をインストールした場合) を確認します。

- UNIX 用の S-TAP インストール・スクリプト・パラメーター

親トピック: S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール

UNIX 用の S-TAP インストール・スクリプト・パラメーター

インストール・スクリプトのコマンド行構文

使用法: guard-stap-setup [options]

[--ni]: 非対話式インストールを実行します。

[-k | -p] - Ktap または Pcap とともに S-TAP をインストールします。

[--ni]: 非対話式インストールを実行します。

[--ignore-compat] - スクリプト互換性検査を無視します。

[-k | -t | -p] - Ktap、Tee、または Pcap とともに S-TAP をインストールします。

[-u]: 以前のインストール済み環境が見つかった場合、その環境を更新します。

[--user | --root]: STAP をユーザーまたは root として実行します。

[--userinst | --rootinst]: STAP をユーザーまたは root としてインストールします。

[--overwrite-existing]: 既存のインストール済み環境が見つかった場合、その環境を上書きします。

[--tls force | failover | none]: STAP の TLS を設定します。

[--dir <dir>]: STAP のインストール・ディレクトリーを指定します。

[--tapfile <file>] - インストールで使用する STAP 設定ファイルを指定します。

[--ipfile <file>] - TAP の IP または SQLGUARD の IP を定義するファイルを指定します。

[--tapip <tapip>] - STAP のインストール先となるマシンの IP を指定します。

[--sqlguardip <sqlguardip>] - STAP の通信相手となる gmachine の IP を指定します。

[--presets <file> | <preset-options>]: インストール設定の読み取り、またはインストール設定のファイルへの書き込みを指定します。

[--no-discovery] - 検査エンジンを構成するためにディスカバリー・ユーティリティーを使用しません。

[--load-balancer-ip <load_balancer_ip>] - STAP が使用するロード・バランサーの IP を指定します。

[--lb-app-group <app_group>] - STAP が属するアプリケーション・グループを指定します。
重要: スペースまたは特殊文字を含むエンタープライズ・ロード・バランサー・グループはサポートされません。

[--lb-mu-group <mu_group>] - STAP が属する管理対象ユニット・グループを指定します。このオプションを使用するには、[--lb-app-group <app_group>] オプションでアプリケーション・グループも指定する必要があります。

[--lb-num-mus <number_of_mus>] - ロード・バランサーが STAP に割り当てる管理対象ユニットの数を指定します。

[--modules <module-bundles>]: 外部の Ktap モジュールのバンドルを指定します。

[--ktap_allow_module_combos]: Ktap のロードで、カーネルのあいまい一致を許可します。

[--load-balancer-ip <load_balancer_ip>] - STAP が使用するロード・バランサーの IP を指定します。

[--lb-app-group <app_group>] - この STAP が属するエンタープライズ・ロード・バランシング用のアプリケーション・グループ。

[--lb-mu-group <mu_group>] - この STAP が属するエンタープライズ・ロード・バランシング用の管理対象ユニット・グループ。このオプションを使用するには、[--lb-app-group <app_group>] オプションでアプリケーション・グループも指定する必要があります。
重要: スペースまたは特殊文字を含むグループ名はサポートされません。

[--lb-num-mus <number_of_mus>] - ロード・バランサーが STAP に割り当てる管理対象ユニットの数を指定します。

[--modules <module-bundles>]: 外部の Ktap モジュールのバンドルを指定します。

親トピック: シェル・インストーラーを使用した Linux、Solaris、AIX、HP-UX S-TAP のインストール

ネイティブ・インストーラーを使用した Linux、Solaris、AIX、HP-UX S-TAP のインストールとアンインストール

ネイティブ・インストーラーは、シェル・インストーラーにシェルを提供します。唯一の利点は、S-TAP がオペレーティング・システムの資産リポジトリーに確実に登録されることです。この登録は、Guardium で S-TAP をインストールする場合の要件ではありませんが、企業の要件になっている場合があります。ネイティブ・インストーラーは、必要な場合にのみ使用してください。

ネイティブ・インストーラーを使用すると、S-TAP がオペレーティング・システムの資産リポジトリーに確実に登録されます。この登録は、Guardium で S-TAP をインストールする場合の要件ではありませんが、企業の要件になっている場合があります。OS タイプごとに別個のネイティブ・インストーラーがあります。

- AIX ネイティブ・インストーラーを使用した S-TAP のインストールおよびアンインストール
- HP-UX ネイティブ・インストーラーを使用した S-TAP のインストールおよびアンインストール
- Solaris ネイティブ・インストーラーを使用した S-TAP のインストールおよびアンインストール

親トピック: S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール

AIX ネイティブ・インストーラーを使用した S-TAP のインストールおよびアンインストール

手順

1. S-TAP のインストール先となっているデータベース・サーバーの IP アドレスを取得します。仮想 IP を使用する場合は、これらもメモしてください (これらは、構成を完了するときに、後で構成する必要があります)。
2. この S-TAP を制御するコレクターであり、かつ S-TAP が報告を行う先のコレクターの IP アドレスを特定します。
3. データベース・サーバーとコレクターの間の接続を確認します。データベースで、nmap -p <port> <ip_address> を入力します。例えば、ポート 16018 (Guardium® で TLS に使用されるポート) に IP アドレス 192.168.3.104 で到達できるか検査するには、次のコマンドを入力します。
   nmap -p 16018 192.168.3.104
   通常の出力は、以下のとおりです。
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. Guardium S-TAP® のインストール DVD から、ご使用の AIX® のバージョン向けの該当するネイティブ・インストーラー・ファイル (.bff ファイル) を見つけます。
5. クリーン・サーバー (以前に S-TAP インストールを行っていない環境) で、以下のコマンドを入力し、AIX 用のシェル・インストーラーを抽出します。ファイル名は該当する .bff ファイル名に置き換えてください。

   ```
   installp -aX -d/var/tmp<filename> SqlGuardInstaller
   例:
   installp -aX -d/var/tmp/guard-stap-guard-8.0.00rc1_r20934_1-aix-5.2-aix-powerpc.bff SqlGuardInstaller
   ```

   シェル・インストーラーが抽出され、/usr/local の下に guardium という名前で置かれます。

6. インストール手順のステップ 6 を続行し、オペレーティング・システムのバージョンのデフォルト・インストール・スクリプトではなく、生成したインストール・スクリプトを実行します。

親トピック: ネイティブ・インストーラーを使用した Linux、Solaris、AIX、HP-UX S-TAP のインストールとアンインストール

ネイティブ・インストーラーを使用した AIX S-TAP の削除

手順

ネイティブ・インストーラーを使用して AIX S-TAP を削除するには、以下のコマンドを使用します。

```
/usr/lib/instl/sm_inst installp_cmd -u -f 'filename'
```

例

```
/usr/lib/instl/sm_inst installp_cmd -u -f'SqlGuardInstaller'
```

HP-UX ネイティブ・インストーラーを使用した S-TAP のインストールおよびアンインストール

このタスクについて

手順

1. S-TAP のインストール先となっているデータベース・サーバーの IP アドレスを取得します。仮想 IP を使用する場合は、これらもメモしてください (これらは、構成を完了するときに、後で構成する必要があります)。
2. この S-TAP を制御するコレクターであり、かつ S-TAP が報告を行う先のコレクターの IP アドレスを特定します。
3. データベース・サーバーとコレクターの間の接続を確認します。データベースで、nmap -p <port> <ip_address> を入力します。例えば、ポート 16018 (Guardium® で TLS に使用されるポート) に IP アドレス 192.168.3.104 で到達できるか検査するには、次のコマンドを入力します。
   nmap -p 16018 192.168.3.104
   通常の出力は、以下のとおりです。
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. Guardium S-TAP® のインストール DVD で、ご使用の HPUX のバージョン向けの該当するネイティブ・インストーラー・ファイル (.depot.gz ファイル) を見つけます。
5. 以下のコマンドを使用して、ファイルを解凍します。

   ```
   gzip -d <filename>.depot.gz
   ```

6. 選択したファイル名 (該当するネイティブ・インストーラー・ファイル) とデータベース・サーバーのホスト名指定して、以下のようにswinstall コマンドを入力します。このコマンドは対話式プログラムを開始します。 プロンプトに従い、該当するコントロールを使用して、該当する S-TAP インストール・プログラム (.sh ファイル) をインストールします。プログラムは /var/spool/sw/var/tmp にインストールされます。

   ```
   swinstall -s /var/tmp/<filename>.depot @ ,hostname>:/var/spool/sw
   ```

7. インストール手順のステップ 6 を続行し、オペレーティング・システムのバージョンのデフォルト・インストール・スクリプトではなく、生成したインストール・スクリプトを実行します。

親トピック: ネイティブ・インストーラーを使用した Linux、Solaris、AIX、HP-UX S-TAP のインストールとアンインストール

ネイティブ・インストーラーを使用した HPUX S-TAP の削除

手順

ネイティブ・インストーラーを使用して HPUX S-TAP を削除するには、次のコマンドを使用します。

```
swremove @<hostname>:/var/spool/sw
```

Solaris ネイティブ・インストーラーを使用した S-TAP のインストールおよびアンインストール

このタスクについて

手順

1. S-TAP のインストール先となっているデータベース・サーバーの IP アドレスを取得します。仮想 IP を使用する場合は、これらもメモしてください (これらは、構成を完了するときに、後で構成する必要があります)。
2. この S-TAP を制御するコレクターであり、かつ S-TAP が報告を行う先のコレクターの IP アドレスを特定します。
3. データベース・サーバーとコレクターの間の接続を確認します。データベースで、nmap -p <port> <ip_address> を入力します。例えば、ポート 16018 (Guardium® で TLS に使用されるポート) に IP アドレス 192.168.3.104 で到達できるか検査するには、次のコマンドを入力します。
   nmap -p 16018 192.168.3.104
   通常の出力は、以下のとおりです。
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. Guardium S-TAP® のインストール DVD で、以下のように、ご使用の Solaris のバージョン向けの該当するネイティブ・インストーラー・ファイル (.pkg ファイル) を見つけます。
5. 以下のように、pkgadd コマンドを入力し、選択したファイルを使用してインストーラーを実行します。

   ```
   pkgadd -d <filename>.pkg
   ```

   シェル・インストーラーが /usr/local/guardium の下に抽出されます。

6. インストール手順のステップ 6 を続行し、オペレーティング・システムのバージョンのデフォルト・インストール・スクリプトではなく、抽出されたシェル・インストーラー・スクリプトを実行します。

親トピック: ネイティブ・インストーラーを使用した Linux、Solaris、AIX、HP-UX S-TAP のインストールとアンインストール

ネイティブ・インストーラーを使用した Solaris S-TAP の削除

手順

ネイティブ・インストーラーを使用して AIX® S-TAP を削除するには、以下のコマンドを使用します。

```
pkgrm GrdTapIns
```

S-TAP のアンインストール

古い構成ファイルを保存する必要がある場合、S-TAP® の新規バージョンをインストールする前にこの手順を実行します。

このタスクについて

以前に S-TAP がインストールされている場合は、/usr/local/guardium/guard_stap という名前のディレクトリーがあります。

A-TAP がインストールされている場合は、アップグレード/インストール操作を行う前に、それを非アクティブにする必要があります。『A-TAP の非アクティブ化』の A-TAP 非活動化コマンドの説明を参照してください。

K-TAP を使用していた S-TAP の旧バージョンを削除している場合は、データベース・サーバーをリブートする必要があります。K-TAP がインストールされている場合は、/dev/guard_ktap という名前のデバイスがあります。

手順

1. root アカウントを使用して、データベース・サーバー・システムにログオンします。
2. オプションで、S-TAP 構成ファイルを安全な場所 (Guardium 以外のディレクトリー) にコピーします。 デフォルトでは、絶対パス名は /usr/local/guardium/guard_stap/guard_tap.ini となります。 このファイルは、このソフトウェア・バージョンを再インストールする必要がある場合に後で使用することも、S-TAP の更新されたバージョンを構成する際に参照することもできます。 古い構成ファイルは、新バージョンのソフトウェアでは絶対に直接使用しないでください。新しいプロパティーが欠落している可能性があり、デフォルトを使用することにより、S-TAP の始動時に予期しない動作になることがあります。
3. アンインストール・スクリプトを実行します。例えば、デフォルト・ディレクトリーが使用されている場合は、以下のようにします。`[root@yourserver ~]# /usr/local/guardium/guard_stap/uninstall`
4. 前のバージョンの S-TAP に K-TAP が含まれていた場合は、ここでデータベース・サーバーのリブートを行います。

   a. アンインストール・スクリプトを再実行します。

5. このステップは、AIX® WPAR と Solaris ゾーンにのみ適用されます (その他すべての場合はスキップします)。K-TAP が含まれていた前のバージョンの S-TAP をアンインストールする場合は、マスター・ノードから次のコマンドを実行します: rm -f /wpars/<server>/dev/ktap* および rm -f /wpars/<server>/dev/guard_ktap*。ここで、/wpars/<server> はマスター・ノードから WPAR へのパスです。

親トピック: S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール

K-TAP の処理

K-TAP は、オペレーティング・システムにインストールされるカーネル・モジュールです。それは、S-TAP インストール時にインストールされます。インストール後、構成ファイル設定を使用して、使用可能にしたり使用不可にしたりすることができます。使用可能に設定された場合、これは、データベース・クライアントとデータベース・サーバーとの間の通信に使用するメカニズムをフックすることにより、データベース・サーバーへのアクセスを監視します。 K-TAP では、データベース・クライアントのサーバーとの接続方法を変更する必要はありません。

インストール時に、サーバーのオペレーティング・システムに K-TAP カーネル・モジュールをロードするかどうかを選択します。これは、そのモジュールをロードする唯一の方法です。 最初に K-TAP をロードせずに、後で K-TAP を使用することにした場合は、S-TAP® を削除してから、再インストールする必要があります。
注: インストール中に K-TAP のロードが適切に行われなかった場合、ハードウェアまたはソフトウェアの互換性が原因である可能性があります。デフォルトの収集メカニズムとして P-CAP がインストールされます。
注: セッション内トラフィックは、コールバックを使用することで古い KTAP から新規 KTAP に転送されます。つまり、ほとんどのデータベースでは、既存のセッションに対する新しい KTAP を使用したインターセプトが再開されるまでに、2 つの SQL 要求を受け取ることができます。Sybase IOCP の場合は、セッションの性質上、3 つの SQL 要求を受け取ります。

- K-TAP の概要
  S-TAP のインストール時、正しい K-TAP バージョンのロードが試行されます。また、K-TAP が UID チェーンを処理する方法の読み取りも試行されます。
- Linux での K-TAP の作成
  使用可能な何百もの Linux ディストリビューションが存在し、そのリストは増え続けています。このことは、ご使用の Linux ディストリビューションで使用可能な K-TAP がまだ存在しない可能性があることを意味します。適切な K-TAP が使用可能でない場合、S-TAP インストール・プロセスにより自動で作成することができます。
- 新規 K-TAP モジュールの他のシステムへのコピー
  Linux データベース・サーバー用の新しい K-TAP モジュールをビルドしたら、そのモジュールを同じ Linux ディストリビューションを稼働する他のデータベース・サーバーにコピーすることができます。

親トピック: S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール

K-TAP の概要

S-TAP のインストール時、正しい K-TAP バージョンのロードが試行されます。また、K-TAP が UID チェーンを処理する方法の読み取りも試行されます。

KTAP ローダー・メカニズム

KTAP ローダー・メカニズムは、Linux S-TAP のインストール (GIM および GIM 以外を使用) で以下のシーケンスを使用します。

注: KTAP ローダー・メカニズムは前のステップが成功しなかった場合、次のステップに自動的に進みます。

1. KTAP ローダーは、オペレーティング・システム・レベルに完全に一致するカーネル・モジュールを探し、見つかった場合は、それをロードします。
2. KTAP ローダーが一致するものを見つけられなかった場合、KTAP モジュールをローカルにコンパイルし、それをロードします。これは、システムに必要なパッケージ (ブートされたカーネルの場合は gcc および kernel-devel) がインストールされている場合にのみ発生する可能性があります。
3. KTAP ローダーが正しいカーネル・モジュールをまだロードできない場合で、かつ FlexLoad メカニズムがオンの場合、KTAP ローダーは最も一致率が高いカーネル・モジュールを見つけ、それをロードします。

   FlexLoad メカニズムをオンにするには、以下のフラグを使用します。
   - シェル・インストールの場合: --ktap_allow_module_combos
   - GIM インストールの場合: KTAP_ALLOW_MODULE_COMBOS=Y
4. KTAP がカーネル・モジュールをロードできない場合、「ロードに失敗しました」メッセージで通知します。それは、KTAP なしで S-TAP をインストールしたか、S-TAP インストールが失敗したかのいずれかです。その場合、一致するモジュールを Guardium サポートに要求できます。これは、準備するのに約 2 週間かかります。

K-TAP および UID チェーン

UID チェーンは、それを使用することで、S-TAP が (K-TAP を介して)、データベース接続前に発生したユーザーのチェーンをトラッキングできるメカニズムです。それは、Solaris ゾーン、AIX WPAR、Solaris 8/9、Solaris 11 SPARC でサポートされています。

あるユーザーが、例えば、ssh informix@barbet、su - db2inst1、su -、su - oracle9 を実行してから、sqlplus scott/tiger@onora1 を実行することで、何回かユーザー名を変更してから、データベースに接続する場合があるとします。Guardium では、UID チェーンを使用して、プロセスを呼び出したプロセスに戻ってプロセスをトレースし、元の (問題の) ユーザーまで戻ることができます。

- Solaris ゾーンの場合は、ユーザー名の代わりにユーザー ID が報告される可能性があります。
- SSH クライアントの IP アドレスとポートが UID チェーンに追加されます。
- ゾーンを使用する Solaris 11 での Postgres はサポートされていません。一部のディレクトリーにマスター・ゾーンからスレーブ・ゾーンへのアクセスを許可しないゾーン構成があるためです。
- Solaris ゾーンおよび AIX® WPAR: guard_tap.ini ファイル内の db2bp_path を、db2bp 実行可能ファイルの絶対パス (グローバル・ゾーン/wpar から見た、関連する db2bp の絶対パス) に設定します。
- Solaris 8/9 では、プロセス間通信 (IPC) 用の UID チェーンはありません。
- Hadoop データベースでは、UID チェーンは検出されません。
- hunter_trace パラメーターは、UNIX S-TAP® での TCP/IP 接続には必須です。インストール時に hunter_trace = 1 を設定して、ローカル TCP/IP 接続の uid_chain を使用可能にします。
- セッションを開始したプロセスが、STAP がそれを調査する前に終了した場合、UID チェーンは機能しません。
- Linux for Db2 では、UID チェーンでローカル TCP はサポートされません。さらに、Db2 出口は、UID チェーンをサポートするために特定バージョンのデータベースを必要とします。
- 非 root ユーザーとして実行する場合、UID チェーンは S-TAP を使用した Db2 共有メモリー (SHM) に対しては機能しません。
- Guardium は、ネットワーク・トラフィックの UID チェーンをログに記録しません。
- Guardium は UID チェーンを判別するためにアプリケーションのプロセス ID に依存するため、Guardium は非常に短時間のセッションの UID チェーンをログに記録しない可能性があります。セッションを開始したプロセスが、STAP がそれを調査する前に終了した場合、UID チェーンは機能しません。

制約事項: トラフィックのインターセプトに A-TAP を必要とするシナリオでは、UID チェーンはサポートされません。以下のものがあります。

- Oracle ASO 暗号化トラフィックをインターセプトする ATAP
- Sybase 暗号化トラフィックをインターセプトする ATAP
- Teradata 暗号化トラフィックをインターセプトする ATAP

- Linux 上の Db2 または Informix 共有メモリー・トラフィック (ATAP が必要)

UID チェーン・レコードのパージ

2 時間を経過した UID チェーン・レコードは、通常の推論プロセスが実行されるときにパージされます。 経過時間が 1 日を超えるレコードは、毎夜パージされます。

注: KTAP パラメーター・トピックの CUSTOM BUNDLES に関する情報を参照してください。
親トピック: K-TAP の処理

Linux での K-TAP の作成

使用可能な何百もの Linux ディストリビューションが存在し、そのリストは増え続けています。このことは、ご使用の Linux ディストリビューションで使用可能な K-TAP がまだ存在しない可能性があることを意味します。適切な K-TAP が使用可能でない場合、S-TAP インストール・プロセスにより自動で作成することができます。

Linux システムに S-TAP をインストールすると、インストール・プロセスは Linux カーネルをチェックして、そのカーネルで処理を実行するための K-TAP が作成されているかどうかを判別します。過去に KTAP がロードされていないカーネルが実行されている場合は、一致するモジュールを検索してそれをロードします。インストール・プロセスは、対応する K-TAP を検出できない場合、当該 Linux カーネルに対応する K-TAP の作成を試みます。

ほとんどの K-TAP コードは、カーネルから独立しています。バージョン 9.1 のインストーラーでは、カーネルに依存しないコードとご使用のカーネルとの対話を可能にする新規層のコードが提供されています。この新規層は、独自仕様のソース・コードとして提供されます。 インストーラーは、この独自仕様のソース・コードをユーザーの Linux カーネルに対してコンパイルすることで、完全な K-TAP を作成します。 これにより、ご使用の Linux ディストリビューションに固有の K-TAP が作成されます。

このプロセスでは、Linux ディストリビューションで提供されている標準のカーネル開発ユーティリティーが、K-TAP が作成されるデータベース・サーバーに存在している必要があります。開発パッケージはカーネルに完全に対応していなければなりません。gcc コンパイラーとバージョン 3.81 以降の MAKE ユーティリティーも必要です。

同じ Linux ディストリビューションを実行している複数のシステムがある場合は、1 つのシステム上で K-TAP を作成し、それをその他のシステムにコピーすることができます。例えば、テスト・システムで K-TAP を作成し、テストを行った後に、1 つ以上の実動データベース・サーバーにその K-TAP をコピーできます。 Guardium Installation Manager (GIM) を使用して S-TAP をインストールする場合、GIM は、新規 K-TAP が含まれているバンドルを、他のデータベース・サーバーへの配布元とすることができる Guardium システムに自動的にコピーできます。

インストーラーが K-TAP モジュールの作成を試みる際、guard-ktap-loader によって発行されるメッセージが表示されます。例えば、以下のメッセージがあります。

- 作成を試みています (It is attempting to build)
- 作成が完了しました (The build has completed)
- K-TAP がロードされました (K-TAP has been loaded)
- カーネル開発パッケージが見つからないため、作成を行うことができません (The build cannot be attempted, because the kernel development package is not found)

親トピック: K-TAP の処理
新規 K-TAP モジュールの他のシステムへのコピー
GIM を使用した K-TAP モジュールのコピー

新規 K-TAP モジュールの他のシステムへのコピー

Linux データベース・サーバー用の新しい K-TAP モジュールをビルドしたら、そのモジュールを同じ Linux ディストリビューションを稼働する他のデータベース・サーバーにコピーすることができます。

始める前に

Linux データベース・サーバー上で K-TAP モジュールをビルドし、テストした後、以下の手順を実行します。

このタスクについて

データベース・サーバー上でのエージェントの管理に Guardium Installation Manager (GIM) を使用している場合は、GIM を使用してモジュールをコピーします。使用する手順については、以下のリンクを参照してください。

手順

1. テスト済みの K-TAP のあるデータベース・サーバーにログインします。
2. /usr/local/guardium/guard_stap/ktap/current/ ディレクトリーに移動して、 ./guard_ktap_append_modules を実行し、ローカルにビルドしたモジュールを modules.tgz に追加します。
3. 更新された modules.tgz ファイルをターゲット・サーバーにコピーします。
4. ターゲット・サーバーにログインして、/usr/local/guardium/guard_stap/ktap/current/ ディレクトリーに移動します。
5. retry パラメーターと、更新された modules.tgz ファイルへの絶対パスを指定して、K-TAP ローダーを実行します。例:

```
guard_ktap_loader retry /tmp/modules-9.0.0_r55927_v90_1.tgz
```

6. S-TAP を再始動して、この新しい K-TAP モジュールに接続します。

タスクの結果

ターゲット・システム上で、カスタム K-TAP モジュールを使用する準備ができました。この K-TAP モジュールのデプロイ先となる対応する Linux システムごとに、この手順を繰り返します。
親トピック: K-TAP の処理
GIM を使用した K-TAP モジュールのコピー

Java または Perl の情報の取得

データ・サーバーで使用されている Java または Perl のバージョンをチェックしなければならない場合があります。

Java 情報の取得

CAS (構成監査システム) を UNIX システムにインストールする場合は、以下の 2 つの要件があります。

- JAVA_HOME ディレクトリーを見つける必要があります。 CAS のインストール中に、その場所を求めるプロンプトが出されます。
- サポートされる Java™ のバージョンがインストールされていることを確認する必要があります (以下の表を参照してください)。 サポートされるバージョンがインストールされていない場合は、CAS をインストールする前にそれをインストールする必要があります。
  CAS Java バージョンの要件

OS タイプ	Java バージョン
HP-UX	1.5 以上
その他すべて	1.4.2 以上

  注: FIPS 準拠の環境で SSL による CAS を使用するには、CAS エージェントが実行されているサーバーに IBM Java がインストールされている必要があります。

  JAVA_HOME ディレクトリーの検索

  最初にこの手順を実行し、JAVA_HOME ディレクトリーを見つけた後で、以下の手順を実行して Java バージョンを確認します。

JAVA_HOME ディレクトリーには、Java コマンドが格納されています。例:

- java コマンドが /usr/local/j2sdk1.4.2_03/bin/java の場合
- JAVA_HOME ディレクトリーは、/usr/local/j2sdk1.4.2_03 です。

以下のいずれかの方法を使用して、java コマンド・ディレクトリーを見つけます。

1. which java コマンドを入力します。例:

```
[root@yourserver ~]# which java
/usr/local/j2sdk1.4.2_03/bin/java
```

2. which java コマンドによってシンボリック・リンクが戻された場合は、ls -ld <symbolic_link> コマンドを使用して、実際の Java ディレクトリー名を判別します。
3. which java コマンドによって「command not found」というメッセージが戻された場合、Java はインストールされていても、PATH 変数には含まれていない可能性があります。 この場合は、find コマンドを使用して、Java ディレクトリーを見つけます。 例:

```
[root@yourserver ~]# find . -name java

./usr/bin/
```

Java バージョンの判別

1. java ディレクトリーから、java -version コマンドを実行して、バージョン番号を確認します。例:

```
[root@yourserver ~]# /usr/local/j2sdk1.4.2_03/bin/java -version
java version "1.4.2_03"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_03-b02)
Java HotSpot(TM) Client VM (build 1.4.2_03-b02, mixed mode)
```

2. 返された Java バージョンをメモします。この情報を求めるプロンプトは出されませんが、後で問題が発生した場合に、サポートされない Java バージョンの可能性を除外できます。

Perl 情報の取得

この Perl の要件は、以下の組み合わせにのみ適用されます。

- Unix S-TAP®
- ローカル・トラフィックのモニター用に TEE メカニズムが選択されている。
- Tee 聴取ポートをバイパスするプロセスを検出し、オプションでそのプロセスを強制終了するためにハンター・プロセスが使用されている。

このような状態では、以下が必要です。

- バージョン 5.8.0 以降の Perl
- Perl は、/usr/bin ディレクトリーにインストールされている必要があります。

インストールされているバージョンを確認するには、次のコマンドを使用します。

```
/usr/bin/perl -v
```

Perl がインストールされていない場合、異なるディレクトリーにインストールされている場合、または古いバージョンがインストールされている場合は、S-TAP をインストールする前に、バージョン 5.8.0 以降の Perl を /usr/bin ディレクトリーにインストールする必要があります。

親トピック: S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストール

S-TAP のインストール後またはアップグレード後にデータベースを再始動またはリブートするタイミング

このトピックでは、S-TAP をインストールした後に、データベース・サーバーまたはデータベース・インスタンスを再始動する必要がある場合、およびリブートする必要がある場合の具体例を詳しく説明します。Windows 上の S-TAP と UNIX/Linux 上の S-TAP の両方について説明します。 v9.0/9.1/9.5 と v10.0/10.1 の両方について説明します。 再始動およびリブートの要件は、GIM による実装と GIM を使用しない実装のどちらの場合も同じです。

UNIX/Linux S-TAP のフレッシュ・インストール後に再始動を必要とするデータベース

トラフィックをすべて表示するには、S-TAP のインストール後に一部のデータベースを再始動する必要があります。

表 1. S-TAP インストール後のデータベースの再始動

OS / データベース	**Oracle**		**Db2**		**Sybase**		**MS-SQL**		**Informix**	
	TPC/IPC	SHM	TPC/IPC	SHM	TPC/IPC	SHM	TPC/IPC	SHM	TPC/IPC	SHM
RedHat	NR	NR	NR	REQ-Exit	NR	NR	NR	NR	NR	REQ-Exit
SuSE	NR	NR	NR	REQ-Exit	NR	NR	NR	NR	NR	REQ-Exit
AIX	REQ*	NR	REQ	NR	REQ	NR	NA	NR	REQ	NR
Solaris	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR
HP-UX	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR
Windows	NR		NR		NR		NR		NR	

SHM - 共有メモリー

NR = 再始動/リブートは不要 (ライブ・アップデート・メカニズムの使用と、ライブ・アップデート・リンクの参照 (ライブ・アップデート・リンクがある場合) に基づく)

REQ = 再始動が必要

REQ-W = v8 および v9 の Windows S-TAP のフレッシュ・インストールの場合は、データベース・インスタンスの再始動のみが必要 (データベース・サーバーの再始動は不要)。ライブ・アップデートの場合は、データベース・サーバー、データベース・インスタンスともに再始動は不要。v10.x Windows S-TAP のフレッシュ・インストールの場合は、再始動は不要。

REQ * = データベースとリスナーの再始動が必要

REQ-Exit = この場合、共用メモリー・トラフィックをキャプチャーするために A-TAP または Exit ドライバーが必要です。プロセスをアクティブ化するには、データベースの再始動が必要です。

NA = 適用されない

注: RedHat データベースを伴う MySQL データベース - NR
注: 接続プーリングが使用される場合に、データベース・インスタンスの再始動が必要になります。 (すべてのセッションを切断して再接続する必要があるので、アプリケーション・サーバー環境で DB リスナーを再始動する必要があります。)
注: (V10.0 UNIX/Linux S-TAP) - 再始動するタイミングについて違いはありません。ただし、v10 ではGuardium は「guard-stap-update スクリプト」をサポートしなくなりました。 代わりに、提供されているシェル・インストーラーに、アップグレード・ロジックが組み込まれています。そのため、新規インストーラーを実行するだけですみます。

UNIX/Linux の S-TAP のライブ・アップグレード後に再始動が必要なもの

ATAP を含まないライブ・アップグレードでは、再始動はまったく不要です。

Windows S-TAP

Windows のフレッシュ・インストールとライブ・アップグレードを区別する必要があります。

スクラッチ・インストール (フレッシュ・インストール) 時には、すべてのデータベース・インスタンスは (リブートではなく) 再始動する必要があります。 V10.0 WFP ドライバーの使用に関する情報の例外を参照してください。ライブ・アップグレード後にデータベース・インスタンスの再始動は必要ありません。

V7.0 からのアップグレード時を除いて Windows サーバーのリブートは必要ありません。これは、V7.0 からのアップグレードでは、S-TAP ソフトウェアのフル・アンインストールが必要になるためです。 ただし、プロキシー・ドライバー・ファイルが更新される場合、 システム・リブートが必要になります。プロキシー・ドライバー・ファイルの例: NmpProxy.sys 注記: リリースごとに、プロキシー・ドライバーが更新されたかどうかを確認するためリリース資料を参照してください。

Guardium V7.0 からのアップグレード時にはリブートが必要です。 これは、すべてのインストール/アップグレード・メソッド (GIM、インタラクティブ、またはバッチ) で当てはまります。

V10.0 Windows STAP は新規 WFP (Windows Filtering Platform) ドライバーを使用します。 この WFP ドライバーは、Transport driver interface (TDI) ベースの TCP ドライバーを置き換えるものです。 Wfpmonitor は、新規の S-TAP TCP ドライバーで、lhmonproxy および lhmon に置き換わるものです。WFP には以下の利点があります。

- リブートせずにアップグレードできます。
- フレッシュ・インストール後に、TCP トラフィックを取得するためにデータベース・インスタンスを再始動する必要がありません。
- すべてのドライバーが、(周期的な) ロギング機能を提供します。ログ・ファイルは、/logs にあります。ドライバーのエラー/警告は表示されないため、この機能はサポート性を拡張するものです。

UNIX/Linux S-TAP

リブートが不要な場合:

「guard-stap-update」ユーティリティーを使用する場合、リブートせずに S-TAP/KTAP をアップグレードできます。このユーティリティーは、V8.0 以降のバージョンから使用できます。(v10.0 UNIX-Linux S-TAP の場合は、Guardium が「guard-stap-update」ユーティリティーをサポートしなくなったことに関する上記の注を参照してください。)

システムを、非 GIM バージョンから同じ GIM バージョンに「アップグレード」する場合、システムをリブートする必要はありません。

非 GIM の S-TAP を、現在稼働している S-TAP と同じリビジョン番号の GIM BUNDLE-STAP でアップグレードする場合、リブートは不要です。

以下の場合のアップグレードでのみ、Bundle-GIM upgrade (Bundle-S-TAP upgrade に加えて) が必要です。

- V8 から V9 へのアップグレードを行う場合。
- インストールされている V9 の Bundle-S-TAP のパッチ・レベルが V9.0 パッチ 100 より前のレベルであるか、またはビルド番号が 9.0.0_r57263 より前の番号である場合。
- これ以外のすべてのアップグレードの場合には、Bundle-GIM upgrade は不要です。

リブートが必要な場合:

Guardium V7.0 からのアップグレード時にはデータベース・サーバーのリブートが必要です。

Guardium アップグレーダー・ユーティリティーで次回リブート時に S-TAP をアップグレードします。このユーティリティーを使用する場合は、リブートが必要です。

KTAP を使用していた S-TAP の旧バージョンを削除している場合は、データベース・サーバーをリブートする必要があります。

GIM を使用した S-TAP のアップグレード時:

- KTAP_LIVE_UPDATE=Y を指定した場合は、リブートは不要です。
- KTAP_LIVE_UPDATE=N を指定した場合は、リブートが必要です。

非 GIM の S-TAP を、現在稼働している S-TAP とは異なるリビジョン番号の GIM BUNDLE-STAP でアップグレードする場合は、リブートが必要です。

S-TAP を KTAP を指定して再インストールするには、同じリビジョン番号を使用する場合でも、アンインストールとリブートが必要です。

Oracle クラスター環境内に UNIX ATAP をインストールした後は、各インスタンスおよびすべてのクラスター間プロセスを再始動する必要があります。

ATAP のための再始動/ロード/インスツルメンテーション/アクティブ化の要件

ATAP、S-TAP、KTAP のいずれもリブートされません。

S-TAP は、停止/開始/再始動されます。KTAP は、ロード/アンロードされます。ATAP では、インスツルメンテーション/アクティブ化/非アクティブ化/インスツルメンテーションの削除が行われます。

ATAP を必要とするデータベース・インスタンスを、インスツルメンテーション (必要な場合) およびアクティブ化を行う前に停止する必要があります。

ATAP のインスツルメンテーションの削除または非アクティブ化でも、該当するデータベース・インスタンスを停止する必要があります。

フィックスパックの適用時など、データベースをアップグレードする前にはいつでも、ATAP を非アクティブ化する必要があります (また該当する場合は、インスツルメンテーションを削除する必要があります)。

最後に、S-TAP をアップグレードする前にはいつでも、ATAP の非アクティブ化およびインスツルメンテーションの削除を行う必要があります (Bundle-GIM upgrade では不要です)。

親トピック: S-TAP のインストール

エンタープライズ・ロード・バランシング

エンタープライズ・ロード・バランサーは、管理対象ユニットをシステムの負荷と利用可能性に基づいて動的に S-TAP エージェントに割り当てます。

概要

ロード・バランシングを行うと、新しい S-TAPs がインストールされた場合や、管理対象ユニットが使用不可である場合のフェイルオーバー時に、管理対象ユニットが S-TAP エージェントに対して自動的に割り当てられます。 ロード・バランシング・アプリケーションは、負荷が低い管理対象ユニットに S-TAP エージェントを再配置することにより、負荷の高い管理対象ユニットやビジー状態の管理対象ユニットの負荷を動的に分散します。

エンタープライズ・ロード・バランシング・アプリケーションにより、いくつかのタスクが自動化されます。

- ロード・バランシングにより、管理対象ユニットを S-TAP エージェントに割り当てる前に、それらの管理対象ユニットの負荷を手動で評価する必要がなくなります。
- ロード・バランシングにより、インストール後の S-TAP の構成作業の一部として、フェイルオーバー用の管理対象ユニットを定義する必要がなくなります。これは、ロード・バランサーにより、フェイルオーバーのシナリオが動的に管理されるためです。
- ロード・バランシングにより、負荷の高い管理対象ユニットから負荷の低い管理対象ユニットに S-TAP エージェントを手動で再配置する必要がなくなります。

重要: エンタープライズ・ロード・バランシング・アプリケーションを使用すると、Guardium システムにより、S-TAP エージェントに対する管理対象ユニットの割り当てが制御されます。 これは、動的な自動プロセスです。使用可能な管理対象ユニットの相対的な負荷に基づいて S-TAPs の関連付けが変化するのを確認することができます。 ロード・バランシングのすべてのアクティビティーを確認するには、「ロード・バランサー・イベント」レポートを使用してください。
注: エンタープライズ・ロード・バランシングを使用するように S-TAP を構成する場合、F5 ベースのロード・バランシングは使用できません。

前提条件

エンタープライズ・ロード・バランサーは中央マネージャーまたは管理対象ユニット上で稼働し、ポート 8443 を listen し、トランスポート層セキュリティー (TLS) を使用します。新しいファイアウォールや追加のシステム設定は必要ありません。エンタープライズ・ロード・バランサーを管理対象ユニット上で実行するように構成する場合、S-TAP が V10.1 以上でなければなりません。

ロード・バランシング機能は、Guardium システム上でデフォルトで有効になっています。S-TAPs を有効にしてロード・バランシングを行う方法については、エンタープライズ・ロード・バランシング用に S-TAP のインストール済み環境を構成するを参照してください。

ロード・バランシングの仕組み

エンタープライズ・ロード・バランシング・アプリケーションは、すべての管理対象ユニットから最新の負荷情報を収集して保守することによって機能します。

このアプリケーションは、管理対象ユニットの負荷情報を使用して、ロード・マップを作成します。このロード・マップにより、ロード・バランシングを指示するデータと、管理対象ユニットの割り当てアクティビティーが指定されます。 GuardAPI コマンドの grdapi get_load_balancer_load_map を使用すると、現在のロード・マップをいつでも表示することができます。

負荷情報は、LOAD_BALANCER_ENABLED=1 パラメーターが構成されているオンライン状態の管理対象ユニットからのみ収集されます。LOAD_BALANCER_ENABLED=0 を設定すると、ロード・バランシングが無効になり、ロード・バランシング・アクティビティーの実行中に管理対象ユニットが S-TAP エージェントに動的に割り当てられることがなくなります。

特定の管理対象ユニットから負荷情報を収集できなかった場合は、「ロード・バランサー・イベント」レポートにエラーとして記録されますが、全体的な負荷情報収集プロセスとロード・バランシング・プロセスには影響しません。ただし、負荷情報を収集できなかった管理対象ユニットは、ロード・バランシング・プロセスの対象から除外されます。

- エンタープライズ・ロード・バランシング機能の使用
  エンタープライズ・ロード・バランシング機能の使用を開始するには、以下のタスク・シーケンスを実行します。
- エンタープライズ・ロード・バランシングの構成パラメーター
  この参照情報では、ロード・バランサーの構成パラメーターについて詳しく説明します。CM では、「管理」 > 「一元管理」 > 「エンタープライズ・ロード・バランシング」 > 「エンタープライズ・ロード・バランシング・プロパティー」からアクセスします。MU では、「セットアップ」 > 「一元管理」 > 「登録およびロード・バランシング」からアクセスします。

親トピック: S-TAPs およびその他のエージェント

エンタープライズ・ロード・バランシング機能の使用

エンタープライズ・ロード・バランシング機能の使用を開始するには、以下のタスク・シーケンスを実行します。

1. エンタープライズ・ロード・バランシング用に S-TAP のインストール済み環境を構成する
   ここでは、S-TAP エージェントのインストール時にエンタープライズ・ロード・バランシング機能を構成する方法について説明します。
2. ロード・バランシング用に S-TAP を管理対象ユニットに関連付ける
   ここでは、S-TAP グループを作成して管理対象ユニットのグループに関連付けることにより、エンタープライズ・ロード・バランシング機能を使用する方法について説明します。
3. エンタープライズ・ロード・バランシングのロード・マップの表示
   ここでは、現在のエンタープライズ・ロード・バランサーのロード・マップを表示する方法について説明します。
4. エンタープライズ・ロード・バランシング・アクティビティー・レポートの表示
   ここでは、エンタープライズ・ロード・バランシングのイベントとアクティビティーのレポートを表示する方法について説明します。

親トピック: エンタープライズ・ロード・バランシング

エンタープライズ・ロード・バランシング用に S-TAP のインストール済み環境を構成する

ここでは、S-TAP エージェントのインストール時にエンタープライズ・ロード・バランシング機能を構成する方法について説明します。

手順

S-TAP をインストールする際に、エンタープライズ・ロード・バランシング機能のパラメーターを指定します。コマンド行インストーラーまたは GIM インストーラーのどちらを使用しても、同じパラメーターを使用できます。
注: コマンド行を使用して S-TAP をインストールし、ロード・バランサー・オプションにデフォルト・アドレス以外のクライアント IP アドレスを指定すると、ロード・バランサーが管理対象ユニットの割り振りを誤る可能性があります。これは、S-TAP のインストール中に非デフォルト・アドレスが指定される前に、デフォルトのクライアント IP アドレスがロード・バランサーに送信されると発生します。
注: 以下の表にリストされているパラメーターについては、UNIX/Linux の場合にはパラメーターの前に -- (ダッシュ 2 つ) を使用し、Windows の場合は単一のダッシュを使用します。例えば、UNIX/Linux: --load-balancer-ip、 Windows: -load-balancer-ip です。

表 1. エンタープライズ・ロード・バランシング用の S-TAP インストール・パラメーター

対話式インストーラーのパラメーター	GIM インストーラーのパラメーター	記述

対話式インストーラーのパラメーター	GIM インストーラーのパラメーター	記述
--load-balancer-ip load_balancer_ip	STAP_LOAD_BALANCER_IP	必須。このオプションにより、この S-TAP がロード・バランシングで使用する中央マネージャーまたは管理対象ユニットの IP アドレスを指定します。 注意: • participate_in_load_balancing=0 および num_mus > 1 を設定してエンタープライズ・ロード・バランシングを使用している場合、フェイルオーバー・データは 2 次システムに送信されません。 代わりにフェイルオーバー・データは、障害のあるサーバーと置き換えるためにロード・バランサーによって割り振られたシステムに送信されます。これが行われるのは、中央マネージャーが実行されていて Enterprise Load Balancer がアクティブである場合に限られます。ロード・バランサーが使用できない場合、トラフィックは 2 次 sqlguard_ip に転送されます。 • Windows S-TAP パラメーターは、アップグレード中に対話式インストーラーを使用して変更することはできません。Windows S-TAP パラメーターを変更するには、アップグレード後に Guardium UI を使用します。 • エンタープライズ・ロード・バランサーを管理対象ユニット上で実行するように構成する場合、S-TAP が V10.1 以上でなければなりません。
--lb-app-group app_group	STAP_INITIAL_BALANCER_TAP_GROUP	オプション。このオプションにより、この S-TAP が属する S-TAP グループを指定します。 重要: スペースまたは特殊文字を含むグループ名はサポートされません。
--lb-mu-group mu_group	STAP_INITIAL_BALANCER_MU_GROUP	オプション。このオプションにより、app-group を関連付ける管理対象ユニット・グループを指定します。このパラメーターを使用するには、アプリケーション・グループも指定する必要があります。 注: スペースまたは特殊文字を含むグループ名はサポートされません。 このパラメーターは、初期インストール時に 1 回しか指定できません。 S-TAP のインストール中に使用できるようにするには、前もって中央マネージャーに MU グループが存在している必要があります。 重要: スペースまたは特殊文字を含むグループ名はサポートされません。
--lb-num-mus number_of_mus	STAP_LOAD_BALANCER_NUM_MUS	オプション。このオプションにより、この S-TAP に対してロード・バランサーが割り当てる管理対象ユニットの数を指定します。

親トピック: エンタープライズ・ロード・バランシング機能の使用
次のトピック: ロード・バランシング用に S-TAP を管理対象ユニットに関連付ける

ロード・バランシング用に S-TAP を管理対象ユニットに関連付ける

ここでは、S-TAP グループを作成して管理対象ユニットのグループに関連付けることにより、エンタープライズ・ロード・バランシング機能を使用する方法について説明します。

このタスクについて

ロード・バランシングを行うと、S-TAP グループと管理対象ユニット・グループとの間に関連付けが作成され、グループ内の S-TAPs を、グループ内で最も可用性が高い管理対象ユニットに再割り当てできるようになります。このタスクでは、エンタープライズ・ロード・バランシング機能を使用できるようにするため、S-TAP グループと管理対象ユニット・グループとの間に関連付けを作成する必要があります。

手順

1. 中央マネージャーで、「管理」 > 「一元管理」 > 「エンタープライズ・ロード・バランサー (Enterprise Load Balancer)」 > 「S-TAP と管理対象ユニットの関連付け」にナビゲートします。
2. まだ S-TAP グループが作成されていないか、新しい S-TAP グループが必要な場合は、新たに S-TAP グループを作成します。
   a. アイコンをクリックして、「新規 S-TAP グループの作成」ダイアログを開きます。
   b. 「グループ名」フィールドに名前を入力します。 例えば、`North_American_S-TAPs` などです。
      推奨: 他の Guardium コンポーネントとの互換性を確保するために、グループ名にスペースまたは特殊文字を使用しないでください。
   c. 既存のホスト名から選択するか、「グループ・メンバー」フィールドを使用して新規メンバーを追加することにより、グループ・メンバーを追加します。 アイコンが表示されている S-TAPs は、新しい S-TAP グループに含まれています。
   d. 「新規グループの作成」をクリックして、S-TAP グループを作成します。
3. S-TAP グループを管理対象ユニット・グループに関連付けます。
   a. 関連付ける S-TAP グループを選択します。 例えば、`North_American_S-TAPS` などです。
   b. 「管理対象ユニットの関連付け」をクリックして、「管理対象ユニット・グループの関連付け」ダイアログを開きます。
   c. 必要な場合は、新しい管理対象ユニット・グループを作成します。
      i. 「管理」 > 「一元管理」 > 「管理対象ユニット・グループ」にナビゲートします。
      ii. アイコンをクリックして、「新規管理対象ユニット・グループの作成」ダイアログを開きます。
      iii. 「グループ名」フィールドに名前を入力します。例えば、`North_American_MUs` などです。
      推奨: 他の Guardium コンポーネントとの互換性を確保するために、グループ名にスペースまたは特殊文字を使用しないでください。

iv. 既存の「管理対象ユニット IP アドレス (Managed Unit IP addresses)」から選択してグループ・メンバーを追加します。

v. 「新規グループの作成」をクリックして、管理対象ユニットの新しいグループを作成します。

d. S-TAP グループに関連付ける管理対象ユニット・グループを選択します。 例えば、`North_American_MUs` などです。
e. 「適用」をクリックします。

4. 「保存」をクリックして、S-TAP グループと管理対象ユニット・グループ間の関連付けを完了します。
5. (オプション) S-TAP グループを管理対象ユニットのフェイルオーバー・グループに関連付けます。
   a. 関連付けたい S-TAP グループを選択します。これには、既に管理対象ユニット・グループに関連付けられているものを選択します。例えば、North_American_S-TAPS などです。
   b. 「フェイルオーバー・グループの関連付け」をクリックして「フェイルオーバー・グループの関連付け」ダイアログを開きます。
   c. 必要な場合は、上記と同じようにして新しい管理対象ユニット・グループを作成します。通常の管理対象ユニット・グループとフェイルオーバー・グループの両方は、S-TAP グループとの関連付けの際に指定されるまで同じです。
   d. S-TAP グループに関連付ける管理対象ユニット・グループを選択します。例えば、North_American_MUs_failover などです。
   e. 「適用」をクリックします。
6. 「保存」をクリックして、S-TAP グループと管理対象ユニット・グループ間の関連付けを完了します。

親トピック: エンタープライズ・ロード・バランシング機能の使用
前のトピック: エンタープライズ・ロード・バランシング用に S-TAP のインストール済み環境を構成する
次のトピック: エンタープライズ・ロード・バランシングのロード・マップの表示

エンタープライズ・ロード・バランシングのロード・マップの表示

ここでは、現在のエンタープライズ・ロード・バランサーのロード・マップを表示する方法について説明します。

このタスクについて

エンタープライズ・ロード・バランシング・アプリケーションは、管理対象ユニットから収集した負荷情報を使用して、ロード・マップを作成します。このロード・マップにより、ロード・バランシングを指示するデータと、管理対象ユニットの割り当てアクティビティーが指定されます。

手順

1. 現在のロード・マップを Guardium UI のレポートとして表示するには、「管理」 > 「レポート」 > 「ユニット使用状況」 > 「ロード・バランサー」にナビゲートします。
2. また、現在のロード・マップは Guardium API を使用して表示することもできます。GuardAPI コマンドの grdapi get_load_balancer_load_map を実行します。

ロード・マップは以下の例のようになります。

```
ID=0

************ LOAD MAP *************

****************  LOADED MU LIST ************************

****************  VACANT MU LIST ************************
  {
   MU=myguard_01.domain.com
   MU_QUEUE_SIZE(MB)=25.0
   MU_TIMES_REBALANED=0
   MU_EFFECTIVE_MAX_USED_QUEUE(%)=0.0
   MU_MAX_LOAD_CONTIB_BY_STAP(MB)=0.0
   MU_ADJUSTED_STAP_CONTRIB_IN_MB=0.0
   MU_BASE_MAX_USED_QUEUE_IN_MB=0.0
   IS_REBALANCABLE=true
   INSTALLED_POLICIES=log full details|
   APPLIANCE_RESOURCE_INFO={NUM_PROCESSORS=4,CPU_SPEED=2800,CPU_CACHE=25600,CPU_CORES=4,
      CACHE_READ_RATE=7870,HARD_DRIVE_READ_RATE=186,MEMORY_SIZE=24607}
   STAP_LIST=
      {
      STAP_IP=01_gct1.domain.com, STAP_HOST=01_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
         PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0,
         AVG_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0
      }
      {
      STAP_IP=02_gct1.domain.com, STAP_HOST=02_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
         PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0,
         AVG_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0
      }
      {
      STAP_IP=03_gct1.domain.com, STAP_HOST=03_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
         PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0,
         AVG_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0
      }
  }

****************  STAP -> MUS ALLOCATION TABLE ************************
03_gct1.domain.com ----> gct1.domain.com
02_gct1.domain.com ----> gct1.domain.com
01_gct1.domain.com ----> gct1.domain.com
ok
```

親トピック: エンタープライズ・ロード・バランシング機能の使用
前のトピック: ロード・バランシング用に S-TAP を管理対象ユニットに関連付ける
次のトピック: エンタープライズ・ロード・バランシング・アクティビティー・レポートの表示

エンタープライズ・ロード・バランシング・アクティビティー・レポートの表示

ここでは、エンタープライズ・ロード・バランシングのイベントとアクティビティーのレポートを表示する方法について説明します。

このタスクについて

「エンタープライズ・ロード・バランサー・イベント」レポートには、S-TAP エージェントと管理対象ユニットとの間の正常な関連付け、管理対象ユニットの負荷の変化、失敗した関連付けなど、ロード・バランシングに関するすべてのイベントとアクティビティーが表示されます。

手順

このレポートを表示するには、「管理」 > 「レポート」 > 「アクティビティー・モニター」 > 「エンタープライズ・ロード・バランサー・イベント」にナビゲートします。

親トピック: エンタープライズ・ロード・バランシング機能の使用
前のトピック: エンタープライズ・ロード・バランシングのロード・マップの表示

エンタープライズ・ロード・バランシングの構成パラメーター

この参照情報では、ロード・バランサーの構成パラメーターについて詳しく説明します。CM では、「管理」 > 「一元管理」 > 「エンタープライズ・ロード・バランシング」 > 「エンタープライズ・ロード・バランシング・プロパティー」からアクセスします。MU では、「セットアップ」 > 「一元管理」 > 「登録およびロード・バランシング」からアクセスします。

パラメーター	デフォルト値 (有効な値)	記述
STATIC_LOAD_COLLECTION_INTERVAL	720 (≥10)	静的な管理対象ユニット・ロード収集間隔 (分)。 ENABLE_DYNAMIC_LOAD_COLLECTION を 0 に設定すると、ロード・バランサーは、STATIC_LOAD_COLLECTION_INTERVAL で指定された間隔で、すべての管理対象ユニットから負荷情報を収集します。
LOAD_BALANCER_ENABLED	1 (0 または 1)	ロード・バランサー機能を制御します。 • 0 を指定すると、ロード・バランサー機能が無効になります。 • 1 を指定すると、ロード・バランサー機能が有効になります。 特定の管理対象ユニット上でロード・バランサー機能を無効にすると、中央マネージャー上で稼働しているロード・バランサーは、その管理対象ユニットの負荷情報を収集しなくなります。また、その管理対象ユニットに接続されているすべての S-TAPs が、ロード・バランシングの対象から除外されます。 CM 上でこのパラメーターを無効にしてから有効にすると、ロード・バランシングが有効になっているすべての管理対象ユニットを対象とする完全なロード収集が即時にトリガーされます。
ENABLE_DYNAMIC_LOAD_COLLECTION	1 (0 または 1)	ロード収集方法を制御します。 • 0 を指定すると、動的なロード収集間隔が無効になります (収集間隔として STATIC_LOAD_COLLECTION_INTERVAL が使用されます)。 • 1 を指定すると、動的なロード収集間隔が有効になります。 このパラメーターを有効 (1 に設定) すると、収集間隔が管理対象ユニットの数に比例します (接続されている 10 台の管理対象ユニットにつき 1 時間)。このパラメーターを変更すると、次回の完全なロード収集時刻が即時に再計算がトリガーされます。
USE_APPLIANCE_HW_PROFILE_FACTOR	1 (0 または 1)	ロード・バランサーは、S-TAPs の再配置を行うための空き管理対象ユニットを評価する際に、管理対象ユニットのハードウェア・プロファイル・インディケーター (APPLIANCE_HW_PROFILE_INDICATORS パラメーターで指定) を使用することができます。 • 0 を指定すると、ハードウェア・プロファイル・インディケーターが無視されます。 • 1 を指定すると、管理対象ユニットのハードウェア・プロファイル・インディケーターが使用されます。
MAX_RELOCATIONS_BETWEEN_FULL_LOAD_COLLECTIONS	3 (≥-1)	完全なロード収集の後に許可される、管理対象ユニット間での S-TAP の再配置の最大回数を定義します。 負の値を指定すると、許可される再配置の回数が無制限になります。
ALLOW_POLICY_MISMATCH_BETWEEN_APPLIANCES	1 (0 または 1)	ロード・バランサーは、管理対象ユニットのインストール済みポリシーを考慮することができます。 • 0 を指定すると、ソースとターゲットの管理対象ユニット間でポリシーが一致していない場合は、S-TAP の再配置が禁止されます。 • 1 を指定すると、ソースとターゲットの管理対象ユニット間でポリシーが一致していない場合でも、S-TAPs の再配置が許可されます。 •
TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD	10 (≥5)	各管理対象ユニットの S-TAPs の負荷統計情報を収集する際に、その管理対象ユニットに対する初期の S-TAP の接続を表すデータを除外したい場合があります。このデータは、ロード・バランサーの誤検出を作成するトラフィック・スパイクを示している場合があります。 TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD パラメーターにより、S-TAP から管理対象ユニッ

		トへの接続後に、指定した時間 (分) だけ S-TAP の負荷をロード・バランサーが無視するように設定することができます。
ENABLE_RELOCATION	1 (0 または 1)	リソースの再配置 (再バランシング) は、完全なロード収集の後にロード・バランサーが実行するプロセスです。ここでの再配置とは、負荷の高い管理対象ユニットから空き管理対象ユニットに S-TAPs を転送するという意味です。 • `0` を指定すると、空き管理対象ユニットに対する S-TAPs の再配置が禁止されます。 • `1` を指定すると、空き管理対象ユニットに対する S-TAPs の再配置が許可されます。
LOADED_SNIFFER_QUEUE_USAGE_THRESHOLD	0.6 (0.1 から 1 の範囲で、0.1 単位で増加)	管理対象ユニットのスニファーにサイズが LOADED_SNIFFER_QUEUE_ USAGE_THRESHOLD に達するキューが少なくとも 1 つある場合、その管理対象ユニットは負荷が高いと見なされます。スニファーのキュー・サイズは、ADMINCONSOLE_PARAMETER_DEFAULT_QUEUE_SIZE パラメーターで定義します。 通常は、このパラメーターを変更することはありません。
DEFAULT_STAP_MAX_QUEUE_USAGE	0.15 (0.10 から 1 の範囲で、0.10 単位で増加)	S-TAP を初めて管理対象ユニットに割り当てた場合、ロード・バランサーはその管理対象ユニットに関する負荷情報を持っていません。このパラメーターの値により、スニファーで使用されるキューの一時的な最大値を定義します。この値は、管理対象ユニットから実際の負荷情報を収集するまでの間 (TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD パラメーターで定義された間隔が経過するまでの間) 使用されます。 通常は、このパラメーターを変更することはありません。
DEFAULT_STAP_MAX_CONTRIBUTION_TO_MAX_QUEUE_USAGE	0.1 (0.1 から 1 の範囲で、0.1 単位で増加)	S-TAP を初めて管理対象ユニットに割り当てた場合、ロード・バランサーはその管理対象ユニットに関する負荷情報を持っていません。このパラメーターの値により、キューの一時的な最大使用量に対する S-TAP の一時的な最大負荷の値を定義します。この値は、管理対象ユニットから実際の負荷情報を収集するまでの間 (TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD パラメーターで定義された間隔が経過するまでの間) 使用されます。 通常は、このパラメーターを変更することはありません。
REBALANCE_IF_MU_CLASSIFIED_AS_LOADED_N_TIMES_IN_M_HOURS	1:168 (≥0 : ≥0)	負荷の高い管理対象ユニットのリバランスを行うには、その管理対象ユニットについて、指定した時間内に指定したインスタンスの回数だけ負荷の高い管理対象ユニットとして分類する必要があります。例えば `1:168` という値の場合、`168` 時間以内に `1` 回以上、その管理対象ユニットを負荷の高い管理対象ユニットとして分類する必要がある、という意味になります。
APPLIANCE_HW_PROFILE_INDICATORS	NUM_PROCESSORS: CPU_SPEED: CPU_CACHE: CPU_CORES: MEMORY_SIZE (*APPLIANCE_RESOURCE_INFO* テーブルの列名)	ロード・バランサーは、管理対象ユニットのハードウェア・プロファイル・インディケーターを考慮することができます。ロード・バランサーは、コロンで区切られたインディケーター (*APPLIANCE_RESOURCE_INFO* テーブルの列名) のリストを使用して、ハードウェア・プロファイルを評価します。 通常は、このパラメーターを変更することはありません。
MAX_CONCURRENT_LOAD_COLLECTIONS	10 (≥1)	ロード・バランサーが任意の時点で実行する同時ロード収集プロセスの最大数。つまり、中央マネージャーから管理対象ユニットに対する、非永続的な同時リモート SQL 接続の数です。
MAX_RELOCATIONS_PER_MU_BETWEEN_FULL_LOAD_COLLECTIONS	3 (≥-1)	指定した管理対象ユニットで許可される S-TAP の再配置の最大回数。 負の値を指定すると、許可される再配置の回数が無制限になります。
ENABLE_FAILOVER_GROUPS_REBALANCE	0 (0 または 1)	メイン MU グループで MU が再び使用可能になった時点で S-TAP をフェイルオーバー・グループからメイン MU グループに戻すための自動再配置を制御します。 0 は、S-TAP をメイン MU グループに戻すための自動再配置を許可しません。 1 は、S-TAP をメイン MU グループに戻すための自動再配置を許可します。

親トピック: エンタープライズ・ロード・バランシング

Kerberos 認証データベース・トラフィック

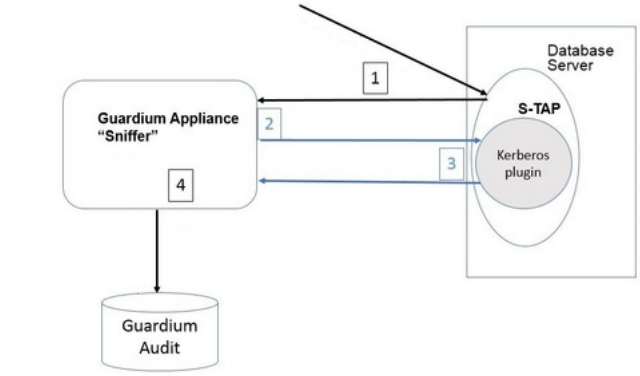
Kerberos は、ネットワーク上で暗号化されていないパスワードの伝送を排除するネットワーク認証プロトコルです。相互認証モードで機能し、認証を要求しているユーザーの ID と、要求された認証を提供するサーバーの両方を検証します。Kerberos 認証メカニズムでは、ネットワーク・サービスにアクセスするためのチケットが発行されます。 これらのチケットには、要求されたサービスに対するユーザーの ID を裏付ける暗号化されたデータ (暗号化されたパスワードなど) が含まれます。

監査およびアラートでは、アクションを実行したデータベース・ユーザーが誰かを把握することが重要です。Kerberos チケットを使用してログインする場合、データベース・ユーザーの判別は必ずしも簡単ではありません。

Guardium S-TAP はネットワーク・トラフィックのみを確認し、それを Guardium アプライアンス上のスニファーに渡します。Kerberos チケットがログインに使用されると、S-TAP はその Kerberos チケットをスニファーに渡します。一部のデータベース・サーバー・タイプでは、スニファーが Kerberos ログイン・トラフィックからデータベース・ユーザーを判別できるため、追加情報は必要ありません。その他のデータベース・サーバー・タイプでは、スニファーはいくらかサポートを必要とします。そのような機能は、S-TAP Kerberos プラグインによって実行されます。

S-TAP Kerberos プラグインはデフォルトでは使用可能になっていないため、追加の構成が必要です。

Kerberos を使用する以上は、プラグインを構成してください。プラグインを構成してもパフォーマンスへの影響やその他のマイナス面はないため、必要になったときのために構成しておいてください。



データベース、Guardium スニファー、および Guardium 監査データの間でのデータ・フローは以下のとおりです。

1. S-TAP が Kerberos 化されたデータベース・ログイン・パケットを (他のアクティビティーとともに) キャプチャーし、Guardium アプライアンスに送信します。
2. スニファーが Kerberos チケットからユーザー名を判別できる場合は、それを解析します。
3. スニファーが Kerberos チケットからユーザー名を判別できない場合は、データベース・ユーザーの要求とともに Kerberos チケットを S-TAP に送信します。S-TAP は、Kerberos プラグインが構成されているかどうかを確認します。Kerberos プラグインが構成されている場合、S-TAP はそのチケットをプラグインに与え、プラグインはチケットから DB_USER を割り出そうとします。プラグインは、データベース・ユーザー名を S-TAP に戻します。(戻されない場合、データベース・ユーザー名は提供されず、レポートにデータベース・ユーザー名が表示されません。)
4. スニファーはそのチケットのデータベース・ユーザーにユーザー名を取り込み、監査でそのユーザー名とそのユーザーの以降のデータベース・アクティビティーとを相互に関連付けられるようになりました。

- Kerberos 認証: サポートされるデータベース
  Kerberos 認証がサポートされているデータベース・サーバーと、それらに Kerberos プラグインが必要かどうかのリストを確認してください。
- Kerberos プラグインの使用可能化
- Kerberos プラグインの構成
  Kerberos 認証 (DB_USER の識別を含む) を使用するサーバー上のデータベース・トラフィックをモニターするには、guardtap.ini ファイルと guardkerbplugin.conf ファイルを適切に構成する必要があります。
- Oracle の Kerberos 構成パラメーターの検索
  Oracle Kerberos の場合、Kerberos キータブと構成ファイルの場所は sqlnet.ora で見つけます。
- Sybase の Kerberos 構成パラメーターの検索

親トピック: S-TAPs およびその他のエージェント

Kerberos 認証: サポートされるデータベース

Kerberos 認証がサポートされているデータベース・サーバーと、それらに Kerberos プラグインが必要かどうかのリストを確認してください。

データベース	Kerberos プラグインが必要か
Db2	いいえ
Oracle	はい
Cassandra	はい
Sybase ASE	はい
HBase	はい
MongoDB	いいえ
HDFS	いいえ
Big SQL	いいえ
Hive	はい
Impala	いいえ

親トピック: Kerberos 認証データベース・トラフィック

Kerberos プラグインの使用可能化

このタスクについて

プラグインを使用可能にするには、guard_tap.ini 構成ファイルを編集し、**kerberos_plugin_dir** 項目が、プラグイン自体 (libguardkerbplugin.so) および構成ファイル (guardkerbplugin.conf) が配置されているディレクトリーを指すように変更します。

手順

1. デフォルト・シェル・インストールの場合: `kerberos_plugin_dir=/usr/local/guardium/guard_stap`
2. デフォルト GIM インストールの場合: (正確なパスは、使用されているソフトウェア・リリースによって異なります)
   `kerberos_plugin_dir=/usr/local/IBM/modules/STAP/10.1.3_r101299_1-1495145548`
3. デフォルト (プラグインが使用不可の場合): `kerberos_plugin_dir=NULL`

親トピック: Kerberos 認証データベース・トラフィック

Kerberos プラグインの構成

Kerberos 認証 (DB_USER の識別を含む) を使用するサーバー上のデータベース・トラフィックをモニターするには、guardtap.ini ファイルと guardkerbplugin.conf ファイルを適切に構成する必要があります。

このタスクについて

Kerberos プラグインのすべてのカスタマイズ設定は guardkerbplugin.conf ファイル内にあります。 このファイルのデフォルトのコンテンツは以下のとおりです。

```
# Kerberos の値
KRB5RCACHETYPE=none
KRB5_KTNAME=/path/to/kerberos/krb5.keytab
KRB5_CONFIG=/path/to/kerberos/krb5.conf
# プラグインの値
KRB5_PLUGIN_CCACHE=/path/to/kerberos/krb5cc_*
KRB5_PLUGIN_GSSAPI_LIBRARY=/path/to/lib/libgssapi_krb5.so
#KRB5_PLUGIN_DEBUG=0
```

ブランク行と # で始まる行はコメントとして扱われ、無視されます。無効な項目があると、エラーが発生し、Kerberos プラグインを実行できなくなります。

構成項目を変更した場合、変更を有効にするために S-TAP を再始動する必要があります。

構成項目は以下のとおりです。

KRB5RCACHETYPE
: `KRB5RCACHETYPE=none`

KRB5_KTNAME
: これは、キータブ・ファイルへのパスです。これは、システムで既に使用されているキータブ・ファイル、またはプラグイン専用に Kerberos ユーティリティーで生成されたキータブ・ファイルのいずれでもかまいません。通常、このファイルの名前は krb5.keytab になります。以下に例を示します。
`KRB5_KTNAME=/home/oracle11/krb5/keytabKRB5_KTNAME=/home/sybase15/kerberos/keytab`

KRB5_CONFIG
: これは、システムで使用されている Kerberos 構成ファイルへのパスです。通常、このファイルの名前は krb5.conf になります。以下に例を示します。
`KRB5_CONFIG=/home/oracle11/krb5/krb5.conf KRB5_CONFIG=/home/sybase15/kerberos/krb5.conf`

KRB5_PLUGIN_CCACHE
: これは、Kerberos システム・キャッシュ・ファイルが配置されている場所へのワイルドカード・パスです。複数のパスは、セミコロン (;) で区切って指定できます。以下に例を示します。
`KRB5_PLUGIN_CCACHE=/tmp/krb5cc* KRB5_PLUGIN_CCACHE=/home/sybase16/krb5cc*;/tmp/krb5cc*`
注: 必要以上に多くのファイルを指定する (例えば、/tmp/* を指定する) と、パフォーマンスが影響を受けます。

KRB5_PLUGIN_GSSAPI_LIBRARY
: これは、Kerberos GSSAPI 動的ライブラリーの場所です。ほとんどのシステムでは、この名前は libgssapi_krb5.so になります。

  場所は、絶対パスで指定できます。以下に例を示します。

  `KRB5_PLUGIN_GSSAPI_LIBRARY=/usr/lib64/libgssapi_krb5.so KRB5_PLUGIN_GSSAPI_LIBRARY=/opt/freeware/lib64/libgssapi_krb5.so`

  あるいは、ライブラリーがシステムの標準ライブラリー検索パスに配置されている場合、指定する必要があるのはファイル名のみです。以下に例を示します。

  `KRB5_PLUGIN_GSSAPI_LIBRARY=libgssapi_krb5.so`
  注: GSSAPI ライブラリー (通常、libkrb5.so、libk5crypto.so、libkrbsupport.so) で必要なライブラリーもすべて、システム上に配置されている必要があります。

KRB5_PLUGIN_DEBUG
: このパラメーターは、プラグインのデバッグのみに使用されます。通常運用時には、この行をコメント化する必要があります。そうしないと、プラグイン・パフォーマンスが影響を受けます。

手順

1. guard_tap.ini ファイルで、kerberos_plugin_dir パラメーターの値を Guardium S-TAP への絶対パスに変更します。プラグインはここに配置されているためです。
   - GIM インストール済み環境: kerberos_plugin_dir=<guardium_base>/modules/STAP/current
   - S-TAP シェル・インストール済み環境: kerberos_plugin_dir=<guardium_base>/guard_stap
2. S-TAP インストール・ディレクトリーにもある guardkerbplugin.conf ファイルで、以下を構成します。
   - KRB5_KTNAME=<kerberos krb5.keytab ファイルへの絶対パス>
   - KRB5_CONFIG=<kerberos krb5.conf ファイルへの絶対パス>
   - チケット・キャッシュ用の任意指定の構成パラメーター。Kerberos プラグインがユーザーを認識しない場合、このパラメーターが必要になる場合があります。通常は複数のキャッシュ・ファイルがあるため、このパラメーターにはワイルドカードを使用できます。複数のパスをコロンで区切って指定できます。
     KRB5_PLUGIN_CCACHE=<kerberos krb5cc_* ファイルへの絶対パス:kerberos krb5cc_* ファイルへの追加の絶対パス:以降同様>

   注: V.10.1.2 より前の Guardium リリースでは、パラメーター allow_weak_crypto = 1 および clockskew = 600 が必要でした。これらのパラメーターは、ほとんどの場合において不要になりました。

親トピック: Kerberos 認証データベース・トラフィック

Oracle の Kerberos 構成パラメーターの検索

Oracle Kerberos の場合、Kerberos キータブと構成ファイルの場所は sqlnet.ora で見つけます。

このタスクについて

手順

1. ~]$ grep –i KERBEROS $ORACLE_HOME/network/admin/sqlnet.ora と入力します。
   次のような出力が表示されます。

```
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
SQLNET.KERBEROS5_CONF = /home/oracle11/krb5/krb5.conf
SQLNET.KERBEROS5_REALMS = /home/oracle11/krb5/krb.realms
SQLNET.AUTHENTICATION_SERVICES= (BEQ,KERBEROS5)
SQLNET.KERBEROS5_CLOCKSKEW = 600
SQLNET.KERBEROS5_KEYTAB = /home/oracle11/krb5/keytab
SQLNET.KERBEROS5_CONF_MIT = TRUE
```

2. Kerberos キャッシュ・パラメーターを見つけるには、~]$ oklist|grep -i cache と入力します。

   次のような出力が表示されます。

```
Ticket cache: /tmp/krb5cc_500
```

親トピック: Kerberos 認証データベース・トラフィック

Sybase の Kerberos 構成パラメーターの検索

手順

1. klist -k と入力します。
   次のような出力が表示されます。

```
env|grep -i KRB
KRB5_KTNAME=/home/sybase15/kerberos/keytab
KRB5_CONFIG=/home/sybase15/kerberos/krb5.conf
```

2. Kerberos キャッシュ・パラメーターを見つけるには、klist -c と入力します。

   次のような出力が表示されます。

```
Ticket cache: FILE:/tmp/krb5cc_533
```

親トピック: Kerberos 認証データベース・トラフィック

出口ライブラリーの使用

出口ライブラリーは、出口メカニズムを使用して Guardium ライブラリーをデータベースに組み込みます。出口ライブラリー、つまり出口モジュールは、Guardium S-TAP と直接通信してデータベース・トラフィックを転送します。

- Db2 Exit と S-TAP の統合
  Db2 出口メカニズムを使用すると、Guardium は、トラフィックが暗号化されているかどうか、およびローカルかリモートかに関係なく、すべての Db2 トラフィックを取得できます。A-TAP も K-TAP も必要としません。
- Informix 出口と UNIX S-TAP の統合
  Informix 出口の ifxguard ユーティリティー (Informix 12.10 以上) は、Informix データベースへの接続をモニターします。
- Teradata 出口の UNIX S-TAP との 統合
  Teradata 出口モジュールを使用すると、暗号化されているかいないか、およびローカルかリモートかに関係なく、Guardium が Teradata トラフィックを取得できるようになります。A-TAP も K-TAP も必要としません。

親トピック: S-TAPs およびその他のエージェント

Db2 Exit と S-TAP の統合

Db2 出口メカニズムを使用すると、Guardium は、トラフィックが暗号化されているかどうか、およびローカルかリモートかに関係なく、すべての Db2 トラフィックを取得できます。A-TAP も K-TAP も必要としません。

このタスクについて

Db2 出口は、DB2_Exit メカニズムを介して Guardium ライブラリーを Db2 に組み込みます。DB2_Exit は直接 Guardium S-TAP と通信し、トラフィックが暗号化されているかどうかに関係なく、ローカルとリモートの両方の Db2 トラフィックをすべて転送します。Db2 出口は TCP トラフィックと SHM トラフィックをキャプチャーします。Db2 とともに UID チェーンを有効にした場合に消費される CPU リソースは、KTAP および UID チェーンよりも大幅に少なくなります。

Db2 出口ライブラリーは、動的リンク・ライブラリーです。Db2 データベースは、データベースの始動中にロードされます。

Db2 出口は、ファイアウォール (STAP 10.1.2 以降は、Db2 バージョン 10.1 以降も必要)、強制終了、および IUD チェーンをサポートします。

KTAP を必要とする S-TAP の他の検査エンジン (IE) がない場合、KTAP をロードする必要はありません。guard_tap.ini で ktap_installed=0 を設定するか、その STAP の GIM ダイアログで GIM を使用して ktap_enabled を no に設定します。Linux OS と STAP のアップグレードは、KTAP モジュールの互換性を気にすることなく実行できます。ただし、KTAP モジュールを必要とする S-TAP の他の IE がある場合は、Linux バージョンのアップグレード時に互換性のある KTAP モジュールが確実に使用可能になっているようにしてください。

S-TAP デバッグ・レベル: S-TAP のログ・レベルが 10 の場合、STAP のログと db2diag.log の両方にデバッグ情報が記録されます。ログ・レベルが 11 の場合、デバッグ情報は db2diag.log にのみ記録されます。Db2 出口モジュールはロギングを実行します。このモジュールは Db2 によってロードされ、ログ・ファイルに diag がパイピングされます。データベース・サーバーは技術的にロギングを実行するサーバーであるため、ロギングの範囲に応じて何らかの影響があります。STAP ロギングはトラブルシューティングのために使用するように意図されているため、常時実行しないようにしてください。

制限事項:

- DB2-Exit は Guardium データ・マスキング (修正/編集) をサポートしません。
- Guardium ファイアウォール (V10.1.2 以降) には Db2 バージョン 10.1 以降が必要です。
- ストアード・プロシージャー: DB2-Exit はストアード・プロシージャーをモニターします。Guardium はストアード・プロシージャーに何が含まれているかを認識しないため、プロシージャー内からの SQL はキャプチャーされません。

STAP および Db2 をアップグレードする場合

1. Db2 を停止します。
2. STAP をアップグレードします。
3. 最新の db2 exit lib を Db2 commexit ディレクトリーにコピーします。
4. Db2 を開始します。

STAP にパッチを適用する場合

1. Db2 を停止します。
2. Db2 データベースにパッチを適用します。
3. Db2 構成が上書きされた場合は、`db2 UPDATE DBM CFG USING COMM_EXIT_LIST libguard_db2_exit_64` を使用して再度有効にする必要があります。
4. Db2 を開始します。

Guardium インストーラーには、32 ビットと 64 ビットの 2 つのバージョンの Db2 出口ライブラリーがあります。インストールされている Db2 に一致したバージョンを使用してください。どちらのバージョンも、lib サブディレクトリーの Guardium インストール・ディレクトリーにあります。Linux サーバー上では、64 ビット・バージョンは lib64 にあります。

Db2 の V101FP4 バージョンと V105FP3 バージョンは UID チェーンをサポートします。

ライブラリー名

- libguard_db2_exit_32.so
- libguard_db2_exit_64.so

手順

1. Db2 のビット単位を判別します。`root` としてログインし、`db2level` を実行します。出力は、以下のようになります。
   `DB21085I インスタンス db2inst1 は、64 ビットおよび Db2 コード・リリース SQL09070 をレベル ID 08010107 で使用します (DB21085I Instance db2inst1 uses 64 bits and DB2 code release SQL09070, with level identifier 08010107)`
2. 通信バッファー出口ライブラリーの場所 (DB2PATH) を確認します。
   a. Db2 ユーザー `trip` としてログインします
   b. Db2 clp で、db2 `get database manager configuration` を実行します。
   c. 出力で、デフォルトのデータベース・パスを見つけます。デフォルトのデータベース・パス:
   `(DFTDBPATH) = /DB2/trip`
   DFTDBPATH は、環境パラメーター DB2PATH に必要な値です。
3. Db2 出口ライブラリーをセットアップします。
   a. ユーザー `root` としてログインします
   b. 次のように環境パラメーターを設定します。`# export DB2PATH=/DB2/trip`
   c. 以下のいずれかのコマンドを入力してディレクトリーを作成します。(これはライブラリーを最初にインストールした時にのみ実行します (ディレクトリーが存在しないため))
      - mkdir $DB2_PATH/sqllib/security/plugin/commexit
      - mkdir $DB2_PATH/sqllib/security64/plugin/commexit
   d. 次のようにアクセス権を変更します。`# chown ${DB2 user}:${DB2 group} $DB2PATH/security64/plugin/commexit`
   e. 以下のいずれかのコマンドを入力して Guardium の libguard ファイルを commexit にコピーします。
   ```
   # cp /opt/IBM/guardium/module/modules/STAP/libguard_db2_exit_64.so $DB2PATH/security64/plugin/commexit
   # cp /opt/IBM/guardium/module/modules/STAP/libguard_db2_exit_64.so $DB2PATH/security/plugin/commexit
   ```
   ここで、$DB2_PATH は、db2 のインストール・ディレクトリーです。

   コピーがエラー「`....: テキスト・ファイルはビジー状態です (Text file busy)`」で失敗する場合は、ターゲット・ディレクトリーからファイルを削除し、コピーを行い、繰り返します。

   f. 以下のいずれかのコマンドを入力してアクセス権を変更します。
   ```
   # chown ${DB2 user}:${DB2 group} $DB2PATH/security64/plugin/commexit/libguard_db2_exit_64.so
   # chown ${DB2 user}:${DB2 group} $DB2PATH/security/plugin/commexit/libguard_db2_exit_64.so
   ```
4. Db2 インスタンスを Guardium グループに追加します。 Guardium グループは、S-TAP のインストール中に作成されます。 この要件により、S-TAP によって作成される共有メモリー領域のセキュリティーが強化されます。
   a. Db2 ユーザーが「trip」の場合、「trip」が既に許可されているかどうか確認します。ATAP フォルダーの下の guardctl を使用します。 `# /opt/IBM/guardium/module/modules/ATAP/10.1.0_r88469_1-1468880597/files/bin/guardctl is-user-authorized trip`
   ユーザー「`trip`」は許可されています。`(User 'trip' is authorized.)`
   b. ユーザー trip が許可されていない場合、次のように、ここで許可します。
   ```
   # /opt/IBM/guardium/module/modules/STAP/10.1.0_r88469_1-1468880597/guardctl authorize-user trip
   guardctl authorize-user guardium
   ```
   ユーザー「`guardium`」は既に許可されています。`(User 'guardium' is already authorized.)`
5. Db2 で db2 出口を有効にします (これにより、SQL トラフィックを S-TAP に送信するようにします)。
   a. db2 ユーザーとしてログインし、次のように db2 clp コマンドを使用して有効にします。
   ```
   db2 UPDATE DBM CFG USING COMM_EXIT_LIST libguard_db2_exit_64
   ```
   b. 有効になると、db2 は SQL トラフィックを STAP に送信します。以下のコマンドを入力して、db2 出口が正常に有効化されたかどうかを確認します。
   ```
   db2 get database manager configuration
   ```
   出力には以下が含まれます。
   通信バッファー出口ライブラリー・リスト `(Communication buffer exit library list) (COMM_EXIT_LIST) = libguard_db2_exit_64`
6. Db2 を再始動します。

a. db2 ユーザーとしてログインし、データベース・サーバーをバウンスします。
```
# db2stop force; ipclean; db2start
```
b. 応答に以下が含まれていることを確認します。
「DB2START コマンドが正常に完了しました」
c. 再始動が失敗した場合、以下のコマンドを入力して、db2 出口を停止して Db2 の警告をクリアします。
```
db2 UPDATE DBM CFG USING COMM_EXIT_LIST NULL
```
次に、以下のコマンドを入力して再始動します。
```
db2 restart
```
d. 再始動しなかった場合、次のログ・ファイルを調べて手掛かりを探してください。~/sqllib/db2dump/db2diag.log

7. A-TAP がアクティブになっていない場合、DB2_EXIT に対して STAP を構成します。(A-TAP がアクティブになっている場合は、8 に進んでください)
a. 通常通り guard_tap.ini または GIM で Db2 に対して IE を構成します。識別を容易にするために、db_type=db2 を設定してください。
b. UNIX タイプのプラットフォームのみ: DB2_EXIT IE のパラメーター db_install_dir が Db2 環境変数の $DB2_HOME または $HOME の値に設定されていることを確認します。
c. Windows のみ: instance_name=Service_name を追加します。S-TAP インストール・フォルダーの db2tap ユーティリティー、または制御パネルを使用して、サービス名を判別します。2 番目のダッシュ (-) 区切り文字の後ろに続くサービス名の部分をインスタンス名に設定します。例えば、コントロール・パネルでサービス名が「DB2 - DB2COPY1 - DB2-01-0」の場合、INSTANCE_NAME を DB2-01-0 に設定します。
d. 新規構成で STAP を再始動します。
8. 始動時に A-TAP がアクティブになっていた場合
a. 以下のコマンドを入力して Db2 を停止します。
```
# db2stop force;ipclean
```
b. 以下のコマンドを入力して ATAP を非アクティブにします。
```
# /opt/IBM/guardium/module/modules/ATAP/10.1.0_r88469_1-1468880597/files/bin/guardctl db_instance=<db_instance> [--
force-action=yes ] deactivate
```
c. 通常通り guard_tap.ini または GIM で Db2 に対して IE を構成します。識別を容易にするために、db_type=db2 を設定してください。
d. UNIX タイプのプラットフォームのみ: DB2_EXIT IE のパラメーター db_install_dir が Db2 環境変数の $DB2_HOME または $HOME の値に設定されていることを確認します。
e. Windows のみ: instance_name=Service_name を追加します。S-TAP インストール・フォルダーの db2tap ユーティリティー、または制御パネルを使用して、サービス名を判別します。2 番目のダッシュ (-) 区切り文字の後ろに続くサービス名の部分をインスタンス名に設定します。例えば、コントロール・パネルでサービス名が「DB2 - DB2COPY1 - DB2-01-0」の場合、INSTANCE_NAME を DB2-01-0 に設定します。
f. 新規構成で STAP を再始動します。
9. ゾーン/WPAR をセットアップします。
a. S-TAP を zones/wpars にコピーします。
i. マスター/グローバル・ゾーン/WPAR 上で (Guardium ソフトウェアが /usr/local/guardium の下のマスター・ゾーン/WPAR にインストールされており、サブゾーン/サブ WPAR 上に十分な空き領域がある書き込み可能ディレクトリー /usr/local が存在することが前提)、以下のコマンドを入力します。
```
cd /usr/local
tar -cvf - guardium | ssh root@subzonehost 'cd /usr/local && tar -xvf -'
```
ii. ゾーン/WPAR 上で、以下を指定して guard_tap.ini に DB2_EXIT IE を追加します。
- -- ktap_installed = 0
- -- tap_run_as_root = 1
- -- tap_ip = ゾーン/WPAR のローカル IP アドレス
- ゾーンで S-TAP を開始するために、他の IE を指定しないでください。

b. /var/guard ディレクトリーを作成します。
c. S-TAP を開始します。
- WPAR では、inittab ファイル内の utap サーバー項目を手動でコピー/追加します。
- Solaris ゾーンでは、次のリンクの情報に従ってください。https://scm.guard.swg.usma.ibm.com/wiki/index.php?page=Use_Solaris_services

d. 初期セットアップの説明に従ってください。
e. ログ・レベルを選択します。
注: **データベース・サーバーでのデバッグ・ロギングの影響:** ロギングは Db2 出口モジュールによって実行されます。このモジュールは Db2 によってロードされ、ログ・ファイルに diag がパイピングされます。データベース・サーバーは技術的にロギングを実行するサーバーであるため、実行されるロギングの量に応じて何らかの影響があります。STAP ロギングはトラブルシューティングの一環として使用するように意図されており、標準機能ではないため、影響があるのはロギングがオンのときのみであることに注意してください。
- S-TAP のログ・レベルが 10 の場合、S-TAP のログと db2_exit ログ (db2diag.log) の両方にデバッグ情報が記録されます。
- S-TAP のログ・レベルが 11 の場合、db2_exit ログ (db2diag.log) のみにデバッグ情報が記録されます。

注: WPAR 環境で、ディスカバリーの実行時にインスタンス名がスレーブ・ゾーンとマスター・ゾーンで同じである場合は、マスター・ゾーンに属する 1 つの検査エンジン項目のみが追加されます。
注: 検査エンジンで tap_identifier を変更する場合、変更を Informix 出口または Db2 出口で有効にするには、データベースを再始動する必要があります。 ATAP が有効になっている状態では、データベースを停止し、ATAP を非アクティブ化し、再アクティブ化し、そして最後にデータベースを再始動する必要があります。 Db2 出口および Informix 出口に対して tap_identifier が機能するようにするには、db_install_dir がデータベースの $HOME 値と完全に同じであることを確認してください。また、データベースを再始動して tap_identifier 値を取得する必要があります。Informix 出口の場合は、ifxguard を停止してからデータベースを再始動し、その後 ifxguard を開始します。

親トピック: 出口ライブラリーの使用

Informix 出口と UNIX S-TAP の統合

Informix 出口の ifxguard ユーティリティー (Informix 12.10 以上) は、Informix データベースへの接続をモニターします。

このタスクについて

Informix 出口を使用すると、Guardium v.10 以上は Informix SQL アクティビティーのすべてのプロトコルを監査できます。 これには、TCP プロトコル、共有メモリー・プロトコル、および名前付きパイプ・プロトコルが含まれます。それは、Guardium のすべての機能 (S-gate、UID チェーン、編集、照会再書き込みなど) をサポートします。Linux プラットフォームでは、ATAP の代わりに Informix 出口を使用して、共有メモリー・トラフィックをキャプチャーできます。Informix 出口は、暗号化トラフィックをキャプチャーします。

ifxguard ユーティリティーは $INFORMIXDIR/bin の下にあります。共有ライブラリー、Informix 出口は、Guardium Unix S-TAP インストールの一部です。それは、ifxguard によって実行時にロードされます。S-TAP には、32 ビットと 64 ビットの .so が含まれます。静的ライブラリーも含まれます。それらは、<guardium_installation_directory>/guard_stap の下にあります。以下に例を示します。
/usr/local/guardium/guard_stap /usr/local/guardium/guard_stap/libguard_informix_exit_32.so
/usr/local/guardium/guard_stap/libguard_informix_exit_64.so.

注: 検査エンジンで tap_identifier を変更する場合、変更を Informix 出口または Db2 出口で有効にするには、データベースを再始動する必要があります。ATAP が有効になっている状態では、データベースを停止し、ATAP を非アクティブ化し、再アクティブ化し、そして最後にデータベースを再始動する必要があります。Db2 出口および Informix 出口に対して tap_identifier が機能するようにするには、db_install_dir がデータベースの $HOME 値と完全に同じであることを確認してください。また、データベースを再始動して tap_identifier 値を取得する必要があります。Informix 出口の場合は、ifxguard を停止してからデータベースを再始動し、その後 ifxguard を開始します。

手順

1. データベースにユーザー informix としてログインし、以下の UNIX コマンドを実行して、それのインスタンス名 (INFORMIXSERVER) とそれのインストール・ディレクトリー (INFORMIXDIR) を探します。
```
$ echo $INFORMIXSERVER
INFORMIXSERVER=test117
$ echo $INFORMIXDIR
INFORMIXDIR=/home/informix
```
2. データベース・ホストに S-TAP をインストールし、始動します。S-TAP クライアントの Linux サーバー、Solaris サーバー、AIX サーバー、HP-UX サーバーへのインストールを参照してください。
3. ユーザー root として、ユーザー informix が guardium グループに属していることを確認します。以下に例を示します。
```
/usr/local/guardium/bin/guardctl authorize-user informix
```
または、UNIX の場合
```
# chgroup users=informix guardium
```
(AIX のみ)
4. ユーザー informix としてログインし、以下を入力します。
```
$ iduid=501(informix) gid=205(informix) groups=215(guardium)
```
5. ユーザー informix として、適切な Informix 出口ライブラリーを guard_stap ディレクトリーから informix ユーザーの lib ディレクトリーにコピーします。以下に例を示します。
```
cp /usr/local/guardium/guard_stap/libguard_informix_exit_64.so
$INFORMIXDIR/lib/libguard_informix.so
```
6. ifxguard をセットアップします。以下の行を使用して、$INFORMIXDIR/etc/ifxguard.$INFORMIXSERVER の下に構成ファイルを作成します。
```
NAME ol_informix1210
WORKERS 2
LIBPATH /home/informix/12.10.FC6/lib/libguard_informix.so
DEBUG 1
LOGFILE /home/informix/12.10.FC6/etc/ifxguard.msg.txtg.txt
```
注: INFORMIXDIR=/home/informix/12.10.FC6
7. ユーザー informix として ifxguard を起動します。
   a. Informix データベース・サーバーがオンラインであることを確認します (onstat -)。
   ```
   $ id
   uid=501(informix) gid=205(informix) groups=215(guardium) $ onstat -
   IBM Informix Dynamic Server Version 12.10.FC6 -- On-Line -- Up 6 days 00:22:25 -- 253104 Kbytes
   ```
   b. ifxguard 構成ファイルが上述のとおりにセットアップされている場合は、以下を使用して ifxguard を起動します。
   ```
   $ ifxguard
   15:20:17 ifxguard set instance name ol_informix1210
   Starting ifxguard ol_informix1210 ...
   check log file: /home/informix/12.10.FC6/etc/ifxguard.msg.txt
   ```
   エラーは表示されないはずです。エラーがある場合は、LOGFILE に示されているファイルを確認します。
   c. ifxguard 構成ファイルが $INFORMIXDIR/ の下にない場合は、-c オプションを使用してファイルの絶対パスを指定します。以下に例を示します。
   ```
   $ ifxguard -c /mnt/conf/ifxguard.ol_informix1210
   ```
   d. ifxguard 構成ファイルがまったくセットアップされていない場合、引き続きエージェントを起動できますが、-p オプションを含む絶対パスと -l オプションを含むメッセージ・ログ・ファイルを使用して、.so ライブラリーを指定する必要があります。以下に例を示します。
   ```
   $ ifxguard -p /home/informix/12.10.FC6/lib/libguard_informix.so -l  home/informix/12.10.FC6/etc/ifxguard.msg.txt
   ```
   e. エラーがある場合は、LOGFILE に示されているログ・ファイルを確認します。
8. ps -ef を使用して、ifxguard と S-TAP が実行されていることを確認します。
```
$ ps -ef|grep guard
root 15401210 1 1 15:14:11 - 0:00
/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
informix 22609968 1 0 15:20:17 - 0:00 ifxguard
```

以下のメッセージが /home/informix/12.10.FC6/etc/ifxguard.msg.txt に表示されます。

```
Wed Feb  3 15:20:17 2016
15:20:17 INFORMIX-ESQL Version 12.10.FC6
15:20:17 Build Number:  N253
15:20:17 Build Host:    cxp01007
15:20:17 Build OS:      AIX 6.1
15:20:17 Build Date:    Wed Nov 4 21:55:13 CST 2015
15:20:17 GLS Version:   glslib-6.00.FC7
15:20:17
15:20:17 Starting ifxguard ol_informix1210 ...
15:20:17 DEBUG[TID1]:Password File /home/informix/12.10.FC6/etc/ passwd_file failed error:No
such file or directory [2] [onguard_main.c:onguard_pw_init:518]
15:20:17 DEBUG[TID1]:ifxguard ol_informix1210 connect to trusted host, Password Manager is i
gnored. [onguard_main.c:onguard_run:2391]
```

```
15:20:17 pcbms = 110023688, spt_fn=fffffffffff300

15:20:17 CBMS: cbms_initialize()
15:20:17 Attached /.guard_writer0 shmem[0] 8001000a0000de8
15:20:17 Attached /.guard_writer1 shmem[1] 8001000a0000eb8
15:20:17 Attached /.guard_writer2 shmem[2] 8001000a0000f88
15:20:17 Attached /.guard_writer3 shmem[3] 8001000a0001058
15:20:17 Attached /.guard_writer4 shmem[4] 8001000a0001128
15:20:17 Attached /.guard_writer5 shmem[5] 8001000a00011f8
15:20:17 Attached /.guard_writer6 shmem[6] 8001000a00012c8
15:20:17 Attached /.guard_writer7 shmem[7] 8001000a0001398
15:20:17 Attached /.guard_writer8 shmem[8] 8001000a0001468
15:20:17 Attached /.guard_writer9 shmem[9] 8001000a0001538
15:20:17 Attached to /.guard_reader
15:20:17 guard_conf_message=70000000149b000: my_ip=96eb8b7, intercept_type=1c, debug_level=0
, ignore_response_db_list=NONE
15:20:17 comm exit shm initialization successful
15:20:17 DEBUG[TID1]:new daemon pid is 22609968 [onguard_main.c:onguard_daemonize:2350]
15:20:17 ifxguard ol_informix1210 started
15:20:17 The connection attempt from  ifxguard ol_informix1210 to server ol_informix1210 suc
ceeded. Process id: 22609968:258
15:20:17 Attached to /.guard_reader
15:20:17 The connection attempt from  ifxguard ol_informix1210 to server ol_informix1210 succeeded. Process id: 22609968:515
```

パスワード・ファイル・エラーは無視してかまいません。それはデバッグ・メッセージです。パスワード・ファイルを 1 つ定義し、「onpassword」を実行してそれを暗号化できます。Ifxguard は、暗号化ファイルからユーザー informix のパスワードを読み取り、Informix Dynamic Server (IDS) に接続します。パスワード・ファイルが定義されていない場合、ifxguard は信頼できるホスト接続として IDS に接続します (パスワードなし)。

9. GRDAPI (create_stap_inspection_engine) を介して、または GUI (「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」) で、以下の特定の Informix 値を指定して INFX_EXIT 検査エンジンを追加します。

GUI でのパラメーター	**GRDAPI でのパラメーター**	**値**
プロトコル	protocol	Informix 出口
データベース・インストール・ディレクトリー	dbInstallDir	/home/informix
プロセス名	procName	/INFORMIXTMP/.inf.sqlexec
インターセプト・タイプ	interceptTypes	<ブランクまたは null>
ID	ieIdentifier	<ブランクまたは null>
	informixVersion	Informix のバージョン

10. S-TAP を再始動します。
11.
12. libguard を無効にするには、ifxguard -kill $INFORMIXSERVER を実行します。

親トピック: 出口ライブラリーの使用

Teradata 出口の UNIX S-TAP との 統合

Teradata 出口モジュールを使用すると、暗号化されているかいないか、およびローカルかリモートかに関係なく、Guardium が Teradata トラフィックを取得できるようになります。A-TAP も K-TAP も必要としません。

このタスクについて

Teradata 16.10 以上での S-TAP には、この構成が必要です。

Teradata 出口は、出口モジュールを介して DB2 に Guardium ライブラリーを組み込みます。出口モジュールは Guardium S-TAP と直接通信して、すべての Teradata トラフィックを転送します。

Teradata 出口は、終端とファイアウォールをサポートします。UID チェーンと編集はサポートしません。

libguard_teradata_exit_64.so およびその他の Guardium ファイルのロケーションは、インストール方式や選択したディレクトリーによって異なります。

手順

1. 以下のように、ローカルの local guard_tap.ini に Teradata 出口検査エンジンを構成します。

```
[DB_0]
connect_to_ip=127.0.0.1
db_exec_file=/opt/teradata/tdat/tgtw/16.00.00.05sks/bin/gtwgateway
db_install_dir=/root
db_type=trd_exit
intercept_types=NULL
tap_identifier=NULL
networks=0.0.0.0/0.0.0.0
exclude_networks=
```

2. ローカルで編集する場合は、S-TAP を再始動します。
3. root として、以下を入力します。

```
ln -s /usr/local/guardium/lib64/libguard_teradata_exit_64.so /opt/teradata/tdat/tgtw/site/libtgtwmonitoring.so
/usr/local/guardium/guard_stap/guardctl --db-user=tdatuser authorize-user
/usr/local/guardium/guard_stap/guardctl --db-user=teradata authorize-user
/usr/local/guardium/guard_stap/guardctl --db-user=root authorize-user
/usr/tgtw/bin/gtwcontrol --monitorlib load=yes
```

4.

親トピック: 出口ライブラリーの使用

特別な環境での構成 (Linux、Solaris、HP-UX、AIX)

ゾーン、RAC、WPAR、クラスターがあるシステムでは、以下の該当する手順を使用してください。

- Solaris ゾーンの S-TAP 構成
  S-TAP をマスター・ゾーン (グローバル・ゾーン) にインストールして構成します。他のすべてのゾーン (ローカル・ゾーン) は、マスター・ゾーンとリソースを共有します。
- Oracle RAC の S-TAP 構成
- S-TAP for DB2 WPAR の構成
- Db2 クラスターのすべてのノードでの A-TAP のアクティブ化
  A-TAP は、Db2 サーバーが Db2 クラスターのノードによって共有されているすべてのノードでアクティブにする必要があります。
- 遅延クラスター・ディスク・マウントの構成
  このトピックは、Oracle、Informix®、および DB2® の各データベース・サーバーにのみ適用されます。

親トピック: S-TAPs およびその他のエージェント

Solaris ゾーンの S-TAP 構成

S-TAP をマスター・ゾーン (グローバル・ゾーン) にインストールして構成します。他のすべてのゾーン (ローカル・ゾーン) は、マスター・ゾーンとリソースを共有します。

このタスクについて

手順

1. ローカル・ゾーンはマスター・ゾーンの情報を共有するため、データベースが実行されているゾーンに関係なく、S-TAP をマスター・ゾーン (グローバル・ゾーン) にインストールします。
2. 検査エンジンを構成するとき、db_install_dir パスと tap_db_process_names にグローバル・ゾーン値を使用します。(S-TAP はグローバル・ゾーンからすべてのゾーン内のデータベースへのアクセスをモニターします。)
3. PCAP を使用している場合、モニターするすべてのゾーンの IP アドレスを、Solaris データベースの guard_tap.ini ファイル内の alternate_ips パラメーターに追加します。
4. インストールの終了時には、以下のようになります。
   - K-TAP は、グローバル・ゾーンにのみロードされるため、ローカル・ゾーンにはロードされません。それはローカル・ゾーンで表示できます。
   - S-TAP はローカル・ゾーンでは実行されません。

親トピック: 特別な環境での構成 (Linux、Solaris、HP-UX、AIX)

Oracle RAC の S-TAP 構成

このタスクについて

Oracle RAC (Real Application: Clusters) を使用すると、複数のコンピューターが単一のデータベースにアクセスする一方で、Oracle RDBMS ソフトウェアを同時に実行でき、クラスタリングが行われます。

RAC 以外の Oracle データベースでは、単一データベースにアクセスするのは単一インスタンスです。データベースは、ディスク上に保管されたデータ・ファイル、制御ファイル、および再実行ログの集合で構成されます。インスタンスは、Oracle 関連メモリーと、コンピューター・システムで実行されるオペレーティング・システム・プロセスとの集合で構成されます。

Oracle RAC 環境では、2 つ以上のコンピューター (それぞれに Oracle RDBMS インスタンスが含まれています) が単一データベースに同時にアクセスします。これにより、アプリケーションまたはユーザーはいずれかのコンピューターに接続し、調整された単一のデータ・セットにアクセスできます。

手順

1. すべてのノードに S-TAP をインストールします。GIM が使用されている場合は、すべてのノードに GIM クライアントをインストールしてから、すべてのノードにバンドル S-TAP をインストールします。
2. STAP パラメーターを構成します。すべてのパラメーターは、GIM UI を使用して構成できます。
   - STAP_TAP_IP: ノード用に構成されたパブリック IP
   - STAP_ALTERNATE_IPS: ノード用に構成された VIP (仮想 IP) のコンマ区切りリストと、スキャン・リスナー
     ヒント: alternate_ips に入れる仮想ホスト名の値を取得するには、コマンド su – grid –c 'cat $ORACLE_HOME/network/admin/*.ora'|grep –i host を使用してください。

     例:

     ```
     [root@racvm121 ~]# su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora'|grep -i host
     LISTENER_RACVM121=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=racvm121-vip.guard.swg.usma.ibm.com)(PORT=1521)
     ```

   - STAP 検査エンジン・パラメーター unix_domain_socket_marker=<key> を構成します。<key> 値は、IPC プロトコル定義内の listener.ora にあります。
     ヒント: unix_domain_socket の値を取得するコマンドは、`su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora'|grep -i KEY` です。
     - 例: listener.ora にある記述が LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=ORCL)))) である場合、unix_domain_socket_marker=ORCL です。
     - 例: listener.ora 内に複数の IPC 行がある場合、すべてのキーの共通項を使用します。

```
su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora'|grep -i KEY
LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER))))
LISTENER_SCAN1=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN1))))
LISTENER_SCAN2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN2))))
LISTENER_SCAN3=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN3))))
```

Guardium はパスで文字列検索を使用します。「LISTENER」は上記の 4 つすべてで機能します。この場合は、unix_domain_socket_marker=LISTENER を使用してください

- 例: 共通項がない場合は、特定の IPC キーに対応する unix_domain_socket_marker を使用して追加の検査エンジンを作成します。例えば、guard_tap.ini は、末尾でこの例に似ている場合があります。

```
[DB_0]
...
unix_domain_socket_marker=EXTPROC1522
...
[DB_1]
...
unix_domain_socket_marker=LISTENER
```

3. Oracle データベースが暗号化 (ASO/SSL) されている場合は、すべてのノード (アクティブとスタンバイ) で ATAP をアクティブ化します。
   a. すべての Oracle サービス (Clusterware を含む) を停止し、ohasd.bin がダウンしていることを確認します。
   b. ユーザーに Oracle およびグリッドを許可します (リスナーがグリッド・ユーザーに属している場合)。
   c. オンライン・ヘルプや Knowledge Center で提供されている情報を使用して、A-TAP パラメーターを構成します。
   d. A-TAP をアクティブにします。
   e. クラスター内のすべての Oracle サービスを開始します。
4. Oracle RAC 環境では、どのユーザーがリスナーを開始するかを検査します。それがユーザー・グリッドに関するものであれば、ユーザーにグリッドを許可します。

親トピック: 特別な環境での構成 (Linux、Solaris、HP-UX、AIX)

S-TAP for DB2 WPAR の構成

このタスクについて

ktap_fast_shmem が 1 に設定され、guard_tap.ini ファイル内で 1 つの WPAR に対して複数の Db2 インスタンスが構成されていて、これらの Db2 インスタンスの db2_shmem_size が同じである場合、その WPAR の最初の Db2 セクションで構成されている db2_fix_pack_adjustment と db2_shmem_client_position が返されます。したがって、WPAR 上で複数の Db2 インスタンスが実行されている場合は、以下のようになります。

- すべての Db2 インスタンスの db2_shmem_size、db2_fix_pack_adjustment、および db2_shmem_client_position が同じである場合は、構成されているインスタンスが 1つだけであっても、すべてのインスタンスからのパケットが収集されます。
- すべての Db2 インスタンスで db2_shmem_size は同じであるが、db2_fix_pack_adjustment または db2_shmem_client_position が異なる場合は、最初に構成された Db2 インスタンスからのパケットのみが収集されます。

手順

1. クライアント入出力域オフセット (db2_shmem_client_position) を計算します。
   a. db2 インスタンス・ユーザーとして新しい bash シェルを開きます。
   b. このシェルに関して db2bp コマンド・プロセッサーが現在実行中でないことを確認するために、ps -x コマンドを実行します。db2bp というコマンドが実行中と表示されないはずです。もし実行中であれば、kill するか、新しいシェルを実行します。
   c. 以下の 2 つのコマンドを実行します。

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print $9 * 4096}'
```

   出力は、db2_shmem_client_position として必要な値です。
2. DB2® 共有メモリー・セグメント・サイズ (db2_shmem_size) を見つけるには、以下のいずれかを実行します。
   - 以下の方法では、最も正確な結果が得られます。
     a. Db2 共有メモリー接続を開始して、開いたままにします。
     b. ps -eaf | grep db2sysc コマンドを実行して、db2sysc のプロセス ID を取得します。出力は、以下のとおりです。

```
db2inst1  5309370  5505772   0   Nov 11      - 1232:12 db2sysc 0
```

     この例では、プロセス IDは 5309370 です。
     c. ipcs -ma コマンドを実行して、共有メモリー・プロセスに関する情報を取得します。出力は、以下のとおりです。

```
IPC status from /dev/mem as of Wed Nov 20 13:21:45 CST 2013
T         ID     KEY        MODE       OWNER    GROUP  CREATOR   CGROUP NATTCH     SEGSZ  CPID
m    2097152 0xffffffff D-rw------- pconsole   system pconsole   system      1 536870912 4522088
m          1 0x78000015 --rw-rw-rw-     root   system     root   system      3  16777216 3605314
m          2 0x78000016 --rw-rw-rw-     root   system     root   system      3 268435456 3605314
m  219152387 0xffffffff D-rw-------     root   system     root   system      1 536870912 5243842
m    1048580 0x61013002 --rw------- pconsole   system pconsole   system      1  10485760 4522088
m   10485765 0xd9fd8a61 --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      5  47644672 5571082
m    9437190 0xd9fd8a74 --rw-rw-rw- db2inst1 db2iadm1 db2inst1 db2iadm1      9 140852104 5571082
m    9437191 0xe1bd8858 --rw-rw----   oracle      dba   oracle      dba     40 53687107584 3801352
m    3145736 0x52594801 --rw-rw----     root informix     root informix     13 223019008 5702650
m    3145737 0xd9fd8b68 --rw-rw---- db2inst1 db2iadm1 db2inst1 db2iadm1      1  58720256 6619354
m    3145738 0xffffffff --rw------- db2fenc1 db2fadm1 db2inst1 db2iadm1      7 268435456 5505772
m         11 0x52594802 --rw-rw----     root informix     root informix     13  33439744 5702650
m         12 0x52594803 --rw-rw-rw-     root informix     root informix     13    573440 5702650
m         13 0xf2033f7e --rw------- sybase15   sybase sybase15   sybase      1 115564544 5178168
m  409993231 0x52594804 --rw-rw---- informix informix informix informix     13   8388608 5702650
m  763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
m  125829140 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
m  201326613 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
m  103750230 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 134217280 5309370
```

出力には、ここに示されている列以外の列がいくつか含まれていますが、この手順に影響を与えるものではありません。ステップ 2.b で特定されたプロセス ID を含み、かつ NATTCH 列の値が 2 である行を探します。Db2 共有メモリー・セグメントのサイズは、SEGSZ 列の値になります。 この例では、131072 です。

d. ヒント: ステップ 2.c で返されるリストが長すぎる場合、プロセス ID を使用してリストをフィルターに掛けることができます。この例では、ipcs -ma | grep 5309370 と入力します。この結果には列見出しは表示されませんが、前の結果を調べて列見出しを確認することで、正しい行と列を特定できます。この例では、最後の行です。

```
m 131072014 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 1342177280 5309370
m 763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
m 227541013 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
m 106353238 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
```

- あるいは、以下の方法を使用します。それはより簡単ですが、精度が下がります。
  ATAP と KTAP は、このサイズに基づいてアプリケーション/エージェントの共有メモリー・セグメントを識別します。 これらのセグメントは、C2S パケットと S2C パケットに使用されます。セグメントは、ASLHEAPSZ パラメーターと RQRIOBLK パラメーターの合計に等しくなります。DB2 では、はるかに大きいセグメントが割り振られます。 ほとんどの場合、このサイズは (ASLHEAPSZ + 1) * 2 ページ、または (ASLHEAPSZ + 1) * 8192 バイトに等しくなります。正確なサイズは、新規 DB2 のローカル接続が作成される前後にシステム内の共有メモリー・セグメントを監視することによって測定できます。以下の一連のコマンドを使用して、共有メモリー・セグメント・サイズを決定します。ipcs コマンド・パラメーターと出力形式は、プラットフォームによって異なります。 以下のスクリプトは AIX® バージョンに基づいています。

```
ipcs -ma | sort -n -2 +3 > /tmp/before.txt
db2 connect to <some_existing_database>ipcs -ma | sort -n -2 +3 > /tmp/after.txt
db2 terminate
diff /tmp/before.txt /tmp/after.txt | awk '{if ($10 == 2) print $11}'
```

DB2 共有メモリー・トラフィックをキャプチャーするには、以下のパラメーターを設定します。

表 1. Db2 パラメーター

パラメーター	STAP 名	ATAP 名	デフォルト値	コメント
パケット・ヘッダー・サイズ	db2_fixed_pack_adjustment	db2_header_offset	20	デフォルト値は、さまざまな 64 ビット・プラットフォーム上の DB2 8.2 以降に関してテストされています。他のバージョンの DB2 と 32 ビット・プラットフォームでは、異なるオフセットが必要である可能性があります。通常考えられるのは 16 と 12 です。
クライアント入出力域オフセット	db2_shmem_client_position	db2_c2soffset	61440	このパラメーターは ASLHEAPSZ DB2 パラメーターから派生します。
DB2 共有メモリー・セグメント・サイズ	db2_shmem_size	db2_shmsize	131072	このパラメーターは経験的に決定されます。 これを得るために使用できる一連のコマンドについては、以下を参照してください。

親トピック: 特別な環境での構成 (Linux、Solaris、HP-UX、AIX)

Db2 クラスターのすべてのノードでの A-TAP のアクティブ化

A-TAP は、Db2 サーバーが Db2 クラスターのノードによって共有されているすべてのノードでアクティブにする必要があります。

手順

1. ノード 1 で Db2 ユーザーを許可します。<guardium_base>/xxx/guardctl authorize-user <user-name>
   例:

   # /usr/local/guardium/bin/guardctl authorize-user db2inst1

   # /usr/local/guardium/bin/guardctl is_user_authorized db2inst1

   ユーザー「db2inst1」が許可されます。

2. ノード 1 で A-TAP をアクティブにします。
   <guardium_base>/xxx/guardctl db_instance=<instance> activate
   例:

   ```
   # /usr/local/guardium/guard_stap/guardctl db_instance=db2inst1 activate

   # /usr/local/guardium/guard_stap/guardctl list-active
   db2inst1
   ```

3. ノード 1 で ATAP をアクティブにした後でノード 1 で元の Db2 サーバーを復元します。これにより、他のノードが ATAP をアクティブにできるようにします。(すべてのノードは実行可能ファイルを共有します。(db2 adm ディレクトリーで、db2sysc-guard-original を db2sysc にコピーします (最初にそれぞれのコピーを作成し、保管してください))。例:
   ```
   # > cp db2sysc-guard-original db2sysc
   ```
4. db2sysc-guard-original を削除します (そうしないと、ノード 2 でアクティベーションが失敗します)。例:
   ```
   # rm -rf db2sysc-guard-original
   ```
5. クラスター・リソースをノード 2 に移動します。例:
   ```
   # pcs resource move resource_id <destination node>
   ```
6. ノード 2 で Db2 ユーザーを許可し、アクティブにします (ステップ 1 とステップ 2)。これにより、ノード 2 でライブラリーが作成され、削除された db2sysc-guard-original が置換されます。 現在の状況は以下のようになります。
   Node01:

~]# /usr/local/guardium/guard_stap/guardctl list-active

db2inst1

Node02:

~]# /usr/local/guardium/guard_stap/guardctl list-active

db2inst1

親トピック: 特別な環境での構成 (Linux、Solaris、HP-UX、AIX)

遅延クラスター・ディスク・マウントの構成

このトピックは、Oracle、Informix®、および DB2® の各データベース・サーバーにのみ適用されます。

これらのデータベース・タイプでは、S-TAP は開始時に、データベース・ホームへのアクセス権限を持っている必要があります。ご使用の環境でクラスタリング・スキームを使用しており、パッシブ・ノードではなく、アクティブ・ノードにマウントされている単一ディスクを複数のノードが共有している場合、パッシブ・ノード上ではフェイルオーバーが発生するまでデータベース・ホームを使用できません。

構成ファイルのプロパティー WAIT_FOR_DB_EXEC を設定することにより、 S-TAP で遅延ロードを構成することができます。S-TAP は、開始時にデータベース・ホームにアクセスできないことを検出すると、WAIT_FOR_DB_EXEC の値を調べて、適切な処置を行います。

- WAIT_FOR_DB_EXEC > 0 の場合、プロセス名の stat() が可能かどうかにかかわらず、S-TAP が始動します。これは、15 分間隔でプロセス名の stat() を試行します。
- WAIT_FOR_DB_EXEC < = 0 の場合、S-TAP は、検査エンジンが起動したすぐ後に、検査エンジンのプロセス名の stat() を試行します。プロセス名の stat() ができない場合、S-TAP は終了します。

このプロパティーを正の値に設定する前に、その他の必要な構成プロパティーがすべて設定されていることを確認し、S-TAP が開始して、正しくデータを収集することをテストしてください。このプロパティーは、構成ファイルを編集することによってのみ設定でき、GUI からは設定できません。

親トピック: 特別な環境での構成 (Linux、Solaris、HP-UX、AIX)
親トピック: S-TAPs およびその他のエージェント

S-TAP 管理ガイド

Guardium の S-TAP® は、データベース・サーバー・システムにインストールされる、単純なソフトウェア・エージェントです。

S-TAP はデータベース・トラフィックをモニターし、そのトラフィックに関する情報を Guardiumシステムに転送します。

S-TAP の概要

- S-TAP は、そのシステムのローカルなデータベース・トラフィックをモニターできます。ローカル接続では、データベースへのバックドア・アクセスが可能であり、そのようなアクセスはすべてモニターと監査を必要とするため、これは重要です。
- S-TAP を使用すると、インストールしたデータベース・サーバーから可視のすべてのネットワーク・トラフィックをモニターできます。このようにして S-TAP は、Guardium システムをインストールすることが実用的でないリモート・ネットワーク・セグメント上でコレクターとして機能します。
- S-TAP は、Guardium® Installation Manager を使用してインストールする以外にも、Windows サーバーと Unix サーバーの両方のコマンド行からリモートでインストールできます。アップグレードを構成して、次回のサーバー・リブートで適用されるようにすることができます。Linux では、S-TAP はブート時に S-TAP カーネル・コンポーネントのアップグレードを処理して、Linux 環境のカーネル・アップグレードに対応します。

フェイルオーバー処理

S-TAP のデータ収集と Guardium ホストへのデータ送信は、ほぼリアルタイムで行われます。S-TAP はデータをバッファーに入れて、Guardium ホストが一時的に使用できない場合でも、処理を継続できるようにします。1 次ホストが長時間使用不可の場合 (バッファーがいっぱいになった場合は短時間でも)、S-TAP を 2 次 Guardium ホストにフェイルオーバーすることができます。S-TAP は以下のいずれかの状況が発生するまで、2 次ホストにデータを送信し続けます。すなわち、その Guardium システムが使用不可になるか、S-TAP が再始動される (その場合、S-TAP は 1 次ホストに最初に接続を試みます) か、または 1 次サーバーへの接続が再確立されて、その後 5*connection_timeout_sec 秒間 (guard_tap.ini で構成可能、デフォルトは 10 秒) 接続が維持されたかのいずれかです。その場合、S-TAP は 2 次 Guardium ホストから 1 次 Guardium ホストに再びフェイルオーバーします。

注: S-TAP は通常データベース・サーバーにデプロイされますが、S-TAP をアプリケーション・サーバーやデータベース・クライアントなどのクライアント・サイド・システムにインストールすることもできます。
注: S-TAP がアプリケーション・サイド (前述の注を参照) とデータベース・サーバーの両方にインストールされている場合は、重複トラフィックのモニターが行われないように、さらに注意が必要です。

セッション・データのフェイルオーバー

S-TAP のフェイルオーバーが発生すると、セッション情報もまた、現在アクティブな Guardium ホストに送られる場合があります。tap_failover_session_size (0 は機能を無効にします) および tap_failover_session_quiesce の設定については、『S-TAP 構成ファイルの編集』を参照してください。

再始動性

wait_for_db_exec が 0 より大きい場合に有効です。システムのリブートまたはユーザーの S-TAP 停止/始動コマンドによって S-TAP が再始動されると、S-TAP はモニター対象として構成されているすべてのデータベースをポーリングし、それらが使用可能な場合にモニターを開始します。 構成の異常 (データベース・サイドでも S-TAP サイドでも) のため、あるデータベースの S-TAP によるモニターが制限される場合でも、その他の正常に構成されているデータベースのモニターは制限を受けずに S-TAP により実行されます。S-TAP は正常に始動され、すべての正常な構成をモニターし、その他のデータベースをポーリングして、それらが使用可能になったらモニターを開始します。障害状況のモニターとレポートには、既存のアラートおよびレポートの使用を推奨します。

Oracle では、Oracle BEQ の再リンク後、トラフィックは 15 分間ログに記録されません。これは、Oracle デバイス・ノードが変更されたかどうかを S-TAP が検査するのにかかる時間です。

プロキシー・ファイアウォール

S-TAP は通常データベース・サーバーにデプロイされますが、K-TAP ベースのファイアウォールをプロキシー・サーバーにデプロイすることができます。パラメーター app_server=1 を設定して S-GATE を使用することにより、プロキシー・サーバーから発生するトラフィックをモニターできます。app_server の設定およびポリシー内での S-GATE の使用について詳しくは、「ポリシー」ヘルプ・トピックで、『S-TAP 構成ファイルの編集』および『S-GATE アクション』(ブロッキング・アクション) を参照してください。

S-TAP エージェント用の 2 次 Guardium ホスト

S-TAP 用の 1 次ホストに指定されている Guardiumシステムが使用不可になった場合、S-TAP は 2 次ホストにフェイルオーバーできます。S-TAP は以下のいずれかの状況が発生するまで、2 次ホストへの接続を継続します。すなわち、S-TAP が再始動される (その場合、S-TAP は 1 次ホストに最初に接続を試みます) か、または 1 次サーバーへの接続が再確立されて、その後 5*connection_timeout_sec 秒間 (guard_tap.ini ファイルで構成可能、デフォルトは 10 秒) 接続が維持されたかのいずれかです。

データベース・サーバーのオペレーティング・システムにより、S-TAP は以下のように多少異なる条件で再始動されます。

- Unix: S-TAP はアクティブ・ホストから構成変更が適用されるたびに再始動されます。

Guardium システムを S-TAP の 2 次ホストとして指定する前に、以下の項目を確認してください。

- その Guardium システムが、S-TAP を管理するように構成されていること。これを確認し、必要な場合に再構成するには、『エージェントを管理するための Guardium システムの構成』を参照してください。
- その Guardiumシステムが、S-TAP がインストールされているデータベース・サーバーに接続可能であること。複数の Guardium システムが使用されている場合、それらはしばしば、ネットワーク上で切り離された分岐に接続されています。
- その Guardiumシステムが、S-TAP がインストールされているデータベース・サーバーからのセッション・データを無視するようなセキュリティー・ポリシーを持たないこと。多くの場合、Guardium セキュリティー・ポリシーは、監視可能なデータベース・トラフィックの狭いサブセットに重点を置き、その他すべてのセッションは無視するように構築されます。2 次ホストが S-TAP からのセッション・データを無視しないことを確認するか、Guardiumシステムのセキュリティー・ポリシーを必要に応じて変更します。

S-TAP の 2 次ホストを定義するには、「GUI からの S-TAP の構成」で、『S-TAP の 2 次 Guardium ホストの定義』を参照してください。

注: S-TAP は通常データベース・サーバーにデプロイされますが、S-TAP をアプリケーション・サーバーやデータベース・クライアントなどのクライアント・サイド・システムにインストールすることもできます。

S-TAP および認証

注: Guardium は、認証局 (CA) サービスは提供しません。また、デフォルトでインストールされているもの以外の証明書をシステムに添付することもありません。 独自の証明書をお求めのお客様は、サード・パーティー CA (VeriSign や Entrust など) にお問い合わせください。
注: コレクターへの S-TAP フィードが暗号化されていることを確認するだけでなく、S-TAP クライアントが対話を試行する Guardium システムを認証するように、S-TAP クライアントを構成することもできます。これにより、トラフィックが暗号化されていることだけでなく、S-TAP が非認証サーバーに対して情報をフィードしていないことも保証できます。

S-TAP の設定

Guardium システムの認証性の確認を有効にするためには、guard_tap.ini 内で、use_tls=1 に加えて以下の 3 つの設定を有効にする必要があります。

1. guardium_ca_path

   guardium_ca_path が、1 つ以上のトラステッド CA 自己署名証明書 (PEM フォーマット) を含むファイルを指すように設定されている場合、Guardium システムの検査が実行されます。

   Guardium システムにインストールされているシステム証明書には、ファイルに提供されているいずれかの CA による署名が必要です。また、Guardium システムには、対応する正しいキーが必要です。

   デフォルトで、Guardium の自己署名ルート証明書が S-TAP インストール (クラシックまたは GIM ベース) で提供されます。guardium_ca_path が Guardium によって提供されるファイルを指すようにすることで、Guardium システムが、Guardium によって署名された鍵/証明書ペアを持つことが保証されます。

   サード・パーティーが署名した証明書と鍵を使用するためには、guardium_ca_path が所定のサード・パーティー (Verisign など) による CA 証明書を含むファイルを指すように設定する必要があります。その場合、Guardium システムは、同じサード・パーティーにより署名された鍵/証明書ペアを持つ必要があります。

2. sqlguard_cert_cn
   Guardium システム証明書の署名、および対応する秘密鍵の保有を検査することに加えて、お客様は、sqlguard_cert_cn で設定された正規表現パターンに一致しない CN (共通名) を持つ証明書を受け入れることもできます。
   注: 同じ証明書/鍵ペアを複数のマシンにインストールできます。お客様は、N 台のマシン用に N 個の証明書を購入する必要はありません。
3. guardium_crl_path

   このパスが、CA からの証明書失効リスト (CRL) を含む、PEM エンコードされたファイルを指す場合、すべての失効した Guardium システム証明書は拒否されます。Guardium CRL は STAP インストール (または GIM) で提供され、ソフトウェア・パッチおよびアップグレードによってアップデートされます。

   さらに、お客様は CA (Guardium またはサード・パーティー) が提供する CRL を手動でインストールできます。

   Guardium システムはインターネットにアクセスしないことを想定しているため、Web ベースの CRL サーバーは自動的には照会されません。

Guardium システム CLI システム証明書関連コマンド

以下のような、システム・キーと証明書の管理に関連する 4 つの CLI コマンドがあります。

- show certificate sniffer

このコマンドは、テキスト形式のシステム証明書と、それに続いて Base64 エンコードの PEM 形式エンコードをプリントします。テキスト形式の目的は、証明書の詳細 (特に CN、および S-TAP でフィルターに掛けられる場合がある署名者/シリアル) を表示することのみです。`---BEGIN CERTIFICATE---` と `---END CERTIFICATE---` の間にある PEM のエンコードされた部分は、他のマシンや関係者に対する証明書のバックアップ、保管、E メール送信に使用する部分です (区切り文字の BEGIN と END は、必ず Base64 エンコード部分に一緒に含める必要があります)。

- store certificate sniffer <console | import>

  このコマンドにより、Guardium システムが (S-TAP との通信に) 使用するシステム証明書を設定できます。証明書は、コンソールから貼り付けるか、標準インポート・プロトコルのいずれかを介してインポートすることができます。証明書の形式は PEM で、BEGIN と END の区切りを含む必要があります。この証明書は、guardium_ca_path を通じて S-TAP ソフトウェアから自己署名証明書が使用可能な CA によって署名されている必要があります。

- store certificate keystore <console | import>
  このコマンドを使用して、使用するシステム・キーを設定できます。この鍵は、証明書の公開部分と一致する必要があります。さらに、鍵は暗号化されたエンベロープ内になければなりません。これを暗号化するために使用するユーザー・パスワードは、保管処理中に提供される必要があります。この store コマンドは、鍵を最終的にシステムに保管する前に、Guardium の内部コードを使用して鍵を再度暗号化します。
  注: 証明書および対応する鍵の両方が Guardium システム上で使用可能になった場合のみ、Guardium システムの認証が S-TAP によって正常に実行されます。
- create csr sniffer

  このコマンドは、PEM 形式の証明書署名要求を作成するために使用します。このコマンドは、内部的に 2048 ビットの鍵を生成し、ユーザーが CSR フォームに記入するための質問のセットを出します (Country (国)、State/Province (都道府県)、Locality/City (地域/ 市区町村)、Organization (組織)、Organizational Unit (組織単位))。最後に、ユーザーは「共通名」を指定する必要があります。 通常、共通名に使用できるのは、文字、数字、下線、およびドットのみです。 これは特定のインストール済み環境における固有 ID にする必要があり、企業名、部門、クラスターまたは Guardium システム固有の名前を含めます。 ただし、外部 CA からの指示があれば、この推奨事項よりもそちらのほうを優先してください。 例:

  GCluster1DataCenterGuardiumIBM - これは、IBM® グループ企業 Guardium の DataCenter にある GCluster1 を意味します。

  SqlGuard1DataCenterGuardiumIBM - これは、SqlGuard1 マシン・システムを意味します (フェイルオーバーもある可能性があります)。

  E メールの入力を求められたときには、有効な E メールを提供してください。サポート担当員から連絡を受けることができるようにするためです。

  「チャレンジ・パスワード (Challenge Password)」と「オプションの会社名 (Optional Company Name)」はブランクのままでかまいません。

  最後に、証明書署名要求が、読み取り可能な形式と PEM エンコードされた形式で表示されます。

  詳細を確認し、PEM のエンコード部分 (`---BEGIN CERTIFICATE REQUEST---` と `---END CERTIFICATE REQUEST---` を含めたその間の部分) を署名のために CA に送信する必要があります。
  注: この時点では、システムは新規の内部生成された鍵を保持していますが、先にインストールされたシステム証明書とは対応付けられていません。 これは、署名のために証明書を送信しているときに S-TAP によって情報がフィードされないようにするためです。 連続した稼働と S-TAP フィードを確保する必要がある場合は、この期間中、S-TAP サイドで Guardium システム認証を無効にする必要があります。

  CSR が検証されると、CA が署名済み証明書を PEM 形式で発行します。この証明書は store system certificate コマンドを使用してインストールする必要があります。

  この時点で、新規の証明書と、「create csr sniffer」コマンドの実行時に内部生成された鍵との突き合わせが行われ、S-TAP で Guardium システム認証を使用する準備が整います。

  S-TAP 構成ファイル内のすべての証明書関連パラメーターが正確であることを確認してください。

  同じ鍵/証明書を複数の Guardium システムにインストールする必要がある場合は、show system certificate | key コマンドを使用して、エクスポートとバックアップを行います。

  ユーザー指定のパスワードで暗号化されている鍵を外部のコンピューターまたはデバイスに保存する場合は特に注意してください。show system key でパスワードを求められた場合には、単純ではないパスワードを使用してください。

親トピック: S-TAPs およびその他のエージェント

S-TAP を管理するための Guardium システムの構成

Guardium GUI から S-TAP を管理するには、事前に Guardium システムを構成し、検査エンジンを再始動します。

このタスクについて

手順

1. Guardium からログアウトします。
2. SSH クライアント・ウィンドウから、cli ユーザーとして Guardium システム・コマンド行インターフェース (CLI) にログインします。

   ```
   ssh -l cli 192.168.2.16
   ```

   Guardium® CLI の使用法について、詳しくは『CLI の概要』を参照してください。

3. 以下の 2 つのコマンドを入力します。

   ```
   store unit type stap
   restart inspection-core
   ```

   この 2 つのコマンドの詳細情報については、『構成および制御 CLI コマンド』、および『検査エンジンの CLI コマンド』をそれぞれ参照してください。

4. quit を入力して Guardium CLI からログアウトします。

親トピック: S-TAPs およびその他のエージェント

S-TAP® 認証

この機能を使用して、無許可の S-TAP が Guardium システムに接続することをブロックします。

「S-TAP 承認が必要」ボックスにチェック・マークが付いていると、S-TAP は、明確に承認を得ない限り、接続できなくなります。

承認を得ていない S-TAP は、この GUI 画面でその S-TAP の IP アドレスに明確に権限が与えられない限り、接続してもすぐに切断されます。

「S-TAP 承認が必要」という機能は、CLI コマンド store stap approval または GuardAPI コマンド grdapi store_stap_approval を使用して制御できます。

CLI コマンドの stap approval ON | OFF を使用する場合、新規構成が有効になるのは restart inspection-core コマンドの実行後になります。

S-TAP の承認

1. 「S-TAP の承認が必要」のボックスにチェック・マークを付けます。
2. 承認された S-TAP クライアントを指定します。

注:

ホスト名ではなく、有効な IP アドレスを使用します。

一元管理された環境内で、承認済みの S-TAP に IP アドレスを追加した後、同期のために 1 時間程度待機します。 同期が完了すると、GUI 内で承認済みの S-TAP の状況が緑色で表示されます。

親トピック: S-TAPs およびその他のエージェント

SSL 証明書を使用する S-TAP 認証のセットアップ

S-TAP サーバーと Guardium システムの間の認証をセットアップします。

付加価値: S-TAP は、指定の証明書または証明書セットを使用して認証される特定のマシン (のグループ) のみに接続するように構成できます。これらの証明書は、Guardium システム上でローカルに生成して認証局 (CA) に署名のために送信するか、または CA 側で作成して、Guardium システム全体にインストールできます。

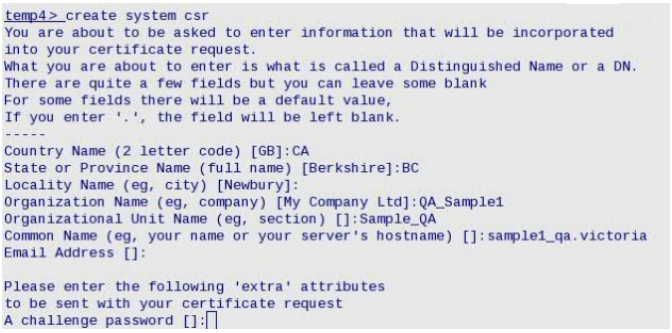
始めに: CA が誰/何であるか、その場所はどこかを確認する必要があります。インストールする証明書全体が CA から送信される場合、PKCS#8 (パスワード保護) フォーマットの秘密鍵と PEM フォーマットの公開鍵の 2 つのファイルが必要です。生成される証明書は、2048 ビットの RSA 鍵である必要があります。

Guardium システムでの証明書署名要求 (CSR) の生成

CLI を使用して Guardium システムにログインします。

cli> create csr sniffer

[データの入力が要求されます]



終了すると、以下のようなものが表示されます。

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CA, ST=BC, L=Newbury, O=QA_Sample1, OU=Sample_QA, CN=sample1_
qa.victoria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e9:5e:a2:81:53:dc:e9:b5:f7:54:33:17:6f:15:
                    9c:00:5c:ff:b2:64:c6:e5:48:be:36:a7:a4:55:f4:
                    b1:df:c9:81:a4:41:fe:29:80:d6:fd:d4:c4:b5:97:
                    b7:c1:3d:42:6c:c0:f8:09:cd:ea:36:f6:3b:b9:d9:
                    ce:15:87:2d:2f:b3:f2:5f:f9:42:06:e2:a0:62:56:
                    06:6d:cc:65:69:62:db:36:34:09:95:5b:c3:d0:e6:
                    85:ee:64:76:3e:ed:d6:47:bb:49:f2:08:81:14:c2:
                    e3:93:db:20:ba:86:e7:60:24:80:01:7f:3d:b7:60:
                    16:ba:06:d4:a1:e0:18:39:73:ca:1e:24:15:56:6d:
                    97:79:81:04:f7:fd:37:06:42:d7:15:82:34:aa:51:
                    2c:cc:e2:f0:d1:42:dd:b5:71:bb:10:19:a0:0a:5c:
                    4f:77:b9:bb:36:95:ed:a4:77:07:e3:50:f9:36:20:
                    13:e2:e1:78:d2:0a:36:8a:b9:39:90:1f:a4:82:12:
                    4f:50:29:3f:19:7d:16:a6:b3:23:7b:b8:7b:85:60:
                    04:21:39:84:1d:9e:81:e5:20:2c:8a:51:f3:52:f7:
                    3c:4f:e6:f2:a5:88:dc:2e:99:0a:b3:65:1e:bf:33:
                    5f:be:dc:53:1c:a6:69:18:c4:c7:75:bf:20:e3:cf:
                    29:af
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword       :guardium
    Signature Algorithm: sha1WithRSAEncryption
        06:4a:b9:db:04:a1:8d:4c:f7:3f:8f:24:fa:7c:ec:a6:70:77:
        8b:b9:38:7c:b6:e6:51:aa:ed:96:20:16:37:85:a7:44:26:2b:
        87:4c:a4:db:0c:f3:d3:87:e3:68:4a:8e:de:f6:0a:09:58:8f:
        68:98:4f:f3:8a:e2:37:5c:d6:42:32:8f:d9:01:56:41:88:df:
        1a:ba:63:03:62:08:89:06:13:08:74:6f:cd:eb:26:f0:67:a4:
        26:9b:a3:4c:ff:7b:c9:19:2c:12:58:06:ce:22:3c:e6:cd:52:
        b0:d0:da:6a:c9:02:df:02:e6:25:77:39:cf:50:80:e7:1d:01:
        fc:40:17:a2:98:04:bf:8b:24:f6:55:46:99:7b:17:05:01:d3:
        09:3d:a2:f0:e0:ba:5d:15:b8:28:74:d2:a3:fe:fd:86:7d:e0:
        60:e8:e4:38:6a:17:9c:80:80:e3:50:11:5e:35:f5:02:2b:65:
        60:41:2a:dc:ed:a8:a9:9a:6f:24:b4:7a:9c:39:01:a4:fc:cf:
        e6:94:86:f1:18:3a:f5:99:6b:f8:66:a2:ff:04:08:7e:ca:6b:
        2a:aa:cf:72:26:d0:c9:96:a0:98:fd:91:bb:b1:e4:8d:6d:10:
        08:ea:56:de:07:20:d3:e6:9a:bf:de:cf:c3:a4:e8:43:60:4f:
        b4:53:aa:d5
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwczELMAkGA1UEBhMCQ0ExCzAJBgNVBAgTAkJDMRAwDgYDVQQH
EwdOZXdidXJ5MRMwEQYDVQQKDApRQV9TYW1wbGUxMRIwEAYDVQQLDAlTYW1wbGVf
UUExHDAaBgNVBAMME3NhbXBsZTFfcWEudmljdG9yaWEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDpXqKBU9zptfdUMxdvFZwAXP+yZMb1SL42p6RV9LHf
yYGkQf4pgNb91MS1l7fBPUJswPgJzeo29ju52c4Vhy0vs/Jf+UIG4qBiVgZtzGVp
Yts2NAmVW8PQ5oXuZHY+7dZHu0nyCIEUwuOT2yC6hudgJIABfz23YBa6BtSh4Bg5
c8oeJBVWbZd5gQT3/TcGQtcVgjSqUSzM4vDRQt21cbsQGaAKXE93ubs21e2kdwfj
UPk2IBPi4XjSCjaKuTmQH6SCEk9QKT8ZfRamsyN7uHuFYAQhOYQdnoHlICyKUfNS
9zxP5vKliNwumQqzZR6/M1++3FMcpmkYxMd1vyDjzymvAgMBAAGgGTAXBgkqhkiG
9w0BCQcxChMIZ3VhcmRpdW0wDQYJKoZIhvcNAQEFBQADggEBAAZKudsEoY1M9z+P
JPp87KZwd4u5OHy25lGq7ZYgFjeFp0QmK4dMpNsM890H42hKjt72Cg1Yj2iYT/0K
4jdc1kIyj9kBVkGI3xq6YwNiCIkGE4h0b83rJvBnpCabo0z/e8kZLBJYBs4iPObN
UrDQ2mrJAt8C5iV3Oc9Qg0cdAfxAF6KYBL+LJPZVRpl7FwUB0wk9ovDgul0VuCh0
0qP+/YZ94GDo5DhqF5yAgONQEV419QIrZWBBKtztqKmabyS0epw5AaT8z+aUhvEY
OvWZa/hmov8ECH7Kayqqz3Im0MmWoJj9kbux5I1tEAjqVt4HINPmmr/ez8Ok6ENg
T7RTqtU=
-----END CERTIFICATE REQUEST-----
ok
temp4>
```

-----BEGIN CERTIFICATE REQUEST----- から -----END CERTIFICATE REQUEST----- までをファイルにコピーして、署名のために CA に送信します。

CA が証明書に署名し、公開鍵が送られてきます。

CA から送信される公開鍵は、以下に似たものになります。

```
enance@enance1 Latest $ cat sample1_qa.victoria.pem
-----BEGIN CERTIFICATE-----
MIID1jCCAsCgAwIBAgIBCDALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3Rvcmlhc1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMDEyMTA5MzhaFw0xNTExMDEyMTA5Mzha
MHMxCzAJBgNVBAYTAkNBMQswCQYDVQQIEwJCQzEQMA4GA1UEBxMHTmV3YnVyeTET
MBEGA1UECgwKUUFfU2FtcGxlMTESMBAGA1UECwwJU2FtcGxlX1FBMRwwGgYDVQQD
DBNzYW1wbGUxX3FhLnZpY3Rvcmlhc1FBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6V6igVPc6bX3VDMXbxWcAFz/smTG5Ui+NqekVfSx38mBpEH+KYDW/dTE
tZe3wT1CbMD4Cc3qNvY7udn0FYctL7PyX/lCBuKgYlYGbcxlaWLbNjQJlVvD00aF
7mR2Pu3WR7tJ8giBFMLjk9sguobnYCSAAX89t2AWugbUoeAYOXPKHiQVVm2XeYEE
9/03BkLXFYI0qlEszOLw0ULdtXG7EBmgClxPd7m7NpXtpHcH41D5NiAT4uF40go2
irk5kB+kghJPUCk/GX0WprMje7h7hWAEITmEHZ6B5SAsilHzUvc8T+bypYjcLpkK
s2UevzNfvtxTHKZpGMTHdb8g488prwIDAQABo2swaTAfBgNVHSMEGDAWgBR0SB68
8syKm4CUQ27LGB9ftHRZyTAMBgNVHRMBAf8EAjAAMA8GA1UdDwEB/wQFAwMHuAAw
JwYDVR0lBCAwHgYIKwYBBQUHAwQGCCsGAQUFBwMCBggrBgEFBQcDATALBgkqhkiG
9w0BAQUDggEBAJe1Dlh623uD9mBjfB3YDKO3agm3vbdMd2vcdKI8TA5dsxMhmHvm
8E+gVsVOrNVbupLoc6OYeJLPvWQ54j9wZnKavBbma067C1QJJ2jEhOhjzoiEDIqT
l/qBhvqabhTG3vIMFSIwOu0zmQD/2iFu9cykKiru8A8djfZWjjfZiHO4dkkiCInP
/dor+Cm5RokGZ+OXhZ/5hxTuGeSAWJIhObVnrnPLZ2c2uYGh6LYip+2GU6L/rp8z
tmLYfldjtTMGYeP4Ivo1s7KHJqqDlATOBwe2XVR98O8SrHI7toSpAbdIqP+f77zv
pb5xvOSfmqLuV6eUvJW8d/Wj2mvgw1qLvqY=
-----END CERTIFICATE-----
```

内容をコピーしたり、Guardium システムにインポートするのに便利な場所にこのファイルを配置してください。

cli> store certificate sniffer [console | import]

console の場合、**-----BEGIN CERTIFICATE-----** から **-----END CERTIFICATE-----** まですべて (コピー内のものを含む) をコピーし、プロンプトが出されたら、cli に貼り付けます。import を選択した場合、ファイルのインポート元を Guardium システムに指示します。

証明書の保管の確認を求められ、確認すると証明書が保管されます。

```
temp4 > store system certificate console
Please paste your new system certificate, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN CERTIFICATE-----
MIID1jCCAscgAwIBAgIBCDALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMDEyMTA5MzhaFw0xNTExMDEyMTA5Mzha
MHMxCzAJBgNVBAYTAkNBMQswCQYDVQQIEwJCQzEQMA4GA1UEBxMHTmV3YnVyeTET
MBEGA1UECgwKUUFfU2FtcGxlMTESMBAGA1UECwwJU2FtcGxlX1FBMRwwGgYDVQQD
DBNzYW1wbGUxX3FhLnZpY3RvcmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6V6igVPc6bX3VDMXbxWcAFz/smTG5Ui+NqekVfSx38mBpEH+KYDW/dTE
tZe3wT1CbMD4Cc3qNvY7udnOFYctL7PyX/lCBuKgYlYGbcxlaWLbNjQJlvvD0OaF
7mR2Pu3WR7tJ8giBFMLjk9sguobnYCSAAX89t2AWugbUoeAYOXPKHiQVVm2XeYEE
9/03BkLXFYI0qlEszOLw0ULdtXG7EBmgClxPd7m7NpXtpHcH41D5NiAT4uF40go2
irk5kB+kghJPUCk/GX0WprMje7h7hWAEITmEHZ6B5SAsilHzUvc8T+bypYjcLpkK
s2UevzNfvtxTHKZpGMTHdb8g488prwIDAQABo2swaTAfBgNVHSMEGDAWgBR0SB68
8syKm4CUQ27LGB0ftHRZyTAMBgNVHRMBAf8EAjAAMA8GA1UdDwEB/wQFAwMHuAAw
JwYDVR0lBCAwHgYIKwYBBQUHAwQGCCsGAQUFBwMCBggrBgEFBQcDATALBgkqhkiG
9w0BAQUDggEBAJe1Dlh623uD9m8jfB3YDKO3agm3vbdMd2vcdKI8TA5dsxMhmHvm
8E+gVsVOrNVbupLoc6OYeJLPvWQ54j9wZnKavBbma067C1QJJ2jEhOhjzoiEDIqT
l/qBhvqabhTG3vIMFSIwOu0zmQD/2iFu9cykKiru8A8djfZWjjfZiHO4dkkiCInP
/dor+Cm5RokGZ+OXhZ/5hxTuGeSAWJIhObVnrnPLZ2c2uYGh6LYip+2GU6L/rp8z
tmLYfldjtTMGYeP4Ivo1s7KHJqqDlATOBwe2XVR98O8SrHI7toSpAbdIqP+f77zv
pb5xvOSfmqLuV6eUvJW8d/Wj2mvgw1qLvqY=
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8 (0x8)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victori
a_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov  1 21:09:38 2010 GMT
            Not After : Nov  1 21:09:38 2015 GMT
        Subject: C=CA, ST=BC, L=Newbury, O=QA_Sample1, OU=Sample_QA, CN=sample1_
qa.victoria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e9:5e:a2:81:53:dc:e9:b5:f7:54:33:17:6f:15:
                    9c:00:5c:ff:b2:64:c6:e5:48:be:36:a7:a4:55:f4:
                    b1:df:c9:81:a4:41:fe:29:80:d6:fd:d4:c4:b5:97:
                    b7:c1:3d:42:6c:c0:f8:09:cd:ea:36:f6:3b:b9:d9:
                    ce:15:87:2d:2f:b3:f2:5f:f9:42:06:e2:a0:62:56:
                    06:6d:cc:65:69:62:db:36:34:09:95:5b:c3:d0:e6:
                    85:ee:64:76:3e:ed:d6:47:bb:49:f2:08:81:14:c2:
                    e3:93:db:20:ba:86:e7:60:24:80:01:7f:3d:b7:60:
                    16:ba:06:d4:a1:e0:18:39:73:ca:1e:24:15:56:6d:
                    97:79:81:04:f7:fd:37:06:42:d7:15:82:34:aa:51:
                    2c:cc:e2:f0:d1:42:dd:b5:71:bb:10:19:a0:0a:5c:
                    4f:77:b9:bb:36:95:ed:a4:77:07:e3:50:f9:36:20:
                    13:e2:e1:78:d2:0a:36:8a:b9:39:90:1f:a4:82:12:
                    4f:50:29:3f:19:7d:16:a6:b3:23:7b:b8:7b:85:60:
                    04:21:39:84:1d:9e:81:e5:20:2c:8a:51:f3:52:f7:
                    3c:4f:e6:f2:a5:88:dc:2e:99:0a:b3:65:1e:bf:33:
                    5f:be:dc:53:1c:a6:69:18:c4:c7:75:bf:20:e3:cf:
                    29:af
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:74:48:1E:BC:F2:CC:8A:9B:80:94:43:6E:CB:18:1F:5F:B4:74:59:C
9

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment, Key Agre
ement
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication, TLS Web Server
 Authentication
    Signature Algorithm: sha1WithRSAEncryption
        97:b5:0e:58:7a:db:7b:83:f6:60:63:7c:1d:d8:0c:a3:b7:6a:
        09:b7:bd:b7:4c:77:6b:dc:74:a2:3c:4c:0e:5d:b3:13:21:98:
        7b:e6:f0:4f:a0:56:c5:4e:ac:d5:5b:ba:92:e8:73:a3:98:78:
        92:cf:bd:64:39:e2:3f:70:66:72:9a:bc:16:e6:6b:4e:bb:0b:
        54:09:27:68:c4:84:e8:63:ce:88:84:0c:8a:93:97:fa:81:86:
        fa:9a:6e:14:c6:de:f2:0c:15:22:30:3a:ed:33:99:00:ff:da:
        21:6e:f5:cc:a4:2a:2a:ee:f0:0f:1d:0d:f6:56:8e:37:d9:88:
        73:b8:76:49:22:08:89:cf:fd:da:2b:f8:29:b9:46:89:06:67:
        e3:97:85:9f:f9:87:14:ee:19:e4:80:58:92:21:39:b5:67:ae:
        73:cb:67:67:36:b9:81:a1:e8:b6:22:a7:ed:86:53:a2:ff:ae:
        9f:33:b6:62:d8:7e:57:63:b5:33:06:61:e3:f8:22:fa:35:b3:
        b2:87:26:aa:83:94:04:ce:07:07:b6:5d:54:7d:f0:ef:12:ac:
        72:3b:b6:84:a9:01:b7:48:a8:ff:9f:ef:bc:ef:a5:be:71:bc:
        e4:9f:9a:a2:ee:57:a7:94:bc:95:bc:77:f5:a3:da:6b:e0:c3:
        5a:8b:be:a6

Do you want to store this certificate? (y/n)
```

新しい証明書を反映するには、inspection-core を再始動する必要があります。

Guardium システム外部で生成された証明書のインストール

CA からファイルのペア (さらに CA の公開証明書) を受け取ります。これが使用する証明書になります。

1 つ目は、以下のような CA の公開証明書です。

```
enance@enance1 Latest $ cat Victoria_QA_CA.pem
-----BEGIN CERTIFICATE-----
MIID2zCCAsWgAwIBAgIBATALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDA4MTIxODMzMDJaFw0zMDA4MTIxODMzMDJa
MIGAMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2x1bWJpYTERMA8G
A1UEBxMIVmljdG9yaWExFDASBgNVBAoTC1FBX3R1c3RfdmljMRQwEgYDVQQLEwtW
aWN0b3JpYV9RQTEXMBUGA1UEAxMOVmljdG9yaWFfUUFfQ0EwggEgMAsGCSqGSIb3
DQEBAQOCAQ8AMIIBCgKCAQEA0x3iAXs1KGNoJThXkO+jcNyMBlfwKWRMTOq9PkF4
piznXCRwPz2nQWk5/fpslchmuVYXJtfZi7umDxp2FEMvMmhJfFZiqbCn1Rb5yH+1
V3RsIerB0DFpoWkdt+wD6BufndO5P9eOlv14bmTl+F0dUM0TxAwtX73CMQOX/n+i
/WrzpWU4lU71KkyWUfJl2Pm8TLEMr5awpzt2rEJ/Q1qItHcksQDbGY0MNLaNojEU
XBzUpu9ezbv+zVH+5iorFYkrH0NQI0NK+YoR1b3Tto0HLDh6istsMfHdNEEQb9BB
vMjqUz4tGB2HDguYTaNbQJj9Yw8uv7/tfwW/cesrqm8DiQIDAQABo2QwYjAPBgNV
HRMBAf8EBTADAQH/MA8GA1UdDwEB/wQFAwMHBgAwHQYDVR0OBBYEFHRIHrzyzIqb
gJRDbssYH1+0dFnJMB8GA1UdIwQYMBaAFHRIHrzyzIqbgJRDbssYH1+0dFnJMAsG
CSqGSIb3DQEBBQOCAQEAbrImEbRyBka0wO/ZuPd0Hw9jpbxIuaYEskakv7aM4TUQ
awf1CiqwwAymmKb2REItLajhjmBFbXBun7d137vBU2KX104I7WGw0xgI5rmlELa+
2fizugY+Bc6mh+5c0haizkyudKzo8mLz2p/IS7SPh2lJ9rnuBleSt9zfiYanPxX1
Q6z1+WRKIRSUmK+ho4bmtgr5F0+ejmZb9nfzeOBj23H9i0mWoaQ/SO+O2iDIvDY0
KYwqCeS2UNEdTcnfuczbBkqnAsf5/GBPIhnWX3onuLkOsHdY0HHPjoqgHauoxPK8
p0sEvlCK8EFOD6wkp0vtNhFQCykxRimHR6Pz9jEVjw==
-----END CERTIFICATE-----
```

次は、使用する Guardium システムに固有の公開証明書で、以下のようなものになります。

```
enance@enance1 Latest $ cat Sample_givenCert.victoria.qa_pub.pem
-----BEGIN CERTIFICATE-----
MIID5jCCAtCgAwIBAgIBCTALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMTUyMDUwNThaFw0xNTExMTUyMDUwNTha
MIGEMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2xvbWJpYTESMBAG
A1UEBxMJVmFuY291dmVyMQswCQYDVQQKEwJRQTESMBAGA1UECxMJUUFfU0FNUExF
MSUwIwYDVQQDExxTYW1wbGVfZ2l2ZW5DZXJ0LnZpY3RvcmlhLnFhMIIBIDALBgkq
hkiG9w0BAQEDggEPADCCAQoCggEBALdt2XhJEJIAognblgFNoiomVvcGIe9PHs0t
3fP5DxAL5PVm+UCRS0xnnCoKe3pdJNagepDwBa2K5UsHbK4vkHJEgWWEd4bx2Ks7
kRoHr83TXK+W8al1HGKRwUSwN0hfm/KV4v8ZX3AFWs2c/BJ2iA77a0mhU0JuWa1/
/scXitJB5ykPjFb2EuReA6ELphaQ/itjZIQTTeVxbamyx42ia9J5B07lFTp3qGdU
yXUwlEFX0HFPmknAAaQrSnpMdQjkOKgzxU0NTV4ILA66hCVkX+ezQeJA90s/AHA5
hAY2fyurKZsOowoE0xlEpFWCGf87zxfkmTaWthqCS0NzEcJ6efECAwEAAaNrMGkw
HwYDVR0jBBgwFoAUdEgevPLMipuAlENuyxgfX7R0WckwDAYDVR0TAQH/BAIwADAP
BgNVHQ8BAf8EBQMDB7gAMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYI
KwYBBQUHAwEwCwYJKoZIhvcNAQEFA4IBAQB+P1m22B72eRESk9rgNdOB+l48k5xw
QHf64TJcoI/Vcz0vtGBC1jDfZzVDIHJaX6ZMtdO23QO6rtjQSnhjhbOt/EiimaNO
tysJOE999E+HQ7UpKYKvdoznwpYEthyoQJ9quKqQc1YW/l8pQMYDEdK8c7yMbJpv
mrxO8h+G3YYQMT6A9KAk/GPA+yKl0fCuogBhPyWM28q35EAIw6H9ahQigWhNkzrL
DCYO8VCLi3BX+OohLvurkyzJm2lnbm7BSb5QB4jISlRBGPoIWhK6VPypboyABfVs
yWHFVs10EUb0Maa/XNZILTAoYAbYK5sX7Ri5hr5KhxnmDd9AJMQsLfik
-----END CERTIFICATE-----
```

最後は秘密鍵 (pkx#8 を使用して暗号化) で、以下のようなものになります。

```
enance@enance1 Latest $ cat Sample_givenCert.victoria.qa_pri.pem
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4jAcBgoqhkiG9w0BDAEDMA4ECAKuMvSla9T4AgIBYgSCBMB/RzDgm4xpRDnA
Cd//wgD9c8junXmVpyJWXWgXhlj3Sgv3toKt2yBQY7Rv0peP1y68nuHKZcp/QZDj
QksDvIJHacpz886KQ2p9xxOCrIO3RTVNULPzrucUNuJ2a5W4IGPGwnrNLKsriRH6
CXQjRu19+kbczmPtrlHu7gj6MuCp58sIyXbsOPCnsZBaAOcf72qeKfVa4tKlpobI
e5YDg+UiJXYv1Kfj9t9tftSfaCym0jK+uE3++y5+ah/k+u/VcEb9b6DrlfG8KaJI
/OYVVmRWVIHEY2QjVOsVEXAARjpugf6cXIn8epw/CMaC0yVg4O9OGDrIz/41DVgk
/b3jlr1oWMRVASSqgOQxE2LrNNAF/XiFwpiLUCBHR0fXX9iKJM7nK6AXlf4hrd31
sMm1hICJvQwuRP+1xCHHs3qKk7oFAdyEdMiYthcOoAaynGmP4vPEMB6ZdOSxd/yN
7IfBT1U7nCtgo4FpAn4FTnkXRdlDqPpvKLqe0kkQCKo9ZWRnnIS1hAs9VJXS6zou
1IohZewrS/TWnPU+ArE/QJ4WkX2dBAe0Q2HMvuXs6J6Rfn+H2eZC+zThOkvqA0ic
UiQAgJB0ohXWEah9BJbIYNULLpbssUySDLPrxYdZRPn5MFKqCXmWw5tAEV8mIcg4
obB6DxVGHz93iPD0XJyBGWpCdcwItzdngnMR316tX4R3jMy2U0hrzk5o01GoZQQ/
eGYsuPzm4zqVJ8S9gUMFR8ocoPWqwhU+Sq4QPCIQEGf5gwxxt9j7L2TtRbD7kxnD
23aPL/wuk45EFJKTQCeZ3kjUqCCuSbqBJXGEjiiUsahus+yJULJ8boFWu1T8zW7m
/CBK1TzY9Fh+gbd0tN4b+zWUrpk5E7ZctFhEwojVFBwgPzUIZEkap4gH+/F5d3rI
uWFBcN7QER35w08au/k5kLKHDh+5U15ltkJ38P1pJYFE0p5/K81YWnfvUaJmynJY
DfnK0X6Au69/F6+QR4S+bchbrqk73plIiXbkwqapQ26QH5ztIK3T6/nY6RKa7u6N
WvnskpAE1uxf+soM+BpEzpTl2gQQmEaZnh9Ci3ZnpTZE5tkAL0oTqXL9sToyeynz
Z91m+uKxYRjFvc1KPh+I8dUR0E5qXhBdRR7heIlm7/Dg+UqCUkXoyW89G14u/mJT
jB50CHxLAFOSeXnKn8G/9r0HA565r8L/z8D12sli5T1zHicZJ80211zCSezdF+GG
mI12jfOZmNIBgCVUtpOBNX5IDbr7L+0bM6vuDmXRhnhX4f34+5HGfj3ntLAV7bmn
IOEGIhyoGFnoxyWaT0xxa6MVQJazcKSyyyhO8UixFEoKI3drpFXB0tXVb0CLFq+y
QVp9dHgO30tzw/yCmCpbQQe8UFRYyC74wBf9yPWDtN6MW/IeEZCBoYaeMR+WyonM
mdq5xbriETXD4zha3NGAv2qnzkfkKMBcVeUULulyixMsHmNNJkINNEsj5deVYtOt
4j5EK/aZsTqTgrVq3oGlwgXM1Yptv1VR+HPWZfpjwbL+7/NhmK7AhEPo+qQCVD7t
ZGRbdbB7FEN23m88IMSd8xkhS2M1pop1Cj7lP/dA+DD/dgcjP2bw7K923d4r3CcS
1yxPhLKM
-----END ENCRYPTED PRIVATE KEY-----
```

これらのファイルを準備して、Guardium システムにインポートする (scp、ftp などを使用) か、Guardium システム上の cli インターフェースにコピー・アンド・ペーストします。

cli を使用して Guardium システムにログインします。

秘密鍵を保管するには、以下を実行します。

cli> store certificate keystore [import | console]

import は、保存されたファイル (コンソール) を取得し、ファイルの内容をコンソール・インターフェースにコピー・アンド・ペーストします。

ファイルと共に保存されたパスワードを尋ねられます。これは、証明書を作成するために CA に提供したものか、あるいは多くの場合、CA からファイルが送信されたときに、CA から提供されたパスワードです。

Guardium システムでは以下のように表示されます。

```
temp4>_store system key console
Please paste your new system key, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4jAcBgoqhkiG9w0BDAEDMA4ECAKuMvSla9T4AgIBYgSCBMB/RzDgm4xpRDnA
Cd//wgD9c8junXmVpyJWXWgXhlj3Sgv3toKt2yBQY7Rv0peP1y68nuHKZcp/QZDj
QksDvIJHacpz886KQ2p9xxOCrIO3RTVNULPzrucUNuJ2a5W4IGPGwnrNLKsriRH6
CXQjRu19+kbczmPtrlHu7gj6MuCp58sIyXbsOPCnsZBaAOcf72qeKfVa4tKlpobI
e5YDg+UiJXYv1Kfj9t9tftSfaCym0jK+uE3++y5+ah/k+u/VcEb9b6DrlfG8KaJI
/OYVVmRWVIHEY2QjVOsVEXAARjpugf6cXIn8epw/CMaC0yVg4O9OGDrIz/41DVgk
/b3jlr1oWMRVASSqg0QxE2LrNNAF/XiFwpiLUCBHR0fXX9iKJM7nK6AXlf4hrd31
sMm1hICJvQwuRP+1xCHHs3qKk7oFAdyEdMiYthcOoAaynGmP4vPEMB6ZdOSxd/yN
7IfBT1U7nCtgo4FpAn4FTnkXRdlDqPpvKLqe0kkQCKo9ZWRnnIS1hAs9VJXS6zou
1IohZewrS/TWnPU+ArE/QJ4WkX2dBAe0Q2HMvuXs6J6Rfn+H2eZC+zTh0kvqA0ic
UiQAgJB0ohXWEah9BJbIYNULLpbssUySDLPrxYdZRPn5MFKqCXmWw5tAEV8mIcg4
obB6DxVGHz93iPD0XJyBGWpCdcwItzdngnMR316tX4R3jMy2U0hrzk5o01GoZQQ/
eGYsuPzm4zqVJ8S9gUMFR8ocoPWqwhU+Sq4QPCIQEGf5gwxxt9j7L2TtRbD7kxnD
23aPL/wuk45EFJKTQCeZ3kjUqCCuSbqBJXGEjiiUsahus+yJULJ8boFWu1T8zW7m
/CBK1TzY9Fh+gbdOtN4b+zWUrpk5E7ZctFhEwojVFBwgPzUIZEkap4gH+/F5d3rI
uWFBcN7QER35wO8au/k5kLKHDh+5Ul51tkJ38P1pJYFE0p5/K81YWnfvUaJmynJY
DfnK0X6Au69/F6+QR4S+bchbrqk73plIiXbkwqapQ26QH5ztIK3T6/nY6RKa7u6N
WvnskpAE1uxf+soM+BpEzpTl2gQQmEaZnh9Ci3ZnpTZE5tkAL0oTqXL9sToyeynz
Z91m+uKxYRjFvc1KPh+I8dUR0E5qXhBdRR7heIlm7/Dg+UqCUkXoyW89G14u/mJT
jB50CHxLAFOSeXnKn8G/9rOHA565r8L/z8D12sli5T1zHicZJ8O211zCSezdF+GG
mI12jfOZmNIBgCVUtpOBNX5IDbr7L+0bM6vuDmXRhnhX4f34+5HGfj3ntLAV7bmn
IOEGIhyoGFnoxyWaT0xxa6MVQJazcKSyyyhO8UixFEoKI3drpFXB0tXVb0CLFq+y
QVp9dHgO3Otzw/yCmCpbQQe8UFRYyC74wBf9yPWDtN6MW/IeEZCBoYaeMR+WyonM
mdq5xbriETXD4zha3NGAv2qnzkfkKMBcVeUULulyixMsHmNNJkINNEsj5deVYtOt
4j5EK/aZsTqTgrVq3oGlwgXM1YptvlVR+HPWZfpjwbL+7/NhmK7AhEPo+qQCVD7t
ZGRbdbB7FEN23m88IMSd8xkhS2M1pop1Cj7lP/dA+DD/dgcjP2bw7K923d4r3CcS
1yxPhLKM
-----END ENCRYPTED PRIVATE KEY-----
Enter pass phrase for /var/tmp/key.pem:
writing RSA key

ok
temp4>
```

次に、以下を使用して署名済み証明書をインポートする必要があります。

cli> store certificate sniffer [import | console]

証明書の情報が表示され、証明書を保管することを確認するよう求められます。

以下のように表示されます。

```
temp4>_store system certificate console
Please paste your new system certificate, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN CERTIFICATE-----
MIID5jCCAtCgAwIBAgIBCTALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMTUyMDUwNThaFw0xNTExMTUyMDUwNTha
MIGEMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2xvbWJpYTESMBAG
A1UEBxMJVmFuY291dmVyMQswCQYDVQQKEwJRQTESMBAGA1UECxMJUUFfU0FNUExF
MSUwIwYDVQQDExxTYW1wbGVfZ2l2ZW5DZXJ0LnZpY3RvcmlhLnFhMIIBIDALBgkq
hkiG9w0BAQEDggEPADCCAQoCggEBALdt2XhJEJIAognblgFNoiomVvcGIe9PHsOt
3fP5DxAL5PVm+UCRS0xnnCoKe3pdJNagepDwBa2K5UsHbK4vkHJEgWWEd4bx2Ks7
kRoHr83TXK+W8al1HGKRwUSwN0hfm/KV4v8ZX3AFWs2c/BJ2iA77a0mhU0JuWa1/
/scXitJB5ykPjFb2EuReA6ELphaQ/itjZIQTTeVxbamyx42ia9J5B07lFTp3qGdU
yXUwlEFX0HFPmknAAaQrSnpMdQjkOKgzxU0NTV4ILA66hCVkX+ezQeJA90s/AHA5
hAY2fyurKZsOowoE0xlEpFWCGf87zxfkmTaWthqCS0NzEcJ6efECAwEAAaNrMGkw
HwYDVR0jBBgwFoAUdEgevPLMipuAlENuyxgfX7R0WckwDAYDVR0TAQH/BAIwADAP
BgNVHQ8BAf8EBQMDB7gAMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYI
KwYBBQUHAwEwCwYJKoZIhvcNAQEFA4IBAQB+Plm22B72eRESk9rgNdOB+l48k5xw
QHf64TJcoI/Vcz0vtGBC1jDfZzVDIHJaX6ZMtdO23QO6rtjQSnhjhbOt/EiimaNO
tysJOE999E+HQ7UpKYKvdoznwpYEthyoQJ9quKqQc1YW/l8pQMYDEdK8c7yMbJpv
mrxO8h+G3YYQMT6A9KAk/GPA+yKl0fCuogBhPyWM28q35EAIw6H9ahQigWhNkzrL
DCYO8VCLi3BX+OohLvurkyzJm2lnbm7BSb5QB4jISlRBGPoIWhK6VPypboyABfVs
yWHFVs10EUb0Maa/XNZILTAoYAbYK5sX7Ri5hr5KhxnmDd9AJMQsLfik
-----END CERTIFICATE-----
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 9 (0x9)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victoria_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov 15 20:50:58 2010 GMT
            Not After : Nov 15 20:50:58 2015 GMT
        Subject: C=CA, ST=British Colombia, L=Vancouver, O=QA, OU=QA_SAMPLE, CN=Sample_givenCert.victoria.qa
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b7:6d:d9:78:49:10:92:00:a2:09:db:96:01:4d:
                    a2:2a:26:56:f7:06:21:ef:4f:1e:c3:ad:dd:f3:f9:
                    0f:10:0b:e4:f5:66:f9:40:91:4b:4c:67:9c:2a:0a:
                    7b:7a:5d:24:d6:a0:7a:90:f0:05:ad:8a:e5:4b:07:
                    6c:ae:2f:90:72:44:81:65:84:77:86:f1:d8:ab:3b:
                    01:1a:07:af:cd:d3:5c:af:96:f1:a9:75:1c:62:91:
                    c1:44:b0:37:48:5f:9b:f2:95:e2:ff:19:5f:70:05:
                    5a:cd:9c:fc:12:76:88:0e:fb:6b:49:a1:53:42:6e:
                    59:ad:7f:fe:c7:17:8a:d2:41:e7:29:0f:8c:56:f6:
                    12:e4:5e:03:a1:0b:a6:16:90:fe:2b:63:64:84:13:
                    4d:e5:71:6d:a9:b2:c7:8d:a2:6b:d2:79:07:4e:e5:
                    15:3a:77:a8:67:54:c9:75:30:94:41:57:d0:71:4f:
                    9a:49:c0:01:a4:2b:4a:7a:4c:75:08:e4:38:a8:33:
                    c5:4d:0d:4d:5e:08:2c:0e:ba:84:25:64:5f:e7:b3:
                    41:e2:40:f7:4b:3f:00:70:39:84:06:36:7f:2b:ab:
                    29:9b:0e:a3:0a:04:d3:19:44:a4:55:82:19:ff:3b:
                    cf:17:e4:99:36:96:b6:1a:82:4b:43:73:11:c2:7a:
                    79:f1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:74:48:1E:BC:F2:CC:8A:9B:80:94:43:6E:CB:18:1F:5F:B4:74:59:C9

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication, TLS Web Server Authentication
    Signature Algorithm: sha1WithRSAEncryption
        7e:3e:59:b6:d8:1e:f6:79:11:12:93:da:e0:35:d3:81:fa:5e:
        3c:93:9c:70:40:77:fa:e1:32:5c:a0:8f:d5:73:3d:2f:b4:60:
        42:d6:30:df:67:35:43:20:72:5a:5f:a6:4c:b5:d3:b6:dd:03:
        ba:ae:d8:d0:4a:78:63:85:b3:ad:fc:48:a2:99:a3:4e:b7:2b:
        09:38:4f:7d:f4:4f:87:43:b5:29:29:82:af:76:8c:e7:c2:96:
        04:b6:1c:a8:40:9f:6a:b8:aa:90:73:56:16:fe:5f:29:40:c6:
        03:11:d2:bc:73:bc:8c:6c:9a:6f:9a:bc:4e:f2:1f:86:dd:86:
        10:31:3e:80:f4:a0:24:fc:63:c0:fb:22:a5:d1:f0:ae:a2:00:
        61:3f:25:8c:db:ca:b7:e4:40:08:c3:a1:fd:6a:14:22:81:68:
        4d:93:3a:cb:0c:26:0e:f1:50:8b:8b:70:57:f8:ea:21:2e:fb:
        ab:93:2c:c9:9b:69:67:6e:6e:c1:49:be:50:07:88:c8:4a:54:
        41:18:fa:08:5a:12:ba:54:fc:a9:6e:8c:80:05:f5:6c:c9:61:
        c5:56:cd:74:11:46:f4:31:a6:bf:5c:d6:48:2d:30:28:60:06:
        d8:2b:9b:17:ed:18:b9:86:be:4a:87:19:e6:0d:df:40:24:c4:
        2c:2d:f8:a4

Do you want to store this certificate? (y/n)
y
ok
temp4>
```

新しい証明書を反映するには、inspection-core を再始動する必要があります。

x.509 証明書認証を使用するための S-TAP の構成

最初に、証明書の CA および CN として割り当てた内容を記録します。覚えていない場合は、show system certificate cli コマンドを使用して値を表示します。

Guardium システムにインストールされた証明書の CN と、Guardium システム上の証明書に署名した CA の公開鍵が必要です。Guardium システムの証明書に署名したのと同じ CA により署名された証明書取り消しリストも必要になることがありますが、ここでは必須ではありません。

guard_tap.ini 内の対象のパラメーターは、以下のように Unix と Windows で同一です。

```
; Where is the CA certificate
guardium_ca_path=NULL
; What's the CN to expect from the SqlGuard certificate?
sqlguard_cert_cn=NULL
; Path to crls file or dir
guardium_crl_path=NULL
```

UNIX と Windows の唯一の機能的な違いは、Windows では、あるパラメーターに対して値を使用しない場合、そのパラメーターを NULL に設定するのではなく、そのパラメーターを guard_tap.ini に含めません。(これは特に CRL パスに関連します。あるいは、証明書認証を中止して TLS に戻るような場合です。)

CA から送信された CA の公開鍵 (および必要な場合は CRL) を、S-TAP ホスト上のディレクトリーにコピーします。このディレクトリーを記録しておきます。

guardium_ca_path=[CA.pem のパス] を設定します。

sqlguard_cert_cn=[Guardium システムの完全 CN または部分 CN (* をワイルドカードとして使用)] を設定します。

guardium_crl_path=[crl.crl のパス] を設定します (この時点で証明書失効リストを使用したい場合のみ)。

実例は以下のようになります。

```
guardium_ca_path=/var/tmp/pki/Victoria_QA_CA.pem
sqlguard_cert_cn=sample1_qa.victoria
guardium_crl_path=/var/tmp/pki/Victoria_QA_CA.crl
```

これらのパラメーターを設定したら、tls=1 を変更し、S-TAP を再始動します。

これで Openssl を使用して接続されます。

親トピック: S-TAPs およびその他のエージェント

S-TAP® スループットの増加

複数の Guardium システムに報告する S-TAP を構成すると、データのスループットを増やすことができます。

複数のスレッドを作成するように S-TAP を構成すると、データのスループットを増やすことができます。 S-TAP 構成ファイルに複数の Guardium システムが定義されている場合、Guardium システムごとにスレッドを作成できます。 S-TAP は、Guardium システムの数に合わせて、追加のスレッドを (v10.1.4 以上で、最大 10 スレッド) 作成します。participate_in_load_balancing パラメーターが 4 に設定されていると、K-TAP は、Guardium システムの数に合わせて、ほぼ同じの数のバッファーを 5 スレッドまで作成します。K-TAP は、バッファー間を行き来して、各バッファーにパケット全体を配置します。 各 S-TAP スレッドは、異なる K-TAP バッファーから読み取りを行い、単一の Guardium システムにトラフィック・データを送信します。

この構成では、S-TAP からすべてのデータを受信する Guardium は 1 つもありません。 配布は、participate_in_load_balancing が 1 に設定されている場合に使用されるのに似ています。
重要: V10 GPU200 より前は、Guardium システムが使用不可になった場合、フェイルオーバーは行われません。Guardium システムに送信されていたデータは、システムが使用可能になるか、構成が変更されるまで失われます。
重要: V10 GPU300 より前に、S-TAP 構成ファイルに複数の Guardium システムが定義されている場合、Guardium システムごとにスレッドを作成できます。 この機能がアクティブになるのは、participate_in_load_balancing パラメーターが 4 に設定されている場合のみです。

A-TAP の暗号化されたトラフィックと暗号化されていないトラフィックを同じ Guardium システムに送信することはできません。これは、participate_in_load_balancing が 1 に設定されている場合と似ています。

親トピック: S-TAPs およびその他のエージェント

UNIX S-TAP

UNIX S-TAP® をインストールして構成します。

UNIX S-TAP は、Guardium システムにデータを送信して分析およびロギングを行うために、さまざまなソースからデータを収集するユーザー・スペース・デーモンです。KTAP (カーネルでインターセプトを実行するカーネル・モジュール)、ATAP (データベースでのトラフィック収集の開始時にロードされるユーザー・スペース·ライブラリー)、および EXIT ライブラリーからトラフィックを収集し、トラフィックをデータベース・サーバーから S-TAP に直接送信します。

v10.1.4 UNIX S-TAP の変更

- データベース・サーバーからのモジュールおよび診断のアップロードの専用アップロード・ディレクトリー
  - シェル・インストール – guardium/guard_stap/.upload
  - GIM インストール – modules/STAP/current/.upload
- ATAP は、セッションが開かれたときに適切なグループ・メンバーシップがないプロセスについての警告を S-TAP ログ内に生成します。
- guardctl の変更
  - save-active-ataps - 現在アクティブ化されている各 ATAP の構成を etc/guard/saved_ataps に保存します。
  - restore-saved-ataps - etc/guard/saved_ataps に保存されている ATAP を、保管済みかつアクティブな状態に復元します。
  - guardctl コマンドによって A-TAP がアクティブ化および非アクティブ化されるときに、repair コマンドが必要であると guardctl ユーティリティーによって評価された場合、repair コマンドが自動的に実行されます。
- guard-config-update は現在、GIM 環境および追加のオプションをサポートしています。
- guard_monitor の変更
  - システム全体またはシングル・プロセッサーをベースとした構成可能な CPU 測定 (cpu_measurement_mode)
  - 強制されたコア生成のクリーナー・ユース・ケース (force_core_when)

V10 の新機能および拡張機能

64 ビット STAP

- 64 ビット・プラットフォーム用の S-TAP バイナリーが、64 ビット・バイナリーとしてビルドされるようになりました。
- S-TAP がバッファーに対してマップできるデータ量が増加しました。
- 符号付き 32 ビット整数の最大値 – およそ 2GB (sqlguard_ip ごとの割り当て量)。

64 ビットのセッション鍵

- トラフィック損失の原因となる鍵の競合が発生する可能性が低下しました。
- 副次作用は、V-10 S-TAP は V10 Guardium システムにしか接続できないことです。

高速 SHMEM 判定

- デフォルトでオンになっています。

- 高速 SHMEM 判定には、パラメーター名 ktap_fast_shmem を使用します。
- Db2 についての必要な情報をカーネルにプッシュにして、セグメントがデータベースに属しているかどうかを判別します。
- 検査エンジン構成に変更はありません。
- db2_shmem_size、db2_shmem_client_position、db2_fix_pack_adjustment、および db_exec_file 内の実行可能ファイルの dev/ino をプッシュします。
- デバッグが困難になる可能性があるため、SHMEM トラフィックのインターセプトで問題が発生した場合、無効化することをお勧めします。
- KTAP Informix では、トラフィックのキャプチャーが改善され、セグメントに関する制限が解除されました。

デフォルトの高速 TCP 判断

- デフォルトでオンになっています。
- Network/Exclude_Network パラメーターが高速判断でサポートされます。
- Network/Exclude_Network では、それぞれ最大 20 個のエントリーを指定できる検査エンジンが 20 個までサポートされています。これを超えると、機能を問題なく低下させて、fast_verdict をオフにします。fast_tcp_verdict がオンになっていて、TCP トラフィックをインターセプトするよう構成された検査エンジン、ネットワーク・マスク、または除外ネットワーク・マスクがサポートされる最大数の 20 個を超えると、fast_tcp_verdict が無効になります。

注: 環境が複雑で多様性があるために、注意事項をよく読み、注意事項に従う必要があります。そうでないと、インストールやアップグレードが失敗したり正しく動作しないことがあります。以下のセクションは、特別に注意する必要がある分野を読者にピンポイントで示すために、リストされています。すべての注は含まれていませんが、これらの一部の注を簡単に見つけることができます。

- K-TAP の非ライブ・アップグレードとライブ・アップグレード (Solaris、AIX®、HP-UX)
- UID チェーン (Solaris Zones、AIX WPAR、Solaris 8/9、Solaris 11 SPARC)
- S-TAP を UNIX ホストにインストールする前に (Solaris Zones)
- GIM による UNIX S-TAP の保守 (IBM® DB2® pureScale®)
- UNIX S-TAP のインストール (Linux、AIX)
- アップグレード手順ユーティリティー (SUSE 11、HP-UX)
- 前の UNIX S-TAP の削除 (手動) (HP-UX、AIX WPAR)

さまざまな OS タイプ/バージョンによる S-TAP/GIM プロセスの初期設定の方法

表 1. さまざまな OS による S-TAP および GIM の初期プロセス

OS	バージョン		初期化方式
AIX	6.1	PowerPC	inittab
AIX	7.1	PowerPC	inittab
AIX	7.2	PowerPC	inittab
HP-UX	11.11	pa9000	inittab
HP-UX	11.23	IA-64	inittab
HP-UX	11.23	pa9000	inittab
HP-UX	11.31	IA-64	inittab
HP-UX	11.31	pa9000	inittab
RHEL	4	i686	inittab
RHEL	4	IA-64	inittab
RHEL	4	x86_64	inittab
RHEL	5	i686	inittab
RHEL	5	IA-64	inittab
RHEL	5	ppc64	inittab
RHEL	5	s390x	inittab
RHEL	5	x86_64	inittab
RHEL	6	i686	inittab
RHEL	6	ppc64	inittab
RHEL	6	s390x	inittab
RHEL	6	x86_64	inittab
RHEL	7	ppc64le	systemd
RHEL	7	ppc64	systemd
RHEL	7	s390x	systemd
RHEL	7	x86_64	systemd
SUSE	11	i686	inittab
SUSE	11	ppc64	inittab
SUSE	11	s390x	inittab

OS	バージョン		初期化方式
SUSE	11	x86_64	inittab
SUSE	12	ppc64le	systemd
SUSE	12	s390x	systemd
SUSE	12	x86_64	systemd
Ubuntu	10.04	x86_64	inittab
Ubuntu	12.04	x86_64	upstart
Ubuntu	14.04	x86_64	upstart
Ubuntu	16.04	x86_64	systemd
Solaris	5.10	i386	サービス
Solaris	5.10	i386_64	サービス
Solaris	5.10	SPARC	サービス
Solaris	5.11	i386_64	サービス
Solaris	5.11	SPARC	サービス

これは、Guardium の全バージョンに対応する一般的な表です。システム要件/サポート対象プラットフォームの資料を参照して、特定のプラットフォームがご使用の Guardium バージョンのサポート対象かどうかを確認してください。

注意

Upstart サーバー

Upstart サーバーの使用時、データベース・サーバーで使用する start コマンドと stop コマンドは以下のとおりです。

S-TAP プロセスを停止する場合:

stop utap

S-TAP プロセスを開始する場合:

start utap

GIM と監視プログラムのプロセスを停止する場合:

stop gim_revision#

stop gsvr_revision#

例： stop gim_46743

GIM と監視プログラムのプロセスを開始する場合:

start gim_revision#

start gsvr_revision#

例: start gim_46743

システムの Guardium 製品の状況を確認する場合:

initctl list

status utap

Systemd サーバー

systemd サーバーの使用時、データベース・サーバーで使用するコマンドは以下のとおりです。

S-TAP プロセスを停止する場合:

systemctl stop guard_utap.service

S-TAP プロセスを開始する場合:

systemctl start guard_utap.service

GIM と監視プログラムのプロセスを停止する場合:

systemctl stop guard_gim.service

systemctl stop guard_gsvr.service

GIM と監視プログラムのプロセスを開始する場合:

systemctl start guard_gim.service

systemctl start guard_gsvr.service

システムの Guardium 製品の状況を確認する場合:

systemctl -t service -a|grep guard

Services サーバー

services サーバーの使用時、データベース・サーバーで使用するコマンドは以下のとおりです。

S-TAP プロセスを停止する場合:

svcadm -v disable guard_utap

S-TAP プロセスを開始する場合:

svcadm –v enable guard_utap

GIM と監視プログラムのプロセスを停止する場合:

svcadm –v disable guard_gim

svcadm –v disable guard_gsvr

GIM と監視プログラムのプロセスを開始する場合:

svcadm –v enable guard_gim

svcadm –v enable guard_gsvr

サーバーの Guardium 製品の状況を確認する場合:

svcs | grep guard

参照

RHEL 7 で S-TAP を実行している場合、Flash Alert (http://www.ibm.com/support/docview.wss?uid=swg21977093) を参照してください。

Guardium V10.0 システム要件 (サポート対象プラットフォーム) (2015 年 10 月)

64 ビット

http://www-01.ibm.com/support/docview.wss?uid=swg27045976

V9.5 システム要件 (サポート対象プラットフォーム) (2015 年 3 月)

32 ビットおよび 64 ビット

http://www-01.ibm.com/support/docview.wss?&uid=swg27045286

RemoveIPC=yes が systemd 用に構成されている場合はデータベース・インストールと操作が失敗する

RedHat Enterprise Linux 7 の場合、 init が systemd によって置き換えられているため、処理を終了するとシステム・ユーザー以外を IPC からクリーンアップしようとします。これは、Db2 の共有メモリー・セグメントを削除するため、Db2 とディスカバリーに問題が発生します。この問題を解決するには、「RemoveIPC=no」を /etc/systemd/logind.conf に設定し、システムをリブートしてください。Oracle も、データベースを正しく操作するためにこの設定が必要であることを文書化しています。 「Database Installation and Operation Fails if RemoveIPC=yes Is Configured for systemd (RemoveIPC=yes が systemd 用に構成されている場合はデータベース・インストールと操作が失敗する)」を検索してください。

Sybase 15 SSL 暗号化スクリプト

Sybase 15 の SSL 暗号化トラフィック・インターセプトは、以下のプラットフォームでサポートされています。

- Linux: サポートされるすべてのディストリビューションおよびバージョン
- Solaris 8、9、10 (SPARC のみ)
- AIX 5.3 (LDR_PRELOAD パッチ適用)
- HPUX 11.00、11.11、11.23 および 11.31 (PARISC のみ)

guardctl 起動メソッドと GUI ベースの起動メソッドの両方がサポートされています。 GUI ベースのメソッドを使用する場合は、起動の前に Sybase OS ユーザーを Guardium グループに追加する必要があります。 Sybase 検査エンジン定義では、DB 実行可能ファイル・パス・パラメーター (guard_tap.ini 内の db_exec_path) を指定する必要がありますが、その中には、Sybase 実行可能ファイル (dataserv) への絶対パスが含まれている必要があります。

Guardium Linux S-TAP インストールの KTAP ローダー・シーケンス

KTAP ローダー・メカニズムは、Linux S-TAP のインストール (GIM および GIM 以外を使用) で以下のシーケンスを使用します。

注: KTAP ローダー・メカニズムは前のステップが成功しなかった場合、次のステップに自動的に進みます。

1. KTAP ローダーは、オペレーティング・システム・レベルに完全に一致するカーネル・モジュールを見つけ、それをロードします。
2. KTAP ローダーは、テストされた互換性のあるカーネル・モジュールが ktap-combos.txt ファイル・リスト (KTAP_List_of_Modules) にあるかどうかをチェックし、それをロードします。
3. KTAP ローダーは KTAP モジュールをローカルにコンパイルし、それをロードします。 KTAP は、システムに必要なパッケージ (ブートされたカーネルの場合は gcc および kernel-devel) がインストールされている場合にのみ、システム上でコンパイルされます 。
4. FlexLoad メカニズムがオンの場合、KTAP ローダーは最も一致率が高いカーネル・モジュールを検索し、それをロードします。

   FlexLoad メカニズムをオンにするには、以下のフラグを使用します。

シェル・インストールの場合、以下のオプションを使用します "--ktap_allow_module_combos"

GIM インストールの場合、以下のオプションを使用します: "KTAP_ALLOW_MODULE_COMBOS=Y"

5. KTAP ローダーは「ロードに失敗しました」メッセージを生成し、KTAP なしで S-TAP をインストールします (そうしないと S-TAP インストールは失敗します)

注: KTAP パラメーター・トピックの CUSTOM BUNDLES に関する情報を参照してください。

UNIX S-TAP のモニター・メカニズム

UNIX S-TAP は、インストールと構成の方法に応じて、さまざまなメカニズムを使用してトラフィックを収集します。トラフィックは、使用されるメカニズムとは関係なくフィルターされ、特定のクライアントとサーバー IP アドレスのセットに対応するデータベース関連トラフィックのみが収集されます。

K-TAP

K-TAP は、オペレーティング・システムにインストールされるカーネル・モジュールです。インストール後、構成ファイル設定を使用して、使用可能にしたり使用不可にしたりすることができます。使用可能に設定された場合、これは、データベース・クライアントとデータベース・サーバーとの間の通信に使用するメカニズムをフックすることにより、データベース・サーバーへのアクセスを監視します。 K-TAP を無効にした場合に、Tee をローカル・トラフィックのモニターに使用することができます。K-TAP と Tee は、ほとんどの場合相互に排他的であるため、ローカル・アクセスをモニターするには、K-TAP または Tee のいずれかを使用します。K-TAP では、データベース・クライアントのサーバーとの接続方法を変更する必要はありません。

インストール時に、サーバーのオペレーティング・システムに K-TAP カーネル・モジュールをロードするかどうかを選択します。これは、そのモジュールをロードする唯一の方法です。 最初に K-TAP をロードせずに、後で K-TAP を使用することにした場合は、S-TAP を削除してから、再インストールする必要があります。
注: インストール中に K-TAP のロードが適切に行われなかった場合、ハードウェアまたはソフトウェアの互換性が原因である可能性があります。デフォルトの収集メカニズムとして Tee がインストールされます。互換性の問題が解決した後に再び K-TAP に切り替えるには、『Tee から K-TAP への切り替え』に概説されている手順に従ってください。
注: セッション内トラフィックは、コールバックを使用することで古い KTAP から新規 KTAP に転送されます。つまり、ほとんどのデータベースでは、既存のセッションに対する新しい KTAP を使用したインターセプトが再開されるまでに、2 つの SQL 要求を受け取ることができます。Sybase IOCP の場合は、セッションの性質上、3 つの SQL 要求を受け取ります。

A-TAP

A-TAP (application-level tapping) メカニズムにより、データベース・サーバーの内部コンポーネント間の通信がモニターされます。それは、例えば DBMS が独自の暗号化を使用すること、またはその他の内部的なデータベース実装の詳細が原因で、データベース・サーバーのアプリケーション・レベルでのみタップできるトラフィックに使用されます。 A-TAP は K-TAP を S-TAP にデータを渡すためのプロキシーとして使用し、モニター対象のデータベース・インスタンスごとに別個に構成する必要があります。

A-TAP は、以下のタイプのトラフィックをモニターするために使用されます。

- AIX、HPUX、Solaris および Linux 上の Oracle (バージョン 9、10、11、12c) 向け ASO 暗号化トラフィック
- Linux、AIX、Solaris および HPUX (LD_PRELOAD をサポートするプラットフォーム) 上の Oracle (バージョン 10、11、12c) 向け SSL 暗号化トラフィック
- AIX (LDR_PRELOAD パッチ適用の AIX 5.3 以降のみ)、Solaris (SPARC)、および Linux (32 ビット) 上の Sybase (バージョン 15) 向け SSL 暗号化トラフィック
- Linux

上の DB2 および Informix® 向け共有メモリー・トラフィック

PCAP

PCAP は、あるデータベース・サーバーに出入りするネットワーク・トラフィックを listen するパケット取り込みメカニズムです。UNIX 環境では、K-TAP がすべてのネットワーク・トラフィックを取り込むので、PCAP が使用されることはまれです。Windows 環境では、非暗号化ネットワーク・トラフィックの取り込みに PCAP が使用されます (IA64 を除く)。また、Linux では、lo デバイスでのローカル TCP/IP トラフィックの取り込みに PCAP が使用されます。

Solaris Zones 環境で PCAP を使用するには、Solaris マシン上の guard_tap.ini ファイルの alternate_ips パラメーターに、モニターするすべてのゾーンの IP アドレスを追加する必要があります。

ヒント: PCAP は、すべてのローカル検査エンジンのためのクライアント IP/マスク値を使用して、モニターおよびレポートの対象を判別します。 PCAP が、複数の検査エンジンを持つ S-TAP と共にインストールされ、これらの検査エンジンのクライアント IP/マスクの値がそれぞれ異なっている場合、PCAP はこれらすべての検査エンジンに定義されたすべてのクライアントからトラフィックを収集します。 これにより、意図したよりも多くの情報が処理され、Guardium システムに送信される結果となる場合があります。

Tee

Tee は、ローカル・クライアントからトラフィックを読み取り、データベース・サーバーへ転送するプロキシー・メカニズムです。 Tee は、データベース・トラフィックを受け取ると、データベース・サーバーにコピーを 1 つ、S-TAP にコピーを 1 つ、それぞれ転送します。 Tee を使用する場合、データベース・クライアントは、データベース聴取ポートではなく、Tee 聴取ポートに接続する必要があります。 つまり、データベース・クライアントがサーバーに接続する方法を変更するか、データベース・サーバーがクライアント接続を受け入れる方法を変更する必要があります。 いずれの場合も、これは通常、1 つまたは 2 つのファイルに対するマイナーな構成変更 (データベース・タイプによって異なります) であり、最終的な結果は、クライアントにとっては Tee がデータベースになり、データベースにとっては Tee がクライアントになります。 これらはすべて、クライアントとサーバーのいずれにも認識されませんが、Tee を介して確実に接続するためには、構成変更が必要です。 Tee を使用する場合、データベース・クライアントは、(Tee 聴取ポートではなく) データベース聴取ポートに接続するか、あるいは、データベース・タイプに応じて、名前付きパイプ、共有メモリー、またはその他のプロセス間接続メカニズムを使用することにより、Tee をバイパスできます。 Tee に接続するためのクライアントの構成について詳しくは、『ローカル・クライアントで Tee を使用するための準備』を参照してください。

Tee 聴取ポートを介さない接続は、不正な接続と呼ばれます。Tee を使用する場合は、ハンターと呼ばれるオプションのコンポーネントを使用可能にして、不正接続に対する監視や報告を行い、オプションでそのような接続を無効にすることができます。 ハンターはランダムな間隔で実行されるので、そのような接続がすべて検出されるわけではありません。 また、不正接続について報告し、オプションでそれらを無効にすることはできますが、これらの接続で実行されたアクションを監査することはできません。 ハンターの別の側面として、不正接続の検出を開始したときに、CPU 集中的となる可能性があります。 したがって、その時点でハンター・プロセスを見ると、サーバーの CPU リソースが大量に消費されている場合があります。 (CPU の使用量は、メモリー・スパイクが発生した後、素早く低下します。)
注: ハンターを使用するには、Perl バージョン 5.8.0 以降が /usr/bin/ ディレクトリーにインストールされていなければなりません。
注: Solaris 11 のみ - Tee が最初にインストールされなかった場合は、再インストールが必要です。または、手動で TEE をインストールする必要があります。

K-TAP のアップグレード - ライブと非ライブ

K-TAP アップグレードでは、必須パラメーター KTAP_LIVE_UPDATE の使用により、ライブでリブート不要なアップグレードがサポートされています。このパラメーターは、毎回アップグレード中に設定する必要がありますが、GUI または BUNDLE-STAP/KTAP インストーラーによって制御します。

- GIM またはシェル・インストーラーを介してライブ・アップデートを実行する前に、K-TAP デバイスを使用中のプロセスがないことを確認する必要があります。S-TAP を停止し、A-Tap を非アクティブにする必要があります。 fuser /dev/ktap_xxx または lsof | grep ktap_xxx (ここで、xxx は古いバージョン番号) を実行し、デバイスを開いているプロセスがあるかどうかを確認します。 これを実行しないと、予期しない動作になる可能性があります。
- アップグレードするたびに、GUI から新規 K-TAP パラメーター KTAP_LIVE_UPDATE が初期化 (ブランク) されます。その他すべての必須の未初期化パラメーターと同様に、このパラメーターは、アップグレード・プロセスを続行する前に設定する必要があります。
  新規パラメーターの有効な値は以下のとおりです。
  - Y/y - ライブ (リブート不要の) K-TAP アップグレード
  - N/n - K-TAP 非ライブ・アップグレード (アップグレードを完了するためにシステムのリブートが必要です)
- DB サーバー上で直接 KTAP/BUNDLE-STAP インストーラーを実行して K-TAP をアップグレードする場合。この新規フィーチャーにより、インストーラーのコマンド行に新規引数の指定が必要になります。引数名は --live_update [Y|N] です。
- K-TAP ライブ・アップグレードの後は、以下のようになります。
  - K-TAP をアップグレードした後の既存のセッションに対する最初の SQL は、取り込まれません。
  - Solaris ローカル・ゾーンでの既存の ATAP セッションは、ログに記録されません。
  - 一部のプロセスでは、引き続き古い K-TAP モジュール内のメモリーが参照される可能性があります。このシナリオでは、将来不安定にならないように、モジュールはリソースを解放しません。 このような場合、ユーザーは、それらのリソースが使用されなくなった後で、guard_ktap_cleanup (ktap ディレクトリーにあります) を実行して、手動でクリーンアップする必要があります。
  - HP-UX 11.11 では、古い K-TAP モジュールはインストールされなくなりますが、kmadmin -s | grep tap を実行したときに、引き続き登録済みとして表示されます。このモジュールは、kmmodreg -U ktap_<version> を使用して手動で登録抹消する必要があります。
  - Solaris および AIX では、リブート後に古いデバイス・ノードが自動的に削除されないので、それらを手動で削除する必要があります。

例外:

- GIM を介してインストールされなかったバージョンの DB サーバーがインストールされていて、その非 GIM K-TAP のバージョンが、インストールされる K-TAP のバージョンと同じではない場合、KTAP_LIVE_UPDATE の値は無視されます。これは、非 GIM バージョンからのアップグレードではシステム・リブートが必要であるためです。
- スクラッチ・インストールでは、KTAP_LIVE_UPDATE の値は無視されます。
- システムを、非 GIM バージョンから同じ GIM バージョンにアップグレードする場合、システムをリブートする必要はありません。
- マシンをリブートせずに、前にインストールした K-Tap バージョンを再インストールすることはできません。

エラー処理:

- 障害が発生した場合、障害によっては、完全なリカバリーのためにシステムのリブートが必要になるため、「GIM イベント・リスト」レポートを確認することが極めて重要です。

注: ODMDIR 環境が定義されていない場合、S-TAP のインストールまたはアップグレード時に AIX 用の K-TAP のみがロードに失敗します。ODMDIR とは、オブジェクト・データ・マネージャー・ディレクトリーを指します。ODM は、OS に統合されるシステムおよびデバイスの構成情報が含まれるデータベースです。これは、システム情報、ソフトウェア情報、およびデバイス情報を格納するためのものです。 すべての ODM コマンドでは、/etc/environment ファイルに設定されている ODMDIR 環境変数が使用されます。ODMDIR のデフォルトの値は /etc/objrepos です。

ディスカバリー・エージェント

Guardium のディスカバリー・エージェントは、データベース・サーバー・システムに S-TAP パッケージにより自動的にインストールされるソフトウェア・エージェントです。 これは、データベース・サーバー上で実行されているデータベース・インスタンスを検出し、検出結果を Guardium システムに報告するためのものです。ディスカバリー・エージェントが機能するには、データベース・サーバー上にあるディスカバー対象のすべてのデータベースを開始する必要があります。

注: Solaris ゾーン・アーキテクチャーでは、DB2 インスタンスがスレーブ・ゾーンで実行されている場合、ディスカバリーは DB2 共有メモリー・パラメーターをディスカバーしません。

新たにディスカバーされたデータベースは「ディスカバーされたインスタンス」レポートで確認できます。 このレポートから、GuardAPI 入力生成ツールを使用して、データ・ソースと検査エンジンへの追加が簡単にできます。

データベース・サーバー上でデータベースが稼働 (開始) していない場合、または後で追加される場合も、そのデータベース・サーバー上でディスカバリー・エージェントがサイクル (使用不可に設定されてから使用可能に設定される) されると、ディスカバリー・エージェントからこれらのインスタンスをディスカバーできます。 インストール済みのモジュール・パラメーターの変更の詳細については、GIM ユーザー・インターフェース を参照してください。そのためには、ディスカバリー・エージェントで discovery_enabled パラメーターを 2 (使用不可) に変更してから 1 (使用可能) に戻して、正しくサイクルさせる必要があります
注: ディスカバリー・エージェントはその検出結果の報告を、GIM_URL または 2 次 S-TAP ターゲットとしてリストされたシステムにではなく、1 次 S-TAP ターゲットに戻します。

GIM による Unix S-TAP の保守

自動的で簡単なインストール機能を持つ Guardium® Installation Manager (GIM) は、Unix 環境における S-TAP および CAS などの Guardium モジュールの基本的なインストール方式です。 データベース・サーバーへの GIM クライアントの単純なウィザード駆動型インストールを行った後で、Guardium システム (GIM サーバー) から、モジュールのインストールを簡単にスケジュールすることができます。

Windows 環境で Guardium コンポーネントをインストールするために GIM をインストールして使用する方法について詳しくは、『データベース・サーバー (UNIX) への GIM のインストール』および『Guardium Installation Manager (GIM) - GUI』を参照してください。
注: A-Tap が使用されている場合、GIM ベースでの S-TAP のアップグレードまたはアンインストールを実行する前に、データベース・サーバーで最初に A-Tap を無効にする必要があります。
注: IBM DB2 pureScale 環境では、S-TAP が確実に開始されるようにするため、リブート中に Perl にアクセス可能にしておく必要があります。

GIM を使用しない UNIX S-TAP の保守

GIM を使用しない Unix S-TAP の保守

Guardium コンポーネントのインストールと管理を容易にするために GIM が提供されていますが、一方で、手動によるアプローチや、より詳細なレベルでのインストールの微調整が有効な環境もあります。手動によるアプローチを活用したり、より低い細分性レベルでのインストールの微調整が必要な環境もあります。 以下のセクション

で、そのような環境について説明します。

- Unix S-TAP のインストール
- コマンド行からの S-TAP のインストール
- コマンド行からの CAS のインストール
- アップグレード手順ユーティリティー
- 前の Unix S-TAP の削除 (手動)
- K-Tap のコマンド行更新 (手動)
- Unix S-TAP の停止
- Unix S-TAP の再始動
- Unix S-TAP のバージョン番号の判別
- Unix S-TAP ネイティブ・インストーラーの使用

Unix S-TAP の停止

S-TAP は、S-TAP のインストール方式に応じて、以下の方法で停止できます。

GIM のインストール

GIM を使用すると、データベース・サーバーにログインしなくても S-TAP を停止できます。 以下のステップを完了して STAP_ENABLED パラメーターを変更し、データベース・サーバーでの変更をスケジュールに入れます。

1. 「管理」 > 「インストール管理」 > 「クライアント別の設定 (レガシー)」をクリックして、「クライアント検索条件」を開きます。
2. 登録済みクライアントに対するフィルター検索を実行するか、「検索」をクリックしてすべての登録済みクライアントを表示します。
3. アクション (S-TAP の停止) の対象となるクライアントを選択します
   - クライアント数が 20 を超える場合には、クライアントのリストは追加ページに分けられます。
     注: 「すべて選択」ボタンをクリックした場合に選択されるのは、表示されている現行ページ上のクライアントのみです。
4. 「次へ」をクリックして、「共通モジュール」パネルを開きます。
5. S-TAP 用のモジュールを選択します。
6. 「次へ」ボタンをクリックして、「モジュール・パラメーター」パネルを開きます。
7. アクション (S-TAP の停止) の対象となるクライアントを選択します。
8. STAP_ENABLED パラメーターを 0 (ゼロ) に変更します。
9. 「クライアントに適用」をクリックして、対象となるクライアントに適用します。
10. 「インストール/更新」 ボタンをクリックして、対象となるクライアントに対する更新をスケジュールに入れます。この更新は、今すぐスケジュールに入れることも、後からスケジュールに入れることもできます。

データベースのホスト上で、stop gsvr_<release number> コマンドを使用して GIM の監視プログラム・サービスを停止することによって、S-TAP (および GIM そのものを除く、他のすべての GIM モジュール) を停止することができます。 サービスの状況のリストを取得するには、initctl list を使用します。

GIM 以外のインストール

1. root アカウントを使用して、データベース・サーバー・システムにログオンします。
2. Red Hat Enterprise Linux 6 以外のすべての場合
   a. /etc/inittab ファイルを編集用に開きます。
   b. /etc/inittab ファイル内で次の 2 つのステートメントを探し、各ステートメントの先頭にコメント文字 (AIX の場合は :、その他の場合は #) を挿入して、この 2 つのステートメントをコメント化します。

      ```
      utap:2345:respawn:/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
      ```

   c. オプション。TEE モニター・メカニズムを使用している場合は、各ステートメントの先頭にコメント文字 (AIX の場合はコロン : 、その他すべての場合はポンド記号 #) を挿入して、以下の 2 つのステートメントをコメント化します。
      注: これらのプロセスはデフォルト構成では使用されないため、ステートメントがすでにコメント化されている場合があります。

      ```
      #utee:2345:respawn:/usr/local/guardium/guard_stap/guard_tee /usr/local/guardium/guard_stap/guard_tap.ini
      #hsof:2345:respawn:/usr/local/guardium/guard_stap/guard_hnt
      ```

   d. init q コマンドを実行して、S-TAP プロセスを再開します。
3. Red Hat Enterprise Linux 6 の場合
   a. オペレーティング・システム・コマンド initctl list を使用して、現在実行中のエージェントをリストします。出力に、エージェントが次の例のように示されます。

      ```
      gim_33264 start/running, process 910
      gsvr_33264 start/running, process 2552
      ```

   b. 実行している可能性がある各エージェントを stop <agent> コマンドを使用して停止します。ここで、agent は、ステップ 3a の出力のリストにある先頭の項目です。

      ```
      stop gim_33264
      stop gsvr_33264
      stop guard_utap
      ```

      stop guard_utap を使用して S-TAP を停止するか、stop guard_tee を使用して S-TAP エージェントの TEE メカニズムを停止します。
4. ps -ef | grep stap を実行して、S-TAP プロセスが停止したことを確認します。
5. この S-TAP の報告先となっていた Guardiumシステムの管理者ポータルから、S-TAP 制御パネルの状況ライトが現在赤になっていることを確認します。

Unix S-TAP の再始動

S-TAP は、S-TAP のインストール方式に応じて、以下の方法で再始動できます。

GIM のインストール

GIM を使用して、データベース・サーバーにログインしなくても S-TAP を開始します。 以下のステップを完了して STAP_ENABLED パラメーターを変更し、データベース・サーバーでの変更をスケジュールに入れます。

1. 「管理」 > 「インストール管理」 > 「クライアント別の設定 (レガシー)」をクリックして、「クライアント検索条件」を開きます。
2. 登録済みクライアントに対するフィルター検索を実行するか、または「検索」をクリックして、すべての登録済みクライアントに対してフィルタリングされない検索を実行します。
3. アクション (S-TAP の開始) の対象となるクライアントを選択します
   - クライアント数が 20 を超える場合には、クライアントのリストは追加ページに分けられます。
     注:「すべて選択」をクリックした場合に選択されるのは、表示されている現行ページ上のクライアントのみです。
4. 「次へ」をクリックして、「共通モジュール」パネルを開きます。
5. S-TAP 用のモジュールを選択します。
6. 「次へ」をクリックして、「モジュール・パラメーター」パネルを開きます。
7. アクション (S-TAP の開始) の対象となるクライアントを選択します。
8. STAP_ENABLED パラメーターを 1 に変更します。
9. 「クライアントに適用」をクリックして、対象となるクライアントに適用します。
10. 「インストール/更新」 をクリックして、対象となるクライアントに対する更新をスケジュールに入れます。この更新は、今すぐスケジュールに入れることも、後からスケジュールに入れることもできます。

GIM 以外のインストール

1. root アカウントを使用して、データベース・サーバー・システムにログオンします。
2. Red Hat Enterprise Linux 6 以外のすべての場合
   a. /etc/inittab ファイルを編集用に開きます。
   b. 各行の先頭のコメント文字 (AIX の場合は :、その他すべての場合は #) を削除して、以下の 2 つのステートメントをアンコメントします。

   ```
   #utap:2345:respawn:/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
   ```

   c. オプション。TEE モニター・メカニズムを使用している場合は、各行の先頭にコメント文字 (AIX の場合は : 、その他すべての場合は #) を削除して、以下の 2 つのステートメントのコメントを外します。
   注: これらのプロセスは、デフォルト構成では使用されません。また、K-Tap モニター・メカニズムを使用している場合は開始してはなりません。

   ```
   #utee:2345:respawn:/usr/local/guardium/guard_stap/guard_tee /usr/local/guardium/guard_stap/guard_tap.ini
   #hsof:2345:respawn:/usr/local/guardium/guard_stap/guard_hnt
   ```

   d. init q コマンドを実行して、S-TAP プロセスを再開します。
3. Red Hat Enterprise Linux 6 の場合
   a. オペレーティング・システム・コマンド initctl list を使用して、現在実行中のエージェントをリストします。出力に、エージェントが次の例のように示されます。

   ```
   gim_33264 start/running, process 910
   gsvr_33264 start/running, process 2552
   ```

   b. 各エージェントを、start <agent> コマンドを使用して開始します。ここで、agent は ステップ a のリストにある先頭の項目です。以下の例を参照してください。

   ```
   start gim_33264
   start gsvr_33264
   start guard_utap
   ```

4. ps -ef | grep stap を実行して、S-TAP が実行されていることを確認します。
5. この S-TAP の報告先となっている Guardiumシステムの管理者ポータルから、S-TAP 制御パネルの状況ライトが緑になっていることを確認します。

Solaris 10 および 11 の Solaris サービスを使用して S-TAP を停止し、再始動します。

Solaris 10 および 11 では、inittab は使用されなくなりました。その代わりに、S-TAP の停止と開始には Solaris サービスが使用されます。svcadm ユーティリティーを使用します。

停止

```
-bash-3.00# svcadm -v disable guard_utap
svc:/site/guard_utap:default disabled.
-bash-3.00# ps -eaf | grep stap
    root  2375  1930   0 14:25:36 pts/2       0:00 grep stap
```

再始動

```
-bash-3.00# svcadm -v enable guard_utap
svc:/site/guard_utap:default enabled.
-bash-3.00# ps -eaf | grep stap
 root  2379     1   0 14:25:57 ?           0:00
/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_
    root  2396  1930   0 14:26:00 pts/2       0:00 grep stap
-bash-3.00# svcs guard_utap
STATE          STIME    FMRI
online         14:25:56 svc:/site/guard_utap:default
-bash-3.00#
```

UNIX S-TAP 用 Kerberos プラグイン

Kerberos はネットワーク認証プロトコルです。このプロトコルは、秘密鍵暗号方式を使用することでクライアント/サーバー・アプリケーションに対して強力な認証を提供するように設計されています。

Kerberos には以下の特性があります。

- パスワードは暗号化されない限り送信されないため、安全です。

- セッションごとに必要なログインは 1 回だけです。ログイン時に定義された資格情報は、追加のログインを必要とせずにリソース間で渡されます。
- 概念は、信頼のおける第三者機関である鍵配布センター (KDC) に依存します。KDC は、ネットワーク内のすべてのシステムを認識しており、それらすべてのシステムによって信頼されています。
- 相互認証を実行します。つまり、クライアントはその ID をサーバーに証明し、サーバーはその ID をクライアントに証明します。

Kerberos 認証済みユーザーをキャプチャーするには、UNIX-S-TAP が必要です。Guardium には、S-TAP の一部となった Kerberos プラグインが組み込まれるようになりました。このプラグインには、追加の構成が必要です。

ユーザーは、システム上で Kerberos ライブラリーを見つける必要があります。必要なライブラリーは、通常は以下のとおりです。

libgssapi_krb5.so

libkrb5.so

libk5crypto.so

libkrbsupport.so

これらのライブラリーはすべて、標準ライブラリー・パスになければなりません。何らかの理由によりない場合には、シンボリック・リンクを作成することをお勧めします。それができない場合は、回避策が用意されているため後述します。

1. STAP Kerberos プラグインはデフォルトで有効になっていないため、ユーザーが STAP 構成ファイル「guard_tap.ini」の「kerberos_plugin_dir」に値を指定することで有効にする必要があります。

   例えば、S-TAP シェル・インストール済み環境の場合は kerberos_plugin_dir=<guardium_base>/guard_stap、または GIM インストール済み環境の場合は kerberos_plugin_dir=<guardium_base>/modules/STAP/current です。

2. 次のステップは、「guardkerbplugin.conf」ファイル内のパラメーターを構成することです。このファイルも S-TAP インストール・ディレクトリーにあります。

   KRB5_KTNAME=<kerberos krb5.keytab ファイルへのパス>

   KRB5_CONFIG=<kerberos krb5.conf ファイルへのパス>

   KRB5_PLUGIN_CCACHE=<kerberos krb5cc_* ファイルへのパス> Kerberos プラグインが何らかの理由でユーザーを認識しなかった場合の代替メソッドのオプション・パラメーター

   Oracle Kerberos の場合、これらの値は「sqlnet.ora」ファイルで見つかります

   例:

   ~]$ grep -i KERBEROS $ORACLE_HOME/network/admin/sqlnet.ora

   SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle

   SQLNET.KERBEROS5_CONF = /home/oracle11/krb5/krb5.conf

   SQLNET.KERBEROS5_REALMS = /home/oracle11/krb5/krb.realms

   SQLNET.AUTHENTICATION_SERVICES= (BEQ,KERBEROS5)

   SQLNET.KERBEROS5_CLOCKSKEW = 600

   SQLNET.KERBEROS5_KEYTAB = /home/oracle11/krb5/keytab

   SQLNET.KERBEROS5_CONF_MIT = TRUE

   この例ではキャッシュ・パラメーターが指定されていませんが、次のコマンドを使用して見つけることができます。

   ~]$ oklist|grep -i cache

   Ticket cache: /tmp/krb5cc_500

   Sybase Kerberos の場合は、Sybase 環境変数または「klist -k」、「klist -c」から見つかります。

   例:

   env|grep -i KRB

   KRB5_KTNAME=/home/sybase15/kerberos/keytab

   KRB5_CONFIG=/home/sybase15/kerberos/krb5.conf

   klist -c

   Ticket cache: FILE:/tmp/krb5cc_533

   Default principal: sybuser1@GUARD.SWG.USMA.IBM.COM

   Valid starting Expires Service principal

   05/17/16 15:04:29 05/17/16 21:44:29 krbtgt/GUARD.SWG.USMA.IBM.COM@GUARD.SWG.USMA.IBM.COM

   klist -k

   Keytab name: FILE:/home/sybase15/kerberos/keytab

Kerberos ライブラリーが標準ライブラリー・パスにない場合。

Kerberos プラグインの新規パラメーターが実装され、「guardkerbplugin.conf」に設定されている必要があります。

KRB5_PLUGIN_GSSAPI_LIBRARY=<libgssapi_krb5.so への絶対パス>

Kerberos ライブラリーへのパスは、ファイル・システムを検索することによって見つかります。

例:

bash-4.2# find / -name libgssapi_krb5.so

/opt/freeware/lib/libgssapi_krb5.so

/opt/freeware/lib64/libgssapi_krb5.so

この例では 2 つのライブラリーが検出されました。「/opt/freeware/lib/libgssapi_krb5.so」は 32 ビット・ライブラリーであり、32 bit ビット・システムでのみ使用可能です。「/opt/freeware/lib64/libgssapi_krb5.so」は 64 ビット・ライブラリーであり、64 ビット・システムで使用する必要があります。

システムが 64 ビットであると想定した場合、Kerberos 構成は次のように設定されます。

Kerberos の値

KRB5RCACHETYPE=none

KRB5_KTNAME=/home/sybase16/kerberos/keytab

KRB5_CONFIG=/home/sybase16/kerberos/krb5.conf

プラグインの値

KRB5_PLUGIN_CCACHE=/home/sybase16/krb5cc_sybase16

KRB5_PLUGIN_GSSAPI_LIBRARY=/opt/freeware/lib64/libgssapi_krb5.so

#KRB5_PLUGIN_DEBUG=0

UNIX S-TAP の操作手順トピック

UNIX S-TAP バージョン番号の判別方法

DB2 パラメーターの判別方法

DB2 共有メモリー・セグメント・サイズの確認方法

S-TAP 統計へのアクセス方法

UNIX S-TAP バージョン番号の判別方法

S-TAP 用 Guardium サーバーの管理者ポータルから、「システム・ビュー」タブの「S-TAP 状況モニター」レポートに S-TAP のバージョン番号が表示されます。

管理者ポータルが使用できない場合は、データベース・サーバーの UNIX コマンド行から guard_stap バイナリーに -version または --version 引数を指定して実行すると、S-TAP バージョン番号を表示できます。

UNIX S-TAP バージョンを確認するには (S-TAP はデフォルトのインストール・ディレクトリーにインストールされていると想定します)、以下のコマンドを実行します。

```
-bash-3.2#  <guardium_base>/modules/STAP/current/guard_stap --version
または
-bash-3.2#  <guardium_base>/guard_stap/guard_stap --version
STAP-doberman_r20511_1-20100728_0514
```

DB2 パラメーターの判別方法

S-TAP での DB2 インターセプトは、以下のパラメーターに従って行われます。

表 2. Db2 パラメーター

パラメーター	STAP 名	ATAP 名	デフォルト値	コメント
パケット・ヘッダー・サイズ	db2_fixed_pack_adjustment	db2_header_offset	20	デフォルト値は、さまざまな 64 ビット・プラットフォーム上の DB2 8.2 以降に関してテストされています。他のバージョンの DB2 と 32 ビット・プラットフォームでは、異なるオフセットが必要である可能性があります。通常考えられるのは 16 と 12 です。
クライアント入出力域オフセット	db2_shmem_client_position	db2_c2soffset	61440	このパラメーターは ASLHEAPSZ DB2 パラメーターから派生します。
DB2 共有メモリー・セグメント・サイズ	db2_shmem_size	db2_shmsize	131072	このパラメーターは経験的に決定されます。 これを得るために使用できる一連のコマンドについては、以下を参照してください。

注: guard_tap.ini ファイル内で、1 つの WPAR に対して複数の Db2 インスタンスが構成されていて、これらの Db2 インスタンスの db2_shmem_size が同じである場合、その WPAR の最初の Db2 セクションで構成されているdb2_fix_pack_adjustment と db2_shmem_client_position が返されます。したがって、WPAR 上で複数の Db2 インスタンスが実行されている場合は、以下のようになります。

1. すべての Db2 インスタンスの db2_shmem_size、db2_fix_pack_adjustment、および db2_shmem_client_position が同じである場合は、構成されているインスタンスが 1つだけであっても、すべてのインスタンスからのパケットが収集されます。
2. すべての Db2 インスタンスで db2_shmem_size は同じであるが、db2_fix_pack_adjustment または db2_shmem_client_position が異なる場合は、最初に構成された Db2 インスタンスからのパケットのみが収集されます。

クライアント入出力域オフセット (db2_shmem_client_position) の計算

1. db2 インスタンス・ユーザーとして新しい bash シェルを開きます。
2. このシェルに関して db2bp コマンド・プロセッサーが現在実行中でないことを確認するために、ps -x コマンドを実行します。db2bp というコマンドが実行中と表示されないはずです。もし実行中であれば、kill するか、新しいシェルを実行します。
3. 以下の 2 つのコマンドを実行します。

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print $9 * 4096}'
```

出力は、db2_shmem_client_position として必要な値です。

ASLHEAPSZ パラメーターは、DB2 では 4K メモリー・ページで指定されます。これは、アプリケーション・サポート・レイヤー・ヒープのサイズを決定します。 前の図に示すように、クライアント入出力域は、エージェント/アプリケーションの共有メモリー・セグメント内のアプリケーション・ヒープの後に始まります。

注: この計算の理論は、「IBM Db2 Universal Database 管理ガイド: パフォーマンス」資料に基づいています。次の図は、DB2 共有メモリーのレイアウトを示しています。

DB2 共有メモリー・セグメント・サイズの確認方法

ATAP と KTAP は、このサイズに基づいてアプリケーション/エージェントの共有メモリー・セグメントを識別します。 これらのセグメントは、C2S パケットと S2C パケットに使用されます。

以下のステップに従ってセグメント・サイズを見つけます。

1. Db2 共有メモリー接続を開始して、開いたままにします。
2. ps -eaf | grep db2sysc コマンドを実行して、db2sysc のプロセス ID を取得します。出力は次のようになります。

```
db2inst1  5309370  5505772   0   Nov 11      - 1232:12 db2sysc 0
```

この例では、プロセス IDは 5309370 です。

3. ipcs -ma コマンドを実行して、共有メモリー・プロセスに関する情報を取得します。出力は次のようになります。

```
IPC status from /dev/mem as of Wed Nov 20 13:21:45 CST 2013
T         ID     KEY        MODE       OWNER    GROUP  CREATOR   CGROUP NATTCH     SEGSZ  CPID
m   2097152 0xffffffff D-rw------- pconsole   system pconsole   system      1 536870912 4522088
m         1 0x78000015 --rw-rw-rw-     root   system     root   system      3  16777216 3605314
m         2 0x78000016 --rw-rw-rw-     root   system     root   system      3 268435456 3605314
m 219152387 0xffffffff D-rw-------     root   system     root   system      1 536870912 5243842
m   1048580 0x61013002 --rw------- pconsole   system pconsole   system      1  10485760 4522088
m  10485765 0xd9fd8a61 --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      5  47644672 5571082
m   9437190 0xd9fd8a74 --rw-rw-rw- db2inst1 db2iadm1 db2inst1 db2iadm1      9 140852104 5571082
m   9437191 0xe1bd8858 --rw-rw----   oracle      dba   oracle      dba     40 53687107584 3801352
m   3145736 0x52594801 --rw-rw----     root informix     root informix     13 223019008 5702650
m   3145737 0xd9fd8b68 --rw-rw---- db2inst1 db2iadm1 db2inst1 db2iadm1      1  58720256 6619354
m   3145738 0xffffffff --rw------- db2fenc1 db2fadm1 db2inst1 db2iadm1      7 268435456 5505772
m        11 0x52594802 --rw-rw----     root informix     root informix     13  33439744 5702650
m        12 0x52594803 --rw-rw-rw-     root informix     root informix     13    573440 5702650
m        13 0xf2033f7e --rw------- sybase15   sybase sybase15   sybase      1 115564544 5178168
m 409993231 0x52594804 --rw-rw---- informix informix informix informix     13   8388608 5702650
m 763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
m 125829140 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
m 201326613 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
m 103750230 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 134217280 5309370
```

出力には、ここに示されている列以外の列がいくつか含まれていますが、この手順に影響を与えるものではありません。ステップ 2 で特定されたプロセス ID を含み、かつ NATTCH 列の値が 2 である行を探します。 Db2 共有メモリー・セグメントのサイズは、SEGSZ 列の値になります。 この例では、131072 です。

4. ヒント: ステップ 3 で返されるリストが長すぎる場合、プロセス ID を使用してリストをフィルターに掛けることができます。この例では、ipcs -ma | grep 5309370 と入力します。この結果には列見出しは表示されませんが、前の結果を調べて列見出しを確認することで、正しい行と列を特定できます。この例では、最後の行です。

```
m 131072014 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 1342177280 5309370
m 763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
m 227541013 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
m 106353238 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
```

DB2 共有メモリー・セグメント・サイズ (db2_shmem_size) を見つけるための、より簡単だが精度が下がる方法としては、以下の代替手順を使用します。

セグメントは、ASLHEAPSZ パラメーターと RQRIOBLK パラメーターの合計に等しくなります。DB2 では、はるかに大きいセグメントが割り振られます。 ほとんどの場合、このサイズは (ASLHEAPSZ + 1) * 2 ページ、または (ASLHEAPSZ + 1) * 8192 バイトに等しくなります。正確なサイズは、新規 DB2 のローカル接続が作成される前後にシステム内の共有メモリー・セグメントを監視することによって測定できます。

以下の一連のコマンドを使用して、共有メモリー・セグメント・サイズを決定します。

ipcs コマンド・パラメーターと出力形式は、プラットフォームによって異なります。 以下のスクリプトは AIX バージョンに基づいています。

```
ipcs -ma | sort -n -2 +3 > /tmp/before.txt
db2 connect to <some_existing_database>ipcs -ma | sort -n -2 +3 > /tmp/after.txt
db2 terminate
diff /tmp/before.txt /tmp/after.txt | awk '{if ($10 == 2) print $11}'
```

結果を必ず確認することをお勧めします。 これは、次のコマンドの出力に等しいか、少なくともそれに近いです。

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print ($9 + 1) * 8192}'
```

S-TAP 統計へのアクセス方法

表「STAP_Statistic」にアクセスすると、ユーザーは結果に基づいてアラートを作成できます。

この表は、S-TAP によりスニファーに送信された統計を保管するために使用します。

この表の事前定義レポートはありません。

1 時間単位の時間間隔 (例えば、5 は 5 時間毎)

1 時間未満の時間間隔には、 - (マイナス) を使用します。

表のフィールド

TIMESTAMP

SOFTWARE_TAP_HOST

TOTAL_BYTES_SO_FAR

TOTAL_BYTES_DROPPED_SO_FAR

TOTAL_BYTES_IGNORED

TOTAL_BUFFER_INIT

IOCTL_REQUESTS

TOTAL_RESPONSE_BYTES_IGNORED

System CPU%

System Idle%

STAP CPU%

Buffer recycled

親トピック: S-TAPs およびその他のエージェント

Windows S-TAP

このセクションは、Windows S-TAP の構成に関する情報を得るために利用してください。

V10 の新機能

ネイティブ・イメージ (32/64 ビット)

新規の TCP トライバーおよび NP ドライバー (WFP、NmpMonitor)

Windows フィルタリング・プラットフォーム (WFP) は、Transport Driver Interface (TDI) ベースの TCP ドライバーを置き換えるものです。

Wfpmonitor は、新規の S-TAP TCP ドライバーで、lhmonproxy および lhmon に置き換わるものです。

WFP には以下の利点があります。

- リブートせずにアップグレードできます。
- インストール後に、TCP トラフィックを取得するためにデータベース・インスタンスを再始動する必要がありません。
- すべてのドライバーが、(周期的な) ロギング機能を提供します。ログ・ファイルは、/logs にあります。ドライバーのエラー/警告は表示されないため、この機能はサポート性を拡張するものです。

名前付きパイプのドライバーが再設計されました。Nptrc に置き換わり、プロキシー (NmpProxy) とモニター (NmpMonitor) に分割されました。これは、機能を基本 OS (NmpProxy) 用と Guardium ロジック (NmpMonitor) 用に分割しています。

Windows S-TAP の開始

S-TAP インストールの方式によって、次の方法で S-TAP を開始できます。

GIM のインストール

GIM を使用すると、データベース・サーバーにログインしなくても S-TAP を始動できます。 以下のステップを使用して、 WINSTAP_ENABLED パラメーターを変更し、データベース・サーバー上で変更を スケジュールに入れます。

1. 「インストール管理」 > 「クライアント別の設定 (レガシー)」をクリックして、「クライアント検索条件」を開きます。
2. 「検索」をクリックして、フィルター検索を実行します。
3. アクション (S-TAP の開始) の対象となるクライアントを選択します。
4. 「次へ」をクリックして、「共通モジュール」パネルを開きます。
5. WINSTAP 用のモジュールを選択します。
6. 「次へ」をクリックして、「モジュール・パラメーター」パネルを開きます。
7. アクション (S-TAP® の開始) の対象となるクライアントを選択します。
8. WINSTAP_ENABLED パラメーターを 1 に変更します。
9. 「クライアントに適用」をクリックして、対象となるクライアントに適用します。
10. 「インストール/更新」 をクリックして、対象となるクライアントに対する更新をスケジュールに入れます。この更新は、今すぐスケジュールに入れることも、後からスケジュールに入れることもできます。この更新のスケジュールが 実行されるときに、対象クライアント上の S-TAP サービスが開始されます。

GIM 以外のインストール

1. システム管理者のアカウントを使用して、データベース・サーバー・システムにログオンします。

2. 「サービス」制御パネルから GUARDIUM_STAP サービスを開始します。
3. この S-TAP の報告先となっている Guardium システムにログインします。 S-TAP 制御パネルの状況ランプがグリーンになっていることを確認します。

注: Windows S-TAP の始動中に構成の問題 (不明のローカル IP アドレス、複数の 1 次 SQL-Guard が定義されているなど) による致命的エラーが発生する場合、Windows イベント・ログにその原因が記録されます。 場合によっては、障害後の終了によって異常終了したり、別のイベントがログに 記録されたりする可能性があります。障害の原因を説明するイベントの後でこの異常終了が 起こる場合は、心配ありません。

Windows S-TAP の停止

S-TAP は、S-TAP のインストール方式に応じて、以下の方法で停止できます。

GIM のインストール

GIM を使用すると、データベース・サーバーにログインしなくても S-TAP を停止できます。 以下のステップを使用して、 WINSTAP_ENABLED パラメーターを変更し、データベース・サーバー上で変更を スケジュールに入れます。

1. 「インストール管理」 > 「クライアント別の設定 (レガシー)」をクリックして、「クライアント検索条件」を開きます。
2. 登録済みクライアントに対するフィルター検索を実行する場合は、「クライアント検索条件」を入力します。
3. 「検索」 をクリックしてフィルター検索を実行し、「クライアント」パネルを表示します。
4. アクション (S-TAP の停止) の対象となるクライアントを選択します。
5. 「次へ」をクリックして、「共通モジュール」パネルを開きます。
6. 「WINSTAP 用モジュール」を選択します。
7. 「次へ」をクリックして、「モジュール・パラメーター」パネルを開きます。
8. アクション (S-TAP の停止) の対象となるクライアントを選択します。
9. WINSTAP_ENABLED パラメーターを 0 に変更します。
10. 「クライアントに適用」をクリックして、対象となるクライアントに適用します。
11. 「インストール/更新」 をクリックして、対象となるクライアントに対する更新をスケジュールに入れます。この更新は、今すぐスケジュールに入れることも、後からスケジュールに入れることもできます。この更新のスケジュールが 実行されるときに、対象クライアント上の S-TAP サービスが停止されます。

GIM 以外のインストール

1. システム管理者のアカウントを使用して、データベース・サーバー・システムにログオンします。
2. 「サービス」制御パネルで次のように行います。
   - GUARDIUM_STAP サービスを停止します。
3. この S-TAP のレポート先となった Guardium システムの UI にログインし、S-TAP 制御パネルの「状況」ライトが赤色であることを確認します。

JAVA_HOME ロケーションの CAS 再構成

ほとんどの場合、インストール・プログラムは JAVA_HOME 値の検索を処理します。 この値は CAS 構成ファイルにあります。

なんらかの理由 (Guardium® CAS 製品のインストール後に新しい Java™ バージョンを インストールするなど) で、JAVA_HOME のロケーションを変更する必要がある場合は、 以下の手順に従ってください。

1. CAS 構成ファイルを見つけて、編集用に開きます。絶対パス名は以下のとおりです。<installation directory>/case/conf/wrapper.conf
2. `wrapper.java.command=<value>` の項目を見つけます。
3. 値を JAVA_HOME ディレクトリーに置換します。
4. ファイルを保存します。

CAS および 64 ビットの Windows レジストリー

Windows では、ソフトウェア構成パラメーターはキー HKEY_LOCAL_MACHINE¥SOFTWARE のレジストリー・ツリーに格納されています。 64 ビット・マシンでは、同じアプリケーションの 64 ビット・バージョンと 32 ビット・バージョンの両方を稼働できるため、64 ビット・アプリケーションと 32 ビット・アプリケーションの構成パラメーターを区別する必要があります。

この問題に対する Microsoft の解決策は、レジストリーをパーティションで区切ることです。WOW6432Node というラベルが付いた特殊キーが、 キー HKEY_LOCAL_MACHINE¥SOFTWARE のレジストリー・ツリーに追加されます。32 ビット・ アプリケーションがキー HKEY_LOCAL_MACHINE¥SOFTWARE にあるパスを介してレジストリーにアクセスしようとすると、 Windows はそのパスに特殊キー WOW6432Node を挿入します。このようにすることで、32 ビット・アプリケーションは 32 ビット・マシンで行うのと同じように Windows レジストリーを扱い、 Windows は正しいパーティションへのリダイレクトを処理します。

CAS は 32 ビットの Java アプリケーションであるため、 通常は 64 ビットのソフトウェア構成パラメーターへのアクセスは持ちません。 CAS は、64 ビットの環境を検出し、パーティション化されたレジストリーを 処理するように拡張されています。CAS がレジストリーに対して関心を持つのは、レジストリー・キーの値を取得して、 変更を検出したり、推奨値と比較したりするためです。

例として、CAS が HKEY_LOCAL_MACHINE¥SOFTWARE¥MyApp¥Parameter1 の値を取得するとします。その値は、 パーティションのどちらかにあるか、両方にあるか、どちらにもないかのいずれかです。値がどちらのパーティションにもない場合、CAS は NULL を取得します。それ以外の場合は、 文字列 WOW6432Node によって区切られた 2 つの値の連結である文字列を戻します。値が 64 ビット・パーティションにはあるが、32 ビット・パーティションにはない場合、 取得される文字列は Value64WOW6432Nodenull のようになります。逆に、値が 32 ビット・パーティションにはあるが、64 ビット・パーティションにはない場合、文字列は nullWOW6432NodeValue32 です。 最後に、値が両方のパーティションにある場合、返される文字列は Value64WOW6432NodeValue32 です。 この新しいレジストリー値パターン検索は、必要に応じて、両方のレジストリー・パーティションを検索します。

ドメイン・コレクターからの SID の収集

GuardiumDC は、ユーザー・アカウント (SID およびユーザー名) の更新を 1 次ドメイン・コントローラーから収集し、その後、Guardium_S-TAP にその変更内容をシグナル通知して、S-TAP 内部の SID/UserName のマップを更新するサービスです。S-TAP がマップから解決済みの SID を見つけられない場合、1 次ドメイン・コントローラーからこれを取得しようとします。その場合、S-TAP は、デバッグ・ログ (レベル 7) にメッセージ「`SID *** のアカウント名 *** を取得しました (The account name *** has been retrieved for SID ***)`」を記録します。

TAP セクションの DC_COLLECT_FREQ は、収集頻度を時間単位で指定します (最小値は 1 で、最大値の 24 がデフォルト)。

TAP セクションの DC_COLLECT_MAXUSERS は、収集するユーザーの最大数を指定します (デフォルトは 200,000 で、最小値は 10,000)。

DOMAIN_CONTROLLER 例: DOMAIN_CONTROLLER=¥¥atari

DB2 共有メモリー・ユーザー・モードの実装

Windows S-TAP を使用して DB2® 共有メモリー・トラフィックをキャプチャーする方法は 2 つあります。

Guardum システムのメニュー S-TAPCONTROL> Shared Memory Monitor > DB2 で、DB2 のチェック・マークを外します。

TAP を使用します (チェック・マークを付けます)。

「DETAIL」(Guardium S-TAP CONTROL) >「共有メモリー モニター」>「TAP」にチェック・マークを付ける必要があります。

(両方の方式にチェック・マークが付けられている場合、DB2 TAP 方式が使用されます)

S-TAP の検査エンジンでは、DB2 のインスタンス名が必要です。インスタンス名は「コントロール パネル」->「サービス」->「名前」で見つけることができます。インスタンスは DB2 サービス名の最後の部分です。例えば、DB2 のサービス名が「DB2-DB2COPY1-DB2-0」である場合、インスタンス名は「DB2-0」です。Guardium ディレクトリーにユーティリティー db2TAP.exe があります。インスタンス名を表示するには、コマンド・ウィンドウで db2tap.exe list を実行します。

検査エンジンの例:

```
[DB_DB21]
PORT_RANGE_START=50001
PORT_RANGE_END=50001
DB2_FIX_PACK_ADJUSTMENT=80
INSTANCE_NAME=DB2_01-0
DB_TYPE=DB2
NETWORKS=1.1.1.1/0.0.0.0
```

DB2 共有メモリー・パラメーター

DB2 共有メモリー調整 / DB2 共有メモリー・クライアント位置

Windows における DB2 共有メモリー・パラメーターの値:

DB2_FIX_PACK_ADJUSTMENT
: このパラメーターのデフォルトは 10 進数の 80 です。DB2 バージョン 8.2 以降では、これが正しい値です。これより前のバージョンの場合は、10 進数の 20 で試行してください。

DB2_CLIENT_OFFSET
: このパラメーターのデフォルトは、10 進数の 61440 です。このパラメーターは、DB2 データベース構成値 ASLHEAPSZ を使用して計算され、4096 で乗算されます。

  ASLHEAPSZ の値を取得するには、DB2 コマンド db2 get dbm cfg を実行して、ASLHEAPSZ の値を探します。通常、この値は 15 で、その結果、デフォルトの 61440 が算出されます。これが 15 ではない場合は、この値を 4096 で乗算して、適切なクライアント・オフセットを算出します。

Db2 Exit と Windows S-TAP の統合

Db2 リリース 10.1 以降を使用している場合、S-TAP はすべての Db2 トラフィックを、Db2 エンジンから直接キャプチャーします。この方式を使用する場合、ファイアウォール、および修正機能と編集機能はサポートされません。また、ストアード・プロシージャーはキャプチャーされません。暗号化およびネットワーク・プロトコルに関係なく、すべての Db2 トラフィックがキャプチャーされます。このソリューションは、このバージョンの Db2 を導入するユーザーの S-TAP 構成を簡素化し、固有の Db2 サポートをそれらのユーザーに提供します。このタイプのデータベースから S-TAP を構成するには、以下のステップに従います。

1. 1. 各インスタンスごとに、DB2 SQLLIB フォルダー内に新しいフォルダー $DB2PATH¥security¥plugin¥commexit¥instance_name を作成します。 例: C:¥Program Files¥IBM¥SQLLIB¥security¥plugin¥commexit¥DB2_01
2. 対応する DLL を、S-TAP のインストール・ディレクトリーから作成したディレクトリーにコピーします。
   32 ビットの Db2 の場合:
   - db2fexitx86.dll
   - db2exitx86.dll

   64 ビットの Db2 の場合:
   - db2exitx64.dll
   - db2fexitx64.dll
3. Db2 インスタンスを停止し、次のコマンドを実行します。

   UPDATE DBM CFG USING COMM_EXIT_LIST db2fexitx86 (32 ビットの場合)

   UPDATE DBM CFG USING COMM_EXIT_LIST db2fexitx (64 ビットの場合))

4. Db2 インスタンスを開始します。
5. Db2 出口の検査エンジンを追加します。

   TAP セクションで:

   DB2_EXIT_DRIVER_INSTALLED=1

   検査エンジンの新しいタイプが DB セクションに反映されます。

   [DB_DB2_EXIT1]

   DB_TYPE=DB2_EXIT

   INSTANCE_NAME=Service_name

サービス名は、インスタンス名ではありません。S-TAP インストール・フォルダーの db2tap ユーティリティー、または制御パネルを使用して、サービス名を判別できます。 2 番目のダッシュ (-) 区切り文字の後ろに続くサービス名の部分をインスタンス名に設定します。例えば、コントロール・パネル内でサービス名が `DB2 - DB2COPY1 - DB2-01-0` である場合、INSTANCE_NAME を `DB2-01-0` に設定します。

6. この機能の使用を停止するには、Db2 を停止し、次のコマンドを実行してから、Db2 を再開します。db2 UPDATE DBM CFG USING COMM_EXIT_LIST NULL

S-TAP の統計

表「STAP_Statistic」にアクセスすると、ユーザーは結果に基づいてアラートを作成できます。

この表は、S-TAP によりスニファーに送信された統計を保管するために使用します。

この表の事前定義レポートはありません。

1 時間単位の時間間隔 (例えば、5 は 5 時間毎)

1 時間未満の時間間隔には、 - (マイナス) を使用します。

表内のフィールド

TIMESTAMP

SOFTWARE_TAP_HOST

TOTAL_BYTES_SO_FAR

TOTAL_BYTES_DROPPED_SO_FAR

TOTAL_BYTES_IGNORED

TOTAL_BUFFER_INIT

IOCTL_REQUESTS

TOTAL_RESPONSE_BYTES_IGNORED

System CPU%

System Idle%

STAP CPU%

Buffer recycled

親トピック: S-TAPs およびその他のエージェント

S-TAP のディスカバリー

S-TAP が定期的にデータベース・インスタンスを検出し、現在のアクティブな S-TAP システムにその結果を送信できるようにします。

概要

Guardium S-TAP のディスカバリー・アプリケーションを使用して、定期的にデータベース・インスタンスを検出し、現在のアクティブな S-TAP システムにインスタンスを送信します。 S-TAP がユーザーとして実行されている場合、ディスカバリー機能は制限されます。 以下のメッセージが表示されます。

警告: ディスカバリーが有効化され、`STAP` がユーザー `guardium` として実行されています。(WARNING: Discovery is enabled and STAP is running as user guardium.)
`STAP` がユーザー `guardium` として実行されている場合、ディスカバリー機能は制限されます。(The discovery function is limited when STAP runs as user guardium.)
ディスカバリーが最も有効なのは、「`tap_run_as_root=1`」の場合です。(Discovery is most effective when 'tap_run_as_root=1')

注: S-TAP のディスカバリーは AIX 5.3 ではサポートされていません。これは、そのプラットフォームに静的ライブラリーが必要であるためです。
注: S-TAP ディスカバリーで Informix データベースがオープンされないという状況が発生しないようにするには、実行可能ファイルの絶対パスを使用してデータベースを開始することをお勧めします。

S-TAP ディスカバリーでサポートされるデータベース

Oracle、Db2、Informix、MySQL、PostgreSGL、Sybase、Hadoop、Teradata、Netezza、MemSQL

S-TAP のディスカバリー・アプリケーションのパラメーターについては、discovery パラメーターで説明します。

ディスカバリーは、以下のパラメーターも使用します。

- tap_ip: データベース・インスタンスが関連付けられている S-TAP。
- sqlguard_ip: S-TAP のディスカバリーの結果が、この IP に送信されます。 (SQLguard パラメーターに primary=1 が指定されている Guardium システム。)

スケジュールされたディスカバリーの実行中に、ユーザー・インターフェースからディスカバリーを実行するための新規要求が届いた場合、その新規要求は無視されます。

構成

S-TAP のディスカバリー・アプリケーションでは、その構成のために UNIX 構成ファイル guard_tap.ini が使用されます。 このファイル内には独自の構成パラメーターがいくつかあり、このファイルはその構成パラメーターに依存して機能します。

S-TAP のディスカバリーは手動で実行できますが、このアクションは推奨されません。 その主な理由は、手動実行はデバッグ目的であるためです。

結果を Guardium システムに送信するには、ファイル・パス <absolute path to guard_discovery binary>/guard_discovery<path to guard_tap.ini>/guard_tap.ini または <absolute path to guard_discovery binary>/guard_discovery <path to guard_tap.ini>/guard_tap.ini --send-to-sqlguard を使用します。

結果を STDOUT に出力するには、コマンド <absolute path to guard_discovery binary>/guard_discovery <path to guard_tap.ini>/guard_tap.ini --print-output を使用します。

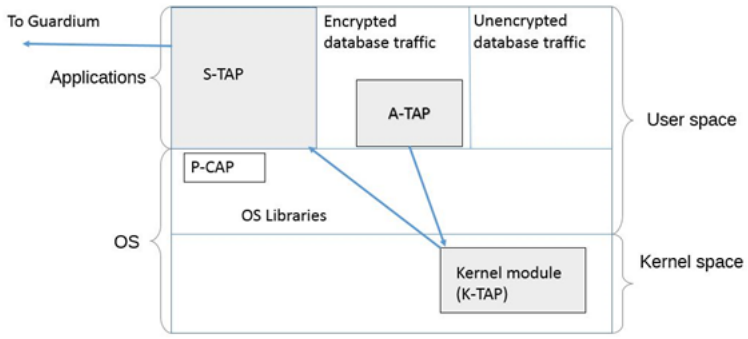
親トピック: S-TAPs およびその他のエージェント

A-TAP の管理

A-TAP は application-level tapping の省略形です。A-TAP はアプリケーション層に配置され、暗号化されたデータベース・トラフィックのモニターをサポートします。このモニターは、K-TAP によってカーネルで実行することはできません。

A-TAP (application-level tapping) メカニズムにより、データベース・サーバーの内部コンポーネント間の通信がモニターされます。データはアプリケーション層で暗号化解除され、そこで A-TAP がそのデータを取得して K-TAP に送信します。K-TAP は、データを S-TAP に渡すためのプロキシーです。そのデータは、続いて S-TAP から Guardium コレクターに送信されます。

以下の図は、データベース・サーバー上の全体のアーキテクチャーで A-TAP が配置される場所を示しています。



A-TAP はすべての S-TAP に含まれますが、A-TAP を必要とするデータベースごとに固有に構成する必要があります。

どのようなときに ATAP を使用するか

A-TAP は、動作中の (非 Windows) DBMS 暗号化が使用されているときに必要になりますが、その他の内部的なデータベース実装の詳細 (A-TAP を必要とする共有メモリーなど) がある場合があります。

Linux での Informix と Db2 は、出口を使用してより緊密に Guardium と統合するため、共有メモリーのサポートに対して推奨される方式です (適用可能な場合)。

制限: 32 ビット・データベースが 64 ビット・サーバーにある環境では A-TAP がサポートされていません。

モニターの制限: A-TAP は編集をサポートしていません。ブロッキングは、2.6.36 以降のリリースで Linux カーネルでサポートされます。

- A-TAP の構成および保守の準備
  A-TAP を構成および保守するには、データベース管理者とシステム管理者の両方との調整が必要です。
- A-TAP の構成とアクティベーション
  各 A-TAP を構成し、アクティブにします。
- A-TAP アクティブ化、非アクティブ化、および DB 停止、再始動のガイドライン
  A-TAP のアクティブ化と非アクティブ化、および DB の停止と再始動のタイミングを把握します。
- A-TAP の guardctl ユーティリティー・コマンド
  guardctl ユーティリティーは、A-TAP の管理ツールです。A-TAP の使用を開始する前に、以下のコマンドを理解してください。
- guardctl の戻りコード
  guardctl エラー・コードは、発生したエラー条件を明確にします。特に、ATAP インスタンスを管理するために別のスクリプト経由で guardctl スクリプトを呼び出す場合に役立ちます。
- データベース固有の guardctl パラメーター
  各データベース・タイプには、固有の guardctl 要件があります。
- A-TAP の非アクティブ化
  データベース OS をアップグレードする前に、A-TAP を非アクティブにする必要があります。
- 特殊な環境での A-TAP の構成とアクティブ化
  ゾーン、WPAR、Teradata、および Oracle には、追加の構成が必要です。
- A-TAP 構成の問題のトラブルシューティング
  このセクションでは、A-TAP の構成中に起こる一般的な失敗、それらの症状、およびそれらを回避する方法をまとめます。

親トピック: S-TAPs およびその他のエージェント

A-TAP の構成および保守の準備

A-TAP を構成および保守するには、データベース管理者とシステム管理者の両方との調整が必要です。

A-TAP を構成およびアクティブにするには、以下の権限が必要です。

- データベース・サーバーに対する root アクセス権限
- データベースを停止および再始動する権限

さらに、DBA と連携して、ユーティリティーに入力する必須パラメーターを取得する必要があります。 必要なパラメーターの詳細については、データベース固有の guardctl パラメーターを参照してください。継続的な保守のためには、OS およびデータベースのアップグレード時に A-TAP のアクティブ化と非アクティブ化を処理するための文書化された手順が組織に用意されている必要があります。A-TAP アクティブ化、非アクティブ化、および DB 停止、再始動のガイドラインを参照してください。クラスター環境では、すべてのノードで A-TAP を構成し、アクティブにする必要があります。

ほとんどの場合、A-TAP のアクティブ化、アップグレード、または非アクティブ化には Guardium の guardctl ユーティリティーを使用します。また、guardctl を ATAP に対するユーティリティー・インターフェースとして使用するラッパー・スクリプトを実装し、独自のユーザー・エクスペリエンスを提供することもできます。guardctl ユーティリティーの構文とオプションについて詳しくは、A-TAP の guardctl ユーティリティー・コマンドを参照してください。

作業を開始する前に、以下を実行してください。

- S-TAP がインストール済みで、K-TAP が有効であることを確認します。
- データベース・サーバーに対する root 権限があることを確認します。
- ご使用のデータベースに当てはまるデータベース固有の guardctl パラメーターを参照し、ユーティリティーの実行に必要なパラメーターがあることを確認します。

親トピック: A-TAP の管理

A-TAP の構成とアクティベーション

各 A-TAP を構成し、アクティブにします。

このタスクについて

前提条件: S-TAP がインストールされていること。

手順

1. guard_tap.ini ファイルで ktap_installed=1 であることを確認します。
2. すべてのアクティブ・データベース・セッションからログオフし、データベースを停止します。データベース管理ユーザーのプロセスがすべて停止されることが重要です。例えば Oracle の場合は ps -ef | grep oracle を実行します
3. root ユーザーとして、以下のように guardctl ユーティリティーに authorize-user コマンドを指定して使用し、データベース管理ユーザーにトラフィックを記録することを許可します。
   `<guardium_base>/xxx/guardctl authorize-user <user-name>`

   シェル・インストーラーの例

   `/usr/local/guardium/guard_stap/guardctl authorize-user postgres`
   ユーザー「postgres」にトラフィックをログに記録することを許可します。

   許可の確認の例

   `/usr/local/guardium/guard_stap/guardctl is_user_authorized postgres`
   ユーザー「postgres」は許可されています。

   GIM インストール済み環境の例

   `/usr/local/guardium/modules/ATAP/current/files/bin/guardctl authorize_user postgres`
   ユーザー「postgres」にトラフィックをログに記録することを許可します。

4. 以下のようにして構成パラメーターを格納します。
   a. ご使用のデータベース・タイプおよびプラットフォームに必要なパラメーターを判別するには、データベース固有の guardctl パラメーターを参照してください。
   b. root ユーザーとして、以下のように guardctl ユーティリティーの store-conf コマンドを使用してデータベース・インスタンスの構成を格納します。
      `<guardium_base>/xxx/guardctl db_instance=<instance> [<name>=<value> ...] store-conf`

   Linux シェル・インストーラーでの Oracle の例:
   /usr/local/guardium/guard_stap/guardctl --db-user=oracle11 --db-type=oracle --db-instance=on12rh60 --db-home=/home/oracle11/product/11.1.0/db_1 --db-version=11.2 store-conf
   Linux GIM インストール済み環境での Oracle の例:
   /usr/local/guardium/modules/ATAP/current/files/bin/guardctl db_instance=$ORACLE_SID db_home=$ORACLE_HOME db_type=oracle db_user=oracle12 db_version=12 store-conf

   注: Guardium V10.1 以上では、インスツルメンテーションはアクティブ化中に自動的に行われるため、明示的なインスツルメンテーションはありません。
5. A-TAP をアクティブにします。
   a. root ユーザーとして、`<guardium_base>/xxx/guardctl db_instance=<instance> activate` を入力します。

      シェル・インストーラーの例

      `/usr/local/guardium/guard_stap/guardctl --db-instance=onrh60x activate`

      GIM インストール済み環境の例

      `/usr/local/guardium/modules/ATAP/current/files/bin/guardctl --db-instance=onrh60x activate`

      注: A-TAP は、Guardium GUI の検査エンジン構成の「暗号化」チェック・ボックスを使用して任意でアクティブにすることができますが、GUI でアクティブ化する利点はありません。このオプションは、Linux プラットフォームでは使用できません。
   b. 次のように guardctl ユーティリティーの list-active コマンドを使用して、インスタンスがアクティブ化されていることを確認します:
      <guardium_base>/xxx/guardctl list-active

      例: <guardium_base>/xxx/guardctl list-active oracle

6. データベース・サーバーを再始動します。

親トピック: A-TAP の管理

A-TAP アクティブ化、非アクティブ化、および DB 停止、再始動のガイドライン

A-TAP のアクティブ化と非アクティブ化、および DB の停止と再始動のタイミングを把握します。

A-TAP のための再始動/ロード/インスツルメンテーション/アクティブ化の要件

シナリオ	説明
Oracle クラスター環境に UNIX A-TAP をインストールした後	すべてのデータベース・インスタンス、およびすべてのクラスター間プロセスを再始動する必要があります
A-TAP をアクティブにする前	データベースを停止します
A-TAP をアクティブにした後	データベースを再始動します
A-TAP を非アクティブにする前	データベースを停止します
データベースをアップグレードする前 (フィックスパックの適用など)	A-TAP を非アクティブにします
S-TAP をアップグレードする前	A-TAP を非アクティブにします

親トピック: A-TAP の管理

A-TAP の guardctl ユーティリティー・コマンド

guardctl ユーティリティーは、A-TAP の管理ツールです。A-TAP の使用を開始する前に、以下のコマンドを理解してください。

guardctl ユーティリティー

guardctl ユーティリティーを使用する場合は、スーパーユーザー特権が必要であるため、**root** としてログインする必要があります。guardctl ユーティリティーは、<guardium_base>/guard_stap ディレクトリーの下にインストールされます。ここで、<guardium_base> は Guardium ソフトウェアがインストールされているディレクトリーです。GIM インストール済み環境の guardctl の場合は、<guardium_base>/modules/ATAP/current/files/bin の下にインストールされます。

構文

<guardium_base>/xxx/guardctl [<parameter>=value>] [<parameter>=<value> ...] <command> [-q | -v | -qv]

データベース固有の guardctl パラメーターに記載されているパラメーターを参照してください。

-q、-v、-qv のフラグ

Guardium V10.1.3 からは、次のフラグを使用して出力を管理します。

- -q (抑制): 名前/値ペアを除き、すべての出力を抑制します
- -v (値のペア): 各コマンドに関連する名前/値ペアを追加します
- -qv: 名前/値ペアのみを出力します

出力は、コマンドのタイプによって異なります。

- 構成済みのすべてのインスタンスに対してアクションを実行するコマンド
  - overall_rv および overall_msg を除き、各インスタンスのすべての名前/値ペアを出力します
  - 末尾に overall_rv の名前/値ペアを出力します。値は以下のいずれかです。
    - 0 (成功)、すべての報告が成功した場合のみ
    - 1 (失敗)、いずれかの報告に何らかの失敗があった場合
  - 末尾に overall_msg の名前/値ペアを出力します。
  - 「overall_rv」 の名前/値ペアで報告された値を戻します。
- 1 つのインスタンスでアクションを実行するコマンド
  - overall_rv および overall_msg を除き、すべての名前/値ペアを出力します
  - 「rv」の名前/値ペアで報告された値を戻します。
- パラメーターの格納、パラメーターの出力、または状況の確認を行うコマンド
  - 名前/値ペアを出力しません。

名前/値ペアの出力は以下のようになります。

```
db_instance: ${db_instance}
db_user: ${db_user}
db_base: ${db_base}
db_home: ${db_base}
db_version: ${db_version}
db_type: ${db_type}
is_active: ${is_active} (「yes」または「no」)
is_instrumented: ${is_db_instrumented} (「yes」または「no」)
msg: some string
rv: ${retval}
overall_rv: ${retval}
overall_msg: (string)
```

commands

コマンド	記述

コマンド	記述
activate	保管されたパラメーターを使用して、指定されたデータベース・インスタンスの A-TAP をアクティブにします。-v または -qv を指定した場合は、名前/値ペアを出力します。 Guardium V10.1.3 からは、既にアクティブなインスタンス (DB が実行中であるかどうかにかかわらず) をアクティブ化してもエラーは生成されません。
authorize-user	ユーザーを「guardium」許可グループに追加します。
deactivate	指定された単一のデータベース・インスタンスの A-TAP を非アクティブにします。-v または -qv を指定した場合は、名前/値ペアを出力します。 Guardium V10.1.3 からは、既に非アクティブなインスタンス (DB が実行中であるかどうかにかかわらず) を非アクティブ化してもエラーは生成されません。
deactivate-all	指定されたデータベース・インスタンスのリストの A-TAP を非アクティブにします。データベース・インスタンスを指定しないと、すべてのアクティブ A-TAP が非アクティブにされます。-v または -qv を指定した場合は、各インスタンスの名前/値ペアを出力します。オプションで db-type を指定し、グループ (例えば、すべての Oracle など) を非アクティブにできます。追加の名前/値ペアについては、最後に「overall_rv={0、1}」を指定します。すべてのインスタンスに対して rv=0 の場合、成功 (0) を戻します。少なくとも 1 つのインスタンスで rv != 0 が報告される場合は、失敗 (1) を戻します。
deinstrument	指定した Oracle DB のインスツルメンテーションを削除します。V10.1 以上は不要です。インスツルメンテーションの削除が必要な場合は、非アクティブ化する際に自動的に行われます。-v または -qv を指定した場合は、名前/値ペアを出力します。 Guardium V10.1.3 からは、DB が実行中であっても、アクティベーション状況を問わず、インスツルメンテーションされていないインスタンスからインスツルメンテーションを削除してもエラーが生成されません。
dump-params	パラメーターの現行値をダンプします。
get-statistics	A-TAP の統計を取得します。
help	デフォルトのコマンドで、サポートされるコマンド、パラメーターおよびそれらのデフォルト値のリストを印刷します。
instrument	再リンクされ、インスツルメンテーションされた Oracle を明示的に作成します。インスツルメンテーションが必要な場合は、通常はアクティブ化する際に自動的に行われます。手動でのインスツルメンテーションは、AIX 上の Oracle バージョン <= 10 でのみ必要です。 既にインスツルメンテーションされているインスタンスをインスツルメンテーションすると、エラーが返されます。-v または -qv を指定した場合は、名前/値ペアを出力します。
is-active	A-TAP がアクティブ化されているインスタンスが少なくとも 1 つある場合、1 を戻します。それ以外の場合は、0 を返します。
is-user-authorized	db-user (A-TAP を実行しているユーザー) がデータベース・トラフィックを K-TAP/S-TAP に記録することを許可されているかどうかを検査します。
list-active	すべてのアクティブな A-TAP データベース・インスタンスのデータベース・インスタンス・ユーザー名をリストします。-v または -qv を指定した場合は、名前/値ペアを出力します。
list-configured	構成はされているが、非アクティブな A-TAP を持つデータベース・インスタンスをリストします。-v または -qv を指定した場合は、名前/値ペアを出力します。
oracle-relink	db-exec によって Oracle を再リンクします。
prepare-libs	Zone/WPAR インストール済み環境で使用するライブラリーを準備します。
repair	このコマンドは、ATAP がアクティブである間に DB が (誤って) アップグレードされた場合に実行します。-guard-original ファイルと -guard-instrumented ファイルは除外されます。修復が成功した場合、または修復が必要ない場合は成功を戻します。現在の DB 実行可能ファイルには影響しません。-v または -qv を指定した場合は、名前/値ペアを戻します。
restore-active-ataps	save-active-ataps によって以前に保存された ATAP のアクティブ状態を復元します。インスタンスがアクティブ化に失敗した場合 (DB が実行中であったり他のエラーが原因で)、残りのインスタンスは引き続きアクティブ化を試みます。このコマンドでは、既にアクティブなインスタンスのアクティブ化がエラーにならないため、問題なく複数回実行することができます。Guardium V10.1.4 で導入されました。
save-active-ataps	現在アクティブな ATAP の構成を単一のファイルに保存し、後でアクティブ状態に復元できるようにします。DB のアップグレードを準備するときに、deactivate-all の前に使用すると役立ちます。Guardium V10.1.4 で導入されました。
store-conf	特定のデータベース・インスタンスの構成を保管します。
store-system-conf	システム構成パラメーターを保管します。

親トピック: A-TAP の管理

guardctl の戻りコード

guardctl エラー・コードは、発生したエラー条件を明確にします。特に、ATAP インスタンスを管理するために別のスクリプト経由で guardctl スクリプトを呼び出す場合に役立ちます。

コード	記述	使用法
0	成功	すべてのコマンドによって返されます。 deactivate への応答として返される場合、すべてのインスタンスが非アクティブ化されています。 is-active への応答として返される場合、アクティブ・インスタンスはありません。
1	誤ったパラメーター	パラメーターが無効であるか欠落している場合に、すべてのコマンドによって返されます。
2	認識されないインスタンスで is-active が呼び出された	指定された db-instance が guardctl で認識されず、そのためアクティブかどうかを判別できない場合に、is-active によって返されます。

コード	記述	使用法
20	データベースの実行中にインスタンスをアクティブ化しようとしたが、まだアクティブでない	activate によって返され、DB インスタンスが実行中であるためアクティブ化を行えなかったことを示します。
21	データベースの実行中にインスタンスを非アクティブ化しようとしたが、まだ非アクティブでない	deactivate によって返され、DB インスタンスが実行中であるため非アクティブ化を行えなかったことを示します。
22	ユーザーは許可されていない	instrument と activate によって返され、指定された db-user が「guardium」グループのメンバーとして許可されていないことを示します。修正するには、authorize-user を実行します。
23	db-home パラメーターが guard_tap.ini の db_install_dir パラメーターと一致しない	store-conf および activate によって返され、現在の guard_tap.ini に、db_install_dir ATAP パラメーターに一致する db_home で構成された IE がないことを示します。これらのいずれかを正しい値に調整しないと、STAP が実行されない恐れがあります。
24	実行可能ファイルが ATAP 実行プログラムでもインスツルメンテーション・バイナリーでもないインスタンスを非アクティブにしようとした	deactivate によって返されます。このインスタンスはアクティブにしておく必要があると思われますが、バイナリーが本来あるべき姿ではありません。ATAP がアクティブな間に DB 実行可能ファイルが更新された可能性があります。repair コマンドを実行して問題を修正し、再度アクティブ化してください。
25	guard_tap.ini に encryption=1 が設定されているときに ATAP をアクティブ化しようとした	IE で encryption パラメーターが 1 に設定されている場合に、activate によって返されます。guardctl でアクティブ化せず、ini の encryption パラメーターを使用します。
26	DB 実行可能ファイルが見つからない	activate、deactivate、instrument、deinstrument、store-conf、prepare-libs、および repair によって返されます。DB 実行可能ファイルがありません (例: Oracle バイナリー自体が指定されたパスにない)。 インスタンスの構成時に使用されたパス・パラメーターを確認してください。
27	インスツルメンテーションが必要だが実施されていない	インスツルメンテーションが必要であるが、まだ実施されていない場合に、activate と store-conf によって返されます。Oracle インスツルメンテーションは、ほとんどの場合は自動的に実行されるようになりましたが、AIX および Oracle のバージョン <= 10 に対しては引き続き手動で指定する必要があります。
28	is-active でインスタンスがアクティブでないと報告される	is-active によって返されます。情報提供のみです。指定された db-instance がアクティブではありません。または、インスタンスが指定されていない場合は、アクティブなインスタンスがありません。
29	deactivate-all が正常に完了しない	少なくとも 1 つのアクティブ・インスタンスを非アクティブ化できなかった場合に、deactivate-all によって返されます。
30	is-instrumented でインスタンスがインスツルメンテーションされていないと報告される	コマンドではエクスポートされません。
40	内部インスツルメンテーション・エラー	インスツルメンテーションを完了できなかった場合に、instrument によって返されます。
41	内部インスツルメンテーション・エラー	インスツルメンテーションを完了できなかった場合に、instrument によって返されます。
42	内部インスツルメンテーション・エラー	インスツルメンテーションを完了できなかった場合に、instrument によって返されます。
43	インスツルメンテーション・エラー。元のバイナリーを保存できない	-guard-original ファイルが既に存在する場合に、instrument によって返されます。A-TAP がインスツルメンテーションとともに現在アクティブであるか、A-TAP は非アクティブであるがインスツルメンテーションがまだアクティブであるかのいずれかです。 後続の instrument および activate が実施される前に、非アクティブ化してインスツルメンテーションを削除します。
44	インスタンスの実行中にインスツルメンテーションを試行し、まだインスツルメンテーションされていない	DB インスタンスが現在実行中のときに instrument によって返されます。DB インスタンスを停止してから、再びインスツルメンテーションを試行してください。
45	A-TAP がアクティブな状態でインスツルメンテーションを試行し、まだインスツルメンテーションされていない	A-TAP は既にアクティブであるが、インスツルメンテーションがアクティブでない場合に、instrument によって返されます。これは、インスツルメンテーションを必要としない Oracle 構成から、必要とする構成に切り替える場合に発生する可能性があります。A-TAP を非アクティブにしてから、インスツルメンテーションを再試行してください。
46	インスツルメンテーションを試みたが、インスタンスが既にインスツルメンテーションされていた	インスタンスが既にインスツルメンテーションされている場合に instrument によって返されます。インスツルメンテーションを再実行する必要がある場合は、まずインスツルメンテーションを削除します。
94	このデータベースをサポートする ATAP ライブラリーがない	instrument、deinstrument、prepare-libs、activate、deactivate、repair、list-active、および list-configured によって返されます。通常は、不明なエラーが発生したことを示します。
93	アクティブ化中、非アクティブ化中、またはインスツルメンテーション中を除く、DB が実行中 (例: repair コマンドの実行中) であることによる詳細不明のエラー (例: repair コマンドを実行している場合)	
95	システム・エラー。グループが見つからない	activate によって返されます。guardium グループは、このシステムに認識されていない可能性があります。
96	システム・エラー。グループを作成できない	authorize-user によって返されます。guardium グループが存在しなかったため、このグループを作成しようとしましたが、失敗しました。
97	ファイル・システム・エラー。ディレクトリーまたはファイルを作成できないか、スペースの不足が発覚した	
98	サポートされないプラットフォーム	instrument、deinstrument、prepare-libs、activate、deactivate、repair、list-active、list-configured、store-conf によって返されます。ATAP で使用しようとしている DB は、このプラットフォームではサポートされていません (例えば、Linux 以外のプラットフォームでの Db2、Informix、Teradata、または mongo など)。
99	その他の詳細不明なエラー	

親トピック: A-TAP の管理

データベース固有の guardctl パラメーター

各データベース・タイプには、固有の guardctl 要件があります。

- Oracle 固有の guardctl パラメーター
  Oracle データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します。
- Sybase 固有の guardctl パラメーター
  Sybase データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します。
- Db2 (Linux のみ) 固有の guardctl パラメーター
  Db2 データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します (Linux のみ)。
- Informix 固有の guardctl パラメーター
  Informix データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します。
- Postgres 固有の guardctl パラメーター
  Postgres データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します。

親トピック: A-TAP の管理

Oracle 固有の guardctl パラメーター

Oracle データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します。

例:

/usr/local/guardium/guard_stap/guardctl --db-user=oracle11 --db-type=oracle --db-instance=on12rh60 --db-home=/home/oracle11/product/11.1.0/db_1 --db-version=11.2 store-conf

Oracle の必須パラメーター

必須パラメーター	値	判別方法
db-user	Oracle ユーザー名	データベース・インスタンス・ユーザー名を使用します。
db_instance	Oracle インスタンス名	$ORACLE_SID の値を使用します。
db_type	Oracle	
db_home	データベース実行可能ファイルのインストール場所。	
db_base	データベース・インスタンス・ユーザーのホーム・ディレクトリー	db_base の値は、$ORACLE_BASE またはデータベース・インスタンス・ユーザーのホーム・ディレクトリーの正しいパスと一致しなければなりません。DB_USER にすることはできません。
db_version	データベース・バージョン	次の SQL を実行: > SELECT * FROM V$VERSION

Oracle のオプション・パラメーター

オプション・パラメーター	値	判別方法	必要なとき
db_relink	no/yes	A-TAP の活動化方式	
db_use_instrumented	no/yes	A-TAP の活動化では、以前に guardctl の instrument コマンドで作成された、Oracle の再リンク済みバージョンが使用されます。	以下の場合にインスツルメンテーションが必要です。 • Windows 以外のすべてのプラットフォームでの Oracle 12 SSL • AIX での Oracle 11.2 SSL • 11.2 より前の AIX での Oracle ASO と SSL **重要:** レベル 10.1 のS-TAP では、インスツルメンテーションは「activate」コマンドまたは Guardium UI を使用して自動的に行われます。
db_bits	32 または 64	DB インスタンス・アーキテクチャー (32 ビットの場合は 32、64 ビットの場合は 64)	A-TAP がアーキテクチャーを認識できない場合にのみ必要。

親トピック: データベース固有の guardctl パラメーター

Sybase 固有の guardctl パラメーター

Sybase データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します。

Sybase の必須パラメーター

例:

/usr/local/guardium/guard_stap/guardctl --db-user=sybase15 --db-type=sybase --db-instance=sn57rh7x --db-version=15 store-conf

必須パラメーター	値	判別方法
db_user	Sybase ユーザー名	データベース・インスタンス・ユーザー名を使用します。
db_instance	Sybase インスタンス名	Sybase サーバー・インスタンス名
db_type	sybase	
db_version	データベース・バージョン	Sybase ユーザーとして以下を実行します。 > select @@version >go

Sybase のオプション・パラメーター

オプション・パラメーター	値	判別方法	必要なとき
db_home	データベースがインストールされている場所を提示します。	db_base と同じ	
db_base	データベース・インスタンス・ユーザーのホーム・ディレクトリー	DB インスタンス・ユーザーのホーム・ディレクトリー。db_base の値は、DB インスタンス・ユーザーのホーム・ディレクトリーの正しいパスに一致している必要があります。DB_USER にすることはできません。	db_base が db_home と同じでない場合。
db_bits	32 または 64	DB インスタンス・アーキテクチャー (32 ビットの場合は 32、64 ビットの場合は 64)	A-TAP がアーキテクチャーを認識できない場合にのみ必要。
db-tcp-min-port	0 から任意の整数	インターセプトする TCP ポート範囲の下限	実際の IP を使用している
db-tcp-max-port	0 から任意の整数	インターセプトする TCP ポート範囲の上限	実際の IP を使用している

親トピック: データベース固有の guardctl パラメーター

Db2 (Linux のみ) 固有の guardctl パラメーター

Db2 データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します (Linux のみ)。

Db2 (Linux のみ) の必須パラメーター

例:

/usr/local/guardium/guard_stap/guardctl --db-user=db2inst1 --db-type=db2 --db-instance=dn0rh7x6 --db-version=10.5 store-conf

必須パラメーター	値	判別方法
db_user	Db2 ユーザー名	DB インスタンス・ユーザー名を提示します
db_instance	Db2 インスタンス名	$ db2 LIST DATABASE DIRECTORY
db_type	db2	
db_version	データベース・バージョン	Db2 ユーザーとして実行: $ db2level

Db2 (Linux のみ) のオプション・パラメーター

オプション・パラメーター	値	判別方法	必要なとき
db_home	DB バージョンがインストールされている場所のパス	db_base と同じ	
db_base	データベース・インスタンス・ユーザーのホーム・ディレクトリー	db_base の値は、DB インスタンス・ユーザーのホーム・ディレクトリーの正しいパスに一致している必要があります。DB_USER にすることはできません。	db_base が db_home と同じでない場合
db_bits	32 または 64	DB インスタンス・アーキテクチャー (32 ビットの場合は 32、64 ビットの場合は 64)	A-TAP がアーキテクチャーを認識できない場合にのみ必要。
db2-shmsize	131072	Db2 共有メモリー・サイズ	値がデフォルト値と異なる場合
db2-c2soffset	61440	Db2 共有メモリー・クライアント域のオフセット	値がデフォルト値と異なる場合
db2-header-offset	20	Db2 共有メモリー・ヘッダーのオフセット	値がデフォルト値と異なる場合

親トピック: データベース固有の guardctl パラメーター

Informix 固有の guardctl パラメーター

Informix データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します。

Informix の必須パラメーター

例:

/usr/local/guardium/guard_stap/guardctl --db-user=informix --db-type=informix --db-instance=in17rh7x --db-version=11.70 store-conf

必須パラメーター	値	判別方法
db_user	Informix ユーザー名	DB インスタンス・ユーザー名を提示します
db_instance	Informix インスタンス名	Informix サーバー・インスタンス名
db_type	informix	
db_version	データベース・バージョン	Informix ユーザーとして実行: dbaccess -V

Informix のオプション・パラメーター

オプション・パラメーター	値	判別方法	必要なとき
db_home	DB バージョンがインストールされている場所のパス	db_base と同じ	
db_base	db_user のホーム・ディレクトリー	DB インスタンス・ユーザーのホーム・ディレクトリー。db_base の値は、DB インスタンス・ユーザーのホーム・ディレクトリーの正しいパスに一致している必要があります。DB_USER にすることはできません。	db_base が db_home と同じでない場合
db_bits	32 または 64	DB インスタンス・アーキテクチャー (32 ビットの場合は 32、64 ビットの場合は 64)	

親トピック: データベース固有の guardctl パラメーター

Postgres 固有の guardctl パラメーター

Postgres データベースに A-TAP を構成する場合には、以下の guardctl パラメーターを使用します。

Postgres の必須パラメーター

例:

/usr/local/guardium/guard_stap/guardctl --db-user=postgres --db-type=postgres --db-instance=guardium_qa --db-version=9.4 --db-base=/home/postgres94 store-conf

必須パラメーター	値	判別方法
db-user	Postgres ユーザー名	DB インスタンス・ユーザー名を提示します
db_instance	Postgres インスタンス名	Postgres サーバー・インスタンス名
db_type	postgres	
db_version	データベース・バージョン	Postgres ユーザーとして以下を実行します。 pg_ctl --version

Postgres のオプション・パラメーター

オプション・パラメーター	値	判別方法	必要なとき
db_home	DB バージョンがインストールされている場所を提示します。	db_base と同じ	
db_base	db_user のホーム・ディレクトリー	DB インスタンス・ユーザーのホーム・ディレクトリー。db_base の値は、DB インスタンス・ユーザーのホーム・ディレクトリーの正しいパスに一致している必要があります。DB_USER にすることはできません。	db-base が db-home と同じでない場合
db_bits	32 または 64	DB インスタンス・アーキテクチャー (32 ビットの場合は 32、64 ビットの場合は 64)	
db-tcp-min-port	0 から任意の整数	インターセプトする TCP ポート範囲の下限	実際の IP を使用する場合
db-tcp-max-port	0 から任意の整数	インターセプトする TCP ポート範囲の上限	実際の IP を使用する場合

親トピック: データベース固有の guardctl パラメーター

A-TAP の非アクティブ化

データベース OS をアップグレードする前に、A-TAP を非アクティブにする必要があります。

このタスクについて

手順

1. データベースが停止していることを確認します。すべてのアクティブ・データベース・セッションからログオフします。
2. データベースの A-TAP を非アクティブにします。
   `<guardium_base>/xxx/guardctl -db-instance=<instance-name> deactivate`
3. あるいは、以下を実行してすべてのアクティブ・インスタンスを非アクティブにします。
   `<guardium_base>/xxx/guardctl deactivate-all`

親トピック: A-TAP の管理

特殊な環境での A-TAP の構成とアクティブ化

ゾーン、WPAR、Teradata、および Oracle には、追加の構成が必要です。

- ゾーン環境および WPAR 環境での A-TAP のインストールとアクティブ化
- ゾーン環境および WPAR 環境での A-TAP の非アクティブ化とアンインストール
- ゾーン環境および WPAR 環境での ATAP のアップグレード
- Teradata データベースでの A-TAP の構成とアクティブ化の手順
- A-TAP の Oracle 構成

親トピック: A-TAP の管理

ゾーン環境および WPAR 環境での A-TAP のインストールとアクティブ化

このタスクについて

手順

1. 通常の方式で、STAP/KTAP をマスターまたはグローバルのゾーン/WPAR にインストールします。
2. Solarisゾーンの場合は、Oracle がインストールされているサブゾーンごとに、以下のようにして Guardium® デバイスがマップされていること確認してください。
   - zoneadm -z <zonename> halt
   - zonecfg -z <zonename>
   - <zonename>> add device
   - <zonename>device> set match=/dev/ktap_xxx (Solaris 10 の場合)
   - <zonename>device> set match=/dev/guard_ktap (Solaris 11 の場合)
   - <zonename>device> end
   - <zonename>> verify
   - <zonename>> exit
   - zoneadm -z <zonename> boot
3. KTAP デバイスが複数の場合、名前 ktap_xxxx (Solaris 10) または guard_ktap_x (Solaris 11) を使用して KTAP デバイスごとに手順を繰り返してください。
4. A-TAP インストール・ディレクトリー全体をサブゾーン/サブ WPAR にコピーします。仮に Guardium ソフトウェアが /usr/local/guardium の下のマスター・ゾーン/WPAR にインストールされており、サブゾーン/サブ WPAR に十分な空き領域がある書き込み可能ディレクトリー /usr/local が存在するとした場合には、マスターまたはグローバルのゾーン/WPAR で次のコマンドを実行します: `cd /usr/local; tar -cvf - guardium | ssh root@subzonehost 'cd /usr/local && tar -xvf -'`
5. A-TAP ライブラリーを各サブゾーン/サブ WPAR にコピーし、活動化します。
   - A-TAP をマスター・ゾーン/WPAR で活動化する場合は、guardctl を使用して通常どおりに活動化します。
     注: 活動化は guardctl を使用して行う必要があります。GUI インターフェースの検査エンジン・セクションで暗号化ボックスを有効にしたり、guard_tap.ini ファイルで encryption=1 を設定したりすることで活動化することはできません。
   - A-TAP がマスター・ゾーン/WPAR で使用されない場合は、guardctl を使用して、ライブラリーの使用準備をします。マスター・ゾーン/WPAR で以下のようにします。`/usr/local/guardium/bin/guardctl --db_instance=<instance-name> --db_type=<database-type> --db_version=<database-version> prepare-libs`
     注: A-TAP の活動化後、データベースで libguard-xxx.so が検出できないことが示される場合、このステップを再確認してください。
6. 任意の各サブゾーン/サブ WPAR で、ステップ 1 から 5 を使用してデータベース・インスタンスに A-TAP をインストールして活動化します。
   注: A-TAP (guardctl) の活動化では、以下に関する指摘と警告が出されることがあります。
   - /usr/lib の下にライブラリーをインストールする際のエラー (そのディレクトリーがグローバル/マスター・ゾーンに属しているため)
   - guard_tap.ini を、oracle ではなく oracle-guard をモニターするように変更できない
   - stap を再始動できない (マスター・ゾーンでのみ実行されているため)
7. 手動で guard_tap.ini ファイルを編集して、マスターまたはグローバルのゾーン/WPAR で guard_tap.ini ファイルを調整します。
   - 以下のように、対応する db_exec_path 行を変更します。
     - Solaris 上の Oracle の場合: db_exec_path を oracle ではなく oracle-guard-original に設定します
     - AIX 上の Oracle の場合: db_exec_path を oracle ではなく oracle-guard-instrumented に設定します
   - IE 定義で参照されるファイルおよびディレクトリーを変更し、グローバル区画ではなく、WPAR のルート・ディレクトリーを基準とするようにします。(IE オーダー、tap_identifier のストリングなどは、すべての guard_tap.ini ファイルで同じでなければなりません。)
8. S-TAP を再始動します。
9. Solaris の場合、各々のサブゾーンで guard_ktap リンクと許可を確認します。この操作は、グローバル/マスター・ゾーンから **root** として実行する必要があります。
   a. サブゾーン・デバイス・ディレクトリーに移動します。例: `cd /export/home2/zones/iris3/dev`

b. KTAP デバイスが存在することを確認します (存在しない場合、ステップ 2 のインストールに問題があります): `ls -l kmmodreg*`
c. guard_ktap シンボリック・リンクが存在することを確認します。`ls -l guard_ktap`
d. 存在しない場合は、作成してください。(注: ktap_xxxxx はリストされたデバイスです): `ln -fs ktap_xxxx guard_ktap`

以下に例を示します。

```
-bash-3.00# ln -fs ktap_83164_0 guard_ktap
-bash-3.00# ln -fs ktap_83164_1 guard_ktap1
-bash-3.00# ln -fs ktap_83164_2 guard_ktap2
-bash-3.00# ln -fs ktap_83164_3 guard_ktap3
-bash-3.00# ln -fs ktap_83164_4 guard_ktap4
-bash-3.00# ln -fs ktap_83164_5 guard_ktap5
```

e. guard_ktap と ktap_xxxxx をすべてのユーザーが使用できるようにします。

```
chmod 0666 ktap_xxxxx_0
chmod 0666 ktap_xxxxx_1
chmod 0666 ktap_xxxxx_2
chmod 0666 ktap_xxxxx_3
chmod 0666 ktap_xxxxx_4
chmod 0666 ktap_xxxxx_5
chmod 0666 guard_ktap
chmod 0666 guard_ktap1
chmod 0666 guard_ktap2
chmod 0666 guard_ktap3
chmod 0666 guard_ktap4
chmod 0666 guard_ktap5
```

注: ATAP、WPAR/ゾーンを使用する場合、暗号化されたトラフィックと暗号化解除されたトラフィックでは、アナライザーに送られる際に IP が異なります。したがって、WPAR/ゾーンの db_user は無意味です。

10.

親トピック: 特殊な環境での A-TAP の構成とアクティブ化

ゾーン環境および WPAR 環境での A-TAP の非アクティブ化とアンインストール

このタスクについて

手順

1. A-TAP がインストール/活動化されているすべてのサブゾーン/サブ WPAR で、以下のようにします。
   a. A-TAP の非アクティブ化 のステップに従い、guardctl を使用してすべての A-TAP を非アクティブにします (AIX 上の Oracle の場合は、必要に応じてインスツルメンテーションの削除も行います)。
   b. インストール・ディレクトリーを手動で削除 (`rm -rf`) します
   c. 以下のようにして、ATAP ライブラリーを手動で削除します `find /usr/lib -type f -name 'libguard-*.so' | xargs rm -f`

   注: ライブラリーを削除する際にエラーが出されることがありますが、無視できます。
2. 通常の方式で、STAP/KTAP をアンインストールします
   a. 以下のようにして、ライブラリーを削除します `find /usr/lib -type f -name 'libguard-*.so' | xargs rm -f o`
   b.
   c. Solaris では、以下のようにして各ゾーンの構成から ktap デバイスを削除します。

```
zoneadm -z <zonename> halt
zonecfg -z <zonename>
<zonename>> info
```

ktap デバイスが検出された場合は、それを削除します。

```
/<zonename> remove device match=/dev/ktap_xxxx (Solaris 10 の場合)
/<zonename> remove device match=/dev/guard_ktap (Solaris 11 の場合)
<zonename>> verify
<zonename>> exit
zoneadm -z <zonename> boot
```

   d. それぞれのサブゾーン/サブ WPAR デバイス・ディレクトリーから、以下の例のように ktap デバイス・ファイルとリンクを削除します。

```
/export/home2/zones/iris3/dev cd /export/home2/zones/iris3/dev
rm -f ktap_xxxx guard_ktap
```

   e. KTAP デバイスが複数の場合、名前 ktap_xxxx (Solaris 10) または guard_ktap_x (Solaris 11) を使用して KTAP デバイスごとに手順を繰り返してください。

親トピック: 特殊な環境での A-TAP の構成とアクティブ化

ゾーン環境および WPAR 環境での ATAP のアップグレード

このタスクについて

手順

1. Solaris Zone の場合:
   a. マスター/グローバル・ゾーンで、以前にインストールした ktap デバイスを削除します。

```
zoneadm -z <zonename> halt
zonecfg -z <zonename>
```

```
<zonename>> info
```

b. ktap デバイスが検出された場合は、それを削除します。

```
/<zonename> remove device match=/dev/ktap_xxxx (Solaris 10 の場合)
/<zonename> remove device match=/dev/guard_ktap (Solaris 11 の場合)


<zonename>> verify
<zonename>> exit
zoneadm -z <zonename> boot
```

c. Solaris サブゾーンについては、サブゾーン・デバイス・ディレクトリーから以前の ktap デバイス・ファイルとリンクを削除します。サブゾーン・デバイス・ディレクトリー (例えば /export/home2/zones/iris3/dev) に移動します。

```
cd /export/home2/zones/iris3/dev
rm -f ktap_xxxx guard_ktap
```

2. Solaris Zone の場合:
   a. マスター/グローバル・ゾーンで、以下のようにして新しい K-TAP デバイスをゾーン構成に追加します。

```
zoneadm -z <zonename> halt
zonecfg -z <zonename>
<zonename>> add device

<zonename>device> set match=/dev/ktap_xxxx (Solaris 10 の場合)
<zonename>device> set match=/dev/ktap_xxxx (Solaris 11 の場合)

<zonename>device> end
<zonename>> verify
<zonename>> exit
zoneadm -z <zonename> boot
```

   b. guard_ktap リンクを追加し、アクセス権を変更します。サブゾーン・デバイス・ディレクトリー (例えば、サブゾーン・デバイス・ディレクトリーは /export/home2/zones/iris3/dev です) に移動します。

```
cd /export/home2/zones/iris3/dev
ln -fs ktap_xxxx guard_ktap
chmod 0666 ktap_xxxx
chmod 0666 guard_ktap
```

   c. 複数の ktap デバイスがあるため、名前 ktap_xxxx_x (solaris 10) または guard_ktap_x (solaris 11) を使用して、ktap デバイスごとに Doberman 用に公表されているステップを繰り返します。
3. AIX WPAR の場合は、ktap デバイスに対するアクセス権を変更します。WPAR デバイス・ディレクトリー (例えば、WPAR デバイス・ディレクトリーは /wpars/odin3/dev です) に移動します。

```
ln -fs ktap_xxxx guard_ktap
chmod 0666 ktap_xxxx
chmod 0666 guard_ktap
```

親トピック: 特殊な環境での A-TAP の構成とアクティブ化

Teradata データベースでの A-TAP の構成とアクティブ化の手順

ステップ 1: gtwgateway を実行しているユーザーおよびパスを判別します。

以下に例を示します。

su11u1x64-tera:~ # ps -ef | grep gtwgateway

teradata 5000 4608 0 Jan03 ? 00:00:05 /usr/tgtw/bin/gtwgateway

root 20128 20063 0 12:35 pts/0 00:00:00 grep gtwgateway

ユーザー teradata として gtwgateway を実行します。

guardctl に対してパラメーター *--db-user=teradata* を設定します。

gtwgateway のパスは /usr/tgtw/bin/gtwgateway です。これは、パラメーター tdc_gtwgateway のデフォルト値であり、この値自体は指定する必要はありません。

そうでない場合、このパラメーターは *--tdc_gtwgateway=/usr/tgtw/bin/gtwgateway* と指定する必要があります。

ステップ 2: pdemain のパスを判別します。

通常、これは /usr/pde/bin/pdemain です。

以下に例を示します。

su11u1x64-tera:~ # ps -ef | grep pdemain

root 4608 1 0 Jan03 ? 00:00:25 pdemain –debug

su11u1x64-tera:~ # ls -l /proc/4608/exe

lrwxrwxrwx 1 root tdtrusted 0 2015-01-03 01:20 /proc/4608root 20620 20063

0 12:40 pts/0 00:00:00 grep pdemain/exe ->

/opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

このファイルおよび /usr/pde/bin/pdemain の inode を調べ、それらの inode は同じであることが分かりました。

su11u1x64-tera:~ # ls -li /opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40

/opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

su11u1x64-tera:~ # ls -li /usr/pde/bin/pdemain

1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40

/usr/pde/bin/pdemain

inode が同一であり、*--db-home* のデフォルト値が */usr/pde* であるため、この場合にはこのパラメーターを指定する必要はありません。そうでない場合、--db-home=/opt/teradata/tdat/pde/15h.00.00.07 または --db-home=/usr/pde を指定できます。このケースでは、両方のパスの bin/pdemain が、ハードリンクされた同一ファイルであるためです。

ステップ 3: Teradata インスタンスを停止します。

以下に例を示します。

su11u1x64-tera:~ # /etc/init.d/tgtw stop

tgtw Shutdown complete

su11u1x64-tera:~ # /etc/init.d/tpa stop

PDE stopped for TPA shutdown

ステップ 4: DB ユーザーに対して Guardium グループの権限を付与します。

以下に例を示します。

/usr/local/guardium/guard_stap/guardctl --db-instance=teradata authorize-user

ステップ 5: ステップ 1 および 2 で決定したパラメーターを使用して、A-TAP の構成を保管します。

以下に例を示します。

/usr/local/guardium/guard_stap/guardctl --db-instance=teradata

--tdc_gtwgateway=/usr/tgtw/bin/gtwgateway --db-type=teradata

--db-home=/opt/teradata/tdat/pde/15h.00.00.07 --db-user=teradata store-conf

ステップ 6: A-TAP を活動化します。

以下に例を示します。

/usr/local/guardium/guard_stap/guardctl --db-instance=teradata activate

ステップ 7: Teradata インスタンスを再始動します。

以下に例を示します。

su11u1x64-tera:~ # /etc/init.d/tpa start

Teradata Database Initiator service is starting...

Teradata Database Initiator service started successfully.

su11u1x64-tera:~ # /etc/init.d/tgtw start

tgtw Startup complete

親トピック: 特殊な環境での A-TAP の構成とアクティブ化

A-TAP の Oracle 構成

Oracle パッチ・インストールを処理する場合の A-TAP の手順

Oracle パッチは relink を起動して、Oracle 実行可能ファイルを置換する場合がありますが、その結果 A-TAP の機能が停止します。

正しい手順は、以下のとおりです。

1. すべての A-TAP インスタンスが非活動化されていることを確認します
2. Oracle パッチを適用します
3. A-TAP を活動化します

ただし、Oracle パッチ・インストールの前に A-TAP が正しく非活動化されなかった場合、パッチ・インストールの後でそれを非活動化しようとしないでください。代わりに、以下の手順を実行します。

1. A-TAP に問題がないことを確認します。

```
grep guardium $ORACLE_HOME/bin/oracle >& /dev/null && echo "ATAP IS OK"
```

a. `ATAP IS OK` が表示された場合、A-TAP は引き続きアクティブなので、何もする必要はありません。
b. `ATAP IS OK` が表示されない場合、$ORACLE_HOME/bin/oracle-guard を削除し、A-TAP を活動化します。

すべての方法が失敗した場合は、以下のようにします。

- $ORACLE_HOME/bin/oracle-guard を削除します。
- relink all を実行します。

Oracle のアクセス許可に関する A-TAP の問題と解決策

ユーザーとグループのアクセス権に関連したいくつかの問題が発生することがあります。

- データベースをインストールしたユーザー以外のユーザーからの「BEQUEATH」アクセスでは、以下のように、アクセス権を手動で設定する必要があります。
  - sqlplus を実行しているユーザーをグループ「guardium」に追加します
  - 以下の 2 つのディレクトリーで「chmod a+rx」により読み取り権限を開きます

    ```
    /usr/local/guardium/xxx/etc/guard
    /usr/local/guardium/xxx/etc/guard/executor
    ```

  - ${ORACLE_HOME}/bin/oracle で、SUID ビットと SGID ビットがオンであることを確認します。
    - オンでない場合は、コマンド chmod ug+s ${ORACLE_HOME}/bin/oracle') を実行します。
- A-TAP は、グループ guardium のメンバーでない場合は、K-Tap デバイスをオープンできないので、次の syslog メッセージが表示されます。`ATAP [UID= GID= EUID= EGID=] Opening ktap '' [OWNER UID= GID= PERMS=]: Permission denied`
- UID または EUID が OWNER グループ GID のメンバーでない場合、Permission denied の理由は、UID または EUID に一致するユーザーが、OWNER GID に一致するグループに属していないことです。
- グループ Guardium への自動追加を無効にする一方で、ユーザーおよびグループの追加にさまざまな OS 構文を処理せずに済むようにして、処理を簡易化するために、guardctl 内で次の 2 つのコマンドを使用できます。これらは、ATAP のアクティブ化に使用する方法 (guardctl または guard_tap.ini) にかかわらず、使用できます。
  - #/path/to/guardium/bin/guardctl is-user-authorized
  - #/path/to/guardium/bin/guardctl authorize-user ...

注: グループ Guardium は、groupdel guardium を使用して、ほとんどの OS で削除できます。ただし、削除した後で、それを正しく再作成して K-TAP デバイスのアクセス権を変更できるのは、guard_ktap_loader パラメーターだけです。
親トピック: 特殊な環境での A-TAP の構成とアクティブ化

A-TAP 構成の問題のトラブルシューティング

このセクションでは、A-TAP の構成中に起こる一般的な失敗、それらの症状、およびそれらを回避する方法をまとめます。

表 1. Oracle の一般的な失敗

症状	失敗	プラットフォーム	エラー・メッセージ	回避方法
活動化コマンドが失敗する。	誤った db_home パラメーター	すべて		db_home 名として必ず $ORACLE_HOME の値を指定してください。
活動化コマンドが失敗する。	OS ユーザーがログインした	すべて		OS ユーザーがログインしていないことを常に確認してください。 どのユーザーがログインしているかを確認するには、w コマンドを使用します。
データベースが始動しない。	誤ったインスタンス名	すべて	oracleon1jumbo-guard を実行できませんでした。該当するファイルまたはディレクトリーが存在しません。エラー: 該当するファイルまたはディレクトリーが存在しません。ORA-12547: TNS: 接続が失われました (Failed to execute oracleon1jumbo-guard: No such file or directory: No such file or directory ERROR: ORA-12547: TNS:lost contact)	db_instance 名として必ず $ORACLE_SID の値を指定してください。
トラフィックがログに記録されない。	db_version の誤りまたは欠落	AIX®		バージョンは、必ず数値 (例えば 10.2 または 9.2) で指定してください。バージョン番号の小数点の後には、1 桁しか指定できません。
活動化に失敗する。	Oracle-guard-instrumented が欠落している。	AIX	Missing Oracle-guard-instrumented.	最初に instrument コマンドを実行し、再リンクされ、インスツルメンテーションされた Oracle 実行可能ファイルを作成してください。

症状	失敗	プラットフォーム	エラー・メッセージ	回避方法
ATAP の活動化中にエラーが発生し、ユーザーが Oracle ファイルをクリーンアップして再試行する必要がある	不十分なディスク・スペース、インストールの終了		一致するモジュールが見つかりました。Oracle は /ngs/lpp/guardium/modules/ATAP/current/files/lib/libguard-atap-oraclestatic-any でサポートされています。ディスク・スペースをテストしています... cp : 0653-447 131072 バイトの書き込みを要求しましたが、126976 バイトしか書き込めませんでした。(Matching module found - oracle is supported by /ngs/lpp/guardium/modules/ATAP/current/files/lib/libguard-atap-oraclesta tic-any Testing for disk space... cp : 0653-447 Requested a write of 131072 bytes, but wrote only 126976.) ディスク・スペースが不足しています。ファイルをいくつか削除し、再試行してください。(Insufficient disk space - please delete some files and try again.)	db_space=8 を db_space=1 に変更してください。
guard_stap ログに、guard-atap-ctl の失敗が示される。	GIM_ROOT_DIR がモジュールへの絶対パスに設定されていない (例: /usr/local/guardium/modules)			guard_tap.ini ファイルを介して A-TAP をアクティブ化すると、encryption=1 が通知なく失敗します。これは、guard_stap を手動で実行する場合に、特に重要です。guard_stap を実行する際は、この環境変数が定義されていることを確認してください。

表 2. Db2 共通の失敗

症状	失敗	プラットフォーム	エラー・メッセージ	回避方法
トラフィックがログに記録されない。	db2_* パラメーターの誤りまたは欠落	Linux		『DB2® パラメーターの判別方法』を参照してください。

表 3. Informix の一般的な失敗

症状	失敗	プラットフォーム	エラー・メッセージ	回避方法
トラフィックが正しくログに記録されない。	db_version の誤りまたは欠落	Linux		バージョンは、必ず数値 (例えば 7 または 11) で指定してください。

親トピック: A-TAP の管理

Tee

Tee は非推奨になりました。この情報は、参照用としてのみ記載しています。

ローカル UNIX DB2 クライアントで Tee を使用するための準備

このトピックは、K-TAP メカニズムを使用してローカル接続をモニターする場合には適用されません。

Tee は、非カーネル・ベースのデータ収集メカニズムで、K-TAP の代わりに使用できるため、クライアントを明示的に Tee に接続することが必要です。

この手順は、S-TAP が DB2® サーバーにインストールされて、データ収集開始の準備ができるまで実行しないでください。ローカル DB2 クライアントが Tee を使用するためには、tee という名前のデータベース別名を作成し、クライアントのログイン・シーケンスを変更して、(DB2 サーバーではなく) tee にログインするようにします。

1. 管理アカウントを使用して、データベース・サーバー・システムにログオンします。
2. /etc/services ファイルで、クライアントがデータベースへの接続に使用するノード名の項目を見つけます。このファイル内の各項目の形式は、以下のとおりです。

   ```
   node_name port_number/protocol [aliases]
   例:
   db2inst1      50000/ tcp      # DB2 connection service port
   ```

   注: ノード名 (この例では db2inst1) とポート番号 (50000) を記録してください。 検査エンジンを構成する場合、これは、Tee 実ポートとして指定するポート番号です。
3. S-TAP で使用するために、1025 から 65535 までの範囲で未使用のポート番号を選択します。/etc/services ファイルで選択したポート番号を検索し、それが未使用であることを確認します。 検査エンジンを構成する場合、これは、Tee 聴取ポートとして指定するポート番号です。
4. db2 コマンドを入力して、db2 コマンド行インターフェースを開始します。このコマンドを実行するには、このコマンドを $PATH に追加するか、システム上でユーザーを db2 ユーザーに切り替える必要があります。
5. list node directory コマンドを入力して、すべての定義済みノードをリストします。以下に、極めて単純な例を示します。

   ```
   db2 => list node directory
   Node Directory
   Number of entries in the directory = 2
   ```

```
Node 1 entry:
 Node name                      = GACCTEST
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = TCPIP
 Hostname                       = merlin
Service name                    = 50000
Node 2 entry:
 Node name                      = LOCGOOSE
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = LOCAL
 Instance name                  = db2inst1
```

注: 前に示した /etc/services 項目では、インスタンス名 db2inst1 がサービス名 50000 に関連付けられていました。

6. catalog コマンドを使用して、Tee 聴取ポートとして割り当てられるポートに対して、ローカル・サーバー上にノードを作成します。例えば、goose という名前のサーバー上のポートに対して localtee という名前のノードを定義するには、次のコマンドを入力します。

```
db2 => catalog tcpip node localtee remote goose server 12344
DB20000I  The CATALOG TCPIP NODE command completed successfully.
DB21056W  Directory changes may not be effective until the directory cache is refreshed.
```

7. terminate コマンドを入力して、ディレクトリーを更新します。(これにより、db2 ユーティリティーが閉じます。)

```
db2 => terminate
DB20000I  The TERMINATE command completed successfully.
```

8. db2 コマンドを使用して db2 ユーティリティーを再始動してから、再度 list node directory コマンドを入力して、新規ノードが正しく定義されたことを確認します。引き続き、以下に単純な例を示します。 新規ノードがリストに表示されています。

```
db2 => list node directory
Node Directory
 Number of entries in the directory = 3
Node 1 entry:
 Node name                      = GACCTEST
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = TCPIP
 Hostname                       = merlin
 Service name                   = 50000
Node 2 entry:
 Node name                      = LOCALTEE
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = TCPIP
 Hostname                       = goose
 Service name                   = 12344
Node 3 entry:
 Node name                      = LOCGOOSE
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = LOCAL
 Instance name                  = db2inst1
```

9. データベース用に tee という名前のデータベース別名を構成します。 以下の例では、SAMPLE (これをご使用のデータベースの名前に置き換えてください) という名前のデータベースを使用します。

```
db2 => catalog database SAMPLE as tee at node localtee
DB20000I  The CATALOG DATABASE command completed successfully.
DB21056W  Directory changes may not be effective until the directory cache is
refreshed.
```

10. terminate コマンドを入力して、ディレクトリーを更新します。(これにより、db2 ユーティリティーが閉じます。)

```
db2 => terminate
DB20000I  The TERMINATE command completed successfully.
```

11. db2 コマンドを使用して db2 ユーティリティーを再始動してから、list database directory コマンドを入力して tee データベース別名が正しく定義されていることを確認します。引き続き、以下に簡単な例を示します。 新規データベースがデータベースのリストに表示されています (ここではリストの一部のみを示します)。

```
db2 => list database directory
System Database Directory
Number of entries in the directory = 6
Database 1 entry:
...
Database 3 entry:
 Database alias                       = DN0GOOSE
 Database name                        = SAMPLE
 Node name                            = DN0GOOSE
 Database release level               = a.00
 Comment                              =
 Directory entry type                 = Remote
 Catalog database partition number    = -1
Database 4 entry:
...
Database 5 entry:
 Database alias                       = TEE
 Database name                        = SAMPLE
 Node name                            = LOCALTEE
 Database release level               = a.00
 Comment                              =
 Directory entry type                 = Remote
 Catalog database partition number    = -1
```

12. 以下のように、quit コマンドを入力して Db2 ユーティリティーを閉じます。

```
db2 => quit
```

まだデータベース・サーバー・システムからログアウトしないでください。 検査エンジンを構成した後で、コマンド行 DB2 ユーティリティーを使用して 1 つ以上の SQL コマンドを入力し、別名接続を確認します。
13. データの収集を開始する準備ができたら、選択した Tee 聴取ポート (この例では 12344) で listen し、Tee 実ポート (この例では 50000) にメッセージを転送するように DB2 検査エンジンを定義します。他で説明しているように、DB2 検査エンジンに必要なその他すべてのプロパティーが設定されていることを確認してください。
14. DB2 コマンド行を使用して、ローカル tee プロセスを介したデータベース接続が正しく機能することを確認します。コマンド行から次のようなコマンドを使用してデータベースにログインします。sample はデータベース (または何らかの tee カタログ名)、db2inst1 はユーザー名、passwd はパスワード、および tee はデータベース別名です。

```
$ db2 connect to sample user db2inst1 using passwd
   Database Connection Information
 Database server        = DB2/LINUXX8664 9.7.0
 SQL authorization ID   = DB2INST1
 Local database alias   = SAMPLE
```

15. SQL 例外を生成することがわかっているコマンド (例えば、select * from my_mistake) を入力して、セッションを終了します。
16. Guardium システム上のユーザー・ポータルにログインし、「レポートとアラート」-「レポート・テンプレート」-「例外」タブにナビゲートして、SQL エラー・レポートを選択します。SQL エラーはレポートの先頭付近にあるはずなので、これを見つけて tee が Informix® トラフィックを参照していることを確認してください。
17. 次に、すべてのクライアント・ログインを変更して、(DB2 サーバーではなく) tee 別名にログインします。

ローカル Unix Informix クライアントで Tee を使用するための準備

このトピックは、K-Tap メカニズムを使用してローカル接続をモニターする場合には適用されません。Tee は、非カーネル・ベースのデータ収集メカニズムで、K-TAP の代わりに使用できるため、クライアントを明示的に Tee に接続することが必要です。

この手順は、S-TAP が Informix サーバーにインストールされて、データ収集開始の準備ができるまで実行しないでください。ローカル Informix クライアントが Tee を使用するためには、/etc/services ファイルに staptcp サービス名を作成し、stap_sqlhosts ファイルを作成して、いくつかの環境変数を変更し、ローカル Informix クライアントが Informix サーバーではなく Tee 聴取ポートに接続するようにします。

1. sqlhosts ファイルを見つけます。 デフォルトのファイル名は sqlhosts で、これは、デフォルトでは $INFORMIXDIR/etc/ ディレクトリーにあります。デフォルトのファイル名とロケーションは、INFORMIXSQLHOSTS 環境変数を使用して指定変更できます。 この環境変数が存在する場合、これによってこのファイルの絶対パス名が定義されます。
2. sqlhosts ファイルのコピーを作成し、stap_sqlhosts という名前を付けます。 このコピーを変更します。 元の sqlhosts ファイルは変更しないでください。 このファイルに対する命名要件はありません。 今後、このセクションでは、stap_sqlhosts という名前を使用します。
3. stap_sqlhosts ファイルをテキスト・エディターで開きます。
4. ローカル・クライアントがデータベースへの接続に使用する項目を見つけます。 各項目には、複数の定位置パラメーターがあり、以下のような形式になっています。

```
dbservername netptype hostname servicename [options]
```

例:

```
jumboinformix onsoctcp jumbo    nettcp
```

5. サービス名のパラメーター値 (この例では nettcp) をメモしてください。 これにより、services ファイル内で、このデータベース・サーバーのポート番号にマップされているサービス名が識別されます。 後でこの名前を使用して、そのファイル内の項目を見つけます。
6. 指定したサービス名を S-TAP® の新規サービス名に置き換えます。 命名要件はありません。 ここでは、例として staptcp を使用します。 さらに、この例で、項目を以下のように変更します。

```
jumboinformix onsoctcp jumbo    staptcp
```

7. stap_sqlhosts ファイルを保存します。
8. services ファイルを見つけます。 デフォルトでは、これは /etc ディレクトリーにありますが、ネットワーク情報サービス (NIS) を使用している場合は、NIS サーバーで services ファイルを編集する必要があります。
9. このファイルのバックアップ・コピーを作成し、オリジナルを編集用に開きます。
10. services ファイルで、stap_sqlhosts ファイルで置き換えたサービス名の項目を見つけます。 このファイル内の各項目の形式は、以下のとおりです。

```
servicename port_number/protocol [aliases]
この例の services ファイルでは、nettcp 項目は以下のように定義されています。
nettcp      1400/tcp
```

注: ポート番号に注意してください (この例では 1400)。 検査エンジンを構成する場合、これは、Tee 実ポートとして指定するポート番号です。
11. S-TAP で使用するために、1025 から 65535 までの範囲で未使用のポート番号を選択します。services ファイルで選択したポート番号を検索し、それが未使用であることを確認します。 この例では、12344 を使用します。 検査エンジンを構成する場合、これは、Tee 聴取ポートとして指定するポート番号です。
12. 以下のように、この例の S-TAP 聴取ポート staptcp の services ファイルに 1 行追加します。

```
staptcp     12344/tcp
```

13. services ファイルを保存します。
14. 環境変数 INFORMIXSQLHOSTS を設定して、以前作成した sqlhosts ファイルの複製バージョンの絶対パス名を指定します。 例:

```
setenv INFORMIXSQLHOSTS $INFORMIXDIR/etc/stap_sqlhosts
```

15. データの収集を開始する準備ができたら、選択した Tee 聴取ポート (この例では 12344) で listen し、Tee 実ポート (この例では 1400) にメッセージを転送するように Informix 検査エンジンを定義します。
16. dbaccess コマンドを使用すると、クライアント SQL 要求が S-TAP によって参照されていることを確認できます。dbaccess を使用するには、3 つの環境変数 INFORMIXDIR、INFORMIXSERVER、および INFORMIXSQLHOSTS を適宜設定する必要があります。 以下のコマンドを使用して、これらの変数が正しく設定されていることを確認してください。

```
-bash-3.00# env | grep INFO
INFORMIXDIR=/data/informix
INFORMIXSERVER=jumboinformix
INFORMIXSQLHOSTS=/data/informix/etc/stap_sqlhosts
```

INFORMIXSERVER は、接続先となるデータベース・サーバー (この例の jumboinformix) を識別します。

INFORMIXSQLHOSTS は、jumboinformix への接続を解決するために使用する sqlhosts ファイルを識別します。 この解決中、これは共有メモリーまたは TCP 接続のいずれかになります。 前の定義では、これは staptcp というサービス名の付いた TCP 接続です。 これにより、/etc/services ファイルで解決された正しい TCP ポート 12344 に接続されます。

17. dbaccess コマンドを入力します。
18. 「接続」-「接続する」-「データベース・サーバーの選択」にナビゲートして、データベース・サーバー名 (この例では jumboinformix) を選択します。
19. プロンプトが出されたら、該当するデータベースのユーザー名とパスワードを入力します。
20. 構成の接続部分を終了して、「照会言語 - データベースの選択」を選択します。
21. 「新規」を選択して SQL コマンドを入力します (例: select * from my_mistake)。
22. Guardium システム上のユーザー・ポータルにログインし、「レポートとアラート」-「レポート・テンプレート」-「例外」タブにナビゲートして、SQL エラー・レポートを選択します。SQL エラーはレポートの先頭付近にあるはずなので、これを見つけて tee が Informix トラフィックを参照していることを確認してください。

ローカル Unix Oracle クライアントで Tee を使用するための準備

このトピックは、K-Tap メカニズムを使用してローカル接続をモニターする場合には適用されません。Tee は、非カーネル・ベースのデータ収集メカニズムで、K-Tap の代わりに使用できるため、クライアントを明示的に Tee に接続することが必要です。

この手順は、S-TAP が Oracle サーバーにインストールされて、データ収集開始の準備ができるまで実行しないでください。以下で概説する手順を使用して、サービス別名をポートにマップする tnsnames.ora ファイルを変更してください。 このファイルは、S-TAP がインストールされて、データ収集開始の準備ができるまで変更しないでください。

1. tnsnames.ora ファイルのバックアップ・コピーを作成します。 このファイルは $ORACLE_HOME/network/admin ディレクトリーにあります。
2. tnsnames.ora ファイルをテキスト・エディター・プログラムで編集用に開きます。
3. このファイルで、データベースへのアクセスに使用するサービス別名の項目を見つけます。 以下に、EAGLE ホスト上の EAGLE10 という名前の項目を示します。

```
EAGLE10 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = eagle)(PORT = 1521)))
    (CONNECT_DATA = (SERVICE_NAME = GUARD10))
   )
```

4. 使用するポート番号をメモしてください (この例では 1521)。検査エンジンを構成する場合、これは、Tee 実ポートとして指定するポート番号です。この項目は、S-TAP が正しく構成されていることが確認されるまで変更しないでください。
5. S-TAP で使用するために、1025 から 65535 までの範囲で未使用のポート番号を選択します。このファイルで選択したポート番号を検索し、それが未使用であることを確認します。 この例では、12344 を使用します。 検査エンジンを構成する場合、これは、Tee 聴取ポートとして指定するポート番号です。
6. 項目をコピーして貼り付け、変更内容を強調表示して、サービス用に重複項目を作成します。 この重複項目に LOCALTEE という名前を付けます。

```
LOCALTEE =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = eagle)(PORT = 12344)))
    (CONNECT_DATA = (SERVICE_NAME = GUARD10))
   )
```

7. tnsnames.ora ファイルを保存します。
8. データの収集を開始する準備ができたら、選択した Tee 聴取ポート (この例では 12344) で listen し、Tee 実ポート (この例では 1521) にメッセージを転送するように Oracle 検査エンジンを定義します。
9. sqlplus を使用してデータベース・サーバーにローカルでログオンし、S-TAP が正しく構成され、ローカル・アクセスを参照することを確認します。例:

```
# sqlplus scott/tiger@LOCALTEE
```

ここで、scott はデータベース・ユーザー名、tiger はパスワード、LOCALTEE はサービスを識別します。

10. 検出が容易な SQL 例外を生成するために、無効な SQL コマンドを入力します。 例: select * from my_mistake
11. Guardium システム上のユーザー・ポータルにログインし、「レポートとアラート」-「レポート・テンプレート」-「例外」タブにナビゲートして、SQL エラー・レポートを選択します。SQL エラーはレポートの先頭付近にあるはずなので、これを見つけて tee が ローカル Oracle トラフィックを参照していることを確認してください。
12. tnsnames.ora ファイルを再オープンし、データベース・サービスのポート番号を選択した番号に置き換えます。 さらに、この例では、以下のように EAGLE10 項目が UPDATED になります。

```
EAGLE10 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = eagle)(PORT = 12344)))
    (CONNECT_DATA = (SERVICE_NAME = GUARD10))
   )
```

13. tnsnames.ora ファイルを保存します。 次に、EAGLE10 に接続されているすべてのローカル・クライアントが、実データベース・ポート (Tee 実ポート) ではなく、ポート 12344 (Tee 聴取ポート) に接続されます。

ローカル Unix Sybase クライアントで Tee を使用するための準備

このトピックは、K-Tap メカニズムを使用してローカル接続をモニターする場合には適用されません。Tee は、非カーネル・ベースのデータ収集メカニズムで、K-Tap の代わりに使用できるため、クライアントを明示的に Tee に接続することが必要です。

以下の手順に従って、ローカル・インターフェース・ファイルを変更します。これにより、サーバーをポートにマップします。 このファイルは、S-TAP がインストールされて、データ収集開始の準備ができるまで変更しないでください。

1. interface ファイルのバックアップ・コピーを作成します。このファイルは $SYBASE/ ディレクトリー にあります。
2. interface ファイルをテキスト・エディター・プログラムで編集用に開きます。
3. このファイルで、名前が Sybase サーバー名に一致する項目を見つけます。 例えば、parrot という名前のサーバーは、以下のように定義されます。

```
parrot
    master tcp ether parrot 4100
    query tcp ether PARROT 4100
```

4. ポート番号 (この例では 4100) をメモしてください。 検査エンジンを構成する場合、これは、Tee 実ポートとして指定するポート番号です。
5. S-TAP で使用するために、1025 から 65535 までの範囲で未使用のポート番号を選択します。このファイルで選択したポート番号を検索し、それが未使用であることを確認します。 この例では、12344 を使用します。 検査エンジンを構成する場合、これは、Tee 聴取ポートとして指定するポート番号です。
6. ポート番号を選択した番号に置き換えます。 例:

```
parrot
    master tcp ether parrot 12344
    query tcp ether PARROT 12344
```

7. interface ファイルを保存します。
8. データの収集を開始する準備ができたら、選択した Tee 聴取ポート (この例では 12344) で listen し、Tee 実ポート (この例では 4100) にメッセージを転送するように Sybase 検査エンジンを定義します。

Tee から K-Tap への切り替え

アンインストールも再インストールも行わずに Tee から K-Tap に切り替えるには、以下の手順を実行します。この状態は、K-Tap のロードが失敗した後に生じている可能性があります。

1. S-TAP を無効にします。詳しくは、『UNIX S-TAP の停止』を参照してください。
2. inittab を使用しない Red Hat 6 では、inittab の guard_tee 行および guard_hnt 行をコメント化するか、適切な変更を行ってください。
3. 「init q」、または Red Hat の同等のコマンドを実行します。あるいは、tee ジョブおよびハンター・ジョブを単に強制終了します。
4. guard_tap.ini を編集し、ktap_installed を 1 に、tee_installed を 0 に変更します。
5. 「guard_ktap_loader install」コマンドを実行します。
   注: Linux の場合は、まず環境変数 NI_ALLOW_MODULE_COMBOS="Y" を設定してください。
   Linux の例:

```
NI_ALLOW_MODULE_COMBOS="Y"
/usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader install
```

   Linux 以外の例:

```
/usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader install
```

6. 「guard_ktap_loader start」コマンドを実行します。

```
example: /usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader start
```

7. S-TAPを再度有効にします。 詳しくは、『UNIX S-TAP の再始動』を参照してください。

親トピック: S-TAPs およびその他のエージェント

GUI からの S-TAP の構成

S-TAP エージェントをデータベース・サーバーにインストールした後、GUI から S-TAP の構成を実行できます。

S-TAP 制御 - S-TAP 構成を完了する

S-TAP 構成を変更するには、S-TAP のアクティブ・ホストである Guardium システムにログインしている必要があります。アクティブな ホストからのみ、S-TAP 構成を編集できます。構成の変更内容によっては、手動で S-TAP エージェントを再始動する必要が生じることがあります。

「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」をクリックして、「S-TAP 制御」を開きます。

「ローカル・タップ」セクションがない場合は、最初に、S-TAP エージェントを管理するように Guardium システムを構成する必要があります。 詳しくは、S-TAP を管理するための Guardium システムの構成を参照してください。

S-TAP の IP アドレス、または S-TAP がインストールされているデータベース・サーバーのシンボリック・ホスト名を探して、「S-TAP ホスト」列に構成する S-TAP を見つけます。 各 S-TAP には、以下の表で説明されている独自のコントロールがあります。

コントロール	記述
削除	S-TAP を除去するには、「削除」をクリックします。 アクティブな S-TAP はリストから削除できません。 削除をクリックしても、S-TAP は情報の送信を停止せず、その S-TAP の構成ファイルに保管されているホストのリストからこの Guardium ホストが削除されることもありません。 S-TAP の削除は、ある S-TAP が非アクティブになったことが分かった場合、またはその S-TAP の構成ファイルで Guardium 装置がホストとしてリストされなくなった場合に、表示をクリーンアップする際に役立ちます。どちらの場合も、S-TAP はオフライン状況では無期限に表示されます。
リフレッシ	「リフレッシュ」をクリックすると、S-TAP 構成の最新のコピーがエージェントから取り出されます。

ュ	
送信	再始動、バッファーの再初期化、診断の実行、あるいは S-TAP または K-TAP ロギングのパラメーターの変更を行う場合に、「送信」をクリックします。
STAP ロギング	S-TAP ロギング・パラメーターは以下のとおりです。 デバッグ・レベル: 0 - クリティカル・エラー情報のみ 1 - 前のレベルのすべての情報と、反復可能な非クリティカル・エラー情報 2 - 前のレベルのすべての情報と、データ脱落情報 (バージョン 4.03 以降では廃止) 3 - 前のレベルのすべての情報と、Guardium® コレクターに送られたパケットについての短い情報 4 - 前のレベルのすべての情報と、ローカル・スニッフィング・ログ 5 - 前のレベルのすべての情報と、ネットワーク・スニッフィング・ログ 6 - 前のレベルのすべての情報と、ハートビート受信ログ 7 - 前のレベルのすべての情報と、各種デバッグ情報 デバッグ期間秒数 : デバッグ・セッションの長さ (秒数)
バッファーの再初期化	S-TAP 要求に対して、バッファーを再初期化し、再始動することを伝えるメッセージを送信します。
KTAP ロギング	「関数名」および「デバッグ期間秒数」に入力します。
診断の実行	S-TAP で診断を実行します。 Windows では、デバッグ・ファイルは STAP_HOME/TempSnapshot/ に格納され、ファイル名は debug_Feb_25_2009_10_59_59.txt のようになります。 UNIX では、デバッグ・ファイルは、/tmp ディレクトリーに格納され、ファイル名は /tmp/guard_stap.stderr.txt になります。
編集	「編集」は、Guardium システムが S-TAP のアクティブ・ホストの場合のみ有効化されます。 注: IP ロード・バランサー環境で、S-TAP 構成の編集が無効になる場合があります。
情報ログ	S-TAP イベント・ログを表示します。
S-TAP ホスト	IP アドレスまたはホスト名
状況	S-TAP の状況 以下の 3 つのランプのいずれかが点灯します。 **グリーン** (オンライン) - S-TAP® は正常に機能しています。 **レッド** (オフライン) - S-TAP は応答していません。 **イエロー** (非同期) - 構成変更が S-TAP に送られましたが、S-TAP は変更が適用されたことをまだ確認できていません。 イエローが点灯した状態が長く続く場合は、S-TAP が新しい構成を受け入れなかったと想定できます。その場合、S-TAP は最後の適切な構成を使って再始動を試みます。 エラーが発生した場合、「ログの表示」をクリックして 「S-TAP イベント」パネルを別のウィンドウで開くことができます。多くの場合、新しい構成の問題点を示すエラー・メッセージがイベント・ログに含まれます。 最後の適切な構成を S-TAP ホストから再ロードするには、「S-TAP 情報のリフレッシュ」をクリックしてください。 注: ランプの色を判別しにくい場合は、一連のランプの上にマウス・ポインターを置くと、S-TAP の現在の状況 (オフライン、非同期、またはオンライン) が表示されます。
最後の応答	S-TAP からの最後の応答の日時

必要な変更を加えて、状況標識が緑色になっていることを確認します。状況標識が緑色でない場合は、Guardium システムと S-TAP は接続されていません。

1. 状況標識が緑色であることを確認します。. そうでない場合、Guardiumシステムと S-TAP が接続されていません。
2. その S-TAP の「編集」ボタンをクリックします。「編集」ボタンがアクティブになっていない場合、この Guardium システムはこの S-TAP のアクティブ・ホストではありません。何らかの変更を行うには、この S-TAP のアクティブ・ホストにログオンする必要があります。
3. 以下の任意の S-TAP 構成セクションを展開して変更します。通常、この時点での唯一の追加タスクは、1 つ以上の検査エンジンを定義することです。(検査エンジンはモニターするデータベース接続のセットを識別します。) 使用方法の詳細な説明を参照するには、以下のいずれかのセクションをクリックしてください。
   - S-TAP 制御 - 詳細
   - S-TAP 制御 - ハンター
   - S-TAP 制御 - 変更監査
   - S-TAP 制御 - アプリケーション・サーバー・ユーザー識別
   - S-TAP 制御 - Guardium ホスト
   - S-TAP 制御 - 検査エンジン
4. 何らかの情報を更新し、新規構成を保存する場合は、「適用」をクリックします。
5. S-TAP 制御パネルの状況ランプがグリーンになっていることを再び確認します。状況ランプがイエローに変わった場合は、リフレッシュ・ボタンを使って S-TAP 画面全体をリフレッシュしてみてください。引き続きイエローが点灯したままになる場合、S-TAP は新しい構成を使って再始動できませんでした。その場合、S-TAP は最後の適切な構成を使って再始動を試みます。S-TAP 制御パネルの中の構成には、適用済みの変更がまだ含まれています (何らかのエラーも含まれています)。最後の適切な構成を S-TAP ホストから「S-TAP 制御」パネルに再ロードするには、「S-TAP 情報のリフレッシュ」をクリックします。

S-TAP 制御 - 詳細

「S-TAP 制御」パネルの詳細セクションは、S-TAP エージェントの基本的な構成設定に適用されます。

コントロール	記述
バージョン	インストールされている S-TAP バージョン
デバイス	Windows サーバーでは常にブランクです。 UNIX サーバーの場合、KTAP の使用時 (現時点ではほとんどすべての場合)、デバイスは常に「なし」に設定する必要があります。
ロード・バランシング	このボックスは、S-TAP がトラフィックを Guardium システムにレポートする方法を制御します。 • 0 = すべてのトラフィックを単一の Guardium システムにレポートします (デフォルト)。 • 1 = ロード・バランシング。クライアント・ポート番号により、すべての Guardium システムに均等にセッションを分散します (単一セッションのトラフィックはすべて同じ Guardium システムに送られます)。 • 2 = 完全冗長。すべてのトラフィックをすべての Guardium システムにレポートします。 • 3 = IP ロード・バランサー環境で、Guardium システムが停止した場合、IP ロード・バランサーにより、S-TAP は異なる Guardium システムに再接続できます。 注: 複数の 1 次 Guardium システムを設定する必要はありません。これは、1 次マシンと 2 次マシンの優先度が同じであるためです。
メッセージ	S-TAP 処理メッセージ (データベース・トラフィックではない) が書き込まれる場所を、次のように制御します。 • **リモート** (アクティブな Guardium ホストに) • **Syslog** (データベース・サーバー上の syslog ファイルに) AIX では syslog メッセージがサポートされないため、通常であれば syslog に送られる S-TAP メッセージは、次のロケーションに書き込まれます: K-TAP ログは /var/log/ktap.log に、S-TAP ログ (S-TAP がデバッグ・モードの場合) は stdout/stderr に書き込まれます。
トレース・ファイル・ディレクトリー	トレース・ファイルが書き込まれるディレクトリーです。
代替 IP	このデータベース・サーバーへの接続に使われる 1 つ以上の代替または仮想 IP アドレス。これが使用されるのは、複数の IP または仮想 IP を持つ複数のネットワーク・カードがサーバーにある場合だけです。 この S-TAP 用に定義された S-TAP ホスト IP、またはリストされているいずれかの代替 IP に宛先 IP が一致する場合にのみ、S-TAP はトラフィックをモニターします。このため、すべての仮想 IP をここにリストすることをお勧めします。
共有メモリー	Windows のみ。 共有メモリー接続が検出された場合に実行するアクションを次のように制御します: • **無効化** (セッションを切断します) • **アラート** (アラートを送信します)
共有メモリー・モニター	Windows のみ。 チェック・ボックスにマークを付けると、共有メモリー・ドライバーが有効になります。パフォーマンスを改善するには、使用されないドライバーをすべて無効にしてください。 **注:** いずれかの共有メモリー・ドライバーを有効化または無効化した後、変更内容を有効にするには S-TAP サービスを再始動する必要があります。
MS SQL 暗号化	Windows のみ。 **注:** これらのいずれかのパラメーターを変更した後、変更内容を有効にするために S-TAP サービスを再始動して、MSSQL モニター・サービスを再始動する必要があります。 S-TAP が認識するトラフィックに適用される自動的な暗号化解除の種類を、次のように制御します。 **なし** - 自動的な暗号化解除なし。SSL トラフィックでの SQL はすべて無視されます。Kerberos トラフィックでの SQL はすべて認識されますが、データベース・ユーザー名は Kerberos により 16 進文字から成る文字列に置換されます。 **Kerberos と SSL** - 自動的に SSL を暗号化解除して Kerberos 名をマップします。対象となる一部のトラフィックで Kerberos が使われているものの、SSL が併用されていない場合には、このオプションを使用してください。対象となるすべてのトラフィックで Kerberos と SSL の両方が使われている場合は、「SSL のみ」オプションを使用してください。 **SSL のみ** - SSL トラフィックを自動的に暗号化解除します。対象となるすべてのトラフィックが SSL トラフィックである場合には、このオプションを使用します。このとき、たとえ Kerberos 認証が併用されていても重要ではありません。メッセージが暗号化される前、Kerberos が実際のデータベース・ユーザー名を置換する前に、S-TAP は必要な情報をすべて得るためです。
Kerberos 資格情報マッピング	Windows のみ。 Kerberos 認証が使われる場合に、S-TAP がデータベース・ユーザー名を得る方法を制御します。**「同期」**オプションを選択した場合、実際のデータベース・ユーザー名を解決するまで S-TAP は Guardium システムにメッセージを転送しません。したがってメッセージの量が非常に多い場合には一部のメッセージが失われる可能性があります。**「非同期」**オプションを使用した場合、すべてのメッセージが Guardium システムに転送されますが、S-TAP が実際のデータベース・ユーザー名を解決するまでは、新しい Kerberos チケットを使用するユーザーの初期セッションでデータベース・ユーザー名フィールドに 16 進文字の文字列が格納されます。

	始動時、同期 - 始動処理時に、S-TAP はドメイン・コントローラーから認証済みの全ユーザーを取得します。 これには非常に時間がかかることがあります。すべてのユーザーを取得して配置した後、S-TAP は Guardium システムにデータを送り始めます。認識できないユーザーからのメッセージを検出した場合は、「要求時、同期」で説明する方法でそのデータベース・ユーザー名を取得します。 **要求時、同期** - 認識されないユーザーの Kerberos メッセージを S-TAP が検出した場合、S-TAP はドメイン・コントローラーからユーザー名を取り出します。実際のデータベース・ユーザー名を得るまでは、そのユーザーからのトラフィックを Guardium システムに一切転送しません。 **要求時、非同期** - **要求時、同期**と同様です。ただし、データベース・ユーザー名が得られるのを待っている間、メッセージは保留されません。
TLS	**使用**: これを選択すると、TLS (暗号化) 接続を使用します。これは、S-TAP および CAS エージェントの両方に適用されます。この設定を変更する前に、この目的で使われるポートがサーバーと Guardium システムの間でファイアウォールによりブロックされていないことを確認してください。S-TAP のインストールの『Guardium のポート要件』表を参照してください。 **フェイルオーバー**: TLS 接続を確立できない場合に非 TLS 接続を使用できることを示します。 **TCP アライブ・メッセージ**: これにチェック・マークを付けると、S-TAP は既存の TCP 接続を介して 5 秒ごとに Guardium システムにアライブ・メッセージを送信します。これがブランクの場合、S-TAP は Guardium システムからの UDP メッセージに応答して、アライブ・メッセージを TCP によって送信します。 **注:**Windows のみ。この設定を変更した後、変更内容を有効にするには S-TAP サービスを再始動する必要があります。 **注:** TLS 接続では大量のトラフィックが発生して、暗号化による追加のオーバーヘッドも発生する可能性があるため、connection_pool_size パラメーターを使って追加的な接続が開かれることがあります (追加の CPU によりサポートされる場合)。
オートディスカバー	Windows の場合のみ、S-TAP を開始するたびに MSSQL データベースのディスカバリーを実行します。 新規 MSSQL データベースがディスカバーされると、検査エンジンが作成され、新規レコードがディスカバリー・ログに書き込まれます。 デフォルトは off です。

TLS 1.0/1.1 の無効化、TLS 1.2 の有効化

Guardium リリース v10.1.4 では、Guardium システムのセキュリティーを強化するために、通信プロトコル TLS 1.0/1.1 をオプションで無効にすることができます。

Guardium のお客様は、中央マネージャーまたはスタンドアロン・ユニット (あるいはその両方) からコマンド行インターフェースを使用して TLS 1.0/1.1 を無効にする必要があります。この新機能を有効にするには、お客様の Guardium アプライアンス、S-TAP エージェント、CAS クライアントおよび GIM クライアントが特定のバージョンでなければなりません。

TLS 1.1 を無効にすると、管理対象ユニットと S-TAP が特定のバージョンであることが自動的に確認されますが、CAS クライアントのバージョンは確認できません。CAS を使用するお客様は、ご使用の CAS クライアントがバージョン 10.1.4 になっていて、それらのデータベース・サーバーで Java 7 が使用可能になっていることを確認する必要があります。この確認を行わないと、データベース・サーバーへの CAS 接続を確認できなくなります。

また、お客様はすべての管理対象ユニットにバージョン 10.1.4 がインストールされており、GIM クライアントと S-TAP が最小バージョン 10.1.2 であることも確認する必要があります。すべての要求を満たさないと TLS 1.0/1.1 は無効になりません。TLS 1.0/1.1 を無効にすると、結果的に TLS 1.2 プロトコルが有効になります。

TLS 1.0/1.1 を無効にするためのステップ

admin ロールを持つ Guardium ユーザーは、CLI プロンプトで以下の GuardAPI コマンドを入力する必要があります。 これらのコマンドは、Guardium v10.1.4 の新しいコマンドです。

```
grdapi get_secured_protocols_info
```

この GuardAPI コマンドは、有効なプロトコル (TLS 1.0/1.1 および TLS 1.2) をリストし、非推奨のプロトコルを無効にできるかどうかを示します。エラー・コード 1000+ は、TLS 1.0/1.1 を無効にする前に管理者が対応する必要があるコンポーネントの問題を示します。表示されるメッセージには、TLS 1.0/1.1 を無効にするための要件を満たしていないコンポーネントが示されます。 警告メッセージは、オフラインまたは到達不能の管理対象ユニットに対して生成されます。オフラインのユニットは、オンラインに戻ったときに個別に管理する必要があります。以下の local_disable_deprecated_protocols を参照してください。

```
grdapi disable_deprecated_protocols
```

この GuardAPI コマンドは、まず上述のバージョン検査を実行します。無効化のための要件が満たされた場合、このコマンドは、中央マネージャーの各サービスおよびすべての管理対象ユニットの構成設定を変更します。

無効化のための要件が満たされなかった場合、このコマンドは、非推奨のプロトコルが有効であり、すべての管理対象ユニットまたはコンポーネント (あるいはその両方) がアップグレードされるまで有効のままにする必要があることを示します。

すべての構成変更が行われた後、admin ロールを持つ Guardium ユーザーは、中央マネージャーおよび管理対象ユニット間の通信が安定して正常に動作していることを確認する必要があります。

```
grdapi local_disable_deprecated_protocols
```

admin ロールを持つ Guardium ユーザーは、非推奨のプロトコルを無効化する際にオフラインだったすべての管理対象ユニットに対して、それらの管理対象ユニット上でコマンド行セッションを手動で開始し、local_disable_depreciated_protocols を実行して構成変更を行う必要があります。

```
grdapi enable_deprecated_protocols all=true
```

この GuardAPI コマンドは、構成設定を元に戻し、中央マネージャーのサービスとすべての管理対象ユニットを再始動して非推奨のプロトコルを有効にするフォールバックです。この GuardAPI コマンドは、中央マネージャーから all=true 引数を指定して実行し、中央マネージャーとすべての管理対象ユニットの非推奨のプロトコルを有効にすることができます。パラメーター all=true を指定しないと、非推奨のプロトコルは GuardAPI を実行するアプライアンスでのみ有効になります。

すべての構成変更が行われた後、admin ロールを持つ Guardium ユーザーは、中央マネージャーおよび管理対象ユニット間の通信が安定して正常に動作していることを確認する必要があります。TLS 1.0/1.1 の使用時にコミュニケーションの安全性が低くなる場合があることに注意してください。

S-TAP 制御 - ハンター

ハンターは推奨されなくなりました。この情報は、参照用としてのみ記載しています。

S-TAP のハンター・コンポーネントは Windows サーバー用には使用されず、推奨される UNIX S-TAP 構成でも使用されません。推奨されるカーネル・レベルのモニター・メカニズムではなく、TEE モニター・メカニズムが使われる場合に、UNIX S-TAP でオプションとしてこれが使用されます。

注: Solaris 11 のみ - Tee が最初にインストールされなかった場合は、再インストールが必要です。または、手動で TEE をインストールする必要があります。
注: K-Tap がインストールされている場合、ハンター・コンポーネントは非可視です。

ハンター・コンポーネントを使用する場合、データベース・サーバー上で検出されるすべての不正な接続をレポートして、オプションで強制終了するように構成できます。不正な接続とは、TEE メカニズムを迂回するすべての接続を指します。

コントロール	記述
ハント	構文 **db_type:process [,db_type:process]** を使用して、強制終了の対象となるプロセスを特定します。 **db_type** には以下を指定できます。 • DB2® • Informix® • Oracle • Sybase • PostgreSQL • Teradata **process** には以下を指定できます。 • **SHM** - 共有メモリー • **IPv4** - インターネット・プロトコル バージョン 4 • **IPv6** - インターネット・プロトコル・バージョン 6 • **FIFO** - 名前付きパイプ IPC メカニズム • **PIPE** - 単純な (名前なし) パイプ IPC • **INET** - インターネット・プロトコル (HPUX) これらの値は大/小文字の区別をせず、各項目と次の項目をコンマで区切ります。 **例**: 単純なパイプを使用する Oracle Bequeath プロセスを強制終了するには、以下のように入力します: oracle:pipe
スリープ時間	ハンターの不正プロセス検索ルーチンのランダムな開始時間の間隔の最大秒数。固定的なタイム・スロットまたはインターバルごとの実行による打破を難しくするために、開始時間はランダム化されます。スリープ時間の推奨値は、60 と 300 の間の任意の値です。
データベース	レポート対象のデータベース・タイプ (コンマ区切りのリストを使用します): • DB2 • Informix • Oracle • Sybase • PostgreSQL • Teradata

S-TAP 制御 - 変更監査

S-TAP 制御パネルの「変更監査」ペインは CAS (構成監査システム) エージェントにのみ適用されます。CAS 製品は、S-TAP とは無関係のオプションのコンポーネントですが、データベース・サーバー上にインストールされているすべての Guardium コンポーネントは、単一の構成ファイルを共有します。

コントロール	記述	
.	タスク・チェックポイント クライアント・チェックポイント	これらのファイルは再始動処理で使われます。この 2 つのファイル名に対して、それぞれ一連のファイルが作成されます。ファイルの各バージョンは固有の番号で終わります。UNIX のデフォルトはそれぞれ task_checkpoint および client_checkpoint です。Windows のデフォルトも同じですが、すべて大文字です。
チェックポイント期間	チェックポイント間の最大秒数。デフォルトは 60 です。	
フェイルオーバー・ファイル	Guardium システムに到達できない場合にデータの書き込み先となるファイルの名前。この期間に、ファイルは指定された最大サイズまで大きくなる可能性があります。制限に達した場合、同じ名前を使用し、名前の末尾に数字 2 を付加して、2 番目のファイルが作成されます。(これは CAS が 2 次サーバーへの接続試行を開始する時点です。) そのファイルもまた最大サイズに達した場合、最初のファイルが上書きされ、最初のファイルが再び満杯になると 2 番目のファイルが上書きされます。したがって、障害が長く続いた後にはデータをいくらか失う可能性がありますが、「フェイルオーバー・ファイルのサイズ制限」の 2 倍までの量のデータが確保されることになります。デフォルトは fail_over_file です。	
フェ	フェイルオーバー・ファイルの最大サイズ (KB 単位、デフォルトは 5000)。該当するファイルが 2 つ存在する	

イルオーバー・ファイルのサイズ制限	ため、ディスク・スペース所要量はここで指定する値の 2 倍です。-1 を指定するとファイル・サイズは無制限になりますが、そのような指定はせずにファイル・サイズを制限することを推奨します。
再接続最大試行回数	Guardium システムとの接続を失った後、CAS が再接続を試みる最大回数。この値を -1 に設定すると、最大回数が除去されます (CAS はいつまでも再接続を試行します)。デフォルトは 5000 回であり、デフォルト再接続間隔を使用すると約 3.5 日になります。最大値に達した後、CAS は (上記の説明のように) フェイルオーバー・ファイルに書き込みながら実行を続けますが、ホストへの再接続は試行しなくなります。
再接続間隔	再接続試行の間隔を示す秒数 (60)。**「再接続最大試行回数」**の再接続プロセスの説明を参照してください。
生データ制限	項目テンプレートの「データを保持」チェック・ボックスを選択した場合に 1 項目に対して書き込まれる最大キロバイト数 (1000)。-1 を指定すると無制限になります。
Md5 サイズ制限	これを超えると MD5 チェックサム計算を実行しなくなる、データ項目の最大サイズ (1000)。-1 を指定すると無制限になります。

S-TAP 制御 - アプリケーション・サーバー・ユーザー識別

「アプリケーション・サーバー・ユーザー識別」ペインは、エンド・ユーザー・アプリケーション ID モニター製品によって使用されます。エンド・ユーザー・アプリケーション ID モニター製品の詳細情報については、Guardium 販売担当またはサポートにお問い合わせください。

コントロール	記述
セッション・タイムアウト	タイムアウトの分数。デフォルトは 1800 です。
ポート	アプリケーション・サーバー・ポート。複数の項目はコンマで区切るか、ハイフンを使って包括的な範囲を指定します。デフォルトは 8080 です。
ログイン・パターン	ユーザー・ログインの識別に使われるパターン。
ユーザー名接頭部	Post/Get データでのユーザー名の始まり。
ユーザー名接尾部	Post/Get データでのユーザー名の終わり。
セッション・パターン	**新しい**セッションの識別に使われるパターン。
セッション接頭部	Post/Get データでのセッション ID の始まり。
セッション接尾部	Post/Get データでのセッション ID の終わり。
セッション ID パターン	**既存の**セッションの識別に使われるパターン。
セッション ID 接頭部	Post/Get データでのセッション ID の始まり。
セッション ID 接尾部	Post/Get データでのセッション ID の終わり。

S-TAP 制御 - Guardium ホスト

このペインには、S-TAP のホストとして定義されているすべての Guardium システムがリストされます。多くの場合、S-TAP のホストとして定義されるシステムは 1 つだけです。フェイルオーバーおよびロード・バランシング機能を提供するために追加のホストを定義することができます。Guardium S-TAP ホストは、以下の 3 つの用語を使って表されます。

用語	Guardium ホスト
アクティブ・ホスト	現在、この S-TAP が接続されているホスト。S-TAP 構成を変更する場合、アクティブ・ホストにログインする必要があります。通常、アクティブ・ホストが 1 次ホストになります。
1 次ホスト	この S-TAP からデータを受け取る (この S-TAP を制御する)、優先される Guardium システム。これは、S-TAP が再始動するたびに、または 1 次ホストとの接続の再確立後に S-TAP からの接続試行先となるホストです。
2 次ホスト	複数の Guardium システムが S-TAP のホストとして定義されている場合、1 次ホストとして指定されていない Guardium システムはすべて 2 次ホストです。S-TAP がアクティブ・ホストとの接続を失って 1 次ホストに再接続できない場合は、リストされた順序で 2 次ホストに接続しようとします。2 次ホストの管理者コンソールにログインすると S-TAP 構成を表示できますが、そのホストがその時点でのアクティブ・ホストでない限り、それを編集することはできません。

「S-TAP 構成」パネルの「Guardium ホスト」ペインには、以下で説明するコントロールが含まれています。示されているボタンは「S-TAP 構成」パネルでのみ使用可能であることに注意してください (「S-TAP 制御」パネルでは使用できません)。

コントロール	記述
アクティブ	この列のチェック・マークは、この S-TAP のアクティブ・ホストを示します。
Guardium ホスト	IP アドレスまたはシンボリック・ホスト名を使用して Guardium システムを指定します。
削除	これをクリックすると、関連付けられているホストが削除されます。この制御は、アクティブ・ホストの行には表示されません。
ダウン	これをクリックすると、関連付けられているホストがリスト内で 1 つ下の位置に移動します。
上	これをクリックすると、関連付けられているホストがリスト内で 1 つ上の行に移動します。
検査	1 次に設定。このホストをリストの先頭に移動して、1 次ホストとして指定します。

S-TAP 制御 - 2 次 Guardium ホストの定義

2 次ホストを定義する前に、2 次ホストの使用方法を理解しておく必要があります。S-TAP 管理ガイドの概要の『S-TAP エージェント用の 2 次 Guardium ホスト』を参照してください。

2 次ホストを定義するには、次のようにします。

1. 「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」をクリックして、「S-TAP 制御」を開きます。
2. リストされている最初のホストは S-TAP 用の 1 次ホストです。障害または再始動の後、S-TAP は 1 次ホストへの接続を最初に試みます。
3. 2 次 Guardium ホストの IP アドレスをテキスト・ボックスに入力します。
4. 「追加」をクリックします。
5. オプション。1 次ホスト (リストの先頭) として指定されるホストを変更するか、2 次ホストの間で順序を変更するには、以下のいずれかを行います。
   - 「下」または「上」をクリックして、リストを再配列します。
   - あるホストの行で「プライマリーに設定」をクリックすると、そのホストがリストの先頭に移動します。
6. オプション。2 次ホストを削除するには、それに対応する「削除」ボタンをクリックします。アクティブ・ホストは削除できません。
7. 完了したら、「適用」をクリックします。

注: 1 次ホストを変更した後、S-TAP でその新しい 1 次ホストを直ちに使い始める必要がある場合、それが Windows サーバーであれば、GUARD_STAP サービスを再始動する必要があります。UNIX サーバーでは、サービスの再始動は必要ありません。

S-TAP 制御 - 検査エンジン

「検査エンジン」ペインのレイアウトは、サーバーのオペレーティング・システム、データベース・プロトコル、(および UNIX システムの場合は K-Tap または TEE メカニズムが使用されるかどうか) に応じて異なります。

注: S-TAP をホストしている Guardium システム、または同じ Guardium システムにレポートしている別の S-TAP によって直接モニターされているネットワーク・トラフィックを、S-TAP 検査エンジンでもモニターするように構成しないでください。 そのような状況が発生すると、Guardium システムは重複する情報を受け取り、セッションを再構成できず、そのトラフィックを無視します。
注: 検査エンジンを編集するには、「変更」をクリックします。

コントロール	記述
プロトコル	モニターされるデータベース・サーバーのタイプ (Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share)。
ポート範囲	このデータベース・サーバーに関してモニターされるポートの範囲。通常は、単一のポートだけが範囲に含まれます。Kerberos 検査エンジンの場合、この値は常に 88-88 と示されるべきです。範囲を使用する場合、余分なポートを範囲に含めないでください。仮に含めた場合、S-TAP が不必要なトラフィックの分析を試みたときにリソースが過剰に消費されることがあります。
TEE 聴取ポート - 実ポート	Windows では使用されません。UNIX では、K-Tap モニター・メカニズムが使用される場合、KTAP データベース実ポートに置き換えられます。TEE モニター・メカニズムを使用する場合、これが必須です。聴取ポートは、S-TAP がローカル・データベース・トラフィックを聴取して受け入れるポートです。実ポートは S-TAP がトラフィックを転送するポートです。
KTAP データベース実ポート	Windows では使用されません。UNIX では、K-Tap モニター・メカニズムが使われる場合にのみ使用されます。K-Tap メカニズムによってモニターされるデータベース・ポートを識別します。
クライアント IP/マスク	モニター対象のクライアントを指定する、クライアント IP アドレスおよび対応するマスクのリスト。IP アドレスがデータベース・サーバーの IP アドレスと同じで、マスク **255.255.255.255** が使用される場合には、**ローカル・トラフィック**だけがモニターされます。アドレス/マスク値 **1.1.1.1/0.0.0.0** は、すべてのクライアントをモニターします。 リストを編集する際、追加の「クライアント IP/マスク」項目を作成するには、「追加」をクリックします。最後の「クライアント IP/マスク」項目を削除するには、「削除」をクリックします。 「クライアント IP/マスク」を指定した場合、「除外クライアント IP/マスク」を同時に指定することはできません。
除外クライアント IP/マスク	除外されるクライアントを指定する、クライアント IP アドレスおよび対応するマスクのリスト。このオプションを使用すると、特定のクライアントやサブネット (またはこれらの集合) を除くすべてのクライアントをモニターするよう S-TAP を構成できます。 リストを編集するときに追加の「除外クライアント IP/マスク」項目を作成するには、「追加」ボタンをクリックします。最後の「除外クライアント IP/マスク」項目を削除するには、「削除」をクリックします。 「除外クライアント IP/マスク」を指定した場合、「クライアント IP/マスク」を同時に指定することはできません。
接続先 IP	S-TAP がデータベースへの接続に使用する IP アドレス。一部のデータベースは、デフォルト (127.0.0.1) ではなく、マシンの実際の IP アドレスでのみローカル接続を受け入れます。
データベ	UNIX のみ。DB2、Informix、または Oracle の場合、データベース・インストール・ディレクトリーの絶対パス名を入力します (例: /home/oracle10)。他の

ース・インストール・ディレクトリー	すべての種類のデータベースの場合、NULL と入力します。
プロセス名	Windows サーバーの場合: Oracle または MS SQL Server のみ (名前付きパイプが使用される場合)。Oracle では、通常、2 つの項目 **oracle.exe**、**tnslsnr.exe** がリストに含まれます。MS SQL Server では、通常、リストは 1 つの項目 **sqlservr.exe** だけです。 UNIX サーバーの場合: DB2、Oracle、または Informix データベースでは、データベース実行可能ファイルの絶対パス名を入力します。 例: • Oracle: /home/oracle10/prod/10.2.0/db_1/bin/oracle • Informix: /INFORMIXTMP/.inf.sqlexec Informix: /INFORMIXTMP/.inf.sqlexec は、すべての Informix プラットフォームに適用されます (Linux を除く)。 Linux での Informix の例: /home/informix11/bin/oninit • MYSQL: mysql • PostgreSQL: POSTGRES.EXE, PG_CTL.EXE • Teradata: GTWGATEWAY.EXE • 他のすべての種類のデータベースの場合、NULL と入力します。
暗号化	Oracle (バージョン 11 と 12) および Sybase (Solaris、HPUX、および AIX 上) 用に ASO または SSL 暗号化トラフィックをアクティブ化します。Oracle の場合は、ini ファイル内に db_version を指定します (例: db_version=12)。Oracle 12 SSL については、すべてのプラットフォームでインスツルメンテーションを行います。Oracle 11 SSL については、AIX でインスツルメンテーションを行います。インスツルメンテーションを必要とするすべての Oracle では、guard_tap.ini で encryption=1 を使用する場合 (この設定は Linux ではサポートされていません)、そのパラメーターを設定する前にインスツルメンテーションを行っておく必要があります。
名前付きパイプ	Windows のみ。ローカル・アクセス用に MS SQL Server で使用される名前付きパイプの名前を指定します。名前付きパイプが使われる場合、ここで何も指定しなければ、S-TAP はレジストリーから名前付きパイプ名を取得しようとします。
インスタンス名	データベース・インスタンス名は、以下の場合に必要です。 • 暗号化を使用する MS SQL Server 2005、または Kerberos 認証を使用する MS SQL Server (デフォルトは MSSQLSERVER) • データベース暗号化を使用する Oracle (デフォルトはありません)
Db2 共有メモリー	以下の 3 つのフィールドは、データベース・タイプとして DB2 を選択した場合にのみ適用されます。共有メモリー接続がモニターされる場合、以下の 3 つのパラメーターを設定する必要があります。
調整	デフォルトは 20 です。
クライアント位置	デフォルトは 61440 です
サイズ	デフォルトは 131072 です。
ID	ID は、検査エンジンを相互に識別するために使用できるオプションのフィールドです。このフィールドに値を指定しない場合、Guardium は、データベース・タイプと GUI 表示シーケンス番号を使用して、固有の名前をこのフィールドに自動入力します。
追加	検査エンジンを追加する場合、必ず、「検査エンジンの追加」パネルで「追加」をクリックしてから、「構成」パネルで「適用」をクリックしてください。

検査レベルの応答の無視

この機能を使用して、S-TAP レベルのすべてのデータベース応答を無視します。このとき、Guardium システムには何も送信されません。

クライアントとのトランザクションのみが必要とされる特定の環境では、この機能を使用すると、S-TAP および Guardium システムの処理能力および処理時間が節約できます。

この機能は、データベースからの不要な応答を、ネットワークからのロードを行わずに無視するより簡単な構成を行うために使用します。

[TAP] セクション DB_IGNORE_RESPONSE

データベース・タイプをコンマ区切りでリストできます。また、すべてのタイプのデータベースからの応答を無視するには ALL を指定できます。以下の例を参照してください。デフォルトは none (なし) です。

none に設定した場合、どの応答も無視されないことを意味します。

all に設定した場合、すべての DB からの応答が無視されることを意味します。

DB_IGNORE_RESPONSE=MSSQL,SYBASE,DB2

DB_IGNORE_RESPONSE=all

DB_IGNORE_RESPONSE=none

DB_IGNORE_RESPONSE_BYPASS_BYTES (デフォルトは 1000)

DB_IGNORE_RESPONSE_BYPASS_TIMEOUT (デフォルトは 5 秒)

有効なデータベース・タイプ: ALL、CIFS、FTP、DB2_EXIT、PGSQL、MSSQL_NP、MSSQL、MYSQL、TRD、SYBASE、INFORMIX、DB2、ORACLE、KERBEROS。

CIFS/FTP 検査を追加するには、CIFS または FTP の固定ポートを使用します。 FTP では常にポート 21 が使用され、CIFS ではポート 139 またはポート 445 が使用されます。

FTP トラフィックの検査エンジンの構成は簡単です。 ネット検査の場合は、プロトコル FTP を選択してポートを 21 と入力し、通常どおりに IP/マスクを入力するだけです。 S_TAP の場合は、プロトコル FTP を選択してすべてのポートに対して 21 と入力し、IP/マスク (データベース・インストール・ディレクトリー、プロセス名、および名前付きパイプは不要) を入力します。

FTP スニッフィングは、クライアントとサーバーの間の FTP トラフィックを、データベース・トラフィックの場合と同様に探知する機能です。 FTP では、ログインに使用している有効なユーザーが存在する限り、任意のマシンをクライアントにすることができ (UNIX または Windows)、任意のシステムをサーバーにすることもできます。 ローカル FTP は存在しないことに注意してください。ただし、FTP は、ネットワーク検査またはネットワーク S-TAP スニッフィングのいずれでも探知できます。 FTP トラフィックは、通常、ポート 21 に出現します。 GDM_CONSTRUCT では、FTP トラフィックは、「_FTP」の後に送信済みの RAW FTP コマンドを伴って出現します (raw FTP コマンドは送信された実際の FTP とは異なることに注意してください)。

CIFS スニッフィング (または Windows ファイル共有スニッフィング) は、クライアントとサーバーの間の Windows ファイルの共有を、データベース・トラフィックの場合と同様に探知する機能です。 Windows でディレクトリーとファイルを共有する場合、この共有システムでは smb または Samba 言語がベースになり、Guardium システムはこれを探知して CIFS 言語に変換します。 Windows ファイル共有トラフィックを探知する場合は smbclient 関数を使用しますが、Windows 共有フォルダーへの UNIX 接続も使用します。ローカル CIFS は存在しないことに注意してください。 ただし、CIFS は、ネットワーク検査またはネットワーク Windows S-TAP スニッフィングのいずれでも探知できます。 CIFS サーバーのようなものがないことも注意してください。いずれの Windows マシンでも、ファイルを共有したり、共有ファイルにアクセスしたりすることができます。したがって、Windows マシンはクライアントまたはサーバーのいずれにもなることができます。 CIFS トラフィックは、通常、ポート 139 またはポート 445 のいずれかに出現します。 GDM_CONSTRUCT では、CIFS トラフィックは、「_CIFS」の後に送信済みの CIFS コマンドを伴って出現します。

S-TAP 制御 - 最後の適切な構成の再ロード

S-TAP 構成を変更した後、「S-TAP 制御」パネルでの状況ランプがイエローに変わることがあります。イエローの点灯は、Guardium システム上の構成と S-TAP 上の構成が一致しないことを意味します。S-TAP が新しい構成を受け取って承認するまでに少し時間がかかるため、一時的なイエローの点灯は許容されます。イエローの点灯が長く続く場合は、通常、S-TAP が新しい構成を受け入れず、認識される最後の適切な構成に復帰したことを意味します。

エラーが発生した場合、「レポート」 > 「リアルタイム Guardium 運用レポート」 > 「S-TAP イベント」を開いて、エラーを確認することができます。 ほとんどの場合、新しい構成の問題点を示すエラー・メッセージがイベント・ログに含まれます。エラー・メッセージの説明については、『S-TAP イベント・パネルの表示』を参照してください。

S-TAP および A-Tap の構成 - Linux で DB2 共有メモリーをモニターするための必須パラメーター

Db2 固有の S-TAP および A-Tap パラメーターは、以下のすべての条件が満たされる場合にのみ適用されます。

- DB2 サーバーが Linux で稼働している。
- K-Tap モニター・メカニズムがインストールされている。
- 共有メモリーを使ってクライアントが DB2 に接続する。

Db2 固有の S-TAP パラメーターは、検査エンジン定義パネルで設定されます。

db2bp で使われる共有メモリー・サイズに応じて、「Position」パラメーター値を次のように設定します。

- Position=61440 (db2bp が 131072 を使用する場合)
- Position=671744 (db2bp が 327680 を使用する場合)
- Position=1064960 (db2bp が 524288 を使用する場合)

db2bp で使用されている共有メモリー・サイズが分からない場合、以下の手順を使用してそれを見つけることができます。

db2 共有メモリー・オフセットを見つける方法

以下の表は、Linux 上で DB2 共有メモリーをモニターするよう構成されている場合に S-TAP および A-Tap で使われる必須パラメーターの要約です。

パラメーター	S-TAP 名	A-TAP 名	デフォルト値	コメント
パケット・ヘッダー・サイズ	db2_fixed_pack_adjustment	db2_header_offset	20	デフォルト値は、さまざまな 64 ビット・プラットフォーム上の DB2 8.2 以降に関してテストされています。他のバージョンの DB2 と 32 ビット・プラットフォームでは、異なるオフセットが必要である可能性があります。通常の値は 16 および 12 です。
クライアント入出力域オフセット	db2_shmem_client_position	db2_c2soffset	61440	このパラメーターは ASLHEAPSZ DB2 パラメーターから派生します。
Db2 共有メモリー・セグメント・サイズ	db2_shmem_size	db2_shmsize	131072	このパラメーターは経験的に決定されます。

クライアント入出力域オフセット (db2_shmem_client_position) の計算

1. Db2 インスタンス・ユーザーとして新しい bash シェルを開きます。
2. このシェルに関して db2bp コマンド・プロセッサーが現在実行中でないことを確認するために、ps -x コマンドを実行します。db2bp というコマンドが実行中と表示されないはずです。もし実行中であれば、kill するか、新しいシェルを実行します。
3. 以下のコマンドを実行します。

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print $9 * 4096}'
```

出力は、db2_shmem_client_position として必要な値です。

ASLHEAPSZ パラメーターは、DB2 では 4K メモリー・ページで指定されます。これは、アプリケーション・サポート・レイヤー・ヒープのサイズを決定します。 前の図に示すように、クライアント入出力域は、エージェント/アプリケーションの共有メモリー・セグメント内のアプリケーション・ヒープの直後に始まります。

注: この計算の理論は、「IBM DB2 管理ガイド: パフォーマンス」の資料に基づいています。

DB2 共有メモリー・セグメント・サイズ (db2_shmem_size) の取得

A-TAP と K-TAP は、このサイズに基づいてアプリケーション/エージェントの共有メモリー・セグメントを識別します。 これらのセグメントは、C2S パケットと S2C パケットに使用されます。この値の検出については、UNIX S-TAPの『DB2 共有メモリー・セグメント・サイズの取得』を参照してください。

親トピック: S-TAPs およびその他のエージェント

S-TAP 構成パラメーターの編集

S-TAP をインストールしてからその構成を変更するにはいくつかの方法があります。

ユーザーが、S-TAP のインストール・プロセス中に決定できないことがあったり、誤った決断をして、それがインストール・プロセスの完了後に検出されたりする場合があります。例えば、SQL Guard IP を定義する際に、IP アドレスを入力し忘れたり間違った IP アドレスを使用したりすることがあります。 このような誤りは、S-TAP® 構成ファイルを編集するか、S-TAP 構成を変更することにより修正できます。

S-TAP を Guardium Installation Manager (GIM) を使用してインストールした場合、GIM GUI または API を使用して一部のパラメーターを更新することができます。パラメーターを更新するためにこれらのいずれの方法も使用できない場合は、データ・サーバー上の構成ファイルを編集することができます。

以下の表には、S-TAP パラメーターの詳細な説明が用意されています。 これらには、Guardium GUI から更新できるパラメーターと、GIM を使用して更新できるパラメーターが示されています。

データベース・サーバーから構成ファイルを変更する必要がある場合は、概略手順に従ってください。このファイルには、パラメーターの多くについて説明するコメントが含まれています。

1. root アカウントを使用して、データベース・サーバー・システムにログオンします。
2. 構成ファイルをテキスト・エディターで開きます。
3. 必要に応じてファイルを編集します。
4. ファイルを保存します。
5. S-TAP を再始動して、変更が取り込まれているかどうかを確認します。

- Windows S-TAP パラメーター
  以下の表に、Windows 上の S-TAP の動作を制御するために使用されるパラメーターの定義を示します。
- UNIX S-TAP パラメーター
  以下の表に、UNIX 上の S-TAP の動作を制御するために使用されるパラメーターの定義を示します。

親トピック: S-TAPs およびその他のエージェント

Windows S-TAP パラメーター

以下の表に、Windows 上の S-TAP の動作を制御するために使用されるパラメーターの定義を示します。

表には、パラメーターごとに、以下の情報が示されています。

パラメーター
: パラメーターの名前。

バージョン
: このパラメーターがバージョン 8.0 以降で導入された場合、このパラメーターを使用できる最も古いバージョン。

GUI
: Guardium ユーザー・インターフェースによってパラメーターを変更できる場合は「はい」、変更できない場合はブランク。

デフォルト値
: パラメーターのデフォルト値。

記述
: 有効な値についての説明を含むパラメーターの意味。

注: パラメーターの説明が「拡張機能」で始まっている場合は、十分に経験を積んだユーザーであるか、IBM に相談済みである場合に限り、値を変更してください。

- SQLGuard パラメーター
  以下のパラメーターは、この S-TAP が接続できる Guardium システムを示します。
- 一般パラメーター
  これらのパラメーターは、Windows サーバー上で実行されている S-TAP および S-TAP のインストール先のサーバーの基本プロパティーを定義し、他のどのカテゴリーにも分類されません。
- 検査エンジン・パラメーター
  これらのパラメーターは、Windows サーバー上のデータ・リポジトリーをモニターするために S-TAP が使用する検査エンジンの動作に影響を与えます。
- ファイアウォール・パラメーター
  これらのパラメーターは、ファイアウォールに関する S-TAP の動作に影響を与えます。
- アプリケーション・サーバー・パラメーター
  S-TAP がデータベース・サーバーではなくクライアント・マシンにインストールされている場合、これらのパラメーターは S-TAP の動作に影響を与えます。
- デバッグ・パラメーター
  これらのパラメーターは、S-TAP デバッグの動作に影響を与えます。
- 構成監査システム (CAS) パラメーター
  これらのパラメーターは、このシステム上の CAS の動作に影響を与えます。
- ドライバー・パラメーター
  これらのパラメーターは、S-TAP が対話するいくつかのドライバーの動作に影響を与えます。

親トピック: S-TAP 構成パラメーターの編集

SQLGuard パラメーター

以下のパラメーターは、この S-TAP が接続できる Guardium システムを示します。

表 1. S-TAP 構成パラメーター: SQLGuard

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
sqlguard_ip		はい	はい	NULL	S-TAP のホストとしての役割を果たす Guardium システムの IP アドレスまたはホスト名。[SQLGuard_1]、[SQLGuard_2]、以降同様を追加することで、複数のホストを定義できます。
primary		はい	はい	1	サーバーが 1 次サーバーであるかどうかを示します: Windows: 0=NO、1=YES。 UNIX: 1= 1 次、2= 2 次、3= 3 次、以降同様。

親トピック: Windows S-TAP パラメーター

一般パラメーター

これらのパラメーターは、Windows サーバー上で実行されている S-TAP および S-TAP のインストール先のサーバーの基本プロパティーを定義し、他のどのカテゴリーにも分類されません。

これらのパラメーターは、S-TAP プロパティー・ファイルの [VERSION] セクションに格納されています。

表 1. [VERSION] セクションの S-TAP 構成パラメーター

パラメーター	バージョン	GUI	デフォルト値	記述
stap_client_build				読み取り専用。インストールされている S-TAP のビルド・バージョン
protocol_version				読み取り専用。Guardium システムのバージョン

これらのパラメーターは、S-TAP プロパティー・ファイルの [TAP] セクションに格納されています。

表 2. [TAP] セクションの S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
tap_type					読み取り専用。UNIX の場合は STAP、Windows の場合は WTAP
tap_version					読み取り専用。サーバーにインストールされている S-TAP のバージョン
tap_ip					S-TAP がインストールされているデータベース・サーバー・システムの IP アドレスまたはホスト名
all_can_control		はい		0	0= S-TAP は 1 次 Guardium システムからのみ制御できます。1= S-TAP は任意の Guardium システムから制御できます。
participate_in_load_balancing				0	以下のように、Guardium システムへのロード・バランシングを制御します。 • 0: ロード・バランシングなし。 • 1: ロード・バランシング。SQLGuard セクションで定義されている 1 次サーバーと 2 次サーバーの間でトラフィックのバランスを取ります。 • 2: 冗長。完全にミラーリングされた S-TAP によって、SQLGuard セクションで定義されているすべての 1 次サーバーと 2 次サーバーにすべてのトラフィックが送信されます。 • 3: ハードウェア・ロード・バランシング。Guardium では、F5 や Cisco などのロード・バランサーが使用されます。S-TAP はトラフィックをロード・バランサーに送信し、ロード・バランサーはそれをプール内のいずれかのコレクターに転送します。 1 次サーバー、2 次サーバーなどのサーバーを指定するには、SQLGUARD セクションでプライマリー・パラメーターを使用します。 このパラメーターが 0 に設定されているときに、複数の Guardium システムでトラフィックをモニターしている場合は、1 次以外の Guardium システムをフェイルオーバー用に使用することができます。
connection_timeout_sec				60	S-TAP が Guardium サーバーは使用不可であると見なすまでの秒数。任意の整数値を指定できます。
use_tls		はい	はい	0	1=SSL を使用して、エージェントと Guardium システムとの間のトラフィックを暗号化します。 0=暗号化しません。警告 - エージェントと Guardium システム間のトラフィックは平文です。 Guardium では、可能な場合は常に S-TAP とコレクター間のネットワーク・トラフィックを暗号化することを推奨しています。この暗号化を無効にする必要があるのは、パフォーマンスの優先順位がセキュリティーより高い場合のみです。
failover_tls		はい	はい	1	1= 何らかの理由で SSL 接続を使用できない場合は、非セキュア接続を使用するようにフェイルオーバーします。0= セキュア接続のみを使用します。
number_of_processors				4	読み取り専用。マシンのプロセッサー数。

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
alternate_ips				NULL	このデータベース・サーバーへの接続に使われる代替または仮想 IP アドレスのコンマ区切りのリスト。これが使用されるのは、複数の IP または仮想 IP を持つ複数のネットワーク・カードがサーバーにある場合だけです。この S-TAP 用に定義された S-TAP ホスト IP、またはここにリストされるいずれかの代替 IP に宛先 IP が一致する場合にのみ、S-TAP はトラフィックをモニターします。このため、すべての仮想 IP をここにリストすることをお勧めします。
db2_tap_installed				0	Db2 共有メモリー・トラフィックをスニッフィングするには 1 に設定します。 1 に設定する場合、Db2 TAP サービスを開始します。
db2_exit_driver_installed		はい			S-TAP への Db2 の統合: Db2 出口ライブラリー統合を有効にするには、1 に設定します。1) S-TAP が Db2 エンジンからすべての Db2 トラフィックをキャプチャーします。これは特定の Db2 リリース (10.1 以降) でのみ使用できることに注意してください。2) この方式を使用する場合、ファイアウォール、および修正機能と編集機能はサポートされません。また、ストアード・プロシージャーはキャプチャーされません。3) 暗号化プロトコルとネットワーク・プロトコルに関係なく、すべての Db2 トラフィックをピックアップすることができます。4) このソリューションは、このバージョンの Db2 を導入するユーザーの S-TAP 構成を簡素化し、固有の Db2 サポートをそれらのユーザーに提供します。
db2_shmem_driver_installed		はい			このパラメーターは非推奨になっており、db2_tap_installed に置き換えられています。 このパラメーターは、インストール後は常に 0 に設定されることに注意してください。
db2_shmem_driver_level					推奨されません
dc_collect_freq	9			24	収集の頻度を時間単位で指定します。 最小値は 1、最大値は 24 です。GuardiumDC は、ユーザー・アカウント (SID およびユーザー名) の更新を 1 次ドメイン・コントローラーから収集し、その後、Guardium_S-TAP にその変更内容をシグナル通知して、S-TAP 内部の SID/UserName のマップを更新するサービスです。S-TAP は、マップから解決済みの SID を見つけられない場合、1 次ドメイン・コントローラーからこれを取得しようとします。その場合、S-TAP は、デバッグ・ログ (レベル 7) にメッセージ「SID *** のアカウント名 *** を取得しました (`The account name *** has been retrieved for SID ***`)」を記録します。
dc_collect_maxusers	9			200,000	収集するユーザーの最大数。最小値は 10,000 です。
db_ignore_response	9				検査レベルの応答の無視。この機能を使用して、S-TAP レベルのすべてのデータベース応答を無視します。このとき、Guardium システムには何も送信されません。クライアントとのトランザクションのみが必要とされる特定の環境では、この機能を使用すると、S-TAP および Guardium システムの処理能力および処理時間が節約できます。この機能は、データベースからの不要な応答を、ネットワークからのロードを行わずに無視するより簡単な構成を行うために使用します。[TAP] セクションの DB_IGNORE_RESPONSE ではデータベース・タイプをコンマ区切りでリストできます。 また、すべてのタイプのデータベースからの応答を無視するには ALL を指定できます。 例えば、DB_IGNORE_RESPONSE=ALL または DB_IGNORE_RESPONSE=MSSQL,DB2 のように指定します。 サポートされる DB タイプ: ALL、MSSQL_NP、MSSQL、MYSQL、TRD、PGRS、MSSYB、 ORACLE、DB2、DB2_EXIT、INFORMIX、KERBEROS、FTP、CIFS。
domain_controller	9				SID/ユーザー名のマップを読み取る特定のコントローラーの名前。
high_resolution_timer				0	0: ミリ秒単位のタイム・スタンプを送信します。1: マイクロ秒単位のタイム・スタンプを送信しますが、ミリ秒のシステム・タイマーを使用します (これはシステム・パフォーマンス・ヒットを減らすためであり、ミリ秒数を 1000 倍します)。 2: マイクロ秒単位のタイム・スタンプを送信し、高解像度 Windows タイマーを使用します (最も正確)。 1 および 2 の場合、S-TAP は、PacketData 内の予約済みバイトを 1 に設定することにより、マイクロ秒が送信されていることを Guardium システムに示します。
buffer_file_size				50	パケット・キューに割り振られているバッファーのサイズ (MB 単位)。
buffer_file_name					BUFFER_MMAP_FILE=1 の場合、メモリー・マップ・ファイルの絶対パス。 デフォルトは、WSTAP 作業フォルダー /StapBuffer/STAP_buffer.dtx です。
buffer_mmap_file	9			0	1=メモリー・マップ・ファイルのオプション。0=仮想メモリーの割り振り。
software_tap_host					Windows のみ - S-TAP がインストールされているデータベース・サーバー・ホストを識別します。DNS サーバーによって認識されている IP アドレスまたは名前を指定できます。デフォルトはありません。構成が無効な SOFTWARE_TAP_HOST は、有効なローカル IP に自動的に置き換えられます。
tcp_alive_message	9			1	1=既存の TCP 接続に依存してアライブ・メッセージを 5 秒ごとに g-machine に送信します。 0=g-machine からの UDP メッセージに応答して、アライブ・メッセージを TCP によって送信します。 注: このパラメーターは、旧バージョンの Guardium (例えば、v9.x) で使用されます。Guardium コレクターは、UDP アライブ・メッセージを送信しなくなりました。このパラメーターの使用は Guardium v10.x より非推奨になりました。
stack_trace_file_mode					ダンプ・オプションと同様です。
minimum_heartbeat_interval				180	Windows のみ - S-TAP が Guardium システムのリストにある次のサーバーへの切り替えを試行する前に、アクティブな Guardium システムからのハートビートを待機する秒数。

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
tracefiles_dir					アクセス・トレーサー・ファイルが格納されるディレクトリー。デフォルトは INSTALLDIR です。
buffer_file_creation_max				3	使用されていない
compression_level				0	1 から 9 までの圧縮レベル。0=圧縮なし。
disable_shared_memory_if_turned_on				0	
file_sniffer_frequency				45	Windows のみ。次の項目の頻度 (秒): • 前の試行が成功しなかった場合の、Guardium システムへの登録の試行 • Program Files¥IBM¥Windows S-TAP¥Logs からコレクターにアップロードできる新しいログの S-TAP による確認
maximum_packet_num				300,000	推奨されません
min_bytes_to_compress				500	拡張機能。圧縮するメッセージの最小サイズ。
network_namedpipes		はい		0	拡張機能
not_send_to_sqlguard				0	拡張機能。Guardium システムに何も送信しません。
recv_level				0	拡張機能。
remote_messages		はい		1	1=アクティブな Guardium システムにメッセージを送信します。0=メッセージを送信しません。
send_level				0	高。スレッドの優先順位付けに使用されます。
sniffed_udp_ports				88	推奨されません。
synch_flag				1	読み取り専用。パラメーターが UI と同期されているかどうかを示します。
tap_dbserver_names					
tap_hb_udp_port				8075	Windows のみ。ハートビートおよびデータが、S-TAP のサーバーとしての役割を果たす任意の Guardium システムから S-TAP に送信される UDP ポート番号。
tap_min_heartbeat_interval				180	S-TAP がフェイルオーバーするまでの秒数。2 次コレクターへの S-TAP のフェイルオーバーについて connection_timeout_sec も参照してください。
tcp_buffer_size				60000	拡張機能。Guardiumにメッセージを送信する前に収集する最小バイト数。
time_network				0	拡張機能。デバッグにのみ使用します。
user_collector_level				0	拡張機能。
web_server_connections				1	.net アプリケーションによる DB 接続の最大数。
web_server_installed				0	推奨されません。以前は、IIS Tap の有効化に使用されていました。
web_server_port				9000	Web サーバーのポート。
guardium_ca_path				NULL	認証局証明書の場所。
sqlguard_cert_cn				NULL	Sqlguard 証明書で予期される共通名。
guardium_crl_path				NULL	証明書失効リストのファイルまたはディレクトリーへのパス。
tap_failover_session_quiesce				240	以前のアクティブ・サーバーからのフェイルオーバー・リストの未使用セッションを、現在のアクティブ・サーバーから削除できるフェイルオーバー後の秒数。
tap_failover_session_size				8192	フェイルオーバー・セッション・リストのサイズ (MB 単位)。0=フェイルオーバー・セッションは保存されません。
db_ignore_response_filter				0.0.0.0/0.0.0.0	DB_IGNORE_RESPONSE_FILTER、デフォルト 0.0.0.0/0.0.0.0
db_ignore_response_local=1					DB_IGNORE_RESPONSE_LOCAL=1 注: このパラメーターでは TCP トラフィックはローカル・トラフィックと見なされません。
db_ignore_response_bypass_bytes				65535	DB_IGNORE_RESPONSE_BYPASS_BYTES、デフォルト 65535
db_ignore_response_resets_per_request				1	DB_IGNORE_RESPONSE_RESETS_PER_REQUEST、デフォルト 1
upload_feature				1	Program Files¥IBM¥Windows S-TAP¥Logs からコレクターへのすべてのログ・ファイルへのアップロードを制御します

親トピック: Windows S-TAP パラメーター

検査エンジン・パラメーター

これらのパラメーターは、Windows サーバー上のデータ・リポジトリーをモニターするために S-TAP が使用する検査エンジンの動作に影響を与えます。

これらのパラメーターは、データ・リポジトリー名を持つ、S-TAP プロパティー・ファイルのデータベース・セクションに格納されています。 プロパティー・ファイルには、複数のセクションが存在する場合があり、各セクションは、この S-TAP によって使用される 1 つの検査エンジンを記述しています。

表 1. Windows 上の検査エンジン用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	デフォルト値	記述
db_type		はい		モニター中のデータ・リポジトリーのタイプ。
instance_name		はい		このサーバー上のデータベースのインスタンスの名前。
port_range_start		はい		データベースに固有のポート範囲の先頭。
port_range_end		はい		データベースに固有のポート範囲の末尾。
named_pipe		はい		パイプの名前。
networks		はい		IP アドレス/マスク形式 (n.n.n.n/m.m.m.m) のアドレスのリストを使用して、モニターされるクライアントを識別します。デフォルトはありません。すべてのクライアントを選択するには、アドレスのリストを省略します。 ローカル・トラフィックのみを選択するには、127.0.0.1/255.255.255.255 を使用します。不適切な IP アドレス/マスクを入力すると、S-TAP は開始しません。
exclude_networks		はい		除外されるクライアントを指定する、クライアント IP アドレスおよび対応するマスクのリスト。このオプションを使用すると、特定のクライアントやサブネット (またはこれらの集合) を除くすべてのクライアントをモニターするよう S-TAP を構成できます。リストを編集するときに追加の「除外クライアント IP/マスク」項目を作成するには、「追加」ボタンをクリックします。最後の「除外クライアント IP/マスク」項目を削除するには、「削除」ボタンをクリックします。
db_install_dir		はい	NULL	Unix のみ。Db2、Informix、または Oracle の場合、データベース・インストール・ディレクトリーの絶対パス名を入力します。例: /home/oracle10 他のすべての種類のデータベースの場合、NULL と入力します。
tap_db_process_names		はい		モニター対象となるデータベースの実行中の実行可能ファイル。

以下の追加のパラメーターは、IBM Db2 データベースで使用します。

表 2. Db2 検査エンジン用の追加の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
db2_client_offset	8	はい		61440	共有メモリー領域のクライアント部分へのオフセット。クライアント・オフセットは、Db2 パラメーター ASLHEAPSZ の値を取得して 4096 を乗算することで適切なオフセットを計算できます。このパラメーターのデフォルトは、10 進数の 61440 です。このパラメーターは、Db2 データベース構成値 ASLHEAPSZ を使用して計算され、4096 で乗算されます。ASLHEAPSZ の値を取得するには、Db2 コマンド db2 get dbm cfg を実行して、ASLHEAPSZ の値を探します。通常、この値は 15 で、その結果、デフォルトの 61440 が算出されます。これが 15 ではない場合は、その値を使用し、4096 で乗算して、適切なクライアント・オフセットを算出します。
db2_fix_pack_adjustment	8	はい		80	共有メモリー領域のサーバー部分へのオフセット。 Db2 共有メモリー・パケットの開始位置へのオフセットで、Db2 のバージョンによって異なります。旧バージョンでは 32、8.2.1 以降では 80 です。
db2_log_size	8	はい		25	機能している DLL が、ログ項目を削除し始める前にバッファーに保持できる最大ファイル・サイズ (メガバイト単位)。
db2_shmem_client_position		はい			Db2 共有メモリー・トラフィックをモニターするために設定する必要があります。
db2_shmem_size		はい		131072	Db2 共有メモリー・トラフィックをモニターするために設定する必要があります。

親トピック: Windows S-TAP パラメーター

ファイアウォール・パラメーター

これらのパラメーターは、ファイアウォールに関する S-TAP の動作に影響を与えます。

表 1. ファイアウォール用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	デフォルト値	記述
firewall_installed			0	ファイアウォール機能を有効にします。1=有効、0=無効。
firewall_timeout			10	タイムアウトになる場合、Guardium システムからの判断を待機する時間 (秒単位)。 接続をブロックするのか、許可するのかを知るために、firewall_fail_close 値を調べます。任意の整数値を指定できます。
firewall_fail_close			0	Guardium システムから判断が返されず、firewall_timeout が経過すると、firewall_close = 0 の場合、接続は許可されます。firewall_close=1 の場合、接続はブロックされます。
firewall_default_state			0	ファイアウォール・モードの開始が何によってトリガーされるか。 0= インストールされているポリシー内のルールをトリガーするイベントが発生する。1= トリガーするイベントに関係なく、ファイアウォール・モードが有効になった状態で開始する。 このフラグは、ルールに関係なく、ファイアウォールの監視 (有効化) を強制しますが、特定のアクション (DROP など) は、ルールによってトリガーされる場合にのみ発生します。

パラメーター	バージョン	GUI	デフォルト値	記述
firewall_force_watch	9.0		NULL	ファイアウォール機能が有効になっていて、firewall_default_state が 0 の場合、セッションの監視は、そのクライアント IP が IP/MASK 値のリストと一致する場合に自動的に行われます。リスト自体は、コンマで区切られます。例: 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2
firewall_force_unwatch	9.0		NULL	ファイアウォール機能が有効になっていて、firewall_default_state が 1 の場合、セッションの監視は、そのクライアント IP が IP/MASK 値のリストと一致する場合に自動的に行われません。リスト自体は、コンマで区切られます。例: 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2,

親トピック: Windows S-TAP パラメーター

アプリケーション・サーバー・パラメーター

S-TAP がデータベース・サーバーではなくクライアント・マシンにインストールされている場合、これらのパラメーターは S-TAP の動作に影響を与えます。

注: これらのパラメーターは、いずれも Windows サーバーでは使用すべきでなく、変更もしないでください。 構成ファイル内で使用されている場合があるため、これらのパラメーターを以下に示します。

表 1. アプリケーション・サーバー用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	デフォルト値	記述
appserver_installed			0	推奨されません (Windows の場合のみ)。0 がデフォルトで、S-TAP は通常どおり機能します。1=S-TAP は「クライアント・モード」に設定され、S-TAP がデータベース・サーバーではなくクライアントにインストールされていることを反映するように S2C と C2S のパケットを切り替えます。 また、1 の場合、他の appserver_* パラメーターが入力されているかどうかを検査し、入力されている場合は、提供されているポートの http パケットを調べて、クライアント・システムに常駐する java アプリケーションのエンド・ユーザーについてのセッション情報を入手します。
appserver_ports		はい	8080	推奨されません (Windows の場合のみ)。java アプリケーションが Web ブラウザーを介してアクセスされるポートのコンマ区切りリスト。特定の estore の URL が http://woodpecker:8888/estore の場合、8888 は、このパラメーターで指定する値になります。
appserver_login_pattern		はい		推奨されません (Windows の場合のみ)。アプリケーションに渡されるログイン・パターンを指定するストリングのコンマ区切りリスト。 これは、java アプリケーションに渡されるユーザーのログインを示すパターンです。
appserver_username_prefix		はい		推奨されません (Windows の場合のみ)。指定のセッションのユーザー名の接頭部を指定するストリングのコンマ区切りリスト。 これは、java アプリケーションが、指定のセッションのユーザー名を示すために使用するパターンです。
appserver_username_postfix		はい		推奨されません (Windows の場合のみ)。指定のセッションのユーザー名の接尾部を指定するストリングのコンマ区切りリスト。 これは、java アプリケーションが、ユーザー名を示す特定の変数の値の終わりを示すために使用するパターン (または文字)です。
appserver_session_pattern		はい		推奨されません (Windows の場合のみ)。特定のデータベース・セッションを使用するエンド・ユーザー・セッションの開始を指定するストリングのコンマ区切りリスト。
appserver_session_prefix		はい		推奨されません (Windows の場合のみ)。セッション ID が開始する場所を指定するストリングのコンマ区切りリスト。
appserver_session_postfix		はい		推奨されません (Windows の場合のみ)。セッション ID が終了する場所を指定するストリングのコンマ区切りリスト。
appserver_usersess_pattern		はい		推奨されません (Windows の場合のみ)。指定の接続が継続しているエンド・セッションをマーキングするための ID を指定するストリングのコンマ区切りリスト。
appserver_usersess_prefix		はい		推奨されません (Windows の場合のみ)。指定の usersess 標識パケットの session_id を識別する (session_id に先行する) 対象を指定するストリングのコンマ区切りリスト。
appserver_usersess_postfix		はい		推奨されません (Windows の場合のみ)。セッション ID が終了する場所を指定するストリングのコンマ区切りリスト。

親トピック: Windows S-TAP パラメーター

デバッグ・パラメーター

これらのパラメーターは、S-TAP デバッグの動作に影響を与えます。

これらのパラメーターは、S-TAP プロパティー・ファイルの [DEBUG_OPTIONS] セクションに格納されています。

表 1. デバッグ用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	デフォルト値	記述
debug_buffer			1	1=ローカル・パケットの内容をログに記録します
debug_firewall			1	1=ファイアウォール・イベントをログに記録します

これらのパラメーターは、S-TAP プロパティー・ファイルの [TAP] セクションに格納されています。

表 2. デバッグ用の追加の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	デフォルト値	記述
debug_file_name				S-TAP デバッグ・ファイルのロケーション。デフォルトのロケーションは c:/guardium/stap.txt です。
debug_max_file_size			200	
debuglevel			0	格納するデバッグ・メッセージのレベル。IBM サポートの指示がない限り、0 のままにしてください。 0 クリティカル・エラー情報のみ 2 つの「始動」デバッグ・ログが bin¥..¥logs に保存されます。ファイル名の構文: startup_hostname_timestamp.new および startup_hostname_timestamp.old。bin¥..¥logs のファイルは、upload_feature がオンの場合は自動的にアップロードされます。 1 前のすべてのメッセージ、および反復可能なクリティカル・エラー情報 2 つの「通常」デバッグ・ログが bin¥StapBuffer に保存されます。ファイル名の構文: stap_hostname_timestamp.new および stap_hostname_timestamp.old。bin¥StapBuffer のファイルはアップロードされません。 2 使用されていない 3 レベル 1 のすべてのメッセージ、および Guardium システムに送信されたパケットの要約情報 4 レベル 3 のすべてのメッセージ、およびローカル・スニッフィング・ログ 5 レベル 4 のすべてのメッセージ、およびネットワーク・スニッフィング・ログ 6 レベル 5 のすべてのメッセージ、およびハートビート受信ログ 7 レベル 6 のすべてのメッセージ、および各種デバッグ情報
dump_file_mode			0	S-TAP が異常終了した場合に、ダンプ・ファイルの取り込みを有効にします。 パラメーターがゼロではないときは、S-TAP が始動するたびに新しいダンプ・ファイルが開かれます。異常終了が発生していない場合は空になります。 • 0: クラッシュ・ダンプは生成されません • 1: クラッシュ・ダンプが生成され、ファイル stap.diag に書き込まれます。このファイルは、S-TAP の作業ディレクトリーに作成されます。 S-TAP は stap.diag ファイルを上書きする前に、既存の stap.diag ファイルをすべてバックアップ・ファイルにコピーします。 • 2: タイム・スタンプ付きのクラッシュ・ダンプが生成され、ファイル stap-TIMESTAMP.diag に書き込まれます。このファイルは、S-TAP の作業ディレクトリーに作成されます。ここで、TIMESTAMP は、クラッシュ・ダンプが生成されたタイミングを示します。 異常終了で問題がある場合は、このオプションを使用して最新のダンプのみではなく、すべてのダンプを取り込んでください。 タイム・スタンプもデバッグに役立ちます。ただし、このオプションでは、使用するディスク・スペースが多くなります。
stack_trace_file_mode				similar to dump_file_mode
kernel_debug_level			0	
syslog_messages			1	1=SYSLOG (UNIX の場合) または EventViewer (Windows の場合) にメッセージを送信します。S0=メッセージは送信されません。
WER_DUMP_FOLDER	10.2.30.15	N	なし	パラメーターが設定されていない場合、以下の値が使用されます。STAP インストール・フォルダーが「C:¥Program Files (x86)¥...」以外のどこかのルート・フォルダーである場合、WER ダンプ・フォルダーは、末尾に「...¥Windows S-TAP¥Bin¥..¥Logs」がある絶対パスに設定されます。STAP インストール・フォルダー名にテキスト「(x86)」が含まれている場合、ダンプ・フォルダーは「C:¥Guardium¥Dumps」に設定され、STAP プロセスでパスが作成されます。 例えば、Windows S-TAP が C:¥PROGRAM FILES¥IBM¥WINDOWS S-TAP にインストールされ、WER_DUMP_FOLDER と WER_DUMP_COUNT のデフォルト値を使用する場合、Windows S-TAP は以下のレジストリー設定を使用します。Windows S-TAP がクラッシュした場合は、Windows S-TAP クラッシュ・ダンプが Windows Error Reporting (WER) 機能を介して生成されます。 HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥Windows Error Reporting¥LocalDumps¥guardium_stapr.exe DumpCount REG_DWORD 0x1 DumpFolder REG_EXPAND_SZ C:¥PROGRAM FILES¥IBM¥WINDOWS S-TAP¥Bin¥..¥LOGS¥ DumpType REG_DWORD 0x2
WER_DUMP_COUNT	10.2.30.15	N	1	最大値は 5 です。

親トピック: Windows S-TAP パラメーター

構成監査システム (CAS) パラメーター

これらのパラメーターは、このシステム上の CAS の動作に影響を与えます。

表 1. CAS 用の S-TAP 構成パラメーター

パラメーター	バージョン	GIM	GUI	デフォルト値	記述
cas_task_checkpoint			はい	task_checkpoint	
cas_client_checkpoint			はい	client_checkpoint	
cas_checkpoint_period			はい	60	チェックのための時間間隔 (秒単位)。
cas_fail_over_file			はい	fail_over_file	出力メッセージ・バッファーが入っているファイルの名前。
cas_fail_over_file_size_limit			はい	50000	フェイルオーバー・ファイルのサイズ。
cas_max_reconnect_attempts			はい	5000	接続が失われた場合の再接続の試行回数。
cas_reconnect_interval			はい	60	次の再接続を試行するまでの待機時間 (秒単位)。
cas_raw_data_limit			はい	1000	Guardium システムに送信される生データのサイズ制限 (キロバイト単位)。
cas_md5_size_limit			はい	1000	MD5SUM を計算する対象の最大ファイル・サイズ (キロバイト単位)。
cas_command_wait	8.0			300	長期実行データ収集プロセスを強制終了するまでの待機時間 (秒単位)。
cas_server_failover_delay	8.0			60	別の Guardium システムへの接続を試行するまでの待機時間 (分単位)。
cas_server_port					Windows のみ。

親トピック: Windows S-TAP パラメーター

ドライバー・パラメーター

これらのパラメーターは、S-TAP が対話するいくつかのドライバーの動作に影響を与えます。

表 1. ドライバー用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	デフォルト値	記述
tcp_driver_installed	v10		1	TCP ドライバーを使用します。デフォルトは 1 です。
nptrc_log_size			2	拡張機能
shstrc_log_size			4	拡張機能
ora_driver_installed			1	Oracle ASO および SSL トラフィックをスニッフィングするには 1 に設定します。
ora_driver_level		はい	0	高。スレッドの優先順位付けに使用されます。
named_pipes_driver_installed			1	ローカルの名前付きパイプをスニッフィングするには 1 に設定します。
named_pipes_driver_level		はい	0	高。スレッドの優先順位付けに使用されます。
shared_memory_driver_level		はい	0	高。スレッドの優先順位付けに使用されます。
krb_mssql_driver_installed			2	MSSQL SSL トラフィックおよび Kerberos チケットをスニッフィングするには 1 に設定します。 Kerberos チケットではなく、MSSQL 暗号化解除トラフィックのみを収集して、プログラムの開始時にドメイン・ユーザー名を収集することによって時間を節約する場合は、2 に設定します。 このパラメーターは、インストール後は常に 0 に設定されることに注意してください。 V10.1 からは、このパラメーターは Correlation を有効/無効にするために使用されます。ゼロ以外の値に設定されている場合は、Correlation を使用します。ゼロの場合は、Correlation を使用しません。デフォルトはゼロ以外の値です。注: このパラメーターは、v10.1.4 で非推奨になりました。
correlation_timeout			5	WFP スニファーおよび NMP スニファーが相関の発生を待機する秒数。この秒数が過ぎると、断念してアプライアンスへのトラフィックのフローを再開します。デフォルトは 5 秒です。

親トピック: Windows S-TAP パラメーター

UNIX S-TAP パラメーター

以下の表に、UNIX 上の S-TAP の動作を制御するために使用されるパラメーターの定義を示します。

表には、パラメーターごとに、以下の情報が示されています。

パラメーター
: パラメーターの名前。

バージョン
: このパラメーターがバージョン 8.0 以降で導入された場合、このパラメーターを使用できる最も古いバージョン

GUI
: Guardium ユーザー・インターフェースによってパラメーターを変更できる場合は「はい」、変更できない場合はブランク

GIM
: Guardium インストール・マネージャーによってパラメーターを変更できる場合は「はい」、変更できない場合はブランク

デフォルト値
: パラメーターのデフォルト値

記述
: 有効な値についての説明を含むパラメーターの意味

注: パラメーターの説明が「拡張機能」で始まっている場合は、十分に経験を積んだユーザーであるか、IBM に相談済みである場合に限り、値を変更してください。

- SQLGuard パラメーター
  以下のパラメーターは、この Linux S-TAP が接続できる Guardium システムを示します。
- 一般パラメーター
  これらのパラメーターは、DB サーバー上で実行されている S-TAP および S-TAP のインストール先のサーバーの基本プロパティーを定義し、他のどのカテゴリーにも分類されません。
- Hadoop パラメーター
- 検査エンジン・パラメーター
  これらのパラメーターは、DB サーバー上のデータ・リポジトリーをモニターするために S-TAP が使用する検査エンジンの動作に影響を与えます。
- ファイアウォール・パラメーター
  これらのパラメーターは、ファイアウォールに関する S-TAP の動作に影響を与えます。
- アプリケーション・サーバー・パラメーター
  アプリケーション・ユーザー名をデータベース・アクティビティーとバインドする必要がある場合、これらのパラメーターは S-TAP の動作に影響を与えます。
- discovery パラメーター
  discovery パラメーターは、データベース・インスタンスのディスカバーと現在アクティブな S-TAP への結果の送信を行うオートディスカバリー機能の動作を定義します。
- 構成監査システム (CAS) パラメーター
  これらのパラメーターは、このシステム上の CAS の動作に影響を与えます。
- デバッグ・パラメーター
  これらのパラメーターは、S-TAP デバッグの動作に影響を与えます。
- K-TAP パラメーター
  これらのパラメーターは、K-TAP の動作に影響を与えます。

親トピック: S-TAP 構成パラメーターの編集

SQLGuard パラメーター

以下のパラメーターは、この Linux S-TAP が接続できる Guardium システムを示します。

表 1. S-TAP 構成パラメーター: SQLGuard

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
sqlguard_ip		はい	はい	NULL	S-TAP のホストとしての役割を果たす Guardium システムの IP アドレスまたはホスト名。[SQLGuard_1]、[SQLGuard_2]、以降同様を追加することで、複数のホストを定義できます。
primary		はい	はい	1	サーバーが 1 次サーバーであるかどうかを示します: Windows: 0=NO、1=YES。 UNIX: 1= 1 次、2= 2 次、3= 3 次、以降同様。
sqlguard_port		はい	はい	16016	読み取り専用。S-TAP が Guardium システムに接続するために使用するポート。
connection_pool_size	8.0	はい	はい	0	S-TAP と Guardium ホスト上のスニファー・プロセスとの間で開かれる接続の数。値を高くすると、TLS などの暗号化を有効にする場合に必要になる可能性があるスループットが増えます。プールされた接続の最大数は 50 です。総合計は、guard_tap.ini 内のすべての [SQLGuard_n] セクションの (connection_pool_size x num_main_threads) の合計です。 有効な値: • 0: プーリングを無効にする • 1 から 10 (定義されたホストごと) デフォルト = 0
num_main_threads		はい		1	S-TAP と 1 つ以上の Guardium ホストとの間で使用されるスレッドの数。 有効な値: 1 から 510 (定義されているすべての Guardium ホストの最大合計は 510) デフォルト = 1 注: エンタープライズ・ロード・バランシングでは、1 つの管理対象ユニットに対して複数のスレッドを使用することがサポートされていません。エンタープライズ・ロード・バランシングを使用する場合には、このパラメーターを 1 に設定してください。

一般パラメーター

これらのパラメーターは、DB サーバー上で実行されている S-TAP および S-TAP のインストール先のサーバーの基本プロパティーを定義し、他のどのカテゴリーにも分類されません。

これらのパラメーターは、S-TAP プロパティー・ファイルの [VERSION] セクションに格納されています。

表 1. [VERSION] セクションの S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
stap_client_build			はい		インストールされている S-TAP のビルド・バージョン
protocol_version					Guardium システムのバージョン

これらのパラメーターは、S-TAP プロパティー・ファイルの [TAP] セクションに格納されています。

表 2. [TAP] セクションの S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
tap_type					UNIX の場合は S-TAP、Windows の場合は W-TAP
tap_version					サーバーにインストール済みの S-TAP のバージョン
tap_ip			はい		S-TAP がインストールされているデータベース・サーバー・システムの IP アドレスまたはホスト名
devices		はい	はい	なし	listen 対象のインターフェース。ifconfig を使用して、正しいインターフェースを見つけます。
all_can_control		はい	はい	0	0= S-TAP は 1 次 Guardium システムからのみ制御できます。1= S-TAP は任意の Guardium システムから制御できます。
participate_in_load_balancing		はい	はい	0	以下のように、Guardium システムへのロード・バランシングを制御します。 • 0: ロード・バランシングなし。 • 1: ロード・バランシング。SQLGuard セクションで定義されている 1 次サーバーと 2 次サーバーの間でトラフィックのバランスを取ります。 • 2: 冗長。完全にミラーリングされた S-TAP によって、SQLGuard セクションで定義されているすべての 1 次サーバーと 2 次サーバーにすべてのトラフィックが送信されます。 • 3: ハードウェア・ロード・バランシング。Guardium では、F5 や Cisco などのロード・バランサーが使用されます。S-TAP はトラフィックをロード・バランサーに送信し、ロード・バランサーはそれをプール内のいずれかのコレクターに転送します。 • 4: トラフィックの分割に複数の KTAP バッファーと S-TAP スレッドが使用されます。 1 次サーバー、2 次サーバーなどのサーバーを指定するには、SQLGUARD セクションでプライマリー・パラメーターを使用します。 このパラメーターが 0 に設定されているときに、複数の Guardium システムでトラフィックをモニターしている場合は、1 次以外の Guardium システムをフェイルオーバー用に使用することができます。 注: Guardium は、v10.x S-TAP と v9.x コレクターを使用したフェイルオーバーをサポートしていません。
connection_timeout_sec			はい	10	S-TAP が Guardium サーバーは使用不可であると見なすまでの秒数。任意の整数値を指定できます。
use_tls		はい	はい	0	1=SSL を使用して、エージェントと Guardium システムとの間のトラフィックを暗号化します。 0=暗号化しません。 警告: エージェントと Guardium システム間のトラフィックは平文です。 Guardium では、可能な場合は常に S-TAP とコレクター間のネットワーク・トラフィックを暗号化することを推奨しています。この暗号化を無効にする必要があるのは、パフォーマンスの優先順位がセキュリティーより高い場合のみです。 TLS が有効である場合、ログイン・パケットの暗号化解除はサポートされていません。 これは、DB_USER が取り込まれず、失敗したログインがアクセスに関連付けられないことを意味します。
failover_tls		はい	はい	0	1= 何らかの理由で SSL 接続を使用できない場合は、非セキュア接続を使用するようにフェイルオーバーします。0= セキュア接続のみを使用します。
wait_for_db_exec			はい	-1	

パラメーター	バージョン	GUI	GIM	デフォルト値	記述

tap_run_as_root	8.2		はい	TAPUSER	S-TAP を通常のユーザーとして実行できるようにします。0 = tap は「guardium」ユーザーとして実行されます。1= tap は「root」として実行されます。
					
					まれに、S-TAP を Guardium として (root ではなく) 実行する必要があります。これは他の問題を引き起こす可能性があるため、必要な場合にのみ使用してください。S-TAP を Guardium ユーザーとして実行すると、許可レベルが原因でデータベースまたはプロトコルが機能しなくなる場合があります。Guardium ユーザーにデータベース・パスまたは exec ファイルの読み取り許可が付与されていることを確認してください。ご使用の環境に応じて、代表的な制限事項は以下のようになります。
					
					• wait_for_db_exec が機能しない可能性があります。クラスターの場合は、Guardium ユーザー読み取り許可のデータベース・パスまたは exec ファイルを確認してください。
					• AIX® WPAR および Solaris Zones のデータベースが機能しない可能性があります。インストール・パスまたは実行ファイルへのアクセス権限を確認してください。
					• Oracle BEQ の場合は、データベースの始動後、または再始動後に S-TAP を再始動してください。
					• Informix® 共有メモリーの場合は、データベースの始動後、または再始動後に S-TAP を再始動してください。
					• Db2 共有メモリーの場合、許可の問題が原因で shmctl が失敗したら、ほとんどの場合に S-TAP® が root として実行されるように変更する必要があります。
					  ◦ グループによる読み取りが共有メモリー・セグメントで許可されている場合は、Db2 インスタンスがユーザー (Guardium) グループに追加されていることを確認してください。ただし依然として、サーバーごとに、DB2® の構成は 1 セットのみサポートされます。
					  ◦ db2 ユーザーによる読み取りのみが共有メモリー・セグメントで許可されている場合は、S-TAP を root として実行する必要があります。(Db2 共有メモリー・セッションを開き、コマンド ipcs -ma を実行し、出力で MODE を確認します)

tap_buf_dir				NULL	S-TAP バッファー・ファイルの場所。デフォルトは NULL で、$inidir/buffers に置かれます。
tap_log_dir				NULL	S-TAP ログ・ファイルの場所: guard_stap.stdout.tx、guard_stap.stderr.txt、guard_stap.fam.txt。デフォルトは NULL です。デフォルトでは、ログ・ファイルは /tmp に書き込まれます。
number_of_processors				4	読み取り専用。マシンのプロセッサー数。
alternate_ips		はい	はい	NULL	このデータベース・サーバーへの接続に使われる代替または仮想 IP アドレスのコンマ区切りのリスト。これが使用されるのは、複数の IP または仮想 IP を持つ複数のネットワーク・カードがサーバーにある場合だけです。この S-TAP 用に定義された S-TAP ホスト IP、またはここにリストされるいずれかの代替 IP に宛先 IP が一致する場合にのみ、S-TAP はトラフィックをモニターします。このため、すべての仮想 IP をここにリストすることをお勧めします。
tee_installed			はい	0	1=Tee が使用されます。0=Tee は使用されません。
tee_msg_buf_len			はい	128	Tee のバッファーのサイズ (MB 単位)。任意の整数値を指定できます。
buffer_file_size			はい	50	拡張機能。パケット・キューに割り振られているバッファーのサイズ (MB 単位)。バッファー・サイズの設定値が大きすぎると、S-TAP を始動できないことがあります。 ファイルが 2560 MB より大きいと、この問題が生じることが認識されています。
buffer_file_name					BUFFER_MMAP_FILE=1 の場合、メモリー・マップ・ファイルの絶対パス。 デフォルトは、WSTAP 作業フォルダー /StapBuffer/STAP_buffer.dtx です。
buffer_mmap_file	9			0	1=メモリー・マップ・ファイルのオプション。0=仮想メモリーの割り振り。
tracefiles_dir		はい			アクセス・トレーサー・ファイルが格納されるディレクトリー。デフォルトは INSTALLDIR です。
compression_level		はい	はい	0	拡張機能。1 から 9 までの圧縮レベル。0=圧縮なし。
min_bytes_to_compress			はい	500	拡張機能。圧縮するメッセージの最小サイズ。
msg_aggregate_timeout				100	K-TAP が、バッファーに累積したパケットを S-TAP に送信する時の時間 (ミリ秒単位)。任意の整数値を指定できます。
msg_count_watermark				64	K-TAP が、バッファーに累積したパケットを S-TAP に送信する時のパケット数。任意の整数値を指定できます。
log_program_name				0	パフォーマンスを向上させるために、ソース・プログラム名の取得を無効にすることはできますが、接続を使用していたプログラム名を識別できなくなります (ユーザーやクライアント・アドレスなどの他のすべての接続情報は入手可能です)。0 = source_program 名を Guardium システムに送信しません。1= source_program 名を Guardium システムに送信します。

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
max_server_write_size				16384	S-TAP が Guardium システムに一度に送信する最大バイト数。任意の整数値を指定できます。
guardium_ca_path				NULL	認証局証明書の場所。
sqlguard_cert_cn				NULL	Sqlguard 証明書で予期される共通名。
guardium_crl_path				NULL	証明書失効リストのファイルまたはディレクトリーへのパス。
tap_failover_session_size				1024	Guardium システムごとのリスト内のフェイルオーバー・セッションの最大数。0= フェイルオーバー機能は無効です。任意の整数値を指定できます。
tap_failover_session_quiesce				240	フェイルオーバー後にセッション・リストがクリーンアップするまでの最大アイドル時間 (分単位)。 S-TAP によってセッションが「非活動」とみなされるセッションの時間 (フェイルオーバー後に failover_session_quiesce 分が経過した場合、これによりセッションがクリーンアップされる) であり、セッションをクローズしてフェイルオーバー状態に参加させないこと、および S-TAP によってセッションのポリシーを消去してセッションをファイアウォール・リストおよび修正リストから削除することなどを目的とします。
kerberos_plugin_dir				NULL	Kerberos ファイルの場所。
db_ignore_response				NULL	応答を無視するデータベース・タイプのコンマ区切りリスト。 none に設定した場合、どの応答も無視されません。all に設定した場合、すべてのデータベースからの応答が無視されます。 注: db_ignore_response=all を使用して Oracle データベースの応答が無視されるように (トラフィック負荷を削減するためキャプチャーされないように) 設定する場合、関係するのはデータベース・サーバー応答だけではないことに注意してください。 データベース・サーバー応答には、アプリケーションが以下のデータベース要求解釈のために使用する重要なデータベース・プロトコル・メタデータ情報も含まれている可能性があります。
stap_statistic				0	S-TAP が S-TAP/K-TAP についての統計情報をスニファーに送信する間隔。0= 送信しません。時間の場合は正の整数、分の場合は負の整数を指定します。
stap_statistic_version				1	STAP 統計は、コレクターに固有のバージョンです。 1: Guardium V10 以上 0: Guardium V9
upload_feature	9.1		はい	1	1 の場合、新規 K-TAP が作成されると、この S-TAP の報告先である Guardium システムに自動的にアップロードされます。 このパラメーターを設定するには、GIM パラメーター STAP_UPLOAD_FEATURE を設定します。
upload_snapshots				1	スナップショットを自動アップロードします。
add_to_verification schedule				0	guard_tap.ini で定義した検査エンジンを S-TAP 検査スケジュールに追加します。 S-TAP 検査はトラフィック・キャプチャーをテストします。0=OFF、1=ON でデフォルトは 0 です。
db_ignore_response_bypass_bytes			はい	4096	結果セットのバイト・サイズの整数。結果セットがこのサイズより大きい場合応答を無視します。
db_ignore_response_resets_per_request			はい	0	DB_IGNORE_RESPONSE_RESETS_PER_REQUEST、デフォルト 1
db_ignore_response_filter				0.0.0.0/0.0.0.0	応答を無視する IP/マスクのコンマ区切りリスト。デフォルトでは、すべてのトラフィックがフィルタリングされます。 指定された IP/マスクに対する、DB_IGNORE_RESPONSE で指定されたタイプのデータベース応答はすべて無視されます。 0= 応答のフィルタリングは行われない 0.0.0.0/0.0.0.0= すべての IP がフィルタリングされる
db_ignore_response_local				1	DB_IGNORE_RESPONSE_LOCAL ローカル・データベース応答のフィルタリング。 0= いいえ 1= はい
debug_snapshot				0	デバッグ情報を取得するために、GUI を使用して S-TAP ログをオンにします (いったん GUI を使用してこの値を設定すると、変更は guard_tap.ini に表示されません。ただし、S-TAP プロセスを再始動すると、ini ファイルにあるこれらの値が GUI に反映されます。つまり、GUI はデフォルト値に戻ります)。

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
debug_snapshot_level		はい		1	GUI を使用してデバッグのレベルを設定するには以下のようにします。 0: クリティカル・エラー情報のみ; 1: クリティカル・エラー情報に加え、反復可能な非クリティカル・エラー情報。 2: レベル 1 のチェックに加えて KTAP 不一致をチェックし、PCAP がバックアップされます。GIM STAP メッセージをチェックします。 3: レベル 1 のチェックに加えて guard_stap 構成ファイルが有効かどうかをチェックします。 4: レベル 1 のチェックに加えて ローカル・スニッフィング・ログをチェックします。 5: レベル 1 のチェックに加えて、ネットワーク・スニッフィング・ログをチェックします。 6: レベル 1 のチェックに加えて、Appserver デバッグ情報をチェックします。 7: レベル 1 のチェックに加えて、診断スクリプトの実行をトリガーします。
debug_snapshot_time				60	このパラメーターは、GUI を使用して S-TAP ログがオンであることが必要な期間を秒単位で設定します。任意の整数値を指定できます。
force_log_limited				0	S-TAP の SQL ステートメントの値を処理するフラグ。 0=無制限。デフォルト 1=制限付きログ、SQL ステートメントでのマスク値
hunter_trace			はい	0	UID_CHAIN を有効にします。 0: 無効にする。 1: 有効にする。Solaris ゾーンや AIX WPAR を含む、ローカル TCP/IP 接続の場合。または、appserver_installed = 1 の場合のリモート TCP/IP 接続の場合。
load_balancer_ip		はい	YES		ロード・バランサー・ユニットの IP アドレス。
load_balancer_num_mus				1	ロード・バランサーから要求する管理対象ユニットの数。
merge_with_template				0	コレクターからの構成が STAP に対してプッシュされたときに、それをテンプレート構成ファイルとマージするかどうかを指定します。 0= いいえ 1= はい
shmid_blacklist				NULL	KTAP は shmid_blacklist を使用して、コンマで区切られた共有メモリー ID のリストをフィルタリングします。
shmid_blacklist_wait				0	shmid_blacklist 項目がディスカバーされるまで、インターセプトをアクティブ化するのを待機します。0: いいえ、1: はい (0)
blacklist_shmem_ops_by_proc				NULL	KTAP は blacklist_shmem_ops_by_proc を使用して、指定されたプロセス (コンマ区切りリスト) の shmem インターセプトをフィルタリングします。
add_to_verification_schedule				0	
uid_chain_ssh_ip				0	sshd が UID チェーン内のプロセスの 1 つとして識別された場合、クライアント IP を UID チェーンにエンコードします。 0= 無効、1= 有効

親トピック: UNIX S-TAP パラメーター

Hadoop パラメーター

Apache Ranger を使用する Hortonworks の guard_tap.ini のパラメーター

Guardium は、Apache Ranger を使用した統合 Hortonworks ディストリビューションをサポートします。以下の表は、S-TAP と Ranger エージェントとの間の接続に必要な S-TAP パラメーターについて説明しています。
注: 一部のパラメーターは、Guardium ユーザー・インターフェースまたは Guardium Installation Manager を介して構成できます。すべてのパラメーターは、Guardium API を使用して構成できます。

表 1. Apache Ranger 統合を使用する Hortonworks の guard_tap.ini のパラメーター

パラメーター	値	記述

パラメーター	値	記述
log4j_reader_enabled	0 または 1 0 は無効 (デフォルト) です。 1 は有効です。	Ranger トラフィックに対する log4j listen モードを有効にします。
log4j_port	整数。 デフォルト値は 5555 です。	Guardium S-TAP が Ranger 監査を listen するポート。
log4j_listen_address	IP アドレス 0.0.0.0 は、システムの任意の IP アドレス (デフォルト) を示します。 localhost は、システムのループバック・アドレスを示します。	このアドレスには、Ranger プラグインが接続します。 デフォルト値の 0.0.0.0 は、S-TAP が任意のホストからトラフィックを受信できるようになるため、お勧めです。 システムを高可用性のために構成する場合は、localhost を使用します。 特定のアドレスへのアクセスを制限することを選択した場合は、モニターのために必要なトラフィックを除外しないようにしてください。
log4j_num_connections	整数 デフォルト値は 20 です。	この S-TAP 用に定義されているサービスに期待される同時接続数。
ranger_dynamic_policy_reader_enabled	0, 1	機能が有効かどうか。0=いいえ、1=はい
ranger_dynamic_policy_port	integer デフォルト = 5556	Ranger プラグインが接続するポート
ranger_dynamic_policy_listen_address	デフォルト = 0.0.0.0	STAP が listen するアドレス HA の場合は localhost を使用します
ranger_dynamic_policy_num_connections	デフォルト = 20	同時接続の数
ranger_dynamic_policy_timeout	デフォルト = 10	判断を待つ時間 (秒数)
ranger_dynamic_policy_default_verdict	0, 1 デフォルト = 1	判断がタイムアウトになった場合、または gmachine が使用できない場合の動作 1= Ranger ポリシーに適合する 0 = Ranger ポリシーに適合しない
ranger_dynamic_policy_reader_enabled	0 または 1 0 は無効 (デフォルト) です。 1 は有効です。	Hortonworks 動的ポリシー・ロギングを有効にします。
ranger_dynamic_policy_port	整数 デフォルト値: 5556	Guardium S-TAP が Ranger 動的ポリシーを listen するポート。
ranger_dynamic_policy_listen_address	IP アドレス 0.0.0.0 は、システムの任意の IP アドレス (デフォルト) を示します。	このアドレスには、Ranger 動的ポリシー・プラグインが接続します。
ranger_dynamic_policy_num_connections	整数 デフォルト値は 20 です。	動的ポリシー・プラグインからサポートする接続の最大数。
ranger_dynamic_policy_timeout	整数 デフォルト値は 10 です	デフォルトの判断結果を送信するまで判断を待機する秒数。
ranger_dynamic_policy_default_verdict	0 または 1 1 = 一致、0 = 不一致 デフォルト: 1	Guardium が到達不能である場合、または判断がタイムアウトになった場合の動作。

Kafka メッセージングを使用する Cloudera Navigator の guard_tap.ini のパラメーター

Guardium は、Kafka メッセージング・システムを使用して監査データを収集する Cloudera Navigator をサポートします。
注: 一部のパラメーターは、Guardium ユーザー・インターフェースまたは Guardium Installation Manager を介して構成できます。すべてのパラメーターは、Guardium API を使用して構成できます。

表 2. Kafka メッセージング統合を使用する Cloudera Navigator の guard_tap.ini のパラメーター

パラメーター	値	記述

パラメーター	値	記述
kafka_reader_enabled	0 または 1 0 は無効 (デフォルト) です。 1 は有効です。	Kafka のパブリッシュとコンシュームを使用した Cloudera Navigator 統合の有効化。
kafka_bootstrap_servers	host name:port のペアのコンマ区切りリスト。 形式: host:port,host:port 例: hostnameofbroker1:9092,hostnameofbroker2:9092	host name:port のリストは、Kafka クラスターへの初期接続を確立するために使用されます。初期接続が確立されると、クラスター内のすべてのサーバーが使用されます。ダウンした場合に備えて、複数のブートストラップを指定しておくことができます。
kafka_use_tls	0 または 1 0 は無効 (デフォルト) です。 1 は有効です。	Kafka クラスターが TLS を使用するかどうかを示します。
kafka_topic_name	文字列 デフォルト値は NavigatorAuditEvents です。	監査イベントを Kafka にパブリッシュするために Cloudera Navigator が使用するトピック名。
kafka_principal	文字列 デフォルト値は NULL です。	Kafka クラスターで Kerberos 認証を必要とする場合に使用される、S-TAP の Kerberos プリンシパル名。
kafka_keytab	NULL	S-TAP サーバー上の Kerberos キータブ・ファイルへのパス。

親トピック: UNIX S-TAP パラメーター

検査エンジン・パラメーター

これらのパラメーターは、DB サーバー上のデータ・リポジトリーをモニターするために S-TAP が使用する検査エンジンの動作に影響を与えます。

これらのパラメーターは、データ・リポジトリー名を持つ、S-TAP プロパティー・ファイルのデータベース・セクションに格納されています。 プロパティー・ファイルには、複数のセクションが存在する場合があり、各セクションは、この S-TAP によって使用される 1 つの検査エンジンを記述しています。

表 1. UNIX 上の検査エンジン用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
db_type		はい			モニター中のデータ・リポジトリーのタイプ。
port_range_start		はい			データベースに固有のポート範囲の先頭。
port_range_end		はい			データベースに固有のポート範囲の末尾。
networks		はい			IP アドレス/マスク形式 (n.n.n.n/m.m.m.m) のアドレスのリストを使用して、モニターされるクライアントを識別します。デフォルトはありません。すべてのクライアントを選択するには、アドレスのリストを省略します。 ローカル・トラフィックのみを選択するには、127.0.0.1/255.255.255.255 を使用します。不適切な IP アドレス/マスクを入力すると、S-TAP は開始しません。
tee_listen_port		はい		12344	Windows では使用されません。Unix では、K-Tap モニター・メカニズムが使用される場合、KTAP データベース実ポートに置き換えられます。TEE モニター・メカニズムを使用する場合、これが必須です。聴取ポートは、S-TAP がローカル・データベース・トラフィックを聴取して受け入れるポートです。実ポートは S-TAP がトラフィックを転送するポートです。
connect_to_ip		はい		127.0.0.1	S-TAP がデータベースへの接続に使用する IP アドレス。Tee が有効になっている場合、このパラメーターは、S-TAP がデータベースへの接続に使用する IP アドレスになります。127.0.0.1 のローカル接続を受け入れるデータベースもあれば、デフォルト (127.0.0.1) ではなく、マシンの「実際の」IP でのみローカル接続を受け入れるデータベースもあります。K-TAP が有効になっている場合、このパラメーターは Solaris Zones および AIX WPAR に使用され、トラフィックを取り込むには、ゾーン IP アドレスでなければなりません。
exclude_networks		はい			除外されるクライアントを指定する、クライアント IP アドレスおよび対応するマスクのリスト。このオプションを使用すると、特定のクライアントやサブネット (またはこれらの集合) を除くすべてのクライアントをモニターするよう S-TAP を構成できます。リストを編集するときに追加の「除外クライアント IP/マスク」項目を作成するには、「追加」ボタンをクリックします。最後の「除外クライアント IP/マスク」項目を削除するには、「削除」ボタンをクリックします。
real_db_port		はい		4100	Windows では使用されません。Unix では、K-Tap モニター・メカニズムが使われる場合にのみ使用されます。K-Tap メカニズムによってモニターされるデータベース・ポートを識別します。
db_install_dir		はい		NULL	Unix のみ。Db2、Informix、または Oracle の場合、データベース・インストール・ディレクトリーの絶対パス名を入力します。例: /home/oracle10 他のすべての種類のデータベースの場合、NULL と入力します。

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
db_exec_file		はい		NULL	Windows サーバーの場合: Oracle または MS SQL Server のみ (名前付きパイプが使用される場合)。Oracle では、通常、2 つの項目 oracle.exe、tnslsnr.exe がリストに含まれます。MS SQL Server では、通常、リストは 1 つの項目 sqlservr.exe だけです。Unix サーバーの場合: Db2、Oracle、または Informix データベースでは、データベース実行可能ファイルの絶対パス名を入力します。例: Oracle の場合: /home/oracle10/prod/10.2.0/db_1/bin/oracle。 Informix の場合: /INFORMIXTMP/.inf.sqlexec。 これは、すべての Informix プラットフォームに適用されます (Linux を除く)。Linux での Informix の例: /home/informix11/bin/oninit MYSQL: "mysql" 他のすべての種類のデータベースの場合、NULL と入力します。
db_version		はい		9	データベース・バージョン。ATAP トラフィックをキャプチャーするために使用されます。
encryption		はい		0	Oracle (バージョン 11 と 12) および Sybase (Solaris、HPUX、および AIX 上) 用に ASO または SSL 暗号化トラフィックをアクティブ化します。 Oracle の場合、ini ファイルに db_version を指定します (例: db_version=12)。 Oracle12 SSL の場合、すべてのプラットフォームでインスツルメンテーションを実行します。 Oracle11 SSL の場合、AIX でインスツルメンテーションを実行します。 インスツルメンテーションを必要とする Oracle に対して、guard_tap.ini 内で encryption=1 (Linux ではサポートされません) を使用する場合、 そのパラメーターを設定する前にインスツルメンテーションを実行する必要があります。
load_balanced		はい	はい	1	1= データベースは、ロード・バランシングに関与します。0= データベースは、ロード・バランシングに関与しません。
unix_domain_socket_marker		はい		NULL	Oracle、Mysql、および Postgres UNIX ドメイン・ソケットのマーカーを設定するために使用されます。通常は、デフォルト値が正しいですが、名前付きパイプまたは UNIX ドメイン・ソケット・トラフィックが動作しない場合は、この値が正しく設定されていることを確認する必要があります。例えば、Oracle では、unix_domain_socket_marker を tnsnames.ora で定義されている IPC のキーに設定する必要があります。 NULL の場合、または設定しない場合、S-TAP は、次のような定義済みのデフォルト・マーカーを使用します。* MySQL - "mysql.sock" * Oracle - "/.oracle/" * Postgres - ".s.PGSQL.5432"
instance_running				1	Solaris Zones および WPAR の場合、S-TAP の開始時に一部のゾーンが停止している場合があります。S-TAP 全体を停止する代わりに、wait_for_db_exec フラグがゼロ以外の場合は、そのゾーンを稼働できるかどうかを定期的に確認します。それが可能な場合は、関連するパラメーターを K-TAP に渡し、新規構成を Guardium システムに送信します。 構成には、どのデータベースが稼働していて、どれが停止しているかの情報が含まれます。instance_running が 1 (ゾーンが稼働していることを意味する) の場合 (1 以外の場合、ゾーンは停止している)、S-TAP はインスタンスが稼働しているかどうか定期的に検査します。
intercept_types		はい		NULL	各 IE のインターセプト・タイプを有効/無効にします。スペースなしのコンマで区切ります。 NULL: データベースがサポートしているすべてのプロトコルを自動的にインターセプトします。
tap_identifier		はい		NULL	データベースを識別するための分かりやすい文字列

注: Solaris での Informix IPC プロトコルの場合、TAP ID はデータベース・トラフィックに関連付けられません。

以下の追加のパラメーターは、IBM Db2 データベースで使用します。

表 2. Db2 検査エンジン用の追加の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
db2_fix_pack_adjustment	8	はい		20	共有メモリー領域のサーバー部分へのオフセット。 Db2 共有メモリー・パケットの開始位置へのオフセットで、Db2 のバージョンによって異なります。旧バージョンでは 32、8.2.1 以降では 80 です。
db2_client_offset	8	はい		61440	共有メモリー領域のクライアント部分へのオフセット。クライアント・オフセットは、Db2 パラメーター ASLHEAPSZ の値を取得して 4096 を乗算することで適切なオフセットを計算できます。このパラメーターのデフォルトは、10 進数の 61440 です。このパラメーターは、Db2 データベース構成値 ASLHEAPSZ を使用して計算され、4096 で乗算されます。ASLHEAPSZ の値を取得するには、Db2 コマンド db2 get dbm cfg を実行して、ASLHEAPSZ の値を探します。 通常、この値は 15 で、その結果、デフォルトの 61440 が算出されます。これが 15 ではない場合は、その値を使用し、4096 で乗算して、適切なクライアント・オフセットを算出します。
db2bp_path		はい		NULL	Solaris Zones および AIX WPAR で、db2bp 実行可能ファイルのパスを使用する場合、特定の時点で複数の DB2 インスタンスの uid_chain をアクティブ化できます。 このパラメーターの値は、グローバル Zone/Wpar から見えるように関連 db2bp の絶対パスである必要があります。例えば、ファイルが /data/db2inst1/sqllib/bin/db2bp であり、ゾーンが /data/zones/oracle2nd/root/ にインストールされている場合、db2bp_path パラメーターに設定する必要がある db2bp への絶対パスは /data/zones/oracle2nd/root/data/db2inst1/sqllib/bin/db2bp です。

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
db2_shmem_size				131072	Db2 共有メモリー・セグメント・サイズ

親トピック: UNIX S-TAP パラメーター

ファイアウォール・パラメーター

これらのパラメーターは、ファイアウォールに関する S-TAP の動作に影響を与えます。

表 1. ファイアウォール用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
firewall_installed			はい	0	ファイアウォール機能を有効にします。1=有効、0=無効。
firewall_timeout			はい	10	タイムアウトになる場合、Guardium システムからの判断を待機する時間 (秒単位)。 接続をブロックするのか、許可するのかを知るために、firewall_fail_close 値を調べます。任意の整数値を指定できます。
firewall_fail_close			はい	0	Guardium システムから判断が返されず、firewall_timeout が経過すると、firewall_close = 0 の場合、接続は許可されます。firewall_close=1 の場合、接続はブロックされます。
firewall_default_state			はい	0	ファイアウォール・モードの開始が何によってトリガーされるか。 0= インストールされているポリシー内のルールをトリガーするイベントが発生する。1= トリガーするイベントに関係なく、ファイアウォール・モードが有効になった状態で開始する。 このフラグは、ルールに関係なく、ファイアウォールの監視 (有効化) を強制しますが、特定のアクション (DROP など) は、ルールによってトリガーされる場合にのみ発生します。 注: S-TAP が firewall_default_state=1 に設定されている場合、照会再書き込みのデフォルトの状態である grw_default_state=1 を同時に設定することはできません。
firewall_force_watch	9.0		はい	NULL	ファイアウォール機能が有効になっていて、firewall_default_state が 0 の場合、セッションの監視は、そのクライアント IP が IP/MASK 値のリストと一致する場合に自動的に行われます。リスト自体は、コンマで区切られます。例: 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2
firewall_force_unwatch	9.0		はい	NULL	ファイアウォール機能が有効になっていて、firewall_default_state が 1 の場合、セッションの監視は、そのクライアント IP が IP/MASK 値のリストと一致する場合に自動的に行われません。リスト自体は、コンマで区切られます。例: 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2,

親トピック: UNIX S-TAP パラメーター

アプリケーション・サーバー・パラメーター

アプリケーション・ユーザー名をデータベース・アクティビティーとバインドする必要がある場合、これらのパラメーターは S-TAP の動作に影響を与えます。

表 1. アプリケーション・サーバー用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
appserver_installed		はい	はい	0	0 の場合、S-TAP は通常どおり機能します。1 の場合、S-TAP は「クライアント・モード」に設定され、S-TAP が データベース・サーバー ではなくクライアントにインストールされていることを反映するように S2C と C2S のパケットを切り替えます。 また、1 の場合、他の appserver_* パラメーターが入力されているかどうかを検査し、入力されている場合は、指定されているポートの http パケットを調べて、クライアント・システムに常駐する java アプリケーションのエンド・ユーザーについてのセッション情報を取得します。
appserver_ports		はい	はい	8080	Java アプリケーションが Web ブラウザーを介してアクセスされるポートのコンマ区切りリスト。
appserver_login_pattern		はい	はい		アプリケーションに渡されるログイン・パターンを指定するストリングのコンマ区切りリスト。 これは、Java アプリケーションに渡されるユーザーのログインを示すパターンです。
appserver_username_prefix		はい	はい		指定のセッションのユーザー名の接頭部を指定するストリングのコンマ区切りリスト。 これは、Java アプリケーションが、指定のセッションのユーザー名を示すために使用するパターンです。
appserver_username_postfix		はい	はい		指定のセッションのユーザー名の接尾部を指定するストリングのコンマ区切りリスト。 これは、Java アプリケーションが、ユーザー名を示す特定の変数の値の終わりを示すために使用するパターン (または文字)です。
appserver_session_pattern		はい	はい		特定のデータベース・セッションを使用するエンド・ユーザー・セッションの開始を指定するストリングのコンマ区切りリスト。
appserver_session_prefix		はい	はい		セッション ID が開始する場所を指定するストリングのコンマ区切りリスト
appserver_session_postfix		はい	はい		セッション ID が終了する場所を指定するストリングのコンマ区切りリスト。
appserver_usersess_pattern		はい	はい		指定の接続が継続しているエンド・セッションをマーキングするための ID を指定するストリングのコンマ区切りリスト。

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
appserver_usersess_prefix		はい	はい		指定の usersess 標識パケットの session_id を識別する (session_id に先行する) 対象を指定するストリングのコンマ区切りリスト。
appserver_usersess_postfix		はい	はい		セッション ID が終了する場所を指定するストリングのコンマ区切りリスト。

親トピック: UNIX S-TAP パラメーター

discovery パラメーター

discovery パラメーターは、データベース・インスタンスのディスカバーと現在アクティブな S-TAP への結果の送信を行うオートディスカバリー機能の動作を定義します。

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
discovery_interval				24	オートディスカバリーが実行される時間間隔 (時間)。使用不可にするには 0 に設定します。
discovery_dbs				oracle:db2:informix:mysql:postgres:sybase:hadoop:teradata:netezza:memsql	ディスカバーするデータベース・タイプのコロン (:) 区切りリスト。
discovery_debug				0	ディスカバリー・デバッグ・レベル 0 = エラーのみ 1 = エラーとデバッグ・ステートメント
discovery_ora_alt_locations					listener.ora ファイルを検索する代替場所
discovery_port				8443	S-TAP のディスカバリーが Guardium システムへの接続に使用する Guardium ポート。

親トピック: UNIX S-TAP パラメーター

構成監査システム (CAS) パラメーター

これらのパラメーターは、このシステム上の CAS の動作に影響を与えます。

表 1. CAS 用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
cas_task_checkpoint		はい		task_checkpoint	
cas_client_baseline				client_baseline	
cas_client_checkpoint		はい		client_checkpoint	
cas_checkpoint_period		はい		3600	チェックのための時間間隔 (秒単位)。
cas_fail_over_file		はい		fail_over_file	出力メッセージ・バッファーが入っているファイルの名前。
cas_fail_over_file_size_limit		はい		50000	フェイルオーバー・ファイルのサイズ。
cas_max_reconnect_attempts		はい		5000	接続が失われた場合の再接続の試行回数。
cas_reconnect_interval		はい		60	次の再接続を試行するまでの待機時間 (秒単位)。
cas_raw_data_limit		はい		1000	Guardium システムに送信される生データのサイズ制限 (キロバイト単位)。
cas_md5_size_limit		はい		1000	MD5SUM を計算する対象の最大ファイル・サイズ (キロバイト単位)。
cas_command_wait	8.0			300	長期実行データ収集プロセスを強制終了するまでの待機時間 (秒単位)。
cas_server_failover_delay	8.0			60	別の Guardium システムへの接続を試行するまでの待機時間 (分単位)。

親トピック: UNIX S-TAP パラメーター

デバッグ・パラメーター

これらのパラメーターは、S-TAP デバッグの動作に影響を与えます。

これらのパラメーターは、S-TAP プロパティー・ファイルの [DEBUG_OPTIONS] セクションに格納されています。

表 1. デバッグ用の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
debug_buffer				1	1=ローカル・パケットの内容をログに記録します
debug_firewall				1	1=ファイアウォール・イベントをログに記録します

これらのパラメーターは、S-TAP プロパティー・ファイルの [TAP] セクションに格納されています。

表 2. デバッグ用の追加の S-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
syslog_messages				1	1= メッセージを syslog に送信します。0=メッセージは送信されません。
tap_debug_output_level					STAP ログ・レベル。ログは、tap_log_dir パラメーターで指定されるディレクトリーにある guard_stap.stderr.txt、guard_stap.stdout.txt、guard_stap.fam.txt です。各 STAP ログ・レベルは以下のとおりです。 • 0: クリティカル・エラー情報のみ • 1: クリティカル・エラー情報に加え、反復可能な非クリティカル・エラー情報 • 2: レベル 1 のチェックに加えて、KTAP がダウンしていることをチェックしてから、PCAP がバックアップを取ります • 3: レベル 1 のチェックに加えて guard_stap 構成ファイルが有効かどうかをチェックします • 4: レベル 1 のチェックに加えてローカル・スニッフィング・ログをチェックします • 5: レベル 1 のチェックに加えて、ネットワーク・スニッフィング・ログをチェックします • 6: レベル 1 のチェックに加えて、Appserver デバッグ情報をチェックします • 7: レベル 1 のチェックに加えて、診断スクリプトの実行をトリガーします
remote_messages		はい		1	• 0=メッセージを送信しません。 • 1=アクティブな SQL Guard ホストにメッセージを送信します。

親トピック: UNIX S-TAP パラメーター

K-TAP パラメーター

これらのパラメーターは、K-TAP の動作に影響を与えます。

表 1. K-TAP 構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
ktap_installed			はい	1	カーネル・モニター・モジュールがインストールされているかどうか。0=いいえ、1=はい。 ktap_installed と tee_installed は、相互に排他的であるため、一方のみを設定できます。
ktap_request_timeout	8.0			5	K-TAP 応答の待機に関するタイムアウトです。K-TAP は、ioctl を stap に送信して情報を求め、stap からの応答を待機します。単位は秒で、任意の値を指定できます。
ktap_dbgev_ev_list	8.0			0	GUI または guard_tap.ini ファイルによって、K-TAP トレース・ログを有効にするために使用されます。0 は、/var/tmp ディレクトリーに置かれる ktap トレース・ログを無効にし、1 は有効にします。
ktap_dbgev_func_name	8.0			すべて	K-TAP トレース・ログに記録する関数のリスト。all を指定すると、すべての関数が記録されます。accept などの特定の関数を指定すると、accept 関数のみがログ・ファイルに記録されます。 K-TAP トレース・ログとは関係のない関数を指定する場合、ログには何も記録されません。
ktap_fast_tcp_verdict	8.0			1	tcp 接続の場合、K-TAP は ioctl を stap に送信し、Ips を検査することによって、セッションが IE で構成されたデータベース接続であることを確認します。ktap_fast_tcp_verdict を 1 に設定すると、セッションのポートが範囲内にある限り、K-TAP は要求を S-TAP に送信しません。1 または 0 の値を指定できます (0)。
ktap_fast_file_verdict	8.0			1	tli 接続の場合、K-TAP は ioctl を S-TAP に送信し、ポートおよび Ips を検査することによって、セッションが IE で構成されたデータベース接続であることを確認します。 ktap_fast_file_verdict を 1 に設定すると、セッションのポートが範囲内にある限り、K-TAP は要求を S-TAP に送信しません。 1 または 0 の値を指定できます (1)。
ktap_buffer_size	8.0			4194304	拡張機能。K-TAP バッファーのバイト単位のサイズ。値の範囲は 1 MB から 16 MB までです。
ktap_buffer_flush	8.0			0	拡張機能。K-TAP から S-TAP にメッセージを送信する手段。1 の場合、S-TAP は K-TAP バッファー全体を読み取り、バッファー内のすべてのパケットを処理します。 ktap_flush_buffer=0 の場合、S-TAP はバッファー全体ではなく、一定量を読み取ります。
ktap_local_tcp	8.2			0	1=ローカル接続のみをインターセプトします (以前にインターセプトされた接続は引き続き取り込まれます) (このパラメーターは、TCP 接続に使用されます)
khash_table_length	8.0			24593	Khash 表に格納できるセッションの数。任意の整数値を指定できます。
khash_max_entries	8.0			8192	特定のセッションのすべての情報を入れる表の長さ。任意の整数値を指定できます。

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
ktap_fast_shmem	9			1	Db2 共有メモリー接続の場合 • 0=KTAP: ioctl を STAP に送信して、プロセス ID を確認することで、セッションが IE で構成されたデータベース接続であることを確認します。 • 1=K-TAP: セッションの db2_shmem_size が、接続されている共有メモリー・セグメントと一致するまで、S-TAP に要求を送信しません。
fam_enable				1	FAM のグローバル有効化/無効化。
ktap_fsmon_buffer_size				4194304	FAM バッファー・サイズ。

表 2. A-TAP および PCAP の構成パラメーター

パラメーター	バージョン	GUI	GIM	デフォルト値	記述
atap_exec_location				/var/guard	検査エンジン・セクションの暗号化ボックスを有効にして ATAP をアクティブにする場合に使用される実行可能ファイルの場所。
pcap_read_timeout	8.0			0	pcap トラフィックのみ (ktap ではない) です。pcap サンプリング間の STAP の待機時間を示します。この値を変更する場合には必ずその前に、Guardium サービスに問い合わせ、問題を検証し、pcap/stap に関連するボトルネックを原因とする損失 (取り込まれないトラフィックがある) を特定します。
pcap_dispatch_count	8.0			16	pcap による取り込みを最適化します。stap にレポートを返す前にバンドル (グループ化) するパケットの数です。パケットをグループ化することによって pcap と stap 間の通信を削減し、パフォーマンスを向上させます。この値を変更する場合には必ずその前に、Guardium サービスに問い合わせ、問題を検証し、pcap/stap に関連するボトルネックを原因とする損失 (取り込まれないトラフィックがある) を特定します。
pcap_buffer_size	8.0			-1	pcap ソケット・バッファーのサイズ。このパラメーターは、LINUX でのみ使用されます。この整数のデフォルト値は -1 です。これは、可能な最大バッファーを取得することを示します。その他の値は、キロバイト単位のバッファー・サイズを示します。0 は無効です。0 の場合は 60 を意味します。これ以外であれば、65535 までの任意の値を指定できます。 バッファーが大きいほど、トラフィックが急激に増大した際に、損失が発生しにくくなります。高トラフィックが発生すると、pcap はすべてを取り込みますが、stap (または pcap から stap へのフロー) は速度が十分ではないため、トラフィックについていくことができません。損失を回避するために、未処理のパケットがバッファーに入れられます。 バッファーが大きいほど、トラフィックが急激に増大した場合に、より高いトラフィックや、より長時間継続するトラフィックの増大に対する回復力が高くなります。この値を変更する場合には必ずその前に、Guardium サービスに問い合わせ、問題を検証し、pcap/stap に関連するボトルネックを原因とする損失 (取り込まれないトラフィックがある) を特定します。
	8.0			1	このパラメーターを有効にすると、IE で定義された Db2 がある限り、ktap_installed が有効かどうかに関係なく、常に PCAP を開始します。

GIM GUI を介してカスタム KTAP モジュール配布の使用を制御するためにパラメーターを追加

GIM ユーザー - カスタム・ビルド KTAP をカスタム・バンドルにコンパイルし、他のデータベース・サーバー上でそれを使用します。

GIM ユーザー以外 - カスタム・バンドルは必要ありません。手動でカスタム KTAP をコンパイルし、データベース・サーバー間でコピーできます。

パラメーター名: GIM_ALLOW_CUSTOM_BUNDLES

有効な値: 「1」 - カスタム・バンドル・インストールを許可します。 「0」 - カスタム・バンドル・インストールを拒否します。

デフォルト値: 1

GIM のスクラッチ・インストール時 (DB サーバー) - ユーザーはオプションの新規インストール・パラメーター (install_custom_bundles) を指定できます。

このパラメーターを指定した場合、カスタム・バンドル・インストール (カスタム・バンドル STAP など) が、その DB サーバー上で許可されます (GIM_ALLOW_CUSTOMED_BUNDLES は「1」に設定されます)。 指定しない場合は許可されません (GIM_ALLOW_CUSTOMED_BUNDLES は「0」に設定されます)。

このパラメーターが含まれていなかった GIM バージョンから (GIM GUI を使用して) GIM をアップグレードする場合 - (その時点までこのカスタム・バンドルのフィーチャーを使用している可能性がある顧客のため、この機能を無効にしないように) デフォルトの値は「1」になります 。

DB サーバー上でコンフィギュレーター・ユーティリティーを使用する場合、このパラメーターは「1」または「0」のどちらにも設定できます。

前の値が「0」の場合、このパラメーターは GUI で「1」に設定できません。

注: この機能は (DB サーバー上への) インストール時にはチェックされますが、バンドル・インストールやパラメーター更新の割り当てまたはスケジューリングを行っているときには (他のすべてのパラメーターが検証されているようには) チェックされません 。

影響する機能: BUNDLE-GIM、configurator.sh、統合インストーラー

GuardAPI コマンドおよびカスタム KTAP バンドル

v10 の場合

1. STAP_UPLOAD_FEATURE インディケーターはデフォルトでオン (1) になっています。 そのため、カスタム KTAP はコンパイル時に自動的にアプライアンスにアップロードされます。

2. 新規カスタム KTAP を組み込むため、カスタム GIM バンドルをコンパイルするには、ユーザーは GrdAPI make_bundle_with_uploaded_kernel_module コマンド (正確な構文のコマンドが必要) を実行する必要があります。
3. どのサーバーでも既にコンパイル済みのカスタム・バンドルを使用できるようにするには、お客様は GIM_ALLOW_CUSTOM_BUNDLES インディケーターをオンにして 1 にする必要があります (これはセキュリティー上の理由により、各 DB サーバー上で手動で実行する必要があります)。GIM_ALLOW_CUSTOM_BUNDLES インディケーターをオフに戻すことは、アプライアンスから実施できます。

親トピック: UNIX S-TAP パラメーター

遅延クラスター・ディスク・マウントの構成

このトピックは、Oracle、Informix®、および DB2® の各データベース・サーバーにのみ適用されます。

これらのデータベース・タイプでは、S-TAP は開始時に、データベース・ホームへのアクセス権限を持っている必要があります。ご使用の環境でクラスタリング・スキームを使用しており、パッシブ・ノードではなく、アクティブ・ノードにマウントされている単一ディスクを複数のノードが共有している場合、パッシブ・ノード上ではフェイルオーバーが発生するまでデータベース・ホームを使用できません。

構成ファイルのプロパティー WAIT_FOR_DB_EXEC を設定することにより、 S-TAP で遅延ロードを構成することができます。S-TAP は、開始時にデータベース・ホームにアクセスできないことを検出すると、WAIT_FOR_DB_EXEC の値を調べて、適切な処置を行います。

- WAIT_FOR_DB_EXEC > 0 の場合、プロセス名の stat() が可能かどうかにかかわらず、S-TAP が始動します。これは、15 分間隔でプロセス名の stat() を試行します。
- WAIT_FOR_DB_EXEC < = 0 の場合、S-TAP は、検査エンジンが起動したすぐ後に、検査エンジンのプロセス名の stat() を試行します。プロセス名の stat() ができない場合、S-TAP は終了します。

このプロパティーを正の値に設定する前に、その他の必要な構成プロパティーがすべて設定されていることを確認し、S-TAP が開始して、正しくデータを収集することをテストしてください。このプロパティーは、構成ファイルを編集することによってのみ設定でき、GUI からは設定できません。

親トピック: 特別な環境での構成 (Linux、Solaris、HP-UX、AIX)
親トピック: S-TAPs およびその他のエージェント

S-TAP 状況モニター

S-TAP 状況モニターを使用すると、ご使用の S-TAP の現在の状況を表示したり、問題を調査したりすることができます。

「管理」 > 「システム・ビュー」 > 「S-TAP 状況モニター」にナビゲートして、各 S-TAP の状況を表示できます。

リスト内の行をクリックすると、この S-TAP 用に構成されている検査エンジンが表示されます。 階層リンクを参照すると、現在位置が分かります。「すべての S-TAP」をクリックして、S-TAP のリストに戻ります。

検査エンジンのリストには、検査エンジンが検証されているかどうかが示されます。 検査エンジンが検証されていない場合、すぐに検証用にサブミットすることも、既存の検証スケジュールに追加することもできます。 検査は、以下のデータベース・タイプでサポートされています。

- DB2
- Greenplum
- Informix
- MSSQL
- MySQL
- Netezza
- Oracle
- PostgreSQL
- Sybase
- Teradata (詳細検査のみ)

サポートされていないタイプのデータベースの横にあるボックスにチェック・マークを付けると、そのタイプは検査用にサポートされていないというメッセージが表示されます。
検査には、以下の 2 つのタイプがあります。

標準検査
: 無効なログイン要求を送信して、適切なエラー・メッセージが返されることを確認することによって、S-TAP および検査エンジンを検査します。

詳細検査
: 失敗ログイン要求を避ける必要がある場合は、詳細検査を使用できます。 このタイプの場合、ターゲット・データベースに関連付けられたデータ・ソース定義を識別または作成する必要があります。 データ・ソース定義には、検査プロセスがデータベースにログインするために使用する資格情報が含まれています。 次に、エラー・メッセージを生成するために、存在しない表からデータを取得するための要求が送信されます。

両方のタイプの検査要求について、実行されたテストと、失敗したテストの推奨アクションについての情報を提供する新しいダイアログに結果が表示されます。

検査結果を表示する前に、システムはデフォルトで 5 秒待機します。 ネットワーク待ち時間が長い場合、これは、データベース・サーバーからの予期される応答を受信するには、十分の時間ではない可能性があります。 より長い時間が必要な場合は、store stap network_latency CLI コマンドを使用して、期間を変更できます。

関連トピック:

- S-TAP 検査結果の確認
- S-TAP 検査スケジュールの構成
- Linux プラットフォームでの S-TAP の問題のトラブルシューティング

親トピック: S-TAPs およびその他のエージェント

S-TAP 検査結果の確認

S-TAP 検査プロセスはいくつかの構成パラメーターを確認し、検査エンジンに接続しようとします。結果は S-TAP 状況モニター・ページに表示されます。

データベースに接続する前に、検査プロセスは、Guardium システム上でスニファー・プロセスが実行されているかどうかを検査します。スニファーは、各 S-TAP との通信と、受信されるデータの処理を担当します。スニファーが実行されていない場合、S-TAP からの応答は認識されません。

検査プロセスでは、間違ったユーザー ID とパスワードを使用してデータベースへのログインが試行され、この試行が認識され、Guardium システムに通知されることが確認されます。要求が行われた Guardium システムにメッセージが到達しないように、S-TAP を構成することができます。

このような構成の詳細には、以下が含まれます。

- ロード・バランシング: 複数の Guardium システムに応答を返すように S-TAP が構成されている場合は、エラー・メッセージをさまざまな Guardium システムに送信できます。
- フェイルオーバー: 2 次 Guardium システムが S-TAP 用に構成されていると、1 次 Guardium システムがビジー状態である場合に、エラー・メッセージを 2 次 Guardium システムに送信できます。
- Db_ignore_response: データベースからのすべての応答を無視するように S-TAP が構成されている場合、エラー・メッセージは Guardium システムに送信されません。
- クライアント IP/マスク: 0.0.0.0 ではないマスクを定義する場合、エラー・メッセージが送信されない可能性があります。
- 除外 IP/マスク: 0.0.0.0 ではないマスクを定義する場合、エラー・メッセージが送信されない可能性があります。

次に、検査プロセスが、データベース・サーバー上の選択された検査エンジンに接続できるかどうか検査します。失敗ログインを示す応答を受信することが想定されています。 異なる応答が受信される場合は、さらに調査を行わなければならない可能性があります。

個々のデータベースからの一部エラー・メッセージは、特定の 1 つの問題を示しているわけではありません。 例えば、いくつかのサポートされるデータベース上で、ポートが間違っているためにエラー・コードが返される場合、データベース自体が開始していないことも意味する可能性があります。

検査プロセスの結果は、ダイアログに表示されます。 失敗した検査が最初に示され、次のステップのための推奨事項が示されます。 リスト末尾の縮小表示されたセクションに、成功した検査が表示されていることを確認します。 状況によっては、成功した検査を調べることが、考えられる複数の次のステップから選択するのに役立つ場合があります。

関連トピック:

- S-TAP 状況モニター
- Linux プラットフォームでの S-TAP の問題のトラブルシューティング
- S-TAP 検査スケジュールの構成

親トピック: S-TAPs およびその他のエージェント

S-TAP 検査スケジュールの構成

S-TAP 検査を実行するためのスケジュールを構成できます。

このタスクについて

デフォルトで、S-TAP の検査のスケジュールは、毎日 1 時間に 1 回です。 検査がスケジュールされているすべての S-TAP に、同じスケジュールが使用されます。このスケジュールは変更可能です。

手順

1. 「管理」 > 「アクティビティー・モニター」 > 「S-TAP 検査スケジューラー」をクリックして、「S-TAP 検査スケジューラー」を開きます。
2. このページの「S-TAP 検査スケジューラー」の部分で、「スケジュールの変更」をクリックします。
3. 「スケジュール定義」ダイアログで、ドロップダウン・リストとチェック・ボックスを使用して、検査実行のスケジュールを設定します。 このスケジュールは、検査がスケジュールされているすべての S-TAP に適用されます。
4. 「保存」をクリックして、変更を保存します。

親トピック: S-TAPs およびその他のエージェント

Linux プラットフォームでの S-TAP の問題のトラブルシューティング

「システム・ビュー」の「S-TAP 状況モニター」タブを使用して、問題の調査を行うことができます。 他のツールを使用しなければならない場合があります。特に、検査エンジンを検査できないデータベースをモニターしている場合です。

- S-TAP が Guardium システムに接続されていない場合は、以下のようにして S-TAP プロセスがデータベース・サーバー上で実行されているかどうかを確認します。

  UNIX: S-TAP® プロセスが実行されていることを確認する
  データベース・サーバー上で、コマンド行でコマンド ps -ef | grep stap を実行して、S-TAP プロセスが実行されていることを確認します。プロセス・リストの中で、/guardium/guard_stap を探します。

- **Linux**: コマンド行から、<stap_program> <parameter_file> <debug_level> という構文でデバッグを実行して、迅速に構成の問題を特定します。ここで、通常デバッグのレベルは 4 です。(他の値では実行内容が異なり、デバッグではないこともあります)。例: /usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini 4
- データベース・サーバーと Guardium システムの間の接続を確認します。
  - データベース・サーバーから *sqlguard_ip* で Guardium システムを ping できることを確認します。
  - ping が成功した場合は、Guardium システム上のポート 16016/16018 に Telnet でログインできることを確認します。
- データベース・サーバーと Guardium システムの間にファイアウォールがある場合は、これら 2 つのシステムの間でのトラフィック用に、TCP ポート 16016 または TLS ポート 16018 (暗号化接続の場合) が開かれていることを確認します。
  注: ポートが使用可能かどうかを確認するには、コマンド `nmap -p port guardium_hostname_or_ip` を使用します。
- sqlguard_ip パラメーターが、接続先の Guardium システムの正しい *guardium_hostname_or_ip* に設定されていることを確認します。
  1. 「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」をクリックして、「S-TAP 制御」を開きます。

2. データベース・サーバーに対応する IP アドレスの S-TAP ホストを見つけます。
3. 「Guardium ホスト」サブセクションを展開して、アクティブな Guardium ホストが正しく構成されていることを確認します。
4. 必要に応じて、「変更」をクリックして、Guardium ホストを更新します。

- S-TAP プロセスが繰り返し再始動していないことを確認します。データベース・サーバー上で、コマンド `ps -eaf | grep stap` を実行して、S-TAP のプロセスが変更されていないことを確認します。
- S-TAP 承認がオンになっていないことを確認します。S-TAP 承認がオンになっていると、Guardium システムに接続されている新規 S-TAP は、すべて拒否されます。
  1. 「管理」 > 「アクティビティー・モニター」 > 「S-TAP 認証」をクリックして、「S-TAP 認証」を開きます。
  2. 「S-TAP 承認が必要」チェック・ボックスを調べます。このボックスにチェック・マークが付いている場合、新規 S-TAP がこの Guardium システムに接続できるのは、承認済み S-TAP のリストに追加されてからになります。
  3. S-TAP 承認がオンになっている場合は、「日次モニター」 > 「承認された Tap クライアント」を選択して、承認済み S-TAP のリストを表示します。 調査対象の S-TAP がこのリストにない場合は、「S-TAP 認証」ペインに戻り、「クライアント・ホスト」フィールドに S-TAP の IP アドレスを入力して、「追加」をクリックします。

S-TAP がグリーンの状況になっているにもかかわらず、データが処理されていない場合は、A-TAP の状況を確認します。

関連トピック:

- S-TAP 状況モニター
- S-TAP 検査結果の確認
- S-TAP 動作のモニター

親トピック: S-TAPs およびその他のエージェント

S-TAP 動作のモニター

S-TAP モニター (guard_monitor) は、S-TAP のパフォーマンスと反応性をモニターするために設計されたプロセスです。さまざまなしきい値に基づいて、特定のアクションを実行できます。

UNIX/Linux の場合、CPU パフォーマンスは *ps* コマンドを使用してチェックします。 反応性は、S-TAP プロセスにコンソール要求を送信し、応答を待機することでチェックします。

S-TAP の CPU 使用率が構成されたしきい値を超える場合、あるいは S-TAP がコンソール要求に応答しない場合、以下のアクションが実行されることがあります。

- 自動的に guard_diag を実行。
- 自動的に S-TAP プロセスを強制終了。
- 自動的にコア・ダンプが行われ、S-TAP プロセスを強制終了。

注: S-TAP モニターは UNIX/Linux および Windows で使用可能です。

表 1. モニター対象 (UNIX/Linux)

UNIX/Linux
CPU 使用率
メモリー
強制終了
コア・ダンプ
診断の実行
「Alive」 - 反応性 (CPU ポーリング)

Guard_monitor はデフォルトでは有効になっていません。

シェル・インストールでは、「umon」行をアンコメントするか、特定のオペレーティング・システムのサービス制御機能 (RedHat 6 以降の場合は initctl、Solaris 10 以降の場合は SMF) を使用することで、inittab から有効にする必要があります。

GIM インストールの場合、以下を設定して guard_monitor を有効にします。

STAP-UTILS_START_MONITOR=y

注: Guard_monitor は管理特権 (root) を必要とします。

S-TAP モニター出力のデフォルトの場所は /var/tmp/monitor です。 この場所は、guard_monitor.ini (構成ファイル) で構成可能です。このトピックの最後にある guard_monitor.ini ファイルの例を参照してください。

guard_monitor を有効にしたら、そのプロセスがデータベース・サーバーで稼働中であることを確認してください。

注: guard_monitor は、その構成ファイル (guard_monitor.ini) を引数として稼働します。 このモニターは、guard_monitor.ini ファイルを使用して制御されます。 シェル・インストールの場合、構成に関するすべての変更は構成ファイルで直接行うことができます。 GIM の場合、GUI のインターフェースを使用して変更を行います。
注: S-TAP インストール後、Guard モニターが自動的にインストールされます。 ユーザー・プロンプトは示されず、インストールの進行状況は表示されません。 S-TAP のアンインストール時、Guard モニターは自動的にアンインストールされます。 そのため、ユーザーはインストーラー内のリブートのオプションが使用できなくなり、代わりに、アンインストールを完了するためにリブートが必要という通知を受けます。 このリブートは重大ではありませんが、システムに S-TAP を再インストールしたい場合には必要です。 アンインストールし、リブートを行わずに再インストールを試みると、インストールをブロッキングするポップアップが表示されて、S-TAP が部分的にインストールされており、サーバーにはリブートが必要ということが通知されます。

設定例

各関数には、デフォルトのしきい値があります。 例えば、CPU 使用率をモニターする場合、診断情報の収集のためのしきい値 (75%) を設定し、S-TAP を強制終了するためのより高いしきい値 (85%) を設定することができます。診断情報の収集を有効にするには auto_diag=1 を設定し、CPU 使用率が 75% に達した場合に診断情報を収集するには diag_high_cpu_level=7500 を設定します。 次いで、S-TAP プロセスの自動強制終了を有効にするために auto_kill_on_cpu_enable=1 を設定し、CPU 使用率が 85% に達した場合にプロセスを強制終了するために auto_kill_on_cpu_level=8500 を設定します。

auto_kill_on_cpu_level=8500 により、CPU 使用率が 85% に達した場合にプロセスが強制終了されます。

S-TAP プロセスを繰り返し強制終了することを避けるために、制限を設けることもできます。kill_num_in_hour=5 を設定することによって、1 時間のうちにプロセスを強制終了する回数を制限できます。 次いで、制限に達した場合の処置を指定します。S-TAP を無効にするには final_action=1 をコーディングし、実行を継続するには final_action=2 をコーディングします。

Guard_monitor CPU ポーリング・パラメーター

guard_monitor は、以下に定義するように、デフォルトでは 10 秒ごとに STAP の CPU 使用率を検査します。

poll_cpu_interval=10 (guard_monitor.ini パラメーター)

STAP-UTILS_MONITOR_POLL_CPU_INTERVAL =10 (GIM インターフェース)

また Guard_monitor は、以下に定義するように 10 秒ごとにコンソール S-TAP 要求を送信します。

poll_stap_interval=10

STAP-UTILS_MONITOR_POLL_STAP_INTERVAL =10

guard_monitor は CPU 使用率をチェックする際、*ps* を使用して guard_stap プロセスの存続期間中の平均の CPU 使用率を測定します。 つまり、STAP は guard_monitor が問題を検出するまで、しばらくの間 CPU しきい値を超えて実行されることになります。

Linux プラットフォームの場合のみ、Guardium は、タイム・スライスでの平均 CPU 使用率に基づいたより正確な S-TAP CPU 測定をサポートします。

cpu_measurement_timeslice=5

Auto-Diag アクション

S-TAP の CPU 使用率が構成されたしきい値を超える場合、guard_monitor により実施される最も基本的なアクションは自動 guard_diag です。

まず、自動 guard_diags を有効にします。

auto_diag=1 (guard_monitor.ini)

STAP-UTILS_MONITOR_AUTO_DIAG =1 (GIM)

次に、guard_monitor が guard_diag を開始する STAP CPU しきい値を定義します。

diag_high_cpu_level=7500 (guard_monitor.ini パラメーター)

STAP-UTILS_MONITOR_DIAG_HIGH_CPU_LEVEL=7500 (GIM パラメーター)

注: CPU レベルは、*ps* 出力による 10 進小数点の問題を回避するため、100 の倍数で入力します。

モニターは、以下のパラメーターの定義に従って、複数の guard_diag 出力を作成できます。

diag_num=2 (guard_monitor.ini)

STAP-UTILS_MONITOR_DIAG_NUM=2 (GIM)

guard_diag からの出力は /var/tmp に配置されます。

Auto-Kill アクション

モニターは、guard_diag 出力の生成に加えて、S-TAP プロセスを自動的に強制終了することもできます。

S-TAP の自動強制終了を以下のように有効にします。

auto_kill_on_cpu_enable=1 (guard_monitor.ini)

STAP-UTILS_MONITOR_AUTO_KILL_ON_CPU_ENABLE =1 (GIM)

次に、guard_monitor が STAP を強制終了する STAP CPU しきい値を定義します。

auto_kill_on_cpu_level=8500 (guard_monitor.ini パラメーター)

STAP-UTILS_MONITOR_AUTO_KILL_ON_CPU_LEVEL=8500 (GIM パラメーター)

guard_monitor が 1 時間以内に強制終了される回数を制限できます。

kill_num_in_hour=5 (guard_monitor.ini)

STAP-UTILS_MONITOR_KILL_NUM_IN_HOUR =5 (GIM)

1 時間あたりの最大強制終了回数に達した場合に実行される内容は次のようになります。 final_action を以下のように構成して、S-TAP を無効化する (1) か、または S-TAP の強制終了を停止して実行を継続します (2)。

final_action=2 (guard_monitor.ini)

STAP-UTILS_MONITOR_FINAL_ACTION =2 (GIM)

強制終了前の S-TAP のコア・ダンプ

S-TAP がループに陥っている場合など、S-TAP の問題によっては guard_diag 出力に示されている内容より詳しい情報が必要になります。

Guardium v10.0 の新機能は、guard_monitor による S-TAP プロセスの自動的なコア・ダンプの実行です。 guard_monitor は、プロセスを強制終了する前に S-TAP のコア・ダンプを行います (S-TAP の自動強制終了が有効な場合)。

自動コア・ダンプを構成するためのパラメーターは 2 つあります。

force_core_before_kill=< sigsegv| gcore|pstack>

kill_oldcore_saved=1

force_core_before_kill は、生成されるコア・ダンプのタイプを指定するストリング・パラメーターです。

sigsegv: これは、最も便利なオプションですが、SA はコア・ダンプを有効にするために ulimit を構成する必要があります。

gcore: 最も便利なオプションですが、システムに gcore がインストールされている必要があります。

pstack: 一番便利でないオプションですが、一部のシステムでは使用できる唯一のユーティリティーです。

kill_old_core_saved は整数のパラメーターです。 ゼロ以外に設定すると、guard_diag は、生成されたすべてのコア・ダンプを維持します。 そうではない場合、新規コア・ダンプが生成されるたびに、古いコア・ダンプを削除します。

guard_monitor で作成されたコア・ダンプは /var/tmp/monitor/coredumps にあります。

guard_monitor.ini の例

; 以下のセクション・ヘッダーは、GIM がこの .ini ファイルを認識するために必要です。

; それ以外の目的はありません

[TAP]

; モニター・ログ、診断、トレースなどの出力ディレクトリー。

monitor_output_dir=/var/tmp

; guardium インストール済み環境の場所 (モニターのインストール場所である必要はありません。例： /usr/local)

stap_dir=/usr/local

; 構成ファイルをダウンロードしたり、診断やトレースの出力をアップロードするために接続する IP

; これは guard_tap.ini から解析されますが、ここのバックアップ値は同期が維持されます。

sqlguard_ip=NULL

; サーバー・エンドが引き続き有効であることを確認するためのポーリング間隔 (秒単位)

poll_server_interval=20

; CPU レベルをチェックするためのポーリング間隔 (秒単位)

poll_cpu_interval=10

; STAP との通信のためのポーリング間隔 (秒単位)

poll_stap_interval=10

; モニター・ログ・ファイルの最大ファイル・サイズ (KB)

monitor_log_rotate_size=1024

; 保持する循環モニター・ログの数

monitor_log_rotate_num_kept=5

; ログ・ファイルの最大ファイル・サイズ (KB)

log_rotate_size=4096

; 保持する循環ログの数

log_rotate_num_kept=5

; 循環するログ

logs_to_rotate=/tmp/guard_stap.stderr.txt,/tmp/guard_stap.stdout.txt,/usr/local/guardium/guard_stap/ktap/ktap_install.log,/usr/local/guardium/guard_stap/guard_discovery.stderr.log

; 1 時間あたりの STAP 強制終了の最大数 (auto_kill_on_intercept により行われた強制終了はカウントしない)

kill_num_in_hour=5

; 1 時間あたりの強制終了回数が上限に達した場合に STAP を無効にするか、強制終了を無効にして STAP を続行する

; STAP を無効にする: 1; 強制終了を無効にする: 2

final_action=2

```
; CPU レベルで STAP を自動的に強制終了する オン/オフ (1/0)
auto_kill_on_cpu_enable=0
; 強制終了のための CPU レベル (% * 100)
auto_kill_on_cpu_level=8500
; 強制終了のための snif タイムアウト (秒単位、0 は無効)
auto_kill_on_snif_timeout=0
; 強制終了のための KTAP タイムアウト (秒単位、0 は無効)
auto_kill_on_ktap_timeout=0
; 強制終了のための PCAP タイムアウト (秒単位、0 は無効)
auto_kill_on_pcap_timeout=0
; 強制終了のための TEE タイムアウト (秒単位、0 は無効)
auto_kill_on_tee_timeout=0
; 強制終了のための SHMEM タイムアウト (秒単位、0 は無効)
auto_kill_on_shmem_timeout=0
; 自動診断 オン/オフ (1/0)
auto_diag=1
; 診断の実行回数
diag_num=2
; 診断実行間の時間 (分)
diag_interval=2
; 古い診断ファイルを保持するかどうか はい/いいえ (1/0)
diag_oldrun_saved=0
; 診断後に STAP を強制終了する はい/いいえ (1/0)
diag_auto_kill=0
; 診断トリガーのための CPU レベル (% * 100)
diag_high_cpu_level=7500
; 診断トリガーのための snif タイムアウト (秒単位、0 は無効)
diag_snif_timeout=0
; 診断トリガーのための KTAP タイムアウト (秒単位、0 は無効)
diag_ktap_timeout=0
; 診断トリガーのための PCAP タイムアウト (秒単位、0 は無効)
diag_pcap_timeout=0
; 診断トリガーのための TEE タイムアウト (秒単位、0 は無効)
diag_tee_timeout=0
; 診断トリガーのための SHMEM タイムアウト (秒単位、0 は無効)
diag_shmem_timeout=0
; 自動トレース オン/オフ (1/0)
auto_trace=0
; トレース実行の最大時間 (秒)
trace_max_time=30
; トレースの最大ログ・ファイル・サイズ (MB)
trace_max_log_size=10
; 古いトレース・ログ・ファイルの保持 はい/いいえ (1/0)
trace_oldlog_saved=0
; トレースが実行完了をしたときに STAP を強制終了する はい/いいえ (1/0)
```

; (例えば、低 CPU によりキャンセルされない場合)

trace_kill_on_complete=0

; トレースをトリガーするための CPU レベル (% * 100)

trace_high_cpu_level=6000

; トレースをキャンセルするための低 CPU レベル (% * 100)

trace_low_cpu_level=3500

; snif 通信トリガーのタイムアウト (秒単位、0 は無効)

trace_snif_timeout=0

; KTAP 通信トリガーのタイムアウト (秒単位、0 は無効)

trace_ktap_timeout=0

; トレースをトリガーするための PCAP タイムアウト (秒単位、0 は無効)

trace_pcap_timeout=0

; トレースをトリガーするための TEE タイムアウト (秒単位、0 は無効)

trace_tee_timeout=0

; トレースをトリガーするための SHMEM タイムアウト (秒単位、0 は無効)

trace_shmem_timeout=0

; 構成されたデータベースをインターセプトしていない場合に STAP を自動的に強制終了する はい/いいえ(1/0)

; guard_tap.ini が STAP がルートとして実行されていることを示す場合にも機能は無効になります。

auto_kill_on_intercept=0

; STAP の要求された強制終了間の最小時間 (分)

intercept_min_time_interval=15

; 1 時間あたりのインターセプトの強制終了の最大数

intercept_max_num_in_hour=0

注: HP-UX 11.11 では、process コマンドに関する情報は 64 文字に制限されています。 つまり、guard_stap バイナリーへの絶対パスが 64 文字を超える場合、S-TAP モニターはそのパスを認識できなくなります。

Windows S-TAP 動作のモニター

Guardium Agent Monitor (GAM) は、Guardium エージェントのパフォーマンスと反応性をモニターするために設計されたプロセスです。さまざまなしきい値に基づいて、特定のアクションを実行できます。

モニター対象エージェントが構成されたしきい値を超える場合、あるいはコンソール要求に応答しない場合 (サポートされるエージェントのみ)、以下のアクションが実行される可能性があります。

- 自動的に diag.bat を実行
- サービスの自動停止/再始動
- サービスのコア・ダンプの自動取得

表 2. モニター対象 (Windows)

Windows
CPU 使用率
メモリー
処理
スレッドの数
「Alive」 - 反応性 (サポートされるエージェントのみ。現在は S-TAP が唯一のサポート対象エージェント)

Guardium Agent Monitor は S-TAP と一緒にインストールされますが、デフォルトでは有効になりません。

注: 注: S-TAP がアンインストールされると、GAM はアンインストールされます。詳しくは、S-TAP インストールの資料を参照してください。
注: 注: GAM には管理特権が必要です。

GAM のデフォルトのインストール・ロケーションは、S-TAP の親フォルダーです (C:¥Program Files¥IBM¥Guardium Agent Monitor¥)。

GAM 出力のデフォルト・ロケーションは ¥Bin¥ サブフォルダーです。

GAM を有効にしたら、そのプロセスがデータベース・サーバーで実行されていることを確認してください (resmon.exe)。

GAM 構成

Guardium Agent Monitor は、その構成ファイル resmon.ini を引数として実行します。このモニターは、resmon.ini ファイルを使用して制御されます。

グローバル構成

NUMBER_OF_SERVICES - モニターされるサービスの数

UPDATE_INTERVAL - 各ポーリング・メトリック間のインターバルの長さ (秒単位)

DEBUG - 1 は GAM デバッグ・ログの有効化、0 はログなしです。

NUMBER_BYTES_IN_LOG - GAM ログの最大バイト数 (KB 単位)。

CPU しきい値構成

CPU_LOAD_LIMIT - CPU しきい値 (%)

CPU_INTERVALS_ALLOWED - アクションがトリガーされるまでに、CPU がしきい値を超えることができるインターバルの数 (時間制限を設定するために UPDATE_INTERVAL と一緒に使用)

CPUAVE - 値 1 は、その CPU パーセンテージが、すべての CPU コアの平均値 (システム平均) であることを意味します。0 は、プロセスが使用するコアのパーセンテージを意味します。

メモリー使用量、ハンドル数、およびスレッド数のしきい値構成

これらのメトリックには、制限とピーク制限の 2 つのしきい値があります。許可される以上のインターバルでピーク制限しきい値を上回るか制限しきい値を下回ると、アクションがトリガーされます。

[METRIC]_LIMIT - 下位しきい値。[METRIC]_INTERVALS_ALLOWED よりも多くのインターバルで下回ると、アクションがトリガーされます。

[METRIC]_PEAK_LIMIT - 上位しきい値。このしきい値を上回ると、アクションがトリガーされます。

[METRIC]_INTERVALS_ALLOWED - アクションがトリガーされるまでに、下限しきい値で許可されるインターバルの数 (時間制限のための UPDATE_INTERVAL と一緒に使用)

アクション構成

アクション構成

アクション構成は 0、1、または 2 に設定できます。0 はアクションなしです。1 はサービスを停止してから開始することを意味します。2 はサービスを停止することを意味します。

2 番目と 3 番目のアクションは、前のアクションの ACTION_RESET_INTERVAL 内でトリガーされた場合にのみ実行されます。ACTION_RESET_INTERVAL 時間の後、トリガーされる次のアクションは FIRST_ACTION となります。

FIRST_ACTION - インターバル中に初めてアクションがトリガーされたときに行う必要のあるアクション

SECOND_ACTION - インターバル中に 2 回目にアクションがトリガーされたときに行う必要のあるアクション

THIRD_ACTION - インターバル中に 3 回目にアクションがトリガーされたときに行う必要のあるアクション

ACTION_RESET_INTERVALS - アクションをリセットするまでの秒数

コア・ダンプ構成

コア・ダンプ構成

[Global] セクション内で ACTION 値を 1 に設定することにより、アクションがトリガーされるたびにコア・ダンプを取ることができます。

ACTION - アクションがトリガーされるたびにコア・ダンプを取る場合は 1、コア・ダンプを取らない場合は 0

MAX_NUM_DUMP - ダンプ・ディレクトリーに保管されるコア・ダンプの最大数 (最新のものを保持)

MDTIMEOUT - コア・ダンプのタイムアウト時間 (ミリ秒単位)

診断構成

診断構成

DIAGACTION 値を 1 に設定することにより、アクションがトリガーされるたびに診断ファイルを実行できます。 サービスの実行可能パスと同じフォルダーにある DIAGNAME 診断スクリプトが、DIAG_PARAMETER のパラメーターによって実行されます。

DIAGACTION - アクションがトリガーされるたびに診断スクリプトを実行する場合は 1、診断スクリプトを実行しない場合は 0

DIAGNAME - 実行する診断ファイルの名前 (サービス実行可能ファイルと同じフォルダー内になければなりません)

DIAG_PARAMETER - 診断ファイルの実行時に使用されるパラメーター

注: [METRIC]_INTERVALS_ALLOWED は、しきい値の制限時間を設定するために UPDATE_INTERVAL と一緒に使用されます。(例えば UPDATE_INTERVAL=1、CPU_INTERVALS_ALLOWED=10、CPU_LOAD_LIMIT=10 の場合は、CPU パーセントが 10 秒以上 10 %を超える場合にアクションがトリガーされることを意味します)

resmon.ini の例

resmon.ini の例

;行の先頭にあるセミコロンはコメントを示します

```
;
[Global]
NUMBER_OF_SERVICES=1
;
;しきい値を確認するインターバル (秒)
UPDATE_INTERVAL=1
;
;モニター・ログの有効化
DEBUG=1
;
;「0」はアクションのミニダンプを取らないことを意味します。「1」はミニダンプを取得します
ACTION=1
;
;ダンプ・ディレクトリーに保管されるダンプの最大数
MAX_NUM_DUMP=3
;
;平均 CPU 時間。「0」は 1 つのコアに対するパーセンテージ、「1」はシステム内のすべてのコアの平均パーセンテージです。
CPUAVE=1
;
;ミニダンプのタイムアウト (ミリ秒単位)
MDTIMEOUT=1000
;モニター・ログの最大バイト数 (KB 単位)
NUMBER_BYTES_IN_LOG=200
;
;サービスの構成
[Service1]
Name=GUARDIUM_STAP
;
;生存を確認するインターバル (サポートされるエージェントのみ)。無効にするには「0」に設定します。
NAMEDPIPE_INTERVAL=30
;
;アクションへの診断の実行。有効にするには「1」に設定します。
DIAGACTION=0
;
;診断ファイル名
DIAGNAME=diag.bat
;
;診断パラメーター。 パラメーターにスペースが含まれている場合は、引用符で囲む必要があります。
DIAG_PARAMETER=
;
;CPU 制限のパーセンテージ
CPU_LOAD_LIMIT=10
;
;CPU_LOAD_LIMIT が許容される最大連続インターバル数
CPU_INTERVALS_ALLOWED=10
```

```
;
;メモリー制限 (KB)
MEM_USAGE_LIMIT=150000
MEM_USAGE_PEAK_LIMIT=200000
MEM_USAGE_INTERVALS_ALLOWED=30
;
;ハンドル制限
HANDLE_COUNT_LIMIT=500
HANDLE_COUNT_PEAK_LIMIT=1000
HANDLE_COUNT_INTERVALS_ALLOWED=20
;
;スレッド制限
THREAD_COUNT_LIMIT=200
THREAD_COUNT_PEAK_LIMIT=300
THREAD_COUNT_INTERVALS_ALLOWED=20
;
;「1」はアクションを実行し、サービスを再始動します。
;「2」はアクションを実行し、サービスを停止して始動しません。
FIRST_ACTION=1
SECOND_ACTION=1
THIRD_ACTION=2
;
;リセット間隔 (秒単位)
ACTION_RESET_INTERVALS=60
```

親トピック: S-TAPs およびその他のエージェント

「S-TAP イベント」パネル

「S-TAP イベント」パネルを使用して、S-TAP® によって出力されるイベント・メッセージを表示することができます。

制御パネルにリストされている任意の S-TAP の「S-TAP イベント」パネルを開くには、次のようにします。

1. 「レポート」 > 「リアルタイム Guardium 運用レポート」 > 「S-TAP イベント」をクリックして、「S-TAP イベント」を開きます。

列	記述
イベント・タイプ	成功、エラー・タイプなど
イベントの記述	イベントの簡略説明
タイム・スタンプ	イベントが発生した日時

注: 「S-TAP イベント」パネルにメッセージが表示されない場合は、その S-TAP の構成ファイル内でイベント・メッセージの生成が無効になっている可能性があります。その場合は、ホスト・システム上のイベント・ログ (Windows) または syslog ファイル (UNIX/Linux) 内に S-TAP イベント・メッセージがある場合があります。

親トピック: S-TAPs およびその他のエージェント

S-TAP レポート

デフォルトでは、このトピックで説明するレポートが「レポート」パネルに表示されます。

「不正な接続」ドメインで新規照会またはレポートを定義したり、 S-TAP が作成した例外に基づいてアラートを作成したりすることができますが、 S-TAP レポートが使用する他のドメインはシステム専用であり、ユーザーは アクセスできません。

システム・ビュー

S-TAP 状況モニター - このレポートは、この Guardium システムへの各 S-TAP レポートについて、S-TAP ホスト、S-TAP バージョン、データベース・サーバー・タイプ、状況 (アクティブまたは非アクティブ)、最後に受信した応答 (日時)、1 次ホスト名、および (KTAP、TEE、MS SQL サーバー共有メモリー、DB2® 共有メモリー、ローカル TCP モニター、名前付きパイプの使用、および暗号化の) true/false インジケーターを示します。

注: DB2 共有メモリー・ドライバーは DB2 Tap フィーチャーに置き換えられました。

TAP モニター

不正な接続 - このレポートは、UNIX サーバーでハンター・オプションが有効になっている場合にのみ使用できます。ハンター・オプションが使用されるのは、TEE モニター方式が使用されている場合に限られます。 このレポートは、データベースに接続するために、 S-TAP® を回避したすべてのローカル・プロセスをリストします。

S-TAP 構成変更履歴 - このレポートは、検査エンジンが追加または変更されたときだけ表示されます。S-TAP の構成変更がリストされます。個々の検査エンジンの変更は別々の行に表示されます。 各行には、S-TAP ホスト、データベース・サーバー・タイプ、データベース・ポート (始まり)、データベース・ポート (終わり)、データベース・クライアント IP、データベース・クライアント・マスク、および変更のタイム・スタンプがリストされます。

プライマリー Guardium® ホスト変更ログ - S-TAP の 1 次ホスト変更のログ。1 次ホストとは、 S-TAP がデータを送信する Guardium システムです。このレポートの各行には、S-TAP ホスト、Guardium ホスト名、期間の開始、期間の終了がリストされます。

S-TAP 状況 - 各 S-TAP ホストで定義されている各検査エンジンについて、状況情報を表示します。 このレポートは現在の状況をレポートするため、開始日と終了日の パラメーターはありません。このレポートの各行は、S-TAP ホスト、データベース・サーバー・タイプ、状況、最後の応答、1 次ホスト名、および属性 (K-TAP (インストール済み)、TEE (インストール済み)、共有メモリー・ドライバー (インストール済み)、DB2 共有メモリー・ドライバー (インストール済み)、名前付きパイプ・ドライバー (インストール済み)、およびアプリケーション・サーバー (インストール済み)) の Yes/No インディケーターをリストします。さらに、ハンター DBS をリストします。

非アクティブな S-TAP - システムで定義されている非アクティブな S-TAP をすべてリストします。 これには 1 つだけ、QUERY_FROM_DATE というランタイム・パラメーターがあり、デフォルトでは now -1 hour に設定されています。このパラメーターを使用して、*非アクティブ*をどのように定義するのかを制御します。このレポートには、S-TAP 状況レポートと同じデータの列が含まれており、レポートの各行のカウントが追加されています。

親トピック: S-TAPs およびその他のエージェント

S-TAP エラー・メッセージ

以下のリストは、S-TAP® が生成するエラー・メッセージをアルファベット順に説明します。

メッセージ	記述
inifile .../guard_tap.ini を読み取れません: セクション SQLGUARD_x 内の IP アドレス・パラメーター sqlguard_ip のホスト名 xxx を解決できません。.../guard_tap.ini.bak に戻ります。	S-TAP 構成ファイル (guard_tap.ini) にエラーがあります。これが発生する可能性が最も高いのは、手動で編集を行った場合です。これが発生すると、S-TAP は最新の既知の良好なバックアップ・ファイル (使用可能な場合) から再始動を試みます。
バインド: アドレスは既に使用されています [データベース・サーバー名または IP] tee の listen ソケットをバインドできません: アドレスが既に使用されています。	S-TAP TEE が使用を試みているポートは、既に使用されています。例えば、ポート 4100 で listen するように TEE を構成し、Sybase がそのポートですでに listen している場合に、このメッセージを受け取ります。
接続: ネットワークは到達不能です	アクセス不能のホストに到達しようとする場合に受け取る標準メッセージ。多くの場合、これは Guardium システムが ping 要求に応答していないことを意味します。
遅延サーバー接続エラー: 接続が拒否されました	Guardiumシステムは、この S-TAP からの接続要求を拒否しています。Guardium システムで検査エンジンが実行していないか (可能性は低い)、S-TAP 接続を受け入れるように設定されていないか (その Guardium システムの unit_type 設定を確認) のいずれかです。
不明の pid:n 上の接続を削除しています	エラー・メッセージではありません。無視されます。
リモート・マシンから接続を取得しました。無視します。	S-TAP が、リモート・ホストのアプリケーションから (TEE ポートへの) 接続要求を受け取り、その要求を無視しています。Tee はローカル接続のみに使用する必要があります。
新規構成を取得しました	Guardium® 管理者が、Guardiumシステムへのログイン中に構成を更新しました。更新された構成ファイルを S-TAP が受け取りました。
Guard Tee がポート 12346 上で接続を受け入れています	通常の TEE プロセス開始メッセージ (TEE のインストール時にのみ表示されます)。
Guardium TAP を開始しています	通常の S-TAP プロセスの開始メッセージ。
ソケットからの読み取り: 接続がピアによってリセットされました	データベース・サーバーまたはデータベース・クライアントがダウンしています。例えば、誰かが Oracle sqlplus セッションを実行して、ctrl-C を使って終了しました。このメッセージは問題を示すものではありません。
サーバーから 180 秒間受信しませんでした。終了して、再始動しています	S-TAP は 180 秒間、Guardiumシステムからハートビート・シグナルを受け取っていません。サーバーへの再接続を試行します。データはバッファー・ファイルにキャッシュされているため、失われることはありません。
SQLguard ソケット読み取り: 接続がピアによってリセットされました	Guardiumシステムが S-TAP への接続を閉じました。これが発生するのは、Guardium システムを再始動する場合、または Guardium システムの検査エンジンが自動的にダウンして、再開する場合 (この場合は、問題を示すものではありません) です。
waitpid: 子プロセスがありません	エラー・メッセージではありません。無視されます。
n を強制終了しました	S-TAP ハンター・プロセスが、n で識別される無許可接続を強制終了しました。

親トピック: S-TAPs およびその他のエージェント

S-TAP 付録

このセクションでは、Informix® のあるバージョンから別のバージョンへの移行について詳述します。

ある Informix バージョンから別のバージョンへの移行の手順 (SUSE 32 ビット)

SUSE 32 ビット Linux では、複数の Informix バージョンがインストールされている場合に、以下の段階的な方法を使用して、一方の Informix バージョンから他方のバージョンへ移行できます。これにより、セマフォーと共有メモリー・セグメントがクリーンアップされるため、Informix データベースをクリーンな状態で使用開始できま

す。以下のステップは、A-TAP が活動化されていることが前提です。

1. ipcs コマンドを使用して、Informix データベースで作成されたすべてのセマフォーと共有メモリー・セグメントのリストを取得する。それらはユーザー root に属するものとして表示される場合があるため、作業には注意が必要ですが、一般的には次のようになります。共有メモリー・セグメントは、アクセス権 0660 のものが 3 つと、アクセス権 0666 のものが 1 つあり、セマフォー配列は、アクセス権 0660 のものが 4 つと、アクセス権 0666 のものが 1 つあります。これらはすべて root に属します。
2. Informix データベースを停止する。
3. Informix データベースで作成されたすべてのセマフォーと共有メモリー・セグメントがなくなっていることを確認する。
4. (Linux のみ) Informix インスタンスが A-TAP で活動化されていた場合は、非アクティブにする。
5. /etc/passwd を変更する (ユーザーの Informix ホーム・ディレクトリーが正しいロケーションを指すようにする)。
6. 新規 Informix インスタンスの S-TAP® 検査エンジン内で、インストール・ディレクトリーが正しいことを確認する。必要な場合は変更を加えて、S-TAP を再始動する。
7. (Linux のみ) A-TAP で Informix を活動化する (必ず正しいバージョンを指定する)。
8. 新規インスタンスを始動する。

親トピック: S-TAPs およびその他のエージェント

コマンド行からの CAS のインストール、始動、停止

以下のコマンドを使用して、CAS をインストール、始動、および停止します。

Unix CAS のインストールに必要なパラメーターは、すべてコマンド行から指定できます。

インストーラー・スクリプトのコマンド行構文

それぞれの構成要素について、以下で説明します。変数は、不等号括弧 (< >) で囲んであります。

使用法: `guard-cas-setup -- install --java-home <JAVA_HOME> --install-path <INSTALL_PATH> --stap-conf <FULL_PATH_TO_GUARD_TAP_INI>`

使用法: `guard-cas-setup -- uninstall`
`<guard-cas-setup> is the name of the script file`
`-- install は、CAS のインストールを示します。`
`-- uninstall は、CAS のアンインストールを示します。`
`--java-home <JAVA_HOME> は、JAVA_HOME ディレクトリーを識別します。『Java 情報の取得』を参照してください。`
`--install-path は、インストール・パスを識別します。`
`--stap-conf <FULL_PATH_TO_GUARD_TAP_INI>identifies where the guard_tap.ini file is located after an S-TAP installation.`

CAS の始動および停止

インストールまたはアンインストールのシナリオに応じて、コマンド行から CAS を始動および停止する必要がある場合があります。シナリオによっては、guard_tap.ini ファイルへの --stap-conf パスを指定しない場合があります (これはオプション・パラメーターであるため)。この場合、CAS は始動しません。CAS を始動または停止する必要がある場合、次の方法を使用します。

1. root アカウントを使用して、データベース・サーバー・システムにログオンします。
2. Red Hat Enterprise Linux 6 の場合
   a. stop cas コマンドまたは start cas コマンドを使用して CAS を始動または停止します。
3. その他すべての場合:
   a. /etc/inittab ファイル内の CAS エージェント項目を、コメント化するか (CAS を停止する場合)、コメントを削除します (CAS を始動する場合)。デフォルト・インストールでは、このステートメントは以下のようになります。

      ```
      cas:<nnnn>::respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
      ```

   b. /etc/inittab ファイルを保存します。
   c. init q コマンドを実行します。
4. -fe | grep cas コマンドを実行することで、CAS が実行されているかどうかを検証できます。

親トピック: S-TAPs およびその他のエージェント

IMS 定義

IMS 定義により、Guardium システムから監査対象の IMS 環境への接続が確立されます。

Guardium システム・インターフェースを使用して IMS 定義の作成や変更を行うには、S-TAP が IMS システムにインストールされていて、エージェント・アドレス・スペース (AUIASTC) と Guardium システムとの接続が事前に確立されている必要があります。エージェントが正常に接続されておらず、接続を確立するための情報が必要な場合は、「IBM Guardium S-TAP for z/OS User's Guide」の『Installing IBM Guardium S-TAP for IMS on z/OS』を参照してください。

IMS が定義されると、エージェントのポリシー・プッシュダウン設定に従い、その IMS 定義が追加のポリシーと共に S-TAP に送信されます。 ポリシーのプッシュダウン時に IMS on z/OS S-TAPS のポリシーを含めるには、そのポリシーを IMS 定義に関連付ける必要があります。 プッシュダウン・イベントの構成について詳しくは、「IBM Guardium S-TAP for z/OS User's Guide」の『Policy pushdown』トピックを参照してください。

IMS 定義の構成におけるステップごとのサポートについては、「IBM Guardium S-TAP for z/OS User's Guide」の『Creating and modifying IMS definitions』を参照してください。

親トピック: S-TAPs およびその他のエージェント

Db2 for i S-TAP

Guardium Db2 for i S-TAP を使用して、IBM i 上のあらゆるデータベース・アクセスをモニターおよびレポートすることができます。これには、ネイティブのデータベース入出力操作または SQL アクセスを使用するあらゆるプログラム (RPG など) が含まれます。

Guardium Db2 for i S-TAP によって収集された情報を使用して、アクティビティー・レポートを作成したり、監査要件を満たしたり、無許可アクティビティーに関するアラートを生成したりすることができます。詳細な監査情報には、以下の内容が含まれます。

- セッションの開始時刻と終了時刻
- TCP/IP アドレスおよびポート
- オブジェクト名 (例えば、表またはビュー)
- ユーザー
- SQLSTATE
- ジョブおよびジョブ番号
- SQL ステートメントおよび変数
- クライアントの特殊レジスター値
- インターフェース情報 (ODBC、ToolboxJDBC、ネイティブ JDBC、.NET など)

S-TAP は、以下の 2 つのソースからデータを受け取ります。

- SQL アプリケーション用の SQL パフォーマンス・モニター (別名はデータベース・モニター) データ
- SQL 以外のインターフェースを使用したアプリケーション用の QSYS/QAUDJRN 監査ジャーナルからの監査項目

これらのソースからのデータには、以下が含まれます。

- あらゆる SQL アクセス。これには、IBM i サーバーで開始されたアクセスも、クライアントから開始されたアクセスも含まれます。
- 監査ジャーナルで取得されたネイティブ・アクセス。

S-TAP は、このデータを Guardium システムにリアルタイムで送信します。
Db2 for i S-TAP および関連するトピックについて詳しくは、以下の情報源を参照してください。

- Using IBM Security Guardium for monitoring and auditing IBM DB2 for i database activity: この developerWorks の記事は、IBM Guardium、DB2 for i S-TAP、および関連する主要な詳細情報を紹介しています。
- IBM i の IBM Knowledge Center: IBM i、監査ジャーナル、およびその他の関連トピックについての情報は、この Web サイトを参照してください。

暗号化、ロード・バランシング、フェイルオーバー用の i S-TAP

IBM i S-TAP では、TLS 暗号化、S-TAP セッションのロード・バランシング、S-TAP セッションのフェイルオーバーがサポートされています。

注: i S-TAP の TLS とロード・バランシングは、IBM i 7.1 と 7.2 でのみサポートされます。

UNIX S-TAP の場合と同様に、i S-TAP の構成パラメーターは、IBM i サーバー上の /usr/local/guardium ディレクトリー内の guard_tap.ini ファイルに保存されます。

管理者は、他の UNIX S-TAP と同じ API と UI (S-TAP 制御) を使用して S-TAP を構成します。GUI または API を使用して S-TAP の構成を変更すると、Guardium のスニファーがメッセージを S-TAP に送信します。メッセージを受信した S-TAP は、古い .ini ファイルのバックアップを作成し、変更された構成情報を新しい .ini ファイルに保存してから、自分自身を再起動します。

管理者は、S-TAP 構成制御を使用して、S-TAP とアプライアンス間の暗号化通信を設定することができます。また、各種のロード・バランシング・オプションを設定することもできます。

S-TAP のフェイルオーバー機能とロード・バランシング機能の使用

i S-TAP のフェイルオーバー・オプションとロード・バランシング・オプションは、UNIX S-TAP のオプションと似ています。participate_in_load_balancing パラメーターを使用して、フェイルオーバー機能またはロード・バランシング機能を使用するかどうかを指定し、S-TAP の SQLGuard セクションを使用して、1 次 Guardium ホスト、2 次 Guardium ホスト、3 次 Guardium ホストを設定します。

i S-TAP と UNIX S-TAP との違いは、i S-TAP の場合は participate_in_load_balancing=3 が必要ないということです。これは、各メッセージについて完全なセッション情報を使用できるように I S-TAP の通信方法が構築されているためです。そのため、このパッチに含まれている拡張機能を適用しなくても、構成ファイルの 1 次 SQLGuard セクションに記述されている participate_in_load_balancing=1 パラメーターと仮想 IP アドレスを使用すれば、F5 などのハードウェア・バランシング機能を使用できるようになっています。

フェイルオーバー構成では、複数のコレクターで登録するように S-TAP が構成されますが、1 回に 1 つのコレクターに対してのみ、トラフィックが送信されます (participate_in_load_balancing=0)。このように構成されている S-TAP は、送信先となる 1 つのコレクターで接続に関する問題が発生しない限り、すべてのトラフィックをそのコレクターに送信します。このコレクターで接続に関する問題が発生すると、2 次コレクターに対してフェイルオーバーがトリガーされます。

IMS からの AppEvent の使用方法

APP_EVENT DLI 呼び出しのユーザー情報を保持するデータは、GuardAppEvent API に類似した構文を使用する必要があります。

先頭の 2 バイトは、それに続くバイトのエンコード方式の CCSID を示します。 例えば、0x04B8 は CCSID 1208 を意味します。 これに続くバイトは、以下のような構文を使用する必要があります。

SELECT

'GuardAppEvent:Start',

'GuardAppEventType:type',

'GuardAppEventUserName:name',

'GuardAppEventStrValue:string',

'GuardAppEventNumValue:number',

'GuardAppEventDateValue:date'

FROM DUAL

type (タイプ)、name (名前)、string (文字列)、number (数値)、date (日付) についての詳細は、「GuardAppEvent API」をご確認ください。

現在サポートされているのは、UTF8 エンコード方式のみです。

- モニター戦略
  法規制およびその他の要件を認識してそれらを満たすための戦略を作成し、モニターおよび監査を効果的かつ効率的に実行できるようにします。
- IBM i 用の S-TAP のインストール
  以下の手順に従って、S-TAP のインストールまたはアンインストールを行います。
- IBM i 用の S-TAP の定義
  S-TAP をインストールした後、S-TAP が Guardium システムと通信できるようにします。

親トピック: S-TAPs およびその他のエージェント

モニター戦略

法規制およびその他の要件を認識してそれらを満たすための戦略を作成し、モニターおよび監査を効果的かつ効率的に実行できるようにします。

どのようなデータが必要か分かったら、無関係のデータをできる限り省いて、必要なデータを収集するための戦略を作成します。不要なデータのモニターおよびロギングにより、ディスク・スペースと処理能力が消費され、余計なネットワーク・トラフィックが発生します。このような戦略をさまざまな領域で実装可能です。

データベースのモニター

グローバル SQL モニターは、SQL 情報をキャプチャーし、その情報を S-TAP のキューに入れます。 モニターのフィルター機能を使用して、キューに入れるユーザーとオブジェクトのタイプを制御することができます。 デフォルトでは、以下のタイプの項目は、S-TAP から Guardium システムに転送されません。

SQL 省略語	意味
AD	ALLOCATE DESCRIPTOR
CL	CLOSE
DA	DEALLOCATE DESCRIPTOR
DE	DESCRIBE
EX	EXECUTE (実行された SQL ステートメントは監査されます)
FE	FETCH
FL	FREE LOCATOR
GD	GET DIAGNOSTICS
GS	GET DESCRIPTOR
HL	HOLD LOCATOR
PR	PREPARE (許可エラーのキャプチャーは除く)
RE	RELEASE
RG	RESIGNAL
SC	SET CONNECTION
SD	SET DESCRIPTOR
SG	SIGNAL

監査ジャーナル

対象となるオブジェクトまたは対象となるユーザーに関係する項目のみキャプチャーするようにシステム監査ジャーナルを構成できます。デフォルトでは、これらのタイプの項目は、S-TAP から Guardium システムに送信されます。

SQL 省略語	意味
ZR	オブジェクトの読み取り
ZC	オブジェクトの変更
CA	権限変更
AD	監査の変更
AF	権限の障害
CO	オブジェクトの作成
DO	オブジェクトの削除
SV	システム値の変更
GR	汎用監査レコード
OM	オブジェクトの移動と名前変更
PG	1 次グループの変更
PW	パスワードまたはユーザー ID が無効
OW	所有者の変更
OR	オブジェクトの復元
RA	権限の変更を復元
RO	所有者の変更を復元

RZ	1 次グループの変更を復元

データベース・オブジェクトに関係する以下の項目のみ転送されます。

- *FILE (表、ビュー、索引、論理ファイル、別名、またはデバイス・ファイル)
- *SQLUDT (SQL ユーザー定義タイプ)
- *SQLPKG (SQL パッケージ)
- *PGM (プロシージャー、関数、またはプログラム)
- *SRVPGM (プロシージャー、関数、グローバル変数、またはサービス・プログラム)
- *DTAARA (SQL シーケンス)

Guardium システム上で
S-TAP から受信した情報の中でどの情報を無視するか、および他の項目に基づいてどのアクションを実行するかを制御するポリシーを定義できます。

ネットワーク上に送信された後にデータを無視することは非効率的です。可能な場合は必ず、S-TAP 用のキューに入れられる前に不要な情報をフィルターで除去してください。

親トピック: Db2 for i S-TAP

IBM i 用の S-TAP のインストール

以下の手順に従って、S-TAP のインストールまたはアンインストールを行います。

始める前に

Db2 for i S-TAP には、Portable Application Solutions Environment (PASE) が必要です。これは、ユーザーが IBM Guardium ユーザー・インターフェースから Db2 for i S-TAP を開始および停止したときに、必要に応じて自動的に開始および停止される環境です。

この S-TAP が接続する Guardium システムの IP アドレスを知っている必要があります。

S-TAP をダウンロードするときには、正しいパッケージがダウンロードされるように、必ず IBM i プラットフォームでフィルターに掛けるようにしてください。

このタスクについて

IBM i では、Guardium Installation Manager (GIM) はサポートされません。

5250 エミュレーター・ソフトウェアを使用して、IBM i システムにリモート接続することができます。

手順

1. IBM i サーバー上で、call qp2term コマンドを入力して、PASE のシェルを開きます。
2. PASE のシェル環境で、S-TAP のインストール・スクリプトを格納するための一時ディレクトリー (/tmp など) を作成します。
3. FTP を使用して、S-TAP のインストール・シェル・スクリプト guard-itap-9.0.0_*rnnnnn*-aix-5.3-aix-powerpc.sh を、作成した一時ディレクトリーに移します。
4. 同じディレクトリーで、以下のコマンドを実行します。

   ```
   guard-itap-9.0.0_rnnnnn-aix-5.3-aix-powerpc.sh guardium_host_IP
   ```

   ここで、*guardium_host_IP* は Guardium システムの IP アドレスです。

タスクの結果

S-TAP が /usr/local/guardium にインストールされます。インストールが完了すると、S-TAP はアクティビティー・モニターを有効にするプロセスを開始し、インストール・コマンドで指定された IP アドレスを使用して、Guardium システムに接続しようとします。

次のタスク

正常なインストールと監査プロセスの開始を確認するには、IBM Guardium Web コンソールに管理者としてログインし、「システム・ビュー」タブにナビゲートして、S-TAP の状況を確認します。

親トピック: Db2 for i S-TAP

S-TAP のアンインストール

手順

S-TAP を停止し、アンインストールするには、以下のコマンドを実行します。

```
RUNSQL SQL('call SYSPROC/SYSAUDIT_End') COMMIT(*NONE)
RMVDIR DIR('/usr/local/guardium') SUBTREE(*ALL)
```

IBM i 用の S-TAP の定義

S-TAP をインストールした後、S-TAP が Guardium システムと通信できるようにします。

始める前に

IBM i システムのログイン資格情報を知っている必要があります。

このタスクについて

S-TAP を構成するための手順の概要を以下に示します。

1. Db2 for i を IBM Guardium に対する認識されたデータ・ソースとして定義し、接続をテストします。
2. Db2 for i S-TAP のインストール時に作成された IBM i 上の構成ファイルの情報を、カスタム表ビルダーのプロセスを使用して Guardium システムに取り込みます。
3. Db2 for i の構成レポートを作成します。このレポート・インターフェースから、モニター・プロセスの開始と停止、状況情報の取得、フィルタリング値を含む構成パラメーターの更新を可能にする Guardium API を呼び出すことができます。

手順

1. 「設定」 > 「ツールとビュー」 > 「データ・ソース定義」をクリックして、「データ・ソース・ビルダー」を開きます。 「アプリケーション選択」ボックスから「カスタム・ドメイン」を選択します。「次へ」をクリックします。
2. 「データ・ソース・ファインダー」で、「新規」をクリックします。これにより、「データ・ソース・ビルダー」が開きます。
3. 「データベース・タイプ」として Db2 for i を選択し、「ホスト」、「サービス名」、「資格情報」に適切な情報を追加します。「適用」をクリックします。
4. 「接続のテスト」をクリックして、構成が正常に行われたことを確認します。
5. 「ツール」 > 「レポートのビルド」をクリックします。
6. 「カスタム表ビルダー」をクリックします。「Db2 for i S-TAP 構成」を選択し、「データのアップロード」をクリックします。 「データ・ソース・ファインダー」に、Db2 for i S-TAP のリストが表示されます。
7. 構成した Db2 for i データ・ソースをこのリストから選択し、「追加」をクリックします。
8. 「データのインポート」画面に、Db2 for i データ・ソースが表示されていることを確認します。「適用」をクリックして、「今すぐ 1 回実行」をクリックします。操作が正常に終了し、行が 1 つ挿入されたことを示すメッセージが表示されます。
9. Guardium のタイトル・バーにある「カスタマイズ」をクリックします。次に、「ペインの追加」をクリックします。
10. ペインに My New Reports などの新しい名前を指定して、「適用」をクリックします。
11. 「カスタマイズ」ペインに「My New Reports」が表示されます。名前の横にあるアイコンをクリックします。「レイアウト」のドロップダウン・リストで、「メニュー・ペイン」を選択します。 「保存」をクリックします。作成した新しいペインがタブの形で表示されます。
12. ナビゲーションペインで、「レポートのビルド」 をクリックします。
13. 照会のドロップダウン・リストから、「Db2 for i S-TAP 構成」をクリックし、次に「検索」をクリックします。
14. 「Db2 for i S-TAP 構成」を選択し、「My New Reports に追加」 (あるいはステップ 10 でペインに指定した名前) をクリックします。
15. 「My New Reports」タブを開きます。この時点でこのタブには、IBM i のレポート行が表示されています。レポート内の行を 1 つダブルクリックし、「呼び出し」を選択します。 選択できる IBM Guardium API のリストが表示されます。
16. update_istap_config を選択します。
17. Guardium API を選択すると、その API の各パラメーターが表示されます。変更が必要な任意の値を変更することができます。start_monitor パラメーターの値を 1 に変更します。「今すぐ呼び出し」 をクリックします。

タスクの結果

update_istap_config API は、入力されたデータを使用して以下のタスクを実行します。

- S-TAP から Guardium システムに項目を送信するために使用されるメッセージ・キューを作成し、INSTEAD OF トリガー (メッセージ・キューに項目を送信する) による、ビューを使用したグローバル・データベース・モニターを開始します。
- PASE および S-TAP を開始します。
- QAUDJRN からジャーナル項目を受け取り、それをメッセージ・キューに追加します。

親トピック: Db2 for i S-TAP

IBM Security Guardium S-TAP for z/OS

IBM Security Guardium S-TAP® for z/OS® ソリューションは、DB2® on z/OS、Data Sets on z/OS、または IMS™ on z/OS のデータ・アクセス情報を収集し、相互に関連付けて、監査員がビジネス・アクティビティーを包括的に把握できるようにするツールです。

IBM Security Guardium S-TAP for DB2 on z/OS

S-TAP for DB2 on z/OS は、各種 DB2 リソースからデータ・アクセス情報を収集し、相互に関連付けて、監査員がビジネス・アクティビティーを包括的に把握できるようにします。S-TAP for DB2 on z/OS は、DB2/zOS データベース・トラフィックをキャプチャーし、そのトラフィックを Guardium® システムに転送します。 S-TAP for z/OS でキャプチャーされるトラフィックは、標準リアルタイム・ポリシーを使用できる Guardium システムに直接転送されます。Guardium は、以下の機能を備えています。

- データ収集 – Guardium は、以下に示すさまざまなタイプの情報を収集し、相互に関連付けて、管理リポジトリーに格納します。
  - オブジェクトの変更 (SQL UPDATE、INSERT 、DELETE)
  - オブジェクトの読み取り (SQL SELECT)
  - 明示的な GRANT および REVOKE 操作 (ユーザーが許可レベルの変更を試行した場合に発生するイベントをキャプチャーするため)
  - 許可 ID の割り当てまたは変更
  - 許可が不十分なために拒否された許可試行
  - オブジェクト (表など) に対する CREATE、ALTER、および DROP 操作
  - オブジェクトへのユーティリティーのアクセス (IBM® ユーティリティーのみ)
  - 入力された DB2 コマンド (特定のコマンドを発行したユーザーを判別する機能を含む)
- 管理ユーザー・インターフェース – これにより、製品管理者は、データ照会を構成できます。

注: DB2 on z/OS の場合、レポート内では、クライアント/サーバー・エンティティー内で定義されたソース・プログラムが、リクエスター・サーバー名と相関 ID を連結させたものになります。
注: DB2 on z/OS の場合、DB2 ユニコード・データベースを使用して、マルチバイト文字をレポート内に正しく表示するには、DB2 パラメーター UIFCIDS を No から Yes に変更します。

IBM Security GuardiumS-TAP for Data Sets on z/OS

S-TAP for Data Sets on z/OS は、レコードからデータ・アクセス情報を収集し、相互に関連付けて、監査員がビジネス・アクティビティーを包括的に把握できるようにするツールです。S-TAP は、以下の機能を備えています。

- データ収集 - S-TAP は、以下に示すさまざまなタイプの情報を収集し、相互に関連付けることができます。
  - SMF により記録される Data Sets データ・セットへのアクセスおよびセキュリティー違反。
  - 削除、名前変更など、Data Sets データ・セットに対して実行されるデータ・セット操作。

IBM Security Guardium S-TAP for IMS on z/OS

S-TAP for IMS on z/OS は、IMS オンライン領域、IMS バッチ・ジョブ、IMS アーカイブ・ログ・データ・セット、および SMF レコードからデータ・アクセス情報を収集し、相互に関連付けて、監査員がビジネス・アクティビティーを包括的に把握できるようにするツールです。IBM Guardium S-TAP は、以下の機能を備えています。

- データ収集 - S-TAP は、以下に示すさまざまなタイプの情報を収集し、相互に関連付けることができます。
  - IMS オンライン領域からのデータベースおよびセグメントへのアクセス。
  - IMS DLI/DBB バッチ・ジョブからのデータベースおよびセグメントへのアクセス。
  - SMF により記録される、データベース、イメージ・コピー、および RECON データ・セットへのアクセス、およびセキュリティー違反。
  - IMS アーカイブ・ログ・データ・セットに記録される IMS オンライン領域の START と STOP、状態アクティビティーのデータベースと PSB の変更、および USER のサインオンとサインオフ。
- 管理ユーザー・インターフェース – ユーザーの管理およびプロファイルの監査のためのフレキシブルなオプションを監査員に提供します。

注: ブロッキング・アクションも、抽出ルールもサポートされていません。制約事項: S-TAP for IMS では、高速処理データベース (DEDB) および IMS 全機能データベースの監査がサポートされています。主記憶データベース (MSDB) の監査はサポートされていません。

IBM Security Guardium S-TAP for z/OS

S-TAP for z/OS クライアントがインストールされていて、トラフィックをキャプチャーするように構成されていることを前提とします。

追加情報については、以下のユーザー・ガイドを参照してください。これらのユーザー・ガイドには、Guardium S-TAP に関する情報が含まれ、概要とその機能、および Guardium を計画、インストール、構成、および使用するためのタスクが記載されています。

入手可能なユーザー・ガイドは、次のとおりです。

- IBM Security Guardium S-TAP for DB2 on z/OS
- IBM Security GuardiumS-TAP for Data Sets on z/OS
- IBM Security Guardium S-TAP for IMS on z/OS

注: これらのガイドの最新バージョンは、Guardium Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSMPHH/SSMPHH_welcome.html) にあります。

ポリシー・プッシュダウン

以下を参照してください。

S-TAP for IMS: http://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.zos/AUI/auiur061.html

S-TAP for DB2: http://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.zos/ADH/adhuc007.html

S-TAP for Data Sets: http://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.zos/AUV/auvur021.html

Guardium for z/OS インターフェース定義

「定義」画面を使用して、z/OS ファイルの取得元となる 1 つ以上のサーバーを保守します。

1. 「セットアップ」 > 「ツールとビュー」 > 「Guardium for z/OS」を選択します。
2. 「新規」 ボタンをクリックして新規の Guardium for z/OS インターフェースを作成するか、Guardium for z/OS インターフェース定義ファインダーから既存のインターフェースを選択し、そのインターフェースを削除したり、変更したり、コメントを付けたりします。
3. 「サーバー IP」ボックスで、 Guardium for z/OS インターフェースがファイルの取得元として使用する IP アドレスを入力します。
4. 「サーバー名」ボックスで、 Guardium z/OS インターフェースがファイルの取得元として使用するサーバー名を入力します。
5. 「ディレクトリー」ボックスで、 z/OS 監査ファイルが配置されているディレクトリーを入力します。
6. 「ユーザー」および 「パスワード」ボックスで、 FTP/SFTP サーバーにアクセスして z/OS ファイルを取り出す (そして削除する) ために使用する名前およびパスワードを入力します。
7. 「SSID」ボックスで、 データベース・サーバーの SSID を入力します。
8. 「ファイル接尾部」ボックスで、コンマで区切った適切なファイル拡張子 (複数可) を入力します。『ロード・バランシング』で追加情報を参照してください。
9. 「転送方式」ボックスで、FTP または SFTP を選択します。
10. アプリケーションから app_user 情報が提供された場合には、「アプリケーション・ユーザー名に END_USER_ID を使用してください」にチェック・マークを付けてください。 それ以外の場合、アプリケーションからデータベースへのトラフィックにはこの情報は含まれません。 つまり、この情報は、app_user 情報のフィールド (end_user_identity マッピング) の内容がどのようになるべきかをパーサーに通知します。
11. 「アクティブ」ボックスにチェック・マークを付けたり、外したりして、 このインターフェースをアクティブにしたり、非アクティブにしたりします。
12. 「ファイルの削除」ボックスにチェック・マークを付けて、 ファイルの転送後それらのファイルをサーバーから削除します。 累積するファイル数が多くなりすぎ、ディスク・スペースに問題が生じることを防ぐため、 これは「ファイルの削除」に設定することを強く推奨します。
13. 「適用」ボタンをクリックしてこの構成を保存します。

注: この「Guardium for z/OS インターフェース定義」メニュー画面には、特定のメニュー選択項目に関するツールチップがあります。カーソルをメニュー選択項目 (ディレクトリーなど) の上に移動すると、簡略説明が表示されます。
注: 既存の定義の編集時に、ユーザー入力のパスワードが空である場合は、古いパスワードが保持されます。 新規レコードの追加時には、ユーザー名およびパスワードの指定は必須です。

Db2 for z/OS SSL 接続データ・ソースのセットアップ

要件: Db2 for z/OS メインフレーム・サーバー・サイドで、DBA による SSL のセットアップ、次のいずれかのオプションへのハンドシェーク・ロールの設定、およびデータ・ソースのセットアップ時にアップロードする必要のある PEM 形式のクライアント証明書の提供が必要になります。

1. HandShakeRole ServerWithClientAuth
2. HandShakeRole Server

「データ・ソースの更新」メニュー画面を以下の選択肢とともに入力します。

1. 「アプリケーション・タイプ」に「セキュリティー・アセスメント」を選択します。
2. 「名前」にお好みのデータ・ソース名を入力します。
3. 「データベース・タイプ」に「Db2 for z/OS」を選択します。
4. 「記述」にデータ・ソースの説明を自由に入力します。
5. 「SSL を使用」ボックスにチェック・マークを付けます。「SSL を使用」ボックスをクリックした後に、「証明書の追加」ボタンをクリックして、Db2 for z/OS の DBA によって提供された PEM ファイルをアップロードする必要があります。
6. 「サーバーの SSL 証明書をインポートします」をクリックします。
7. 認証については、「資格情報の割り当て」にチェック・マークを付けて以下を入力します。
    a. 「ユーザー名」に Db2 z/OS ユーザーを入力します。
    b. 「パスワード」に Db2 z/OS ユーザーのパスワードを入力します。
    c. 「ホスト名/IP」に Db2 z/OS インスタンスのホスト名または IP を入力します。
    d. 「データベース名」に Db2 z/OS データベースの名前を入力します。
    e. 「ポート番号」に Db2 z/OS データベースのポート番号を入力します。

注: 「接続プロパティー」には、エンド・ユーザーが使いやすいように sslConnection=true がハードコーディングされています。

文字セットのサポート

ホスト変数値として、さまざまなコード化文字セット ID (CSSID) が使用される 可能性がありますが、サポートされるものとサポートされないものがあります。

- サポートされている CSSID 変数は適切に変換されます。
- サポートされない CSSID 変数は、CSSID と無変換の値の連結 (例えば、CSSID [number_of_CSSID] : xxxxxxxxxxxxx) で表されます。「x」は、ファイルから受け取ったときの無変換の値です。

サポートされない文字セット

- MacCE
- Cp853

親トピック: S-TAPs およびその他のエージェント

Guardium Installation Manager

Guardium® Installation Manager (GIM) を使用して、管理対象サーバー上で Guardium コンポーネントをインストールおよび保守できます。

GIM コンポーネントには GIM サーバーと GIM クライアントが含まれています。GIM サーバーは Guardium システムの一部としてインストールされます。また、GIM クライアントは、モニターするデータベースまたはファイル・システムをホストするサーバー上にインストールされている必要があります。GIM クライアントは、各管理対象サーバー上で実行される一連の Perl スクリプトです。GIM クライアントをインストールすると、これは GIM サーバーと連動して以下のタスクを実行します。

- インストールされたソフトウェアの更新がないか検査する
- 新規ソフトウェアを転送およびインストールする
- ソフトウェアをアンインストールする
- ソフトウェア・パラメーターを更新する
- データベース・サーバー上で実行中のプロセスをモニターおよび停止する

例えば、GIM を使用して S-TAP モジュールをインストールし、これを最新の状態に維持することができます。

GIM クライアントは、ポート 8444 を使用して、GIM サーバーと通信します。

GIM サーバーは、Guardium ユーザー・インターフェースまたはコマンド行インターフェース (CLI) を介して使用できます。

GIM を使用してデプロイできるソフトウェア・モジュールは、GIM バンドルとしてパッケージされます。*バンドル*とは、GIM を使用してデプロイできるソフトウェアを格納する gim タイプのファイルです。

ご使用の環境に、中央マネージャーとして構成されている Guardium システムが含まれている場合、GIM サーバーとして使用する Guardium システムを決定する必要があります。中央マネージャーのような単一の Guardiumシステム から最大 4000 個のすべての GIM クライアントを管理することも、GIM クライアントをグループとして別々の Guardiumシステム から管理することもできます。 単一の Guardiumシステムからすべての GIM クライアントを管理する場合は、その 1 つの UI で、すべての GIM クライアントの状況を表示し、関連するタスクを実行することができます。グループ内の GIM クライアントを別個の Guardium システムから管理することを選択した場合、各 UI を使用して、それが管理する GIM クライアントで作業することができます。全体的なビューは使用できません。

V9.0 GPU パッチ 50 以降からバージョン 10.0 にアップグレードする場合、GIM クライアントに関する情報の表示方法に変更はありません。それより前のバージョンからアップグレードする場合に、次の制限が適用されます。つまり、ご使用の中央マネージャーをアップグレードした後、他の Guardium システムに割り当てられている GIM

クライアントに関する情報は引き続き表示できますが、これらの GIM クライアントに対するプロビジョニング作業を中央マネージャーから実行できなくなります。ご使用のすべての Guardium システムをアップグレードした後、各 GIM クライアントは、その GIM サーバーである Guardium システムからしか表示できません。

多数の GIM インストール済み環境を管理する場合、GIM クライアントのグループを作成できます。これにより、そのグループを使用して、ソフトウェア・バンドルとしてインストール、更新、管理することができます。

GIM クライアントは、ユーザーが GIM を使用してインストールしたプロセスをモニターします。GIM クライアントは、1 分に一度、各プロセスのハートビートをチェックし、それらのプロセスの状況変更を GIM サーバーに渡します。各プロセスの状況は、「プロセス・モニター」パネルに表示されます。 変更は、3 分以内に反映されます。GIM クライアント自体の状況の変更は、クライアントがサーバーをポーリングし、その「アライブ・メッセージ」を送信する間隔に従って反映されます。

注: システム・バックアップを実行し、GIM が定義されているサーバーから別のサーバーにバックアップを復元する場合、復元先のサーバーに対する GIM フェイルオーバーを構成する必要があります。この GIM 構成は、バックアップ中央マネージャーまたはシステムのバックアップとリストアに適用されます。

- モニター・エージェントをデプロイするためのクイック・スタート
  デプロイ・モニター・エージェント・ツールを使用すると、GIM クライアントのアクティブ化、S-TAP のインストール、およびデータベース・トラフィックのモニター開始を自動的に行えます。
- GIM によるソフトウェアの管理
- GIM サーバーの割り振り
  事前インストールされた非アクティブな (どのコレクターにも接続されていない) GIM エージェントにリモートで接続し、そのエージェントがデータベース・サーバーにアクセスすることなく何らかのコレクターに接続するようにします。
- Windows サーバーへの GIM クライアントのインストール
  対話式インストーラーまたはサイレント・インストールのいずれかを使用して、GIM クライアントを Windows にインストールする方法を説明します。GIM クライアントのアンインストールについても説明します。
- UNIX サーバーへの GIM クライアントのインストール
  このコマンドを使用して、GIM クライアントを各データベース・サーバーにインストールします。
- GIM クライアントのアップグレード
  GIM を使用して GIM クライアントを新しいバージョンにアップグレードできます。
- GIM でのグループの使用
  グループを使用することによって、一部の GIM タスクを実行しやすくすることができます。
- GIM を使用した K-TAP モジュールのコピー
  Linux データベース・サーバー用のカスタム K-TAP モジュールを作成する場合、GIM を使用して、そのモジュールを他の Linux データベース・サーバーにコピーできます。
- GIM の動的更新
  GIM クライアントは、GIM サーバーからの更新がないかを一定の間隔でチェックします。GIM サーバーは、使用する最適なポーリング間隔をシステムの状態に基づいて計算することができます。
- データベース・サーバーのオペレーティング・システムをアップグレードするとき
  データベース・サーバーでオペレーティング・システムをアップグレードするときに、GIM クライアントが、GIM クライアント自体と GIM によってインストールされたモジュール内で必要な変更を行えるようにすることができます。
- 管理対象ユニットへの GIM バンドルの配布
  管理対象ユニットによって管理される GIM クライアント上に GIM バンドルをデプロイするために、管理対象ユニットに GIM バンドルを配布することができます。
- 使用されていない GIM バンドルの削除
  GIM バンドルがデータベース・サーバーで使用されなくなった場合、GIM サーバーから削除することができます。
- GIM 診断の実行
  GIM サーバーが、各 GIM クライアントについて正確なデータを持っているかどうかを確認するために、GIM クライアント上で診断を実行することができます。
- GIM 動作のデバッグ
  問題をトラブルシューティングするためにデバッグをオンにすることが必要な場合があります。
- SMF サポートを備えた Solaris 用の監視プログラムの再始動
  一連の CLI コマンドを使用して、SMF サポートを備えた Solaris サーバーで監視プログラムを再始動します。

モニター・エージェントをデプロイするためのクイック・スタート

デプロイ・モニター・エージェント・ツールを使用すると、GIM クライアントのアクティブ化、S-TAP のインストール、およびデータベース・トラフィックのモニター開始を自動的に行えます。

デプロイ・モニター・エージェント・ツールは、Guardium デプロイメントを確立するプロセスを簡単にします。デプロイ・モニター・エージェント・ツールは、既存の Guardium インストール・マネージャー (GIM) インフラストラクチャーにビルドすることで、データベース・サーバーの検索、モニター・エージェント (S-TAP) のインストール、およびデータベースの検査エンジンの構成を迅速に行えるようにします。また、このツールはデプロイメント状況を追跡および検討するための一元化されたビューを提供します。

- モニター・エージェントをデプロイするための前提条件
  モニター・エージェントのデプロイを開始する前に、前提条件と制限事項を確認してください。
- モニター・エージェントのデプロイ
  S-TAP のデプロイと検査エンジンの構成を迅速に行う方法について説明します。

親トピック: Guardium Installation Manager

モニター・エージェントをデプロイするための前提条件

モニター・エージェントのデプロイを開始する前に、前提条件と制限事項を確認してください。

デプロイ・モニター・エージェント・ツールを使用してデータベース・サーバーに S-TAP をインストールし、検査エンジンを構成する前に、以下の前提条件を確認してください。

GIM クライアントをリスナー・モードでインストールする
ご使用の環境内の 1 つ以上のデータベース・サーバーに GIM クライアントをリスナー・モードでインストールします。Windows システムで GIM クライアントをリスナー・モードでインストールするには、`--host` パラメーターを省略します。AIX や Linux などのシステムで GIM クライアントをリスナー・モードでインストー

ルするには、`--sqlguardip` パラメーターを省略します。GIM リスナー・モードについて詳しくは、GIM サーバーの割り振りを参照してください。
重要: データベース・サーバーの GIM クライアントと、デプロイ・モニター・エージェント・ツールを実行する Guardium システムとの間にポートを開ける必要がある場合があります。GIM クライアントのインストール時に別のポートを指定しない限り、デフォルト・ポート 8445 が使用されます。

Guardium システムへの GIM S-TAP モジュールのアップロード

アグリゲーターとして構成されていない任意の Guardium システムから、管理ユーザーとしてデプロイ・モニター・エージェント・ツールを実行します。作業を開始する前に、以下の手順を使用して GIM S-TAP モジュールを Guardium システムにアップロードします。

1. 「管理」 > 「モジュール・インストール」 > 「モジュールのアップロード」にナビゲートします。
2. 「ファイルの選択 (Choose file)」をクリックし、インストールするモジュールを選択します。
3. 「アップロード」をクリックして、モジュールを Guardium システムにアップロードします。アップロードが完了すると、「アップロード済みモジュールのインポート」表にモジュールが表示されます。
4. 「アップロード済みモジュールのインポート」表で、インストールするモジュールの横にあるチェック・ボックスをクリックします。モジュールがインポートされ、インストール可能な状態になります。モジュールがインポートされると「モジュールのアップロード」ページが再ロードされ、モジュールが 「アップロード済みモジュールのインポート」表に表示されなくなります。

S-TAP オファリングとサポート対象プラットフォームについて詳しくは、System requirements and supported platforms for IBM Security Guardium を参照してください。

検出可能なデータベース・サーバーがすべて実行中であることを確認する

検査エンジンは、以下を含む一部のデータベース用に自動的に構成できます。

- Db2 for Linux, UNIX, and Windows
- Informix
- Microsoft SQL Server
- MySQL
- Oracle
- Postgre SQL
- Sybase
- Teradata

検査エンジンの自動構成を許可するには、モニター・エージェントをデプロイする前にデータベース・サーバーが稼働していることを確認してください。

データベース・インスタンスの自動検出について詳しくは、S-TAP のディスカバリーを参照してください。

親トピック: モニター・エージェントをデプロイするためのクイック・スタート

モニター・エージェントのデプロイ

S-TAP のデプロイと検査エンジンの構成を迅速に行う方法について説明します。

始める前に

アグリゲーターとして構成されていない任意の Guardium システムから、管理ユーザーとしてデプロイ・モニター・エージェント・ツールを実行します。インストールを開始する前に、以下の点を確認してください。

- GIM クライアントがリスナー・モードでインストールされている。
- GIM S-TAP モジュールが Guardium システムにインポートされている。
- 検出可能なデータベース・サーバーが実行されている。

詳しくは、モニター・エージェントをデプロイするための前提条件を参照してください。

このタスクについて

以下の手順は、データベース・トラフィックをモニターするために、デプロイ・モニター・エージェント・ツールを使用して S-TAP のインストールおよび検査エンジンの構成を迅速に行う方法を示しています。

手順

1. 「セットアップ」 > 「クイック・スタート」 > 「モニター・エージェントのデプロイ」にナビゲートし、デプロイ・モニター・エージェント・ツールを開きます。
2. 「データベース・サーバーの識別」セクションの「IP アドレス」フィールドを使用して、リスナー・モードの GIM クライアントを検索する IP アドレスの範囲を指定します。 アイコンを使用して追加の IP アドレスを指定します。検索を拡張するには、ワイルドカード文字 (*) や範囲文字 (–) を含めます。例えば、`10.0.0-5.*` などです。
   重要: 大量の IP アドレスをスキャンすると時間がかかり、スキャンが完了する前にタイムアウトになる可能性があります。「IP アドレス」フィールドを使用して、リスナー・モードの GIM クライアントが検出されると思われる狭い範囲の IP アドレスを定義します。
3. 「ディスカバー」をクリックして、リスナー・モードの GIM クライアントのスキャンを開始します。
   ヒント: デフォルトでは、GIM クライアントのディスカバリーとモニター・エージェント (S-TAP) のデプロイメントは、まずディスカバリーして、次にデプロイメントするという 2 つのステップで実行されます。そのため、以下のステップで説明されているように、S-TAP をインストールするデータベース・サーバーを手動で選択できます。

   ただし、IP アドレスのスキャン中にディスカバーされた、互換性のある GIM クライアントすべてに S-TAP を自動的にインストールすることによって、プロセスを簡素化することができます。自動化モードを有効にするには、 をクリックして「設定のカスタマイズ」ダイアログを開き、「ディスカバーされたデータベース・サーバーにエージェントを自動的にデプロイ」を選択します。自動化モードを使用する場合は、スキャンする IP アドレスを指定した後に「ディスカバーおよびデプロイ」ボタンをクリックするだけです。
4. 「データベース・サーバーの状況」セクションで、モニター・エージェントをデプロイするデータベース・サーバーを選択し、「エージェントのデプロイ」をクリックして「モニター・エージェントの構成」ダイアログを開きます。

5. 「モニター・エージェントの構成」ダイアログから、インストール・パラメーターを確認して調整します。「適用」をクリックし、モニター・エージェントのインストールを開始します。

   ほとんどの新規デプロイメントは、デフォルト・パラメーターでうまく機能します。ただし、特定の環境に応じて以下の設定を調整することができます。

   Windows インストール・ディレクトリー

   Windows データベース・サーバーにデプロイされる S-TAP のインストール・ディレクトリーを指定します。他のプラットフォームにデプロイする場合にはこのパラメーターは無視され、デフォルトのインストール・パスが使用されます。S-TAP インストール・パラメーターについて詳しくは、S-TAPs およびその他のエージェントを参照してください。

   Guardium コレクターの割り当て

   一元的に管理された環境で Guardium コレクターの相対的な負荷や可用性に基づいて自動的に S-TAP を割り当てるには、「エンタープライズ・ロード・バランシングの使用」を選択します。詳しくは、エンタープライズ・ロード・バランシングを参照してください。

   特定の Guardium コレクターに S-TAP を割り当てるには、「コレクターの指定」を選択します。

6. 「データベース・サーバーの状況」セクションで、「S-TAP のインストール状況」列を使用してモジュール・インストールの進行状況をモニターします。`Installed` 状況は、インストールが正常に完了したことを示します。

次のタスク

データベース・サーバーの「S-TAP のインストール状況」に `Failed` のマークが付けられている場合は、アイコンをクリックして問題の詳細を確認します。モニター・エージェントをデプロイしようとした後に「データベース・サーバーの状況」からデータベース・サーバーが消える場合は、「エラー・ログ」をクリックして問題の詳細を確認します。

ヒント: 「エラー・ログ」には、デプロイ・モニター・エージェント・ツールに関連した問題が収集されます。例えば、インストールに必要なモジュールがデプロイ・モニター・エージェントで見つからない場合は、「エラー・ログ」 にメッセージが追加されます。その他のエラーはコンポーネント固有のログに記録され、「S-TAP のインストール状況」列の アイコンをクリックすることで調査に使用できます。

モニター・エージェントが正常にデプロイされたら、データベース・サーバー上のトラフィックをモニターし、セキュリティー・コンプライアンス要件への適合を始める準備は完了です。コンプライアンス・モニターを構成するには、「セットアップ」 > 「クイック・スタート」 > 「コンプライアンス・モニター」にナビゲートし、詳細について「コンプライアンス・モニターのクイック・スタート」を参照してください。

親トピック: モニター・エージェントをデプロイするためのクイック・スタート

GIM によるソフトウェアの管理

- クライアント別の設定
  Guardium Installation Manager (GIM)「クライアント別の設定」ツールを使用して、S-TAP とその他のソフトウェア・パッケージを迅速にデプロイします。
- GIM ユーザー・インターフェース
  GIM はモジュールの自動インストール機能の提供を目的とし、各データベース・サーバーおよび Guardiumシステムごとに常駐する GIM クライアントと GIM サーバーを活用します。
- GIM コマンド行インターフェース
  データベース・サーバー上でモジュールをインストールまたはアップグレードするために、CLI を使用できます。

親トピック: Guardium Installation Manager

クライアント別の設定

Guardium Installation Manager (GIM)「クライアント別の設定」ツールを使用して、S-TAP とその他のソフトウェア・パッケージを迅速にデプロイします。

始める前に

「クライアント別の設定」ツールを使用する前に、次の事項を確認してください。

- GIM クライアントが、データベース・サーバーにインストールされ、Guardium システムに接続されていること。
- 互換性のある GIM バンドルがアップロードされ、Guardium システムにインポートされていること。

手順

1. 「管理」 > 「モジュール・インストール」 > 「クライアント別の設定」にナビゲートします。
2. 「クライアントの選択」セクションで、GIM を使用してソフトウェアをインストールまたは更新するデータベース・サーバーを選択します。表内のチェック・ボックスを使用して個々のクライアントを選択するか、「クライアント・グループを選択してください」メニューを使用してクライアントのグループを選択します。「次へ」をクリックして先に進みます。
   重要: 「クライアント別の設定」ツールを使用中に新しいクライアントを追加した場合、その新しいクライアントを表示するには、ブラウザーをリフレッシュします。
3. 「バンドルの選択」セクションで、「バンドルを選択してください」メニューを使用して、インストールまたは更新するソフトウェアを特定します。「次へ」をクリックして先に進みます。 ソフトウェア・バンドルを選択すると、「選択されたバンドルのアクション」列に、各クライアントに対して実行される次のアクションが示されます。

   インストール
   : 選択したバンドルがクライアントにインストールされます。このアクションは、クライアントへのソフトウェアの初回のインストールを示します。

   アップグレード
   : バンドルがクライアント上でアップグレードされます。このアクションは、ソフトウェアの旧バージョンがクライアントに現在インストールされていることを示します。

パラメーターの更新
: バンドルのパラメーターがクライアント上で更新されます。このアクションは、選択したソフトウェアと現在インストールされているソフトウェアが同じバージョンであることを示します。

ダウングレード
: 選択したバンドルがクライアントにインストールされます。このアクションは、選択したソフトウェアが、クライアントに現在インストールされているソフトウェアより古いことを示します。

なし (バンドルが見つかりません)
: アクションは実行されず、選択したバンドルに対してクライアントに互換性のあるアクションがないことを示します。

なし (より新しいバージョンがインストールされています)
: 選択したバンドルは、クライアントに現在インストールされているバージョンより古いため、アクションは実行されません。ソフトウェアの古いバージョンをインストールするには、目的のバージョンをインストールする前に、現在インストールされているバージョンをアンインストールしてください。

ヒント:
- バンドルの旧バージョンを表示して操作するには、「最新バージョンのみを表示」チェック・ボックスをクリアします。
- バンドル内の個々のモジュールを特定するには、「バンドルのみを表示」チェック・ボックスをクリアします。
- 選択したバンドルと互換性がないクライアントを非表示にするには、「互換性のあるクライアントのみを表示」チェック・ボックスを選択します。

重要:
- デフォルトでは、「バンドルの選択」メニューには、プラットフォームや選択したクライアントとの互換性に関係なく、アップロードされた最新のバンドル・バージョンのみが表示されます。特定のプラットフォームまたはクライアントに対して異なるバンドル・バージョンをインストールするには、「最新バージョンのみを表示」チェック・ボックスをクリアし、必要なバンドルを選択してください。
- 「クライアント別の設定」ツールを使用中に新しいバンドルをアップロードしてインポートした場合、その新しいバンドルを表示するには、ブラウザーをリフレッシュします。
- 既にバンドルのインストールのスケジュールが設定されている場合、新しいバンドルをインストールすると、既存のスケジュールが削除されます。

4. 「パラメーターの選択」セクションで、必須パラメーターとオプション・パラメーターの値を指定します。オプション・パラメーターを追加または削除するには、アイコンまたは アイコンを使用します。名前または説明でパラメーターを検索するには、 アイコンを使用します。「次へ」をクリックして先に進みます。
   重要: クライアント固有のパラメーターとして特定された場合を除き、「パラメーターの選択」セクションで指定された値は、ソフトウェアのインストール、アップグレード、または更新先のすべてのクライアントに適用されます。クライアント固有のパラメーターについては、値のフィールドが無効になり、「クライアントの構成」セクションでクライアントごとに値が定義されます。
5. 「クライアントの構成」セクションで、表を使用して、各クライアントのパラメーター値を検討し、編集します。 編集可能なパラメーターには、パラメーター値の横に アイコンが表示されます。その アイコンをクリックして、値を編集します。
6. 「インストール」をクリックして、ソフトウェアのインストールを開始します。 アイコンを使用して、インストールをスケジュールし、「OK」 をクリックして続行します。

次のタスク

「バンドルの選択」セクションを使用して、ソフトウェアのインストールをモニターします。 インストール状況が「状況」列に表示されます。インストール状況をリフレッシュするには、 アイコンを使用します。
親トピック: GIM によるソフトウェアの管理

GIM ユーザー・インターフェース

GIM はモジュールの自動インストール機能の提供を目的とし、各データベース・サーバーおよび Guardiumシステムごとに常駐する GIM クライアントと GIM サーバーを活用します。

ユーザーは、CLI を介して GIM と対話することもできます。CLI を使用した GIM によるモジュールのインストールおよびアップグレードについては、GIM コマンド行インターフェースを参照してください。

以下のタスクで Guardium Installation Manager (GIM) の GUI を使用できます。

- プロセスの モニター
- モジュール・パッケージの アップロード
- モジュールの構成、インストールまたは更新 (クライアント別)
- モジュールの構成、インストールまたは更新 (モジュール別)
- ロールバックのメカニズム

注: A-TAP が使用されている場合、GIM ベースでの S-TAP® のアップグレードまたはアンインストールを実行する前に、データベース・サーバーで最初に A-TAP を無効にする必要があります。
注: GIM はネイティブ S-TAP インストーラー (rpm、dept、bff など) を サポートしていません
注: GIM ユーティリティーを使用して特定のクライアントにモジュールを初めてインストールする場合、バンドルの形式にする必要があります。インストール済みのバンドルに属する特定モジュールの将来のアップグレードは、単一のモジュールまたはバンドルとして提供されます。

プロセスのモニター

サーバー上の GIM プロセスの状況を表示します。

監視プログラム

GIM モニター・プログラムは、Guardium® プロセスのモニターおよび モニターを主な目的としたプロセスです。具体的には、この監視プログラムは常に すべての Guardium プロセスの開始、停止、またこれらのプロセスの稼働を確認し、失敗した場合はプロセスを再始動する役割を担っています。

注: Guardium V9.0 では、Solaris 5.10/5.11 上で GIM と SUPERVISOR が SMF サービスになります。これらは inittab エントリーではなくなります。

gim/supervisor を開始および停止するには、以下を使用します。

svcadm -v enable guard_gim

svcadm -v enable guard_gsvr

svcadm -v disable guard_gim

svcadm -v disable guard_gsvr

GIM

GIM プロセスは GIM クライアント・プロセスです。このプロセスの役割は GIM サーバーへの登録、ソフトウェアの更新チェック要求の開始、新規ソフトウェアのインストール、モジュール・パラメーターの更新、モジュールのアンインストールなどです。

モジュール・パッケージの アップロード

モジュール・パッケージ・ファイル (1 つ以上のモジュールのサブパッケージを含む単一の .gim ファイル) をデータベースにロードします。

1. 「管理」 > 「インストール管理」 > 「アップロード」をクリックして、「アップロード」を開きます。
2. 「表示」をクリックして、該当パッケージ (.gim ファイル) のディスク上の場所を表示します。
3. 「アップロード」をクリックしてパッケージをアップロードします。
4. 「アップロード済みモジュールのインポート」の下にあるアップロード済みパッケージの「インポート」 アイコンをクリックして、パッケージをロードします。

モジュールの構成、インストールまたは更新 (クライアント別)

ヒント: 最新の GIM ソフトウェア管理ツールについては、クライアント別の設定を参照してください。

このオプションを使用すると、任意の数のクライアントに対して、既にロードされたパッケージから、モジュールを構成/インストールすることができます。

最も簡単で安全かつ迅速にモジュールをインストールまたはアンインストールする方法は、バンドルを使用することです。 バンドルを使用すると、従属関係と順序が自動的に解決されます。

クライアントのグループを既に作成済みの場合は、グループを使用して、指定されたアクションの対象になるクライアントを指定できます。そうでない場合は、以下の手順を使用して、クライアントのリストを選択します。

1. 「管理」 > 「インストール管理」 > 「クライアント別の設定」(レガシー) をクリックして、「クライアント検索条件」を開きます。
2. 「検索」ボタンをクリックしてフィルター検索を実行し、「クライアント」パネルを表示します。
3. 指定されたアクションの対象になるクライアントを選択します。
   - クライアント数が 20 を超える場合には、クライアントのリストは追加ページに分けられます。
     注: 「すべて選択」ボタンをクリックした場合に選択されるのは、表示されている現行ページ上のクライアントのみです。
4. 「クライアント」パネルからは、以下の 2 つのアクションを実行できます。
   - 共通パラメーターの 構成/インストール
   - モジュールの 構成/インストール
   - クライアントのリセット - 「クライアントのリセット」をクリックすると、選択したクライアントからモジュールを分離して、そのクライアントの定義を Guardium システム・データベースから削除できます。注: クライアントをリセットしても、そのデータベース・サーバーでモジュールの削除は トリガーされません。
   - このクライアントの インストール状況を表示 - この情報アイコンをクリックすると、 インストール状況パネルが開き、 クライアントのインストール状況を表示できます。このパネルは、 クライアント上のすべてのモジュール (インストール済み、または更新/アンインストールの スケジュールがされているモジュール) を表示します。このパネルから、「このモジュールを編集」アイコンを使用して各モジュールに対して個別にパラメーターを構成することができます。

モジュールの 構成、インストールまたは更新 (モジュール別)

モジュールを基本に、任意の数のクライアントにモジュールを構成および インストールできます。この場合、事前に必要なパッケージがすべてロードされている 必要があります。

1. 「管理」 > 「モジュール・インストール」 > 「モジュール別の設定」をクリックして、「モジュール検索条件」を開きます。
2. 「検索」をクリックしてフィルター検索を実行し、使用可能なすべてのモジュールとバンドルを表示する「モジュール」パネルを表示します。
3. モジュールを 1 つ以上選択し、「次へ」をクリックして「クライアント」パネルを開きます。
4. 指定したアクションの対象となるクライアントを選択します。
   注: クライアント数が 20 を超える場合、クライアントのリストは追加ページにまたがります。「すべて選択」ボタンをクリックすると、現在表示されているページ上のクライアントのみが選択されます。
5. 「クライアント」パネルからは、以下のアクションを実行できます。
   - モジュールのインストール/更新: ターゲット・クライアントを 1 つ以上選択して「次へ」をクリックし、「インストール/更」をクリックします。
   - モジュール・パラメーター構成の変更: ターゲット・クライアントを 1 つ以上選択して「次へ」をクリックし、パラメーター値を変更し、そのターゲット・クライアントを選択して「クライアントに適用」をクリックします。
   - 「クライアントのリセット」をクリックすると、選択したクライアントからモジュールを分離し、そのクライアント定義を Guardium システム・データベースから削除できます。注: クライアントをリセットしても、そのデータベース・サーバーでモジュールの削除は トリガーされません。
   - このクライアントのインストール状態を表示するには、情報アイコン をクリックして「インストール状況」パネルを開き、クライアントのインストール状況を表示します。このパネルは、クライアント上のすべてのモジュール (インストール済みまたは更新のスケジュールがされているモジュール) を表示します。このパネルから、「このモジュールを編集」アイコンを使用して各モジュールに対して個別にパラメーターを構成することができます。
   - 「診断の実行」をクリックすると、クライアントが次にアライブ・メッセージを送信したときに診断レポートが実行され、GIM イベント・リストに記録されます。

共通パラメーターの 構成/インストール

1. 「設定」 > 「ツールとビュー」 > 「パラメーター構成」をクリックします。
2. 「クライアント・モジュール・パラメーター」セクションから、パラメーターの変更対象のクライアントを選択します
3. 「クライアント・モジュール・パラメーター 」セクション内にリストされたモジュール・パラメーターから任意のパラメーターを変更します
   注: 「選択したものに適用」ボタンをクリックして、パラメーターを「共通モジュール・パラメーター」セクションに入力すると、「クライアント・モジュール・パラメーター」セクションに選択したクライアントを入力できます。

4. 選択したすべてのクライアントに、必須パラメーターの値をすべて入力後、「クライアントに適用」をクリックして、データベースに構成を保存します。 保存する前に、すべての必須フィールドに値が入力されているか、またそれらの値が事前定義された範囲内にあることを確認する検証が行われます。
5. 構成を保存した後、 「インストール/更新」をクリックして、選択したクライアントへの モジュールのインストールをスケジュールします。さらに、この「モジュール・パラメーター」のパネルから、 アンインストール、インストール/更新のキャンセル、アンインストールのキャンセル、 および現行の変更を元に戻すことができます。スケジュールの日時は、選択したクライアントの 日時に対応することに注意してください。
   注: 「クライアント用モジュール・パラメーター」セクションの下のクライアント行の前には、「Grdapi の生成」ボタンがあります。このボタンを使用すると、ユーザーがモジュールに加えた変更 (モジュールの割り当て、インストール、アンインストール、スケジュール、更新など) を反映する grdapi コマンドのリストを表示できます。これらの grdapi コマンドを提供することによって、ユーザーが変更を再現したい場合に、一連のコマンドをスクリプトとして使用し、他のクライアントに適用できるようにします。
   注: すべての書き込み可能なプロパティーの前に「プロパティー・コンテンツを開く」ボタンが表示されます。このボタンで表示されるウィンドウを使用すると、長いフィールドの編集を簡単に行うことができます。
   注: 「クライアント・モジュール・パラメーター」セクションの下のクライアント行の前には、「このクライアントのインストール状況を表示」ボタンもあります。このボタンを使用すると、モジュールの現在のインストール状況が表示されます。
   注: KTAP を BUNDLE-STAP の一部としてインストールする場合、実際の KTAP モジュールが特定のプラットフォームに見つからなくても、 KTAP の状況は INSTALLED に設定されます。ただし、 GIM-EVENTS レポートでは、KTAP モジュールが見つからない、という内容のメッセージが表示されます。
   注: データベース・サーバーにバンドルをインストールした後には、GIM-EVENTS レポートを確認する必要があります。
6. 「戻る」 をクリックして「クライアント」パネルに戻ります。

GIM における Windows S-TAP パラメーター

WINSTAP_CMD_LINE パラメーターを使って追加のインストール・オプションを指定することができます。例えば、特定のフィーチャー (Db2、Oracle、CAS、他) のインストールを制御できます。

デフォルトのコマンド行の他に何も指定されていない場合、通常のインストール・フィーチャー・セットに従って各フィーチャーがインストールされます。

以下にオプションのリストを示します。それぞれを 0 (インストールしない) または 1 (インストールする) に設定できます。

- MSSQLSharedMemory
- DB2SharedMemory
- CAS
- NamedPipes
- START: このパラメーターは、インストール後に S-TAP を開始するかどうかを制御します。
- INSTALL_DIR: ソフトウェアをどこにインストールするかを指定します。
- QUIET: Windows インストーラーに渡されるスイッチを制御します。これには何も変更を加えないでください。これはインストール問題のデバッグに使われます。
- DBALIAS: データベース・サーバー・マシンの別名です。マシンのホスト名を使用できます。サーバーにインストールされている実際のデータベースとは無関係です。
- AUTO_DISCOVERY

  システム上でデータベースを自動的にディスカバーし、そのデータベース用の検査エンジンを作成するために使用します。0=OFF、1=ON、デフォルトは 1。自動ディスカバリーを使用不可にするには 0 を使用します。

例えば、次のコマンド行オプションの場合、

```
CAS=0 NamedPipes=0
```

CAS および名前付きパイプ・サポートのインストールをスキップします。
インストール中の S-TAP が MSSQL データベースを自動的にディスカバーしないようにする場合、WINSTAP_CMD_LINE 列に `START=0` と入力し、インストール時に S-TAP が開始されないようにします。以下のとおり GIM API を使用して、単一のデータベース・サーバーに対してこのパラメーターを指定することもできます。

```
grdapi gim_update_client_params clientIP=xx.xx.xx.xx paramName=WINSTAP_CMD_LINE paramValue="START=0"
```

S-TAP 用のインストール・ディレクトリーは、存在しないか、または空である必要があります。既にファイルが格納されているディレクトリーに、S-TAP をインストールすることはできません。 64 ビット・マシンでのインストールの場合は、32 ビット・プログラム・ファイル・フォルダーを指定する必要があります (例えば、C:/program files (x86)/guardium/stap です。C:/program files/guardium/stap ではないことに注意してください)。そうでない場合、64 ビット・フォルダーへの書き込みができないため、インストールが失敗します。

インストール時に、追加の guard_tap.ini パラメーターも設定しなければならない場合があります。例として、「paramValue="START=1 !client_timeout_sec=120&use_tls=1!"」が挙げられます。

注: GuardAPI コマンドを使用する場合は、上記の例のように、WINSTAP_CMD_LINE の paramValue を引用符で囲み、各パラメーターをスペースで区切る必要があります (例: paramValue="START=1 CAS=0")。スペースを挿入しないと、後続のインストールが予期したように実行されない場合があります。

モジュールの 構成/インストール

1. 構成、インストールまたは更新の手順を次に示します。
   a. クライアント 別
      i. 「次へ」をクリックして「共通モジュール」パネルを表示します。このパネルには、選択したクライアントにインストールできる選択可能なすべての共通モジュールおよびバンドルのリストが表示されます。
      ii. 選択したクライアントに構成/インストールする モジュールまたはバンドルを選択します。
      注: モジュールまたはバンドルの状況は、そのバージョンがインストール済みバージョンかスケジュール済みバージョンのいずれかに一致する場合にのみ表示されます。
      iii. リストからモジュールまたはバンドルを選択した後に、「次へ」ボタンをクリックします。
   b. モジュール 別
      i. リストからクライアントを選択した後に、「次へ」ボタンをクリックします。
2. 選択したモジュールまたはバンドル、また、 考えられる従属関係によって、以下に示す選択タイプに該当するオプションが 表示されます。
   - バンドル
     バンドルの「次へ」をクリックすると、このバンドルのすべてのモジュールの全パラメーターを示した「モジュール・パラメーター」パネルが表示されます。「クライアント・モジュール・パラメーター」セクション内にリストされた モジュール・パラメーターから任意のパラメーターを変更します。
     注: バンドルは通常のモジュールとして扱われます。

- 必須従属関係を持たないモジュール

  必須従属関係を持たないモジュールの「次へ」をクリックすると、そのモジュールのパラメーターを表示する「モジュール・パラメーター」パネル が表示されます。 「クライアント・モジュール・パラメーター」セクション内にリストされた モジュール・パラメーターから任意のパラメーターを変更します。

- 従属関係を持つモジュール
  従属関係を持つモジュールの「次へ」をクリックすると、そのモジュールおよび従属関係を持つすべてのモジュールが 「従属モジュール」画面に表示されます。任意のモジュールの「編集」アイコンをクリックして、選択したすべてのクライアントに対して、そのモジュールのパラメーターを構成すると、「モジュール・パラメーター」パネルが表示され、モジュールのパラメーターが示されます。任意のパラメーターを変更して、「OK」 ボタンをクリックすると「従属モジュール」画面に戻ります。
  注: モジュールおよびそのモジュールのすべての従属関係の構成は、データベースに同時に保存する必要があります。 また、これらのモジュールはバンドルとしてのみインストールできます。 つまり、これらの構成されたモジュールは個別に保存、または個別にインストールをスケジュールできません。 例えば、スケジュールされたインストール中に複数のクライアントの 1 つで複数のモジュールの 1 つの処理が失敗した場合、それまでのすべての処理は ロールバックされます。
  注: 「選択したものに適用」ボタンをクリックして、パラメーターを「共通モジュール・パラメーター」セクションに入力すると、「クライアント・モジュール・パラメーター」セクションに選択したクライアントを入力できます。

3. 選択したすべてのクライアントに、必須パラメーターの値をすべて入力後、「クライアントに適用」をクリックして、データベースに構成を保存します。 保存する前に、すべての必須フィールドに値が入力されているか、またそれらの値が事前定義された範囲内にあることを確認する検証が行われます。
4. 構成を保存した後、 「インストール/更新」をクリックして、選択したクライアントへのモジュールおよびその従属関係のインストールをスケジュールします。 さらに、「従属モジュール・パラメーター」パネルから、アンインストール、 インストール/更新のキャンセル、アンインストールのキャンセル、および現在の変更を元に戻すことができます。スケジュールの日時は、選択したクライアントの 日時に対応することに注意してください。
   注: 「クライアント・モジュール・パラメーター」セクションの下のクライアント行の前にある「Grdapi の生成」ボタンを使用すると、ユーザーがモジュールに加えた変更 (モジュールの割り当て、インストール、アンインストール、スケジュール、更新など) を反映する grdapi コマンドのリストを表示できます。これらの grdapi コマンドが提供されることによって、ユーザーは 一連のコマンドをスクリプトとして必要に応じて他のクライアントに適用し、再現できます。
   注: すべての書き込み可能なプロパティーの前に「プロパティー・コンテンツを開く」ボタンが表示されます。このボタンで表示されるウィンドウを使用すると、長いフィールドの編集を簡単に行うことができます。
   注: 「クライアント・モジュール・パラメーター」セクションの下のクライアント行の前には、「このクライアントのインストール状況を表示」ボタンもあります。このボタンを使用すると、モジュールの現在のインストール状況が表示されます。
   注: K-TAP を BUNDLE-STAP の一部としてインストールする場合、実際の K-TAP モジュールが特定のプラットフォームに見つからなくても、 K-TAP の状況は INSTALLED に設定されます。ただし、 GIM-EVENTS レポートでは、K-TAP モジュールが見つからない、という内容のメッセージが表示されます。
   注: データベース・サーバーにバンドルをインストールした後には、必ず GIM-EVENTS レポートを確認してください。
   注: モジュールのアンインストール時に GIM は、選択したモジュールのみをアンインストールし、従属関係はアンインストールしません。

ロールバックのメカニズム

GIM のロールバック・メカニズムの目的は、インストール中のエラーを処理し、 モジュールをリカバリーして以前の状態に戻すことです。ロールバックのメカニズムは以下のリカバリー・シナリオをサポートします。

1. ライブ・アップグレードのリカバリー
   バンドルの場合
   - バンドルのインストールの場合、そのバンドル内でインストールに失敗したモジュールを ロールバックします。
   - `NO_ROLLBACK` とマークされたモジュール (<MODULE>_NO_ROLLBACK=1 という読み取り専用パラメーターの形式) は、失敗が発生した場合にロールバックされません。S-TAP と KTAP はこのような 2 つのモジュールで、いったん正常にインストールされると、別のモジュールで失敗が発生した場合にロールバックされません。

   バンドル以外の場合
   - スクラッチ・インストールの場合、ロールバックはスタンドアロン・モジュール の削除を伴いますが、アップグレードの場合は、以前のバージョンに戻されます。
2. ブート・タイム・インストールのリカバリー
   システムのリブート時にインストールが失敗した場合は、リカバリーを完了するために 2 回目のシステム・リブートが必要になります。リブート後も、IP-PR 状態のままになり、GIM_EVENT エントリーには、リカバリー・プロセスを完了するために 2 回目のリブートが必要であることが示されます。2 回目のリブート後に、モジュール/バンドルの状態は "FAILED" 状態を示します。
   注: 状態が 'IP-PR' の場合、 データベース・サーバーのブート方法は OS によって異なります (以下の方法以外でシステムをリブートした場合は、 保留中のモジュールは保留状態のままになります)

   ```
   Linux   : shutdown -r
   SuSe    : reboot
   HP      : shutdown -r
   Solaris : shutdown -i [6|0] (注: 「0」を使用できるのは、端末サーバーから shutdown を実行する場合のみです。)
   AIX     : reboot
   Tru64   : reboot
   ```

   注: また、リブートの前に A-TAP インスタンスを使用不可/非活動化する必要があります。

GIM クライアントに対応する GIM サーバーの変更

1 つ以上の GIM クライアントを管理する GIM サーバーを変更することができます。GIM サーバーの変更により、ご使用の GIM サーバー間で負荷のバランスを取ったり、GIM パッケージを容易に配布したりすることができます。GIM クライアントのグループを別の GIM サーバーに再割り当てするには、以下のステップを実行します。

1. 「管理」 > 「インストール管理」 > 「モジュール別の設定」をクリックして、GIMクライアント用の GIM サーバーを変更します。
2. 再割り当ての対象とするクライアントにインストールされている GIM バンドルを選択します。「次へ」をクリックします。
3. 変更するクライアントを選択してください。「すべて選択」をクリックすることも、クライアントを個々に選択することもできます。「次へ」をクリックします。
4. 「すべて選択」をクリックします。
5. GIM_URL パラメーターで、選択した GIM クライアントを再割り当てする GIM サーバー (Guardium システム) のホスト名または IP アドレスを入力します。「選択したものに適用」をクリックします。
6. 同じパネルで、「クライアントに適用」をクリックした後、「インストール/更新」をクリックし、更新をスケジュールします。

更新が処理されると、GIM クライアントは新規 GIM サーバーによって管理されます。
親トピック: GIM によるソフトウェアの管理

GIM コマンド行インターフェース

データベース・サーバー上でモジュールをインストールまたはアップグレードするために、CLI を使用できます。

以下は、一般的なシナリオの一部のみ を示す例です。サポートされるすべての CLI コマンドの完全なリストおよび詳細については、「GuardAPI GIM 関数」を参照してください。

- モジュール・パッケージ のロード
- バンドルを 使用したアップグレードまたはスクラッチ・インストール
- モジュール/バンドルの アンインストール
- インストール状況
- モジュール状態の 照会

モジュール・パッケージ のロード

モジュールを DB サーバーにインストールできるようにするには、まずそれらのモジュールを中央マネージャー GIM データベースにロードする必要があります。中央マネージャーがアーキテクチャーの一部ではない場合、パッケージを各 Guardium システムにロードする必要があります。 データベースにロードされたパッケージを取得するには、GIM UI の「パッケージのロード (Load package)」オプションを使用します。

バンドルを 使用したアップグレードまたはスクラッチ・インストール

注: スクラッチ・インストールは、古い (以前の GIM) S-TAP® がデータベース・サーバーにインストールされているケースも指します。
バンドルとは、 グループ化してまとめられたモジュールのリストです。これによりインストール・プロセスが 容易になります。モジュールのインストールまたはアップグレードには、常にバンドルを使用してください。

1. 以下のとおり、登録済みクライアント (つまり、GIM サーバーに登録済みの GIM クライアントがインストールされているデータベース・サーバー) のリストを取得します。

```
grdapi gim_list_registered_clients
ID=0
####### ENTRY 0 #######
CLIENT_ID:          1
IP:                 192.168.2.204
OS:                 HP-UX
OS_RELEASE:         B.11.00
OS_VENDOR:          hp
OS_VENDOR_VERSION:  B.11.00
OS_BITS:            64
PROCESSOR           9000
####### ENTRY 1 #######
CLIENT_ID:          2
IP:                 192.168.2.210
OS:                 Linux
OS_RELEASE:         2.6.16.54-0.2.5-smp
OS_VENDOR:          suse
OS_VENDOR_VERSION:  10.1
OS_BITS:            64
PROCESSOR           x86_64
```

2. 使用可能な最新のバンドルを 特定クライアントに割り当てます (インストールを準備するもので、実際にそのクライアントへのインストールを要求 するものではありません)

```
grdapi gim_assign_latest_bundle_or_module_to_client  clientIP=198.168.2.210 moduleName=BUNDLE-STAP
```

注: 特定のバンドルまたは特定のモジュールをクライアントに割り当てるには、ステップ 2 を以下の手順に置き換えてください。

```
gim_get_available_modules clientIP="client ip"
gim_assign_bundle_or_module_to_client_by_version clientIP="client ip" modulesName="Bundle/Module name"
moduleVersion="Bundle/Module version"
```

3. インストールをスケジュールします。

```
grdapi gim_schedule_install clientIP=192.168.2.210 date=now
```

注: 複数のクライアントをインストールする場合は、ステップ 2 からステップ 3 を繰り返してください。
注: フレキシブルな GIM スケジューリングを行う場合は、以下を使用します: now + [1-9][0-9]* minute | hour | day | week | month。例: now + 1 day、now + 3 minutes

GIM スケジューリング

すべての時刻が、Guardium のシステム時刻を基にしています。ここで使用する「now」とは、Guardium システムで指定された現在時刻のことです。 例えば「now +30 minute」となっている場合、Guardium の現在のシステム時刻から 30 分先の時刻になります。これは、インストール状況を調べる際に、クライアント (「管理」 > 「モジュール・インストール」 > 「クライアント別の設定」(レガシー) など) の横に表示されている小さな「i」をクリックすると確認できます。データベース・サーバー上の時刻が、インストール用に指定された Guardium システムの時刻を過ぎた場合、インストールが開始されます。

例 1: (a) Guardium のシステム時刻からマイナス 1 時間に設定されているクライアント、(b) Guardium のシステム時刻に設定されているクライアント、(c) Guardium のシステム時刻からプラス 1 時間に設定されているクライアント、という 3 つのクライアントがあるとします。

この状態で、GIM による S-TAP のインストールを「now +30 minute」に設定します。

Guardium システム (a) は、インストール用に設定された時刻よりも既に 30 分先であるため、即時にインストールを開始します。

Guardium システム (b) は、30 分後にインストールを開始します。

Guardium システム (c) は、システム (b) の 1 時間後にインストールを開始します。

例 2: 例 1 と同じ設定で、今度は「now」を指定します。

この場合、すべてのクライアントで、IP に対するインストールの状況が即時に変更されます。

モジュール/バンドルのアンインストール

```
grdapi gim_uninstall_module clientIP=192.168.2.210 module=BUNDLE-STAP date=now
```

`date=now` と指定するか、`YYYY-MM-DD HH:mm` という形式を使用します。アンインストールは、次に GIM クライアントが更新の有無をチェックしたとき (GIM_INTERVAL) に行われます。

インストール状況

クライアントが 送信した最新状況に関する追加情報は、 次のコマンドを実行して取得できます (状況メッセージは GIM_EVENTS 表内の項目として表示され、そのメッセージからレポートを生成できます)

汎用的な 状況メッセージは次の CLI コマンドで取得できます。

```
grdapi gim_get_client_last_event clientIP="client ip"
grdapi gim_get_client_last_event clientIP=winx64
grdapi gim_get_client_last_event clientIP=9.70.144.73
```

このコマンドの出力の例を以下に示します。

```
ID=0
OK
BUNDLE-STAP-8.0_r2609_1 INSTALLED
STAP-UTILS-8.0_r2609_1 INSTALLED
COMPONENTS-8.0_r2609_1 INSTALLED
KTAP-8.0_r2609_1 INSTALLED
STAP-8.0_r2609_1 INSTALLED
TEE-8.0_r2609_1 INSTALLED
ATAP-8.0_r2609_1 INSTALLED
```

モジュール状態の 照会

クライアントごとに インストールされたモジュールの状態を照会するには、次の CLI コマンドを実行してください。

```
grdapi gim_list_client_modules clientIP=”client ip”
```

次のような状態 があります。

INSTALLED
: モジュールはインストール済み。

PENDING-INSTALL
: モジュールのインストールのスケジュール設定を保留中

PENDING-UNINSTALL
: モジュールのアンインストールのスケジュール設定を保留中

PENDING-UPDATE
: モジュールのアップデートのスケジュール設定を保留中

IP
: モジュールのインストールが進行中

FAILED
: モジュールの最終操作が失敗しました

IP-PR
: モジュールのインストール・プロセスを完了するには、クライアントをリブートしてください。リブートする前に、すべての A-TAP インスタンスを非アクティブ化してください。データベース・サーバーのリブート方法は OS によって異なります (以下の方法以外でシステムをリブートした場合は、 保留中のモジュールは保留状態のままになります)

  - AIX: reboot
  - Linux : shutdown -r
  - SuSe: reboot
  - HP-UX: shutdown -r
  - Solaris : shutdown -i [6|0] (注: 「0」を使用できるのは、端末サーバーから shutdown を実行する場合のみです。)
  - Tru64: reboot

出力例

```
ID=0
####### ENTRY 0 #######
MODULE_ID:          11
NAME:               INIT
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 1 #######
MODULE_ID:          -1
NAME:               COMMON
INSTALLED_VERSION   8.0_r0_1
SCHEDULED_VERSION   8.0_r0_1
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 2 #######
```

```
MODULE_ID:          12
NAME:               UTILS
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 3 #######
MODULE_ID:          13
NAME:               SUPERVISOR
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 4 #######
MODULE_ID:          14
NAME:               GIM
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 5 #######
MODULE_ID:          15
NAME:               BUNDLE-GIM
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
STATE:              INSTALLED
IS_SCHEDULED:       N
```

K-TAP の使用可能化

インストール・プロセスの実行中に、K-TAP が正しくロードを行えない場合 (おそらく、ハードウェアまたはソフトウェアの非互換性が原因)、デフォルトの収集メカニズムとして Tee がインストールされます。互換性の問題が解決した後に再び K-TAP に切り替えるには、以下の手順を行います。

1. S-TAP を無効にします。詳しくは、『UNIX S-TAP の停止』を参照してください。
2. guard_tap.ini を編集し、*ktap_installed* を 1 に、*tee_installed* を 0 に変更します。
3. guard_ktap_loader install コマンドを実行します。

   例:
   ```
   /usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader install
   ```
4. guard_ktap_loader start コマンドを実行します。

   ```
   example: /usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader start
   ```
5. S-TAP を再度有効にします。詳しくは、『UNIX S-TAP の再始動』を参照してください。

親トピック: GIM によるソフトウェアの管理

GIM サーバーの割り振り

事前インストールされた非アクティブな (どのコレクターにも接続されていない) GIM エージェントにリモートで接続し、そのエージェントがデータベース・サーバーにアクセスすることなく何らかのコレクターに接続するようにします。

概要

以下のプロセス (GIM オートディスカバリーとも呼ばれます) により、事前インストールされた非アクティブな GIM エージェントにリモートで接続し、そのエージェントがデータベース・サーバーにアクセスせずにコレクターに接続するようにすることができます。

1. 非アクティブ GIM クライアントがリスナー・モードで実行され、コレクターからの接続を待機しています。
2. コレクターのグラフィック・ユーザー・インターフェース (GUI) または GuardAPI から、コレクターの IP アドレスを非アクティブな GIM クライアントに送信することができます。
3. 非アクティブな GIM クライアントは、コレクターの IP アドレスを受け入れて、その IP アドレスに接続します。

コレクターの IP アドレス (--sqlguardip) が指定されずに GIM がインストールされている場合、GIM はサーバー・モードで実行されます。GIM エージェントがサーバー・モードで実行されている場合、GIM は、証明書認証および共有パスワード検査を保持する検証済みコレクターからのみ SSL を介してメッセージを受け入れます。30 回以上連続して認証が失敗すると、GIM エージェントは要求の listen を停止し、サーバー・モードで実行されます。このアクションにより、サービス妨害 (DoS) 攻撃が回避されます。

ユーザーは、独自の証明書、共有パスワード、およびポート番号を定義できます。他の証明書を使用するには、証明書と鍵の絶対パス名をインストール・パラメーター (--key_file および --cert_file) に指定します。 GuardAPI コマンド store certificate gim を使用して、証明書をコレクター鍵ストアにロードします。

デフォルト以外の共有パスワードを設定するには、GuardAPI コマンド grdapi gim_set_global_param paramName=gim_listener_default_shared_secret paramValue=<password> を使用します。フォーマットは文字列でなければなりません。共有パスワードは、データベース・サーバーとコレクターで同一でなければなりません。

注: 暗号化されていない共有パスワードをコマンド行で指定しないでください。

デフォルト以外のポートを使用するには、インストール・パラメーター --listener_port にポートを指定します。 「GIM グローバル・パラメーター (GIM Global Parameters)」で、GIM グローバル・パラメーター gim_listener_default_port に新規ポートを設定します。

注: ファイアウォールでデフォルト・ポートまたはユーザー定義ポートを有効化する必要があります。

パラメーター

次のリストは、GIM インストール・パラメーターを説明したものです。

- --sqlguardip - GIM クライアントの接続先のコレクターの IP アドレスまたはホスト名を設定します。これが指定されていない場合、GIM クライアントは「リスナー・モード」で動作します。
- --ca_file - 認証局 PEM ファイルへの完全ファイル名パス。
- --key_file - 秘密鍵 PEM ファイルへの完全ファイル名パス。
- --cert_file - 証明書 PEM ファイルへの完全ファイル名パス。
- --shared_secret - コレクターを検査するための共有パスワードを指定します。
- --listener_port - デフォルトとは異なるポート番号を指定します。
- --no_listener - --sqlguardip が指定されていない場合でも、GIM が「リスナー・モード」で実行されないようにします。

以下の操作を実行しようとするとします。

- パラメーターの更新
- モジュールのインストール
- データベース・サーバーでの GIM の直接アンインストール

GIM エージェントはサーバー・モードを終了して、要求を処理します。 GIM クライアントは、指定されたコレクターに接続できない場合、サーバー・モードに戻ります。 GIM エージェントが有効なコレクターの IP アドレスまたはホスト名に割り当てられた後は、サーバー・モードで再実行されるように GIM サーバーを設定できません。新規の GIM エージェント・サーバー・モード・パラメーターはすべて READ-ONLY と表示されます。
注: 以下のパラメーターは、ファイル・システムに存在している必要があります。存在しない場合、インストールは失敗します。

- ca_file
- key_file
- cert_file

追加のコマンド行パラメーター

GIM の GIM インストーラーと統合インストーラーには、以下に挙げる追加のコマンド行パラメーターがあります。

--allow_ip_hostname_combo <0|1>

パラメーター名 : GIM_ALLOW_IP_HOST_COMBO

パラメーター値: 1 - 有効、0 - 無効

パラメーターのデフォルト値: 0

パラメーターの説明 : このパラメーターが有効に設定され、GIM_CLIENT_IP が DB サーバーのホスト名と異なる場合、GIM_CLIENTS.GIM_CLIENT_NAME は、`hostname`_<GIM_CLIENT_IP> の組み合わせである値を使用して設定されます。

GIM_CLIENT_IP が IP アドレスを使用して設定され、GIM_ALLOW_IP_HOST_COMBO が有効に設定されている場合、GIM のホスト名は <hostname>_<GIM_CLIENT_IP> の組み合わせになります。 これにより、「共通」のホスト名を持つデータベース・サーバー間で GIM クライアントの固有性が確保されます。

制限事項: 「共通」のホスト名を使用して GIM_CLIENT_IP を設定することはできません。 「共通」ホスト名を使用した GIM_CLIENT_IP の設定は、重複 ID で登録する試みとみなされます。

サーバー・モード・グローバル・パラメーターでの GIM の設定

以下の GuardAPI コマンドを使用して、サーバー・モード GIM パラメーターを設定できます。

```
grdapi gim_set_global_param
paramName=gim_listener_default_shared_secret
paramValue=<password>
```

この値は暗号化されてデータベースに保管されます。GIM エージェントをデータベース・サーバーにインストールする場合、この値は、共有パスワードとしての暗号化されていない値と同一でなければなりません。

新規のデフォルト・サーバー・モード GIM ポートを設定するには、以下の GuardAPI コマンドを使用します。

```
grdapi gim_set_global_param paramName=gim_listener_default_port paramValue=<port number>
```

GIM エージェントをデータベース・サーバーにインストールする場合、この値は共有パスワードの暗号化されていない値と同一でなければなりません。

注: 異なるポートまたは共有パスワードを使用する場合、コレクター IP またはコレクター・ホスト名をサーバー・モード GIM エージェントに接続するたびに、共有パスワードまたはポートを指定する必要があります。

GIM リモート・アクティベーション

事前インストールされた GIM エージェントにリモートで接続し、GIM リモート・アクティベーションを使用してデータベース・サーバーにアクセスせずにそのエージェントをコレクターに接続します。

1. 「管理」 > 「モジュール・インストール」 > 「GIM リモート・アクティベーション (GIM Remote Activation)」をクリックします。
2. GIM がリスナー・モードで実行されている IP アドレスまたはホスト名を「IP / ホスト名」フィールドに入力します。それ以外の方法では、下にあるリストからサーバー・グループを選択します。
3. GIM リスナー・ポートが GIM グローバル設定と異なる場合、「GIM リスナー・ポート」に数値を入力します。デフォルト値は 8445 です。
4. GIM リスナー・パスワードが GIM グローバル設定と異なる場合、「GIM リスナー・パスワード」フィールドに共有パスワードを入力します。
5. 「実行」をクリックして情報を処理するか、「リセット」をクリックして、情報をクリアします。

注: IP アドレスまたはホスト名を入力するか、サーバー・グループを選択する必要があります。ただし、GIM リスナー・ポートおよび GIM リスナー・パスワードはオプションです。 GIM クライアントをリスナー・モードでインストールすると、共有パスワードおよび証明書の設定は、GIM クライアントを再インストールしない限り変更できません。

注: 「GIM リモート・アクティベーション」の「コレクター IP」フィールドがブランクの場合、コレクターのホスト名がサーバーに送信されます。 IP を指定すると、それが代わりに送信されます。

GIM オートディスカバリー・プロセスの作成

オートディスカバリー・プロセスがスキャンするホストとポートを指定します。

1. 「ディスカバー」 > 「データベース・ディスカバリー」 > 「GIM オートディスカバリーの構成」をクリックし、オートディスカバリーを構成します。
2. 「新規」をクリックして新規プロセスを作成し、「オートディスカバリー・プロセス・ビルダー」を開きます。
3. Guardium® システム上で固有の「プロセス名」を入力します。
4. スキャン・ジョブの完了直後にプローブ・ジョブを実行するには、「スキャン後にプローブを実行」チェック・ボックスにチェック・マークを付けます。
5. スキャンするホストまたはサブネットごとに、ホストとポートを入力して「スキャンの追加」をクリックします。スキャンを追加するたびに、スキャンがタスク・リストに追加されます。
   注:
   - ワイルドカード文字が使用可能です。例えば、192.168.2 で始まるアドレスをすべて選択するには、「192.168.2.*」と指定します。
   - 一定範囲のポートを指定するには、その範囲内の最初のポート番号と最後のポート番号の間にダッシュを入れます。例: 4100-4102。
   - スキャンを追加した後、ホストまたはポートを上書き入力で変更します。 「適用」をクリックして、変更を保存します。
   - デュアル・スタック構成がある場合は、IPV4 アドレスと IPV6 アドレスの両方に対してスキャンを設定する必要があります。
   - スキャンを削除するには、そのスキャンの「このタスクを削除」アイコンをクリックします。タスクに、それに従属するスキャン結果がある場合は、そのスキャンは削除できません。
6. スキャンの追加が完了したら「適用」をクリックし、ジョブを実行するか、ジョブを後で実行するようスケジュールします。スケジュールを定義する際に支援が必要な場合は、『スケジューリング』を参照してください。

GIM グローバル・パラメーター

ユーザー独自の共有パスワードまたは GIM リスナー・ポートをユーザー・インターフェースを介して定義します。

1. 「GIM グローバル・パラメーター (GIM Global Parameters)」を開くには、「管理」 > 「モジュール・インストール」 > 「GIM グローバル・パラメーター (GIM Global Parameters)」をクリックします。
2. gim_listener_default_shared_secret を選択して共有パスワードを設定するか、gim_listener_default_port を選択してポートを設定します。
3. アイコンをクリックして、選択したパラメーターを編集します。
4. 値を変更し、「保存」をクリックしてパラメーターを変更するか、「閉じる」をクリックしてページに戻ります。

親トピック: Guardium Installation Manager

Windows サーバーへの GIM クライアントのインストール

対話式インストーラーまたはサイレント・インストールのいずれかを使用して、GIM クライアントを Windows にインストールする方法を説明します。GIM クライアントのアンインストールについても説明します。

このタスクについて

GIM クライアントには現在、ご使用の GIM クライアントのバージョンに基づいて、2 つのタイプのインストーラーがあります。 バージョン 10.1.2 以前は、r89755 までのビルド番号を使用しますが、バージョン 10.1.3 以降は、10.2.30.5 からのビルド番号を使用します。この説明を参照するときは、ご使用の GIM クライアントのバージョンとビルド番号に注意してください。

親トピック: Guardium Installation Manager

対話式インストーラーを使用した GIM クライアントのインストール: GIM クライアント・バージョン 10.1.2 以前

GIM クライアントを各データベース・サーバーにインストールする際に役立つウィザードが用意されています。

手順

1. GIM クライアント・インストーラーをデータベース・サーバーの任意のフォルダーに配置します。
2. setup.exe ファイルを実行して、GIM クライアントをインストールするウィザードを開始します。 setup.exe ファイルは Windows_GimClient フォルダーにあります。
3. インストール・ウィザードの質問に答えます。

次のタスク

インストールの結果は、ログ・ファイル c:¥guardiumstaplog.txt で確認できます。

対話式インストーラーを使用した GIM クライアントのインストール: GIM クライアント・バージョン 10.1.3 以降

GIM クライアントを各データベース・サーバーにインストールする際に役立つウィザードが用意されています。

手順

1. GIM クライアント・インストーラーをデータベース・サーバーの任意のフォルダーに配置します。
2. setup.exe ファイルを実行して、GIM クライアントをインストールするウィザードを開始します。 setup.exe ファイルは GIM-Installer-10.2* フォルダーにあります。
3. インストール・ウィザードの質問に答えます。

次のタスク

インストールの結果は、ログ・ファイル C:¥IBM Windows GIM.ctl で確認できます。

サイレント・インストールを使用した GIM クライアントのインストール: GIM クライアント・バージョン 10.1.2 以前

ウィザードを使用する代わりにコマンド行から GIM クライアントをインストールすることもできます。

このタスクについて

手順

1. GIM クライアント・インストーラーをデータベース・サーバーの任意のフォルダーに配置します。
2. コマンド・プロンプトを開き、インストーラーを配置したフォルダーの下にある Windows_GimClient フォルダーにナビゲートします。
3. 次のコマンドを改行を入れずに入力します。`setup.exe /s /z" --host=g10.guardium.com --path=c:¥¥program files (x86)¥¥guardium¥¥GIM --perl=c:¥¥perl¥¥bin --localip=192.168.1.100"`。すべてのスペースおよび引用符を、この例に示すとおりに含めます。スペースを削除または追加すると、インストーラーが失敗します。 --perl= パラメーターは、このコンピューター内で Perl がインストールされている場所を示します。このパラメーターはオプションです。 これを指定しない場合、インストーラーは Perl インスタンスをインストールします。
   重要:
   - クライアントを GIM リスナー・モードでインストールするには、--host パラメーターを省略します。 リスナー・モードは、GIM クライアントを Guardium システムからのリモート登録に使用できるようにします。リスナーとしてインストールする方法の例: setup.exe /s /z"--path=c:¥program files (x86)¥guardium¥GIM --host=GIM_HOST"。詳しくは、GIM リモート・アクティベーションおよび GIM オートディスカバリー・プロセスの作成を参照してください。
   - データベース・サーバーを複製して大量のデプロイメントを設定する場合は、--auto_assign_ip=1 を使用してデータベース・サーバーの有効な IP アドレスのいずれかからランダム IP アドレスを割り振ります。GIM クライアントのインストール時に auto_assign_ip と localip の両方を指定しないでください。「管理」 > 「モジュール・インストール」 > 「クライアント別の設定」または「モジュール別の設定」を使用して GIM_AUTO_SET_CLIENT_IP パラメーターを更新する場合は、新規設定を有効にするために GIM クライアント・サービスを再始動する必要があります。

次のタスク

インストールの結果は、ログ・ファイル c:¥guardiumstaplog.txt で確認できます。

サイレント・インストールを使用した GIM クライアントのインストール: GIM クライアント・バージョン 10.1.3 以降

ウィザードを使用する代わりにコマンド行から GIM クライアントをインストールすることもできます。

手順

1. GIM クライアント・インストーラーをデータベース・サーバーの任意のフォルダーに配置します。
2. コマンド・プロンプトを開き、インストーラーを配置したフォルダーの下にある GIM_Installer* フォルダーにナビゲートします。
3. 次のコマンドを改行を入れずに入力します。`setup.exe -UNATTENDED -INSTALLPATH "c:¥Program Files(x86)¥Guardium Installation Manager" -LOCALIP 10.9.876.543`
   重要:
   -
     - UNATTENDED パラメーターと LOCALIP パラメーターは必須です。APPLIANCE はオプションで、指定しない場合は、リスナー・モードがトリガーされます。パラメーター AUTO_ASSIGN_IP を使用する場合、LOCALIP は不要です。
     - クライアントを GIM リスナー・モードでインストールするには、-APPLIANCE パラメーターを省略します。リスナー・モードは、GIM クライアントを Guardium システムからリモート登録できるようにします。リスナーとしてインストールする方法の例: setup.exe -UNATTENDED -INSTALLPATH C:¥program files (x86)¥guardium¥GIM -LOCALIP 10.9.876.543。詳しくは、『GIM リモート・アクティベーション』と『GIM オートディスカバリー・プロセスの作成』を参照してください。
     - データベース・サーバーを複製して大量のデプロイメントを設定するときは、--auto_assign_ip=1 を使用してデータベース・サーバーの有効な IP アドレスのいずれかからランダム IP アドレスを割り振ります。GIM クライアントのインストール時に auto_assign_ip と localip の両方を指定しないでください。「管理」 > 「モジュール・インストール」 > 「クライアント別の設定」または「モジュール別の設定」を使用して GIM_AUTO_SET_CLIENT_IP パラメーターを更新する場合は、新規設定を有効にするために GIM クライアント・サービスを再始動する必要があります。
   - **Windows GIM コマンド行インストールのリファレンス**

すべての .NET インストーラーに適用可能なパラメーター

パラメーター	説明
-UNATTENDED	サイレント・インストールを実行します 値は不要です。
-UNINSTALL	アンインストールします。値は不要です。
-INSTALLPATH	これはインストール・ディレクトリーです。デフォルトのインストール・パスは「C:¥Program Files (x86)¥Guardium¥Guardium Installation Manager」です。
-CUSTOMER	カスタマー名を変更する場合に使用します。
-COMPANY	会社名を変更する場合に使用します。
-SERVICEUSER	サービスを実行するユーザーを指定する場合に使用します。
-SERVICEPASSWORD	ユーザーのパスワードを指定します。

GIM .NET インストーラーに固有のパラメーター

パラメーター	説明
-APPLIANCE	GIM が接続するアプライアンスのアドレスを設定するために使用します。このパラメーターを指定しないと、リスナー・モードを使用して GIM がインストールされます。

パラメーター	説明
-LOCALIP	これは、GIM のインストール先サーバーの IP です。
-KEY_FILE	鍵ファイルを非デフォルト・ファイルに設定するために使用します。
-CERT_FILE	証明書ファイルを非デフォルト・ファイルに設定するために使用します。
-CA_FILE	CA ファイルを非デフォルト・ファイルに設定するために使用します。
-SHARED_SECRET	-APPLIANCE パラメーターを使用して共有秘密鍵が指定されない場合の、アプライアンスへの登録用の共有秘密鍵を設定するために使用します。
-LISTENER_PORT	-APPLIANCE パラメーターを使用しない場合、アプライアンスへの登録用のリスナー・ポートを設定します。デフォルト値は 8445 です。
-AUTO_ASSIGN_IP	値を 1 に設定するときは、ローカル IP が自動的に割り当てられるため、-LOCALIP を使用して指定しないでください。デフォルト値は 0 です。

次のタスク

インストールの結果は、ログ・ファイル C:¥IBM Windows GIM.ctl で確認できます。

GIM クライアントのアンインストール: GIM クライアント・バージョン 10.1.2 以前

手順

1. コマンド・プロンプトを開き、クライアントをインストールしたフォルダーの下にある Windows_GimClient* フォルダーにナビゲートします。
2. 次のコマンドを入力します。 InstallShield に対して、次を使用します。

```
setup.exe /s /z"--host=g10.guardium.com --remove=true"
```

--host= パラメーターはオプションです。

GIM クライアントのアンインストール: GIM クライアント・バージョン 10.1.3 以降

手順

1. コマンド・プロンプトを開き、クライアントをインストールしたフォルダーの下にある GIM_Installer* フォルダーにナビゲートします。
2. 次のコマンドを入力します。

```
setup.exe -UNINSTALL
```

UNIX サーバーへの GIM クライアントのインストール

このコマンドを使用して、GIM クライアントを各データベース・サーバーにインストールします。

このタスクについて

Guardium 9.1 からは、GIM クライアントを Solaris スレーブ・ゾーンや AIX ワークロード・パーティション (WPAR) にインストールして使用することができます。これにより、GIM クライアントを使用して、 S-TAP をスレーブ・ゾーンや WPAR にインストールすることができます。S-TAP をスレーブ・ゾーンまたは WPAR にインストールする際には、ktap_enabled パラメーターの設定に関係なく、K-TAP は無効になっています。 GIM クライアントを使用して、CAS (構成監査システム) エージェントをスレーブ・ゾーンや WPAR にインストールすることもできます。スレーブ・ゾーンや WPAR にディスカバリー・バンドルをインストールすることはできません。グローバル・ゾーンで稼働するディスカバリー・エージェントは、他のゾーンから情報を収集できます。GIM クライアントを Solaris スレーブ・ゾーンまたは AIX ワークロード・パーティションにインストールするプロセスは、マスター・ゾーンにインストールするプロセスと同じです。インストールにかかる時間は、マスター・ゾーンへのインストールよりも数秒長くなる場合があります。マスター・ゾーンとスレーブ・ゾーンがある Solaris システムに GIM クライアントをインストールする場合、クライアントをマスター・ゾーンとスレーブ・ゾーンで同じロケーションにインストールする必要があります。このロケーションは共用ディレクトリーにすることはできません。

Solaris では、各スレーブ・ゾーン内の GIM クライアントと監視プログラム は、マスター・ゾーンで実行される GIM 監視プログラムのプロセスによって制御されます。マスター・ゾーンの監視プログラムのプロセスがシャットダウンされると、スレーブ・ゾーンの GIM プロセスもすべてシャットダウンされます。

注: GIM には 300 MB 以上のディスク・スペースが必要ですが、FAM モジュールもインストールする場合は 700 MB 以上必要です。

手順

1. GIM クライアント・インストーラーをデータベース・サーバーの任意のフォルダーに配置します。
2. インストーラーを次のように実行します。`./<installer_name> [-- --dir <install_dir> <--sqlguardip> <g-machine ip> --tapip <db server ip address> --perl <perl dir> -q]`
   重要:
   - クライアントを GIM リスナー・モードでインストールするには、--sqlguardip パラメーターを省略します。 リスナー・モードは、GIM クライアントを Guardium システムからのリモート登録に使用できるようにします。詳しくは、GIM リモート・アクティベーション および GIM オートディスカバリー・プロセスの作成を参照してください。
   - データベース・サーバーを複製して大量のデプロイメントを設定する場合は、--auto_set_gim_tapip を使用してデータベース・サーバーの有効な IP アドレスのいずれかからランダム IP アドレスを割り振ります。GIM クライアントのインストール時に auto_set_gim_tapip と tapip の両方を指定しないでください。GIM クライアントのインストール後に、「管理」 > 「モジュール・インストール」 > 「クライアント別の設定」または「モジュール別の設定」を使用して GIM_AUTO_SET_CLIENT_IP パラメーターを更新してください。

3. Red Hat Linux バージョン 6 以降では、次のコマンドを実行して、各ファイルが追加されたことを確認します。

```
ls -la /etc/init/gim*
ls -la /etc/gsvr*
```

Solaris バージョン 10 以降では、次のコマンドを実行します。

```
ls /lib/svc/method/guard_g*
```

その他のすべてのプラットフォームでは、次のコマンドを実行して、以下の新しい項目が /etc/inittab に追加されたことを確認します。

```
gim:2345:respawn:<Perl ディレクトリー>/perl <モジュール・インストール・ディレクトリー>/GIM/<バージョン>/gim_client.pl

gsvr:2345:respawn:<モジュール・インストール・ディレクトリー>/perl<モジュール・インストール・ディレクトリー>/SUPERVISOR/<バージョン
>/guard_supervisor
```

ここで、モジュール・インストール・ディレクトリー は、すべての GIM モジュールのインストール先のディレクトリーで、例えば /usr/local/guardium/modules などです。

4. 次のコマンドを入力して、GIM クライアント、 SUPERVISOR プロセス、および各モジュールが実行されていることを確認します。

```
ps -afe | grep modules
```

5. Guardium システムにログインして、プロセス・モニター状況を確認します。

次のタスク

親トピック: Guardium Installation Manager

GIM クライアントのアンインストール

手順

1. 次のコマンドを実行します。<GIM installation directory>/GIM/current/uninstall.pl
2. <GIM installation directory> が削除されていることを確認します。

GIM クライアントのアップグレード

GIM を使用して GIM クライアントを新しいバージョンにアップグレードできます。

手順

1. 使用可能な最新の BUNDLE-GIM.gim ファイルを Guardium システムにアップロードします。
2. GIM GUI を使用して、新しい BUNDLE-GIM.gim ファイルのインストールをスケジュールします。
3. 「i」アイコンをクリックし、「リフレッシュ」を押して、インストール・プロセスをモニターします。インストールが正常に完了すると、「INSTALLED」状況が表示されます。

親トピック: Guardium Installation Manager

GIM でのグループの使用

グループを使用することによって、一部の GIM タスクを実行しやすくすることができます。

始める前に

このタスクについて

GIM クライアントのグループを作成し、そのグループを使用して更新を管理対象サーバーに展開することができます。

手順

1. 「設定」 > 「ツールとビュー」 > 「グループ・ビルダー」をクリックします。グループ・ビルダーで、新しいグループを作成します。「グループ・タイプの記述」で、「クライアントのホスト名」を選択します。 新しいグループが、既存グループのリストに追加されます。
2. 「既存グループの変更」リストでその新しいグループを選択し、グループにメンバーを追加します。メンバーを手動で追加するか、または照会からリストにメンバーを追加することもできます。 照会からリストにメンバーを追加する場合は、「照会から取り込み」をクリックして、以下の必要な情報に注意してください。
    a. 「照会」では、「GIM」で始まるレポート名を選択します。
    b. 「列からメンバーをフェッチ」では、「GIM クライアント名」を選択します。
    c. 各「入力してください (Like)」フィールドには、マッチングする値を入力します。このフィールドをクライアントの識別に使用しない場合は、「%」を入力します。
    d. グループを保存して、照会を実行するか、照会のスケジュールを設定します。

タスクの結果

そのグループを「管理」 > 「モジュール・インストール」 > 「クライアント別の設定」画面で使用して、個々のクライアントで作業する代わりに、このクライアント・セットをグループとして作業に使用することができます。

親トピック: Guardium Installation Manager

GIM を使用した K-TAP モジュールのコピー

Linux データベース・サーバー用のカスタム K-TAP モジュールを作成する場合、GIM を使用して、そのモジュールを他の Linux データベース・サーバーにコピーできます。

始める前に

カスタム K-TAP モジュールは、現行カーネル用に事前作成された K-TAP がない Linux サーバー上に S-TAP をインストールするときに作成されます。カスタム K-TAP モジュールは、kernel-devel パッケージがインストールされている場合にのみ作成されます。S-TAP バンドルをインストールするときは、GIM UI を使用して、GIM パラメーター STAP_UPLOAD_FEATURE の値を 1 に設定してください。この設定は、カスタム K-TAP モジュールが作成された後、Guardium システムにそのモジュールをアップロードし、次に、カスタム S-TAP バンドルを自動的に作成するよう GIM クライアントに指示します。

手順

1. GIM を使用して S-TAP を Linux データベース・サーバーにインストールします。 インストーラーは、カスタム K-TAP モジュールが必要と判断し、そのモジュールを作成します。
2. カスタム K-TAP モジュールは、その sha256sum 値とともに、S-TAP が構成されている Guardium システムに自動的にアップロードされます。これは、GIM サーバーとして使用する Guardium システムと同じシステムではない場合があることに注意してください。
3. K-TAP のアップロード先となる Guardium システムで、CLI コマンドの grdapi make_bundle_with_uploaded_kernel_module を実行します。これにより、新しく作成された K-TAP モジュールが、対応する S-TAP バンドルに追加されます。ビルド番号とオペレーティング・システム属性が、アップロードされた K-TAP モジュールのものと一致する S-TAP バンドルが少なくとも 1 つ必要です。ロードされたバンドルは /var/gim_dist_packages に保管されます。 スクリプトにより、_8XX がビルド番号に追加された新規 S-TAP バンドルが作成されます。この新規バンドルは、/var/dump に配置されます。GuardAPI コマンド grdpi make_bundle_with_uploaded_kernel_module を実行した後、新規 GIM バンドルをロードする必要があります。ロードしない場合、そのバンドルは GIM GUI で表示されません。GuardAPI コマンドの grdpi make_bundle_with_uploaded_kernel_module が正常に実行されると、新しい STAP バンドルの名前を示す次のようなメッセージが出力されます:「カーネル ktap-71327-suse-11-linux-x86_64-xCUSTOMxeagle910-3.0.101-303.gefb7031-default-x86_64-SMP で guard-bundle-STAP-9.0.0_r71327_v90_800-suse-11-linux-x86_64.gim が作成されました」。 次に、GuardAPI コマンドの grdapi gim_load_package を実行して、上記のメッセージに記載されている新しいバンドルの名前を指定します。
4. 新規バンドルが、ご使用の GIM サーバーではない Guardium システム上にある場合、新規バンドルを GIM サーバーにコピーします。
5. GIM GUI または CLI を使用して、カスタム K-TAP が作成されたサーバーと同じ Linux ディストリビューションを実行しているその他のデータベース・サーバーに新規バンドルを配布します。使用可能な何百もの Linux ディストリビューションが存在し、そのリストは増え続けています。 このことは、ご使用の Linux ディストリビューションで K-TAP がまだ使用可能になっていない可能性があることを意味します。適切な K-TAP が使用可能でない場合、S-TAP インストール・プロセスにより K-TAP を作成することができます。Linux データベース・サーバー用に新規 K-TAP モジュールを作成するときに、同じ Linux ディストリビューションを実行している他のデータベース・サーバーにそのモジュールをコピーすることができます。

親トピック: Guardium Installation Manager
新規 K-TAP モジュールの他のシステムへのコピー

GIM の動的更新

GIM クライアントは、GIM サーバーからの更新がないかを一定の間隔でチェックします。GIM サーバーは、使用する最適なポーリング間隔をシステムの状態に基づいて計算することができます。

各 GIM クライアントは、GIM サーバーに対して定期的に「アライブ」メッセージを送信して、処理する準備ができた更新があるかどうかを確認します。このポーリング間隔は、GIM サーバーの状態に基づいて計算され、更新されます。間隔は定期的に計算され、「アライブ」メッセージに応答して、新しい値が GIM クライアントに渡されます。この機能はデフォルトで有効になりますが、代わりに固定間隔を使用したい場合は、オフに切り替えることができます。

GIM クライアントが GIM サーバーに接続しようとして 5 回連続で失敗した場合、フェイルオーバー・サーバーが指定されていれば、GIM クライアントは自動的にそちらに接続します。元の GIM サーバーが使用可能になると、GIM クライアントはその GIM サーバーへの接続を再開します。GIM サーバーとフェイルオーバー・サーバーは、それぞれ GIM_URL パラメーターと GIM_FAILOVER_URL パラメーターを使用して構成されます。

動的更新は Guardium API コマンド gim_set_global_param に以下のパラメーターを指定して制御されます。

dynamic_alive_enabled
: 動的アライブ機能のコントロール。1 – 有効、0 – 無効。デフォルト = 1

dynamic_alive_check_interval
: ポーリング間隔が再計算される間隔 (分単位)。デフォルト = 5

例:

```
grdapi gim_set_global_param dynamic_alive_enabled=0
```

各 GIM クライアントがサーバーにアライブ・メッセージを送信すると、サーバーは応答として、新しいポーリング間隔を渡すほか、そのクライアント用にスケジュールされたその他の更新があればをそれを送信します。

以下のパラメーターはバージョン 10.0 では有効でしたが、バージョン 10.1 以上からは削除されました。

- dynamic_alive_default_load_factor
- dynamic_alive_cpu_level1_threshold
- dynamic_alive_cpu_level2_threshold
- dynamic_alive_db_conn_level1_threshold
- dynamic_alive_db_conn_level2_threshold
- dynamic_alive_cpu_load_sample_time

親トピック: Guardium Installation Manager

データベース・サーバーのオペレーティング・システムをアップグレードするとき

データベース・サーバーでオペレーティング・システムをアップグレードするときに、GIM クライアントが、GIM クライアント自体と GIM によってインストールされたモジュール内で必要な変更を行えるようにすることができます。

始める前に

http://www-01.ibm.com/support/docview.wss?uid=swg21679002 の情報を参照して、ご使用の GIM クライアントのレベルに応じて使用可能なオプションを確認してください。

このタスクについて

アップグレードを手動で行うか、自動的に行うかにかかわらず、アップグレードの後すぐに、GIM によってインストールされたモジュールすべてを更新することをお勧めします。デフォルトでは、これらのモジュールを自動更新するオプションは無効になっています。自動更新を使用したい場合は、このオプションをサポートするために、GIM サーバーとして機能する Guardium システムを構成する必要があります。また、必要なバンドルをこのサーバー上で使用可能にする必要もあります。

手順

1. データベース・サーバーにインストールされている各モジュールについて、新しいオペレーティング・システムのバージョンをサポートする、このモジュールの最新バージョンが含まれている GIM バンドルを探します。各バンドルのビルド番号が、現在インストールされているバンドルの番号と同じか、それより大きい番号である必要があります。各バンドルを GIM サーバーにロードします。
2. gim_set_global_param コマンドを使用して、グローバル・パラメーター auto_install_on_db_server_os_upgrade の値を 1 に設定します。これにより、GIM サーバー上で自動更新オプションが有効になります。

   ```
   grdapi gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="1"
   ```

   デフォルトでは、このパラメーターは 0 に設定されています。これはこのオプションが無効であることを示します。
3. その他の準備をすべて完了した後、データベース・サーバー上でオペレーティング・システムをアップグレードします。

タスクの結果

OS のアップグレード後の最初のブート時に、GIM クライアントは、オペレーティング・システムがアップグレードされたことを認識します。また、自動更新オプションが有効になっているため、以下のステップを実行します。

1. GIM によってインストールされたすべてのモジュールの構成ファイルを、新しいオペレーティング・システムの属性がサポートされるように変更します。
2. すべてのモジュールを GIM サーバーに、更新後の属性で再登録します。
3. OS のアップグレードが実行されたことを示し、実行すべきアクションをリストしたアラートを GIM_EVENTS レポートに記録します。

モジュールが再登録されている場合、GIM サーバーは、以前にインストールされたバンドルと同じビルド番号を持つが、アップグレードされた OS と互換性のあるバンドルを最初に探します。このようなバンドルを検出できない場合、サーバーは新しい OS 属性をサポートする最新のバンドルを探します。サーバーは、該当するバンドルを検出できない場合、エラー・メッセージを出します。 サーバーが該当するバンドルを検出した場合は、それらのアップグレードをスケジュールし、アップグレード・プロセスを直ちに実行します。

次のタスク

GIM_EVENTS レポート内のメッセージを確認します。 GIM サーバーによって、モジュールが正常にアップグレードされたことが報告された場合は、更新後と同様に、各モジュールが正しく動作することを確認します。

GIM_EVENTS レポートに、アップグレードが正常に行われなかったことを示すエラー・メッセージが書き込まれている場合は、エラー・メッセージを調べてアドバイスがないか確認します。

スケジュールされた OS のアップグレードが完了したら、GIM サーバーで自動更新オプションを無効にします。 これにより、GIM クライアントで誤って更新プロセスが開始されるのを防ぐことができます。

```
grdapi gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="0"
```

別の OS のアップグレードを実行するときに、自動更新オプションを再度有効にすることができます。
親トピック: Guardium Installation Manager

管理対象ユニットへの GIM バンドルの配布

管理対象ユニットによって管理される GIM クライアント上に GIM バンドルをデプロイするために、管理対象ユニットに GIM バンドルを配布することができます。

始める前に

このタスクについて

すべての GIM クライアントを中央マネージャーから管理する場合は、すべての GIM クライアントに中央マネージャーから直接バンドルをデプロイすることができます。クライアントのグループを複数の管理対象ユニットから管理する場合は、中央マネージャーから管理対象ユニットに GIM バンドルを配布することができます。

配布に必要な時間は、バンドルのサイズとネットワークの状態によって異なります。相当な待ち時間があるネットワークでは、転送に数時間かかることがあります。

手順

1. 配布するバンドルを、中央マネージャー上の /var/gim/dist_packages ディレクトリーにコピーします。このディレクトリー内のすべてのファイルが配布されます。配布するバンドルを選択することはできません。
2. バンドルを配布する管理対象ユニットを選択します。
3. 「GIM バンドルの配布」をクリックします。 選択した管理対象ユニットにバンドルがコピーされます。

タスクの結果

各管理対象ユニットから、その管理対象ユニットが管理する GIM クライアントに、バンドルをインストールすることができます。
親トピック: Guardium Installation Manager

使用されていない GIM バンドルの削除

GIM バンドルがデータベース・サーバーで使用されなくなった場合、GIM サーバーから削除することができます。

このタスクについて

この機能を使用すると、GIM バンドルのインベントリーを管理し、インベントリーによってディスク・スペースが無駄に使用されるのを防ぐことができます。

2 つの新しい Guardium API コマンドを使用して、使用されていない GIM バンドルを特定し、削除できます。GIM サーバーとして機能する各 Guardium システム上で、以下の手順を実行します。

手順

1. gim_list_unused_bundles コマンドを実行して、FAM インストールの未使用のバンドルを特定します。includeLatest パラメーターは、コマンドによって返されるリストに、各 GIM バンドルの最新バージョンを含めるかどうかを指定する目的で使用します。まだ配布していないバンドルがある場合があります。また、必要になったときに再インストールできるように旧バージョンを保存しておきたい場合もあります。各バンドルの使用されていない最新のバージョンをコマンドの結果から除外する場合は、includeLatest を 0 に設定します。 使用されていないすべてのバージョンを含める場合は、1 に設定します。このパラメーターは必須で、デフォルト値は提供されていません。例:

   ```
   gim_list_unused_bundles includelatest=0
   ```

   このコマンドにより、GIM サーバー上で見つかったが、この GIM サーバーとともに動作する GIM クライアントが存在するデータベース・サーバー上にはインストールされていない GIM バンドルのリストが返されます。
2. ステップ 1 で使用されていないバンドルがいくつか示されたら、gim_remove_bundle コマンドを使用して、不要な各バンドルを削除します。このコマンドは、削除するバンドルを指定する 1 つのパラメーター bundlePackageName を取ります。このパラメーターは必須で、デフォルト値は提供されていません。
   gim_list_unused_bundles コマンドによって返された名前を指定してください。
   次の条件を満たす場合にのみ、指定されたバンドルが削除されます。
   - bundlePackageName に指定された名前が、特定の 1 つだけの GIM バンドルの名前と一致する場合。
   - この GIM サーバーとともに動作する GIM クライアントが存在するデータベース・サーバーに、bundlePackageName と名前が一致する GIM バンドルがインストールされていない場合。

   例:

   ```
   gim_remove_bundle bundlePackageName=name
   ```

   ここで、name は gim_list_unused_bundles コマンドによって返されたバンドル名です。

タスクの結果

必要のない GIM バンドルが GIM サーバーから削除されます。
親トピック: Guardium Installation Manager

GIM 診断の実行

GIM サーバーが、各 GIM クライアントについて正確なデータを持っているかどうかを確認するために、GIM クライアント上で診断を実行することができます。

このタスクについて

GIM クライアントで問題が発生した場合、最初のステップとして、GIM サーバーがそのクライアントについて正確なデータを持っていることを確認する必要があります。GIM 診断を実行すると、GIM サーバー上でそのクライアントについてリストされたモジュールが、そのクライアントにインストールされているモジュールと一致するかどうか、および GIM クライアントに保管されているパラメーターが、GIM サーバーに保管されているパラメーターと一致するかどうかが検査されます。

GIM 診断は、Guardium ユーザー・インターフェースまたはコマンド行のいずれかから実行できます。コマンド行から実行する場合は、次のコマンドを使用します。

```
grdapi gim_run_diagnostics clientIP=xx.xx.xx.xx
```

clientIP の値には、IP アドレスまたはホスト名を指定できます。このコマンドは、このクライアントの GIM サーバーである Guardium システムで実行する必要があります。

GIM 診断を GUI から実行する場合は、次の手順を使用します。

手順

1. 各クライアントの横にあるチェック・ボックスを使用して、GIM 診断の実行対象とするクライアントを選択します。
2. 「診断の実行」をクリックします。 各クライアントは、次回に更新について GIM サーバーをポーリングするときに、診断コマンドを受け取り、コマンドを直ちに実行します。

タスクの結果

この結果を GIM_EVENT レポートで確認することができます。
親トピック: Guardium Installation Manager

GIM 動作のデバッグ

問題をトラブルシューティングするためにデバッグをオンにすることが必要な場合があります。

このタスクについて

以下のステップを使用して、GIM サーバーで GIM デバッグをオンにします (Guardium システム)。

手順

1. GIM プロパティー・ファイル /usr/local/jakarta-tomcat-4.1.30/webapps-http/ROOT/WEB-INF/conf/gimserver.log4j.properties を編集します。
2. 値 ERROR を DEBUG に変更します。
3. ファイルを保存します。

タスクの結果

デバッグは数秒後にオンになり、デバッグ・メッセージは /var/log/guard/debug-logs/ 内の日次デバッグ・ログ・ファイルに書き込まれます。

次のタスク

デバッグが終了したら、ファイルを再び編集して DEBUG を ERROR に戻します。

親トピック: Guardium Installation Manager

GIM クライアントのデバッグの有効化

このタスクについて

GIM クライアントでデバッグを有効にするには、パラメーター module_DEBUG を 1 に変更します。ここで、module は、操作のデバッグ対象となるインストール済みモジュールの名前です。CLI またはユーザー・インターフェースを使用することにより、パラメーターを変更できます。デバッグの完了時に値を 0 に設定します。

SMF サポートを備えた Solaris 用の監視プログラムの再始動

一連の CLI コマンドを使用して、SMF サポートを備えた Solaris サーバーで監視プログラムを再始動します。

このタスクについて

監視プログラムを再始動するには、以下の手順を実行します。この手順は、SMF サポートを備えた Solaris サーバー上でのみ使用してください。

手順

1. コマンド svcadm -v disable guard_gsvr を実行して、監視プログラムを停止します。
2. svccfg delete -f guard_gsvr コマンドを実行します。
3. コマンド svccfg import <gim install dir>/SUPERVISOR/current/guard_gsvr.xml を使用して監視プログラムを再始動します。ここで、<gim install dir> は、GIM インストール・ディレクトリーへのファイル・パスです。

タスクの結果

SMF サポートを備えた Solaris で監視プログラムが再始動されました。
親トピック: Guardium Installation Manager

Guardium システムのインストール

この資料では、IBM Security Guardiumシステムをインストールして構成するのに必要なステップについて詳しく説明します。

また、この資料では、アプライアンスでパーティショニングをカスタマイズする方法や、リモート・ドライブ (SAN) にインストールする方法についても説明します。

具体的なステップは以下のとおりです。

1. 作業を始める前に、必要な構成情報とハードウェアを集めます。
2. 物理アプライアンスまたは仮想アプライアンスを設定します。
3. Guardium® イメージをインストールします。
4. 初期構成と基本構成を設定します。
5. インストールが成功したかどうか検証します。

IBM Security Guardium ソリューションは、以下の形態で提供されます。

- ハードウェア・オファリング – IBM® 提供の物理アプライアンスに組み込んで提供される、完全に構成されたソフトウェア・ソリューション。
- ソフトウェア・オファリング - ユーザーが所有するハードウェアに直接デプロイする、または仮想アプライアンスとしてデプロイするソフトウェア・イメージとして提供されるソリューション。

この資料に記載する要件は、特に指定のないかぎり、物理アプライアンスと仮想アプライアンスの両方のインストールに適用されます。

- 動作モード
  Guardium システムは、複数の動作モードのうち、任意のモードでデプロイすることができます。
- ライセンス・キー
  Guardium システムを機能する状態にするには、基本ライセンスと 1 つ以上の追加ライセンスの両方が必要になります。
- ハードウェア要件
  詳細なハードウェア要件およびサイジングの推奨事項は、IBM サポート・ポータルより入手できます。
- Guardium のポート要件
  各 Guardium システムには、何種類かの通信を行うためのポートが必要です。以下の表に、これらの通信を行うための接続と、その接続に割り当てられているデフォルトのポート番号を示します。
- ステップ 1. 始める前の準備
  Guardium システムのデプロイメントを準備するために、ネットワーク管理者は以下の情報を提供する必要があります。
- ステップ 2. 物理アプライアンスまたは仮想アプライアンスの設定
  このセクションで示すセットアップ手順は、物理アプライアンスでインストールする場合と、仮想アプライアンスでインストールする場合で異なります。
- ステップ 3. Guardium イメージのインストール
  このセクションでは、イメージのインストールおよびディスクのパーティション化を行う方法について説明します。
- ステップ 4. 初期構成および基本構成の設定
  最初のステップとしてネットワーク構成を行います。これは、シリアル・ポートまたはシステム・コンソールからアクセス可能なコマンド行インターフェース (CLI) を使用してローカルに行う必要があります。
- ステップ 5. 次の作業
  このセクションでは、インストールの検証、ライセンス・キーのインストール、および入手可能な保守パッチのインストールの各ステップについて詳しく説明します。
- 仮想イメージの作成
  仮想イメージをインストールする場合は、このセクションを参照してください。
- カスタム・パーティション
  ハード・ディスクのパーティションをカスタマイズする場合は、いくつかの選択を行う必要があります。
- 暗号化された LVM によるパーティション化の方法
  暗号化されたディスクを使用する場合は、以下の手順を実行して、論理ボリューム / と /var を含む暗号化された LVM ボリュームを作成します。
- SAN 構成の例
  この付録では、ハード・ディスクの事前パーティション化 (SAN をインストールする場合に必要) を行うために、コマンド・プロンプトに移動して実行する手順について説明します。

動作モード

Guardium システムは、複数の動作モードのうち、任意のモードでデプロイすることができます。

Guardium の環境を計画する際に、システムを以下のいずれかの動作モードでデプロイすることも、すべての動作モードでデプロイすることもできます。

コレクター
: コレクターは、データベース・サーバーとファイル・サーバー上にデプロイされているエージェントから、データベースのアクティビティーまたはファイルのアクティビティーに関するデータを受信します。 コレクターは、コレクターにインストールされているポリシーに従い、受信したデータを処理して応答します。コレクターは、アグリゲーターにデータをエクスポートすることができます。

アグリゲーター
: アグリゲーターは複数のコレクターからデータを収集し、そのデータの集約ビューを提供します。アグリゲーターは、データベース・サーバーやファイル・サーバーに直接接続されることはありません。場所や機能に応じて、コレクターをアグリゲーターに割り振ることができます。例えば、人事関連リソースのデータベース・サーバーをモニターするコレクターを単一のアグリゲーターに接続すると、それらすべてのサーバーに関連するデータを 1 カ所で表示することができます。必要な場合は、コレクターからではなく、他のすべてのアグリゲーターからデータを収集するアグリゲーターをデプロイすることにより、第 2 の集約層を実装することもできます。
  注: 中央マネージャーとしてアプライアンスを使用する予定の場合、アグリゲーター・オプションを選択する必要があります。

中央マネージャー
: Guardium 環境には中央マネージャーが 1 つしか存在しませんが、バックアップ用の中央マネージャーとして別の Guardium システムを指定することができます。中央マネージャーを使用することにより、単一コンソールからポリシーを定義してそのポリシーをすべてのコレクターに配布したり、すべての Guardium システムに影響する他の構成タスクを実行したり、他のさまざまな管理タスクを実行したりすることができます。 中央マネージャーをアグリゲーターとして動作させて、データをコレクターや他のアグリゲーターから収集することもできます。この場合、全社規模でのアクティビティーのビューを表示したり、すべての Guardium システムから集約されたデータに基づくレポートを表示したりすることができます。

コレクターに割り当てるモニター対象のデータベース・サーバーとファイル・サーバーの数は、サーバーからコレクターに流れるデータ量によって異なります。現在の環境で必要なコレクターとアグリゲーターの数に関する情報と、最良の結果を得るための Guardium システムの配置方法については、「Deployment Guide for IBM Guardium」を参照してください。

Guardium 脆弱性評価コンポーネントを使用する場合は、評価テストを実行する場所を決める必要があります。 一部のユーザーは、この機能のために専用の Guardium システムを個別に設定しています。コレクター、アグリゲーター、または中央マネージャーとしてデプロイされた任意の Guardium システムからテストを実行することもできます。

親トピック: Guardium システムのインストール

ライセンス・キー

Guardium システムを機能する状態にするには、基本ライセンスと 1 つ以上の追加ライセンスの両方が必要になります。

基本ライセンスと追加ライセンスの概要を以下に示します。

- 基本ライセンス・キー (リセット・キーとも呼ばれます) は、システムのマシン・タイプを反映します。例えば、コレクター・システムを設定する場合は、コレクター用の基本ライセンスが必要になります。
- 追加ライセンス・キーを使用すると、特定の機能セットが有効になります。例えば、通常のデータ・アクティビティー・モニター機能を使用する場合は、DAM Standard 追加ライセンスが必要になります。複数の追加ライセンスを組み合わせてインストールすると、Guardium の拡張機能を使用できるようになります。

基本ライセンスを適用するとマシン・タイプがチェックされ、互換性があるかどうかが確認されます。基本ライセンスには、以下の 2 つのタイプがあります。

表 1. 基本ライセンスのタイプ

基本ライセンスのタイプ	ライセンスの説明
コレクター	スタンドアロン・システムやコレクターを設定する場合は、コレクター用の基本ライセンスを使用します。
アグリゲーター	アグリゲーターや中央マネージャー・システムを設定する場合は、アグリゲーター用の基本ライセンスを使用します。

Guardium システムで使用できる機能は、インストールされている追加ライセンスによって異なります。有効な追加ライセンスを以下に示します。これらのライセンスは、組み合わせて使用することができます。

表 2. 追加ライセンスのタイプ

追加ライセンスのタイプ	ライセンスの説明
DAM Express	データ・アクティビティー・モニターの事前定義機能。
DAM Standard	データ・アクティビティー・モニターの主要機能を使用するためのライセンス。
DAM Advanced	DAM Standard 機能、詳細なアクセス制御機能、マスキング機能、隔離機能、ブロッキング機能 (アクティビティーの強制終了機能) を使用するためのライセンス。
FAM Standard	ファイル・アクティビティー・モニターの主要機能を使用するためのライセンス。
FAM Advanced	FAM Standard 機能とブロッキング機能を使用するためのライセンス。
VA Standard	脆弱性評価機能、データベース保護サービス (DPS)、変更監査システム (CAS)、データベース・ライセンス・レポートを使用するためのライセンス。

Guardium ライセンスのインストールについては、ライセンス・キーのインストールを参照してください。

親トピック: Guardium システムのインストール
関連タスク:
ライセンス・キーのインストール

ハードウェア要件

詳細なハードウェア要件およびサイジングの推奨事項は、IBM サポート・ポータルより入手できます。

詳細なハードウェア仕様およびサイジングの推奨事項については、IBM Guardium V10.1 Software Appliance Technical Requirements を参照してください。

親トピック: Guardium システムのインストール

Guardium のポート要件

各 Guardium システムには、何種類かの通信を行うためのポートが必要です。以下の表に、これらの通信を行うための接続と、その接続に割り当てられているデフォルトのポート番号を示します。

オープン・ポート

Guardium システムで使用されるポート。

DB サーバー – コレクター

TCP 8443 - DB サーバーからコレクター

TCP 16016 – Unix STAP、両方向、登録、ハートビート、およびデータ (PASE で稼働中の IBM i S-TAP を含む)

TCP 16017 - Windows/Unix CAS、両方向、テンプレートおよびデータ

TCP 16018 – Unix STAP (TLS)、両方向、登録、ハートビート、およびデータ

TCP 16019 - Windows/Unix CAS (TLS)、両方向、テンプレートおよびデータ

TCP 16020 - UNIX STAP 接続プーリングから

TLS 16021 - STAP エージェントの暗号化された UNIX STAP 接続プーリングから

TCP 8081 – Guardium Installation Manager、両方向、データベース・サーバーからコレクター/中央マネージャー

TCP 9500 – Windows STAP、両方向、DB サーバーからコレクター、STAP 登録およびデータ

TCP 9501 – Windows STAP (TLS)、両方向、DB サーバーからコレクター、STAP 登録およびデータ

コレクター – アグリゲーター (セキュア・シェル – SSL)

TCP 22 – コレクターからアグリゲーター、SCP データ・エクスポート、両方向

中央マネージャー – 管理対象デバイス

TCP 22 – SSH/SCP データ転送、両方向

TCP 8443 – SSL、両方向

TCP 8444 – SSL、STAP から GIM へのファイル・アップロード

TCP 3306 – MySQL、特定ソースに対してオープン (例えば、中央マネージャーはすべての管理対象ユニットに対してオープンであり、管理対象ユニットは中央マネージャーに対してオープンです)

TLS 8447 - フェデレーテッド環境または一元管理環境内の Guardium システム間の通信用に、リモート・メッセージング・サービス・インフラストラクチャー (およびプロファイル配布インフラストラクチャー) で使用されます。構成プロファイルを使用すると、中央マネージャーから構成とスケジューリングの設定を定義して、中央マネージャー自体の構成を変更することなく、これらの設定を管理対象ユニット・グループに容易に配布できます。

ファイル・アクティビティー・モニター (FAM)

TCP/TLS 16022/16023 - 汎用フィード。16022 (FAM モニター、非暗号化) と 16023 (FAM モニター、暗号化) の両方が双方向にオープンである必要があります。スニファーでは、16016 から 16023 までのブロックが双方向にオープンである必要があります

18087 - FAM がインストールされているのと同一マシン上にある IBM Content Classification (ICM) サーバー上の FAM のリスナー・ポート (serverSettings.icmURL=http://localhost:18087)。双方向にオープン。

Guardium Installation Manager (GIM)

8445 - GIM クライアント・リスナー、両方向。GIM クライアントが listen を行っています。中央マネージャーまたはコレクターいずれかの GIM サーバーが、それ (GIM クライアント) に到達できます。

8446 - GIM 認証 TLS、両方向。GIM クライアントと GIM サーバー (中央マネージャーまたはコレクター上) の間で使用します。GIM_USE_SSL が無効に設定されていない場合、gim_client はポート 8446 を介してその証明書に通信しようと試みます。ポート 8446 がオープンされていない場合、デフォルトは 8444 ですが、証明書は渡されません (証明書の検証なしの TLS など)。

8081 - TLS - GIM クライアントを GIM サーバーに接続するために 8081 を使用する場合、GIM_USE_SSL パラメーターを無効にする必要があります。デフォルトではオンになっています。このパラメーターは、GUI の GIM 共通パラメーターに含まれています。 GIM_USE_SSL が無効に設定されていない場合、gim_client はポート 8446 を介してその証明書に通信しようと試みます。ポート 8446 がオープンされていない場合、デフォルトは 8444 ですが、証明書は渡されません (証明書の検証なしの TLS など)。

エンタープライズ・ロード・バランサー

TLS 8443 - S-TAP ロード・バランサー - これは、UNIX/Linux S-TAP でインスタンスをコレクターに通信させる際に必要です。ただし、このポートは中央マネージャーのロード・バランサーにも使用されます。 インストール済み環境でエンタープライズ・ロード・バランサーを使用することが示されると、S-TAP は HTTPS メッセージを送信することにより、8443 で中央マネージャー (ロード・バランサー) に対する要求を開始します。お客様がデータベースから中央マネージャーへの直接的なオープン・ポートを希望しない場合、データベース・サーバーと中央マネージャー間にプロキシー・サーバーを使用する機能が存在します。

Quick Search for Enterprise

TCP 8983 - SOLR - 着信、SSL

TCP 9983 - SOLR - 着信、SSL

ユーザー・インターフェース - Guardium システム (スタンドアロン、アグリゲーター、中央マネージャー)

TCP 22 – ユーザーからシステム、CLI 接続、両方向

TCP 8443 - ユーザーからシステム、GUI 接続 (構成可能)、両方向

システム - SMTP サーバー

TCP 25 - システムから SMTP サーバー、E メール・アラート

システム - SNMP サーバー

UDP 161 - SNMP クライアントからシステム - SNMP ポーリング

UDP 162 - システムから SNMP サーバー、SNMP トラップ

システム - SYSLOG サーバー

UDP/TCP 514 –他のシステムとの送受信リモート syslog メッセージ、通常は SIEM。**注:** ローカル・ポートは 514 ですが、リモート・ポートを構成に入力する必要があります。暗号化を使用する場合、プロトコルは UDP ではなく、TCP でなければなりません。

システム – NTP サーバー

TCP/UDP 123 – システムから Network Time Protocol サーバー

システム - DNS サーバー

TCP/UDP 53 - システムからドメイン・ネーム・サーバー

システム – EMC Centera (バックアップ)

TCP 3218 - システムから EMC Centera

システム - Tivoli LDAP

UDP 389 –システムと Tivoli LDAP 間

システム - メインフレーム

TCP 16022 - S-TAP を Db2 z/OS、S-TAP IMS、S-TAP VSAM (S-TAP データ・セット) に接続

TCP 16023 - TLS 接続、具体的には IBM の Application Transparent Transport Layer Security (AT-TLS)

Windows データベース・サーバーに接続するためのポート

ポート	プロトコル	目的
8075	UDP	Windows S-TAP ハートビート・シグナル (両方向トラフィック)。注: UNIX S-TAP エージェントは、ハートビート・シグナルで UDP を使用しないため、この機能に対応する UNIX ポートはありません。
9500	TCP	クリアな Windows S-TAP
9501	TLS	暗号化された Windows S-TAP (オプション)
16017	TCP	クリアな Windows CAS
16019	TLS	暗号化された Windows CAS (オプション)

Guardium アプリケーションへのアクセスに使用されるデフォルト・ポート

ポート	プロトコル	目的
8443	TCP	Guardium のユーザー・インターフェースに対する Web ブラウザー・アクセス (HTTPS)。注: Guardium の管理者は、このポートを変更することができます。また、このポートを使用して、管理対象ユニットが中央マネージャーに登録されます。
22	TCP	Guardium アプライアンスを管理するための、クライアントからの SSH アクセス
3306	TCP	中央マネージャーと管理対象ユニット間の通信

z/OS データベース・サーバーに接続するためのポート

ポート	プロトコル	目的
16022	TCP	S-TAP for Db2 z/OS、S-TAP for IMS、S-TAP for Data Sets への接続
16023	TCP	TLS 接続、具体的には IBM の Application Transport Layer Security (AT-TLS)
41500	TCP	内部メッセージ・ロギング通信用のデフォルトの開始ポート – LOG_PORT_SCAN_START
39987	TCP	エージェントとエージェントの 2 次アドレス・スペース間のデフォルトのエージェント固有通信ポート – ADS_LISTENER_PORT

他の機能で使用されるデフォルト・ポート

ポート	プロトコル	目的
20, 21	TCP	バックアップ/アーカイブのための FTP サーバー (オプション)
22	TCP	バックアップ/アーカイブ、パッチの配布、ファイル転送のための SCP
25	TCP	アラートおよびその他の通知のための SMTP (E メール・サーバー)
53	TCP	DNS Servers
123	TCP、UDP	時刻の同期のための NTP (タイム・サーバー)
161	TCP、U	SNMP ポーリング (オプション)

	DP	
162	TCP、UDP	SNMP トラップ (オプション)
389	TCP	LDAP (Active Directory や Sun One Directory など)
514	TCP	Syslog サーバー (オプション)
636	TCP	LDAP (SSL 経由の Active Directory や Sun One Directory など) (オプション)
1500	TCP	Tivoli Storage Manager のバックアップ・ホスト (オプション)
3218	TCP、UDP	EMC 中央バックアップ・ホスト (オプション)
ユーザー定義	TCP	Guardium データ・ソース・アクセス用のデータベース・サーバーのリスナー・ポート (例えば、Oracle の場合は 1521、MS-SQL の場合は 1433) (オプション)
16022/16023	TCP/TLS	汎用フィード - ファイル・アクティビティー・モニター (FAM)
18027		IBM Content Classification をローカルに使用した FAM (serverSettings.icmURL=http://localhost:18087)
8445		GIM クライアント・リスナー、両方向 GIM クライアントが listen を行っています。中央マネージャーまたはコレクターいずれかの GIM サーバーが、それ (GIM クライアント) に到達できます。
8446	TLS	GIM 認証 TLS、両方向 GIM クライアントと GIM サーバー (中央マネージャーまたはコレクター上) の間で使用します。 GIM_USE_SSL が無効に設定されていない場合、gim_client はポート 8446 を介してその証明書に通信しようと試みます。ポート 8446 がオープンされていない場合、デフォルトは 8444 ですが、証明書は渡されません (証明書の検証なしの TLS など)。
8447	TLS	フェデレーテッド環境または一元管理環境内の Guardium システム間の通信用に、リモート・メッセージング・サービス・インフラストラクチャー (およびプロファイル配布インフラストラクチャー) で使用されます。構成プロファイルを使用すると、中央マネージャーから構成とスケジューリングの設定を定義して、中央マネージャー自体の構成を変更することなく、これらの設定を管理対象ユニット・グループに容易に配布できます。
8443	TLS	エンタープライズ・ロード・バランサー これは UNIX/Linux S-TAP でインスタンスをコレクターに通信させる際に必要です。 ただし、このポートは中央マネージャーのロード・バランサーにも使用されます。 インストール環境でエンタープライズ・ロード・バランサーを使用する場合、S-TAP は HTTPS メッセージを送信することにより ポート 8443 上で中央マネージャーへの要求を開始します。 そのため、お客様がデータベースから中央マネージャーへの直接的なオープン・ポートを希望しない場合、データベース・サーバーと中央マネージャー間にプロキシー・サーバーを使用する機能が存在します。
8081	TLS	GIM クライアントを GIM サーバーに接続するために 8081 を使用する場合、GIM_USE_SSL パラメーターを無効にする必要があります。デフォルトではオンになっています。 このパラメーターは、GUI の GIM 共通パラメーターに含まれています。 GIM_USE_SSL が無効に設定されていない場合、gim_client はポート 8446 を介してその証明書に通信しようと試みます。ポート 8446 がオープンされていない場合、デフォルトは 8444 ですが、証明書は渡されません (証明書の検証なしの TLS など)。
8983	TCP	SOLR、着信、SSL (Quick Search for Enterprise)
99	T	

83	CP	SOLR、着信、SSL (Quick Search for Enterprise)

親トピック: Guardium システムのインストール

ステップ 1. 始める前の準備

Guardium システムのデプロイメントを準備するために、ネットワーク管理者は以下の情報を提供する必要があります。

- インターフェース・カード (eth0) の IP アドレス。
- 1 次 IP アドレスのサブネット・マスク。
- デフォルトのルーター IP アドレス。
- システムに割り当てるホスト名およびドメイン名。
- DNS サーバーの IP アドレス (最大 3 つのアドレス)、および DNS ドメインへの新規 Guardium システムの追加。
- (オプション) 2 次管理インターフェースの IP アドレス。
- (オプション) 2 次 IP 管理インターフェースのマスク。
- (オプション) 2 次 IP 管理インターフェースのゲートウェイ。
- (オプション) NTP サーバーのホスト名。
- (オプション) SMTP 構成情報 (E メール・アラート用): IP アドレス、ポート、 および (認証使用の場合に) SMTP ユーザー名とパスワード。
- (オプション) SNMP 構成情報 (SNMP アラート用): SNMP サーバーの IP アドレスと使用するトラップ・コミュニティー名。

- SAN ストレージ・デバイス
  インストール処理をストレージ・エリア・ネットワーク (SAN) 上でデプロイする場合は、デプロイメントを実行する前に、SAN で必要な構成情報をすべて準備しておく必要があります。また、SAN ストレージ・デバイスをパーティション化し、Guardium OS をインストールするための追加のインストール・ステップを実行する必要があります。

親トピック: Guardium システムのインストール

SAN ストレージ・デバイス

インストール処理をストレージ・エリア・ネットワーク (SAN) 上でデプロイする場合は、デプロイメントを実行する前に、SAN で必要な構成情報をすべて準備しておく必要があります。また、SAN ストレージ・デバイスをパーティション化し、Guardium OS をインストールするための追加のインストール・ステップを実行する必要があります。

注: SAN へのインストールはサポートされていますが、NAS へのインストールはサポートされていません。
親トピック: ステップ 1. 始める前の準備

ステップ 2. 物理アプライアンスまたは仮想アプライアンスの設定

このセクションで示すセットアップ手順は、物理アプライアンスでインストールする場合と、仮想アプライアンスでインストールする場合で異なります。

- 物理アプライアンス
  ラックにアプライアンスを設置したら、次の方法でアプライアンスをネットワークに接続します。
- eth0 とその他のネットワーク・ポートの識別方法
  次の CLI コマンドを使用して、ネットワーク・ポートをマップします。
- 物理アプライアンスのデフォルト・パスワード
  定義済みユーザーには、デフォルトのパスワードが設定されています。
- 仮想アプライアンス
  IBM Security Guardium 仮想マシン (VM) は、ゲスト仮想マシン (VMware ESX Server など) でライセンス交付およびインストールを行う、ソフトウェア専用ソリューションです。

親トピック: Guardium システムのインストール

物理アプライアンス

ラックにアプライアンスを設置したら、次の方法でアプライアンスをネットワークに接続します。

1. 電源接続部を見つけます。適切な電源コードを、これらの接続部に接続します。
2. ネットワーク・ケーブルを eth0 ネットワーク・ポートに接続します。必要に応じて、オプションの 2 次ネットワーク・ケーブルを接続します。
3. キーボード、ビデオ、マウスを、直接または KVM 接続 (シリアル・ポートまたは USB ポート) 経由でシステムに接続します。
4. システムの電源を入れます。

親トピック: ステップ 2. 物理アプライアンスまたは仮想アプライアンスの設定
関連情報:
Lenovo System x3550 M5 Installation and Service Guide
技術要件に関する資料
eth0 管理ポートの変更点

eth0 とその他のネットワーク・ポートの識別方法

次の CLI コマンドを使用して、ネットワーク・ポートをマップします。

show network interface inventory

この CLI コマンドを使用して、インストールされているすべてのネットワーク・インターフェースのポート名および MAC アドレスを表示します。

```
show network interface inventory
eth0 00:13:72:50:CF:40
eth1 00:13:72:50:CF:41
eth2 00:04:23:CB:11:84
eth3 00:04:23:CB:11:85
eth4 00:04:23:CB:11:96
eth5 00:04:23:CB:11:97
```

show network interface port

この CLI コマンドを使用して、アプライアンスの背面にある物理コネクターを見つけます。show network interface inventory コマンドを使用してすべてのポート名を表示したら、以下のコマンドを使用して、「n」で指定される物理ポートのランプを 20 回明滅させます (「n」は、eth0、eth1、eth2、eth3 などのように、*eth* の後に続く数字です)。

```
show network interface port 1
```

ポート eth1 のランプが 20 回明滅します。

専用コンピューターにソフトウェアを直接インストールする

Guardium ソフトウェアを専用コンピューターのディスクに直接インストールする場合は、物理アプライアンスの手順を実行します。

親トピック: ステップ 2. 物理アプライアンスまたは仮想アプライアンスの設定

物理アプライアンスのデフォルト・パスワード

定義済みユーザーには、デフォルトのパスワードが設定されています。

IBM から物理アプライアンスを受け取ったら、以下のパスワードを使用して初期構成を行ってください。
注: インストールが完了したら、すべてのデフォルト・パスワードを必ず変更してください。

表 1. 定義済みユーザーのデフォルト・パスワード

ユーザー	デフォルトのパスワード
accessmgr	guard1accessmgr
admin	guard1admin
cli	guard1cli

親トピック: ステップ 2. 物理アプライアンスまたは仮想アプライアンスの設定

仮想アプライアンス

IBM Security Guardium 仮想マシン (VM) は、ゲスト仮想マシン (VMware ESX Server など) でライセンス交付およびインストールを行う、ソフトウェア専用ソリューションです。

Guardium VM をインストールするには、『仮想イメージの作成』に記載されているステップに従います。具体的なステップは以下のとおりです。

- システム互換性の検証
- VMware ESX Server のインストール
- ネットワーク・ケーブルの接続
- VM 管理ポータルの構成
- 新規仮想マシンの作成
- IBM Security Guardium 仮想アプライアンスのインストール

VM をインストールした後に、『ステップ 4. 初期構成および基本構成の設定』に戻って Guardium システムの構成方法に関する詳しい説明を参照してください。

親トピック: ステップ 2. 物理アプライアンスまたは仮想アプライアンスの設定

ステップ 3. Guardium® イメージのインストール

このセクションでは、イメージのインストールおよびディスクのパーティション化を行う方法について説明します。

1. UEFI/BIOS の「ブート・シーケンス」が、ハード・ディスクを使用する前に取り外し可能メディア (CD/DVD ドライブ) から始動するように設定されていることを確認します。
   注: インストールは DVD から実行できます。必要に応じて、技術サポートから UEFI/BIOS のパスワードを入手してください。
2. インストール DVD から Guardium イメージをロードします。
3. 次の 2 つのオプションが表示されます。

   標準インストール: これはデフォルトです。ディスクをパーティション化している場合は、ほとんどの場合この項目を使用します。

   カスタム・パーティション・インストール: すべてのパーティションを (ローカルに、または SAN ディスク上で) 詳細にカスタマイズできます。このオプションを実装する方法について詳しくは、『カスタム・パーティショニング』を参照してください。

   注:
   - 標準インストールでは、ディスク内容がすべて消去され、ディスクの再パーティション化と再フォーマットが行われ、新規オペレーティング・システムがインストールされます。
   - インストール後の最初のブート時に、ご使用条件への同意を求められます。Page Down キーでご使用条件を確認するか、Q キーで末尾にスキップします。ご使用条件に同意するには、`q` を入力して終了し、`yes` と入力します。`yes` と入力してご使用条件に同意する必要があります。同意しないとマシンはブートさ

れません。

4. システムは DVD からブートされます。このインストールには約 12 分かかります。

   (d) インストール・プロセスで、コレクターまたはアグリゲーターを選択するよう求められます (10 秒間入力されなかった場合、自動的に「コレクター」に設定されます)。コレクターとアグリゲーターの説明については、製品概要を参照してください。 アグリゲーターを選択しようとしたが 10 秒以内に選択しなかった場合は、アグリゲーターを選択できるこの時点まで戻るために、再インストールを実行する必要があります。

   注: 中央マネージャーとしてアプライアンスを使用する予定の場合、アグリゲーター・オプションを選択する必要があります。

5. この時点でシステムが自動的にリブートされ、インストールが完了します。リブート後の初回ログイン時に、パスワードを変更する必要があります。

親トピック: Guardium システムのインストール

ステップ 4. 初期構成および基本構成の設定

最初のステップとしてネットワーク構成を行います。これは、シリアル・ポートまたはシステム・コンソールからアクセス可能なコマンド行インターフェース (CLI) を使用してローカルに行う必要があります。

前に指定した一時 *CLI* パスワードを入力します。

以降のステップでは、CLI コマンドを使用して各種ネットワーク・パラメーターを指定して、Guardium システムをご使用の環境に統合します。

CLI 構文では、変数が不等号括弧で示されます (<ip_address> など)。

各変数を、ご使用のネットワークおよびインストール済み環境に適した値で置き換えます。括弧は含めないでください。

- 1 次システムの IP アドレスの設定
  1 次 IP アドレスは eth0 接続用で、以下の 2 つのコマンドを使用して定義されます。
- デフォルト・ルーター IP アドレスの設定
  次の CLI コマンドを使用します。
- DNS サーバーの IP アドレスの設定
  1 つ以上の DNS サーバーの IP アドレスを設定します。これは、アプライアンスがホスト名と IP アドレスの解決に使用します。 最初のリゾルバーは必須で、他はオプションです。
- SMTP サーバー
  システム・アラートを送信するには、SMTP サーバーが必要です。次のコマンドを入力して、ご使用の SMTP サーバー IP アドレスの設定、メッセージのリターン・アドレスの設定、および始動時の SMTP アラートの有効化を行います。
- ホスト名とドメイン・ネームの設定
  アプライアンスのホスト名とドメイン・ネームを構成します。 この名前は、DNS サーバーに登録されたアプライアンスのホスト名と一致する必要があります。
- タイム・ゾーンおよび日時の設定
  アプライアンスの日時を設定するには、以下のオプションがあります。
- 初期ユニット・タイプの設定
  アプライアンスは、スタンドアロン・ユニット、マネージャー・ユニット、または管理対象ユニットとして設定できます。また、アプライアンスがネットワーク検査または S-TAP、またはその両方を介してデータベース・アクティビティーをキャプチャーするように設定できます。標準的な構成はスタンドアロン・アプライアンス用 (すべてのアプライアンス用) で、最も一般的な設定では S-TAP を使用してキャプチャーを行います (コレクター専用)。
- root パスワードのリセット
  次の CLI コマンドを実行することで、独自の専用パス・キーを使用してアプライアンスの root パスワードをリセットします (アクセス・キーが必要: 「*t0Tach*」)。
- すべての設定の検証
  CLI からログアウトして次の構成ステップに進む前に、以下のコマンドを使用して、構成した設定をレビューして検証します。
- システムのリブート
  システムが最終ロケーションにない場合は、ここでシステムをシャットダウンし、最終的なネットワーク・ロケーションに配置して、再始動します。

親トピック: Guardium システムのインストール

1 次システムの IP アドレスの設定

1 次 IP アドレスは eth0 接続用で、以下の 2 つのコマンドを使用して定義されます。

```
store network interface ip <ip_address>
store network interface mask <subnet_mask>
```

デフォルトのネットワーク・インターフェース・マスクは 255.255.255.0 です。これがご使用のネットワークでの正しいマスクである場合は、2 番目のコマンドをスキップできます。

2 次 IP アドレスを割り当てるには、CLI コマンド store network interface secondary [on <interface> <ip> <mask> <gw> | off] を使用します。このコマンドを使用して、2 次インターフェースを有効/無効にすることができます。

次に、CLI コマンド restart network を使用してネットワークを再始動する必要があります。2 次 IP アドレスの割り当ては、CLI からのみ実行でき、GUI を使用して実行することはできません。

アプライアンス上の他のネットワーク・インターフェース・カードは、データベース・トラフィックのモニターに使用でき、IP アドレスは割り当てられません。

親トピック: ステップ 4. 初期構成および基本構成の設定

デフォルト・ルーター IP アドレスの設定

次の CLI コマンドを使用します。

```
store network routes defaultroute <default_router_ip>
```

親トピック: ステップ 4. 初期構成および基本構成の設定

DNS サーバーの IP アドレスの設定

1 つ以上の DNS サーバーの IP アドレスを設定します。これは、アプライアンスがホスト名と IP アドレスの解決に使用します。 最初のリゾルバーは必須で、他はオプションです。

```
store network resolver 1 <resolver_1_ip>
store network resolver 2 <resolver_2_ip>
store network resolver 3 <resolver_3_ip>
```

親トピック: ステップ 4. 初期構成および基本構成の設定

SMTP サーバー

システム・アラートを送信するには、SMTP サーバーが必要です。次のコマンドを入力して、ご使用の SMTP サーバー IP アドレスの設定、メッセージのリターン・アドレスの設定、および始動時の SMTP アラートの有効化を行います。

```
store alerter smtp relay <smtp_server_ip>
store alerter smtp returnaddr <first.last@company.com>
store alerter state startup on
```

注: SMTP サーバーはユーザー・インターフェースで構成することもできます。「設定」 > 「アラート機能」をクリックします。
親トピック: ステップ 4. 初期構成および基本構成の設定

ホスト名とドメイン・ネームの設定

アプライアンスのホスト名とドメイン・ネームを構成します。 この名前は、DNS サーバーに登録されたアプライアンスのホスト名と一致する必要があります。

```
store system hostname <host_name>
store system domain <domain_name>
```

親トピック: ステップ 4. 初期構成および基本構成の設定

タイム・ゾーンおよび日時の設定

アプライアンスの日時を設定するには、以下のオプションがあります。

タイム・ゾーン、日付、時刻、および NTP

1. タイム・ゾーンの設定
2. 日付と時刻の設定。オプション 1 - NTP の設定。オプション 2 - store system clock datetime

日付/時刻のオプション 1: Network Time Protocol

アクセス可能な NTP サーバーの詳細を指定して、 これを使用できるようにします。

```
store system ntp server
store system ntp state on
```

日時オプション 2: タイム・ゾーン、日付、および時刻の設定

次のコマンドを使用して、有効なタイム・ゾーンのリストを表示します。

```
store system clock timezone list
```

リストから適切なタイム・ゾーンを選択し、 同じコマンドを使用して設定します。

```
store system clock timezone <selected time zone>
```

注: 新しいタイム・ゾーンを設定すると、内部サービスが再始動し、その再始動中にデータ・モニターが数分無効になります。

日付と時刻を YYYY-mm-dd hh:mm:ss 形式で保存します。

```
store system clock datetime <date_time>
```

注: 同じ CLI セッションでホスト名とタイム・ゾーンを変更しないでください。

親トピック: ステップ 4. 初期構成および基本構成の設定

初期ユニット・タイプの設定

アプライアンスは、スタンドアロン・ユニット、マネージャー・ユニット、または管理対象ユニットとして設定できます。また、アプライアンスがネットワーク検査または S-TAP、またはその両方を介してデータベース・アクティビティーをキャプチャーするように設定できます。標準的な構成はスタンドアロン・アプライアンス用 (すべてのアプライアンス用) で、最も一般的な設定では S-TAP を使用してキャプチャーを行います (コレクター専用)。

store unit type standalone - このコマンドはすべてのアプライアンスに使用します。

store unit type stap - このコマンドはコレクターに使用します。

スタンドアロン・ユニット・タイプおよび STAP ユニット・タイプは、デフォルトで設定されます。マネージャー・ユニット・タイプは指定する必要があります (必要な場合)。

注: ユニット・タイプの設定は、アプライアンスが完全に作動可能になってから、後で行うことができます。

親トピック: ステップ 4. 初期構成および基本構成の設定

root パスワードのリセット

次の CLI コマンドを実行することで、独自の専用パス・キーを使用してアプライアンスの root パスワードをリセットします (アクセス・キーが必要: 「*t0Tach*」)。

```
support reset-password root <random>
```

資料で使用されているパス・キーを保存して、将来的に技術サポートの担当者が root アクセスできるようにします。 現在のパス・キーを確認するには、次の CLI コマンドを使用します。

```
support show passkey root
```

質問 - Guardium システムの root パスワードはどの程度安全ですか? 誰がアクセスできますか?

Guardium アプライアンスは「ブラック・ボックス」環境です。エンド・ユーザーのみがオペレーティング・システム・アカウントへの限定アクセス権を持ちます。以下に例を挙げます。

cli、guardcli1、guardcli2、guardcli3、guardcli4、guardcli5。

グラフィカル・ユーザー・インターフェースのユーザー・アカウント (admin や accessmgr など) は、Guardium システムのオペレーティング・システムによって定義されるのではなく、 アプリケーション・インターフェース (accessmgr) によって定義および管理されるアプリケーション ID です。

セキュアなサーバーであるため、 事前にすべてのユーザーが root アクセスを使用できるようにはなっていませんが、 多くの場合は、問題のトラブルシューティングおよび解決の目的で Guardium アプライアンスにアクセスするために Guardium サポートによって必要とされます。Guardium サポートは、Guardium アプライアンスにアクセスするために sudo を使用せず、また root 以外のいかなるユーザー ID も使用しません。

root のパスワードは、 「結合パスワード」の仕組みを使用してセキュリティーを確保しています。お客様は、8 桁の数値のパス・キーの形でアプライアンスに対するキーを保持します。IBM はパス・キー・デコーダーを保持します。パス・キーとパス・キー・デコーダーの両方がなければ、IBM もお客様も root としてアプライアンスにアクセスすることはできません。

パス・キーは、 お客様が CLI インターフェースで管理します。お客様は、 以下の CLI コマンドを使用して、IBM に通知せずにいつでもパス・キーを変更できます。

```
support reset-password root
```

CLI アクセス権を持つすべてのユーザーは、以下の CLI コマンドを使用して root のパス・キーを取得できます。

```
support show passkey root
```

Guardium サポートと連携するときには、 リモート・デスクトップ共有セッションで、 サポート・アナリストが問題の Guardium アプライアンスに対する root パス・キーを要求します。パス・キーがデコードされると、Guardium サポートが root パスワードを使用して root としてアプライアンスにアクセスします。リモート・デスクトップ共有セッションが終了したら、お客様は、上記の CLI コマンドを使用してパス・キーを変更することで、IBM が今後そのアプライアンスの root パスワードを所有しないようにすることができます。

パス・キーは 8 桁の数値キーであり、 範囲は 10000000 から 99999999 までです。この範囲で 89,999,999 通りのパスワードを作成できます。エンコード後のパスワードはすべて強固です。一般的なパスワードや辞書にある単語は含まず、 長さはそれぞれ異なり、各国語文字、特殊文字、英字 (大文字と小文字)、および/または数字を含んでいます。

パス・キー・デコーダーへのアクセスは、選ばれた少数の IBM Guardium 従業員 (Guardium R&D、Guardium QA、Guardium サポート・スタッフのメンバーなど) に制限されています。IBM スタッフからは使用できません。

上記の CLI ユーザー ID (cli、guardcli1、guardcli2、guardcli3、guardcli4、guardcli5) はパス・キーの仕組みを使用しません。 これらのユーザーのパスワードは完全にお客様によって管理され、IBM がそのパスワードにアクセスすることはできません。このような理由から、root パス・キーをパスワード・ボールトに保管しておき、CLI アカウント・パスワードを忘れたり紛失したりした場合でもアプライアンスにアクセスできるように備えることを IBM は推奨します。

親トピック: ステップ 4. 初期構成および基本構成の設定

すべての設定の検証

CLI からログアウトして次の構成ステップに進む前に、以下のコマンドを使用して、構成した設定をレビューして検証します。

```
show network interface all
show network routes defaultroute
show network resolver all
show system hostname
show system domain
show system clock timezone
show system clock datetime
show system ntp all
show unit type
```

親トピック: ステップ 4. 初期構成および基本構成の設定

システムのリブート

システムが最終ロケーションにない場合は、ここでシステムをシャットダウンし、最終的なネットワーク・ロケーションに配置して、再始動します。

システムをリブートする前に、インストール DVD を取り出してください。

システムを停止するには、CLI で次のコマンドを入力します。

```
stop system
```

システムがシャットダウンします。システムを最終ロケーションに移動し、システムのケーブル接続を修正し、電源を再びオンにします。システムの電源がオンになると、指定した IP アドレスまたはホスト名を使用して、(CLI および GUI から) ネットワーク経由でシステムにアクセスできるようになります。

親トピック: ステップ 4. 初期構成および基本構成の設定

ステップ 5. 次の作業

このセクションでは、インストールの検証、ライセンス・キーのインストール、および入手可能な保守パッチのインストールの各ステップについて詳しく説明します。

- インストールが成功したかどうかの検証
  インストールを検証するには、次のステップを実行します。
- ユニット・タイプの設定
  フェデレーテッド環境を設定するには、いずれかのアプライアンスを中央マネージャーとして構成し、他のすべてのアプライアンスが中央マネージャーによって管理されるように設定します。
- ライセンス・キーのインストール
  このトピックでは、Guardium のライセンス・キーをインストールして使用条件に同意する手順について説明します。
- 保守パッチのインストール (該当する場合)
  CLI または GUI を使用してパッチをインストールすることができます。
- 追加のステップ (オプション)
  次のセクションでは、ベースラインの英語を別の言語に変更する方法について説明します。これを行うには、S-TAP® エージェントをインストールし、検査エンジンを定義し、CAS エージェントをインストールします。

親トピック: Guardium システムのインストール

インストールが成功したかどうかの検証

インストールを検証するには、次のステップを実行します。

1. CLI にログインします。ssh cli@<ip of appliance>
2. GUI にログインします。https://<hostname of appliance>.<full domain>:8443 (管理ユーザー ID を使用)

リブート後の初回ログイン時に、パスワードを変更することが必要です。

Guardium の Web ベースのインターフェースにログインし、組み込みのオンライン・ヘルプで以下のタスクの詳細を参照してください。

親トピック: ステップ 5. 次の作業

ユニット・タイプの設定

フェデレーテッド環境を設定するには、いずれかのアプライアンスを中央マネージャーとして構成し、他のすべてのアプライアンスが中央マネージャーによって管理されるように設定します。

各 Guardium システムのタイプを設定するには、CLI コマンドの store unit type を使用します。

親トピック: ステップ 5. 次の作業

ライセンス・キーのインストール

このトピックでは、Guardium のライセンス・キーをインストールして使用条件に同意する手順について説明します。

始める前に

- パスポート・アドバンテージからライセンス・キーをダウンロードします。
- Guardium システムのインストールまたはアップグレードを行います。
- マシン・タイプがシステムに対して正しく設定されていることを確認します。

このタスクについて

Guardium のライセンス・キーをインストールする場合は、最初にライセンス・キーをインストールしてから、使用条件を読んで同意する必要があります。Guardium のライセンス・キーがインストールされると、ユーザー・インターフェースが再ロードされ、新しいライセンスで使用できる機能が表示されます。

Guardium システムを機能する状態にするには、基本ライセンスと 1 つ以上の追加ライセンスの両方をインストールする必要があります。基本ライセンスをインストールして使用条件に同意してから、追加ライセンスをインストールして使用条件に同意する必要があります。

Guardium のライセンス・キーについては、ライセンス・キーを参照してください。

重要:

Guardium システムをアップグレードする場合は、ライセンスを適用する必要はありません。既存のインストール済み環境に基づいて、ライセンス・キーが自動的に生成されます。ただし、Guardium システムを使用する前に、使用条件を読んで同意する必要があります。アップグレードするシステムのライセンスの使用条件を読んで同意するには、「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートして「ライセンスを読んで同意してください」をクリックします。

手順

1. `admin` ユーザーとして Guardium システムにログインします。

2. Guardium バナーに表示されている「マシン・タイプ」が、ライセンス対象のシステムに対して正しく設定されていることを確認します。 マシン・タイプは、以下のいずれかになります。
   - スタンドアロン
   - 中央マネージャー
   - アグリゲーター

   重要: 「マシン・タイプ」がアグリゲーターに設定されている状態で中央マネージャーを設定する場合は、CLI コマンドの `store unit type manager` を使用して、システムをアグリゲーターから中央マネージャーに変換してください。
3. 基本ライセンスをインストールします。
   a. 「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートします。
   b. 「ライセンス」ページの「ライセンス・キー」フィールドでシステムの基本キーを入力し、「適用」をクリックして操作を続行します。
      重要: 設定するシステムに応じて、基本コレクター・キーを適用するか基本アグリゲーター・キーを適用するかが異なります。中央マネージャー・システムを設定する場合は、基本アグリゲーター・キーが必要になります。
   c. 「ご使用条件」ダイアログで基本キーに関する使用条件を読み、条件に同意する場合は「同意する」をクリックします。 使用条件に同意すると、Guardium のインターフェースが自動的に更新されます。ただし、基本ライセンス・キーをインストールしても、使用可能な機能は変更されません。
4. 1 つ以上の追加ライセンスをインストールします。 複数の追加ライセンスを購入した場合は、ライセンスごとに以下の手順を繰り返してインストールしてください。
   a. 「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートします。
   b. 「ライセンス」ページの「ライセンス・キー」フィールドで追加キーを入力し、「適用」をクリックして操作を続行します。
   c. 「ご使用条件」ダイアログで追加キーに関する使用条件を読み、条件に同意する場合は「同意する」をクリックします。 使用条件に同意すると、Guardium のインターフェースが自動的に更新され、追加ライセンスに関連する新しい機能を使用できるようになります。
   d. インストールする追加ライセンスごとに、上記の手順を繰り返します。

次のタスク

中央マネージャーが設定されている環境の場合、「管理」 > 「一元管理」 > 「一元管理」ページで アイコンをクリックすると、中央マネージャーから管理対象ユニットに対してライセンスを配布することができます。

中央マネージャーが設定されている環境では、中央マネージャーとその管理対象ユニットで同じ共有パスワードを使用する必要があります。共有パスワードは、「設定」 > 「ツールとビュー」 > 「システム」ページで設定することも、CLI コマンドの store system shared secret を使用して設定することもできます。

親トピック: ステップ 5. 次の作業
関連概念:
ライセンス・キー

保守パッチのインストール (該当する場合)

CLI または GUI を使用してパッチをインストールすることができます。

注: フェデレーテッド環境では、保守パッチは Central Manager からすべてのアプライアンスに適用できます。

インストール・データには、保守パッチが含まれていない場合もあります。 含まれている場合は、以下の手順を実行してパッチを適用してください。

1. 前のインストール手順で定義した CLI の一時パスワードを使用して、CLI ユーザーとして Guardium® コンソールにログインします。これは、ssh クライアントを使用して実行できます。
2. 以下のいずれかを実行します。
   - ネットワーク上のロケーションからインストールする場合、次のコマンドを入力します (ftp または scp を選択)。

     ```
     store system patch install [ftp | scp]
     ```

     次のプロンプトに応答します (パッチ・ファイルの絶対パス名を指定してください)。

     Host to import patch from:

     User on <hostname>

     Full path to patch, including name:

     Password:
   - ファイル・サーバー機能を使用してインストールする場合は、次のコマンドを入力します。

     ```
     store system install patch sys
     ```

     適用するパッチを選択するよう求めるプロンプトが出されます。複数のパッチを取得するには、パス名にワイルドカードを使用します。また、パッチ名をコンマで区切ります。
3. 追加でパッチをインストールするには、ステップ 2 を繰り返します。
4. パッチが正常にインストールされたかどうかを確認するには、次の CLI コマンドを使用します。

   ```
   show system patch installed
   ```

   パッチはバックグラウンド・プロセスでインストールされます。インストールが完了するまで数分かかる場合があります。

親トピック: ステップ 5. 次の作業

追加のステップ (オプション)

次のセクションでは、ベースラインの英語を別の言語に変更する方法について説明します。これを行うには、S-TAP® エージェントをインストールし、検査エンジンを定義し、CAS エージェントをインストールします。

言語の変更

IBM Guardium のインストールは、常に英語で行われます。このベースライン言語の英語を別の言語に変更し、データベースをその言語に変換するには、CLI コマンドの store language を使用します。インストールされた Guardium システムは、日本語または中国語 (繁体字または簡体字) にのみ変更することができます。store language コマンドは、Guardium システムのセットアップ処理の一部とみなされ、このシステムの初期セットアップ中に実行されるように設計されています。 特定の言語でアプライアンスをデプロイメントした後にこの CLI コマンドを実行すると、既にキャプチャー、保管、カスタマイズ、アーカイブ、またはエクスポートされた情報が変更される可能性があります。 例えば、psmls (作成済みのペインとポートレット) は新しい言語で再作成する必要があるため、削除されます。

注: Guardium UI に言語が混合されて表示されるのを回避するには、中央マネージャーと管理対象ユニットを同じ言語に設定します。

S-TAP エージェントのインストール

S-TAP エージェントをデータベース・サーバーにインストールし、その検査エンジンを定義します。S-TAP は、データベース・サーバーにインストールされる単純なソフトウェア・エージェントです。このエージェントは、ローカル・データベースとネットワーク・データベースのトラフィックをモニターし、関連する情報を Guardium システム (コレクター) に送信します。この情報を使用して、詳細な分析、レポート作成、アラート処理が実行されます。S-TAP をインストールするには、インフォメーション・センターで S-TAP に関するセクションを参照してください。S-TAP がインストールされて Guardium システムに接続されていることを確認するには、以下の手順を実行します。

1. 管理者ポータルにログインします。
2. 以下のいずれかを実行します。

「管理」 > 「システム・ビュー」にナビゲートし、メニューで「S-TAP 状況モニター」をクリックします。アクティブなすべての S-TAP は、緑色の背景で表示されます。赤色の背景は、S-TAP がアクティブでないことを示しています。

「管理」 > 「アクティビティー・モニター」 > 「S-TAP 制御」にナビゲートし、対象の S-TAP の状況ライトが緑色になっていることを確認します。

検査エンジンの定義

ネットワーク・ベースのアクティビティー・モニター用の検査エンジンの定義

CAS エージェントのインストール

データベース・サーバーへの構成監査システム (CAS) エージェントのインストール

親トピック: ステップ 5. 次の作業

仮想イメージの作成

仮想イメージをインストールする場合は、このセクションを参照してください。

- VMware インフラストラクチャーの概要
  Guardium VM は任意の VMware 製品にインストールできますが、仮想ソリューション用のプラットフォームには VMware ESX Server が推奨されます。VMware ESX Server について、ここで紹介します。
- VM のインストールの概要
  IBM Security Guardium VM をインストールするには、ここで説明するステップに従います。VM をインストールしたら、『ステップ 3. IBM Security Guardium イメージのインストール』および『ステップ 4. 初期構成と基本構成の設定』に戻ってください。
- Hyper-V 仮想マシンの作成

親トピック: Guardium システムのインストール

VMware インフラストラクチャーの概要

Guardium VM は任意の VMware 製品にインストールできますが、仮想ソリューション用のプラットフォームには VMware ESX Server が推奨されます。VMware ESX Server について、ここで紹介します。

Guardium VM をインストールできる VMware ESX Server は、VMware インフラストラクチャーの 1 つのコンポーネントです。Guardium VM をサポートするために VMware インフラストラクチャーのすべてのコンポーネントが必要となるわけではありませんが、インストール済み環境で使用しているコンポーネントは、すべて熟知しておく必要があります。

ESX Server: このコンポーネントは、ESX Server ホストと呼ばれる物理ホスト上の VMware 仮想マシンを構成し、制御するために使用されます。Guardium VM をインストールするには、まず ESX Server ホスト上で仮想マシンを定義し、その仮想マシンに Guardium VM イメージをインストールして構成します。1 つの ESX Server に複数の Guardium VM を作成できます。

VI Client (Virtual Infrastructure Client): このコンポーネントは、スタンドアロン ESX Server または VirtualCenter Server に接続するために使用されます。VirtualCenter Server に接続する場合は、複数の ESX Server ホストに作成された複数の仮想マシンを管理できます。

Web ブラウザー: ESX Server ホストまたは VirtualCenter Server から VI Client ソフトウェアをダウンロードして使用するために使用されます。

VirtualCenter 管理サーバー (オプション): このコンポーネントは、リモートの Windows マシンで実行され、複数の ESX Server ホスト上にある複数の仮想マシンを管理するために使用できます。すべての ESX Server ホストの単一制御点として機能します。

データベース (オプション): VirtualCenter Server では、データベースを使用してインフラストラクチャーの構成情報が保管されます。VirtualCenter Server を使用しない場合、データベースは不要です。

ライセンス・サーバー (オプション): VMware インフラストラクチャーを保守するために必要なライセンスを保管し、管理します。

詳しくは、www.vmware.com にアクセスし、ESX Quick Start を検索してください。

VM のインストールの概要

IBM Security Guardium VM をインストールするには、ここで説明するステップに従います。VM をインストールしたら、『ステップ 3. IBM Security Guardium イメージのインストール』および『ステップ 4. 初期構成と基本構成の設定』に戻ってください。

VMware VirtualCenter 管理サーバー環境に複数の Guardium VM システムをインストールする場合は、最初に作成する Guardium VM からテンプレート・システムを作成し、必要に応じてそのテンプレートをコピーできます。その後は、コピーした各システムで IP アドレスを設定するだけで済みます。詳しくは、ステップ 7 の後の注を参照してください。

ステップ 1: システム互換性の検証

1. ホストが VMware ESX Server に対応していることを検証します (Guardium システムを実行するには、ESX 4.0 Update 4 以降が最低限必要です)。 詳しくは、VMware の資料「Systems Compatibility Guide for ESX Server」を参照してください (PDF 版がオンラインで提供されています)。
2. ホストにインストールされる仮想マシンが、Guardium システムに推奨最小リソースを提供できるかどうかを検証します (この場合、システムをコレクター、中央マネージャー、アグリゲーターのいずれとして使用するかは関係ありません)。この資料の『ハードウェア要件』セクションに記載している最小/推奨リソースを参照してください。
3. 64 ビット VM を初めて作成する場合、または 32 ビット VM を 64 ビットにアップグレードする場合は、仮想ハードウェアが 64 ビット操作に対応するように正しく構成されていることを確認します。場合によっては、仮想ハードウェアのアップグレード操作を実行するが必要があります。詳しくは、VMware の資料を参照してください。

ステップ 2: VMware ESX Server のインストール

VMware ESX Server をインストールします (まだインストールしていない場合)。VMware では、インストールに関する説明を Web サイトに掲載して、VMware インフラストラクチャーおよび ESX Server のインストールと構成を支援しています。

注: ESX Server は、特定のハードウェア・デバイス・セットでのみサポートされます。詳しくは、VMware Virtual Infrastructure の資料を参照してください。

ステップ 3: ネットワーク・ケーブルの接続

Guardium VM に使用する仮想スイッチを定義する前に、適切な NIC をネットワークに接続する必要があります。NIC を物理的に接続しないと、NIC を仮想ネットワークや仮想スイッチに割り当てることはできません。

Guardium VM がネットワーク・インターフェースをどのように使用するかを次の表で説明します。Guardium VM が使用するように仮想スイッチを構成する前に、この表を参照して適切に接続を行ってください。

表 1. IBM Security Guardium VM ネットワーク・インターフェースの使用

インターフェース	記述
プロキシー・インターフェース (eth0)	このインターフェースは、アプライアンスに対するメインゲートウェイであり、以下の目的で使用されます。 • ソリューションを管理し、構成し、使用するための Web ベースのグラフィカル・ユーザー・インターフェース (GUI) • 初期設定と基本構成を行うためのコマンド行インターフェース (CLI) • 外部システム (バックアップ・システム、データベース・サーバー、LDAP サーバーなど) との接続 • 他の Guardium コンポーネントとの通信。他のコンポーネントとは、他のアプライアンス (アグリゲーターや中央マネージャーなど) や、データベース・サーバーやファイル・サーバーにインストールされたエージェント (S-TAP や CAS クライアントなど) などです。
アプリケーション・サーバー・インターフェース (eth1)	このインターフェースは、Guardium システムを透過プロキシーとして構成する場合に必要となります。このインターフェースは、Guardium システムでコンテンツがマスクされるように構成されているアプリケーション・サーバーに接続します。

ステップ 4: Guardium VM 管理ポータルの構成

VMware ESX Server の新規インストール済み環境のデフォルトの構成では、VMware サービス・コンソールとすべての仮想マシンが使用する 1 つのポート・グループが作成されます。Guardium VM では、VMware コンソールや他の仮想マシンとポートを共有しないことを強くお勧めします。以下の手順に従って、Guardium VM で使用される仮想スイッチを 1 つ以上作成します。

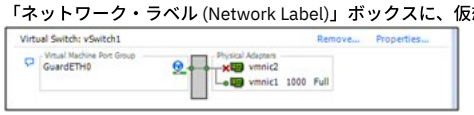
1. VMware VI Client を開き、新規の仮想マシンを作成する VirtualCenter Server または ESX Server ホストにログオンします。
2. VirtualCenter Server にログインした場合は、ナビゲーション・バーで「インベントリ (Inventory)」をクリックし、必要に応じてインベントリーを展開して、Guardium VM をインストールする管理対象ホストまたはクラスターを表示します。
3. インベントリー表示で、Guardium VM をインストールするホストまたはクラスターをクリックします。
4. 「構成 (Configuration)」タブをクリックし、「ハードウェア (Hardware)」ボックスで「ネットワーク (Networking)」をクリックし、「ネットワークの追加 (Add Networking)」をクリックします。

さまざまな目的に使用される「ネットワークの追加ウィザード (Add Network Wizard)」が開きます。

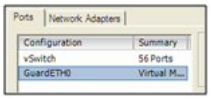
「ネットワークの追加ウィザード (Add Network Wizard)」を使用して、Guardium VM ネットワーク・インターフェース用の新しい仮想スイッチを定義します。この接続を介して、ユーザーは Guardium VM 管理コンソールにアクセスし、Guardium VM は他の Guardium コンポーネント (例えば S-TAP (後で 1 つ以上のデータベース・サーバーにインストールするソフトウェア・エージェント) など) と通信します。

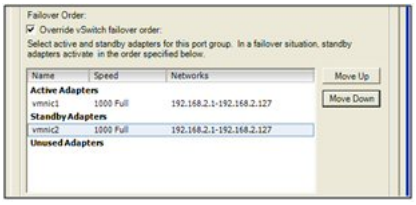
5. 「接続タイプ (Connection Types)」ボックスで、「仮想マシン (Virtual Machine)」をクリックし、「次へ (Next)」をクリックします。
6. 「ネットワーク アクセス (Network Access)」パネルで、「仮想スイッチの作成 (Create a virtual switch)」をクリックし、Guardium VM ネットワーク・インターフェースに使用する未要求ネットワーク・アダプターにマークを付けます。

7. VMware IP チーミング機能を使用して 2 次 (フェイルオーバー) ネットワーク・インターフェースを提供する場合は、オプションとして 2 番目の未要求ネットワーク・アダプターにマークを付けます。この 2 番目のアダプターは、後でスタンバイ・アダプターとして指定します (もちろん、両方の NIC を適切にケーブル接続する必要があります)。
8. 「次へ (Next)」をクリックして「ネットワークの追加ウィザード (Add Network Wizard)」の「接続設定 (Connection Settings)」ページに進みます。
9. 「ネットワーク・ラベル (Network Label)」ボックスに、仮想マシン・ポート・グループの名前 (GuardETH0 など) を入力し、「次へ」をクリックします。



10. 「サマリ (Summary)」ページで「終了 (Finish)」をクリックします。新規の仮想スイッチが「構成 (Configuration)」タブに表示されます。
11. オプション。フェイルオーバーの目的で 2 番目のアダプターを定義した場合は、(a) 作成したばかりの仮想スイッチの「プロパティ リンク (Properties link)」をクリックして仮想スイッチの「プロパティ (Properties)」パネルを開きます。(b) 「ポート (Ports)」タブをクリックし、作成したばかりの仮想ポート・グループ (GuardETH0 など) を選択し、「編集 (Edit)」をクリックします。(c) 仮想ポート・グループの「プロパティ (Properties)」パネルで、「NIC チーミング (NIC Teaming)」タブをクリックし、「vSwitch のフェイルオーバーの置き換え (Override vSwitch Failover)」ボックスにチェック・マークを付けて、2 番目のアダプターを「スタンバイ アダプタ (Standby Adapters)」リストに移動します。(d) 「OK」をクリックして仮想ポート・グループの「プロパティ (Properties)」ボックスを閉じ、「閉じる (Close)」をクリックして仮想スイッチの「プロパティ (Properties)」ボックスを閉じます。





ステップ 5: 新規仮想マシンの作成

Guardium VM をインストールする新規仮想マシンを作成します (まだ作成していない場合)。

このタスクは、VMware VI Client を使用して実行します。

1. VMware VI Client を開き、新規の仮想マシンを作成する VirtualCenter Server または ESX Server ホストにログオンします。
2. VirtualCenter Server にログインした場合は、ナビゲーション・バーで「インベントリ (Inventory)」をクリックし、必要に応じてインベントリーを展開し、新規仮想マシンを追加する管理対象ホストまたはクラスターを選択します。
3. 「ファイル」メニューで、「新規 – 仮想マシン」をクリックして「新規仮想マシン・ウィザード (New Virtual Machine wizard)」の「構成タイプ (Configuration Type)」パネルを開きます。
4. 構成タイプとして「標準 (Typical)」をクリックし、「次へ (Next)」をクリックして「名前とフォルダ (Name and Folder)」パネルに進みます。
5. 「名前とフォルダ (Name and Folder)」パネルで、以下の作業を行います。

   「仮想マシン名 (Virtual Machine Name)」フィールドに新規仮想マシンの名前を入力します。この名前は VI Client のインベントリーに表示され、仮想マシン・ファイルの名前としても使用されます。

   新規仮想マシンのインベントリーの場所を設定するには、「仮想マシン インベントリの場所 (Virtual Machine Inventory Location)」のリストからフォルダーまたはデータ・センターのルート・ロケーションを選択します。

   「次へ (Next)」をクリックします。

6. ホストまたはクラスターにリソース・プールが含まれている場合は、「リソース プール (Resource Pool)」パネルが表示されるので、仮想マシンを実行するリソース (ホスト、クラスター、またはリソース・プール) を選択する必要があります。「次へ (Next)」をクリックします。
7. 「データストア (Datastore)」パネルで、新規仮想マシン・ファイルを保管するデータ・ストアを必要に応じて選択し、「次へ (Next)」をクリックします。

8. 「ゲスト OS を選択 (Choose the Guest Operating System)」パネルで、インストールする Guardium イメージに対応するオペレーティング・システムを選択します。「バージョン」ボックスで「Linux」 > 「RedHat Enterprise Linux 6、64-bit (RedHat Enterprise Linux 6, 64-bit)」をクリックし、「次へ」をクリックします。.

   この時点でオペレーティング・システムはインストールされていませんが、仮想マシンの適切なデフォルト値を設定するには、OS タイプが必要となります。

   VM の最小リソースについては、『始める前に』セクションの『ハードウェア要件』を参照してください。

9. 「仮想 CPU (Virtual CPU)」パネルで、インストールする Guardium VM のタイプに対して推奨される CPU の数を選択し、「次へ (Next)」をクリックします。
10. 「メモリ (Memory)」パネルで、インストールする Guardium VM のタイプに対して推奨されるメモリー量を選択し、「次へ (Next)」をクリックします。重要: 初期値は 16 GB 以上にする必要があります。ユーザーが必要な範囲を超えて作業することを求めている場合は、技術サポートにお問い合わせください。
11. 「ネットワーク (Network)」パネルで、必要なポート数として「1」をクリックし、「次へ (Next)」をクリックします。
12. 選択したポートに対して、「ネットワーク (Network)」プルダウン・メニューで、仮想ネットワークでの使用のために構成したポート・グループを選択します (このポート・グループは、前の手順で定義したものです)。
13. 選択したポート・グループに対し、「パワーオン時に接続 (Connect at Power On)」チェック・ボックスにマークを付け (デフォルトでマークが付いた状態になっています)、「次へ (Next)」をクリックします。
14. 「仮想ディスク容量 (Virtual Disk Capacity)」パネルの「ディスク サイズ (Disk Size)」フィールドに、新規仮想マシン用に確保するディスク・スペースのサイズを入力します。
15. 「終了準備 (Ready to Complete)」パネルで、設定内容を確認し、「終了 (Finish)」をクリックします。

これで、新規仮想マシンの定義は完了しました。オペレーティング・システムがまだインストールされていないため、仮想マシンを始動しようとしても失敗します。

ステップ 6: Guardium システムのインストール

このタスクは、VMware Virtual Infrastructure Client を使用して実行します。

1. VMware VI Client を開き、新規の仮想マシンを作成する VirtualCenter Server または ESX Server ホストにログオンします。
2. VirtualCenter Server にログインした場合は、ナビゲーション・バーで「インベントリ (Inventory)」をクリックし、必要に応じてインベントリーを展開し、Guardium VM をインストールする仮想マシンを選択します。
3. 「サマリ (Summary)」タブで「設定の編集 (Edit Settings)」をクリックします。
4. 「CD/DVD ドライブ 1 (CD/DVD Drive 1)」をクリックします。
5. 以下のいずれかのオプションを選択して、仮想 CD-ROM/DVD デバイスが Guardium® インストール・プログラムを読み取る場所を決定します。**最初のオプションを選択することを強くお勧めします。**:

   「データストア ISO ファイル (Datastore ISO File)」 – データストア上にある Guardium インストール ISO ファイルに接続します。仮想マシンをインストールする ESX Server ホストからアクセス可能なデータ・ストアに、Guardium ISO ファイルをコピーします (まだコピーしていない場合)。「参照 (Browse)」をクリックしてファイルを選択します。

   注意: 他のオプションを選択する場合は、Guardium インストール CD/DVD を CD-ROM/DVD ドライブに挿入します。CD-ROM/DVD ドライブに Guardium インストール CD/DVD を入れた状態でシステムをリブートすると、そのシステムに Guardium がインストールされ、ホスト・オペレーティング・システムとファイルがすべて消去されます。

   「クライアント デバイス (Client Device)」 – VI Client が実行されているシステムの CD-ROM/DVD デバイスに接続します。 このオプションを選択する場合は、VI Client が実行されているシステムの CD-ROM/DVD ドライブに Guardium CD/DVD を挿入します。

   「ホスト デバイス (Host Device)」 – 仮想マシンをインストールする ESX Server ホスト・マシンの CD-ROM/DVD デバイスに接続します。このオプションを選択する場合は、ドロップダウン・メニューからデバイスを選択し、ESX Server ホスト・マシンの CD-ROM/DVD ドライブに Guardium CD/DVD を挿入します。

6. 「OK」をクリックします。
7. 「パワーオン (Power On)」をクリックして仮想マシンを始動します。
8. CD/DVD ドライブのオプションとしてクライアント・デバイスを選択した場合は、ツールバーで「仮想 CD-ROM (Virtual CD-ROM)」(ide0:0) をクリックし、接続先のローカル CD-ROM デバイスを選択します。
9. 「コンソール (Console)」タブをクリックして、仮想マシン・コンソールを表示します。インストール・プロセスでは、いくつかのプロンプトに応答する必要があります。
10. Guardium DVD を使用する場合は、このステップをスキップしてください。

    2 枚目の CD を要求するプロンプトが出されたら、ステップ 5 で選択したオプションに応じて、2 枚目の CD をドライブに挿入するか、2 番目の CD ISO イメージを選択します。Enter キーを押して続行します。CLI パスワードを求めるプロンプトが出されたら、Guardium CLI へのログイン時に使用する一時パスワードを入力します。この作業は、アプライアンスの IP 構成パラメーターを設定するために必要となります。

11. GUI 管理パスワードを要求するプロンプトが出されたら、Guardium のユーザー・インターフェースに管理ユーザーとしてログインする際に使用する一時パスワードを入力します。
12. コレクターまたはアグリゲーターを作成するかどうかを尋ねられたら、該当するタイプを選択します。
13. マスター・パスキーのプロンプトに対して、「いいえ (No)」をクリックします。

    注意: CD-ROM/DVD ドライブを使用した場合は、インストールが完了すると CD/DVD がイジェクトされます。必ずドライブからインストール CD/DVD を取り出してください。ISO ファイルを使用した場合は、必ず仮想 CD/DVD をクライアント・ドライブまたはホスト・ドライブに変更して ISO CD ROM を削除してください。そうしないと、次回リブートしたときに Guardium がホスト・マシンにインストールされ、ホスト・マシンのオペレーティング・システムとすべてのファイルが消去されます。

    マシンは自動的にリブートされ、CLI ユーザーとしてログインするように求めるプロンプトが出されます。

14. この時点で、『ステップ 4. 初期構成と基本構成の設定』に戻って、Guardium システムの構成に関する包括的な説明を参照してください。

ステップ 7: 複数の VM のインストール

(オプション) Guardium VM を複数インストールする場合は、アプライアンスごとに手順を繰り返してもかまいませんが、最初に作成した Guardium VM をコピーし、以下のステップを実行することで作業を最小限にすることができます。

1. VMware の仮想インフラストラクチャー・サーバー製品を使用して、最初に構成した Guardium VM をテンプレートにコピーします。
2. このテンプレートから、追加で構成する Guardium VM ごとにコピーを作成します。

3. 各コピーに対し、Guardium VM コンソールに一時 CLI パスワードを使用して CLI ユーザーとしてログインし、前の手順で設定した IP 構成パラメーターをすべてリセットします。必要な作業は、IP アドレスのリセット、ホスト名 (store system hostname) のリセットです。ただし、前の手順で入力した IP 構成の設定をすべて確認してください。

   ```
   store network interface ip <ip_address>
   store network interface mask <subnet_mask>
   store system hostname <host_name>
   ```

   作業が終了したら、restart network コマンドを入力します。

   ```
   restart network
   ```

   注: 複数のアプライアンスに同じ固有 ID が設定されないようにするために、ホスト名を変更するたびにアプライアンスの固有 ID が再計算されます。

親トピック: 仮想イメージの作成

Hyper-V 仮想マシンの作成

始める前に

- Hyper-V は Microsoft の仮想化ソリューションです。Hyper-V を使用する Guardium ユーザーには Hyper-V の経験があることを前提とします。 Hyper-V のインストール手順の大部分は単純で分かりやすいものです。 この Guardium ヘルプ・トピックに示されている手順は、必要以上に複雑である可能性があります。
- インストール対象の Guardium のバージョンに対するシステム要件を確認します。
- 仮想マシンの IP アドレスを予約します。

このタスクについて

手順

1. Hyper-V サーバーに管理者としてログインします。
2. Hyper-V マネージャーを「スタート」メニュー >「管理ツール」 >「Hyper-V マネージャー」で開始します。
3. Hyper-V サーバーを右クリックして、「新規」 >「仮想マシン」を選択します。
   a. 「名前」フィールドにホスト名を入力し、デフォルトの「格納」場所を使用して、「次へ」をクリックします。
   b. 「記憶メモリ」フィールドに必要メモリーを入力し、「次へ」をクリックします。 指定した RAM がご使用の Guardium バージョンの最小システム要件を満たしていることを確認します。
   a. 接続「トランク」 >「仮想ネットワーク」を選択し、「次へ」をクリックします。
   b. 「仮想ディスク」ダイアログで必要なディスク・サイズを指定し、「次へ」をクリックします。 指定した仮想ディスク・サイズがご使用の Guardium バージョンの最小システム要件を満たしていることを確認します。
   c. 「インストール オプション」の下のデフォルト設定を受け入れて、「次へ」をクリックします。
   d. 「完了」をクリックして、新しい仮想マシンを作成します。
4. 「仮想マシン」リストで新規仮想マシンを右クリックし、「接続」を選択してコンソールを開きます。
5. 緑のボタンをクリックするか、「アクション」 >「開始」を選択して仮想マシンを起動し、Mac アドレスを予約します。
6. ブート障害のプロンプト時には、グレイのボタンをクリックするか、「アクション」 >「オフにする」を選択して、仮想マシンをオフにします。
7. 「ファイル」 >「設定」を選択して、仮想マシンの構成を続行します。
   a. 「ハードウェア」 >「プロセッサー」 >「論理プロセッサー」の下で、論理プロセッサーの必要な数を指定します。 プロセッサーに指定した数が、ご使用の Guardium バージョンの最小システム要件を満たしていることを確認します。
   b. 「ハードウェア」 >「ネットワーク アダプタ」の下で割り当てられている Mac アドレスを記録します。 この情報は、インストール処理で後ほど必要になります。
   c. ネットワーク・アダプターを選択して、「削除」をクリックします。
   d. 「ハードウェア」 >「ハードウェアの追加」 >「レガシ ネットワーク アダプタ」を選択して、「追加」をクリックします。 選択は、自動的に「レガシ ネットワーク アダプタ」に移動されます。
   e. 「トランク」 >「仮想ネットワーク」を選択します。
   f. 「MAC アドレス」 >「静的」を選択し、先ほど記録した MAC アドレスを入力します。
   g. 「仮想 LAN ID を有効にする」チェック・ボックスを選択します。
   h. 「VLAN 指定」に `3xxx` と入力します。 例えば、`3156` などです。
   i. 「ハードウェア」 >「BIOS」を選択し、「レガシ ネットワーク アダプタ」を手前に上げて、「OK」をクリックします。
8. 仮想マシンの MAC アドレスを IP 予約に追加します。
9. 仮想マシンの IP アドレス、ホスト名、MAC アドレスを gmachine_list.txt に追加します。
10. 仮想マシンを始動します。 Dev-IT 管理の「OS ブート」ダイアログが表示され、タイムアウトになるまで「BOOT:」で停止し、その後、「ブート障害」プロンプトに戻ります。
11. PXE コマンドを実行し、CTRL-ALT-DEL マクロ・ボタンを使用して、仮想マシンをリブートします。 マシンを作成できます。
12. TOUCH と SU - CLI を使用して正しい IP アドレス、ルート、DNS 設定を割り当てます。 ホストおよびドメインの設定は、通常、自動的に構成されます。
13. 「SU - CLI」 >「STOP SYSTEM」を使用してシステムをシャットダウンします。
14. 仮想マシンを右クリックして、「設定」を選択します。
   a. 「レガシ ネットワーク アダプタ」をデフォルトのネットワーク・アダプターの選択に置き換えます。
   b. 「トランク」 >「仮想ネットワーク」を選択します。
   c. 「MAC アドレス」 >「静的」を選択し、先ほど記録した MAC アドレスを入力します。
   d. 「VLAN 指定」に `3xxx` と入力します。 例えば、`3156` などです。
15. 仮想マシンをブートします。

次のタスク

仮想マシンから OTIS を ping し、リモート・ホストから SSH を介して仮想マシンにログインすることで、その仮想マシンが機能することを確認します。

次に一般的な問題を示します。

- デフォルトのネットワーク・アダプターをレガシー・ネットワーク・アダプターに置き換えないと、PXE が許可されない。
- レガシー・ネットワーク・アダプターをデフォルトのネットワーク・アダプターに置き換えないと、Guardium システムがネットワーク接続なしの状態になる。
- MAC アドレスの変更前、レガシー・ネットワーク・アダプターの置き換え後にマシンを始動すると、新規 Mac アドレスと仮想アダプターが仮想マシン上に生成される。 システムを稼働させるためには、この問題に対処する必要があります。Mac アドレスを以前に記録した Mac アドレスに変更し、通常の方法で ifcfg-eth0 と 70-persistent-nework.rules をクリーンアップしてください。

親トピック: 仮想イメージの作成

カスタム・パーティション

ハード・ディスクのパーティションをカスタマイズする場合は、いくつかの選択を行う必要があります。

1. ブート画面で「カスタム・パーティションのインストール (Custom Partitioning Installation)」を選択します。
   「カスタム・レイアウトの作成 (Create custom layout)」を選択し、以下の表に記載されている推奨パーティション・スキームを使用します。
   注: オペレーティング・システムをメモリーにロードする特殊なプログラムであるブート・ローダーは、すべてのカスタム・パーティションのインストールに含まれています。
2. カスタム・レイアウトを作成します。この場合、ディスク上に既存のパーティションが存在しています。これらのパーティションは削除しないでください。必要なパーティションをディスク上の既存のパーティションに追加するには、「カスタム・レイアウト (custom layout)」を選択してください。以下の表に、カスタム・レイアウトの推奨値を示します。

表 1. カスタム・レイアウトの推奨値

パーティション	値
/	25 GB
スワップ・パーティション	RAM サイズの半分
/boot	5 GB
/var	残りすべて

すべての使用可能なドライブも、この画面に表示されます。パーティション化用のドライブを選択してから、インストールを実行してください。

パーティショニングが完了すると、Guardium® システム・ソフトウェアが自動的にインストールされます。

ディスク上の空きスペースを超える値が作成された場合は、エラー・メッセージが表示されます。

「OK」をクリックしてシステムをリブートし、「カスタム・パーティション (Custom Partitioning)」の最初に戻ります。

Red Hat ディストリビューションでのパーティションの処理方法について詳しくは、Red Hat Enterprise Linux の資料を参照してください。

親トピック: Guardium システムのインストール

暗号化された LVM によるパーティション化の方法

暗号化されたディスクを使用する場合は、以下の手順を実行して、論理ボリューム / と /var を含む暗号化された LVM ボリュームを作成します。

暗号化された LVM をインストールする場合、暗号鍵の入力を要求されます。その後、リブートのたびにこの暗号鍵を入力して、LVM ボリュームのロックを解除する必要があります (そのため、コンソールを使用してアプライアンスに物理的にアクセスするか、リモートからアクセスする必要があります)。

重要 – 暗号鍵をなくした場合は復元できないため、安全な場所に保管しておく必要があります。

注: オペレーティング・システムをメモリーにロードする特殊なプログラムであるブート・ローダーは、カスタム・パーティションのインストールに含まれています。このトピックの最後に、サンプルのパスワード入力画面を示します。

1. IBM Guardium の DVD を挿入してマシンをブートします。
2. ブート画面で「カスタム・パーティションのインストール (Custom Partition Installation)」を選択します。
3. Enter キーを押します。
4. 最初の RedHat Enterprise Linux 画面で、「すべてのパーティションを削除してデフォルトのレイアウトを作成 (Remove all partitions and create default layout)」をクリックします。 また、「システムの暗号化 (Encrypt system)」チェック・ボックスと「パーティション・レイアウトの確認と変更 (Review and modify partitioning layout)」チェック・ボックスも選択します。
5. 「次へ」をクリックします。
6. 次の画面に、本当にすべてのパーティションを削除するのかを尋ねる警告メッセージが表示されます。「はい」をクリックします。
7. 次の画面で「LogVol00」をクリックし、次に「編集」をクリックすると、「LVM ボリューム・グループの編集 (Edit LVM Volume Group)」ダイアログが表示されます。
8. 前の画面のリストで「LogVol00」をクリックし、次に「編集」をクリックします。
9. 次の画面で、サイズを 10240 に変更して「OK」をクリックします。
10. 次の画面のリストで「LogVol01」をクリックし、次に「編集」をクリックします。
11. システムにインストールされているメモリーの半分のサイズのスワップ・パーティションを割り振ります。このスワップ・パーティションのサイズを指定して「OK」をクリックします。
12. 「追加」をクリックします。「論理ボリュームの作成 (Make Logical Volume)」ダイアログが表示されます。
13. マウント・ポイントとして /var を指定し、残っているサイズをシステムに自動的に設定させます。
14. 各パーティションのサイズを確認します。次に「OK」クリックします。
15. 次に、「LVM ボリューム・グループの編集: VolGroup00 (Edit LVM Volume Group: VolGroup00)」ダイアログで「OK」をクリックします。
16. 次の画面で「次へ」をクリックします。パスフレーズ・ダイアログが表示されます。
17. 任意のパスフレーズを「パスフレーズの入力 (Enter passphrase)」フィールドに入力し、同じパスフレーズを「パスフレーズの確認 (Confirm passphrase)」フィールドに入力します。「OK」をクリックします。
    注: このパスフレーズは、システムをブートするたびに入力する必要があります。LVM のパスフレーズを紛失した場合、復旧することはできません。

ブート・ローダーの構成ダイアログが表示されます。Red Hat Enterprise Linux が使用可能になっているコンピューターを起動すると、ブート・ローダーと呼ばれる特殊なプログラムにより、オペレーティング・システムがメモリーにロードされます。通常、ブート・ローダーはシステムのプライマリー・ハード・ディスク (または他のメディア・デバイス) 上に存在し、Linux カーネルおよびその必須ファイルまたは (場合によっては) 他のオペレーティング・システムをメモリーにロードします。それ以外の処理は実行しません。

ほとんどの場合、デフォルトのオプションをそのまま使用して問題ありませんが、場合によっては、デフォルトのオプションを変更しなければならないことがあります。

18. この画面で「次へ」をクリックします。暗号化インストールが開始されます。

    このインストール中とその後のリブート時に、LVM の LUKS (Linux Unified Key Setup) パスフレーズの入力をブート中に要求されます。LUKS パスフレーズを入力すると、システムによってブート・プロセスが実行されます。

親トピック: Guardium システムのインストール

SAN 構成の例

この付録では、ハード・ディスクの事前パーティション化 (SAN をインストールする場合に必要) を行うために、コマンド・プロンプトに移動して実行する手順について説明します。

最初に SAN ストレージ・デバイス上のスペースをパーティション化してから、IBM Security Guardium OS をインストールします。このインストール用のハード・ディスクを 1 つ選択してください。

注: 使用する SAN ハードウェアにより、実際の手順が異なる場合があります。SAN へのインストールはサポートされていますが、NAS へのインストールはサポートされていません。

ステップの要約

1. システム・セットアップに入り (初期ブート時に IBM® サーバーで F1 キーを押す)、開始オプションを変更して、ブート元となる適切な PCI スロット (QLogic カードが挿入されているスロット) を選択します。
2. QLogic BIOS のロード中に Ctrl-Q を押して QLogic カードの BIOS を変更し、ブート・デバイスとして使用可能にします。 次に、ブート・デバイスの LUN (論理装置番号) を選択します。
3. RedHat 5.8 の DVD からブートし、fdisk を実行するために Rescue モードに入り、以下の表の仕様を参照して、SAN デバイス上にパーティションを作成します。

   表 1. SAN デバイス上のパーティション

パーティション	スペース
1	/boot 用に 500 MB
2	システム・メモリーの量 + 4 GB
3	/ 用に 25 GB
4	/var 用に残りすべてのスペース

   注: RedHat のインストール・プロセスでは、パーティションを作成して OS をロードできますが、fdisk を使用してパーティションを事前に作成しておかないと、インストール後にシステムが正しくブートされません。
4. これまでに定義したパーティションを使用して、OS のインストールを実行します (/dev/sda デバイスのみ使用してください)。
5. システムをリブートし、残りのインストール手順 (ホスト名の指定や IP の構成など) を完了します。

注:

SAN 環境では、SAN 上のネットワーク・スイッチ内の冗長パスが原因で、単一の LUN が複数のデバイスとして RedHat 5.8 に示されます。(SDD ストレージは 8 個のデバイスでした)。

これは SAN ストレージ・ブランド/タイプの機能で、各サイトでこのように構成されます。

IBM Guardium のインストール済み環境で認識されている既存のパーティションのみを編集することが非常に重要です。そのためには、マウント・ポイントを追加してファイル・システム (ext4 または swap) を設定します。サイズなど、他の設定は変更しないでください。また、OS のロード先となるデバイスを選択する際に、/dev/sda 以外のデバイスは、すべて選択を解除してください。

fdisk の実行手順

RedHat のレスキュー・モードで fdisk を実行して SAN ストレージの事前パーティション化を行うには、以下の手順を実行します。

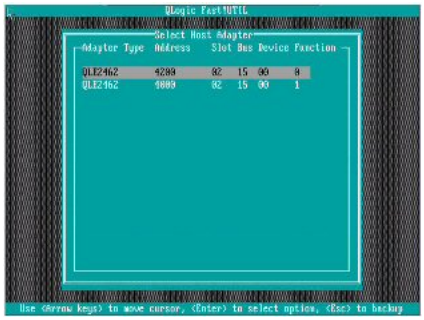
1. `fdisk /dev/sda` と入力します (サーバーに接続されているストレージが SAN だけであると想定)。デバイス全体での処理に関する警告が表示された場合は、`y` を入力します。
2. 新しいパーティションとして `n` を入力します。
3. プライマリー・パーティションとして `p` を入力します。
4. パーティション #1 として `1` を入力します。
5. Enter キーを押して、デフォルトの開始位置を受け入れます。
6. `+512M` と入力して、パーティション #1 のサイズを 500MB に設定します (これが /boot パーティションになります)。
7. 新しいパーティションとして `n` を入力します。
8. プライマリー・パーティションとして `p` を入力します。
9. パーティション #2 として `2` を入力します。
10. Enter キーを押して、デフォルトの開始位置を受け入れます。
11. `+12288M` と入力して、パーティション #2 のサイズを 12GB に設定します (物理 RAM のサイズを 8GB と仮定した場合)。推奨サイズは、物理 RAM に 4GB を加算した値です (これがスワップ・パーティションになります)。
12. 新しいパーティションとして `n` を入力します。
13. プライマリー・パーティションとして `p` を入力します。
14. パーティション #3 として `3` を入力します。

15. Enter キーを押して、デフォルトの開始位置を受け入れます。
16. `+10240M` と入力して、パーティション #3 のサイズを 10 GB に設定します。
17. 新しいパーティションとして `n` を入力します。
18. プライマリー・パーティションとして `p` を入力します (デフォルトでパーティション #4 になります)。
19. Enter キーを押して、デフォルトの開始位置を受け入れます。
20. Enter キーを押して、残りのすべてのスペースを割り当てます (これが /var パーティションになります)。
21. `w` と入力して、パーティション・テーブルを SAN に書き込みます。
22. `exit` と入力してレスキュー・モードを終了し、システムをリブートしてカスタム・パーティションのインストールを開始します (ステップ 3: IBM Security Guardium イメージのインストール)。

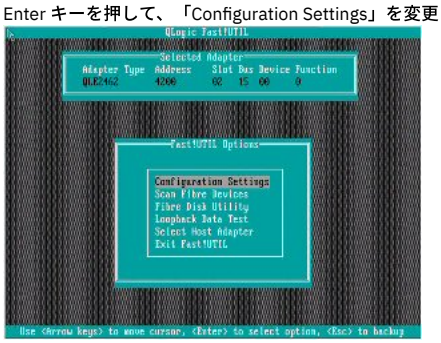
QLogic のセットアップ画面のサンプル・スクリーン・ショット

以下の Q-Logic 画面は、必要な手順を示す代表的な画面です。 他のファイバー・チャネル・カードも使用できます。

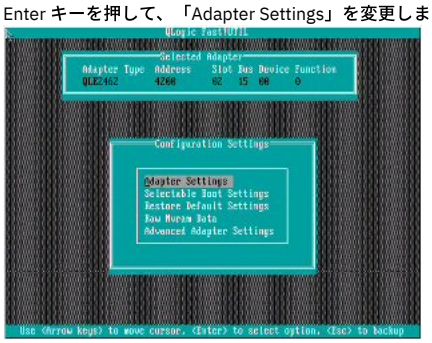
1. CTRL+D を押して、QLogic カードの BIOS を変更します。構成セットアップ・ユーティリティーに入るようにプロンプトが表示された場合に Ctrl+Q を押すと、最初に以下の画面が表示されます。これは 2 ポート・カードです。適切なポートを選択して、Enter キーを押します。



2. Enter キーを押して、「Configuration Settings」を変更します。



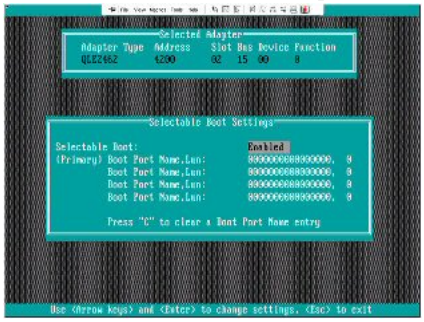
3. Enter キーを押して、「Adapter Settings」を変更します。



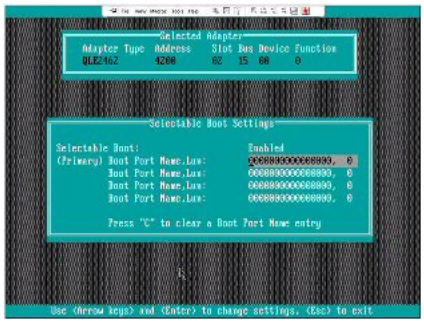
4. 矢印キーを使用して「Host Adapter BIOS」を選択し、Enter キーを押して「Enabled」に切り替えます。

5. Esc キーを押して前の画面に戻り、下矢印キーを使用して「Selectable Boot Settings」を選択し、Enter キーを押します。

6. Enter キーを押して、「Selectable Boot」を「Enabled」に変更します。



7. 最初の「Boot Port Name, LUN」を選択し、Enter キーを押して LUN のリストを表示します。正しいカード/ポートが構成されていれば、ここで LUN 番号が表示されます。リストの先頭に表示されている LUN を選択します。



8. 「Reboot」と表示されている画面に戻るまで Esc キーを押し、「Reboot」を選択してシステムをリブートします。これで、IBM Security Guardium をインストールする準備ができました。

親トピック: Guardium システムのインストール

Guardium システムのアップグレード

ここでは、IBM Security Guardium システムを最新の V10 オファリングにアップグレードする方法について説明します。

アップグレードを開始する前に、アップグレードの計画、アップグレード方法の選択、およびアップグレード中の混合バージョン環境の各セクションを参照してください。

さらに、アップグレード操作をサポートするために、次のリソースを使用できます。

- IBM Security Guardium high-level upgrade roadmap: Guardium の各種リリースからのサポートされるアップグレード・パスの概要について説明しています。
- IBM Guardium V10.1 Software Appliance Technical Requirements: 物理マシンと仮想マシンの両方のインストールに関するハードウェア要件について説明しています。
- Hints and tips on upgrading to V10: アップグレードの計画、実行、およびトラブルシューティングに関する情報をビデオで提供しています。

- アップグレードの計画
  ここでは、各種のアップグレード・シナリオについて説明し、 最小限のダウン時間で Guardium システムをアップグレードするための適切な方法を判別します。
- 共通アップグレード・タスク
  システム・データのパージ、インストールのモニター、アップグレード後のクリーンアップなどのタスクは、すべての Guardium アップグレード・シナリオに共通しています。
- 32 ビット環境のアップグレード
  バックアップ中央マネージャーを使用せずに、32 ビットの Guardium 環境をアップグレードします。
- 64 ビット環境のアップグレード
  バックアップ中央マネージャーを使用せずに、64 ビットの Guardium 環境をアップグレードします。
- バックアップ中央マネージャーを使用した 32 ビット環境のアップグレード
  バックアップ中央マネージャーを使用して、32 ビットの Guardium 環境をアップグレードします。
- バックアップ中央マネージャーを使用した 64 ビット環境のアップグレード
  バックアップ中央マネージャーを使用して、64 ビットの Guardium 環境をアップグレードします。

アップグレードの計画

ここでは、各種のアップグレード・シナリオについて説明し、 最小限のダウン時間で Guardium システムをアップグレードするための適切な方法を判別します。

- アップグレード方法の選択
  Guardium をアップグレードするための最良の方法は、アップグレード元のバージョン、ご使用のシステムのハードウェア、特別なパーティショニング要件 (存在する場合) などの複数の要因によって異なります。
- アップグレード中の混合バージョン環境
  アップグレード中に、Guardium 環境は、機能が制限される混合バージョンの状態になります。
- 中央マネージャーおよびアグリゲーターでのアップグレード
  トップダウン・アップグレード方式に従うことにより、ご使用の Guardium 環境への悪影響を最小限に抑えます。

親トピック: Guardium システムのアップグレード

アップグレード方法の選択

Guardium をアップグレードするための最良の方法は、アップグレード元のバージョン、ご使用のシステムのハードウェア、特別なパーティショニング要件 (存在する場合) などの複数の要因によって異なります。

メイン・ユーザー・インターフェースの アイコンをクリックして「Guardium バージョン情報」を選択することによって、 現在の Guardium バージョンおよびパッチ・レベルを判別します。

以下のいずれかの方法を使用して、最新バージョンの Guardium にアップグレードします。

アップグレード・パッチ
: アップグレード・パッチを使用して、管理対象環境内のすべてのシステムをアップグレードします。新しい UI アーキテクチャーのため、UI カスタマイズは例外となりますが、アップグレード・パッチはすべてのデータおよび構成を保持します。デフォルトのパーティションを使用する 64 ビット環境には、バックアップ中央マネージャーを定義せずにアップグレード・パッチを使用することをお勧めします。

バックアップ、再ビルド、リストア
: バックアップ、再ビルド、およびリストアの方法を使用します。これには、システムのフルバックアップ、最新 ISO からのシステムの再ビルド、バックアップからのシステム・データおよび構成のリストアが必要になります。カスタム・パーティションを使用する 32 ビットの環境またはシステムには、バックアップ中央マネージャー付きでバックアップ、再ビルド、およびリストアを使用する方法をお勧めします。

重要: カスタム・パーティションを使用するシステムは、アップグレード・パッチを使用して V10 にアップグレードすることはできません。代わりに、バックアップ、再ビルド、およびリストアの方法を使用する必要があります。システムのパーティションについて不確実な点がある場合は、Health Check p9997 をダウンロードしてインストールしてください。結果のパッチ・ログに、システムのパーティションに関する情報が含まれます。

以下の表を使用して、ご使用のシステムを最新バージョンの Guardium にアップグレードするための最良の方法を判別します。

表 1. アップグレード方法の判別

Guardium システム	**V10 へのアップグレード方法**	
	V9 のバックアップ、最新の V10 へのシステムの再ビルド、V9 バックアップからのリストア	**最新の V10 アップグレード・パッチの適用**
V9 パッチ 600 (64 ビット) 以降	はい	はい
V9 パッチ 600 (32 ビット) 以降	はい	いいえ
V9.0 パッチ 600 未満	はい	いいえ
V8.2 以前	いいえ	いいえ

表 2. V10 アップグレード・パスの概要

現行システムの Guardium レベル	**最新の V10 へのアップグレード・パス**
V8.2	V8.2 システムを V10 システムに直接アップグレードすることはできません。最新の V9 (64 ビット) ISO を使用してアプライアンスを再ビルドしてから、最新の V9 から V10 へのアップグレード・パッチをインストールする必要があります。 1. V8.2 のシステム・バックアップを作成します。 2. 最新の V9 (64 ビット) ISO を使用してアプライアンスを再ビルドします。 3. V9 パッチ 600 以降 (64 ビット) の GPU をインストールします。 4. 元の V8.2 システムからシステム・バックアップをリストアします。 注: コレクターについては、次のステップに進む前に、対応するすべての S-TAP を最新の V9 にアップグレードします。 5. ヘルス・チェック p9997 をインストールします。 6. V9 (64 ビット) のシステム・バックアップを作成します。 7. 最新の V9 から V10 へのアップグレード・パッチをインストールします。
V9 (32 ビット)	1. V9 (32 ビット) のシステム・バックアップを作成します。 2. 最新の V10 (64 ビット) ISO を使用してアプライアンスを再ビルドします。 3. V10 パッチ 100 以降の GPU を適用します。 4. 元の V9 (32 ビット) システムからシステム・バックアップをリストアします。

現行システムの Guardium レベル	最新の V10 へのアップグレード・パス
V9 パッチ 600 (64 ビット) 未満	1. V9 (64 ビット) のシステム・バックアップを作成します。 2. V9 パッチ 600 以降 (64 ビット) の GPU をインストールします。 3. V9 (64 ビット) のシステム・バックアップを作成します。 4. ヘルス・チェック p9997 をインストールします。 5. 最新の V9 から V10 へのアップグレード・パッチをインストールします。
V9 パッチ 600 (64 ビット) 以降	1. ヘルス・チェック p9997 をインストールします。 2. V9 (64 ビット) のシステム・バックアップを作成します。 3. 最新の V9 から V10 へのアップグレード・パッチをインストールします。
V10	1. 最新の V10 GPU を適用します。

親トピック: アップグレードの計画
関連概念:
32 ビット環境のアップグレード
バックアップ中央マネージャーを使用した 32 ビット環境のアップグレード
64 ビット環境のアップグレード
バックアップ中央マネージャーを使用した 64 ビット環境のアップグレード

アップグレード中の混合バージョン環境

アップグレード中に、Guardium 環境は、機能が制限される混合バージョンの状態になります。

すべてのシステム (中央マネージャー、アグリゲーター、およびコレクター) とすべての S-TAPs において、アップグレード・プロセスを同時に完了することはできないため、Guardium 環境は、アップグレード中に混合バージョンの状態になります。例えば、中央マネージャーを最新の V10 にアップグレードした後も、管理対象ユニットは V9 GPU 600 で動作を続行します。混合バージョン環境はサポートされますが、すべてのアップグレード計画の一環として、いくつかの制限事項を考慮する必要があります。例えば、データ収集、データ・アセスメント、およびポリシー (いくつかの制限事項あり) は混合モードでも引き続き機能しますが、新機能と拡張機能は混合環境では機能しません。

重要: ご使用の環境全体を、可能な限り迅速に最新のパッチ・レベルである V10 にアップグレードしてください。アップグレード中に混合バージョン環境で操作する際には、以下の点に注意してください。

- 環境全体が最新の V10 にアップグレードされるまで、Guardium のすべての機能を使用することはできません。
- 混合バージョン環境での操作時には、構成を変更しないでください。
- Guardium V10 は、V9 GPU 600 未満の管理対象ユニットがある混合環境をサポートしません。

構成および設定の配布
V10 中央マネージャーと V9 パッチ 600 以降の管理対象ユニットの間では、構成の配布はサポートされません。この制限には、以下が含まれます。

- V10 中央マネージャーから V9 パッチ 600 の管理対象ユニットにポリシーを配布することはできません。アップグレード前に管理対象ユニットに既にインストール済みのポリシーは変更されません。
- パッチ・バックアップ設定は、V10 中央マネージャーから V9 パッチ 600 以降の管理対象ユニットに配布することはできません。アップグレード前に定義されたパッチ・バックアップ設定は変更されません
- V9 (パッチ 600 以降) の管理対象ユニットがある V10 中央マネージャーでは、UI レイアウトのカスタマイズおよび配布はサポートされません。

管理対象ユニット
中央マネージャーを V10 にアップグレードした後は、V9 パッチ 600 以降の管理対象ユニットを追加登録できません。アップグレード前に登録されたユニットは、アップグレード後も登録されたままになります。

クイック検索
Quick Search for Enterprise は、V10 中央マネージャーおよび V9 パッチ 530 以降の管理対象ユニットで構成される混合環境で機能します。Quick Search for Enterprise を再初期化するために、ユーザー・インターフェースを再始動する必要があります。GPU 500 より前の管理対象ユニットは、Enterprise Search を利用できません。ただし、ローカル・クイック検索は引き続き使用可能です。
中央マネージャーが V9 から最新の V10 にアップグレードされ、管理対象ユニットが V9 のままである場合は、管理対象ユニットが V10 にアップグレードされるまで、V9 管理対象ユニットでクイック検索は無効になります。

レポート
一部のレポートを V9 パッチ 600 以降の管理対象ユニットで表示すると、SQL エラーが発生するか、以下のデータが正しく表示されない場合があります。

- 統合/アーカイブ・ログ
- 隔離された接続
- インストール済みのパッチ
- 非アクティブな検査エンジン
- S-TAP 検査
- 接続プロファイル・リスト
- リプレイ統計
- リプレイ・サマリー

エンタープライズ・バッファー使用状況モニター のデータを除き、V9 パッチ 600 以降の管理対象ユニットからのデータは、V10 中央マネージャー上の次のレポートではアクセスできません。

- エンタープライズ S-TAP 検査
- エンタープライズ・ロード・バランシング・イベント

親トピック: アップグレードの計画

中央マネージャーおよびアグリゲーターでのアップグレード

トップダウン・アップグレード方式に従うことにより、ご使用の Guardium 環境への悪影響を最小限に抑えます。

つまり、最初に 1 つの上位システムをアップグレードしてからそのシステムに従属するシステムまたはエージェントをアップグレードした後に、次の上位システムをアップグレードしてからそのシステムに従属するシステムまたはエージェントをアップグレードする、という方法で進めていきます。この方式を使用すると、混合バージョンの Guardium 環境の運用による影響を最小限に抑えられます。

トップダウン方式で行う必要がある理由は、アップグレードされたアグリゲーターは以前のリリースのデータを集約できますが、 以前のアグリゲーターは新しいリリースのデータを集約できないためです。同様に、アップグレードされた中央マネージャーは以前のリリースを実行しているユニットを管理できますが、管理対象ユニットがアップグレードされて中央マネージャーと整合するまで、管理対象ユニットは一部の機能を使用できません。

この問題を回避するには、中央マネージャーをアップグレードしてからその管理対象ユニットをアップグレードします。複数の中央マネージャーが存在する場合は、 最初に 1 つの中央マネージャーをアップグレードしてからその管理対象ユニットをアップグレードした後に、次の中央マネージャーとその管理対象ユニットのアップグレードに進みます。

同様に、1 つのアグリゲーターをアップグレードした後に、そのアグリゲーターにデータをエクスポートするユニットをアップグレードしてください。複数のアグリゲーターが存在する場合は、 最初に 1 つのアグリゲーターをアップグレードしてからそのアグリゲーターに従属するコレクターをアップグレードした後に、次のアグリゲーターとそのコレクターのアップグレードに進みます。

最後に、1 つのコレクターをアップグレードした後に、そのコレクターに登録された S-TAPs をアップグレードします。1 つのコレクターおよびそのコレクターに登録されたすべての S-TAPs をアップグレードした後に、次のコレクターおよびその S-TAPs のアップグレードに進みます。

この方式を使用すると、すべての中央マネージャーまたはアグリゲーターをアップグレードしてからすべてのコレクターをアップグレードする場合と比べて、ご使用の環境の各ブランチでのシステム (中央マネージャーからアグリゲーター、コレクター、および S-TAPs まで) の互換性がより迅速に確保されます。

親トピック: アップグレードの計画

共通アップグレード・タスク

システム・データのパージ、インストールのモニター、アップグレード後のクリーンアップなどのタスクは、すべての Guardium アップグレード・シナリオに共通しています。

- システム・データのパージ
  Guardium システムから不要なデータをパージすると、アップグレード・プロセスを大幅に迅速化することができます。
- パッチのインストール、配布、およびモニター
  アップグレードを開始する前に、パッチをアップロードしてインストールする方法、パッチのインストールのモニター方法、およびインストールが成功したかどうかを検証する方法について把握しておくと役立ちます。
- diag を使用したインストール進行状況のトラッキング
  `diag` コマンドを使用して、アップグレード・ログにアクセスし、アップグレードの進行状況をトラッキングします。
- アップグレード後の検査およびクリーンアップ
  アップグレードが正常に完了したことを確認し、アップグレード後のメンテナンスを実行します。

親トピック: Guardium システムのアップグレード

システム・データのパージ

Guardium システムから不要なデータをパージすると、アップグレード・プロセスを大幅に迅速化することができます。

このタスクについて

最適なパフォーマンスを得るために、また大量のデータのアップグレードに付随するリスクを最小限に抑えるために、不要なシステム・データをパージして、内部データベースの使用率を 20% 未満にしてください。

手順

1. 「管理」 > 「データ管理」 > 「データ・アーカイブ」を開きます。
2. 「パージ」チェック・ボックスをクリックしてパージ操作を定義します。
   重要: 「データ・アーカイブ」のパージ構成に対する変更は、 データ・エクスポートのパージ構成にも適用されます。
3. 「次の期間を経過したデータをパージ」の期間を定義します。 指定した日数、週数、または月数より古いすべてのデータがシステムからパージされます。
4. 「エクスポートまたはアーカイブなしのパージを許可」チェック・ボックスをクリックします。
5. 「保存」をクリックして、構成変更を保存します。
6. 「今すぐ 1 回実行」をクリックし、 パージ操作を実行して古いシステム・データをパージします。

次のタスク

「管理」 > 「レポート」 > 「アクティビティー・モニター」 > 「スケジュール済みジョブ」を開き、 データ・アーカイブ・ジョブの状況をモニターします。

親トピック: 共通アップグレード・タスク

パッチのインストール、配布、およびモニター

アップグレードを開始する前に、パッチをアップロードしてインストールする方法、パッチのインストールのモニター方法、およびインストールが成功したかどうかを検証する方法について把握しておくと役立ちます。

scp を使用したパッチのインストール

Guardium 環境のアップグレード時に、中央マネージャーおよび管理対象ユニットにパッチをアップロードしてインストールするには、いくつかの方法があります。

重要: ZIP 形式でダウンロードしたパッチは、アップロードおよびインストールの前に Guardium システム外部で unzip しておく必要があります。データベース構造の変更を伴うパッチについて以下の制約事項に注意してください。

- 負荷の高いレポート、監査プロセス、バックアップ、インポートなどの長期実行プロセスとの競合を避けるために、パッチのインストールは Guardium システムの負荷が低い時間に実行またはスケジュールしてください。
- パッチ・インストールの正確な所要時間は、データベース使用状況、データ分布などの考慮事項によって異なります。
- パッチのインストールはトップダウン方式、つまり最初に中央マネージャーにパッチを適用してから、アグリゲーターに適用し、最後にコレクターに適用してください。

`scp` を使用してパッチをアップロードしてインストールするには、CLI コマンドの `store system patch install scp` を実行します。

アップロードが完了すると、パッチのインストールを続行するよう自動的にプロンプトが出されます。

fileserver を使用したパッチのインストール

Guardium ファイル・サーバーを使用してパッチをアップロードしてインストールするには、以下の手順に従います。

1. CLI コマンドの `fileserver [ip_address]` を使用して、ファイル・サーバーを初期化します。ここで、`[ip_address]` は、Guardium システムに接続するために使用されるシステムです。
2. Web ブラウザーから、Guardium システムに接続します。
    a. 「パッチのアップロード (Upload Patch)」をクリックします。
    b. パッチ・ファイルを参照して選択し、「アップロード」をクリックします。
3. CLI コマンドの `store system patch install system` を実行してパッチをインストールします。

パッチの配布

中央マネージャーから管理対象ユニットにパッチを配布するには、以下のいずれかが行われている必要があります。

- 中央マネージャーにパッチがインストールされている
- CLI コマンドの `store system patch available` を実行して、中央マネージャー上でパッチが使用可能になっている

中央マネージャーの「一元管理」ページを使用して、管理対象ユニットにパッチを配布します。「管理」 > 「一元管理」 > 「一元管理」にナビゲートし、「パッチ配布」をクリックします。

パッチ・インストールのモニターおよび検証

以下の方法で、パッチのインストールをモニターおよび検証できます。

- CLI コマンドの `show system patch install` を実行します。
- CM の「一元管理」ページを使用します (「管理」 > 「一元管理」 > 「一元管理」 > 「パッチ・インストール状況」)。

重要: Guardium システムを V10 にアップグレードすると、V9 のパッチは使用できなくなります。
親トピック: 共通アップグレード・タスク

diag を使用したインストール進行状況のトラッキング

`diag` コマンドを使用して、アップグレード・ログにアクセスし、アップグレードの進行状況をトラッキングします。

手順

1. Guardium システムの CLI にログインします。
2. `diag` コマンドを実行します。
3. `diag` コマンド・メニューで、以下を行います。
    a. 「1 Output management」を選択し、「OK」をクリックします。
    b. 「3 Export recorded files」を選択し、「OK」をクリックします。
    c. 必要なログ・ファイルを選択し、「OK」をクリックします。
    d. 「1 FTP」または「2 SCP」を選択し、「OK」をクリックします。
    e. アップロード先のホスト名を入力し、「OK」をクリックします。
    f. ユーザー名を入力し、「OK」をクリックします。
    g. パスワードを入力し、「OK」をクリックします。
    注: 「2 SCP」を選択した場合は、パスワードの前に、宛先パスを要求されます。
    h. 宛先パスを入力し、「OK」をクリックします。
    i. 情報を確認し、「OK」をクリックします。 ファイルがターゲット・システムにアップロードされます。
    j. 「OK」を選択して終了します。
    k. 「3 Exit」を選択し、「OK」をクリックします。
    注: 別のファイルをアップロードする必要がある場合は、**3a** に戻ります。必要ない場合は、次のステップに進みます。
    l. 「5 Exit to CLI」を選択し、「OK」をクリックします。

親トピック: 共通アップグレード・タスク

アップグレード後の検査およびクリーンアップ

アップグレードが正常に完了したことを確認し、アップグレード後のメンテナンスを実行します。

手順

1. アップグレード・パッチを使用してアップグレードした場合は、CLI ユーザーとしてログインして、 コマンド `show upgrade-status` を実行します。 このコマンドにより、アップグレード・プロセスの状況に関する詳細な情報が出力され、出力の最終行に「`INFO:Migration Complete`」というメッセージが表示されます。
2. 中央マネージャーをアップグレードした場合は、「管理」 > 「一元管理」 > 「一元管理」ページに管理対象ユニットが表示されていることを確認します。
3. 以前のバージョンの Guardium で作成したカスタム・レポートを 「レポート」 > 「マイ・カスタム・レポート」で使用できることを確認します。

   「マイ・カスタム・レポート」には、新規に作成したレポートと、以前のバージョンの Guardium で変更した事前定義レポートがすべて含まれているはずです。

4. アップグレードされた管理対象ユニットにライセンスを配布できるように、「一元管理」ページですべての管理対象ユニットをリフレッシュします。
5. アップグレード手順またはリストア手順の後に Guardium DPS ファイルを更新する必要がある場合があります。最新の DPS ファイルをダウンロードしてから、「強化」 > 「脆弱性評価」 > 「カスタム・アップロード」ツールを使用し、 新しい DPS ファイルをアップロードしてインポートします。
6. アップグレード手順またはリストア手順の実行前にアップロードした会社ロゴを再ロードする必要がある場合があります。カスタマー・ロゴを再ロードするには、以下のステップを実行します。
   a. 管理ユーザーとしてログインします。
   b. 「設定」 > 「ツールとビュー」 > 「グローバル・プロファイル」にアクセスします。
   c. 会社ロゴ・ファイルを参照します。
   d. ロゴ・ファイルをアップロードします。
7. CLI コマンド show gui csrf_status および show gui xss_status を使用して、クロスサイト・リクエスト・フォージェリー (CSRF) サービスおよびクロスサイト・スクリプティング (XSS) サービスの状況を確認します。

親トピック: 共通アップグレード・タスク

32 ビット環境のアップグレード

バックアップ中央マネージャーを使用せずに、32 ビットの Guardium 環境をアップグレードします。

バックアップ中央マネージャーを使用せずに、ISO を介して 32 ビットの Guardium 環境をアップグレードする前に、以下のチェックリストを確認して各項目を完了してから、アップグレードを試行してください。

重要: V10 システムで `restore db` を実行する前に、システムが V10 にビルドされた後に最新の保守パッチを適用します。32 ビットのコレクター・ベースの中央マネージャーを使用している場合、V10 にアップグレードする前に、64 ビットのコレクター・ベースの中央マネージャーにビルドし直す必要があります。

アップグレード・チェックリスト

- Fix Central から最新のヘルス・チェック・パッチ (p9997) をダウンロードします。詳しくは、「Guardium health check patch release notes」を参照してください。
- 現行システムでは、 Guardium V9 および 32 ビット・アーキテクチャーを使用する必要があります。
- 最新の Guardium V9 リリースをダウンロードするか、後でこれを Fix Central から入手します (オプション)。
- パスポート・アドバンテージからの最新の Guardium V10 ISO のダウンロード
- パスポート・アドバンテージからのすべての基本ライセンスおよび追加ライセンスのダウンロード
- Fix Central から最新の V10 GPU をダウンロードします (入手できる場合)
- 次の Guardium CLI コマンドによって返されるすべてのネットワーク構成パラメーターを記録します。

```
show network interface all
show network route defaultroute
show network resolver 1
show system hostname
show system domain
```

1. 32 ビットの中央マネージャーのアップグレード
   32 ビットの Guardium 環境をアップグレードするには、以下のステップに従って、ヘルス・チェック・パッチを実行し、バックアップ、再ビルド、およびリストアの手順を使用して中央マネージャーをアップグレードします。
2. 32 ビットの管理対象ユニットのアップグレード
   バックアップ、再ビルド、およびリストアの手順を使用して、32 ビットの管理対象ユニットをアップグレードします。

親トピック: Guardium システムのアップグレード
関連概念:
アップグレードの計画

32 ビットの中央マネージャーのアップグレード

32 ビットの Guardium 環境をアップグレードするには、以下のステップに従って、ヘルス・チェック・パッチを実行し、バックアップ、再ビルド、およびリストアの手順を使用して中央マネージャーをアップグレードします。

始める前に

32 ビット環境のアップグレードのアップグレード・チェックリストを完成させます。

手順

1. システムを V9 パッチ 600 以降にアップグレードします。
2. 時刻をローカル・タイム・ゾーンに設定し、NTP サーバーを使用して、すべての Guardium システムにわたって時刻を同期します。
3. 最新のヘルス・チェック・パッチ (p9997) をダウンロードしてインストールし、インストールが正常に完了したことを確認します。その方法については、パッチのインストール、配布、およびモニターを参照してください。
4. 中央マネージャーのシステム・バックアップを取り、バックアップが正常に行われたことを確認します。
   a. 「管理」 > 「データ管理」 > 「システム・バックアップ」にナビゲートします。
   b. 設定に基づいてプロトコルを構成し、すべてのフィールドに入力します。

c. 構成とデータの両方をバックアップします。

重要: アップグレード手順を開始する前に、少なくとも 1 つの有効なバックアップを作成してください。

5. 最新の Guardium V10 ISO をマウントします。
   a. Guardium インストーラーに入って最初の 5 秒以内に、システム・タイプを選択します。「スタンドアロン・コレクター (standalone collector)」ユニット・タイプの「標準インストール (非 CM) (Standard Installation (non CM))」がデフォルトの選択です。中央マネージャーまたはアグリゲーターをアップグレードする場合は、「アグリゲーター」を選択します。
   b. インストールが完了し、システムがリブートされるまで待ちます。
6. ネットワーク・パラメーターを構成します。 Guardium CLI にログインし、以下のコマンドを実行します。

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

7. Guardium ユーザー・インターフェースにログインし、デフォルトのコンポーネントを検証します。
   注: 初回ログインの場合、デフォルトのパスワードは `guardium` です。
   a. 「ようこそ」および「設定」のナビゲーション項目のみが表示されていることを確認します。
   b. 「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートするか、  アイコンをクリックして、システムにライセンスがインストールされていないことを確認します。
8. ライセンスをインストールします。
   a. 通知リンクに従うか、「設定」 > 「ツールとビュー」 > 「ライセンス」を選択して、ライセンス・ページにナビゲートします。
   b. 関連するすべての基本ライセンスおよび追加ライセンスを適用し、使用条件に同意します。
   c. 必要に応じて、CLI にログインして CLI コマンドの `store unit type <type>` を実行し、システム・ユニット・タイプを変更します。ここで、`<type>` は、`manager`、`standalone`、`netinsp`、`mainframe`、`sink`、または `stap` です。
9. 最新の V10 GPU (最新の V10 ISO より新しい場合) および最新の保守パッチを中央マネージャーにインストールし、それらが正常にインストールされたことを確認します。
10. 中央マネージャーのデータおよび構成をリストアします。
    a. Guardium CLI コマンドの `import file` を実行して、バックアップ・ファイルをインポートします。
    b. データ・ファイルと構成ファイルは個別にインポートします。
    c. CLI コマンドの `restore db-from-prev-version` を実行して、データおよび構成のリストアを実行します。

    ヒント: restore db ログには、`diag` CLI コマンドを実行してアクセスできます。詳しくは、diag を使用したインストール進行状況のトラッキングを参照してください。
11. データおよび構成を中央マネージャーにリストアしたら、関連するすべての管理対象ユニットの情報が「一元管理」ページに表示されていることを確認します。
12. 管理対象環境が予期したとおりに機能していることを確認します。
    a. カスタム・レポートがリストアされたことを確認します。
    b. 管理対象ユニットがオンラインになっており、「一元管理」ページからアクセスできることを確認します。

    重要: 混合環境での操作時には、予期される制限事項に注意してください。詳しくは、アップグレード中の混合バージョン環境を参照してください。

次のタスク

32 ビットの Guardium 中央マネージャーのアップグレードが正常に完了したら、32 ビットの管理対象ユニットのアップグレードを行います。

親トピック: 32 ビット環境のアップグレード

次のトピック: 32 ビットの管理対象ユニットのアップグレード

32 ビットの管理対象ユニットのアップグレード

バックアップ、再ビルド、およびリストアの手順を使用して、32 ビットの管理対象ユニットをアップグレードします。

始める前に

32 ビットの管理対象ユニットをアップグレードする前に、以下のタスクを確認して完了します。

- 32 ビット環境のアップグレード
- 32 ビットの中央マネージャーのアップグレード

重要: 最新の V10 にアップグレードする前に、ご使用の環境を V9 パッチ 600 以降にアップグレードする必要があります。

手順

1. 最新のヘルス・チェック・パッチ (p9997) を管理対象ユニットに配布し、正常にインストールされたことを確認します。 詳しくは、パッチのインストール、配布、およびモニターを参照してください。
2. すべての管理対象ユニットのシステム・バックアップを取ります。
3. 以下の手順を使用して、管理対象ユニットを再ビルドします。
   a. 最新の Guardium V10 ISO イメージをマウントします。
   b. Guardium インストーラーに入って 5 秒以内にシステム・タイプを選択します。 デフォルトの選択である「スタンドアロン・コレクター (standalone collector)」ユニット・タイプの「標準インストール (非 CM) (Standard Installation (non CM))」を使用するか、自動ブートするのに任せます。
   c. インストールが完了し、システムがリブートされるまで待ちます。
4. ネットワーク・パラメーターを構成します。 Guardium CLI にログインし、以下のコマンドを実行します。

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

5. Guardium ユーザー・インターフェースにログインし、システムにライセンスがインストールされていないことを確認します。

ヒント:
- 初回ログインの場合、デフォルトのパスワードは `guardium` です。
- 最終的に管理対象ユニットになるスタンドアロン・システムで作業している場合は、ライセンスをインストールする必要はありません。

a. Guardium のメイン・ナビゲーションで、「ようこそ」および「設定」のナビゲーション項目のみが使用可能であることを確認します。

b. 「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートするか、  アイコンをクリックして、システムにライセンスがインストールされていないことを確認します。

6. 管理対象ユニットのデータおよび構成をリストアします。
注: バックアップから管理対象ユニットをリストアする場合、リストア時に中央マネージャーがダウンしていると、その管理対象ユニットのカスタム・レイアウトは失われます。
   a. Guardium CLI コマンドの `import file` を実行して、バックアップ・ファイルをインポートします。
   b. データ・ファイルと構成ファイルは個別にインポートします。
   c. CLI コマンドの `restore db-from-prev-version` を実行して、データおよび構成のリストアを実行します。
7. すべての管理対象ユニットが正常にアップグレードされたら、中央マネージャーから管理対象ユニットにライセンスを配布します。
   a. 中央マネージャーのユーザー・インターフェースにログインします。
   b. 「一元管理」 > 「管理」 > 「一元管理」にナビゲートし、管理対象ユニットがリストされていることを確認します。
   c. 「すべて選択」チェック・ボックスをクリックして、すべての管理対象ユニットを選択します。
   d. 「リフレッシュ」ボタンをクリックして、管理対象ユニットにライセンスを配布します。
   e. リフレッシュ・プロセスが完了するまで待ちます。
   f. 管理対象ユニットのユーザー・インターフェースにログインし、「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートして、正しいライセンスがインストールされていることを確認します。 正しいライセンスがインストールされている場合、以下のようになります。
      - 予期されるナビゲーション・メニュー・オプションが管理対象ユニットで使用可能になります。
      - 管理対象ユニットについてのレポートが機能します。
      - 中央マネージャーからリモート・データ・ソースを介してレポートにアクセスできます。
8. 中央マネージャーに最新の Guardium V10 GPU (最新の V10 ISO より新しい場合) および保守パッチがインストールされた場合、その GPU と保守パッチを管理対象ユニットに配布します。
9. VMware ツールを使用する場合は、アップグレードの完了後にツールを再インストールする必要があります。VMware ツールを再インストールするには、Guardium CLI にログインして `setup vmware_tools install` コマンドを実行し、プロンプトに従います。

タスクの結果

これで、32 ビット Guardium 環境の最新の V10 へのアップグレードが正常に完了しました。Guardium 環境の安定性を確認してください。
親トピック: 32 ビット環境のアップグレード
前のトピック: 32 ビットの中央マネージャーのアップグレード

64 ビット環境のアップグレード

バックアップ中央マネージャーを使用せずに、64 ビットの Guardium 環境をアップグレードします。

バックアップ中央マネージャーを使用せずに、ISO を介して 64 ビットの Guardium 環境をアップグレードする前に、以下のチェックリストを確認して各項目を完了してから、アップグレードを試行してください。

重要: V10 システムで `restore db` を実行する前に、システムが V10 にビルドされた後に最新の保守パッチを適用します。64 ビットのコレクター・ベースの中央マネージャーを使用している場合、アップグレード・パッチによってアップグレードが処理され、システムがコレクター・ベースの中央マネージャーからアグリゲーター・ベースの中央マネージャーに変換されます。

アップグレード・チェックリスト

- 現行システムは V9 パッチ 600 以上で、64 ビット・アーキテクチャーを使用している必要があります。
- 最新の Guardium V9 リリースをダウンロードするか、後でこれを Fix Central から入手します (オプション)。
- アップグレード・パッチ p10000 のダウンロード
- Fix Central からの最新の保守パッチのダウンロード
- Fix Central から最新のヘルス・チェック・パッチ (p9997) をダウンロードします。詳しくは、「Guardium health check patch release notes」を参照してください。

不測の事態に対応するために、以下をダウンロードしてください。

- 必要なすべての基本ライセンスおよび追加ライセンス。
- パスポート・アドバンテージから、最新の V10 ISO。

1. 64 ビットの中央マネージャーのアップグレード
   64 ビットの Guardium 環境をアップグレードするには、以下のステップに従って、ヘルス・チェック・パッチを実行し、中央マネージャーをアップグレードします。
2. 64 ビットの管理対象ユニットのアップグレード
   アップグレード・パッチを使用して、64 ビットの管理対象ユニットをアップグレードします。

親トピック: Guardium システムのアップグレード
関連概念:
アップグレードの計画

64 ビットの中央マネージャーのアップグレード

64 ビットの Guardium 環境をアップグレードするには、以下のステップに従って、ヘルス・チェック・パッチを実行し、中央マネージャーをアップグレードします。

始める前に

64 ビット環境のアップグレードのアップグレード・チェックリストを完成させます。

手順

1. システムを V9 パッチ 600 以降にアップグレードします。
2. 時刻をローカル・タイム・ゾーンに設定し、NTP サーバーを使用して、すべての Guardium システムにわたって時刻を同期します。
3. 最新のヘルス・チェック・パッチ (p9997) をダウンロードしてインストールし、インストールが正常に完了したことを確認します。その方法については、パッチのインストール、配布、およびモニターを参照してください。
4. 中央マネージャーのシステム・バックアップを取り、バックアップが正常に行われたことを確認します。
   a. 「管理」 > 「データ管理」 > 「システム・バックアップ」にナビゲートします。
   b. 設定に基づいてプロトコルを構成し、すべてのフィールドに入力します。
   c. 構成とデータの両方をバックアップします。
   重要: アップグレード手順を開始する前に、少なくとも 1 つの有効なバックアップを作成してください。
5. 中央マネージャーに p10000 をインストールし、そのインストールをモニターします。
   重要: パッチのインストールが完了すると、アップグレード・プロセスが自動的に開始し、システムがリブートされます。システムを手動でリブートしないでください。
6. オペレーティング・システムのインストールが完了するまで待ちます。
   - インストールにかかる時間は、関係するデータの量、およびシステムの仕様と構成によって異なります。
   - オペレーティング・システムのインストールが完了すると、システムは最新の Guardium V10 で初めてリブートされます。
     重要: 最新の V10 が正常にインストールされたら、システムでの最初のブート後に以下が行われます。
     - ネットワーク構成、データベース・データのマイグレーション、データベースの始動。
     - ライセンスのアップグレード、PSML のアップグレード、言語設定。
     - データベースの再始動、証明書および鍵のマイグレーション、パスワードのマイグレーション、およびファイルのクリーンアップ。
7. 中央マネージャーが正常にアップグレードされたことを確認します。
   a. Guardium CLI にログインします。CLI がリカバリー・モードに入る場合、アップグレードはまだ進行中です。
   b. CLI コマンドの show upgrade-status を実行します。 このコマンドは、リカバリー・モードの CLI から実行することもできます。
   c. 出力の最終行が「5.0:INFO:Migration Complete」であることを確認します。
   d. CLI がまだリカバリー・モードの場合は、CLI を終了して再度ログインし、通常の Guardium CLI モードに入ります。
   e. CLI コマンドの show system patch install を実行します。
   f. p10000 の状況が「Phase 5: Migration completed」であることを確認します。
8. Guardium ユーザー・インターフェースにログインし、使用条件に同意して、製品の機能を有効にします。
   a. 「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートします。
   b. 基本ライセンス契約に同意します。
   c. 該当するすべての追加ライセンス契約に同意します。
   注: このステップをスキップすると、Guardium 機能は有効になりません。
9. 管理対象ユニットがオンラインになっており、かつ「一元管理」ページからアクセスできることを確認して、管理対象環境が予期したとおりに機能していることを確認します。
   重要: 混合環境での操作時には、予期される制限事項に注意してください。詳しくは、アップグレード中の混合バージョン環境を参照してください。
10. 中央マネージャーに最新の保守パッチをインストールし、それらが正常にインストールされたことを確認します。

次のタスク

64 ビットの Guardium 中央マネージャーのアップグレードが正常に完了したら、64 ビットの管理対象ユニットのアップグレードを行います。
親トピック: 64 ビット環境のアップグレード
次のトピック: 64 ビットの管理対象ユニットのアップグレード

64 ビットの管理対象ユニットのアップグレード

アップグレード・パッチを使用して、64 ビットの管理対象ユニットをアップグレードします。

始める前に

アップグレード・パッチを使用して 64 ビットの管理対象ユニットをアップグレードする前に、以下のタスクを確認して完了します。

- 64 ビット環境のアップグレード
- 64 ビットの中央マネージャーのアップグレード

重要: 最新の V10 にアップグレードする前に、ご使用の環境を V9 パッチ 600 以降にアップグレードする必要があります。

手順

1. 最新のヘルス・チェック・パッチ (p9997) を管理対象ユニットに配布し、正常にインストールされたことを確認します。 詳しくは、パッチのインストール、配布、およびモニターを参照してください。
2. すべての管理対象ユニットのシステム・バックアップを取ります。
3. p10000 アップグレード・パッチをすべての管理対象ユニットに配布し、パッチのインストールをモニターします。 詳しくは、パッチのインストール、配布、およびモニターを参照してください。
   重要: パッチのインストールが完了すると、アップグレード・プロセスが自動的に開始し、システムがリブートされます。システムを手動でリブートしないでください。
   アップグレードに必要な時間は、関係するデータの量、およびシステムの仕様と構成によって異なります。アップグレードが完了してシステムがリブートされたら、アップグレードされたシステムの最初のブート後に以下が行われます。
   - ネットワーク構成、データベース・データのマイグレーション、データベースの始動。
   - ライセンスのアップグレード、PSML のアップグレード、言語設定。
   - データベースの再始動、証明書および鍵のマイグレーション、パスワードのマイグレーション、およびファイルのクリーンアップ。

   このプロセスの間は、データベースのマイグレーションが完了するまで、アップグレードされた管理対象ユニットにログインできなくなります。
4. 各管理対象ユニットで、アップグレード・プロセスが正常に完了したことを確認します。

a. アップグレード対象システムの Guardium CLI にログインします。 CLI がリカバリー・モードに入る場合、アップグレードはまだ進行中です。
b. CLI コマンドの `show upgrade-status` を実行します。 このコマンドは、リカバリー・モードの CLI から実行することもできます。
c. 出力の最終行が「 `5.0:INFO:Migration Complete`」であることを確認します。
d. CLI がリカバリー・モードの場合は、CLI を終了して再度ログインし、CLI モードに入ります。
e. CLI コマンドの `show system patch install` を実行します。
重要: 最初のリブート後にアップグレードが完了するまで、`show system patch install` は結果を返しません。
f. アップグレード・パッチのインストール状況が「`Phase 5: Migration completed`」であることを確認します。

5. すべての管理対象ユニットが正常にアップグレードされたら、中央マネージャーから管理対象ユニットにライセンスを配布します。
a. 中央マネージャーのユーザー・インターフェースにログインします。
b. 「一元管理」 > 「管理」 > 「一元管理」にナビゲートし、管理対象ユニットがリストされていることを確認します。
c. 「すべて選択」チェック・ボックスをクリックして、すべての管理対象ユニットを選択します。
d. 「リフレッシュ」ボタンをクリックして、管理対象ユニットにライセンスを配布します。
e. リフレッシュ・プロセスが完了するまで待ちます。
f. 管理対象ユニットのユーザー・インターフェースにログインし、「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートして、正しいライセンスがインストールされていることを確認します。 正しいライセンスがインストールされている場合、以下のようになります。
   - 予期されるナビゲーション・メニュー・オプションが管理対象ユニットで使用可能になります。
   - 管理対象ユニットについてのレポートが機能します。
   - 中央マネージャーからリモート・データ・ソースを介してレポートにアクセスできます。
6. 最新の V10 GPU および保守パッチが中央マネージャーにインストールされた場合は、その GPU および保守パッチを管理対象ユニットに配布します。
7. VMware ツールを使用する場合は、アップグレードの完了後にツールを再インストールする必要があります。VMware ツールを再インストールするには、Guardium CLI にログインして `setup vmware_tools install` コマンドを実行し、プロンプトに従います。

タスクの結果

これで、64 ビット Guardium 環境の最新の V10 へのアップグレードが正常に完了しました。Guardium 環境の安定性を確認してください。
親トピック: 64 ビット環境のアップグレード
前のトピック: 64 ビットの中央マネージャーのアップグレード

バックアップ中央マネージャーを使用した 32 ビット環境のアップグレード

バックアップ中央マネージャーを使用して、32 ビットの Guardium 環境をアップグレードします。

バックアップ中央マネージャーを使用して 32 ビットの Guardium 環境をアップグレードする前に、以下のチェックリストを確認して各項目を完了してから、アップグレードを試行してください。

重要: V10 システムで `restore db` を実行する前に、システムが V10 にビルドされた後に最新の保守パッチを適用します。32 ビットのコレクター・ベースの中央マネージャーを使用している場合、V10 にアップグレードする前に、64 ビットのコレクター・ベースの中央マネージャーにビルドし直す必要があります。

アップグレード・チェックリスト

- 現在の環境で定義されているすべての管理対象ユニットを識別し、記録します。
- Fix Central から最新のヘルス・チェック・パッチ (p9997) をダウンロードします。詳しくは、「Guardium health check patch release notes」を参照してください。
- 現行システムでは、 Guardium V9 および 32 ビット・アーキテクチャーを使用する必要があります。
- 最新の Guardium V9 リリースをダウンロードするか、後でこれを Fix Central から入手します (オプション)。
- パスポート・アドバンテージからの最新の Guardium V10 ISO のダウンロード
- パスポート・アドバンテージからのすべての基本ライセンスおよび追加ライセンスのダウンロード
- Fix Central から最新の V10 GPU をダウンロードします (入手できる場合)
- 次の Guardium CLI コマンドによって返されるすべてのネットワーク構成パラメーターを記録します。

```
show network interface all
show network route defaultroute
show network resolver 1
show system hostname
show system domain
```

1. 32 ビットのバックアップ中央マネージャーのアップグレード
32 ビットの Guardium 環境をアップグレードするには、以下のステップに従って、ヘルス・チェック・パッチを実行し、バックアップ、再ビルド、およびリストアの手順を使用してバックアップ中央マネージャーをアップグレードします。
2. 以前のプライマリー中央マネージャーのアップグレード (32 ビット)
バックアップ中央マネージャーを使用する場合は、以下の手順に従って、バックアップ、再ビルド、およびリストアの手順を使用して以前の 32 ビットのプライマリー中央マネージャーをアップグレードします。
3. 32 ビットの管理対象ユニットのアップグレード
バックアップ、再ビルド、およびリストアの手順を使用して、32 ビットの管理対象ユニットをアップグレードします。

親トピック: Guardium システムのアップグレード
関連概念:
アップグレードの計画

32 ビットのバックアップ中央マネージャーのアップグレード

32 ビットの Guardium 環境をアップグレードするには、以下のステップに従って、ヘルス・チェック・パッチを実行し、バックアップ、再ビルド、およびリストアの手順を使用してバックアップ中央マネージャーをアップグレードします。

始める前に

バックアップ中央マネージャーを使用した 32 ビット環境のアップグレードのアップグレード・チェックリストを完成させます。

手順

1. システムを V9 パッチ 600 以降にアップグレードします。
2. 時刻をローカル・タイム・ゾーンに設定し、NTP サーバーを使用して、すべての Guardium システムにわたって時刻を同期します。
3. 最新のヘルス・チェック・パッチ (p9997) をダウンロードしてインストールし、インストールが正常に完了したことを確認します。その方法については、パッチのインストール、配布、およびモニターを参照してください。
   重要: バックアップ中央マネージャーを指定する前に、プライマリー中央マネージャーとバックアップ中央マネージャー候補の両方に、最新のヘルス・チェック・パッチ (p9997) をインストールする必要があります。
4. バックアップ中央マネージャーを定義します。
   a. プライマリー中央マネージャーの「一元管理」ページにナビゲートします。
   b. 管理対象アグリゲーターを選択します。
   c. プライマリー中央マネージャーとバックアップ中央マネージャーの候補に同じパッチがインストールされていることを確認します。
   d. アグリゲーターをバックアップ中央マネージャーとして指定します。
   e. プライマリー中央マネージャーの「統合/アーカイブ・ログ」を確認して、cm_sync_file.tgz ファイルが作成されたことを確認します。
5. バックアップ中央マネージャーのシステム・バックアップを取り、バックアップが正常に行われたことを確認します。
   a. 「管理」 > 「データ管理」 > 「システム・バックアップ」にナビゲートします。
   b. 設定に基づいてプロトコルを構成し、すべてのフィールドに入力します。
   c. 必ず、構成とデータの両方をバックアップしてください。
   重要: アップグレード手順を開始する前に、少なくとも 1 つの有効なバックアップを作成してください。
6. 最新の V10 ISO を使用して、バックアップ中央マネージャーを再ビルドします。
   a. 最新の V10 ISO をマウントします。
   b. Guardium インストーラーに入って最初の 5 秒以内に、システム・タイプを選択します。 「スタンドアロン・コレクター (standalone collector)」ユニット・タイプの「標準インストール (非 CM) (Standard Installation (non CM))」がデフォルトの選択です。
7. インストールが完了し、システムがリブートされるまで待ちます。
8. ネットワーク・パラメーターを構成します。 Guardium CLI にログインし、以下のコマンドを実行します。

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

9. Guardium ユーザー・インターフェースにログインし、デフォルトのコンポーネントを検証します。
   注: 初回ログインの場合、デフォルトのパスワードは `guardium` です。
   a. 「ようこそ」および「設定」のナビゲーション項目のみが表示されていることを確認します。
   b. 「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートするか、  アイコンをクリックして、システムにライセンスがインストールされていないことを確認します。
10. ライセンスをインストールします。
    a. 通知内のリンクに従うか、「設定」 > 「ツールとビュー」 > 「ライセンス」を選択して、ライセンス・ページにナビゲートします。
    b. 関連するすべての基本ライセンスおよび追加ライセンスを適用し、使用条件に同意します。
11. 最新の V10 GPU (最新の V10 ISO より新しい場合) および最新の保守パッチを中央マネージャーにインストールし、それらが正常にインストールされたことを確認します。
12. CLI コマンドの `store system shared secret` を使用するか、「設定」 > 「ツールとビュー」 > 「システム」にナビゲートして、バックアップ中央マネージャーに共有パスワードを設定します。
13. 中央マネージャーのデータおよび構成をリストアします。
    a. Guardium CLI コマンドの `import file` を実行して、バックアップ・ファイルをインポートします。
    b. データ・ファイルと構成ファイルは個別にインポートします。
    c. CLI コマンドの `restore db-from-prev-version` を実行して、データおよび構成のリストアを実行します。
    ヒント: restore db ログには、`diag` CLI コマンドを実行してアクセスできます。詳しくは、diag を使用したインストール進行状況のトラッキングを参照してください。
14. プライマリー中央マネージャーから、V10 バックアップ中央マネージャーが使用可能かつオンラインであることを確認します。プライマリー中央マネージャーの配下にある管理対象ユニットの数を確認して記録します (この情報は、バックアップ中央マネージャーへの移行後に使用されます)。
    重要: バックアップ中央マネージャー (最新の Guardium V10 を実行) は、赤色の状況ライトを表示する場合があります。これは、中央マネージャーが V10 システムに V9 シグナルを送信して失敗した場合に発生しますが、バックアップ中央マネージャーの同期ファイルがバックアップ中央マネージャーに存在する限り、引き続きサーバーをプロモートできます。リフレッシュは試みないでください。
15. プライマリー中央マネージャーの「統合/アーカイブ・ログ」を確認して、cm_sync_file.tgz ファイルがプライマリー中央マネージャーからバックアップ中央マネージャーへの転送を少なくとも 2 つ完了したことを確認します。転送は、30 分間隔で発生する必要があります。
16. バックアップ中央マネージャーをプライマリー中央マネージャーにします。 バックアップ中央マネージャーにログインすると、次のメッセージが表示される場合があります。

```
The central manager version is lower than the version of this managed unit. Functionality is limited until the version
mismatch is corrected.
```

    a. 「設定」 > 「一元管理」にナビゲートします。
    b. 「プライマリー CM に設定」をクリックします。このオプションが表示されない場合、cm_sync_file が正常に転送されていることを確認します。
    c. 「このユニットをプライマリー CM にしますか?」というメッセージに、「はい」と答えます。
    d. 「この変更には数分間かかります。また、GUI を再始動する必要があります。GUI 再始動の実行時にログオフされます。」というポップアップ・メッセージで、「閉じる」をクリックします。 ユーザー・インターフェース・ページに進行状況アイコンが表示されます。
    注: 変換プロセス中は、Guardium ユーザー・インターフェースは一時的に使用不可になります。プロセスが完了すると、ログイン画面は正常に戻ります。
17. 管理対象ユニットを新規プライマリー中央マネージャーに移行します。この処理は、完了までに時間がかかる場合があります。SSH クライアントを使用して、新規プライマリー中央マネージャーに接続して結果ログを表示します。
    a. `fileserver [ip_address] [duration]` コマンドを使用して、ファイル・サーバーを初期化します。
    b. Web ブラウザーから、新規プライマリー中央マネージャーに接続します。
    c. load_secondary_cm_sync_file.log ファイルを表示して、進行状況を確認します。このファイルは、gim-snif-guard-logs ディレクトリーにあります。
    d. 最終行の「Import CM sync info done」が表示されたら、プロセスは正常に終了しています。

e. この時点で、ユーザー・インターフェースがリフレッシュされ、ログイン・ページが表示されます。
f. 管理対象ユニットが新規プライマリー中央マネージャーへの移行を開始するため、プロセスが完了するのを正時まで待ちます。

18. Guardium ユーザー・インターフェースにログインし、以下のステップを完了します。
a. 管理対象ユニットが新規プライマリー中央マネージャーによって管理されるようになったことを確認します。
b. 以前のプライマリー中央マネージャーを除くすべての管理対象ユニットが移行済みであることを確認します。

次のタスク

バックアップ中央マネージャーのアップグレードおよび管理対象ユニットの移行が正常に完了したら、以前のプライマリー中央マネージャーのアップグレード (32 ビット)を行います。
親トピック: バックアップ中央マネージャーを使用した 32 ビット環境のアップグレード
次のトピック: 以前のプライマリー中央マネージャーのアップグレード (32 ビット)

以前のプライマリー中央マネージャーのアップグレード (32 ビット)

バックアップ中央マネージャーを使用する場合は、以下の手順に従って、バックアップ、再ビルド、およびリストアの手順を使用して以前の 32 ビットのプライマリー中央マネージャーをアップグレードします。

始める前に

バックアップ中央マネージャーが新規プライマリー中央マネージャーになったら、以前のプライマリー中央マネージャーを最新の Guardium V10 にアップグレードできます。以前のプライマリー中央マネージャーをアップグレードする前に、以下のタスクを確認して完了します。

- バックアップ中央マネージャーを使用した 32 ビット環境のアップグレード
- 32 ビットのバックアップ中央マネージャーのアップグレード

手順

1. CLI コマンドの `delete unit type manager` を実行して、以前のプライマリー中央マネージャーを再構成します。 続行する前に、以前のプライマリー中央マネージャーがスタンドアロン・アグリゲーターになったことを確認します。
2. 以前のプライマリー中央マネージャーからシステム・バックアップを取ります。 バックアップにデータと構成の両方を含めます。
3. 以下の手順を使用して、以前のプライマリー中央マネージャーを再ビルドします。
a. 最新の Guardium V10 ISO イメージをマウントします。
b. Guardium インストーラーに入って 5 秒以内にシステム・タイプを選択します。 以前のプライマリー中央マネージャーを使用するときは、「アグリゲーター」を選択します。
c. インストールが完了し、システムがリブートされるまで待ちます。
4. ネットワーク・パラメーターを構成します。 Guardium CLI にログインし、以下のコマンドを実行します。

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

5. Guardium ユーザー・インターフェースにログインし、システムにライセンスがインストールされていないことを確認します。
ヒント:
- 初回ログインの場合、デフォルトのパスワードは `guardium` です。
- 最終的に管理対象ユニットになるスタンドアロン・システムで作業している場合は、ライセンスをインストールする必要はありません。
a. Guardium のメイン・ナビゲーションで、「ようこそ」および「設定」のナビゲーション項目のみが使用可能であることを確認します。
b. 「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートするか、 

アイコンをクリックして、システムにライセンスがインストールされていないことを確認します。
6. 以前のバックアップ中央マネージャーをプライマリー中央マネージャーに変換する前に、以前のバックアップ中央マネージャーに最新の V10 GPU (最新の V10 ISO より新しい場合) および保守パッチがインストールされた場合は、同じ GPU および保守パッチを以前のプライマリー中央マネージャーにインストールします。
7. 以前のプライマリー中央マネージャーのデータおよび構成をリストアします。
a. Guardium CLI コマンドの `import file` を実行して、バックアップ・ファイルをインポートします。
b. データ・ファイルと構成ファイルは個別にインポートします。
c. CLI コマンドの `restore db-from-prev-version` を実行して、データおよび構成のリストアを実行します。
8. 「設定」 > 「ツールとビュー」 > 「システム」にナビゲートして、以前のプライマリー中央マネージャーに共有パスワードを設定します。
9. 以前のプライマリー中央マネージャー (アップグレードしたばかりのシステム) を新規プライマリー中央マネージャーに対して登録します。
10. 新規バックアップ中央マネージャーを定義します。
a. 新規プライマリー中央マネージャーで、「管理」 > 「一元管理」 > 「一元管理」にナビゲートします。
b. 以前のプライマリー中央マネージャーを選択します。
c. 以前のプライマリー中央マネージャーを新規バックアップ中央マネージャーとして指定します。
d. 少なくとも 1 回のバックアップ同期が完了するまで待ちます。 最初のバックアップ同期は、1 時間以内に実行されます。
e. 新規プライマリー中央マネージャーの「統合/アーカイブ」ログを確認して、cm_sync_file.tgz ファイルが作成されたことを確認します。
11. オプションで、新規バックアップ中央マネージャーをプライマリー中央マネージャーとして再定義することで、元の管理対象環境の構成に戻します。
a. 「このユニットをプライマリー CM にしますか?」というメッセージに、「はい」と答えます。
b. 「情報 (Information)」ポップアップ・メッセージで「閉じる」をクリックします。ユーザー・インターフェース・ページに進行状況アイコンが表示されます。
重要: 変換プロセス中は、ユーザー・インターフェースは一時的に使用不可になります。プロセスが完了すると、ログイン画面は正常に戻ります。
12. 管理対象ユニットを新規プライマリー中央マネージャーに移行します。 このプロセスは、完了までに時間がかかる場合があります。SSH クライアントを使用して、新規プライマリー中央マネージャーに接続して結果ログを表示します。
a. `fileserver [ip_address] [duration]` コマンドを使用して、ファイル・サーバーを初期化します。
b. Web ブラウザーから、新規プライマリー中央マネージャーに接続します。
c. load_secondary_cm_sync_file.log ファイルを表示して、進行状況を確認します。このファイルは、gim-snif-guard-logs ディレクトリーにあります。

d. 最終行の「Import CM sync info done」が表示されたら、プロセスは正常に終了しています。
e. この時点で、ユーザー・インターフェースがリフレッシュされ、ログイン・ページが表示されます。
f. 管理対象ユニットが新規プライマリー中央マネージャーへの移行を開始するため、プロセスが完了するまで 5 分間待ちます。

13. 「管理」 > 「一元管理」 > 「一元管理」にナビゲートし、すべての管理対象ユニットが緑色で表示され、元のプライマリー中央マネージャーによって管理されるようになったことを確認します。 元のバックアップ中央マネージャーは、バックアップ中央マネージャーとして再構成されていない限り、管理対象ユニットのリストには表示されません。

次のタスク

これで、中央マネージャーとバックアップ中央マネージャーがアップグレードされたので、32 ビットの管理対象ユニットのアップグレードを行います。
親トピック: バックアップ中央マネージャーを使用した 32 ビット環境のアップグレード
前のトピック: 32 ビットのバックアップ中央マネージャーのアップグレード
次のトピック: 32 ビットの管理対象ユニットのアップグレード

32 ビットの管理対象ユニットのアップグレード

バックアップ、再ビルド、およびリストアの手順を使用して、32 ビットの管理対象ユニットをアップグレードします。

始める前に

32 ビットの管理対象ユニットをアップグレードする前に、以下のタスクを確認して完了します。

- バックアップ中央マネージャーを使用した 32 ビット環境のアップグレード
- 32 ビットのバックアップ中央マネージャーのアップグレード
- 以前のプライマリー中央マネージャーのアップグレード (32 ビット)

重要: 最新の V10 にアップグレードする前に、ご使用の環境を V9 パッチ 600 以降にアップグレードする必要があります。

手順

1. 最新のヘルス・チェック・パッチ (p9997) を管理対象ユニットに配布し、正常にインストールされたことを確認します。 詳しくは、パッチのインストール、配布、およびモニターを参照してください。
2. すべての管理対象ユニットのシステム・バックアップを取ります。
3. 以下の手順を使用して、管理対象ユニットを再ビルドします。
   a. 最新の Guardium V10 ISO イメージをマウントします。
   b. Guardium インストーラーに入って 5 秒以内にシステム・タイプを選択します。 デフォルトの選択である「スタンドアロン・コレクター (standalone collector)」ユニット・タイプの「標準インストール (非 CM) (Standard Installation (non CM))」を使用するか、自動ブートするのに任せます。
   c. インストールが完了し、システムがリブートされるまで待ちます。
4. ネットワーク・パラメーターを構成します。 Guardium CLI にログインし、以下のコマンドを実行します。

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

5. Guardium ユーザー・インターフェースにログインし、システムにライセンスがインストールされていないことを確認します。
   ヒント:
   - 初回ログインの場合、デフォルトのパスワードは `guardium` です。
   - 最終的に管理対象ユニットになるスタンドアロン・システムで作業している場合は、ライセンスをインストールする必要はありません。

   a. Guardium のメイン・ナビゲーションで、「ようこそ」および「設定」のナビゲーション項目のみが使用可能であることを確認します。
   b. 「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートするか、 

アイコンをクリックして、システムにライセンスがインストールされていないことを確認します。
6. 管理対象ユニットのデータおよび構成をリストアします。
   注: バックアップから管理対象ユニットをリストアする場合、リストア時に中央マネージャーがダウンしていると、その管理対象ユニットのカスタム・レイアウトは失われます。
   a. Guardium CLI コマンドの `import file` を実行して、バックアップ・ファイルをインポートします。
   b. データ・ファイルと構成ファイルは個別にインポートします。
   c. CLI コマンドの `restore db-from-prev-version` を実行して、データおよび構成のリストアを実行します。
7. すべての管理対象ユニットが正常にアップグレードされたら、中央マネージャーから管理対象ユニットにライセンスを配布します。
   a. 中央マネージャーのユーザー・インターフェースにログインします。
   b. 「一元管理」 > 「管理」 > 「一元管理」にナビゲートし、管理対象ユニットがリストされていることを確認します。
   c. 「すべて選択」チェック・ボックスをクリックして、すべての管理対象ユニットを選択します。
   d. 「リフレッシュ」ボタンをクリックして、管理対象ユニットにライセンスを配布します。
   e. リフレッシュ・プロセスが完了するまで待ちます。
   f. 管理対象ユニットのユーザー・インターフェースにログインし、「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートして、正しいライセンスがインストールされていることを確認します。 正しいライセンスがインストールされている場合、以下のようになります。
      - 予期されるナビゲーション・メニュー・オプションが管理対象ユニットで使用可能になります。
      - 管理対象ユニットについてのレポートが機能します。
      - 中央マネージャーからリモート・データ・ソースを介してレポートにアクセスできます。
8. 中央マネージャーに最新の Guardium V10 GPU (最新の V10 ISO より新しい場合) および保守パッチがインストールされた場合、その GPU と保守パッチを管理対象ユニットに配布します。
9. VMware ツールを使用する場合は、アップグレードの完了後にツールを再インストールする必要があります。VMware ツールを再インストールするには、Guardium CLI にログインして `setup vmware_tools install` コマンドを実行し、プロンプトに従います。

タスクの結果

これで、バックアップ中央マネージャーを使用した、32 ビット Guardium 環境の最新の V10 へのアップグレードが正常に完了しました。Guardium 環境の安定性を確認してください。
親トピック: バックアップ中央マネージャーを使用した 32 ビット環境のアップグレード
前のトピック: 以前のプライマリー中央マネージャーのアップグレード (32 ビット)

バックアップ中央マネージャーを使用した 64 ビット環境のアップグレード

バックアップ中央マネージャーを使用して、64 ビットの Guardium 環境をアップグレードします。

バックアップ中央マネージャーを使用して 64 ビットの Guardium 環境をアップグレードする前に、以下のチェックリストを確認して各項目を完了してから、アップグレードを試行してください。

重要: V10 システムで `restore db` を実行する前に、システムが V10 にビルドされた後に最新の保守パッチを適用します。64 ビットのコレクター・ベースの中央マネージャーを使用している場合、アップグレード・パッチによってアップグレードが処理され、システムがコレクター・ベースの中央マネージャーからアグリゲーター・ベースの中央マネージャーに変換されます。

アップグレード・チェックリスト

- 現在の環境で定義されているすべての管理対象ユニットを識別し、記録します。
- 現行システムは V9 パッチ 600 以上で、64 ビット・アーキテクチャーを使用している必要があります。
- 最新の Guardium V9 リリースをダウンロードするか、後でこれを Fix Central から入手します (オプション)。
- アップグレード・パッチ p10000 のダウンロード
- Fix Central からの最新の保守パッチのダウンロード
- Fix Central から最新のヘルス・チェック・パッチ (p9997) をダウンロードします。詳しくは、「Guardium health check patch release notes」を参照してください。

1. 64 ビットのバックアップ中央マネージャーのアップグレード
   64 ビットの Guardium 環境をアップグレードするには、以下のステップに従って、ヘルス・チェック・パッチを実行し、バックアップ、再ビルド、およびリストアの手順を使用してバックアップ中央マネージャーをアップグレードします。
2. 以前のプライマリー中央マネージャーのアップグレード (64 ビット)
   バックアップ中央マネージャーを使用する場合は、以下の手順に従って、アップグレード・パッチを使用して以前の 64 ビットのプライマリー中央マネージャーをアップグレードします。
3. 64 ビットの管理対象ユニットのアップグレード
   アップグレード・パッチを使用して、64 ビットの管理対象ユニットをアップグレードします。

親トピック: Guardium システムのアップグレード
関連概念:
アップグレードの計画

64 ビットのバックアップ中央マネージャーのアップグレード

64 ビットの Guardium 環境をアップグレードするには、以下のステップに従って、ヘルス・チェック・パッチを実行し、バックアップ、再ビルド、およびリストアの手順を使用してバックアップ中央マネージャーをアップグレードします。

始める前に

バックアップ中央マネージャーを使用した 64 ビット環境のアップグレードのアップグレード・チェックリストを完成させます。

手順

1. システムを V9 パッチ 600 以降にアップグレードします。
2. 時刻をローカル・タイム・ゾーンに設定し、NTP サーバーを使用して、すべての Guardium システムにわたって時刻を同期します。
3. 最新のヘルス・チェック・パッチ (p9997) をダウンロードしてインストールし、インストールが正常に完了したことを確認します。その方法については、パッチのインストール、配布、およびモニターを参照してください。
   重要: バックアップ中央マネージャーを指定する前に、プライマリー中央マネージャーとバックアップ中央マネージャー候補の両方に、最新のヘルス・チェック・パッチ (p9997) をインストールする必要があります。
4. バックアップ中央マネージャーを定義します。
   a. プライマリー中央マネージャーの「一元管理」ページにナビゲートします。
   b. 管理対象アグリゲーターを選択します。
   c. プライマリー中央マネージャーとバックアップ中央マネージャーの候補に同じパッチがインストールされていることを確認します。
   d. アグリゲーターをバックアップ中央マネージャーとして指定します。
   e. プライマリー中央マネージャーの「統合/アーカイブ・ログ」を確認して、cm_sync_file.tgz ファイルが作成されたことを確認します。
5. バックアップ中央マネージャーのシステム・バックアップを取り、バックアップが正常に行われたことを確認します。
   a. 「管理」 > 「データ管理」 > 「システム・バックアップ」にナビゲートします。
   b. 設定に基づいてプロトコルを構成し、すべてのフィールドに入力します。
   c. 必ず、構成とデータの両方をバックアップしてください。
   重要: アップグレード手順を開始する前に、少なくとも 1 つの有効なバックアップを作成してください。
6. 中央マネージャーに p10000 をインストールし、そのインストールをモニターします。
   重要: パッチのインストールが完了すると、アップグレード・プロセスが自動的に開始し、システムがリブートされます。システムを手動でリブートしないでください。
7. オペレーティング・システムのインストールが完了するまで待ちます。
   - インストールにかかる時間は、関係するデータの量、およびシステムの仕様と構成によって異なります。

- オペレーティング・システムのインストールが完了すると、システムは最新の Guardium V10 で初めてリブートされます。
  重要: 最新の V10 が正常にインストールされたら、システムでの最初のブート後に以下が行われます。
  - ネットワーク構成、データベース・データのマイグレーション、データベースの始動。
  - ライセンスのアップグレード、PSML のアップグレード、言語設定。
  - データベースの再始動、証明書および鍵のマイグレーション、パスワードのマイグレーション、およびファイルのクリーンアップ。

8. 以下のステップを使用して、バックアップ CM のアップグレードが正常に完了したことを確認します。
   a. CLI にログインします。
   b. CLI コマンドの show upgrade-status を実行します。
   c. 出力の最終行が「5.0:INFO:Migration Complete」であることを確認します。
   d. CLI コマンドの show system patch install を実行します。
   e. p10000 の状況が「Phase 5: Migration completed」であることを確認します。
9. 中央マネージャーに最新の保守パッチをインストールし、それらが正常にインストールされたことを確認します。
10. プライマリー中央マネージャーが、アップグレードされたバックアップ中央マネージャーを引き続き参照していることを確認します。
    重要: バックアップ中央マネージャー (最新の Guardium V10 を実行) は、赤色の状況ライトを表示する場合があります。これは、中央マネージャーが V10 システムに V9 シグナルを送信して失敗した場合に発生しますが、バックアップ中央マネージャーの同期ファイルがバックアップ中央マネージャーに存在する限り、引き続きサーバーをプロモートできます。リフレッシュは試みないでください。
11. プライマリー中央マネージャーの「統合/アーカイブ・ログ」を確認して、cm_sync_file.tgz ファイルがプライマリー中央マネージャーからバックアップ中央マネージャーへの転送を少なくとも 2 つ完了したことを確認します。転送は、30 分間隔で発生する必要があります。
12. バックアップ中央マネージャーをプライマリー中央マネージャーにします。 バックアップ中央マネージャーにログインすると、次のメッセージが表示される場合があります。

    ```
    The central manager version is lower than the version of this managed unit. Functionality is limited until the version mismatch is corrected.
    ```

    a. 「設定」 > 「一元管理」にナビゲートします。
    b. 「プライマリー CM に設定」をクリックします。このオプションが表示されない場合、cm_sync_file が正常に転送されていることを確認します。
    c. 「このユニットをプライマリー CM にしますか?」というメッセージに、「はい」と答えます。
    d. 「この変更には数分間かかります。また、GUI を再始動する必要があります。GUI 再始動の実行時にログオフされます。」というポップアップ・メッセージで、「閉じる」をクリックします。 ユーザー・インターフェース・ページに進行状況アイコンが表示されます。
    注: 変換プロセス中は、Guardium ユーザー・インターフェースは一時的に使用不可になります。プロセスが完了すると、ログイン画面は正常に戻ります。
13. 管理対象ユニットを新規プライマリー中央マネージャーに移行します。この処理は、完了までに時間がかかる場合があります。SSH クライアントを使用して、新規プライマリー中央マネージャーに接続して結果ログを表示します。
    a. `fileserver [ip_address] [duration]` コマンドを使用して、ファイル・サーバーを初期化します。
    b. Web ブラウザーから、新規プライマリー中央マネージャーに接続します。
    c. load_secondary_cm_sync_file.log ファイルを表示して、進行状況を確認します。このファイルは、gim-snif-guard-logs ディレクトリーにあります。
    d. 最終行の「Import CM sync info done」が表示されたら、プロセスは正常に終了しています。
    e. この時点で、ユーザー・インターフェースがリフレッシュされ、ログイン・ページが表示されます。
    f. 管理対象ユニットが新規プライマリー中央マネージャーへの移行を開始するため、プロセスが完了するのを正時まで待ちます。
14. Guardium ユーザー・インターフェースにログインし、使用条件に同意して、製品の機能を有効にします。
    a. 「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートします。
    b. 基本ライセンス契約に同意します。
    c. 該当するすべての追加ライセンス契約に同意します。
    注: このステップをスキップすると、Guardium 機能は有効になりません。
15. 「一元管理」ページにナビゲートし、管理対象ユニットが、新規プライマリー中央マネージャーによって管理されるようになったことを確認します。以前のプライマリー中央マネージャーは、管理対象ユニットのリストには表示されなくなっています。

次のタスク

バックアップ中央マネージャーのアップグレードおよび管理対象ユニットの移行が正常に完了したら、以前のプライマリー中央マネージャーのアップグレード (64 ビット)を行います。
親トピック: バックアップ中央マネージャーを使用した 64 ビット環境のアップグレード
次のトピック: 以前のプライマリー中央マネージャーのアップグレード (64 ビット)

以前のプライマリー中央マネージャーのアップグレード (64 ビット)

バックアップ中央マネージャーを使用する場合は、以下の手順に従って、アップグレード・パッチを使用して以前の 64 ビットのプライマリー中央マネージャーをアップグレードします。

始める前に

バックアップ中央マネージャーが新規プライマリー中央マネージャーになったら、以前のプライマリー中央マネージャーを最新の Guardium V10 にマイグレーションできます。以前のプライマリー中央マネージャーをアップグレードする前に、以下のタスクを確認して完了します。

- バックアップ中央マネージャーを使用した 64 ビット環境のアップグレード
- 64 ビットのバックアップ中央マネージャーのアップグレード

手順

1. CLI コマンドの `delete unit type manager` を実行して、以前のプライマリー中央マネージャーを再構成します。 続行する前に、以前のプライマリー中央マネージャーがスタンドアロン・アグリゲーターになったことを確認します。
2. 以前のプライマリー中央マネージャーからシステム・バックアップを取ります。 バックアップにデータと構成の両方を含めます。
3. p10000 アップグレード・パッチを使用して以前のプライマリー中央マネージャーをアップグレードし、パッチのインストールをモニターします。 詳しくは、パッチのインストール、配布、およびモニターを参照してください。
   重要: パッチのインストールが完了すると、アップグレード・プロセスが自動的に開始し、システムがリブートされます。システムを手動でリブートしないでください。

アップグレードに必要な時間は、関係するデータの量、およびシステムの仕様と構成によって異なります。アップグレードが完了してシステムがリブートされたら、アップグレードされたシステムの最初のブート後に以下が行われます。
   - ネットワーク構成、データベース・データのマイグレーション、データベースの始動。
   - ライセンスのアップグレード、PSML のアップグレード、言語設定。
   - データベースの再始動、証明書および鍵のマイグレーション、パスワードのマイグレーション、およびファイルのクリーンアップ。

   このプロセスの間は、データベースのマイグレーションが完了するまで、アップグレードされた管理対象ユニットにログインできなくなります。
4. 以前のプライマリー中央マネージャーで、アップグレード・プロセスが正常に完了したことを確認します。
   a. アップグレード対象システムの Guardium CLI にログインします。 CLI がリカバリー・モードに入る場合、アップグレードはまだ進行中です。
   b. CLI コマンドの `show upgrade-status` を実行します。 このコマンドは、リカバリー・モードの CLI から実行することもできます。
   c. 出力の最終行が「 `5.0:INFO:Migration Complete`」であることを確認します。
   d. CLI がリカバリー・モードの場合は、CLI を終了して再度ログインし、CLI モードに入ります。
   e. CLI コマンドの `show system patch install` を実行します。
      重要: 最初のリブート後にアップグレードが完了するまで、`show system patch install` は結果を返しません。
   f. アップグレード・パッチのインストール状況が「`Phase 5: Migration completed`」であることを確認します。
5. 以前のバックアップ中央マネージャーをプライマリー中央マネージャーに変換する前に、以前のバックアップ中央マネージャーに最新の V10 GPU (最新の V10 ISO より新しい場合) および保守パッチがインストールされた場合は、同じ GPU および保守パッチを以前のプライマリー中央マネージャーにインストールしてください。
6. 「設定」 > 「ツールとビュー」 > 「システム」にナビゲートして、以前のプライマリー中央マネージャーに共有パスワードを設定します。
7. 以前のプライマリー中央マネージャー (アップグレードしたばかりのシステム) を新規プライマリー中央マネージャーに対して登録します。
8. 新規バックアップ中央マネージャーを定義します。
   a. 新規プライマリー中央マネージャーで、「管理」 > 「一元管理」 > 「一元管理」にナビゲートします。
   b. 以前のプライマリー中央マネージャーを選択します。
   c. 以前のプライマリー中央マネージャーを新規バックアップ中央マネージャーとして指定します。
   d. 少なくとも 1 回のバックアップ同期が完了するまで待ちます。 最初のバックアップ同期は、1 時間以内に実行されます。
   e. 新規プライマリー中央マネージャーの「統合/アーカイブ」ログを確認して、cm_sync_file.tgz ファイルが作成されたことを確認します。
9. オプションで、新規バックアップ中央マネージャーをプライマリー中央マネージャーとして再定義することで、元の管理対象環境の構成に戻します。
   a. 「このユニットをプライマリー CM にしますか?」というメッセージに、「はい」と答えます。
   b. 「情報 (Information)」ポップアップ・メッセージで「閉じる」をクリックします。ユーザー・インターフェース・ページに進行状況アイコンが表示されます。
      重要: 変換プロセス中は、ユーザー・インターフェースは一時的に使用不可になります。プロセスが完了すると、ログイン画面は正常に戻ります。
10. 管理対象ユニットを新規プライマリー中央マネージャーに移行します。 このプロセスは、完了までに時間がかかる場合があります。SSH クライアントを使用して、新規プライマリー中央マネージャーに接続して結果ログを表示します。
    a. `fileserver [ip_address] [duration]` コマンドを使用して、ファイル・サーバーを初期化します。
    b. Web ブラウザーから、新規プライマリー中央マネージャーに接続します。
    c. load_secondary_cm_sync_file.log ファイルを表示して、進行状況を確認します。このファイルは、gim-snif-guard-logs ディレクトリーにあります。
    d. 最終行の「Import CM sync info done」が表示されたら、プロセスは正常に終了しています。
    e. この時点で、ユーザー・インターフェースがリフレッシュされ、ログイン・ページが表示されます。
    f. 管理対象ユニットが新規プライマリー中央マネージャーへの移行を開始するため、プロセスが完了するまで 5 分間待ちます。
11. 「管理」 > 「一元管理」 > 「一元管理」にナビゲートし、すべての管理対象ユニットが緑色で表示され、元のプライマリー中央マネージャーによって管理されるようになったことを確認します。 元のバックアップ中央マネージャーは、バックアップ中央マネージャーとして再構成されていない限り、管理対象ユニットのリストには表示されません。

次のタスク

これで、中央マネージャーとバックアップ中央マネージャーがアップグレードされたので、64 ビットの管理対象ユニットのアップグレードを行います。
親トピック: バックアップ中央マネージャーを使用した 64 ビット環境のアップグレード
前のトピック: 64 ビットのバックアップ中央マネージャーのアップグレード
次のトピック: 64 ビットの管理対象ユニットのアップグレード

64 ビットの管理対象ユニットのアップグレード

アップグレード・パッチを使用して、64 ビットの管理対象ユニットをアップグレードします。

始める前に

アップグレード・パッチを使用して 64 ビットの管理対象ユニットをアップグレードする前に、以下のタスクを確認して完了します。

- バックアップ中央マネージャーを使用した 64 ビット環境のアップグレード
- 64 ビットのバックアップ中央マネージャーのアップグレード
- 以前のプライマリー中央マネージャーのアップグレード (64 ビット)

重要: 最新の V10 にアップグレードする前に、ご使用の環境を V9 パッチ 600 以降にアップグレードする必要があります。

手順

1. 最新のヘルス・チェック・パッチ (p9997) を管理対象ユニットに配布し、正常にインストールされたことを確認します。 詳しくは、パッチのインストール、配布、およびモニターを参照してください。
2. すべての管理対象ユニットのシステム・バックアップを取ります。
3. p10000 アップグレード・パッチを中央マネージャーに転送し、管理対象ユニットで使用できるようにします。
   a. アップグレード・パッチを中央マネージャーに転送します。 詳しくは、パッチのインストール、配布、およびモニターを参照してください。
   b. 中央マネージャーから CLI コマンドの `show system patch available` を実行して、管理対象ユニットでアップグレード・パッチを使用できるようにします。
4. p10000 アップグレード・パッチをすべての管理対象ユニットに配布し、パッチのインストールをモニターします。 詳しくは、パッチのインストール、配布、およびモニターを参照してください。

重要: パッチのインストールが完了すると、アップグレード・プロセスが自動的に開始し、システムがリブートされます。システムを手動でリブートしないでください。
アップグレードに必要な時間は、関係するデータの量、およびシステムの仕様と構成によって異なります。アップグレードが完了してシステムがリブートされたら、アップグレードされたシステムの最初のブート後に以下が行われます。
- ネットワーク構成、データベース・データのマイグレーション、データベースの始動。
- ライセンスのアップグレード、PSML のアップグレード、言語設定。
- データベースの再始動、証明書および鍵のマイグレーション、パスワードのマイグレーション、およびファイルのクリーンアップ。

このプロセスの間は、データベースのマイグレーションが完了するまで、アップグレードされた管理対象ユニットにログインできなくなります。

5. 各管理対象ユニットで、アップグレード・プロセスが正常に完了したことを確認します。
   a. アップグレード対象システムの Guardium CLI にログインします。 CLI がリカバリー・モードに入る場合、アップグレードはまだ進行中です。
   b. CLI コマンドの `show upgrade-status` を実行します。 このコマンドは、リカバリー・モードの CLI から実行することもできます。
   c. 出力の最終行が「 `5.0:INFO:Migration Complete`」であることを確認します。
   d. CLI がリカバリー・モードの場合は、CLI を終了して再度ログインし、CLI モードに入ります。
   e. CLI コマンドの `show system patch install` を実行します。
   重要: 最初のリブート後にアップグレードが完了するまで、`show system patch install` は結果を返しません。
   f. アップグレード・パッチのインストール状況が「`Phase 5: Migration completed`」であることを確認します。
6. すべての管理対象ユニットが正常にアップグレードされたら、中央マネージャーから管理対象ユニットにライセンスを配布します。
   a. 中央マネージャーのユーザー・インターフェースにログインします。
   b. 「一元管理」 > 「管理」 > 「一元管理」にナビゲートし、管理対象ユニットがリストされていることを確認します。
   c. 「すべて選択」チェック・ボックスをクリックして、すべての管理対象ユニットを選択します。
   d. 「リフレッシュ」ボタンをクリックして、管理対象ユニットにライセンスを配布します。
   e. リフレッシュ・プロセスが完了するまで待ちます。
   f. 管理対象ユニットのユーザー・インターフェースにログインし、「設定」 > 「ツールとビュー」 > 「ライセンス」にナビゲートして、正しいライセンスがインストールされていることを確認します。 正しいライセンスがインストールされている場合、以下のようになります。
      - 予期されるナビゲーション・メニュー・オプションが管理対象ユニットで使用可能になります。
      - 管理対象ユニットについてのレポートが機能します。
      - 中央マネージャーからリモート・データ・ソースを介してレポートにアクセスできます。
7. 中央マネージャーに最新の Guardium V10 GPU (最新の V10 ISO より新しい場合) および保守パッチがインストールされた場合、その GPU と保守パッチを管理対象ユニットに配布します。
8. VMware ツールを使用する場合は、アップグレードの完了後にツールを再インストールする必要があります。VMware ツールを再インストールするには、Guardium CLI にログインして `setup vmware_tools install` コマンドを実行し、プロンプトに従います。

タスクの結果

これで、バックアップ中央マネージャーを使用した、64 ビット Guardium 環境の最新の V10 へのアップグレードが正常に完了しました。Guardium 環境の安定性を確認してください。
親トピック: バックアップ中央マネージャーを使用した 64 ビット環境のアップグレード
前のトピック: 以前のプライマリー中央マネージャーのアップグレード (64 ビット)

CLI および API

Guardium® コマンド行インターフェース (CLI) は、Guardium システムの構成、トラブルシューティング、および管理を行えるようにするための管理ツールです。
Guardium アプリケーション・プログラミング・インターフェース (API) は、多くの Guardium 関数にコマンド行からアクセスできるようにします。

- CLI の概要
  Guardium コマンド行インターフェース (CLI) は、Guardium システムの構成、トラブルシューティング、および管理を行えるようにするための管理ツールです。
- GuardAPI リファレンス
  GuardAPI を使用すると、コマンド行から Guardium 機能にアクセスできます。

CLI の概要

Guardium® コマンド行インターフェース (CLI) は、Guardium システムの構成、トラブルシューティング、および管理を行えるようにするための管理ツールです。

本書の規則

すべての CLI コマンドの例は、クーリエ・フォントのテキスト (例えば、show system clock) で書かれています。

構文のルールを図示するために、一部のコマンドではその記述に従属区切り文字が使われています。 そのような区切り文字は、どのコマンド引数が必須であるか、またどのようなコンテキストで使用するかを示します。 各構文の説明では、コマンド引数間の従属関係を以下の特殊文字を使用して示します。

- < および > 記号は必須の引数を表します。
- [および] 記号はオプションの引数を表します。
- | (垂直バー) 記号は、選択項目から 1 つしか選択できない場合に各選択肢を分離するものです。 例:

```
store full-bypass <ON | OFF>
```

CLI コマンドの使用法

- コマンドとキーワードは、コマンドがあいまいにならないだけの十分な文字を入力すれば、省略可能です。 例えば、show は省略して sho にすることができます。
- ほとんどの Guardium CLI コマンドは、コマンド・ワードとそれに続く 1 つ以上の引数で構成されています。 引数は、キーワードの場合もありますし、キーワードに変数値 (例えば、IP アドレス、サブネット・マスク、日付など) が続く場合もあります。
- コマンドとキーワードには大/小文字の区別はありませんが、エレメント名には区別があります。
- コマンド構文と使用法オプションを表示するには、コマンド・ワードの後ろに引数として疑問符 (?) を入力します。
- 語句を引用符で囲むと、検索語が正確に定義されます。

CLI へのアクセス

管理者は次の方法で CLI にアクセスできます。

- 物理的に接続した PC コンソールまたは直列伝送端末
- SSH クライアントを使用したネットワーク接続

物理コンソール・アクセス

Guardium アプライアンスへの対話式アクセスは、シリアル・ポートまたはシステム・コンソールを介して行います。

PC キーボードおよびモニター - アプライアンスのフロント・パネルのビデオ・コネクターまたは背面のビデオ・コネクターのいずれかに、1 台の PC ビデオ・モニターを取り付けることができます。

PS/2 スタイルのコネクターを持つ PC キーボードは、アプライアンスの背面にある PS/2 コネクターに取り付けることができます。 また、USB キーボードは、アプライアンスの前面または背面に配置された USB コネクターに接続できます。

シリアル・ポート・アクセス - ヌル・モデム・ケーブルを使用して、端末装置または別のコンピューターをアプライアンスの背面にある 9 ピン・シリアル・ポートに接続します。 端末装置、または接続したコンピューターの端末エミュレーターは、19200-N-1 (19200 ボー、パリティーなし、ストップ・ビット 1) で通信するよう設定する必要があります。

端末をシリアル・ポートに接続するか、キーボードとモニターをコンソールに接続すると、ログイン・プロンプトが表示されます。 ユーザー名として cli と入力し、続けて、CLI ログイン手順に進みます。

ネットワーク SSH アクセス

CLI へのリモート・アクセスは、SSH クライアントを使用して、管理 IP アドレスまたはドメイン名で使用できます。 SSH クライアントは、ほとんどのデスクトップおよびサーバー・プラットフォームで、無料または商用のものを使用できます。 UNIX SSH 接続コマンドで cli ユーザーとしてログインする場合、以下のようになります。

```
ssh -l cli 192.168.2.16
```

Guardium アプライアンスの暗号指紋を受け入れるかどうか、SSH クライアントから質問が出される場合があります。 指紋を受け入れて、パスワード・プロンプトに進んでください。

注: 初回の接続後に再度指紋について尋ねられた場合、だれか他の人物が不適切なマシンにログインさせようとしている可能性があります。

CLI ログイン

CLI へのアクセスは、admin CLI アカウント cli または 5 つの CLI アカウント (guardcli1、...、guardcli5) のうちの 1 つのいずれかで行います。 5 つの CLI アカウント (guardcli1、...、guardcli5) は、管理責任を分けられるようにするために存在しています。

GuardAPI (繰り返し行うタスクを自動化する際に役立つ一連の CLI コマンド) へアクセスするためには、アクセス・マネージャーでユーザー (GUI username/guiuser) を作成し、それらのアカウントに admin または cli ロールのいずれかを付与する必要があります。 GuardAPI を使用するために CLI に適切にログインするには、5 つの CLI アカウント (guardcli1、...、guardcli5) の 1 つでログインし、さらに「set guiuser」コマンドを発行して guiuser でログインすることが必要です。 詳しくは、『GuardAPI リファレンスの概要』または『set guiuser 認証』を参照してください。

パスワード強化

さまざまな監査およびコンプライアンスの要件を満たすため、CLI アカウントに対して以下のようなパスワード規則が適用されます。

- アカウント cli については、提供されている cli パスワードを使用するか、あるいは十分に強いパスワードを設定してこのアカウントを保護してください。 システムをインストール DVD から再ビルドした直後では、Guardium の cli ユーザーにはデフォルトのパスワード guardium が設定されています。 このパスワードはただちに変更してください。
- CLI および 5 つの CLI アカウントに有効期間を規定する (デフォルトは 90 日)。 パスワードが期限切れになると、ログイン処理の間に、パスワードの変更を要求する処理が呼び出されます。
- パスワードの長さは 8 文字以上でなければならない。
- パスワードには、以下の 4 つのクラスのうち 3 つから、1 つ以上の文字を使用する必要がある。
  - 任意の大文字
  - 任意の小文字
  - 任意の数字 (0、1、2、...)
  - 任意の非英数字 (特殊文字)
- 別の GUI ユーザー名 (guiuser) を使用したアクセスがいったん認可されると、CLI 監査証跡に、ログインに使用された CLI_USER+GUI_USER のペアが示されます。
- CLI ユーザーは、管理アカウントであると見なされ、LDAP サーバーへの接続に関係なくログイン可能でなければならないため、LDAP を介して認証することはできません。

内部データベース保守中の CLI コマンドへの制限

CLI には 3 つのコマンド・セット (汎用コマンド、特殊なサポート・コマンド、およびリカバリー・コマンド) があります。サポート・コマンドは、技術サポートがシステムを分析するために使用します。リカバリー・コマンドは、データベースがダウンした場合に、システムをリカバリーするために使用します。

初期 CLI ログインは次のようになっています。

```
Welcome to CLI - your last login was <date>
```

保守またはアップグレードのため内部データベースが停止している場合、ウェルカム・メッセージにさらに情報が追加されます。

この場合には、使用可能な CLI コマンドの数が制限されています。

```
The internal database on the appliance is currently down and CLI will be working
in "recovery mode";  only a limited set of commands will be available.
```

リカバリー モード時に使用できる CLI コマンドを以下に示します。

```
support reset-password root
restart mysql
restart stopped_services
restart system
restore pre-patch-backup
restore system
```

- アグリゲーター CLI コマンド
  このセクションでは、アグリゲーター CLI コマンドをリストします。
- アラート機能 CLI コマンド
  このセクションでは、アラート機能 CLI コマンドをリストします。
- 証明書 CLI コマンド
  証明書コマンドを使用して、証明書署名要求 (CSR) の作成、および、Guardium システム上へのサーバー証明書、CA (認証局) 証明書、またはトラステッド・パス証明書のインストールを行います。
- 構成および制御 CLI コマンド
  構成および制御用に、以下の CLI コマンドを使用します。
- diag CLI コマンド
  これらの CLI コマンドを使用して、DIAG を介してトラブルシューティング・ユーティリティーおよびメンテナンス・ユーティリティーにアクセスできます。
- ファイル処理 CLI コマンド
  これらのコマンドは、システム情報のバックアップとリストアに使用します。これらのタスクの多くは、Guardium ユーザー・インターフェースから実行できます。
- 検査エンジンの CLI コマンド
  これらの CLI コマンドは、検査エンジンの構成に使用します。
- 調査ダッシュボードの CLI コマンド
  これらの CLI コマンドは、調査ダッシュボードを構成するために使用します。
- ネットワーク構成 CLI コマンド
  ネットワーク構成 CLI コマンドは、IP アドレスの設定、結合/フェイルオーバーの処理、2 次機能の処理、およびネットワークのリセットに使用します。
- サポート CLI コマンド
  以下の CLI コマンドは、技術サポートから指示された場合にのみ使用します。
- システム CLI コマンド
  これらの CLI コマンドは、システム設定の構成に使用します。
- ユーザー・アカウント、パスワード、および認証 CLI コマンド
  これらの CLI コマンドを使用して、ユーザー・アカウント、パスワードおよび認証を構成します。

親トピック: CLI および API
関連情報:
高度な Guardium システム管理および構成 (ビデオ)

アグリゲーター CLI コマンド

このセクションでは、アグリゲーター CLI コマンドをリストします。

aggregator backup keys file

このコマンドは、共有パスワード・ファイルを指定位置にバックアップするために使用します。

構文

aggregator backup keys file <user@host:/path/filename>

パラメーター

user@host:/path/filename ファイル転送操作において、バックアップ鍵ファイルのユーザー、ホスト、および絶対パス名を指定します。 指定するユーザーには、指定したディレクトリーに対する書き込み権限が必要です。

注: 共有パスワードの使用について詳しくは、『システム共有パスワード』を参照してください。

aggregator clean shared-secret

システム共有パスワードの値を NULL に設定します。 NULL の共有パスワードを使用してユニットからアーカイブまたはエクスポートされたすべてのファイルは、共有パスワードが NULL であるシステム上でのみリストアまたはインポートすることができます。

構文

aggregator clean shared-secret

注: 共有パスワードの使用について詳しくは、『システム共有パスワード』を参照してください。

aggregator debug

統合アクティビティーに関連するデバッグ情報の書き込みを開始または停止します。 これらのコマンドは、Guardium® サポートからの指示に従ってのみ使用し、十分な情報を収集した後には必ず stop コマンドを実行してください。

注: デバッグ・モードは、7 日後に自動的に期限切れになります。

構文

aggregator debug <start | stop>

aggregator list failed imports

共有パスワードの不一致が原因でインポート操作に失敗した場合、問題のファイルは /var/importdir ディレクトリーから /var/dump ディレクトリーに移動し、元のファイル名に .decrypt_failed という接尾部が付いた形式で名前変更されます。 このコマンドは、そのようなファイルをすべてリストするために使用します。

構文

aggregator list failed imports

aggregator recover failed import

このコマンドは、障害があるインポート・ファイルの再インポート操作または再リストア操作を試行する前に、これらのファイルを移動して名前変更するために使用します。 障害があるインポート・ファイルは、接尾部 .decrypt_failed が付いて /var/dump ディレクトリーに保管されます。 インポート操作またはリストア操作を再試行する前に、これらのファイルを (.decrypt_failed 接尾部を削除して) 名前変更し、/var/importdir ディレクトリーに移動する必要があります。

構文

aggregator recover failed import <all | filename>

パラメーター

all オプションを使用すると、接尾部 .decrypt_failed が末尾にあるすべてのファイルが /var/dump ディレクトリーから移動します。filename オプションを使用する場合は、移動する 1 つのファイルを指定します。

注: 障害があるファイルの移動後、リストア操作またはインポート操作を実行する前に、エクスポートまたはアーカイブしたファイルの暗号化に使用された共有パスワードとシステム共有パスワードが一致することを確認してください。

aggregator restore keys file

このコマンドは、共有パスワード・ファイルを指定位置からリストアするために使用します。

構文

aggregator restore keys file <user@host:/path/filename>

パラメーター

user@host:/path/filename ファイル転送操作において、バックアップ鍵ファイルのユーザー、ホスト、および絶対パス名を指定します。

注: 共有パスワードの使用について詳しくは、『システム共有パスワード』を参照してください。

store aggregator drop_ad_hoc_audit_db

アグリゲーターに関する監査プロセス・レポート - タスクごとに、そのタスクに関連する日のみが含まれる一時データベースを作成します。これらの一時データベースは、14 日間 (分析用として) 保持することも、使用後すぐに削除することもできます。 この CLI コマンドは、一時データベースのパージ・ポリシーを定義します。 0 または 1 を選択します (0 - 14 日間保持、または 1 - 使用後に削除)。

構文

store aggregator drop_ad_hoc_audit_db [1|0]

Drop ad-hoc merge databases? 0

show aggregator drop_ad_hoc_audit_db

store aggregator orphan_cleanup_flag

この CLI コマンドは、アグリゲーターで静的オーファンのクリーンアップを定期的に実行するために使用します。

3 日より前のデータに対して実行するようにスケジュールされ、パージの終了時に実行されるアグリゲーターで、オーファンを消去するためにこの CLI コマンドを使用します。

この処理はユーザーによってこの CLI コマンドで開始されるため、大規模なデータベースの場合、ユーザーには処理時間の長さがわかります。

アグリゲーター上のデータ全体が網羅されますが、それらすべての実行は別の一時データベースで行われます。

注: コレクターでは、オーファンのクリーンアップは変更されません。small クリーンアップ方針で実行され、エクスポート/アーカイブ前に呼び出されます。

show aggregator orphan_cleanup_flag small、large または analyze を表示します。

store aggregator orphan_cleanup_flag

store aggregator orphan_cleanup_flag <flag>, ここで、flag は < small large analyze > のうちのいずれか 1 語です。

これらのコマンドは、アグリゲーターにのみ適用できます。

small、large または analyze のいずれかを設定した場合、オーファン・クリーンアップ・スクリプトは各マージ処理実行後に呼び出されます。

アグリゲーターのオーファン・クリーンアップでは、最後の 3 日間のオーファン・レコードは削除されませんが、3 日より前のオーファンはすべて削除されます。

small が指定されている場合、マージの完了後に開始可能な監査プロセスが、この処理によって妨げられることはありません。

large が指定されている場合、多数のオーファンがある場合に処理はより高速で実行されますが、この実行によって監査プロセスが妨げられることがあります。large が指定されている場合、監査プロセスはオーファン・クリーンアップが完了するまで開始されません。

analyze が指定されている場合、この処理では最初にオーファンの数が評価され、オーファンが 20% より多い場合は「large」方針が使用されます。「analyze」が指定されている場合、監査プロセスはオーファン・クリーンアップが完了するまで開始されません。

構文

store aggregator orphan_cleanup_flag [small | large | analyze]

表示コマンド

show aggregator orphan_cleanup_flag

store archive_static_table

この CLI コマンドは、アーカイブ静的表のオン/オフを切り換えるために使用します。

使用法: store archive_static_table <state>,

where state is on/off.

表示コマンド

show archive_static_table

store next_export_static

統合ソフトウェアでは、2 つのタイプの表が区別されています。

- 静的表 - ゆっくり拡大していきます。この種の表のデータは、時間に依存していません (GDM_OBJECT、GDM_FIELD、GDM_SENTENCE、GDM_CONSTRUCT など)。
- 動的表 - 急速に拡大していきます。データは、時間に依存しています (GDM_CONSTRUCT_INSTANCE、GDM_SESSION、GDM_CONSTRUCT_TEXT など)。

上記で説明したように、静的表のデータは時間に依存していません。時間に依存する動的表のデータは静的データにリンクされます。 静的表は非常に大きくなる可能性があるため、エクスポート/アーカイブ処理ではすべての静的データが毎日保存されるわけではありません。エクスポート/アーカイブ処理では、その最初の実行時にすべての静的データが保存され、それ以降は毎月 1 日に保存されます。毎月 1 日以外の任意の日においては、その日の間に変更された静的データのみが保存されます。この理由により、任意の日のデータをリストアするときは、その月の 1 日のデータもリストアする必要があります。これにより、確実にすべての静的データが存在するようになり、参照も壊れません。

CLI コマンド store next_export_static は、次のエクスポートにすべての静的データが含まれるようにフラグを設定するときに使用します。

構文

store next_export_static [ON | OFF]

表示コマンド

show next_export_static

store last_used

この CLI コマンドは、 パージおよび統合のときに使用します。

構文

store last_used [size | interval | logging]

表示コマンド

show last_used [size | interval | logging]

LAST_USED SIZE - 整数、デフォルトは 50

LAST_USED INTERVAL - 整数、デフォルトは 60 (分)

LAST_USED LOGGING - 整数

すべての表 - 1

GDM_Object のみ - 2

なし - 0 (デフォルト)

store aggregator static_data

store aggregator static_data [TIMESTAMP | LAST_USED_FOR_OBJECT_ONLY | LAST_USED]

注: このコマンドを使用する前に、CLI コマンド last_used logging を設定してください。

静的表の LAST_USED 列をスニファー によって更新する場合、それらの表のデータをパージするとき、 またはそれらの表のデータをアーカイブしてエクスポートするときに、この列を参照することができます。

この列の値は、 データをアグリゲーターにインポートするときに更新することもできます。

以下の 3 つのオプションがあります。

1. デフォルトでは、システムは前のバージョンと同様に動作します。 つまり、LAST_USED 列は、パージ、アーカイブ、およびエクスポートにおいて考慮されず、 インポート時に更新されることもありません。アーカイブおよびエクスポートは TIMESTAMP によって行われます。
2. LAST_USED_FOR_OBJECT_ONLY が、GDM_OBJECT 表に関してのみ考慮されます。
3. LAST_USED が、GDM_CONSTRUCT、GDM_SENTENCE、GDM_OBJECT、 GDM_FIELD、GDM_JOIN、GDM_JOIN_OBJECT に関して考慮されます。

注: オプション 2 および 3 は、このデータを収集して更新するようにスニファーが構成されている場合にのみ有効です。
注: 検証はコレクター上でのみ行われます。ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=0 の場合には、TIMESTAMP のみが許可されます。 ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=1 の場合には、 すべてのパラメーターが許可されます。ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=2 の場合には、 TIMESTAMP および LAST_USED_FOR_OBJECT_ONLY が許可されます。アグリゲーター上では、 すべてのパラメーターが許可されます。

構文

store aggregator static_data <type>

ここで <type> は、 <TIMESTAMP | LAST_USED | LAST_USED_FOR_OBJECT_ONLY> です。これは、last_used logging フラグに応じて異なります。

show/store last_used logging コマンドを使用してください。

表示コマンド

show aggregator static_data

store archive_table_by_date

この CLI コマンドは、アグリゲーターに対してのみ使用します。この CLI コマンドを使用すると、すべての静的表を日次ベースでアーカイブしたり、静的表のデータを最初の実行時にアーカイブしたり、毎月 1 日にアーカイブしたりすることができます。デフォルトでは、アグリゲーター上のデータのアーカイブは、すべての静的表を対象として日次ベースで実行されます。この CLI コマンドを ENABLE に設定すると、静的表は、毎月 1 日またはデータのアーカイブの初回実行時にのみアーカイブされます。

store run_cleanup_orphans_daily

この CLI コマンドを使用して、使用されなくなった古い構成レコードをすべて消去します。この CLI コマンドは、コレクターおよびアグリゲーターに関連し、デフォルトで有効になります。

store run_cleanup_orphans_daily

使用法: store run_cleanup_orphans_daily [on|off]

表示コマンド

show run_cleanup_orphans_daily

store max_number_collector

アグリゲーターによって管理されるコレクターの最大数を設定します。デフォルトは 10 です。

表示コマンド

show max_number_collector

store purge_age_period

パージ基準経過日数の期間を設定します。

表示コマンド

show purge_age_period

親トピック: CLI の概要

アラート機能 CLI コマンド

このセクションでは、アラート機能 CLI コマンドをリストします。

アラート機能サブシステムは、他のコンポーネントによってキューに入れられたメッセージを送信します。このようなメッセージの例には、異常検出サブシステムによってキューに入れられた相関アラートや、セキュリティー・ポリシーによって生成されたランタイム・アラートなどがあります。 アラート機能サブシステムは、SMTP サーバーと SNMP サーバーの両方にメッセージを送信するように構成できます。 アラートは syslog やカスタム・アラート・クラスに送信することもできますが、これら 2 つのオプションについては、アラート機能を開始する以外に特別な構成は必要ありません。 アラート機能コマンドには 4 つのタイプがあります。 リストのリンクを使用するか、このリストに続いて英字順に示されているコマンドを参照してください。

アラート機能の開始およびポーリング・コマンド

- stop alerter
- restart alerter
- store alerter state operational
- store alerter state startup
- store alerter poll
- store anomaly-detection poll
- store anomaly-detection state

SMTP 構成コマンド

- store alerter smtp authentication password
- store alerter smtp authentication type
- store alerter smtp authentication username
- store alerter smtp port
- store alerter smtp relay
- store alerter smtp returnaddr

SNMP 構成コマンド

- store alerter snmp community
- store alerter snmp traphost

restart alerter

アラート機能を再始動します。 次のように store alerter state operational コマンドを使用してアラート機能を停止してから開始すると、同様の機能を実行できます。

store alerter state operational off

store alerter state operational on

構文

restart alerter

stop alerter

アラート機能を停止します。

次のように store alerter state operational コマンドを使用すると、同様の機能を実行できます。

store alerter state operational off

構文

stop alerter

store alerter poll

アラート機能を開始 (on) または停止 (off) します。 インストール時のデフォルト状態は off です。 アラート機能サブシステムを再始動または停止する場合、restart alerter または stop alerter コマンドを使用することもできます。

構文

store alerter state operational <on | off>

表示コマンド

show alerter state operational

store alerter state operational

アラート機能が、SNMP トラップを送信するか SMTP を使用して E メールを送信するためにその出力メッセージ・キューを検査するまでに待機する秒数 n を設定します。 デフォルトは 30 です。

構文

store alerter poll <n>

表示コマンド

show alerter poll

store alerter state startup

システム始動時のアラート機能の自動開始を有効または無効にします。 インストール時のデフォルト状態は off です。

構文

store alerter state startup <on | off>

表示コマンド

show alerter state startup

store anomaly-detection poll

異常検出ポーリング間隔を、分単位 (n) で設定します。 これにより、Guardium® がログ・データで異常を検査する頻度を制御します。

構文

store anomaly-detection poll <n>

表示コマンド

show anomaly-detection poll

store anomaly-detection state

異常検出サブシステムを有効または無効にします。このサブシステムには、すべてのアクティブな統計アラートを実行し、ログで異常を検査し、アラート機能サブシステムの必要に応じてアラートをキューに入れる機能があります。

構文

store anomaly-detection state <on | off>

表示コマンド

show anomaly-detection state

store alerter smtp authentication password

アラート機能 SMTP 認証パスワードを、value で指定する値に設定します。 対応する show コマンドはありません。

構文

store alerter smtp authentication <value>

store alerter smtp authentication type

SMTP サーバーが必要とする認証タイプを、以下のいずれかの値に設定します。

none: 認証なしで送信。

auth: ユーザー名/パスワードでの認証。 使用する場合、以下のコマンドを使用してユーザー・アカウントおよびパスワードを設定してください。

store alerter smtp authentication username

store alerter smtp authentication password

構文

store alerter smtp authentication type <none | auth>

表示コマンド

show alerter smtp authentication type

store alerter smtp authentication username

アラート機能 SMTP E メール認証ユーザー名を、name で指定する値に設定します。

構文

store alerter smtp authentication username <name>

表示コマンド

show alerter smtp authentication username

store alerter smtp port

SMTP サーバーで listen するポート番号を、n で指定する値に設定します。 デフォルトは 25 (標準 SMTP ポート) です。

構文

store alerter smtp port <n>

表示コマンド

show alerter smtp port

store alerter smtp relay

Guardium アプライアンスが使用する SMTP サーバーの IP アドレスを設定します。

構文

store alerter smtp relay <ip address>

表示コマンド

show alerter smtp relay

store alerter smtp returnaddr

E メール・アラート返信用の E メール・アドレスを設定します。 送り返されたメッセージや E メールの障害はすべてこのアドレスに返信されます。

構文

store alerter smtp returnaddr <email address>

表示コマンド

show alerter smtp returnaddr

store alerter snmp community

アラート機能が使用する SNMP トラップ・コミュニティーを、name で指定する値に設定します。 対応する show コマンドはありません。

構文

store alerter snmp community <name>

store alerter smtp traphost

アラートを受信するアラート機能 SNMP トラップ・サーバーを、指定する IP アドレスまたは DNS ホスト名に設定します。

構文

store alerter snmp traphost <snmp host>

表示コマンド

show alerter snmp traphost

store syslog-trap

Usage: store syslog-trap ON | OFF

親トピック: CLI の概要

証明書 CLI コマンド

証明書コマンドを使用して、証明書署名要求 (CSR) の作成、および、Guardium® システム上へのサーバー証明書、CA (認証局) 証明書、またはトラステッド・パス証明書のインストールを行います。

注: Guardium は、認証局 (CA) サービスは提供しません。また、デフォルトでインストールされているもの以外の証明書をシステムに添付することもありません。独自の証明書をお求めのお客様は、サード・パーティー CA (VeriSign や Entrust など) に問い合わせる必要があります。

証明書の有効期限

証明書の有効期限が切れると機能が失われます。show certificate warn_expire コマンドを定期的に実行して、証明書の有効期限が切れていないか確認してください。コマンドにより、6 カ月以内に有効期限が切れるか既に有効期限が切れた証明書が表示されます。ユーザー・インターフェースからも、有効期限が切れる証明書がユーザーに通知されます。すべての証明書の要約を表示するには、show certificate summary コマンドを実行します。

新規証明書

新規証明書を取得するには、証明書署名要求 (CSR) を生成し、VeriSign や Entrust などのサード・パーティー認証局 (CA) に問い合わせてください。Guardium は CA サービスは提供しません。また、デフォルトでインストールされているもの以外の証明書をシステムに添付することもありません。証明書の書式は PEM で、BEGIN および END の区切り文字を含む必要があります。証明書は、コンソールから貼り付けるか、標準インポート・プロトコルのいずれかを介してインポートすることができます。

注: このアクションは、システム・ネットワーク構成パラメーターの設定が終了するまで実行しないでください。

create csr

Guardium システム用の証明書署名要求 (CSR) を作成します。 このアクションは、システム・ネットワーク構成パラメーターの設定が終了するまで実行しないでください。生成された CSR の中に、割り当てられたホスト名とドメイン名に基づく共通名 (CN) が自動作成されます。

create csr alias は、別名を使用した認証要求を作成します。

create csr gim は、gim (GIM リスナー) 用の認証要求を作成します。

create csr gui は、tomcat 用の認証要求を作成します。

create csr sniffer は、スニファー用の認証要求を作成します。

構文

create csr <alias | gimi | gui | sniffer>

restore certificate gim

証明書 gim をレコード上の最新の証明書 gim または最初に提供されたデフォルトの証明書 gim に復元します。

restore certificate gim backup は、gim 証明書を最後に保存されたスニファー gim 証明書に復元します。

restore certificate gim default は、gim 証明書をシステムに提供されたデフォルトの gim 証明書に復元します。

構文

restore certificate gim <backup | default>

restore certificate keystore

証明書鍵ストアをレコード上の最新の証明書鍵ストアまたは最初に提供されたデフォルトの証明書鍵ストアに復元します。

restore certificate keystore backup は、証明書鍵ストアを最後に保存された証明書鍵ストアに復元します。

restore certificate keystore default は、証明書鍵ストアをシステムに提供されたデフォルト値に復元します。

構文

restore certificate keystore <backup | default>

restore certificate mysql

クライアント証明書をレコード上の最新の証明書に復元します。

restore certificate mysql backup は、最後に保存された mysql 証明書を復元します。

構文

restore certificate mysql <backup>

restore certificate mysql backup client

クライアント証明書をレコード上の最新の証明書に復元します。

restore certificate mysql backup client ca は、最後に保存されたクライアント認証局 (CA) 証明書を復元します。

restore certificate mysql backup client cert は、最後に保存されたクライアント証明書を復元します。

構文

restore certificate mysql backup client <ca | cert>

restore certificate mysql backup server

サーバー証明書をレコード上の最新の証明書に復元します。

restore certificate mysql backup server ca は、最後に保存されたサーバー認証局 (CA) 証明書を復元します。

restore certificate mysql backup server cert は、最後に保存されたサーバー証明書を復元します。

構文

restore certificate mysql backup server <ca | cert>

restore certificate mysql default client

mysql クライアント証明書をシステムに提供されたデフォルト・バージョンに復元します。

restore certificate mysql default client ca は、mysql クライアント ca 証明書をシステムに提供されたデフォルト・バージョンに復元します。

restore certificate mysql default client cert は、mysql クライアント証明書をシステムに提供されたデフォルト・バージョンに復元します。

構文

restore certificate mysql default client <ca | cert>

restore certificate mysql default server

mysql サーバー証明書をシステムに提供されたデフォルト・バージョンに復元します。

restore certificate mysql default server ca は、mysql サーバー ca 証明書をシステムに提供されたデフォルト・バージョンに復元します。

restore certificate mysql default server cert は、mysql サーバー証明書をシステムに提供されたデフォルト・バージョンに復元します。

構文

restore certificate mysql default server <ca | cert>

restore certificate sniffer

証明書をレコード上の最新の証明書に復元します。

restore certificate sniffer backup は、スニファー証明書を最後に保存されたスニファー証明書に復元します。

restore certificate sniffer default は、スニファー証明書をデフォルト・スニファー証明書に復元します。

構文

restore certificate sniffer <backup | default>

restore cert_key mysql backup

mysql クライアント認証鍵またはサーバー認証鍵を最後に保存された値に復元します。

restore cert_key mysql backup client は、最後に保存された mysql クライアント認証鍵を復元します。

restore cert_key mysql backup server は、最後に保存された mysql サーバー認証鍵を復元します。

構文

restore cert_key mysql backup <client | server>

restore cert_key mysql default

mysql クライアント認証鍵またはサーバー認証鍵を、システムに提供されたデフォルト・バージョンに復元します。

restore cert_key mysql default client は、システムに提供されたデフォルトの mysql クライアント認証鍵を復元します。

restore cert_key mysql default server は、システムに提供されたデフォルトの mysql サーバー認証鍵を復元します。

構文

restore cert_key mysql default <client | server>

show certificate

すべての証明書の要約、証明書情報、別名リスト、鍵ストア内の証明書、有効期限が切れたあるいは間もなく切れる証明書を表示します。

この認証局は、Guardium CA 公開鍵で検証可能です (公開鍵は、クライアント・ソフトウェアと共に配布される CA 証明書に含まれています)。この証明書は 顧客企業固有の CN (共通名 - 例えば、「acme.com」) またはマシン固有の CN (例えば、x4.acme.com) のどちらかを保持します。これによってクライアントは、Guardium システムが有効な証明書を持っている (つまり正式な Guardium システムである) ことだけでなく、それが、クライアントが接続を意図している特定の Guardium システム (または Guardium システムのセット) であることも確証できます。

show certificate all は、すべての証明書の要約を表示します。

show certificate alias は、別名リストを表示します。

show certificate gim は、すべての GIM 証明書情報 (GIM リスナー) を表示します。

show certificate gui は、すべての Tomcat 証明書情報を表示します。

show certificate keystore は、鍵ストア内のすべての証明書と、表示する証明書をユーザーが選択するための別名リストを表示します。

show certificate mysql は、クライアントおよびサーバーの mysql 証明書情報を表示します。

show certificate sniffer は、すべてのスニファー証明書情報を表示します。

show certificate stap は、鍵ストア内のすべての S-TAP 証明書情報を表示します。

show certificate summary は、すべての証明書情報の要約を表示します。

show certificate trusted は、すべてのトラステッド証明書情報を表示します。

show certificate warn_expired は、有効期限が切れたすべての証明書または 6 カ月以内に有効期限が切れる証明書を表示します。

構文

show certificate <alias | all | gim | gui | keystore | mysql | sniffer | stap | summary | trusted | warn_expired >

show certificate keystore

鍵ストア内の証明書情報を表示します。

show certificate keystore all は、鍵ストア内のすべての証明書を表示します。

show certificate keystore alias は、表示する証明書をユーザーが選択するための別名リストを表示します。

構文

show certificate keystore <all | alias>

show certificate mysql

mysql 証明書情報を表示します。

パラメーター

show certificate mysql client は、クライアント mysql 情報を表示します。

show certificate mysql server は、サーバー mysql 情報を表示します。

構文

show certificate mysql <client | server>

store certificate

証明書を保管します。証明書を PEM 形式で貼り付け、BEGIN および END 行を追加します。

パラメーター

store certificate alias は、CSR が生成された後に証明書を鍵ストアに保管します。この CLI コマンドは、ユーザーが中間のトラステッド証明書を最初から作成することを可能にする CLI コマンド create csr alias をサポートします。これらの両方のコマンドを使用して、中間のトラステッド証明書を作成します。これらの中間のトラステッド証明書は、必要に応じて他の証明書を後で署名するためにも使用できます。

store certificate gim は、証明書、鍵 (オプション)、および CA 証明書 (GIM リスナー) を求めるプロンプトを出すことによって、カスタム gim 証明書を鍵ストア内に保管することができます。

store certificate gui は、CSR が生成された後に鍵ストア内に Tomcat 証明書を保管します。

store certificate keystore は、トラステッド証明書を一意的に識別するための 1 単語の別名を尋ね、別名を鍵ストア内に保管します。

store certificate mysql は mysql クライアント証明書およびサーバー証明書を保管します。

store certificate sniffer はスニファー証明書を保管します。

store certificate stap は S-TAP 証明書を保管します。

構文

store certificate <gim | gui | keystore | mysql | sniffer | stap >

store certificate mysql client

mysql クライアント証明書を保管します。

store certificate mysql client ca はクライアント認証局 (CA) 証明書を保管します。

store certificate mysql client cert はクライアント証明書を保管します

構文

store certificate mysql client <ca | cert>

store certificate mysql server

mysql サーバー証明書を保管します。

store certificate mysql server ca はサーバー認証局 (CA) 証明書を保管します。

store certificate mysql server cert はサーバー証明書を保管します

構文

store certificate mysql server <ca | cert>

store cert_key

システム認証鍵と mysql クライアントおよびサーバーの認証鍵を保管します。

store cert_key mysql は mysql クライアントおよびサーバーの認証鍵を保管します。

store cert_key sniffer はスニファー認証鍵を保管します。

構文

store cert_key <mysql | sniffer>

store cert_key mysql

mysql クライアントまたはサーバーの認証鍵を保管します。

store cert_key myself client mysql クライアントの認証鍵を保管します。

store cert_key myself server mysql サーバーの認証鍵を保管します。

構文

store cert_key mysql <client | server>

store cert_key sniffer

システム認証鍵を保管します。このコマンドにより、Guardium システムが (S-TAP® との通信に) 使用するシステム証明書を設定できます。証明書は、コンソールから貼り付けるか、標準インポート・プロトコルのいずれかを介してインポートすることができます。証明書の形式は PEM で、BEGIN および END の区切り文字を含む必要があります。この証明書は、guardium_ca_path を通じて S-TAP ソフトウェアから自己署名証明書が使用可能な CA によって署名されている必要があります。

store cert_key sniffer console は、鍵をコンソールに貼り付けることによってスニファー認証鍵を保管します。

store cert_key sniffer import は鍵ファイルをインポートすることによってスニファー認証鍵を保管します。

構文

store cert_key sniffer <console | import>

バックアップおよびデフォルトのオプション

バックアップまたはデフォルトのパラメーターを使用して、証明書および認証鍵を復元することを選択できます。証明書を最後に保存された証明書に復元するには、バックアップ・パラメーターを使用します。証明書を Guardium によって提供された元の証明書に復元するには、デフォルト・パラメーターを使用します。

証明書の有効期限および要約コマンド

show certificate warn_expire コマンドを定期的に実行してください。 このコマンドは、6 カ月以内に有効期限が切れる証明書について警告を出し、有効期限が切れた証明書のリストを表示します。詳細については、show certificate CLI コマンドを参照してください。すべての証明書の要約を表示するには、CLI コマンド show certificate summary を実行します。 コマンドを定期的に実行して、証明書の有効期限を確認してください。

親トピック: CLI の概要

構成および制御 CLI コマンド

構成および制御用に、以下の CLI コマンドを使用します。

? (疑問符)

コマンドを入力するとき、任意の時点で疑問符を入力すると、引数が表示されます。

構文

<コマンドの一部> ?

例

CLI> show account strike ?

使用法: show account strike <arg> ここで、arg は以下のとおりです。

?, count, interval, max

ok

CLI>

delete unit type

このコマンドを使用して、1 つ以上のユニット・タイプ属性を消去します。なお、このコマンドを使ってすべてのユニット・タイプ属性を消去できるわけではないことに注意してください。詳しくは、store unit type コマンドの後にある表を参照してください。

構文

delete unit type [manager | standalone] [aggregated] [netinsp] [network routes static] [stap] [mainframe]

commands

すべての CLI コマンドをアルファベット順のリストで表示します。

構文

commands

debug

デバッグ・モードを有効/無効にします。引数を指定しない場合、デバッグ状態が切り替わります。オプションで、状態を指定する引数を渡すことができます。

構文

debug <on | off>

eject

このコマンドは CD-ROM を取り外してイジェクトします。これは CD-ROM で配布されたパッチのインストール、またはシステムのアップグレード/再インストールの後で役立ちます。

構文

eject

delete scheduled-patch

パッチ・インストール要求を削除するには、CLI コマンド delete scheduled-patch を使用します。

パッチ・インストールの詳細については、CLI コマンド store system patch install を参照してください。

forward support email

サポート状態オプションが有効の場合 (これがデフォルトです)、このコマンドはシステム・アラートを受信する E メール・アドレスを設定します。

構文

forward support email to <email address>

表示コマンド

show support-email

iptraf

IPTraf は、基礎となるオペレーティング・システムと共に配布されるネットワーク統計ユーティリティーです。これは TCP 接続のパケットとバイトの数、インターフェースの統計とアクティビティーの指標、TCP/UDP トラフィック明細、LAN ステーションのパケットとバイトの数など、さまざまな情報を収集します。 IPTraf ユーザー・マニュアルは、インターネットの以下のロケーションで入手可能です (このリンクが機能しない場合、他のロケーションで入手できる可能性があります):

http://iptraf.seul.org/2.7/manual.html

構文

iptraf

license check

インストール済みライセンスが有効であるかどうかを示します。新しいプロダクト・キーをインストールした後、このコマンドを使用します。

構文

license check

ping

ICMP ping パケットをリモート・ホストに送信します。ネットワーク接続を検査するには、このコマンドが役立ちます。host の値は、IP アドレスまたはホスト名のいずれかです。

構文

ping <host>

quit

コマンド行インターフェースを終了します。

構文

quit

recover failed

失敗した CSV/CEF/PDF 転送ファイルを復元するコマンドです。別のエクスポート試行で使用できるように、ファイルを元のエクスポート・フォルダーに入れます。

構文

recover failed [csv|cef|pdf]

register management

指定された中央マネージャーによる管理の Guardium システムを登録します。この Guardium システムの事前登録構成は保存されます。後でユニットが登録抹消された場合には、この構成が復元されます。

構文

register management <manager ip> <port>

パラメーター

manager ip は中央マネージャーの IP アドレスです。

port は中央マネージャーによって使われるポート番号です (通常は 8443)。

restart gui

IBM® Guardium® Web インターフェースを再始動します。オプションで、GUI の再始動を 1 日に一度 (または週に一度) スケジュールするには、追加のパラメーターを使用します。HH は時間 (01 から 24)、MM は分 (01 から 60) です。W は曜日 (0 から 6) で、日曜日が 0 です。HHMM が 2 度リストされている場合、最後の項目だけが使用されます。パラメーター clear は、スケジュール済みの時間を削除します。

分類およびセキュリティー・アセスメント・プロセスを再始動するには、(GUI からではなく) CLI から restart gui コマンドを実行します。

GUI からの restart GUI の実行は Web サービスだけを再始動させます。分類およびセキュリティー・アセスメント・プロセスを含む、すべてのプロセスを完全に再始動するには、CLI から restart GUI コマンドを実行する必要があります。分類リスナーを再始動するには、管理対象ユニットごとに CLI から restart GUI コマンドを実行する必要があります。

構文

restart gui [HHMM|HHMMW|clear]

restart stopped_services

store auto_stop_services_when_full CLI コマンドで以前に停止したサービスを再始動するには、この CLI コマンドを使用します。

構文

restart stopped_services

restart system

Guardium システムをリブートします。 システムは完全にシャットダウンして再始動します。つまり cli セッションが終了します。

構文

restart system

show buffer

このコマンドは、検査エンジン・プロセスに関するバッファー使用状況のレポートを表示します。ロードで問題が発生する場合、このコマンドを実行するよう IBM 技術サポートから要請されることがあります。

構文

show buffer <log | snif>

show buffer log

この CLI コマンドを使用して、検査エンジン・プロセスのバッファーの使用状況を表示します。

show buffer snif

この CLI コマンドを使用して、スニファーのバッファーの使用状況を表示します。

show build

インストール済みソフトウェアのビルド情報を表示します (ビルド、リリース、スニフ・バージョン)。

構文

show build

show defrag

断片化したパケットを識別して、それらがネットワーク・スニッフィング・プロセスに到達する前にパケットの再構成を試みます。デフラグは SPAM または TAP デバイスを介したネットワーク・スニッフィングにのみ関連があります。

構文

show defrag

パラメーター

Packet size- パケット・サイズ。バイト単位で、最大 217 (131072)

時間間隔 - 時間間隔

トリガー・レベル - トリガー・レベル。

リリース・レベル - 秒数で指定されるリリース・レベル。最大で 2 の 31 乗 (2147483648)。

show network routes static

ユーザーに対し、所有する IP アドレスが 1 アプライアンスにつき 1 つだけ (eth0 を通じて) であっても、静的ルーティング表を使用することにより、異なるルーターからの直接トラフィックを許可します。 現在の静的ルートとその ID をリストします。

構文

show network routes static

削除コマンド

delete network routes static

show password

この CLI コマンドはパスワード機能を表示します。password disable [0|1] は、値 1 を保管することによりパスワードの使用を解除します。password expiration [CLI|GUI] [日数] はパスワード変更が要求される間隔 (日数) を表示します。デフォルトは 90 日です。password validation [ON|OFF] はパスワードに必要な強さを指定します。

構文

show password disable [0|1]

show password expiration [CLI|GUI] 90

show password validation [ON|OFF]

show security policies

セキュリティー・ポリシーのリストを表示します。

構文

show security policies

show system patch available

既にインストール済みのパッチ、およびインストールするようスケジュールされたパッチを表示します。日時とインストール状況を示します。

構文

show system patch installed

show system patch installed

既にインストール済みのパッチ、およびインストールするようスケジュールされたパッチを表示します。日時とインストール状況を示します。

構文

show system patch installed

show system public key

cli または tomcat 用の公開鍵を表示します。存在しない場合、このコマンドはそれを作成します。

注: 証明書 CLI コマンドの中の show system key、store system key を参照してください。

構文

show system public key <cli | tomcat | grdapi>

stop gui

Web ユーザー・インターフェースを停止します。

構文

stop gui

stop system

アプライアンスを停止して電源を遮断します。

構文

stop system

store apply_user_hierarchy

ユーザー階層を監査受信者に適用するには、この CLI コマンドを使用します。

ON の場合、非監査グループ受信者 (監査グループ受信者以外の受信者 (通常またはロール)) には、受信者の階層 (受信者を含む) 以下のグループ IP に関連する監査結果のみ表示されます。

構文

store apply_user_hierarchy [ON | OFF]

表示コマンド

show apply_user_hierarchy

store allow_simulation

アプライアンスでのポリシー・シミュレーション実行機能を有効 (on) または無効 (off) にします。

シミュレーションを実行するには、ルール・エンジンを介して元のトラフィックを (テストする必要のあるポリシーで) リプレイする必要があります。そのためには、アプライアンス上の元の SQL とその値を部分的に保存する必要があります。allow_simulation を有効にすると、IBM Guardium は SQL や値を保存します。無効にすると、保存しません。

構文

store allow_simulation [on|off]

表示コマンド

show allow_simulation

store alp_throttle

この CLI を使用して、ログに記録されるデータの量を制御します。

使用法: store alp_throttle <num>

ここで、<num> は -2147483647 から 2147483647 までの範囲の数値です。

デフォルトは 0 です。

0 - GDM_FLAT_LOG にログを記録せず、tapks ファイルを作成しません

>0 - GDM_FLAT_LOG にログを記録し、tapks ファイルを作成しません

<0 - GDM_FLAT_LOG にログを記録し、tapks ファイルを作成します

99999 - GDM_FLAT_LOG にログを記録しませんが、tapks ファイルを作成します

例

10 - ステートメントの 10% のログを GDM_FLAT_LOG に記録します。

10 - ステートメントの 10% のログを GDM_FLAT_LOG に記録し、tapks ファイルを作成します

store analyzer

セッションを無視: 現行の要求およびセッションの残りが無視されます。このアクションは、ポリシー違反をログに記録しますが、構成体のロギングを停止し、セッションの残りに対していかなるタイプのポリシー違反もテストしません。 このアクションは、例えば、データベースにテスト領域が含まれ、データベースのその領域に対してポリシー・ルールを適用する必要がない場合などに役立ちます。

このコマンドは「セッションを無視」のタイムアウト値を設定して、「セッションを無視」の期間を設定します。

構文

store analyzer [ignore_sess_timeout | max_open_sess]

表示コマンド

show analyzer

store auto_stop_services_when_full

ON にすると、データベースの充満率がしきい値 90% を超えた場合に内部サービスを停止します。

検査エンジン、分類、その他の収集関連サービスが停止します。また、統合のインポートと復元では新しいファイルが処理されなくなります。

修正を行うには、さまざまなサポート・コマンド (support clean audit_task、support clean log_files、support clean DAM_data、support show large_files) を使って分析し、大きな表を手動でパージしてください。

構文

store auto_stop_services_when_full [ON | OFF]

表示コマンド

show auto_stop_services_when_full

store connect oracle_parser

このコマンドを使用して、Db2 パーサーから Oracle パーサーへの接続と、接続の切断を行います。デフォルトは OFF (切断) です。

構文

store connect oracle_parser [ON | OFF]

使用法: store connect_oracle_parser [state]。state は、ON または OFF です。ON は接続、OFF は切断です。

表示コマンド

show connect oracle_parser

store csv_fetch_size

CSV_FETCH_SIZE および CSV_MAX_SIZE は、CLI を介してのみ変更できる GLOBAL_PROFILE パラメーターです。

Guardium レポートは、CSV ファイル形式でダウンロードできます。

CSV_MAX_SIZE は、レポート・エクスポート・メニューから「レコードをすべてダウンロード」をクリックすると取得される CSV ダウンロードのサイズを制御するために使用されます。

CSV_FETCH_SIZE は、レコードの合計数を制御するために、レポート REST サービスによって使用されます

注: csv_max_size は、変更を有効にするために GUI を再始動する必要があります。csv_fetch_size は、変更を有効にするために GUI を再始動する必要はありません。

表示コマンド

CLI> show csv_fetch_size

使用法

CLI> store csv_fetch_size

使用法: store csv_fetch_size <number>

ここで、number は 0 より大きい数値です。

store csv_max_size

CSV_FETCH_SIZE および CSV_MAX_SIZE は、CLI を介してのみ変更できる GLOBAL_PROFILE パラメーターです。

Guardium レポートは、CSV ファイル形式でダウンロードできます。

CSV_MAX_SIZE は、レポート・エクスポート・メニューから「レコードをすべてダウンロード」をクリックすると取得される CSV ダウンロードのサイズを制御するために使用されます。

CSV_FETCH_SIZE は、レコードの合計数を制御するために、レポート REST サービスによって使用されます

注: csv_max_size は、変更を有効にするために GUI を再始動する必要があります。csv_fetch_size は、変更を有効にするために GUI を再始動する必要はありません。

表示コマンド

CLI> show csv_max_size

使用法

CLI> store csv_max_size

使用法: store csv_max_size <number>

ここで、number は 0 より大きい数値です。

store default_queue_size

この CLI コマンドを使用して、構成パラメーター ADMINCONSOLE_PARAMETER.DEFAULT_QUEUE_SIZE を制御します。 デフォルトは 25 です。値の範囲は 25 から 300 です。

値を変更したら、スニファーを再始動する必要があります。

構文

store default_queue_size <N>。N は、25 から 300 までの範囲の数値です。

表示コマンド

show default_queue_size 25

store defrag

このコマンドを使用すると、デフラグのデフォルトを復元したり、デフラグ・サイズを設定したりすることができます。このコマンドを入力した後、変更内容を有効にするには restart inspection-core コマンドを発行する必要があります。デフラグは SPAM または TAP デバイスを介したネットワーク・スニッフィングにのみ関連があります。

構文

store defrag [default | size <s> interval <i> trigger <t> release <r>]

表示コマンド

show defrag

パラメーター

default - デフォルト・サイズを復元します。

s - パケット・サイズ。バイト単位で、最大 2^17 (131072)

i - 時間間隔

t - トリガー・レベル

r - 秒数で指定されるリリース・レベル。最大で 2 の 31 乗 (2147483648)。

store delayed_firewall_correlation

この CLI コマンドを使用して、暗号化解除の相関が行われるまでユーザー接続を保留します。

構文

store delayed_firewall_collection [on | off]

表示コマンド

show delayed_firewall_correlation

store full-bypass

このコマンドは緊急用です。Guardium システムによってトラフィックが予期せずブロックされている場合にのみ、これを使用します。これを on にすると、すべてのネットワーク・トラフィックはシステムを直接通過するようになり、Guardium システムからは「認識」できません。

このコマンドを使用するときには、admin ユーザー・パスワードを求められます。

構文

store full-bypass <on | off>

store gdm_analyzer_rule

アナライザー・ルール - いくつかのルールをアナライザー・レベルで適用することができます。アナライザー・ルールには、例えば、ユーザー定義の文字セット、ソース・プログラムの変更、ファイアウォールの監視モードや非監視モードなどがあります。以前のリリースでは、ポリシーやルールは、ロギング状態での要求処理の最後に適用されていました。これは、場合によっては、それらのルールに基づく決定に遅れが生じることを意味していました。アナライザー・レベルでルールを適用するということは、より早い段階で決定を行えることを意味します。

注: ソース・プログラムの変更に関するアナライザー・ルールを適用する場合、 ソース・プログラムがパターンに完全一致しない場合は、 パターンの末尾に .* を追加して、ソース・プログラムの末尾にスペースがある (ユーザーには見えない) 可能性に対処してください。

構文

store gdm_analyzer_rule [active_flag | new]

store gdm_analyzer_rule active_flag

使用法: store gdm_analyzer_rule active_flag <id> <on|off>

ここで <id> は、ルール ID です。

GDM アナライザー・ルールのリストを表示するには、CLI コマンド show gdm_analyzer_rule を使用してください。

store gdm_analyzer_rule new

ルールの説明を入力します (オプション)。

ルールのタイプを入力します (必須)。

表示コマンド

show gdm_analyzer_rule

store gdm_analyzer_rule new

Guardium CLI を使用して、直接正規表現のアナライザー・ルールをマスク UID チェーン・パターンに追加します。

CLI> store gdm_analyzer_rule new

ルールの記述を入力してください: new rule 4

ルール・タイプ:

1. ソース・プログラムを変更する

2. 代替文字セットを設定する

3. 判定を送信する

4. HADOOP の除外

5. プロトコルとポートを定義する

6. パケット後のセッションを無視する

7. ログイン情報が欠落している場合に、空の Oracle DB ユーザーを設定する

8. MS SQL ログインを強制する

9. 文字列を変換する

ルール・タイプを選択してください (必須): 9

パターンを入力してください (必須、正規表現文字列): (.*)(-ppassword)(.*)

形式を入力してください (必須、正規表現文字列): ¥¥¥¥1-p****¥¥¥¥3

ルールを今すぐアクティブ化しますか? (はい/いいえ)

Y

ok

store gdm_http_session_template

この CLI コマンドを使用して、HTTP セッションのテンプレートを設定します。

使用法

```
store gdm_http_session_template [activate] [add] [deactivate] [remove]
```

表示コマンド

```
show gdm_http_session_template
```

テンプレート情報の取得を試行します。時間がかかる場合があります。 お待ちください。

表 1. store gdm_http_session_template

ID#	アクティブな URL の正規表現	セッションの正規表現	ユーザー名正規表現	Login_Session の正規表現	コメント	Logout_Session_ID	Logout_URL_Regex
1	1	Cookie.*PHPSESSID=([[:a	.*user_name=([[:alnum:]	Set-Cookie:.*PHPSESSID=	削除される HTTP セッションの例		
2	1	Cookie.*PSJSESSIONID=([	.*SignOnDefault=([[:aln		HTTP セッションの例	cmd=logout	
3	1	Cookie.*JSESSIONID=([0-	.*username=([[:alnum:]]	Set-Cookie:.*JSESSIONID	HTTP セッションの例		Logout.jsp

外部ログの保管

このコマンドを使用して、外部ログのファイル・サイズ、フラッシュ期間、gdm エラーおよび状態を設定します。

このルールは、以下の CLI コマンドが実行される場合のみ表示されます。

store log external state on

そして外部ログは、ポリシー・アクションとして表示されます

状態をチェックするための CLI コマンド:

show log external state

このアクションを有効および無効にするための CLI コマンド:

store log external state on/off

使用法

```
store log external [file_size] [flush_period] [gdm_error] [state]
```

使用法: store log external gdm_error <state>

where state is on/off. 'on' is to enable and 'off' is to disable.

使用法: store log external file_size <num>

ここで、<num> はファイルのサイズです。

デフォルトは 4096 バイトです。

使用法: store log external flush_period <num>

ここで、<num> はフラッシュ期間です。

デフォルトは 60 秒です。

使用法: store log external state <state>

where state is on/off. 'on' is to enable and 'off' is to disable.

表示コマンド

```
show log external [file_size] [flush_period] [gdm_error] [state]
```

store monitor gdm_statistics

この CLI コマンドは、ユニット使用状況に関する情報を取得するために使用します。デフォルトは 1 (1 時間おきにスクリプトを実行する) です。

構文

```
CLI> store monitor gdm_statistics
USAGE: store monitor gdm_statistics <hour>, where hour is value from 0 to 24.
       Default value is 1, means to run the script every hour.
       Value 0, means not to run the script.
```

表示コマンド

CLI> show monitor gdm_statistics

gdm_statistics モニターを無効にします。

store gui

store gui [port | session_timeout | csrf_status]

IBM Guardium アプライアンス管理インターフェースで接続を受け入れる TCP/IP ポート番号を設定します。デフォルトは 8443 です。**n** は 1024 から 65535 までの範囲の値でなければなりません。別の目的で必須であるか使用中のポートを使用しないようにしてください。

セッションのタイムアウトの設定 - アクティビティーのない状態が何秒続いたら、タイムアウトにするかを指定します。 アクティビティーがないためタイムアウトに達した場合、IBM Guardium に再びログオンする必要があります。デフォルトの長さは 900 秒 (15 分) です。

Cross-site Report Forgery (CSRF) (ON | OFF) の設定 - 『GUI の概要』ヘルプ・トピックで、『**CSRF および 403 アクセス許可エラー**』のセクションを参照してください。アップグレード済みのシステムでは、デフォルト値が有効になっています。特定の Web ブラウザー機能 (例えば、F5/CTRL-R/最新の情報に更新/再読み込みや、戻る/進む) の使用を試みると、403 アクセス許可エラー・メッセージが出されます。

新しいセッション・タイムアウト値は、次回の GUI 再始動後に初めて有効になります。

構文

store gui port <n>

store gui session_timeout <n>

store gui csrf_status [on | off]

表示コマンド

GUI ポート番号、状態、セッション・タイムアウト (秒)、または CSRF 状況の一部または全部を表示します。

構文

show gui [port | state | all | session_timeout | csrf_status]

store gui cache

この CLI コマンドを使用して、Web ブラウザーのキャッシングをオンまたはオフ (有効または無効) に切り替えます。

応答:

The parameter has been changed.(パラメーターが変更されました。)

Restarting gui (GUI を再始動しています)

Changing to port 8443 (ポート 8443 に変更しています)

Stopping..... (停止しています.....)

Safekeeping xregs

ok

ブラウザーのキャッシングのデフォルト設定は「有効」です。

キャッシュの設定を変更する処理によって、自動的に Guardium Web サーバーが再始動されます。

Firefox の場合は、設定を有効にするために、それぞれのブラウザー上のキャッシュをクリアする必要があります。

構文

store gui cache [ON | OFF]

表示コマンド

show gui cache

store gui session_timeout

タイムアウトになるまでの、アクティビティーのない状態の時間の長さ (秒) を設定します。アクティビティーがないためタイムアウトに達した場合、IBM Guardium に再びログオンする必要があります。デフォルトの長さは 900 秒 (15 分) です。

構文

store gui session_timeout

表示コマンド

show gui session_timeout

store gui csrf_status

この CLI コマンドは、 Cross-site Request Forgery (CSRF) 状況を有効化または無効化するときに使用します。

構文

store gui scrf_status [on | off]

表示コマンド

show gui scrf_status

store gui xss_status

この CLI コマンドは、クロスサイト・スクリプティング (XSS) 状況を有効化または無効化するときに使用します。アップグレード済みのシステムでは、デフォルトでこのオプションは有効になっています。

構文

store gui xss_status [on | off]

表示コマンド

show gui xss_status

store gui hsts_status

この CLI コマンドは、HSTS (HTTP Strict Transport Security Filter) を有効化または無効化するときに使用します。アップグレードされたシステムではこのオプションはデフォルトで無効になっており、有効な証明書がインストールされた後にオンにすることが推奨されています。 詳しくは、トピック『ブラウザーの SSL 証明書チャレンジを回避するためのアプライアンス証明書のインストール方法』を参照してください。

構文

store gui hsts_status [on | off]

表示コマンド

show gui hsts_status

store installed security policy

policy-name で指定されるセキュリティー・ポリシーを、インストール済みセキュリティー・ポリシーとして設定します。

構文

store installed security policy <policy-name>

表示コマンド

show installed security policy

store keep_psmls

この CLI コマンドは、Guardium アプリケーションのユーザーの作成時に使用した現在のレイアウト/プロファイル/ポートレットを保持するときに使用します。この CLI コマンドを ON に設定してからアップグレードを実行すると、旧バージョンの psml が保持されます。

構文

store keep_psmls [ON | OFF]

show keep_psmls

store ldap-mapping

LDAP マッピング・パラメーターを保管します。これにより、LDAP サーバー・スキーマ用のカスタム・マッピングが可能になります。このコマンドは、E メール、ファーストネーム、およびラストネーム属性に関する LDAP サーバー・スキーマへのカスタマイズされたマッピングを可能にします。任意の LDAP サーバー・タイプ (Active Directory、Novell Directory、Open LDAP、Sun One Directory、Tivoli® Directory) の間の転送を可能にするために、paging パラメーターが使用されます。paging パラメーターを on に設定しても、サーバーでページングがサポートされない場合には、ページングなしで検索が実行されます。

ページングの例: CLI コマンド **ldap-mapping paging** が ON に設定された場合、Microsoft Active Directory は LDAP インポート構成画面の制限値で定義された最大数のユーザーをダウンロードします。CLI コマンド **ldap-mapping paging** が OFF に設定された場合、Active Directory は制限の設定値にかかわらず、最大 1000 ユーザーだけをダウンロードします。制限の設定値までユーザーをダウンロードするには、他のすべての LDAP サーバー構成で CLI コマンド **ldap-mapping paging off** を使用する必要があります。

注: CLI ldap-mapping 属性を変更するたびに、更新の前に、IBM Guardium GUI の LDAP インポート構成画面の「既存の変更のオーバーライド」 を選択する必要もあります。CLI ldap-mapping の E メール、ファーストネーム、またはラストネーム属性を変更して LDAP ユーザーをインポートするたびに、この操作が必要です。

表示コマンド

show ldap-mapping [email] [firstname][lastname] <名前>

show ldap-mapping paging ON|OFF

新しいパラメーターを有効にするには、CLI の GUI 再始動が必要です。

例

いくつかの例を示します。

store ldap-mapping firstname name

store ldap-mapping lastname sn

store ldap-mapping email mail

store ldap-mapping paging on

属性が次のように指定されている場合、検出される最初の属性がマッピング・プロセスで使われます。これが適切でない場合は、いずれかの例を使って特定の属性にマップしてください。

firstname 属性の値: gn,givenName,name

lastname 属性の値: attribute: sn,surname,name

email 属性の値: userPrincipalName,mail,email,emailAddress,pkcs9email,rfc822Mailbox

paging の値: on, off

store license

このコマンドは、新規ライセンス・キーをアプライアンスに適用します。

ライセンス・キーには、オーバーライド・タイプと追加タイプの 2 種類があります。オーバーライド・タイプは現在インストールされているライセンスを置換し、追加タイプ・ライセンスは現在インストールされているライセンスに追加されます。 追加タイプ・ライセンスでは、機能の追加以外は行われません。新規機能が使用可能になる場合のほか、関連があれば、有効期限が更新されたり、残りのスキャン数やデータ・ソース数が増えたり、特定のライセンスの数値フィールド (管理対象ユニットの数など) が置換されたりします。

構文

store license

表示コマンド

show license

例

store license コマンドを使用するとき、次のように、新しいプロダクト・キーを貼り付けるよう求められます。

CLI> store license

IBM Guardium から受け取った文字列を貼り付けて、Enter キーを押します。

新しいプロダクト・キーをコピーしてカーソル位置に貼り付けた後、Enter を押します。プロダクト・キーには改行や空白文字が含まれず、常に末尾の等号 (これも含まれます) で終わります。一連のメッセージが表示され、その最後は次のようになります。

We recommend that the machine be rebooted at the earliest opportunity in order to complete the license updating process.

ok

CLI>

この時点で restart gui コマンドを実行します。

store log classifier level

分類のデバッグ・レベルを、表示されるいずれかの値に設定します。

構文

store log classifier level DEBUG|INFO|WARN|ERROR|FATAL

表示コマンド

show log classifier level

store log sql parser_errors

構文的に間違った SQL コマンドのロギングを設定します。

構文

store log sql parser_errors [on|off]

注: 保管コマンドを発行した後、変更内容を適用するには検査エンジンを再始動する必要があります。

表示コマンド

show log sql parser_errors

store log object_join_info

object_join のロギングを設定します。

結合表は、多対多の関係を実装するための 1 つの方法です。結合エンティティーは、SELECT SQL ステートメントで表を結合する場合に使用します。

構文

store log object_join_info [on | off]

表示コマンド

show log object_join_info

store log session_info

スニファー関連

構文

store log session_info [on | off]

表示コマンド

show log session_info

store log exception sql

on に設定された場合、例外のロギング時に SQL コマンド全体をログに記録します。

構文

store log exception sql <on | off>

表示コマンド

show log exception sql

store logging granularity

ロギング細分度を、指定された分数に設定します。構文に示されているいずれかの分の値を使用する必要があります。デフォルトは 60 です。

構文

store logging granularity <1、2、5、10、15、30、または 60>

表示コマンド

show logging granularity

store max_audit_reporting

監査レポートしきい値を表示します。デフォルトは 32 です。監査プロセスでレポートを定義するとき、(FROM-TO フィールドで定義される) レポートの日数は特定のしきい値を超えることができません (デフォルトでは 1 カ月)。この CLI コマンドの使用法について詳しくは、『コンプライアンス・ワークフロー自動化』ヘルプ・トピックの『ワークフロー・プロセス、一元管理および統合』のセクションを参照してください。

構文

store max_audit_reporting

表示コマンド

show max_audit_reporting

store max_result_set_size

max_result_set_size を保管します。このデフォルト値は 100 (サイズの範囲は 1 から 65535) で、戻りデータを監視するときの検査エンジンの調整に役立ちます。このコマンドは、結果セットの合計サイズの制限を設定します。このパラメーターはあらゆる種類のデータベースに対して機能します。この値が、定義済みのしきい値を超える場合には、アナライザーは影響を受けるレコード値を計算するためにデータを取り出しません。

構文

store max_result_set_size <サイズ>

表示コマンド

show max_result_set_size

store max_result_set_packet_size

max_result_set_packet_size を保管します。このデフォルト値は 32 (サイズの範囲は 1 から 65535) で、戻りデータを監視するときの検査エンジンの調整に役立ちます。このコマンドは、応答のパケット・サイズの制限を設定します。このパラメーターはあらゆる種類のデータベースに対して機能します。この値が、定義済みのしきい値を超える場合には、アナライザーは影響を受けるレコード値を計算するためにデータを取り出しません。

構文

store max_result_set_packet_size <サイズ>

表示コマンド

show max_result_set_packet_size

store max_tds_response_packets

max_tds_response_packets を保管します。このデフォルト値は 5 (サイズの範囲は 1 から 65535) で、戻りデータを監視するときの検査エンジンの調整に役立ちます。このコマンドは、応答でのパケット数の制限を設定します。このパラメーターは MS SQL でのみ機能します。この値が、定義済みのしきい値を超える場合には、アナライザーは影響を受けるレコード値を計算するためにデータを取り出しません。

構文

store max_tds_response_packets <サイズ>

注: max_tds_response_packets (表データ・ストリーム) は MS SQL Server および Sybase だけに適用されます。

表示コマンド

show max_tds_response_packets

store maximum query duration

照会の最大秒数を、**n** で指定された値に設定します。デフォルトは 180 です。この値をデフォルトより大きく設定した場合、照会の処理でシステムが過負荷になる可能性が増すため、そのように設定**しない**ことをお勧めします。なお、管理者ポータルの実行状況モニター・パネルからこの値を設定することもできます。

構文

store maximum query duration <n>

表示コマンド

show maximum query duration

store monitor [buffer | custom_db_usage | gdm_statistics]

この CLI コマンドを使用して、「IBM Guardium モニター」タブのバッファー使用状況モニター・レポート内の表示情報を取り出すスクリプトの実行間隔を設定する monitor buffer を保管します。

構文: store monitor buffer

以下の CLI コマンドを使用して、状態をオンに設定してこのジョブの実行時刻を指定する monitor custom_db_usage を保管します。

構文

```
CLI> store monitor custom_db_usage
USAGE: store monitor custom_db_usage <state> <hour>
where state is on/off.
If state is on, specify the hour to run.
Valid value is number from 0 to 23
```

以下の CLI コマンドを使用して、ユニット使用状況に関する情報を取得する monitor gdm_statistics を保管します。デフォルトは 1 (1 時間おきにスクリプトを実行する) です。

構文

```
CLI> store monitor gdm_statistics
USAGE: store monitor gdm_statistics <hour>, where hour is value from 0 to 24.
       Default value is 1, means to run the script every hour.
       Value 0, means not to run the script.
```

表示コマンド

show monitor buffer

show monitor custom_db_usage

show monitor gdm_statistics

store mysql_utf8mb4

4 バイトの UTF-8 エンコード (utf8mb4) のサポートを有効にします。

このコマンドは、4 バイトの UTF-8 文字を正しくキャプチャーして保管するように、Guardium スニファー・プロセスおよび内部データベースを変更します。 ご使用の環境のデータ・ソースに 4 バイト文字が含まれている場合 (中国語、日本語、および韓国語の表意文字に使用されている場合など)、utf8mb4 が有効であると便利な場合があります。

このコマンドを使用するときは、以下のことを確認してください。

- 4 バイト文字をキャプチャーして保管するために必要な追加の処理は、Guardium システムのパフォーマンスに悪影響を与えます。このため、ご使用の環境で 4 バイト文字のサポートを必要としない限り、utf8mb4 を有効にしないでください。
- 集約された環境または一元管理された環境で 4 バイトの UTF-8 エンコードをサポートする必要がある場合は、環境内のすべての Guardium システムで utf8mb4 を有効にする必要があります。環境内の一部のシステムでのみ utf8mb4 を有効にすると、集約が失敗したりレポートが正しく表示されないなど、問題が発生することがあります。
- utf8mb4 を有効にする前に収集されたデータや集約されたデータは、utf8mb4 を有効にした後も引き続き使用可能であり、正しく機能します。

注意:
store mysql_utf8mb4 コマンドを使用して 4 バイトの UTF-8 のサポートを有効にした後で、変更を元に戻すことはできません。Guardium システムで utf8mb を有効にした後、4 バイトの UTF-8 文字のサポートを除去する唯一の方法は、システムを完全に再構築することです。

構文

store mysql_utf8mb4

表示コマンド

show mysql_utf8mb4

例

```
> show mysql_utf8mb4
mysql configuration NOT set with UTF8MB4.
ok

> store mysql_utf8mb4
Attempting to change the mysql config file. 時間がかかる場合があります。お待ちください。
Start to modify mysql config file
Restarting mysql
Mysql has been restarted. Please exit CLI and log back on.
The parameter IS_UTF8MB4 has been changed to 1.

> show mysql_utf8mb4
mysql configuration set with UTF8MB4.
ok
```

store packet max-size

スニファーからのパケットの最大サイズを制限します。

構文

store packet max-size 1536

表示コマンド

show packet max-size

store pdf-config

このコマンドを使用すると、(ヘッダー/フッターを除く) PDF イメージ本文コンテンツの pdf フォント・サイズと pdf 用紙の向きを変更できます。

サイズは 1 (最小) から 10 (最大) までの範囲で、デフォルト値は 6 です。

用紙の向き (orientation) は 1 (横長) または 2 (縦長) です。デフォルト値は 1 です。

CLI コマンドを入力して Enter キーを押すと、変更内容が直ちに有効になります。

構文

store pdf-config [orientation | size]

表示コマンド

show pdf-config [orientation | size]

store pdf-config multilanguage_support

英語 (英語バージョンで使用) と言語 C/J (中国語/日本語で使用) では、静的 PDF ジェネレーター構成ファイルが異なります。この CLI コマンドを使用して、PDF ジェネレーターのフォントを定義します。Default は英語です。Multi-language は言語 C/J です。

構文

```
CLI> store pdf-config multilanguage_support
Current setting is Default

1  Default
2  Multi-language
Please select the option (1,2, or q to quit)
```

表示コマンド

show pdf-config multilanguage_support

store populate_from_query_maxrecs

照会からのグループおよび別名の取り込みに使用できるレコードの最大数を設定します。

この CLI コマンドを使ってレコード最大数の値を設定するときには、注意が必要です。高く設定し過ぎると、照会からグループに取り込む プロセスが完了しない可能性があります。最大しきい値は動的で、システム負荷とメモリー使用状況に依存します。この CLI コマンドの最大値は 200000 に制限されています。

構文

store populate_from_query_maxrecs 100000

表示コマンド

show populate_from_query_maxrecs

store product gid

保管される固有のプロダクト <n> GID 値を設定します。

構文

store product gid <n>

表示コマンド

show product gid

store purge object

不必要なオブジェクトがパージされる経過日数を設定します。show purge objects age コマンドを使用すると、パージ経過日数を維持する対象となる各オブジェクト・タイプの索引、オブジェクト名、経過日数を示す表が表示されます。次に、その表の適切な索引をコマンド内で使用して、パージ経過日数を設定します。

注: ユニット・タイプが管理対象ユニット、Manager、またはスタンドアロン・ユニットの間で変更されるとき、日数の値はデフォルト (90 日) に設定されます。

構文

store purge object age <索引> <日数>

表示コマンド

show purge object age

例

イベント・ログを 30 日間にわたって保持する必要が生じたとします。まず show purge objects age コマンドを発行して索引を判別します (表を使用しないでください。実際のリストは異なる可能性があります)。次に store purge object コマンドを入力します。

CLI>show purge objects age

Index Name, Age

1. 一元管理永続処理、7
2. S-TAP イベント・ログ、14
4. アセスメント・テスト、7
5. 一元管理一時ポリシー、7
6. S-TAP 変更履歴、14
7. Kerberos 認証情報、1
8. コメント履歴、60
9. コメント・ローカル履歴、60
10. グラフ呼び出し履歴、90

. . .

ok

CLI> **store purge object age 2 30**

ok

store quartz_thread_run

この CLI コマンドは技術サポートによって使用されます。

Java™ 仮想マシンでは、アプリケーションが複数のスレッドを使用できます。スレッドとはプログラム実行の断片です。

同時に実行可能なスレッドの数を設定するには、CLI コマンド store quartz_thread_num を使用します。

このコマンドを使用すると、同時に実行されるスレッドが多すぎる場合の互いの競合を軽減できます。

CLI コマンド show quartz_thread_num は、同時に実行される Quartz スケジューラー・スレッドの数を表示します。

構文

store quartz_thread_run <number>

使用法: store quartz_thread_num <number> (ここで number は 3 から 15 までの範囲、デフォルト値は 5)

表示コマンド

show quartz_thread_num

org.quartz.threadPoll.threadCount= 5

store remotelog

リモート・ロギングの使用を制御します。システム・メッセージに加えて、統計アラートおよびポリシー・ルール違反メッセージを (オプションで) syslog に書き込むことができます。それぞれの **facility.priority** の組み合わせごとに、メッセージを特定のホストに送信することができます。また、このコマンドは、オプションのポート番号を介したリモート・ロギングの使用も制御することができ、必須のプロトコル (UDP または TCP) も指定できます。このコマンドは TCP をサポートする任意の syslog 実装に対して機能します。

リモート・ロギングを有効にする場合、受信側ホストでこの機能が既に有効になっていることを確認してください (『注』を参照)。

構文

store remotelog [help|add|clear] facility.priority host [optional port number:mandatory protocol (UDP または TCP)]

表 2. store remotelog のパラメーター

パラメーター	記述
help	サポートされる機能と優先度を表示します。
add	指定された facility.priority の組み合わせを、指定されたリモート・ホストに送られるメッセージのリストに追加します。
clear	指定された facility.priority の組み合わせを、指定されたホストに送られるメッセージのリストから消去します。
facility	デーモンを使用します。IBM Guardium アプライアンスによって発行されるほとんどのメッセージは daemon 機能から出されます。
priority	これは alert、all、crit、debug、emerg、err、info、notice、warning のいずれか 1 つです。 アラートと違反に関する標準的な IBM Guardium 重大度コードは、次のようにマップされます。 Guardium severity / Syslog priority INFO / info LOW / warning MED / err HIGH / alert
host	この facility.priority の組み合わせを受信するホストを指定します。
optional port number (オプションのポート番号)	
mandatory protocol	UDP または TCP。

注:

リモート・ロギングを受け入れるよう受信側システムを構成するには、そのシステムの /etc/sysconfig/syslog を編集して -r オプションを含めます。例:

```
SYSLOGD_OPTIONS=-r -m 0
```

その後、次のように syslog デーモンを再始動します。

```
/etc/init.d/syslog  restart
```

Linux での標準的な syslog ファイルの名前は、次のとおりです。

```
/var/log/messages
```

コモン・クライテリアでは、Guardium システムからリモート syslog サーバーへのすべての通信は暗号化される必要があります。リモート syslog サーバーへの通信は平文であってはなりません。

CLI コマンド

show remotelog

store remotelog ?

store remotelog add ?

store remotelog add encrypted

使用法: store remotelog add encrypted <facility.priority> <host[:port]> <tcp|udp>

使用可能な機能: all auth authpriv cron daemon ftp kern local0 local1 local2 local3 local4 local5 local6 local7 lpr mail mark news security syslog user uucp

使用可能な優先順位: alert all crit debug emerg err info notice warning

注:

暗号化されたリモート・ログ・メッセージをサーバーに送信する場合、サーバー内の rsyslog 構成は、暗号化されたメッセージを受け入れる必要があります。

クライアントおよびサーバー上の暗号化設定は TCP モードでのみ機能します。

同じリモート・サーバー上での 1 つのモードから別のモードへの切り替え: 指定されたモードと同期するように構成ファイルを変更する必要があり、リモート・サービスを再始動する必要があります。

例

```
store remotelog add non_encrypted
store remotelog clear
g32.guard.swg.usma.ibm.com> show remotelog
*.*    @9.70.148.175:10514
```

この例を使用して、証明書を ca.pem として /etc/pki/rsyslog/ に保管します。これにより新しいウィンドウが開き、証明書を貼り付けることをユーザーに求めます。

```
store remote add encrypted all.all <IP address>:<port number> tcp
```

syslog の暗号化

アラートおよびその他のメッセージを SIEM システムなどのリモート syslog 受信者に転送できます。コレクターまたはアグリゲーターからリモート syslog 受信者まで、このメッセージ・トラフィックを暗号化することができます。

注: 暗号化は TCP モードでのみ機能します。デフォルトでは、syslog 転送には UDP が使用されるため、暗号化が必要な場合は CLI コマンド store remotelog で TCP を指定します。

作業を開始する前に、以下を実行してください。

ここに記載されている手順は、暗号化ホストにトラフィックを送信するすべてのコレクターまたはアグリゲーター上で繰り返す必要があります。

リモート syslog 受信者によって使用される証明書が必要です。この証明書を Guardium システム上に保管します。

1. CA (認証局) (Verisign、Thwate、Geotrust、GoDaddy、Comodo、自社内など) から取得した公開証明書を使用できる状態にします。
2. 暗号化された syslog の送信元となる個々の Guardium システムで CLI にログインします。コマンドを実行する前に、該当する証明書 (PEM 形式) を CA から取得して、証明書の「Begin」と「End」の行を含めてクリップボードにコピーします。
3. 次の CLI コマンドを入力します: store remotelog add encrypted daemon.all <暗号化されたリモート・ホストの IP アドレス>:<リモート・ホストのポート番号> tcp
   注: Guardium はデーモンを使用してアプリケーション・イベントを送信するため、この例ではデーモンを使用しています。
4. 次の指示が表示されます。

   ```
   Please paste your CA certificate, in PEM format. Include the BEGIN and END lines, and then press CTRL-D.
   ```

   PEM 形式の証明書をコマンド行に貼り付け、**CRTL-D** を押します。Guardium はこの入力を取り込み、/etc/pki/rsyslog/ca.pem として保管します。

   保管操作の成功または失敗を通知するメッセージが続きます。

   成功した場合、Guardium は正しい鍵を使用して暗号化トラフィックをリモート・システムに送信できます。

5. syslog トラフィックを暗号化ホストに送信するすべてのコレクターおよびアグリゲーターに対してこの手順を繰り返します。

store s2c

ADMINCONSOLE のいくつかの構成可能パラメーターを設定します。これらのパラメーターは、サーバーからクライアントへの (S2C) トラフィックをスロットルするために使用されます。

注: この CLI コマンドは、IBM Guardium 技術サービスから指示された場合にのみ使用してください。

最小値と最大値は次のとおりです:

ANALYZER_S2C_IGNORE = {0,1,2,3}

MAX_S2C_VELOCITY (K バイト/秒) - 数値 >=0 かつ <= 2147483647

MAX_S2C_INTERVAL (秒) - 数値 >=1 かつ <= 2147483647

CLI コマンド store throttle も参照してください。

構文

store s2c

使用法: store s2c ignore I maxrate M maxinterval T

ここで、0<=I<=3 (レベル)、0<=M<=2147483647 (K/秒)、および 1<=T<=2147483647 (秒) です。あるいは store throttle default を使用します

store s2c ignore 3 maxrate 300 maxinterval 5007

新しい構成は、CLI コマンドの restart inspection-core コマンドが実行された後で有効になります。

表示コマンド

show s2c

スロットル S2C パラメーター (デフォルト):

無視: 0

最大速度: 999999

最大間隔: 30

ANALYZER_S2C_IGNORE (0,1,2,3) - シナリオに基づいて、s2c スロットル・メカニズムの on/off を切り替えます。このフラグはビットに基づいています。0 は s2c スロットル・メカニズムを OFF にします。1 は「シナリオ 1」に示されている機能を on に設定し、2 は「シナリオ 2」で示される機能を on にします。3 は両方を on にします。

MAX_S2C_VELOCITY - 最大速度 (K バイト/秒)。この速度を超えた場合、アナライザーは CLI コマンド「セッションを無視」または「セッション応答を無視」要求を S-TAP® またはスニファーに送ります。

MAX_S2C_INTERVAL - CLI コマンド「セッションを無視」または「セッション応答を無視」要求が出される時間間隔 (秒数、デフォルトは 30 秒)。

シナリオ 1

大きな照会の途中で、スニファーが S-TAP またはネットワークからトラフィックを受信し始めます。すべての着信パケットは DB サーバー応答であるため、アナライザーは新しいセッションを作成しません。したがってロガーおよびルール・エンジンには情報が送られません。この種類のトラフィックはスニファーにとって無用です。他方、この種類のトラフィックは追加的な S-TAP およびスニファーの負荷を発生させる可能性があります。スロットル・メカニズムは、S2C 速度が MAX_S2C_VELOCITY より大きい場合にアナライザーからセッションを無視メッセージを送ることで、S-TAP およびネットワーク・スニファーの負荷を軽減するのに役立ちます。何らかの理由で S-TAP またはネットワーク・スニファーにこのメッセージが影響を及ぼしていない場合、アナライザーは MAX_S2C_INTERVAL の秒数が経過した後、「セッションを無視」要求を再び送ります。このスロットル・メカニズムを on に切り替えるには、ANALYZER_S2C_IGNORE フラグを 1 に設定してください。

シナリオ 2

着信トラフィックの S2C 速度が大きい場合 (>MAX_S2C_VELOCITY)、スロットル・メカニズムは、S2C 速度が MAX_S2C_VELOCITY を超える場合のローカル・データベース接続に関して「セッション応答を無視」要求を S-TAP に送ります。何らかの理由で S-TAP にこのメッセージが影響を及ぼしていない場合、アナライザーは MAX_S2C_INTERVAL の秒数が経過した後、セッション応答を無視要求を再び送ります。このスロットル・メカニズムを on に切り替えるには、ANALYZER_S2C_IGNORE フラグを 2 に設定してください。

store sender_encoding

この CLI コマンドは、以前はすべて UTF8 でエンコードされていた出力メッセージ (E メールおよび SNMP トラップ) を異なるエンコード・スキームでエンコードするために使用します。

例えば、Guardium ユーザーがすべての出力 SNMP メッセージを SJIS (代替日本語エンコード方式) でエンコードする場合など。

注: 変換が失敗し、その理由が、(a) 指定されたエンコード・スキームが無効だった、または (b) エンコードする文字を要求されたエンコード・スキームで表せなかった、のいずれかである場合は、デフォルトのエンコード・スキームである UTF8 を使用してメッセージが送信されます。

構文

store sender_encoding <str>,

ここで、str は最大長 16 のエンコード方式です。

表示コマンド

show sender_encoding

store stap approval

この機能を使用して、無許可の STAP が Guardium アプライアンスに接続することをブロックします。

ON にすると、STAP は、特定の承認を得ない限り、接続できなくなります。

承認を得ていない STAP は、自身の IP アドレスに特定の権限が与えられない限り、接続してもすぐに切断されます。

承認されたクライアント用の事前定義レポート「承認済み TAP クライアント」があります。このレポートは「日次モニター」タブで表示できます。

注:

ホスト名ではなく、有効な IP アドレスが必要です。

CLI コマンド store stap approval は、IP ロード・バランサーがある環境内では機能しません。

一元管理された環境内では、承認された STAP に IP を追加した後、同期に関連する待ち時間が発生します。この待ち時間は、最大で 1 時間かかる可能性があります。同期が完了すると、承認された STAP 状況は GUI に緑色で表示されます。

構文

store stap approval ON | OFF

表示コマンド

show stap approval

GuardAPI コマンド

grdapi store_stap_approval

新しい構成は、CLI コマンド restart inspection-core の実行後に有効になります。

store stap certificate

IBM Guardium アプライアンス上で、S-TAP ホスト (通常はデータベース・サーバー) からの証明書を保管します。このコマンドの機能は、後で説明する store certificate console コマンドとまったく同じです。

構文

store stap certificate

次のようなプロンプトが出されます。

新規のサーバー証明書を PEM 形式で貼り付けてください。(Please paste your new server certificate, in PEM format.)

BEGIN 行および END 行を含め、CTRL-D キーを押します。

サーバー証明書をクリップボードにまだコピーしていない場合は、コピーします。PEM 形式の証明書をコマンド行に貼り付け、CRTL-D を押すと、保管操作の成功または失敗が通知されます。

完了したら、**restart gui** コマンドを使って IBM Guardium GUI を再始動します。

store stap network_latency

S-TAP 検査は、S-TAP によってデータベース・トラフィックがモニターされているかどうかをユーザーが検査するための機能です。この検査機能は、ユーザーのネットワーク・トラフィック/待ち時間の影響を受けます。待ち時間は各ユーザーごとに異なるため、この検査機能で使用されるデフォルト値をリストおよび変更する手段が必要です。

構文

store stap network_latency

使用法: store stap network_latency <N>

N は 0 より大きい数値 (秒) です。

デフォルト値は 5 秒です。

この数値が大きくなるほど、S-TAP 検査プロセスの速度が低下します。

表示コマンド

show stap network_latency

store set_partitions_for_queries

この CLI コマンドは、照会でパーティション選択を有効/無効にするときに使用します。

使用法:

store set_partitions_for_queries <on|off>

store storage-system

store storage-system

アーカイブ用またはシステム・バックアップ用のストレージ・システム・タイプを追加または削除します。

構文

store storage-system <Centera | TSM> <backup | archive> <on | off>

表示コマンド

show storage-system

例

現在、システム・バックアップ用に Centera を使用していて、TSM システムに切り替えることを決定したとします。(別のオプションとして残しておく場合を除き) Centera バックアップ・オプションを off にして、TSM バックアップ・オプションを on にする必要があります。これを行うためのコマンドが、例に強調表示されています。表示コマンドは必要ありませんが、説明のためにこの例に含まれています。

CLI> show storage-system

NETWORK :

CENTERA : backing-up

TSM :

SCP : archiving and backing-up

FTP : archiving and backing-up

ok

CLI>store storage centera backup off

ok

CLI>store storage tsm backup on

ok

CLI> show storage-system

NETWORK :

CENTERA :

TSM : backing-up

SCP : archiving and backing-up

FTP : archiving and backing-up

ok

CLI>

store support state

サポート E メール・アドレスへの E メール・アラートの送信を有効 (**on**) または無効 (**off**) にします。この E メール・アドレスは **forward support email** コマンドを使って構成可能です。デフォルトではサポート状態が有効 (**on**)、デフォルトのサポート E メール・アドレスは support@guardium.com です。

構文

store support state <on | off>

表示コマンド

show support state

store throttle

この CLI コマンドは、スロットル・パラメーターを保管します。 このコマンドを入力した後、変更内容を有効にするには CLI コマンド restart inspection-core を発行する必要があります。

このコマンドは、大きなパケットをフィルターで除外 (無視) するために使用されます。2 つのスロットル・モードがあります。まず、「しきい値 (セッションごと)」は、大きなパケット (サイズ構成可能) の長すぎるバースト (期間は構成可能) を識別したときにセッションを無視し、トラフィックが特定のしきい値 (これも構成可能) を下回ったときにセッション無視を停止します。次に、「全体」は、特定のサイズ (構成可能) より大きいすべてのパケットをすべてのセッションで無視します。このスロットル・モードは、定義済みサイズよりも小さい、長く過剰な非データベース・パケットを完全に無視します (VNC クライアントおよび他の種類のホワイト・ノイズ・トラフィックに対して役立ちます)。SPAM ポートまたはハードウェア TAP を介したネットワーク・トラフィックに使用します。S-TAP トラフィックの場合は、PCAP によって扱われるネットワーク TCP トラフィックだけです。CLI コマンド store s2c も参照してください。

構文

store throttle [default | size <s> interval <i> trigger <t> release <r>]

使用法: store throttle size S interval I trigger T release R

ここで、0<=S<=2^17 (**バイト**)、1<=I,T,R,<=2^31 (秒) です。

あるいは、store throttle default を使用します。

表示コマンド

show throttle

Throttle parameters:

Packet size: 228000

Time interval: 604800

Trigger level: 10000000

Release level: 10000000

パラメーター

default - キーワード default を入力すると、システム・デフォルトが復元されます (他のパラメーターは使用されません)。デフォルト・スロットル・パラメーターは、「スロットルなし」です。

s - パケット・サイズ。バイト単位で、最大 2^17 (131072)。

残りのパラメーターは秒単位で、最大 231 (2147483648) です:

i - 時間間隔

t - トリガー・レベル

r - リリース・レベル

注: スロットルのデフォルトを復元するには、CLI コマンド store throttle default を使用してください。

store timeout

CLI セッションまたはファイル・サーバー・セッション (あるいはこの両方) のタイムアウト値を設定します。デフォルト値は 600 秒です。タイムアウトが発生すると、CLI セッションも閉じられます。

タイムアウトが発生したためにファイル・サーバーが停止すると、次のメッセージが表示されます。「警告 ： タイムアウトになったため、ファイル・サーバーが停止しました。ファイルのアップロードは完了していない可能性があります。処理を停止します。」

conf ファイルの socketTimeout 値を表示するには CLI コマンド show timeout db_connection を使用し、タイムアウトの値を設定するには store timeout db_connection <値> を使用します。この値には 0 より大きい値を指定する必要があります。デフォルト値は 25000 秒です。これらの CLI コマンドは、DNS が構成されていない場合に中央マネージャーと管理対象ユニットの間の通信を管理するために使用します。

構文

store timeout cli_session <n>

store timeout fileserver_session <n>

store timeout db_connection <n>

表示コマンド

show timeout cli_session 600

show timeout fileserver_session 600

show timeout db_connection 25000

store transfer-method

CSV/CEF エクスポートで使われるファイル転送方式を設定します。ファイルをエクスポートする場合、CLI コマンド store transfer-method csv を使用して転送方式を設定する必要があります。バックアップまたはアーカイブを実行する場合、CLI コマンド store transfer-method backup を使用して転送方式を設定します。

構文

store transfer-method <FTP | SCP>

表示コマンド

show transfer-method

注: 1 つの IBM Guardium アプライアンスから別のアプライアンスに (例えばコレクターからアグリゲーターに) 送信されるファイルは、常に SCP を使って送られます。

store uid_chain_polling_interval

この CLI コマンドを使用して、UID チェーン・ポーリングの間隔を設定します。UID チェーン・メカニズムを使用すると、S-TAP は (K-Tap を介して)、データベース接続前に発生したユーザーのチェーンをトラッキングできます。

データベースのパフォーマンスを向上させるために UID チェーン処理をオフにするには、間隔を 0 に設定します。 UID チェーン処理がオフになっている場合、UID チェーンの計算および子セッションの更新はスキップされます。

注: データベースを使用するとき、セッションが非常に短い場合には、すべてのセッションで UID チェーンがログに記録されるとは限りません。

構文

store uid_chain_polling_interval <N>

N は分単位の時間です (1 分以上、デフォルトは 2 分)

N を 0 に設定すると、UID チェーン処理はオフになります。

表示コマンド

show uid_chain_polling_interval

store upd_session_end

この CLI コマンドは、セッション終了時刻の更新をスキップするオプションを追加します。

構文

store upd_session_end [enable | disable]

表示コマンド

show upd_session_end

store unit type

この CLI コマンドを使用して、Guardium アプライアンスのユニット・タイプ属性を設定します。このコマンドによって表示できるすべてのユニット・タイプ属性についての説明は、ユニット・タイプ属性表を参照してください。

構文

store unit type [manager | standalone] [netinsp] [stap] [mainframe] [sink]

収集された DRDA トラフィックのタイム・スタンプの細分度を 1 ミリ秒から 1 マイクロ秒に切り替えるには、`store unit type sink` を使用します。

表示コマンド

show unit type

注: リストされているいくつかの属性は store unit type コマンドを使って設定され、delete unit type コマンドを使って消去されます。アグリゲーター属性は、IBM Guardium ソフトウェアのインストール時にのみ設定できます。IBM Guardium ソフトウェアの再インストール以外では、変更できません。

ユニット・タイプ属性

以下の表では、show unit type コマンドによって表示できる Guardium システムのユニット・タイプ属性について説明します。特に明記しない限り、これらの属性は store unit type コマンドを使って設定し、delete unit type コマンドを使って消去することができます。

表 3. ユニット・タイプ属性

属性	記述
mainframe	このユニットはメインフレーム (z/OS®) ネットワーク検査アプライアンスです。
manager	このユニットで中央マネージャー機能が有効になります。
netinsp	ネットワーク・トラフィックの検査が有効になります。
network route static	静的ルーティング表から 1 行を除去します
standalone	ローカル管理 (中央マネージャーから独立)
stap	このユニットは S-TAP および CAS エージェントからデータを受信し、これらを管理することができます。

unregister management

unregister (登録抹消) コマンドは、アプライアンスの一元管理の登録時に保存された構成を復元します。以前のリリースの IBM Guardium ソフトウェアの下で登録が行われた場合、保存済み構成を現在のソフトウェア・リリース・レベルに引き上げる目的でまずパッチを適用せずにその構成を復元した場合、アプライアンスが使用不可になり、これが原因で、そこに保管されているデータがすべて失われる可能性があります。したがって、登録前の構成が現在のソフトウェア・リリース・レベルになっていることを確認するまでは、ユニットを登録抹消しないでください。この確認方法が分からない場合は、ユニットを登録抹消する前に技術サポートに連絡してください。

構文

unregister management

注:

- このコマンドは緊急用です。中央マネージャーが使用不可になった場合にのみ、これを使用します。
- このコマンドを使って登録抹消した後、中央マネージャーからも登録抹消する必要があります (管理コンソールから)。管理対象ユニットの数を減らすには、これが唯一の方法であるためです。許可される管理対象ユニットの数は、プロダクト・キーによって決められています。

親トピック: CLI の概要
関連情報:
Guardium のトラブルシューティングとサポート (ビデオ)

diag CLI コマンド

これらの CLI コマンドを使用して、DIAG を介してトラブルシューティング・ユーティリティーおよびメンテナンス・ユーティリティーにアクセスできます。

技術サポートの指示どおりに diag コマンドを使用します。

このコマンドを使用して定期的に実行する必要がある機能はありません。メインメニューの各項目について、個別のトピックで説明します (『メインメニュー・コマンド』を参照してください)。

DIAG によるトラブルシューティング・ユーティリティーおよびメンテナンス・ユーティリティー:

- Aggregator Fix Schema - インポートされた表のうち、アグリゲーターのスキーマよりも古いスキーマを持つすべての表のスキーマを、アグリゲーターの最新パッチ・レベルに変更します (バックグラウンドで実行され、完了までに数時間かかる場合があります)。注: (a) アグリゲーターのパッチ・レベルが最新ではない、または (b) インポートされた表の中に、パッチ・レベルが最新のものがある、という状況により、インポートされたすべての表が「最新のパッチ・レベル」を持っているわけではない場合があります。
- Aggregator Maintenance - アグリゲーターの完全な分析およびリカバリーです。このユーティリティーは、AGG 関連ログを収集して diag エクスポート・フォルダーに配置し、Aggregator Fix Schema を呼び出してすべてのデータベースのスキーマを同期し、AGG ワークスペースのクリーンを行い、マージ処理を再開して、インポートされたすべての表の完全な分析が確実に行われるようにします (バックグラウンドで実行され、完了までに数時間かかる場合があります)。
- Clean Static Orphans on an Aggregator - このオプションは、静的表が増えすぎたために消去する必要がある場合にのみ、必ず技術サポート限定で使用します。このユーティリティーは、使用されなくなった古い構成レコードをすべて消去します。

診断メインメニューを開く

diag コマンドを使用するには、概説する手順に従ってください。

1. コマンド行プロンプトで、CLI を使用して Guardium® アプライアンスにログインします。

   diag コマンドを使用する Guardium ユーザーには、CLI ロールまたは admin ロールが割り当てられている必要があります。デフォルトで「CLI」ロールを持っているユーザーは、admin のみです。「CLI」ロールまたは「admin」ロールを持つユーザーは、diag コマンドの入力、unlock admin CLI コマンドおよび unlock

accessmgr CLI コマンドの使用、および export audit-data CLI コマンドの制限なしの使用を許可されます。CLI ロールを持つユーザーは、GUI ログインに必要なユーザー名とパスワードを入力する必要がなく、それ以降のロールの確認も行われません。

CLI を使用する Guardium ユーザーが「CLI」ロールまたは「admin」ロールを持っていない場合、CLI は開始しません。CLI ロールおよび admin ロールは、accessmgr により割り当てられます。

2. CLI が開始したら、コマンド行プロンプトで diag コマンド (引数なし) を入力します。
3. diag コマンドを使用する Guardium ユーザーには、Guardium システム上で diag ロールが割り当てられている必要があります。デフォルトでは、admin にのみこのロールが割り当てられています。diag へのアクセスは、このユーザーに割り当てられているロールに基づいて、許可または却下されます (diag へのアクセスは、このユーザーに「diag」ロールが割り当てられている場合にのみ許可されます)。diag ロールは、accessmgr により割り当てられます。
4. メイン・コマンド・メニューが表示されます。以下のいずれかを行って、オプション選択カーソル (例では最初の項目を選択しています) を移動させます。
   - 目的の項目番号を入力します (選択カーソルが選択された項目に移動します)。
   - 上矢印キーまたは下矢印キーを使用して、目的の項目を選択します。
5. スペース・バー、左矢印キー、または右矢印キーを押して、画面にあるコマンド選択カーソル (例では OK コマンドを選択しています) を移動させます。
6. 表示域の適切なオプションを選択して操作を実行し、次に以下のいずれかを実行します。
   - コマンド選択カーソルを使用して、適切なコマンドを選択し、Enter キーを押します。
   - 適切な操作コマンドをクリックします。

diag 出力について

diag コマンドでは、以下の 2 つのディレクトリーに出力が作成されます。

- .../guard/diag/current
- .../guard/diag/depot

この出力にアクセスするには、fileserver CLI コマンドを使用します。詳しくは、『fileserver』を参照してください。

各ディレクトリーについては、以下のサブセクションで説明します。

.../guard/diag/current ディレクトリー

diag コマンドからの出力のほとんどは、テキスト形式で current ディレクトリーに書き込まれます。ほとんどのコマンドでは、このディレクトリーにコマンドごとの個別の出力ファイルが含まれます。同じコマンドを実行する度に、それぞれのコマンド用の単一ファイルに出力が追加されます。幾つかのコマンドでは、実行ごとに個別のファイルが作成され、通常はファイル名に日時スタンプが取り込まれます。

セッションが終了する度に、以降のセッションで古い情報が表示されることがないよう、「クリーンアップ」することをお勧めします。エクスポート用にファイルを単一の圧縮ファイルに圧縮する場合 (以下のトピックを参照)、current ディレクトリー内のファイルがすべて削除されます。または、「Output Management」メニューの「Delete recordings」コマンドを使用して、個別のファイルを削除できます。

current ディレクトリー内のファイルは、メニュー名およびコマンド名から名前が付けられているため、簡単に特定することができます。例えば、「System Interactive Queries」メニューの「File Summary」コマンドを使用した場合、interactive_filesummary.txt という名前のファイルが current ディレクトリーに作成されます。

コマンドを使用している途中に current ディレクトリーを見ると、そのコマンドの出力を含むファイルと同じ名前の隠し一時ファイルが表示されている場合があります。一時ファイルは、コマンドの出力ファイルに出力が追加されると削除されます。

.../guard/diag/depot ディレクトリー

current ディレクトリーで diag 出力ファイルを (例えば、Guardium 技術サポートに送信するために) 圧縮ファイルに圧縮すると、その圧縮ファイルは depot ディレクトリーに保管されます。ファイル名は diag_session_<dd_mm_hhmm>.tgz という形式になります。この名前の変数部分は、ファイルが作成された時を示します。例えば、ファイルが 5 月 20 日の 12:15 PM に作成された場合、名前は diag_session_20_5_1215.tgz になります。

ファイルをエクスポートしたら (『Export recorded files 』トピックを参照)、「Output Management」メニューの「Delete recordings」コマンドを使用して、depot ディレクトリーからエクスポートしたファイルを削除できます。

1 Output Management

「Output Management」コマンドは、diag コマンドによって作成された出力に対する操作を制御します。各「Output Management」コマンドについて、個別に説明します。

1.1 End and pack current session

このコマンドを使用して、current ディレクトリー内の診断ファイルをすべて単一の圧縮ファイルに圧縮し、current ディレクトリーからそれらのファイルを削除します。このコマンドを入力した場合、コマンドが完了したことを示すフィードバックは返されません。depot ディレクトリーのディレクトリーを表示することにより、このコマンドが完了したことを検証できます。コマンドが完了すると、diag_session_<mm_dd_hhmm>.tgz という形式で名前が付けられたファイルが作成されます。前述したとおり、この名前の変数部分は日時スタンプです。「Output Management」メニューの「Export recorded files」コマンドを使用して、別のシステムにファイルを送信します。

1.2 Delete recordings

このコマンドを使用して、depot ディレクトリーまたは current ディレクトリー内のファイルを削除します。(現行セッションのファイルのみを削除するには、「Delete current session files」コマンドを使用します。) このコマンドを入力すると、depot ディレクトリー構造が表示されます。

上矢印キーおよび下矢印キーを使用し、Enter キーを押して、ディレクトリー内をナビゲートできます。例えば、../ を選択して Enter キーを押すと、選択をディレクトリー構造内で 1 つ上のレベルに移動できます。

次に current ディレクトリーを選択して Enter キーを押すと、そのフォルダーまでナビゲートし、個別のコマンド出力ファイルを削除できます。他のディレクトリーにナビゲートすることはできますが、current ディレクトリーおよび depot ディレクトリー以外のディレクトリーからファイルを削除することはできないことに注意してください。

削除するファイルを選択したら、Enter キーを押します。

注意: 削除操作の確認を求めるプロンプトは出されません。

1.3 Export recorded files

このコマンドを使用して、depot ディレクトリーから他のサイトにファイルを送信します。ファイルをエクスポートするには、次のようにします。

1. 「Output Management」メニューから「Export recorded files」を選択します。depot ディレクトリーが表示されます。
2. 送信するファイルを選択するか、../ エントリーおよび ./ エントリーを使用して、ディレクトリー構造内で上または下にナビゲートします。(ただし、エクスポートできるのは depot ディレクトリーのファイルのみであることに注意してください。)
3. 送信するファイルを選択した状態で、Enter キーを押します。
4. FTP を選択するか、終了するよう求めるプロンプトが出されます。FTP を選択し、Enter キーを押します。
5. ホスト名を入力するよう求めるプロンプトが出されます。受信システムのホスト名 (またはその IP アドレス) を入力し、Enter キーを押します。
6. ユーザー名を入力するよう求めるプロンプトが出されます。受信システムのユーザー・アカウント名を入力し、Enter キーを押します。
7. パスワードを入力するよう求めるプロンプトが出されます。受信システムのユーザーのパスワードを入力します。
8. 受信システムで送信されたファイルを受け取るディレクトリーを指定するよう求めるプロンプトが出されます。 受信システム上の、ファイルを格納するディレクトリーの FTP ルートに対する相対パスを入力し、Enter キーを押します。
9. 転送の詳細 (送信されるファイルとその宛先) を確認するよう求めるプロンプトが出されます。Enter キーを押して転送を実行するか、「Cancel」を選択して Enter キーを押し、最初からやり直します。
10. 操作が成功 (または失敗) したことが通知されます。

1.4 Delete current session files

このコマンドを使用して、現行セッション中に作成されたファイルを削除します。

1.5 Exit

「Exit」コマンドを使用して、メインメニューに戻ります。

2 System Static Reports

メインメニューの「System Static Reports」コマンドを使用して、詳細なレポートを作成します。

1. メインメニューから「System Static Reports」を選択します。プロセスが実行中であることが通知されます。
2. レポートの作成が完了すると、表示域にレポートが表示されます。(このレポートは長大であり、デスクトップ・コンピューターにエクスポートしてからテキスト・エディターを使用して表示したほうが見やすい場合があります。)

   上矢印キーおよび下矢印キーを使用して、レポート内をスクロールアップおよびスクロールダウンします。レポートの確認が終わったら、Enter キーを押してメインメニューに戻ります。

System Static Reports の概要

以下のサブトピックでは、「System Static Reports」出力の主要コンポーネントの概要を示します。示されている出力の一部は、実際の内容を詳細に説明するためではなく (本書で扱う範囲を超えています)、レポートに含まれる情報の種類とレベルを説明するためのものです。

システム構成情報

「System Static Reports」出力には、ビルド・バージョン、適用されているパッチ、現在のシステム・アップタイム、およびネーム・サーバーの情報が示されます。

```
Build version: 34e1eb12eb68ba76cb49028251c9a0d6  /opt/IBM/guardium/etc/cvstag
Patches:
2009/02/22 16:16:50: START Installation of 'Update 5.0'
2009/02/22 16:18:04: Installation Done - Successfully Installed

< lines deleted… >

Current uptime:
  09:03:43  up 6 days, 17:34,  1 user,  load average: 0.44, 0.50, 0.41
System nameservers:
192.168.3.20
DB nameservers:
192.168.3.20
Gateway: 192.168.3.1 (system) 192.168.3.1 (def)
```

次に、ファイル・システム情報が示されます (一部を示します)。

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdc3             2.0G  1.1G  813M  58% /
/dev/hdc1              97M  9.2M   83M  10% /boot
none                  504M     0  504M   0% /dev/shm
/dev/hdc2              71G  1.2G   66G   2% /var
         total:    used:    free:  shared: buffers:  cached:
Mem:  1055199232 1041711104 13488128        0 63275008 186220544
Swap: 536698880 295432192 241266688
MemTotal:      1030468 kB
MemFree:         13172 kB

< lines deleted… >
```

続けて、構成されているメール・サーバーおよび SNMP サーバーについての情報が示されます。

```
SMTP server: 192.168.1.7 on port 25 : REACHABLE
SMTP user: undef
```

```
SMTP password: undef
SMTP auth: NONE
SNMP trapsink: undef UNREACHABLE
SNMP trap community: undef
SNMP read community: undef
```

システム構成セクションの最後のセクションでは、IP アドレス、ホスト名、およびドメイン名などの、ユニットのネットワーク構成が示されます。

```
eth0:                192.168.3.101  (system) 192.168.3.101 (def)
hostname:                        (system)  g1 (def)
domain:                            (system)  guardium.com (def)
mac address:      00:04:23:A7:77:F2  (MAC1)  00:04:23:A7:77:F2 (MAC2)
unit type:           548 Standalone STAP
```

内部データベース情報

「System Static Reports」出力の次の主要セクションには、内部データベース状況およびスレッドに関する情報が含まれます (最初の数スレッドのみを示します)。

```
uptime 77097  seconds.
27  threads.
78545028  queries.
+------+------------+-----------------------------+---------+---------+------+-----------
| Id   | User       | Host                        | db      | Command | Time | State |  +----------------------------------------
-----------------------------------------------
| 1137 | enchantedg | localhost                   | TURBINE | Sleep   | 26   |
| 1257 | enchantedg | localhost.localdomain:33587 | TURBINE | Sleep   | 0    |
| 1258 | enchantedg | localhost.localdomain:60409 | TURBINE | Sleep   | 7716 |
| 1259 | enchantedg | localhost.localdomain:48233 | TURBINE | Sleep   | 322  |

< lines deleted… >
```

スレッドのリストに続けて、表の状況の分析が示されます。

Web サーブレット・コンテナーの情報

「System Static Reports」出力の次の数セクションには、Web サーブレット・コンテナー環境 (Tomcat) に関する情報が含まれます。

```
================================================================================
Currently defined Tomcat port is 8443.
The TOMCAT daemon is running and listening on port(s): 8005 8443.
Currently OPEN ports
java run by tomcat on port *:8443

< lines deleted… >
================================================================================

These are the nanny latest actions:
May 19 14:13:09 guard nanny:[5528]: Also checking tomcat.
May 19 14:13:09 guard nanny:[5528]: Going for my initial nap.

< lines deleted… >

This is the TOMCAT command line:
  463 sh -c ps -o pid,cmd -e | grep Dcatalina.base
21917 grep Dcatalina.base.
```

検査エンジンの情報

「System Static Reports」出力の次の主要セクションには、検査エンジンに関する情報が含まれます。

```
================================================================================
This is the SNIF (pid: 13036) command line:  13036 /opt/IBM/guardium/bin/snif.
This is the SNIF status:
Name:               snif
State:                R (running)
Tgid: 13036

< lines deleted… >
================================================================================

Current timestamp is 2009-05-20 11:56:41
This is the last timestamp at GDM_CONSTRUCT_INSTANCE: 2009-05-20 11:56:41
This is the last timestamp at GDM_EXCEPTION: 2009-05-20 11:56:41
This is the last timestamp at GDM_POLICY_VIOLATIONS_LOG: 2009-05-20 11:56:41

================================================================================

Snif buf usage at Fri May 20 11:56:44 2009:
100 204800 buffers out of 204800
126 connection used, 32642 unused, 0 dropped (sniffer), 9 ignored (analyzer)
0 bytes lost, 60 connections ended, 601752099 bytes sent, 579063 request sent
Dropped Packets: 0 buffer full, 0 too short , 451 ignored
 time now is 1116604603
Analyzer/Parser buffers size: 6 (66533) 0 (62902)
 ms-tsql-logger  0 (11331)
 syb-tsql-logger  0 (70)
 ora-tsql-logger  79 (67803)
 db2-sql-logger  0 (20544)

< lines deleted… >
```

IP 表の情報

次の主要セクションには、IP 表に関する情報が含まれます。

```
================================================================================
IPTABLES:
-------------
       tcp  --  192.168.2.0/24       192.168.1.0/24      tcp spts:1521:60000  set 0x23
       tcp  --  192.168.1.0/24       192.168.2.0/24      tcp dpts:1521:60000  set 0x22
< lines deleted… >
```

S-TAP の情報

次の主要セクションには、S-TAP® の情報が含まれます。

```
================================================================================
STAP:
----
    0     0 ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp spt:9500
    0     0 ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp dpt:9500
 2696  148K ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp spt:16016
 2835  175K ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp dpt:16016

< lines deleted… >
```

IP トラフィックの情報

次の主要セクションには、IP トラフィックの情報が含まれます。

```
IP traffic statistics.
OUTPUT OF ETH0
Fri May 20 11:57:04 2012; ******** Detailed interface statistics started ********

*** Detailed statistics for interface eth0, generated Fri May 20 11:58:04 2009

< lines deleted… >

OUTPUT OF ETH1
Fri May 20 11:57:04 2012; ******** Detailed interface statistics started ********

*** Detailed statistics for interface eth1, generated Fri May 20 11:58:04 2009

Total:                82440 packets, 53892382 bytes
        (incoming: 82440 packets, 53892382 bytes; outgoing: 0 packets, 0 bytes)
IP:    82440 packets, 52632747 bytes
        (incoming: 82440 packets, 52632747 bytes; outgoing: 0 packets, 0 bytes)

< lines deleted… >
```

情報エンジンの STDERR および STDOUT の情報

次のセクションには、スニファーによる最終メッセージ出力が含まれます。

```
Snif  STDERR:

< lines deleted… >

Snif STDOUT:
Fri_20-May-2009_04:04:35 : Guardium Engine Monitor starting
Fri_20-May-2009_04:14:37 : Guardium Engine Monitor starting
Fri_20-May-2009_04:24:38 : Guardium Engine Monitor starting

< lines deleted… >
```

インポート・ディレクトリーの情報

次のセクションには、インポート・ディレクトリーの内容がリストされます。

```
These are the contents of the importdir directory:
total 0
```

アグリゲーターのアクティビティーの情報

このセクションには、アグリゲーターのアクティビティーがリストされます (例では何も示されていません)。

```
================================================================================
This is the aggregator last activities:
```

監査レポート

このセクションには、次の要約情報がリストされます (例を参照してください)。

```
================================================================================
Range of time in logs: 01/14/10 13:12:26.348 - 01/18/10 12:48:01.073
Selected time for report: 01/14/10 13:12:26 - 01/18/10 12:48:01.073
Number of changes in configuration: 4   - changes to the audit configuration
Number of changes to accounts, groups, or roles: 0
```

```
Number of logins: 22    - logins into the machine - ssh and console
Number of failed logins: 114
Number of authentications: 22 - "su", etc.
Number of failed authentications: 5
Number of users: 2
Number of terminals: 18
Number of host names: 9
Number of executables: 7
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 3
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 0
Number of process IDs: 9173
Number of events: 98669
============================================================================
```

異常レポート

このセクションには、以下がリストされます (例を参照してください)。

```
============================================================================
# Date Time Type Exe Term Host AUID Event
============================================================================
1. 01/14/10 13:16:02 ANOM_PROMISCUOUS /usr/sbin/brctl (none) ? -1 8 -  this is expected
to appear - it means the bridge is listening to all traffic
```

認証レポート

このセクションには、以下がリストされます (例を参照してください)。

```
============================================================================
# Date Time Type Exe Term Host AUID Event
============================================================================
1. 01/14/10 13:13:22 tomcat ? console /bin/su yes 4
2. 01/14/10 13:16:44 tomcat ? console /bin/su yes 11
3. 01/14/10 13:16:44 tomcat ? console /bin/su yes 17
4. 01/14/10 13:16:45 tomcat ? console /bin/su yes 23
5. 01/14/10 13:16:48 tomcat ? console /bin/su yes 29
6. 01/14/10 13:22:29 tomcat ? ? /bin/su yes 155
7. 01/14/10 13:28:10 ? ? tty1 /bin/login no 252
8. 01/14/10 13:28:20 ? ? tty1 /bin/login no 254
```

ログイン・レポート

このセクションには、以下がリストされます (例を参照してください)。

```
============================================================================
# Date Time Type Exe Term Host AUID Event
============================================================================
1. 01/14/10 13:22:15 root 192.168.2.9 sshd /usr/sbin/sshd no 142
2. 01/14/10 13:22:15 root 192.168.2.9 sshd /usr/sbin/sshd no 143
3. 01/14/10 13:22:17 root 192.168.2.9 sshd /usr/sbin/sshd no 144
4. 01/14/10 13:22:17 root 192.168.2.9 sshd /usr/sbin/sshd no 145
5. 01/14/10 13:22:20 root 192.168.2.9 sshd /usr/sbin/sshd no 146
```

3 Interactive Queries

メインメニューから「System Interactive Queries」を選択し、「Interactive Queries」メニューを開きます。(このメニューの項目をすべて表示するには、下矢印キーを使用して 10 個目の項目より先までスクロールしてください。)

各対話式照会コマンドでは、要求された情報の表示に加え、その出力を含む個別のテキスト・ファイルを current ディレクトリー内に作成します。作成されるファイルについて詳しくは、概要トピックを参照してください。

各コマンドについては、以下のセクションで説明します。

3.1 Files Changed

「Files Changed」コマンドを使用して、指定した日数より前または後に変更されたファイルのリストを表示します。

1. 「Interactive Queries」メニューから、「Files Changed」を選択します。日数を入力するよう求めるプロンプトが出されます。数値を入力し、Enter キーを押します。
2. 入力した日数より前または後に変更されたファイルを表示するかどうかを確認するプロンプトが出されます。1 または 2 を選択し、Enter キーを押します。
3. 変更された各ファイルの絶対ディレクトリー・パスが表示されます。表示域にすべてのデータが収まらない場合は、上矢印キーおよび下矢印キーを使用して、スクロールしてデータを表示してください。ファイル内での現在位置は、ディスプレイの数値により示されます。表示域の白いバーに正符号が表示されている場合、さらにデータが存在することを示します。

3.2 List Folder

このコマンドを使用して、さまざまなディレクトリーの内容をリストします。

1. 「Interactive Queries」メニューから、「List Folder」を選択します。

2. ディレクトリーを選択するよう求めるプロンプトが出されます。ディレクトリーを選択し、Enter キーを押します。選択されたディレクトリーが表示されます。同じ種類のコマンドが複数実行された場合、各コマンドの実行により作成されたデータは、そのコマンド用に維持されている単一のテキスト・ファイルに追加されます。
3. 完了後、Enter キーを押すか、「Exit」をクリックします。

3.3 Summarize Folder

「Summarize Folder」コマンドを使用して、du (ディスク使用状況) コマンドの出力を表示します。

1. 「Interactive Queries」メニューから、「Summarize Folder」を選択します。プロンプトは出されません。さまざまなディレクトリーのディスク使用状況が表示されます。
2. 上矢印キーおよび下矢印キーを使用して、スクロールしてディレクトリーを表示します。
3. 完了後、Enter キーを押すか、「Exit」をクリックします。

3.4 File Summary and Export

このコマンドを使用して、ログ・ファイルのすべてまたは一部分をリストします。

1. 「Interactive Queries」メニューから、「File Summary」を選択します。
2. ファイルを選択するよう求めるプロンプトが出されます。上矢印キーおよび下矢印キーを使用して、表示するファイルまで選択カーソルをスクロールします。
3. Enter キーを押すか、「OK」をクリックします。
4. 表示する行数を選択するよう求めるプロンプトが出されます。選択したら、Enter キーを押します。
5. オプションの検索文字列を入力するよう求めるプロンプトが出されます。特定のログ・メッセージを検索する場合は、このボックスを使用します (正規表現を入力できます)。そうでない場合は、このボックスを空のままにして、Enter キーを押します。
6. プロンプトに従って操作し、Enter キーを押して「Yes」を選択します。これにより、固有のメッセージのみが表示されます。そうでない場合は、「No」を選択して Enter キーを押します (すべてのメッセージが表示されます)。

   「Summary Style」が使用されている場合は、変数がポンド記号文字 (#) で置き換えられることに注意してください。IP アドレスや日付といった変数を含む一部のログ・データでは、より広い範囲で置換が行われる場合があります。

3.5 Test Email

このコマンドを使用して、構成済みの SMTP サーバーを使用してテスト E メールを送信します。

1. 「Interactive Queries」メニューから、「Test Email」を選択します。
2. 宛先を選択するよう求めるプロンプトが出されます。「Custom」を選択し、Enter キーを押します。
3. E メール・アドレスを入力するよう求めるプロンプトが出されます。E メール・アドレスを入力し、Enter キーを押します。操作の出力が通知されます。管理コンソールで、アラート機能構成パネルの SMTP ペイン内の「Test Connection」リンクを使用すると、SMTP ポートが構成されているかどうかのテストのみが行われ、そのサーバー経由で実際にメールを送信できるかどうかはテストされないことに注意してください。このコマンドを使用して、統計アラートやリアルタイム・アラート、または監査プロセスの通知を構成および起動することなく、E メールの送信をテストできます。

3.6 Test SNMP

このコマンドを使用して、構成済みの SNMP サーバーにテスト SNMP トラップを送信します。

1. 「Interactive Queries」メニューから、「Test SNMP」を選択します。
2. アクティビティーとその結果が通知されます。アラート機能構成パネルの、SNMP ペイン内の「Test Connection」リンクを使用すると、SNMP ポートが構成されているかどうかのテストのみが行われ、そのサーバー経由で実際にトラップを送信できるかどうかはテストされないことに注意してください。このコマンドを使用して、統計アラートやリアルタイム・アラート、または監査プロセスの通知を構成 (および起動) することなく、トラップの送信をテストできます。

3.7 Report Query Data

このコマンドを使用して、レポート照会に使用される実際の select ステートメントを表示します。これは、ユーザー作成レポートにより予期しない出力が生成された場合に、役立つことがあります。

1. 「Interactive Queries」メニューから「Report Query Data」を選択します。
2. レポート・タイトルのリストの中から選択するよう求めるプロンプトが出されます。上矢印キーおよび下矢印キーを使用して項目を選択し、Enter キーを押します。このリストの各項目は、レポート・エンティティーです。すべての事前定義レポートが、リストの先頭に表示されます。これらには、100 から 225 までの番号が付けられています (バージョン 3.6.1 の場合。リリースごとにさらに多くの事前定義レポートが作成されるため、通常この数字は大きくなっていきます)。

   ユーザー作成レポートは、事前定義レポートの後に表示され、20001 から番号が付けられます (バージョン 3.6.1 の場合)。

   選択したレポートの select ステートメントが表示されます。

3.8 GDM Queries

このコマンドを使用して、100 秒間隔で監視された SQL 呼び出しの数を表示します。

1. 「Interactive Queries」メニューから、「GDM Queries」を選択します。
2. 待機するよう求めるメッセージが表示されます。「Yes」を選択して続行します。表示画面上の CMD_CT 列に、指定したクライアントから指定したサーバーへの SQL 呼び出しの監視数がリストされます。
3. レポートの確認が完了した後で、Enter キーを押します。

3.9 Generate TCP Dump

このコマンドを使用して、TCP ダンプを作成します。このコマンドでは、出力はコマンド・ファイルにのみ書き込まれ、表示画面には書き込まれません。他の多くのコマンドとは異なり、このコマンドを実行する度に、current ディレクトリーに個別のファイルが作成されます。ファイル名は、 tcpdump_<mmyyyy-hhmmss> という形式になります。ここで変数部分は日時スタンプです。mmyyyy は月と年、および hhmmss は時、分、および秒です。

1. 「Interactive Queries」メニューから、「Generate TCP dump」を選択します。
2. インターフェースを選択するよう求めるプロンプトが出されます。ポートを選択し、Enter キーを押します。
3. オプションのフィルター IP アドレスを入力するよう求めるプロンプトが出されます。特定のアドレスからのトラフィックのみが必要な場合は、その IP アドレスを入力して Enter キーを押します。そうでない場合は、そのまま Enter キーを押します。
4. オプションのポート番号を入力するよう求めるプロンプトが出されます。特定のポートからのトラフィックのみが必要な場合は、そのポート番号を入力して Enter キーを押します。そうでない場合は、そのまま Enter キーを押します。
5. 何秒間トラフィックを取り込むのかを選択するよう求めるプロンプトが出されます。秒数を選択し、Enter キーを押します。
6. Enter キーを押して、データの収集を開始するよう求めるプロンプトが出されます。Enter キーを押します。(ほぼ) 指定した秒数後、メニューに戻ります。
7. TCP ダンプ・データを表示するには、「Read TCP dumps」コマンドを選択するか、ファイルをエクスポートします (前述した「Output Management」メニューの「Export Reported Files」を参照してください)。

3.10 Read TCP Dumps

このコマンドを使用して、先ほど作成した TCP ダンプ・ファイルを表示します。

1. 「Interactive Queries」メニューから「Read TCP dumps」を選択します。
2. ファイルを選択するよう求めるプロンプトが出されます。TCP ダンプ・ファイルは、古いものから新しいものの順にリストされます。ファイル名は tcpdump_<mmddyy-hhmmss> という形式になります。ここで変数部分は日時スタンプです。 mmddyy が月、日、および年、hhmmss が時、分、および秒です。表示するファイルを選択し、Enter キーを押します。
3. 選択したファイルが表示されます。 上矢印キーおよび下矢印キーを使用して表示をスクロールし、完了した後で Enter キーを押します。

3.11 Watch Buffer

このコマンドを使用して、Guardium バッファー内のアクティビティーを監視します。

1. 「Interactive Queries」メニューから、「Watch Buffer」を選択します。表示は毎秒更新されます。
2. Ctrl キーを押しながら C を押して、表示を閉じます。

3.12 SLON Utility

このコマンドを使用して、パケットをトラッキングする slon ユーティリティーを実行します。通常は、技術サポートの指示があった場合にのみ、このコマンドを実行します。このコマンドでは、出力は表示画面に書き込まれません。出力は、コマンドの実行ごとに、current ディレクトリー内にある 2 つのコマンド・ファイル、apks.txt.<day_dd-mmm-yyyy_hh.mm.ss.ttt> または requests.txt.<day_dd-mmm-yyyy_hh.mm.ss.ttt> のいずれかに書き込まれます。

ファイル名の変数部分は日時スタンプです。例えば、apks.txt.Fri_20-May-2011_08.52.00.789 です。

1. 「Interactive Queries」メニューから、「Slon Utility」を選択します。
2. 実行する操作を選択し、「OK」をクリックします。選択項目は、以下のとおりです。

   (a) アナライザーのルール情報をダンプする

   (f) IP またはマスク (あるいはこの両方) に基づいてアナライザー・パケットをフィルターに掛ける

   (p) パケットを apks.txt にダンプする

   (l) ロガーの要求を requests.txt にダンプする

   (m) STAP パケットをダンプする (実行時間を選択します。完了するまで待ってから、/var/log/guard/diag/current/tap/ の下の msg-dump ファイルを確認します。)

   (r) IPQ トラフィックを記録する

   (s) 状態マシン情報をダンプする

   (t) スロットル・パラメーターを構成する

3. 選択内容にかかわらず、操作の実行期間を選択するよう求めるプロンプトが出されます。期間を選択し、Enter キーを押します。
4. 指定した期間プログラムが実行されることが通知され、Enter キーを押すよう求めるプロンプトが出されます。 Enter キーを押して待機します。
5. 処理が完了すると、メッセージが表示されます。「File Summary」コマンドを使用して、このコマンドの出力を表示できます。このコマンドにより大量のデータが生成される場合があるため、テキスト・エディターを使用してファイルの内容を表示できる別のシステムにファイルをエクスポートすることをお勧めします。(現行セッション・データを圧縮し、このセクションで前述したように記録をエクスポートします。)

3.13 Show Indexes

このコマンドを使用して、さまざまな内部表の索引を表示します。

1. 「Interactive Queries」メニューから、「Show Indexes」を選択します。
2. 表を選択するよう求めるプロンプトが出されます。表を選択し、Enter キーを押してその表の索引を表示します。
3. 上矢印キーおよび下矢印キーを使用して、表示をスクロールします。完了後、Enter キーを押します。

3.14 S-TAP Check

このコマンドを使用して、S-TAP 定義およびトラフィック情報を表示します。

1. 「Interactive Queries」メニューから、「S-TAP Check」を選択します。
2. システムのユニット・タイプが数値形式で表示されます。Enter キーを押します。
3. S-TAP トラフィックをモニターする秒数を選択するよう求めるプロンプトが出されます。上矢印キーおよび下矢印キーを使用して選択を行い、Enter キーを押します。
4. 出力を待機するおおよその時間が通知され、Enter キーを押すよう求めるプロンプトが出されます。Enter キーを押します。
5. 「S-TAP Definitions」レポートおよび「Server Traffic」レポートが表示されます。レポートの確認が完了した後で、Enter キーを押します。

3.15 Interface Link Status

このコマンドを使用して、インターフェース・リンクの状況を表示します。

1. 「Interactive Queries」メニューから、「Interface link status」を選択します。
2. すべてのインターフェースの状況が表示されます。上矢印キーおよび下矢印キーを使用して、表示をスクロールします。
3. 完了後、Enter キーを押します。このコマンドにより表示されるのは、リンクの状況のみであることに注意してください。インターフェース構成情報を表示するには、show network interface all CLI コマンドを使用します。

3.16 Show Throttle Data

このコマンドを使用して、スロットル・データを表示します。

1. 「Interactive Queries」メニューから、「Show Throttle data」を選択します。
2. Enter キーを押して、スロットル統計を 3 秒間待機します。
3. 上矢印キーおよび下矢印キーを使用して表示をスクロールし、完了した後で「Exit」を押します。

3.17 Generate TCP dump and slon

このコマンドを使用して、TCP ダンプを作成し、パケットをトラッキングする slon ユーティリティーを実行します。通常は、技術サポートの指示があった場合にのみ、このコマンドを実行します。上記の個別トピック Generate TCP dump および Slon Utility を参照してください。

3.18 Generate SSL dump

このコマンドを使用して、SSL ダンプを作成します。

1. 「Interactive Queries」メニューから、「Generate SSL dump」を選択します。
2. インターフェースを選択し、「OK」を押します。フィルター IP アドレスを入力し、「OK」を押します。フィルター・ポート番号を入力し、「OK」を押します。
3. 実行期間を選択し、「OK」を押します。「OK」を押し、TCP ダンプを収集するために指定した時間待機します。
4. SSL ダンプを表示する場合は、「OK」を押します。
5. 完了後、「Exit」を押します。

3.19 View bash history

このコマンドを使用して、bash 履歴を表示します。

1. 「Interactive Queries」メニューから、「View Bash History」を選択します。
2. 「OK」を押します。
3. 上矢印キーおよび下矢印キーを使用して表示をスクロールし、完了した後で「Exit」を押します。

3.20 Generate GDM_Error dump

このコマンドを使用して、GDM_ERROR ダンプを作成します。

1. 「Interactive Queries」メニューから、「Generate GDM_Error dump」を選択します。
2. 「OK」を押し、パスワードを入力します。Enter キーを押します。
3. 上矢印キーおよび下矢印キーを使用して表示をスクロールし、完了した後で「Exit」を押します。

3.21 Prepare Tomcat Memory dump

Tomcat では最初にメモリー不足エラーを検出したときに、/var/tmp/tomcat/tomcat.dmp にメモリー・ダンプを行います。このコマンドを使用して、このファイルを圧縮し、暗号化して、/var/log/guard/diag/tomcat/ に移動し、ファイル・サーバーがこのファイルを取得できるようにします。

1. 「Interactive Queries」メニューから、「Prepare Tomcat Memory dump」を選択します。
2. 「OK」を押します。
3. 上矢印キーおよび下矢印キーを使用して表示をスクロールし、完了した後で「Exit」を押します。

3.22 拡張ネットワーク情報

システムの対話式照会の 下にある「拡張ネットワーク情報」オプションをクリックして、 ネットワーク診断情報を表示します。

例

SQLGuard Diagnostics

Network Parameters from ADMINCONSOLE_PARAMETER:

SYSTEM_NETMASK1: 255.255.255.0

SYSTEM_DOMAIN:

SYSTEM_DEFAULT_ROUTE:

SYSTEM_DNS1:

SYSTEM_DNS2:

SYSTEM_DNS3:

TOMCAT_IP:

MANAGER_IP:

HOST_MAC_ADDRESS:

SECOND_DEVICE:

3.23 Generate TCP dump in rotation

この選択肢は、「Generate TCP Dump」セクションと「Generate TCP dump and slon」にある他の diag の選択肢とは異なります。

「Generate TCP dump in rotation」の場合、フィルター IP アドレスを入力します (すべての IP にブランクを入力します)。次に、フィルターのポート番号を入力します。循環の TCP ダンプが既に実行中である場合は、実行期間を尋ねる質問で、「Rotation OFF」または「Rotation」(ON) のいずれかのオプションを選択します。「Rotation」を選択した場合は、ファイル・サイズを追加してください。

TCP ダンプが、/var/log/guard/tcp.bin1 と /var/log/guard.bin2 に交替で出力されます。

プロセス loop_tcpdump.sh を停止するには、「TCP dump in rotation」をもう一度選択します。

4 Perform Maintenance Actions

メインメニューから「Perform Maintenance Actions」オプションを選択し、「Maintenance」メニューを開きます。これらのコマンドは、必ず技術サポートの指示を受けて使用してください。これらのコマンドを定期的に実行する必要はありません。

4.1 TURBINE analysis (update index cardinality)

このコマンドを使用して、Guardium の内部データベースで索引のカーディナリティーを最適化します。操作の実行中は、進行状況表示バーが表示されます。操作が完了すると、「Maintenance」メニューに戻ります。

4.2 TURBINE optimize (rebuild indexes, takes longer)

このコマンドを使用して、Guardium の内部データベースを分析し、再索引します。

1. 「Maintenance」メニューから、「TURBINE optimize (index cardinality)」を選択します。操作の実行中は、進行状況表示バーが表示されます。操作が完了すると、「Maintenance」メニューに戻ります。

4.3 Clean disk space

このコマンドを使用して、使用されていないディスク・スペースのクリーンを行います。手順が完了すると、「Maintenance」メニューに戻ります。

1. 「Maintenance」メニューから、「Clean disk space」を選択します。ディレクトリーを選択するよう求めるプロンプトが出されます。
2. ファイルを削除するディレクトリーを選択します。ディレクトリーの内容がリストされ、すべてのファイルを削除することの確認を求めるプロンプトが出されます。
3. 操作が完了すると、「Maintenance」メニューに戻ります。

4.4 RAID maintenance

このコマンドは、必ず技術サポートを指示を受けて使用してください。このコマンドでは、RAID ドライブの状況を表示するために使用できる、RAID コントローラー・ユーティリティー・プログラムの管理メニューに対するアクセス権限を提供します。ご使用のシステムに RAID コントローラーがない場合は、このコマンドを選択するとエラー・メッセージが表示されます。RAID コントローラー・ユーティリティー・プログラムで提供される機能の中には、ディスク上のすべての情報を消去するものがあるため、このプログラムを使用する際には十分に注意してください。

4.5 Application Debugging Utility

このコマンドを使用して、デバッグをオンまたはオフにします。ロギングを使用可能または使用不可にするか、システム・デフォルトにリセットするよう求めるプロンプトが出されます。

4.6 Modify TURBINE watchdog threshold

このオプションを使用して、長時間かかる照会に対するタイムアウト制限を変更します。

4.7 Force unrecoverable MySQL to start

このオプションは、技術サポートの指示があった場合にのみ使用してください。

4.8 Transfer backups and system recovery

このコマンドを使用して、バックアップされた内部データベースをリストアします。操作の確認を求めるプロンプトが出されます。

4.9 Tomcat Logging Level

このコマンドを使用して、コンポーネントのデバッグ・レベルを選択します。次のオプションのいずれかを選択してください。

「Classifier」、「Data Level Security」、「Workflow」、または「Other」。

「Classifier」を選択して、デバッグ・レベル・オプション (ERROR、WARN、INFO、DEBUG、ALL) を選択します。

「DLS (data level security)」、「Workflow」、または「Other (text input)」を選択して、デバッグ・レベル・オプション (ERROR、WARN、INFO、DEBUG、ALL) を選択します。

Other を選択する場合は (コンマ区切りによるテキスト入力)、有効なコンポーネント (DLS、ワークフロー、監査、カスタム表、GUI、その他、ジョブ) を入力します。

4.10 Aggregator Maintenance

アグリゲーターの完全な分析およびリカバリーです。このユーティリティーは、AGG 関連ログを収集して diag エクスポート・フォルダーに配置し、Aggregator Fix Schema を呼び出してすべてのデータベースのスキーマを同期し、AGG ワークスペースのクリーンを行い、マージ処理を再開して、インポートされたすべての表の完全な分析が確実に行われるようにします (バックグラウンドで実行され、完了までに数時間かかる場合があります)。

4.11 Aggregator Fix Schema

インポートされたすべての表のスキーマを、最新のパッチ・レベルにします (バックグラウンドで実行され、完了までに数時間かかる場合があります)。

4.12 Clean Static Orphans

このオプションは、静的表が増えすぎたために消去する必要がある場合にのみ、技術サポートが使用する必要があります。このユーティリティーは、関連付けられているインスタンスがない古い構成レコードをすべて消去します。(コレクターまたはアグリゲーターで使用する) 静的オーファンの消去中には、進行状況メッセージが表示されます。

5 Exit to CLI

メインメニューで「Exit to CLI」を選択します。Enter キーを押して diag コマンドを閉じ、CLI に戻ります。

親トピック: CLI の概要

ファイル処理 CLI コマンド

これらのコマンドは、システム情報のバックアップとリストアに使用します。これらのタスクの多くは、Guardium® ユーザー・インターフェースから実行できます。

アーカイブ・データ・ファイル名について

Guardium データがアーカイブ (またはアグリゲーターにエクスポート) されると、日ごとに別のデータ・ファイルができます。エクスポート/パージ操作またはアーカイブ/パージ操作の構成によって、同日のエクスポート・データのコピーが複数できる場合があります。アーカイブ・データ・ファイル名とエクスポート・データ・ファイル名の形式は同じで、次のようになります。

<daysequence>-<hostname.domain>-w<run_datestamp>-d<data_date>.dbdump.enc

daysequence は、アーカイブ・データの日付を表す数値で、0 年からの日数として表現されます。名前の data_date 部分では同じ日付が yyyy-mm-dd 形式で表されます。

hostname.domain は、アーカイブが作成された Guardium アプライアンスのホスト名で、その後にドット文字とドメイン・ネームが続きます。

run_datestamp は、データがアーカイブまたはエクスポートされた日付で、yyyymmdd.hhmmss 形式で表されます。

data_date は、アーカイブ・データの日付で、yyyy-mm-dd 形式で表されます。

例: 732423-g1.guardium.com-w20050425.040042-d2005-04-22.dbdump.enc

backup config

これらのコマンドは、内部管理表にある構成情報のバックアップとリストアを行います。 backup config コマンドは、/media/backup ディレクトリーにデータを保管します。backup config コマンドは、ライセンスなどのマシン固有の情報を削除します。 backup system コマンドは、構成およびシステム全体をさらに包括的にバックアップします。

構文

backup config

restore config

backup system

このトピックでは、Guardium 内部データベースに対するバックアップ操作とリストア操作を説明します。 構成情報のみ、またはシステム全体のどちらかをバックアップまたはリストアできます (システム全体とは、データに構成情報が加わったものです。ただし、共有パスワード・ファイルは除きます。このファイルのバックアップとリストアは別に行われます。aggregator backup keys file および aggregator restore keys file コマンドを参照してください。)。これらのコマンドは検査エンジンと Web サービスをすべて停止し、操作完了後にそれらを再始動します。

ファイルをリストアする前に、そのファイルを作成したシステムのシステム共有パスワードをアプライアンスが使用できるようにしておいてください (そうしないと、情報の暗号化を解除できません)。 「Guardium 管理者ガイド」の『システム共有パスワードについて』を参照してください。
注: システム・リストアは、システム・バックアップと同じパッチ・レベルに対して実行する必要があります。例えばバージョン 7.0 パッチ 7 の時点でアプライアンスをバックアップした後、新しく構築したアプライアンスにこのバックアップをリストアするには、まずバージョン 7.0 のパッチ 1 から 7 までをアプライアンスにインストールした後で、ファイルをリストアする必要があります。
リストア処理には、次の 2 つのコマンドが関係します。

- import file - アーカイブ・バックアップ・ファイルをシステムに返します。
- restore system - import file 操作によって既に返されているバックアップ・ファイルからシステムをリストアします。

backup、import、および restore コマンドのすべてで、どのストレージ・システムが構成されているか、およびリストア操作のタイプに応じて、以下の項目を組み合わせて提供する一連のプロンプトが出されます。 操作に合わせて各プロンプトに応答してください。次の表に、プロンプトが出される対象になる情報を示します。

注:

SCP/FTP/TSM/Centera ファイル転送の 1 コピーが保存されます (転送が成功したか失敗したかは無関係)。ファイルによっては再生成に数時間かかることがあるので (例えばシステム・バックアップ)、すぐに使用できるコピーがあることは (特にファイル転送が失敗した場合)、ユーザーにとって価値があります。 各ファイル・タイプ (アーカイブ/システム・バックアップ/構成バックアップなど) に対して 1 コピーのみ保持されます。

バックアップ・システムは現在のライセンス、課金、およびデータ・ソース数をコピーしてから、データをバックアップします。リストア・システムはデータをリストアしてから、ライセンス、課金、およびデータ・ソース数をリストアします。 このシーケンスは、通常のリストア・システムにも当てはまります。以前のシステムからリストアする場合は、ライセンス、課金、およびデータ・ソース数の再構成が必要になります。

バックアップの構成時にポート番号の値が「0」である場合、デフォルトのポートがそのプロトコルに使用されていてそれを変更する必要がないことを示しています。

表 1. backup system

項目	記述
SCP、FTP、TSM、Centera、Snapshot	ファイルの転送に使用する方式を選択します。 TSM と Centera は、転送に使用するストレージ方式が使用可能に設定されている場合のみ表示されます (store storage-method コマンドを参照)。
Data または Configuration	定義と構成情報のみをバックアップするには、「Configuration」を選択します。構成情報に加えてデータもバックアップするには、「Data」を選択します。
restore from archive または restore from backup	アーカイブ・データをリストアするには、「restore from archive」を選択します。構成情報をリストアするには、「restore from backup」を選択します。
normal または upgrade	同じソフトウェア・バージョンの Guardium からリストアする場合は、「normal」を選択します。 Guardium アプライアンスのソフトウェア・アップグレードの後で構成情報をリストアする場合は、「upgrade」を選択します。
host	バックアップ・ファイルのリモート・ホスト。
remote directory	バックアップ・ファイルのディレクトリー。 FTP の場合は、使用する FTP ユーザー・アカウントの FTP ルート・ディレクトリーからの相対ディレクトリー・パスです。SSH の場合、このディレクトリー・パスは絶対ディレクトリー・パスです。 Windows SSH サーバーの場合は、Windows スタイルの円記号ではなく、Unix スタイルのスラッシュを使用したパス名にします。
username	操作に使用するユーザー・アカウント名 (バックアップ操作の場合、このユーザーには指定したディレクトリーに対する書き込み/実行権限が必要です)。 **注:** Windows の場合、ドメイン・ユーザーは domain¥user の形式にしてください。
password	ユーザー名のパスワード。
file name	アーカイブ・ファイルまたはバックアップ・ファイルのファイル名。 『アーカイブ・データ・ファイル名について』を参照してください。 ファイル名の中にワイルドカード文字 * を使用することにより、複数のファイルを選択できます。転送方式として FTP、SCP、および Snapshot を使用する場合、ワイルドカード文字 * を使用できます。TSM または Centera 転送方式では、ワイルドカード文字 * は使用できません。
Centera server	Centera サーバー名を入力します。PEA ファイルを使用する場合は、形式 <Host name/IP>? <full PEA file name> を使用します。例えば、次のように入力します。 128.221.200.56?/var/centera/us_profile_rwqe.pea.txt
Centera clipID	Centera リストア操作で、バックアップ操作から返されるコンテンツ・アドレス。 例: 6M4B15U4JM4LBeDGKCPF9VQO3UA

バックアップまたはリストア操作に必要な情報をすべて提供すると、操作の結果を通知する一連のメッセージが表示されます。 例えば restore system 操作の場合、メッセージは次のようなものになります (リストアのタイプと使用されるストレージ方式によって異なります)。

```
gpg: Signature made Thu Feb 22 11:38:01 2009 EST using DSA key ID 2348FF9E gpg: Good signature from "Backup Signer
<support@guardium.com>" Proceeding to shutdown services Proceeding to startup services Safekeeping admin.xreg Safekeeping
client.xreg Safekeeping controllers.xreg Safekeeping controls.xreg Safekeeping guardium-portlets.xreg Safekeeping local-
portlets.xreg Safekeeping local-security.xreg Safekeeping local-skins.xreg Safekeeping media.xreg Safekeeping portlets.xreg
Safekeeping security.xreg Safekeeping skins.xreg guard_sniffer.pl -reorder Recovery procedure was successful. ok
```

バックアップ/アーカイブのスクリプトによる /var 容量の使い尽くしの防止

バックアップ・プロセスは、実行前に /var の空き容量をチェックして失敗を防止します。 このプロセスは、バックアップ用のスペースが十分にない場合にも、 ユーザーに警告を出します。

アーカイブ・プロセスは、 静的表のサイズをチェックし、アーカイブを作成できる空き容量が /var にあることを 確認します。

バックアップが 50% を超えると、 ログ・ファイルおよび GUI にエラーが記録されるようになっています。

例:

```
ERROR: /var backup space is at 60% used. Insufficient disk space for backup. CLI> backup system     1. DATA     2. CONFIGURATION
Please enter the number of your choice: (q to quit) 1      1. SCP     2. CONFIGURED DESTINATION  Enter the number of your choice:
(q to quit) 2 Make sure destination is configured in the GUI under the System Backup option Please wait, this may take some time.
```

backup profile

このコマンドは、バックアップ・プロファイル・データを保守するために使用します (パッチ・メカニズム)。

バックアップ・ファイルは、バックアップ・プロファイルに基づいて宛先にコピーされます。 バックアップ・ファイルを保持するかどうかを示すパラメーターが「1」で、ディスク・スペースが十分にある場合、システム内にバックアップ・ファイルが保持されます (それ以外の場合は削除されます)。

4 つのフィールド (backup destination host、backup destination directory、backup destination user、backup destination password) すべてに入力する必要があります。

構文

show backup profile

例

```
patch backup flag is 1    patch backup automatic recovery flag is 1    patch backup dest host is    patch backup dest dir is
patch backup dest user is    patch backup dest pass is    ok
```

構文

store backup profile

例

```
Do you want to set up for automatic recovery? (y/n)    Enter the patch backup destination host:    Enter the patch backup
destination directory:    Enter the patch backup destination user:    Enter the patch backup destination password:
```

export audit-data

指定された日付 (yyyy-mm-dd) の監査データを、さまざまな内部 Guardium 表から圧縮アーカイブ・ファイルにエクスポートします。指定した日付のデータは、/var/dump ディレクトリーの圧縮アーカイブ・ファイルに保管されます。 作成されたファイルは、システムが生成するメッセージで示されます。 例を参照してください。このコマンドは、必ず Guardium サポートの指示に従って使用してください。

注: このコマンドを実行できるのは、admin ロールが設定されたユーザーのみです。

構文

export audit-data <yyyy-mm-dd>

例

```
If you enter the audit-data command for the date 2005-09-16, a set of messages similar to the following will be created: CLI>
export audit-data 2005-09-16 2005-09-16 Extracting  GDM_ACCESS  Data ... Extracting  GDM_CONSTRUCT  Data ... Extracting
 GDM_SENTENCE  Data ... Extracting  GDM_OBJECT  Data ... Extracting  GDM_FIELD  Data ... Extracting  GDM_CONSTRUCT_TEXT  Data ...
Extracting  GDM_SESSION  Data ... Extracting  GDM_EXCEPTION  Data ... Extracting  GDM_POLICY_VIOLATIONS_LOG  Data ... Extracting
 GDM_CONSTRUCT_INSTANCE  Data ... Generating tar file ...  /var/csvGenerationTmp ~ GDM_ACCESS.txt GDM_CONSTRUCT.txt
GDM_CONSTRUCT_INSTANCE.txt GDM_CONSTRUCT_TEXT.txt GDM_EXCEPTION.txt GDM_FIELD.txt GDM_OBJECT.txt GDM_POLICY_VIOLATIONS_LOG.txt
GDM_SENTENCE.txt GDM_SESSION.txt ~ Generation completed, CSV Files saved to /var/dump/732570-supp2.guardium.com-w20050919110317-
d2005-09-16.exp.tgz ok
```

名前付の内部データベース表それぞれのデータが、CSV 形式でテキスト・ファイルに書き込まれます。 アーカイブ・ファイルの名前の最後に exp.tgz が付けられ、名前の残りの部分は『アーカイブ・データ・ファイル名について』での説明のとおりに形成されます。

export file コマンドを使用して、このファイルを別のシステムに転送できます。

delete audit-data

このコマンドは、必ず Guardium サポートの指示に従って使用してください。 このコマンドは、圧縮監査データ・ファイルを削除するために使用します。 削除するファイルを特定する索引番号を入力する必要があります。 アーカイブ・データ・ファイル名の形式については、『アーカイブ・データ・ファイル名について』を参照してください。

削除するファイルを特定するようにプロンプトが出されます。

構文

delete audit-data

show audit-data

このコマンドは、CLI コマンド export audit-data を実行して作成されたすべてのファイルを表示するために使用します。監査データ・ファイルについて詳しくは、『export audit-data』を参照してください。

構文

show audit-data <yyyy-mm-dd>

export file

このコマンドは、/var/IBM/Guardium/data/dump、/var/log、または /var/IBM/Guardium/data/importdir ディレクトリーから、filename という名前の単一ファイルをエクスポートします。

このコマンドは、必ず Guardium サポートの指示に従って使用してください。 Guardium データをアグリゲーターにエクスポートするか、データをアーカイブするには、「管理コンソール」パネル上の該当するメニュー・コマンドを使用します。

構文

export file </local_path/filename> <user@host:/path/filename>

local_path は、/var/IBM/Guardium/data/dump、/var/log、または /var/IBM/Guardium/data/importdir のいずれかでなければなりません。

fileserver

このコマンドは、Guardium アプライアンス上で実行される HTTP ベースのファイル・サーバーを開始するために使用します。 このファシリティーは、ユニットへのパッチのアップロード、またはユニットからのデバッグ情報のダウンロードを容易に実行できるようにすることを目的としています。このファシリティーは開始のたびに、パ

ッチのアップロード先のディレクトリーに含まれるすべてのファイルを削除します。

注: ファイル・サーバーがアクセスすることになるファイルを生成する操作は、ファイル・サーバーの開始前に完了する必要があります (ファイルをファイル・サーバーが使用できるようにするため)。

構文

fileserver [https://ip address:8445] [duration]

ip address は、指定された IP アドレスからファイル・サーバーへのアクセスを可能にするオプション・パラメーターです。デフォルト (パラメーターなし) では、アクセスは、ファイル・サーバーを開始した SSH クライアントの IP アドレスに制限されます。

duration は、ファイル・サーバーがアクティブである秒数を指定するオプション・パラメーターです。指定された秒数が経過すると、ファイル・サーバーは自動的にシャットダウンします。期間は 60 秒から 3600 秒までの任意の秒数に設定できます。

ブラウザー・セッションがプロキシー・サーバー経由でリダイレクトされるセキュリティー設定では、ファイル・サーバー・クライアントの IP アドレスは、ファイル・サーバーを開始した SSH クライアントと同じにはなりません。その代わり、ファイル・サーバー・クライアントはプロキシー・サーバーの IP アドレスを保持し、このアドレスはオプションの ip address パラメーターを渡す必要があります。プロキシー IP アドレスを見つけるには、「Guardium モニター」インターフェースの「Guardium へのログイン」レポートに表示されるブラウザー設定またはクライアント IP アドレスを確認します。

例

ファイル・サーバーを開始するには、次のように fileserver コマンドを入力します。

CLI> fileserver <ip address> <duration>

ファイル・サーバーを開始しています。これは https://(アプライアンスの名前):8445 にあります。

ファイル・サーバーを停止するには ENTER を押してください。

ブラウザー・ウィンドウでファイル・サーバーを開き、以下のいずれかを実行します。

- パッチをアップロードするには、「Upload a patch」をクリックし、指示に従います。
- ログ・データをダウンロードするには、「Sqlguard logs」をクリックし、目的のファイルにナビゲートして、他のファイルの場合と同様にダウンロードします。

完了した後で CLI セッションに戻り、Enter を押してセッションを終了します。

fileserver を使用した VA および資格スクリプトへのアクセス方法

操作手順

CLI から、「fileserver <デスクトップ IP> 3600」を実行します。

脆弱性評価:

ブラウザーを開き、https://<アプライアンス ip>/log/debug-logs/gdmmonitor_scripts/ にアクセスします。

ご使用のデータベース・タイプに一致するファイルを選択します。

資格:

ブラウザーを開き、https://<アプライアンス IP>/log/debug-logs/entitlemnts_monitor_role/ にアクセスします。

ご使用のデータベース・タイプに一致するファイルを選択します。

import file

『backup config』および『restore config』を参照してください。

import file CLI コマンドでは、scp、ftp、および snapshot 方式の場合、ファイル名にワイルドカード * を使用できます。

構文

import file

import tsm config

TSM クライアント構成ファイルを Guardium アプライアンスにアップロードします。この操作は、TSM を使用するアーカイブまたはバックアップ操作を実行する前に行う必要があります。 どの場合も、dsm.sys ファイルをアップロードする必要があります。また、このファイルに servername セクションが複数ある場合は、dsm.opt ファイルもアップロードする必要があります。 これらのファイルの作成方法については、お客様の会社の TSM 管理者に確認してください。

指定したホストのユーザー・アカウントのパスワードを求めるプロンプトが出されます。

構文

import tsm config <user@host:/path/[dsm.sys | dsm.opt]>

パラメーター

user@host - 指定したホスト上のファイルにアクセスするためのユーザー・アカウント。

/path/[dsm.sys | dsm.opt] - インポートするファイルの絶対パス・ファイル名。

注: 各コレクターに TSM を設定する場合、初期構成に失敗すると、テスト・ファイルを送信できなかったという通知エラーが出される結果になります。コレクターに root としてログインし、TSM サーバーに対して dsmc アーカイブ・コマンドを実行すると、同じ資格情報で TSM ファイルを構成できます。 GUI に戻り、前に使用したオプシ

ョンと同じオプションを使用しても構成できます。

tsm config に passwordaccess=generate が含まれている場合、ローカル・ファイルに格納されているパスワードが探索されます。このローカル・パスワード・ファイルを作成するために、root ユーザーは dsmc コマンドを 1 回実行する必要があります。

tsm config ファイルのアップロード後、tsm config に「passwordaccess generate」プロンプトが含まれていれば、「passwordaccess」が生成されるように設定されます。

```
Would you like to run a dsmc command now to ensure password is set locally (y/n)?     If the answer is y, run a "dsmc query
options>>/dev/null" command, which will prompt user for password.
```

import tsm property

この CLI コマンドを使用して、/opt/tivoli/tsm/client/ba/bin/guard_tsm.properties にファイルをアップロードします。

ファイルのサイズは、1K にしてください。

構文

import tsm property user@host:file

このコマンドを実行すると、入力ファイルが /opt/tivoli/tsm/client/ba/bin/guard_tsm.properties にアップロードされます。

restore config

これらのコマンドは、内部管理表にある構成情報のバックアップとリストアを行います。 backup config コマンドは、/media/backup ディレクトリーにデータを保管します。backup config コマンドは、ライセンスなどのマシン固有の情報を削除します。 backup system コマンドは、構成およびシステム全体をさらに包括的にバックアップします。

構成をリストアするときには、バックアップ作成時の元のアプライアンスと同じバージョン、同じパッチ・レベルのバックアップをリストアする必要があります。

構文

backup config

restore config

restore db-from-prev-version

このコマンドは、直前のシステムからバックアップを取り (バックアップ・データの提供が必要、構成バックアップはオプション)、最新のシステム上でリストアを実行します。これには、データやポートレットなどのアップグレードが含まれます。

Guardium システムをアップグレードする前に、システムのフルバックアップを実行します。何らかの理由でアップグレードに失敗し、マシンが使用できない状況になった場合、アップグレードを修正して再実行を試みるのではなく、マシンを最新のシステムとして再構築し、この最新システムを基本ネットワーク情報 (IP、リゾルバー、経路、システム・ホスト名、およびドメイン) のみによって設定します。

結果として、前のシステムのデータとカスタマイズ (構成ファイルが提供された場合) が取り込まれた最新のシステムになります。

まず、以前のシステムから最新システムへの通常のアップグレードを試行してください。正常にアップグレードできなかった場合に、以前のシステムから最新システムにアップグレードするための代替方法として、backup を使用してください。

注: (調査センターではなく) アグリゲーターにリストアされる古いデータで、マージ期間外のデータは、マージ期間が変更されてマージ・プロセスが再実行されるまで表示されません。

このコマンドを実行するには、現在のサーバーのデータと構成の両方をバックアップします。バックアップが完了した後、最新のリリースを同じサーバーにインストールしてください。次に、CLI から import file コマンドを使用して、データ・ファイルと構成ファイルの両方をインポートします。2 つのバックアップ・ファイルがインポートされた後、再度 CLI からコマンド restore db-from-prev-version を実行します。 これにより、古いバージョンからのバックアップ・ファイル (データと構成) が、新しくインストールされたサーバーにリストアされます。
注: Guardium を英語以外の言語で使用している場合には、restore CLI コマンドにより、レポート・ヘッダーなどの一部の文字列が英語に設定されます。このような文字列を英語以外の言語で表示するには、restore CLI コマンドを実行した後に、store language CLI コマンドを実行します。

オプション・パラメーターの「override」は、バックアップからの中央マネージャー・アプライアンスのリストアにのみ適用できます。

デフォルトでは、ユーザーが中央マネージャー・アプライアンス上で「restore db-from-prev-version」コマンドを実行すると、管理対象の管理対象ユニットにリンクする、この中央マネージャーにある既存の構成情報を保存します。

ユーザーが restore コマンドに「override」を追加すると、既存の中央マネージャー/管理対象ユニット構成は、バックアップ・データからの中央マネージャー/管理対象ユニット構成によってオーバーライドされます。

構文

restore db-from-prev-version [override]

例

restore db-from-prev-version

restore db-from-prev-version override

注: この CLI コマンドを使用すると、「S-TAP と管理対象ユニットの関連付け」の管理対象ユニットと S-TAP の関連付けは復元されません。ユーザーは関連付けを再度定義する必要があります。
構文

```
restore db-from-prev-version
```

```
This procedure will restore and upgrade a previous backup on a newly-installed latest system. If the older files are currently
located on a remote system, use the "import file" cli command to transfer them locally prior to running this procedure. The
imported files will be put in the /var/dump/ directory. Continue (y/n)?
```

注:

CLI コマンド restore db-from-prev-version の実行中に次の質問に Y (はい) と応答すると、非標準装備/カスタマイズ・タイプのすべてのレポートとペインが圧縮されて「v.x.0 カスタム・レポート」という名前の 1 つのペインに入ります。

これらの同じ質問に N (いいえ) と応答すると、すべてのペインが以前のバージョンの状態にリストアされます。

```
Update portal layout (panes and menus structure) to the new v8 default (current instances of custom reports will be copied to the
new layout, as well as parameter changes on predefined reports) for the user admin? (y/n) n  Update portal layout (panes and menus
structure) to the new v8 default (current instances of custom reports will be copied to the new layout, as well as parameter
changes on predefined reports) for all other users? (y/n)
```

restore keystore

このコマンドは、必ず技術サポートの指示に従って使用してください。

このコマンドは、Web サーブレット・コンテナー環境 (Tomcat) によって使用される認証と秘密鍵をリストアするために使用します。

構文

restore keystore

restore pre-patch-backup

このコマンドは、必ず技術サポートの指示に従って使用してください。

このコマンドは、アプライアンス・データベースが稼働時または停止時に pre-patch-backup をリカバリーするために使用します。

構文

```
restore pre-patchbackup Please enter the information to retrieve the file: Is the file in the local system? (y/n) n Start to
recover with the backup profile parameters. Please check the recovery status in the log
/var/log/guard/diag/depot/patch_installer.log ok ------------------------------------ If answer 'n', abort the operation. If
answer 'y', need to enter the file name.
```

restore system

このトピックでは、Guardium 内部データベースに対するバックアップ操作とリストア操作を説明します。 構成情報のみ、またはシステム全体のどちらかをバックアップまたはリストアできます (システム全体とは、データに構成情報が加わったものです。ただし、共有パスワード・ファイルは除きます。このファイルのバックアップとリストアは別に行われます。aggregator backup keys file および aggregator restore keys file コマンドを参照してください。)。これらのコマンドは検査エンジンと Web サービスをすべて停止し、操作完了後にそれらを再始動します。

ファイルをリストアする前に、そのファイルを作成したシステムのシステム共有パスワードをアプライアンスが使用できるようにしておいてください (そうしないと、情報の暗号化を解除できません)。「Guardium 管理者ガイド」の『システム共有パスワードについて』を参照してください。

注: システム・リストアは、システム・バックアップと同じパッチ・レベルに対して実行する必要があります。
リストア処理には、次の 2 つのコマンドが関係します。

- import file - アーカイブ・バックアップ・ファイルをシステムに返します。
- restore system - import file 操作によって既に返されているバックアップ・ファイルからシステムをリストアします。

backup、import、および restore コマンドのすべてで、どのストレージ・システムが構成されているか、およびリストア操作のタイプに応じて、以下の項目を組み合わせて提供する一連のプロンプトが出されます。 操作に合わせて各プロンプトに応答してください。次の表に、プロンプトが出される対象になる情報を示します。

注:

SCP/FTP/TSM/Centera ファイル転送の 1 コピーが保存されます (転送が成功したか失敗したかは無関係)。ファイルによっては再生成に数時間かかることがあるので (例えばシステム・バックアップ)、すぐに使用できるコピーがあることは (特にファイル転送が失敗した場合)、ユーザーにとって価値があります。 各ファイル・タイプ (アーカイブ/システム・バックアップ/構成バックアップなど) に対して 1 コピーのみ保持されます。

バックアップ・システムは現在のライセンス、課金、およびデータ・ソース数をコピーしてから、データをバックアップします。リストア・システムはデータをリストアしてから、ライセンス、課金、およびデータ・ソース数をリストアします。 このシーケンスは、通常のリストア・システムにも当てはまります。以前のシステムからリストアする場合は、ライセンス、課金、およびデータ・ソース数の再構成が必要になります。

表 2. restore system

項目	記述
SCP、FTP、TSM、Centera、Snapshot	ファイルの転送に使用する方式を選択します。 TSM と Centera は、転送に使用するストレージ方式が使用可能に設定されている場合のみ表示されます (store storage-method コマンドを参照)。
Data または Configuration	定義と構成情報のみをバックアップするには、「Configuration」を選択します。構成情報に加えてデータもバックアップするには、「Data」を選択します。
restore from archive または restore from backup	アーカイブ・データをリストアするには、「restore from archive」を選択します。構成情報をリストアするには、「restore from backup」を選択します。
normal または upgrade	同じソフトウェア・バージョンの Guardium からリストアする場合は、「normal」を選択します。 Guardium アプライアンスのソフトウェア・アップグレードの後で構成情報をリストアする場合は、「upgrade」を選択します。
host	バックアップ・ファイルのリモート・ホスト。

項目	記述
remote directory	バックアップ・ファイルのディレクトリー。 FTP の場合は、使用する FTP ユーザー・アカウントの FTP ルート・ディレクトリーからの相対ディレクトリー・パスです。SSH の場合、このディレクトリー・パスは絶対ディレクトリー・パスです。Windows SSH サーバーの場合は、Windows スタイルの円記号ではなく、Unix スタイルのスラッシュを使用したパス名にします。
username	操作に使用するユーザー・アカウント名 (バックアップ操作の場合、このユーザーには指定したディレクトリーに対する書き込み/実行権限が必要です)。 **注:** Windows の場合、ドメイン・ユーザーは domain¥user の形式にしてください。
password	ユーザー名のパスワード。
file name	アーカイブ・ファイルまたはバックアップ・ファイルのファイル名。 『アーカイブ・データ・ファイル名について』を参照してください。 ファイル名の中にワイルドカード文字 * を使用することにより、複数のファイルを選択できます。転送方式として FTP、SCP、および Snapshot を使用する場合、ワイルドカード文字 * を使用できます。TSM または Centera 転送方式では、ワイルドカード文字 * は使用できません。
Centera server	Centera サーバー名を入力します。PEA ファイルを使用する場合は、形式 <Host name/IP>? <full PEA file name> を使用します。例えば、次のように入力します。 128.221.200.56?/var/centera/us_profile_rwqe.pea.txt サーバー IP と PEA ファイル名の間の ? に注意してください。 この IP アドレスおよび .PEA ファイルは、EMC Centera から取得します。 パスを構成する際には、疑問符が必須です。「.../var/centera/...」を含むパス名でなければバックアップが失敗するため、このパス名は重要です。 .PEA ファイルは、Centera バックアップ要求ごとにアクセス権、ユーザー名、およびパスワード認証を提供します。
Centera clipID	Centera リストア操作で、バックアップ操作から返されるコンテンツ・アドレス。 例: 6M4B15U4JM4LBeDGKCPF9VQO3UA

バックアップまたはリストア操作に必要な情報をすべて提供すると、操作の結果を通知する一連のメッセージが表示されます。 例えば restore system 操作の場合、メッセージは次のようなものになります (リストアのタイプと使用されるストレージ方式によって異なります)。

```
gpg: Signature made Thu Feb 22 11:38:01 2009 EST using DSA key ID 2348FF9E gpg: Good signature from "Backup Signer
<support@guardium.com>" Proceeding to shutdown services Proceeding to startup services Safekeeping admin.xreg Safekeeping
client.xreg Safekeeping controllers.xreg Safekeeping controls.xreg Safekeeping guardium-portlets.xreg Safekeeping local-
portlets.xreg Safekeeping local-security.xreg Safekeeping local-skins.xreg Safekeeping media.xreg Safekeeping portlets.xreg
Safekeeping security.xreg Safekeeping skins.xreg guard_sniffer.pl -reorder Recovery procedure was successful. ok
```

setup help (バックアップ用 2 次ディスク)

R610 R710 アプライアンスにバックアップ用 2 次ディスクを取り付けてください。このディスクはスロット番号 2 に取り付けます。続いて setup snapshotdisk を実行してパーティションを構成し、ドライブをフォーマットした後にマウントします。選択可能な 2 つの CLI は、setup help および setup snapshotdisk です。

構文

setup [help | snapshotdisk | vmware_tools]

store language

この CLI コマンドを使用して、ベースライン言語の英語を希望する言語に変更し、データベースをその言語に変換します。 Guardium のインストールは、常に英語で行われます。 Guardium システムは、インストール後に日本語、中国語 (繁体字または簡体字)、フランス語、スペイン語、ドイツ語、またはポルトガル語に変更できます。

CLI コマンド store language はアプライアンスのセットアップと見なされ、アプライアンスの初期セットアップ時に実行されることを目的としています。

特定の言語でアプライアンスをデプロイメントした後にこの CLI コマンドを実行すると、既にキャプチャー、保管、カスタマイズ、アーカイブ、またはエクスポートされた情報を変更することができます。

注: 英語から目的の言語に切り替えた後は、この CLI コマンドを使用してその言語を英語に戻すことはできません。Guardium システムを英語で再インストールする必要があります。

構文

CLI> store language [English | Japanese | SimplifiedChinese | TraditionalChinese | French | German | Spanish | Portuguese]

表示コマンド

show language

setup vmware tools

この CLI コマンドを使用して、ESX インフラストラクチャーで実行される VMware をインストールします。

構文

setup vmware_tools [install | uninstall]

ステップ 1: VM クライアント/コンソールを開き、IBM Guardium アプライアンスが含まれる VM インスタンスを選択します。インスタンスを右クリックし、(ポップアップ・メニューから) ゲスト => VMware ツールのインストール/アップグレードを選択します。これにより、インスタンスがマウント・ポイントを介して VMware ツールに

アクセスできるようになります。

ステップ 2: (VM クライアント/コンソール内から) CLI コマンド setup vmware_tools install を実行して、VM ツールをインストールします。

Vmware のリブート後のカーネル・パニック

Guardium を稼働する VMware SX 4.1 仮想マシンが、リブート後にカーネル・パニックを起こすことがあります。

この状況を修正するには、VMware では ESX4.1 の Update 2 をインストールするか、CPU/MMU 仮想化を「Use software for instruction set and MMU Virtualization」に設定することが推奨されています。このオプションは、「Settings」/「Options」/「CPU/MMU」/「Use software for instruction set and MMU Virtualization」にあります。

親トピック: CLI の概要

検査エンジンの CLI コマンド

これらの CLI コマンドは、検査エンジンの構成に使用します。

検査エンジンは 1 つ以上のサーバーからなるサーバー・セットと、1 つ以上のクライアントからなるクライアント・セットとの間の、特定のデータベース・プロトコル (Oracle や Sybase など) を使用したトラフィックをモニターします。 検査エンジンはネットワーク・パケットから SQL を抜き出し、センテンス、要求、コマンド、オブジェクト、およびフィールドを識別する構文解析ツリーをコンパイルして、そのトラフィックについての詳細情報を内部データベースに記録します。

add inspection-engines

検査エンジンのリストの最後に、検査エンジン構成を追加します。 パラメーターを示します。新しい検査エンジンを追加した後に、reorder inspection-engines コマンドを使用して、検査エンジンのリストを再配列できます。検査エンジンを追加しても、その検査エンジンの実行は開始されません。実行を開始するには start inspection-engines コマンドを使用します。

構文

add inspection-engines <name> <protocol>

<fromIP/mask> <port> <toIP/mask>

<exclude client list> <active on startup>

パラメーター

name - 新しい検査エンジンの名前です。これはユニットで固有である必要があります。

protocol - モニター対象のプロトコル。以下のいずれかの値でなければなりません。Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share

fromIP/mask - IP アドレスおよびサブネット・マスクで識別されるクライアントのリスト。 IP アドレスとマスクはそれぞれスラッシュで区切り、複数のエントリーはコンマで区切ります。 アドレスとマスクがすべてゼロの場合は、ワイルドカードです。 除外クライアント・リストのオプションが Y の場合、検査エンジンはこのリストにあるクライアント以外のすべてのクライアントのトラフィックをモニターします。 除外クライアント・リストのオプションが N の場合、検査エンジンはこのリストのクライアントのトラフィックのみをモニターします。

port - 指定したクライアントとデータベース・サーバー間のトラフィックは、このポートまたはポート範囲を使用する場合にモニターされます。 範囲を指定するには、2 つの数字をハイフンでつなぎます。

toIP/mask - トラフィックがモニター対象となるデータベース・サーバーのリスト。IP アドレスとサブネット・マスクで識別されます。 IP アドレスとマスクはそれぞれスラッシュで区切り、複数のエントリーはコンマで区切ります。 アドレスとマスクがすべてゼロの場合は、ワイルドカードです。

exclude client list - Y/N の値をとります。デフォルトは N です。Y の場合、検査エンジンはこのクライアント・リストで識別されるクライアントを除く、すべてのクライアントのトラフィックをモニターします 。N の場合、検査エンジンはクライアント・リストに挙げられたクライアントのトラフィックのみをモニターします。

active on startup - 値は Y または N であり、デフォルトは N です。Y の場合、検査エンジンはシステム始動時に活動化します。

delete inspection-engines

name で識別される、単一の検査エンジンを削除します。 名前は文字、数字、空白のみを含むことができます。検査エンジンの名前に特殊文字が含まれている場合は、管理者ポータルの GUI を使用してこれを削除します。

構文

delete inspection-engines <name>

reorder inspection-engines

検査エンジンの新しい順序を、list inspection-engines コマンドで作成されたリストの索引値を使用して指定します。

構文

reorder inspection-engines <index>, <index>...

例

表示される索引が 1、2、3、4 の場合、次のコマンドによりエンジンの配列が逆になります。

reorder inspection-engines 4,3,2,1

restart inspection-core

検査エンジン・コアを再始動しますが、検査エンジンは再始動しません。 このコマンドが発行されると、データベース・トラフィックの収集は停止します。

構文

restart inspection-core

注: 1 つ以上の特定の検査エンジンのトラフィック収集を再開するには、このコマンドの後に 1 つ以上の start inspection engine コマンドを続けます。 またはすべての検査エンジンのトラフィック収集を再開するには、restart inspection-engines コマンドを使用します。

restart inspection-engines

データベース検査エンジン・コアおよびすべての検査エンジンを再始動します。 これが起こるとデータベース・トラフィックの収集は一時的に停止し、データベース接続が再び開始された場合にのみ、再開されます。

構文

restart inspection-engines

show inspection-engines

以下のような、検査エンジンの構成情報を表示します。

all - すべての検査エンジン。

configuration <index> - 指定した索引 (list inspection-engines コマンドで作成したもの) で識別される検査エンジンのみ。

type <db_type> - 特定のデータベース・タイプの構成を表示。このデータベース・タイプは、サポートされている以下のモニター対象プロトコル・タイプのいずれかである必要がある。Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share。

構文

show inspection-engines <all | configuration <index> | log sqlstrings | type <type> >

注: スパン・ポートなどの非 STAP 検査エンジンを表示するには、CLI コマンド show inspection-engines all を使用します。CLI コマンド list_inspection_engines は、STAP によって作成された検査エンジンを表示します。

start inspection-core

検査エンジン・コアを始動します。

構文

start inspection-core

start inspection-engines

list inspection-engines コマンドで作成されたリストの索引値を使用して識別される、1 つ以上の検査エンジンを始動します。

構文

start inspection-engines <all | id>

start inspection-engines all

すべての検査エンジンを開始します。

構文

start inspection-engine all

start inspection-engines id

使用法: start inspection-engines id <n> (n は数値のスニファー ID)

構文

start inspection-engines id <n>

stop inspection-engines id

使用法: stop inspection-engines id <n> (n は数値のスニファー ID)

stop inspection-core

検査エンジン・コアを停止します。

構文

stop inspection-core

stop inspection-engines

list inspection-engines コマンドで作成されたリストの索引値を使用して識別される、1 つ以上の検査エンジンを停止します。すべての検査エンジンを停止することもできます。

構文

stop inspection-engine <all | id>

stop inspection-engines all

すべての検査エンジンを停止します。

構文

stop inspection-engines all

stop inspection-engines id

list inspection-engines コマンドで作成されたリストの索引値を使用して識別される、1 つ以上の検査エンジンを停止します。

構文

stop inspection-engine <n> (<n> はスニファー ID の数字)

store ignored port list

すべての検査エンジンにより無視されるポート番号の完全なセットを設定します。 指定するリストは既存のリストをすべて置き換えます。リストではそれぞれの数字と次の数字をコンマで区切り、ブランクやその他の空白文字を入れてはなりません。 ハイフンを使用すると、その数字を含めた範囲の範囲指定ができます。

構文

store ignored port list <n>

例

store ignored port list 33,60-70

表示コマンド

show ignored port list

親トピック: CLI の概要

調査ダッシュボードの CLI コマンド

これらの CLI コマンドは、調査ダッシュボードを構成するために使用します。

show solr connection_timeout

このコマンドを使用して、現在の connection_timeout 値を表示します。

```
show solr connection_timeout
```

show solr so_timeout

このコマンドを使用して、現在の so_timeout 値を表示します。

```
show solr so_timeout
```

show solr time_allowed

このコマンドを使用して、現在の time_allowed 値を表示します。

```
show solr time_allowed
```

store solr connection_timeout

このコマンドを使用して、接続タイムアウトを設定します。指定されたタイムアウト期間内に調査ダッシュボードがコレクターに接続できない場合、そのコレクターから結果は返されません。

```
store solr connection_timeout [value]
```

パラメーター	値	記述
connection_timeout	integer	タイムアウトは、`0` から `2147483647` ミリ秒の値で表されます。 デフォルト値は `100000` ミリ秒です。

store solr so_timeout

このコマンドを使用して、ソケット・タイムアウトを設定します。

store solr so_timeout [value]

パラメーター	値	記述
so_timeout	integer	タイムアウトは、0 から 2147483647 ミリ秒の値で表されます。 デフォルト値は 100000 ミリ秒です。

store solr time_allowed

このコマンドを使用して、ソケット・タイムアウトを設定します。

store solr time_allowed [value]

パラメーター	値	記述
time_allowed	integer	タイムアウトは、0 から 2147483647 ミリ秒の値で表されます。 デフォルト値は 90000 ミリ秒です。 注: 深い検索では、time_allowed の 10 倍の値が使用されます。

親トピック: CLI の概要

ネットワーク構成 CLI コマンド

ネットワーク構成 CLI コマンドは、IP アドレスの設定、結合/フェイルオーバーの処理、2 次機能の処理、およびネットワークのリセットに使用します。

ネットワーク構成 CLI コマンドは、以下の目的で使用します。

- マシンの背面のコネクターを識別する。(show network interface port)
- ネットワーク・カードをインストールした後または移動した後に、ネットワーキングをリセットする。(store network interface inventory)
- IP アドレスを設定する。(store network interface ip、store network interface mask、store network resolver、store network routes defaultroute)
- 高可用性を有効または無効にする。(store network interface high-availability)
- ネットワーク・カードが接続されているスイッチで設定が自動ネゴシエーションされない場合に、ネットワーク・カードを構成する (store network interface auto-negotiation、store network interface speed、store network interface duplex)

restart network

ネットワーク構成のみを再始動します。 例えば、IP アドレスを変更した後に、この CLI コマンドを実行します。

構文

restart network

show network interface all

このコマンドは、Guardium® アプライアンスをデスクトップ LAN に接続するために使用されるネットワークの設定を表示します。IP アドレス、マスク、状態 (有効か無効か) および高可用性状況が表示されます。 IP 高可用性が有効な場合、システムは 2 つのインターフェース (ETH0 および ETH3) を表示します。そうでない場合は ETH0 のみが表示されます。

構文

show network interface all

show network routes operational

使用中の IP ルーティング構成を表示します。

構文

show network routes operational

例

CLI> show net rout ope

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 nic1

169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0 nic2

0.0.0.0 192.168.3.1 0.0.0.0 UG 0 0 0 nic1

ok

CLI>

show network verify

現行のネットワーク構成を表示します。

構文

show network verify

```
CLI> show network verify

Current Network Configuration
-------------------------------------------------------------------------------
Hostname =
-------------------------------------------------------------------------------
Device     | Address          | Netmask          | Gateway          | Member of
-------------------------------------------------------------------------------
eth0       |
-------------------------------------------------------------------------------
Ethtool Options
-------------------------------------------------------------------------------
Device     | Options (speed,autoneg,duplex)
-------------------------------------------------------------------------------
eth0       |
-------------------------------------------------------------------------------
DNS Servers
-------------------------------------------------------------------------------
Index      | DNS Server
-------------------------------------------------------------------------------
1          |
2          |
-------------------------------------------------------------------------------
Static Routes
-------------------------------------------------------------------------------
Device     | Index      | Address          | Netmask          | Gateway
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Basic Network Settings Verified
```

store network interface auto-negotiation

Guardium ポートが接続されているスイッチでオートネゴシエーションが使用可能な場合は、オートネゴシエーションが使用され、このコマンドの再始動オプションのみでは何も影響しません。 このコマンドを使用して、ethN という名前のネットワーク・インターフェースのオートネゴシエーションを有効にしたり、無効にしたり、または再始動したりします。 show network interface inventory コマンドを使用して、すべてのポート名を表示します。

構文

store network interface auto-negotiation <ethN> <on | off | restart>

表示コマンド

show network interface auto-negotiation

store network interface duplex

このコマンドは、Guardium ポートが接続されているスイッチ上でオートネゴシエーションが使用できない場合にのみ使用します。 このコマンドは、ethn という名前のポートに二重モードを構成します。 show network interface inventory コマンドを使用して、すべてのポート名を表示します。

構文

store network interface duplex <ethn> <half | full>

表示コマンド

show network interface duplex <ethn>

store network interface high-availability

IP のチーミング (結合とも言う) を有効または無効にします。IP のチーミングは、Guardium システムの 1 次 IP アドレスのフェイルオーバー機能を提供します。

使用される 2 つのポート (ETH0 および 2 番目のインターフェース) は、同じネットワークに接続されている必要があります。 スイッチがポート構成を再学習することにより、わずかな遅延があります。 デフォルト設定は off です。

1 次 IP アドレスに使用されるポートは常に ETH0 です。高可用性オプションが有効になっている場合、Guardium システムは、必要に応じて、指定した 2 番目のインターフェースに自動的にフェイルオーバーし、実質的に 1 次 IP アドレスを 2 番目のインターフェースに移動します。

注: IP のチーミングと 2 次インターフェースは、同時に実行できません。
構文:

```
store network interface high-availability [on <NIC> | off ]
```

show network interface high-availability コマンドはありません。

store network interface inventory

Guardium 内部の表に保管されているネットワーク・インターフェースの MAC アドレスをリセットします。 このコマンドは、ネットワーク・カードを取り換えたり、移動したりした後にのみ使用する必要があります。

注: store network interface inventory コマンドは、Guardium アプライアンス内のオンボード NIC カードを検出し、これらのカードを eth0 および eth1 として割り当てます。このコマンドは NIC カードの位置を変える可能性があるため、Guardium サポートからそうするよう特に指示された場合にのみ実行してください。

構文

```
CLI> > store network interface inventory
WARNING: Running this function will reorder your NICS and may make the machine unreachable.
WARNING: It is suggested to run this from the console or equivalent.
Are you SURE you want to continue? (y/n)
```

show コマンドは、インストールされているすべてのネットワーク・インターフェースのポート名および MAC アドレスを表示します。

構文

show network interface inventory

例

CLI> show network interface inventory

Current network card configuration:

Device | Mac Address | Member of

eth0 | 00:50:56:3b:c3:73 |

eth1 | 00:50:56:8a:0d:fa |

eth2 | 00:50:56:8a:0d:fb |

eth3 | 00:50:56:8a:00:c1 |

注: 「Member of」は、結合が存在する場合に、どの NIC が結合ペアであるかを示します。

store network interface ip

Guardium アプライアンスの 1 次 IP アドレスを設定します。ネットワーク・インターフェースの IP アドレスを変更する際には、そのサブネット・マスクも変更しなければならない場合があります。 store network interface mask を参照してください。2 次 IP アドレスの作成および管理を行うには、store network interface secondary を参照してください。 結合/フェイルオーバーは、CLI コマンド store network interface high-availability を使用して管理します。

構文

store network interface ip <ip address>

表示コマンド

show network interface ip

store network interface ip6

Guardium アプライアンスの 1 次 IP V6 アドレスを設定します。ネットワーク・インターフェースの IP アドレスを変更する際には、そのサブネット・マスクも変更しなければならない場合があります。 store network interface mask を参照してください。2 次 IP アドレスの作成および管理を行うには、store network interface secondary を参照してください。 結合/フェイルオーバーは、CLI コマンド store network interface high-availability を使用して管理します。

構文

store network interface ip6 <ip address>

表示コマンド

show network interface ip6

store network interface map

ethn で識別されたイーサネット・ポートを MAC アドレス mac にマップします。

構文

store network interface map <ethn> <mac>

store network interface mask

1 次 IP アドレスのサブネット・マスクを設定します。ネットワーク・インターフェース・マスクを変更する際には、その IP アドレスも変更しなければならない場合があります。store network interface ip を参照してください。2 次 IP アドレスのサブネット・マスクは、「セットアップ」 > 「ツールとビュー」 > 「システム」からしか割り当てることができないので、注意してください。

構文

store network interface mask <ip mask>

store network interface mtu

この CLI コマンドは、MTU (最大転送単位) を設定するときに使用します。

```
CLI> store network interface mtu
Usage: store network interface mtu <interface> <mtu>]
       where <interface> is the interface name,
       that is one of ( eth0 )
       and <mtu> is number between 1000 and 9000.
```

表示コマンド

show network interface mtu

eth0 1500

show network interface port

このコマンドを使用して、アプライアンスの背面にある物理コネクターを見つけます。 *show network interface inventory* コマンドを使用してすべてのポート名を表示したら、以下のコマンドを使用して、「n」で指定される物理ポートのランプを 20 回明滅させます (「n」は、eth0、eth1、eth2、eth3 などのように、eth の後に続く数字です)。

構文

show network interface port <n>

例

CLI> show network interface port 1

ポート eth1 のオレンジ色のライトが 20 回明滅します。

store network interface remap

この CLI コマンドは、 NIC を再マップするときに使用します。

構文

store network interface remap

store network interface reset

この CLI コマンドは、 既存の OS ネットワーク構成を消去し、 保存されていた Guardium ネットワーク設定を再適用するときに使用します。

構文

```
CLI> store network interface reset
WARNING: This command will reset the network configuration to the stored Guardium network settings.
Are you SURE you want to continue? (y/n)
```

store network interface secondary

このコマンドは、1 次管理インターフェースとは異なる IP アドレス、ネットワーク・マスク、およびゲートウェイを持つ 2 次管理インターフェースとして Guardium システム上のポートを構成する場合に使用します。

注: IP のチーミングと 2 次インターフェースは、同時に実行できません。
構文:

```
store network interface secondary [on <NIC> <ip> <mask> <gateway> | off ]
```

表示コマンド

show network interface secondary

store network interface speed

このコマンドは、Guardium ポートが接続されているスイッチ上でオートネゴシエーションが使用できない場合にのみ使用します。 このコマンドは ethn という名前のポートの速度設定を構成します。 show network interface inventory コマンドを使用して、すべてのポート名を表示します。

構文

store network interface speed <ethn> <10 | 100 | 1000>

表示コマンド

show network interface speed <ethn>

show network arp-table

アドレス解決プロトコル (ARP) 表を表示します。これは操作可能なシステム値です。 このコマンドはサポート目的としてのみ提供されています。

構文

show network arp-table

例

CLI> sho net arp

IP address HW type Flags HW address Mask Device

192.168.3.1 0x1 0x2 00:0E:D7:98:07:7F * nic1

192.168.3.20 0x1 0x2 00:C0:9F:40:33:30 * nic1

ok

CLI>

show network macs

MAC アドレスのリストを表示します (show network interface inventory コマンドと同様)。

構文

show network macs

例

Network card configuration:

Device | Mac Address | Member of

eth0 | 00:50:56:3b:c3:73 |

eth1 | 00:50:56:8a:0d:fa |

eth2 | 00:50:56:8a:0d:fb |

eth3 | 00:50:56:8a:00:c1 |

注: 「Member of」は、結合が存在する場合に、どの NIC が結合ペアであるかを示します。

ok

store network interface ip6

使用法: store network interface ip <ip> (IP は有効な IP6 アドレス)。

store network resolver

Guardium アプライアンスが使用する第 1、第 2、および第 3 DNS サーバーの IP アドレスを設定します。 それぞれのリゾルバー・アドレスは固有でなければなりません。 DNS サーバーを削除するには、IP アドレスの代わりに null を入力します。

構文

store network resolver <1 | 2 | 3> <ip address | null>

表示コマンド

show network resolver <1 | 2 | 3>

store network routes defaultroute

デフォルト・ルーターの IP アドレスを、指定した値に設定します。

構文

store network routes defaultroute <ip address>

表示コマンド

show network routes defaultroute

store network routes static

ユーザーに対し、所有する IP アドレスが 1 アプライアンスにつき 1 つだけ (eth0 を通じて) であっても、静的ルーティング表を使用することにより、異なるルーターからの直接トラフィックを許可します。 静的ルーティング表に行を追加します。

構文

store network routes static

表示コマンド

現在の静的ルートと ID (デバイス、インデックス、アドレス、ネットマスク、ゲートウェイ) をリストします。

show network routes static

削除コマンド

delete network routes static

store system domain

システム・ドメイン・ネームを指定値に設定します。

構文

store system domain <値>

表示コマンド

show system domain

store system hostname

システムのホスト名を指定値に設定します。

構文

store system hostname <値>

表示コマンド

show system hostname

親トピック: CLI の概要

サポート CLI コマンド

以下の CLI コマンドは、技術サポートから指示された場合にのみ使用します。

技術サポートがマシンの状況を分析し、一般的な問題のトラブルシューティングと修正を行ううえで、これらのコマンドは役立ちます。定期的にこれらのコマンドを使って何らかの機能を実行する必要はありません。

support clean audit_results

監査結果を手動でパージします。このコマンドは本当に必要な場合にのみ使用してください (監査タスクで非常に多数のレコードが生成され、過大なディスク・スペースを占有する場合)。

このコマンドを実行する前に技術サポートに相談することを強くお勧めします。

このコマンドの実行時には警告メッセージが表示され、確認手順が必要になります。

このコマンドは、監査プロセスとタスクについての情報をリストします。

最も大きい結果セットから最も小さい結果セットの順番で、特定の行数が示されます。レポート結果の数は、入力値以上になります。

次に、レポートが表示された後、ユーザーは行番号を 1 つ選んで、その行番号に対応する監査プロセスの結果をパージできます。このように行番号を選択すると、選択されたプロセス名の監査データが削除されます。

構文

support clean audit_results <rows>

入力パラメーター

rows - 表示する行数 (整数)。 デフォルトは 10 です。

注: 監査タスクが非常に多いシステムでは、このコマンドの完了に時間がかかることがあります。

support clean log_files

この CLI コマンドは、指定されたファイルを削除します (その前にユーザーに削除の確認を求めます)。ファイルが見つからない場合、/var/log 内の 10MB より大きいファイルがリストされ、このリストからユーザーは大きなファイルを削除できます。警告メッセージが表示され、確認手順が含まれます。

構文

support clean log_file <filename> >> filename を追加

support clean DAM_data

データベース・アクティビティー・モニター・データを手動でパージします。このコマンドは本当に必要な場合にのみ使用してください。

このコマンドを実行する前に技術サポートに相談することを強くお勧めします。

このコマンドでは警告メッセージが表示され、確認手順が含まれます。

構文

support clean DAM_data <purge_type> <start_date> <end_date>

入力パラメーター

purge_type オプション: agg, exceptions, full_details, msgs, constructs, access, policy_violations, parser_errors, flat_log

start_date: YYYY-mm-dd

end_date: YYYY-mm-dd

support clean centera_files

Centera 内に保管された Guardium のアーカイブ/バックアップには、Guardium によって削除日マーカーが付加されています。ただし、削除処理を呼び出すための後続機能はありません。Centera は、独自のファイルを保守するための GUI を持っていないため、クライアント・アプリケーションからの API 呼び出しに依存します。

この CLI コマンド support clean centera_files を使用して、Centera 内のマークが付けられたファイルを削除してください。

support clean InnoDB-dumps

この CLI コマンドを使用して、InnoDB 表をパージします。

これはパスワードで保護されたコマンドです (技術サポートの場合のみ)。

support clean hosts

使用法: support clean hosts <IP address> <fully qualified domain name>

support clean servlets

jsp.java ファイルおよび *jsp*.class ファイルを削除し、GUI を再始動します。

この CLI コマンドは、生成された Java™ サーブレットとそのクラスを削除するために使用します。

support execute

このユーティリティーは、直接リモート・アクセスが使用できないか許可されていない場合に、Guardium 拡張サポートがリモート診断およびリモート・サポートを行えるように設計されています。

Support Execute は、直接リモート接続に代わるものではありませんが、Guardium サポートが直接アクセスを使用せずに少なくともある程度のルート・アクセスをセキュアな方法で実行できるようにします。

Guardium 拡張サポートから提供されるコマンドには、SQL ステートメント、O/S コマンド、シェル・スクリプト、SQL スクリプトがあります。これらのコマンドは、セキュア・キーとともにお客様に提供され、CLI を使用したコマンドの実行が可能になります。セキュア・キーは、お客様と Guardium サポートが取り組んでいるシステムに結び付けられます。このキーは、他のすべてのシステムでは無効です。このコマンドは、Guardium サポートによって許可された特定の回数のみ実行でき、同意日から 7 日間のみ有効です。

この機能は、デフォルトで無効になっています。通常モードとリカバリー・モードの両方で CLI コマンドを使用して有効にするには、以下を実行します。

support execute [enable | disable]

Guardium 拡張サポート・チームがセキュア・キーを生成できるようにするために、該当のシステムの MAC アドレスを eth0 に対して指定する必要があります。インターフェースおよび MAC アドレスの例を以下に示します。

お客様の使用 / CLI でログイン

support execute <CMD String> <PMR #> <KEY>

Guardium 拡張サポートから提供される主要な実行コマンド

support execute showlog [<Secure Key>|main|files]

使用ログを表示

#「<Secure Key>」: 単一エントリーの完全な詳細を表示

#「main」: 主要な実行ログを表示

「files」: ログのディレクトリー・リストを表示

support execute mac

セキュア・キーを生成するためにサポートが必要とする Eth0 MAC アドレス

support execute info

eth0 MAC アドレス、ルート・パス・キー、およびその他のシステム情報を表示

support execute version

#「Support Execute」の内部 2 進コード・バージョンを表示

support execute help

ユーティリティー情報のヘルプの詳細および目的

Guardium 拡張サポートから提供されるコマンドの例を以下に示します。

support execute "select * from GDM_ACCESS%5CG" 11111,111,111 6254130c0f0c3c504b33687c57f41363e4c00

support reset-password accessmgr

このコマンドは accessmgr アカウントのパスワードをリセットします。

構文

support reset-password accessmgr 10000000-99999999|random

パラメーター

新規パスワードを生成するために使われる 8 桁のキー番号。このキー番号を記録して技術サポートに提示すると、新しい accessmgr アカウント・パスワードを受け取ることができます。random を選択すると 8 桁の乱数が生成されます。

注: accessmgr アカウントの E メールが設定済みの場合、システムはそこに通知を送信しようとします。

support reset-password root

このコマンドは IBM® Guardium® アプライアンス上のルート・パスワードをリセットします。

構文

support reset-password root 10000000-99999999|random

パラメーター

新規パスワードを生成するために使われる 8 桁のキー番号。このキー番号を記録して技術サポートに提示してください。random を選択すると 8 桁の乱数が生成されます。

また、このコマンドを実行するとき、ユーザーはルート・パスワードを変更するために秘密のキーワードを提供する必要があります。ルート・パスワードを変更する必要がある場合には、技術サポートに連絡してください。

注: ビジネス・ルールに従って本当に必要な場合を除き、ルート・パスワードをリセットしないでください。

support schedule find_crashed_tables

この CLI コマンド、support schedule find_crashed_tables [ON/OFF] は、find_crashed_tables.sh スクリプトの日次の cron ジョブを有効または無効にするために使用します。
使用法: support schedule find_crash_tables on ALL|db
support schedule find_crash_tables off
このコマンドは、find_crashed_tables スクリプトの日次スケジュールを有効または無効にします。
注: 入力するデータベースに特に注意してください。ユーザーは、破損した表の 5 つの有効なデータベースすべてを処理するために「ALL」を入力するか、または「TURBINE」、「GDMS」、「CUSTOM」、「DATAMART」、「DIST_INT」の 5 つの有効なデータベースのいずれか 1 つを入力することができます。

support show db-processlist

このコマンドはすべての db プロセスを (実行時間でソートして) リストします。

構文

support show db-processlist all

support show db-processlist locked

support show db-processlist running

support show db-process full

パラメーター:

support show db-processlist [ ]

Where

running は、実行中のすべての sql ステートメントを表示するオプションです

all は、スリープ状態のプロセスも含めるオプションです

locked はロックされているすべてのプロセスと、最も古い 1 つのプロセスを表示します

full [任意指定] は、sql 照会を拡張形式で表示します

support show db-struct-check

このコマンドは、統合プロセスで見つかった構造の違いをすべて表示します。

構文

support show db-struct-check

support show db-top-tables

このコマンドは、サイズの大きい順にソートした上位 20 個のデータベース表をリストします。また、80% を超える空き領域を使用している表については、空き表スペースの使用量 (パーセント単位) でソートして表をリストします。表名によるフィルター処理が可能です。表のサイズはすべて MB で表示され、空き領域の使用量はパーセントで表示されます。

構文

support show db-top-tables all

support show db-top-tables like

パラメーター

support show db-top-tables all

DB 全体の中から、サイズの大きい表をソートしてリストします

support show db-top-tables like

サイズの大きい表で、表名の任意の部分が基準に一致するものをリストします

support show db-status

このコマンドはデータベースの使用状況を表示します。

free (空き)、used (使用)、メガバイト、パーセントを選択できます。

構文

support show db-status free %

support show db-status used %

support show db-status free m

support show db-status used m

support show hardware-info

このコマンドは、ハードウェア情報を収集し、収集された情報を取り出せるようにディレクトリー内に入れるスクリプトを使用します。

この CLI コマンドの実行後に、以下のメッセージが表示されます。

Collected HW Info as /var/log/guard/Gather_hw_info-2012-06-25-17-43.tgz

その後 CLI コマンド fileserver を実行して、サーバーからこの .tar ファイルを取り出します。

support show iptables

このコマンドはシステム iptables コマンドの出力を表示します。

構文

support show iptables diff

support show iptables list

パラメーター

[diff | list] パラメーターは、通常の iptables 出力表示、または違い/差分だけの表示 (diff) のどちらにするかを制御します

[accept | full] パラメーターは、出力をフィルターに掛けて受け入れる行だけにするか、あるいはフィルターなしでリストします

support show large_files

このコマンドは、/var /tmp /root の各フォルダー内にある、特定の MB より大きく、特定の日数より古いファイルをすべてリストします。

使用法

support show large_files

このコマンドは、/var /tmp /root の各フォルダー内にある、特定の MB より大きく、特定の日数より古いファイルをすべてリストします

入力パラメーター:

* size - 10 より大きい整数 (MB)

* age - ゼロ以上の整数 (日数)

構文:

support show large_files <size> <age>

パラメーター

support show large_files

<size> は表示するファイルの最小サイズです (デフォルトは 100M)

<age> は最後に変更された日以降の日数です

support show netstat

このコマンドはシステム netstat コマンドの出力を表示します。grep パラメーターを使用して、内容に応じて出力をフィルターに掛けることができます。

構文

support show netstat all

support show netstat grep

パラメーター

support show netstat grep

検索対象となる英数字文字列

support show netstat all

support show port open

このコマンドは、telnet を使用して、開いている TCP ポートをローカルで、またはリモート・ホストで検出するのと似ています。

正常に接続できた場合、「Connection to 127.0.0.1 8443 port [tcp/*] succeeded!」のようなメッセージが表示されます。

接続できなかった場合、「connect to 127.0.0.1 port 1 (tcp) failed: Connection refused」のようなメッセージが表示されます。

構文: support show port open

IP port - IP は、127.0.0.1 のような、有効な IPv4 アドレスでなければなりません。

port は、1 から 65535 までの値の整数でなければなりません。

support show top

このコマンドは、システム top コマンドの出力を CPU、メモリー、または実行時間でソートして表示します。構成可能な反復回数 (デフォルトは 1)、表示する行数 (デフォルトは 10) を指定できます。

構文

support show top [cpu | memory | time]

パラメーター

support show top cpu

N は 1 から 10 までの範囲の反復回数、R は表示する行数 (少なくとも 10) です

support show top memory

N は 1 から 10 までの範囲の反復回数、R は表示する行数 (少なくとも 10) です

support show top time

N は 1 から 10 までの範囲の反復回数、R は表示する行数 (少なくとも 10) です

support check tables [DB name] [table name}

表に対して mysqlcheck –c コマンド (表にエラーがないか検査する) を呼び出します。

パラメーターを 1 つも指定しない場合、このコマンドは各検査のタイムアウトを 3 分として TURBINE データベース内のすべての表を検査します。各検査は並行して実行されるため、全体の時間は変動します。コマンドの進行状況がパーセント単位で表示されます。検査の実行時間が 3 分を超えると強制終了されます。タイムアウトによって検査が強制終了された表は、コマンドの完了後に画面上にすべてリストされます。コマンドの処理中に発生したエラーは、ログ・ファイル /var/log/guard/<dbname>_check_tables/errors.<date>.log に報告されます。<date> は現在の日付で、<dbname> はデータベースの名前です。

各表の検査処理で検出されたエラーは、/var/log/guard/<dbname>_check_tables/check_table_child.<tablename>.<date>.log ファイルに報告されます。<date> は現在の日付、<dbname> はデータベースの名前、<tablename> は検査された表の名前です。正常な表のファイルは作成されません。 1 番目のパラメーターとして dbname を指定した場合、このコマンドは指定されたデータベース内のすべての表を同じタイムアウト設定 (3 分) で検査します。パラメーターを 1 つも指定しない場合、TURBINE の表をすべて検査します。

パラメーターとして dbname と tablename を指定した場合、このコマンドは指定されたデータベース内にある指定された表を、タイムアウトなしで検査処理が完了するまで検査します。この方法により、3 分以内に検査が完了しなかった表を手動で検査することができます。パーセント記号 (%) を使用して、tablename パラメーター内でマスクを使用できます。

support shrink innodb-size

この CLI コマンドは、ibdata1 ファイルのサイズを小さくするために使用します。

ここでは、以下のステップが実行されます。

- すべての InnoDB 表をダンプします
- mysql を停止します
- ibdata1、ib_logfile0、ib_logfile1 の各ファイルを削除します
- mysql を開始します
- ダンプした表を復元します

これはパスワードで保護されたコマンドです (技術サポートの場合のみ)。

support show innodb-status

この CLI コマンドは、MySQL の問題をトラブルシューティングする場合に使用します。この CLI コマンドを使用して、実行時に MySQL 表で行われている処理を確認します。 この CLI コマンドを使用して、MySQL 表での検査時間が長い原因は、レコードのロックか表のロックかを判別します。

```
support show innodb-status
```

0 queries inside InnoDB, 0 queries in queue

0 read views open inside InnoDB

Main thread process no. 7959, id 139923805550336, state: sleeping Number of rows inserted 6894, updated 6934, deleted 93, read 24787 0.33 inserts/s, 0.00 updates/s, 0.00 deletes/s, 0.67 reads/s

---

END OF INNODB MONITOR OUTPUT

support analyze static-table

この CLI コマンドは、最大のグループに基づいて値の長さおよび値の出現回数によって静的表をソートすることで、静的表の内容を分析するために使用します。

support must_gather commands

任意の Guardium システムの状態に関する特定の情報を生成する、ユーザー CLI で実行できる単純な must_gather コマンドがいくつかあります。PMR (問題管理レコード) が記録されているときであればいつでも、この情報をアプライアンスからアップロードでき、Guardium 技術サポートに送信できます。

これらのコマンドを実行するには、適切な must_gather パッチがインストールされている必要があります。

正しいパッチをインストールした後は、いつでも以下の手順に従ってユーザー CLI で must_gather コマンドを実行できます。

1. 問題となっている Guardium システムに対する Putty セッション (または同様のセッション) を開きます。
2. ユーザー CLI でログインします。
3. 発生している問題のタイプに応じて、関連する must_gather コマンドを CLI プロンプトに貼り付けます。問題を診断するために、複数の must_gather コマンドが必要な場合があります。

   support must_gather system_db_info

   support must_gather purge_issues

   support must_gather audit_issues

   support must_gather agg_issues

   support must_gather cm_issues

   support must_gather alert_issues

   support must_gather patch_install_issues

   以下は、実行の完了までに数分かかる場合があります。

   support must_gather miss_dbuser_prog_issues

   support must_gather sniffer_issues

   以下のコマンドの場合、問題を再現している間にデバッガーを実行する時間の長さ (分) を入力するように求められます。

   support must_gather backup_issues

   support must_gather scheduler_issues

   出力は、must_gather ディレクトリーに、例えば must_gather/system_logs/.tgz のようなファイル名で書き込まれます。
4. 結果の出力を IBM サポートに送信してください。

ファイル・サーバーを使用すると、tgz ファイルをアップロードして、サポートに送信できます。

E メールで送信するか、ECUREP にアップロード (例えば、PMR 番号とアップロードするファイルを指定してファイル標準データ・アップロードを使用) します。

Guardium for z/OS トラフィック診断コマンド

support store zdiag on [N]

オプションの N は、診断を実行する時間 (分) です (10 から 600。デフォルトは 60)。

Guardium for z/OS トラフィック診断をオンにします。これには、TCPDUMP と SLON の収集が含まれます。この収集は、対応するファイルのサイズが 2 GB に達すると停止します。処理が完了したら、fileserver コマンドを使用して、結果ファイルの tcpdump.tar.gz と slon_all.tar.gz を検索することができます。/var パーティションには、15 GB 以上の空き領域が必要です。

support store zdiag off

Guardium for z/OS トラフィック診断をオフにします。CLI コマンド fileserver を使用して、結果のファイル tcpdump.tar.gz および slon_all.tar.gz をダウンロードできます。

support show zdiag

Guardium for z/OS トラフィック診断の状況を表示します。

SLON 収集コマンド

support store slon on [parameter]

スニファーによってデバッグ用に取得されたパケットを収集する SLON ユーティリティーをオンにします。結果ファイルの slon_packets.tar.gz、slon_messages.tar.gz、slon_all.tar.gz は、fileserver コマンドを使用して検索することができます。/var パーティションには、15 GB 以上の空き領域が必要です。

オプション・パラメーターは、次のとおりです。

packets: アナライザー・パケットをダンプします (デフォルト)。

snifsql: スニファーの SQL アクティビティーをログに記録し、アナライザー・パケットをダンプします。

secparams: セキュア・パラメーター情報をログに記録し、アナライザー・パケットをダンプします。

sgate: S-GATE デバッグ情報をログに記録し、アナライザー・パケットをダンプします。

messages: メッセージ・データ・ダンプをタップします。

support store slon off [parameter]

SLON ユーティリティーをオフにします。結果ファイルの slon_packets.tar.gz、slon_messages.tar.gz、slon_all.tar.gz は、fileserver コマンドを使用して検索することができます。

オプション・パラメーターは、次のとおりです。

packets: パケットのダンプを停止し、セキュア・パラメーター、S-GATE デバッグ情報、スニファーの SQL アクティビティーのロギングを停止します (デフォルト)。

messages: メッセージ・データ・ダンプのタップを停止します。

all: すべてのアクティビティーを停止します。

support show slon

SLON ユーティリティーの状況を表示します。

TCPDUMP 収集コマンド

support store snif_memory_max
使用法: support snif_memory_max <num> (num は数値 | 33 | 50 | 75 |)
このコマンドは、64 ビット・システムにのみ適用されます。
表示コマンド
support show snif_memory_max

support store tcpdump on <type> <period> <loglimit> [interface] [IP] [port] [protocol]

support store tcpdump on <type> <period> <loglimit> [interface] [IP] [port] [protocol]

TCPDUMP ユーティリティーをオンにします。指定された期間が経過すると、fileserver コマンドを使用して結果ファイル tcpdump.tar.gz を検索することができます。/var パーティションには、15 GB 以上の空き領域が必要です。

各部の意味は次のとおりです。

<type> - ダンプのタイプ。「headers」(収集されたヘッダーのみ) または「raw」(収集されたパケット全体) のいずれかです。

<period> - ダンプ期間 NUMBER[SUFFIX]。オプションの SUFFIX は、秒の場合は「s」、分の場合は「m」(デフォルト) です。

<loglimit> - ダンプ・ログ・ファイルのサイズ制限。値の範囲は 1 から 6 ギガバイトです。

オプションのフィルター引数は以下のとおりです。

[interface] - ネットワーク・インターフェース名 (デフォルトは eth0)

[IP] - IP アドレス

[port] - ポート

[protocol] - プロトコル。「tcp」、「udp」、「ip」、「ip6」、「arp」、「rarp」、「icmp」、「icmp6」のいずれかです。

例

support store tcpdump on headers 10m 1

このコマンドでは、10 分間のパケット・ヘッダーを 1GB のログ・ファイルのサイズ制限で保存する TCPDUMP が実行されます。

support show tcpdump

TCPDUMP ユーティリティーの状況を表示します。

support store tcpdump off

TCPDUMP ユーティリティーをオフにします。停止後、fileserver コマンドを使用して結果ファイル tcpdump.tar.gz を検索することができます。

support must_gather datamining_issues

異常値、クイック検索、およびデータマート機能に必要な診断情報を収集します。情報には、対応する内部表のダンプ、必要なログ、対応するプロセスの状態、および標準 must_gather 診断 (一般的なシステムおよび内部データベースの情報) が含まれます。

support must_gather network_issues [--host=<HOST>] (オプション・パラメーター <HOST> は、ホスト名または IP アドレス)

このコマンドは、アプライアンスからすべてのネットワーク情報を収集し、ping、traceroute、対応するポートのプローブ、その他の手段によって Guardium が対話するホストに対してポーリングします。オプション・パラメーターを指定した場合、指定されたホストに対してのみポーリングします (Guardium が当該ホストに対していずれかのアクティビティーを実行するように構成されている場合)。

store antlr3_max

この CLI コマンドは、パーサーとロガーの間のデータ・フローの制御を支援するために使用します。CLI コマンド store antlr3_max は、熟練したユーザーおよびカスタマー・サポートを対象とした拡張パラメーターであり、Oracle、Db2、MySql、および MSSql 用のスニファーのパーサー・コンポーネントとロガー・コンポーネントの間のデータ・フローの制御を支援します。

この値 (デフォルトは 20,000) により、ロガーがキューに入れることができる同時解析 SQL ステートメントの数が変更されます。

これが改善に役立つ可能性がある問題は、スニファーがメモリー不足で再始動する問題や、スニファーがメモリーを十分に使用していない問題です。

スニファーがメモリー不足で再始動することに気付いた場合は、コンテキストの上限を下げると、この問題を軽減するのに役立ちます。あるいは、スニファーが、使用可能なシステム・メモリーを十分に使用していない場合は、コンテキストの上限を上げると、メモリーをさらに使用できるようにすることができます。

store active_parser_engine
この CLI コマンドは、スニファーによって使用されるパーサー・エンジンを制御するために使用されます。この CLI コマンドは、ANTLR3 パーサー (Oracle、Db2、MS SQL、MySQL) によってサポートされるデータベース・タイプにのみ適用されます。
使用法: store active_parser_engine <num>
ここで、<num> は以下のいずれかです。
1: ANTLR2 によって ANTLR3 パーサー・エラーが再解析される (デフォルト)
2: ANTLR2 のみ
3: ANTLR3 のみ
表示コマンド
show active_parser_engine

親トピック: CLI の概要

システム CLI コマンド

これらの CLI コマンドは、システム設定の構成に使用します。

store system apc

このコマンドを使用すると、UPS 接続時の自動パワーダウン・オプションを構成できます。USB コネクターに UPS を接続する必要があることに注意してください (UPS のシリアル接続はサポートされていません)。

パワーダウンするまでの最小充電パーセント (0 から 100)、またはパワーダウン前にバッテリー電力で稼働する秒数を設定します。デフォルトはそれぞれ 25、ゼロです。

さらに、apc プロセスを開始/停止するコマンドもあります。デフォルトでは apc プロセスが無効になっています。

構文

store system apc [battery-level <パーセント> | timeout <秒数>]

store system apc start

store system apc stop

表示コマンド

show system apc [battery-level | timeout]

store system auditlog-passthrough

このコマンドは、auditd サービスからローカルの syslog へのシステム監査ログ・データのパススルーを有効または無効にするために使用します。システム監査ログは詳細であるため、auditlog-passthrough 機能はリモート・ロギングと組み合わせて使用するのが最適です。リモート・ロギングについて詳しくは、構成および制御 CLI コマンドを参照してください。

auditlog-passthrough 機能は、デフォルトでは無効になっています。

構文: store system auditlog-passthrough [on | off]

例:

```
> store sys aud on
Restarting auditd service to pick up the change.
Reloading configuration: [ OK ]
Auditd to syslog passthrough is enabled.
ok
```

表示コマンド: show system auditlog-passthrough

store system banner

store system banner [message | clear]

CLI ログイン時のバナー (無許可アクセスなどに関する警告、またはウェルカム・メッセージ) を作成するには、CLI コマンド store system banner [message | clear] を使用します。

構文

store system banner clear - この CLI コマンドを使用して、既存バナー・メッセージを削除します。

store system banner message - この CLI コマンドを使用して、バナー・メッセージを作成します。バナー・メッセージを入力して、CTRL-D を押してください。

表示コマンド

show system banner - この CLI コマンドを使用して、既存のバナー・メッセージを表示します。

store system clock datetime

システム・クロックの日時を、指定された値に設定します。**YYYY** は年、**mm** は月、**dd** は日、**hh** は時間 (24 時間形式)、**mm** は分、**ss** は秒です。秒の部分は必須ですが、常に 00 に設定されます。

構文

store system clock datetime YYYY-mm-dd hh:mm:ss>

表示コマンド

show system clock <all |datetime |timezone>

例

store system clock datetime 2008-10-03 12:24:00

store system clock timezone

使用可能なタイム・ゾーン値をリストします (list オプション)。または、このシステムのタイム・ゾーンを、指定されたタイム・ゾーンに設定します。まず list オプションを使ってすべてのタイム・ゾーンを表示した後、リストから適切なタイム・ゾーンを選んで入力してください。

さらに、IBM® Guardium® では標準の監査証跡にローカル時間帯が記録されます。これにより、別のタイム・ゾーンで収集されたデータの中でデータが使われる (またはそのようなデータと共にデータが統合される) 場合に対処できます。

注: 夏時間が始まっても、タイム・ゾーン設定は自動的に更新されません。マシンを更新するには、ユーザーはタイム・ゾーンをリセットする必要があります。タイム・ゾーンのリセットとは、現在と異なる新しいタイム・ゾーンを設定した後、正しいタイム・ゾーンにリセットすることです。同じタイム・ゾーンにリセットするだけでは効果がなく、「No change for the timezone」というメッセージが出されます。

構文

store system clock timezone <list | timezone>

表示コマンド

show system clock <all | timezone | datetime>

例

まず **list** オプションを指定してコマンドを使用し、すべてのタイム・ゾーンを表示します。その後、適切なゾーンを使ってコマンドを再び入力します。

CLI> store system clock timezone list

Timezone: Description:

--------- -----------

Africa/Abidjan:

Africa/Accra:

Africa/Addis_Ababa:

...

...output deleted

...

CLI> store system clock timezone America/New_York

store system conntrack

Linux カーネルの接続トラッキング・サブシステムの現在の状況を設定します。状況は ON|OFF のいずれかです。

構文

store system conntrack ON|OFF

表示コマンド

show system conntrack

store system cpu profile

CPU スケーリングをサポートするハードウェアにおいて、CLI コマンドにより、CPU スケーリングの構成を許可します。

この CLI コマンドを使用して、必要に応じた適切な CPU スケーリング・ポリシーを設定します。

- 控えめ = 低い電力使用量、控えめなスケーリング
- 平衡 = 中程度の電力使用量、迅速な拡大
- パフォーマンス = 最大クロック速度での CPU の実行

Guardium ソフトウェアでは、インストール時にスケーリング・ポリシーは「パフォーマンス」に設定されます。

構文

store system cpu profile [min|perf|max]

表示コマンド

show system cpu profile

store system custom_db_size

この CLI コマンドは、カスタム・データベース表の最大サイズ (MB 単位) を設定するときに使用します。デフォルト値は 4000 MB です。

構文

```
CLI> store system custom_db_max_size
USAGE: store system custom_db_max_size <N>
       where N is number larger than 4000.
```

表示コマンド

show system custom_db_size

store system domain

システム・ドメイン・ネームを指定値に設定します。

構文

store system domain <値>

表示コマンド

show system domain

store system hostname

システムのホスト名を指定値に設定します。

構文

store system hostname <値>

表示コマンド

show system hostname

store system issue

store system issue [message | clear]

CLI コマンド store system issue message は Ctrl-d までコンソールから入力を受け取り、入力の中の $、¥、￥ の後の 1 文字、および ` 文字をすべて除去した後、それを /etc/motd に書き込みます。これは、このシステムをカスタマーのセキュリティー・ポリシーに準拠させるメッセージを入力する方法の 1 つです。

CLI コマンド store system issue clear は /etc/motd をデフォルト・バージョンに復元します。

バージョンは、/etc/guardium-release から取得されます。 例えば、SG70 -> 7.0、SG80 -> 8.0 です。/etc/guard-release の中に SG が見つからない場合、デフォルト・バージョンは空文字列です。

store system netfilter-buffer-size

netfilter バッファーのサイズを設定します。

構文

store system netfilter-buffer-size

表示コマンド

S-TAP® netfilter バッファー・サイズを表示します。デフォルトは 65536 です。

show system netfilter-buffer-size

show system ntp diagnostics

この CLI コマンドは、ntpq -p および ntptime を実行し、 その出力を直接画面に送信するときに使用します。Guardium システムは、UDP を介してローカル・ホストから NTPD を 照会します。

構文

show system ntp diagnostics

例

```
CLI> show system ntp diagnostics
Output from ntpq -p :
localhost.localdomain:
-------------------------------------------------------------------------
Output from ntptime :
(Note that if you have just started the ntp server, it may report an 'ERROR' until it has synchronized.)
-------------------------------------------------------------------------
ntp_gettime() returns code 5 (ERROR)
  time d3443c21.47a46000  Thu, Apr 26 2012 17:26:57.279, (.279852),
  maximum error 16384000 us, estimated error 16384000 us
ntp_adjtime() returns code 5 (ERROR)
  modes 0x0 (),
  offset 0.000 us, frequency 0.000 ppm, interval 1 s,
  maximum error 16384000 us, estimated error 16384000 us,
  status 0x40 (UNSYNC),
  time constant 2, precision 1.000 us, tolerance 512 ppm,
```

store system ntp [all | server | state]

store system ntp server

最大で 3 つの NTP (Network Time Protocol) サーバーから成る**ホスト名**を設定します。なお、NTP サーバーの使用を有効にするには、**store system ntp state on** コマンドを使用する必要があります。1 つの NTP サーバーを定義するには、そのホスト名または IP アドレスを入力します。複数の NTP サーバーを定義するには、引数なしでコマンドを入力し、NTP サーバーのホスト名を指定するプロンプトを表示させます。

構文

store system ntp server

使用法: store system ntp server

サーバーごとに IP またはホスト名のいずれかを入力します。

ストアする NTP サーバーを最大 3 つ入力します。

表示コマンド

show system ntp <all |server>

削除コマンド

delete ntp-server

store system ntp state

NTP (Network Time Protocol) サーバーの使用を有効または無効にします。

構文

store system ntp state <on | off>

表示コマンド

show system ntp <all |state>

store system patch install

1 つのパッチ、または複数のパッチをバックグラウンド・プロセスとしてインストールします。**ftp** および **scp** オプションは、圧縮されたパッチ・ファイルをネットワーク上のロケーションから IBM Guardium アプライアンスにコピーします。圧縮された 1 つのパッチ・ファイルに複数のパッチが含まれることがありますが、一度にインストールできるパッチは 1 つだけであることに注意してください。複数のパッチをインストールするには、インストールする必要があるすべてのパッチをコンマで区切って選択します。CLI は内部的に、リストの各パッチに関する要求を (ユーザーによって指定された順序で) 実行依頼しますが、その際、最初のパッチはユーザーによって指定された要求時間に行われ、後続の各パッチは前のパッチの 3 分後になります。さらに CLI は、指定された (1 つまたは複数の) パッチが既に要求されているかどうか確認し、重複要求を許可しません。

最後のオプション (sys) は、以前にこのコマンドを使って IBM Guardium アプライアンスに既にコピーされた圧縮ファイルに含まれる、2 番目 (またはそれ以降) のいずれかのパッチをインストールするときに使用します。

適用済みのパッチの全リストを表示するには、「管理」>「レポート」>「インストール管理」>「インストール済みのパッチ」、「管理」>「メンテナンス」>「一般」>「インストール済みのパッチ」、または「レポート」>「Guardium 運用レポート」>「インストール済みのパッチ」のいずれかで「インストール済みのパッチ」レポートを参照してください。

CLI コマンド **store system patch install** では、ユーザーはリストから複数のパッチを選択できます。

構文

store system patch install <type> <date> <time>

<type> はインストール・タイプ cd | ftp | scp | sys

<date> および <time> はパッチ・インストールの要求時間で、日付の形式は YYYY-mm-dd、時刻の形式は hh:mm:ss

日時が入力されない場合、または NOW が入力された場合、インストール要求時間は「今すぐ」です。

パラメーター

どのオプションを選択した場合も、適用対象のパッチを選択するようプロンプトが出されます。

Please choose one patch to apply (1-n,q to quit):

cd - パッチを CD からインストールするには、このコマンドを実行する前に IBM Guardium CD-ROM ドライブに CD を挿入してください。CD に含まれるパッチのリストが表示されます。

tp または **scp -** ネットワーク上の任意の場所にある圧縮パッチ・ファイルからパッチをインストールするには、**ftp** オプションまたは **scp** オプションを使用し、示されるプロンプトに応答します。 パッチのファイル名を含む絶対パス名を指定してください。

Host to import patch from:

User on hostname:

Full path to the patch, including name:

パスワード:

CLI コマンド store system patch install scp では、ユーザーはパッチ・ファイル名にワイルドカード * を使用できます。

圧縮パッチ・ファイルが IBM Guardium アプライアンスにコピーされ、ファイルに含まれるパッチのリストが表示されます。

sys - 以前の store system patch 実行により IBM Guardium アプライアンスに既にコピーされたパッチ・ファイルに含まれる、2 番目 (またはそれ以降) のいずれかのパッチを適用するには、このオプションを使用します。

store system patch install コマンドは、インストール後にパッチ・ファイルを IBM Guardium アプライアンスから削除しません。既存のパッチの上に同じパッチを再インストールすることが可能で、パッチ・ファイルを手元に残しておくとさまざまな問題の分析に役立つ可能性があるため、パッチ・ファイルを必ずしも削除する必要はありません。ただし、ユーザーは手操作で、または CLI コマンド diag を使ってパッチ・ファイルを削除できます (なお CLI コマンド diag は特定のユーザーやロールに制限されています)。

パッチ・インストール要求を削除するには、CLI コマンド delete scheduled-patch を使用します。

store system public key reset

CLI コマンド show system public key tomcat または show system public key cli を使用して SSH 公開鍵を生成した後、CLI コマンド store system public key reset を使用すると、SSH 鍵が削除されます。SSH 鍵が生成されなかった場合、この CLI コマンドは何も行いません。このコマンドは、削除前に確認を要求します。

構文

store system public key reset

store system remote-root-login

SSH (ルート・アクセス) を有効/無効にします。SSH つまりセキュア・シェルは、ネットワークで結ばれた 2 つのデバイス間でセキュア・チャネルを使ってデータ交換できるようにするネットワーク・プロトコルです。

構文

store system remote-root-login ON|OFF

表示コマンド

show system remote-root-login

store system serialtty

一部の環境では、シリアル TTY を使用できないため、正常に開始できません。これは、システム・ログに出力され、SIEM に転送される可能性があります。これは、接続を許可するためにデフォルトでは有効になっていますが、後で、システムでシリアル・コンソールを使用できないと判別された場合、無効にできます。

構文

store system serialtty <on, off>

表示コマンド

show system serialtty

システムでシリアル TTY が有効になっているかどうかを報告します。

次のいずれかを報告します。

このシステムではシリアル TTY コンソールが有効になっています。

このシステムではシリアル TTY コンソールが無効になっています。

store system scheduler

スケジューリングは、IBM Guardium アプリケーション内のタイミング・メカニズムによって管理されます。タイミング機能が中断した場合、この CLI コマンドで指定された再始動インターバル後に再始動します。

store system scheduler restart_interval [5 から 1440、または -1] を使用すると、5 分後から 1440 分後までの範囲でタイミング機能を再始動することができます。デフォルトは -1 で、タイミング再始動メカニズムがインストールされていないことを示します。

現在実行中のすべてのジョブが終了した後でスケジューラーを再始動するには、store system scheduler wait_for_shutdown [ON | OFF] を使用します。パラメーターは ON または OFF です。

構文

store system scheduler restart_interval [5 から 1440、または -1]

store system scheduler wait_for_shutdown [ON | OFF]

表示コマンド

show system scheduler

store system shared secret

システムの共有パスワード値を指定値に設定します。この鍵は、中央マネージャーおよび管理されるすべてのアプライアンスの間で同じでなければなりません。または、アグリゲーターとデータ統合対象のすべてのアプライアンスの間で同じでなければなりません。あるアプライアンスを中央マネージャーによる管理対象として登録した後、そのユニットの共有パスワードは使用されなくなります。(この値を変更してユニットを一元管理から「登録抹消」することはできません。)

aggregator OS ユーザーの動的パスワード

aggregator パスワードは、共有パスワードに連結される <現行パスワード> です (つまり、パスワード = <現行パスワード><共有パスワード>)

ユーザーは、コレクターの共有パスワードとアグリゲーターの共有パスワードがまったく同じであることを確認する必要があります。そうでない場合、コレクターからアグリゲーターへの SCP 転送が失敗します。(これは管理対象ユニットとアグリゲーター、コレクターとアグリゲーター、およびエクスポート設定画面での要件です。) 共有パスワードは、CLI、および管理コンソール・タブの「システム」ペインのどちらからでも設定可能です。

構文

store system shared secret <key>

store system snif-alerts-facility

このパラメーターを使用すると、ユーザーはスニフ生成アラートの機能を構成できます。 前もってスニフによって直接生成されたアラートはユーザー機能を使用しますが、間接アラートは (guard_sender ユーティリティーを介して) デーモン機能を使用します。

構文

store system snif-alerts-facility <facility>

使用法: store snif-alerts-facility <facility>

facility は、daemon ftp local0 local1 local2 local3 local4 local5 local6 local7 lpr user のいずれかです。

デフォルトの facility は daemon です。

表示コマンド

show system snif-alerts-facility

store system snif-buffers-reclaim

この CLI コマンドは、IBM Guardium 技術サービスから指示された場合にのみ使用してください。

新しい構成は、CLI コマンド restart inspection-core が実行された後で有効になります。

構文

store system snif-buffers-reclaim [ON | OFF]

表示コマンド

show system snif-buffers-reclaim

store system snif-thread-number

この CLI コマンドは、実行するスレッド数を指定する場合に使用します。

新しい構成は、CLI コマンド restart inspection-core が実行された後で有効になります。

構文

store system snif-thread-number [new | default]

表示コマンド

show system snif-thread-number

snif は、32 ビット・システムでは 6 スレッドで実行されています。

store system snmp contact

IBM Guardium アプライアンスの snmp contact (syscontact) の E メール・アドレスを保管します。デフォルトでは info@guardium.com です。

構文

store system snmp contact <email-address>

表示コマンド

show system snmp contact

store system snmp location

IBM Guardium アプライアンスの snmp システム・ロケーション (syslocation) を保管します。デフォルトでは Unknown です。

構文

store system snmp location <文字列>

表示コマンド

show system snmp location

store system snmp query community

IBM Guardium アプライアンスの snmp システム照会コミュニティーを保管します。デフォルトでは guardiumsnmp です。

構文

store system snmp query community <文字列>

表示コマンド

show system snmp query community

親トピック: CLI の概要

ユーザー・アカウント、パスワード、および認証 CLI コマンド

これらの CLI コマンドを使用して、ユーザー・アカウント、パスワードおよび認証を構成します。

set guiuser 認証

デフォルト CLI アカウント (guardcli1、... guardcli5) のうちの 1 つを使用して CLI 経由でログオンする場合、CLI コマンド set guiuser を実行した後でなければ、GuardAPI コマンドは作動しません。 GUI において制限されたロールしかないユーザーが、GuardAPI コマンドに無許可アクセスを行わないようにするために、この認証が必要です。

guardcli1 ... guardcli5 アカウントを使用するには、ローカル・パスワードの設定が必要です。CLI コマンド set guisuer を使用して guardcli1 ... guardcli5 アカウントをリセットしてから、下記の構文に示すように、ローカル・パスワードを追加します。

CLI コマンドの中には、guiuser のロールに依存するものがあります。例えば、grdapi create_user、grdapi set_user_roles、および grdapi update_user にアクセスするには、guiuser のロール (accessmgr ビューから新規ユーザーを作成するときにマークが付けられます) は accessmgr である必要があります。

構文

set guiuser <gui_user> password <password>

例

$ ssh guardcli1@a1.corp.com

IBM Security Guardium, Command Line Interface (CLI)

guardcli1@a1.corp.com's password:

Last login: Thu Nov 4 14:56:34 2012 from 123.a1.corp.com

==========

IBM Security Guardium

Unauthorized access is prohibited

==========

a1.corp.com> set guiuser johny_smith password 3wel9s887s

ok

a1.corp.com>

例

>grdapi create_user firstName=john lastName=smith

password=pASSW0rd confirmPassword=pASSW0rd email=jsmith@us.ibm.com

userName=john disabled=0

ID=20000

```
>grdapi set_user_roles userName="john"
roles="dba,diag,cas,user"
```

ID=20000

ロール (dba) が追加されました。

ロール (diag) の追加に失敗しました。 診断は、cli または admin のいずれかのロールを持つ必要があります。

ロール (cas) が追加されました。

ロール (user) が追加されました。

```
> grdapi set_user_roles userName="john"
roles="dba,diag,cas,user,cli"
```

ID=20000

ロール (dba) が追加されました。

ロール (diag) が追加されました。

ロール (cas) が追加されました。

ロール (user) が追加されました。

ロール (cli) が追加されました。

```
> grdapi update_user userName="john"
email="john.smith@gmail.com"
```

ID=20000

> grdapi list_users

ID=0

####### User 3 #######

ユーザー名: accessmgr

名: accessmgr

姓: accessmgr

E メール:

無効: false

####### User 1 #######

ユーザー名: admin

名: admin

姓: admin

E メール:

無効: false

####### User 33 #######

ユーザー名: anon

名: anon

姓: anon

E メール:

無効: false

####### User 20000 #######

ユーザー名: john

名: john

姓: smith

E メール: john.smith@gmail.com

無効: false

####### User 2 #######

ユーザー名: bill

名: bill

姓: green

E メール:

無効: true

set_user_roles

set_user_roles

set_user_roles を実行するたびに、ユーザーのロールをリセットします。 ロールには何も追加しないでください。リセットしてください。

GrdAPI を使用してユーザーを作成すると、user ロールを持つユーザーが作成されます。ロールを設定する際には、そのロールのすべてを指定する必要があります。これは、既存のロールの削除と新規ロールの追加を有効にするために行われます。

GUI でも、チェック・マークを付けたり外したりできるロールがすべて表示されます。ロールを保存すると、チェック・マークの付いたすべてのロールが保存されます。

GrdAPI で、ユーザー kevin にロール INV のみを付与します。ユーザーには、user、cli、admin、または accessmgr のいずれかのロールが必要です。

この GrdAPI の正しい呼び出し方法は次のとおりです。

```
grdapi set_user_roles userName="kevin"  roles="user,inv"
```

例

> set guiuser accessmgr password ASDFasdf

ok

> grdapi create_user firstName=kevin

lastName=smith password=pASSW0rd confirmPassword=pASSW0rd

email=ksmith@company.com userName=kevin disabled=0

ID=20000

ok

```
> grdapi set_user_roles userName="kevin" roles="inv"
```

set_user_roles:

ERR=3700

ユーザーには、user、cli、admin、accessmgr のいずれかのロールが必要です。

コマンドを実行中にエラーが発生しました

ok

```
> grdapi set_user_roles userName="kevin"
roles="user,inv"
```

ID=20000

ロール (user) が追加されました。

ロール (inv) の追加に失敗しました。 inv ロールを割り当てる前に、ユーザーの姓を次の 3 つの調査データベースのいずれかの名前に設定する必要があります。

INV_1、INV_2、または INV_3 (大/小文字の区別あり)

ok

```
> grdapi set_user_roles userName="kevin"
roles="dba,diag,cas,user"
```

ID=20000

ロール (dba) が追加されました。

ロール (diag) の追加に失敗しました。 診断は、cli または admin のいずれかのロールを持つ必要があります。

ロール (cas) が追加されました。

ロール (user) が追加されました。

ok

>

show guiuser

これにより、GUI のユーザー (ロール別) が表示されます。

表示コマンド

show guiuser

パスワード制御コマンド

以下のコマンドを使用して、次のようにユーザー・パスワードを制御します。

- store password disable - 非アクティブなアカウントが無効になるまでの日数を設定します。
- store password expiration - パスワードが期限切れになるまでの日数を設定します。
- store password validation - 強化されたパスワードの検証ルールを有効または無効にします。

アカウント・ロックアウト・コマンド

アカウント・ロックアウト・コマンドを使用して、ログイン試行が 1 回以上失敗した後に Guardium® ユーザー・アカウントを無効にします。 これらのコマンドは、以下の目的で使用します。

- 機能を有効または無効にする。 store account lockout を参照してください。
- 1 つのアカウントについて、所定の時間間隔の間に許容されるログイン失敗の最大回数を設定する。 store account strike count および store account strike interval を参照してください。
- 1 つのアカウントについて、Guardium アプライアンスの存続期間中に許容される失敗の最大回数を設定する。 store account strike max を参照してください。
- admin ユーザー・アカウントがロック状態になった場合にアンロックする。 unlock admin コマンドの説明を参照してください。

Guardium ユーザー・アカウントが無効化された後、accessmgr ロールを持つユーザーか admin ユーザーに限り、このアカウントを Guardium ポータルから有効にすることができます。

例

アカウント・ロックアウトを有効にし、10 分以内に 5 回のログインが失敗したらアカウントをロックし、許容される失敗の最大数を 999 に設定します。

store account lockout on

store account strike count 5

store account strike interval 10

store account strike max 999

注:

admin ユーザー・アカウントがロックされている場合、unlock admin コマンドを使用してアンロックします。

アカウント・ロックアウトが有効になっている場合、strike count または strike max をゼロに設定しても、そのタイプのチェックは無効になりません。 それどころか、1 回でも失敗するとそのユーザー・アカウントが無効になることを意味します。

store account lockout

指定回数ログインが失敗したらユーザー・アカウントを無効にする自動アカウント・ロックアウト機能を有効 (on) または無効 (off) にします。

構文

store account lockout <on | off>

表示コマンド

show account lockout

store account strike count

構成されたストライク間隔において、アカウントが無効になるログイン試行失敗回数 (n) を設定します。

構文

store account strike count <n>

表示コマンド

show account strike count

store account strike interval

ここに設定した秒数 (n) の間に、構成されたログイン試行失敗回数に達すると、アカウントが無効になります。

構文

store account strike interval <n>

表示コマンド

show account strike interval

store account strike max

サーバーの存続期間中に、アカウントが無効になるまでに許容されるログイン試行失敗の最大回数 (n) を設定します。

構文

store account strike max <n>

表示コマンド

show account strike max

store password disable

days で設定した日数の間アクティビティーがなければ、ユーザー・アカウントが無効になります。 0 (ゼロ) に設定すると、アクティビティーがなくてもアカウントは無効になりません。 インストール時のデフォルト値はゼロです。 この設定値の変更後には、GUI を再始動する必要があります (restart gui を参照してください)。

構文

store password disable <days>

表示コマンド

show password disable

store password expiration

ユーザー・パスワードの有効期限の存続期間 (日数) を設定します。 -1 に設定すると、パスワードの有効期限が切れることはありません。0 以外の値を設定した場合、アカウント・ユーザーは、現行パスワードが有効期限切れになった後の初回ログイン時にパスワードを再設定する必要があります。 デフォルト値は 90 です。 この設定値の変更後には、GUI を再始動する必要があります。

構文

store password expiration <days>

表示コマンド

show password expiration

store password validation

パスワードの検証をオンまたはオフに切り替えます。 デフォルト値は on です。 このコマンドを実行すると、GUI が再始動されてこの設定が適用されます。

パスワード検証が有効になっている場合、パスワードは 8 文字以上の長さでなければなりません。さらに、英大文字 (A-Z)、英小文字 (a-z)、数字 (0-9)、および表に示す特殊文字を、それぞれ 1 つ以上含んでいなければなりません。無効になっている (非推奨) 場合は、任意の長さおよび文字の組み合わせが許可されます。

構文

store password validation <on | off>

表示コマンド

show password validation

表 1. Guardium パスワードに使用できる特殊文字

文字	記述
@	アットマーク (単価記号)
#	ナンバー記号
$	ドル記号
%	パーセント記号
^	曲折アクセント記号 (カラット)
&	アンパーサンド
.	終止符 (ピリオド)
;	セミコロン
!	感嘆符
-	ハイフン (マイナス記号)

文字	記述
+	プラス記号
=	等号
_	下線 (アンダースコアー)

store user password

このコマンドは、cli ユーザー・パスワードをリセットするために使用します。 サポート処理を簡略化するため、初期状態で Guardium によって割り当てられた cli ユーザー・パスワードを覚えておくことを推奨します。 一度設定した cli ユーザー・パスワードを検索する方法はありません。 このパスワードを紛失した場合は、Guardium サポートに連絡し、パスワードのリセットを依頼してください。

構文

store user password

現行のパスワードと、それに続いて新規パスワード (2 回) の入力を求めるプロンプトが出されます。 キーボードで入力したパスワードの値は、画面上には表示されません。

cli ユーザー・パスワード要件は、ユーザー・パスワードの要件とは異なります。 cli ユーザー・パスワードは、 6 文字以上の長さでなければなりません。さらに、次のタイプの文字をそれぞれ 1 つ以上含んでいなければなりません。

- 数字 (0-9)
- 英小文字 (a-z)
- 英大文字 (A-Z)

この CLI コマンドを実行すると、パスワード有効期限ファイル内の変更日時レコードも更新されます。

unlock accessmgr

このコマンドは、無効になっている Guardium accessmgr ユーザー・アカウントを有効にするために使用します。 このコマンドで、accessmgr ユーザー・アカウント・パスワードがリセットされることはありません。

注: この CLI コマンドの実行を許可されるのは、admin ロールを持つユーザーだけです。

構文

unlock accessmgr

restart gui

unlock admin

このコマンドは、無効になっている Guardium admin ユーザー・アカウント を有効にするために使用します。 このコマンドで、admin ユーザー・アカウント・パスワードがリセットされることはありません。

注: この CLI コマンドの実行を許可されるのは、admin ロールを持つユーザーだけです。

構文

unlock admin

restart gui

認証コマンド

以下のコマンドは、使用される認証のタイプを表示または制御します。

store auth

このコマンドは、Guardium アプライアンス、SQL_GUARD へのログオンに使用する認証のタイプをリセットする (つまり、デフォルトのローカル Guardium 認証) ために使用します。

オプションの認証方式 (LDAP や Radius など) の構成および有効化は、管理者ポータルから行うことはできますが、CLI から行うことはできません。詳しくは、『認証の構成』を参照してください。

構文

store auth SQL_GUARD

表示コマンド

show auth

親トピック: CLI の概要

GuardAPI リファレンス

GuardAPI を使用すると、コマンド行から Guardium® 機能にアクセスできます。

これにより反復作業の自動化が可能となるため、特に大規模な実装環境においては利用価値があります。 これらの GuardAPI 関数を呼び出すことにより、素早くさまざまな操作を行うことができます。 例えば、データ・ソースの作成、ユーザー階層の保守、S-TAP® のような Guardium 機能の保守などの操作を行えます。

GuardAPI を使用するために CLI に適切にログインするには、5 つの CLI アカウント (guardcli1、...、guardcli5) の 1 つでログインし、さらに、アクセス・マネージャーで作成されて admin または cli ロールを付与されたユーザー (GUI username/guiuser) でログイン (「set guiuser」コマンドを発行) することが必要です。 詳しくは、『set guiuser 認証』を参照してください。

GuardAPI は一連の CLI コマンドで、すべてキーワード grdapi で始まります。

- 使用可能なすべての GuardAPI コマンドをリストするには、引数を指定せずに grdapi コマンドを実行するか、または検索引数を指定せずに「grdapi commands」コマンドを実行します。 例:

```
CLI> grdapi
または
CLI> grdapi commands
```

- 特定のコマンドのパラメーターを表示するには、コマンドに続けて「--help=true」を入力します。例:

```
CLI> grdapi list_entry_location --help=true
ID=0
function parameters :
fileName
hostName - required
path - required
ok
```

- 検索文字列を指定して GuardAPI コマンドを検索するには、CLI コマンド grdapi commands <search-string> を使用します。例:

```
CLI> grdapi commands user
ID=0
Matching API Function list :
create_db_user_mapping
create_user_hierarchy
delete_allowed_db_by_user
delete_db_user_mapping
delete_user_hierarchy_by_entry_id
delete_user_hierarchy_by_user
execute_appUserTranslation
execute_ldap_user_import
list_allowed_db_by_user
list_db_user_mapping
list_user_hierarchy_by_parent_user
update_user_db
```

- パラメーターの値リストを表示するには、コマンドに「--get_param_values=<parameter>;」を付けて入力します。 例:

```
CLI> grdapi create_group --get_param_values=appid
Value for parameter 'appid' of function 'create_group' must be one of:
パブリック
監査プロセス・ビルダー
分類
DB2 zOS グループ
エクスプレス・セキュリティー
IMS zOS グループ
ポリシー・ビルダー
セキュリティー・アセスメント・ビルダー
ID=0
ok
```

表 1. -get_param_values コマンドの構造をサポートする API

API 関数	パラメーター
create_datasource	application、type、severity、shared
create_group	appid、type

大/小文字の区別

パラメーターの構成要素となるキーワードと値には、いずれも大/小文字の区別があります。

スペースを含むパラメーター値

パラメーター値に 1 つ以上のスペースが含まれる場合は、二重引用符文字で囲む必要があります。

例:

```
grdapi create_datasource type ="MS SQL SERVER" ...
```

NULL 値および空文字列

一般的に、GuardAPI 関数を呼び出すときに、必須ではないパラメーターに値を指定しないか、または空文字列 ("""") を設定すると、そのパラメーターは GuardAPI 関数呼び出し時に GuardAPI によって NULL 値に変換されます。そのため GuardAPI に変換されると、そのパラメーターが指定されていない場合と同様に無視されます。

例えば、ポリシー・ルールからあるグループを消去する場合、そのグループに空文字列 ("" "") ではなく、スペース ("" "") を設定します。空文字列 ("""") を使用すると、そのグループを無視し、そのグループ選択を変更しないように GuardAPI に通知されます。

ポリシー値からグループを消去する例

```
grdapi update_rule fromPolicy=V8 ruleDesc="LogFull Details" dbUserGroup=" " dbUser=" " objectGroup=" " commandsGroup=" "
```

戻りコード

GuardAPI コマンドの結果に関わらず、戻りコードは常に出力の最初の行に次に示すフォーマットで返されます。

表 2. 戻りコード

戻りコード	記述
ID=identifier	成功。identifier は操作対象オブジェクトの ID です。例えば、直前に定義したグループの ID です。
ERR=error_code	エラー。error_code はエラーを識別するためのものです。これに続いてエラーについてのテキストの記述が 1 行以上あります。 『概要』に共通エラー表があり、『GuardAPI エラー・コード』にエラー・コードの全リストがあります。

例えば、create_group コマンドを使用して agroup という名前のグループ objects を定義する場合、正常に行われればそのグループの ID が返されます。

```
CLI> grdapi create_group desc=agroup type=objects appid=Public
ID=20001
ok
CLI>
```

この ID を list_group_by_id コマンドで使用すると、グループ定義を表示することができます。

```
CLI> grdapi list_group_by_id id=20001
ID=20001
Group GroupId=20001
Group GroupTypeId=3
Group ApplicationId=0
Group GroupDescription=agroup
Group GroupSubtype=null
Group CategoryName=null
Group ClassificationName=null
Group Timestamp=2008-05-10 07:34:11.0
Group type = OBJECTS
Application Type = Public
Touple Group
ok
```

実行不成功の場合は、エラー・コードが返されます。 例えば、無効な ID を指定して再度 list_group_by_id コマンドを実行した場合、次のメッセージを受け取ります。

```
a1.corp.com> grdapi list_group_by_id id=20123
ERR=140
Could not retrieve Group - check Id.
ok
```

共通エラー・コード

100 より小さい値のエラー・コードは、共通のエラー条件用です。100 より大きなエラー・コードは特定の関数に適用され、各関数の後で説明します。

GuardAPI エラー・コードの全リストを表示するには、CLI コマンド・プロンプトで grdapi-errors と入力します。

表 3. 共通エラー・コード

エラー	記述
0	パラメーターが欠落しているか、予期しない例外などの不明エラーです。
1	例外が発生しました。Guardium のサポートに連絡してください。
2	要求された関数を取得できませんでした。関数名を確認してください。すべての関数をリストするには、CLI コマンド grdapi または grdapi commands を引数なしで入力します。 検索文字列を指定して関数名によって検索するには、CLI コマンド grdapi commands <search-string> を使用します。
3	引数が多すぎます。この関数のパラメーター・リストを取得するには、--help=true を指定してこの関数を呼び出します。
4	必須パラメーターが欠落しています。この関数のパラメーター・リストを取得するには、--help=true を指定してこの関数を呼び出します。
5	パラメーターを暗号化解除できませんでした。正しい共有パスワードを使用して暗号化されたかどうかを確認してください。
6	パラメーター・フォーマットが間違っています。関数名に続けて <name=value> フォーマットを使用してパラメーター・リストを指定してください。
7	パラメーター・タイプに対するパラメーター値が間違っています。
8	パラメーター名が間違っています。パラメーターには大/小文字の区別があります。
9	ユーザーの特権は、要求された API 関数には不十分です。
10	パラメーターの暗号化が有効になっていません。共有パスワードが設定されていません。
11	targetHost に API 呼び出し要求を送信できませんでした。
12	パラメーターの検証中にエラーが発生しました。
13	ターゲット・ホストは中央マネージャーの IP アドレスでなければなりません。

エラー	記述
14	ターゲット・ホストはこのマネージャーによって管理されていません。
15	ターゲット・ホストがオンラインではありません。
16	ターゲット・ホストはスタンドアロン・ユニットでは指定できません。
17	ユーザーは指定されたオブジェクトで操作を行うことが許可されていません。
18	ターゲット・ホストを指定できません。
19	終了引用符がありません。
20	ユーザーは grdapi commands を実行することが許可されていません。
21	--username および --source-host は grdapi の予約語であり、コマンド行で渡すことはできません。
22	1 つのパラメーター名を複数回指定することはできません。コマンド行を調べて、重複したパラメーターがないか確認してください。
23	値は定数リストに含まれていません。
24	暗号化された値は有効ではありません。
25	有効なパラメーター・フォーマットではありません。パラメーターは <name=value> として指定する必要があり、スペースは使用できません。

GuardAPI アクティビティー・ログ

Guardium アクティビティー・ログでは、システムで実行されるすべての grdapi コマンドが記録されます。 管理者ポータルからコマンドを表示するには「Guardium モニター」タブにある「ユーザー・アクティビティー監査証跡」レポートにナビゲートします。

すべての grdapi アクティビティーは、cli ユーザーに属するものと見なされます。 そのレポートの cli 行をダブルクリックして、「Guardium ユーザー・アクティビティーの詳細」ドリルダウン・レポートを選択します。入力されたすべてのコマンドが、加えられたすべての変更とともにリストされます。 また、コマンド発行元の IP アドレスもリストされます。

暗号化されたパラメーター

GuardAPI はスクリプトから呼び出されますが、スクリプトにはデータ・ソースのパスワードなどの機密情報が含まれる場合があります。 機密情報を常に暗号化しておくため、grdapi コマンドは 1 つの暗号化されたパラメーターを API 関数に渡すことができます。 この暗号化は、システムの共有パスワードを使用して行われます。共有パスワードは管理者によって設定され、多数のシステムで、またすべての一元管理ユニットと統合クラスターの間で共有されます。このため、暗号化されたパラメーターを使用するスクリプトを、同じ共有パスワードを持つマシン上で実行することができます。

注: 共有パスワードが設定されていないシステムで暗号化されたパラメーターを使用する API 呼び出しを実行しようとすると、次のエラー・メッセージが表示されます。

パラメーター暗号化が有効になっていません – 共有パスワードが設定されていません

GUI を介して生成される GuardAPI スクリプトの場合、暗号化が必要な場合には、スクリプト生成を実行するシステムの共有パスワードを使用して暗号化されます。

すべての grdapi 呼び出しにおいて、オプション・パラメーターの encryptedParam を使用可能です。 このパラメーターは、暗号化された値を別のパラメーターに渡すために使用できます。

手動による暗号化の手順を以下に示します。

1. パラメーター暗号化 API を使用します。

   encrypt_value API は、暗号化する値およびターゲット・システムの共有パスワード (鍵) を受け入れた後、暗号化された値をプリント出力します。 鍵がシステムの共有パスワードでない場合は、警告がプリント出力されます。

```
a1.corp.com> grdapi encrypt_value --help=true
ID=0
function parameters :
key - required
valueToEncrypt - required
api_target_host
ok
```

表 4. 暗号化されたパラメーター

パラメーター	記述
key	ターゲット・システムの共有パスワード
valueToEncrypt	暗号化される値
api_target_host	一元管理構成に限り、API が実行されるターゲット・ホストを指定できます。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

   例

```
a1.corp.com> grdapi encrypt_value valueToEncrypt="some value" key=guard
ID=0
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (GNU/Linux)
jA0EAgMCTEIUShudn0tgyTB9GL7wR79UL9X9DCAa6RkUQRbegG52olA4gwOzmpHF
0qEhsd6Uz7l8rUsheUyX9v4=
=c1Cq
-----END PGP MESSAGE-----
```

2. 生成された内容をコピーして、CLI スクリプト内に組み込みます。

```
cli.gsh  コードの例:
set guiuser johny_smith password 3wel9s887s
 grdapi create_datasource type=oracle name=myOra host=somehost application=AuditTask owner=admin user=sa serviceName=ora
encryptedParam=password
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (GNU/Linux)
jA0EAgMCTEIUShudn0tgyTB9GL7wR79UL9X9DCAa6RkUQRbegG52olA4gwOzmpHF
0qEhsd6Uz7l8rUsheUyX9v4=
=c1Cq
-----END PGP MESSAGE-----
```

3. 次のようにスクリプトを実行して grdapi を呼び出します。

```
user> ssh cli@a1.corp.comuser> ssh cli@a1.corp.com
```

一元管理での注意

一元管理環境で GuardAPI を使用する場合は、中央マネージャーでどのようなコンポーネントが定義されているのか、さらに管理対象ユニットでどのようなコンポーネントが定義されているのかを把握しておく必要があります。このトピックについては、『一元管理』を参照してください。

クエリー・ビルダーにおける特定のユーザーの属性の表示

admin ユーザーはすべての照会属性をクエリー・ビルダーで参照可能であり、非 admin ユーザーは admin のみとして設計されている属性 (ID など) 以外の照会属性をクエリー・ビルダーで参照可能です。

一部のエンティティー (完全な SQL など) には多数の属性があります。

デフォルトでは、すべてのユーザー (admin および非 admin) に関するすべての属性が表示されます。

特定のユーザーに関する特定の属性を表示したり非表示にしたりするために、2 つの GuardAPI コマンドが追加されています。

これらの GuardAPI コマンドは、完全な SQL の特定の属性のグループ (VSAM、ISAM、MApReduce、APEX、Hive、BigInsight) のみ有効化/無効化します。

これら 2 つの新しい GuardAPI の名前は、grdapi enable_special_attributes と grdapi disable_special_attributes です。

両方とも、1 つのパラメーター attributesGroup のみ受け取ります。

このパラメーターの有効値は、VSAM、IMS、MapReduce、APEX、Hive、BI (BigInsights)、IMS/VSAM、DB2 i、F5 です (大/小文字の区別はありません)。

各 Grdapi はグループに対応している属性をすべて有効化 (無効化) します。例えば、VSAM の場合は以下の属性を有効化 (無効化) します。

- VSAM レコード
- 削除済みの VSAM レコード
- 挿入済みの VSAM レコード
- 取得済みの VSAM レコード
- 更新済みの VSAM レコード
- VSAM ユーザー・グループ ID

Hive は以下の属性を有効化 (無効化) します。

- Hive コマンド
- Hive データベース
- Hive エラー
- Hive 解析 SQL
- Hive 表名
- Hive ユーザー

注: ユーザーが admin ロールを持つ場合は、引き続き属性が表示されます。これらの属性の有効化または無効化は非 admin ユーザー (admin ロールを持たないユーザー) のみに適用されます。
注: 変更内容を有効にするために GUI を再始動する必要はありません。 ただし、次のような場合を除きます。すなわち、グループ F5 の属性を持つレポートが作成されていて、それが「My New Reports」に追加されている場合は、その属性が有効化されていても、admin ユーザーはレポートを表示する特権を持っていません。レポート・フィールドを表示するためには、GUI を再始動する必要があります。

- GuardAPI アーカイブおよびリストア関数
- GuardAPI アセスメント関数
  以下の CLI コマンドは、アセスメント関数を追加、削除、および更新するために使用します。
- GuardAPI オートディスカバリー関数
  以下の CLI コマンドは、オートディスカバリー関数を作成、変更、リスト、および実行するために使用します。
- GuardAPI カタログ・エントリー関数
  これらの GuardAPI コマンドは、カタログ・エントリー関数の作成、リスト、削除、および更新に使用します。
- GuardAPI 分類関数
  次の GuardAPI コマンドを使用して、分類ポリシー構成、テスト自動化、および前提条件データの準備のスクリプト記述を行います。
- GuardAPI クラウド・データ・ソース関数
- GuardAPI データベース・ユーザー関数
  これらの GuardAPI コマンドは、データベース・ユーザー・マッピングの保守、非資格情報スキャン、およびデバッグ・レベルの設定に使用します。
- GuardAPI データ・ソース関数
  これらの GuardAPI コマンドは、データ・ソース関数の作成、リスト、削除、および更新に使用します。
- GuardAPI データ・ソース・リファレンス関数
  これらの GuardAPI コマンドは、データ・ソース・リファレンス関数の作成、リスト、および削除に使用します。
- GuardAPI データ・ユーザー・セキュリティー関数
  以下の GuardAPI コマンドは、データ・ユーザー・セキュリティー関数を作成、リスト、削除、および更新するために使用します。

- GuardAPI エンタープライズ・ロード・バランシング関数
  以下の GuardAPI コマンドを使用して、ロード・バランシング・パラメーターの表示と設定、現在のロード・マップの表示、および S-TAP と管理対象ユニット・グループの関連付けの管理を行います。
- GuardAPI 資格最適化機能
  これらの GuardAPI コマンドは、資格最適化データ・ソースおよびレポート作成を有効化および構成するために使用します。
- GuardAPI 外部フィード関数
  これらの GuardAPI 関数は、外部フィードのマッピングを作成するために使用します。
- GuardAPI ファイル・アクティビティー・モニター関数
  以下の GuardAPI コマンドは、ファイル・アクティビティー・モニターの有効化および無効化、ファイルの調査ダッシュボードのアクティビティーおよびライセンス抽出のスケジュールの構成、ファイル・アクティビティー・モニターに関する情報の取得を行う場合に使用します。
- GuardAPI GIM 関数
  これらの CLI コマンドは、GIM 関数のリスト、更新、割り当て、削除、およびキャンセルに使用します。
- GuardAPI グループ関数
  これらの GuardAPI コマンドは、データ・ソース・グループ関数の作成、リスト、および削除に使用します。
- GuardAPI 入力生成
  GuardAPI 入力生成を使用すると、ユーザーは 1 つの Guardium レポートの出力を取得して、それを別の Guardium エンティティーへの入力とすることができます。 つまり、ユーザーは準備済みの呼び出しを使用して素早く API の機能を呼び出すことができます。
- GuardAPI 調査ダッシュボード機能
  これらの GuardAPI コマンドは、調査ダッシュボードの機能とパラメーターを有効化、無効化、または構成するために使用します。
- GuardAPI ネイティブ監査関数
  これらの GuardAPI コマンドを使用して、クラウド・データベースに対する DB 監査 (ネイティブ監査) の有効化、無効化、オブジェクト監査 (監査証跡) に対するオブジェクトの追加と削除、構成、コレクター、およびオブジェクトの取得を実行します。
- GuardAPI 異常値検出機能
  以下の GuardAPI コマンドは、異常値検出機能を有効化、無効化、および構成するために使用します。
- GuardAPI プロセス制御関数
  これらの GuardAPI コマンドは、プロセス制御関数の実行、コピー、アップロード、リスト、および削除に使用します。
- GuardAPI 照会再書き込み関数
  コマンド行インターフェースで Guardium API を使用して、ユーザー・インターフェースから実行できない特定の複雑な照会のテストを自動化したり、そうした照会の定義を作成したりします。
- GuardAPI ロール関数
  これらの GuardAPI コマンドは、ロール関数の付与、リスト、および取り消しに使用します。
- GuardAPI S-TAP 関数
  これらの CLI コマンドは、S-TAP 関数の作成、リスト、削除、再始動、および設定に使用します。
- GuardAPI 脅威検出分析機能

親トピック: CLI および API

GuardAPI アーカイブおよびリストア関数

list_expiration_dates_for_restored_days

すべてのリストア日における有効期限をリストします。

表 1. list_expiration_dates_for_restored_days

パラメーター	記述
newExpDate	必須。 リストア日における新しい有効期限。
restoredDay	必須。 データのリストア日を指定します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi list_expiration_dates_for_restored_days

get_expiration_date_for_restored_day

特定のリストア日に関連付けられた有効期限を取得します。

表 2. get_expiration_date_for_restored_day

パラメーター	記述
newExpDate	必須。 リストア日における新しい有効期限。
restoredDay	必須。 データのリストア日を指定します。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi get_expiration_date_for_restored_day restoredDay=restoredDay
```

ここで、restoredDay は、実際の日 `yyyy-mm-dd hh:mi:ss` または `NOW -10 day` のような相対日のいずれかの形式になります。

set_expiration_date_for_restored_day

特定のリストア日における有効期限を設定します。

表 3. set_expiration_date_for_restored_day

パラメーター	記述
newExpDate	必須。 リストア日における新しい有効期限。
restoredDay	必須。 データのリストア日を指定します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi set_expiration_date_for_restored_day newExpDate=newExpDate restoredDay=restoredDay
```

ここで、newExpDate および restoredDay は、実際の日 `yyyy-mm-dd hh:mi:ss` または `NOW -10 day` のような相対日のいずれかの形式になります。

set_import

統合データのインポートを開始または停止します。

表 4. set_import

パラメーター	記述
state	必須。START または STOP
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi set_import [START]
```

configure_export

統合データのエクスポートを構成します。

表 5. configure_export

パラメーター	記述
aggHost	必須。文字列。アグリゲーター のホスト名。
aggSecHost	文字列

パラメーター	記述
exportOlderThan	必須。整数。エクスポートするデータの時間別詳細。
exportValues	必須。整数。 0 または 1
ignoreOlderThan	必須。整数。無視するデータの時間別詳細。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi configure_export [aggHost] [aggSecHost] [exportOlderThan] [exportValues] [ignoreOlderThan]
```

configure_archive

統合データのアーカイブを構成します。

表 6. configure_archive

パラメーター	記述
accessKey	文字列。アグリゲーターの共有パスワード。
archiveOlderThan	必須。整数。アーカイブするデータの時間別詳細。
archiveValues	必須。整数。 0 または 1
bucketName	文字列
destHost	文字列。アーカイブ先のホスト名。
ignoreOlderThan	必須。整数。無視するデータの時間別詳細。
passwd	文字列。パスワード。
passwdRetype	文字列。パスワードの再入力
port	整数。ポート番号
protocol	必須。文字列。SCP、FTP、または AMAZON
retention	整数。保持する期間。
secretKey	文字列
targetDir	文字列
userName	文字列。ユーザー名。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi configure_archive [accessKey] [archiveOlderThan] [archiveValues][bucketName][destHost][ignoreOlderThan][passwd]
[passwdRetype] [port] [protocol] [retention] [secretKey] [targetDir] [userName]
```

親トピック: GuardAPI リファレンス

GuardAPI アセスメント関数

以下の CLI コマンドは、アセスメント関数を追加、削除、および更新するために使用します。

下記の GuardAPI コマンドは、以下の目的で使用します。

- セキュリティー・アセスメント定義の追加、削除、更新
- 既存のセキュリティー・アセスメントでのデータ・ソースの追加、削除
- 既存のセキュリティー・アセスメントでのテストの追加、削除

create_assessment

この GuardAPI コマンドは、セキュリティー・アセスメントを追加するために使用します。

表 1. create_assessment

パラメーター	検証内容
assessmentDescription	必須。フリー・テキスト (固有)。同じ記述のアセスメントが前に存在していないことを確認する必要があります。 既に存在している場合はエラーになります。
fromDate	有効な日付、または相対的な日付。必須ではありません。デフォルトは NOW -1 DAY
toDate	有効な日付、または相対的な日付。必須ではありません。デフォルトは NOW
FilterClientIP	有効な IP アドレス。必須ではありません。デフォルトは NULL
FilterServerIP	有効な IP アドレス。必須ではありません。デフォルトは NULL

アクション: すべてのパラメーターが検証されたら、SECURITY_ASSESSMENT 表に新規レコードが作成されます (MODIFIED_FLAG はデフォルトの 0 のままです)

例

```
grdapi create_assessment assessmentDescription=Assess1
```

add_assessment_datasource

この GuardAPI コマンドは、セキュリティー・アセスメントにデータ・ソースを追加するために使用します。

表 2. add_assessment_datasource

パラメーター	検証内容
assessmentDescription	必須。フリー・テキスト (固有)。同じ記述のアセスメントが前に存在していないことを確認する必要があります。 既に存在している場合はエラーになります。
datasourceName	必須。フリー・テキスト: 既存のデータ・ソースの名前でなければなりません。既存のデータ・ソースが存在しない場合はエラーになります。

アクション: すべてのパラメーターが検証されたら、ASSESSMENT_DATASOURCE にレコードが追加されます。その際に、アセスメントとデータ・ソースの ASSESSMENT ID と DATASOURCE ID には指定された名前が使用されます。

例

```
grdapi add_assessment_datasource assessmentDescription=Assess1 datasourceName=DS1
```

add_assessment_test

この GuardAPI コマンドは、既存のセキュリティー・アセスメントにテストを追加するために使用します。

表 3. add_assessment_test

パラメーター	検証内容
assessmentDescription	必須 - フリー・テキスト (固有)。同じ記述のアセスメントが前に存在していないことを確認する必要があります。既に存在している場合はエラーになります
testDescription	必須 - AVAILABLE_TEST 内の既存のテストの TEST_DESC と一致している必要があります。既存のテストが存在しない場合はエラーになります。
severity	SEVERITY_DESC 表と照合して検証します (DESCRIPTION を使用) - 必須ではありません。デフォルトは INFO です。
thresholdValue	available_test で必須のしきい値が 0 の場合、このパラメーターを無視します。 そうではなく、available_test で必須の値 (しきい値) が 1 の場合、パラメーターは整数である必要があります このパラメーターが指定しないと、AVAILABLE_TEST の DEFAULT_THRESHOLD_VALUE が使用されます。
exceptionsGroup	AVAILABLE_TEST 内の CAN_HAVE_EXCEPTIONS_GROUP 値を確認します。 このパラメーターは必須ではありません。 0 の場合、(例外グループはこのテストでサポートされない): このパラメーターを指定するとエラーになります (このテストでは例外グループを指定できません)。パラメーターが指定されない場合、-1 を使用してデータを設定します。 そうでない場合 (例外グループがこのテストでサポートされる): パラメーターが指定されない場合、-1 を使用してデータを設定します。パラメーターが指定された場合、グループを検証してグループ ID を使用します。 グループを検証するには、GROUP_DESCRIPTION が指定した記述と一致するレコードを GROUP_DESC から選択し、レコードが存在するかどうか、および GROUP_TYPE_ID を確認します。 そのグループが存在し、GROUP_TYPE_ID != 55 の場合はエラー「例外グループのタイプは「VA 例外」でなければなりません」が出されます。 そのグループが存在し、タイプが 55 である場合は、GROUP_ID が使用されます。

追加の検証: ASSESSMENT_TEST 内に ASSESSMENT_ID および TEST_ID のレコードが既に存在するかどうかを確認します。そのレコードが存在する場合はエラー「このテストは既にアセスメントに存在するため、再度追加することはできません」が出されます。

アクション: すべてのパラメーターが検証されたら、ASSESSMENT_TEST にレコードを追加します (注: 重大度として、記述に指定された値を設定する必要があります)。

例

```
grdapi add_assessment_test  assessmentDescription=Assess1 testDescription="The first test"
```

delete_assessment

この GuardAPI コマンドは、セキュリティー・アセスメントを削除するために使用します。

表 4. delete_assessment

パラメーター	検証内容
assessmentDescription	必須 - フリー・テキスト (固有)。同じ記述のアセスメントが前に存在していないことを確認する必要があります。既に存在している場合はエラーになります

追加の検証: 以下を行って、削除対象のアセスメントの結果が存在していないことを確認する必要があります。

Select count (*) from ASSESSSMENT_RESULT_HEADER where ASSESSMENT_ID = TheIdToRemve

select で 0 より大きい値が返された場合、削除されずに、エラーになります。

アクション: パラメーターが検証されたら (セキュリティー・アセスメント・レコードが特定され、そのアセスメントの結果が存在しない場合)、SECURITY_ASSESSMENT レコード、ASSESSMENT_TEST レコード、および ASSESSMENT_DATASOURCE レコードを削除します (この 3 つはすべて ASSESSMENT_ID を使用して削除します)。

例

```
grdapi delete_asssessment assessmentDescription=Assess1
```

delete_assessment_datasource

この GuardAPI コマンドは、セキュリティー・アセスメントからデータ・ソースを削除するために使用します。

表 5. delete_assessment_datasource

パラメーター	検証内容
assessmentDescription	必須。フリー・テキスト (固有)。同じ記述のアセスメントが前に存在していないことを確認する必要があります。 既に存在している場合はエラーになります。
datasourceName	必須。フリー・テキスト: 既存のデータ・ソースの名前でなければなりません。既存のデータ・ソースが存在しない場合はエラーになります。

アクション: すべてのパラメーターが検証されたら、指定されたアセスメントとデータ・ソースのレコードが ASSESSMENT_DATASOURCE 内にあるかどうかを確認します。そのレコードがない場合はエラーになります。それ以外の場合、そのレコードを削除します。

例

```
grdapi delete_asssessment_datasource assessmentDescription=Assess1 datasourceName=DS1
```

delete_assessment_test

この GuardAPI コマンドは、既存のセキュリティー・アセスメントからテストを削除するために使用します。

表 6. delete_assessment_test

パラメーター	検証内容
assessmentDescription	必須。フリー・テキスト (固有)。同じ記述のアセスメントが前に存在していないことを確認する必要があります。既に存在している場合はエラーになります
testDescription	フリー・テキスト: AVAILABLE_TEST 内の既存のテストの TEST_DESC と一致している必要があります。既存のテストが存在しない場合はエラーになります。

追加の検証: ASSESSMENT_TEST 内に ASSESSMENT_ID および TEST_ID のレコードがあるかどうかを確認します。そのレコードがない場合はエラー「このテストはアセスメントに存在していません」が出されます。

アクション: すべてのパラメーターが検証されたら、ASSESSMENT_TEST からそのレコードを削除します。

例

```
grdapi delete_asssessment_test assessmentDescription=Assess1
```

list_assessments

この GuardAPI コマンドは、セキュリティー・アセスメントをリストするために使用します。

表 7. list_assessments

パラメーター	検証内容
assessmentDescription	必須。フリー・テキスト (固有)。同じ記述のアセスメントが前に存在していないことを確認する必要があります。既に存在している場合はエラーになります

例

```
grdapi list_assessments
```

list_assessment_tests

この GuardAPI コマンドは、セキュリティー・アセスメントのテストのリストを表示するために使用します。

list_available_tests の出力は次の形式になります。TEST=[<test description>], DS_TYPE=[<datasource type>] (実際の値は大括弧内にカプセル化されます)

list_assessment_tests の出力は次の形式になります。TEST_DESC=[<available test description>], DS_TYPE=[<datasourcetype>]

list_assessment_tests API コマンドのパラメーターは必須ではなく、フィルタリングをサポートします。

表 8. list_assessment_tests

パラメーター	検証内容
assessmentDescription	この API は以下を行います。 • その記述が唯一の有効なアセスメントの記述であることを確認し、アセスメントの ID を取得します。(アセスメントがない場合、エラーになります。) • アセスメントのテスト (およびデータ・ソース・タイプ) のリストを表示します。 Select AVAILABLE_TEST.TEST_DESC, DATASOURCE_TYPE.NAME from ASSESSMENT_TEST, DATASOURCE_TYPE, AVAILABLE_TEST, SECURITY_ASSESSMENT where AVAILABLE_TEST.DATASOURCE_TYPE_ID = DATASOURCE_TYPE.DATASOURCE_TYPE_ID and ASSESSMENT_TEST.ASSESSMENT_ID = SECURITY_ASSESSMENT.ASSESSMENT_ID and SECURITY_ASSESSMENT.ASSESSMENT_DESC like “Your Param”

例

```
grdapi list_assessment_tests
```

update_assessment

この GuardAPI コマンドは、セキュリティー・アセスメントのレコードを更新するために使用します。

表 9. update_assessment

パラメーター	検証内容
assessmentDescription	SECURITY_ASSESSMENT 内の既存レコードと一致している必要があります。
newAssessmentDescription	フリー・テキスト - 空の場合、記述を更新しないことを意味し、前のパラメーターの値が使用されます。空でない場合は固有であり、同じ記述のアセスメントが前に存在していないことを確認する必要があります。既に存在している場合はエラーになります。
fromDate	有効な日付または相対的な日付
toDate	有効な日付または相対的な日付
filterContentIP	有効な IP アドレス
filterServerIP	有効な IP アドレス

アクション: すべてのパラメーターが検証され (さらに、指定された記述を含む SECURITY_ASSESSMENT レコードが特定され) たら、指定された値によってそのレコードを更新します。

例

```
grdapi update_assessment assessmentDescription=Assess1 filterClientIP=192.168.1.1.
```

親トピック: GuardAPI リファレンス

GuardAPI オートディスカバリー関数

以下の CLI コマンドは、オートディスカバリー関数を作成、変更、リスト、および実行するために使用します。

add_autodetect_task

このコマンドは、指定されたプロセスにタスクを追加します。

表 1. add_autodetect_task

パラメーター	記述
process_name	必須。プロセスの名前
hosts_list	必須。ホストのリスト。192.168.0.1 192.168.1.* のような、スペースで区切られた IP のリストまたは IP 範囲とワイルドカード
ports_list	必須。ポートのリスト。22,23,1400-1600 のような、コンマ区切りのポートのリストまたはポート範囲

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi add_autodetect_task process_name=myProcess hosts_list="192.168.1.1 192.168.1.3" ports_list="22,23"
```

create_autodetect_process

このコマンドは自動検出プロセスを作成します。

表 2. create_autodetect_process

パラメーター	記述
check_ICMP_echo	必須。nmap に対する PE パラメーター (*)。値は「true」または「false」
host_timeout	必須。nmap に対するパラメーター (*)。タイムアウト値。
process_name	必須。プロセスの名前
run_probe_after_scan	必須。値は「true」または「false」。
use_dns	必須。nmap に対するパラメーター[1]。 値は常に「R」または「true」であり、「n」または「false」はあり得ません。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

注: * nmap オプションは、API からのみアクセス可能であり、GUI からはアクセスできません。nmap パラメーターについて、およびスキャンのパフォーマンスへのそれらの影響について詳しくは、man nmap を参照してください。

例

```
grdapi create_autodetect_process process_name=myProcess
```

modify_autodetect_process

このコマンドは自動検出プロセスを変更します。

表 3. modify_autodetect_process

パラメーター	記述
check_ICMP_echo	必須。nmap に対する PE パラメーター (*)。値は「true」または「false」
host_timeout	必須。nmap に対するパラメーター (*)。タイムアウト値。
process_name	必須。プロセスの名前
run_probe_after_scan	必須。値は「true」または「false」。
use_dns	必須。nmap に対するパラメーター[1]。 値は常に「R」または「true」であり、「n」または「false」はあり得ません。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

注: * nmap オプションは、API からのみアクセス可能であり、GUI からはアクセスできません。nmap パラメーターについて、およびスキャンのパフォーマンスへのそれらの影響について詳しくは、man nmap を参照してください。

例

```
grdapi modify_autodetect_process process_name=myProcess
```

delete_autodetect_scans_for_process

このコマンドは、プロセスのすべてのタスクを削除しますが、プロセスが実行中またはスケジュールされている場合、またはプロセスに結果がある場合、このコマンドは実行できません。

表 4. delete_autodetect_scans_for_process

パラメーター	記述
process_name	必須。プロセスの名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_autodetect_scans_for_process process_name=myProcess
```

list_autodetect_processes

このコマンドはすべてのプロセスをリストします。

表 5. list_autodetect_processes

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_autodetect_processes
```

list_autodetect_tasks_for_process

このコマンドは指定されたプロセスのすべてのタスクをリストします。

表 6. list_autodetect_tasks_for_process

パラメーター	記述
process_name	必須。プロセスの名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_autodetect_tasks_for_process process_name=myProcess
```

execute_autodetect_process

このコマンドは、指定されたプロセスを実行しますが、プロセスに何もタスクが定義されていない場合またはプロセスが現在実行中である場合、このコマンドは実行できません。

表 7. execute_autodetect_process

パラメーター	記述
process_name	必須。プロセスの名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_autodetect_process process_name=myProcess
```

show_autodetect_process_status

このコマンドは、プロセスの状況および進行状況サマリーを表示します。

表 8. show_autodetect_process_status

パラメーター	記述
process_name	必須。プロセスの名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi show_autodetect_process_status process_name=myProcess
```

stop_autodetect_process

このコマンドは。特定のプロセスの実行を停止します。

表 9. stop_autodetect_process

パラメーター	記述
process_name	必須。プロセスの名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi stop_autodetect_process process_name=myProcess
```

親トピック: GuardAPI リファレンス

GuardAPI カタログ・エントリー関数

これらの GuardAPI コマンドは、カタログ・エントリー関数の作成、リスト、削除、および更新に使用します。

create_entry_location

新しいアーカイブ項目を内部カタログ・ロケーション表に追加します。

表 1. create_entry_location

パラメーター	記述
entryType	必須文字列。次のいずれかでなければなりません。 • CollectorDataArchive • AggDataArchive • AggResultArchive
processDesc	文字列。entryType が AggResultArchive である場合のみ使用され、必須となります。
fileName	必須文字列。ファイルを指定します。
hostName	必須文字列。ホストを識別します。
path	必須文字列。FTP の場合、FTP アカウントのホーム・ディレクトリーを基準にした相対パスでディレクトリーを指定します。SCP の場合、絶対パスとしてディレクトリーを指定します。
user	必須文字列。ホストにアクセスするユーザー・アカウント。
password	必須文字列。ユーザーのパスワード。
retention	オプションの整数。 このエントリーをカタログに保持する日数 (デフォルトは 365)。
storageSystem	必須文字列。EMC、CENTERA、FTP、SCP、TSM のいずれかでなければなりません。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi  create_entry_location entryType=CollectorDataArchive  fileName=733392-a1.corp.com-w20071223.133546-d2007-12-27.dbdump.enc
password=somePassword user=someUser path=/var/dump/ hostName=192.168.1.241  storageSystem=scp
```

list_entry_location

fileName を指定した場合、1 つのアーカイブ・ロケーションがリストされます。fileName を省略した場合、複数のアーカイブ・ロケーションがリストされます。

表 2. list_entry_location

パラメーター	記述
fileName	オプションの文字列。リストする単一のファイル・ロケーションを指定します。 省略した場合、指定した hostName および path にあるすべてのファイル・ロケーションがリストされます。
hostName	必須文字列。ホストを識別します。
path	必須文字列。FTP の場合、FTP アカウントのホーム・ディレクトリーを基準にした相対パスでディレクトリーを指定します。SCP の場合、絶対パスとしてディレクトリーを指定します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_entry_location   path=/mnt/nfs/ogazit/archive_results/ hostName=192.168.1.33
```

delete_entry_location

fileName を指定した場合、1 つのアーカイブ・ロケーションが削除されます。fileName を省略した場合、複数のアーカイブ・ロケーションが削除されます。

表 3. delete_entry_location

パラメーター	記述
fileName	オプションの文字列。削除する単一のファイル・ロケーションを指定します。 省略した場合、指定した hostName および path にあるすべてのファイル・ロケーションが削除されます。
hostName	必須文字列。ホストを識別します。
path	必須文字列。FTP の場合、FTP アカウントのホーム・ディレクトリーを基準にした相対パスでディレクトリーを指定します。SCP の場合、絶対パスとしてディレクトリーを指定します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_entry_location  path=/var/dump/mojgan hostName=192.168.1.18
```

update_entry_location

fileName を指定した場合、1 つのアーカイブ・ロケーションが更新されます。 fileName を省略した場合、複数のアーカイブ・ロケーションが更新されます。

表 4. update_entry_location

パラメーター	記述
fileName	オプションの文字列。更新する単一のファイル・ロケーションを指定します。 省略した場合、指定した hostName および path にあるすべてのファイル・ロケーションが更新されます。
hostName	必須文字列。ホストを識別します。
path	必須文字列。FTP の場合、FTP アカウントのホーム・ディレクトリーを基準にした相対パスでディレクトリーを指定します。SCP の場合、絶対パスとしてディレクトリーを指定します。
newHostName	オプションの文字列。使用する場合、新しいホスト名を指定します。
newPath	オプションの文字列。使用する場合、新しいパスを指定します。
user	必須文字列。ホストにアクセスするユーザー・アカウント。
password	必須文字列。ユーザーのパスワード。
retention	オプションの整数。 このエントリーをカタログに保持する日数 (デフォルトは 365)。
storageSystem	オプションの文字列。EMC、CENTERA、FTP、SCP、TSM のいずれかを使用します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi update_entry_location  fileName=a1.corp.com-1_4_2008-01-10_10:27:24.res.70.tar.gz.enc path=/mnt/nfs/ogazit/archive_results/
hostName=qaserver    storageSystem=SCP newPath=/var/dump/mojgan  newHostName=192.168.1.18
```

親トピック: GuardAPI リファレンス

GuardAPI 分類関数

次の GuardAPI コマンドを使用して、分類ポリシー構成、テスト自動化、および前提条件データの準備のスクリプト記述を行います。

GuardAPI コマンドの使用方法については、『GuardAPI リファレンスの概要』ヘルプ・トピックを参照してください。

create_classifier_action

表 1. create_classifier_action

パラメーター	記述

パラメーター	記述
actionName	必須。文字列
actualMemberContent	必須。文字列
actionType	必須。文字列 参照用に、関連付けられている必須パラメーターを持つアクション・タイプのリストを以下に示します。 アクション・タイプに選択する内容に応じて、必須パラメーターが決まります。 add_to_group_objects actionName - 文字列 - 必須 actualMemberContent - 文字列 - 必須 objectGroup - 文字列 - 必須 policyName - 文字列 - 必須 ruleName - 文字列 - 必須 add_to_group_object_fields actionName - 文字列 - 必須 objectFieldGroup - 文字列 - 必須 policyName - 文字列 - 必須 ruleName - 文字列 - 必須 create_access_rule accessPolicy - 文字列 - 必須 accessRuleAction - 文字列 - 必須 actionName - 文字列 - 必須 ruleName - 文字列 - 必須 create_privacy_set actionName - 文字列 - 必須 policyName - 文字列 - 必須 privacySet - 文字列 - 必須 ruleName - 文字列 - 必須 log_policy_violation actionName - 文字列 - 必須 policyName - 文字列 - 必須 ruleName - 文字列 - 必須 action_send_alert actionName - 文字列 - 必須 policyName - 文字列 - 必須 receiver - 文字列 - 必須 ruleName - 文字列 - 必須
description	文字列
objectGroup	必須。文字列
policyName	必須。文字列
ruleName	必須。文字列
replaceGroupContent	ブール値
objectFieldGroup	必須。文字列
accessPolicy	必須。文字列
accessPolicy	必須。文字列
accessRuleAction	必須。文字列
commandsGroup	文字列
includeField	ブール値

パラメーター	記述
includeServerIP	ブール値
receiver	文字列
privacySet	必須。文字列
severity	文字列
notificationType	文字列
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_classifier_action actionType=add_to_group_objects policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
objectGroup="DW All Objects" replaceGroupContent=1 actualMemberContent=%FULLLIKE

grdapi create_classifier_action actionType=add_to_group_object_fields policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc objectFieldGroup="DW All Object-Field" replaceGroupContent=1

grdapi create_classifier_action actionType=create_access_rule policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
accessPolicy=pci accessRuleAction="alert daily" commandsGroup="Select command" includeField=1 includeServerIP=0
receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"

grdapi create_classifier_action actionType=create_privacy_set policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
privacySet=-b

grdapi create_classifier_action actionType=log_policy_violation policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
severity=MED

grdapi create_classifier_action actionType=send_alert policyName=-policy1 ruleName=-rule1 actionName=-action1 description=desc
notificationType=High receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"
```

GuardAPI コマンドの値

GUI で使用されるコマンド grdapi create_classifer_action の GuardAPI コマンド値のリストについては、表を参照してください。 これらの値は、グループを作成するときに使用します。

表 2. GrdAPI create_classifer_action

GUI 値	GrdAPI 値
%/%.Name	%/NAME
%/Full	%/FULL
Change/%.Name	CHANGE/NAME
Change/Full	CHANGE/FULL
完全修飾名 (スキーマ.オブジェクト)	FULLNAME
Like %Full	%FULLLIKE
Like %Full%	%FULLLIKE%
Like %Name	%NAMELIKE
Like %Name%	%NAMELIKE%
Like Full%	FULLLIKE%
Like Name%	NAMELIKE%
オブジェクト名のみ	NAMEONLY
Read/%.Name	READ/NAME
Read/Full	READ/FULL

例

```
grdapi create_classifier_action actionName=classgrpobjectseach1 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent=NAMEONLY description="object type NAMEONLY"
```

グループ・オブジェクト・タイプの例

```
grdapi create_group appid=Classifier type=OBJECTS desc="Classifier Group of Each Objects" owner=admin category=classifier
classification=classifier subtype=classifier

grdapi create_datasource type="Oracle (DataDirect)" user=scott password=tiger host="swan.guard.swg.usma.ibm.com"
name="Swan Oracle Object Each" shared=true owner=admin application=Classifier port=1521 serviceName=on8swan0

grdapi create_classifier_policy policyName="A Group Object Each Type Policy" category="Object Each Process"
classification="Object Each Process"

grdapi create_classifier_rule policyName="A Group Object Each Type Policy" category="Object Each Process"
classification="Object Each Process" ruleName=groupobjects1 ruleType=SEARCH_FOR_DATA dataTypes=TEXT continueOnMatch=1
tableNameLike="EMP_INFORMATION"
columnNameLike="PHONE" tableTypeTable=1

grdapi create_classifier_action actionName=classgrpobjectseach1 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent=NAMEONLY description="object type NAMEONLY"

grdapi create_classifier_action actionName=classgrpobjectseach2 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent=FULLNAME description="object type FULLNAME"

grdapi create_classifier_action actionName=classgrpobjectseach3 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%NAMELIKE" description="object type %NAMELIKE"

grdapi create_classifier_action actionName=classgrpobjectseach4 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="NAMELIKE%" description="object type NAMELIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach5 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%NAMELIKE%" description="object type %NAMELIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach6 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%FULLLIKE" description="object type %FULLLIKE"

grdapi create_classifier_action actionName=classgrpobjectseach7 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="FULLLIKE%" description="object type FULLLIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach8 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%FULLLIKE%" description="object type %FULLLIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach9 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="Change/Full" description="object type Change/Full"

grdapi create_classifier_action actionName=classgrpobjectseach10 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="CHANGE/NAME" description="object type Change/%.name"

grdapi create_classifier_action actionName=classgrpobjectseach11 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="Read/Full" description="object type Read/Full"

grdapi create_classifier_action actionName=classgrpobjectseach12 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="READ/NAME" description="object type Read/%.name"

grdapi create_classifier_action actionName=classgrpobjectseach13 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%/Full" description="object type %/Full"

grdapi create_classifier_action actionName=classgrpobjectseach14 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%/NAME" description="object type %/%.name"

grdapi create_classifier_process policyName="A Group Object Each Type Policy"
processName="A Group Object Each Type Process" datasourceNames="Swan Oracle Object Each"

grdapi create_classifier_action actionName=classgrpobjectseach10 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="FULLNAME" description="Fully Qualified Name(Schema.Object)
```

create_classifier_policy

表 3. create_classifier_policy

パラメーター	記述
category	必須。文字列
classification	必須。文字列
description	文字列

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_classifier_policy policyName=-policy1 classification=class1 description=desc1 category=cat1
```

create_classifier_process

create_classifier_process

注: この GuardAPI を呼び出す前に、分類ポリシーとデータ・ソースを作成してください。

表 4. create_classifier_process

パラメーター	記述
comprehensive	ブール値
datasourceNames	必須。文字列
includeInternalTables	ブール値。この設定は、デフォルトでは使用不可になっています。 includeInternalTables を使用可能にすると、データベース・ソフトウェア・プロバイダーが使用する内部システム・データベースおよびスキーマをスキャンできることを示します。内部システム・データベースおよびスキーマは、機密データを含む可能性が低く、デフォルトではスキャンされません。内部表を組み込む場合は、分類データ・ソース・ユーザーが内部データベースおよびスキーマをスキャンするための十分な特権を持っていることを確認してください。特権が不十分であると、予期しない分類ポリシー・エラーが発生することがあります。 includeInternalTables パラメーターの影響を受けるデータベースおよびスキーマを表示および編集するには、「グループ・ビルダー」を使用して、事前定義の「除外する分類 (Excluded Classification)」グループのいずれかを編集します。
policyName	必須。文字列
processName	必須。文字列
sampleSize	整数
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_classifier_process  datasourceNames=sample_cls_0001 policyName=APITEST_Cls_Ply_10001_1
processName=APITEST_Clps_10001_1
```

create_classifier_rule

表 5. create_classifier_rule

パラメーター	記述
policyName	必須。文字列
ruleName	必須。文字列

パラメーター	記述
ruleType	必須。文字列 参照用に、関連付けられている必須パラメーターを持つ有効なルール・タイプのリストを以下に示します。 ルール・タイプに選択する内容に応じて、必須パラメーターが決まります。 catalog_search_add policyName - 文字列 - 必須 ruleName - 文字列 - 必須 search_by_permissions_add policyName - 文字列 - 必須 ruleName - 文字列 - 必須 grantTypes - 文字列 - 必須 search_for_data_add policyName - 文字列 - 必須 ruleName - 文字列 - 必須 search_for_unstructured_data_add policyName - 文字列 - 必須 ruleName - 文字列 - 必須
category	文字列
classification	文字列
continueOnMatch	ブール値
description	文字列
columnNameLike	文字列
fireOnlyWithMarker	文字列
tableNameLike	文字列
tableTypeSynonym	ブール値
tableTypeSystemTable	ブール値
tableTypeTable	ブール値
tableTypeView	ブール値
grantTypes	文字列
role	文字列
roleGroup	文字列
user	文字列
userGroup	文字列
withAdminOption	ブール値
compareToValuesInGroup	文字列
compareToValuesInSQL	文字列
dataTypes	文字列
evaluationName	文字列
hitPercentage	整数
maxLength	整数
minLength	整数
searchExpression	文字列
searchLike	文字列
grantTypes	文字列
showUniqueValues	True または False
uniqueValueMask	値

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=CATALOG_SEARCH continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
tableNameLike=t1
columnNameLike=c1 fireOnlyWithMarker=m1

grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_BY_PERMISSIONS continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
user=user1
userGroup="suspicious users" role=role1 roleGroup=-role1 withAdminOption=1 grantTypes=CONTROL,DELETE,DROP fireOnlyWithMarker=m1

grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_DATA continueOnMatch=1 tableTypeSynonym=1 tableNameLike=tl1 dataTypes=DATE,NUMBER,TEXT columnNameLike=cl1
minLength=11 searchLike=sel1 searchExpression=se1 evaluationName=en1 hitPercentage=44 compareToValuesInSQL=cv1sql
compareToValuesInGroup="dw all objects" fireOnlyWithMarker=m1

grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_UNSTRUCTURED_DATA continueOnMatch=1 searchLike=s1 searchExpression=e1 fireOnlyWithMarker=m1

grdapi create_datasource type="Oracle (DataDirect)" user=scott password=tiger host="swan.guard.swg.usma.ibm.com"
name="Swan Oracle8 all values" shared=true owner=admin application=Classifier port=1521 serviceName=on8swan0

grdapi create_group appid=Classifier type=OBJECTS desc="AA Classifier ALL Values" owner=admin category=classifier
classification=classifier subtype=classifier

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=ACCOUNTING

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=ACCOUNTTING

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=ACCOUNTTING

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=AG

grdapi create_classifier_policy policyName="Search ALL DATA SEARCH smoke values" category="ALL" classification="ALL"

grdapi create_classifier_rule policyName="Search ALL DATA SEARCH smoke values" category="ALL" classification=ALL
ruleName=ALL1 ruleType=SEARCH_FOR_DATA dataTypes=TEXT,NUMBER continueOnMatch=1 tableNameLike="DEPT14%" minLength=1 maxLength=100
tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeTable=1 tableTypeView=1 fireOnlyWithMarker=ACCT searchLike="A%"
searchExpression="^AA*" columnNameLike="DNAME" evaluationName="com.guardium.classifier.custom.RichardEvaluation" hitPercentage=10
compareToValuesInGroup="AA Classifier ALL Values" compareToValuesInSQL="select DNAME from SCOTT.DEPT where DNAME like 'A%G'"
showUniqueValues="true" uniqueValueMask="^AA*"

grdapi create_classifier_process policyName="Search ALL DATA SEARCH smoke values"
processName="Search ALL DATA SEARCH smoke values Process" datasourceNames="Swan Oracle8 all values"
```

delete_classifier_action

表 6. delete_classifier_action

パラメーター	記述
actionName	必須。文字列
policyName	必須。文字列

例

```
grdapi delete_classifier_action policyName=-policy1 ruleName=-rule1 actionName=-action1
```

delete_classifier_policy

表 7. delete_classifier_policy

パラメーター	記述
policyName	必須。文字列

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_classifier_policy policyName=-policy1
```

delete_classifier_process

表 8. list_classifier_process

パラメーター	記述
processName	文字列
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_classifier_process processName=APITEST_Clps_10001_1
```

delete_classifier_rule

表 9. delete_classifier_rule

パラメーター	記述
policyName	必須。文字列
ruleName	必須。文字列
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_classifier_rule policyName=-policy1 ruleName=-rule1
```

execute_cls_process

分類プロセスの実行 (サブミット)

分類プロセスを実行します。 分類プロセス・ビルダーから「今すぐ 1 回実行」を実行することに相当します。 これは、Guardium® ジョブ・キューにプロセスを配置するジョブをサブミットします。このキューからアプライアンスは一度に 1 つのジョブを実行します。 管理者は、「Guardium モニター」>「Guardium ジョブ・キュー」と選択することによりジョブ状況を表示できます。

注: この API を呼び出す前に分類プロセスを作成してください。

表 10. execute_cls_process

パラメーター	記述
processName	分類プロセスの名前

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_cls_process processName="classPolicy1"
```

以下は、分類関数およびその各パラメーターのリストです。 パラメーターに有効な項目の設定リストがある場合、このリストが提供されます。

list_classifier_policies

表 11. list_classifier_policies

パラメーター	記述
policyName	必須。文字列
ruleName	必須。文字列
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_classifier_policy policyName=-policy1 ruleName=-rule1 actionName=-action1 recursive=1
```

注: 引数を指定せずにこの関数を実行すると、すべてのポリシーがリストされます。 ポリシーの引数を渡すと、そのポリシーのすべてのルールおよびアクションがリストされます。 ポリシーとルールを渡すと、そのルールのすべてのアクションがリストされます。

list_classifier_process

表 12. list_classifier_process

パラメーター	記述
processName	文字列
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi list_classifier_process processName=APITEST_CLPS_30001

set_classification_concurrency_limit

set_classification_concurrency_limit コマンドは、同時に実行できる分類プロセスの数を定義します。

構文: grdapi set_classification_concurrency_limit limit=[value].

表 13. set_classification_concurrency_limit パラメーター

パラメーター	値	記述
limit	整数: Guardium システムのハードウェア構成に応じて、1-100 になります。 デフォルト値は 1 です。	limit 値は、同時に実行できる分類プロセスの数を定義します。limit 値は、100 よりも小さいか、Guardium システムにインストールされている CPU コアの 2 倍の数になります。 例えば、システムに 8 つの CPU コアがある場合、limit の最大値は 16 です。システムに 64 個の CPU コアがある場合、limit の最大値は 100 です。 limit のデフォルト値は 1 です。

例:

```
grdapi set_classification_concurrency_limit limit=11
```

値の表示: grdapi get_classification_concurrency_limit

update_classifier_action

表 14. update_classifier_action

パラメーター	記述
actionName	必須。文字列
actualMemberContent	必須。文字列
description	文字列
objectGroup	必須。文字列
policyName	必須。文字列
ruleName	必須。文字列
replaceGroupContent	ブール値
objectFieldGroup	必須。文字列
accessPolicy	必須。文字列
accessRuleAction	必須。文字列
commandsGroup	文字列
includeField	ブール値
includeServerIP	ブール値
receiver	文字列
privacySet	必須。文字列
severity	文字列
notificationType	文字列
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi update_classifier_action actionType=add_to_group_objects policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc objectGroup="DW All Objects" replaceGroupContent=1 actualMemberContent=%FULLLIKE

grdapi update_classifier_action actionType=add_to_group_object_fields policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc objectFieldGroup="DW All Object-Field" replaceGroupContent=1

grdapi update_classifier_action actionType=update_access_rule policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc accessPolicy=pci accessRuleAction="alert daily" commandsGroup="Select command" includeField=1 includeServerIP=0
receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"

grdapi update_classifier_action actionType=update_privacy_set policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc privacySet=-b

grdapi update_classifier_action actionType=log_policy_violation policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc severity=MED

grdapi update_classifier_action actionType=send_alert policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc notificationType=High receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"
```

update_classifier_policy

表 15. update_classifier_policy

パラメーター	記述
policyName	必須。文字列
category	必須。文字列
classification	必須。文字列
description	文字列
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi update_classifier_policy policyName=-policy1 classification=class1 description=desc1 category=cat1
```

update_classifier_process

update_classifier_process

表 16. update_classifier_process

パラメーター	記述
comprehensive	ブール値
datasourceNames	必須。文字列
includeInternalTables	ブール値。この設定は、デフォルトでは使用不可になっています。 includeInternalTables を使用可能にすると、データベース・ソフトウェア・プロバイダーが使用する内部システム・データベースおよびスキーマをスキャンできることを示します。内部システム・データベースおよびスキーマは、機密データを含む可能性が低く、デフォルトではスキャンされません。内部表を組み込む場合は、分類データ・ソース・ユーザーが内部データベースおよびスキーマをスキャンするための十分な特権を持っていることを確認してください。特権が不十分であると、予期しない分類ポリシー・エラーが発生することがあります。 includeInternalTables パラメーターの影響を受けるデータベースおよびスキーマを表示および編集するには、「グループ・ビルダー」を使用して、事前定義の「除外する分類 (Excluded Classification)」グループのいずれかを編集します。
newName	文字列
policyName	必須。文字列
processName	必須。文字列
sampleSize	整数
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi update_classifier_process datasourceNames=sample_cls_0001,sample_cls_0002 policyName=APITEST_Cls_Ply_10001_1 processName=APITEST_Clps_10001_1 comprehensive=0 sampleSize=3000

update_classifier_rule

表 17. update_classifier_rule

パラメーター	記述
policyName	必須。文字列
ruleName	必須。文字列

パラメーター	記述
ruleType	必須。文字列 値 - catalog_search search_by_permissions search_for_data search_for_unstructured_data
category	文字列
classification	文字列
continueOnMatch	ブール値
description	文字列
columnNameLike	文字列
fireOnlyWithMarker	文字列
tableNameLike	文字列
tableTypeSynonym	ブール値
tableTypeSystemTable	ブール値
tableTypeTable	ブール値
tableTypeView	ブール値
grantTypes	文字列
role	文字列
roleGroup	文字列
user	文字列
userGroup	文字列
withAdminOption	ブール値
compareToValuesInGroup	文字列
compareToValuesInSQL	文字列
dataTypes	文字列
evaluationName	文字列
hitPercentage	整数
maxLength	整数
minLength	整数
searchExpression	文字列
searchLike	文字列
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=CATALOG_SEARCH continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
tableNameLike=t1
columnNameLike=c1 fireOnlyWithMarker=m1

grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_BY_PERMISSIONS continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
user=user1
userGroup="suspicious users" role=role1 roleGroup=-role1 withAdminOption=1 grantTypes=CONTROL,DELETE,DROP fireOnlyWithMarker=m1

grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_DATA continueOnMatch=1 tableTypeSynonym=1 tableNameLike=tl1 dataTypes=DATE,NUMBER,TEXT columnNameLike=cl1
minLength=11
maxLength=22 searchLike=sel1 searchExpression=se1 evaluationName=en1 hitPercentage=44 compareToValuesInSQL=cv1sql
compareToValuesInGroup="dw all objects" fireOnlyWithMarker=m1

grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_UNSTRUCTURED_DATA continueOnMatch=1 searchLike=s1 searchExpression=e1 fireOnlyWithMarker=m1
```

GuardAPI クラウド・データ・ソース関数

このコマンドを使用して、クラウド・データ・ソースを定義します。

create_cloud_datasource

パラメーター	値のタイプ	記述
application	文字列。説明を参照	必須。データ・ソースの定義対象のアプリケーション。次のいずれかです。 アクセス・ポリシー アプリケーション・ユーザー・トランスレーション 監査タスク 変更監査システム Classifier カスタム・ドメイン データベース・アナライザー 値のモニター セキュリティー・アセスメント S-TAP 検査
cloudTitle	文字列。説明を参照	必須。Guardium で既に定義されているクラウド・アカウントの名前
compatibilityMode	文字列	表のモニター時に使用されるモード。
conProperty	文字列	オプション。 このデータ・ソースとの JDBC 接続を確立するために JDBC URL に追加の接続プロパティーを含める必要がある場合にのみ使用します。 使用するフォーマットは、「property=value」である必要があります。このとき、プロパティーと値の各ペアはコンマで区切ります。
customURL	文字列	オプション。 データ・ソースに対する接続文字列。これを入力しない場合は、前回入力したフィールドのホスト、ポート、インスタンス、プロパティーなどを使用して接続が行われます。これは、例えば Oracle Internet Directory (OID) の接続を作成するときに便利です。
dbInstanceAccount	文字列	オプション。CAS によって使用されるデータベース・アカウント・ログイン名
dbInstanceDirectory	文字列	オプション。CAS によって使用される、データベース・ソフトウェアがインストールされたディレクトリー
dbName	文字列	オプション。Db2® データ・ソースまたは Oracle データ・ソースの場合、スキーマ名を入力します。他の場合は、データベース名を入力します。
description	文字列	オプション。データ・ソースの詳細説明。
host	文字列	必須。ホスト名または IP アドレス。
importServerSSLcert	ブール値	
KerberosConfigName	文字列	オプション。Guardium システムで既に定義されている Kerberos 構成の名前。
name	文字列	必須。Guardium システム内のデータ・ソースに対する固有の名前
objectLimit	0、正の整数	必須。分類プロセスで見つかった機密オブジェクトで、監査対象オブジェクトに自動的に追加される最大数。デフォルトは 20 です。
password	文字列	ユーザーのパスワード。
port	整数	オプション。ポート番号。
primaryCollector	整数	クラウド・データベースから監査データを抽出するコレクター。
region	値のリスト	必須。
savePassword	ブール値	Guardium アプライアンス上の認証資格情報を保存して暗号化します。 (オンデマンドではなく) スケジュールされたタスクとして実行されるアプリケーションでデータ・ソースを定義する場合は、必須になります。yes に設定した場合は、ログイン名とパスワードが必須になります。
serviceName	文字列	オプション。Oracle、Informix®、Db2、および IBM® ISeries の場合は必須。Db2 データ・ソースにはデータベース名を入力し、それ以外にはサービス名を入力します。
severity	文字列 - 定数値リスト	オプション。データ・ソースの重大度分類 (あるいは影響レベル)。以下のいずれか。 低 なし 中 高

パラメーター	値のタイプ	記述
shared	文字列 - 定数値リスト	オプション。他のアプリケーションと共有するには **True** または **Share** に設定します。データ・ソースを他のユーザーと共有する場合は、GUI からロールを割り当てる必要があります。値は次のとおりです。 Share Not Shared True False
type	値のリスト	必須。データ・ソース・タイプを識別します。有効な値: Oracle (DataDirect - SID) Oracle (DataDirect - サービス名)
useKerberos	ブール値	オプション (ブール値)。Kerberos 認証を使用する場合は、yes に設定します。yes の場合は、KerberosConfigName を指定する必要があります。
useLDAP	ブール値	オプション (ブール値)。LDAP を使用する場合は、yes に設定します。
user	文字列	オプション。データ・ソースのユーザー。使用する場合、パスワードも使用する必要があります。
useSSL	ブール値	オプション (ブール値)。SSL 認証を使用する場合は、yes に設定します。

list_cloud_datasource_by_name

パラメーター	値のタイプ	記述
name	文字列	必須。Guardium で定義されているクラウド・データ・ソース。
api_target_host	文字列	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

restart_cloud_instance

指定したクラウド・インスタンスを再開します。

パラメーター	値のタイプ	記述
datasource_name	文字列	必須。Guardium で定義されているクラウド・データ・ソース。
api_target_host	文字列	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

update_cloud_datasource

クラウド・データ・ソース構成を更新します。

パラメーター	値のタイプ	記述
cloudTitle	文字列。定数値リスト	必須。GRDAPI コマンドで定義されたタイトル
conProperty	文字列	オプション。 このデータ・ソースとの JDBC 接続を確立するために JDBC URL に追加の接続プロパティーを含める必要がある場合にのみ使用します。 使用するフォーマットは、「property=value」である必要があります。このとき、プロパティーと値の各ペアはコンマで区切ります。
customURL	文字列	オプション。 データ・ソースに対する接続文字列。これを入力しない場合は、前回入力したフィールドのホスト、ポート、インスタンス、プロパティーなどを使用して接続が行われます。これは、例えば Oracle Internet Directory (OID) の接続を作成するときに便利です。
dbInstanceAccount	文字列	オプション。CAS によって使用されるデータベース・アカウント・ログイン名

パラメーター	値のタイプ	記述
dbInstanceDirectory	文字列	オプション。 CAS によって使用される、データベース・ソフトウェアがインストールされたディレクトリー
dbName	文字列	オプション。Db2® データ・ソースまたは Oracle データ・ソースの場合、スキーマ名を入力します。他の場合は、データベース名を入力します。
description	文字列	オプション。データ・ソースの詳細説明。
host	文字列	必須。ホスト名または IP アドレス。
importServerSSLcert	ブール値	
KerberosConfigName	文字列	Guardium システムで既に定義されている Kerberos 構成の名前。
name	文字列	必須。Guardium システム内のデータ・ソースに対する固有の名前
newName		
objectLimit	整数: 0 以上	必須。分類プロセスで見つかった機密オブジェクトで、監査対象オブジェクトに自動的に追加される最大数。
password		ユーザーのパスワード
port	整数	Guardium で定義されているクラウド・データ・ソース。
primaryCollector	整数	クラウド DB からデータを受信するコレクター
region	値のリスト	必須。
savePassword	ブール値	Guardium アプライアンス上の認証資格情報を保存して暗号化します。 (オンデマンドではなく) スケジュールされたタスクとして実行されるアプリケーションでデータ・ソースを定義する場合は、必須になります。yes に設定した場合は、ログイン名とパスワードが必須になります。
serviceName	文字列	オプション。Oracle、Informix®、Db2、および IBM® ISeries の場合は必須。Db2 データ・ソースにはデータベース名を入力し、それ以外にはサービス名を入力します。
severity	文字列 - 定数値リスト	オプション。データ・ソースの重大度分類 (あるいは影響レベル)。以下のいずれか。 低 なし 中 高
shared	文字列 - 定数値リスト	オプション。他のアプリケーションと共有するには **True** または **Share** に設定します。データ・ソースを他のユーザーと共有する場合は、GUI からロールを割り当てる必要があります。値は次のとおりです。 Share Not Shared True False
useKerberos	ブール値	オプション (ブール値)。Kerberos 認証を使用する場合は、yes に設定します。yes の場合は、KerberosConfigName を指定する必要があります。
useLDAP	ブール値	オプション (ブール値)。LDAP を使用する場合は、yes に設定します。
user	文字列	オプション。データ・ソースのユーザー。使用する場合、パスワードも使用する必要があります。
useSSL	ブール値	オプション (ブール値)。SSL 認証を使用する場合は、yes に設定します。

親トピック: GuardAPI リファレンス

GuardAPI データベース・ユーザー関数

これらの GuardAPI コマンドは、データベース・ユーザー・マッピングの保守、非資格情報スキャン、およびデバッグ・レベルの設定に使用します。

non_credential_scan

usersGroup に属する使用可能なデフォルト・ユーザーを見つけるために serversGroup 内のデータベースをスキャンするジョブを実行依頼できるようにする API。 実行依頼されたジョブは分類リスナーの下で実行され、分類/アセスメントのジョブ・キュー・レポートを使用してトラッキングできます。 実行依頼されたジョブをキャンセルする場合、分類/アセスメントのジョブ・キュー・レポートでジョブをダブルクリックし、「ジョブの停止」を選択します。

注: serversGroup 内のサーバーに到達できない場合、「スケジュールされたジョブの例外」タイプの例外が追加され、サーバーはスキャンされません。

表 1. non_credential_scan

パラメーター	記述
databaseType	必須。ORACLE、DB2®、SYBASE、MS SQL SERVER、MYSQL、TERADATA、POSTGRESQL、NETEZZA、IBM ISERIES、INFORMIX のいずれかでなければなりません。
serversGroup	必須。グループ・ビルダーで定義された、有効なサーバーのグループ (サーバー IP/インスタンス名/ポート) でなければなりません。

パラメーター	記述
usersGroup	必須。 グループ・ビルダーで定義された、有効なユーザーのグループ (データベース・ユーザー/データベース・パスワード) でなければなりません。グループ・ビルダーには、デフォルト・グループがあります。

例

```
grdapi non_credential_scan databaseType=ORACLE serversGroup=oracleServers usersGroup="ORACLE Default Users"
```

データベース・マッピングの保守

これらの API は、データベース・ユーザー (違反の原因となった SQL の起動者) とリアルタイム・アラート用 E メール・アドレス間のマッピングを保守するのに役立ちます。 起動者についての詳細は『アラート・アクション』を参照してください。

- create_db_user_mapping
- delete_db_user_mapping
- list_db_user_mapping

create_db_user_mapping

ワイルドカードの使用:

- 「delete」および「list」コマンドでは、4 つのすべてのパラメーターでワイルドカード (「%」) を使用できます。
- 「create」コマンドの場合には、次のようになります。
  - serverIp - ワイルドカードは有効です。IP アドレス・フォーマットの数値の代わりに「%」を指定できます
  - 192.168.2.% - 有効
  - 192.%.2.% - 有効
  - 192.% - 無効
- serviceName - ワイルドカード (%) を使用できます
- dbUserName - ワイルドカードは使用できません。「%」は有効ですが、記号「%」であると見なされます
- emailAddress - ワイルドカードは使用できません。「%」は有効ですが、記号「%」であると見なされます

表 2. create_db_user_mapping

パラメーター	記述
serverIp	必須 (IP アドレス)。IP アドレス A.B.C.D のフォーマットであることが必要です。
serviceName	必須 (任意の文字列)。サービス名を識別します。
dbUserName	必須 (任意の文字列)。データベース・ユーザー名を識別します。
emailAddress	必須 (任意の文字列で、「@」記号が必要)。E メール・アドレスを識別します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_db_user_mapping serverIp=192.168.1.104 serviceName=ora1 dbUserName=scott emailAddress=scott@oracle.com
```

delete_db_user_mapping

ワイルドカードの使用:

- 「delete」および「list」コマンドでは、4 つのすべてのパラメーターでワイルドカード (「%」) を使用できます。
- 「create」コマンドの場合には、次のようになります。
  - serverIp - ワイルドカードは有効です。IP アドレス・フォーマットの数値の代わりに「%」を指定できます
  - 192.168.2.% - 有効
  - 192.%.2.% - 有効
  - 192.% - 無効
- serviceName - ワイルドカード (%) を使用できます
- dbUserName - ワイルドカードは使用できません。「%」は有効ですが、記号「%」であると見なされます
- emailAddress - ワイルドカードは使用できません。「%」は有効ですが、記号「%」であると見なされます

表 3. delete_db_user_mapping

パラメーター	記述
serverIp	必須 (IP アドレス)。IP アドレス A.B.C.D のフォーマットであることが必要です。
serviceName	必須 (任意の文字列)。サービス名を識別します。
dbUserName	必須 (任意の文字列)。データベース・ユーザー名を識別します。

パラメーター	記述
emailAddress	必須 (任意の文字列で、「@」記号が必要)。E メール・アドレスを識別します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_db_user_mapping serverIp=192.168.1.104 serviceName=ora1 dbUserName=scott emailAddress=scott@oracle.com
```

list_db_user_mapping

ワイルドカードの使用:

- 「delete」および「list」コマンドでは、4 つのすべてのパラメーターでワイルドカード (「%」) を使用できます。
- 「create」コマンドの場合には、次のようになります。
  - serverIp - ワイルドカードは有効です。IP アドレス・フォーマットの数値の代わりに「%」を指定できます
  - 192.168.2.% - 有効
  - 192.%.2.% - 有効
  - 192.% - 無効
- serviceName - ワイルドカード (%) を使用できます
- dbUserName - ワイルドカードは使用できません。「%」は有効ですが、記号「%」であると見なされます
- emailAddress - ワイルドカードは使用できません。「%」は有効ですが、記号「%」であると見なされます

表 4. list_db_user_mapping

パラメーター	記述
serverIp	必須 (IP アドレス)。IP アドレス A.B.C.D のフォーマットであることが必要です。
serviceName	必須 (任意の文字列)。サービス名を識別します。
dbUserName	必須 (任意の文字列)。データベース・ユーザー名を識別します。
emailAddress	必須 (任意の文字列で、「@」記号が必要)。E メール・アドレスを識別します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_db_user_mapping serverIp=192.168.1.104 serviceName=ora1 dbUserName=scott emailAddress=scott@oracle.com
```

デバッグ・レベルの取得

この GuardAPI コマンドは、IMS™ 出力のデバッグ・レベルを表示するために使用します。

set_debug_level

この GuardAPI コマンドは、IMS 出力を制御するために使用します。

IMS debug_level = 1 の場合、IMS デバッグ・フィールド (mvs_is_plex、mvs_ipaddr、mvs_dlta_sign、mvs_dlta_val など) が内部データベース表 (GDM_CONSTRUCT_TEXT.FULL_SQL または GDM_EXCEPTION.FULL_SQL) に出力されます。IMS デバッグ・レベルが 0 の場合、IMS デバッグ・フィールドは配布されません。

親トピック: GuardAPI リファレンス

GuardAPI データ・ソース関数

これらの GuardAPI コマンドは、データ・ソース関数の作成、リスト、削除、および更新に使用します。

create_datasource

このコマンドは、新規データ・ソースを定義するために使用します。

注: 中央マネージャー環境では、データ・ソースは中央マネージャー上で定義します。 GuardAPI を使用して管理対象ユニットにデータ・ソースを作成することはできますが、それらデータ・ソースを表示または使用することはできません。

クラウド・データ・ソースを作成するには、GuardAPI クラウド・データ・ソース関数を参照してください。

表 1. create_datasource

パラメーター	記述
application	必須。 データ・ソースの定義対象となるアプリケーションを指定します。 次のいずれかでなければなりません。 Access_policy アプリケーション・ユーザー・トランスレーション AuditDatabase AuditTask ChangeAuditSystem Classifier CustomDomain DatabaseAnalyzer MonitorValues SecurityAssessment Stap_Verification
compatibilityMode	互換モード: 選択項目は「デフォルト」と「MSSQL 2000」です。表のモニター時に使用する互換モードをプロセッサーに指示します。
conProperty	オプション。 このデータ・ソースとの JDBC 接続を確立するために JDBC URL に追加の接続プロパティーを含める必要がある場合にのみ使用します。 使用するフォーマットは、「property=value」である必要があります。このとき、プロパティーと値の各ペアはコンマで区切ります。 Roman8 をデフォルトの文字セットとする Sybase データベースの場合、次のプロパティーを入力します。 charSet=utf8
customURL	オプション。 データ・ソースに対する接続文字列。これを入力しない場合は、前回入力したフィールドのホスト、ポート、インスタンス、プロパティーなどを使用して接続が行われます。 これは、例えば Oracle Internet Directory (OID) の接続を作成するときに便利です。
dbInstanceAccount	オプション。 CAS によって使用されるデータベース・アカウント・ログイン名
dbInstanceDirectory	オプション。 CAS によって使用される、データベース・ソフトウェアがインストールされたディレクトリー
dbName	オプション。 DB2® または Oracle データ・ソースの場合、スキーマ名を入力します。他の場合は、データベース名を入力します。
description	オプション。データ・ソースの詳細説明。
host	必須。 ホスト名または IP アドレスを入力できます。
KerberosConfigName	オプション。Guardium システムで既に定義されている Kerberos 構成の名前。
name	必須。 システム上のデータ・ソースに固有の名前を付けます。
password	オプション。ユーザーのパスワード。
port	オプション (整数)。ポート番号。
savePassword	Guardium アプライアンス上の認証資格情報を保存して暗号化します。 (オンデマンドではなく) スケジュールされたタスクとして実行されるアプリケーションでデータ・ソースを定義する場合は、必須になります。yes に設定した場合は、ログイン名とパスワードが必須になります。
serviceName	Oracle、Informix®、DB2、および IBM® ISeries の場合は必須。DB2 データ・ソースではデータベース名を入力します。それ以外ではサービス名を入力します。
severity	オプション。データ・ソースの重大度分類 (あるいは影響レベル)。
shared	オプション (ブール値)。他のアプリケーションと共有する場合は **true** に設定します。データ・ソースを他のユーザーと共有する場合は、GUI からロールを割り当てる必要があります。

パラメーター	記述
type	必須。データ・ソース・タイプを識別します。有効な値: DB2 DB2 for i Db2 for z/OS Informix MS SQL Server MS SQL サーバー (DataDirect) MySQL NA Netezza Oracle (DataDirect) Oracle (サービス名) Oracle (SID) PostgreSQL Sybase Sybase IQ Teradata アプリケーションが CustomDomain または Classifier である場合、以下も使用できます。 TEXT TEXT:FTP TEXT:HTTP TEXT:HTTPS TEXT:SAMBA
useKerberos	オプション (ブール値)。Kerberos 認証を使用する場合は、yes に設定します。yes の場合は、KerberosConfigName を指定する必要があります。
useLDAP	オプション (ブール値)。LDAP を使用する場合は、yes に設定します。
user	オプション。データ・ソースのユーザー。使用する場合、パスワードも使用する必要があります。
useSSL	オプション (ブール値)。SSL 認証を使用する場合は、yes に設定します。

例

```
grdapi create_datasource type=DB2 name=chickenDB2  password=guardium user=db2inst1 dbName=dn0chick application=Access_policy
shared=true port=50000 host=chicken.corp.com
```

create_test_exception

このコマンドは、テスト例外にレコードを追加するために使用します。 これは、脆弱性評価の動作に影響を及ぼします。 特定のデータ・ソースのテストが不合格となった場合、該当テスト/データ・ソースのテスト例外表の最終レコードが検査されます。このとき実行日付が最終レコードの開始日付と終了日付の間であれば、テストは PASS に設定され、推奨事項が (例外レコードから) 説明に対して設定されます。さらに結果テキストに次のように設定されます。

テストにパスしました。例外の承認者:　。有効期間　から　まで。

注: この API は例外を除去するためにレコードを追加するだけです。必要に応じて新しい日付で新しいレコードを作成してください。

表 2. create_test_exception

パラメーター	記述
datasourceName	必須。定義したデータ・ソースの有効な名前。
testDescription	必須。セキュリティー・アセスメント内で有効なテスト名。
fromDate	必須。例外が有効である場合の開始日付。
toDate	必須。例外が有効である場合の終了日付。
explanation	必須。 テストに合格する理由に関する推奨事項。

例

```
grdapi create_test_exception datasourceName=ORAPROD5 testDescription="CVE-2009-0997" fromDate="2012-07-01 08:00:00" toDate="2012-
07-31 08:00:00" explanation="Currently in testing stage"
```

list_datasource_by_name

名前で識別されるデータ・ソース定義を表示します。

表 3. list_datasource_by_name

パラメーター	記述
name	必須。データ・ソース名。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
CLI> grdapi list_datasource_by_name name=chickenDB2
ID=20000
Datasource DatasourceId=20000
Datasource DatasourceTypeId=2
Datasource Name=chickenDB2
Datasource Description=null
Datasource Host=chicken.corp.com
Datasource Port=50000
Datasource ServiceName=
Datasource UserName=db2inst1
Datasource Password=[B@1415de6
Datasource PasswordStored=true
Datasource DbName=dn0chick
Datasource LastConnect=null
Datasource Timestamp=2008-04-18 15:40:58.0
Datasource ApplicationId=2
Datasource Shared=true
Datasource ConProperty=null
Datasource type =DB2
Application Type = Access_policy
ok
```

list_datasource_by_id

ID キーで識別されるデータ・ソース定義を表示します。

表 4. list_datasource_by_id

パラメーター	記述
id	必須 (整数)。リストするデータ・ソースの ID 番号を入力します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_datasource_by_id id=2
```

delete_datasource_by_name

データ・ソースがアプリケーションで使用されているのでない限り、指定したデータ・ソース定義を削除します。 この関数は、作成者に関係なくデータ・ソースを削除します。

表 5. delete_datasource_by_name

パラメーター	記述
name	必須。データ・ソース名。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_datasource_by_name name=swanSybase
```

delete_datasource_by_id

データ・ソースがアプリケーションで使用されているのでない限り、指定したデータ・ソース定義を削除します。 この関数は、作成者に関係なくデータ・ソースを削除します。

表 6. delete_datasource_by_id

パラメーター	記述
id	必須 (整数)。リストするデータ・ソースの ID 番号を入力します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_datasource_by_id id=2
```

update_datasource_by_name

データ・ソース定義を更新します。

表 7. update_datasource_by_name

パラメーター	記述
name	必須。更新するデータ・ソースを指定します。
newName	オプション。 新規名を指定します。これはシステム上のデータ・ソースで固有でなければなりません。
description	オプション。データ・ソースの詳細説明。
host	オプション。 ホスト名または IP アドレスを入力できます。
port	オプション (整数)。ポート番号。
savePassword	Guardium アプライアンス上の認証資格情報を保存して暗号化します。 (オンデマンドではなく) スケジュールされたタスクとして実行されるアプリケーションでデータ・ソースを定義する場合は、必須になります。yes に設定した場合は、ログイン名とパスワードが必須になります。
serviceName	オプション。 Oracle データ・ソースの場合、サービス名を入力します。
user	オプション。データ・ソースのユーザー。使用する場合、パスワードも使用する必要があります。
password	オプション。ユーザーのパスワード。使用する場合、ユーザーも使用する必要があります。
dbName	オプション。DB2 データ・ソースの場合、データベース名を入力します。
conProperty	オプション。 このデータ・ソースとの JDBC 接続を確立するために JDBC URL に追加の接続プロパティーを含める必要がある場合にのみ使用します。 使用するフォーマットは、「property=value」である必要があります。このとき、プロパティーと値の各ペアはコンマで区切ります。 Roman8 をデフォルトの文字セットとする Sybase データベースの場合、次のプロパティーを入力します。 CHARSET=utf8
dbInstanceAccount	オプション。 CAS によって使用されるデータベース・アカウント・ログイン名

パラメーター	記述
dbInstanceDirectory	オプション。 CAS によって使用される、データベース・ソフトウェアがインストールされたディレクトリー
shared	オプション (ブール値)。他のアプリケーションと共有する場合は **true** に設定します。データ・ソースを他のユーザーと共有する場合は、GUI からロールを割り当てる必要があります。
customURL	オプション。 データ・ソースに対する接続文字列。これを入力しない場合は、前回入力したフィールドのホスト、ポート、インスタンス、プロパティーなどを使用して接続が行われます。 これは、例えば Oracle Internet Directory (OID) の接続を作成するときに便利です。
severity	オプション。データ・ソースの重大度分類 (あるいは影響レベル)。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。
useKerberos	オプション (ブール値)。Kerberos 認証を使用する場合は、yes に設定します。yes の場合は、KerberosConfigName を指定する必要があります。
useLDAP	オプション (ブール値)。LDAP を使用する場合は、yes に設定します。
useSSL	オプション (ブール値)。SSL 認証を使用する場合は、yes に設定します。

例

```
grdapi update_datasource_by_name name=chickenDB2  newName="chicken DB2" user=" " password=" "
```

update_datasource_by_id

データ・ソース定義を更新します。

表 8. update_datasource_by_id

パラメーター	記述
id	必須 (整数)。データ・ソースを指定します。
newName	オプション。 新規名を指定します。これはシステム上のデータ・ソースで固有でなければなりません。
description	オプション。データ・ソースの詳細説明。
host	オプション。 ホスト名または IP アドレスを入力できます。
port	オプション (整数)。ポート番号。
savePassword	Guardium アプライアンス上の認証資格情報を保存して暗号化します。 (オンデマンドではなく) スケジュールされたタスクとして実行されるアプリケーションでデータ・ソースを定義する場合は、必須になります。yes に設定した場合は、ログイン名とパスワードが必須になります。
serviceName	オプション。 Oracle データ・ソースの場合、サービス名を入力します。
user	オプション。データ・ソースのユーザー。使用する場合、パスワードも使用する必要があります。
password	オプション。ユーザーのパスワード。使用する場合、ユーザーも使用する必要があります。
dbName	オプション。DB2 データ・ソースの場合、データベース名を入力します。
conProperty	オプション。 このデータ・ソースとの JDBC 接続を確立するために JDBC URL に追加の接続プロパティーを含める必要がある場合にのみ使用します。 使用するフォーマットは、「property=value」である必要があります。このとき、プロパティーと値の各ペアはコンマで区切ります。 Roman8 をデフォルトの文字セットとする Sybase データベースの場合、次のプロパティーを入力します。 CHARSET=utf8
dbInstanceAccount	オプション。 CAS によって使用されるデータベース・アカウント・ログイン名
dbInstanceDirectory	オプション。 CAS によって使用される、データベース・ソフトウェアがインストールされたディレクトリー
shared	オプション (ブール値)。他のアプリケーションと共有する場合は **true** に設定します。データ・ソースを他のユーザーと共有する場合は、GUI からロールを割り当てる必要があります。
customURL	オプション。 データ・ソースに対する接続文字列。これを入力しない場合は、前回入力したフィールドのホスト、ポート、インスタンス、プロパティーなどを使用して接続が行われます。 これは、例えば Oracle Internet Directory (OID) の接続を作成するときに便利です。
severity	オプション。データ・ソースの重大度分類 (あるいは影響レベル)。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。
useKerberos	オプション (ブール値)。Kerberos 認証を使用する場合は、yes に設定します。yes の場合は、KerberosConfigName を指定する必要があります。
useLDAP	オプション (ブール値)。LDAP を使用する場合は、yes に設定します。
useSSL	オプション (ブール値)。SSL 認証を使用する場合は、yes に設定します。

例

```
grdapi update_datasource_by_id id=20000 user=" " password=" " newName="chickenDB2hooo"
```

list_db_drivers

現在データ・ソース・タイプとして Oracle (DataDirect) および MS SQL サーバー (DataDirect) をサポートしている データベース・ドライバーの名前のみをリストします。

list_db_drivers_by_details

各データベース・ドライバーの詳細 (名前、クラス、ドライバー・クラス、URL、およびデータ・ソース・タイプ ID) をリストします。

親トピック: GuardAPI リファレンス

GuardAPI データ・ソース・リファレンス関数

これらの GuardAPI コマンドは、データ・ソース・リファレンス関数の作成、リスト、および削除に使用します。

create_datasourceRef_by_id

特定のアプリケーション・タイプ (特定の分類プロセスなど) の特定のオブジェクトに対して、データ・ソースへの参照を作成します。

表 1. create_datasourceRef_by_id

パラメーター	記述
appId	必須 (整数)。アプリケーションを識別します。このリストのいずれかである必要があります。 • 8 = SecurityAssessment • 47 = CustomTables • 51 = Classifier
datasourceId	必須 (整数)。データ・ソースを (データ・ソース定義から) 識別します。
objId	必須 (整数)。指定された appID タイプのインスタンスを識別します。例えば、apID=51 である場合、これは分類プロセスの ID になります。

例

```
grdapi create_datasourceRef_by_id appId=51 datasourceId=20000 objId=2
```

create_datasourceRef_by_name

特定のアプリケーション・タイプ (特定の分類プロセスなど) の特定のオブジェクトに対して、データ・ソースへの参照を作成します。

表 2. create_datasourceRef_by_name

パラメーター	記述
application	必須。アプリケーションを識別します。このリストのいずれかである必要があります。 SecurityAssessment CustomTables Classifier
datasourceName	必須。データ・ソースを (データ・ソース定義から) 識別します。
objName	必須。指定されたアプリケーション・タイプのインスタンスを識別します。アプリケーションが Classifier である場合、これは特定の分類プロセスの名前になります。

例

```
grdapi  create_datasourceRef_by_name  application=Classifier  datasourceName=swanSybase  objName="class process1"
```

list_datasourceRef_by_id

特定のアプリケーション・タイプ (特定の分類プロセスなど) の特定のオブジェクトに対して、参照されるすべてのデータ・ソースをリストします。

表 3. list_datasourceRef_by_id

パラメーター	記述
appID	必須 (整数)。アプリケーションを識別します。このリストのいずれかである必要があります。 8 = SecurityAssessment 47 = CustomTables 51 = Classifier
objID	必須。指定されたアプリケーション・タイプのインスタンスを識別します。 例えば、アプリケーションが Classifier である場合、これは特定の分類プロセスの ID になります。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_datasourceRef_by_id appId=13 objId=1
```

list_datasourceRef_by_name

特定のアプリケーション・タイプ (特定の分類プロセスなど) の特定のオブジェクトに対して、参照されるすべてのデータ・ソースをリストします。

表 4. list_datasourceRef_by_name

パラメーター	記述
application	必須。アプリケーションを識別します。このリストのいずれかである必要があります。 SecurityAssessment CustomTables Classifier
objName	必須。指定されたアプリケーション・タイプのインスタンスを識別します。アプリケーションが Classifier である場合、これは特定の分類プロセスの名前になります。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdap list_datasourceRef_by_name application=Classifier  objName="class process1"
```

delete_datasourceRef_by_id

特定のアプリケーション・タイプ (特定の分類プロセスなど) の特定のオブジェクトに対して、データ・ソース参照を削除します。

表 5. delete_datasourceRef_by_id

パラメーター	記述

パラメーター	記述
appId	必須 (整数)。アプリケーションを識別します。このリストのいずれかである必要があります。 8 = SecurityAssessment 47 = CustomTables 51 = Classifier
datasourceId	必須 (整数)。データ・ソースを (データ・ソース定義から) 識別します。
objId	必須 (整数)。指定された appID タイプのインスタンスを識別します。例えば、apID=51 である場合、これは分類プロセスの ID になります。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_datasourceRef_by_id appId=51 datasourceId=2 objId=1
```

delete_datasourceRef_by_name

特定のアプリケーション・タイプ (特定の分類プロセスなど) の特定のオブジェクトに対して、データ・ソース参照を削除します。

表 6. delete_datasourceRef_by_name

パラメーター	記述
application	必須。アプリケーションを識別します。このリストのいずれかである必要があります。 SecurityAssessment CustomTables Classifier
datasourceName	必須。データ・ソースを (データ・ソース定義から) 識別します。
objName	必須。指定されたアプリケーション・タイプのインスタンスを識別します。アプリケーションが Classifier である場合、これは特定の分類プロセスの名前になります。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_datasourceRef_by_name application=Classifier datasourceName=swanSybase objName="class process1"
```

親トピック: GuardAPI リファレンス

GuardAPI データ・ユーザー・セキュリティー関数

以下の GuardAPI コマンドは、データ・ユーザー・セキュリティー関数を作成、リスト、削除、および更新するために使用します。

create_user_hierarchy

ユーザー・データ・セキュリティー階層にユーザーと親の関係を追加します。

表 1. create_user_hierarchy

パラメーター	記述

パラメーター	記述
userName	必須。ユーザーの名前。
parentUserName	必須。親ユーザーの名前。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi create_user_hierarchy userName=admin parentUserName=accessmgr

注: 循環的な挿入 (親レポートが子に挿入される) の場合、エラーとなります。

list_user_hierarchy_by_parent_user

ユーザー・データ・セキュリティー階層内の関係をリストします。

表 2. list_user_hierarchy_by_parent_user

パラメーター	記述
userName	必須。ユーザーの名前。
create	create_user_hierarchy API 呼び出しの create ステートメントを、true を設定すると作成し、false を設定すると生成しません。 このパラメーターは、バッチ・ファイルの生成に必要なすべてのコマンドを取得するときに使用します。 このバッチ・ファイルは、親と子のそれぞれの対を別の Guardium® システムに移動するときに使用できます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi list_user_hierarchy_by_parent_user userName=admin create=true

注: 直接的な親子関係のみがリスト表示されます。「孫」は表示されません。

delete_user_hierarchy_by_entry_id

項目 ID ごとにユーザー・データ・セキュリティー階層にある関係を削除します。

表 3. delete_user_hierarchy_by_entry_id

パラメーター	記述
id	必須 (整数)。項目を指定します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi delete_user_hierarchy_by_entry_id id=1

注: 項目が存在しない場合、失敗条件はありません。

delete_user_hierarchy_by_user

ユーザー・データ・セキュリティー階層にある関係をユーザーごとに削除します。

表 4. delete_user_hierarchy_by_user

パラメーター	記述
userName	必須。 ユーザーの名前。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi delete_user_hierarchy_by_user userName=admin

注:

ユーザーが存在しない場合、失敗条件はありません。

ユーザーが複数の親を持つ場合、削除が複数回行われます。

create_allowed_db

ユーザーとデータベースの関連を作成します。

表 5. create_allowed_db

パラメーター	記述
userName	必須。ユーザーの名前。
serverIp	必須。サーバー IP
instanceName	必須。インスタンス名
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi create_allowed_db userName=admin serverIp=192.168.1.1 instanceName=abcd

list_allowed_db_by_user

ユーザーとデータベースの関連をユーザーごとにリストします。

表 6. list_allowed_db_by_user

パラメーター	記述
userName	必須。ユーザーの名前。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi list_allowed_db_by_user userName=admin

delete_allowed_db_by_entry_id

ユーザーとデータベースの関連を項目 ID ごとに削除します。

表 7. delete_allowed_db_by_entry_id

パラメーター	記述
id	必須 (整数)。項目を指定します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi delete_allowed_db_by_entry_id id=1

delete_allowed_db_by_user

ユーザーとデータベースの関連をユーザーごとに削除します。

表 8. delete_allowed_db_by_user

パラメーター	記述
userName	必須。ユーザーの名前。
serverIp	サーバー IP。
instanceName	インスタンス名。 注: インスタンス名を「blank」にする場合、instanceName=[blank] と入力します (instanceName=blank ではありません)。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi delete_allowed_db_by_user userName=scott

update_user_db

アクティブなユーザー - DB 関連付けマップに最近のすべての変更を全面的に適用

表 9. update_user_db

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi update_user_db

注: 一元管理構成では、このコマンドは中央マネージャー上で実行してください。
親トピック: GuardAPI リファレンス

GuardAPI エンタープライズ・ロード・バランシング関数

以下の GuardAPI コマンドを使用して、ロード・バランシング・パラメーターの表示と設定、現在のロード・マップの表示、および S-TAP と管理対象ユニット・グループの関連付けの管理を行います。

get_load_balancer_load_map

現在のロード・マップを表示します。

```
grdapi get_load_balancer_load_map
```

get_load_balancer_params

現在のロード・バランサーの構成パラメーターを表示します。

```
grdapi get_load_balancer_params
```

set_load_balancer_param

ロード・バランサーの構成パラメーターを設定します。

```
grdapi set_load_balancer_param [paramName=value][paramValue=value][paramType=STAP]
```

使用可能なパラメーターおよび許可される値のリストについては、『エンタープライズ・ロード・バランシング構成パラメーター』を参照してください。

例えば、`grdapi set_load_balancer_params paramName=LOAD_BALANCER_ENABLED paramValue=0 paramType=STAP` です。

次の形式を使用して正しく入力します。

grdapi set_load_balancer_param --help=true

ID=0

関数パラメーター : paramName - 文字列 - 必須

paramType - 文字列 - 必須

paramValue - 文字列 - 必須

パラメーターの定数値リストを取得するには、関数に「--get_param_values」を指定して呼び出します。

assign_load_balancer_groups

管理対象ユニット・グループをアプリケーションまたは S-TAP グループに割り当てます。

```
grdapi assign_load_balancer_groups muGroupName=[value] appGroupName=[value]
```

パラメーター	値	記述
muGroupName	管理対象ユニット・グループ名	例えば、`muGroupName=mu_group_NA` です。
appGroupName	アプリケーションまたは `S-TAP` グループ名	例えば、`appGroupName=app_group_NA` です。
ifFailoverGroup	`1` または `0`	例えば、`isFailoverGroup=0` です。

unassign_load_balancer_groups

アプリケーションまたは S-TAP グループから管理対象ユニット・グループの割り当てを解除します。

```
grdapi unassign_load_balancer_groups muGroupName=[value] appGroupName=[value]
```

パラメーター	値	記述
muGroupName	管理対象ユニット・グループ名	例えば、muGroupName=mu_group_NA です。
appGroupName	アプリケーションまたは S-TAP グループ名	例えば、appGroupName=app_group_NA です。

親トピック: GuardAPI リファレンス

GuardAPI 資格最適化機能

これらの GuardAPI コマンドは、資格最適化データ・ソースおよびレポート作成を有効化および構成するために使用します。

enable_entitlement_optimization

このコレクターでの資格最適化機能を有効にします。

```
grdapi enable_entitlement_optimization
```

disable_entitlement_optimization

このコレクターでの資格最適化機能を無効にします。

```
grdapi disable_entitlement_optimization
```

add_datasource_to_entitlement_optimization

このソースから資格最適化データ収集にデータを追加し、指定されたとおりに個々のタブにデータを追加します。

```
grdapi add_datasource_to_entitlement_optimization
```

パラメーター	値	記述
datasourceName	datasourceName	データ・ソースの名前
isEnabled	true、false のいずれか	資格最適化に対して、データ・ソースが有効化または無効化されます。 デフォルトは false です。
userScope	1 つ以上のコンマ区切りの Guardium ユーザー・グループ ID (グループにはユーザーのみを含める必要があります)	オプション。「資格の推奨」の結果は、このユーザー・グループによってフィルタリングされます。「資格の参照」の結果は、 この範囲内にユーザーが含まれているかどうかを示し、範囲外のユーザーのユーザー・アクティビティー・カウントは表示しません。 デフォルトは NULL です。
objectScope	1 つ以上のコンマ区切りの Guardium オブジェクト・グループ ID (グループにはオブジェクトのみを含める必要があります)	オプション。「資格の推奨」の結果は、このオブジェクト・グループによってフィルタリングされます。 デフォルトは NULL です。
extractActivity	true、false のいずれか	データ・ソース・アクティビティーの抽出を有効または無効にします。 「資格の参照」および「仮定」の場合は、true である必要があります。 デフォルトは false です。
extractEntitlement	true、false のいずれか	資格データの抽出を有効または無効にします。 「新機能」、「ユーザーおよびロール」、「推奨」、および「資格の参照」の場合は、true である必要があります。 デフォルトは false です。
generateRoleClusters	true、false のいずれか	**「仮定」**タブで使用される、データ・ソースからの動作ロール・クラスタリングの抽出を有効または無効にします。 「仮定」の場合は、true である必要があります。 デフォルトは false です。
generateNews	true、false のいずれか	このデータ・ソースからのアクティビティーが**「新機能」**タブに含まれます。 デフォルトは false です。
generateRecommendations	true、false のいずれか	このデータ・ソースからのアクティビティーが**「推奨」**タブに含まれます。 デフォルトは false です。
filterTempObjects	true、false のいずれか	将来に使用の予定。 一時オブジェクトがデータ・ソースの収集データからフィルタリングされます。 デフォルトは true です。
filterIgnoreVerbs	true、false のいずれか	将来に使用の予定。 無視動詞がデータ・ソースの収集データからフィルタリングされます。 デフォルトは true です。

remove_datasource_from_entitlement_optimization

このソースからのすべてのデータを、資格最適化データ収集から削除します。

```
remove_datasource_from_entitlement_optimization
```

set_entitlement_datasource_parameter

資格の最適化に対して既に有効になっているデータ・ソースのパラメーターを変更します。add_datasource_to_entitlement_optimization と同じパラメーターを使用します。

```
grdapi set_entitlement_datasource_parameter
```

get_entitlement_datasource_parameter

このコレクターの各データ・ソースのパラメーター設定を表示します。

```
grdapi get_entitlement_datasource_parameter
```

例:

```
資格最適化は有効です
==================================
Datasource: SCALE-DB16
==================================
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
==================================
Datasource: on12scal
==================================
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
```

親トピック: GuardAPI リファレンス

GuardAPI 外部フィード関数

これらの GuardAPI 関数は、外部フィードのマッピングを作成するために使用します。

create_ef_mapping

この関数はマッピングを作成し、*reportName* パラメーターで指定されたレポートの名前に基づいて、表にデータを取り込みます。 各マッピングの名前は、EF_MAP_TYPE_HDR.EF_TYPE_DESC に保管されます。この名前は、*reportName* の値と同一になります。 ターゲット表名も、*reportName* パラメーターに基づきますが、単語間に下線が追加されます。例えば、「My Report」は MY_REPORT になります。

表 1.

パラメーター	記述
reportName	外部フィード・マッピングで使用するレポートの名前。このパラメーターは、マッピングの名前およびターゲット表名の決定も行います。

modify_ef_mapping

場合によっては、create_ef_mapping によって生成される名前が特定のデータベースに適さないことがあります。その場合、modify_ef_mapping を使用して、データベース要件に適合するように名前を調整できます。事前定義の Guardium マッピングを保護するため、変更できるマッピングは ID >= 20000 のマッピングのみです。

表 2.

パラメーター	記述
reportName	変更するマッピングの名前。
modifyObj	変更するデータベース・オブジェクト (*table* (表) または *column* (列)) を指定します。 既存の値は、list_ef_mapping 関数を使用して取得できます。
oldName	削除する古い表名を指定します。
newName	使用する新しい表名を指定します。

delete_ef_mapping

この関数を使用すると、既存のマッピングを削除できます。事前定義の Guardium マッピングを保護するため、削除できるマッピングは ID >= 20000 のマッピングのみです。

表 3.

パラメーター	記述
reportName	削除するマッピングの名前。

list_ef_mapping

パラメーターを指定せずに実行した場合、この関数は、お客様が作成したすべてのマッピングのリストを返します。*reportName* パラメーターを指定して実行した場合、この関数は、指定したマッピングの詳細 (外部フィードで使用される表名や列名など) を返します。

表 4.

パラメーター	記述
reportName	オプション。詳細を返すマッピングの名前。

親トピック: GuardAPI リファレンス

GuardAPI ファイル・アクティビティー・モニター関数

以下の GuardAPI コマンドは、ファイル・アクティビティー・モニターの有効化および無効化、ファイルの調査ダッシュボードのアクティビティーおよびライセンス抽出のスケジュールの構成、ファイル・アクティビティー・モニターに関する情報の取得を行う場合に使用します。

GuardAPI コマンドの grdapi create_policy を使用して FAM ポリシーを作成します。ポリシーを作成したら、FAM 固有の GuardAPI コマンドを使用します。

例:

grdapi create_policy ruleSetDesc='TEST'

grdapi create_fam_rule policyName='TEST' ruleName=r-test-sles11 actionName="Log As Violation and Audit" serverHost="9.70.144.98:FAM" filePath="/famtest/*"

GuardAPI コマンドの使用手順については、GuardAPI リファレンスを参照してください。

enable_fam_crawler

クローラー結果およびファイル・アクティビティー・データを処理するように Guardium システムを設定します。 結果は、クイック検索索引ファイルに自動的に追加されます。 各種パラメーターを使用して、ファイル・クイック検索アクティビティー、ライセンス抽出、およびリモート・グループへのデータ取り込みをスケジュールします。

注: 調査ダッシュボードも、コマンド grdapi enable_quick_search schedule_interval=1 を使用して有効にする必要があります。

表 1. enable_fam_crawler

パラメーター	記述
extraction_start	ファイル・クイック検索へのデータの抽出を開始する初回の日時。過去 2 日以内に制限されます。デフォルトは現在の時刻です。単位を HOUR に設定した場合、時間単位で丸められます。DAY に設定した場合、日単位で丸められます。
schedule_start	デフォルトは現在の時刻です。
activity_schedule_interval	必須。このパラメーターは、アクティビティー・スケジュール間隔を設定します。推奨間隔は、単位を MINUTE に設定した 2 です。
activity_schedule_units	必須。このパラメーターは、アクティビティー・ユニットの単位を設定します。値は MINUTE と HOUR のいずれかです。推奨単位は MINUTE です。
entitlement_schedule_interval	必須。このパラメーターは、ライセンス・スケジュール間隔を設定します。推奨間隔は、単位を DAY に設定した 1 です。
entitlement_schedule_units	必須。このパラメーターは、ライセンス・スケジュールの単位を設定します。指定可能な値は MINUTE、HOUR、および DAY です。 推奨単位は DAY です。

例

```
grdapi enable_fam_crawler extraction_start=< > schedule_start=< >
 activity_schedule_interval=2 activity_schedule_units=MINUTE
entitlement_schedule_interval=10 entitlement_schedule_units=MINUTE
```

disable_fam_crawler

ファイル・アクティビティー・モニターを無効にします。ファイル・クイック検索アクティビティーおよびライセンス抽出のスケジューラーが削除されます。この関数は、リモート・グループへのデータ取り込みも無効化します。

例

```
grdapi disable_fam_crawler
```

get_fam_crawler_info

ファイル・アクティビティー・モニターの状況を表示します。有効になっている場合、このコマンドにより、ライセンス抽出およびファイル・クイック検索アクティビティーのスケジュールの設定が表示されます。

```
FAM クローラー (サーバー・サイド) が無効になっています。
```

```
FAM クローラー (サーバー・サイド) が有効になっています。ライセンス (1 DAY) アクティビティー (2 MINUTE) (Entitlement(1 DAY) Activity(2 MINUTE))
```

例

```
grdapi get_fam_crawler_info
```

list_policy_fam_rule

FAM ポリシー内のすべてのルールをリストします。

パラメーター	記述
policyName	必須。文字列。ポリシー名
ruleName	オプション。文字列。ruleName が指定されていない場合、すべてのポリシー・ルールが詳細とともに表示されます。ruleName が指定されている場合、そのルールの詳細がリストされます。

create_fam_rule

新しい FAM ルールを作成します。

パラメーター	記述
policyName	必須。文字列。ポリシー名。
ruleName	必須。文字列。ルール名。
filePath	文字列。モニター対象のファイル・パス。filePath と filePathGroup のいずれかを指定する必要があります。
notfilePath	文字列。「はい」または「いいえ」にする必要があります。「はい」を指定すると、指定されているパス内のファイルを除くすべてのファイルにこのルールが適用されます。
filePathGroup	文字列。ファイル・パスのグループ。filePath と filePathGroup のいずれかを指定する必要があります。
includeSubDirectory	文字列。「はい」または「いいえ」にする必要があります。「はい」を指定した場合、すべてのサブディレクトリー内のファイルが含められます。
removableMedia	文字列。「はい」または「いいえ」にする必要があります。
osUser	文字列。OS ユーザー名。
osUserGroup	文字列。OS ユーザーのグループ。
notOSUser	文字列。「はい」または「いいえ」にする必要があります。「はい」を指定した場合、指定した osUser を除くすべてのユーザーが使用されます。
serverHost	文字列。ホスト名。
serverHostGroup	文字列。ホスト名のグループ。
command	文字列。ルールに含めるコマンド名。以下のいずれか。 • DELETE • EXECUTE • FILEOP • READ • WRITE
commandGroup	文字列。コマンドのグループ。
notCommand	文字列。「はい」または「いいえ」にする必要があります。「はい」を指定した場合、指定したコマンドを除くすべてのコマンドが使用されます。
actionName	文字列。必須、FAM アクションの名前。
messageTemplate	文字列。メッセージ・テンプレート名。
notificationType	文字列。通知タイプ。以下のいずれか。 • メール • SNMP • カスタム • SYSLOG
userLoginName	文字列。ユーザーのログイン名。
classDestination	文字列。呼び出すカスタム・クラスの名前。

policy_fam_rule_delete

FAM ポリシーからルールを削除します。

パラメーター	記述
policyName	必須。文字列。ポリシー名
ruleName	必須。文字列。削除するルールの名前。

add_action_to_fam_rule

既存の FAM ルールにアクションを追加します。

パラメーター	記述

actionName	文字列。必須。FAM アクションの名前。
alertReceiver	AlertReceiver は、アプライアンスの任意のユーザー (管理者や他のユーザー) です。
command	文字列。ルールに含めるコマンド名。以下のいずれか。 • DELETE • EXECUTE • FILEOP • READ • WRITE
messageTemplate	文字列。メッセージ・テンプレート名。
notificationType	文字列。通知タイプ。以下のいずれか。 • メール • SNMP • カスタム • SYSLOG
policyName	必須。文字列。有効なポリシー名。
ruleName	必須。文字列。更新するルールの名前。

親トピック: GuardAPI リファレンス

GuardAPI GIM 関数

これらの CLI コマンドは、GIM 関数のリスト、更新、割り当て、削除、およびキャンセルに使用します。

gim_list_registered_clients

登録済みのすべてのクライアントをリストします。

表 1. gim_list_registered_clients

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_list_registered_clients
```

gim_list_client_params

特定のクライアントに割り当てられたすべての (モジュール) パラメーターをリストします。

表 2. gim_list_client_params

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_list_client_params clientIP=192.168.12.210
```

gim_update_client_params

特定のクライアントの単一モジュール・パラメーターを更新します。

表 3. gim_update_client_params

パラメーター	記述
clientIP	必須。ターゲット・クライアントの IP
paramName	必須。パラメーター名
paramValue	必須。パラメーター値
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_update_client_params clientIP=192.168.1.100 paramName=STAP_TAP_IP paramValue=192.168.1.100
```

gim_list_client_modules

特定のクライアントに割り当てられたすべてのモジュールとその状態をリストします。

表 4. gim_list_client_modules

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_list_client_modules clientIP=192.168.2.210
```

gim_load_package

「filename」内のすべてのモジュールをロードします。

注: このコマンドは、ローカル・ファイル・システムにあるファイルをロードします。したがって、このコマンドの前に CM/Guardium アプライアンスへファイルをロードするプロシージャー (cmd='fileserver') が必要です。

表 5. gim_load_package

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_load_package  filename=*.gim
```

注: filename にはワイルドカード「*」を使用することができます。

gim_assign_bundle_or_module_to_client_by_version

クライアントにバンドル/モジュールを割り当てます。

表 6. gim_assign_bundle_or_module_to_client_by_version

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
module	必須 - モジュール
moduleVersion	必須 - モジュール・バージョン
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=192.168.1.100  module=BUNDLE-STAP moduleVersion="8.0_r1234_1"
```

gim_schedule_install

お客様に割り当てられていて、まだインストールしていない (保留中など) モジュール/バンドルすべてのインストールをスケジュールします。 パラメーター module が指定される場合、要求されたモジュールのみがスケジュールに入れられます。

表 7. gim_schedule_install

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
module	オプション - モジュール。モジュールがコマンド内で指定されていない場合、指定された clientIP のモジュールすべてがインストール対象としてスケジュールに入れられます。
date	必須 - 日付。形式: 'now' または 'yyyy-MM-dd HH:mm'
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_schedule_install clientIP=192.168.1.100 module=BUNDLE-STAP  date="2008-07-02 14:50"
```

```
grdapi gim_schedule_install clientIP=192.168.1.100 date="2008-07-02 14:50"
```

注: 即時に実行するものがある場合は、過去の日付を使用することができます。

gim_list_client_status

特定のクライアントに対して実行した最新の操作の状況を表示します。

表 8. gim_list_client_status

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_list_client_status clientIP=192.168.1.100
```

gim_uninstall_module

特定のクライアントのモジュール/バンドルをアンインストールします。

表 9. gim_uninstall_module

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
module	必須 - モジュール。
date	必須 - 日付。形式: 'now' または 'yyyy-MM-dd HH:mm'
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_uninstall_module clientIP=192.168.1.100 module=BUNDLE-STAP
```

gim_cancel_install

特定のクライアントへのバンドル/モジュールのインストールをキャンセルします。 インストールのキャンセルは、モジュール/バンドルがクライアントによってインストールのプロセスに入っていない (STATE=IP または IP-PR) 場合のみ行うことができます。

表 10. gim_cancel_install

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
module	必須 - モジュール。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_cancel_install clientIP=192.168.1.100 module=BUNDLE-STAP
```

gim_list_bundles

使用可能なバンドルすべてをリストします。 バンドルとは、クライアントにインストールできるモジュールの集まりです。

表 11. gim_list_bundles

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_list_bundles
```

gim_list_mandatory_params

1 つのモジュールの必須パラメーターをリストします。

表 12. gim_list_mandatory_params

パラメーター	記述
module	必須パラメーターを表示する GIM モジュールの名前
version	必須パラメーターを表示する GIM モジュールのバージョン

例

```
grdapi gim_list_mandatory_params module=name version=number
```

gim_assign_latest_bundle_or module_to_client

特定のクライアントに使用可能な最新 (つまり最上位バージョン) のバンドルまたはモジュールを割り当てます。

表 13. gim_assign_latest_bundle_or module_to_client

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
module	必須 - モジュール。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: api_target_host=10.0.1.123 • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_assign_latest_bundle_or_module_to_client clientIP=192.168.1.100  module=BUNDLE_STAP
```

gim_schedule_uninstall

クライアントに割り当てられており、まだアンインストールしていない (つまり「PENDING」) モジュール/バンドルすべてのアンインストールをスケジュールに入れます。 パラメーター module が指定される場合、要求されたモジュールのみがスケジュールに入れられます。

表 14. gim_schedule_install

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
module	オプション - モジュール。モジュールがコマンド内で指定されていない場合、指定された clientIP のモジュールすべてがインストール対象としてスケジュールに入れられます。
date	必須 - 日付。形式: 'now' または 'yyyy-MM-dd HH:mm'
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: api_target_host=10.0.1.123 • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_schedule_uninstall clientIP=192.168.1.100 module=BUNDLE-STAP  date="2008-07-02 14:50"   grdapi gim_schedule_uninstall
clientIP=192.168.1.100 date="2008-07-02 14:50"
```

gim_cancel_uninstall

特定のクライアントのバンドル/モジュールのアンインストールをキャンセルします。 アンインストールのキャンセルは、モジュール/バンドルがクライアントによってインストールのプロセスに入っていない (STATE=IP または IP-PR) 場合のみ行うことができます。

表 15. gim_cancel_uninstall

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
module	必須 - モジュール。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_cancel_uninstall clientIP=192.168.1.100 module=BUNDLE-STAP
```

gim_remove_bundle

このコマンドは、bundlePackageName をデータベースおよびファイル・システム (/var/log/guard/gim_packages。Guardium システムが中央マネージャーである場合はさらに /var/gim_dist_packages も) から削除します。

パラメーター (必須):

bundlePackageName

パラメーター値として、gim_list_unused_bundles の出力に指定されたバンドル・パッケージ名を取ります。 このコマンドは、次の条件を満たす場合にのみ成功します。

2.1 bundlePackageName の値がバンドルを参照している

2.2 bundlePackageName の値がどのクライアントにも割り当てられていない

2.3 bundlePackageName の値が存在する

2.4 bundlePackageName の値を参照するバンドルが 1 つだけ存在する

バンドルをデータベース/ファイル・システムから削除するには、これらのすべての条件 (2.1 から 2.4) が true である必要があります。そうでない場合は、エラーが生成されます。

例

```
grdapi gim_remove_bundle  bundlePackageName= bundlePackageName
```

gim_unassign_client_module

クライアントからモジュールを割り当て解除します。 gim_remove_module とは異なり、このコマンドは CM/Guardium アプライアンス上でモジュールと特定のクライアント間の関連付けを解除します。 このコマンドは実際のデータベース・サーバー・マシンでモジュールをアンインストールしたり、削除したりするものではありません。モジュールの現在状態に関して、データベース・サーバー (つまりクライアント) の情報と CM/Guardium アプライアンスの情報の間で、同期の問題が生じた場合にのみ使用されるものです。

表 16. gim_unassign_client_module

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
module	オプション - モジュール。モジュールがコマンド内で指定されていない場合、指定された clientIP のモジュールすべてがインストール対象としてスケジュールに入れられます。
date	必須 - 日付。形式: 'now' または 'yyyy-MM-dd HH:mm'
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_unassign_client_module clientIP=192.168.1.100  module=STAP
```

gim_get_purge_list

以前 Guardium® アプライアンスまたは CM にアップロードした古いソフトウェア・パッケージ (GIM ファイル) をリストします。

表 17. gim_get_purge_list

パラメーター	記述

パラメーター	記述
olderThan	必須 - 日数。 指定された日数より古いファイルがパージされます。 0 以上の任意の数字が有効です。
excludeLatest	オプション - true または false (デフォルト値は true)。 true - モジュール、OS ごとの最新バージョンはパージしません。 false – モジュール、OS ごとの最新バージョンをパージします。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_get_purge_list olderThan=30 excludeLatest=true
```

gim_purge

以前 Guardium アプライアンスまたは CM にアップロードした古いソフトウェア・パッケージ (GIM ファイル) を削除します。

表 18. gim_purge

パラメーター	記述
olderThan	必須 - 日数。 指定された日数より古いファイルがパージされます。 0 以上の任意の数字が有効です。
excludeLatest	オプション - true または false (デフォルト値は true)。 true - モジュール、OS ごとの最新バージョンはパージしません。 false – モジュール、OS ごとの最新バージョンをパージします。
filename	オプション - 削除する特定のファイル。 指定したファイルがバンドル (guard-bundle で始まるなど) である場合、このバンドルの内容が削除されます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_purge olderThan=30
```

注:

このコマンドには filename パラメーターまたは (olderThan または excludeLatest のどちらか、またはその両方) を指定できます。

gim_purge は、現在インストールのスケジュールに入っているファイルはパージしません。

gim_purge では、「/」文字を含むファイル (パラメーター のファイル名など) を削除できません。

gim_get_available_modules

特定のサーバーにインストール可能なモジュール/バンドルをリストします。

表 19. gim_get_available_modules

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス

例

```
grdapi gim_get_available_modules clientIP=192.168.1.100
```

gim_get_client_last_event

特定のクライアントに対して実行された最新の操作をリストします。

gim_get_client_last_event は、機能が限定された GrdAPI コマンドです。このコマンドが行うのは、最新のインストール試行中に最後に発生したイベントを表示することだけです。例えば、最後に S-TAP をインストールした際にいくつかのエラーが発生した場合は、その grdapi コマンドを実行することで、それが表示されます。ただし、データベース・サーバー上で直接にインストールの問題を手動で修正した場合、(S-TAP が現在実行中であっても) この grdapi コマンドは引き続き元の同じエラー・メッセージを表示します。このコマンドは、データベース・サーバーでの手動修正後に S-TAP 状況を評価するためには使用しないでください。

表 20. gim_get_client_last_event

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス

例

grdapi gim_get_client_last_event clientIP=192.168.1.100

grdapi gim_get_client_last_event clientIP=winx64

grdapi gim_get_client_last_event clientIP=9.70.144.73

gim_get_modules_running_status

特定のサーバー上で現在稼働しているモジュールおよびバンドルをリストします。

表 21. gim_get_modules_running_status

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
process	プロセスの名前
status	ON または OFF
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_get_modules_running_status clientIP=192.168.1.100 process= status=
```

gim_list_unused_bundles

このコマンドは、未使用の (どのデータベース・サーバーにもインストールされていない) バンドル、およびアップロード可能な個々の Windows モジュール (Windows CAS、Windows FAM など) のリストを返します。

パラメーター (必須):

includeLatest (valid values 0/1)

1 に設定した場合、最新の未使用のバンドルを含めた、使用されていないバンドルのリストが返されます。

例

```
grdapi gim_list_unused_bundles includeLatest=1
```

gim_reset_client

選択されたクライアントからモジュールを分離します。

表 22. gim_reset_client

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_reset_client clientIP=192.168.1.100
```

gim_set_diagnostics

GIM 内に診断収集を設定します。

表 23. gim_set_diagnostics

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_set diagnostics clientIP=192.168.1.100
```

gim_set_global_param

GIM 内にグローバル・パラメーターを設定します。

表 24. gim_set_global_param

パラメーター	記述
clientIP	必須 - クライアントの IP アドレス
paramName	必須 - マップされる API 関数内のパラメーターの名前
paramValue	必須 - マップされる API 関数内のパラメーターの値
sqlguardip	オプション - この GIM エージェントが接続するコレクターの IP アドレス/ホスト名。
ca_file	オプション - 認証局 PEM ファイルの完全なファイル名パス。
key_file	オプション - 秘密鍵 PEM ファイルの完全なファイル名パス。
cert_file	オプション - 証明書 PEM ファイルの完全なファイル名パス。
gim_listener_default_port	オプション - GIM エージェント・サーバー・モード用に別のポートを設定します。
gim_listener_default_shared_secret	オプション - 新しいサーバー・モード GIM エージェントに要求を送信するコレクターを検証するための共有パスワードを設定します。
no_listener	オプション - サーバー・モードの GIM エージェントを無効化します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_set_global_param clientIP=192.168.1.100 paramName=gim_listener_default_port paramValue=8445
```

gim_remote_activation

コレクターの IP アドレスをサーバー・モードの GIM エージェントまたは GIM エージェントのグループに接続します。

表 25. gim_remote_activation

パラメーター	記述
targetGroup	オプション - コレクターが接続するすべてのデータベース・サーバーのグループ名。targetHost パラメーターとともに指定することはできません。
sharedSecret	オプション - インストール時に構成された共有パスワード。
targetPort	オプション - GIM エージェントのポート・サーバー・モード。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi gim_remote_activation targetGroup=<someGroup> sharedSecret=<password> targetPort=8445
```

親トピック: GuardAPI リファレンス

GuardAPI グループ関数

これらの GuardAPI コマンドは、データ・ソース・グループ関数の作成、リスト、および削除に使用します。

注: 一元管理環境では、すべてのグループが中央マネージャーで定義され、スケジュールに基づいて管理対象ユニットに送信されます。

グループ関数

create_group

list_group_by_id

list_group_by_desc

delete_group_by_id

delete_group_by_desc

update_group_by_id

update_group_by_desc

flatten_hierarchical_groups

メンバー関数

create_member_to_group_by_id

create_member_to_group_by_desc

list_group_members_by_id

list_group_members_by_desc

delete_member_from_group_by_id

delete_member_from_group_by_desc

create_group

create_group

グループ定義を作成します。

表 1. create_group

パラメーター	記述
desc	必須。新規グループの固有の記述を入力します。
type	必須。次のいずれかでなければなりません。 アプリケーション・イベントの値の数値 アプリケーション・イベントの値の文字列 アプリケーション・イベントの値のタイプ アプリケーション項目名 アプリケーション・モジュール アプリケーション・システム ID

パラメーター	記述
	アプリケーションのトランザクション・コード
	アプリケーション・ユーザー
	監査タスク・タイプ
	クライアントのホスト名
	クライアント IP
	クライアント IP/データベース・ユーザー
	クライアント IP/ソース・アプリケーション/データベース・ユーザー
	クライアント IP/ソース・アプリケーション/データベース・ユーザー/ サーバー IP/サービス名前
	クライアントの MAC アドレス
	クライアント OS
	コマンド
	CVE 定義済みテスト
	データベース名
	データベース・エラー・コード
	データベース・プロトコル
	データベース・プロトコル・バージョン
	データベースのロール
	データベース・ユーザー/オブジェクト/特権
	DB のバージョン/パッチ
	例外タイプ
	フィールド
	ファイルの許可
	グローバル ID
	Guardium® 監査カテゴリー
	Guardium のロール
	Guardium ユーザー
	ログイン成功コード
	ネット・プロトコル
	オブジェクト/コマンド
	オブジェクト/フィールド
	オブジェクト
	操作タイプ
	OS ユーザー
	ポート
	修飾されたオブジェクト
	影響を受けるレコード
	スキーマ
	センテンスの深さ
	サーバーの記述
	サーバーのホスト名
	サーバー IP
	サーバー IP/データベース・ユーザー
	サーバー IP/サーバー・ポート
	サーバー IP/サービス名/データベース・ユーザー

パラメーター	記述
	サーバー OS サーバー・タイプ サービス名 ソース・プログラム SQL ベースの定義済みテスト TeraData プロファイル/データベース・ユーザー TTL ユーザー 脆弱性診断テストの例外 曜日 年
appid	必須。グループのアプリケーションを識別します。以下のいずれかの値でなければなりません。 パブリック 監査プロセス・ビルダー ベースライン・ビルダー 重要: 「ベースライン・ビルダー」と関連機能は、Guardium V10.1.4 から非推奨になりました。 Classifier DB2_zOS グループ エクスプレス・セキュリティー IMS zOS グループ ポリシー・ビルダー セキュリティー・アセスメント・ビルダー
subtype	オプション。サブタイプは、同じグループ・タイプの複数グループをまとめ、各グループのメンバーシップは排他的になるようにするために使用します。 例えば、データベース・サーバーが 3 つのデータ・センターに配置されていて、サーバーをロケーション別にグループ化するとします。 ロケーションごとにデータベース・サーバーの個別のグループを定義して、3 つのグループすべてに同じサブタイプ (例えば datacenter) を定義できます。
category	オプション。 category は、ポリシー違反とレポート用グループをグループ化するために使用される、オプション・ラベルです。
classification	オプション。classification は、ポリシー違反とレポート用グループをグループ化するために使用される、もう 1 つのオプションのラベルです。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例 (記載されている大文字と小文字に厳密に従ってください)

```
grdapi create_group desc=agroup type=OBJECTS  appid=Public owner=admin
```

```
grdapi create_group appid=Access_policy owner=admin  type="OBJECTS"  desc=groupName1
```

list_group_by_id

特定グループのプロパティーを表示します。

表 2. list_group_by_id

パラメーター	記述
id	必須 (整数)。グループを識別します。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_group_by_id id=100003
```

list_group_by_desc

特定グループのプロパティーを表示します。

表 3. list_group_by_desc

パラメーター	記述
desc	必須。表示されるグループの名前。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_group_by_desc desc=agroup
```

delete_group_by_id

表 4. delete_group_by_id

パラメーター	記述
id	必須 (整数)。グループを識別します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_group_by_id id=100005
```

delete_group_by_desc

表 5. delete_group_by_desc

パラメーター	記述
desc	必須。削除されるグループの名前。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_group_by_desc desc=agroup
```

update_group_by_id

指定されたグループのプロパティーを更新します。

表 6. update_group_by_id

パラメーター	記述
id	必須 (整数)。更新するグループを識別します。
newDesc	オプション。新規グループの固有の記述を入力します。
subtype	オプション。サブタイプは、同じグループ・タイプの複数グループをまとめ、各グループのメンバーシップは排他的になるようにするために使用します。 例えば、データベース・サーバーが 3 つのデータ・センターに配置されていて、サーバーをロケーション別にグループ化するとします。 ロケーションごとにデータベース・サーバーの個別のグループを定義して、3 つのグループすべてに同じサブタイプ (例えば datacenter) を定義できます。
category	オプション。 category は、ポリシー違反とレポート用グループをグループ化するために使用される、オプション・ラベルです。
classification	オプション。classification は、ポリシー違反とレポート用グループをグループ化するために使用される、もう 1 つのオプションのラベルです。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi update_group_by_id id=100002 newDesc=beegroup subtype=bee category=be classification=bea
```

update_group_by_desc

指定されたグループのプロパティーを更新します。

表 7. update_group_by_desc

パラメーター	記述
desc	必須。更新されるグループの名前。
newDesc	オプション。グループの固有の記述を入力します。
subtype	オプション。サブタイプは、同じグループ・タイプの複数グループをまとめ、各グループのメンバーシップは排他的になるようにするために使用します。 例えば、データベース・サーバーが 3 つのデータ・センターに配置されていて、サーバーをロケーション別にグループ化するとします。 ロケーションごとにデータベース・サーバーの個別のグループを定義して、3 つのグループすべてに同じサブタイプ (例えば datacenter) を定義できます。
category	オプション。 category は、ポリシー違反とレポート用グループをグループ化するために使用される、オプション・ラベルです。
classification	オプション。classification は、ポリシー違反とレポート用グループをグループ化するために使用される、もう 1 つのオプションのラベルです。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi update_group_by_desc desc=beegroup newDesc=beegroupee category=bebebe classification=bebebebe
```

flatten_hierarchical_groups

グループ・ビルダーに存在するすべての階層グループを更新します。

表 8. flatten_hierarchical_groups

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi flatten_hierarchical_groups
```

create_member_to_group_by_id

グループ ID で指定されたグループにメンバーを追加します。

表 9. create_member_to_group_by_id

パラメーター	記述
id	必須 (整数)。メンバーを追加する先のグループを識別します。
member	必須。新規メンバー名。これはグループ内で固有でなければなりません。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_member_to_group_by_id  id=100005 member=turkey
```

create_member_to_group_by_desc

指定されたグループにメンバーを追加します。

表 10. create_member_to_group_by_desc

パラメーター	記述
desc	必須。メンバーを追加する先のグループの名前。
member	必須。新規メンバー名。これはグループ内で固有でなければなりません。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_member_to_group_by_desc  desc=bgroup  member=turkey
```

次のコマンドを使用して、メンバーをグループに追加します。

```
grdapi create_member_to_group_by_desc desc=groupName1 member=member_1
grdapi create_member_to_group_by_desc desc=groupName1 member=member_2
grdapi create_member_to_group_by_desc desc=groupName1 member=member_3
grdapi create_member_to_group_by_desc desc=groupName1 member=member_4
grdapi create_member_to_group_by_desc desc=groupName1 member=member_5
```

追加のグループ GuardAPI コマンド

create_hierarchical_member_to_group_by_desc

delete_hierarchical_member_from_group_by_desc

関数パラメーター:

desc - 文字列 - 必須

member - 文字列 - 必須

list_group members_by_id

指定されたグループのメンバーをリストします。

表 11. list_group members_by_id

パラメーター	記述
id	必須 (整数)。リストされるメンバーのグループを識別します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_group_members_by_id  id=100001
```

list_group_members_by_desc

指定されたグループのメンバーをリストします。

表 12. list_group_members_by_desc

パラメーター	記述
desc	必須。メンバーをリストするグループの名前。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_group_members_by_desc  desc=bgroup
```

delete_member_from_group_by_id

指定されたグループから 1 メンバーを削除します。

表 13. delete_member_from_group_by_id

パラメーター	記述
id	必須 (整数)。メンバーが削除されるグループを識別します。
member	必須。削除するメンバーの名前。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_member_to_group_by_id  id=100005 member=turkey
```

delete_member_from_group_by_desc

指定されたグループから 1 メンバーを削除します。

表 14. delete_member_from_group_by_desc

パラメーター	記述
desc	必須。メンバーが削除されるグループの名前。
member	必須。削除するメンバーの名前。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_member_from_group_by_desc desc=bgroup member=boston
```

親トピック: GuardAPI リファレンス

GuardAPI 入力生成

GuardAPI 入力生成を使用すると、ユーザーは 1 つの Guardium® レポートの出力を取得して、それを別の Guardium エンティティーへの入力とすることができます。 つまり、ユーザーは準備済みの呼び出しを使用して素早く API の機能を呼び出すことができます。

Guard API 呼び出しの入力生成

レポートからの Guard API 呼び出しの生成は、2 とおりの方法で実行できます。それは、レポート内の単一行から実行する方法と、レポート全体 (画面に表示されているもの) に基づいた複数の行から実行する方法です。 例については、How-to トピック『レポートから API 呼び出しを生成する方法』を参照してください。

レポートが表示されている状態で次のように実行します。

単一行の場合:

1. 行をダブルクリックしてドリルダウンすると、「呼び出し...」オプションが表示されます。「呼び出し...」オプションをクリックすると、このレポートにマップされている API のリストが表示されます。

複数行の場合

1. 「呼び出し...」アイコン (レポートの状況表示行内にある) をクリックして、このレポートにマップされている API のリストを表示します。

   単一行と複数行の両方について、手順を続行します。

2. 呼び出す API をクリックします。 レポートと呼び出される API 関数の「API 呼び出し形式」が表示されます。レポートから複数行を対象に API 呼び出しを起動すると「API 呼び出し形式」が生成されて表示され、画面に表示されたすべてのレコードを編集できるようになります。表示されるレコードはフェッチ・サイズによって異なり、最大で 20 レコードです。
3. 選択した API 呼び出しの必須パラメーターを入力し、必須以外のパラメーターがあれば入力します。パラメーターの多くはレポートに基づいてあらかじめ入力されていますが、変更して固有の API 呼び出しを作成することもできます。必須のパラメーターと必須以外のパラメーターの入力に関する固有のヘルプについては、「GuardAPI リファレンス・ガイド」の個々の API 関数呼び出しを参照してください。
   複数行の場合、API についてのパラメーター・セット (パラメーターごとのボタンが付いたもの) を使用して、パラメーターの値を入力し、下矢印ボタンをクリックして、すべてのレコードの当該パラメーターにデータを設定します。 また、各行のチェック・ボックスを使って、API 呼び出しに含める行を選択または選択解除します。
   注: 「password」という名前を持つパラメーターはマスクされます。
4. ドロップダウン・リストを使用して「ログ・レベル」を選択します。この「ログ・レベル」は次のような意味を持ちます。0: 「戻りコード」に定義されたとおりに ID=identifier と ERR=error_code が返されます。1: 画面に追加情報が表示されます。2: Guardium アプリケーションのデバッグ・ログに情報を出力します。3: 1 と 2 の両方を実行します。
5. ドロップダウン・リストを使用して「暗号化するパラメーター」を選択します。
   注: パラメーター暗号化は共有パスワードを設定することによって有効になり、スクリプト生成を介して API 関数を呼び出す場合のみ該当します。
6. 「今すぐ呼び出し」または「スクリプトを生成」を選択します。
   a. 「今すぐ呼び出し」を選択すると、ただちに API 呼び出しが実行され、「API 呼び出し出力」画面に API 呼び出しの状況が表示されます。
   b. 「スクリプトを生成」を選択した場合は、次のようにします。
      i. お好きなエディターを使用して、生成したスクリプトを開きます。あるいは、オプションとして、ディスクに保存して後から編集および実行することもできます。

         スクリプトの例

         # A template script for invoking Sqlguard API function delete_datasource_by_name seven times:

         # Usage: ssh cli@a1.corp.com<delete_datasource_by_name_api_call.txt

         # replace any < > with the required value

         #

         set guiuser <username> password <password>

         grdapi delete_datasource_by_name name=192.168.2.91

         grdapi delete_datasource_by_name name=egret-oracle

         grdapi delete_datasource_by_name name=egret-oracle3

      ii. スクリプトを変更します。空のパラメーター値 (< > で示される) をすべて置換します。
         注: API 呼び出しでは空のパラメーターは無視されるため、スクリプトに空のパラメーターが残っていても構いません。

         変更スクリプトの例

         # A template script for invoking Sqlguard API function delete_datasource_by_name seven times:

         # Usage: ssh cli@a1.corp.com<delete_datasource_by_name_api_call.txt

         # replace any < > with the required value

         #

         set guiuser <username> password <password>

         grdapi delete_datasource_by_name name=egret-oracle3

      iii. CLI 関数呼び出しの実行

         呼び出しの例

         $ ssh

         cli@a1.corp.com<c:/download/delete_datasource_by_name_api_call.txt

レポート結果への GuardAPI のマッピング

Guardium には定義済みレポートのバッテリーが付属しています。それらの多くは、構成しやすいように既に GuardAPI 関数にマップされています。 さらに、Guardium では、追加レポートを定義でき、ユーザー独自のカスタム・レポートであっても定義できます。作成したレポートは、レポートごとに GuardAPI 関数にマップできます。

1. 「日次モニター」、「Guardium モニター」、または「TAP モニター」の各タブ内の任意の定義済みレポートに移動します。
2. 「呼び出し ...」ボタンをクリックします。
3. 「API マッピングの追加」の選択項目を選択します。
4. 新規ウィンドウの「API マッピングの追加」には、レポートの名前 (例えば Guardium ログイン)、適切な GuardAPI コマンドを検索するための検索/フィルター・メカニズム、および「定義済みレポート」で使用可能な API 関数の選択項目が表示されます。「API 関数」を選択してから、「レポート属性のマップ」をクリックします。
5. 新規ウィンドウの「API - レポート・パラメーター・マッピング」で、パラメーター名をレポート・フィールドにマップします。Guardium レポートに提供されていないデータがある場合もあります。 このような場合には、定数を作成してレポートに追加し、API パラメーター・マッピング内で使用することができます。
   注: 保存すると、現行のマッピングがオーバーライドされます。
   注: 定数が追加された Guardium レポートをエクスポートしても、その定数はエクスポートされません。

GuardAPI パラメーターと Guardium 属性との間のマッピングを簡素化するために、Guardium には事前定義レポートである「照会エンティティーと属性」が作成されています。このレポートには、Guardium の属性がすべてリストされ、ユーザーに GUI インターフェースが示されるため、ユーザーはレポートから簡単にドリルダウンしてリンケージを素早く作成できます。

既存の Guardium 属性またはユーザー定義の定数は、既存の属性または定数の GuardAPI パラメーターにマップできます。

注: GuardAPI パラメーターがレポート属性にマップされる際に、レポート内で同じ GuardAPI パラメーターに対して複数の属性がマップされている場合、その API 呼び出しで選ばれる値は、レポートの表示順序に従って最初に表示される属性です。

既存の属性

1. 「照会エンティティーと属性」レポートに進み、API パラメーターのマッピングを追加します。(「Guardium モニター」->「照会エンティティーと属性」)
2. 「照会エンティティーと属性」レポートは、Guardium 属性をすべてリストするため長くなります。 「カスタマイズ」ボタンを使用して対象となるレコードを絞り込んでください。
3. マッピングを作成するには、パラメーター名を割り当てる属性行をダブルクリックします。
4. 「呼び出し...」オプションをクリックします。
5. create_api_parameter_mapping API 関数を選択します。
6. 「API 呼び出しフォーム」で functionName と parameterName に入力します。
7. 「今すぐ呼び出し」ボタンをクリックして、API - レポート・パラメーター・マッピングを作成します。

GUI を使用して GuardAPI パラメーターをマップする完全なシナリオについては、How-To トピック『カスタム・レポートからの API 呼び出しの使用』を参照してください。

定数

Guardium レポート内に提供されていないデータもあります。 このような場合には、定数を作成してレポートに追加し、API パラメーター・マッピング内で使用することができます。

1. 「照会エンティティーと属性」レポートに進み、API パラメーターのマッピングを追加します。(「Guardium モニター」->「照会エンティティーと属性」)
2. 「照会エンティティーと属性」レポートは、Guardium 属性をすべてリストするため長くなります。 「カスタマイズ」ボタンを使用して対象となるレコードを絞り込んでください。
3. 定数属性を作成するには、定数属性を作成したいエンティティーの任意の行をダブルクリックします。
4. 「呼び出し...」オプションをクリックします。
5. create_constant_attribute API 関数を選択します。
6. 使用する値を constant に、 付ける名前を attributeLabel に入力します。
7. 「今すぐ呼び出し」ボタンをクリックして定数を作成します。
8. マッピングを作成するには、新しく作成した属性行をダブルクリックします。
9. 「呼び出し...」オプションをクリックします。
10. create_api_parameter_mapping API 関数を選択します。
11. 「API 呼び出しフォーム」で functionName と parameterName に入力します。
12. 「今すぐ呼び出し」ボタンをクリックして、API - レポート・パラメーター・マッピングを作成します。
13. 新しく作成した属性はレポートに追加する必要があります。 「クエリー・ビルダー」で照会を変更し、フィールドを追加します。

GUI を使用して定数属性を作成およびマップする完全なシナリオについては、How-to トピック『API 呼び出しでの定数の使用』を参照してください。

注: 定数が追加された Guardium レポートをエクスポートしても、その定数はエクスポートされません。
注: API マッピングを使用する場合、レポート内の表の列は、その表の列がエンティティーの属性である限り、レポート・フィールドに表示されます。カウント列などの一部の列は、マップできないため、レポート・フィールドには表示されません。

一部の GuardAPI コマンドのオブジェクト・セキュリティー

ロール検証では、一部の GuardAPI コマンドにコントロールを実装して、特定のコンポーネント (アプリケーションだけでなく) のロールを考慮し、ロールが一致しない場合にアクションを禁止します。

これは、ポリシー・ビルダーに対して適切なロールを持つユーザーであれば、どのポリシーにも (その特定のポリシーのロールに関係なく) GuardAPI コマンド delete_rule を実行できることを意味します。

ポリシー・ルールの GuardAPI コマンド change_rule_order、copy_rule、copy_rules、delete_rule、update_rule に対してロール検証が存在します。

グループの記述 GuardAPI コマンド create_member_to_group_by_desc、create_member_to_group_by_id、delete_group_by_desc、delete_group_by_id、delete_member_from_group_by_desc、delete_member_from_group_by_id、update_group_by_id、update_group_by_desc に対してロール検証が存在します。

データ・ソース GuardAPI コマンド delete_datasource_by_id、delete_datasource_by_name、update_datasource_by_id、update_datasource_by_name に対してロール検証が存在します。

監査プロセス GuardAPI コマンド stop_audit_process に対してロール検証が存在します。

表形式レポートおよびグラフィカル・レポートから監査プロセスを実行する API

GuardAPI は、どのレポート・ポートレットからでも自動的に呼び出すことができます。 GuardAPI は呼び出されると新しい監査プロセス・レポートを作成します。

ユーザーに対してそのようなプロセスが存在している場合、パラメーターが更新され、同じプロセスが使用されます。

GuardAPI の振る舞いは以下のようになります。

1 - 新しいプロセスの場合、リスト内に emailContentType パラメーターで示されているコンテンツ・タイプの E メールがあるなら、その E メールごとにレシーバーを 1 つ作成します。また、includeUserReceiver パラメーターが true の場合は、(API を呼び出して) ログインしているユーザーのためのユーザー・レシーバーも作成します。

2 - 既存のプロセスの場合は、すべての E メール・レシーバーが削除され、emailContentType パラメーターに定義されているコンテンツ・タイプで、新規リスト (存在する場合) の E メールに置き換えられます。 リストが空の場合は、E メール・アドレス・レシーバーがすべて削除されます。 ユーザーのレシーバーが既に存在する場合は、includeUserreceiver が false でもそれは削除されませんが、このパラメーターが true で、かつそのようなレシーバーが存在しない場合は、追加されます。

監査プロセスが生成されると、これは (「今すぐ 1 回実行」と同じように) 自動的に実行され、ユーザーはその監査プロセスが自分の To-Do リスト上のアイテムとなることを期待します。

create_ad_hoc_audit_and_run_once

パラメーター:

1 - reportId - 監査プロセスの唯一のタスクに使用される、レポートの ID

2 - isForReportRunOnce - このブール値は、そのプロセスが作成後に 1 回実行する必要があるかどうかを示します。

3 - changeParIfExist ブール値は、プロセスが存在する場合に、タスク・パラメーターを更新するかどうかを示します

4 - taskParameter - それぞれが文字列 ^^ で連結されたすべてのタスク・パラメーターと値は、PAR1=Val1^^PAR2=Val2^^ のようになります。パラメーターを空のままにしても有効です。例えば、PAR2 が空のままにする場合、PAR1=VAL1^^PAR2=^^PAR3=VAL3^^... のようになります。

5 - processNamePar - プロセスの名前。空のときは、名前を持つプロセスが作成されます。

6 - sendToEmails: E メール・アドレスのコンマ区切りリスト

7 - emailContentType 0-PDF または 1-CSV (E メール・レシーバーにのみ適用)

8 - includeUserReceiver ブール値は、ログインしているユーザーのレシーバーを作成するかどうかを示します。

GuardAPI は、どのレポート・ポートレットからでも自動的に呼び出すことができます。 GuardAPI は呼び出されると新しい監査プロセス・レポートを作成します。

スケジュール API

modify_schedule パラメーター jobName jobGroup cronString startTime オプション

list schedule

delete_schedule パラメーター jobName jobGroup deleteJob オプション

schedule_job パラメーター jobType objectName optional cronString startTime オプション

注: grdapi schedule_job 関数の一部のジョブ・タイプでは、オブジェクト名は必要ありません。特定のジョブ・タイプ (csvExportJob、systemBackupJob、dataArchiveJob、dataExportJob、dataImportJob、resultsArchiveJob、AppUserTranslation、IpHostToAlias) について objectName パラメーターとして入力した内容を使用してこの関数が実行された場合、オブジェクト名パラメーターに対して検証は実行されず、標準的な「OK」プロンプトが表示されます。

grdapi schedule_job --get_param_values=jobType - 関数「schedule_job」のパラメーター「jobType」の値は、CustomTableDataUpload、AutoDetectProbeJob、AppUserTranslation、InstallPolicy、AuditJob、ResultArchive、AutoDetectScanJob、CustomTableDataPurge、CSVExport、DataExport、DataArchive、DataImport、PopulateGrpFromQry、SystemBackup、PopulateAlias、IpHostToAlias、UnitUtilization のいずれかでなければなりません。

grdapi set_purge_batch_size

パージ中に使用されるバッチ・サイズを設定します。このバッチ・サイズはパージのパフォーマンスに貢献し、デフォルト設定は 200,000 です。パフォーマンスとディスク・スペース使用量とのトレードオフには注意が必要です。大きなバッチ・サイズを設定すると、パージの速度は上がりますが、より多くのディスク・スペースが消費されます。小さいバッチ・サイズを設定すると、パージの速度は下がりますが、それほど多くのディスク・スペースを消費することはありません。

関数パラメーター : batchSize - 必須 api_target_host 例 vx29> grdapi set_purge_batch_size batchSize=200000 ID=0 ok

grdapi get_purge_batch_size

パージ・バッチ・サイズの現在の設定を取得します

関数パラメーター : api_target_host 例 vx29> grdapi get_purge_batch_size ID=0 パージ・バッチ・サイズ = 200000 ok

grdapi patch_install

関数パラメーター : patch_date patch_number - 必須

grdapi populate_from_dependencies

関数パラメーター : descOfEndingGroup - 必須 descOfStartingGroup - 必須 flattenNamespace getFunctions getJavaClasses getPackages getProcedures getSynonyms getTables getTriggers getViews isAppend - 必須 isEndingGroupQualified owner - 必須 reverseIt selectedDataSourceName - 必須 api_target_host

create_computed_attribute

レポートで使用。

表 1. create_computed_attribute

パラメーター	記述
attributeLabel	必須。
entityLabel	必須。データベース・ユーザー
expression	必須。サーバー IP 必須。ユーザーは、式の中で tableName.field を指定する必要があります。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

grdapi create_computed_attribute attributeLabel="CustomUserName" entityLabel="App User Name"
expression="SUBSTRING_INDEX(GDM_CONSTRUCT_INSTANCE.APP_USER_NAME,'.',1)"

delete_computed_attribute

レポートで使用。

表 2. delete_computed_attribute

パラメーター	記述
attributeLabel	必須。
entityLabel	必須。
expression	必須。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

update_computed_attribute

レポートで使用。

表 3. update_computed_attribute

パラメーター	記述
attributeLabel	必須。
entityLabel	必須。
expression	必須。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

create_constant_attribute

レポートで使用。

表 4. create_constant_attribute

パラメーター	記述
attributeLabel	必須。
entityLabel	必須。
constant	必須。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

delete_constant_attribute

レポートで使用。

表 5. delete_constant_attribute

パラメーター	記述
attributeLabel	必須。
entityLabel	必須。
constant	必須。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

update_constant_attribute

レポートで使用。

表 6. update_constant_attribute

パラメーター	記述
attributeLabel	必須。
entityLabel	必須。
constant	必須。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

create_ad_hoc_audit_and_run_once

レポートで使用。

表 7. create_ad_hoc_audit_and_run_once

パラメーター	記述
chnageParlfExist	ブール値。必須。
emailContentType	整数
includeUserReceiver	ブール値
isForReportRunOnce	ブール値。必須。

パラメーター	記述
processNamePar	文字列
reportID	整数。必須
sendToEmails	文字列
taskParameter	文字列
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

REST API

JSON (JavaScript Object Notation) 出力オプションは、GuardAPI 関数をサポートします。これは、REST API の一部です。REST は Representational State Transfer の略です。ステートレスのクライアント/サーバーのキャッシュ可能通信プロトコルを利用します。また、ほとんどすべての場合に、HTTP プロトコルが使用されます。REST は、ネットワーク・アプリケーションを設計するためのアーキテクチャー・スタイルです。マシン間の接続に CORBA、RPC、SOAP などの複雑なメカニズムを使用するのではなく、単純な HTTP を使用してマシン間で呼び出しを実行するという考えに基づいています。RESTful アプリケーションでは、HTTP 要求を使用して、データのポスト (作成/更新)、データの読み取り (例えば、照会)、およびデータの削除を行います。そのため、REST では、作成/読み取り/更新/削除の 4 つの操作すべてで HTTP を使用します。REST は、RPC (リモート・プロシージャー・コール) や Web サービス (SOAP、WSDL) などのメカニズムの代わりとなる軽量なメカニズムです。

Guardium での REST の実装

1. アプリケーションを (1 回だけ) 登録し、クライアント・パスワードを取得します。
2. クライアント・パスワードを安全な場所に保管します。
3. 許可のためにアクセス・トークンを要求します。
4. grdAPI コマンドが正しく認証されるように、アクセス・トークンを保管します。
5. アクセス・トークンを使用して GuardAPI コマンドを実行依頼する。

ユース・ケースの例

- Guardium GUI にログインすることなく、特定の IP アドレスの少量の監査データを動的に取得できるようにしたい。
- ポリシーを更新して機密情報への無許可アクセスを防止できるように、既存グループにデータを取り込みたい。
- 特定の許可されたアクセス・グループ内のすべてのユーザーのリストを取得したい。
- モニターする必要がある機密表をアプリケーション開発チームが特定できるようにしたい。
- ターゲット・システムからの応答テキストのコーディングをユーザーに求める、「要求する」スクリプト言語を使用せずに grdAPI にスクリプトでアクセスしたい。

HTTP には操作のボキャブラリー (要求メソッド) があります。

- GET (URL でパラメーターを渡す)
- POST (JSON オブジェクトでパラメーターを渡す)
- PUT (変更するパラメーターを JSON オブジェクトとして渡す)
- DELETE (JSON オブジェクトとしてパラメーターを渡す)

内部 REST API 要求の特殊ユーザー

内部 REST API 要求用に、システム内に特殊なロールとユーザーが事前定義されています。

このユーザーは、accessmgr UI を使用して削除および変更できず、UI でのログインに使用できません。

このユーザーのパスワードは、有効期限切れとなることはありませんが、クライアント ID が取り消された場合は取り消されます。

OAuth クライアント登録時に、新しい関数がこのユーザーとクライアント ID を受け入れます。これは、当該ユーザーに対してランダムで強固なパスワードを生成し、TURBINE_USER 表に保管します。

これは、クライアント・パスワードと、生成されたパスワードを返します。

内部 (S-TAP など) のクライアントでは、クライアント・パスワードとパスワードを保護する必要があります。

accessmgr UI を使用して、各種関数に対する許可をロールに割り当てることができます。

RestAPI と GuardAPI の比較

GET = List

POST = Create

PUT = Update

DELETE = Delete

GuardAPIs

```
list_datasourcename_by_name (parameters - ?name="MSSQL_1")

-X GET https://10.10.9.239:8443/restAPI/datasource/?name="MSSQL_1"
```

create_datasource

```
-X POST https://10.10.9.239:8443/restAPI/datasource

update_datasource_by_name - JSON Object '{password:guardium}'

-X PUT -d '{password:guardium, name:"MSSQL_1}'

delete_datasource_by_id - JSON Object '{"id":20020}'

-X DELETE -d '{"id":20020}'
```

詳しくは、DeveloperWorks の記事『Using the IBM Security Guardium REST API』を参照してください。

http://www.ibm.com/developerworks/data/library/techarticle/dm-1404guardrestapi/index.html

内部 UnitPinger スレッドの照会および再始動

この GuardAPI コマンドは、内部 UnitPinger スレッドを照会および再始動するために使用します。
注: この GuardAPI コマンドは、api_target_host=127.0.0.1 パラメーターを使用して呼び出す必要があります。
例
grdapi get_unit_pinger api_target_host=127.0.0.1

register_oauth_client

この GuardAPI コマンドは、サポートされる GuardAPI 関数を、入出力で JSON (JavaScript Object Notation) を使用する RESTful API にラップする場合に使用します。

GrdAPI コマンド grdapi register_oauth_client は、クライアントを登録し、REST サービスの呼び出しに必要なアクセス・トークンを取得する場合に使用します。

REST は Representational State Transfer の略です。ステートレスのクライアント/サーバーのキャッシュ可能通信プロトコルを利用します。また、ほとんどすべての場合に、HTTP プロトコルが使用されます。

REST は、ネットワーク・アプリケーションを設計するためのアーキテクチャー・スタイルです。マシン間の接続に CORBA、RPC、SOAP などの複雑なメカニズムを使用するのではなく、単純な HTTP を使用してマシン間で呼び出しを実行するという考えに基づいています。

RESTful アプリケーションでは、HTTP 要求を使用して、データのポスト (作成/更新)、データの読み取り (例えば、照会)、およびデータの削除を行います。そのため、REST では、作成/読み取り/更新/削除の 4 つの操作すべてで HTTP を使用します。REST は、RPC (リモート・プロシージャー・コール) や Web サービス (SOAP、WSDL) などのメカニズムの代わりとなる軽量なメカニズムです。

関数パラメーター:

client_id - 文字列 - 必須

grant_types - 文字列 - 必須。サポートされる唯一の権限付与タイプは password です。

redirect_uris - 文字列 - 必須

scope - 文字列 - 必須

fetchSize - 文字列 - オプション。後方互換性を維持するために、デフォルトは 20 レコードです。最大値は 30000 です。

sortColumn - オプション - 指定する場合、いずれかのレポート・フィールドの列タイトルでなければなりません。

sortType - オプション - asc または desc。

構文

grdapi register_oauth_client <client_id> <grant_types> <redirect_uris> <scope>

getOAuthTokenExpirationTime

この GuardAPI コマンドは、REST API トークンの有効期限を取得する場合に使用します。

関数パラメーター:

api_target_host - 文字列

setOAuthTokenExpirationTime

この GuardAPI コマンドは、REST API トークンの有効期限を設定する場合に使用します。

関数パラメーター:

expirationTime - 整数 - 必須。

api_target_host - 文字列

構文

grdapi setOAuthTokenExpirationTime ExpirationTime=10000

親トピック: GuardAPI リファレンス

GuardAPI 調査ダッシュボード機能

これらの GuardAPI コマンドは、調査ダッシュボードの機能とパラメーターを有効化、無効化、または構成するために使用します。

disable_quick_search

調査ダッシュボードには、「クイック検索結果表 (Quick Search Results Table)」、「アクティビティー・グラフ」、およびその他のさまざまな事前定義グラフが含まれていることに注意してください。

調査ダッシュボード機能を無効にします。

```
grdapi disable_quick_search
```

パラメーター	値	記述
すべて	`true` または `false`	中央マネージャーがある環境では、このパラメーターを使用してすべての管理対象ユニットでの検索を無効にします。例えば、`all=true` です。 このパラメーターはオプションです。
api_target_host	ホスト名または IP アドレス	一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。 API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトでは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP このパラメーターはオプションです。

enable_quick_search

調査ダッシュボード機能を有効にします。

```
grdapi enable_quick_search schedule_interval=[value] schedule_units=[value]
```

例えば、以下のコマンドは、調査ダッシュボードを 2 分間のデータ抽出間隔で有効にします: `grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE`。

パラメーター	値	記述
すべて	`true` または `false`	中央マネージャーがある環境では、このパラメーターを使用してすべての管理対象ユニットでの検索を有効にします。例えば、`all=true` です。 このパラメーターはオプションです。
api_target_host	ホスト名または IP アドレス	一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。 API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトでは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP このパラメーターはオプションです。
extraction_start	date	検索用監査データ抽出の開始期限の日付を定義します。このパラメーターを省略した場合、抽出は即時に開始されます。 このパラメーターはオプションです。
includeViolations	`true` または `false`	検索索引に違反を含めるかどうかを決定します。違反を省略すると、検索索引のサイズを削減できます。 このパラメーターはオプションです。
schedule_interval	integer	schedule_units パラメーターとともに使用して、監査データの抽出の間隔を定義します。例えば、`schedule_interval=2 schedule_units=MINUTE` です。 このパラメーターは必須です。

schedule_start	date	schedule_interval パラメーターと schedule_units パラメーターによって定義された抽出間隔の後に開始する日付。 このパラメーターはオプションです。
schedule_units	`HOUR` または `MINUTE`	schedule_interval パラメーターとともに使用して、監査データの抽出の間隔を定義します。例えば、`schedule_interval=2 schedule_units=MINUTE` です。 このパラメーターは必須です。

set_enterprise_search_options

調査ダッシュボードの検索モードを定義します。

```
grdapi set_enterprise_search_options distributed_search=[value]
```

例えば、以下のコマンドは、all_machines モードで調査ダッシュボードを構成して、Guardium 環境全体にわたるデータの検索を、その環境内の任意の Guardium マシンから実行できるようにします。`grdapi set_enterprise_search_options distributed_search=all_machines`

パラメーター	値	記述
api_target_host	ホスト名または IP アドレス	一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。 API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトでは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP このパラメーターはオプションです。
distributed_search	cm_only、local_only、または all_machines	cm_only 中央マネージャーから実行依頼された検索では、Guardium 環境全体からの結果が返されますが、管理対象ユニットから実行依頼された検索では、その管理対象ユニットからのローカルの結果のみが返されます。 local_only 個々のマシンから実行依頼された検索では、そのマシンからの結果のみが返されます。Guardium 環境全体からデータを検索することはできません。 all_machines 任意のマシンから検索を実行依頼でき、Guardium 環境全体からの結果が返されます。 このパラメーターは必須であり、デフォルト値は cm_only です。

親トピック: GuardAPI リファレンス

GuardAPI ネイティブ監査関数

これらの GuardAPI コマンドを使用して、クラウド・データベースに対する DB 監査 (ネイティブ監査) の有効化、無効化、オブジェクト監査 (監査証跡) に対するオブジェクトの追加と削除、構成、コレクター、およびオブジェクトの取得を実行します。

add_ip_to_sg

指定した Guardium IP をクラウド・セキュリティー・グループに追加します。

```
add_objects_native_audit parameter=value
```

パラメーター	値	記述
datasource_name	文字列。	必須。Guardium で定義されているクラウド・データ・ソース
api_target_host	文字列。	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

add_objects_native_audit

指定したデータ・ソースのオブジェクト監査 (監査証跡) にオブジェクトを追加します。

```
add_objects_native_audit parameter=value
```

パラメーター	値	記述

datasource_name	文字列。	必須。Guardium で定義されているクラウド・データ・ソース
objects	文字列。	オブジェクトのコンマ区切りリスト。オブジェクトの表示は、get_native_audit_objects または GUI で行います。
api_target_host	文字列。	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

disable_native_audit

指定したクラウド・データ・ソースの DB 監査 (ネイティブ監査) を無効にします。

`disable_native_audit parameter=value`

パラメーター	値	記述
datasource_name	文字列	必須。Guardium で定義されているクラウド・データ・ソース
api_target_host	文字列	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

enable_native_audit

指定したデータ・ソースの DB 監査 (ネイティブ監査) を有効にします。

`enable_native_audit parameter=value`

パラメーター	値	記述
datasource_name	文字列	必須。Guardium で定義されているクラウド・データ・ソース
api_target_host	文字列	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

get_native_audit_collectors

環境内の、つまり指定したホスト、ポート、およびサービス名からデータを受信するコレクターの名前を返します。

`get_native_audit_collectors parameter=value`

パラメーター	値	記述
host	文字列	必須。AWS ホスト名
port	integer	必須。
service_name	文字列	必須。
api_target_host	文字列	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

get_native_audit_configurations

指定したホスト、ポート、サービス名のすべての詳細 (クラウド環境 ID、クラウド環境、プロバイダー、データ・ソース ID、インスタンス名、データベース・エンジン、サービス名、ホスト、ポート、Guardium セキュリティー・グループ、オブジェクト制限、オブジェクト、コレクター) を返します。

```
get_native_audit_configurations parameter=value
```

パラメーター	値	記述
host	文字列	必須。AWS ホスト名
port	integer	必須。
service_name	文字列	必須。
api_target_host	文字列	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

get_native_audit_objects

指定したホスト、ポート、サービス名上の分類プロセスによって検出されたすべてのオブジェクトを返します。

```
get_native_audit_objects parameter=value
```

パラメーター	値	記述
host	文字列	必須。AWS ホスト名
port	integer	必須。
service_name	文字列	必須。
api_target_host	文字列	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

remove_objects_native_audit

指定したデータ・ソース内の指定したオブジェクトのオブジェクト監査 (監査証跡) を無効にします。

```
remove_objects_native_audit parameter=value
```

パラメーター	値	記述
datasource_name	文字列	必須。Guardium で定義されているクラウド・データ・ソース
objects	文字列	オブジェクトのコンマ区切りリスト。オブジェクトの表示は、get_native_audit_objects または GUI で行います。
api_target_host	文字列	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトは、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP

親トピック: GuardAPI リファレンス

GuardAPI 異常値検出機能

以下の GuardAPI コマンドは、異常値検出機能を有効化、無効化、および構成するために使用します。

grdapi enable_outliers_detection_agg

grdapi enable_outliers_detection_agg

grdapi disable_outliers_detection_agg

指定されたアグリゲーターにデータを送信する、CM 環境内のすべてのコレクター (ローカルで異常値検出を実行しているコレクターを除く) からのエクスポート・データの送信を有効または無効にするために、中央マネージャーで実行します。データは毎時収集され、異常値検出処理のためにアグリゲーターに送信されます。データを抽出してアグリゲーターに送信するために、配布レポート・メカニズムが使用されます。

表 1. grdapi enable_outliers_detection_agg

パラメーター	記述
schedule_interval	必須。1 に設定する必要があります。
schedule_units	必須。hour に設定する必要があります。
aggregator_host_name	異常値検出のために有効化/無効化される特定のアグリゲーター。
DAM_FAM	オプション。異常値のタイプを指定します。デフォルトは DAM です。

grdapi enable_outliers_detection

grdapi enable_outliers_detection

grdapi disable_outliers_detection

コレクターでのローカルの異常値検出を有効化/無効化するために、コレクターで実行します。

表 2. grdapi enable_outliers_detection

パラメーター	記述
schedule_interval	必須。1 に設定する必要があります。
schedule_units	必須。hour に設定する必要があります。
DAM_FAM	オプション。異常値のタイプを指定します。デフォルトは DAM です。

grdapi set_outliers_detection_parameter privUsersGroupIds

追加のユーザー・グループを異常値検出アルゴリズムに追加します。次のコマンドは、グループ ID を検出するために使用します。grdapi list_group_by_desc desc=[group name]

表 3. grdapi set_outliers_detection_parameter

パラメーター	記述
privUsersGroupIds	1 つ以上の管理ユーザー・グループ ID。
sensitiveObjectGroupIds	1 つ以上の機密オブジェクト・グループ ID。

親トピック: GuardAPI リファレンス

GuardAPI プロセス制御関数

これらの GuardAPI コマンドは、プロセス制御関数の実行、コピー、アップロード、リスト、および削除に使用します。

分類プロセスの実行 (サブミット)

分類プロセスを実行します。 分類プロセス・ビルダーから「今すぐ 1 回実行」を実行することに相当します。 これは、Guardium® ジョブ・キューにプロセスを配置するジョブをサブミットします。このキューからアプライアンスは一度に 1 つのジョブを実行します。 管理者は、「Guardium モニター」>「Guardium ジョブ・キュー」と選択することによりジョブ状況を表示できます。

注: この API を呼び出す前に分類プロセスを作成してください。

表 1. 分類プロセスの実行 (サブミット)

パラメーター	記述
processName	分類プロセスの名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_cls_process processName="classPolicy1"
```

セキュリティー・アセスメントの実行 (サブミット)

指定された評価を実行します。 セキュリティー・アセスメント・ファインダーから「今すぐ 1 回実行」を実行することに相当します。 ジョブがサブミットされます。 これによって、Guardium ジョブ・キューにプロセスが配置され、このキューからアプライアンスは一度に 1 つのジョブを実行します。管理者は、「Guardium モニター」> 「Guardium ジョブ・キュー」と選択することによりジョブ状況を表示できます。

注: この API を呼び出す前にセキュリティー・アセスメントを作成してください。

表 2. セキュリティー・アセスメントの実行 (サブミット)

パラメーター	記述
assessmentDesc	評価の名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_assessment assessmentDesc="assessment1"
```

監査プロセスの実行

監査プロセスを実行します。 指定された監査プロセスを実行します。 監査プロセス・ビルダーから「今すぐ 1 回実行」を実行することに相当します。

注: この API を呼び出す前に監査プロセスを作成してください。
注: 監査レポートによって多くのデータが返される場合、CLI コマンドのヒープ・サイズ制限のため、ユーザーは GUI から監査プロセスを実行する必要があります。

表 3. 監査プロセスの実行

パラメーター	記述
auditProcess	監査プロセスの名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_auditProcess  auditProcess="Appliance Monitoring"
```

監査プロセスの停止

stop_audit_process API は GuardAPI コマンド行からは使用できません。この関数はドリルダウンからの呼び出しとしてのみ使用可能です。 Workload Automation ヘルプ・トピック『コンプライアンス』のサブトピック『監査プロセスの停止』を参照してください。

表 4. 監査プロセスの停止

パラメーター	記述
process	監査プロセスの名前
run	監査プロセスの RunID
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
stop_audit_process
```

照会からのグループ取り込みの実行

構成された照会を実行することで選択されているグループを取り込みます。 「照会設定からのグループに取り込み」画面から「今すぐ 1 回実行」を実行することに相当します。 グループがインポート向けに構成されていない場合、エラー・メッセージが表示されます。

注: この grdapi は、「照会設定からのグループに取り込み」画面で既に構成されているグループに対してのみ使用できます (照会が選択されていて、パラメーターが設定されていなければなりません)。

表 5. 照会からのグループ取り込みの実行

パラメーター	記述
groupDesc	グループ名
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_populateGroupFromQuery  groupDesc="A test"
```

アプリケーション・ユーザー・トランスレーションの実行

「アプリケーション・ユーザー・トランスレーション構成」画面で構成済みのすべてのアプリケーションのユーザー定義をインポートします。 これは「アプリケーション・ユーザー・トランスレーション構成」画面から「今すぐ 1 回実行」を実行することに相当します。

注: この grdapi を実行するには、「アプリケーション・ユーザー・トランスレーション構成」画面で「アプリケーション・ユーザー検出」を 1 つ以上定義する必要があります。 定義しないと、メッセージが表示されます。

表 6. アプリケーション・ユーザー・トランスレーションの実行

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_appUserTranslation
```

未解析ログ処理の実行

未解析ログ情報を内部データベースにマージします。 「未解析ログ処理」画面から「今すぐ 1 回実行」を実行することに相当します。

注: この grdapi は、「未解析ログ処理」画面で「未解析ログ処理」が「処理」として構成されている場合のみ実行できます。 そうでない場合、エラー・メッセージが表示されます。

表 7. 未解析ログ処理の実行

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_flatLogProcess
```

インシデント生成プロセスの実行

ポリシー違反ログに対して、選択されたインシデント生成プロセスに定義されている照会を実行します。 その照会に基づいてインシデントが生成されます。 「インシデント生成プロセスの編集」画面から「今すぐ 1 回実行」を実行することに相当します。

注: この API を呼び出す前にインシデント生成プロセスを作成してください。

インシデント生成プロセスは固有の名前を持たないため、特定のインシデント生成プロセスを識別するには、processID または queryName を使用できます。

この grdapi は次の 2 とおりの方法で呼び出すことができます。

- execute_incidentGenProcess
- execute_incidentGenProcess_byDetails

表 8. インシデント生成プロセスの実行

パラメーター	記述
processID	インシデントのプロセス ID
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_incidentGenProcess   processId=20003
```

表 9. execute_incidentGenProcess_byDetails

パラメーター	記述
queryName	照会名
categoryName	カテゴリー名
user	ユーザー
threshold	しきい値
severity	重大度レベル
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi  execute_incidentGenProcess_byDetails  queryName="Policy Violation Count" user=admin severity=info
```

カスタム・データのアップロード - 分類プロセスの実行 (サブミット)

tableName で指定されたカスタム表にデータをアップロードします。 カスタム表ビルダーの「データのインポート」画面から「アップロード」を実行することに相当します。この grdapi を実行するには、カスタム表ビルダーの「表構造のインポート」画面で、指定されたカスタム表を構成しておく必要があります。 UI から「ツール」/「レポート・ビルダー」/「カスタム表ビルダー」と移動し、カスタム表を選択して「データのアップロード」をクリックし、データ・ソースを選択します。

注: tableName は、既存のカスタム表の名前を指定します。

表 10. カスタム・データのアップロード - 分類プロセスの実行 (サブミット)

パラメーター	記述
tableName	カスタム表の名前

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi upload_custom_data tableName="TEST_TABLE"
```

LDAP ユーザーのインポート

「LDAP ユーザーのインポート」画面で構成されている LDAP サーバーから Guardium ユーザー定義をインポートします。「LDAP ユーザーのインポート」画面から「今すぐ 1 回実行」を実行することに相当します。(accessmgr としてログインし、「LDAP インポート」を選択します)

注: LDAP を構成する必要があります。構成していないと、エラー・メッセージが表示されます。

表 11. LDAP ユーザーのインポート

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi execute_ldap_user_import
```

ポリシーのインストール

ポリシーを 1 つ、または複数インストールします。 複数のポリシーをインストールする場合、インストールしたい順番でポリシーを指定して、パイプ文字「|」で区切る必要があります。 これは 1 つのポリシーしか変更していない場合でも行う必要があります。

複数のポリシーをインストールする場合は、grdapi policy_install コマンドを使用します。 インストールしたい順番でポリシーを指定して、位置ごとにインストールします。

UI の場合であっても、別のインストール済みポリシーの後にポリシーをインストールすると、それらはすべて再インストールされますが、これは grdapi policy_install コマンドの場合と同じです。

表 12. ポリシーのインストール

パラメーター	記述
policy	ポリシー名
api_target_host	一元管理構成に限り、API が実行されるターゲット・ホストを指定できます。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi policy_install policy="Policy 1|Policy 2"
```

```
grdapi policy_install policy="policy 20|policy 30|policy 40"
```

ポリシーの削除

delete_policy コマンドは、policyDesc パラメーターで指定したポリシーを削除する場合に使用します。

表 13. ポリシーの削除

パラメーター	記述
policyDesc	ポリシー名。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_policy policyDesc="Hadoop Policy"
```

ポリシーのリスト

list_policy コマンドは、使用可能なポリシーのリストを表示する場合、または単一のポリシーに関する詳細を表示する場合に使用します。

表 14. ポリシーのリスト

パラメーター	記述
policyDesc	ポリシー名。未指定の場合、list_policy コマンドは、使用可能なポリシーのリストを返します。
detail	値 true または false を受け入れます。 デフォルト値は true で、ポリシーの詳細を返します。 値 false を指定すると、ポリシー名のみが返されます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

特定のポリシーの詳細を表示するには、以下のようにします。

```
grdapi list_policy policyDesc="Hadoop Policy"
```

使用可能なポリシーの詳細リストを表示するには、以下のようにします。

```
grdapi list_policy
```

詳細なしで、使用可能なポリシー名のリストを表示するには、以下のようにします。

```
grdapi list_policy detail=false
```

単一のポリシー・ルールのコピー

<fromPolicy> のルール <ruleDesc> を <toPolicy> のルールのリストの最後にコピーします。

注: <fromPolicy> のルールは、<toPolicy> のルールのリストの最後にコピーされます。 この grdapi を実行する前に、<fromPolicy> と <toPolicy> の両方を作成する必要があります。

表 15. 単一のポリシー・ルールのコピー

パラメーター	記述
ruleDesc	ルールの記述
fromPolicy	ポリシー名
toPolicy	ポリシー名
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi copy_rule ruleDesc="Rule Description" fromPolicy="policy1"  toPolicy=" policy2  "
```

ポリシーのコピー作成

この GuardApi コマンドは、ポリシーのコピーを作成するために使用します。

表 16. ポリシーのコピー作成

パラメーター	記述
policyDesc	ポリシー名
clonedpolicyDesc	コピーしたポリシー名
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi clone_policy policyDesc="Hadoop Policy" clonedPolicyDesc="Hadoop Policy cloned1"
```

ポリシー・ルールの更新

<fromPolicy> のルール <ruleDesc> をルール・パラメーターに従って更新します。

update_rule API 呼び出しで変更できる以下のポリシー・ルール・パラメーターの追加情報については、『ポリシー』を参照してください。

表 17. ポリシー・ルールの更新

パラメーター	記述
ruleDesc	ルールの記述
fromPolicy	ポリシー名
newDesc	新しいルールの記述
clientIP	クライアント IP
clientNetMask	クライアント・ネットマスク
serverIP	サーバー IP
serverNetMask	サーバー・ネットマスク
objectName	オブジェクト名
sourceProgram	ソース・プログラム
dbName	データベース名
dbUser	データベース・ユーザー
command	コマンド
appUserName	アプリケーション・ユーザー名
dateTime	日時
logFlag	ログ・フラグ
exceptionType	例外タイプ
minCount	最小カウント
continueToNext	次を続行
resetInterval	リセット間隔
serviceName	サービス名
osUser	O/S ユーザー
dbType	データベース・タイプ
netProtocol	ネット・プロトコル
clientMac	クライアント MAC
fieldName	フィールド名
pattern	パターン

パラメーター	記述
appEventExists	アプリケーション・イベントの存在
eventType	イベント・タイプ
appEventStrValue	アプリケーション・イベントの文字列値
appEventNumValue	アプリケーション・イベントの数値
appEventDate	アプリケーション・イベントの日付
eventUserName	イベント・ユーザー名
errorCode	エラー・コード
severity	重大度
category	カテゴリー
classification	分類
dataPattern	データ・パターン
sqlPattern	SQL パターン
xmlPattern	XML パターン
mvcSystem	MVS™ システム
clientIpNotFlag	「クライアント IP」の「Not」フラグ
serverIpNotFlag	「サーバー IP」の「Not」フラグ
objectNameNotFlag	「オブジェクト名」の「Not」フラグ
sourceProgramNotFlag	「ソース・プログラム」の「Not」フラグ
dbNameNotFlag	「データベース名」の「Not」フラグ
dbUserNotFlag	「データベース・ユーザー」の「Not」フラグ
commandNotFlag	「コマンド」の「Not」フラグ
appUserNameNotFlag	「アプリケーション・ユーザー名」の「Not」フラグ
exceptionTypeIdNotFlag	「例外タイプ ID」の「Not」フラグ
serviceNameNotFlag	「サービス名」の「Not」フラグ
osUserNotFlag	「O/S ユーザー」の「Not」フラグ
clientMacNotFlag	「クライアント MAC」の「Not」フラグ
fieldNameNotFlag	「フィールド名」の「Not」フラグ
errorCodeNotFlag	「エラー・コード」の「Not」フラグ
replacementChar	置換文字
messageTemplate	メッセージ・テンプレート
recordsAffectedThreshold	影響を受けるレコードしきい値
matchedReturnedTreshold	一致戻りしきい値
clientIpGroup	クライアント IP グループ
serverIpGroup	サーバー IP グループ
objectGroup	オブジェクト・グループ
objectCommandGroup	オブジェクト・コマンド・グループ
objectFieldGroup	オブジェクト・フィールド・グループ
dbUserGroup	データベース・ユーザー・グループ
commandsGroup	コマンド・グループ
dbNameGroup	データベース名グループ
sourceProgramGroup	ソース・プログラム・グループ
appUserGroup	アプリケーション・ユーザー・グループ
serviceNameGroup	サービス名グループ
osUserGroup	O/S ユーザー・グループ
netProtocolGroup	ネット・プロトコル・グループ
fieldNameGroup	フィールド名グループ
errorGroup	エラー・グループ
appEventStrGroup	アプリケーション・イベントの文字列グループ
clientProgramUserServerInstanceGroup	クライアント・プログラム・ユーザー・サーバー・インスタンス・グループ

パラメーター	記述
quarantineMinutes	隔離分数
clientInfo	DB2 と DB2_COLLECTION_PROFILE に使用します
clientInGroup	DB2_COLLECTION_PROFILE に使用します
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi update_rule ruleDesc="Rule Description" fromPolicy="policy1"  serviceName="ANY"
```

ポリシー・ルールの順序の変更

ポリシー内のルールの順序位置を変更します。

表 18. ポリシー・ルールの順序の変更

パラメーター	記述
fromPolicy	ポリシー名
order	ルールの新しい順序位置
ruleDesc	ルールの記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi change_rule_order ruleDesc="Copy of policy1 exception1"  fromPolicy="policy1"  order=10
```

ポリシー・ルールのリスト

ポリシーのルールをリストします。

表 19. ポリシー・ルールのリスト

パラメーター	記述
policy	ポリシー名
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_policy_rules  policy="policy1"
```

ポリシー・ルールの削除

ポリシーからルールを削除します。

表 20. ポリシー・ルールの削除

パラメーター	記述
fromPolicy	ポリシー名
toPolicy	ポリシー名
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_rule ruleDesc="Copy (3) of policy1 exception1"  fromPolicy="policy1"
```

ポリシー・ルールのアンインストール

uninstall_policy_rule コマンドは、policy パラメーターおよび ruleName パラメーターで指定したポリシー・ルールをアンインストールする場合に使用します。

表 21. ポリシー・ルールの再インストール

パラメーター	記述
policy	ポリシー名。
ruleName	ルール名 (複数可)。複数のポリシー・ルールを指定する場合は、パイプ文字を使用します (例えば、`ruleName="rule1|rule2|rule3"`)。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

単一のポリシー・ルールをアンインストールするには、以下のようにします。

```
grdapi uninstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow"
```

複数のポリシー・ルールをアンインストールには、以下のようにします。

```
grdapi uninstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow|Low Interest Commands: Allow"
```

ポリシー・ルールの再インストール

reinstall_policy_rule コマンドは、policy パラメーターおよび ruleName パラメーターで指定したポリシー・ルールを再インストールする場合に使用します。

表 22. ポリシー・ルールの再インストール

パラメーター	記述
policy	ポリシー名。
ruleName	ルール名 (複数可)。複数のポリシー・ルールを指定する場合は、パイプ文字を使用します (例えば、`ruleName="rule1|rule2|rule3"`)。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

単一のポリシー・ルールを再インストールするには、以下のようにします。

```
grdapi reinstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow"
```

複数のポリシー・ルールを再インストールするには、以下のようにします。

```
grdapi reinstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow|Low Interest Commands: Allow"
```

監査プロセスの結果の削除

このコマンドは、監査プロセスの結果を削除するために使用します。

表 23. 監査プロセスの結果の削除

パラメーター	記述
ExecutionDateFrom	監査プロセスが開始した時期
ExecutionDateTo	監査プロセスが終了した時期
ProcessName	必須。監査プロセスの名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_Audit_process_result ExecutionDateFrom=, ExecutionDateTo=, ProcessName=abab
```

ドメイン・エンティティーと属性への API パラメーターのマップ

API パラメーターをドメイン・エンティティーと属性にマップします。これによって API 呼び出し生成または API 自動化でのレポート値でパラメーターを設定することができます。

注: 『GuardAPI 入力プロセスの生成』の『GuardAPI パラメーターのドメイン・エンティティーおよび属性へのマッピング』には、システムのドメイン、エンティティー、および属性が示され、この API 関数を呼び出す GUI インターフェースがあります。

表 24. ドメイン・エンティティーと属性への API パラメーターのマップ

パラメーター	記述
functionName	API 関数の名前
parameterName	マップされる API 関数内のパラメーターの名前
domain	「アクセス」、「アラート」、「ディスカバーされたインスタンス」、「例外」、「グループのトラッキング」など、Guardium レポート・ドメインのいずれか。
entityLabel	レポート・ドメインの任意のエンティティー
attributeLabel	エンティティー内の任意の属性
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_api_parameter_mapping functionName="create_group" parameterName="desc" domain="Group Tracking" entityLabel="Group"
attributeLabel="Group Description"
```

ドメイン・エンティティーと属性への API パラメーターのマッピングのリスト

API 関数のパラメーター・マッピングをリストします。

注: 『GuardAPI 入力プロセスの生成』の『GuardAPI パラメーターのドメイン・エンティティーおよび属性へのマッピング』には、システムのドメイン、エンティティー、および属性が示され、この API 関数を呼び出す GUI インターフェースがあります。

表 25. ドメイン・エンティティーと属性への API パラメーターのマッピングのリスト

パラメーター	記述

パラメーター	記述
functionName	API 関数の名前
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi list_param_mapping_for_function functionName="create_group"
```

ドメイン・エンティティーと属性への API パラメーターのマッピングの削除

API 関数のパラメーター・マッピングを削除します。

注: 『GuardAPI 入力プロセスの生成』の『GuardAPI パラメーターのドメイン・エンティティーおよび属性へのマッピング』には、システムのドメイン、エンティティー、および属性が示され、この API 関数を呼び出す GUI インターフェースがあります。

表 26. ドメイン・エンティティーと属性への API パラメーターのマッピングの削除

パラメーター	記述
functionName	API 関数の名前
parameterName	マップされる API 関数内のパラメーターの名前
domain	「アクセス」、「アラート」、「ディスカバーされたインスタンス」、「例外」、「グループのトラッキング」など、Guardium レポート・ドメインのいずれか。
entityLabel	レポート・ドメインの任意のエンティティー
attributeLabel	エンティティー内の任意の属性
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_api_parameter_mapping functionName="create_group" parameterName="desc" domain="Group Tracking" entityLabel="Group"
attributeLabel="Group Description"
```

特定のプロセス/タスク/実行に定義されているすべてのイベントのクローズ

レポート・タイプのタスクに対する特定のプロセス/タスク/実行に定義されたイベントをすべてクローズします。 特に大量のレコードを返したデフォルトのイベントを持つタスクが存在する場合などに必要です。このようなタスクはすべてのイベントがクローズされない限り割り当てることができません。

表 27. 特定のプロセス/タスク/実行に定義されているすべてのイベントのクローズ

パラメーター	記述
eventStatus	必須。イベント状況。 監査タスクに定義されたデフォルトのイベントに有効な状況でなければならず、最終状況でなければなりません。
execDate	必須。実行の日時
processDesc	必須。監査プロセスの記述。
taskDesc	必須。監査タスクの記述。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi close_default_events eventStatus=Done execDate="2010-03-01 08:00:00" processDesc="Audit Process" taskDesc="Task Description"
```

create_quarantine_allowed_until

ポリシーで使用。

表 28. create_quarantine_allowed_until

パラメーター	記述
allowedUntil	必須。
dbUser	必須。データベース・ユーザー
serverIP	必須。サーバー IP
serverName	必須。サーバー名
タイプ	必須。値は、normal、DB2z、または IMS のいずれかでなければなりません。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

create_quarantine_until

ポリシーで使用。

表 29. create_quarantine_until

パラメーター	記述
quarantineUntil	必須。
dbUser	必須。データベース・ユーザー
serverIP	必須。サーバー IP
serverName	必須。サーバー名
タイプ	必須。値は、normal、DB2z、または IMS のいずれかでなければなりません。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

delete_quarantine_until

ポリシーで使用。

表 30. delete_quarantine_until

パラメーター	記述

パラメーター	記述
quarantineUntil	必須。
dbUser	必須。データベース・ユーザー
serverIP	必須。サーバー IP
serverName	必須。サーバー名
タイプ	必須。値は、normal、DB2z、または IMS のいずれかでなければなりません。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

must_gather

grdapi must_gather コマンドは、Guardium サポートが使用できる Guardium システムの状態に関する情報を収集するために使用します。 詳細は、IBM サポートのための基本情報を参照ください。

表 31. must_gather

パラメーター	記述
commandsList	文字列 - 必須
description	文字列 - 必須
duration	整数 - 必須
emailDestination	文字列 - 必須
invokingUser	文字列 - 必須
maxLength	整数 - 必須
pmrNumber	文字列 - 必須
start	日付 - 必須
timestamp	日付 - 必須
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

restart_job_queue_listener

ジョブ・キューの開始に失敗した場合、ジョブ・キューで待機中のジョブが実行されない場合、または長時間にわたってジョブが実行中状況または停止中状況のままになっているように思われる場合は、restart_job_queue_listener コマンドを使用してジョブ・キュー・リスナーを再始動します。このコマンドを発行すると、ジョブ・キューが即時に再始動され、現在実行中のすべてのジョブが停止され、再始動されます。

例:

```
grdapi restart_job_queue_listener
```

restart_job_queue_listener コマンドは、いかなるパラメーターも受け入れません。

update_quarantine_allowed_until

ポリシーで使用。

表 32. update_quarantine_allowed_until

パラメーター	記述
allowedUntil	必須。
dbUser	必須。データベース・ユーザー
serverIP	必須。サーバー IP

パラメーター	記述
serverName	必須。サーバー名
タイプ	必須。値は、normal、DB2z、または IMS のいずれかでなければなりません。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

update_quarantine_until

ポリシーで使用。

表 33. update_quarantine_until

パラメーター	記述
quarantineUntil	必須。
dbUser	必須。データベース・ユーザー
serverIP	必須。サーバー IP
serverName	必須。サーバー名
タイプ	必須。値は、normal、DB2z、または IMS のいずれかでなければなりません。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

親トピック: GuardAPI リファレンス

GuardAPI 照会再書き込み関数

コマンド行インターフェースで Guardium API を使用して、ユーザー・インターフェースから実行できない特定の複雑な照会のテストを自動化したり、そうした照会の定義を作成したりします。

注: API を使用して照会再書き込み定義を作成した場合でも、UI を使用して、「照会再書き込みビルダー」でテストするためにその定義を取得できます。

照会再書き込みに関係した GuardAPI 関数には、以下のものがあります。

assign_qr_condition_to_action

create_qr_action

create_qr_add_where

create_qr_add_where_by_id

create_qr_condition

create_qr_definition

create_qr_replace_element

create_qr_replace_element_byId

list_qr_action

list_qr_add_where

list_qr_add_where_by_id

list_qr_condition

list_qr_condition_to_action

list_qr_definitions

list_qr_replace_element

list_qr_replace_element_byId

remove_all_qr_replace_elements

remove_all_qr_replace_elements_byId

remove_qr_action

remove_qr_add_where_by_id

remove_qr_condition

remove_qr_definition

remove_qr_replace_element_byId

update_qr_action

update_qr_add_where_by_id

update_qr_condition

update_qr_definition

update_qr_replace_element_byId

assign_qr_condition_to_action

照会再書き込み条件と関連アクションの間に関連付けを作成します。

パラメーター	記述
actionName	必須。照会再書き込みアクションの名前。
conditionName	必須。指定したアクションに関連付ける照会再書き込み条件の名前。
definitionName	必須。指定した条件およびアクションに関連付ける照会再書き込み定義の名前。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi assign_qr_condition_to_action definitionName="case 15" actionName="qr action15_2" conditionName="qr cond15_2"
```

create_qr_action

指定した照会再書き込み定義に対する照会再書き込みアクションを作成します。

パラメーター	記述
actionName	必須。照会再書き込みアクションの固有の名前。
definitionName	必須。当該アクションに関連付ける照会再書き込み定義。
description	説明 (オプション)。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi create_qr_action definitionName="case 15" actionName="qr action15_3"
```

create_qr_add_where

照会再書き込み関数を関連付け、指定した照会再書き込みアクションに WHERE 条件を追加します。

パラメーター	記述
actionName	必須。照会再書き込みアクションの固有の名前。
definitionName	必須。当該アクションに関連付ける照会再書き込み定義。
whereText	WHERE 節に追加するテキスト。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi create_qr_add_where definitionName="qrw_def_Oracle_1" actionName="qrw_act__addwhere_id2" whereText="id=2"

create_qr_add_where_by_id

照会再書き込み関数を関連付け、指定した照会再書き込みアクションに WHERE 条件を追加します。

パラメーター	記述
qrActionId	必須 (整数)。照会再書き込みアクションの固有の ID。
whereText	WHERE 節に追加するテキスト。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi create_qr_add_where_by_id qrActionId=10002 whereText="id=2"

create_qr_condition

照会再書き込み条件を作成します。

パラメーター	記述
conditionName	必須。当該照会再書き込み条件の固有の名前。
definitionName	必須。当該条件に関連付ける照会再書き込み定義。
depth	当該条件が適用される、解析された SQL の深さを指定する整数 (1 以上)。デフォルトの -1 の場合、照会再書き込み条件が、すべての深さのすべての一致する SQL に適用されます。
isForAllRuleObjects	True または false。このパラメーターは、ポリシー・アクセス・ルール内のオブジェクトに当該条件を関連付ける場合に使用します。true の場合、指定した条件が、実行されたルールのアクセス・ルールのオブジェクト・フィールドまたはオブジェクト・グループ内のすべてのオブジェクトに適用されます。デフォルトは false であり、当該条件で定義されているオブジェクトを使用して照会条件が指定されます。いずれのオプションも、ルールをトリガーする動作に影響しません。
isForAllRuleVerbs	True または false。このパラメーターは、ポリシー・アクセス・ルール内のオブジェクトに当該条件を関連付ける場合に使用します。true の場合、指定した条件が、実行されたルールのアクセス・ルールの verb フィールドまたは verb グループ内のすべての verb に適用されます。デフォルトは false であり、当該条件で定義されている verb を使用して照会条件が指定されます。いずれのオプションも、ルールをトリガーする動作に影響しません。
isObjectRegex	True または false。正規表現を使用して、指定したオブジェクトを指定することを指示します。デフォルトは false です。
isVerbRegex	True または false。正規表現を使用して、指定した verb を指定することを指示します。デフォルトは false です。
object	オブジェクト (表、ビュー)。デフォルトの「*」は、すべてのオブジェクトを意味します。これは、正規表現として指定することもできます。その場合、isVerbRegex を true に設定します。
order	複雑な SQL の複数の関連した照会再書き込み条件を組み立てる順序を指定するために使用します。デフォルトは 1 です。
verb	verb (select (選択)、insert (挿入)、update (更新)、delete (削除))。 デフォルトの「*」は、すべての verb を意味します。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi create_qr_condition definitionName="case 15" conditionName="qr cond15_3" verb=select isForAllRuleObjects=false object=* depth=2 order=3

create_qr_definition

照会再書き込み定義を作成します。

パラメーター	記述
dataBaseType	必須。当該照会再書き込み定義を関連付けるデータベースのタイプ。許容値は ORACLE または DB2 です。
definitionName	必須。当該照会再書き込み定義条件の固有の名前。
description	説明 (オプション)。
isNegateQrCond	この定義に関連付けられている照会再書き込み条件セットに NOT フラグがあるかどうかを示します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi create_qr_definition dataBaseType="ORACLE" definitionName="case 15"

create_qr_replace_element

SQL 文全体や SELECT リストなど、置換要素または置換要素セットを作成します。

パラメーター	記述
actionName	必須。当該再書き込み関数を関連付ける照会再書き込みアクションの固有の名前。
definitionName	必須。当該照会再書き込み定義条件の固有の名前。
isFromAllRuleElements	True または false。当該アクションがすべての FROM 要素に適用されることを指示します。デフォルトは false です。
isFromRegex	True または false。正規表現を使用して「from」要素を指定することを指示します。デフォルトは false です。
isReplaceToFunction	True または false。「replaceTo」が関数 (ユーザー定義関数など) の名前であることを指示します。
replaceFrom	置き換え元となる、一致するルールの入力文字列。調べる入力照会の要素を具体的に指示するには、replaceType を使用します。
replaceTo	一致する要素の置換文字列。
replaceType	必須。置き換え対象を指示します。 次のいずれかでなければなりません。 • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi create_qr_replace_element definitionName="case 15" actionName="qr action15_2" replaceType=VERB replaceFrom="select" replaceTo="select++"

create_qr_replace_element_byId

指定した照会再書き込みアクションに対して置換仕様を作成します。

パラメーター	記述
isFromAllRuleElements	True または false。当該アクションがすべての FROM 要素に適用されることを指示します。デフォルトは false です。
isFromRegex	True または false。正規表現を使用して from 要素を指定することを指示します。デフォルトは false です。
isReplaceToFunction	True または false。「replaceTo」が関数 (ユーザー定義関数など) の名前であることを指示します。
qrActionId	必須 (整数)。照会再書き込みアクションの固有の ID。
replaceFrom	置き換え元となる、一致するルールの入力文字列。調べる入力照会の要素を具体的に指示するには、replaceType を使用します。
replaceTo	一致する要素の置換文字列。
replaceType	必須。置き換え対象を指示します。 次のいずれかでなければなりません。 • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi create_qr_replace_element_byId qrActionID="1116" replaceType=OBJECT replaceFrom="employee" replaceTo="employee_2"

list_qr_action

指定した照会定義の照会アクションをリストします。

パラメーター	記述
actionName	照会再書き込みアクションの名前。
definitionName	必須。照会再書き込み定義名。
detail	True または false。デフォルトは true であり、アクションの関連付けられているすべての属性がリストされます。false の場合、名前のみが返されます。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi list_qr_action definitionName="case 2"

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_action definitionName="case 2"
######################################################################


         QR actions of definition 'case 2' - (id = 1 )

######################################################################
qr action ID: 1
qr action name: qr action2
qr action description: add where by id

ok
例:
grdapi list_qr_action definitionName="case 2" detail=false

Output:

qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_action definitionName="case 2" detail=false
################################
         QR actions of definition 'case 2' - (id = 1 )
################################
qr action2
ok
```

list_qr_add_where

指定した照会アクションと照会定義のペアの「add where」関数をリストします。

パラメーター	記述
actionName	照会再書き込みアクションの名前。
definitionName	必須。照会再書き込み定義名。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi list_qr_add_where actionName="qrw_act_addwhere_id2" definitionName="qrw_def_Oracle_1"

list_qr_add_where_by_id

指定した照会アクションの「add where」関数をリストします。

パラメーター	記述
qrActionId	必須 (整数)。照会再書き込みアクションの固有 ID。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi list_qr_add_where_by_id qrActionId=20023

list_qr_condition

特定の照会再書き込み定義に関連付けられている照会再書き込み条件をリストします。

パラメーター	記述
conditionName	照会再書き込み条件の名前。
definitionName	必須。照会再書き込み定義。
detail	True または false。デフォルトは true であり、条件の関連付けられているすべての属性がリストされます。false の場合、名前のみが返されます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi list_qr_condition definitionName="case 2" conditionName="qr cond2"

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_condition definitionName="case 2" conditionName="qr cond2"
########################################################################
         QR Condtions of Definition 'case 2' - (id = 1 )

########################################################################

qr condition id: 1
qr condition name: qr cond2
qr definition ID: 1
qr condition verb: *
qr condition object: *
qr condition dept: -1
is verb regex: false
is object regex: false
is action for all rule verbs: false
is action for all rule objects: false
qr condition order: 1
```

list_qr_condition_to_action

特定の照会定義について、照会再書き込み条件と照会再書き込みアクションの間の関連付けをリストします。

パラメーター	記述
actionName	必須 (整数)。照会再書き込みアクションの固有 ID。
definitionName	必須。照会再書き込み定義。
Detail	True または false。デフォルトは true であり、指定したアクションおよび定義の条件の関連付けられているすべての属性がリストされます。false の場合、名前のみが返されます。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi list_qr_condition_to_action actionName="qr action15_2" definitionName="case 15"

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_condition_to_action actionName="qr action2" definitionName="case 2"
########################################################################

         QR Condtions of Action 'qr action2' - (id = 1 )

########################################################################

qr condition id: 1
qr condition name: qr cond2
qr definition ID: 1
qr condition verb: *
qr condition object: *
qr condition dept: -1
is verb regex: false
is object regex: false
is action for all rule verbs: false
is action for all rule objects: false
qr condition order: 1
```

list_qr_definitions

照会再書き込み定義をリストします。

パラメーター	記述
definitionName	必須。照会再書き込み定義。
Detail	True または false。デフォルトは true であり、指定したアクションおよび定義の条件の関連付けられているすべての属性がリストされます。false の場合、名前のみが返されます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi list_qr_definitions

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_definitions
########################################################################
         QR  Definitions

########################################################################
qr definition ID: 1
qr definition name: case 2
qr definition description:
is negation set on qr conditions: false
```

list_qr_replace_element

指定した照会再書き込みアクションと照会再書き込み定義のペアに関する置換をリストします。

パラメーター	記述
actionName	必須。照会再書き込みアクション。
definitionName	必須。照会再書き込み定義。

パラメーター	記述
Detail	True または false。デフォルトは true であり、指定したアクションおよび定義の置換要素の関連付けられているすべての属性がリストされます。false の場合、名前のみが返されます。
replaceType	指定する場合、以下のいずれかにする必要があります。 • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi list_qr_replace_element actionName="qr action2" definitionName="case 2"

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_replace_element actionName="qr action2" definitionName="case 2"
########################################################################
         QR replace elements for action 'qr action2' - (qrActionId = 1 )

########################################################################

qr replace element ID: 1
qr replace type: object
qr replace from: emp
qr replace to: NEW_EMP
qr is from regex: false
qr is from all rule elements: false

************************************************************************
qr replace element ID: 2
qr replace type: selectList
qr replace from: Whole select list
qr replace to: EMPNO,SAL
qr is from regex: false
qr is from all rule elements: false
```

list_qr_replace_element_byId

指定した照会再書き込みアクションに関する置換をリストします。

パラメーター	記述
detail	True または false。デフォルトは true であり、指定したアクションおよび定義の置換要素の関連付けられているすべての属性がリストされます。false の場合、名前のみが返されます。
qrActionId	必須 (整数)。照会再書き込みアクションの固有 ID。
replaceType	指定する場合、以下のいずれかにする必要があります。 • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi list_qr_replace_element_byId detail=true qrActionId="22222" replaceType="OBJECT"

remove_all_qr_replace_elements

照会置換仕様をシステムから削除します。

パラメーター	記述
actionName	必須。照会再書き込みアクション。
definitionName	必須 (整数)。照会再書き込みアクションの固有 ID。
replaceType	指定する場合、以下のいずれかにする必要があります。 • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi remove_all_qr_replace_elements definitionName="new case 2" actionName="new qr action2“

remove_all_qr_replace_elements_byId

照会置換仕様をシステムから削除します。

パラメーター	記述
qrActionId	必須 (整数)。照会再書き込みアクション ID。
definitionName	必須。照会再書き込み定義。
replaceType	指定する場合、以下のいずれかにする必要があります。 • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST replaceType が指定されていない場合、指定したアクションおよび定義に関するすべての置換が削除されます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi remove_all_qr_replace_elements actionName="qr action15_2" definitionName="case 15" replaceType="OBJECT"

remove_qr_action

指定した照会再書き込みアクションをシステムから削除します。

パラメーター	記述
actionName	必須。照会再書き込みアクション。
definitionName	必須。照会再書き込み定義。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi remove_qr_action actionName="qr action15_2" definitionName="case 15"

remove_qr_add_where_by_id

指定した「add where」関数をシステムから削除します。

パラメーター	記述
qrAddWhereId	必須 (整数)。「add where」関数。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi remove_qr_add_where_by_id qrAddWhereId=22666

remove_qr_condition

照会再書き込み条件をシステムから削除します。

パラメーター	記述
conditionName	必須。照会再書き込み条件。
definitionName	必須。照会再書き込み定義。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi remove_qr_condition conditionName="qr cond15_1" definitionName="case 15"

remove_qr_definition

照会再書き込み定義をシステムから削除します。

パラメーター	記述
definitionName	必須。照会再書き込み定義。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi remove_qr_definition definitionName="case 15"

remove_qr_replace_element_byId

指定した照会要素置換をシステムから削除します。

パラメーター	記述
qrReplaceElementId	必須 (整数)。置換定義 ID。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi qrReplaceElementId=33333

update_qr_action

新しい名前および説明 (オプション) で、既存の照会再書き込みアクションを更新します。

パラメーター	記述
actionName	必須。照会再書き込みアクションの固有の名前。
definitionName	必須。当該アクションに関連付ける照会再書き込み定義。
description	説明 (オプション)。
newName	照会再書き込みアクションの新規名。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi update_qr_action definitionName="case 2" actionName="qr action2" newName="new qr action2"

update_qr_add_where_by_id

新しい置換テキストで、既存の「add where」関数を更新できます。

パラメーター	記述
qrAddWhereId	必須 (整数)。照会再書き込みの「add where」関数の固有 ID。
whereText	特定された where 節の置換テキスト。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi update_qr_add_where_by_id 22222 whereText="1=2"

update_qr_condition

既存の照会再書き込み条件を更新します。

パラメーター	記述
conditionName	必須。当該照会再書き込み条件の固有の名前。
definitionName	必須。当該条件に関連付ける照会再書き込み定義。
depth	当該条件が適用される、解析された SQL の深さを指定する整数 (1 以上)。デフォルトの -1 の場合、照会再書き込み条件が、すべての深さのすべての一致する SQL に適用されます。
isForAllRuleObjects	True または false。指定した条件が、実行されたルールのすべてのオブジェクトに適用されることを指示します。デフォルトは false です。
isForAllRuleVerbs	True または false。指定した条件が、実行されたルールのすべての verb に適用されることを指示します。デフォルトは false です。
isObjectRegex	True または false。正規表現を使用して、指定したオブジェクトを指定することを指示します。デフォルトは false です。
isVerbRegex	True または false。正規表現を使用して、指定した verb を指定することを指示します。デフォルトは false です。
newName	照会再書き込み条件の新規名。
Object	オブジェクト (表またはビュー)。デフォルトの「*」は、すべてのオブジェクトを意味します。これは、正規表現として指定することもできます。その場合、isVerbRegex を true に設定します。
Order	複雑な SQL の複数の関連した照会再書き込み条件を組み立てる順序を指定するために使用します。デフォルトは 1 です。
verb	verb (select (選択)、insert (挿入)、update (更新)、delete (削除))。 デフォルトの「*」は、すべての verb を意味します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

grdapi update_qr_condition definitionName="case 16" conditionName="qr cond15_3" newName="qr cond16_3" verb=select object=* dept=2 order=3

update_qr_definition

既存の照会再書き込み定義を更新します。

パラメーター	記述
dataBaseType	必須。当該照会再書き込み定義を関連付けるデータベースのタイプ。ORACLE または DB2 のいずれかにする必要があります。
definitionName	必須。当該照会再書き込み定義条件の固有の名前。
description	説明 (オプション)。
isNegateQrCond	この定義に関連付けられている照会再書き込み条件セットに NOT フラグがあるかどうかを示します。
newName	オプション。新しい固有の名前を指定します。
sampleSql	オプション。サンプル SQL ステートメントを指定します。 ほとんどの場合、これを使用することはありません。ただし、UI で入力したサンプル SQL を後で使用する場合を除きます。

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi update_qr_definition dataBaseType="DB2" definitionName="case 15" sampleSql="select EMPNO from EMP where ENAME = (select
ENAME from EMP where SAL = (select SAL from EMP where HIREDATE = to_date('06/09/1981 00:00:00', 'MM/DD/YYYY HH24:MI:SS')))"
newName="DB2_case 15"
```

update_qr_replace_element_byId

指定した照会再書き込みアクションに関する既存の置換仕様を更新します。

パラメーター	記述
isFromAllRuleElements	必須。当該照会再書き込み定義を関連付けるデータベースのタイプ。ORACLE または DB2 のいずれかにする必要があります。
isFromRegex	True または false。正規表現を使用して from 要素を指定することを指示します。デフォルトは false です。
isReplaceToFunction	True または false。「replaceTo」が関数 (ユーザー定義関数など) の名前であることを指示します。
qrReplaceElementId	必須 (整数)。照会再書き込みアクションの固有の ID。
replaceFrom	置き換え元となる、一致するルールの入力文字列。調べる入力照会の要素を具体的に指示するには、replaceType を使用します。
replaceTo	一致する要素の置換文字列。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi update_qr_replace_element_byId qrReplaceElementId=1 isFromAllRuleElements=false isFromRegex=false isReplaceToFunction=false
replaceFrom=emp replaceTo=NEW_EMP_UPDATED
```

親トピック: GuardAPI リファレンス

GuardAPI ロール関数

これらの GuardAPI コマンドは、ロール関数の付与、リスト、および取り消しに使用します。

注: 一元管理環境では、ロールを追加するオブジェクトは、中央マネージャー上または管理対象ユニット上にある場合があります。詳しくは、『統合および一元管理ヘルプ・ブック』の概要を参照してください。

grant_role_to_object_by_id

指定されたオブジェクト (例えば分類プロセス) にロールを追加します。 ロールを追加する前に従属関係がチェックされます。 例えば、分類プロセスにロールを追加するには、その前にその分類プロセスが含むすべてのコンポーネント (分類ポリシーおよび参照されるあらゆるデータ・ソース) にそのロールを割り当てる必要があります。

表 1. grant_role_to_object_by_id

パラメーター	記述

パラメーター	記述
objectTypeId	必須 (整数)。ロールを割り当てるオブジェクトのタイプを識別します。 以下のいずれかの整数でなければなりません。 1=Query 2=Report 3=Alert 4=Baseline 5=Policy 6=SecurityAssessment 7=PrivacySet 8=AuditProcess 12=CustomTable 13=Datasource 14=CustomDomain 15=ClassifierPolicy 16=ClassificationProcess
objectId	必須 (整数)。ロールを割り当てるオブジェクトを識別します。
roleId	必須 (整数)。割り当てるロールを識別します。 既存のロール ID または特殊値 -1 (すべてのロールによるアクセスを許可する) を指定できます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi grant_role_to_object_by_id objectTypeId=13 objectId=2 roleId=3

grant_role_to_object_by_Name

指定されたオブジェクト (例えば分類プロセス) にロールを追加します。 ロールを追加する前に従属関係がチェックされます。 例えば、分類プロセスにロールを追加するには、その前にその分類プロセスが含むすべてのコンポーネント (分類ポリシーおよび参照されるあらゆるデータ・ソース) にそのロールを割り当てる必要があります。パラメーター

表 2. grant_role_to_object_by_Name

パラメーター	記述
objectType	必須。ロールを割り当てるオブジェクトのタイプを識別します。 次のいずれかでなければなりません。 照会 レポート アラート Baseline ポリシー SecurityAssessment PrivacySet AuditProcess CustomTable データ・ソース CustomDomain ClassifierPolicy ClassificationProcess

パラメーター	記述
objectName	必須。 ロールを割り当てるオブジェクト (例えば照会やレポート) の名前。
role	必須。割り当てるロールの名前。 既存のロール、または **all_roles** (すべてのロールによるアクセスを許可する) を指定できます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi grant_role_to_object_by_Name objectType=Datasource objectName= “swanSybase” role=admin

list_roles_granted_to_object_by_id

指定されたオブジェクト (例えば分類プロセス) に割り当てられたロールを表示します。

表 3. list_roles_granted_to_object_by_id

パラメーター	記述
objectTypeId	必須 (整数)。ロールを割り当てるオブジェクトのタイプを識別します。 以下のいずれかの整数でなければなりません。 1=Query 2=Report 3=Alert 4=Baseline 5=Policy 6=SecurityAssessment 7=PrivacySet 8=AuditProcess 12=CustomTable 13=Datasource 14=CustomDomain 15=ClassifierPolicy 16=ClassificationProcess
objectId	必須 (整数)。ロールを割り当てるオブジェクトを識別します。
roleId	必須 (整数)。割り当てるロールを識別します。 既存のロール ID または特殊値 -1 (すべてのロールによるアクセスを許可する) を指定できます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi list_roles_granted_to_object_by_id objectTypeId=7 objectId=1

list_roles_granted_to_object_by_Name

指定されたオブジェクト (例えば分類プロセス) に割り当てられたロールを表示します。

表 4. list_roles_granted_to_object_by_Name

パラメーター	記述

パラメーター	記述
objectType	必須。ロールを割り当てるオブジェクトのタイプを識別します。 次のいずれかでなければなりません。 照会 レポート アラート Baseline ポリシー SecurityAssessment PrivacySet AuditProcess CustomTable データ・ソース CustomDomain ClassifierPolicy ClassificationProcess
objectName	必須。 ロールを割り当てるオブジェクト (例えば照会やレポート) の名前。
role	必須。割り当てるロールの名前。 既存のロール、または **all_roles** (すべてのロールによるアクセスを許可する) を指定できます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi list_roles_granted_to_object_by_Name objectType=PrivacySet objectName="privaceSet 1"

revoke_role_from_object_by_id

指定されたオブジェクト (例えば分類プロセス) からロールを削除します。 従属関係は自動的に処理されます。 例えば、ロール foo を特定の照会から削除した場合、その照会に基づくレポートからもロール foo が削除されます。

表 5. revoke_role_from_object_by_id

パラメーター	記述
objectTypeId	必須 (整数)。ロールを割り当てるオブジェクトのタイプを識別します。 以下のいずれかの整数でなければなりません。 1=Query 2=Report 3=Alert 4=Baseline 5=Policy 6=SecurityAssessment 7=PrivacySet 8=AuditProcess 12=CustomTable 13=Datasource 14=CustomDomain 15=ClassifierPolicy 16=ClassificationProcess
objectId	必須 (整数)。ロールを割り当てるオブジェクトを識別します。

パラメーター	記述
roleId	必須 (整数)。割り当てるロールを識別します。 既存のロール ID または特殊値 -1 (すべてのロールによるアクセスを許可する) を指定できます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi revoke_role_from_object_by_id objectTypeId=13 objectId=5 role=-1

revoke_role_from_object_by_Name

指定されたオブジェクト (例えば分類プロセス) からロールを削除します。 従属関係は自動的に処理されます。 例えば、ロール foo を特定の照会から削除すると、その照会を使用しているレポートからもロール foo が削除されます。

表 6. revoke_role_from_object_by_Name

パラメーター	記述
objectType	必須。ロールを割り当てるオブジェクトのタイプを識別します。 次のいずれかでなければなりません。 照会 レポート アラート Baseline ポリシー SecurityAssessment PrivacySet AuditProcess CustomTable データ・ソース CustomDomain ClassifierPolicy ClassificationProcess
objectName	必須。 ロールを割り当てるオブジェクト (例えば照会やレポート) の名前。
role	必須。割り当てるロールの名前。 既存のロール、または **all_roles** (すべてのロールによるアクセスを許可する) を指定できます。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

grdapi revoke_role_from_object_by_Name objectType=Datasource objectName="swanSybase" role=admin

親トピック: GuardAPI リファレンス

GuardAPI S-TAP® 関数

これらの CLI コマンドは、S-TAP 関数の作成、リスト、削除、再始動、および設定に使用します。

create_stap_inspection_engine

指定された S-TAP に検査エンジンを追加します。S-TAP 構成は、その S-TAP のアクティブな Guardium® ホストからのみ、S-TAP がオンラインである場合に限って変更できます。

表 1. create_stap_inspection_engine

パラメーター	記述
stapHost	必須。S-TAP がインストールされているデータベース・サーバーのホスト名または IP アドレスです。
protocol	必須。データベース・プロトコルです。以下のいずれかの値でなければなりません。 DB2® DB2 出口 (DB2 バージョン 10) FTP Informix® Kerberos Mysql Netezza® Oracle PostgreSQL Sybase Teradata Windows ファイル共有 IE を除外 Windows S-TAP ホストでは、以下のプロトコルも使用できます。 MSSQL named pipes
portMin	必須 (整数)。データベースに構成されている聴取ポート範囲の開始ポート番号です (S-TAP のパフォーマンスが低下するため、大きな包括的範囲を使用しないでください)。
portMax	必須 (整数)。データベースの聴取ポート範囲の終了ポート番号です。
teeListenPort teeRealPort	オプション (整数)。Windows では使用されません。UNIX では、K-TAP モニター・メカニズムが使用される場合、KTAP データベース実ポートに置き換えられます。TEE モニター・メカニズムを使用する場合、これが必須です。聴取ポートは、S-TAP がローカル・データベース・トラフィックを聴取して受け入れるポートです。実ポートは S-TAP がトラフィックを転送するポートです。
connectToIp	オプション (整数)。S-TAP がデータベースへの接続に使用する IP アドレス。デフォルト (127.0.0.1) ではなく、マシンの「実」IP アドレスでのみローカル接続を受け入れるデータベースがあります。
client	必須。モニター対象のクライアントを指定する、クライアント IP アドレスおよび対応するマスクのリスト。IP アドレスがデータベース・サーバーの IP アドレスと同じで、マスク 255.255.255.255 が使用される場合は、ローカル・トラフィックだけがモニターされます。クライアント・アドレス/マスク値 1.1.1.1/0.0.0.0 では、すべてのクライアントがモニターされます (例を参照してください)。
encryption	オプション。ASO 暗号化トラフィックをアクティブにします。encryption=0 (アクティブにしない) または encryption=1 (アクティブにする) です。
excludeClient	オプション。除外されるクライアントを指定する、クライアント IP アドレスおよび対応するマスクのリスト。このオプションを使用すると、特定のクライアントやサブネット (またはこれらのオプションの集合) を除く、すべてのクライアントをモニターするように S-TAP を構成できます。
procNames	Windows サーバーの場合: Oracle または MS SQL Server のみ (名前付きパイプが使用される場合)。Oracle では、通常、2 つの項目 oracle.exe、tnslsnr.exe がリストに含まれます。MS SQL Server では、通常、リストは 1 つの項目 sqlservr.exe だけです。
namedPipe	Windows のみ。名前付きパイプの名前を指定します。名前付きパイプを使用し、ここで何も指定しなければ、S-TAP はレジストリーから名前付きパイプ名を取得します。
ktapDbPort	オプション (整数)。Windows では使用されません。UNIX では、K-TAP モニター・メカニズムが使われる場合にのみ使用されます。K-TAP メカニズムによってモニターされるデータベース・ポートを識別します。
dbInstallDir	UNIX のみ。データベース・インストール・ディレクトリーの絶対パス名を入力します。例: /home/oracle10
procName	UNIX サーバーの場合: DB2、Oracle、または Informix データベースでは、データベース実行可能ファイルの絶対パス名を入力します。例: /home/oracle10/prod/10.2.0/db_1/bin/oracle
procNames	オプション

パラメーター	記述
db2SharedMemAdjustment db2SharedMemClientPosition db2SharedMemSize	これらの 3 つのパラメーターは、以下の条件下でのみ DB2 検査エンジンに使用されます。 • DB2 サーバーが Linux で稼働している。 • K-TAP モニター・メカニズムがインストールされている。 • 共有メモリーを使ってクライアントが DB2 に接続する。 これらのパラメーターを使用した場合、grdapi は、プロトコルが db2 であることのみを検証し、条件を満たしているかどうかは検証しません。 これらのパラメーターの使用方法の詳細な説明については、トピック『DB2 Linux の S-TAP 構成パラメーター』を参照してください。
instanceName	オプション (文字列)。MSSQL または Oracle 暗号化トラフィックのみに使用されます。このパラメーターを使用する前に、MSSQL または ORACLE 暗号化フラグをオンにする必要があります。
informixVersion	Informix バージョン
ieIdentifier	オプション (文字列)。
interceptTypes	オプション (文字列)。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi create_stap_inspection_engine stapHost=192.168.2.118 protocol=Oracle portMin=1521 portMax=1521 dbInstallDir=/data/oracle10
procName=/data/oracle10/oracle/product/10.2.0/db_1/bin/oracle client=192.168.0.0/255.255.0.0 ktapDbPort=1521
```

注:

構成が拒否されず、正しくインストールされていても、検査エンジンを追加する場合に、「構成は S-TAP によって拒否されました - 詳細は S-TAP イベント・ログを参照してください」という誤ったメッセージが表示されることがあります。

UNIX S-TAP の場合、クライアント IP/マスクは必須ですが、Windows S-TAP の場合はオプションです。

list_inspection_engines

指定されたホスト上のすべての S-TAP のプロパティーを表示します。オプションとして、特定のデータベース・タイプのみのものを表示します。

表 2. list_inspection_engines

パラメーター	記述
stapHost	必須。S-TAP がインストールされている (およびこの Guardium アプライアンスにレポートするように構成されている) データベース・サーバーのホスト名または IP アドレスです。
type	オプション。 使用した場合、指定されたデータベース・タイプのみの検査エンジンがリストされます。タイプは以下のいずれかになります。 db2 informix mssql mssql-np oracle sybase
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
a1.corp.com> grdapi list_inspection_engines stapHost=192.168.2.33 type=oracle
ID=20162
Stap Host: 192.168.2.33 - Not Active
oracle Inspection Engines:
    name =ORACLE2
    type =ORACLE
        connect to IP=127.0.0.1
        install dir = /home/oracle10
        exec file = /home/oracle10/product/10.2.0/db_1/bin/oracle-guard
        instance name = MSSQLSERVER
        encrypted = no
        port range = 1521 - 1521
tee listen port = null, tee rel port = 1521
                client = 127.0.0.1/255.255.255.255
                client = 192.168.0.0/255.255.0.0
    name =ORACLE3
    type =ORACLE
        connect to IP=127.0.0.1
        install dir = /home/oracle9
        exec file = /home/oracle9/bin/oracle
        instance name = MSSQLSERVER
        encrypted = no
        port range = 1521 - 1521
ok
```

list_staps

S-TAP がこの Guardium システムにレポートする元のデータベース・サーバーを表示し、オプションとして、この Guardium システムがアクティブなホストになる S-TAP を持つサーバー (すなわち、S-TAP がデータを送信する先のサーバー、および S-TAP 構成を変更できるサーバー) のみをリストします。

表 3. list_staps

パラメーター	記述
onlyActive	オプション (ブール値)。この Guardium システムがアクティブなホストになる S-TAP を持つホストのみをリストするには、**true** と入力するか、このパラメーターを省略します。この Guardium システムを 1 次ホストまたはまたは 2 次ホストとして使用するように S-TAP が構成されている、すべてのホストをリストするには、**false** と入力します。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
a1.corp.com> grdapi list_staps onlyActive=false
ID=0
staps:
stap host = FALCON
stap host = 192.168.2.33
stap host = 192.168.2.173
```

stap host = 192.168.2.248

stap host = jumbo

ok

delete_stap_inspection_engine

S-TAP 検査エンジンを削除します。この Guardium システムは、検査エンジンを削除する S-TAP のアクティブ・ホストでなければなりません。

表 4. delete_stap_inspection_engine

パラメーター	記述
stapHost	必須。S-TAP がインストールされているデータベース・サーバーのホスト名または IP アドレスです。
type	必須。削除する検査のタイプを識別します。タイプは以下のいずれかになります。 Cassandra、CouchDB、Db2、Db2 Exit、FTP、GreenPlumDB、Hadoop、HTTP、iSERIES、Informix、KERBEROS、MongoDB、MS SQL、mssql-np、Mysql、名前付きパイプ、Netezza、Oracle、PostgreSQL、SAP Hana、Sybase、Teradata、または Windows ファイル共有
sequence	必須 (整数)。指定されたタイプの一連の検査エンジンのうち、削除される検査エンジンのシーケンス番号です。最初に type オプションを指定して grdapi list_inspection_engines コマンドを使用して、削除される検査エンジンのシーケンス番号を確認できます。
waitForResponse	オプション。API が S-TAP からの応答を待機するかどうかを指定します。 有効な値は 0 (待機しない) および 1 (応答を待機する) です。デフォルトは、stapHost が単一のホスト名または IP アドレスの場合は 1 で、その他の場合はすべて 0 です。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi delete_stap_inspection_engine stapHost=192.168.2.118 type=Oracle sequence=1
```

注: 検査エンジンを削除する場合、削除が成功していても「検査エンジンを削除できませんでした - 指定された検査エンジンが見つかりません」という誤ったメッセージが表示されることがあります。

restart_stap

S-TAP 検査エンジンを再始動します。

表 5. restart_stap

パラメーター	記述
stapHost	必須。S-TAP がインストールされているデータベース・サーバーのホスト名または IP アドレスです。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi restart_stap stapHost=192.168.2.118
```

set_stap_debug

すべてのトラフィックをログにダンプするのではなく、データベース、プロトコル、クライアント情報でログの内容をフィルターに掛けます。

関数パラメーター:

stapDebugInterval - required

stapDebugLevel - required

stapDebugOn - required

stapHost - required

api_target_host

store_stap_approval

この機能を使用して、無許可の S-TAP が Guardium システムに接続することをブロックします。

ON にすると、S-TAP は、特定の承認を得ない限り、接続できなくなります。

承認を得ていない S-TAP は、その S-TAP の IP アドレスに特定の権限が与えられない限り、接続してもすぐに切断されます。

承認されたクライアント用の事前定義レポート「承認済み Tap クライアント」があります。この機能は「日次モニター」タブにあります。

注:

ホスト名ではなく、有効な IP アドレスが必要です。

store_stap_approval コマンドは、IP ロード・バランサーがある環境内では機能しません。

一元管理された環境内では、承認された S-TAP に IP アドレスを追加した後、同期に関連する待ち時間が発生します。この待ち時間は、最大で 1 時間かかる可能性があります。同期が完了すると、承認された S-TAP の状況が GUI に緑色で表示されます。

関数: store_stap_approval

function parameters :

isNeeded - ブール値 - 必須

api_target_host - 文字列

構文

grdapi store_stap_approval ON | OFF

CLI コマンド

「store stap approval」および「show stap approval」

add_approved_stap_client

この GuardAPI コマンドは、承認済み S-TAP クライアントを追加するときに使用します。

この GuardAPI コマンドを使用しても、 スニファーは再始動せず、既に接続している S-TAP への影響もありません。このコマンドは、新しい S-TAP 接続にのみ影響を及ぼします。

関数: add_approved_stap_client

function parameters :

stapHost - 文字列 - 必須

api_target_host - 文字列

構文

grdapi add_approved_stap_client <stapHost>

list_approved_stap_client

この GuardAPI コマンドは、承認済み S-TAP クライアントをリストするときに使用します。

関数: add_approved_stap_client

function parameters :

api_target_host - 文字列

構文

grdapi list_approved_stap_client

list_stap_verification_results

この GuardAPI コマンドは、S-TAP の検査結果をリストするために使用します。

関数パラメーター:

stapHost - 文字列。S-TAP がインストールされているデータベース・サーバーのホスト名または IP アドレスです。

構文

grdapi list_stap_verification_results <stapHost>

delete_approved_stap_client

この GuardAPI コマンドは、承認済み S-TAP クライアントを削除するときに使用します。

この GuardAPI コマンドを使用しても、 スニファーは再始動せず、既に接続している他の S-TAP への影響もありません。このコマンドは、指定した S-TAP 接続にのみ影響を及ぼします。

関数: add_approved_stap_client

function parameters :

stapHost - 文字列 - 必須

api_target_host - 文字列

構文

grdapi delete_approved_stap_client <stapHost - 文字列 - 必須>

set_ktap_debug

ID=0

関数パラメーター:

ktapDebugInterval - required

ktapFunctionNames

stapHost - required

api_target_host

display_stap_config

指定されたホスト上のすべての S-TAP のすべてのプロパティーを表示します。

表 6. display_stap_config

パラメーター	記述
stapHost	必須。S-TAP がインストールされていて、この Guardium システムにレポートするように構成されているデータベース・サーバーのホスト名または IP アドレス、あるいはホスト名または IP アドレスのコンマ区切りのリスト。以下の値を使用することもできます。 all_active この Guardium システムにレポートするように構成されているすべての S-TAP all_windows_active この Guardium システムにレポするように構成され、Windows マシン上で稼働しているすべての S-TAP all_unix_active この Guardium システムにレポートするように構成され、UNIX マシン上で稼働しているすべての S-TAP

例:

```
grdapi display_stap_config stapHost=myhost1,myhost2
grdapi display_stap_config stapHost=all_active
```

update_stap_config

指定されたホスト上のすべての S-TAP のプロパティーを更新します。

表 7. update_stap_config

パラメーター	記述
stapHost	必須。Guardium システムのデータベース・サーバーのホスト名または IP アドレス、あるいはホスト名または IP アドレスのコンマ区切りのリスト。以下の値を使用することもできます。 all_active この Guardium システムにレポートするように構成されているすべての S-TAP all_windows_active この Guardium システムにレポするように構成され、Windows マシン上で稼働しているすべての S-TAP all_unix_active この Guardium システムにレポートするように構成され、UNIX マシン上で稼働しているすべての S-TAP
updateValue	必須。1 つ以上の鍵と値のペア (形式は *section.parameter_name*:*new_value*)。 *section* は、パラメーターが含まれている guard_tap.ini ファイルのセクションを示します。これは TAP または DB_x のいずれかで、DB_x はファイル内のセクション・ヘッダーとして表示される検査エンジンを指定します。 項目をアンパーサンド (&) で区切ることにより、複数のパラメーターに新しい値を指定できます。
waitForResponse	オプション。API が S-TAP からの応答を待機するかどうかを指定します。有効な値は 0 (待機しない) および 1 (応答を待機する) です。デフォルトは、stapHost が単一のホスト名または IP アドレスの場合は 1 で、その他の場合はすべて 0 です。

例:

```
grdapi update_stap_config stapHost=all_windows_active updateValue=TAP.XXXX
```

verify_stap_inspection_engine_with_sequence

このコマンドは、S-TAP 検査エンジンを検証するために使用します。

関数パラメーター:

addToSchedule - 文字列 - 定数値リスト。有効な値は「Yes」および「No」です。

datasourceName - 文字列。このパラメーターを指定した場合、指定したデータ・ソースに対して詳細検査が実行されます。このパラメーターを省略した場合、標準検査が実行されます。

シーケンス - 整数 - 必須 検査のための既存の検査エンジンのシーケンス番号。 最初に type オプションを指定して grdapi list_inspection_engines コマンドを使用して、検査される検査エンジンのシーケンス番号を確認できます。

stapHost - 文字列 - 必須 - S-TAP がインストールされているデータベース・サーバーのホスト名または IP アドレスです。

プロトコル - 必須。データベース・プロトコル。これは、Db2、Db2 Exit (Db2 バージョン 10)、FTP、Informix、Kerberos、Mysql、Netezza、Oracle、PostgreSQL、Sybase、Teradata、Windows ファイル共有、IE を除外、のいずれかの値にしなければなりません。Windows S-TAP ホストでは、プロトコルとして MSSQL、名前付きパイプも使用できます。

例:

```
grdapi verify_stap_inspection_engine_with_sequence stapHost=9.70.144.212
sequence=3
```

revoke_ignore_stap

このコマンドは、S-TAP セッション・トラフィックを無視する既存の「S-TAP セッションを無視 (取り消し可能)」ポリシー・ルール・アクションを取り消します。このコマンドは、ソフトな無視ルール (「取り消し可能」とマークされているもの) のみを取り消し、ハードなルール (「取り消し可能」とマークされていないもの) を取り消すことはできません。

表 8. revoke_ignore_stap

パラメーター	記述
stapHost	必須。S-TAP がインストールされていて、この Guardium システムにレポートするように構成されているデータベース・サーバーのホスト名または IP アドレス、あるいはホスト名または IP アドレスのコンマ区切りのリスト。以下の値を使用することもできます。 all_active この Guardium システムにレポートするように構成されているすべての S-TAP all_windows_active この Guardium システムにレポするように構成され、Windows マシン上で稼働しているすべての S-TAP all_unix_active この Guardium システムにレポートするように構成され、UNIX マシン上で稼働しているすべての S-TAP
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例

```
grdapi revoke_ignore_stap stapHost=myhost1
```

set_ztap_logging_config

このコマンドは、後述のロギング・パラメーターを制御します。

構文: grdapi set_stap_logging_config parameter=[parameter] value=[value]。

表 9. set_ztap_logging_config パラメーター

パラメーター	値	記述
log_db2z_target	0 (使用不可にする場合) 1 (使用可能にする場合) パラメーターは、デフォルトでは使用不可になっています。	`log_db2z_target=1` を使用して使用可能にすると、db2z protobuf メッセージ内のターゲットは、パーサーからのオブジェクトに加えて、GDM_OBJECT にも記録されます。
log_zkey_to_full_sql	0 (使用不可にする場合) 1 (使用可能にする場合) パラメーターは、デフォルトでは使用不可になっています。	`log_zkey_to_full_sql=1` を使用して使用可能にすると、VSAM または IMS キー値が、「全詳細をロギング」を使用したポリシーの完全な SQL ステートメントにログインします。

例

```
grdapi set_ztap_logging_config parameter=log_db2z_target value=1
```

値の表示: grdapi get_ztap_logging_config。

親トピック: GuardAPI リファレンス

GuardAPI 脅威検出分析機能

enable_advanced_threat_scanning

特定のデータベース攻撃 (SQL インジェクションや悪意のあるストアード・プロシージャーなど) がないか検査するスキャナー・プロセスを有効にします。

表 1. enable_advanced_threat_scanning のパラメーター

パラメーター	記述
すべて	オプション。一元管理構成に限り、すべての管理対象ユニット上のすべての脅威検出スキャナーを有効にします。指定可能な値: `true`、`false`。
schedule_start	オプション。プロセスの実行を開始する日時を指定します。許容される形式は、yyyy-mm-dd hh:mm:ss (24 時間クロック) です。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi enable_advanced_threat_scanning all=true schedule_start="2016-03-24 12:00:05”
```

異常値検出が無効になっているときに脅威分析が有効になっている場合は、以下のメッセージが表示されます。

```
Warning - Enabling advance threat scanning (AKA Eagle Eye) when Analytic anomaly detection is disabled.
Advance threat scanning (AKA Eagle Eye) enabled.
ok
```

disable_advanced_threat_scanning

コレクター上の脅威検出スキャナーを無効にします。

表 2. disable_advanced_threat_scanning のパラメーター

パラメーター	記述
すべて	一元管理構成に限り、すべての管理対象ユニット上のすべての脅威検出スキャナーを無効にします。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

get_eagle_eye_info

脅威検出パラメーターの現在の設定を表示します。

表 3. get_eagle_eye_info のパラメーター

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi get_eagle_eye_info
Eagle Eye Parameters Values:
EI_CASES_DISPLAY_LIMIT = 3
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY_CASE = 30
EI_EAGLE_EYE_ENABLED = 1
```

```
EI_PROCESSOR_TIMEOUT_SEC = 420
EI_SCANNER_PATCH_DEF = 10
EI_SCANNER_TIMEOUT_SEC = 300ok
```

set_eagle_eye_parameter

IBM 担当者の指示に従って使用してください。脅威検出の構成パラメーターを変更します。 これらのパラメーターは、以下のように、`parameter_name` および `parameter_value` を使用して明示的に設定する必要があります。

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

表 4. set_eagle_eye_parameter のパラメーター

パラメーター	記述
EI_CASES_DISPLAY LIMIT	To-do リスト・レポートに表示されるケースの数。デフォルトは 3 です。
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY CASE	To-do リスト・レポートにこのケースが既に表示されていても、そこに再表示されるようにする「信頼度」変更のパーセンテージ。Guardium が、このパーセンテージ値によって信頼度を引き上げる別の兆候を検出した場合、これが発生する可能性があります。デフォルトは 30 です。
EI_PROCESSOR_TIMEOUT_SEC	このしきい値より長い時間実行されたプロセッサーはオフになります。デフォルトは 420 秒です。
EI_SCANNER_PATCH_DEF	パッチ・インストールの結果として誤検出が発生するのを防ぐために、単一プロセス実行で作成されたストアード・プロシージャーの数がこのパラメーターを越えた場合、そのプロセスはパッチがインストールされたと想定し、兆候の分析を停止します。デフォルトでは、1 回の実行で検出されるストアード・プロシージャーの作成数は 10 です。
EI_SCANNER_TIMEOUT_SEC	このしきい値より長い時間実行されたスキャナーはオフになります。デフォルトは 300 秒です。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

get_eagle_eye_scanners_info

スキャナー設定情報を返します。

表 5. get_eagle_eye_scanners_info のパラメーター

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

返されるデータには、以下の情報が含まれます。

表 6. get_eagle_eye_scanners_info のパラメーター

フィールド	記述
ID	スキャナー ID。
Name	スキャナー名。
Status	最後の実行以降のスキャナーの状況: I: 進行中 D: 完了 K: 強制終了 E: エラーで終了
Enabled	スキャナーが有効であるかどうかを示します。 True: 有効 False: 無効

フィールド	記述
Permanent disabled	スキャナーが 24 時間で 3 回無効になった場合、そのスキャナーは永続的に無効になります。 True: 無効 False: 有効

例:

```
grdapi get_eagle_eye_scanners_info
ID=0
ID:1, Name:SQLInjectionExceptionsScanner, Status:D, Enabled:true, Permanent disabled:false
ID:2, Name:NumNewConstructScanner, Status:D, Enabled:true, Permanent disabled:false
ID:3, Name:SQLInjectionSuspiciousObjectScanner, Status:D, Enabled:true, Permanent disabled:false
ID:4, Name:SqliQueryScanner, Status:Unknown, Enabled:false, Permanent disabled:true
ID:5, Name:EagleEyeSTPCreateProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:6, Name:EagleEyeSTPCallProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:7, Name:EagleEyeSTPExceptionProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:8, Name:EagleEyePreviousStpUsageProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:9, Name:EagleEyeSTPViolationProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:10, Name:EagleEyeSTPUserOutlierScanner, Status:D, Enabled:true, Permanent disabled:false
ok
```

set_eagle_eye_scanner_parameter

IBM 担当者の指示に従って使用してください。スキャナーをアクティブ化または非アクティブ化します。これらのパラメーターは、以下のように `parameter_name` および `parameter_value` を使用して明示的に設定する必要があります。

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

表 7. set_eagle_eye_scanner_parameter のパラメーター

パラメーター	記述
scanner_id	必須。スキャナーの固有 ID。これは、get_eagle_eye_scanners_info GuardAPI コマンドから取得できます。
is_active	スキャナーを実行するかどうかを定義します。タイムアウトになったために自動的に停止されたスキャナーを開始するために使用されます。 0 : スキャナーは停止される 1: スキャナーはアクティブ化される
is_permanent_inactive	スキャナーが 24 時間で 3 回無効になった後に永続的に無効になった場合、この GuardAPI を使用することでのみ再び有効にすることができます。 1: スキャナーは永続的に停止される 0: スキャナーは有効化される
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

以下の例では、永続的に非アクティブ化されたスキャナーを再アクティブ化します。

```
set_eagle_eye_scanner_parameter scanner_id=2 parameter_name=is_permanent_inactive parameter_value=0
```

get_eagle_eye_symptom_period_hours

徴候期間パラメーターの値を時間単位で示します。徴候期間は、1 つのケースについて収集された徴候を、どのくらい前までプロセスが検索して分析するかを決定します。

表 8. get_eagle_eye_symptom_period_hours のパラメーター

パラメーター	記述
case_name	必須。ケース・タイプ。以下の値を使用できます。 STP: 悪意のあるストアード・プロシージャーのケース SQL_INJECTION: SQL インジェクションのケース

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi get_eagle_eye_symptom_period_hours case_name=STP
The symptoms period for case type: STP is: 168 in hours
ok
```

set_eagle_eye_symptom_period_hours

徴候期間パラメーターの値を時間単位で設定します。徴候期間は、1 つのケースについて収集された徴候を、どのくらい前までプロセスが検索して分析するかを決定します。

表 9. set_eagle_eye_symptom_period_hours のパラメーター

パラメーター	記述
case_name	必須。ケース・タイプ。以下の値を使用できます。 STP: 悪意のあるストアード・プロシージャーのケース SQL_INJECTION: SQL インジェクションのケース
symptom_period_hours	必須。整数。1 つのケースの兆候を分析するための過去の時間数。
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi set_eagle_eye_symptom_period_hours case_name=STP symptom_period_hours=170
The symptoms period for case type: STP was changed. The old value was: 168. The new value is: 170
ok
```

get_eagle_eye_debug_level

IBM サービス担当員によって使用されます。現在のデバッグ・レベルを表示します。

- 1: オン
- 0: オフ

表 10. get_eagle_eye_debug_level のパラメーター

パラメーター	記述
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi get_eagle_eye_debug_level
ID=0
component=EAGLE_EYE level=1
ok
```

set_eagle_eye_debug_level

IBM サービス担当員によって使用されます。現在のデバッグ・レベルを表示します。

表 11. set_eagle_eye_debug_level のパラメーター

パラメーター	記述
level	整数。必須。指定可能な値: 1: オン 0: オフ
api_target_host	API を実行するターゲット・ホストを指定するオプション・パラメーター。未指定の場合、デフォルトで、コマンドが実行されるユニットになります。有効な値: • all_managed: すべての管理対象ユニット • all: すべての管理対象ユニットおよび CM • group:<group name>: group name は管理対象ユニットのグループです。 • CM からに限定: 任意の管理対象ユニットのホスト名または IP。例: `api_target_host=10.0.1.123` • 管理対象ユニットから: CM のホスト名または IP Guardium V10.1 および 10.1.2: 一元管理構成に限り、API が実行されるターゲット・ホストを指定します。中央マネージャー (CM) では、この値は任意の管理対象ユニットのホスト名または IP です。管理対象ユニット上では、この値は CM のホスト名または IP です。

例:

```
grdapi set_eagle_eye_debug_level level=0
ID=0
ok
```

親トピック: GuardAPI リファレンス

S-TAP for z/OS V10.1.3 User's Guide

- **IBM Security Guardium S-TAP for Db2 on z/OS**
  These topics describe how to use IBM® Security Guardium® S-TAP® for DB2® on z/OS® V10.1.3 (also referred to as IBM Guardium S-TAP for Db2). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Db2 collects and correlates data access information from a variety of Db2 resources to produce a comprehensive view of business activity for auditors.
- **IBM Security Guardium S-TAP for IMS on z/OS**
  These topics describe how to use IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for IMS). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for IMS collects and correlates data access information from a variety of IMS resources to produce a comprehensive view of business activity for auditors.
- **IBM Security Guardium S-TAP for Data Sets on z/OS**
  These topics describe how to use IBM Security Guardium S-TAP for Data Sets on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for Data Sets). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Data Sets collects and correlates data access information from a variety of resources to produce a comprehensive view of business activity for auditors.

IBM Security Guardium S-TAP for Db2 on z/OS

These topics describe how to use IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for Db2). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Db2 collects and correlates data access information from a variety of Db2 resources to produce a comprehensive view of business activity for auditors.

About these topics

This information is designed to help database administrators, system programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for Db2
- Install and operate IBM Guardium S-TAP for Db2
- Configure the IBM Guardium S-TAP for Db2 environment
- Diagnose and recover from IBM Guardium S-TAP for Db2 problems

A PDF of this User's Guide is also available here.

- **IBM Security Guardium S-TAP for Db2 on z/OS overview**
  IBM Security Guardium S-TAP for Db2 on z/OS (also referred to as IBM Guardium S-TAP for Db2) collects and correlates data access information from Db2 to produce a comprehensive view of business activity for auditors. IBM Guardium S-TAP for Db2 enables you to determine which users updated or read a particular table, on a specific z/OS Db2 system, within a specific time period.
- **Configuring IBM Security Guardium S-TAP for Db2 on z/OS**
  After you install IBM Guardium S-TAP for Db2, you must customize some files for your system. All configuration steps are required in both stand-alone and data sharing environments.
- **Data collection**
  IBM Guardium S-TAP for Db2 collects data from an audited Db2 subsystem, in accordance with the collection policies that you create through the IBM Guardium system. Use a collection policy to specify filtering criteria that captures relevant data and filters out irrelevant data. The filtering criteria that you specify determines which data is streamed to your IBM Guardium system.
- **Reference information**
  These reference topics are designed to provide you with quick access to information about IBM Guardium S-TAP for Db2 sample library members, parameters, and variables.
- **Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS**

Parent topic: S-TAP for z/OS V10.1.3 User's Guide

IBM Security Guardium S-TAP for Db2 on z/OS overview

IBM Security Guardium S-TAP for Db2 on z/OS (also referred to as IBM Guardium S-TAP for Db2) collects and correlates data access information from Db2 to produce a comprehensive view of business activity for auditors. IBM Guardium S-TAP for Db2 enables you to determine which users updated or read a particular table, on a specific z/OS Db2 system, within a specific time period.

Use IBM Guardium S-TAP for Db2 to collect and correlate the following types of data to the Guardium system:

- Modifications to an object (SQL UPDATE, INSERT, DELETE)
- Reads of an object (SQL SELECT)
- Explicit GRANT and REVOKE operations to capture events where users might be attempting to modify authorization levels
- Assignment or modification of an authorization ID
- Authorization attempts that are denied because of inadequate authorization
- CREATE, ALTER, and DROP operations against an object (such as a table)
- Utility access to an object (IBM utilities only)
- Db2 commands entered, including which users are issuing specific commands

IBM Guardium S-TAP for Db2 uses Db2 data sharing to obtain audit information from all members of the data sharing group.

- **What's new in IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3?**
  Version 10.1.3 of IBM Guardium S-TAP for Db2 provides speed and monitoring enhancements.
- **The IBM Security Guardium S-TAP for Db2 on z/OS installation environment**
  The IBM Guardium S-TAP for Db2 SQL Collector Agent collects data from an audited Db2 subsystem in accordance with the filtering policies you set with the Guardium system.
- **Installation and operation requirements**
  Verify that you have the hardware and software that is required to install and operate IBM Guardium S-TAP for Db2.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

What's new in IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3?

Version 10.1.3 of IBM Guardium S-TAP for Db2 provides speed and monitoring enhancements.

Enhancements to this version of the product include:

- New Simulation mode enables you to test policies without sending data to the appliance. Data is collected on z/OS.
- Support for the collection of BIND/REBIND events
- Support for the collection of CICS Unit of Work ID
- Improved memory management
- Support for blocking policies pushed-down from the appliance
- Improved filtering of events
- MODIFY command now collects more diagnostic information
- Ability to exclude host variables
- Support for initiating an appliance MUST GATHER command from z/OS
- Support for S-TAP logging
- Support for Internet Protocol version 6 (IPV6) introduced with PH16991

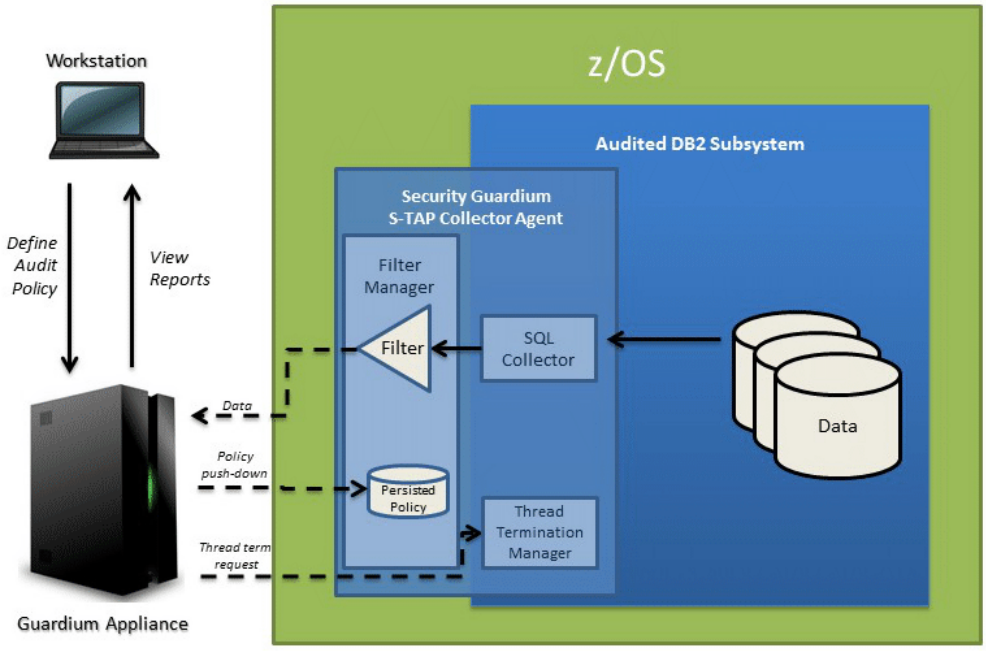
Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS overview

The IBM Security Guardium S-TAP for Db2 on z/OS installation environment

The IBM Guardium S-TAP for Db2 SQL Collector Agent collects data from an audited Db2 subsystem in accordance with the filtering policies you set with the Guardium system.

The IBM Guardium S-TAP for Db2 collector agent runs as a started task and is responsible for the collection of audit data in an IBM Guardium S-TAP for Db2 environment. As shown in the following diagram, SQL collector data is filtered and sent to the Guardium system, enabling you to view reports on your workstation.

Figure 1. An overview of the IBM Guardium S-TAP for Db2 environment



Guardium Appliance System

The Guardium system can gather, and report on, information from multiple agents running on multiple z/OS systems. The Guardium system:

- Provides the user interface, which processes requests and displays the resulting information.
- Enables you to create filtering policies, which specify the types of data to be collected by the agent.
- Stores the collected data.

Guardium Appliance System and S-TAP Collector Agent communication

The Guardium system and the IBM Guardium S-TAP for Db2 agent communicate by using a TCP/IP connection. The filtering policies that you create instruct the agent about the data to collect, such as which jobs and data sets to monitor for data accesses.

The IBM Guardium S-TAP for Db2 agent is responsible for:

- Collecting Db2 audit data based on the policy settings.
- Enabling activities to be blocked.
- Streaming collected event activity to the Guardium system.

For more information about how Guardium system policies are interpreted and enabled by the S-TAP, see Policy pushdown.

With the Guardium system installed, configured, and running in your environment, you can test your connection from the z/OS platform to the Guardium system by configuring and running the IBM Guardium S-TAP for Db2 sample library member, ADHTCPD. Consult your network security team to review the results and confirm that connection from the z/OS platform to the Guardium system is available.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS overview

Installation and operation requirements

Verify that you have the hardware and software that is required to install and operate IBM Guardium S-TAP for Db2.

FEC common code FMID H25F132 is required, and must be present on the system for the successful installation of this product.

IBM Db2 Data Access Common Collector for z/OS V1.1 (CQC) common code FMID HCQC110 is required, and must be present on the system for the successful installation of this product.

Hardware requirements

Any hardware that is capable of running Db2 for z/OS (V11 or later, until end of service).

Collector agent requirements

- Db2 Version 11 or later, until end of service.
- z/OS Version 2 Release 2 or later, until end of service.
- The IBM Guardium S-TAP for Db2 collector agent must be run on an operating system version that is equivalent to the operating system version on which the product SMP/E installation is performed.
- Resource Recovery Services (RRS) must be configured and enabled for IBM Guardium S-TAP for Db2 to use the RRSAF attachment facility to connect to Db2.

- **Compatibility with IBM Db2 Query Monitor for z/OS**
  IBM Guardium S-TAP for Db2 does not require Db2 Query Monitor to be installed or activated on a Db2 subsystem that IBM Guardium S-TAP for Db2 audits. If you are running Db2 Query Monitor on your system, be aware that IBM Guardium S-TAP for Db2 can audit a Db2 subsystem that is running Db2 Query Monitor Version 3.2 or later. Certain IBM Guardium S-TAP for Db2 PTFs require Db2 Query Monitor PTFs through SMP/E IFREQ.
- **Required user ID authorizations**
  To operate IBM Guardium S-TAP for Db2, the S-TAP collector agent started task must run under the authority of a Time Sharing Option (TSO) user ID with these authorizations.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS overview

Compatibility with IBM Db2 Query Monitor for z/OS

IBM Guardium S-TAP for Db2 does not require Db2 Query Monitor to be installed or activated on a Db2 subsystem that IBM Guardium S-TAP for Db2 audits. If you are running Db2 Query Monitor on your system, be aware that IBM Guardium S-TAP for Db2 can audit a Db2 subsystem that is running Db2 Query Monitor Version 3.2 or later. Certain IBM Guardium S-TAP for Db2 PTFs require Db2 Query Monitor PTFs through SMP/E IFREQ.

To implement Db2 Query Monitor, your site must have the appropriate operating system, environment, hardware, software, and network requirements. For information about installing and operating Db2 Query Monitor, refer to the IBM Db2 Query Monitor for z/OS Knowledge Center.

Compatible releases and maintenance levels

The following product abbreviations are used:

- InfoSphere® Guardium S-TAP for Db2: STP
- IBM Security Guardium S-TAP for Db2 on z/OS: STP
- Db2 Query Monitor: CQM

Table 1. Compatible releases and maintenance levels

	CQM 3.2	**CQM 3.3**	**STP 9.1**	**STP 10.0**	**STP V10.1.3**
CQM 3.2	---	LPAR	Db2	Db2	Db2
CQM 3.3	LPAR	---	Db2	Db2	Db2
STP 9.1	Db2	Db2	---	LPAR	LPAR
STP 10.0	Db2	Db2	LPAR	---	LPAR
STP 10.1.3	Db2	Db2	LPAR	LPAR	---

Where:

LPAR
: The two products releases can coexist on the same LPAR (provided they use a different MASTER name), but cannot be active on the same Db2 subsystem.

Db2
: The two products releases can coexist on the same LPAR and can both be active on the same Db2 subsystem/shared collector.

Parent topic: Installation and operation requirements

Required user ID authorizations

To operate IBM Guardium S-TAP for Db2, the S-TAP collector agent started task must run under the authority of a Time Sharing Option (TSO) user ID with these authorizations.

The collector agent user ID requires Db2 privileges. Grant the collector agent user ID SYSCTRL authority, and the authority to issue the SELECT statements on these tables:

- SYSIBM.SYSTABLES
- SYSIBM.SYSTABLESPACE
- SYSIBM.SYSINDEXES

OMVS segment

The collector agent uses UNIX System Services (USS) callable services as the network interface to the appliance. The USS callable services require that an OMVS segment is defined in the RACF® profile for the user ID under which the collector agent job runs. The OMVS segment that is defined for the user ID must contain the following minimum requirements:

- A numeric user ID that is assigned to the user
- A valid path to an existing home directory
- A program name, for example: /bin/sh or /bin/echo for non-shell
- A numeric group ID that is assigned to the user's DEFAULT group

To verify that the ID has an OMVS segment in its RACF profile, use the following command:

```
LU user ID OMVS
```

To add an OMVS segment to the RACF profile of an ID, refer to this sample command:

```
ALTUSER user ID
OMVS(UID(nnn)HOME('/u/ user ID)
PROGRAM('/bin/sh')
```

Parent topic: Installation and operation requirements

Configuring IBM Security Guardium S-TAP for Db2 on z/OS

After you install IBM Guardium S-TAP for Db2, you must customize some files for your system. All configuration steps are required in both stand-alone and data sharing environments.

Before you begin

Review the collector agent security and system requirements before proceeding with the following steps. A list of sample library members is provided in this User's Guide.

About this task

The following table describes the configuration steps and the corresponding SADHSAMP sample library member that is required for customization.

Table 1. Configuration steps

Step	Description of configuration step	SADHSAMP sample library member to use
1	APF authorizing the LOAD library data set	(Not applicable)
2	Customizing JCL members using the ADHEMAC1 macro	ADHEMAC1
3	Binding DBRMs using the JCL bind job	ADHBIND
4	Granting required authorizations to USERID and ADHPLAN by using the JCL authorization member	ADHGRANT
5	Creating the IBM Guardium S-TAP for Db2 control file	ADHSJ000
6	Configuring the IBM Guardium S-TAP for Db2 control file	ADHSJ001
7	Configuring the collector agent	ADHCFGP and ADHCSSID
8	Authorizing ADHPLCY for policy pushdown	Define ADHPLCY to RACF or an equivalent security system

- **Upgrading from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0**
  You can upgrade to IBM Guardium S-TAP for Db2 V10.1.3 from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0 by completing these steps.
- **Configuring IBM Security Guardium S-TAP for Db2 on z/OS**
  After installation, configure IBM Guardium S-TAP for Db2 by completing the steps that are described in this section.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Upgrading from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0

You can upgrade to IBM Guardium S-TAP for Db2 V10.1.3 from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0 by completing these steps.

Procedure

1. Complete the SMP/E installation of IBM Guardium S-TAP for Db2 V10.1.3.
2. APF-authorize the V10.1.3 SADHLOAD data set.
3. Customize and run the Db2 bind job in SADHSAMP(ADHBIND).
4. Customize and run the Db2 grant job in SADHSAMP(ADHGRANT).
5. Export and save your collection profiles.
   (V8.1 collection profiles, or policies, were administered either with the InfoSphere® Guardium S-TAP for Db2 administration client, or the IBM Guardium system.)
6. Stop the previous version's collector agent and server address spaces.
7. Update the collector started task JCLs (ADHC*ssid*) to:
   - Remove the previous version of the product SADHLOAD data sets.
   - Include the new V10.1.3 product SADHLOAD data sets in the STEPLIB DD concatenation members.

   Note: ADHS*ssid* and ADHA*ssid* started tasks are not used in IBM Guardium S-TAP for Db2 V10.1.3.
8. Update the V10.1.3 collector configuration member (typically SADHSAMP(ADHCFGP).
9. Install a collection policy on the IBM Guardium system.
   - If policy pushdown was used for V8.1 collection administration, follow the Guardium Policy Builder instructions for migrating policies for V8.1 to V10.1.3.
   - If the InfoSphere Guardium S-TAP for Db2 administration client was used for V8.1 collection administration, use the XML exported in Step 4 as a reference for the Guardium Policy Builder to define collection policies for V10.1.3.
10. Start the collector address space by typing `/S ADHC`*ssid* at the z/OS® command prompt.

What to do next

Now you can install policies on the z/OS host by using the IBM Guardium system interface. No additional configuration steps are required.
Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Configuring IBM Security Guardium S-TAP for Db2 on z/OS®

After installation, configure IBM Guardium S-TAP for Db2 by completing the steps that are described in this section.

- **APF authorizing the LOAD library data set**
  The system programmer must APF authorize the product LOAD library for data collection to work correctly. The system programmer must modify the IEAAPFxx or PROGxx PARMLIB members to define the IBM Guardium S-TAP for Db2 data set, as specified by ADHEMAC1 macro value #SADHLOAD, as an APF authorized library.

- **Enabling the dynamic LPA facility service CSVDYLPA**
  The user ID that was used to start the Collector Agent PROC must be enabled to use the dynamic LPA facility CSVDYLPA to enable the collector agent to collect data.
- **Service class considerations**
  The collector agent started task must be set at a dispatching priority that is the same as, or higher than, that of Db2.
- **Customizing JCL members**
  Use the edit macro ADHEMAC1 to customize the variables in the JCL to be run. Running ADHEMAC1 allows you to modify members without requiring you to remember plan names, creators, and other variables from one editing session to the next editing session.
- **Creating the IBM Guardium S-TAP for Db2 control file**
  IBM Guardium S-TAP for Db2 configuration information is stored in a VSAM data set, which is the product control file.
- **Configuring the IBM Guardium S-TAP for Db2 control file**
  IBM Guardium S-TAP for Db2 requires information that identifies target Db2 subsystems, product options, and data set attributes. The product configuration is saved in the VSAM product control file data set that you created previously.
- **Configuring the collector agent**
  To configure the collector agent, complete the steps provided in each of the subsequent sections. The address space dispatching priority for IBM Guardium S-TAP for Db2 must be the same as, or higher than, that of Db2.
- **Configuring the collector agent for additional Db2 subsystems**
  The collector agent must be configured for each Db2 subsystem that is to be audited.
- **Support Services Address Space overview**
  IBM Guardium S-TAP for Db2 uses a Support Services Address Space, also referred to as a Master Address Space. Learn about how the Master Address Space works, as well as the implications for using and stopping it.
- **Enabling CICS Login User ID reporting**
  You can capture the CICS® Login User ID for SQL Statements that are run in Db2 for CICS. The capture of CICS transactions is limited to CICS versions TS 4.2 or later, until end of support.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

APF authorizing the LOAD library data set

The system programmer must APF authorize the product LOAD library for data collection to work correctly. The system programmer must modify the IEAAPFxx or PROGxx PARMLIB members to define the IBM Guardium S-TAP for Db2 data set, as specified by ADHEMAC1 macro value #SADHLOAD, as an APF authorized library.

About this task

The IBM Guardium S-TAP for Db2 agent requires that all data sets accessed in the STEPLIB of the collector job be APF authorized, including:

- the LOAD library data set
- adhhlq.SADHLOAD
- the FEC data set fechlq.SFECLOAD (where *adhhlq* and *fechlq* are the data set high level qualifier where S-TAP and FEC products are installed)
- the CQC data set cqchlq.SCQCLOAD (where adhhlq and cqchlq are the data set high level qualifier where S-TAP and CQC products are installed)

Other data sets that require APF authorization are:

- CEE.SCEERUN
- CEE.SCEERUN2
- Db2 EXIT data set (i.e. DSN.VAR1.SDNEXIT)
- Db2 LOAD library data set (i.e. DSN.VAR1.SDSNLOAD)
- SYS1.LINKLIB

Refer to the *z/OS® Knowledge Center* for more information about how to APF authorize libraries.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Enabling the dynamic LPA facility service CSVDYLPA

The user ID that was used to start the Collector Agent PROC must be enabled to use the dynamic LPA facility CSVDYLPA to enable the collector agent to collect data.

About this task

Determine whether the dynamic LPA facility CSVDYLPA is SAF protected. If the dynamic LPA facility CSVDYLPA is not SAF protected, this step is not required.

Procedure

Provide the user ID with ADD/UPDATE/DELETE authority.
For more information about how to enable the CSVDYLPA resource, see section 5.6.3 of the *z/OS® V1R7.0 MVS™ Planning: Operations Guide* (SA22-7601-06), section *Controlling/Adding A Module to LPA after IPL*.
Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Service class considerations

The collector agent started task must be set at a dispatching priority that is the same as, or higher than, that of Db2.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Related tasks

- Configuring the collector agent

Customizing JCL members

Use the edit macro ADHEMAC1 to customize the variables in the JCL to be run. Running ADHEMAC1 allows you to modify members without requiring you to remember plan names, creators, and other variables from one editing session to the next editing session.

Procedure

1. Copy member ADHEMAC1 from the adhhilvl.SADHSAMP to your site's CLIST library, and then edit the ADHEMAC1 macro with the appropriate variables.
2. After you copy the edit macro to your CLIST library, use it to edit each sample library member individually. You might need to update the macro between edits depending on the member being edited and the context of the variable to be modified in the sample library.
3. To run the macro, type the ADHEMAC1 command to automatically update the appropriate variables in the member that you are editing.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Related reference

- ADHEMAC1 edit macro variables

Creating the IBM Guardium S-TAP for Db2 control file

IBM Guardium S-TAP for Db2 configuration information is stored in a VSAM data set, which is the product control file.

About this task

Using the sample JCL that is included with the product, complete these steps to create the IBM Guardium S-TAP for Db2 control file:

Procedure

1. Edit SADHSAMP member ADHSJ000.
2. Add the appropriate job card to ADHSJ000.
3. In the DELETE instruction, change the data set name.
4. In the DEFINE CLUSTER instruction, change the following text within parentheses:
   - Data set NAME
   - VOLUMES
   - DATA NAME
   - INDEX NAME
5. In the REPRO instruction, change the name of the OUTDATASET.
6. Run ADHSJ000 to create the control file. The job steps must end with a return code of zero.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Configuring the IBM Guardium S-TAP for Db2 control file

IBM Guardium S-TAP for Db2 requires information that identifies target Db2 subsystems, product options, and data set attributes. The product configuration is saved in the VSAM product control file data set that you created previously.

About this task

Update the product control file by using the sample JCL that is included with IBM Guardium S-TAP for Db2. Sample library member ADHSJ001 contains the JCL to update the control file. The following steps list the tasks required to configure the product control file data set.
Important: The Db2 plan names that are specified in the product configuration options must match the product plan names assigned to the product's Db2 plans bind plan job.

Procedure

1. Edit SADHSAMP member ADHSJ001.
2. Add the appropriate job card to ADHSJ001.
3. Change ADH.V0A00.CONTROL to the name of the VSAM control data set that you created using member ADHSJ000.
4. Change #SADHLOAD to the name of the product LOADLIB used for IBM Guardium S-TAP for Db2.
5. Modify the SYSIN DD statements as instructed in the sample member. For more information, see Required statements for each subsystem.
   Important: In a data-sharing environment, specify subsystem names (not group names) in ADHSJ001.
6. Run ADHSJ001.
   Ensure that the update job steps of the product control file end with a return code of zero. If a non-zero return code occurs, review the job output for errors, correct the problem, and resubmit the JCL.

- **Required statements for each subsystem**
  The following statements are required for each Db2 subsystem that is added to the control file.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Required statements for each subsystem

The following statements are required for each Db2 subsystem that is added to the control file.

Table 1. Required statements for

each subsystem

Statement	Setting
SET DB2 SSID	#SSID
UPDATE DB2 ZPARMS	#SZPARM
UPDATE DB2 BOOTSTRAP 1	#SBSDS01
UPDATE DB2 LOADLIB 1	#SDSNEXIT
UPDATE DB2 LOADLIB 2	#SDSNLOAD
SET PRODUCT CFG	NULL
SET PRODUCT VER	NULL
UPDATE ADH PLAN 1	ADHPLAN1
UPDATE ADH CORR ID 1	ADH ID 1
UPDATE ADH CORR ID 2	ADH ID 2

Parent topic: Configuring the IBM Guardium S-TAP for Db2 control file

Configuring the collector agent

To configure the collector agent, complete the steps provided in each of the subsequent sections. The address space dispatching priority for IBM Guardium S-TAP for Db2 must be the same as, or higher than, that of Db2.

1. Configuring the JCL for ADHBIND
   SADHSAMP(ADHBIND) is a job that binds the packages and plan used by the collector agent.
2. Configuring the JCL for ADHGRANT
   SADHSAMP(ADHGRANT) is a job that grants authorizations to the user ID and plan that are used by the collector agent.
3. Configuring the ADHCFGP data set
   The ADH#MAIN program uses parameters to define the IBM Guardium S-TAP for Db2 subsystem name, the monitored Db2 subsystem, the Guardium system host name or network address TCP/IP port, and other parameters that control how the IBM Guardium S-TAP for Db2 collector agent is implemented.
4. Defining the collector agent started task JCL
   The collector agent runs as a started task. The sample library member ADHC*SSID* contains the sample JCL to set up the IBM Guardium S-TAP for Db2 collector agent started task.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Related reference

- Service class considerations

Configuring the JCL for ADHBIND

SADHSAMP(ADHBIND) is a job that binds the packages and plan used by the collector agent.

Procedure

1. Customize and submit the JCL according to the instructions in the member.
2. Submit the ADHBIND JCL to bind the collector agent packages and plan on each Db2 subsystem on which you want to use IBM Guardium S-TAP for Db2.

Parent topic: Configuring the collector agent
Next topic: Configuring the JCL for ADHGRANT

Configuring the JCL for ADHGRANT

SADHSAMP(ADHGRANT) is a job that grants authorizations to the user ID and plan that are used by the collector agent.

Procedure

1. Customize and submit the JCL according to the instructions in the member.
2. Submit the ADHGRANT JCL to grant authorizations to the user ID and plan that are used by the collector agent for each Db2 subsystem on which you want to use IBM Guardium S-TAP for Db2.
   Note: The ADHGRANT job contains examples of the GRANTs that meet the minimal authorization requirements for the collector agent. Alternative authorizations and, subsequently, GRANTs, can be used to meet the minimal authorization requirements for the collector agent.

Parent topic: Configuring the collector agent
Previous topic: Configuring the JCL for ADHBIND
Next topic: Configuring the ADHCFGP data set

Configuring the ADHCFGP data set

The ADH#MAIN program uses parameters to define the IBM® Guardium® S-TAP® for DB2® subsystem name, the monitored Db2 subsystem, the Guardium system host name or network address TCP/IP port, and other parameters that control how the IBM Guardium S-TAP for Db2 collector agent is implemented.

About this task

These parameters are defined in an 80-byte sequential or partitioned data set that you must allocate to the ADHPARMS DD. A sample is available in the SADHSAMP library member ADHCFGP.

Note: The AUDIT parameter is required. It instructs the collector agent to audit a specific Db2 subsystem. It supports only one Db2 subsystem.

To use the sample ADHCFGP member:

Procedure

1. Copy ADHCFGP to the appropriate location (PARMLIB) on your system.
2. Verify that the parameters are valid for your environment. If necessary, edit the parameter file for your IBM Guardium S-TAP for Db2 objects.
3. Edit the ADHPARMS DD in the started task JCL to point to the ADHCFGP data set that you have customized.

Example

An example of the ADHCFGP member contents is as follows:

```
BROWSE    ADH.SMPE.SAMPLIB(ADHCFGP) - 01 L
Command ===>
SUBSYS(#SSID)
AUDIT(#SSID)
MASTER_PROCNAME(ADHMST31)
APPLIANCE_SERVER(#APPSRVR)
```

Parent topic: Configuring the collector agent
Previous topic: Configuring the JCL for ADHGRANT
Next topic: Defining the collector agent started task JCL

Defining the collector agent started task JCL

The collector agent runs as a started task. The sample library member ADHC*SSID* contains the sample JCL to set up the IBM Guardium S-TAP for Db2 collector agent started task.

Before you begin

To run the collector agent as a started task, the JCL must be in a cataloged procedure library. Modify the sample started task JCL in SADHSAMP library member ADHC*SSID* for your site, according to the instructions in the member.

About this task

The started task requires:

- READ access to the ADHCFGP data set in the RACF® DATASET class
- UPDATE access to the DB2PARMS data set in the RACF DATASET class
- The ability to connect to the Db2 subsystem that is monitored by the collector agent
- The ability to read data from the following Db2 subsystem catalog tables:
  - SYSTABLES
  - SYSINDEXES
  - SYSDBRM
  - SYSPACKAGE
  - SYSPACKSTMT
  - SYSSTMT

Procedure

1. Using the sample library member ADHC*SSID* as a template, customize the member according to the directions contained in the sample JCL. Any valid member name can be used for the started task name, but the suggested started task name is ADHC*SSID*, where *SSID* is the identifier of the Db2 subsystem that is to be monitored.
2. Copy the customized JCL to an appropriate SYSPROC data set. The JCL must include definitions for the following data descriptions:

   ADHPARMS
   : ADHPARMS must name the IBM Guardium S-TAP for Db2 collector agent configuration file.

   DB2PARMS
   : DB2PARMS must name the IBM Guardium S-TAP for Db2 product control file (example: ADH.V0A00.CONTROL).

   ADHPLCY
   : ADHPLCY enables policy persistence. For more information, see the Policy Persistence information provided in Policy pushdown.
   If ADHPLCY is defined, it must point to a data set that is allocated with a record format of fixed blocked (RECFM=FB) and a record length (LRECL) greater than or equal to 256.
   The ADHPLCY data set should be allocated with a minimum of 50 primary tracks and 10 secondary tracks. The ADHPLCY data set can be sequential, PDS, or PDS/E. If you use PDS or PDS/E, the space requirements might need to be increased in relation to the number of members that are contained within the data set.

   ADHLOG
   : ADHLOG is the SYSOUT data set to which IBM Guardium S-TAP for Db2 collector agent log messages will be written.

   STEPLIB
   : STEPLIB must include the IBM Guardium S-TAP for Db2 SADHLOAD data set.
   Note: Every data set allocated to STEPLIB must be APF-authorized.

   SYSPRINT
   : SYSPRINT is the SYSOUT data set to which log messages will be written.

Parent topic: Configuring the collector agent
Previous topic: Configuring the ADHCFGP data set

Related reference

- Sample library members

Configuring the collector agent for additional Db2 subsystems

The collector agent must be configured for each Db2 subsystem that is to be audited.

Before you begin

You must have the following user ID authorities:

- READ access to ADHCFGx parameter data sets, Db2 catalogs, and VSAM control data sets
- Access to the DSNR resource class in Db2
- OMVS segment definition
- GRANT authority for SYSCTRL Db2 to communicate with the agent started task user IDs on all Db2 subsystems to be audited
- READ authority for the Db2 catalog tables
- Authority to use the dynamic LPA facility CSVDYLPA

To define additional Db2 subsystems for auditing, follow these steps:

Procedure

1. For additional stand-alone Db2 subsystems, use the SADHSAMP member ADHBIND to bind IBM Guardium S-TAP for Db2 plans on each Db2 subsystem that is to be audited.
   - For data sharing group members, use ADHBIND to bind one member of the data sharing group. The bind will apply to all additional group members.
   - When configuring the product control file for each member of the data sharing group, the PLAN value that is used in the ADHBIND job can also be used for the ADHPLAN1 value in the SJ001 JCL job.
   - For the first member of the data sharing group, PACKAGES and PLANS that are used in the ADHBIND job will work for all members of the data sharing group.
2. For each data sharing group or additional stand-alone Db2 subsystem, grant EXECUTE permission for the agent started task ID to the ADH PLAN 1, as specified in the PCF file for the Db2 subsystem. Refer to the JCL SADHSAMP member ADHGRANT for additional details on granting EXECUTE permission to the ADH PLAN.
3. Update the control file with the new SSID, or create a new S-TAP control file for each SSID by using the SADHSAMP member ADHSJ001.
4. Configure a new S-TAP agent configuration file.
5. Add the agent started task name to the z/OS® started task table.
6. Start the new S-TAP agent.
   Note:
   - Dispatching priority must be the same as, or higher than, Db2.

   After you start the agent, review the agent log and MVS™ log for any error messages. When an active collection policy is received, the agent starts collecting audit data.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Support Services Address Space overview

IBM Guardium S-TAP for Db2 uses a Support Services Address Space, also referred to as a Master Address Space. Learn about how the Master Address Space works, as well as the implications for using and stopping it.

A Support Services Address Space, also referred to as a Master Address Space, starts for each z/OS® image after the first instance of IBM Guardium S-TAP for Db2, InfoSphere® Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS starts with a MASTER_PROCNAME value that is not yet in use on that z/OS image.

The Master Address Space is a Service Address Space for all instances of IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS that specify the same MASTER_PROCNAME parameter value that is running on the z/OS image. The Master Address Space acts as a placeholder for shared collector resources, and is similar to other Master Address Spaces that are used throughout MVS™. For sample, MVS and Db2 both have Master Address Spaces.

The Master Address Space:

- Never shuts down
- Does not run any code except for its initialization routines
- Owns resources that are needed by the shared collector
- Does not require a formal shutdown and should not be canceled or forced to shut down during the operation of IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS.
- Forcing the Master Address Space to stop causes the abnormal termination of all IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, and IBM Db2 Query Monitor for z/OS subsystems on the LPAR.

Important: During installation, do not stop or start the Master Address Space unless required by product maintenance or instructed to do so by IBM Software Support.

- **Usage considerations for the Master Address Space**
  The following considerations apply to the use of the Support Services Address Space when you are using IBM Guardium S-TAP for Db2 to monitor the same Db2 subsystem, or multiple Db2 subsystems, on the same LPAR.
- **Stopping the Master Address Space**
  Do not stop the Master Address Space unless you are directed to do so by IBM Software Support or by a ++HOLD(ACTION) in a PTF.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Usage considerations for the Master Address Space

The following considerations apply to the use of the Support Services Address Space when you are using IBM Guardium S-TAP for Db2 to monitor the same Db2 subsystem, or multiple Db2 subsystems, on the same LPAR.

Monitoring the same Db2 subsystem

If you use multiple collector products (such as IBM Guardium S-TAP for Db2, InfoSphere® Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS®) to monitor the same Db2 subsystem, each product must specify the same value for the MASTER_PROCNAME parameter.

Monitoring multiple Db2 subsystems that reside on the same LPAR

If you use multiple collector products (such as IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS) or multiple instances of the same product to monitor different Db2 subsystems that reside on the same LPAR, each product can have a different value for the MASTER_PROCNAME parameter.

Note: This rule applies to instances when you are running different maintenance levels of the same product on the same LPAR (for example, if you are testing new maintenance levels prior to upgrading your production system).

Parent topic: Support Services Address Space overview

Stopping the Master Address Space

Do not stop the Master Address Space unless you are directed to do so by IBM Software Support or by a ++HOLD(ACTION) in a PTF.

To ensure product stability, the Master Address Space should only be stopped by using the sample job that is provided in SADHSAMP, member ADHMSTR. This job verifies that no IBM Guardium S-TAP for Db2, InfoSphere® Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS® subsystems are using the Master Address Space before it is stopped.

Parent topic: Support Services Address Space overview

Enabling CICS Login User ID reporting

You can capture the CICS® Login User ID for SQL Statements that are run in Db2 for CICS. The capture of CICS transactions is limited to CICS versions TS 4.2 or later, until end of support.

About this task

Update the CICS Connection definition to capture the CICS Login User ID:

Procedure

1. Set the ATTACHSEC parameter to ATTACHSEC(IDENTIFY) for the user ID to be passed from the Terminal-Owning Region (TOR) to the Application-Owning Region (AOR).
   This makes the user ID available for collection.
2. Ensure that the CICS_USERID collector agent parameter is set to *Y* to enable reporting of the CICS login user ID. For more information, see Collector agent parameters.

Results

The CICS Login User ID is reported in Guardium interface DB2 Client Info field for SQL Statements that are run in Db2 for CICS transactions.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Data collection

IBM Guardium S-TAP for Db2 collects data from an audited Db2 subsystem, in accordance with the collection policies that you create through the IBM Guardium system. Use a collection policy to specify filtering criteria that captures relevant data and filters out irrelevant data. The filtering criteria that you specify determines which data is streamed to your IBM Guardium system.

You can define and manage data collection and filtering in the Guardium Policy Builder of the IBM Guardium system interface.

- **Data collection process**
  During the collection process, IBM Guardium S-TAP for Db2 collects event data and verifies the data against the collection criteria that is defined in the collection policy.
- **Filtering**
  IBM Guardium S-TAP for Db2 V10.1.3 greatly simplifies the filtering process from that which was used in past product versions. All filtering occurs at the point of collection regardless of the field types that are included in the rules for the active collection policy. Filtering occurs at the point of collection with or without the specification of object types, which results in efficient CPU usage.
- **Policy pushdown**
  At startup, the IBM Guardium S-TAP for Db2 collector agent waits for a policy to be streamed (or pushed down) from the Guardium system before activating a collection. When the collector agent receives a policy, it inactivates the active collection (if a collection is active), updates the collection profile with the new policy, and then activates the collection policy.
- **Streaming audit data to multiple systems**
  Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).
- **Starting and stopping the collector agent**
  After you configure the product and review the data collection information, you can start the collector agent. Use the commands provided to start and stop the collector agent started task from a cataloged procedure library.
- **Including or excluding failed accesses and negative SQL code**
  IBM Guardium S-TAP for Db2 enables you to include or exclude failed accesses and negative SQL code on a per-policy basis.
- **Quarantining SQL activity**
  IBM Guardium S-TAP for Db2 enables you to quarantine the SQL activity of specific users for specific periods of time.
- **SQL Blocking**
  You can block the SQL activity of Db2 users' (Auth IDs) access to specific tables and databases. SQL statements that are run against accelerated tables are eligible for blocking if the blocking filtering criteria is met. If a SQL statement matches the blocking criteria, the SQL statement is prevented from running. Use the Guardium appliance interface to define blocking policies.

- **Controlling host variable collection**
  IBM Guardium S-TAP for Db2 enables you to specify, on a per-rule basis, whether host variable information will be sent to the appliance for activity that matches that rule.
- **Collecting Command activity by using the Audit SQL Collector**
  IBM Guardium S-TAP for Db2 enables you to collect Command activity by using the Audit SQL Collector.
- **Collecting SET CURRENT SQLID events by using the Audit SQL Collector**
  IBM Guardium S-TAP for Db2 V10.1.3 enables you to collect SET CURRENT SQLID events by using the Audit SQL Collector.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Data collection process

During the collection process, IBM Guardium S-TAP for Db2 collects event data and verifies the data against the collection criteria that is defined in the collection policy.

Collection includes the following:

- All reads and all changes (with collector agent based collection)
- Host variables up to a maximum of 256 bytes per variable
- Dynamic SQL text up to 2 million bytes per statement
- Static SQL text up to 4000 bytes

Data collected from Db2 is filtered during the collection process, and non-relevant events are discarded. Specify filtering criteria by defining a collection policy so that only relevant events are captured. This limits the amount of unnecessary data that is collected and stored by IBM Guardium S-TAP for Db2.

- **Collection policy**
  The collection policy is defined by the Guardium policy. It is used to determine which events (SQL, Command, Utilities, etc.) are streamed from the z/OS collector agent to the Guardium appliance. The following methodology determines how the collection policy determines whether to stream events to the Guardium appliance.
- **Collected event types**
  All event types are collected with the SQL Collection mechanism, which is not dependent on other SQL Trace information such as the Db2 Trace (IFI) or SMF data. Filtering criteria is defined and managed through the IBM Guardium system interface. This table lists the types of events that can be collected.

Parent topic: Data collection

Collection policy

The collection policy is defined by the Guardium policy. It is used to determine which events (SQL, Command, Utilities, etc.) are streamed from the z/OS collector agent to the Guardium appliance. The following methodology determines how the collection policy determines whether to stream events to the Guardium appliance.

The collection policy is comprised of one or more rules. Each rule includes a list of filtering criteria (fields), which is used to determine the events that are streamed. An event is streamed to the appliance if the fields within the event match all of the fields defined within any rules of the collection policy. (Evaluation of the rules within the collection policy is *or*.) For example, if a collection policy is composed of three rules (rule 1, rule 2, and rule 3), an event is streamed if it matches rule 1, or rule 2, or rule 3.

Each rule is made up of filter types and values (fields) that are used to determine if an event should be collected. If the fields of the rule are equivalent to the corresponding fields in the event, the rule evaluates the event to be true, or a match, and the event is captured. A rule is considered true if one of each specified filter type and value matches that of the event. (Evaluation of the rule is *and*.) For example:

- If a rule is comprised of the filters DBUser=`User1` and PLAN=`DSNTEP2`, an event is collected by the rule if both DBUser=`User1` and PLAN=`DSNTEP2` are present in the event. If only one of the filtering criterion is present, or neither of the filtering criteria are present, the event does not meet the conditions of the rule and will not be collected by the rule.
- If a rule is comprised of the filters NET_PROTOCOL=`TSO` and OS_USER=`User1`, then only TSO workload events executed by User1 will be collected by the rule (wherein User1 is Original Auth ID). Non-TSO workloads run by User1 will not be collected by the rule, nor will TSO workloads run by User2.

The following sections further describe how to filter the collector agent.

Parent topic: Data collection process

Collected event types

All event types are collected with the SQL Collection mechanism, which is not dependent on other SQL Trace information such as the DB2® Trace (IFI) or SMF data. Filtering criteria is defined and managed through the IBM® Guardium® system interface. This table lists the types of events that can be collected.

Table 1. Collected event types

Collected event types
All reads (SQL SELECT)
All changes (SQL UPDATE, INSERT, DELETE)
Authorization
Audit data for Db2 utilities
Grant/Revoke
Access attempts
Binds/Rebinds
Commit/Rollbacks
Db2 commands
Db2 utilities
Failed logins
Create, Alter, Drop table
Create, Alter, Drop all other object types

Collected event types
Static SQL host variables
Static SQL text
Dynamic SQL host variables
Dynamic SQL text
Negative SQL events
SQL events involving Accelerated/IDAA tables

Information collected for CICS events

For events that are collected with Net Prtcl of a type that originates from CICS, the Internet Protocol (IP) address is reported as Terminal ID and the CICS End User is reported as the DB2 User Name in the IBM Guardium system interface.

- **Audit data for Db2 Utilities**
  You can collect table information for Db2 utility operations that are run against tablespaces. The IBM Guardium S-TAP for Db2 collector agent reports the name of the table associated with the tablespace. Configure audit data for Db2 utilities according to the following rules.

Parent topic: Data collection process

Audit data for Db2 Utilities

You can collect table information for Db2 utility operations that are run against tablespaces. The IBM Guardium S-TAP for Db2 collector agent reports the name of the table associated with the tablespace. Configure audit data for Db2 utilities according to the following rules.

Set the STAP_UTILITY_TS_TO_TABLE parameter to `Y` to collect audit data for Db2 utilities. See Collector agent parameters for more information.
Audit data for Db2 utilities is collected according to the following rules:

- When a single table is contained in the tablespace, the table information is reported.
- When more than one table is contained in the tablespace, the product can be configured to report either:

  No tables
  : The tablespace is reported, but no tables are reported.

  All tables in the tablespace
  : Utility operations are reported against the accessed table.
  This option can result in false positives being reported against tables in the tablespace that were not affected by the running of the utility.

Parent topic: Collected event types

Filtering

IBM Guardium S-TAP for Db2 V10.1.3 greatly simplifies the filtering process from that which was used in past product versions. All filtering occurs at the point of collection regardless of the field types that are included in the rules for the active collection policy. Filtering occurs at the point of collection with or without the specification of object types, which results in efficient CPU usage.

Filtering occurs when you create a filter that uses one or more of the following filter fields:

Net Prtcl
: Specifies the appliance connection type to Db2.

OS User
: Specifies the original operator user ID that is used to connect to Db2.

DB User
: Specifies the primary AUTHID that is used for authorization within Db2. In most situations, this value is the same as OS User.

App. User (PROG=*program*)
: Specifies a valid DB2 program name, such as `DSNTEP2`.

App. User (PLAN=*plan*)
: Specifies a valid DB2 plan name, such as `DSNTEP2`.

Client Info (APPL=*transaction name*)
: Specifies a valid program (or user workstation transaction) name, such as `db2.exe`.

Client Info (WKSTN=*workstation name*)
: Specifies a valid user workstation name, such as `PCsys1`.

Client Info (USER=*user name*)
: Specifies a valid user name, such as `PCuser1`.

Object type (%/SYSIBM.SYSTABLE)
: Specifies a table.

These fields can be fully qualified, or partially qualified by using the percent sign wildcard character. For more information about using wildcard characters, see Filter wildcard support.
The most efficient CPU usage is achieved when you create a filter that eliminates the greatest number of events. To increase filtering efficiency, refine your filtering criteria by indicating the additional filtering types with specific values that are associated with the data that you want to collect.

Improving filtering efficiency

You can improve the CPU efficiency of filtering by including filter types in the filter. Specifying the plan, auth ID, connection type, operator ID, program, workstation user, workstation name, or object filter types that are associated with the performed action improves efficiency, as shown in the following example.

Example

To capture access to a table called *MY.TABLE*, you could create the following filter:

Filter 1
Schema.Table equal to *MY.TABLE*

This filter causes IBM Guardium S-TAP for Db2 to capture only those events that access MY.TABLE.

To increase efficiency in this example, specify a filter field, such as plan, even if you are sure that plan is the only plan that accesses this table. To capture access to the table *MY.TABLE* for an application that runs under a specific plan, such as *MYPLAN*, the following is an example of a more efficient filter:

Filter 2
Plan equal to *MYPLAN*
Schema.Table equal to *MY.TABLE*

Specifying the plan results in only those events with the specified plan and object being streamed to appliance. Fewer events streamed to the appliance results in improved CPU usage.

- **Event types and filtering**
  The following table shows the correlation between the event type and filtering. You can define and manage filtering criteria by setting the Database Type to DB2 Collection Profile in the Guardium Policy Builder of the Guardium appliance interface.
- **Filtering by database name**
  IBM Guardium S-TAP for Db2 enables you to filter by database name. You can specify database name filters, on a per-rule basis, to be included in the SQL activity filters.
- **Filter wildcard support**
  When you are creating a filter, value strings can include the percent sign (%) as a wildcard character. The wildcard character (%) enables the collector to match strings without you having to provide all possible string values for a filter value.

Parent topic: Data collection

Event types and filtering

The following table shows the correlation between the event type and filtering. You can define and manage filtering criteria by setting the Database Type to DB2 Collection Profile in the Guardium® appliance interface.

If you enable collection of SELECT/UPDATE/INSERT/DELETE events, then the event collection is subjected to additional filtering. If you enable collection of event types other than SELECT/UPDATE/INSERT/DELETE, then the events are collected without being subjected to filtering.

Table 1. Event types and filtering

Event type	Subjected to filtering?
SELECT/UPDATE/INSERT/DELETE (SUID)	Yes
CREATE/ALTER/DROP	No
GRANT/REVOKE	No
SET CURRENT SQLID	No
DB2® COMMANDS	No
Db2 UTILITIES	No
FAILED LOGINS	No
NEGATIVE SQLCODEs	No
COMMIT/ROLLBACK	No
BINDS/REBINDS	No

Enabling the collection of specific event types

The active policy determines which event types are enabled for collection. If the event type is enabled within a rule for the active policy, it is enabled for all rules within the active policy.

An event that is enabled in Rule 1 is subjected to subsequent rule filters. The following is an example using ASC event type collection:

- Rule 1 contains an Object field value of `%/%.%`.
- Rule 1 contains AUTHID filtering for User 1.
- Rule 2 contains AUTHID filtering for User 2.
- SELECT/UPDATE/DELETE/INSERT/SET CURRENT USERID/CREATE/ALTER/DROP events are collected for all tables for both User 1 and User 2.

Tip: This example could be simplified by placing both AUTHIDs into a group within a single rule.
The following is an example using event type collection:

- Rule 1 contains the collection of Utility events.
- Rule 1 contains AUTHID filtering for User 1.
- Rule 2 does not contain the collection of Utility events, but it contains AUTHID filtering for User 2.
- All Utility events are collected because they are enabled for Rule 1.

This list describes how you can enable the collection of specific event types:

SELECT/UPDATE/INSERT/DELETE (SUID)
Enable collection by including any filter type or non-blank value in the Object field of the rule.
Two target records are reported for nested INSERT/UPDATE/DELETE events: SELECT, and either INSERT, UPDATE, or DELETE. All nested INSERT/UPDATE/DELETE events are considered Table Change events. If the table filter is set to collect only READ events, then these events are filtered out (not collected).
Wildcarding can be used within the Object field value, for example: `%/SYSIBM.SYSTABLES` or `%/%.%`.
CREATE/ALTER/DROP
Collection is automatically enabled by including any filter type or non-blank value in the Object field of the rule.
Wildcarding can be used within the Object field value, for example: `%/SYSIBM.SYSTABLES` or `%/%.%`.
GRANT/REVOKE
Enable collection through the GRANT/REVOKE command setting.

SET CURRENT SQLID
: Collection is automatically enabled by including any filter type or non-blank value in the Object field of the rule.
  Wildcarding can be used within the Object field value, for example: `%/SYSIBM.SYSTABLES` or `%/%.%`.

DB2 COMMANDS
: Enable collection through the DB2 Commands command setting.

DB2 UTILITIES
: Enable collection through the UTILITES command setting.

FAILED LOGINS
: Enable collection through the FAILED AUTHID CHANGES command setting.

NEGATIVE SQLCODES
: Enable collection through the presence of a negative SQLCODE list. Only one list is allowed per policy.
  SQLCODE collection can be added to an active collection policy. A policy that contains a single rule with only negative SQLCODES results in an inactive policy.

COMMIT/ROLLBACK
: Enable collection by adding COMMIT/ROLLBACK to the Guardium appliance policy.

Parent topic: Filtering

Filtering by database name

IBM Guardium S-TAP for Db2 enables you to filter by database name. You can specify database name filters, on a per-rule basis, to be included in the SQL activity filters.

The following operations are supported:

Included operations
: The event is audited if any of the objects are in any of the DBNAMEs.

Excluded operations
: If all of the objects are not in any of the DBNAMEs, then it is a considered a match.
  Example: All of the objects must be in one or more of the DBNAMEs for them to be excluded. If an object is from a DBNAME that is not in the list, then it is considered a match. If any database that is accessed by the query is not in the EXCLUDE DB list, then the query must be captured.

Wildcarding
: Filter values can include the percent sign (%) as a wildcard character.

Parent topic: Filtering

Filter wildcard support

When you are creating a filter, value strings can include the percent sign (%) as a wildcard character. The wildcard character (%) enables the collector to match strings without you having to provide all possible string values for a filter value.

Note: The use of wildcards in filters can potentially result in the collection of significant amounts of captured data.
Filtering fields can be fully qualified, or partially qualified, by using the percent sign wildcard character. You can insert the wildcard character (%) anywhere within the value string. The presence of the wildcard character (%) represents a string of zero of more characters. It can be embedded within a string in the following ways to achieve the following results:

%
: Matches all strings.

%*a*
: Matches all strings that end with the letter *a*, for example: *a*, *ba*, *cba*.

a%
: Matches all strings that start with the letter *a*, for example: *a*, *ab*, *abc*.

a%*a*
: Matches all strings the begin and end with the letter *a*, for example *a*, *aba*, *aca*.

Note: The wildcard character (%) cannot be used explicitly as part of the filter value.
Parent topic: Filtering

Policy pushdown

At startup, the IBM Guardium S-TAP for Db2 collector agent waits for a policy to be streamed (or pushed down) from the Guardium system before activating a collection. When the collector agent receives a policy, it inactivates the active collection (if a collection is active), updates the collection profile with the new policy, and then activates the collection policy.

The following processing occurs in the collector agent when a policy is received:

1. The new policy is compared to the currently active policy if the new policy contains one or more rules.
   a. If the policies are identical, no further processing is required.
   b. If the policies are not identical, the policy is written to DD:ADHPLCY (if defined) and it becomes the active collection policy.
2. If the new policy does not apply to this subsystem, processing continues without any changes. In this case, if there is an active policy, the collection continues to use it. If no policy is active, none is started.
3. If the new policy is inactive (contains no general audit settings, table or target definitions), the active policy is inactivated.

Policy persistence

For a policy to be pushed down, the z/OS collector agent requires connection to the Guardium appliance. If the z/OS collector agent is unable to connect to the appliance, the z/OS collector agent will read the policy from the ADHPLCY DD (if it is defined in the started task JCL). The z/OS collector agent will activate collection based on the policy that is read from the DD until a connection with the appliance is established. When the connection is established, the policy that is pushed down from the appliance replaces the policy that was read from the DD.

The file contents defined by the ADHPLCY DD contains the policy from the last successful policy pushdown from the appliance.

If ADHPLCY is defined, it must point to a data set that is allocated with a record format of fixed blocked (RECFM=FB) and a record length (LRECL) greater than or equal to 80.

Suggested ADHPLCY DD settings are as follows:

- Record format (RECFM): FB
- Record length (LRECL): 80
- Block size (BLCKSIZE): 3120
- Data set name type (DSNTYPE): LIBRARY
- Data set organization (DSORG): PO

The ADHPLCY data set should be allocated with a minimum of 50 primary tracks and 10 secondary tracks. The ADHPLCY data set can be sequential, PDS, or PDS/E. If you use PDS or PDS/E, the space requirements might need to be increased in relation to the number of members that are contained within the data set.

For more information about creating, activating, and inactivating policies from the Guardium system interface, see the how-to topics in the *Security Guardium V10.1.3* documentation in the IBM Knowledge Center.

For more information about using data sets, see the z/OS documentation in the IBM Knowledge Center, https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.idad400/toc.htm.

Parent topic: Data collection

Streaming audit data to multiple systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).

Multistream mode provides a mechanism for distributing a high-volume workload over multiple connected appliances. In multistream mode, a single audit event is only sent to a single appliance. Multistream mode does not enable mirroring of the same set of audit events to multiple appliances.

IBM Guardium S-TAP for Db2 sends events to a single appliance until a ping occurs, or the number of records that is specified by MEGABUFFER_COUNT is reached.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the APPLIANCE_SERVER_LIST parameter. Parameters APPLIANCE_SERVER and APPLIANCE_SERVER_[1-5] specify the appliances to which you intend to stream events. The appliance that is specified by APPLIANCE_SERVER provides the policy that is used for event matching.

The APPLIANCE_SERVER parameter specifies the first appliance to which audit events are streamed. The collection policy that is pushed down from the first appliance determines which events are collected and streamed to all appliances that are enabled for multistreaming.

The IBM Guardium S-TAP for Db2 agent streams events to the first appliance, then sequentially to each subsequent appliance in the multistreaming set. Each appliance in the multistreaming set then processes (logs and discards) each event in accordance with the locally installed policies.

Parent topic: Data collection

Starting and stopping the collector agent

After you configure the product and review the data collection information, you can start the collector agent. Use the commands provided to start and stop the collector agent started task from a cataloged procedure library.

Procedure

1. To start the collector agent, use the START command.
   Example: /S ADHCSSID
2. To stop the collector agent, use the STOP command, or the MODIFY command with the STOP parameter.
   Example:

   ```
   /P ADHCSSID
   ```

   or

   ```
   /F ADHCSSID,STOP
   ```

Parent topic: Data collection

Including or excluding failed accesses and negative SQL code

IBM® Guardium® S-TAP® for DB2® enables you to include or exclude failed accesses and negative SQL code on a per-policy basis.

In the Guardium appliance interface, create a list of SQL codes to include of exclude during data collection. A policy can contain either all values to be included, or all values to be excluded. In an *include* list, any SQL activity that fails within the SQLCODE list will be collected. In an *exclude* list, any SQL activity that does not fail within the SQLCODE list will be collected.
Note:

- No other filtering criteria will be ANDed with the SQLCODE filter rule when determining the collection status of the event.
- Enabling AUDIT TRACE CLASS 1 (collection of failed accesses) is deprecated because negative SQL codes for these failed accesses will be collected.
- Failed access events are streamed to the appliance if the negative SQL code is:
  - Included in the list of negative SQLCODE to be captured
  - Not based on *ALL FAILED AUTHORIZATIONS* being included in the COMMANDS filter setting for the policy. *ALL FAILED AUTHORIZATIONS* can be removed from the COMMANDS filter setting.

Parent topic: Data collection

Quarantining SQL activity

IBM® Guardium® S-TAP® for DB2® enables you to quarantine the SQL activity of specific users for specific periods of time.

Quarantining a user of a specific Db2 subsystem means that for the period of time that is specified, the quarantined user will not be able to run SQL statement in the targeted Db2 subsystem. If a quarantined user attempts access during a restricted time, access will be denied. Use the Guardium appliance interface to quarantine user activity.

Note: Quarantine does not take effect immediately. The SQL statement that produces the event to trigger the quarantine is completed before the quarantine takes effect. It is possible for additional SQL statements to be run by the quarantined user before the quarantine takes effect.
Parent topic: Data collection

SQL Blocking

You can block the SQL activity of DB2® users' (Auth IDs) access to specific tables and databases. SQL statements that are run against accelerated tables are eligible for blocking if the blocking filtering criteria is met. If a SQL statement matches the blocking criteria, the SQL statement is prevented from running. Use the Guardium® appliance interface to define blocking policies.

Enabling blocking policy

Blocking policy pushdown maps blocking policies to the S-TAP® blocking mechanism within the collector agent. At startup, the collector agent checks if a blocking policy was streamed (or pushed down) from the IBM® Guardium system when a collection policy was pushed. When the collector agent receives a blocking policy, it inactivates any incidence of active blocking, updates the blocking policy, and activates blocking.

When a blocking policy is received, the collector agent completes the following steps:

1. Compares the new blocking policy to the currently active blocking policy, if the new policy contains one or more rules.
    - If the blocking policies are identical, the collector agent determines that no further processing is required.
    - If the blocking policies are different, then the new blocking policy replaces the old one.
2. Evaluates the pushed-down list and filters to determine which events to block.
3. Validates the list of supplied objects.
    - The object must exist at the time of the installation of the blocking policy.
    - If a table that is included in the blocking policy does not exist when the blocking policy is installed, message ADHP190W is generated to identify the table.
    - Blocking is not enabled for tables that are reported by a ADHP190W message.
    - The obid/dbid for the object are checked for performance reasons.
    - If the object is dropped and then recreated, the policy must be reinstalled.

If the field values of the SQL event match corresponding filter values (blocking rule conditions) in the blocking policy, then the SQL statements are blocked and ended with a -807 error code.

For more information about creating, activating, and inactivating blocking policies from the IBM Guardium system interface, refer to the Security Guardium documentation in the IBM Knowledge Center.

Enable or disable blocking on the host

If permitted, you can enable blocking, disable blocking, or report the blocking status (enabled or disabled) by using the following operator commands:

- /F <adhstc>,BLOCKING ENABLE
- /F <adhstc>,BLOCKING DISABLE
- /F <adhstc>,BLOCKING STATUS

These commands override and determine the blocking status whether or not a blocking policy is present. By default, blocking is enabled at startup; but if you use the /F <adhstc>,BLOCKING DISABLE command and push down blocking rules, the blocking rules will be processed and blocking will be established within the z/OS® agent, but blocking will not be enabled. If you use the /F <adhstc>,BLOCKING ENABLE command, blocking is not activated until a blocking policy is pushed down.

The ADHPARMS z/OS collector agent parameter, STAP_BLOCKING, controls whether the blocking operator command is permitted and whether blocking is enabled or disabled. For more information about STAP_BLOCKING, see Collector agent parameters.

Parent topic: Data collection

Controlling host variable collection

IBM® Guardium® S-TAP® for DB2® enables you to specify, on a per-rule basis, whether host variable information will be sent to the appliance for activity that matches that rule.

In the Guardium appliance interface, specify whether host variable information should be sent to the appliance for activity that matches a rule. When host variable collection is enabled, up to 256 bytes per variable of host variable data is sent to the Guardium appliance. For enhanced security of Personally Identifiable Information (PII), host variables are not collected by default in IBM Guardium S-TAP for Db2 V10.0 and later.

In the Guardium appliance interface, specify whether host variable information should be sent to the appliance for activity that matches a rule.

The Guardium appliance interface can be overridden by the FORCE_LOG_LIMITED parameter. This parameter enables you to restrict the collection of personal data by controlling whether the active policy controls the collection of host variables.

- If FORCE_LOG_LIMITED is set to *Y*, the policy setting for the collection of host variables is ignored, and host variables are not collected.
- If FORCE_LOG_LIMITED is set to *N*, the collection of host variables is controlled by the host variable settings in the active policy.

For more information, see Collector agent parameters.
Parent topic: Data collection

Collecting Command activity by using the Audit SQL Collector

IBM Guardium S-TAP for Db2 enables you to collect Command activity by using the Audit SQL Collector.

Command events are not subjected to filtering. All command events are streamed directly to the Guardium appliance for post-collection filtering. All command events are streamed directly to the Guardium appliance for optional post-collection filtering.

Parent topic: Data collection

Collecting SET CURRENT SQLID events by using the Audit SQL Collector

IBM Guardium S-TAP for Db2 V10.1.3 enables you to collect SET CURRENT SQLID events by using the Audit SQL Collector.

In IBM Guardium S-TAP for Db2 V10.1.3, IFI TRACE CLASS 7 is no longer enabled, and SET CURRENT SQLID events are automatically collected by using the Audit SQL Collector. SET CURRENT SQLID events are streamed to the Guardium appliance without being subjected to filtering.

Parent topic: Data collection

Reference information

These reference topics are designed to provide you with quick access to information about IBM Guardium S-TAP for Db2 sample library members, parameters, and variables.

Topics:

Other resources

The following IBM documentation provides more information about configuring and operating this product.

- IBM Ported Tools for z/OS®: Open SSH User's Guide
- z/OS UNIX System Services Planning
- z/OS MVS™ JCL User's Guide
- Db2 Administration Guide
- Monitoring and Tuning Db2 Performance

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Sample library members

Use the following sample library members that are included with IBM Guardium S-TAP for Db2 for installation and configuration.

Table 1. Installation and configuration sample library members

Member	Type	Description
ADHBIND	JCL	Bind job used to bind DBRMs.
ADHBINDB	JCL	Bind job used to bind packages.
ADHCFGP	80-byte sequential or partitioned data set	A listing of required parameters that control how the collector is implemented.
ADHCFGPE	80-byte sequential or partitioned data set	A listing of optional parameters that control how the collector is implemented.
ADHCSSID	Procedure	IBM Guardium S-TAP for Db2 collector started task procedure. Runs an instance of the IBM Guardium S-TAP for Db2 collector started task.
ADHGRANT	JCL	Grants required authorizations to USERID and PLAN.

Member	Type	Description
ADHEMAC1	(edit macro)	Customizes the variables that appear in the DDL and JCL to be run.
ADHMSTR	JCL	Stops the IBM Guardium S-TAP for Db2 master address space.
ADHSJ000	JCL	Allocates VSAM product control file.
ADHSJ001	JCL	Sets product configuration options.
ADHSJ003	JCL	Generates the product control file content report.
ADHSTAPD	JCL	Produces an IBM Guardium S-TAP for Db2 diagnostic report.
ADHTCPD	JCL	Produces a TCP/IP diagnostic report to use for troubleshooting network connectivity and throughput issues.

Parent topic: Reference information

Related tasks

- Defining the collector agent started task JCL

MODIFY command

The MODIFY command allows you to issue requests against, and dynamically change, characteristics of an active S-TAP task.

The abbreviated version of the MODIFY command is the letter F. The general format of MODIFY is as follows:

```
>>-+-MODIFY-+--procname--,--parameter-------------------------><
   '-F------'
```

wherein:

procname
: The name of the member in a procedure library that was used to start the server or address space.

parameter
: Any of the parameters that are valid for the server.

S-TAP supported MODIFY options with descriptions

The following is a sample syntax diagram:

```
>>-+-MODIFY-+--procname,--+-STAP-+-----------------+
                          |      +-,HELP ----------|
                          |      +-,ALL-----------|
                          |      +-,POLICY--------|
                          |      +-,COUNTS--------|
                          |      +-,CONFIG--------|
                          |      +-,HISTORY_QUEUE--|
                          |      +-,HISTORY_FILTER-|
                          |      +-,HISTORY_IO-----|
                          |      +-,BLOCKING-------|
                          |      +-,QUARANTINE-----|
                          |      +-,GET_STATUS-----|
                          +-BLOCKING--+ ENABLED-----|
                          |           -+ DISABLED----|
                          |           -+ STATUS------|
                          |      +-,MUSTGATHER------|
                          |      +-,TRACE_POLICY,ENABLE----|
                          |      +-,TRACE_POLICY,DISABLE---|
                          |      +-,TRACE_COMPILE,ENABLE---|
                          |      +-,TRACE_COMPILE,DISABLE--|
                          |      +-,TRACE_PROTOBUF,ENABLE--|
                          |      +-,TRACE_PROTOBUF,DISABLE-|
                          |      +-,LOG_EVENTS,ENABLE------|
                          |      +-,LOG_EVENTS,DISABLE-----|
                          |      +-,LOG_LEVEL,F|I|W|E|S----|
                          |      +-,RESET_CONFIG-----------|
```

Note the space (rather than the comma) before BLOCKING ENABLED, DISABLED, and STATUS.
Options are defined as follows:

HELP
: Display all available commands

STAP
: Display the current status of the started task

ALL
: View all log information

POLICY
: View log information about the active policy

COUNTS
: View a log of detailed counts

CONFIG
: View a log about the current configuration

HISTORY_QUEUE

View log details about the internal events queue

HISTORY_FILTER
: View log information about event filter results

HISTORY_IO
: View log details about the streaming of events

BLOCKING
: View log information about the active blocking policy

QUARANTINE
: View log information about the active quarantine policy

GET STATUS
: Request the most recent count of events that were received/processed by the appliance

BLOCKING
: **ENABLED:** Enable the blocking feature. Blocking is activated if a blocking rule is pushed.
DISABLED: Disable the blocking feature.
STATUS: Display blocking status.

MUSTGATHER
: Send a must-gather request to the appliance

TRACE_POLICY,ENABLE
: View information about the policy component

TRACE_POLICY,DISABLE
: Hide information about the policy component

TRACE_COMPILE,ENABLE
: View information about the filter component

TRACE_COMPILE,DISABLE
: Hide information about the filer component

TRACE_PROTOBUF,ENABLE
: View information about the streaming component

TRACE_PROTOBUF,DISABLE
: Hide information about the streaming component

LOG_EVENTS,ENABLE
: Log events that are streamed to the appliance

LOG_EVENTS,DISABLE
: Hide events that are streamed to the appliance

LOG_LEVEL,F|I|W|E|S
: Control the amount of output log information that is generated by the agent: debugging, informational, warning, error, severe

RESET_CONFIG
: Reset agent configurations to the default settings

The following example displays the active S-TAP policy:

```
F ADHPROC,STAP,POLICY

ADHP110I  IBM Security Guardium DB2 S-TAP mode: STREAMING EVENTS
ADHP140I  Event Counts:
ADHP141I  CONNTYPE_OTHER (0) . . . . . . . . . . . 1
ADHP141I  CONNTYPE_TSO (1) . . . . . . . . . . . . 0
ADHP141I  CONNTYPE_CALL_ATTACH (2) . . . . . . . . 0
ADHP141I  CONNTYPE_DLI_BATCH (3)  .  . . . . . . . 0
ADHP141I  CONNTYPE_CICS_ATTACH (4) . . . . . . . . 0
ADHP141I  CONNTYPE_IMS_ATTACH_BMP (5)  . . . . . . 0
ADHP141I  CONNTYPE_IMS_ATTACH_MPP (6)  . . . . . . 0
ADHP141I  CONNTYPE_DB2_PRIVATE_PROTOCOL (7)  . . 0
ADHP141I  CONNTYPE_DRDA_PROTOCOL (8) . . . . . . . 0
ADHP141I  CONNTYPE_IMS_CONTROL_REGION (9)  . . . 0
ADHP141I  CONNTYPE_IMS_TRANSACTION_BMP (10)  . . 0
ADHP141I  CONNTYPE_DB2_UTILITIES (11)  . . . . . 0
ADHP141I  CONNTYPE_RRSAF (12)  . . . . . . . . . 0
ADHP142I  MISC sent  . . . . . . . . . . . . . . 0
ADHP142I  UTILITY sent . . . . . . . . . . . . . 0
ADHP142I  DB2 COMMAND sent . . . . . . . . . . . 1
ADHP142I  SELECT sent  . . . . . . . . . . . . . 0
ADHP142I  UPDATE sent  . . . . . . . . . . . . . 0
ADHP142I  DELETE sent  . . . . . . . . . . . . . 0
ADHP142I  INSERT sent  . . . . . . . . . . . . . 0
ADHP142I  REVOKE sent  . . . . . . . . . . . . . 0
ADHP142I  GRANT sent   . . . . . . . . . . . . . 0
ADHP142I  COMMIT-ROLLBACK sent   . . . . . . . . 0
ADHP142I  BIND-REBIND sent   . . . . . . . . . . 0
ADHP142I  FAILED_SQLCODE sent   . . . . . . . .  0
ADHP143I  ALTER sent   . . . . . . . . . . . . . 0
ADHP143I  DROP sent  . . . . . . . . . . . . . . 0
ADHP143I  CREATE sent  . . . . . . . . . . . . . 0
ADHP144I  Bytes sent   . . . . . . . . . . . . . 363
ADHP145I  Events Sent  . . . . . . . . . . . . . 1
ADHP146I  Statements processed   . . . . . . . . 0
ADHP140I  Event Counts:
ADHQ3270I STAP INFO: STAGE1 FILTER IS.............. ACTIVE
ADHQ3270I STAP INFO: STAGE2 FILTER IS.............. NOTACTIV
ADHQ3270I STAP INFO: TOTAL EXEC SQL CALLS SEEN..... 0000000000000000
ADHQ3270I STAP INFO: STMTS PASSED STAGE1 FILTER....  0000000000000000
ADHQ3270I STAP INFO: STMTS FAILED STAGE1 FILTER....  0000000000000000
ADHQ3270I STAP INFO: STMTS PASSED, STAGE1 BYPASSED.  0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS QUEUED............. 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS SENT TO APPLIANCE.. 0000000000000001
ADHQ3270I STAP INFO: AUDS BLOCKS NOT SENT TO APPL... 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS FREED ............. 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS FREED LOST ........ 0000000000000000
ADHQ3270I STAP INFO: BYTES SENT..................... 000000000000016B
```

```
ADHQ3270I STAP INFO: UTILITY EVENTS QUEUED.......... 0000000000000000
ADHQ3270I STAP INFO: UTILITY EVENTS FREED........... 0000000000000000
ADHQ3270I STAP INFO: UTILITY REQ COUNT.............. 0000000000000000
```

The following example displays the S-TAP blocking status:

```
F ADHPROC,STAP,POLICY

ADHQ9899I - BLOCKING STATUS
ADHQ2023I - AUTHID BLOCKING IS ENABLED
ADHQ2034I - BLOCK TABLE 181_9901F000 HASH TABLES 181_99101000 SQLHS 1E8B6000

<policy>
    <selectblocking-rule>
        <target>
            <schema>DBTROS</schema>
            <name>TABLE1</name>
        </target>
        <target>
            <schema>DBTROS</schema>
            <name>TABLE2</name>
        </target>
    </selectblocking-rule>
</policy>
```

The following example displays the results of S_TAP GET_STATUS:

```
F ADHPROC,STAP,GET STATUS
ADHP170I - Event count reported by the appliance at time: 112
```

Parent topic: Reference information

Requesting and viewing S-TAP logging information

Use the S-TAP Logging command to issue a request for logging information from the S-TAP agent collector.

About this task

From the S-TAP control panel of the IBM® Guardium® system interface:

Procedure

1. Locate the policy component for your S-TAP (for example, RS22:A91A:POLICY) and select the G icon.
2. Select STAP Logging for Command.
3. Select a logging level and click Apply to request S-TAP logging.
   S-TAP logging levels provide log information as follows:

   Level 0
   : Logs program levels, event queue statistics, agent configuration, policy, and event counts.

   Level 1
   : Logs agent configuration, policy, and event counts.

   Level 2
   : Logs agent configuration.

   Level 3
   : Logs policy.

   Level 4 or higher
   : Logs event counts.

4. To view the S-TAP logging information, locate the policy component of your S-TAP and click the i icon.

Parent topic: Reference information

Collector agent parameters

The collector agent parameters are described in this section.

APPLIANCE_CONNECT_RETRY_COUNT

Required: No

Default: 0

Description: The number of consecutive failed connection attempts before terminating. The value of 0 indicates to never stop attempting connections. A value of 1 indicates a stop immediately after connection attempt fails. Range: 0 - 99999.

Syntax:

APPLIANCE_CONNECT_RETRY_COUNT*(retry_count)*

Example:

```
APPLIANCE_CONNECT_RETRY_COUNT(1000)
```

APPLIANCE_NETWORK_REQUEST_TIMEOUT

Default: 0

Range: 0 or 500 - 12000

Description: The value in milliseconds of the period of time to wait for network communication request send or receive to complete. A value of 0 results in no timeout period.

Syntax:

```
APPLIANCE_NETWORK_REQUEST_TIMEOUT(timeout)
```

Example:

```
APPLIANCE_NETWORK_REQUEST_TIMEOUT(0)
```

APPLIANCE_PING_RATE

Required: No

Default: 5

Description: Specifies the time interval between accesses to the Guardium system to prevent timeouts (disconnects) during idle periods. The value is in number of seconds.

Syntax:

```
APPLIANCE_PING_RATE(ping_interval)
```

Example:

```
APPLIANCE_PING_RATE(5)
```

APPLIANCE_PORT

Required: No

Default: 16022

Valid ports: 16022 or 16023

Description: The IP port number of the Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should connect. This parameter must be properly configured to enable collection of audit data and a connection to the IBM Guardium system. If port 16023 is used, encryption support is required for the connection to the appliance.

Note: Specifying this keyword and parameter designates the port on which the Guardium appliance is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS® by another application.

Syntax:

```
APPLIANCE_PORT(port_number)
```

Example:

```
APPLIANCE_PORT(16022)
```

APPLIANCE_RETRY_INTERVAL

Required: No

Default: 3

Description: Specifies the time interval between attempts to establish a connection to the IBM Guardium system. The value is in number of seconds.

Syntax:

```
APPLIANCE_RETRY_INTERVAL(retry_interval)
```

Example:

```
APPLIANCE_RETRY_INTERVAL(3)
```

APPLIANCE_SERVER

Required: Yes

Default: None

Description: The host name or IP address (in dotted-decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should connect.

Note: This parameter must be properly configured to enable collection of audit data, and a connection to the IBM Guardium system. The value can contain up to 128 characters.

Syntax:

```
APPLIANCE_SERVER(hostname|ip_address)
```

Example:

```
APPLIANCE_SERVER(192.168.2.205)
```

APPLIANCE_SERVER_FAILOVER_[1-5]

Required: No

Default: None

Description: The host name or IP address (in dotted-decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should fail over to if APPLIANCE_SERVER is not available.

Note:

1. This parameter must be properly configured to enable collection of audit data and a connection to the IBM Guardium system. The value can contain up to 128 characters.
2. The collector agent attempts to connect to the fail over systems beginning with APPLIANCE_SERVER_FAILOVER_1, and ending with APPLIANCE_SERVER_FAILOVER_5.
3. Both the APPLIANCE _SERVER_FAILOVER_[1-5] and APPLIANCE_SERVER_[1-5] parameters can be used to designate servers for multistreaming or failover. Use the APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER) parameter to designate how these parameters are used.

Syntax:

```
APPLIANCE_SERVER_FAILOVER_1(hostname|ip_address)
```

Example parameter settings to enable multistream support:

```
APPLIANCE_SERVER_LIST(MULTI_STREAM)
APPLIANCE_SERVER(guardium1.company.com)
APPLIANCE_SERVER_1(guardium2.company.com)
APPLIANCE_SERVER_2(guardium3.company.com
```

APPLIANCE_SERVER_LIST(FAILOVER|MULTI_STREAM|HOT_FAILOVER)

Required: No

Default: FAILOVER

Description: If set to MULTI_STREAM, this parameter specifies that a Guardium appliance connection is to be established for each server that is identified by the APPLIANCE_SERVER_n parameter.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

If set to FAILOVER, this parameter specifies that one Guardium appliance connection is to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the APPLIANCE_SERVER_FAILOVER_n parameter.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

With either setting of APPLIANCE_SERVER_LIST, if all connections fail, and a spill file is specified (parameter OUTAGE_SPILLAREA_SIZE), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.

If set to HOT_FAILOVER, this parameter causes all connection types (POLICY and ASC) for each connected Guardium appliance to be kept active by pings. You can specify the primary Guardium appliance by using the APPLIANCE_SERVER parameter. If the primary Guardium appliance becomes unavailable and failover occurs, HOT_FAILOVER maintains the activity of the primary appliance policy.

Syntax:

```
APPLIANCE_SERVER_LIST_FAILOVER
```

Example:

```
APPLIANCE_SERVER_LIST_FAILOVER
```

AUDIT

Required: Yes

Default: None

Description: The Db2 subsystem ID for the Db2 subsystem on which the IBM Guardium S-TAP for Db2 Collector Agent should capture query data.

Note: This parameter must be properly configured to enable collection of capture data. The value can contain up to 4 characters.
Syntax:

```
AUDIT(ssid)
```

Example:

```
AUDIT(DSN1)
```

AUTHID

Required: No

Default: Defaults to the user ID under which the started task will run.

Description: The AUTHID parameter defines the Db2 AUTHID that IBM Guardium S-TAP for Db2 uses when establishing a connection to Db2 during interval processing. If you are using RACF® on your Db2 system, this ID must be defined to RACF. The AUTHID specified needs to be authorized through the resident security package, such as RACF, to perform the functions needed for all processes done by the started task and the Collector Agent monitoring subsystem. Such processes include connecting to each of the monitored Db2 SSIDs and performing file update activities against the IBM Guardium S-TAP for Db2 VSAM control file.

Notes:

1. The ID specified in the startup parameter AUTHID must be a valid TSO user ID and not a RACF group name.

2. If the AUTHID parameter is defined in the RACF Started Procedures Table (ICHRIN03), it should not be used as a startup parameter. The Started Procedures Table (ICHRIN03) associates the names of started procedures with specific RACF user IDs and group names. It can also contain a generic entry that assigns a user ID or group name to any started task that does not have a matching entry in the table. However, it is recommended that you use the STARTED class for most cases rather than the started procedures table.

Syntax:

```
AUTHID(db2authid)
```

Where *db2authid* is the Db2 AUTHID that IBM Guardium S-TAP for Db2 uses when establishing a connection to Db2 during interval processing.
Example:

```
AUTHID(DB2USER)
```

CICS_USERID

Required: No

Default: N

Description: If set to Y, the CICS_USERID parameter enables the capture of CICS Login User ID for SQL statements that are run in Db2 for CICS. For more information see Enabling CICS Login User ID reporting.

Syntax:

```
CICS_USERID(YES|NO)
```

Example:

```
CICS_USERID(Y)
```

COLLECT_COMMIT_ROLLBACK

Required: No

Default: N

Description: If set to Y, the COLLECT_COMMIT_ROLLBACK parameter enables the collection of COMMIT and ROLLBACK events.

Syntax:

```
COLLECT_COMMIT_ROLLBACK(YES|NO)
```

Example:

```
COLLECT_COMMIT_ROLLBACK(Y)
```

DEBUG

Required: No

Default: N

Description: The DEBUG parameter turns on debug mode and produces diagnostic messages for use by IBM Software Support.

Syntax:

```
DEBUG(YES|NO)
```

Example:

```
DEBUG(Y)
```

FORCE

Required: No

Default: N

Description: The FORCE parameter forces installation of a monitoring agent. If you use this parameter, any return codes from any failure reported in message ADHQ2002E are overridden.
Note: This parameter should not be specified without instruction by IBM Software Support.
Syntax:

```
FORCE(YES|NO)
```

Example:

```
FORCE(Y)
```

FORCE_LOG_LIMITED

Required: No

Default: N

Description: This parameter enables you to restrict the collection of sensitive data by controlling whether the active policy controls the collection of host variables.

If this parameter is set to *Y*:

- The policy setting for collection of host variables is ignored and host variables are not collected.

- The APPLIANCE_PORT parameter must be set to 16023. Port 16023 is used for AT-TLS-configured encrypted communications. If APPLIANCE_PORT is not set to 16023, the S-TAP agent will generate a log message indicating the configuration inconsistency, and shut down.

If this parameter is set to *N*, the collection of host variables is controlled by the host variable settings in the active policy.

Syntax:

```
FORCE_LOG_LIMITED(YES|NO)
```

Example:

```
FORCE_LOG_LIMITED(Y)
```

HOSTVAR_LIMIT

Required: No

Default: 1500

Description: This parameter designates the number of storage blocks to be allocated for host variable collection per event. The valid range is 1 -- 9999. If this parameter is not customized, the default value of 1500 is set.

If error message ADHQ1203I is encountered with RC=0008 and RSN=003F, increase the HOSTVAR_LIMIT setting to accommodate the collection of host variables for the monitored workload.

If IBM Guardium S-TAP for Db2 and IBM Db2 Query Monitor for z/OS are simultaneously monitoring the same Db2 subsystem, both products must have matching HOSTVAR_LIMIT settings to avoid receiving a mismatch error.

Syntax:

```
HOSTVAR_LIMIT(n)
```

where *n* is an integer between 1 - 9999.
Example:

```
HOSTVAR_LIMIT(1500)
```

ISM_CONSTRAINT_AGE

Required: No

Default: 300

Description: This parameter controls how much time must have passed since the last storage constraint occurrence for a given ISM storage space before the constraint event is considered to have been relieved.

Syntax:

```
ISM_CONSTRAINT_AGE(n)
```

where *n* is an integer between 1 - 60000 specified in .01 seconds. The default value is 300.
Example:

```
ISM_CONSTRAINT_AGE(16)
```

ISM_ERROR_DETAIL

Required: No

Default: Y

Description: This parameter controls whether messages ADHQ1203I and ADHQ1204I are issued to provide detailed information for ISM Storage Constraint situations. The product recommendation is to leave this parameter set to Y. This setting can be overridden at run time with the /f cqmstc,ISMERROR_DETAIL command.

Syntax:

```
ISM_ERROR_DETAIL(Y|N)
```

Example:

```
ISM_ERROR_DETAIL(Y)
```

ISM_ERROR_BLOCKS

Required: No

Default: 256

Description: This parameter determines the number of ISM Error Blocks that are allocated when IBM Guardium S-TAP for Db2 initializes.

If this value is too low, message ADHQ1219W might be issued. ISM Error Blocks communicate a storage constraint event from somewhere in the product to the task that issues storage constraint messages. If you run out of ISM Error Blocks, the storage constraint message will not be issued. However, an abend table entry will be created to document this event. This is most likely a temporary situation and it does not impact the overall performance of IBM Guardium S-TAP for Db2.

Syntax:

```
ISM_ERROR_BLOCKS(n)
```

where *n* is an integer, 16 - 8192. The default value is 256.
Example:

```
ISM_ERROR_BLOCKS(256)
```

ISM_ERROR_MSG_BLOCKS

Required: No

Default: 256

Description: This parameter determines the number of ISM Error Message Blocks that are allocated when IBM Guardium S-TAP for Db2 initializes. If this value is too low, duplicate ISM error message can be issued for the same space and reason instead of incrementing the occurrence count.

ISM Error Message Blocks are used by the task that issues storage constraint messages to do two things:

1. To consolidate similar storage constraint events to eliminate duplicate messaging for the same condition, and
2. To keep track of storage constraint events so that the Storage Constraint Relieved situation can be detected and messaged.

If you run out of ISM Error Message Blocks, this consolidation will not always occur. This would result in additional, duplicate messages in the log for the similar storage constraint events.

Syntax:

```
ISM_ERROR_MSG_BLOCKS(n)
```

where *n* is an integer between 16 - 8192. The default value is 256.
Example:

```
ISM_ERROR_MSG_BLOCKS(256)
```

MASTER_PROCNAME

Required: Yes

Default: None.

Description: The MASTER_PROCNAME parameter enables users to specify the PROCNAME to be used for the Master Address Space. Specifying this parameter causes IBM Guardium S-TAP for Db2 to use the Master Address Space with the same name.

- The MASTER_PROCNAME for IBM Guardium S-TAP for Db2 and Query Monitor must be the same when each is started at the same time for the same Db2 Subsystem.
- If this Master Address Space is already started, it is shared with other IBM Guardium S-TAP for Db2 subsystems that are already using it.
- If this Master Address Space has not already been started, it will start automatically.

Syntax:

```
MASTER_PROCNAME(procname)
```

where *procname* is the specified Master Address Space PROCNAME (character, 8 bytes).)
Example:

```
MASTER_PROCNAME(CQMMASTR)
```

MAXIMUM_ALLOCATIONS

Required: No

Default: 2048

Description: This parameter determines the maximum amount of global shared memory to be allocated by IBM Guardium S-TAP for Db2 for internal Integrated Storage Manager spaces.

Syntax:

```
MAXIMUM_ALLOCATIONS(n)
```

where *n* is an integer between 512 - 32768 specified in megabytes; must be smaller than SMEM_SIZE.
Example:

```
MAXIMUM_ALLOCATIONS(2048)
```

MESSAGE_LOG_LEVEL

Required: No

Default: I

Description: Controls the amount of output log information that is generated by the agent:

I
: Includes all log messages with an *informational* severity or higher

W
: Includes all log messages with a *warning* severity or higher

E
: Includes all log messages with an *error* severity or higher

S
: Includes all log messages with a *severe* severity or higher

The ADHPARMS file is read when the agent is started. Modifying the log-level setting in the ADHPARMS file does not implement the new setting until you restart the collector agent.
Note: During installation, it is recommended that you set the MESSAGE_LOG_LEVEL to I.

Syntax:

```
MESSAGE_LOG_LEVEL(I|W|E|S)
```

Example:

```
MESSAGE_LOG_LEVEL(I)
```

OUTAGE_SPILLAREA_SIZE

Required: No

Default: 0

Description: This parameter determines the maximum amount of memory to be allocated to support the retention of audit data in the event of a Guardium system connection outage.
Note: A value of 0 disables spillfile support. When enabled, OUTAGE_SPILLAREA_SIZE supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.
Syntax:

```
OUTAGE_SPILLAREA_SIZE(n)
```

where *n* is an integer between 0 - 1024 specified in megabytes.
Example:

```
OUTAGE_SPILLAREA_SIZE(2)
```

PREFER_IPV4_STACK

Required: No

Default: N

Description: If set to Y, this parameter causes a request to be issued to the Domain Name Server (DNS) for an IPV4 address for the hostname that is specified in the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

If this parameter is set to N or omitted from configuration, a request for an IPV6 address is issued to the DNS for the hostname that is specified by the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV4 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this parameter is used, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for Db2 started task will terminate.
Syntax:

```
PREFER_IPV4_STACK(Y|N)
```

Example:

```
PREFER_IVP4_STACK(Y)
```

SEND_FAIL_EVENT_COUNT

Required: No

Default: 100

Description: Specifies the maximum number of events to be buffered during a communication outage with the Guardium system. Events are buffered in internal memory objects and streamed to the appliance at the time of reconnection.
Note: SEND_FAIL_EVENT_COUNT and OUTAGE_SPILLAREA_SIZE are mutually exclusive. When OUTAGE_SPILLAREA_SIZE is specified, spillfile support is enabled, which supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.
Syntax:

```
SEND_FAIL_EVENT_COUNT (event_count)
```

where *event_count* is an integer between 0 – 1024 that represents the number of events to be buffered.
Example:

```
SEND_FAIL_EVENT_COUNT(100)
```

SMEM_SIZE(5|n)

Required: No

Default: 5

Description: This parameter determines the maximum amount global shared memory to be allocated by IBM Guardium S-TAP for Db2 for all purposes.

Syntax:

```
SMEM_SIZE(n)
```

where *n* is an integer between 3 - 32 specified in gigabytes; must be three times larger than MAXIMUM_ALLOCATIONS.
Example:

```
SMEM_SIZE(5)
```

STAP_BLOCKING

Required: No
Default: ENABLED
Description: The STAP_BLOCKING parameter controls whether blocking is enabled or disabled and whether the blocking operator command is permitted to enable, disable, or report status for blocking. This parameter cannot be overwritten by the BLOCKING operator command. STAP_BLOCKING parameter options are as follows:

- STAP_BLOCKING(ENABLED) enables the blocking feature. Blocking is activated if a blocking rule is pushed.
- STAP_BLOCKING(DISABLED) disables the blocking feature.
- STAP_BLOCKING(OPERATOR) enables the blocking feature and enables the BLOCKING operator command. Blocking is activated if a blocking rule is pushed.

Syntax: STAP_BLOCKING(ENABLED|DISABLED|OPERATOR)
Example: STAP_BLOCKING(ENABLED)

STAP_MEGABUFFER

Required: No

Default: Y

Description: When multiple IBM Guardium S-TAP for Db2 audit events are accumulated in a buffer, it is referred to as a megabuffer. A megabuffer reduces the CPU usage that is related to TCP/IP activity. To optimize IBM Guardium S-TAP for Db2 performance, STAP_MEGABUFFER must remain set to `Y`. However, STAP_MEGABUFFER can be set to `N` when buffering is not desired.

Setting the STAP_MEGABUFFER parameter to `N` eliminates buffering, and provides near real-time event streaming to the Guardium appliance. It also increases CPU usage, due to additional TCP/IP calls.

Syntax:

```
STAP_MEGABUFFER(Y|N)
```

Example:

```
STAP_MEGABUFFER(Y)
```

STAP_STREAM_EVENTS

Required: No

Default: Y

Description: This parameter specifies whether events will be streamed to the IBM Guardium system. The default value, *Y*, enables streaming. Specify *N* to disable streaming and enable Simulation mode.

Syntax:

```
STAP_STREAM_EVENTS(Y|N)
```

Example:

```
STAP_STREAM_EVENTS(Y)
```

STAP_TERMINATE_OPTIMIZE

Required: No

Default: N

Description: This parameter can be used to improve the response time for processing STAP_TERMINATE requests from the Guardium appliance. Roundtrip time for STAP_TERMINATE activity is impacted by the STAP_MEGABUFFER parameter. STAP_TERMINATE policies require near real-time event recording to the IBM Guardium system to analyze events against the policy and issue the termination requests to IBM Guardium S-TAP for Db2. To enable near real-time event recording to the Guardium appliance, set the STAP_MEGABUFFER parameter to `N`.

Syntax:

```
STAP_TERMINATE_OPTIMIZE(Y|N)
```

Example:

```
STAP_TERMINATE_OPTIMIZE(N)
```

STAP_UTILITY_MULTITABLE

Required: No

Default: N

Description: The STAP_UTILITY_MULTITABLE parameter works in conjunction with the STAP_UTILITY_TS_TO_TABLE parameter. These parameters control how table information is reported for Db2 Utility access events that involve tablespaces. The STAP_UTILITY_MULTITABLE parameter controls the behavior of the collector when multiple tables are contained in the tablespace. When STAP_UTILITY_MULTITABLE is set to Y:

- The collector will report all tables in the tablespace that are impacted by the utility. This guarantees that tablespace access by a utility execution will result in an audit event against the table name.
- Tables within a tablespace, which were not accessed by the utility, might be reported.

When STAP_UTILITY_MULTITABLE is set to N, no attempt is made to report table information for multi-table tablespaces accessed by a utility. Only the tablespace name is reported.

Syntax:

```
STAP_UTILITY_MULTITABLE(Y|N)
```

Example:

```
STAP_UTILITY_MULTITABLE(N)
```

No table names are reported (default).

```
STAP_UTILITY_MULTITABLE(Y)
```

All table names are reported.

STAP_UTILITY_TS_TO_TABLE

Required: No

Default: Y

Description: The STAP_UTILITY_TS_TO_TABLE parameter controls how table information is reported for Db2 Utility accesses to tablespaces. When the parameter is set to Y, the collector queries the Db2 catalog. The collector then determines and reports on which table exists within the tablespace that has been accessed by the utility execution. If multiple tables are contained in the tablespace, the STAP_UTILITY_MULTITABLE parameter controls whether the collector reports either:

All tables
: All table names in the accessed tablespace

No tables
: Only the tablespace is reported.

This action is controlled by STAP_UTILITY_MULTITABLE parameter setting.

Syntax:

```
STAP_UTILITY_TS_TO_TABLE(Y|N)
```

Example:

```
STAP_UTILITY_TS_TO_TABLE(Y)
```

STARTUP_DIAGNOSTICS

Required: No

Default: N

Description: The STARTUP_DIAGNOSTICS parameter causes IBM Guardium S-TAP for Db2 to produce diagnostic information output during startup of the collector agent. This output might be useful to IBM Support when diagnosing reported problems.

Syntax:

```
STARTUP_DIAGNOSTICS(Y|N)
```

Example:

```
STARTUP_DIAGNOSTICS(Y)
```

SHUTDOWN_DIAGNOSTICS

Required: No

Default: N

Description: The SHUTDOWN_DIAGNOSTICS parameter causes IBM Guardium S-TAP for Db2 to produce diagnostic information output during shutdown (stop) of the collector agent. This output might be useful to IBM Support when diagnosing reported problems.

Syntax:

```
SHUTDOWN_DIAGNOSTICS(Y|N)
```

Example:

```
SHUTDOWN_DIAGNOSTICS(Y)
```

SUBSYS

Required: No

Default: The default value is the Db2 subsystem name.

Description: The SUBSYS parameter defines the SQL Collector subsystem name. The subsystem name does not need to correspond to a Db2 subsystem nor an MVS™ operating system name. The name must be 1-4 characters in length.

Syntax:

```
SUBSYS(ssid)
```

Where *ssid* is the 1-4 character SQL Collector subsystem name.
Note: The SQL Collector subsystem ID must be unique across the SYSPLEX. A SQL Collector component subsystem must be running on each LPAR that has a Db2 subsystem to be captured. When choosing a collector agent subsystem ID name, be sure it will not conflict with another on the SYSPLEX. If the specified SUBSYS is not unique across the SYSPLEX, message ADHQ1003E will be issued.

Example:

`SUBSYS(ADH1)`

TS_OFFSET(E|W.HH.MM)

Required: No

Default: None (no offset)

Description:

- This parameter enables you to adjust the event timestamps that are steamed to the appliance by specifying the amount of time to adjust (offset) based on timezone.
  - For example, if running with a clock that is set to UTC 0.0 in a timezone that it is UTC + 9, GMT can be considered 9 hours west of the current time. In this situation, the parameter should be set as follows: `TS_OFFSET(W.09.00)`. Event timestamps will be adjusted (offset) by subtracting 9 hours from the original timestamp.
- If TS_OFFSET is not supplied, the timestamps that are streamed to the appliance are not adjusted based on timezone.

Syntax:

E|W
: East or west offset from GMT

HH
: Number of hours

MM
: Number of minutes

Example: TS_OFFSET(W.09.00)

ZIIP_FILTER(Y|N)

Required: No

Default: ZIIP_FILTER(N)

Description:

- ZIIP_FILTER(Y) indicates that the z/OS image running the collector agent started task has an IBM System z® Integrated Information Processor (zIIP). In this case, allow collector agent to perform offload profile filtering to a zIIP.
- If ZIIP_FILTER(Y) is specified and the collector agent started task is running on a z/OS that has no zIIP, message ADHQ1060I is issued, indicating the WLM related service has failed. In this case, collector agent continues to run as if ZIIP_FILTER(N) were set.

Syntax:ZIIP_FILTER(Y)

Example:ZIIP_FILTER(Y)

ZIIP_TCP(Y|N)

Required: No

Default:ZIIP_TCP(N)

Description:

- ZIIP_TCP(Y) indicates that the z/OS image running the collector agent started task has an IBM System z Integrated Information Processor (zIIP). In this case, allow collector agent to offload TCP/IP message processing to a zIIP.
- If ZIIP_TCP(Y) is specified and the collector agent started task is running on a z/OS that has no zIIP, message ADHQ1060I is issued, indicating the WLM related service has failed. In this case, collector agent continues to run as if ZIIP_TCP(N) were set.
  Note: ZIIP_TCP(Y) requires that zIIP filter support be enabled: ZIIP_FILTER(Y). If ZIIP_FILTER(N) and ZIIP_TCP(Y) are specified together, ZIIP_FILTER will be automatically set to Y.

Syntax:ZIIP_TCP(Y)

Example:ZIIP_TCP(Y)

/f cqmstc,ISMERROR_DETAIL(Y|N)

Description: This parameter controls whether ISM constraint message detail is on or off. When the parameter is specified, messages ADHQ1203I and ADHQ1204I are issued for ISM storage constraint situations.

Parent topic: Reference information

Keeping connections active when HOT_FAILOVER is enabled

When the HOT_FAILOVER feature is enabled by the APPLIANCE_SERVER_LIST parameter, all connection types (POLICY and ASC) for each connected Guardium® appliance are kept active by pings.

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Parent topic: Reference information

Collector agent sample parameter file

The following sample parameter file is the minimum set of parameters required in a collector agent parameter file (ADHCFGP). If you want to use this sample file, verify that the values on each parameter are appropriate for your environment.

```
-  5655-STP
-  (C) COPYRIGHT ROCKET SOFTWARE, INC. 1999 - 2015 ALL RIGHTS RESERVED.
-
-  MEMBER: ADHCFGP
-
-  DESCRIPTION: THIS IS A SAMPLE MINIMUM ADHCFGP MEMBER
-               USED FOR IBM SECURITY GUARDIUM S-TAP for DB2 on z/OS
-               COLLECTOR AGENT STARTUP.
-               VERIFY THAT THE VALUES ON EACH PARM ARE APPROPRIATE
-               FOR YOUR ENVIRONMENT.
-
- NOTE:  AFTER USING THE EDIT MACRO, VERIFY THAT NONE OF THE
-        STATEMENTS EXCEED COLUMN 72 IN LENGTH.
-
-
SUBSYS(#SSID)              -
AUDIT(#SSID)              -
MASTER_PROCNAME(ADHMST31)  -
APPLIANCE_SERVER(#APPSRVR)
```

Parent topic: Reference information

ADHEMAC1 edit macro variables

This table shows the ADHEMAC1 edit macro variables, including their default value and instructions for use. An example is also provided.

Table 1. ADHEMAC1 Edit macro variables

Variable	Default	Instructions
#SSID	MYSSID	Change the default to a valid Db2 subsystem ID. Note: The ADHEMAC1 macro sets the SUBSYS parameter using the #SSID variable. Running the macro sets SUBSYS to the Db2 subsystem ID used by the collector agent task. Do not change the #SSID variable in the ADHEMAC1 macro to be anything other than the Db2 subsystem ID used by the collector agent task.
#ADHOWNER	&ZUSER	Change &ZUSER to the value of #ADHQUALIFIER. #ADHOWNER is used to configure the owner of the plans and packages. It is used as the owner value of objects created by statements contained within the package or plan.
#ADHQUALIFIER	SYSTOOLS	Change the default to the schema name being used with this product.
#ADHUSERID	&ZUSER	Use as the authorization ID for the collector agent task.
#SADHLOAD	ADH.IBMTAPE.SADHLOAD	Change the default to the data set containing the IBM Guardium S-TAP for Db2 load modules.
#SADHDBRM	ADH.IBMTAPE.SADHDBRM	Change the default to the data set containing the IBM Guardium S-TAP for Db2 DBRMs.
#SDSNLOAD	DSN.Vxxx.SDSNLOAD	Change the default to the data set containing the Db2 load modules.
#SDSNRUNL	DSN.Vxxx.RUNLIB.LOAD	Change the default to the data set containing the Db2 DSNTEP2 module.
#DSNTEP2	DSNTEP2	Change the default to the DSNTEP2 plan name.
ADHPLAN1	ADHPLAN1	Change the default to a valid plan name. This plan used to collect information about the Db2 System catalog during audit data collection.
#SZPARM	MYSSIDPARM	Change the default to the Db2 ZPARM member that is associated with the Db2 subsystem.
#SBSDS01	MYSSID.BSDS01	Change the default to the DSN of the bootstrap data set 01.
#SBSDS02	MYSSID.BSDS02	Change the default to the DSN of the bootstrap data set 02.
#SDSNEXIT	DSN.Vxxx.SDSNEXIT	Change the default to the data set containing the Db2 ZPARMs.
#SFECLOAD	None	Data set name of the required FEC load library.
#SCQCLOAD	None	Data set name of the required CQC load library.
#ADHCNTRLFILE	ADH.V0A00.CONTROL	Change the default to an appropriate DSN HLQ for the IBM Guardium S-TAP for Db2 VSAM Control file.
#APPSRVR	appliance.company.com	Host name or IP address of the IBM Guardium system.

The following example shows the contents of the ADHEMAC1 member:

```
ISREDIT MACRO (NP)
ISPEXEC VGET (ZUSER)
ISREDIT CHANGE ALL '#SSID'         MYSSID
```

```
ISREDIT CHANGE ALL '#ADHOWNER'     &ZUSER
ISREDIT CHANGE ALL '#ADHUSERID'    &ZUSER
ISREDIT CHANGE ALL '#SADHLOAD'     ADH.IBMTAPE.SADHLOAD
ISREDIT CHANGE ALL '#SADHDBRM'     ADH.IBMTAPE.SADHDBRM
ISREDIT CHANGE ALL '#SDSNLOAD'     DSN.Vxxx.SDSNLOAD
ISREDIT CHANGE ALL '#SDSNRUNL'     DSNxxx.RUNLIB.LOAD
ISREDIT CHANGE ALL '#DSNTEP2'      DSNTEP2
ISREDIT CHANGE ALL 'ADHPLAN1'      ADHPLAN1
ISREDIT CHANGE ALL '#SZPARM'       MYSSIDPARM
ISREDIT CHANGE ALL '#SBSDS01'      MYSSID.BSDS01
ISREDIT CHANGE ALL '#SBSDS02'      MYSSID.BSDS02
ISREDIT CHANGE ALL '#SDSNEXIT'     DSN.Vxxx.SDSNEXIT
ISREDIT CHANGE ALL '#SFECLOAD'     FEC.IBMTAPE.SFECLOAD
ISREDIT CHANGE ALL '#SCQCLOAD'     CQC.IBMTAPE.SCQCLOAD
ISREDIT CHANGE ALL '#ADHCNTRLFILE' ADH.V0A00.CONTROL
ISREDIT CHANGE ALL '#APPSRVR'      appliance.company.com
```

Parent topic: Reference information

Related tasks

- Customizing JCL members

Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

These topics document the messages and error codes issued by Security Guardium S-TAP for DB2. Messages are presented in ascending alphabetical and numerical order.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Error messages

Security Guardium S-TAP for DB2 messages adhere to the following format: ADH*nnnx*

Where:

ADH
: Indicates that the message was issued by Security Guardium S-TAP for DB2.

nnn
: Indicates the message identification number.

x
: Indicates the severity of the message:

Table 1. Error message severity codes

Severity Code	Description
E	Indicates that an error occurred, which might or might not require operator intervention.
I	Indicates that the message is informational only.
S	Indicates that operator intervention is required before processing can continue.
W	Indicates that the message is a warning to alert you to a possible error condition.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

Error messages and codes: ADHAxxx

The following information is about error messages and codes that begin with ADHA.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHA507E Callable service invocation failed with return code = *rc* and reason code = *rs*

Explanation

A callable service invocation failed with a return code and reason code that are identified in the message.

User response

Refer to the *IBM Db2 for z/OS®* product documentation for an explanation of this reason and return code.

Common causes of this error include:

Insufficient authorization to ADH PLAN specified in the control file
: If either of these issues are indicated by the reason code, verify that SAMPLIB member ADHGRANT was customized and submitted during configuration of the IBM® Guardium® S-TAP® for DB2® agent.

A DB2 Trace is currently running
: Issue the Db2® command -DISPLAY TRACE to view info about any audit traces that might still be running. If audit traces are running, stop them by using the Db2 command -STOP TRACE and then restart the agent. If this does not resolve the problem, check for the existence of additional messages.

If the problem is not resolved after attempting all user responses for existing additional messages, contact IBM Software Support.

Parent topic: Error messages and codes: ADHAxxx

Error messages and codes: ADHGxxx

The following information is about error messages and codes that begin with ADHG.

- **ADHG000I**
  Attempting connection to server *server-address* port=*server-port*
- **ADHG001I**
  Establishing ASC connection to server [*server-address*]
- **ADHG002I**
  Connection established to server [*server-address*]
- **ADHG003I**
  Connection re-established to [*server-address*]
- **ADHG004W**
  Connection was lost from server [*server-address*]
- **ADHG005S**
  Unable to establish a connection to a server [*server-address*]
- **ADHG006E**
  Data loss has occurred as the result of a network send failure
- **ADHG007E**
  Unable to create a communications interface
- **ADHG008S**
  Required parameter was not supplied. Parameter=*parameter-name*
- **ADHG009I**
  TCP/IP streaming disabled due to user setting.
- **ADHG010I**
  Disconnecting from server *server-name*
- **ADHG011E**
  Unable to create an output stream
- **ADHG012E**
  Unable to set socket timeout value. rc=*return-code* reason=*reason-code*
- **ADHG013I**
  Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts*
- **ADHG014I**
  Spillfile support enabled. Spill area size: [*size*] MB
- **ADHG015W**
  Primary server is unavailable
- **ADHG017W**
  Data is being temporarily stored in a spillfile until a connection is re-established
- **ADHG018I**
  Spillfile contents have been successfully be sent to server [*server*]
- **ADHG019S**
  Spillfile storage has been exhausted. Data loss will occur.
- **ADHG020I**
  Registering server [*server*] as eligible for failover.
- **ADHG021E**
  Spillfile is approaching [50% | 85% | 95% |100$] capacity.
- **ADHG022I**
  A connection has been established to failover server [*server*].
- **ADHG026W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **ADHG027I**
  Registering server *server* as eligible for multi-stream.
- **ADHG030I**
  Security Guardium S-TAP for DB2 Collector Agent is terminating
- **ADHG031I**
  Security Guardium S-TAP for DB2 V10.1.3 [*component*] connection established
- **ADHG097E**
  Unexpected error: [*error_description*]. Return code:[*return_code*].
- **ADHG098I**
  This event will be logged due to an unexpected data condition.
- **ADHG099E**
  Unexpected error: *error-condition*
- **ADHG210I**
  A thread termination request was received for thread [*thread-token*]
- **ADHG501E**
  pbSend: Bad host name. code=*error-code*

- **ADHG502E**
  pbSend: Interface not open. code= *error-code*
- **ADHG503E**
  pbSend: Socket I/O problem. code= *error-code*
- **ADHG550E**
  Unable to send message. Connection to server is unavailable.
- **ADHG510E**
  pbWrite: No such message. code= *error-code*
- **ADHG511E**
  pbWrite: Nested too deep. code= *error-code*
- **ADHG512E**
  pbWrite: Stack underflow. code= *error-code*
- **ADHG513E**
  pbWrite: Not in message. code= *error-code*
- **ADHG514E**
  pbWrite: No such field in message. code= *error-code*
- **ADHG515E**
  pbWrite: Not a 32-bit integer field. code= *error-code*
- **ADHG516E**
  pbWrite: Not implemented. code= *error-code*
- **ADHG517E**
  pbWrite: Not a message type. code= *error-code*
- **ADHG520W**
  Encoding exception: Event exceeds protocol message size limit. code=*error-code*
- **ADHG521W**
  Total encoding exceptions encountered due to exceeded message size: *exception-count*
- **ADHG522E**
  Write failed length=*length* rc=*returncode* rsn=*reasoncode*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHG000I Attempting connection to server *server-address* port=*server-port*

Explanation

The S-TAP® collector will attempt to establish a TCP/IP connection to a Guardium® system at the specified server address and port.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG001I Establishing ASC connection to server [*server-address*]

Explanation

The S-TAP® collector is preparing to establish the TCP/IP connection to the specified Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG002I Connection established to server [*server-address*]

Explanation

The S-TAP® collector was successful in establishing a TCP/IP connection to the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG003I Connection re-established to [*server-address*]

Explanation

The S-TAP® collector was successful in re-establishing a TCP/IP connection to the Guardium® system following a disconnect.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG004W Connection was lost from server [*server-address*]

Explanation

The TCP/IP connection between the S-TAP® collector and the Guardium® system was lost. The S-TAP collector will automatically attempt to re-establish the connection, however a potential for data loss does exist if the connection is not re-established. A data loss condition is indicated by message ADHG006E.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be re-established.
Parent topic: Error messages and codes: ADHGxxx

ADHG005S Unable to establish a connection to a server [*server-address*]

Explanation

The S-TAP® collector was unable to establish a TCP/IP connection to the Guardium® system.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHG001I.
- Ensure that no firewalls are blocking connections between the collector and Guardium system.
- If port 16023 is used, ensure that AT-TLS has been configured properly between the z/OS® LPAR and the appliance.

Parent topic: Error messages and codes: ADHGxxx

ADHG006E Data loss has occurred as the result of a network send failure

Explanation

During a disconnected state, the S-TAP® collector exceeded the number of events to retain in memory while waiting for the network connection to the Guardium® system to be reestablished.

User response

- Determine the cause of the network interruption and correct the problem so that the connection can be reestablished.
- If deemed necessary, increase the SEND_FAIL_EVENT_COUNT value in the ASC ADHPARMS parameter file to increase the number of events that can be retained in memory during short outages.

Parent topic: Error messages and codes: ADHGxxx

ADHG007E Unable to create a communications interface

Explanation

An attempt to create an internal communications interface failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG008S Required parameter was not supplied. Parameter=*parameter-name*

Explanation

A required parameter was not supplied.

User response

Supply a parameter and value for the specified parameter.
Parent topic: Error messages and codes: ADHGxxx

ADHG009I TCP/IP streaming disabled due to user setting.

Explanation

A debug setting was specified that has disabled TCP/IP streaming between the S-TAP® collector and the Guardium® appliance.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG010I Disconnecting from server *server-name*

Explanation

The S-TAP® collector is disconnecting from the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG011E Unable to create an output stream

Explanation

An attempt to create an internal output stream failed.

User response

Contact IBM® Customer Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG012E Unable to set socket timeout value. rc=*return-code* reason=*reason-code*

Explanation

An attempt to set the timeout threshold in the socket interface failed.

User response

Contact IBM® Customer Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG013I Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts*

Explanation

The S-TAP® collector agent was unable to establish a TCP/IP connection to the Guardium® system within the timeout period. The connection will be reattempted until the *reattempt-number* specified meets the *total-reattempts* number specified.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHG001I.
- Ensure that there no firewalls are blocking connections between the collector and Guardium system.

Parent topic: Error messages and codes: ADHGxxx

ADHG014I Spillfile support enabled. Spill area size: [*size*] MB

Explanation

A spillfile area was successfully allocated at the specified size.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG015W Primary server is unavailable

Explanation

A connection to the primary Guardium® system is not available. Failover systems will be attempted for connection.

User response

Determine the cause of the connection interruption to the primary Guardium system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG017W Data is being temporarily stored in a spillfile until a connection is re-established

Explanation

A Guardium® system connection is unavailable. Collected data is written to the spillfile area until a system connection can be established.

User response

Determine the cause of the system connection outage and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG018I Spillfile contents have been successfully be sent to server [*server*]

Explanation

The Guardium® system connection has been restored. The spillfile data that was collected during a connection outage has been sent to the specified system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG019S Spillfile storage has been exhausted. Data loss will occur.

Explanation

A Guardium® system connection is unavailable and the spillfile is out of space. Data collected after this time will be lost.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection. Notify others of the outage as necessary.
Parent topic: Error messages and codes: ADHGxxx

ADHG020I Registering server [*server*] as eligible for failover.

Explanation

The specified server will be added to the list of failover servers to register for the connection. Registration is attempted after all failover servers have been added. A successful failover registration is indicated by message ADHG012I.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG021E Spillfile is approaching [50% | 85% | 95% |100$] capacity.

Explanation

A Guardium® system connection is unavailable and the spillfile area is at the specified capacity.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG022I A connection has been established to failover server [*server*].

Explanation

A connection to the primary Guardium® system is not available. A connection has successfully been established to one of the specified failover server.

User response

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.
Parent topic: Error messages and codes: ADHGxxx

ADHG027I Registering server *server* as eligible for multi-stream.

Explanation

The specified server will be added to the list of servers that are eligible for multistream support.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG030I Security Guardium® S-TAP® for DB2® Collector Agent is terminating

Explanation

The collector is terminating.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG031I Security Guardium® S-TAP® for DB2® V10.1.3 [*component*] connection established

Explanation

The specified component successfully established a TCP/IP connection to the Guardium system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG097E Unexpected error: [*error_description*]. Return code:[*return_code*].

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG098I This event will be logged due to an unexpected data condition.

Explanation

A collected event contained unexpected or invalid data fields. The event fields are written to DD:ADHLOG for use in diagnosing the problem.

User response

Contact IBM® Software Support with the error log.
Parent topic: Error messages and codes: ADHGxxx

ADHG099E Unexpected error: *error-condition*

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG210I A thread termination request was received for thread [*thread-token*]

Explanation

A –CANCEL THREAD command was issued by Security Guardium® S-TAP® for DB2® as a result of a request received by the Guardium system. The command ended successfully. *Thread-token* represents the cancelled thread token, as would be reported by a –DISPLAY THREAD DB2 command.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG501E pbSend: Bad host name. code=*error-code*

Explanation

While sending a message, the socket interface encountered a bad host name condition.

User response

- Verify that the host name value provided for APPLIANCE_SERVER in the ASC ADHPARMS parameter file is valid.
- Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHGxxx

ADHG502E pbSend: Interface not open. code= *error-code*

Explanation

While sending a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG503E pbSend: Socket I/O problem. code= *error-code*

Explanation

While sending a message, the socket interface encountered a socket I/O problem.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG550E Unable to send message. Connection to server is unavailable.

Explanation

An attempt to send a status (non-audit) message to the Guardium® system failed because a connection was unavailable.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG510E pbWrite: No such message. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG511E pbWrite: Nested too deep. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG512E pbWrite: Stack underflow. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG513E pbWrite: Not in message. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG514E pbWrite: No such field in message. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG515E pbWrite: Not a 32-bit integer field. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG516E pbWrite: Not implemented. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG517E pbWrite: Not a message type. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG520W Encoding exception: Event exceeds protocol message size limit. code=*error-code*

Explanation

The network protocol used to communicate to the Guardium® system is limited to 64 KB in payload size. If an audited event results in a payload that exceeds this limit, this message is issued, and a truncated message is built and sent to the system. This message is only issued once per collector instance. At termination, message ADHG521W reports the total number of events impacted by this exception. The specified *error-code* value is for use by technical support.

User response

No action is required. If an excessive number of exceptions are observed, or if you are concerned that the exceptions are impacting audit data integrity, use APPLIANCE_PORT(16022), which uses a communications protocol capable of delivering events with larger payloads.
Parent topic: Error messages and codes: ADHGxxx

ADHG521W Total encoding exceptions encountered due to exceeded message size: *exception-count*

Explanation

The network protocol used to communicate to the Guardium® system is limited to 64 KB in payload size. If an audited event results in a payload that exceeds this limit, message ADHG520W is issued. At termination, this message reports the total number of events that have been impacted by this exception, displayed as *exception-count*.

User response

No action is required. If an excessive number of exceptions are observed, or if you are concerned that the exceptions are impacting audit data integrity, use APPLIANCE_PORT(16022), which uses a communications protocol capable of delivering events with larger payloads.
Parent topic: Error messages and codes: ADHGxxx

ADHG522E Write failed length=*length* rc=*returncode* rsn=*reasoncode*

Explanation

During an attempted TCP/IP data send of the length specified, the send failed with the specified return and reason code.

User response

Refer to the IBM manual, *z/OS UNIX System Services Messages and Codes*, for an explanation of the reason code. The last 4 digits of the reason code correspond to the errors of the send API. Also, review the ADHLOG of the S-TAP Collector Agent for other messages that might indicate problems with the connection between the S-TAP Collector Agent and the Guardium appliance.

This send failure might be the result of excessive amounts of data being sent to the appliance. Refer to the appliance reporting to determine whether excessive numbers of events were sent to the appliance prior to the send failure. If you determine the failure to be the result of excessive amounts of data, review and modify the active policy to decrease the amount of data that is sent to the appliance.

Parent topic: Error messages and codes: ADHGxxx

Error messages and codes: ADHIxxxx

The following information is about error messages and codes that begin with ADHI.

- **ADHI026W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **ADHI031I**
  Security Guardium S-TAP for DB2 V10.1.3 [component] connection established
- **ADHI530E**
  DB2 connection failed [*function*] SQLCODE=[*sqlcode*] RSN=[*reason-code*]
- **ADHI531W**
  Option STAP_UTILITY_TS_TO_TABLE(Y) is ignored due to a previous error

- **ADHI612E**
  Termination requested as the result of a previous error
- **ADHI613E**
  SQLCODE -805 encountered for plan name [*plan_name*]
- **ADHI697E**
  Unexpected error: [*error_description*]. Return code:[*return_code*]
- **ADHI699E**
  Unexpected error: [*error-condition*]

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHI026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.
Parent topic: Error messages and codes: ADHIxxxx

ADHI031I Security Guardium® S-TAP® for DB2® V10.1.3 [component] connection established

Explanation

The specified component successfully established a TCP/IP connection to the Guardium system.

User response

None action is required.
Parent topic: Error messages and codes: ADHIxxxx

ADHI530E DB2® connection failed [*function*] SQLCODE=[*sqlcode*] RSN=[*reason-code*]

Explanation

A DB2 attachment facility error occurred.

User response

An error occurred while performing a DB2 attachment function. See the *IBM® DB2 for z/OS® Messages and Codes* manual for more information about the return and reason codes.
Parent topic: Error messages and codes: ADHIxxxx

ADHI531W Option STAP_UTILITY_TS_TO_TABLE(Y) is ignored due to a previous error

Explanation

The option STAP_UTILITY_TS_TO_TABLE was set to enable collection of expanded utility information. However, an error occurred when attempting to establish the DB2® connection, which is required for this feature. The option is disabled.

User response

Review ADHLOG for occurrences of message ADHG503E to determine the cause of the DB2 connection failure.
Parent topic: Error messages and codes: ADHIxxxx

ADHI612E Termination requested as the result of a previous error

Explanation

An unrecoverable error condition was encountered. A shutdown request will sent to the collector agent.

User response

Check the ADHLOG for prior errors and attempt to resolve any previous errors.
Parent topic: Error messages and codes: ADHIxxxx

ADHI613E SQLCODE -805 encountered for plan name [*plan_name*]

Explanation

A DB2® bind error -805 was encountered for the specified plan name.

User response

Run the ADHBIND job located in the SADHSAMP library.
Parent topic: Error messages and codes: ADHIxxxx

ADHI697E Unexpected error: [*error_description*]. Return code:[*return_code*]

Explanation

An unexpected error was encountered.

User response

Contact IBM® Support.
Parent topic: Error messages and codes: ADHIxxxx

ADHI699E Unexpected error: [*error-condition*]

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHIxxxx

Error messages and codes: ADHKxxxx

The following information is about error messages and codes that begin with ADHK.

- **ADHK001I**
  Scope expression received, len = *length of expression text*
- **ADHK002I**
  Starting Compilation...
- **ADHK004I**
  Constant Pool for routine: (at *memoryLocation*).
- **ADHK005W**
  Level *level* '*compilerMessage*'.
- **ADHK101I**
  Compiling filter. Flags1 *Flags*; Compile Trace *True/False*; Runtime Trace *RuntimeTraceFlag*; RuntimeTrace *RuntimeTraceValue*; Stage 1 Requested *True/False*.
- **ADHK102I**
  Rule Expression.
- **ADHK103I**
  Profile contained no filter information for this agent.
- **ADHK104I**
  Filter Compile Failed.
- **ADHK105I**
  Variable text
- **ADHK106I**
  Compiled filter requires *bytes* bytes of dynamic save area.
- **ADHK110I**
  Rule expression:
- **ADHK111I**
  Compiling filter. flags1 *flags1* trace=*trace* runtimeTraceFlag *runtimeTraceFlag* runtimeTrace *runtimeTrace*
- **ADHK203I**
  Stage one filtering was not enabled.
- **ADHK204I**
  Error while creating stage one filter.
- **ADHK205I**
  No valid stage one filter criteria found.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHK001I Scope expression received, len = *length of expression text*

Explanation

The filter compiler has received a filter expression of length *length* and expression text of *expression Text*. Only the first line of the expression text is output with this message. Only issued when trace-filter is true.

User response

None required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK002I Starting Compilation...

Explanation

The expression compiler is starting to compile the filter expression. Only issued when trace-filter is true.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK004I Constant Pool for routine: (at *memoryLocation*).

Explanation

This is a debugging message that shows the memory location of an important data structure for the compiled filter. This line is followed by a hexadecimal printout of the contents of that memory. Only issued when trace-filter is true.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK005W Level *level* '*compilerMessage*'.

Explanation

These are messages generated by the filter compiler if there is anything wrong with the generated filter expression. The compiled filter will not be used. The agent and/or collector will shut down.

User response

Contact IBM® Software Support. Provide the agent and/or collector logs along with the xml file for the active profile at the time the message was generated.
Parent topic: Error messages and codes: ADHKxxxx

ADHK101I Compiling filter. Flags1 *Flags*; Compile Trace *True/False*; Runtime Trace *RuntimeTraceFlag*; RuntimeTrace *RuntimeTraceValue*; Stage 1 Requested *True/False*.

Explanation

An informational message is issued whenever a new profile is about to be compiled into a compiled filter.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK102I Rule Expression.

Explanation

The following lines show the filter expression that was generated from the profile.

User response

No response required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK103I Profile contained no filter information for this agent.

Explanation

The currently active filter had nothing specified to be collected in the current context. For example, in the ASC started task, if the filter has no targets, or if none of the targets had any events checked, then there is nothing for the ASC started task to collect.

User response

No response is required, in general. However, if you had intended data to be collected, you may wish to review the active profile. If you believe the message is issued in error, contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK104I Filter Compile Failed.

Explanation

The expression that was generated from the currently active profile could not be compiled into a filter.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK105I *Variable text*

Explanation

This message has been issued from the filter compiler

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK106I Compiled filter requires *bytes* bytes of dynamic save area.

Explanation

The compiled filter needs a certain amount of filter working memory to be able to do filtering, and this message only appears if the amount of filter working memory allocated (8192 bytes) is insufficient. This is unusual, and indicates a very large and complicated profile.

User response

You can consider reducing the size of the profile through the use of wildcards. If that is not possible, contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK110I Rule expression:

Explanation

his message will be followed by a full, multi-line, display of the filter expression generated from the profile. This message is only printed if trace-filter is true.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK111I Compiling filter. flags1 *flags1* trace=*trace* runtimeTraceFlag *runtimeTraceFlag* runtimeTrace *runtimeTrace*

Explanation

An informational message issued whenever a new profile is about to be compiled into a compiled filter.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK203I Stage one filtering was not enabled.

Explanation

Stage 1 filtering must be enabled.

User response

To enable stage 1 filtering, enter `STAGE1_FILTER(Y)` in the ADHCPARMS DD.
Parent topic: Error messages and codes: ADHKxxxx

ADHK204I Error while creating stage one filter.

Explanation

A bug in the filtering code prevented the correct creation of a filter for stage 1. If the stage 2 filter compiled correctly, filtering proceeds successfully at a higher overhead.

User response

Contact IBM® Software Support with XML export of the profile, and the JES output that contained this message.
Parent topic: Error messages and codes: ADHKxxxx

ADHK205I No valid stage one filter criteria found.

Explanation

Stage 1 filtering is based on a subset of the profile fields. If one or more rules in the profiles do not include at least one of the profile fields, then stage 1 filtering might not apply.

User response

Review the filtering stages section of the User's Guide and adjust the profile accordingly.
Parent topic: Error messages and codes: ADHKxxxx

Error messages and codes: ADHPxxxx

The following information is about error messages and codes that begin with ADHP.

- **ADHP000I**
  Attempting connection to server *server-address* port=*server-port*
- **ADHP001I**
  Establishing Policy connection to server [*server-address*]
- **ADHP002I**
  Connection established to server [*server-address*]
- **ADHP003I**
  Connection was re-established to [*server name*]
- **ADHP004W**
  Connection was lost from server [*server-address*]
- **ADHP005S**
  Unable to establish a connection to server [*server-address*]
- **ADHP006E**
  Data loss has occurred as the result of a network send failure
- **ADHP007E**
  Unable to create a communications interface
- **ADHP008S**
  Required parameter was not supplied. Parameter=*parameter-name*
- **ADHP009I**
  TCP/IP streaming disabled due to user setting.
- **ADHP010I**
  Disconnecting from server *server-name*
- **ADHP012I**
  Failover support enabled
- **ADHP013I**
  Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts*.
- **ADHP015W**
  Primary server is unavailable
- **ADHP017W**
  Data is being temporarily stored in a spillfile until a connection is re-established
- **ADHP018I**
  Spillfile contents have been successfully be sent to server [*server*]
- **ADHP019S**
  Spillfile storage has been exhausted. Dataloss will occur
- **ADHP020I**
  Registering server [*server*] as eligible for failover
- **ADHP021E**
  Spillfile is approaching [50% | 85% | 95% |100%] capacity
- **ADHP022I**
  A connection has been established to failover server [server]
- **ADHP023I**
  A persisted policy from DD:ADHPLCY is being used.

- **ADHP026W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **ADHP028E**
  Required policy not available at initialization.
- **ADHP030I**
  Security Guardium S-TAP for DB2 Policy component is terminating
- **ADHP031I**
  Security Guardium S-TAP for DB2 V10.1.3 *component* connection established
- **ADHP093E**
  Policy discarded because all DB2 rules contain errors
- **ADHP094E**
  Policy discarded due to error
- **ADHP095E**
  error: rule discarded due to error
- **ADHP096E**
  rule error: *[error]*
- **ADHP097E**
  Unexpected error: [*error_description*]. Return code:[*return_code*]
- **ADHP099E**
  Unexpected error: *error-condition*
- **ADHP101W**
  Invalid value for filter. Reason: [*reason*]. Value: [*value*]
- **ADHP102E**
  Invalid value for sqlcode: [*_sqlcode_*]
- **ADHP110I**
  Security Guardium S-TAP for DB2 mode: *****
- **ADHP111I**
  STAP command [STAP MODIFY command]
- **ADHP120I**
  Installed Policy:
- **ADHP121I**
  [*policy segment*]
- **ADHP122I**
  Installed Quarantine:
- **ADHP123I**
  [*quarantine segment*]
- **ADHP124I**
  Installed Blocking:
- **ADHP125I**
  [*blocking segment*]
- **ADHP126I**
  STAP BLOCKING mode: [ENABLED|DISABLED|OPERATOR]
- **ADHP130I**
  Agent configuration:
- **ADHP131I**
  [*agent configuration segment*]
- **ADHP140I**
  Event Counts:
- **ADHP141I**
  [*event type*] [*total collected*]
- **ADHP142I**
  [*event type*] [*total collected*]
- **ADHP143I**
  [*event type*] [*total collected*]
- **ADHP144I**
  [*event type*] [*total collected*]
- **ADHP145I**
  [*event type*] [*total collected*]
- **ADHP146I**
  [*event type*] [*total collected*]
- **ADHP150I**
  Program levels:
- **ADHP151I**
  [*program level segment*]
- **ADHP160I**
  S-TAP allocation queue history:
- **ADHP161I**
  TimeStamp-------Queued----------Freed
- **ADHP162I**
  [*allocation queue segment*]
- **ADHP163I**
  S-TAP filter history:
- **ADHP164I**
  TimeStamp----Pass Stage 1-- ---Pass Stage2
- **ADHP165I**
  [*filter queue segment*]
- **ADHP166I**
  S-TAP IO history:
- **ADHP167I**
  TimeStamp--------Sent----------Bytes sent--------Write time

- **ADHP168I**
  [*filter queue segment*]
- **ADHP170I**
  Event count reported by the appliance at time: [*count*]
- **ADHP179E**
  Option [*option*] is invalid for STAP command
- **ADHP180I**
  [*policy* | *quarantine* | *blocking*] policy push detected.
- **ADHP183E**
  FORCE_LOG_LIMITED is enabled but APPLIANCE_PORT is not compatible.
- **ADHP182I**
  SUPPORT_FORCE_LOG_LIMITED is enabled.
- **ADHP183I**
  FORCE_LOG_LIMITED is not supported by the appliance.
- **ADHP184I**
  A pushed down [*policy* | *blocking* | *quarantine*] is in use.
- **ADHP185I**
  A [*policy* | *quarantine* | *blocking*] from DD is in use.
- **ADHP186I**
  A [*policy* | *quarantine* | *blocking*] from DD is in use, ignoring any pushed down policy.
- **ADHP188I**
  Blocking policy removed.
- **ADHP189W**
  There is no table found in database: [*database name*]
- **ADHP190W**
  DB2 object: [*object type*] with name: [*object name*] does not exist.
- **ADHP191W**
  Blocking is NOT ACTIVE because there is no valid target in the policy.
- **ADHP192E**
  SQL statement execution was unsuccessful, SQLCODE is: [*sqlcode value*] SQLSTATE is: [*sqlstate value*]
- **ADHP193I**
  STAP Logging command pushed down from UI to request STAP logging information.
- **ADHP200E**
  Unexpected element in policy definition: *<element>*
- **ADHP201E**
  A policy must contain at least one rule
- **ADHP203E**
  Duplicate schema specification: [*schema-name*]
- **ADHP204E**
  Duplicate table specification: [*table-name*]
- **ADHP205E**
  Duplicate First Read event specification.
- **ADHP206E**
  Duplicate First Change event specification.
- **ADHP207E**
  Expected <*policy*> specification but found <*****>.
- **ADHP208E**
  Policy syntax error
- **ADHP209E**
  Error in opening data set: [*dataset*]
- **ADHP210I**
  A thread termination request was received for thread [*thread ID*]
- **ADHP211W**
  Policy syntax error [*error*]
- **ADHP212W**
  [*policy* | *quarantine* | *blocking*] not enabled for ddname [*ddname*] reason: XML error
- **ADHP213E**
  Blocking policy syntax error: Invalid network [*network*]
- **ADHP214E**
  Blocking policy syntax error: Invalid netmask [*netmask*]
- **ADHP215E**
  Blocking policy syntax error: Invalid IP address [*IP address*]
- **ADHP216W**
  Blocking policy is ignored due to a previous error.
- **ADHP217W**
  Incomplete rule discarded. Rule name: [*_rule-name_*]
- **ADHP218W**
  Only one SQLCODE list is allowed. SQLCODE is discarded: [*sqlcode*]
- **ADHP220I**
  Appliance connect retry count has been reached, appliance ping rate is now increased to [*number*]
- **ADHP250E**
  Unable to send message. Connection to server is unavailable.
- **ADHP550E**
  Unable to send message. Connection to server is unavailable

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHP000I Attempting connection to server *server-address* port=*server-port*

Explanation

The S-TAP® policy component will attempt to establish a TCP/IP connection to a Guardium® system at the specified server address and port.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP001I Establishing Policy connection to server [*server-address*]

Explanation

The Security Guardium® S-TAP® for DB2® policy component is preparing to establish the TCP/IP connection to the specified Guardium system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP002I Connection established to server [*server-address*]

Explanation

The S-TAP® policy component was successful in establishing a TCP/IP connection to the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP003I Connection was re-established to [*server name*]

Explanation

The S-TAP® policy component was successful in establishing a TCP/IP connection to the Guardium® system following a disconnect.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP004W Connection was lost from server [*server-address*]

Explanation

The TCP/IP connection between the S-TAP® policy component and the Guardium® system was lost. The S-TAP policy component will automatically attempt to reestablish the connection, however a potential for data loss exists if the connection is not established. A data loss condition is indicated by message ADHP006E.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be established.
Parent topic: Error messages and codes: ADHPxxxx

ADHP005S Unable to establish a connection to server [*server-address*]

Explanation

The S-TAP® Policy component was unable to establish a TCP/IP connection to the Guardium® system.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHP001I. .
- Ensure that there are no firewalls blocking connections between the collector and the Guardium system.

Parent topic: Error messages and codes: ADHPxxxx

ADHP006E Data loss has occurred as the result of a network send failure

Explanation

During a disconnection, the S-TAP® policy component exceeded the number of events that can be retained in memory while waiting for the network connection to the Guardium® system to be reestablished.

User response

- Determine the cause of the network interruption and correct the problem so that the connection can be established.
- If necessary, increase the SEND_FAIL_EVENT_COUNT value in the ASC ADHPARMS parameter file to increase the number of events that can be retained in memory during short outages.

Parent topic: Error messages and codes: ADHPxxxx

ADHP007E Unable to create a communications interface

Explanation

An attempt to create an internal communications interface failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHPxxxx

ADHP008S Required parameter was not supplied. Parameter=*parameter-name*

Explanation

A required parameter was not supplied.

User response

Supply a parameter and value for the specified parameter.
Parent topic: Error messages and codes: ADHPxxxx

ADHP009I TCP/IP streaming disabled due to user setting.

Explanation

A debug setting was specified that has disabled TCP/IP streaming between the S-TAP® policy component and the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP010I Disconnecting from server *server-name*

Explanation

The S-TAP® policy component is disconnecting from the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP012I Failover support enabled

Explanation

One or more failover servers were successfully registered with the communications interface, enabling failover support.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP013I Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts.*

Explanation

The S-TAP® policy component was unable to establish a TCP/IP connection to the Guardium® system within the timeout period. An attempt to be made to reestablish the connection until the *reattempt-number* reaches the *total-reattempts* number.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHP001I.
- Ensure that no firewalls are blocking connections between the collector and Guardium system.

Parent topic: Error messages and codes: ADHPxxxx

ADHP015W Primary server is unavailable

Explanation

A connection to the primary Guardium® system is not available. Failover appliances will be attempted for connection.

User response

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP017W Data is being temporarily stored in a spillfile until a connection is re-established

Explanation

A Guardium® system connection is unavailable and collected data is being written to the spillfile area until an system connection can be restored.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP018I Spillfile contents have been successfully be sent to server [*server*]

Explanation

The spillfile data that was collected during a connection outage has been sent to the specified Guardium® system upon reconnection.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP019S Spillfile storage has been exhausted. Dataloss will occur

Explanation

A Guardium® system connection is unavailable and the spillfile is out of space. Data collected after this time will be lost.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection. Notify others of the outage as necessary.
Parent topic: Error messages and codes: ADHPxxxx

ADHP020I Registering server [*server*] as eligible for failover

Explanation

The specified server will be added to the list of failover servers to register for the connection. Registration is attempted after all failover servers have been added. A successful failover registration is indicated by message ADHP012I.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP021E Spillfile is approaching [50% | 85% | 95% |100%] capacity

Explanation

A Guardium® system connection is unavailable and the spillfile area has reached the specified percentage of capacity.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP022I A connection has been established to failover server [server]

Explanation

A connection to the primary Guardium® system is not available. A connection has successfully been established to one of the specified failover server.

User response

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP023I A persisted policy from DD:ADHPLCY is being used.

Explanation

The S-TAP® policy component was unable to establish a connection to the Guardium® system. A persisted policy from DD:ADHPLCY is being used.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.
Parent topic: Error messages and codes: ADHPxxxx

ADHP028E Required policy not available at initialization.

Explanation

At startup, the policy manager did not receive a policy from the Guardium appliance or policy DD.

User response

If APPLIANCE_SERVER_LIST is set to *FAILOVER*, this problem can be resolved by verifying that either:

- the primary server is active and a policy is installed, or
- the persistence policy DD is configured and has a valid policy installed from a previous policy.

IF APPLIANCE_SERVER_LIST is set to *MULTI_STREAM*, verify that the primary server is active during startup.
Parent topic: Error messages and codes: ADHPxxxx

ADHP030I Security Guardium® S-TAP® for DB2® Policy component is terminating

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP031I Security Guardium® S-TAP® for DB2® V10.1.3 *component* connection established

Explanation

The S-TAP Policy component successfully established a TCP/IP connection to the Guardium system.

User response

No action is required.

Parent topic: Error messages and codes: ADHPxxxx

ADHP093E Policy discarded because all DB2® rules contain errors

Explanation

All of the DB2 collection profile interception policies that were pushed down from the Guardium® appliance contain errors. As a result, Security Guardium S-TAP® for DB2 collection is deactivated.

User response

Review the ADHLOG for messages that were issued prior to this message that indicate why the DB2 rules were discarded. Examples of relevant messages include ADHP096E and ADHP101W. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP094E Policy discarded due to error

Explanation

One or more errors were detected while processing an interception policy that was pushed down from the Guardium appliance. As a result, the entire policy, as well as any rules that are contained within the policy, are ignored.

User response

Review the ADHLOG for messages that were issued prior to this message (for example, ADHP101W) that indicate why the policy was discarded. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP095E error: rule discarded due to error

Explanation

One or more errors were detected while processing an interception policy rule that was pushed down from the Guardium appliance. As a result, the rule containing these errors is ignored.

User response

Review the ADHLOG for messages that were issued prior to this message that indicate why the rule was discarded. Examples of relevant messages include ADHP096E and ADHP101W. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP096E rule error: *[error]*

Explanation

An error was detected while processing an interception policy rule that was pushed down from the Guardium appliance.

User response

Use the error text that is provided in this message to correct the value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP097E Unexpected error: [*error_description*]. Return code:[*return_code*]

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHPxxxx

ADHP099E Unexpected error: *error-condition*

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHPxxxx

ADHP101W Invalid value for filter. Reason: [*reason*]. Value: [*value*]

Explanation

An invalid value was detected while processing the collection policy received from the Guardium® system.

User response

Attempt to correct the invalid value or error in the collection policy by referencing the reason and value reported in the message.
Parent topic: Error messages and codes: ADHPxxxx

ADHP102E Invalid value for sqlcode: [*_sqlcode_*]

Explanation

A SQL code that was detected while processing the collection policy from the IBM® Guardium® system is not valid.

User response

Attempt to correct the SQL code in the collection policy by referencing the value that is reported in the message. See *SQL error codes* in the IBM Knowledge Center for more information.
Parent topic: Error messages and codes: ADHPxxxx

ADHP110I Security Guardium® S-TAP® for DB2® mode: *****

Explanation

This message is issued when information about the event streaming mode is requested by issuing the /F STAP command, where ***** is either *STREAMING EVENTS* or *POLICY SIMULATION*.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP111I STAP command [STAP MODIFY command]

Explanation

This message indicates that an S-TAP MODIFY command has been issued.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP120I Installed Policy:

Explanation

The header of the installed policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP121I [*policy segment*]

Explanation

A segment of the installed policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP122I Installed Quarantine:

Explanation

The header of the installed quarantine policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP123I [*quarantine segment*]

Explanation

A segment of the installed quarantine policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP124I Installed Blocking:

Explanation

The header of the installed blocking policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP125I [*blocking segment*]

Explanation

A segment of the installed blocking policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP126I STAP BLOCKING mode: [ENABLED|DISABLED|OPERATOR]

Explanation

This message indicates whether S-TAP blocking is enabled, disabled, or in operator mode.

User response

No action is required. See SQL Blocking for more information.
Parent topic: Error messages and codes: ADHPxxxx

ADHP130I Agent configuration:

Explanation

The header of the agent configuration

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP131I [*agent configuration segment*]

Explanation

A segment of the agent configuration

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP140I Event Counts:

Explanation

The header of the event collection statistics

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP141I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP142I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP143I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP144I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP145I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP146I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP150I Program levels:

Explanation

The header of S-TAP program levels

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP151I [*program level segment*]

Explanation

A segment of S-TAP program levels

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP160I S-TAP allocation queue history:

Explanation

The header of S-TAP allocation queue history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP161I *TimeStamp-------Queued-----------Freed*

Explanation

The subheader of S-TAP allocation queue history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP162I [*allocation queue segment*]

Explanation

A segment of the allocation queue history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP163I S-TAP filter history:

Explanation

The header of S-TAP filter history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP164I *TimeStamp----Pass Stage 1-- ---Pass Stage2*

Explanation

The subheader of the S-TAP filter history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP165I [*filter queue segment*]

Explanation

A segment of S-TAP filter history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP166I S-TAP IO history:

Explanation

The header of S-TAP IO history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP167I *TimeStamp--------Sent----------Bytes sent--------Write time*

Explanation

The subheader of S-TAP IO history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP168I [*filter queue segment*]

Explanation

A segment of S-TAP IO history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP170I Event count reported by the appliance at time: [*count*]

Explanation

Number of collected events reported by the appliance.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP179E Option [*option*] is invalid for STAP command

Explanation

An invalid value was detected while processing the S-TAP command.

User response

Check the command and try again.
Parent topic: Error messages and codes: ADHPxxxx

ADHP180I [*policy* | *quarantine* | *blocking*] policy push detected.

Explanation

A policy pushdown from the Guardium appliance has been detected.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP183E FORCE_LOG_LIMITED is enabled but APPLIANCE_PORT is not compatible.

Explanation

The FORCE_LOG_LIMITED parameter is enabled but APPLIANCE_PORT is not set correctly.

User response

Check the compatible values for FORCE_LOG_LIMITED and APPLIANCE_PORT.
Parent topic: Error messages and codes: ADHPxxxx

ADHP182I SUPPORT_FORCE_LOG_LIMITED is enabled.

Explanation

The S-TAP has been configured not to collect host variables.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP183I FORCE_LOG_LIMITED is not supported by the appliance.

Explanation

The appliance does not support the FORCE_LOG_LIMITED feature.

User response

Check for the compatible appliance with which to use the FORCE_LOG_LIMITED feature.
Parent topic: Error messages and codes: ADHPxxxx

ADHP184I A pushed down [*policy* | *blocking* | *quarantine*] is in use.

Explanation

Policy push down is in use.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP185I A [*policy* | *quarantine* | *blocking*] from DD is in use.

Explanation

A policy supplied by DD is in use rather than one from push down.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP186I A [*policy* | *quarantine* | *blocking*] from DD is in use, ignoring any pushed down policy.

Explanation

A policy supplied by DD is in use. Any pushed down policy will be discarded.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP188I Blocking policy removed.

Explanation

All blocking policies have been uninstalled.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP189W There is no table found in database: [*database name*]

Explanation

The database [*database name*] that was specified in the blocking policy is either empty or not defined.

User response

Rebuild the blocking policy with a valid database for blocking to be active for the database.
Parent topic: Error messages and codes: ADHPxxxx

ADHP190W DB2 object: [*object type*] with name: [*object name*] does not exist.

Explanation

The DB2 object [*object type*] specified in the blocking policy does not exist.

User response

Rebuild the blocking policy with valid blocking targets for blocking to be active for the DB2 object.
Parent topic: Error messages and codes: ADHPxxxx

ADHP191W Blocking is NOT ACTIVE because there is no valid target in the policy.

Explanation

No valid blocking target has been found in the blocking policy. Blocking will not be activated.

User response

Rebuild the blocking policy with valid blocking targets for blocking to be activated.
Parent topic: Error messages and codes: ADHPxxxx

ADHP192E SQL statement execution was unsuccessful, SQLCODE is: [*sqlcode value*] SQLSTATE is: [*sqlstate value*]

Explanation

A SQL statement execution was unsuccessful during policy pushdown process.

User response

Determine the cause of the SQLCODE. Correct the installed policy if necessary.
Parent topic: Error messages and codes: ADHPxxxx

ADHP193I STAP Logging command pushed down from UI to request STAP logging information.

Explanation

S-TAP logging levels provide log information as follows:

Level 0
: Logs program levels, event queue statistics, agent configuration, policy, and event counts.

Level 1
: Logs agent configuration, policy, and event counts.

Level 2
: Logs agent configuration.

Level 3
: Logs policy.

Level 4 or higher
: Logs event counts.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP200E Unexpected element in policy definition: *<element>*

Explanation

An unexpected element has been found while parsing policy.

User response

Correct the unexpected element and update the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP201E A policy must contain at least one rule

Explanation

No rule was found in the policy.

User response

Update the policy to contains at least one rule.
Parent topic: Error messages and codes: ADHPxxxx

ADHP203E Duplicate schema specification: [*schema-name*]

Explanation

A duplicated schema within one target has been detected.

User response

Update the policy with only one schema per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP204E Duplicate table specification: [*table-name*]

Explanation

A duplicate table within one target has been detected.

User response

Update the policy with only one table per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP205E Duplicate First Read event specification.

Explanation

A duplicate First Read event has been detected.

User response

Update the policy with only one First Read event per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP206E Duplicate First Change event specification.

Explanation

A duplicate First Change event has been detected.

User response

Update the policy with only one First Change event per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP207E Expected <*policy*> specification but found <***>.

Explanation

The <*policy*> tag was expected but a different tag (<***>) was found.

User response

Correct the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP208E Policy syntax error

Explanation

A syntax error was found while parsing the policy.

User response

Correct the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP209E Error in opening data set: [*dataset*]

Explanation

An error occurred while opening a data set for policy parsing.

User response

Make sure the dataset exists and is associated with the appropriate permissions.
Parent topic: Error messages and codes: ADHPxxxx

ADHP210I A thread termination request was received for thread [*thread ID*]

Explanation

A termination request was received for thread [*thread ID*].

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP211W Policy syntax error [*error*]

Explanation

A syntax error was found while parsing the policy.

User response

Correct the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP212W [*policy* | *quarantine* | *blocking*] not enabled for ddname [*ddname*] reason: XML error

Explanation

The policy from DD is not enabled because a syntax error was found.

User response

Correct the policy in the DD.
Parent topic: Error messages and codes: ADHPxxxx

ADHP213E Blocking policy syntax error: Invalid network [*network*]

Explanation

Network value is not valid in the installed blocking policy.

User response

Correct the network value and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP214E Blocking policy syntax error: Invalid netmask [*netmask*]

Explanation

Netmask value is not valid in the installed blocking policy.

User response

Correct the netmask value and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP215E Blocking policy syntax error: Invalid IP address [*IP address*]

Explanation

IP address value is not valid in the blocking policy.

User response

Correct the IP address value and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP216W Blocking policy is ignored due to a previous error.

Explanation

The installed blocking policy contains a syntax error. The blocking policy is discarded.

User response

Resolve the error and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP217W Incomplete rule discarded. Rule name: [_*rule-name*_]

Explanation

An incomplete policy rule is detected.

System action

The rule is discarded.

User response

Use the Guardium Policy Builder of the Guardium® appliance interface to define and manage data collection and filtering. Correct the specified rule *rule-name* and add the necessary filters to make it a complete rule.
Parent topic: Error messages and codes: ADHPxxxx

ADHP218W Only one SQLCODE list is allowed. SQLCODE is discarded: [*sqlcode*]

Explanation

More than one SQLCODE list is detected.

System action

The first list is accepted. Additional lists are discarded.

User response

Ensure that there is only one SQLCODE list for each installed policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP220I Appliance connect retry count has been reached, appliance ping rate is now increased to [*number*]

Explanation

Ping rate has been increased to a larger value after reaching the specified number of APPLIANCE_CONNECT_RETRY_COUNT attempts.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP250E Unable to send message. Connection to server is unavailable.

Explanation

S-TAP was unable to send messages to the appliance.

User response

Make sure the appliance is online and reachable by the S-TAP.
Parent topic: Error messages and codes: ADHPxxxx

ADHP550E Unable to send message. Connection to server is unavailable

Explanation

An attempt to send a non-audit status message to the Guardium® system failed because no connection to the appliance is available.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

Error messages and codes: ADHQxxxx

The following information is about error messages and codes that begin with ADHQ. These messages are generated from the collector agent.

- **ADHQ1000E**
  NOT APF AUTHORIZED
- **ADHQ1001I**
  DB2 QUERY COMMON COLLECTOR INITIALIZATION IN PROGRESS FOR SUBSYSTEM
- **ADHQ1002I**
  DB2 AUDIT SQL COLLECTOR INITIALIZATION COMPLETE FOR SUBSYSTEM
- **ADHQ1003E**
  SUBSYSTEM *ssid* ALREADY ACTIVE
- **ADHQ1004I**
  QUERY COMMOON COLLECTOR TERMINATION IN PROGRESS FOR SUBSYSTEM *subsystem*
- **ADHQ1005I**
  QUERY COMMON COLLECTOR TERMINATION COMPLETE FOR SUBSYSTEM *ssid*
- **ADHQ1006E**
  statement DD STATEMENT MISSING
- **ADHQ1007E**
  INVALID USERID SPECIFIED FOR AUTHID
- **ADHQ1010I**
  DEBUG MODE ON
- **ADHQ1011I**
  DEBUG MODE OFF
- **ADHQ1016E**
  INVALID COMMAND SYNTAX
- **ADHQ1017E**
  INVALID COMMAND
- **ADHQ1019I**
  INTERVAL EXTERNALIZATION MODE OFF
- **ADHQ1020E**
  DB2 SUBSYSTEM *ssid* IS NOT DEFINED
- **ADHQ1024E**
  dsn SPECIFICATION INVALID
- **ADHQ1026E**
  SHARED MEMORY FAILURE FOR OBJECT *object request* RC =*rc* RS=*rs*
- **ADHQ1027I**
  CPU=*CPU Type-CPU Model-CPU Manufacturer*. *OS Name OS Version.OS Release.OS Modification*.
- **ADHQ1028E**
  Component requires a 64 bit processor and z/OS® 1.5 or higher.
- **ADHQ1031E**
  Serious error in master address space *address space*.
- **ADHQ1032I**
  Recreating master address space.
- **ADHQ1033E**
  Unable to create master address space *address space*.
- **ADHQ1034I**
  Master address space has started.
- **ADHQ1035E**
  Unable to restart master (RS=rc).
- **ADHQ1055E**
  CQM1055E DB2 ssid IS EXPERIENCING STORAGE CONSTRAINTS, DATA LOSS MAY OCCUR, REASON=code
- **ADHQ1060I**
  ZIIP SUPPORT IS NOT ACTIVE. *nnnnnnnn* RC=*yy* RSN=*zzzzzzzz nnnnnnnn* is the name of the service that failed with a nonzero return code (RC).
- **ADHQ1061E**
  MISSING PARAMETER: *parameter*
- **ADHQ1062E**
  COMMUNICATION INTERFACE DISABLED BY CROSS MEMORY FAILURE
- **ADHQ1062I**
  ZIIP SUPPORT IS INSTALLED
- **ADHQ1065E**
  REQUIRED DATA ACCESS COMMON COLLECTOR MODULE NOT FOUND
- **ADHQ1066E**
  Subsystem terminating due to abend while compiling the collection profile. SVCDUMP collected.
- **ADHQ1070E**
  Terminating due to XML profile processing error RC (xxxxxxxx)
- **ADHQ1071E**
  Terminating due to missing XML profile at start up
- **ADHQ1080I**
  POLICY MANAGER STARTED.
- **ADHQ1081I**
  POLICY MANAGER STOPPED.
- **POLICY PUSH DETECTED.**
- **ADHQ1083I**
  POLICY PUSH SENT.
- **ADHQ1084I**
  QUARANTINE ONLY POLICY DETECTED.
- **ADHQ1085I**
  CURRENT QUARANTINE POLICY IS REMOVED.
- **ADHQ1086I**
  BOTH NEW POLICY AND QUARANTINE POLICY DETECTED.
- **ADHQ1086E**
  ADHQ1086E *statement* DD STATEMENT MISSING

- **ADHQ1153E**
  RETURN CODE *return_code* REASON CODE *reason_code* WAS ENCOUNTERED DURING TRANSLATION SOURCE CCSID *ccsid* TARGET CCSID *ccsid*
- **ADHQ1202I**
  STORAGE CONSTRAINT RELIEVED FOR SPACE – *space* – OCCURRENCES: *count*
- **ADHQ1203I**
  ASID=*asid*,TCB=*tcb*,CPID=*cpid*, MODULE=*module*,ADDR=*addr*, RC=*rc*,RSN=*rsn*
- **ADHQ1204I**
  FUNC=*func*,SP=*subpool*,FLG2=*flag*,FLG3=*flag*
- **ADHQ1205E**
  ISM ERROR OCCURRED, DETAIL FOLLOWS: *note*
- **ADHQ1209I**
  ISM ERROR RC=*rc*,RSN=*rsn*,SPACE – *space*
- **ADHQ1210E**
  ISM SPACE IS DISABLED – space
- **ADHQ1211I**
  AN ABEND OCCURRED DURING ISM PROCESSING FOR SPACE – *space*
- **ADHQ1212E**
  AN ERROR OCCURRED IN THE EXTENT EXIT ROUTINE FOR SPACE – *space*
- **ADHQ1213W**
  SPACE IS FULL AND NO MORE EXTENTS CAN BE OBTAINED FOR SPACE – space
- **ADHQ1214W**
  OWNER LIMIT EXCEEDED FOR SPACE – *space*
- **ADHQ1215W**
  SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*
- **ADHQ1216E**
  EXTENT PROCESSING FAILED (ABEND) FOR SPACE – *space*
- **ADHQ1217W**
  SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*
- **ADHQ1218W**
  MAXIMUM EXTENTS HAS BEEN REACHED FOR SPACE – *space*
- **ADHQ1219W**
  ALL ISMERROR MESSAGE BLOCKS ARE IN USE
- **ADHQ1500E**
  ABNORMAL EOT FOR *subtask* SUBTASK
- **ADHQ2001E**
  DB2 SUBSYSTEM *ssid* ALREADY MONITORED BY SUBSYSTEM *ssid*
- **ADHQ2002E**
  MONITORING AGENT INSTALLATION FAILED FOR SUBSYSTEM *ssid*
- **ADHQ2003I**
  FORCING MONITORING AGENT INSTALLATION FOR *ssid*
- **ADHQ2005I**
  MULTIPLE MONITORING AGENT INSTALLATION FOR SUBSYSTEM *ssid*
- **ADHQ2008E**
  DB2 SYSTEM *ssid* IS BEING MONITORED BY A 2.2 OR BELOW VERSION CQM SUBSYSTEM AND CANNOT BE AUDITED
- **ADHQ2009E**
  DB2 SYSTEM ssid WAS PREVIOUSLY MONITORED BY A 2.2 OR EARLIER CQM SUBSYSTEM qmid WHICH HAS NOT APPLIED APAR PK55535.
- **ADHQ2010I**
  CURRENTLY ACTIVE POLICY RESULTS IN DISABLED COLLECTION
- **ADHQ2013I**
  CURRENTLY ACTIVE POLICY RESULTS IN GRANT/REVOKE COLLECTION
- **ADHQ2014I**
  CURRENTLY ACTIVE POLICY RESULTS NO HOST VARIABLE COLLECTION.
- **ADHQ2015I**
  CURRENTLY ACTIVE POLICY RESULTS NEGATIVE SQL CODES COLLECTION.
- **ADHQ2016I**
  CURRENTLY ACTIVE POLICY RESULTS DB2 COMMANDS COLLECTION.
- **ADHQ2017I**
  CURRENTLY ACTIVE POLICY RESULTS IN DBNAMES OPTIMIZATION.
- **ADHQ2018I**
  CURRENTLY ACTIVE POLICY RESULTS IN A QUARANTINE LIST.
- **ADHQ2019I**
  CURRENTLY ACTIVE POLICY RESULTS IN DB2 UTILITIES COLLECTION
- **ADHQ2020I**
  CURRENTLY ACTIVE POLICY RESULTS IN FAILED LOGIN COLLECTION.
- **ADHQ2100E**
  UNRECOGNIZED PARAMETER
- **ADHQ2101E**
  PARAMETER ERROR DETECTED FOR *parameter*
- **ADHQ2103E**
  DUPLICATE PARAMETER DETECTED FOR *parameter*
- **ADHQ2110E**
  TERMINATING DUE TO ERRORS IN PARAMETER FILE
- **ADHQ2111E**
  ERROR READING PARAMETER DATASET - MEMBER NOT FOUND
- **ADHQ2402I**
  DATASPACE MANAGEMENT IN PROGRESS FOR *dsmgmt*
- **ADHQ2403I**
  n DATASPACE PAGES RELEASED FOR *ssid*
- **ADHQ2408E**
  INVALID REPLY. REPLY "U" TO ACCEPT OR "R" TO REJECT

- **ADHQ2601E**
  ALLOCATION FAILED FOR VSAM DATASET *dsn* RETCD=*rc* REAS=*rs*
- **ADHQ2603E**
  DEALLOCATION FAILED FOR DATASET *data_set* RETCD=*return_code* REAS=*reason_code*
- **ADHQ3001I**
  DB2 STARTUP DETECTED FOR SUBSYSTEM *ssid*
- **ADHQ3002I**
  MONITORING AGENT STARTED FOR SUBSYSTEM *ssid*
- **ADHQ3003I**
  DB2 SHUTDOWN DETECTED FOR SUBSYSTEM *ssid*
- **ADHQ3005I**
  MONITORING AGENT DEACTIVATED FOR *ssid*
- **ADHQ3006I**
  AUDITING AGENT ACTIVATED FOR *ssid*
- **ADHQ3192E**
  LEVEL STATUS DB2(ssid) message
- **ADHQ3192I**
  LEVEL STATUS DB2(ssid) message
- **ADHQ3200I**
  DISPLAY AGENTS
- **ADHQ3201I**
  DB2 SUBYSYSTEM *ssid* AGENT ADDRESS *address*
- **ADHQ3202I**
  ssid AGENT ADDRESS *address*
- **ADHQ3203I**
  ASC DIAGNOSTIC DISPLAY:
- **ADHQ3204I**
  SDA ADDRESS *address*
- **ADHQ3205I**
  ssid ADDRESS *address*
- **ADHQ3206I**
  DIAGNOSTIC DATA FOR ABEND AT PSW *psw*
- **ADHQ3207I**
  SYSTEM COMPLETION CODE *code*
- **ADHQ3208I**
  OCCURRENCES *n* DATE *date* TIME *time*
- **ADHQ3209I**
  GPR 0-3 *info*
- **ADHQ3210I**
  GPR 4-7 *info*
- **ADHQ3211I**
  GPR 8-11 *info*
- **ADHQ3212I**
  GPR 12-15 *info*
- **ADHQ3213I**
  AR 0-3 *info*
- **ADHQ3214I**
  AR 4-7 *info*
- **ADHQ3215I**
  AR 8-11 *info*
- **ADHQ3216I**
  AR 12-15 *info*
- **ADHQ3240I**
  DB2 QM DATASPACE USAGE DISPLAY:
- **ADHQ3241I**
  dataspace DATASPACE
- **ADHQ3242I**
  NODE SIZE *size*
- **ADHQ3243I**
  TOTAL NODES *n*
- **ADHQ3244I**
  AVAILABLE NODES *n*
- **ADHQ3245I**
  PERCENT UTILIZED *n*
- **ADHQ3250I**
  POSTING INTERVAL PROCESSOR
- **ADHQ3251I**
  INTERVAL PROCESSOR NOT POSTED - DB2 UNAVAILABLE
- **ADHQ3252I**
  INTERVAL PROCESSING ALREADY IN PROGRESS
- **ADHQ3308E**
  DB2 SYSTEM ssid IS MONITORED BY DB2 QUERY MONITOR ssid WHICH HAS MISMATCHED OBJ AGENT
- **ADHQ3315E**
  MASTER SUBSYSTEM DOES NOT MATCH
- **ADHQ3402I**
  ISSUING COMMAND *cmd*
- **ADHQ3551E**
  VSAM LOGIC ERROR ENCOUNTERED WHILE ACCESSING CONTROL FILE FOR DB2 *ssid*. VSAMRC='*rc*' VSAMRS=X'*rs*'
- **ADHQ3552E**
  SETUP INFORMATION MISSING FROM CONTROL FILE FOR DB2 *ssid*

- **ADHQ3553E**
  message ERROR *message*
- **ADHQ4001E**
  CONNECT TO DB2 *ssid* FAILED FOR PLAN *plan* RETURN CODE *rc* REASON CODE *rs*
- **ADHQ4003E**
  CONNECT FAILED - DB2 NOT OPERATIONAL
- **ADHQ5010I**
  MONITORING AGENT DEINSTALLATION IN PROGRESS FOR SUBSYSTEM *ssid*
- **ADHQ5011I**
  MONITORING AGENT DEINSTALLATION COMPLETE FOR SUBSYSTEM *ssid*
- **ADHQ5012I**
  REQURESTING MONITORING AGENT ACTIVATION FOR DB2 SUBSYSTEM *ssid*
- **ADHQ5013I**
  REQUESTING MONITORING AGENT DEACTIVATION FOR DB2 SUBSYSTEM *ssid*
- **ADHQ6101E**
  LOCATE FAILED FOR *dataset* R0=*code* RC=*rc*
- **ADHQ6102E**
  SCRATCH FAILED FOR *file* SCRATCH STATUS CODE=*code* RO=*ro*
- **ADHQ7001E**
  table TABLE NOT LOCATED IN DB2 CATALOG
- **ADHQ7008E**
  QUERY COMMON COLLECTOR *ssid* NOT VALID OR HAS NOT BEEN STARTED SINCE IPL
- **ADHQ7009E**
  OUT OF SPACE CONDITION DETECTED WHILE WRITING TO THE *dsn* DATASET
- **ADHQ7010E**
  MISSING "ADD" PARAMETER FOR *parameter* AT LINE *line* COLUMN *column*
- **ADHQ7011E**
  INTERNAL ERROR - UNABLE TO RESOLVE ALTERNATE COLUMN *column*
- **ADHQ7015E**
  NUMBER OF BSDS SPECIFICATIONS INVALID OR MISSING
- **ADHQ7016E**
  DUPLICATE RECORD STORE ATTEMPTED FOR DB2 SUBSYSTEM *ssid*
- **ADHQ8001E**
  ERRORS DETECTED IN *parameters* PARAMETERS:
- **ADHQ8002E**
  UNIDENTIFIED KEYWORD DETECTED AT LINE *line* COLUMN *column*
- **ADHQ8003E**
  INVALID SYNTAX SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8004E**
  PARAMETER LENGTH EXCEEDED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8005E**
  PARAMETER MISSING FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8006E**
  NON NUMERIC DATA SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8007E**
  INVALID VALUE SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8008E**
  value MUST BE *value* THAN *value*
- **ADHQ8009E**
  DUPLICATE PARAMETER *parameter* AT LINE *line* COLUMN *column*
- **ADHQ8010E**
  DUPLICATE SUBPARAMETER DETECTED FOR PARAMETER *parameter* AT LINE *line* COLUMN *column*
- **ADHQ8011E**
  DB2 VERSION NOT SUPPORTED
- **ADHQ8012E**
  ERROR OPENING DDNAME *ddname*
- **ADHQ8013E**
  INVALID PARAMETER LENGTH FOR *parameter*
- **ADHQ8014E**
  LOGIC ERROR: *error*
- **ADH8022I**
  adh parameter value
- **ADH9899I**
  adh modify command

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHQ1000E NOT APF AUTHORIZED

Explanation

The collector agent started task or job is not APF authorized.

User response

The collector agent requires that the target load libraries be APF-authorized.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1001I DB2® QUERY COMMON COLLECTOR INITIALIZATION IN PROGRESS FOR SUBSYSTEM

Explanation

This message appears during the normal initialization process of the collector agent.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1002I DB2® AUDIT SQL COLLECTOR INITIALIZATION COMPLETE FOR SUBSYSTEM

Explanation

This message appears during the normal initialization process of the collector agent and confirms the initialization process has completed.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1003E SUBSYSTEM *ssid* ALREADY ACTIVE

Explanation

The collector agent indicated in the message is already active and can therefore cannot process another activate command.

User response

Verify that you are activating the correct system. If you are attempting to activate a subsystem that is already active, do not attempt activation.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1004I QUERY COMMOON COLLECTOR TERMINATION IN PROGRESS FOR SUBSYSTEM *subsystem*

Explanation

This message appears during normal shutdown of the Collector Agent and indicates the collector is undergoing shutdown.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1005I QUERY COMMON COLLECTOR TERMINATION COMPLETE FOR SUBSYSTEM *ssid*

Explanation

The collector agent subsystem has been terminated. This message could appear as part of normal shutdown or as a failure to connect to a subsystem.

User response

Investigate other write-to-operator (WTO) messages preceding this one to determine the reason for the termination.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1006E *statement* DD STATEMENT MISSING

Explanation

The parameter DD statement (for example, ADHCFGP DD statement) is missing from the JCL for the collector agent started task.

User response

Create the necessary DD statement and code the appropriate parameters in the data set.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1007E INVALID USERID SPECIFIED FOR AUTHID

Explanation

The user ID entered in the AUTHID parm in the ADHCFGP data set has not been defined to RACF® or an equivalent security system.

User response

Correct the user ID, or ensure the ID is defined to your security system.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1010I DEBUG MODE ON

Explanation

Debugging mode has been turned on.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1011I DEBUG MODE OFF

Explanation

Debugging mode has been turned off.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1016E INVALID COMMAND SYNTAX

Explanation

The command syntax is invalid.

User response

Correct the command.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1017E INVALID COMMAND

Explanation

An invalid MVS™ Modify command was issued.

User response

Correct the command and execute it again.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1019I INTERVAL EXTERNALIZATION MODE OFF

Explanation

The collector agent subsystem was started with externalization mode set to off.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1020E DB2® SUBSYSTEM *ssid* IS NOT DEFINED

Explanation

The DB2 subsystem indicated in the message is not defined.

User response

Verify that you have specified the correct DB2 subsystem.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1024E *dsn* SPECIFICATION INVALID

Explanation

The data set name listed in this message is not valid.

User response

Verify that you specified the correct data set name in ADHCFGP.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1026E SHARED MEMORY FAILURE FOR OBJECT *object request* RC =*rc* RS=*rs*

Explanation

A shared memory failure has occurred for the indicated object.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1027I CPU=*CPU Type-CPU Model-CPU Manufacturer. OS Name OS Version.OS Release.OS Modification.*

Explanation

This message displays information about the CPU and the operating system.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1028E Component requires a 64 bit processor and z/OS® 1.5 or higher.

Explanation

Your system does not meet the minimum system requirements.

User response

Upgrade to the minimum requirements.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1031E Serious error in master address space *address space*.

Explanation

A serious error has occurred in the master address space specified.

User response

Verify that the master address space is available.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1032I Recreating master address space.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1033E Unable to create master address space *address space*.

Explanation

DB2® Query Monitor is not able to create the master address space specified.

User response

Many issues that cause this error relate to security setup. If you encounter this message, send your console log to IBM® Software Support.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1034I Master address space has started.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1035E Unable to restart master (RS=rc).

Explanation

The master address space could not be restarted.

User response

verify the master address space is available and restart.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1055E CQM1055E DB2® ssid IS EXPERIENCING STORAGE CONSTRAINTS, DATA LOSS MAY OCCUR, REASON=code

Explanation

The DB2 subsystem indicated in the message is experiencing storage constraints.

User response

Verify that your DB2 subsystem has the needed storage allocations.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1060I ZIIP SUPPORT IS NOT ACTIVE. *nnnnnnnn* RC=*yy* RSN=*zzzzzzzz nnnnnnnn* is the name of the service that failed with a nonzero return code (RC).

Explanation

Table 1. Return code explanations

Service	Description
IWM4ECRE (WLM Enclave Create)	The return codes and reason codes are documented in *z/OS V1R10.0 MVS™ Programming Workload Management Services*.
IWM4EoCT (WLM CPU Offload Time Service)	The return codes and reason codes are not documented in any existing WLM manual. However, RC=4 typically means no ZIIP is configured on the instance of z/OS®. If you have a ZIIP processor and it is properly configured, report the RC to the vendor.
MAXWFLOAD (Enclave SRB load service)	An error occurred trying to LOAD ADHMAXWF (the enclave SRB routine that runs on the ZIIP). Make sure you have the correct STEPLIB configured.
IEAVAPE (Z/OS Allocate Pause Element)	These return codes are described in *z/OS V1R10.0 MVS Programming Assembler Services References V2*. If the ADHQ1060I has IEAVAPE has the failing service, contact the vendor for resolution.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1061E MISSING PARAMETER: *parameter*

Explanation

The specified parameter has not been defined in the sample library member ADHCFGP.

User response

Add the missing parameter to the ADHCFGP sample library member.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1062E COMMUNICATION INTERFACE DISABLED BY CROSS MEMORY FAILURE

Explanation

A cross memory failure has occurred and as a result the communication interface has been disabled.

User response

Troubleshoot the memory failure and restart the ASC.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1062I ZIIP SUPPORT IS INSTALLED

Explanation

The collector agent has detected that WLM is configured for zIIP support. This does not necessarily indicate that zIIP processors are installed or are available for zIIP offload of collector agent processing.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1065E REQUIRED DATA ACCESS COMMON COLLECTOR MODULE NOT FOUND

Explanation

The started task did not find the Data Access Common Collector (CQC) initialization module, which prevented successful startup.

User response

Verify that the Data Access Common Collector (CQC) has been installed and that the load library is included in the started task STEPLIB concatenation
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1066E Subsystem terminating due to abend while compiling the collection profile. SVCDUMP collected.

Explanation

An abend was detected when compiling the collection profile. A memory dump was collected to gather the diagnostic information.

User response

If you are unable to take corrective measures to resolve the abend, then the SVCDUMP, the collector joblog, and the details of the collection profile in use should be reported to IBM® Software Support for resolution of this error.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1070E Terminating due to XML profile processing error RC (xxxxxxxx)

Explanation

A policy is sent from the Guardium® system to the Security Guardium S-TAP® for DB2® collector agent during their initial communication. If the policy received by the collector agent is not composed of valid XML syntax, the collector terminates.

User response

Verify that the Guardium system is properly configured, using the APPLIANCE_SERVER parameter. The system should be set up to accept connections from collectors. If the problem persists, contact IBM® Software Support with the return code specified in this message.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1071E Terminating due to missing XML profile at start up

Explanation

A policy is sent from the Guardium® system to the Security Guardium S-TAP® for DB2® collector agent during their initial communication. If the policy is not received by the collector agent during the initial communication set up, then the collector terminates.

User response

Verify that the Guardium system is properly configured, using the APPLIANCE_SERVER parameter. The appliance should be set up to accept connections from collectors. If the problem persists, contact IBM® Software Support.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1080I POLICY MANAGER STARTED.

Explanation

The internal policy manager task has started.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1081I POLICY MANAGER STOPPED.

Explanation

The internal policy manager task has stopped.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

POLICY PUSH DETECTED.

Explanation

A policy was received from the appliance.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1083I POLICY PUSH SENT.

Explanation

The policy was sent to Audit SQL Collector.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1084I QUARANTINE ONLY POLICY DETECTED.

Explanation

A pushed policy was included on a quarantine list. The currently active audit policy is unchanged and is still active.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1085I CURRENT QUARANTINE POLICY IS REMOVED.

Explanation

A new policy push occurred which resulted in the removal of the quarantine list.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1086I BOTH NEW POLICY AND QUARANTINE POLICY DETECTED.

Explanation

A new policy push occurred, which resulted in new policy and quarantine lists to be activated.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1086E ADHQ1086E *statement* DD STATEMENT MISSING

Explanation

The parameter DD statement (for example, ADHPARMS DD statement) is missing from the JCL for the collector agent started task.

User response

Create the necessary DD statement and code the appropriate parameters in the data set.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1153E RETURN CODE *return_code* REASON CODE *reason_code* WAS ENCOUNTERED DURING TRANSLATION SOURCE CCSID *ccsid* TARGET CCSID *ccsid*

Explanation

An error was encountered during the translation of the indicated CCSIDs. This may be the result of not having defined conversion paths between the CCSID of the collected SQL text and CCSID 1208 when performing a DB2® offload.

User response

To offload SQL text, verify that all necessary CCSID paths to 1208 are installed. You must define conversion paths between the CCSID of the collected SQL text and CCSID 1208.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1202I STORAGE CONSTRAINT RELIEVED FOR SPACE – *space* – OCCURRENCES: *count*

Explanation

An Integrated Storage Manager error had previously occurred due to a storage constraint for the space named in the message. The storage constraint has now been relieved. The number of storage constraint occurrences for this incident is displayed in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1203I ASID=*asid*,TCB=*tcb*,CPID=*cpid*, MODULE=*module*,ADDR=*addr*, RC=*rc*,RSN=*rsn*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message provides details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1204I FUNC=*func*,SP=*subpool*,FLG2=*flag*,FLG3=*flag*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message provides details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1205E ISM ERROR OCCURRED, DETAIL FOLLOWS: *note*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1209I ISM ERROR RC=*rc*,RSN=*rsn*,SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1210E ISM SPACE IS DISABLED – space

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1211I AN ABEND OCCURRED DURING ISM PROCESSING FOR SPACE – *space*

Explanation

A Query Monitor Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any dumps that may have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1212E AN ERROR OCCURRED IN THE EXTENT EXIT ROUTINE FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that might been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1213W SPACE IS FULL AND NO MORE EXTENTS CAN BE OBTAINED FOR SPACE – space

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager operation has failed because no more extents can be obtained for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

This may be a temporary situation due to the level of DB2 activity currently monitored by Security Guardium S-TAP for DB2. If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by Security Guardium S-TAP for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1214W OWNER LIMIT EXCEEDED FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Monitor Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that might have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1215W SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Monitor Integrated Storage Manager operation has failed because no more large extents can be obtained for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Support to diagnose the problem.

User response

This might be a temporary situation due to the level of DB2 activity currently being monitored by Security Guardium S-TAP for DB2. If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by Security Guardium S-TAP for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1216E EXTENT PROCESSING FAILED (ABEND) FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1217W SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager operation has failed because the request would have exceeded the maximum storage allocation specified in the MAXIMUM_ALLOCATIONS parameter in ADHPARMS. At the time of the error, Security Guardium S-TAP for DB2 was attempting to allocate additional storage for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

This might be a temporary situation due to the level of DB2 activity currently being monitored by Security Guardium S-TAP for DB2. If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by Security Guardium S-TAP for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1218W MAXIMUM EXTENTS HAS BEEN REACHED FOR SPACE – *space*

Explanation

An Integrated Storage Manager operation has failed because the request would have exceeded the maximum number of extents allowed for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

This might be a temporary situation due to the level of DB2® activity currently being monitored. If message ADHQ1202I is issued later to indicate that the Storage Constraint has ended, then processing resumes normally. If this situation rarely occurs, it might not be a problem. If this situation occurs frequently, adjust the amount of data collected by Security Guardium® S-TAP® for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with tuning these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1219W ALL ISMERROR MESSAGE BLOCKS ARE IN USE

Explanation

An Integrated Storage Manager error has occurred. However there were no free ISMERROR message blocks available.

User response

Increase the value of the ISM_ERROR_BLOCKS parameter in the ADHPARMS file. If this parameter is already set to the maximum value and the problem persists, contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1500E ABNORMAL EOT FOR *subtask* SUBTASK

Explanation

An abnormal end of task occurred for the subtask indicated in the message.

User response

Verify conditions surrounding the abnormal end of task and reissue the subtask.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2001E DB2® SUBSYSTEM *ssid* ALREADY MONITORED BY SUBSYSTEM *ssid*

Explanation

The indicated DB2 subsystem is already being monitored by the collector agent shown in the message.

User response

A DB2 subsystem can only be monitored by a single collector agent. To monitor the DB2 subsystem with another collector agent, first stop the monitoring of the DB2 subsystem by the collector agent (shown in the message).

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2002E MONITORING AGENT INSTALLATION FAILED FOR SUBSYSTEM *ssid*

Explanation

A monitoring agent was unable to start. Another SQL-type monitoring product might be active within the specified DB2® subsystem.

User response

Check to see if another SQL-type monitoring product is active. If so, shut down the other product and restart the S-TAP® collector. If this does not resolve the problem, contact IBM® Software Support.

If you encounter message ADHQ2002E and receive a memory dump, contact IBM Software Support and provide the memory dump for diagnostic purposes.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2003I FORCING MONITORING AGENT INSTALLATION FOR *ssid*

Explanation

The collector agent has detected that a monitoring agent is already active, but is forcing installation because `FORCE (Y)` was included.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2005I MULTIPLE MONITORING AGENT INSTALLATION FOR SUBSYSTEM *ssid*

Explanation

The collector agent has installed multiple monitoring agents for the subsystem shown in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2008E DB2 SYSTEM *ssid* IS BEING MONITORED BY A 2.2 OR BELOW VERSION CQM SUBSYSTEM AND CANNOT BE AUDITED

Explanation

This message indicates an incompatibility between DB2 Query Monitor and S-TAP. InfoSphere® Guardium S-TAP for DB2 Version 9.1 will not start auditing a DB2 subsystem that is running Query Monitor at Version 3.1 or earlier.

User response

Ensure that you are running compatible versions of S-TAP and Query Monitor, or run only one product at a time.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2009E DB2® SYSTEM ssid WAS PREVIOUSLY MONITORED BY A 2.2 OR EARLIER CQM SUBSYSTEM qmid WHICH HAS NOT APPLIED APAR PK55535.

Explanation

You must apply Query Monitory V2R2 APAR PK55535.

User response

Apply the required maintenance.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2010I CURRENTLY ACTIVE POLICY RESULTS IN DISABLED COLLECTION

Explanation

The currently installed collection policy, as received from the Guardium® system, results in no ASC collection. This can be the result of:

- No policies are installed on the system.
- No DB2® Collection Profile policies are installed on the system.
- No DB2 Collection Profile policies matching the Svc. Name of the collector agent SSID are installed on the system.
- No DB2 Collection Profile policies contain Object entries that would result in ASC collection.

User response

If ASC collection is expected when this message is issued, review installed policy definitions in the Guardium system administration interface for the previously listed conditions. If no ASC collection is expected when this message is issued, no action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2013I CURRENTLY ACTIVE POLICY RESULTS IN GRANT/REVOKE COLLECTION

Explanation

The activated policy enables the collection of GRANT and REVOKE SQL statements. GRANT and REVOKE SQL statements are collected if they match the policy filter criteria.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2014I CURRENTLY ACTIVE POLICY RESULTS NO HOST VARIABLE COLLECTION.

Explanation

Host variables, which are also known as BIND variables, are not collected.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2015I CURRENTLY ACTIVE POLICY RESULTS NEGATIVE SQL CODES COLLECTION.

Explanation

The active policy contains a negative SQL code list that results in the collection of events ending with a negative SQL code.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2016I CURRENTLY ACTIVE POLICY RESULTS DB2 COMMANDS COLLECTION.

Explanation

Collection of COMMAND events is enabled.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2017I CURRENTLY ACTIVE POLICY RESULTS IN DBNAMES OPTIMIZATION.

Explanation

The currently active policy contains rules with DBNAME filters, which enables optimized filtering of audit events.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2018I CURRENTLY ACTIVE POLICY RESULTS IN A QUARANTINE LIST.

Explanation

The active policy contains a quarantine list that might cause DB2 activity to be quarantined.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2019I CURRENTLY ACTIVE POLICY RESULTS IN DB2 UTILITIES COLLECTION

Explanation

The active policy enables the collection of DB2 utilities.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2020I CURRENTLY ACTIVE POLICY RESULTS IN FAILED LOGIN COLLECTION.

Explanation

The active policy enables the collection of Failed Login events.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2100E UNRECOGNIZED PARAMETER

Explanation

The collector agent has encountered an unrecognized parameter.

User response

Check the startup parameters to ensure that the parameters specified are all valid.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2101E PARAMETER ERROR DETECTED FOR *parameter*

Explanation

The collector agent has encountered an error in one of the startup parameters.

Note: Message ADHQ2101E can be issued when the collector agent is started if the ADHCFGP file specifies primary space allocations for back store data sets that are less than the default.

User response

Check the startup parameters to ensure that all are specified properly. Check that primary space allocations for back store data sets are not set for less than their default values.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2103E DUPLICATE PARAMETER DETECTED FOR *parameter*

Explanation

Duplicate parameters were specified in the Query Common Collector startup parameters.

User response

Check the startup parameters to ensure that all are specified properly. Remove any duplicate parameters.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2110E TERMINATING DUE TO ERRORS IN PARAMETER FILE

Explanation

An error in the collector agent parameter file caused the termination of processing.

User response

Verify that the input you specified for your collector agent parameters in ADHCFGP is valid and correct for your objectives.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2111E ERROR READING PARAMETER DATASET - MEMBER NOT FOUND

Explanation

The collector agent encountered an error while attempting to read the ADHCFGP data set. The ADHPARMS DD statement specified a PDS data set and the member name specified did not exist.

User response

Correct the JCL specification for the ADHPARMS DD statement and specify a valid member name.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2402I DATASPACE MANAGEMENT IN PROGRESS FOR *dsmgmt*

Explanation

Indicates dataspace management is in progress for the subsystem shown in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2403I *n* DATASPACE PAGES RELEASED FOR *ssid*

Explanation

Displays the number of dataspace pages that have been released for the subsystem shown in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2408E INVALID REPLY. REPLY "U" TO ACCEPT OR "R" TO REJECT

Explanation

The replay you entered is not valid.

User response

Enter U to accept or R to reject.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2601E ALLOCATION FAILED FOR VSAM DATASET *dsn* RETCD=*rc* REAS=*rs*

Explanation

This message is issued by the started task if there is a problem during the dynamic allocation of a data set. When this message occurs, the collector agent stops and the startup process and terminates.

User response

To further diagnose and resolve the problem using the return code and reason code listed in the message, refer to the *MVS™ Programming Authorized Assembler Services Guide* (SA22-7608-07).

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2603E DEALLOCATION FAILED FOR DATASET *data_set* RETCD=*return_code* REAS=*reason_code*

Explanation

This message reports errors encountered during the execution of a CLOSE macro instruction.

User response

To further diagnose and resolve the problem using the return code and reason code listed in the message, refer to the *z/OS® V1R1.0 DFSMS/DFP Diagnosis Reference* (GY27-7618-01) or the following Web page:

http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/dgt2r101/20.8.1.2
Parent topic: Error messages and codes: ADHQxxxx

ADHQ3001I DB2® STARTUP DETECTED FOR SUBSYSTEM *ssid*

Explanation

The collector agent determined that a DB2 subsystem in its monitor list has started.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3002I MONITORING AGENT STARTED FOR SUBSYSTEM *ssid*

Explanation

Security Guardium® S-TAP® for DB2® has initiated monitoring for the named subsystem.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3003I DB2® SHUTDOWN DETECTED FOR SUBSYSTEM *ssid*

Explanation

The collector agent determined that a DB2 subsystem in its monitor list has shut down.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3005I MONITORING AGENT DEACTIVATED FOR *ssid*

Explanation

The monitoring agent has been deactivated for the indicated Collector Agent.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3006I AUDITING AGENT ACTIVATED FOR *ssid*

Explanation

The collector agent has been instructed to start the monitoring agent for a given DB2® subsystem when it becomes active. Monitoring of SQL for the DB2 subsystem will start when the monitoring agent is started indicated by message ADHQ3002I. Monitoring will continue after message ADHQ3002I is issued until one of the following

events occur:

1. The DB2 subsystem is stopped.
2. A deactivate for the monitoring agent is performed.
3. The collector agent subsystem that is monitoring the DB2 subsystem is stopped.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3192E LEVEL STATUS DB2(ssid) message

Explanation

This message displays if a mismatch in code level exists between Security Guardium® S-TAP® for DB2® and Query Monitor. One message per mismatched code level will occur.

User response

Ensure that all the programs listed have the Query Monitor and corresponding Security Guardium S-TAP for DB2 maintenance applied.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ3192I LEVEL STATUS DB2(ssid) message

Explanation

This message displays if a mismatch in code level exists between Security Guardium® S-TAP® for DB2® and DB2 Query Monitor. This message occurs once per mismatched code level.

User response

Verify that all the programs listed have the Query Monitor and corresponding S-TAP for DB2 maintenance applied.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ3200I DISPLAY AGENTS

Explanation

This message is used in conjunction with other messages to indicate display agents.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3201I DB2® SUBYSYSTEM *ssid* AGENT ADDRESS *address*

Explanation

Indicates the DB2 subsystem and agent address.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3202I *ssid* AGENT ADDRESS *address*

Explanation

Indicates the monitoring agent address.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3203I ASC DIAGNOSTIC DISPLAY:

Explanation

Indicates ASC diagnostic display is in effect.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3204I SDA ADDRESS *address*

Explanation

Indicates the SDA address.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3205I *ssid* ADDRESS *address*

Explanation

This message is used in conjunction with other messages to indicate the address.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3206I DIAGNOSTIC DATA FOR ABEND AT PSW *psw*

Explanation

The message displays diagnostic data for the abend.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3207I SYSTEM COMPLETION CODE *code*

Explanation

The message indicates the system completion code.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3208I OCCURRENCES *n* DATE *date* TIME *time*

Explanation

Indicates the number of occurrences and the date and time at which the took place.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3209I GPR 0-3 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3210I GPR 4-7 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3211I GPR 8-11 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3212I GPR 12-15 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3213I AR 0-3 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3214I AR 4-7 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3215I AR 8-11 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3216I AR 12-15 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3240I DB2® QM DATASPACE USAGE DISPLAY:

Explanation

This message appears in conjunction with other messages as a result of the MVS™ Modify command DISPLAY DATASPACES.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3241I *dataspace* DATASPACE

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3242I NODE SIZE *size*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command DISPLAY DATASPACES. This message lists the node size for the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3243I TOTAL NODES *n*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`. This message lists the total number of nodes allowed for the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3244I AVAILABLE NODES *n*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`. This message lists the total number of nodes available for use by the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3245I PERCENT UTILIZED *n*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`. This message lists the percentage of nodes used for the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3250I POSTING INTERVAL PROCESSOR

Explanation

This message appears to inform you that the interval processor has been started through an MVS™ Modify INTERVAL command.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3251I INTERVAL PROCESSOR NOT POSTED - DB2® UNAVAILABLE

Explanation

The interval processor was not started because a DB2 subsystem is not available.

User response

Verify the status of all monitored DB2 subsystems.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3252I INTERVAL PROCESSING ALREADY IN PROGRESS

Explanation

This message appears to inform you that the interval processor was already started through an MVS™ Modify `INTERVAL` command.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3308E DB2® SYSTEM ssid IS MONITORED BY DB2 QUERY MONITOR ssid WHICH HAS MISMATCHED OBJ AGENT

Explanation

This message indicates that the maintenance levels of one or more object modules do not match between the Security Guardium® S-TAP® for DB2 and Query Monitor installations. The maintenance code levels for Security Guardium S-TAP for DB2 and Query Monitor installations must match.

User response

Ensure that the maintenance levels match between the Security Guardium S-TAP for DB2 and Query Monitor installations. Apply maintenance as required to one or both environments to ensure that the maintenance levels match.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3315E MASTER SUBSYSTEM DOES NOT MATCH

Explanation

For monitoring and auditing to be active on the DB2® subsystem, a DB2 subsystem that is monitored by DB2 Query Monitor or Workload Replay for DB2 for z/OS® or audited by Security Guardium® S-TAP® for DB2 must have a matching MASTER_PROCNAME parameter between the Query Monitor subsystem and the Workload Replay DB2 subsystem, or the Security Guardium S-TAP for DB2 ASC started task.

User response

Update the MASTER_PROCNAME parameter for DB2 Query Monitor, Security Guardium S-TAP for DB2, or Workload Replay so that the same MASTER_PROCNAME is in use by all products for the monitored DB2 subsystem. After updating the MASTER_PROCNAME, restart the started task for the task that is affected by the parameter change.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3402I ISSUING COMMAND *cmd*

Explanation

Indicates command execution.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3551E VSAM LOGIC ERROR ENCOUNTERED WHILE ACCESSING CONTROL FILE FOR DB2® *ssid*. VSAMRC='*rc*' VSAMRS=X'*rs*'

Explanation

A VSAM logic error was encountered when accessing the control file for the DB2 subsystem indicated in the message.

User response

Verify that the DB2 control file for the DB2 subsystem listed in the message has been properly allocated and that the appropriate DB2 subsystem and plan names information have been specified correctly.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3552E SETUP INFORMATION MISSING FROM CONTROL FILE FOR DB2® *ssid*

Explanation

There is insufficient information in the control file for the DB2 subsystem indicated in the message.

User response

Modify the control file to include the necessary information.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3553E *message* ERROR *message*

Explanation

An error has occurred. This message is customized to display various messages such as initialization errors.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ4001E CONNECT TO DB2® *ssid* FAILED FOR PLAN *plan* RETURN CODE *rc* REASON CODE *rs*

Explanation

Security Guardium® S-TAP® for DB2 was not able to connect to the DB2 subsystem using the plan shown in the message.

User response

Refer to *DB2 Universal Database for z/OS® V8 Messages* (GC18-9602-01) and *DB2 Universal Database for z/OS V8 Codes* (GC18-9603-01) to further diagnose and resolve the problem.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ4003E CONNECT FAILED - DB2® NOT OPERATIONAL

Explanation

The collector agent was not able to connect to the DB2 subsystem because DB2 is not currently operational.

User response

Verify that DB2 is functioning correctly.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ5010I MONITORING AGENT DEINSTALLATION IN PROGRESS FOR SUBSYSTEM *ssid*

Explanation

The monitoring agent deinstallation is in progress for the DB2® subsystem indicated in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ5011I MONITORING AGENT DEINSTALLATION COMPLETE FOR SUBSYSTEM *ssid*

Explanation

The monitoring agent deinstallation completed for the DB2® subsystem indicated in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ5012I REQURESTING MONITORING AGENT ACTIVATION FOR DB2® SUBSYSTEM *ssid*

Explanation

The monitoring agent for the indicated DB2 subsystem is being requested for activation.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ5013I REQUESTING MONITORING AGENT DEACTIVATION FOR DB2® SUBSYSTEM *ssid*

Explanation

The monitoring agent for the indicated DB2 subsystem is being requested for deactivation.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ6101E LOCATE FAILED FOR *dataset* R0=*code* RC=*rc*

Explanation

A catalog located failed during interval data set expiration processing. r0 contains the contents of the register zero and rc is the LOCATE return code.

User response

See *z/OS® DFSMSdfp Advanced Services* (SC26-7400-02) for a description of the return codes issued by LOCATE.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ6102E SCRATCH FAILED FOR *file* SCRATCH STATUS CODE=*code* RO=*ro*

Explanation

The scratch failed for the indicated file.

User response

See *z/OS® DFSMSdfp Advanced Services* (SC26-7400-02) for a description of the return codes issued by LOCATE.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7001E *table* TABLE NOT LOCATED IN DB2® CATALOG

Explanation

The table indicated in the message cannot be found in the DB2 catalog.

User response

Verify that the table you specified exists.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7008E QUERY COMMON COLLECTOR *ssid* NOT VALID OR HAS NOT BEEN STARTED SINCE IPL

Explanation

The collector agent shown in the message is not a valid collector agent.

User response

Verify that you specified the correct Query Common Collector subsystem ID, and that the collector agent is available.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7009E OUT OF SPACE CONDITION DETECTED WHILE WRITING TO THE *dsn* DATASET

Explanation

An out-of-space condition was encountered when attempting to write to the data set indicated in the message.

User response

Verify that adequate space has been allocated to the data set.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7010E MISSING "ADD" PARAMETER FOR *parameter* AT LINE *line* COLUMN *column*

Explanation

The ADD parameter is missing for the indicated line and column.

User response

Specify an ADD parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7011E INTERNAL ERROR - UNABLE TO RESOLVE ALTERNATE COLUMN *column*

Explanation

There has been an internal error.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7015E NUMBER OF BSDS SPECIFICATIONS INVALID OR MISSING

Explanation

An invalid number of BSDS parameters has been sent as input to the ADH#CTLF utility.

User response

Verify that the two boot strap data sets used for your DB2® subsystem are properly specified.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7016E DUPLICATE RECORD STORE ATTEMPTED FOR DB2® SUBSYSTEM *ssid*

Explanation

This message describes an error condition when attempting to load records into the control file that already exist without specifying REPLACE(Y) for the DB2 subsystem indicated in the message.

User response

Edit your ADH#CTLF job to include REPLACE(Y). Refer to the instructions in SADHSAMP library member ADH#CTLF for details.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8001E ERRORS DETECTED IN *parameters* PARAMETERS:

Explanation

Errors have been detected in ADHCFGP.

User response

Verify that the parameters you specified in ADHCFGP are correct and modify any syntax errors before proceeding.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8002E UNIDENTIFIED KEYWORD DETECTED AT LINE *line* COLUMN *column*

Explanation

An unknown keyword has been found.

User response

Verify the correct syntax and modify the keyword as needed.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8003E INVALID SYNTAX SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

The syntax specified for the parameter indicated in the message is not valid.

User response

Correct the syntax and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8004E PARAMETER LENGTH EXCEEDED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

The length of the value specified for the parameter indicated in the message exceeded the valid length for that parameter.

User response

Correct the syntax and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8005E PARAMETER MISSING FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

A required parameter is missing from ADHLOADP.

User response

Correct the syntax and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8006E NON NUMERIC DATA SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

Non-numeric data was specified in ADHLOADP for the parameter listed in the message.

User response

Specify numeric data for the parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8007E INVALID VALUE SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

An invalid value was specified in ADHLOADP.

User response

Correct the value and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8008E *value* MUST BE *value* THAN *value*

Explanation

The value of the parameter shown in the message must be within the specified range.

User response

Correct the value of the parameter so it falls within the range indicated in the message text.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8009E DUPLICATE PARAMETER *parameter* AT LINE *line* COLUMN *column*

Explanation

A parameter you specified is a duplicate.

User response

Correct the syntax to eliminate the duplicate parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8010E DUPLICATE SUBPARAMETER DETECTED FOR PARAMETER *parameter* AT LINE *line* COLUMN *column*

Explanation

A sub-parameter you specified is a duplicate.

User response

Correct the syntax to eliminate the duplicate sub-parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8011E DB2® VERSION NOT SUPPORTED

Explanation

The version of DB2 with which you are attempting to use is not supported by unload functionality of the collector agent.

User response

The collector agent unloads data to DB2 Version 8, DB2 Version 9, or DB2 Version 10.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8012E ERROR OPENING DDNAME *ddname*

Explanation

The collector agent encountered an error attempting to open the TEXTDATA data set.

User response

Verify that the TEXTDATA data set is configured properly and has adequate space available.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8013E INVALID PARAMETER LENGTH FOR *parameter*

Explanation

The value you specified for the TBCREATOR parameter is too long and is therefore invalid.

User response

Specify a valid value for TBCREATOR. Valid values are up to eight characters in length.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8014E LOGIC ERROR: *error*

Explanation

The collector agent has encountered a logic error.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADH8022I *adh parameter value*

Explanation

This message is used to display the contents of the ADHPARMS file that was processed when Security Guardium® S-TAP® for DB2® was started.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADH9899I *adh modify command*

Explanation

This message is used to display the text of a modify command that was issued to Security Guardium® S-TAP® for DB2®.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

IBM Security Guardium S-TAP for IMS on z/OS

These topics describe how to use IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for IMS). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for IMS collects and correlates data access information from a variety of IMS resources to produce a comprehensive view of business activity for auditors.

About these topics

This information is designed to help database administrators, appliance programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for IMS
- Install and operate IBM Guardium S-TAP for IMS
- Configure the IBM Guardium S-TAP for IMS environment
- Diagnose and recover from IBM Guardium S-TAP for IMS problems

A PDF of this User's Guide is available here.

- **IBM Security Guardium S-TAP for IMS on z/OS**
  These topics describe how to use IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for IMS). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for IMS collects and correlates data access information from a variety of IMS resources to produce a comprehensive view of business activity for auditors.
- **What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?**
  IBM Security Guardium S-TAP for IMS on z/OS (also referred to as IBM Guardium S-TAP for IMS) is an auditing tool that collects and correlates data access information from IMS Online regions, IMS batch jobs, IMS archived log data sets, and SMF records to produce a comprehensive view of business activity that occurs within one or more IMS environments.
- **Installing IBM Security Guardium S-TAP for IMS on z/OS**
  The following sections describe hardware, software, and user ID authority prerequisites for product installation.
- **IBM Security Guardium S-TAP for IMS on z/OS security**
  IBM Guardium S-TAP for IMS requires access to various IMS data sets and IBM Guardium system components.
- **Configuration overview**
  These actions are required to configure IBM Guardium S-TAP for IMS.
- **Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent**
  This section describes the information necessary for configuring the agent.
- **Setting up an IMS environment for auditing**
  This section describes how to customize IMS environments to capture DLI calls, including customizing IMS catalogued procedures, coexisting with other DFSFLGX0 and DFSISVI0 exit routines, customizing IMS to use a zIIP, copying common load modules from SAUILOAD to SAUIIMOD, and the security considerations related to IMS processing.
- **Using agent configuration keywords to customize auditing**
  Some agent configuration keywords must be used for the product to function. You can also use agent configuration keywords for optional auditing specifications.
- **IBM Security Guardium S-TAP for IMS on z/OS agent reference information**
  The IBM Guardium S-TAP for IMS agent provides access to database and appliance services, in support of the product's remote clients. The agent also reads audited DLI events placed in the z/OS System Logger log streams by the IMS Online and DLI/DBB batch Data collectors and sends the DLI events to the IBM Guardium system using TCP/IP connections.
- **Data collection**
  The collection process involves the gathering of audit event data at run time. Specify various filtering criteria to capture all relevant events and limit the amount of data that is collected and stored.
- **Creating and modifying IMS definitions**
  An IMS definition establishes a connection from your Guardium system to the IMS environment that you want to audit. To create and modify IMS definitions from the Guardium system interface, the agent address space (AUIA*STC*) must have a preestablished connection to the Guardium system.
- **Reference information**
  This chapter provides IBM Guardium S-TAP for IMS reference information.
- **Troubleshooting**
  Use the following topics to diagnose and correct problems that you experience with IBM Guardium S-TAP for IMS.

Parent topic: S-TAP for z/OS V10.1.3 User's Guide
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Security Guardium S-TAP for IMS on z/OS (also referred to as IBM Guardium S-TAP for IMS) is an auditing tool that collects and correlates data access information from IMS Online regions, IMS batch jobs, IMS archived log data sets, and SMF records to produce a comprehensive view of business activity that occurs within one or more IMS environments.

IBM Guardium S-TAP for IMS assists auditors in determining who read or updated a particular IMS database and its associated data sets, what mechanism was used to perform that action, and when the access took place.

IBM Guardium S-TAP for IMS can collect and correlate many different types of information, including:

- Accesses to databases and segments from IMS Online regions.
- Accesses to databases and segments from IMS DLI/DBB batch jobs.
- Accesses to databases, image copies, IMS logs, and RECON data sets and security violations to these data sets as recorded by SMF.
- IMS Online region START and STOP, database, and PSB change of state activity and user signon and signoff as recorded in the IMS Archived Log data sets.

Restriction: IBM Guardium S-TAP for IMS supports auditing of Data Entry Databases (DEDBs) and IMS Full Function databases. Auditing of Main Storage Databases (MSDBs) is not supported.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

What's new in IBM Security Guardium S-TAP for IMS on z/OS V10.1.3?

Here's what's new in version 10.1.3 of IBM Guardium S-TAP for IMS.

Enhancements to this version include:

- Echoing of active policy XML as described in Echoed XML statement definitions.
- Increased security of online and batch log streams as described in z/OS log streams.
- Filtering of DLI called based on IMS LTERM names
- Collection of the accessed HALDB PARTITION name during DLI call processing
- Check agent status without accessing z/OS by using a Guardium interface command
- Ability to enable simulation mode to simulate mainframe activity levels, test deployment, and gauge appliance requirements without sending data to the Guardium appliance
- New parameters to simplify audit record validation, debugging, and agent configuration
- Simplified agent configuration:
  - Complete SMF configuration is no longer required if the SMF_CYCLE_INTERVAL(0) parameter is specified in the AUICONFG file and SMF processing is disabled.
  - Complete IMSL configuration is no longer required if the IMSL_CYCLE_INTERVAL(0) parameter is specified in the AUICONFG file and IMSL processing is disabled.
- Messages AUII050I and AUIJ250I now include the IMSID to help identify which IMS system issued the message.
- Reduced CPU consumption and greater reliability during processing of IMS DLI calls in IMS online environments.
- RECON data sets that are read by the SMF (AUIF*STC* and IMS SLDS (AUIL*STC*) can optionally be copies of the live IMS RECON data sets.
- Option to disable DLI call auditing of IMS online DLI calls that originate from the following IMS region types: AER, BMP, CICS®, DBCTL, IFP, MPP, and ODBA.
- Support for Internet Protocol version 6 (IPV6) introduced with PH16991

Parent topic: What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Guardium S-TAP for IMS components

IBM Guardium S-TAP for IMS consists of an agent, a Common Storage Management Utility, and the IBM Guardium system.

Parent topic: What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Guardium system

The IBM Guardium system can gather and report information from multiple agents running on multiple z/OS systems.

Note: In environments where multiple agents connect to a common IBM Guardium system or appliance, the z/OS agent started task names (AUIAS*TC*, AUILS*TC*, AUIFS*TC*) must be unique. Unique started task names enable the IBM Guardium S-TAP for IMS policies that are pushed from the IBM Guardium system to be attributed to, and monitored by, the correct z/OS agent.

IBM Guardium system components

The IBM Guardium system:

- Provides the user interface, which processes requests and displays the resulting information.
- Enables you to create collection policies, which specify the types of data to be collected by the agent.
- Stores the collected data.

IBM Guardium system and S-TAP agent communication

The IBM Guardium system and the IBM Guardium S-TAP for IMS agent communicate using a TCP/IP connection. The policies you create, using the user interface, tell the agent what data to collect. The policy specifies filter information, such as which data sets are to be monitored for data accesses.

Parent topic: IBM Guardium S-TAP for IMS components

IBM Guardium S-TAP for IMS agent

The IBM Guardium S-TAP for IMS agent coordinates the collection of audited data, and the transmission of audited DLI call data to the IBM Guardium system.

The IBM Guardium S-TAP for IMS agent can collect data from one or more of the following sources within a SYSPLEX:

- A single IMS system
- Multiple IMS systems that share a common set of RECON data sets
- Multiple IMS systems using diverse RECON data sets

The agent maintains the communication links that are needed to exchange information with:

- The IBM Guardium system
- IMS Online and Batch data collectors and activity monitors
- The IMS Archive Log data set and SMF activity monitors

The agent also provides data collection schemas, called policies, to the activity monitors on which detail the IMS artifacts are to be audited, and to what level.

The agent runs as a started task on the z/OS host. An example of the JCL to be used is in member AUIASTC of the SAUISAMP installation data set.

The agent collects data from the following sources:

- IMS online activities
- IMS batch activities
- SMF data
- IMS archived log data
- IMS RECON data sets

For more information about how data is collected from these sources, see Data collection monitors.
Parent topic: IBM Guardium S-TAP for IMS components

Installing IBM Security Guardium S-TAP for IMS on z/OS

The following sections describe hardware, software, and user ID authority prerequisites for product installation.

Review the IBM Guardium S-TAP for IMS V10.1.3 Program Directory for a list of product materials and SMP/E installation instructions.

- **Hardware and software prerequisites**
  The following hardware and software are required to operate IBM Guardium S-TAP for IMS V10.1.3.
- **User ID authorities that are required for installation**
  The following z/OS USERID authorities are needed to install IBM Guardium S-TAP for IMS.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Hardware and software prerequisites

The following hardware and software are required to operate IBM Guardium S-TAP for IMS V10.1.3.

- z/OS Version 2 Release 2 or later, until end of service.
- IMS V13 -- V15, until end of service.
- Any hardware capable of running z/OS Version 2 Release 1 or later, until end of service.

IBM Guardium S-TAP for IMS requires use of the following:

- 64-bit memory
- TCP/IP connectivity
- z/OS System logger log streams
- UNIX System Services
- OMVS segment

Parent topic: Installing IBM Security Guardium S-TAP for IMS on z/OS

User ID authorities that are required for installation

The following z/OS USERID authorities are needed to install IBM Guardium S-TAP for IMS.

If you are installing this product, your z/OS user ID must have the authority to:

- Define z/OS system log streams
- Update the IMS cataloged procedure data set members DLIBATCH and DBBBATCH to include product load libraries

Parent topic: Installing IBM Security Guardium S-TAP for IMS on z/OS

IBM Security Guardium S-TAP for IMS on z/OS security

IBM Guardium S-TAP for IMS requires access to various IMS data sets and IBM Guardium system components.

- **APF authorization**
  IBM Guardium S-TAP for IMS requires certain data sets to be accessible and APF-authorized on all LPARS of the SYSPLEX where IMS batch jobs or monitored IMS online regions might run.
- **OMVS segment**
  TCP/IP connectivity and other UNIX System services on z/OS require that the address space that is using these services use a z/OS user ID or group name that is defined with an OMVS segment.
- **TCP/IP connections**
  IBM Guardium S-TAP for IMS uses Transmission Control Protocol/Internet Protocol (TCP/IP) to connect to the Guardium appliance. To enable this communication, make sure you have the correct permissions assigned.
- **z/OS log streams**
  IBM Guardium S-TAP for IMS monitors the IMS batch jobs and online regions and writes audit data to z/OS log streams.
- **IMS RESLIB data sets**
  READ access to the IMS RESLIB/SDFSRESL data sets is required for each IMS system that requires the IMS SLDS to be processed by IBM Guardium S-TAP for IMS. READ access is required to allow a LOAD/READ of module DFSVC000 to determine the version release level of the audited IMS.
- **SMF and IMS archive log data sets**
  READ access to the SMF data sets and the IMS archived logs data sets (SLDS) is required for the user under whose authority the agent runs. If these data sets are protected by RACF® or another security product, a policy must be defined to grant this access. The z/OS catalogs containing the names of these data sets, as well as the physical data sets themselves, must be accessible from the LPAR on which the IBM Guardium S-TAP for IMS agent runs.
- **DBRC RECON data sets**
  IBM Guardium S-TAP for IMS uses the native VSAM services to read data from the RECON data sets. These RECON data sets must be accessible from all the LPARS where the IBM Guardium S-TAP for IMS agents might run.
- **Operator commands**
  You can use z/OS Operator commands, to start IBM Guardium S-TAP for IMS tasks.
- **Quarantining Database DLI calls**
  IBM Guardium S-TAP for IMS enables you to quarantine the DB DLI calls of specific users for specific periods of time.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

APF authorization

IBM Guardium S-TAP for IMS requires certain data sets to be accessible and APF-authorized on all LPARS of the SYSPLEX where IMS batch jobs or monitored IMS online regions might run.

About this task

Refer to the *z/OS Knowledge Center* for more information about how to APF authorize libraries.

Procedure

1. APF-authorize product data set SAUILOAD on all LPARS of the SYSPLEX.
   SAUILOAD contains the IMS Online and Batch Activity Monitor executable code.
2. APF-authorize product data set SAUIIMOD on all LPARS of the SYSPLEX where IMS batch jobs or IMS online regions to be monitored might run.
   SAUIIMOD contains IMS specific executable load modules.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

OMVS segment

TCP/IP connectivity and other UNIX System services on z/OS require that the address space that is using these services use a z/OS user ID or group name that is defined with an OMVS segment.

Defining your z/OS user ID or group name with an OMVS segment might require the use of the IBM RACF command ADDUSER/ALTUSER xxxxxx OMVS(UID(zzz)) or a security product equivalent command. Review your z/OS Security Server documentation for more information.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

TCP/IP connections

IBM Guardium S-TAP for IMS uses Transmission Control Protocol/Internet Protocol (TCP/IP) to connect to the Guardium appliance. To enable this communication, make sure you have the correct permissions assigned.

If you are working from a secure communications port, enable the user ID that is associated with the agent started task to have READ/WRITE permissions on the ports that are assigned to the agent.

See Using agent configuration keywords to customize auditing for more information about the ADS_LISTENER_PORT, APPLIANCE_PORT, and LOG_PRT_SCAN_START configuration keywords.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

z/OS log streams

IBM Guardium S-TAP for IMS monitors the IMS batch jobs and online regions and writes audit data to z/OS log streams.

The IBM Guardium S-TAP for IMS Online and DLI/DBB batch data collectors audit DLI events that occur in the IMS Online and DLI/DBB Batch regions. Audited DLI events are written to z/OS System Logger log streams, which are then read by the IBM Guardium S-TAP for IMS agent. The IMS agent sends the audit data to the IBM Guardium appliance by using TCP/IP connections.

To permit the IMS Online and DLI/DBB batch collectors to write to the log streams, systems authorization facility (SAF) security access of UPDATE to the z/OS log stream is required for all user IDs associated with the audited IMS Control region and DLI/DBB batch jobs that might cause IMS DLI calls to be audited.

You can now use an additional SAF resource to further secure the online and batch log streams. For example, you can now prevent the log streams from being read by a user program or utility that is initiated by a user who is authorized to update to the log stream. Apply z/OS V2R3 and V2R4 APAR OA56050 to optionally add an additional authority check for a SAF profile that covers resource (WRITE_ONLY_log-stream-name) in class LOGSTRM. This new profile option enables you to limit users to only connecting to (IXGCONN REQUEST=CONNECT), writing to (IXGWRITE), and disconnecting from (IXGCONN REQUEST=DISCONNECT) the log stream. Other IXG calls, such as IXGBRWSE (read), are rejected with return code 8 and reason code '081C'x. For more information, refer to the documentation provided in the HOLD data for APAR OA56050.

Note: User IDs that are associated with the IBM Guardium S-TAP for IMS agent must have authority to read and delete data from the log stream and should not be limited by using resource (WRITE_ONLY_log-stream-name). Log stream UPDATE authority is recommended for the IBM Guardium S-TAP for IMS agents.
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

IMS RESLIB data sets

READ access to the IMS RESLIB/SDFSRESL data sets is required for each IMS system that requires the IMS SLDS to be processed by IBM Guardium S-TAP for IMS. READ access is required to allow a LOAD/READ of module DFSVC000 to determine the version release level of the audited IMS.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

SMF and IMS archive log data sets

READ access to the SMF data sets and the IMS archived logs data sets (SLDS) is required for the user under whose authority the agent runs. If these data sets are protected by RACF® or another security product, a policy must be defined to grant this access. The z/OS catalogs containing the names of these data sets, as well as the physical data sets themselves, must be accessible from the LPAR on which the IBM Guardium S-TAP for IMS agent runs.

Consult your security administrator to determine what is currently protected and how to grant the required access.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

DBRC RECON data sets

IBM Guardium S-TAP for IMS uses the native VSAM services to read data from the RECON data sets. These RECON data sets must be accessible from all the LPARS where the IBM Guardium S-TAP for IMS agents might run.

VSAM access to the RECON data sets is READ-ONLY, allowing the IBM Guardium S-TAP for IMS jobs and started tasks with a security access of READ to process the RECON data sets.

Consult your security administrator to determine how your RECON data sets are protected, and how to grant the required access.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

Operator commands

You can use z/OS Operator commands, to start IBM Guardium S-TAP for IMS tasks.

The user ID that is assigned to the IBM Guardium S-TAP for IMS agent started task must be permitted to issue START commands to initiate the AUIF*stc*, AUIL*stc*, and AUIU*stc* tasks. During installation, administrators can configure the z/OS security product to restrict users and programs from issuing z/OS Operator commands.
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

Quarantining Database DLI calls

IBM Guardium S-TAP for IMS enables you to quarantine the DB DLI calls of specific users for specific periods of time.

Quarantining a user of a specific IMS subsystem means that for the specified time period, the quarantined user is not able to run DB DLI calls either by using the targeted IMS subsystem, or while running DLI/DBB batch jobs.

If a quarantined user attempts access during a restricted time, the DLI call is not performed, and a status code of `AI` is returned in the DBPCB status code field.

To create quarantine rules, access the Policy Builder from the Tools and Views section of the Guardium appliance interface Setup menu.

Note:

- DLI calls that are made to IMS Fast Path databases by using IMS Fast Path exclusive transactions or BMPs cannot be quarantined.
- Quarantine does not take effect immediately. The audited DLI call that produces the event to trigger the quarantine is completed before the quarantine takes effect. It is possible for DLI calls to be run by the quarantined user before the quarantine takes effect.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

Configuration overview

These actions are required to configure IBM Guardium S-TAP for IMS.

Review the following steps, which are described in greater detail in the following sections:

- Verify that you have the resource authorizations that are required to configure the product.

- Review the steps to plan your configuration and customize your environment.
- Set up the z/OS log streams. Review the CFRM and log stream size requirements, and the related security considerations, limitations, and restrictions. Define the log streams for batch and online jobs.
- Determine a naming convention for the agent (AUIA*STC*, AUIF*STC*, AUIL*STC*, and AUIU*STC*) started tasks, where *STC* can be changed to any 1 - 4 character length string.
  Tip: Retain the AUI prefix to simplify task identification.
- Configure the agent by customizing the configuration file, customizing the agent JCL, and starting the agent.
- Set up the IMS environment for auditing by customizing the IMS cataloged procedure, configuring IMS exits, customizing IMS to use an IBM System z® Integrated Information Processor (zIIP), and review the related security considerations.

Note: No WLM (Workload Manager) considerations are necessary. All agent started tasks use the STC WLM class.

- **Upgrading from Guardium S-TAP for IMS V9.0**
  Complete the following steps to upgrade from InfoSphere® Guardium S-TAP for IMS V9.0 to IBM Guardium S-TAP for IMS V10.1.3. These steps enable V9.0 product assets, such as JCLs and configuration and repository contents, to be upgraded to V10.1.3, while allowing the full use and functionality of the V10.1.3 product.
- **Upgrading from Guardium S-TAP for IMS V9.1 or V10.0**
  The agent JCL and configuration file that are used by IBM Guardium S-TAP for IMS V9.1 and V10.0 are compatible with IBM Guardium S-TAP for IMS V10.1.3. No configuration changes are required to upgrade from IBM Guardium S-TAP for IMS V9.1 to IBM Guardium S-TAP for IMS V10.1.3.
- **Planning your configuration and customizing your environment**
  Collect user ID and environment information before you configure IBM Guardium S-TAP for IMS V10.1.3.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Upgrading from Guardium S-TAP for IMS V9.0

Complete the following steps to upgrade from InfoSphere® Guardium S-TAP for IMS V9.0 to IBM Guardium S-TAP for IMS V10.1.3. These steps enable V9.0 product assets, such as JCLs and configuration and repository contents, to be upgraded to V10.1.3, while allowing the full use and functionality of the V10.1.3 product.

Before you begin

New versions or releases of IBM Guardium S-TAP for IMS should be installed as a new installation base. However, if circumstances prevent you from doing so, follow these instructions to upgrade from the previous version's installation base.

Procedure

1. Deactivate or uninstall all policies that apply to the agent that you are upgrading.
2. Shut down the agent that you are upgrading.
3. Customize the AUIMIG10 SAMPLIB member to convert the configuration file and repository to V10.1.3 format, and submit.
   The comments that are contained in the AUIMIG10 SAMPLIB member describe how to customize the JCL. A V10.1.3 format configuration file, and an IMS definition report will be produced.
4. Use the IMS definition report, which is produced by the AUIMIG10 utility, to add the IMS definitions to your IBM Guardium system.
5. Update the new configuration file, which is produced by the AUIMIG10 utility, with any changes.
6. Update the AGENT (AUIA*STC*) and Memory Management Utility (AUIU*STC*) JCLs as follows:
   a. Remove the //AUICFG DD JCL statement.
   b. Add a //AUICONFG DD JCL statement, and set it to reference the new configuration member produced by the AUIMIG10 utility.
   c. Change the //STEPLIB DD JCL statement to reference the V10.1.3 product load library (SAUILOAD).
   d. Remove the //AUIREPOS DD JCL statement from the AUIU*STC* JCL.
7. Update the SMF (AUIF*STC*) and IMS Archive Log (AUIL*STC*) JCLs as follows:
   a. Remove the //AUICFG DD JCL statement, and any procedure parameters that reference it.
   b. Change the //STEPLIB DD JCL statement to reference the V10.1.3 product load library (SAUILOAD).
8. Update the IMS Control region JCLs that are audited by the agent to use the V10.1.3 product IMS load library (SAUIIMOD).
9. Update the IMS DBBBATCH and DLIBATCH cataloged procedures, and any equivalent JCL members, to use the V10.1.3 product IMS load library (SAUIIMOD).
10. Start the agent.
11. Install or activate the policies that you want to apply.
12. Stop and restart your IMS systems.

What to do next

Now, you can:

- Install additional policies on the z/OS host by using the IBM Guardium system user interface.
- Manage agent and IMS definitions by using the IBM Guardium system user interface.

Note: The format of the data that is written to the z/OS logstreams has changed from V9.0 to V10.1.3. IBM Guardium S-TAP for IMS V10.1.3 converts any existing V9.0 data from existing logstreams to a usable format. If you migrate from a V10.1.3 system back to a V9.0 system, you must reinitialize the z/OS log streams before restarting InfoSphere Guardium S-TAP for IMS V9.0.

Parent topic: Configuration overview

Upgrading from Guardium S-TAP for IMS V9.1 or V10.0

The agent JCL and configuration file that are used by IBM Guardium S-TAP for IMS V9.1 and V10.0 are compatible with IBM Guardium S-TAP for IMS V10.1.3. No configuration changes are required to upgrade from IBM Guardium S-TAP for IMS V9.1 to IBM Guardium S-TAP for IMS V10.1.3.

Before you begin

Do not attempt to run AUIMIG10 to upgrade from Guardium S-TAP for IMS V9.1 or V10.0 to IBM Guardium S-TAP for IMS V10.1.3.

About this task

The format of the data that is written to the z/OS logstreams has changed in V10.1.3. IBM Guardium S-TAP for IMS V10.1.3 converts any existing Guardium S-TAP for IMS V9.1 and V10.0 data from existing logstreams to a usable format. If you migrate from a V10.1.3 system back to a V9.1 or V10.0 system, you must reinitialize the z/OS log streams before restarting the previous product version.
Parent topic: Configuration overview

Planning your configuration and customizing your environment

Collect user ID and environment information before you configure IBM Guardium S-TAP for IMS V10.1.3.

Tip: To upgrade to IBM Guardium S-TAP for IMS from a previous version, refer to the appropriate topic:

- Upgrading from Guardium S-TAP for IMS V9.0
- Upgrading from Guardium S-TAP for IMS V9.1 or V10.0

If you are upgrading from a previous version to V10.1.3, no further configuration steps are required. Upgrading to V10.1.3 requires the use of, and modifications to, the same agent name and JCLs that were used with previous versions. For your reference, see the Sample library members table.
Before you configure a new installation of IBM Guardium S-TAP for IMS V10.1.3, determine the following:

- The user IDs that will be used to run the agent started tasks
- Where the agent started tasks will run

Then, customize the ISPF edit macro, review the job card requirement, and set up the z/OS log streams, as described in the following sections.

- **Customizing the ISPF edit macro**
  The SAUISAMP data set shipped with IBM Guardium S-TAP for IMS includes an ISPF edit macro to help with the editing of the rest of the SAMPLIB members to be used in the subsequent steps.
- **Job cards for the sample JCL in the SAMPLIB**
  Some JCL members included with the product SAMPLIB have a filler card for the job card.
- **Setting up z/OS log streams**
  IBM Guardium S-TAP for IMS uses the z/OS System Logger to funnel events from IMS online regions and DLI/DBB batch jobs to the DLI event processor (AUIA*STC* task). Both XCF based and DASD based log streams are supported.

Parent topic: Configuration overview

Customizing the ISPF edit macro

The SAUISAMP data set shipped with IBM Guardium S-TAP for IMS includes an ISPF edit macro to help with the editing of the rest of the SAMPLIB members to be used in the subsequent steps.

About this task

The edit macro is named AUIEMAC1 and provides a straightforward way to customize the variable values for the variables that appear in the JCL that will run. Use this edit macro as part of a command list (CLIST) to edit the other SAMPLIB members.

Procedure

1. To set up the edit macro, copy AUIEMAC1 from the #HLQ.SAUISAMP to a CLIST library.
2. Edit the macro by providing the appropriate values for each of the variables.
3. To run the macro, type the name of the edit macro in the command line in ISPF.

Results

After you modify the edit macro, you can use it as a command to customize other SAMPLIB members in the following steps, unless otherwise specified.

Example

The contents of the edit macro AUIEMAC1 included in the SAMPLIB are as follows:

```
ISREDIT MACRO (NP)
ISPEXEC VGET (ZUSER)
ISREDIT CHANGE ALL '#AUILOAD'           AUI.IBMTAPE.SAUILOAD
ISREDIT CHANGE ALL '#AUIIMOD'           AUI.IBMTAPE.SAUIIMOD
ISREDIT CHANGE ALL '#AUISAMP'           AUI.IBMTAPE.SAUISAMP
ISREDIT CHANGE ALL '#AUICONFG'          AUICONFG
```

This table describes each variable in the edit macro AUIEMAC1 included in the SAMPLIB:

Table 1. AUIEMAC1 Edit macro variables

Variable	Default	Instructions
#AUILOAD	AUI.IBMTAPE.SAUILOAD	Change the default value to point to the location of the SAUILOAD for IBM Guardium S-TAP for IMS.
#AUIIMOD	AUI.IBMTAPE.SAUIIMOD	Change the default value to point to the location of the SAUIIMOD for IBM Guardium S-TAP for IMS.
#AUISAMP	AUI.IBMTAPE.SAUISAMP	Change the default value to point to the location of the SAUISAMP data set, or copy of that data set where you will be performing the configuration and customization edits.
#AUICONFG	AUICONFG	Change the default value to point to the member name in the configuration file that you want to use.

Parent topic: Planning your configuration and customizing your environment

Job cards for the sample JCL in the SAMPLIB

Some JCL members included with the product SAMPLIB have a filler card for the job card.

A valid job card conforming to your site's JCL standards must be provided before submitting any of the JCL.
Parent topic: Planning your configuration and customizing your environment

Setting up z/OS log streams

IBM Guardium S-TAP for IMS uses the z/OS System Logger to funnel events from IMS online regions and DLI/DBB batch jobs to the DLI event processor (AUIA*STC* task). Both XCF based and DASD based log streams are supported.

Each agent requires two unique log streams:

- one log stream for DLI events generated by IMS Control regions
- one log stream for DLI events generated by DLI/DBB batch jobs

Log streams cannot be shared between agents. Each log stream name must be unique.

It is recommended that XCF based log streams be used whenever possible, because this type of log stream is accessible from any LPAR within a sysplex, and has performance benefits. For more information about log streams, refer to the IBM publication: *System Programmer's Guide to: z/OS System Logger*.

- **Log stream security**
  Verify the following conditions have been met to insure log stream security.
- **XCF-based log streams**
  The advantages of using XCF-based log streams, as opposed to DASD-based log streams, include accessibility from any LPAR within the sysplex, and improved performance.
- **DASD-based log streams**
  This section provides rules and information about DASD-based log streams. Using DASD-based log streams limits auditing by the agent to the LPAR within which the agent is started. IMS Control regions and IMS DLI/DBB batch jobs that run on other LPARS will not be audited.

Parent topic: Planning your configuration and customizing your environment

Log stream security

Verify the following conditions have been met to insure log stream security.

Important:

- The USERID your IMS online control region runs under must have WRITE access to the log stream.
- If DLI/DBB batch jobs runs under a common USERID, that USERID must have WRITE permission to the log stream.
- The USERID under which the DLI Event Collector (AUIA*STC* task) executes must have READ/WRITE access to the log streams.
- If individual users are permitted to run DLI/DBB batch jobs under their own USERID, a universal access of WRITE is recommended for the log stream.

Parent topic: Setting up z/OS log streams

XCF-based log streams

The advantages of using XCF-based log streams, as opposed to DASD-based log streams, include accessibility from any LPAR within the sysplex, and improved performance.

AUILSTR1

Two JCL members in the SAUISAMP product data set are included to assist in the definition of XCF-based log streams.

This JCL is used to define the XCF structures to a CFRM policy needed by the log streams used by the DLI/DBB batch and IMS online control regions. Detailed instructions are in the comments of the JCL.
Note: The addition of structures to a CFRM policy are cumulative, and the execution of this JCL without consideration to previously defined structures within the CFRM policy result in the loss of existing CFRM structure definitions. It is highly recommended that a systems programmer customize and submit this JCL.

There are two DEFINE STRUCTURE sections for this JCL: one for the batch structure, and one for the online structure. The following values must be customized for the batch structure:

The name of the batch structure
    (NAME(batch_struc_name))
The coupling facility used to contain the structure
    (PREFLIST(cfname))

The following values must be customized for the online structure:

The name of the online structure
    (NAME(online_struc_name))
The coupling facility used to contain the structure
    (PREFLIST(cfname))

Do not change any other values, such as SIZE, INITSIZE, and ALLOWAUTOALT without carefully considering the impact that your changes will have on performance and data integrity.

Note:

- AUILSTR1 must run successfully before proceeding.
- When auditing in a large test or production environment, the INITSIZE and SIZE parameters can be increased to a higher value (example: 49200) for improved throughput.

AUILSTR2

This JCL is used to add the XCF based log streams to a LOGR policy used by the IMS Control region and DLI/DBB batch jobs. Detailed instructions are in the comments of the JCL.
Note: The addition of structures to a CFRM policy are cumulative, and the execution of this JCL without consideration to previously defined structures within the CFRM policy result in the loss of existing CFRM structure definitions. It is highly recommended that a systems programmer customize and submit this JCL.

There are two DEFINE STRUCTURE sections for this JCL: one for the batch structure and log stream, and one for the online structure.

Values that must be customized for IMS Batch processing include:
DEFINE STRUCTURE values:

The name of the batch structure (from AUILSTR1)
(NAME(batch_struc_name))

The name of this log stream is used as input to the Batch DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIB keyword of the configuration member that is specified by the AUICONFG DD statement of the agent (AUIA*STC*) JCL. The LOGSNUM, MAXBUFSIZE and AVGBUFSIZE should not be changed from the default values.

The name of the batch structure (from AUILSTR1)
(STRUCTNAME(batch_struc_name))
The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters.

The size of the Batch Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The allocation/size of the offload data sets
(LS_SIZE(13500))

The default value is 13500 (the number of 4K blocks). The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size. When auditing in a large test or production environment, a value of 40500 might improve throughput.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

You must customize the following values for online structure and log stream processing:

DEFINE STRUCTURE values:

The name of the online structure (from AUILSTR1)
(NAME(online_struc_name))

The LOGSNUM, MAXBUFSIZE and AVGBUFSIZE should not be changed from the default values.
DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(online_logstream_name))

The name of this log stream is used as input to the Online DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIO keyword of the configuration member specified by AUICONFG DD statement of the agent (AUIA*STC*) JCL.

The name of the online structure (from AUILSTR1)
(STRUCTNAME(online_struc_name))
The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

The size of the ONLINE Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

The allocation/size of the offload data sets
(LS_SIZE(13500))

The default value is 13500 (the number of 4K blocks). The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size. When auditing in a large test or production environment, a value of 40500 might improve throughput.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.
Parent topic: Setting up z/OS log streams

DASD-based log streams

This section provides rules and information about DASD-based log streams. Using DASD-based log streams limits auditing by the agent to the LPAR within which the agent is started. IMS Control regions and IMS DLI/DBB batch jobs that run on other LPARS will not be audited.

DASD-based logs streams can only be accessed from one LPAR at a time. Any IMS Online Control regions and DLI/DBB batch jobs to be audited must run on the same LPAR as the agent runs on.

One JCL member in the SAUISAMP product data is included to assist in the definition of DASD-based log streams.

AUILSTR3

This JCL is used to add the DASD based log streams to a LOGR policy used by the IMS Control region and DLI/DBB batch jobs. Detailed instructions can be found within the comments of the JCL.
Note: It is highly recommended that a systems programmer customize and submit this JCL.
There are two DEFINE STRUCTURES sections to this JCL: one for the batch structure, and one for the online structure. Values which must be customized for IMS batch log stream processing are as follows:
DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(batch_logstream_name))

The name of this log stream is used as input to the Batch DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIO keyword of the configuration member specified by AUICONFG DD statement of the agent (AUIA*STC*) JCL.

The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The size of the Batch Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The allocation/size of the offload data sets
(LS_SIZE(13500))

A value of 13500 (the number of 4K blocks) is the default/supplied value. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size, and can be found on the IBM Information Center.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter, and can be found on the IBM Information Center.

Values which must be customized for IMS ONLINE processing include the following:

DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(online_logstream_name))

The name of this log stream is used as input to the Online DLI Log Stream Name field when defining log streams to the agent using the Guardium user interface.

The selection of the Staging data set classes

(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The size of the ONLINE Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The allocation/size of the offload data sets
(LS_SIZE(13500))

A value of 13500 (the number of 4K blocks) is the default/supplied value. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size, and can be found on the IBM Information Center.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter, and can be found on the IBM Knowledge Center
Parent topic: Setting up z/OS log streams

Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

This section describes the information necessary for configuring the agent.

The agent has a primary agent address space that runs as a started task (AUIA*STC*) and multiple secondary address spaces (AUIF*STC*, the SMF collector, AUIL*STC*, the IMS log collector, AUIU*STC*, the common storage utility) that are automatically started and stopped by the primary address space.

The agent primary address space reads the configuration file specified by the AUICONFG DD statement in the AUIA*STC* JCL, and passes the appropriate configuration information to the associated AUIF*STC* and AUIL*STC* tasks. The AUIU*STC* JCL requires the same configuration file to be specified as was specified for the AUIA*STC* task. Use the AUICONFG DD statement to specify the configuration file.

The SAUISAMP member AUICONFG provides a sample configuration that can be used by the agent primary address space started task.

Refer to the following instructions about the AUICONFG data set or the instructions in the data sets to complete the next steps.

Note:

- The data set must be edited using the EBCDIC encoding (1047 CCSID).
- It is recommended that you make a copy of the AUICONFG from SAUISAMP and customize it for use by a given agent.

- **Customizing the agent by using agent parameter keywords**
  Use agent parameter keywords to customize the agent. The agent configuration file provides the parameters that can be customized. The parameters that do not have a default value must be specified before you start the agent started task.
- **Agent configuration**
  The IP addresses of the IBM Guardium system appliances are specified using the SAUISAMP data set AUICONFG member using the APPLIANCE_SERVER and APPLIANCE_SERVER_FAILOVER_[1-5] keywords.
- **Customizing the agent JCL**
  The SAUISAMP member AUIA*STC* provides a sample JCL that can be used for the agent started task. This topic describes how to customize the JCL.
- **Starting and stopping the agent**
  Start the agent by issuing the command /S AUIASTC from the SDSF command line. The primary agent address space starts the AUIF*STC* address spaces. One or more instances of AUIL*STC* might also be started, depending on the list of active collections.
- **Agent security considerations**
  The user ID of the agent started tasks (the primary and the secondary started tasks) should have the necessary RACF® profiles for reading the configuration member contents.
- **Modifying the frequency of AUIJ012I messages**
  You can modify how frequently the agent provides a count of DLI calls (from the default of every 10K DLI calls to a value of your choice, 10K – 999K, 1M – 10M.)

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Customizing the agent by using agent parameter keywords

Use agent parameter keywords to customize the agent. The agent configuration file provides the parameters that can be customized. The parameters that do not have a default value must be specified before you start the agent started task.

How to use the agent parameters

- Use the AUICONFG DD statement to reference these parameters with the agent JCL (AUIA*STC*) and Memory Management secondary address space JCL (AUIU*STC*).
- The AUICONFG DD can be used in other agent secondary address space JCLs (AUIF*STC* and AUIL*STC*).
- Define the data set (DSORG=PS) or data set member (DSORG=PDS|PDS/E) that contains these parameters as RECFM=FB LREL=80.

- Specify only one keyword and parameter per line.
- An asterisk (*) or hyphen (-) in column one indicates that the line is a comment.
- Characters in column 72 and beyond are ignored.

Required parameters

The following parameters must be manually configured:

- APPLIANCE_SERVER
- LOG_STREAM_DLIB
- LOG_STREAM_DLIO
- SMF_DSN_MASK
- SMF_SPILL_FILE

All available agent parameters

ADS_SHM_ID

Required: No
Default: None
Description: This keyword is optional when only one agent exists in a sysplex environment. If more than one agent exists, the configuration file for each agent should have this keyword specified with a unique integer with a value of 100000 - 999999 specified as its parameter. This keyword identifies a shared memory segment that is specific to each agent.
Note:

- This keyword must be used in combination with ADS_LISTENER_PORT.
- If you specify this keyword, you must add an //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the agent AUIA*STC* and AUIU*STC* JCLs to enable communication between all participating address spaces.

Syntax: ADS_SHM_ID*(Shared_Memory_label)*
Example: ADS_SHM_ID(100010)

ADS_LISTENER_PORT

Required: No
Default: 39987
Description: This keyword is optional when only one agent exists in a sysplex environment. If more than one agent exists, the configuration file for each agent should have this keyword specified with a unique port number specified. This keyword identifies an agent-specific communications port between the agent (AUIA*STC*) and the agent secondary address spaces (AUIF*STC*, AUIL*STC*). Valid port numbers are 1 - 65535. Check with your network administrator for a list of ports available for this use.
Note:

- This keyword must be used in combination with ADS_SHM_ID.
- If you specify this keyword, you must add an //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the agent AUIA*STC* and AUIU*STC* JCLs to enable communication between all participating address spaces.

Syntax: ADS_LISTENER_PORT*(port_number)*
Example: ADS_LISTENER_PORT(16055)

APPLIANCE_SERVER

Required: Yes
Default: None
Description: The host name or IP address (in dotted decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the agent (AUIA*STC*) should connect.
Note: This parameter must be correctly configured to enable a connection to the IBM Guardium system. This value can contain up to 128 characters.
Syntax: APPLIANCE_SERVER*(hostname|IP_address)*
Example:

```
APPLIANCE_SERVER(wal-vm-guardium20)
APPLIANCE_SERVER(192.168.2.205)
```

APPLIANCE_SERVER_[1-5]

Required: No
Default: None
Description: Enables alternative host names or TCP/IP addresses to be used for multistream Guardium appliance destinations or failover recovery processing. Up to five alternative host names or TCP/IP addresses are supported.
To specify one or more entries, include this parameter with a numeric suffix from 1 - 5. Provide a unique host name or TCP/IP address for each entry.
Valid values are any valid host name or TCP/IP address.
Note:

- The use of this keyword does not eliminate the need for the APPLIANCE_SERVER keyword.
- The APPLIANCE_SERVER_LIST parameter designates how this parameter is used.
- If used in combination, this parameter overrides the APPLIANCE _SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_[1-5] parameter.

Syntax:

```
APPLIANCE_SERVER_n(hostname|IP_addr)
```

where *n* can be 1, 2, 3, 4, or 5.
Example:

```
APPLIANCE_SERVER_1(nwt-vm-guardium3)
APPLIANCE_SERVER_1(192.168.2.205)
```

APPLIANCE_SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_[1-5]

Required: No

Default: None
Description: The host name or IP address (in dotted decimal notation, for example: 1.2.3.4) of the IBM Guardium system for the IBM Guardium S-TAP for IMS agent to use to stream to multiple Guardium appliance destinations or for failover processing. This value can contain up to 128 characters.
Note:

- The use of this keyword does not eliminate the need for the APPLIANCE_SERVER keyword.
- If this parameter, or the APPLIANCE_SERVER_[1-5] parameter, is not detected at startup, then neither failover nor hot failover processing is activated.
- The APPLIANCE_SERVER_LIST parameter designates how this parameter is used.
- If used in combination, this parameter is overridden by the APPLIANCE_SERVER_[1-5] parameter.

Syntax:

```
APPLIANCE_SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_n(hostname|IP_address)
```

where *n* can be 1, 2, 3, 4, or 5.
Example:

```
APPLIANCE_SERVER_MULTI_STREAM_1(wal-vm-guardium20)
APPLIANCE_SERVER_FAILOVER_1(nwt-vm-guardium8)
APPLIANCE_SERVER_HOT_FAILOVER_1(wal-vm-guardium16)
APPLIANCE_SERVER_MULTI_STREAM_1(192.168.2.201)
APPLIANCE_SERVER_FAILOVER_1(192.168.2.202)
APPLIANCE_SERVER_HOT_FAILOVER_1(192.168.2.203)
```

APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER|HOT_FAILOVER)
Required: No
Default: FAILOVER
Description: Set APPLIANCE_SERVER_LIST to *MULTI_STREAM* for a Guardium appliance connection to be established for each server that is identified by the APPLIANCE_SERVER_MULTI_STREAM_n parameter.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *FAILOVER* for one Guardium appliance connection to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the APPLIANCE_SERVER_FAILOVER_n parameter. The agent attempts to connect to subsequent Guardium systems, beginning with APPLIANCE_SERVER_FAILOVER_1 and ending with APPLIANCE_SERVER_FAILOVER_5.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *HOT_FAILOVER* to cause connection types for each connected Guardium appliance identified by the APPLIANCE_SERVER_HOT_FAILOVER_n parameter to be kept active by pings.

- You must specify the primary Guardium appliance by using the APPLIANCE_SERVER parameter.
- If the primary Guardium appliance becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.

With any setting of APPLIANCE_SERVER_LIST, if all connections fail, and a spill file is specified (parameter OUTAGE_SPILLAREA_SIZE), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.
The default is *FAILOVER*.

APPLIANCE_PORT
Required: No
Default: 16022
Valid ports: 16022 or 16023
Description: The IP port number of the IBM Guardium system to which the IBM Guardium S-TAP for IMS agent should connect. This parameter must be correctly configured to enable a connection to the IBM Guardium system. If port 16023 is used, encryption support is required for the connection to the appliance.
Note: Specifying this keyword and parameter designates the port on which the IBM Guardium system is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS by another application.
Syntax: APPLIANCE_PORT*(port_number)*
Example: APPLIANCE_PORT(16022)

APPLIANCE_PING_RATE
Required: No
Default: 5
Description: Specifies the interval time between accesses to the IBM Guardium system to prevent timeout disconnections during idle periods. The value is in number of seconds.
Syntax: APPLIANCE_PING_RATE*(ping_interval)*
Example: APPLIANCE_PING_RATE(5)

APPLIANCE_NETWORK_REQUEST_TIMEOUT
Required: No
Default: 500
Description: Specifies a value in milliseconds of time to wait for the completion of a network communication request to send or receive. A value of 0 results in no timeout period. Range: 0 or 500 - 12000.
Syntax: APPLIANCE_NETWORK_REQUEST_TIMEOUT*(milliseconds)*
Example: APPLIANCE_NETWORK_REQUEST_TIMEOUT(500)

AUIU_EXCLUDE_LPAR
Required: No
Default: None
Description: Specifies a list of LPAR names (one to eight characters) in a SYSPLEX environment where the Common Storage Management Utility (AUIU*STC*) should not be scheduled. Multiple AUIU_EXCLUDE_LPAR statements can be specified to allow for LPAR name strings that are longer than 53 bytes.
Note: Use this keyword with caution. DLI calls run on the excluded LPARS are not audited.
With the exception of the LPAR where the agent resides, all LPARS can be excluded by using the option *ALL in place of an LPAR name.
Syntax: AUIU_EXCLUDE_LPAR(*list_of_lpars*)

Example: AUIU_EXCLUDE_LPAR(RS21,MYLPAR,YOURLPAR) or AUIU_EXCLUDE_LPAR(*ALL)

AUIU_PROC_NAME

Required: No

Default: AUIU*STC*

Description: Specifies the PROCLIB member name that contains the Common Storage Management Utility JCL. This JCL is supplied as member name AUIU*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIU*STC* address space.

Syntax: AUIU_PROC_NAME*(auiu_mbr_name)*

Example: AUIU_PROC_NAME(AUIUV1013)

DISPLAY_IMSMSG_DLIB(Y|N)

Required: No

Default: N

Description: Controls the output of informational messages AUIJ255I, AUIJ256I, AUIJ257I, and AUIJ258I in the AUILOG output DD of the AUIA*STC* agent address space. These messages are generated from data that is produced by the IMS DLI/DB batch jobs, and is passed to the agent from the DLIB z/OS log stream.

The default setting, *N*, prevents these messages from being written to the AUILOG DD.

Specify *Y* for these messages to be written to the AUILOG DD.

Syntax: DISPLAY_IMSMSG_DLIB*(Y|N)*

Example: DISPLAY_IMSMSG_DLIB(Y)

DISPLAY_IMSMSG_DLIO(Y|N)

Required: No

Default: N

Description: Controls the output of informational messages AUIJ255I, AUIJ256I, AUIJ257I, and AUIJ258I in the AUILOG output DD of the AUIA*STC* agent address space. These messages are generated from data that is produced by the IMS Control Region and passed to the agent from the DLIO z/OS log stream.

The default setting, *N*, prevents these messages from being written to the AUILOG DD.

Specify *Y* for these messages to be written to the AUILOG DD.

Syntax: DISPLAY_IMSMSG_DLIO*(Y|N)*

Example: DISPLAY_IMSMSG_DLIO(Y)

DLIFREQ

Required: No

Default: 100K

Description: Enables you to customize the number of DLI calls that are sent to the Guardium appliance before message AUIJ012I (providing a count of the number of events sent to appliance) is issued.

The count can be represented in thousands (K) or millions (M). Valid values are 10K – 999K and 1 – 10M.

Syntax: DLIFREQ*(100K)*

Example: DLIFREQ(100K)

FORCE_LOG_LIMITED

Required: No

Default: N

Description: Enables you to force limited audit logging by removing sensitive information (such as IMS segment data and concatenated key values) from data that is sent to the Guardium appliance by the S-TAP.

Specify *Y* to restrict sensitive data from being sent to the Guardium appliance.

Syntax: FORCE_LOG_LIMITED*(Y|N)*

Example: FORCE_LOG_LIMITED(N)

IMSL_AUDIT_LEVELS

Required: No

Default: ALL

Description: Specifies the events to be audited from those that are found using the IMS Archive Log task (AUIL*STC*) for each IMS instance under control of this agent. A specification other than `ALL` limits auditing to the events you specify.

For example, if you specify `USERS`, then all audited IMS instances under the agent report user signons and signoffs. If you specify `ALL`, you can use the Guardium interface to specify further limitations on what is audited for each audited IMS subsystem.

Table 1. IMSL_AUDIT_LEVELS audit parameters and events.

Parameter	Audited event
ALL	All events are audited (default)
CTL_STRT	IMS control region stops and starts
USERS	User signon and signoff
DBOPN	Database opens and closes
DB_PSB	DBDDUMP, DB/PSB START/STOP/LOCK/UNLOCK

Syntax: IMSL_AUDIT_LEVELS*(ALL|CTL_STRT|USERS|DBOPN|DB_PSB)*

Example: IMSL_AUDIT_LEVELS(ALL)

IMSL_CYCLE_INTERVAL

Required: No

Default: 15

Description: Specifies the frequency (in minutes) that the IMS Archive Log task (AUIL*STC*) checks the RECON data sets for new IMS SLDS (System Log Data Sets) to process. This value should correspond to the frequency at which IMS generates SLDS data sets during a normal workload. For example, if IMS SLDS are produced every 20 minutes, the IMSL_CYCLE_INTERVAL should be set to 20. A value of 0 (zero) can be specified to instruct the agent not start the AUIL*STC* task for any IMS subsystem that the agent controls. Valid parameters are 0 – 1440.

Syntax: IMSL_CYCLE_INTERVAL*(time_in_minutes)*

Example: IMSL_CYCLE_INTERVAL(45)

IMSL_ID_PREFIX

Required: No
Default: None
Description: Allows the partial customization of the 8-byte ID that is used when starting the AUILSTC task.
When this keyword is not used, the string *AAAAAAAA* is used for the first AUILSTC task to be started. Subsequent started AUILSTC tasks cause the ALPHA string to be incrementally increased by one character until the value of *ZZZZZZZZ* is reached. When *ZZZZZZZZ* is reached, the string is reset to *AAAAAAAA* when the agent (AUIASTC) is stopped and restarted.
When this keyword is used, the specified prefix (up to 6 bytes) is used, while the remaining two to seven characters are incrementally increased in the manner previously described. This enables a constant value (the specified prefix) to be used, alongside a wildcard character, when you are defining the ID to the TCP/IP security package to permit access to TCP/IP ports.
Note: The first character of the keyword must be an alphabetic character.
Syntax: IMSL_ID_PREFIX*(your_prefix)*
Example: IMSL_ID_PREFIX(MYPFX)
The example IMSL_ID_PREFIX(MYPFX) results in a generated AUILSTC ID of *MYPFXAAA -- MYPFXZZZ*.

IMSL_PROC_NAME
Required: No
Default: AUIL*STC*
Description: Specifies the PROCLIB member name that contains the IMS Archive Log JCL. This JCL is supplied as member name AUIL*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIL*STC* address space.
Syntax: IMSL_PROC_NAME*(auil_mbr_name)*
Example: IMSL_PROC_NAME(AUILV1013)

IMSL_SLDS_SRCH
Required: No
Default: 30
Description: This keyword can be used to limit the number of days within which the IMS log reader (AUILxxxx) will search for IMS system log data sets (SLDS) to process.

- If an IMS checkpoint does not exist for the SLDS reader, AUILxxxx will search for IMS SLDS that were created on the current day and for *x* days prior to the current day (where *x* is the value that you set for this parameter).
- If an IMS checkpoint that is set for the SLDS reader exceeds the number of days between the current day and the value that you set for this parameter, then the IMS checkpoint will be used as the starting point for IMS SLDS to be read and processed.
- If you set a value of *0* (zero) for this parameter, then only the current day's IMS SLDS will be processed. Also, IMS SLDS that were migrated from a hierarchical storage manager product will not be recalled for processing.
  Note: If you set a value of *0* (zero) for this parameter, AUILxxxx processing will omit any IMS SLDS that were created on the previous day. This can cause data to be missed if, for example, the AUILxxxx task is run at 12:05 AM. IMS SLDS that were created prior to midnight will not be recognized as being within the current day, and thus will not be processed.

Syntax: IMSL_SLDS_SRCH*(number_of_days)*
Example: IMSL_SLDS_SRCH(15)

LOG_FILTER(I/E)
Required: No
Default: I (include)
Description: Specifies whether to include or exclude messages that have been specified by the LOG_FILTER_MSG_ID parameter.

- The default value, `I`, allows only the specified message IDs to be included in the AUILOG output stream. Message IDs that are not specified by the LOG_FILTER_MSG_ID(messages) parameter will be suppressed. The default value should be used unless there is a specific business need to suppress messages.
- The optional value, `E`, suppresses the specified message IDs from the AUILOG output stream.
  Tip: The `E` value should only be used if the LOG_FILTER_MSG_ID keyword has been customized to suppress specific messages. Do not use the optional value (E) in conjunction with LOG_FILTER_MSG_ID(*) unless you want to prevent all messages from being written to the AUILOG output stream. Suppressing all messages is not recommended.

Syntax: LOG_FILTER*(include/exclude)*
Example: LOG_FILTER(E)

LOG_FILTER_MSG_ID(messages)
Required: No
Default: * (all messages)
Description: Can be used in conjunction with the LOG_FILTER(I/E) parameter to suppress specific messages from being written to the AUILOG output stream.
Tip: The LOG_FILTER_MSG_ID(*) default value should only be used with the LOG_FILTER(I) default value. Do not specify LOG_FILTER(E) in conjunction with LOG_FILTER_MSG_ID(*) unless you want to prevent all messages from being written to the AUILOG output stream. Suppressing all messages is not recommended.
Syntax: LOG_FILTER_MSG_ID*(id1,id2,id3...)*
Example: LOG_FILTER_MSG_ID(AUIZ014W)

LOG_PORT_SCAN_START
Required: No
Default: 41500
Description: Specifies the first communications port number to be checked for availability to be used for internal message logging communications. Use this keyword if environmental conditions dictate that a sequential scan and test of ports from port numbers 41500 - 65535 should not be performed. You can override the starting port with a port of your choice. This keyword and parameter can be used with the LOG_PORT_SCAN_COUNT keyword to limit the ports that are scanned to a specific range.
Syntax: LOG_PORT_SCAN_START*(port_number)*
Example: LOG_PORT_SCAN_START(41500)

LOG_PORT_SCAN_COUNT
Required: No
Default: 10
Description: This keyword can be used in conjunction with the LOG_PORT_SCAN_START keyword to limit number of the ports that are scanned and tested for availability. The integer specified (1 - 65535) represents the number of ports that should be scanned. If the port number specified by the LOG_PORT_SCAN_START value plus the LOG_PORT_SCAN_COUNT value exceeds 65535, the scan terminates at port 65535.
Syntax: LOG_PORT_SCAN_COUNT*(number_of_ports)*
Example: LOG_PORT_SCAN_COUNT(1000)

LOG_STREAM_DLIB
Required: Yes
Default: None

Description: This required keyword is used to specify the z/OS System Logger log stream to stream audited events from DLI DBB batch jobs. The value should be the BATCH_LOGSTREAM_NAME value specified as the DEFINE LOGSTREAM NAME parameter of the AUILSTR2 or AUILSTR3 JCLs.
Syntax: LOG_STREAM_DLIB*(log_stream_name)*
Example: LOG_STREAM_DLIB(AUI_BATCH_LOG_STREAM)

LOG_STREAM_DLIO

Required: Yes
Default: None
Description: This required keyword is used to specify the z/OS System Logger log stream to be used to stream audited events from IMS Control Regions. The value should be the ONLINE_LOGSTREAM_NAME value specified as the DEFINE_LOGSTREAM_NAME parameter of the AUILSTR2 or AUILSTR3 JCLs.
Syntax: LOG_STREAM_DLIO*(log_stream_name)*
Example: LOG_STREAM_DLIO(AUI_ONLINE_LOG_STREAM)

LOOPBACK_ADDRESS

Required: No
Default: LOCALHOST
Description: Specifies the loopback host or IP address that is used for communications between the agent and the agent secondary address spaces. For most network configurations, the default value of `LOCALHOST` can be used. If `LOCALHOST` cannot be resolved on your system, consult your network specialist for the correct loopback mnemonic or IP address to be used.
Syntax: LOOPBACK_ADDRESS*(hostname|IP_address)*
Example: LOOPBACK_ADDRESS(LOCALHOST)

LPAR_MONITOR_INTERVAL

Required: No
Default: 5
Description: Specifies the frequency (in minutes) for the agent to request a list of LPARs that are active within the SYSPLEX. Schedule the Common Storage Management Utility (AUIU*STC*) tasks on any LPAR coming online to the SYSPLEX. Valid parameters are integers between 1 and 60.
Syntax: LPAR_MONITOR_INTERVAL*(minutes)*
Example: LPAR_MONITOR_INTERVAL(5)

MESSAGE_LOG_LEVEL

Required: No
Default: I
Description: Controls the amount of output log information that is generated by the agent.

Table 2. Message severity codes and descriptions.

Message severity code	Description
I	Includes all log messages
W	Includes all log messages with a warning severity or higher
E	Includes all log messages with an error severity or higher
O	Instructs the agent not to log error messages
S	Includes all log messages with a severe error code

Syntax: MESSAGE_LOG_LEVEL*(I|W|E|O|S)*
Example: MESSAGE_LOG_LEVEL(I)

OUTAGE_SPILL_AREA_SIZE

Required: No
Default: 0
Description: Determines the maximum amount of memory in megabytes to be allocated for the retention of audit data in the event of a IBM Guardium system connection outage. A value of `0`, or the absence of this keyword, disables spill area support. The maximum value permitted as a parameter is 1024.
Syntax: OUTAGE_SPILL_AREA_SIZE*(memory_size)*
Example: OUTAGE_SPILL_AREA_SIZE(15)

POLICY_READ_INTERVAL

Required: No
Default: 5
Description: Determines the frequency in seconds that the connection to the IBM Guardium system checks for changes to the installed policies that are used to determine audited event collection.
Syntax: POLICY_READ_INTERVAL*(time_in_seconds)*
Example: POLICY_READ_INTERVAL(5)

STAP_STREAM_EVENTS

Required: No
Default: Y
Description: Specifies whether events will be streamed to the IBM Guardium system. The default value, *Y*, enables streaming. Specify *N* to disable streaming and enable Simulation mode.
Syntax: STAP_STREAM_EVENTS*(Y|N)*
Example: STAP_STREAM_EVENTS(Y)

PREFER_IPV4_STACK

Required: No

Default: N

Description: If set to Y, this parameter causes a request to be issued to the Domain Name Server (DNS) for an IPV4 address for the hostname that is specified in the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

If this parameter is set to N or omitted from configuration, a request for an IPV6 address is issued to the DNS for the hostname that is specified by the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV4 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this parameter is used, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for IMS started task will terminate.

Syntax:

```
PREFER_IPV4_STACK(Y|N)
```

Example:

```
PREFER_IVP4_STACK(Y)
```

SMF_AUDIT_LEVELS

Required: No

Default: ALL

Description: Specifies which events to audit of those found using the SMF task (AUIF*STC*). A specification other than `ALL` limits the events to be audited to the events you specify. For example, if `DELETE` is specified, then all audited IMS instances under the agent would only be capable of reporting data set `DELETE` events. If `ALL` is specified, you can further limits what is audited for each audited IMS subsystem, using the user interface.

Table 3. SMF_AUDIT_LEVELS audit parameters and events

Parameter	Audited event
ALL	All events are audited (default)
UPDATE	Data sets opened with UPDATE access
DELETE	Data sets deleted
READ	Data sets opened with READ access
CREATE	Data sets created
ALTER	Data sets opened with ALTER access
RACF®	RACF violations on data sets

Syntax: SMF_AUDIT_LEVELS*(ALL|UPDATE|DELETE|READ|CREATE|ALTER|RACF)*

Example: SMF_AUDIT_LEVELS(ALL)

SMF_CYCLE_INTERVAL

Required: No

Default: 300

Description: Specifies the frequency (in minutes) that the SMF task (AUIFSTC) checks the z/OS catalog for new data sets, which meet the specified data set masks, using the SMF_DSN_MASK keyword. This value should correspond to the frequency at which your z/OS system swaps SMF logging VSAM files (sometimes known as SMF MANX|MANY) during a normal workday. For example, if the SMF logging files are swapped every 8 hours, the SMF_CYCLE_INTERVAL should be set to `480` (8 hours * 60 minutes). A value of zero can be specified to indicate that the agent should not start the AUIF*STC* task and SMF auditing should not be performed. Valid parameters are 0 – 1440.

Syntax: SMF_CYCLE_INTERVAL*(time_in_minutes)*

Example: SMF_CYCLE_INTERVAL(45)

SMF_DSN_MASK_[1-10]

Required: Yes

Default: None

Description: At least one instance of this keyword is required (SMF_DSN_MASK_1). This keyword provides a data set mask used to query the z/OS catalog for sequential format data sets containing SMF data offloaded from the SMF log-files (MANX|MANY) using the IFASMFDP program. These sequential files can be the original files created when offloading the MANX|MANY files, or a copy of these sequential files created by customizing and running AUISMFDF and AUISMFDP jobs located in the product sample data set. In most environments, only one SMF_DSN_MASK would be specified, but up to 10 are allowed.

Table 4. Masking character rules

Character	Rule
%	Indicates that only one alphanumeric or national character can occupy that position
%%%	Indicates that more than one character can be substituted, with the number of substitution characters being equal to the number of percent signs specified.

Example 1: specifying a GDG data set in the mask: If the AUISMFDP job has been customized to produce a GDG data set as the SORTOUT DD output data sets, you can choose to specify the fully qualified GDG base name in the mask for system name field. For example, A.B.C. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged GDG entries under this name, for example:

- A.B.C.G0001V00
- A.B.C.G0002V00
- A.B.C.G0003V00

Example 2: specifying a data set name explicitly: Provide the generation and version values as a mask. For example, A.B.C.G%%%%V%%. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged data sets that match this mask, for example:

- A.B.C.G0021V00
- A.B.C.G0022V00
- A.B.C.G0023V00

Example 3: specifying a DSN using a DATE/TIME naming convention: If you have customized the AUISMFDP job to produce a data set name that contains date and time values as qualifiers within the data set name as the SORTOUT DD output data sets, you can specify the data set name using a string of percent signs within the date and time qualifier names. For example: HLQ.D%%%%%%.T%%%%%%.SMFDATA. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged data sets matching the mask, for example:

- HLQ.D091122.T131000.SMFDATA
- HLQ.D091123.T131100.SMFDATA
- HLQ.D091124.T131200.SMFDATA

Note: The percent (%) wildcard character should only be specified for the numeric characters of the generation and version node of GDG data sets, or as the numeric characters of date or time nodes of the SMF dataset.
Syntax: SMF_DSN_MASK_1*(SMF.DUMP.DSN)*
Example:

```
SMF_DSN_MASK_1(AUI.SMF.DUMP.COPY)
SMF_DSN_MASK_2(AUI.SMF.DUMP.GDG.G%%%%V%%)
SMF_DSN_MASK_3(AUI.SMF.D%%%%%%.T%%%%%%.COPY)
```

SMF_EVENT_EXPIRY
Required: No
Default: 5
Description: Specifies the number of days that incomplete SMF events should be retained in the SMF spill file. Incomplete SMF events are audited events that have not yet received the associated SMF Type 30 record, which indicates that the step/job is complete, and contains information that is needed to complete the reporting of the event. When an event exceeds the expiration date, it is flagged as incomplete, sent to the IBM Guardium system, and removed from the SMF spill file. The valid range is 1 to 180 days.
Syntax: SMF_EVENT_EXPIRY*(days)*
Example: SMF_EVENT_EXPIRY(5)

SMF_PROC_NAME
Required: No
Default: AUIFSTC
Description: Specifies the PROCLIB member name that contains the SMF secondary address space JCL. This JCL is supplied as member name AUIF*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIF*STC* address space.
Syntax: SMF_PROC_NAME*(auif_mbr_name)*\
Example: SMF_PROC_NAME(AUIFV91)

SMF_SELF_AUDIT
Required: No
Default: N
Description: Indicates whether to audit the accesses of IMS data sets that are used by the product to determine the names of IMS artifacts to be audited. Examples of IMS data sets that can be accessed include RECON data sets and IMS archived logs (SLDS). A value of `N` indicates that these accesses should not be audited. A value of `Y` indicates that these data sets should be considered for auditing.
Syntax: SMF_SELF_AUDIT*(N|Y)*
Example: SMF_SELF_AUDIT(N)

SMF_SPILL_FILE
Required: Yes
Default: None
Description: Specifies the DSN of a sequential format fixed block data set with a LRECL of 300. This data set is used to store incomplete audited SMF events. Incomplete audited SMF events are events triggered by SMF records that have yet to encounter an SMF Type 30 record, indicating the step or job has completed. The AUIFUSPL member of the SAUISAMP data set provides an example of the allocation specifications for this data set.
Syntax: SMF_SPILL_FILE*(dsn)*
Example: SMF_SPILL_FILE(AUI.V1013.SPILL)

TCPIP_BUFFER_SIZE
Required: No
Default: 32768
Description: Specifies the size of an internal buffer that is used to hold audited events in preparation of the TCP/IP send to the IBM Guardium system, and specifies the size of the TCP/IP buffer. In most environments, the size of this buffer should not be changed
Syntax: TCPIP_BUFFER_SIZE*(buffer_size)*
Example: TCPIP_BUFFER_SIZE(32768)

TRACE_CONFIG
Required: No
Default: ON
Description: TRACE_CONFIG(ON) enables IBM Guardium S-TAP for IMS configuration values to display by default at agent startup. You can optionally use this keyword to disable the IBM Guardium S-TAP for IMS configuration value display. To prevent the displayed report of agent configuration parameters during agent startup, specify TRACE_CONFIG(OFF).
Syntax: TRACE_CONFIG*(ON|OFF)*
Example: TRACE_CONFIG(OFF)

WTO_MSG
Required: No
Default: None
Description: Allows a user to request that specific informational, warning, or error messages written to the AUILOG DD statement of the agent (AUIA*STC*) or agent secondary address spaces (AUIF*STC*, AUIL*STC* or AUIU*STC*) also be written to the Operator Console (WTO). This enables these messages to be recognized by an automated operations tool, or provides higher operator visibility for these messages and allows appropriate action to be taken. Each message requires a separate keyword, and each keyword must be specified on a separate line.
Syntax: WTO_MSG*(msgnumber)*
Example:

```
WTO_MSG(AUIJ011I)
WTO_MSG(AUIL607W)
WTO_MSG(AUIY006E)
```

XML_ECHO_AUILOG(Y|N)
Required: No
Default: N
Description: Indicates that when an audit policy is installed on a IBM Guardium system appliance, its corresponding XML is to be echoed to the AUILOG DD. If there is more than one policy installed on the agent, the XML of each policy is echoed. If all installed policies are subsequently uninstalled, then the echoed XML reflects that there are no installed policies. For more information about echoed XML statements, see XML statement definitions.
Syntax: XML_ECHO_AUILOG(Y|N)
Example: XML_ECHO_AUILOG(Y)

XML_ECHO_DATASET(Data_Set_Name[,Cylinders])
Required: No
Default: None
Description:

Indicates that when the IBM Guardium system installs an audit policy, its corresponding XML is echoed to a data set (specified by the data set name value in this parameter). If there is more than one policy installed on the agent, the XML of each is echoed. If all installed policies are subsequently uninstalled, then the echoed XML reflects that there are no installed policies. The XML will not be echoed when the installed policy is already active, is being reinstalled, and there have been no changes to the policy.

If *Data_Set_Name* is intended to be a Generation Data Group (GDG), then it must be set as the GDG base name. The agent checks the system catalog to determine whether *Data_Set_Name* exists and whether or not it is a GDG base name.

Data_Set_Name can contain z/OS system symbols such as &SYSNAME. To determine the names of the system symbols that are currently defined to the system, issue the DISPLAY SYMBOLS command to the system console.

If *Data_Set_Name* does not exist, and there is no GDG base defined in this name, the agent allocates the data set as non-GDG. If *Data_Set_Name* is a regular physical sequential data set (non-GDG based) and does exist, the agent allocates space for the *Cylinders* keyword when the agent is restarted.

Cylinders defaults to 1 and can range from 1 – 10.
Syntax: XML_ECHO_DATASET*(&Data_Set_Name[,Cylinders])*
Example: XML_ECHO_DATASET(AUIAGENT.ECHO.XML.GDG.BASE,2)

ZIIP_AGENT_DLI
Required: No
Default: N
Description: Indicates that the following agent processes should be zIIP capable: agent reads of audited events from the z/OS System Logger log streams, formatting of these events into protobuf style messages, and sending of these messages to the IBM Guardium system using TCP/IP.
Note: Use of the zIIP depends on the presence of a zIIP on the LPAR where the agent is running, as well as use of the Workload Management Service Policies. For more information about zIIP, see the topic on Customizing IMS to use a System z® Integrated Information Processor (zIIP).
Syntax: ZIIP_AGENT_DLI*(Y|N)*
Example: ZIIP_AGENT_DLI(Y)

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Related reference

- Customizing IMS to use a System z Integrated Information Processor (zIIP)

Agent configuration

The IP addresses of the IBM Guardium system appliances are specified using the SAUISAMP data set AUICONFG member using the APPLIANCE_SERVER and APPLIANCE_SERVER_FAILOVER_[1-5] keywords.

See Providing Guardium system failover for more information.
Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Customizing the agent JCL

The SAUISAMP member AUIA*STC* provides a sample JCL that can be used for the agent started task. This topic describes how to customize the JCL.

Before you begin

In environments where multiple agents connect to a common IBM Guardium system or appliance, the z/OS agent started task names (AUIA*STC*, AUIL*STC*, AUIF*STC*) must be unique. Unique started task names enable the IBM Guardium S-TAP for IMS policies that are pushed from the IBM Guardium system to be attributed to, and monitored by, the correct z/OS agent.

Procedure

1. Edit SAUISAMP members AUIA*STC*, AUIF*STC*, AUIL*STC* and AUIU*STC* by running the ISPF edit macro.
   See Planning your configuration and customizing your environment for more details.
2. Modify the CFG=AUI.V100.AGTCFG(AUICONFG) in AUIA*STC* to specify the location of the customized configuration data set for the agent created in the previous section.
3. Optional: You can rename the AUIA*STC* member to any character name that is valid for started tasks in your environment.
4. Optional: You can rename the AUIF*STC*, AUIL*STC*, and AUIU*STC*. AUIF*STC*, AUIL*STC*, and AUIU*STC* names should match the values of the IMSL_PROC_NAME, SMF_PROC_NAME, and AUIU_PROC_NAME keywords that you supply in the configuration file.
5. Copy the AUIA*STC*, AUIF*STC*, AUIL*STC* and AUIU*STC* members to the PROCLIB for the site.
   Contact the z/OS systems programmer to determine the location of the PROCLIB.
   Note: APF authorization of the AUILOAD file is required for each of these members before they are started.

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Starting and stopping the agent

Start the agent by issuing the command /S AUIASTC from the SDSF command line. The primary agent address space starts the AUIF*STC* address spaces. One or more instances of AUIL*STC* might also be started, depending on the list of active collections.

Stop the agent by issuing the command /STOP AUIASTC, or /MODIFY AUIASTC,STOP, from the SDSF command line. The primary agent address space then stops all the secondary address spaces that are online, and shuts down. Depending on the load, and the activity in the other secondary address spaces, the shut down process can take time. Monitor the AUILOG DD of the primary address space AUIA*STC* for informational messages on the status of the secondary address spaces.

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Agent security considerations

The user ID of the agent started tasks (the primary and the secondary started tasks) should have the necessary RACF® profiles for reading the configuration member contents.

Important: Contact your system administrator to ensure that localhost is resolving to 127.0.0.1 (loopback address). The TCP/IP communication between the agent and the secondary address spaces relies on this resolution. If this is not possible at your site, use the *loop-back-address* element in the AUICONFG sample library member to avoid localhost resolution by specifying the loopback IP address directly, or by specifying an appropriate host name that resolves to the loopback address.
Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Modifying the frequency of AUIJ012I messages

You can modify how frequently the agent provides a count of DLI calls (from the default of every 10K DLI calls to a value of your choice, 10K – 999K, 1M – 10M.)

Use the agent parameter keyword DLIFREQ to modify the frequency of AUIJ012I messages, or issue the command /MODIFY AGENT,SET CONFIG DLIFREQ *aaaK* / *bbM*, from the SDSF command line.

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Setting up an IMS environment for auditing

This section describes how to customize IMS environments to capture DLI calls, including customizing IMS catalogued procedures, coexisting with other DFSFLGX0 and DFSISVI0 exit routines, customizing IMS to use a zIIP, copying common load modules from SAUILOAD to SAUIIMOD, and the security considerations related to IMS processing.

- **Security considerations for IMS processing**
  IBM Guardium S-TAP for IMS does not impose any additional RACF® or other security restrictions on IMS assets during IMS processing. However, the IMS control region and any DLI/DBB batch jobs being executed, must have UPDATE authority to the z/OS system log streams you have defined for use by IBM Guardium S-TAP for IMS.
- **Customizing IMS environments to capture DLI calls**
  For IBM Guardium S-TAP for IMS to report on IMS database accesses, it needs to be sensitive to IMS DL/I calls. Use the following sections to establish proper set-up of the relationship between your IMS online and batch environments and IBM Guardium S-TAP for IMS.
- **Customizing IMS cataloged procedures**
  For IBM Guardium S-TAP for IMS to monitor DL/I calls from IMS online Transactions, BMPs and DLI/DBB batch jobs, the IMS Control region and DLI/DBB batch jobs require access to these IBM Guardium S-TAP for IMS programs.
- **Coexisting with other DFSFLGX0 and DFSISVI0 exit routines**
  IBM Guardium S-TAP for IMS provides product-specific DFSFLGX0 (IMS Logger) and DFSISVI0 (IMS Batch) exits to enable the product to report on IMS DL/I call activity. In some IMS environments, user requirements or third-party vendor products also require the use of these exits. IBM Guardium S-TAP for IMS can accommodate the use of multiple DFSFLGX0 and DFSISVI0 exit routines.
- **Defining LOGWRT exits**
  Use the EXITDEF parameter in the USER_EXITS section of the DFSDFxxx IMS PROCLIB member to define LOGWRT exits to be used by your IMS subsystem.
- **Customizing IMS to use a System z Integrated Information Processor (zIIP)**
  IBM Guardium S-TAP for IMS allows you to configure an IMS control region to prepare specific auditing functions for execution on a System z® Integrated Information Processor (zIIP). Execution on a zIIP is governed by the Workload Management software on your appliance, as well as the workload already assigned to the zIIP.
- **Copying common load modules from SAUILOAD to SAUIIMOD**
  After the initial SMP/E installation of IBM Guardium S-TAP for IMS, copy common load modules from the SAUILOAD to SAUIIMOD data set using the modules described in this topic.
- **Configuring APP_EVENT support**
  IBM Guardium S-TAP for IMS allows IMS DLI application programs to store user information on the IBM Guardium system. This enables your user data to be linked with DLI DB calls that are made from within the same application checkpoint, unit-of-work, or commit. APP_EVENT calls are linked to audited DLI calls by subsystem ID, application sequence number, and number of commits within a schedule. Follow these steps to install and configure a new IMS database, named AUIAPPEV, to be used for this purpose.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Security considerations for IMS processing

IBM Guardium S-TAP for IMS does not impose any additional RACF® or other security restrictions on IMS assets during IMS processing. However, the IMS control region and any DLI/DBB batch jobs being executed, must have UPDATE authority to the z/OS system log streams you have defined for use by IBM Guardium S-TAP for IMS.

Parent topic: Setting up an IMS environment for auditing

Customizing IMS environments to capture DLI calls

For IBM Guardium S-TAP for IMS to report on IMS database accesses, it needs to be sensitive to IMS DL/I calls. Use the following sections to establish proper set-up of the relationship between your IMS online and batch environments and IBM Guardium S-TAP for IMS.

Note: The IBM Guardium S-TAP for IMS programs that are used to communicate with your IMS environments are found in the SAUIIMOD data set, and are created during product installation.
Parent topic: Setting up an IMS environment for auditing

Customizing IMS cataloged procedures

For IBM Guardium S-TAP for IMS to monitor DL/I calls from IMS online Transactions, BMPs and DLI/DBB batch jobs, the IMS Control region and DLI/DBB batch jobs require access to these IBM Guardium S-TAP for IMS programs.

The IBM Guardium S-TAP for IMS programs that must be accessed reside in the SAUIIMOD installation data set. The preferred method of installing IBM Guardium S-TAP for IMS into your IMS environment is to copy the entire contents of the SAUIIMOD data set into your IMS RESLIB (IMS.SDFSRESL) data set.

If copying IBM Guardium S-TAP for IMS programs into your IMS RESLIB is not possible, then the SAUIIMOD data set must be included in your IMS control region JCL as the first data set of the STEPLIB DD concatenation. The SAUIIMOD data set must also be included as the first data set of the STEPLIB DD concatenation of the DLI batch cataloged procedure (DLIBATCH member of the IMS PROCLIB data set) and the DBB batch cataloged procedure (DBBBATCH member of the IMS PROCLIB data set).

Note:

- If the SAUIIMOD data set is included in any JCL, you must ensure that it is APF-authorized.
- IBM Guardium S-TAP for IMS provides and uses the DFSFLGX0 and DFSISIV0 IMS exits to establish communication with IMS services, however no customization of these exits is required.

Parent topic: Setting up an IMS environment for auditing

Coexisting with other DFSFLGX0 and DFSISVI0 exit routines

IBM Guardium S-TAP for IMS provides product-specific DFSFLGX0 (IMS Logger) and DFSISVI0 (IMS Batch) exits to enable the product to report on IMS DL/I call activity. In some IMS environments, user requirements or third-party vendor products also require the use of these exits. IBM Guardium S-TAP for IMS can accommodate the use of multiple DFSFLGX0 and DFSISVI0 exit routines.

Using IMS Tools Generic Exits

IMS Tools Generic Exits are a collection of components that provide common command and exit routine interfaces to support the operation of IMS tools in an IMS environment.

IBM Guardium S-TAP for IMS supports the protocols used by the IMS Tools Generic Exit product. You can define the IBM Guardium S-TAP for IMS copy of the DFSFLGX0 exit by either supplying IMS with a PROCLIB member using a BPE-style control statement, or by building a load module that contains the required information.

An example of the PROCLIB control statement follows:

```
EXITDEF(TYPE(LOGR) EXITNAME(AUIFLGX0) LOADLIB(AUI.SAUIIMOD))
```

See the IBM IMS Tools Generic Exit Reference Manual for Generic Logger Exit setup and usage.
Important: The IBM IMS Tools Generic Exit product does not support exit DFSISVI0.

Using IBM Guardium S-TAP for IMS exit cascading

For situations where the IBM IMS Tools Generic Exit is not available for use, IBM Guardium S-TAP for IMS provides a method of supporting two instances of the DFSFLGX0 and DFSISVI0 exits.

When loaded and run, the IBM Guardium S-TAP for IMS supplied program AUIFLGX0 (DFSFLGX0) and AUIISVI0 (DFSISIV0) determines from which DSN within the JOBLIB/STEPLIB concatenation it was loaded from. It then searches all subsequent DSNs within the JOBLIB/STEPLIB DD concatenation, looking for the next occurrence of the exit with the same name.

- If none are found, or it is determined that the IMS Tools Generic Exit product is involved in executing the exit, no cascading is done.
- If an exit is found, and it is determined that the exit found is in fact another instance of the IBM Guardium S-TAP for IMS exit (as could happen if the SAUIIMOD data set was specified multiple times in the JOBLIB/STEPLIB concatenation), the search will continue with the remainder of the DSNs in the concatenation.
- If a non-IBM Guardium S-TAP for IMS Exit is found, this new exit is loaded, and called with R13 pointing to the save area supplied by IMS. A new 512 byte user work area, obtained specifically for this exit instance, is then pointed to by the SXPLAWRK field of the IMS Standard User Exit Parameter List (DFSSXPL). This 512 byte work area is obtained when the first (or INIT) call is done; the work area address (in the SXLPAWRK field) and work area content are maintained for all subsequent calls.

Exit cascading restrictions

Note: These restrictions only apply when using the exit cascading feature, and not when using the IBM IMS Tools Generic Exit product.
The IBM Guardium S-TAP for IMS Exit (AUIFLGX0 or AUIISVI0) must be first in the JOBLIB/STEPLIB concatenation, unless the exit that exists in a prior DSN also has a method of cascading calls to other exits, and is capable of providing an IMS formatted area in R13 and the address of a unique, persistent 512 byte work area in the SXPLAWRK parameter list field to the AUIFLGX0 or AUIISVI0 program.

In a non-APF-authorized environment, such as when executing program DFSULTR0 or an IMS DLI/DBB batch program, the exit load module to be cascaded to must have an ALIAS, and the ALIAS must be appropriately either DFSFLGX0 or DFSISVI0, if the target exit module has the RENT or REUS attribute on.

Parent topic: Setting up an IMS environment for auditing

Defining LOGWRT exits

Use the EXITDEF parameter in the USER_EXITS section of the DFSDFxxx IMS PROCLIB member to define LOGWRT exits to be used by your IMS subsystem.

You must specify the exit name AUIFLGX0 in the list of LOGWRT exits to be used. This disables the cascading feature, which prevents other LOGWRT exits in the STEPLIB from being unintentionally invoked. You must include the SAUIIMOD load library in the IMS Control Region STEPLIB concatenation.

Example:

```
<SECTION=USER_EXITS>
EXITDEF=(TYPE=LOGWRT,EXITS=(AUIFLGX0))
```

Parent topic: Setting up an IMS environment for auditing

Customizing IMS to use a System z Integrated Information Processor (zIIP)

IBM Guardium S-TAP for IMS allows you to configure an IMS control region to prepare specific auditing functions for execution on a System z® Integrated Information Processor (zIIP). Execution on a zIIP is governed by the Workload Management software on your appliance, as well as the workload already assigned to the zIIP.

To use this feature, the LPAR on which the IMS Control region executes must have a zIIP installed. The IMS Control Region should also make use of the z/OS Workload Manager product. For more information on using z/OS Workload Manager with the IMS Control Region, see the *Workload Manager and IMS* section of the *IBM IMS System Administration* manual.

The following processes can be scheduled on a zIIP:

- Calling of the compiled filter to determine if the DLI event is to be audited, and if the segment concatenated key or segment data should be sent to the Guardium appliance.
- Movement of the audited DLI calls to a storage buffer used to hold audited data until a write to the z/OS System Logger log-stream can be executed
- Calling of the z/OS System Logger IXGWRITE, which moves the audited data from the buffer to the log-stream when the buffer fills, or a flush of the buffer is scheduled

To indicate that the IMS Control region should attempt to schedule these processes on the zIIP, a //AUIZIIP DD DUMMY DD statement should be added to the IMS Control Region JCL. When detected, the audit code produces the informational message AUII055I, indicating that zIIP processing will be attempted.

Warning messages AUII042W and AUII043W are issued if zIIP processing is requested when a zIIP is not available, and when IMS is not using Workload Manager. Error message AUII044E indicates that the request was rejected. In all instances where the attempt to use the zIIP has failed, audit processing continues without attempting to execute the audit code on the zIIP.

Parent topic: Setting up an IMS environment for auditing

Related reference

- Customizing the agent by using agent parameter keywords

Copying common load modules from SAUILOAD to SAUIIMOD

After the initial SMP/E installation of IBM Guardium S-TAP for IMS, copy common load modules from the SAUILOAD to SAUIIMOD data set using the modules described in this topic.

AUI$NAP
: Module used to trace data
Provided in the SAUILOAD data set
Also needed in the SAUIIMOD data set

AUICPMOD
: An SAUISMAP member
Performs a copy of the AUI$NAP module from the SAUILOAD to the SAUIIMOD data set
Should be customized and submitted after the initial SMP/E installation

Parent topic: Setting up an IMS environment for auditing

Configuring APP_EVENT support

IBM Guardium S-TAP for IMS allows IMS DLI application programs to store user information on the IBM Guardium system. This enables your user data to be linked with DLI DB calls that are made from within the same application checkpoint, unit-of-work, or commit. APP_EVENT calls are linked to audited DLI calls by subsystem ID, application sequence number, and number of commits within a schedule. Follow these steps to install and configure a new IMS database, named AUIAPPEV, to be used for this purpose.

Procedure

1. Perform a Database Descriptor Generator (DBD gen) for the AUIAPPEV database.
   An example of the DBD source to use is in member AUIAPPEV of the SAUISAMP data set.
2. Create a database data set for the AUIAPPEV database.
3. If appropriate for your site, register the DB and DDN to DBRC, specifying NOREOV if possible.
4. If appropriate for your site, create a dynamic allocation (MDA) member for the database data set.
5. Modify application program PSBs to include a PCB for the AUIAPPEV database.
   Use a PROCOPT of *G* and a KEYLENGTH of *0*.
6. If the APP_EVENT feature is to be used by an IMS Online system, perform an ACBGEN for DBD member AUIAPPEV and the modified PSBs.
7. Modify application programs to send APP_EVENT information using the AUIAPPEV PCB:
   a. In the 2000 byte I/O area, modify the application programs to include the information that you want to be sent to the appliance.
   b. Perform a DLI GET call by using the AUIAPPEV PCB.
      A DLI status code of blanks will be returned.

- **APP_EVENT examples**
  Examples of the AUIAPPEV database, a PSB with DBPCB for the AUIAPPEV database included, the Assembler language of an IMS DLI call, and a C program are provided here. These code samples are for example purposes only. There is no guarantee of the reliability, serviceability, or function of these programming examples.

Parent topic: Setting up an IMS environment for auditing

APP_EVENT examples

Examples of the AUIAPPEV database, a PSB with DBPCB for the AUIAPPEV database included, the Assembler language of an IMS DLI call, and a C program are provided here. These code samples are for example purposes only. There is no guarantee of the reliability, serviceability, or function of these programming examples.

AUIAPPEV database

The AUIAPPEV database is used to support the transmittal of environmental information from an application program to the Guardium appliance. The following is an example:

```
DBD                    NAME=AUIAPPEV,ACCESS=(HDAM,OSAM),RMNAME=(DFSHDC40,10,20)
DATASET                DD1=AUIAPPEV,SIZE=2048
SEGM       NAME=ROOT,PARENT=0,BYTES=2000
DBDGEN
FINISH
END
```

PSB with DBPCB for the AUIAPPEV database included

The following is an example of a PSB with DBPCB for the AUIAPPEV database included:

```
PCB             TYPE=DB,PROCOPT=A,KEYLEN=4,DBDNAME=AUEVOL01,  PCBNAME=ODBPCB1
SENSEG          NAME=ROOT,PARENT=0
PCB             TYPE=DB,PROCOPT=G,KEYLEN=0,DBDNAME=AUIAPPEV,  PCBNAME=APPEV01
SENSEG          NAME=ROOT,PARENT=0
PSBGEN          LANG=ASSEM,CMPAT=YES,PSBNAME=AUIPSBAV
END
```

Assembler language of an IMS DLI call

The following is an example in the Assembler language of an IMS DLI call that will send a string to the Guardium appliance:

```
MVC       IOAREA(20),=CL20'THIS IS AN APP_EVENT'    /Set APP_EVENT message
XC      PARM@(12*4),PARM@                           /Clear parameter area
LA       R1,GN                          /Addr of GN literal
ST              R1,PARM@+0                                    /Save in parmlist
L       R2,APPCB@                                             /Addr of AUIAPPEV PCB
ST      R2,PARM@+4                                   /Save in parmlist
LA      R1,IOAREA                                             /Addr of IOAREA
ST       R1,PARM@+8                    /Save in parmlist
OI      PARM@+8,X'80'           /Terminate parmlist
LA       R1,PARM@                 /Addr of parmlist
L       R15,DLI@                /Addr of ASMTDLI program
BASR    R14,R15                                               /Call ASMTDLI
```

C program

The following is an example of a C program:

```
#define    iopcb     (IO_PCB_TYPE *)(__pcblist)        /* I/O PCB */
#define    dbpcb     (PCB_STRUCT_8_TYPE *)(__pcblist)  /* DB PCB  */
#define    aepcb     (PCB_STRUCT_8_TYPE *)(__pcblist)  /* AUIAPPEV DB PCB  */

int  rc = 0;
const static char GU = "GU  ";

struct {
  char output 2000¨;
} iodata ;


....
....

/* create a APP_EVENT */
sprintf(iodata.output, "THIS IS AN APP_EVENT");
rc = ctdli(GU, aepcb, &iodata);
```

Parent topic: Configuring APP_EVENT support

Using agent configuration keywords to customize auditing

Some agent configuration keywords must be used for the product to function. You can also use agent configuration keywords for optional auditing specifications.

Required keywords

The following keywords must be set for the product to function:

APPLIANCE_SERVER
: This is the host name, or IP address, of the IBM Guardium system to which the agent should connect.

LOG_STREAM_DLIO
: This is the log stream name for online DLI calls.

LOG_STREAM_DLIB
: This is the log stream name for batch DLI calls.

You can also audit accesses to database-related data sets using SMF records. To audit accesses to IMS data sets that occur outside of IMS services, use the following keywords:

SMF_SPILL_FILE

This is the data set name.

SMF_DSN_MASK_1
This is the data set mask value.

Optional keywords

To set the following optional specifications, use the keyword that is listed. More information about each specification is provided, following this list.

Enabling Simulation mode
STAP_STREAM_EVENTS(N)

Restricting IMS segment and concatenated key data from being sent to the Guardium appliance
FORCE_LOG_LIMITED(Y)

Using multiple SMF data set masks
SMF_DSN_MASK_2 through SMF_DSN_MASK_10

Disabling SMF auditing at the agent level
SMF_CYCLE_INTERVAL(0)
Note: If SMF_CYCLE_INTERVAL(0) is specified, no additional SMF configuration parameters are required.

Controlling the frequency of SMF z/OS catalog queries
SMF_CYCLE_INTERVAL(time in minutes)

Changing the retention period of incomplete SMF events
SMF_EVENT_EXPIRY(number of days)

Changing the name of the SMF address space JCL
SMF_PROC_NAME(new name)

Auditing IMS data set access
SMF_SELF_AUDIT(Y)

Changing the type of events audited using SMF records
SMF_AUDIT_LEVELS(ALL|UPDATE|DELETE|READ|CREATE|ALTER|RACF)

Overriding the range of ports used for address space communications
LOG_PORT_SCAN_START(41501), LOG_PORT_SCAN_COUNT(24003)

Requesting specific agent messages to be issued to the operator console
WTO_MSG(AUIF507E), WTO_MSG(AUIT013I)

Determining the context of APPLIANCE_SERVER_[1-5] or APPLIANCE_SERVER_[FAILOVER|MULTI_STREAM|HOT_FAILOVER]_[1-5]
APPLIANCE_SERVER_LIST(FAILOVER|MULTI_STREAM|HOT_FAILOVER)

Providing Guardium system failover support
APPLIANCE_SERVER_FAILOVER_[1-5](IP address or host name)

Providing Guardium system multistream support
APPLIANCE_SERVER_MULTI_STREAM_[1-5](IP address or host name)

Providing Guardium system hot failover support
APPLIANCE_SERVER_HOT_FAILOVER_[1-5](IP address or host name)

Providing a spill area for short term outages
OUTAGE_SPILL_AREA_SIZE(megabytes)

Disabling IMS SLDS auditing at the agent level
IMSL_CYCLE_INTERVAL(0)
Note: If IMSL_CYCLE_INTERVAL(0) is specified, no additional IMSL configuration parameters are required.

Controlling the frequency IMS System Log Data Sets are allocated and read
IMSL_CYCLE_INTERVAL(time in minutes)

Changing the name of the IMSL address space JCL
IMSL_PROC_NAME(new name)

Changing the type of events audited using IMS SLDS records
IMSL_AUDIT_LEVELS(ALL|CTL_STRT|USERS|DBOPN|DB_PSB)

Changing the name of the Common Memory Management address space JCL
AUIU_PROC_NAME(new name)

Excluding DLI calls occurring on specific LPARS from being audited
AUIU_EXCLUDE_LPAR(lpar1, lpar2...lpar9)

Running more than one agent in a SYSPLEX
ADS_SHM_ID(100010), ADS_LISTENER_PORT(16055)

Removing Segment data and Concatenated Key values from audited data at the agent level
FORCE_LOG_LIMITED(Y)

Using the System z Integrated Information Processor (zIIP)
ZIIP_AGENT_DLI

Viewing AUI messages that are produced by the IMS Control regions in the AUI agent log
DISPLAY_IMSMSG_DLIO(N|Y)

Viewing AUI messages produced by the IMS DLI/DBB batch jobs in the AUI agent log
DISPLAY_IMSMSG_DLIB(N|Y)

Restricting auditing to specific IMS systems when multiple IMSs share RECON data sets
IMSNAME_EQ_IMSSSID(N|Y)

Enabling/Disabling the IBM Guardium S-TAP for IMS configuration value display at agent startup
TRACE_CONFIG(ON|OFF)

Setting the number of days within which AUILxxxx will process IMS system log data sets (SLDS)
IMSL_SLDS_SRCH(number of days)

- **Simulation mode**
  Simulation mode enables you to simulate agent processing. IBM Guardium S-TAP for IMS uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.
- **Specifying multiple SMF data set masks**
  You can use the SMF_DSN_MASK keyword to specify up to nine additional SMF data set masks.
- **Disabling SMF auditing at the agent level**
  You can use the SMF_CYCLE_INTERVAL keyword to disable SMF auditing at the agent level.

- **Controlling the frequency of SMF z/OS catalog queries**
  You can change the frequency of SMF z/OS catalog queries by using the SMF_CYCLE_INTERVAL keyword to specify a value in minutes:
- **Changing the retention period of incomplete SMF events**
  By default, incomplete SMF events will be retained in your SMF spill data set for 5 days. You can change this time range by specifying the SMF_EVENT_EXPIRY keyword:
- **Changing the name of the SMF address space JCL**
  To change the name of the AUIFS*TC* JCL member name, use the SMF_PROC_NAME keyword to change AUIFSTC to a name of your choice:
- **Auditing IMS data set access**
  To obtain a report of IMS artifact access, use the SMF_SELF_AUDIT keyword.
- **Changing the types of events that are audited using SMF records**
  Use the SMF_AUDIT_LEVELS keyword to indicate a list of events to be audited, instead of collecting all event types.
- **Using alternate RECON data sets for SMF and SLDS processing**
  You can optionally use copies of the IMS RECON data sets when processing SMF (AUIF*STC*) and IMS SLDS (AUIL*STC*) data instead of using the live RECON data sets.
- **Overriding the range of ports used for communication between address spaces**
  You can set the available port scan starting point and limit the number of ports to check for availability.
- **Overriding the TCP/IP DNS resolver table**
  IBM Guardium S-TAP for IMS uses TCP/IP as a host path for intra- and inter-address space communication of information such as collection policy details and address space status updates. To receive information from an AUIU*STC*_(Common Storage Management Utility) address space running on a different LPAR in the sysplex, the AUIA*STC*_(agent) address space must determine its own physical IP address and make it known to AUIU*STC*.
- **Specifying agent messages to issue to the operator console**
  You can use the WTO_MSG keyword to specify the messages to issue to the operator console.
- **Creating a spill area for short-term outages**
  Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area.
- **Disabling IMS SLDS auditing at the agent level**
  You can turn off the auditing process that uses IMS SLDS records by specifying the IMSL_CYCLE_INTERVAL keyword with a value of zero.
- **Controlling the frequency with which IMS System Log Data Sets are allocated and read**
  You can specify the frequency of IMS RECON data set queries by specifying the IMSL_CYCLE_INTERVAL keyword.
- **Changing the name of the IMSL address space JCL**
  To change the JCL member name AUIL*STC*, use the IMSL_PROC_NAME keyword.
- **Changing the types of events audited using IMS SLDS records**
  To audit some, instead of all event types, you can specify each event type to be audited by using the IMSL_AUDIT_LEVELS keyword.
- **Changing the name of the Common Memory Management address space JCL**
  Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice.
- **Excluding DLI calls on specific LPARS from being audited**
  To stop the transmission of the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS.
- **Running more than one agent in a SYSPLEX**
  If two or more IMS agents are running on one SYSPLEX, use the ADS_SHM_ID and ADS_LISTENER_PORT keywords to differentiate the shared memory segment and port for each agent environment.
- **Restricting auditing to specific IMS systems when multiple IMS systems share RECON data sets**
  If multiple unrelated IMS systems share RECON data sets, and you want to audit only on one or more specific IMS systems, use the keyword IMSNAME_EQ_IMSSSID(Y) to isolate auditing to the desired IMS system.
- **Using the System z Integrated Information Processor (zIIP)**
  You can use the System z® Integrated Information Processor (zIIP) when running IBM Guardium S-TAP for IMS Control region address space, and in the agent address space (AUIA*STC*). Use the ZIIP_AGENT_DLI keyword with the Y parameter to cause the agent to make a zIIP-enabled enclave SRB initialization attempt.
- **Using multiple Guardium systems**
  You can configure multiple Security Guardium systems for automatic failover. By configuring one or more backup systems, you ensure continuous auditing capability. This process is known as failover. You can also enable the streaming of audited data from one or more IBM Guardium S-TAP for IMS agents to up to 6 connected Security Guardium systems. This process is known as multistreaming.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Simulation mode

Simulation mode enables you to simulate agent processing. IBM® Guardium® S-TAP® for IMS uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.

When STAP_STREAM_EVENTS is set to *N*, the parameter stops the agent TCP/IP data transmission process. The agent performs all data collection processes but does not send the audit record to the Guardium appliance.

Parent topic: Using agent configuration keywords to customize auditing

Specifying multiple SMF data set masks

You can use the SMF_DSN_MASK keyword to specify up to nine additional SMF data set masks.

Specifying multiple SMF data set masks

The naming conventions of some environments prohibit the use of a SMF_DSN_MASK_1 value, which allows all required data sets to be read. To audit accesses to database-related data sets from multiple LPARS of your SYSPLEX, you can specify up to nine additional data set mask values: SMF_DSN_MASK_2 through SMF_DSN_MASK_10.

Parent topic: Using agent configuration keywords to customize auditing

Disabling SMF auditing at the agent level

You can use the SMF_CYCLE_INTERVAL keyword to disable SMF auditing at the agent level.

For any IMS systems that are audited by this agent, you can disable audit access to IMS data sets that occur outside the use of IMS services. To do so, specify the following keyword with the value of zero: SMF_CYCLE_INTERVAL(0)

Specifying SMF_CYCLE_INTERVAL(0) turns off auditing process that uses SMF records. The agent address space (AUIA*STC*) will not start the SMF auditing address space (AUIF*STC*).

Parent topic: Using agent configuration keywords to customize auditing

Controlling the frequency of SMF z/OS catalog queries

You can change the frequency of SMF z/OS catalog queries by using the SMF_CYCLE_INTERVAL keyword to specify a value in minutes:

To determine if any new, unread data sets match the specified SMF_DSN_MASK_x values, the SMF processing address space (AUIF*STC*) periodically performs a query against the z/OS catalog, looking for data sets to process. By default, this query is performed when the AUIF*STC* task is started, and repeated every 300 minutes (5 hours). To change the default time value, use the keyword SMF_CYCLE_INTERVAL*(time in minutes)*. If you specify a time value of zero, the SMF auditing feature will be disabled.
Parent topic: Using agent configuration keywords to customize auditing

Changing the retention period of incomplete SMF events

By default, incomplete SMF events will be retained in your SMF spill data set for 5 days. You can change this time range by specifying the SMF_EVENT_EXPIRY keyword:

In some situations, such as a canceled job or end-of-memory events, a type 30 record is not produced for a step or job. To keep these types of records from filling your SMF spill data set, you can set a time limit in days to determine how long incomplete SMF records are retained. The default value is 5 days and can be changed by specifying the SMF_EVENT_EXPIRY keyword to indicate the number of days of your choice: SMF_EVENT_EXPIRY*(number of days)*.
Parent topic: Using agent configuration keywords to customize auditing

Changing the name of the SMF address space JCL

To change the name of the AUIF*STC* JCL member name, use the SMF_PROC_NAME keyword to change AUIFSTC to a name of your choice:

AUIF*STC* is the name of the JCL that provides auditing of data set accesses using SMF records. AUIF*STC* is provided in the product installation sample data set (SAUISAMP). If the name AUIF*STC* conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL. Use the SMF_PROC_NAME keyword to change the member name from AUIF*STC* to a name of your choice: SMF_PROC_NAME*(new name)*.

Ensure that this JCL resides in a procedure data set (PROCLIB) that allows the z/OS START command S taskname to be used.

Parent topic: Using agent configuration keywords to customize auditing

Auditing IMS data set access

To obtain a report of IMS artifact access, use the SMF_SELF_AUDIT keyword.

IBM Guardium S-TAP for IMS reads the IMS RECON data sets and system log data sets produced by IMS (SLDS) to obtain IMS environment information, such as IMS artifact names. IMS artifact names determine the databases and data sets that are used to create audit information.

By default, IBM Guardium S-TAP for IMS does not report accesses of IMS artifacts. To obtain a report of these accesses, specify a value of Y using the SMF_SELF_AUDIT keyword: SMF_SELF_AUDIT*(Y)*.

Parent topic: Using agent configuration keywords to customize auditing

Changing the types of events that are audited using SMF records

Use the SMF_AUDIT_LEVELS keyword to indicate a list of events to be audited, instead of collecting all event types.

When auditing using SMF records is enabled, the default action is to provide auditing for all of the following accesses to data sets:

- Open events with READ access
- Open events with UPDATE/WRITE access
- Open events with ALTER access
- Data set DELETE events
- Data set CREATE events
- Access denied (RACF violation)

To specify some and not all of these events for auditing, you can specify each type of event to be audited by using the SMF_AUDIT_LEVELS keyword: SMF_AUDIT_LEVELS (*ALL*|*READ*|*UPDATE*|*DELETE*|*CREATE*|*ALTER*|*RACF*).
Remember: This keyword affects the SMF auditing level for all IMS subsystems controlled by this agent. If you do not include READ accesses in the SMF_AUDIT_LEVELS parameter, then no READ accesses will be reported for any of the IMS environments that are audited by using the agent.
Note: You can separate parameters for the collection of different event types. For example, to audit UPDATE and READ events, include the UPDATE and READ records as follows:

```
SMF_AUDIT_LEVELS(UPDATE)
SMF_AUDIT_LEVELS(READ)
```

instead of:

```
SMF_AUDIT_LEVELS(UPDATE|READ)
```

Parent topic: Using agent configuration keywords to customize auditing

Using alternate RECON data sets for SMF and SLDS processing

You can optionally use copies of the IMS RECON data sets when processing SMF (AUIF*STC*) and IMS SLDS (AUIL*STC*) data instead of using the live RECON data sets.

To use alternate RECON data sets for SMF and SLDS processing:

1. Add a //AUIARCN DD statement to the AUIF*STC* and AUIL*STC* JCLs that contain the name of the IMS system (as defined in the IMS Definition panel of the Guardium interface).
2. Add the alternate RECON data set names to be used when processing these two types of data sources.
   Note: Specifying alternate RECON data set names only affects AUIF*STC* and AUIL*STC* task processing. It has no effect on processing of any other tasks.

Use IDCAMS, or another VSAM-compatible method, to create cataloged, VSAM copies of your live RECON data sets.

The data set that is specified by the AUIARCN DD statement must be defined as Fixed Block (FB) with a record length of 80 bytes (LRECL=80), and it can be a PDS, PDS/E, or sequential file. The following guidelines apply:

- An asterisk (*) in column 1 indicates that the line is a comment.
- Keywords must start in column 1.
- No spaces are allowed within keywords and parameters.
- Multiple IMSNAME keywords can be specified in one AUIARCN file.
- At least one RECON data set must be included under each IMSNAME identifier.
- Alternate RECON data sets must be cataloged and in IMS format.

Table 1. IMSNAME and RECON data set values, defined:

Value	Purpose
IMSNAME=	Specifies the IMS to which the subsequent RECON1, 2, and 3 keywords pertain.
RECON1=	Specifies the alternate data set name to be used for RECON1.
RECON2=	Specifies the alternate data set name to be used for RECON2.
RECON3=	Specifies the alternate data set name to be used for RECON3.

Example:

```
IMSNAME=IMSV14
RECON1=IMSEA1.ALT.RECON1
RECON2=IMSEA1.ALT.RECON2
RECON3=IMSEA1.ALT.RECON3
*
IMSNAME=IMSV13
RECON1=IMSDA1.ALT.RECON1
RECON2=IMSDA1.ALT.RECON2
```

Parent topic: Using agent configuration keywords to customize auditing

Overriding the range of ports used for communication between address spaces

You can set the available port scan starting point and limit the number of ports to check for availability.

IBM Guardium S-TAP for IMS uses a communications port to pass messages between threads within each address space. The default port is 41500. If the address space determines that port 41500 is not available for use, all subsequent ports up to 65535 are examined, and the first available port is used.
Some installations have restrictions on which ports should be examined and used. Use the LOG_PORT_SCAN _START and LOG_PORT_SCAN_COUNT keywords to set the available port scan starting point and limit the number of ports to be checked for availability:

- LOG_PORT_SCAN_START(41501)
- LOG_PORT_SCAN_COUNT(24003)

The sum of the value of the SCAN_START port number plus the SCAN_COUNT should not exceed 65535.
Parent topic: Using agent configuration keywords to customize auditing

Overriding the TCP/IP DNS resolver table

IBM Guardium S-TAP for IMS uses TCP/IP as a host path for intra- and inter-address space communication of information such as collection policy details and address space status updates. To receive information from an AUIU*STC*_(Common Storage Management Utility) address space running on a different LPAR in the sysplex, the AUIA*STC*_(agent) address space must determine its own physical IP address and make it known to AUIU*STC*.

To determine its physical IP address, the IBM Guardium S-TAP for IMS agent uses the z/OS getaddrinfo function and passes it to the LPAR name specified in the CVTSNAME field of the z/OS CVT control block. The getaddrinfo function uses the DNS resolver table to map the agent's LPAR name to its physical IP address. The DNS resolver table should contain entries that associate each LPAR within the sysplex to its physical IP address. If there is no association found, the agent (AUIA*STC*) uses the z/OS gethostname and getaddrinfo services to obtain the physical IP address of its own LPAR; but the IP addresses of other LPARs in the sysplex cannot be determined. In that case, inter-address space communication is not possible and events that occur on other LPARs are not reported to the Guardium appliance. Similarly, inter-address space communications can fail if users of Dynamic Virtual IP Addressing (VIPA) attempt to associate multiple IP addresses to a single VIPA token.

To determine if the LPAR name, in the CVTSNAME field, is included in the DNS table:

1. Run the Rexx executable that is located in the SAUISAMP data set of member AUIPING.
2. If the ping is successful, the LPAR name is defined in the DNS table and no further action is required.
3. If the ping fails due to an unknown host error, the LPAR name was not found in the DNS table. Contact your network administrator to request the addition of the LPAR name and the associated IP address to the DNS table.

Network administrators can manually associate the LPAR name that is found in the z/OS CVTSNAME field with the name that is used in the DNS revolver table by including the AUIHOST DD statement file in all IMS S-TAP agent task address space JCLs.

cvts_lpar_name(*dns_name*)

Required if AUIHOST DD is specified.
Default: None.
Description: Translates the CVTSNAME to the name in the DNS table.

lpar_name
Found in the z/OS CVTSNAME field.
Use the AUIPING REXX exec found in the SAUISAMP data set to obtain that name.
The *lpar_name* value can be from 1 -- 8 bytes in length.

dns_name
Found in the DNS table that associates the LPAR with an IP address.
The DNS_NAME value must conform to the following z/OS TCP/IP HOSTNAME rules:

- Must contain 1 or more tokens separated by a period.
- Each token must be at least 1 character and less than 64 characters.
- Each token must start with a letter or number.
- Remaining characters in each token must be a letter, number, or hyphen.

Example: PRODA(SYSTEM_1)
wherein:

- *PRODA* is the LPAR name found in the CVTSNAME field of your z/OS system
- *SYSTEM_1* is the mnemonic used in your DNS table to relate this LPAR to a TCP/IP address.

The AUIHOST DD statement file must meet the following standards:

- It must be a sequential file, or a member of a Partitioned Data Set (PDS) or Extended Partitioned Data Set (PDSE).
- It must be defined with a Fixed Blocked (FB) Record Format (RECFM).
- It must have a Logical Record Length (LRECL) of 80 bytes.
- Commented lines can be indicated by an asterisk (*) in column one or by a slash-asterisk (/*) in columns one and two.
- It must contain all host definitions on one line.
- Up to 16 DNS names can be specified.

The following is an example of an AUIHOST DD statement file:

```
MYLPAR20(MYLPAR20.mycompany.com)
MYLPAR21(MYLPAR21.mycompany.com)
MYLPAR22(MYLPAR22.mycompany.com)
MYLPAR23(MYLPAR23.mycompany.com)
MYLPAR24(MYLPAR24.mycompany.com)
MYLPAR25(MYLPAR25.mycompany.com)
MYLPAR26(MYLPAR26.mycompany.com)
```

Parent topic: Using agent configuration keywords to customize auditing

Specifying agent messages to issue to the operator console

You can use the WTO_MSG keyword to specify the messages to issue to the operator console.

IBM Guardium S-TAP for IMS allows you to specify informational, warning, or error messages to be written to the operator console. This allows an automated operations product to take some predefined action or provide a higher level of operator visibility to these messages. You can use the WTO_MSG to specify which messages should be write-to-operated.

- WTO_MSG(AUIF507E)
- WTO_MSG(AUIT013I)

You can specify one message ID per WTO_MSG instance. Messages originating from the AUIA*STC*, AUIF*STC*, AUIL*STC*, and AUIU*STC* address spaces are supported.
Parent topic: Using agent configuration keywords to customize auditing

Creating a spill area for short-term outages

Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area.

Short-term communication outages between the agent address spaces and the IBM Guardium system can be handled by using a z/OS data space spill area. Use of the spill area can prevent the loss of audited data by allowing the z/OS agent to save audited data until the connection to the IBM Guardium system is restored. The restoration of the communications link results in the flushing of the data space contents to the IBM Guardium system.

Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area: OUTAGE_SPILL_AREA_SIZE*(megabytes)*. If you specify zero or omit this keyword, the spill area will not be allocated or used. The maximum value you can specify is 1024 MB.

Parent topic: Using agent configuration keywords to customize auditing

Disabling IMS SLDS auditing at the agent level

You can turn off the auditing process that uses IMS SLDS records by specifying the IMSL_CYCLE_INTERVAL keyword with a value of zero.

For any IMS systems to be audited by this agent, you can disable audit events that are determined by reading IMS System Log Data Sets (SLDS). To disable the auditing process that uses IMS SLDS records, specify the following keyword with the value of zero: IMSL_CYCLE_INTERVAL*(0)*. The agent address space (AUIA*STC*) will not start the IMS SLDS auditing address space (AUIL*STC*).

Parent topic: Using agent configuration keywords to customize auditing

Controlling the frequency with which IMS System Log Data Sets are allocated and read

You can specify the frequency of IMS RECON data set queries by specifying the IMSL_CYCLE_INTERVAL keyword.

For the product to determine if any new, unread IMS System Log Data Sets LDS data sets have been created by the IMS Online system, the IMSL processing address space (AUIL*STC*) periodically performs a query against the IMS RECON data sets, looking for new SLDS. This query is performed when the AUIL*STC* task is started, and then by default, every 15 minutes. The frequency can be changed by providing a value in minutes by using the IMSL_CYCLE_INTERVAL keyword: IMSL_CYCLE_INTERVAL*(time in minutes)*

A value of zero will cause the IMS SLDS auditing feature to be disabled.

Parent topic: Using agent configuration keywords to customize auditing

Changing the name of the IMSL address space JCL

To change the JCL member name AUIL*STC*, use the IMSL_PROC_NAME keyword.

AUIL*STC* is the name of the JCL that is used to audit data sets using IMS SLDS records. AUIL*STC* is provided in the product installation sample data set (SAUISAMP). If this name conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL.

Use the IMSL_PROC_NAME keyword to change the member name from AUIL*STC* to a name of your choice: IMSL_PROC_NAME*(new name)*

Ensure that this new JCL is in a procedure data set (PROCLIB) that allows the z/OS START command S taskname to be used.

Parent topic: Using agent configuration keywords to customize auditing

Changing the types of events audited using IMS SLDS records

To audit some, instead of all event types, you can specify each event type to be audited by using the IMSL_AUDIT_LEVELS keyword.

When you enable auditing by using IMS SLDS records, the default is to provide auditing for all of the following event types:

- IMS Online region starts and stops
- Users sign on/sign off
- Database Opens and Closes
- PSB|DBD start, stop, lock, unlock, and DBDDUMP

To audit only some of these events, you can specify each event type to be audited using the IMSL_AUDIT_LEVELS keyword: IMSL_AUDIT_LEVELS (*ALL*|*CTL_STRT*|*USERS*|*DBOPN*|*DB_PSB*).

This keyword governs the IMS SLDS auditing level for all IMS subsystems that are controlled by this agent. For example, if user signon/signoff is not included in the IMSL_AUDIT_LEVELS parameter, then no signon or signoff events will be reported from any of the IMS environments that are audited using the agent.

Note: You can separate parameters for the collection of different event types. For example, to audit CTL_STRT and DBOPN events, include the CTL_STRT and DBOPN records as follows:

```
IMSL_AUDIT_LEVELS(CTL_STRT)
IMSL_AUDIT_LEVELS(DBOPN)
```

instead of:

```
IMSL_AUDIT_LEVELS(CTL_STRT|DBOPN)
```

Parent topic: Using agent configuration keywords to customize auditing

Changing the name of the Common Memory Management address space JCL

Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice.

AUIU*STC* is the name of the JCL that is used to build filtering criteria in E/CSA on all LPARS of the SYSPLEX. AUIU*STC* is provided in the product installation sample data set (SAUISAMP). If this name conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL.

Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice: AUIU_PROC_NAME*(new name)*.

Ensure that this JCL resides in a procedure data set (PROCLIB) that allows the z/OS START command S taskname to be used.

Parent topic: Using agent configuration keywords to customize auditing

Excluding DLI calls on specific LPARS from being audited

To stop the transmission of the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS.

By default, the IBM Guardium S-TAP for IMS agent creates Common Memory Management address spaces (AUIU*STC*) on all LPAR members of a SYSPLEX. This allocates E/CSA memory, and inserts DLI call filtering criteria across all LPARS. A single agent monitors IMS control regions and DLI/DBB batch jobs running on any LPAR of the SYSPLEX.

If you do not want to transmit the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS: AUIU_EXCLUDE_LPAR*(lpar1, lpar2...lpar9)*

The LPAR where the agent is running cannot be excluded. All other LPARS can be excluded by using the *ALL option in place of the LPAR name.

For example, AUIU_EXCLUDE_LPAR(*ALL).
Parent topic: Using agent configuration keywords to customize auditing

Running more than one agent in a SYSPLEX

If two or more IMS agents are running on one SYSPLEX, use the ADS_SHM_ID and ADS_LISTENER_PORT keywords to differentiate the shared memory segment and port for each agent environment.

The agent address space (AUIA*STC*) and subordinate address spaces (AUIF*STC* and AUIL*STC*) communicate by using a shared memory segment and communications port. Multiple agents require multiple unique shared memory segments and port values to ensure correct inter-address space communications. If you need to have two or more IBM Guardium S-TAP for IMS agents available on one SYSPLEX, the following keywords provide a method of uniquely identifying the shared memory segment and port for each agent environment:

- ADS_SHM_ID(100010)
- ADS_LISTENER_PORT(16055)

Specification of the ADS_SHM_ID and ADS_LISTENER_PORT requires the addition of a //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the AUIA*STC* and AUIU*STC* JCLs for the agent, to ensure that communications between all participant address spaces use the correct memory object and ports.

See Customizing the agent by using agent parameter keywords for complete descriptions of all valid parameters, including the ADS_SHM_ID and ADS_LISTENER_PORT keywords.

Parent topic: Using agent configuration keywords to customize auditing

Restricting auditing to specific IMS systems when multiple IMS systems share RECON data sets

If multiple unrelated IMS systems share RECON data sets, and you want to audit only on one or more specific IMS systems, use the keyword IMSNAME_EQ_IMSSSID(Y) to isolate auditing to the desired IMS system.

The default option, IMSNAME_EQ_IMSSSID(N), causes only the IMS RECON data sets to be used when IBM Guardium S-TAP for IMS attempts to find and match IMS systems to active audit policies.

Specifying IMSNAME_EQ_IMSSSID(Y) causes both the IMS RECON data sets, and the 8-byte IMS subsystem/DBCTL RSENAME to be used when IBM Guardium S-TAP for IMS attempts to find and match IMS systems to active audit policies.

Consider the following example:

RECON data sets A.B.C1/C2/C3 contain information for IMSA and IMSB. Auditing is only desired for IMSB. Policy AUDIT_ALL is installed by using IMS appliance definition *MY_IMS*, which references RECON data sets A.B.C1/C2/C3.

If subsystems IMSA and IMSB both use RECON data sets that are referenced by the policy, AUDIT_ALL, and associated with the IMS definition, *MY_IMS*, then both IMSA and IMSB are audited when the default, IMSNAME_EQ_IMSSSID(N), is specified.

To restrict auditing to IMSB:

1. Specify IMSNAME_EQ_IMSSSID(Y) in the AUICONFG file.
2. Name the IMS definition in the appliance `IMSB`.
3. Relate policy AUDIT_ALL to `IMSB`.
4. Install the policy.

As a result, IMSB is audited with the criteria that is set in policy AUDIT_ALL, and IMSA is not audited.
Note: DLI batch jobs (DLI/DBB) might not be tightly associated with an IMSID, therefore IBM Guardium S-TAP for IMS will report on all DLI batch jobs that use the audited RECON data set. The IMSNAME_EQ_IMSSID parameter does not affect DLI/DBB batch job auditing.
Parent topic: Using agent configuration keywords to customize auditing

Using the System z Integrated Information Processor (zIIP)

You can use the System z® Integrated Information Processor (zIIP) when running IBM Guardium S-TAP for IMS Control region address space, and in the agent address space (AUIA*STC*). Use the ZIIP_AGENT_DLI keyword with the Y parameter to cause the agent to make a zIIP-enabled enclave SRB initialization attempt.

IMS control region

The following processes are moved to the zIIP in the IMS Online Control Region, pending redirection by the operating system:

- DLI call filtering
- IXGWRITE of audited DLI call data to the z/OS System Logger log stream

To use a zIIP in the IMS Online Control region, add a //AUIZIIP DD DUMMY to the IMS control region JCL.

Agent address space

The following processes are moved to the zIIP in the agent address space (AUIA*STC*), pending redirection by the operating system:

- IXGBROWSE read of audited data from the z/OS System Logger log streams for both Online and Batch DLI calls
- TCP/IP send of the data to the Guardium system

To use a zIIP in the agent address space, use the ZIIP_AGENT_DLI keyword with the Y parameter to the configuration file that is pointed to by the AUICONFG DD statement in the agent JCL (AUIA*STC*).

Parent topic: Using agent configuration keywords to customize auditing

Using multiple Guardium systems

You can configure multiple Security Guardium systems for automatic failover. By configuring one or more backup systems, you ensure continuous auditing capability. This process is known as failover. You can also enable the streaming of audited data from one or more IBM Guardium S-TAP for IMS agents to up to 6 connected Security Guardium systems. This process is known as multistreaming.

- **Providing Guardium system failover**
  You can specify up to five additional Guardium systems to be connected to the agent by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit between one and five.
- **Streaming to multiple Guardium systems**
  Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 IBM Guardium system (APPLIANCE_SERVER + APPLIANCE_SERVER_MULTI_STREAM_*n*, where *n* can be 1 - 5).
- **Keeping connections active when HOT_FAILOVER is enabled**
  When the HOT_FAILOVER feature is enabled by setting the APPLIANCE_SERVER_LIST parameter to *HOT_FAILOVER*, connections for each connected Guardium appliance are kept active by pings. (The following connection types are kept active: DLIO, DLIB, SMF, IMSL, and MLOG.)

Parent topic: Using agent configuration keywords to customize auditing

Providing Guardium system failover

You can specify up to five additional Guardium systems to be connected to the agent by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit between one and five.

The failover process

IBM Guardium S-TAP for IMS uses the concept of a single primary IBM Guardium system and multiple secondary backup systems.

- When a primary IBM Guardium system goes offline, the IBM Guardium S-TAP for IMS agent automatically establishes a connection to a secondary IBM Guardium system, and the audited data is sent to the secondary system.
- When a primary IBM Guardium system comes back online, the IBM Guardium S-TAP for IMS agent detects it, and reestablishes the connection to the primary IBM Guardium system and restarts, sending data to the primary system.

This allows the use of any IBM Guardium system as a short-term backup, while always attempting to use the primary system as the main data storage medium.

In the following example failover scenario, where none of the systems are online, the IBM Guardium S-TAP for IMS agent attempts to connect to the primary IBM Guardium system at a regular interval and follows the usual failover logic if the primary IBM Guardium system is offline. A connection is reestablished to any of the configured appliances as soon as one becomes available.

Enabling multiple system failover support

IBM Guardium S-TAP for IMS allows the specification of up to five additional IBM Guardium system to be connected to the agent. This feature provides failover protection, which allows the agent to continue to send audited data to one of a number of backup IBM Guardium system in the event of a communication failure with the primary system. You must use the APPLIANCE_SERVER keyword to enable this feature, because the IBM Guardium system that is referenced by this keyword is the primary connection. You can specify additional IBM Guardium system by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit from 1 to 5.

- APPLIANCE_SERVER_FAILOVER_1(IP address 1)
- APPLIANCE_SERVER_FAILOVER_2(host name 2)
- APPLIANCE_SERVER_FAILOVER_3(IP address 3)
- APPLIANCE_SERVER_FAILOVER_4(IP address 4)
- APPLIANCE_SERVER_FAILOVER_5(host name 5)

Example failover scenario

Audit data flows to the primary IBM Guardium system, A.

The TCP/IP connection from the IBM Guardium S-TAP for IMS agent to the primary IBM Guardium system fails.

A connection is made to the secondary IBM Guardium system, B.

Audit data is now flowing to the secondary IBM Guardium system, B.

The TCP/IP connection from the IBM Guardium S-TAP for IMS agent to the primary IBM Guardium system is reestablished.

Audit data now flows to the primary IBM Guardium system, A.

The IBM Guardium S-TAP for IMS agent and IBM Guardium system B disconnect.

Parent topic: Using multiple Guardium systems

Streaming to multiple Guardium systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 IBM Guardium system (APPLIANCE_SERVER + APPLIANCE_SERVER_MULTI_STREAM_*n*, where *n* can be 1 - 5).

IBM Guardium S-TAP for IMS sends events to a single appliance until a ping occurs, or the number of records that is specified by MEGABUFFER_COUNT is reached. Audited DLI events are distributed amongst additional appliances in a round-robin sequence.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the APPLIANCE_SERVER_LIST parameter. The APPLIANCE_SERVER and APPLIANCE_SERVER_[MULTI_STREAM]_[1-5] parameters specify the appliances to which you intend to stream events. The appliance that is specified by APPLIANCE_SERVER provides the policy that is used for event matching.

Enabling multistream support

Use the APPLIANCE_SERVER keyword to enable multistream support. The IBM Guardium system that is referenced by the APPLIANCE_SERVER keyword is the primary connection, and it provides the policy used to match DLI events. You can specify additional appliances by using the APPLIANCE_SERVER_MULTI_STREAM_*n* keyword, where *n* is a digit from 1 - 5.

Specify up to 5 additional IBM Guardium system IP addresses or host names. For example:

- APPLIANCE_SERVER_MULTI_STREAM_1(IP address 1)
- APPLIANCE_SERVER_MULTI_STREAM_2(host name 2)
- APPLIANCE_SERVER_MULTI_STREAM_3(IP address 3)
- APPLIANCE_SERVER_MULTI_STREAM_4(IP address 4)
- APPLIANCE_SERVER_MULTI_STREAM_5(host name 5)

Parent topic: Using multiple Guardium systems

Keeping connections active when HOT_FAILOVER is enabled

When the HOT_FAILOVER feature is enabled by setting the APPLIANCE_SERVER_LIST parameter to *HOT_FAILOVER*, connections for each connected Guardium® appliance are kept active by pings. (The following connection types are kept active: DLIO, DLIB, SMF, IMSL, and MLOG.)

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Parent topic: Using multiple Guardium systems

IBM Security Guardium S-TAP for IMS on z/OS agent reference information

The IBM Guardium S-TAP for IMS agent provides access to database and appliance services, in support of the product's remote clients. The agent also reads audited DLI events placed in the z/OS System Logger log streams by the IMS Online and DLI/DBB batch Data collectors and sends the DLI events to the IBM Guardium system using TCP/IP connections.

- **Sample library members**
  Use the following sample library members shipped with IBM Guardium S-TAP for IMS to install and configure the product.
- **Agent environment**
  The agent must be running before you can use product functions related to the IMS subsystems monitored by that agent.
- **APF authorization**
  For security, the agent must be APF-authorized before it can be run.
- **Agent job output**
  The primary output of the agent job consists of log messages written to the AUILOG DD. These messages provide status information about the ongoing operation of the agent, and also record additional messages if errors occur.
- **Stopping the agent**
  When running on z/OS, the agent accepts standard z/OS /MODIFY and /STOP commands. When stopping the agent, all secondary address spaces controlled by the agent will also receive a stop request.
- **Starting and stopping the secondary address spaces**
  This topic describes the /MODIFY commands to start and stop the secondary address spaces.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Sample library members

Use the following sample library members shipped with IBM Guardium S-TAP for IMS to install and configure the product.

Table 1. Sample library members

Member	Type	Description
AUIAPPEV	DBD source statements	DBD source statements, used to define the optional APP_EVENT DBD
AUIA*STC*	JCL	Primary agent address space JCL
AUICONFG	CONFIG	Configuration file containing only the minimum required keywords
AUICONFX	CONFIG	Configuration file containing all available keywords
AUICPMOD	JCL	JCL to copy utility programs from SAUILOAD to SAUIIMOD data set
AUIEMAC1	MACRO	Edit macro to facilitate changes to other sample library members
AUIF*STC*	JCL	SMF data collection address space JCL

Member	Type	Description
AUIFUSPL	JCL	JCL to create the SMF incomplete event spill file for an agent
AUIL*STC*	JCL	IMS archived log data collection address space JCL
AUILSTR1	JCL	JCL to add CFRM structures for batch and online log streams to a CFRM policy
AUILSTR2	JCL	JCL to add batch and online log streams to your CFRM environment
AUILSTR3	JCL	JCL to add DASD-only log streams to your LOGR environment
AUIMIG10	JCL	JCL used to assist in the upgrade from V9.0 to V10.1.3
AUIMLOG	JCL	JCL used to read the IMS RECONS, detect missing logs, and send notification to the Guardium system
AUIPING	REXX EXEC	EXEC used to determine the LPAR name, as found in the CVTSNAME field, and issue a PING to determine if the LPAR name is in the network DNS table
AUISMFDF	JCL	JCL sample, showing the creation of a GDG file base for SMF data collection
AUISMFDP	JCL	JCL sample, showing the use of program IFASMFDP to filter SMF record types
AUITCPD	JCL	JCL used to generate a network diagnostic report
AUIU*STC*	JCL	Common storage management utility address space JCL

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Agent environment

The agent must be running before you can use product functions related to the IMS subsystems monitored by that agent.

Important: Before the agent is started, system services should be started, and completely available for use. Examples of system services include JES, TCP/IP and the associated DNS RESOLVER, XCF, and the z/OS System Logger.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

APF authorization

For security, the agent must be APF-authorized before it can be run.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Agent job output

The primary output of the agent job consists of log messages written to the AUILOG DD. These messages provide status information about the ongoing operation of the agent, and also record additional messages if errors occur.

In the event of exceptional conditions, additional messages might be written to the SYSOUT DD. If an abend occurs, dump information can be written to the CEEDUMP and SYSUDUMP DDs, if they are supplied. That information can be used in diagnosis by product support.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Stopping the agent

When running on z/OS, the agent accepts standard z/OS /MODIFY and /STOP commands. When stopping the agent, all secondary address spaces controlled by the agent will also receive a stop request.

Important: System services, such as but not limited to the following, should remain available for use until the agent has completed termination: JES, TCP/IP and associated DNS RESOLVER, XCF and the z/OS System Logger.
From SDSF (or anywhere else that you can issue commands), you can issue one of these commands to the agent:

/STOP agent-job-name
: This is the recommended command to use to stop the agent. It initiates a graceful agent shutdown, which causes the agent to:

1. Wait for all existing requests to finish.
2. Exit.

/MODIFY agent-job-name,STOP
: Performs the same function as the /STOP agent-job-name command.

/MODIFY agent-job-name,FORCE
: This initiates an agent hard stop which causes the agent to:

1. Initiate hard cancels on all running threads.
2. Exit as soon as the threads exit.

Note: Use of the FORCE option can result in DUMP-producing ABENDS.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Starting and stopping the secondary address spaces

This topic describes the /MODIFY commands to start and stop the secondary address spaces.

Commands to start and stop the SMF data collector address space

When the agent address space is started, secondary address spaces under the control of the agent may also be started. These include the SMF data collector address space (SAUISAMP member AUIF*STC*) which collects events using SMF log data as input and sends the events to the Guardium appliance. One IMS Archive Log event Data collector (SAUISAMP member AUIL*STC*) is also started for each IMS with an active collection.

Note: The following commands should be used against the agent's primary address space.

- /MODIFY <jobname>,START COLLECTOR SMF
- /MODIFY <jobname>,STOP COLLECTOR SMF

Optionally, the STOP command may be used to stop the SMF address space:

- /STOP <jobname>

Commands to start and stop the IMS Archive Log Data collector

There is no z/OS command to start the address space because the IMS Archive Log data collector address space is specific to an IMS definition with an active collection. The AUIL*STC* address is started by the agent address space, or activation of a collection.

Stopping a specific AUIL*STC* address space requires the use of the /STOP <jobname>.<token> command. The <token> value to be used can be found during AUIL*STC* startup in the AGENT JOBLOG.

In the following example, AAAAAAAC is the token value:

```
/S AUILRS22.AAAAAAAC
```

Or, when viewing the AUIL*STC* task in TSO SDFS, the token is displayed as the STEPNAME.
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Data collection

The collection process involves the gathering of audit event data at run time. Specify various filtering criteria to capture all relevant events and limit the amount of data that is collected and stored.

IBM Guardium S-TAP for IMS gathers audited events from the following sources:

- IMS database DLI calls performed from within IMS Online Control regions and DLI/DBB batch jobs
- SMF records
- IMS Log records from IMS System Log Data Sets (SLDS).

A single policy containing selection criteria that indicates the events to be audited, is applied to each source.

- **IMS database DLI calls**
  IBM Guardium S-TAP for IMS can filter audit events generated by database DLI calls by the following call types: Read, Update, Insert, and Delete.
- **SMF records**
  IBM Guardium S-TAP for IMS allows the filtering of audit events generated by access methods outside of IMS DLI services, including z/OS access methods such as VSAM or QSAM requests generated from z/OS batch jobs or TSO.
- **Records from IMS system log data sets (SLDS)**
  IBM Guardium S-TAP for IMS allows the filtering of audit events that are generated by IMS Online Control regions, which are logged to IMS log data sets and are processed from within the AUIL*STC* started task.
- **Filtering stages**
  Stage 0, Stage 1, and Stage 2 filtering is available for Collector Agent audit event collection when processing DLI calls.
- **Policy pushdown**
  This topic describes the policy pushdown process of mapping policies to an IBM Guardium S-TAP for IMS collection profile.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

IMS database DLI calls

IBM Guardium S-TAP for IMS can filter audit events generated by database DLI calls by the following call types: Read, Update, Insert, and Delete.

Note: Database DLI calls that do not result in a DBPCB status code of blanks, GA, or GK, are not audited unless the IMS policy indicates that one or more non-blank DLI codes should be reported. DLI calls performed using an IOPCB or TPPCB are not audited.

Database DLI calls issued from specific PSBs and user IDs can be included or excluded from auditing. PSB names and user IDs can be specified for auditing using fully qualified names, or by using wildcard characters.

Further filtering can be performed by including or excluding specific database and segment names. Wildcard support is available for both the database and segment name.

When auditing IMS DLI calls, you can obtain the concatenated key value of segments that are audited for all or specific database DLI calls, as well as the segment data for UPDATE, and INSERT calls. The segment data can also be obtained for READ and UPDATE calls where these calls are logically linked in the Guardium appliance to provide a before and after image of updated segments.

Parent topic: Data collection

SMF records

IBM Guardium S-TAP for IMS allows the filtering of audit events generated by access methods outside of IMS DLI services, including z/OS access methods such as VSAM or QSAM requests generated from z/OS batch jobs or TSO.

Some IMS Database Batch Utilities access IMS databases using access methods other the IMS Database DLI calls. As a result, the source of auditing records for these batch jobs will be the SMF records produced.

These audit events are based on z/OS SMF records and are processed from within the AUIF*STC* agent subtask. Policy criteria input for SMF data auditing is the same as for IMS DLI calls, but because of the nature of the SMF data, it is used differently.

The following data is not relevant, and therefore not used:

- DLI calls types
- PSB names
- Segment names

Database names are relevant because SMF data is based on data set names (part of the process that converts a policy to a filter, examines the IMS RECON data sets for artifacts in the RECON which relate to the INCLUDED database). These artifacts include database data set names (DSG/AREA/ADS) and database image copy data sets for each database data set. The AUIF*STC* tasks also audit other IMS related data sets.

By default, these data sets have been included because changes to these data sets can have an effect on data integrity:

- IMS RECON data sets
- Logging data sets generated by IMS DLI/DBB batch jobs
- SLDS/RLDS data sets
- IMS Online log data sets (OLDS)

It is possible to ignore the auditing of these data set types, as well as the database image copy data sets, by adding a DUMMY DD statement to the AUIF*STC* JCL.
This table lists the data sets and corresponding DD DUMMY statement to include in the AUIFSTC JCL if you want to exclude the auditing of each of these types.

Table 1. Data sets and DD DUMMY statements

Data set Type	IMS RECONS	IMS LOGS	IMS OLDS	DB Image Copies
DD NAME	AUINRCN	AUINLOG	AUINOLD	AUINICS

Specify filtering of SMF events at the agent level, using access type or security violation, with the use of the SMF_AUDIT_LEVELS keyword in the configuration file. The keyword is pointed to by the AUICONFG DD statement of the agent (AUIA*STC*) JCL. Data set accesses to be audited are:

- OPEN for Read/Update
- Data set Alter/Create/Delete
- Any security product (such as RACF®) violations

The auditing of these accesses can be specified at the agent level (for example, all IMS systems defined to the agent), or at the IMS level. See the *Changing the type of events audited using SMF records* section for more details.

Parent topic: Data collection

Records from IMS system log data sets (SLDS)

IBM Guardium S-TAP for IMS allows the filtering of audit events that are generated by IMS Online Control regions, which are logged to IMS log data sets and are processed from within the AUIL*STC* started task.

Policy criteria input for IMS Log data auditing is the same as for IMS DLI calls, but is used differently because of the nature of IMS log data:

- DLI calls types are not relevant and therefore not used.
- Segment names are not relevant and therefore not used.
- PSB names are checked only when relevant to the event being examined.
- User IDs are checked only when relevant to the event being examined.
- DBD names are checked only when relevant to the event being examined.

In addition to filtering performed using the policy criteria, you can further filter IMS log data by event types, using the Guardium user interface. Using the IMSL_AUDIT_LEVELS keyword, you can set specific events to be audited, including:

- IMS Control Region Starts and Stops
- USER signon and signoffs
- Database OPEN/CLOSE
- DBD and PSB STARTS/STOPS/LOCK/UNLOCK

Occurrences of the DB DBDUMP command can also be audited. Auditing of these events can be specified at the agent level (for example, all IMS systems defined to the agent), or at the IMS level (for example, only for a specific IMS system). For more information, see *Changing the types of events audited using IMS SLDS records*.

Parent topic: Data collection

Filtering stages

Stage 0, Stage 1, and Stage 2 filtering is available for Collector Agent audit event collection when processing DLI calls.

Filtering occurs at one or more of the stages, 0, 1, and 2, depending on what fields are included in your filter. As many audit events as possible are filtered at the earliest possible stage (0, 1, or 2). You can control filtering performance by the fields you include in the rules for the active collection profile.

- **Stage 0 filtering**
  Stage 0 filtering occurs immediately after IMS executes the DLI call and it is determined that the call is a candidate for auditing, meaning one of the supported DLI call types and blanks, or another acceptable DLI status code, is returned.
- **Stage 1 filtering**
  Stage 1 filtering occurs through the use of USERID and PSB name values.
- **Stage 2 filtering**
  Stage 2 filtering occurs through the use of a filtering program that is compiled at the time of policy installation, using the criteria specified in the policy.

Parent topic: Data collection

Stage 0 filtering

Stage 0 filtering occurs immediately after IMS executes the DLI call and it is determined that the call is a candidate for auditing, meaning one of the supported DLI call types and blanks, or another acceptable DLI status code, is returned.

IBM Guardium S-TAP for IMS checks for an active policy for the IMS subsystem and determines if any rules governed by the active policy require the auditing of the DLI call type. If no policy is active, or no rules require the auditing of the DLI call type, processing control is returned to the application program. This is the most efficient form of filtering and should be used when possible.

Consider this example, wherein an active policy contains three rules:

- One rule only addresses INSERT requests.
- The second rule only addresses DELETE requests.
- The third rule only addresses UPDATE requests.

In this example, the READ DLI call is performed, and returns a status code of blanks. Since IBM Guardium S-TAP for IMS determines that no rules in the policy can reference a READ, processing control returns to the application program.

If the event that the DLI call performed in the example was an INSERT request, Stage 1 filtering would be invoked.

Parent topic: Filtering stages

Stage 1 filtering

Stage 1 filtering occurs through the use of USERID and PSB name values.

For Stage 1 filtering to occur, all rules of the active policy must contain identical USERID and PSB name values. Any inconsistencies in these values between rules prevents Stage 1 filtering from occurring.

Stage 1 filtering allows DLI calls that should be rejected, due to USERID or PSB name, to be excluded from the list of values to be audited. This can be due to the items not being included, or being intentionally excluded.

The determination that the USERID or PSB is causing the DLI call to be rejected is made by call to the Stage 2 compiled filters. The call to the Stage 2 complied filters is made when the USERID or PSB name of the current DLI call is not the same as the USERID or PSB name of the previous DLI call made in the same processing region.

In this example, the processing flow is demonstrated when discussing a BMP:

- The first DLI call is made and passes through Stage 0 processing.
- Stage 2 filtering is invoked, and it is determined that DLI calls from this USERID should not be audited. The DLI call is not audited, and control is returned to the application program.
- The next DLI call is made, and the USERID is the same as the previous DLI call in the region. The previous DLI call was not audited due to the USERID value, therefore this DLI call will not be audited.
- This process continues until the BMP STEP terminates with only one DLI call going through to Stage 2 filtering, and the remaining DLI calls are rejected during Stage 1 processing.

The same benefit can be seen with DLI and DBB batch jobs, because the USERID and PSB will not change during the execution step.

This process benefits online transactions and other processing threads where multiple DLI calls are performed from within a single unit-of-work, as well as when DLI calls are performed using C and D IMS command codes where multiple segments are affected by a single DLI call and auditing might be required on more than one segment within the hierarchical path.

Parent topic: Filtering stages

Stage 2 filtering

Stage 2 filtering occurs through the use of a filtering program that is compiled at the time of policy installation, using the criteria specified in the policy.

All DLI calls that are not rejected by Stage 0 and Stage 1 filtering are processed by the compiled filter. The compiled filter determines if the DLI call is to be audited based on all the policy criteria including DBD and segment name.

If the DLI call is to be audited, additional information is returned by the compiled filter, such as if the segment data and concatenated key should be included in the audited data block.

Parent topic: Filtering stages

Policy pushdown

This topic describes the policy pushdown process of mapping policies to an IBM Guardium S-TAP for IMS collection profile.

When the IBM Guardium S-TAP for IMS agent starts, it establishes a dedicated connection to the Guardium appliance for the reading of installed policies. Immediately after the connection is established, any installed policies are pushed down to the IBM Guardium S-TAP for IMS agent by the Guardium appliance. The Guardium appliance pushes down a full policy to all connected IBM Guardium S-TAP for IMS agents each time a policy is installed or uninstalled from the Guardium appliance.

Upon receipt of a policy, the IBM Guardium S-TAP for IMS agent compares the applicable rules with the existing collections, and performs a differential install.

Differential install
: A differential install of the policy indicates that only policies that have been modified since the last install are acted upon.

The following processing occurs in the IBM Guardium S-TAP for IMS agent upon receipt of a policy:

- The new policy is compared to the currently active policy if the new policy contains one or more rules.

    - If the policies are identical, no further processing is required.
- If the new policy does not apply to this subsystem, processing continues without any changes.
    - If there is an active policy, the collection continues using it.
    - If no policy is active, none is started.

Parent topic: Data collection

Creating and modifying IMS definitions

An IMS definition establishes a connection from your Guardium system to the IMS environment that you want to audit. To create and modify IMS definitions from the Guardium system interface, the agent address space (AUIA*STC*) must have a preestablished connection to the Guardium system.

- **Navigating to the IMS Definitions panel**
  IMS definitions can be created, modified, and deleted from the IMS Definitions panel of the Guardium system interface.
- **IMS Definition fields**
  The following fields are available in the IMS Definitions panel for your use in definition an IMS entry. Required fields are indicated with an asterisk.
- **IMSPLEX data sharing and XRF considerations**
  When you are considering IMS data sharing and XRF systems, take the following IMSPLEX data sharing and XRF considerations into account.
- **Adding an IMS definition**
  Add an IMS definition to the IMS Definitions List to include a defined IMS environment in the list of environments to be audited.
- **Modifying an IMS definition**
  You can modify the attributes that are set for an IMS definition on the IMS Definitions List.
- **Deleting an IMS definition**
  Delete an IMS definition from the IMS Definitions List to remove the IMS entry from the list of IMS environments to be audited.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Navigating to the IMS Definitions panel

IMS definitions can be created, modified, and deleted from the IMS Definitions panel of the Guardium system interface.

Procedure

1. From the Administration Console tab, select the Local Taps menu.
2. Select the IMS Definitions option.

Parent topic: Creating and modifying IMS definitions

IMS Definition fields

The following fields are available in the IMS Definitions panel for your use in definition an IMS entry. Required fields are indicated with an asterisk.

IMS Name

*IMS Entry Name
: A unique 1 - 8 character name to identify this IMS entry.

Description
: An optional description of the IMS Entry.

*Agent Name
: The name of the agent that audits this IMS entry.

RECONs

The RECON data set names are used to logically link the IMS definition, the active policy, the IMS Online Control region, and the DLI/DBB batch jobs that are running on z/OS, to audit the correct IMS instances.

*RECON1 Data Set Name
: The RECON1 data set name that is used by IMS on z/OS.

*RECON2 Data Set Name
: The RECON2 data set name that is used by IMS on z/OS.

RECON3 Data Set Name
: The RECON3 data set name that is used by IMS on z/OS.

IMS Data Sets

The IMS RESLIB data sets are used to determine the IMS release, during processing of the IMS System Log Data Sets (SLDS), using the AUIL*STC* address space. If more than one data set name is required, the data set names can be delimited by a comma.

*RESLIB Data Set Names
: A data set containing the IMS DFSVC000 module.

AUII050I Message Frequency
: Message AUII050I provides the number of DLI calls that are considered for auditing, and the number of DLI calls that were audited, based on the auditing criteria of the active policy. This message is produced based on the number of DLI calls that are considered, based on the following formula:

  Number of DLI calls in thousands (K) or Millions (M)

  or, by using both the formula and the time interval since the last AUII050I message was issued.

Example: If you provide values of `100K` (Number of DLI calls = 100,000) and `0100` (time interval of 1 hour), message AUII050I is issued when 100,000 DLI calls are seen by the product code, or by the 1 hour time interval, whichever comes first. The DLI counts and time interval reset when message AUII050I is issued.

Number of DLI calls
    xxx K|M
Time Interval
    HH:MM

Auditing Levels

Auditing levels can be set for both IMS Log and SMF events. For an explanation of the levels of auditing that are available for IMS Log and SMF events, see Configuration overview for a description of the IMSL_AUDIT_LEVELS and SMF_AUDIT_LEVELS configuration keywords.

IMS LOG Events
- Audit All IMS Log Events
- Audit Control Region Starts/Stops
- Audit User Signon/Signoff
- Audit DBD Open/Close
- Audit DBD/PSB/DUMP/START/STOP/LOCK/UNLOCK

SMF Events
- Audit All SMF Events
- Audit Dataset Open for Update
- Audit Dataset Deletes
- Audit Dataset Open for Read
- Audit Dataset Create
- Audit Dataset Alter
- Audit Dataset RACF® Violations

Parent topic: Creating and modifying IMS definitions

IMSPLEX data sharing and XRF considerations

When you are considering IMS data sharing and XRF systems, take the following IMSPLEX data sharing and XRF considerations into account.

IMSPLEX Data Sharing Considerations

Regardless of the number of LPARS that are involved, only one IMS definition is required in an IMS data sharing environment where all databases are shared by multiple IMS subsystems.

In an IMS data sharing environment where only a subset of databases is shared, an IMS definition must be created for each IMS subsystem with nonshared databases to be audited.

XRF Considerations

Only one IMS definition is required in an IMS XRF environment. IBM Security Guardium S-TAP for IMS on z/OS is not sensitive to which XRF partner is currently active. The product continues to produce audit data in the event of an XRF ACTIVE/BACKUP switch.

Parent topic: Creating and modifying IMS definitions

Adding an IMS definition

Add an IMS definition to the IMS Definitions List to include a defined IMS environment in the list of environments to be audited.

Procedure

1. From the IMS Definitions List, select the Add symbol, indicated by a plus sign, to the list of defined IMS systems.
   Enter the information in the IMS Definitions panel to define the new IMS environment to be audited.
2. Select Apply to save the new IMS definition.

Parent topic: Creating and modifying IMS definitions

Modifying an IMS definition

You can modify the attributes that are set for an IMS definition on the IMS Definitions List.

Procedure

1. Select the entry that you want to modify.
2. Modify the IMS definition fields.
3. Select Apply to save your changes.

Parent topic: Creating and modifying IMS definitions

Deleting an IMS definition

Delete an IMS definition from the IMS Definitions List to remove the IMS entry from the list of IMS environments to be audited.

About this task

IMS definitions can be deleted if no active IMS policies reference the IMS definition name. Only IMS definitions that are not part of an installed policy can be deleted.

Procedure

1. From the IMS Definitions List, select the IMS Definition that you want to delete.
2. Click the Delete icon.
   Click OK in the confirmation message to confirm the IMS entry deletion.

Parent topic: Creating and modifying IMS definitions

Reference information

This chapter provides IBM Guardium S-TAP for IMS reference information.

- **Data collection monitors**
  IBM Guardium S-TAP for IMS collects data from IMS online and batch activities, SMF, IMS archived logs, and IMS RECON data sets, by using the following internal product monitors.
- **IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS**
  The following tables show the IMS log types and SMF records types and descriptions that are collected by IBM Guardium S-TAP for IMS.
- **Fields that are used for IMS policy pushdown**
  The following fields defined in the Guardium system Access Rule Definition panel are used by IBM Guardium S-TAP for IMS to create policies and rules. Use the following information as a guideline.
- **Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS**
- **Echoed XML statement definitions**
  IBM Guardium S-TAP for IMS echoes the XML statements that are produced by the Guardium appliance to represent an Audit Policy. These statements are issued to a physical data set, agent AUILOG DD, or both, as determined by the XML_ECHO_DATASET and XML_ECHO_AUILOG parameters. This topic provides definitions of all XML statements that could be echoed from the appliance by the S-TAP.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Data collection monitors

IBM Guardium S-TAP for IMS collects data from IMS online and batch activities, SMF, IMS archived logs, and IMS RECON data sets, by using the following internal product monitors.

IMS Online Activity Monitor
: The IMS Online Activity Monitor interfaces with IMS DL/I Language call analyzer module (DFSDLA00), and the IMS/VS Fast-Path Inter-region Communications Controller module (DBFIRC10), in order to be sensitive to the DL/I call type, and to access the data that is necessary for producing an audited event. When an INIT call is made to the IMS logger Exit routine (DFSFLGX0), interfaces to the IMS modules are activated, and they remain active until the DFSFLGX0 routine receives a TERM notification.
  For the activity monitor to be recognized by the IMS Online region, the IMS control region must be stopped and restarted with the SAUIIMOD data sets included as the first data sets in the STEPLIB DD concatenation.
  The IMS Online Activity Monitor and the agent communicate data collection criteria by using E/CSA control blocks. Determination of which DL/I calls and databases/segments is made at the time the DL/I call is performed, by using information that is derived from the data collection policy that is created through the IBM Guardium system's Access Rule definition process.
  The z/OS System Logger transports the audit data from the IMS Online Activity Monitor to the agent. All IMS online systems that are controlled by an agent use the same z/OS System Logger log stream. This z/OS system log stream is unique to the agent, and only contains audited events from IMS Online regions.

IMS Batch Activity Monitor
: The IMS Batch Activity Monitor interfaces with IMS DL/I language call analyzer module (DFSDLA00) in order to identify the DL/I call type and data that is necessary to produce an audited event. When the IMS Batch Exit routine (DFSISVI0) is invoked, the interface with the DL/I call analyzer is activated, and remains active until the batch step terminates.
  The IMS Batch Activity Monitor and the agent use E/CSA control blocks to communicate data collection criteria. The DLI calls and databases/segments determination is made at the time the DL/I call is performed, by using information that is derived from the data collection policy, which is created on the IBM Guardium system. The audit data from the IMS Batch Data Collector to the agent is transported through the z/OS System Logger.
  All IMS batch jobs that are controlled by an agent use the same z/OS System Logger log stream. This z/OS system log stream is unique to the agent, and only contains audited events from IMS Batch jobs.

IMS Online and Batch Data Collectors
: The IMS Online and Batch Data Collectors run as separate threads under the control of the agent address space (AUIA*STC*). The function of the data collector is to read audited events from the z/OS System Logger log stream, and send the events to the IBM Guardium system for storage by using a TCP/IP connection.
  Each thread maintains its own persistent TCP/IP connection to the Guardium system.

SMF Data Collector
: The SMF Data Collector reads a subset of SMF records from SMF memory dump data sets to determine whether data sets associated with audited IMS artifacts were read, written, deleted, or renamed. Security violations against these data sets can also be reported.
  IMS artifact associated data set types include database data sets, database image copy data sets, IMS log data sets (OLDS, SLDS and RLDS), and RECON data sets. The list of IMS artifact data sets to be monitored during SMF data collection is derived from the data collection policy that is created through the IBM Guardium system.
  As the processing of the SMF data sets is deferred, the data collection policy in force at the time of the SMF data set READ is the collection policy used, not the data collection policy in effect when the SMF event occurred. The names of the SMF memory dump data sets to be read is based on one or more SMF data set MASK values that are supplied by the use of one or more SMF_DSN_MASK keywords in the agent configuration file (AUICONFG). The data set names to that the SMF MASK refers reflects the SMF memory dump data sets that are created during offloading of the SMF recording data sets, or a copy of these data sets containing a subset of SMF record types that are created explicitly for the use of this product.
  Because an agent can monitor SMF events from all LPARS within a SYSPLEX, all SMF data sets to be read must be accessible from the LPAR on which the agent runs. The SMF Data Collector periodically queries the z/OS catalog for new data set names that meet the SMF MASK value. When cataloged data sets are found, these data sets are dynamically allocated and read by the SMF Data Collector. Auditable events that are found are formatted, and sent to the IBM Guardium system by using a TCP/IP connection.

The SMF Data Collector creates and maintains its own TCP/IP connection to the IBM Guardium system. The frequency that the SMF Data Collector queries the z/OS catalog is determined by the option you set during configuration of this product. The SMF Data Collector can be configured to audit only a subset of events by use of available options when configuring the agent and defining the IMS appliance through the Guardium system interface. The SMF Data Collector is run as a started task under the control of the agent. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIF*STC* member.
Note: IBM Guardium S-TAP for IMS only reports audited events for SMF record types that are collected by SMF. If specific SMF record types are not collected by your appliance or SMF recording data set memory dump utility, the event cannot be reported. Refer to the IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS topic for a list of SMF record types that are used by IBM Guardium S-TAP for IMS.

IMS Archived Log Data Collector

The IMS Archived Log Data Collector reads IMS Archived Log data sets (SLDS) and provides audit information about the following actions:

- IMS user signon and signoff
- IMS online region starts and stops
- Changes to the status of DBDs and PSBS within the IMS Online environment

The list of IMS artifacts to be monitored during IMS Archived Log collection is derived from the data collection policy you create, by using the Guardium system. As the processing of the IMS Archived Log sets is deferred, the data collection policy in force at the time that the IMS Archived Log data sets are read is the collection policy used (as opposed to the data collection policy in effect when the IMS Archived Log event as written to the IMS log data set).
The IMS Archived Log Collector periodically queries the DBRC RECON data sets that are associated with an IMS that is defined to IBM Guardium S-TAP for IMS to determine if new SLDS data sets were created since the last RECON data set query. New data sets that are found are dynamically allocated and read. Audited events are sent to the IBM Guardium system by using a TCP/IP connection.
The IMS Archive Log Data Collector can be configured to audit only a subset of events, by using the options available when configuring the agent and defining the IMS appliance through the Guardium system interface. The IMS Archived Log Data Collector is run as a started task under the control of the agent. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIL*STC* member.
IBM Guardium S-TAP for IMS starts one AUIL*STC* task for each set of RECON data sets that is actively monitored with a data collection policy.

- If an IMS data sharing environment with five IMS subsystems that share a single set of RECON data sets exists, only one AUIL*STC* task is started.
- If two separate IMS subsystems by using two separate sets of RECON data sets are being monitored, two separate AUIL*STC* tasks are started.
  Note: To collect events from the IMS archived logs, the DFSSLOGP (Primary Output SLDS) data set must be created and cataloged by your IMS Log Archive Utility process (program DFSUARC0).

IBM Guardium S-TAP for IMS dynamically starts and stops the appropriate number of AUIL*STC* tasks as required.

IMS Missing Log Utility

The IMS Missing Log Utility analyzes IMS RECON data sets to confirm the existence of SLDS/RLDS data sets. This function can be included or excluded, as well as scheduled without regard to the execution cycle setting for the AUIL*STC* task. This utility is run by a job or started task (see SAUISAMP member AUIMLOG for an example). It processes the RECON data sets of IMS systems with active policies audited by the agent and pointed to by the configuration member that is defined in the AUICONFG DD statement in the AUIMLOG JCL. The IMS RECON data sets are analyzed in search of IMS SLDS and RLDS data sets. If these are found, the z/OS appliance catalog is queried by using the SLDS/RLDS data set name. If the SLDS/RLDS data set is not found, a missing log event is sent to the IBM Guardium system.
Note: The AUIMLOG utility must be run under the same user ID, and on the same LPAR, as the AUIA*STC* task.

Common Storage Management Utility

IBM Guardium S-TAP for IMS uses memory in E/CSA to provide information regarding active data collection policies to the IMS Batch and Online Activity Monitors. An IBM Guardium S-TAP for IMS agent can be called to monitor IMS Online regions or DL/I batch jobs on many LPARS within a SYSPLEX. A started task is generated for execution on all LPARS of a SYSPLEX to read all active data collection policies and build the appropriate E/CSA control blocks. This started task is run when the IBM Guardium S-TAP for IMS agent starts and stops, as well as when a change is made to the state of any collection policy. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIUSTC member.
The LPARs where the AUIU*STC* task is run might be limited by adding the AUIU_EXCLUDE_LPAR keyword and LPAR names to the configuration file, which is specified by the AUICONFG DD statement in the AUIA*STC* JCL.

Parent topic: Reference information

IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS

The following tables show the IMS log types and SMF records types and descriptions that are collected by IBM Guardium S-TAP for IMS.

Table 1. IMS Logtypes collected by IBM Guardium S-TAP for IMS

Log type number	IMS log type	IMS log type description
06	IMS/VS Accounting Record X'06'	IMS Online was started or stopped.
16	A /SIGN command was successfully completed.	A /SIGN command successfully completed.
20	A database was opened.	A database was opened.
21	A database was closed.	A database was closed.
4C	DB/PSB Activity	Activity that is related to database or PSB processing
59xx	DEDB ADS OPEN Log record	DEDB area data set was opened.
5922	DEDB ADS CLOSE Log record	DEDB area data set was closed.
5923	DEDB ADS STATUS Log record	DEDB area data set status was changed.

SMF is used to obtain additional data set activity that is related to the monitored IMS databases and image copies.

Table 2. SMF record types and descriptions

SMF record Number	Type
00	IPL record
14	INPUT or RDBACK data set activity
15	OUTPUT, UPDATE, INOUT, or OUTIN data set activity
17	Scratch data set status
18	Rename non-VSAM data set
30	Common address space work, accounting information
60	VSAM volume data set updated
61	ICF catalog entry define

SMF record Number	Type
62	VSAM component or cluster opened
65	ICF delete activity
66	ICF alter activity
80	RACF® operator record
89	Usage data

Note: When image copies are read, they are collected as SMF type 14. When image copies are written, they are collected as SMF type 15. Image copies are sequential files, with some exceptions. If the image copy is opened as a VSAM file, the image copy is collected as SMF type 60.
Remember: IBM Guardium S-TAP for IMS can only report events that are being collected by SMF. If an SMF record type in this table is not being collected at your site, IBM Guardium S-TAP for IMS cannot report that event.
Parent topic: Reference information

Fields that are used for IMS policy pushdown

The following fields defined in the Guardium system Access Rule Definition panel are used by IBM Guardium S-TAP for IMS to create policies and rules. Use the following information as a guideline.

Table 1. Fields that are used for IMS Policy pushdown

Label	Hover text
Service Name	IMS names to which this rule applies (case sensitive)
Application User	INCLUDE/PSB or EXCLUDE/PSB
Database User	INCLUDE/USERID or EXCLUDE/USERID
Object	INCLUDE/read+update+delete+insert+data+image/DBNAME.SEGNAME or EXCLUDE/DBDNAME.SEGNAME

Service name/IMS name
: Required.
Must be 1 -- 8 characters.
Mixed case is allowed, and field is case sensitive.
Wildcard characters are not allowed.

Application user/PSB
: Must be 1 -- 8 characters.
All typed characters should be folded to uppercase.
Supports % as a wildcard character. % matches zero or more characters.
Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

Database user/User ID
: Must be 1 -- 8 characters.
All typed characters should be folded to uppercase.
Supports % as a wildcard character. % matches zero or more characters.
Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

Object/Target DB/Segment
: database_name must be 1 -- 8 characters.
segment_name must be 1 -- 8 characters.
wildcard_pattern supports % as a wildcard character. % matches zero or more characters.
All typed characters should be folded to uppercase.
Note: You must specify at least one INCLUDE with at least one DLI call type. DBD and segment must also be specified.

DLI Call Code
: Used to generate audit records for DLI calls that result in a non-blank status codes. Non-blank status codes can indicate that the DLI call failed or completed with a warning.
The following DLI status codes can be audited:

- FD
- FW
- GA
- GB
- GD
- GE
- GK
- L2
- LB
- LS
- NI
- UC
- US
- UX

You can specify one or more DLI status codes.
For more information about DLI status codes, see the About DLI status codes information in the IBM Knowledge Center.

Audit
: Used to limit the types of DLI calls to be audited.
NOHLVL causes audit information to be collected for only the target segment of a DLI Patch call (Command code C or D) instead of generating audit data for each segment of the hierarchical path. This can reduce the volume of audited data that is sent to, and stored by, the Guardium appliance in cases where the target segment concatenated key is sufficient for auditing purposes.

LTERM Filtering
: Must be 1 -- 8 characters.
All typed characters should be folded to uppercase.
Supports % as a wildcard character. % matches zero or more characters.
Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

By default, auditing is considered for any DLI call that has a blank/null LTERM (for example, from a BMP or other region type that does not present IMS with an LTERM value). When an LTERM value or a group of LTERMs is specified, an option box is presented to enable you to turn off BLANK LTERM auditing. Turning off BLANK LTERM auditing does not affect the auditing of BMPs; any other region types without an LTERM value are excluded from auditing.

Filtering DLI calls from specific IMS Region types

You can filter out DLI calls from specific IMS Region types. DLI calls that originate from one or more of these region types can be excluded from auditing consideration:

- AER
- BMP
- CICS
- DBCTL
- IFP
- MPP
- ODB

In the Guardium interface, click the pencil icon alongside the Region Types to Exclude field to open a set of check-boxes that enable you to remove regions from auditing

Parent topic: Reference information

Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

This section details the process of sizing the z/OS System Logger Log Streams. The z/OS System Logger Log Stream is used to transport audited DLI call data from the IMS control region or DLI/DBB batch jobs to the IBM® Guardium® S-TAP® for IMS agent (AUIAxxxx address space) where it is reformatted to a PROTOBUF protocol and sent to the target Guardium appliance.

- **Calculating the Optimal Log Stream Size**
  Filtering by using the IMS POLICY from the Guardium appliance occurs in the IMS Control region, therefore only DLI calls that are to be audited are written to the log stream(s).
- **Considerations**
  There are several variables that must be considered when sizing the log stream(s), including:
- **Using IBM Documentation**
  The System Logger Performance and Tuning section of the System Programmer's Guide to: z/OS System Logger provides a detailed description of the processes that are needed to tune the System Logger for use with IBM Guardium S-TAP for IMS and other products.
- **Pertinent Report Fields**
  Some key fields provided in the System Logger Activity Report (IXGRPT1) are the BYT WRITTN TO INTERIM STORAGE, BYT WRITTN TO DASD, and STRUC FULL.
- **Additional Resources**
  IBM provides a spreadsheet utility to assist in the analysis of the log stream SMF88 data and provide suggestions on how to define the log stream for more efficient use in your environment.

Parent topic: Reference information

Calculating the Optimal Log Stream Size

Filtering by using the IMS POLICY from the Guardium appliance occurs in the IMS Control region, therefore only DLI calls that are to be audited are written to the log stream(s).

For most users, the size of the log stream that is provided with the LS_SIZE parameter of the AUILSTR2/3 log stream definition member (LS_SIZE(100)) is appropriate to use when auditing accesses to sensitive data or when auditing DLI calls performed by a group, or groups, of users who have access to all databases for diagnostic purposes.

There might be instances where an LS_SIZE parameter value of 13500 (LS_SIZE(13500)) might be used, such as:

- during product testing, or
- when the number of audited DLI calls exceed twenty-five thousand DLI calls per second, or
- when the audited DLI calls include large concatenated key or large segment fields, which can occur when the IMS POLICY includes the `+DATA` keyword in the TARGET/DB INCLUDE filter statement

Note: Log stream sizing can be an iterative process. When attempting to audit many DLI calls, the CPU, memory, and disk storage capacity of the Guardium appliance should be considered.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Considerations

There are several variables that must be considered when sizing the log stream(s), including:

- the number of IXGWRITEs that are performed every second
- the average number of bytes written, or average buffer size written with each IXGWRITE calls
- the rate that the data is offloaded from the log stream
- the number/rate of IXGDELETEs that are performed

The average number of IXGWRITEs that are performed and the average number of bytes/average buffer size is determined by the volume of audited DLI calls and the size of the DLI call event data that is being captured.

IBM® Guardium® S-TAP® for IMS uses a set of 35K buffers to hold the audited DLI call data. Each buffer is written to the log stream when it fills to capacity, or every five seconds. The time interval is used to ensure that audited DLI call data is sent to the Guardium appliance in a timely manner. Therefore, the frequency of IXGWRITEs can vary greatly depending on the IMS Policy and databases that are being accessed.

The log stream offload process IBM Guardium S-TAP for IMSis performed by the agent address space (AUIAxxxx). The agent address space constantly polls the log stream (once per second) looking for new data to process. When new data is found, the data is read by using the IXGBRWSE call. The data is formatted into a PROTOBUF protocol and sent to the Guardium appliance by using TCP/IP. The IBM Guardium S-TAP for IMS agent will continually read and process log stream data until no new data exists, at which time, polling every second will reoccur.

The log stream data is deleted by using the IXGDELETE call after every three blocks of data are successfully read and sent to the Guardium appliance. This ensures that audited data is not lost in the event of a communication loss between the IBM Guardium S-TAP for IMS agent and the Guardium appliance.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Using IBM Documentation

The System Logger Performance and Tuning section of the System Programmer's Guide to: z/OS System Logger provides a detailed description of the processes that are needed to tune the System Logger for use with IBM® Guardium® S-TAP® for IMS and other products.

You can perform an analysis of the performance and efficiency of the initial log stream size by running program IBM program IXGRPT1 and JCL IXGRPT2 found in 'SYS1.PROCLIB'. This program uses the SMF88 records to help with log stream capacity planning.

SMF88 records can be collected by z/OS by providing the 88 value in the SMPRM parmlib member prior to a system IPL, or by using the z/OS command, "SET SMF=xx" (where xx is the suffix of the parmlib member).

Example:

```
SYS(TYPE(30,70:79,88,89,100,101,110)),
```

The IXGRPT1 utility will assemble sub-routine IXGRA1 and compile and link program IXGRPT1, which can be used to extract SMP88 records in preparation for analysis.

The IXGRPT2 JCL can be used to produce other SMP88/log stream reports.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Pertinent Report Fields

Some key fields provided in the System Logger Activity Report (IXGRPT1) are the BYT WRITTN TO INTERIM STORAGE, BYT WRITTN TO DASD, and STRUC FULL.

BYT WRITTN TO INTERIM STORAGE

The BYT WRITTN TO INTERIM STORAGE value (bytes written to interim storage) indicates the amount of data being written to the log stream during the SMP interval. This value can provide insight as to the volume of data being written to the log stream.

BYT WRITTN TO DASD

The BYT WRITTN to DASD value (bytes written to DASD offload data sets) indicates the number of bytes that were written to the DASD offload/overflow VSAM data sets.

This number indicates that the interim storage filled up, and in order to retain the data, a set of VSAM files are being used as overflow buffers. This number can rise and fall during the day as the volume of audited DLI calls increase and decrease.

Some use of the overflow VSAM files can be acceptable because spikes in audited DLI call data can certainly be expected due to the nature of IMS POLICY filtering. However, constant or extensive use of the VSAM overflow files indicate that the log stream should be sized larger.

STRC FULL

The STRC FULL (Structure Full) value indicates the number of times that the capacity of the CF structure was filled up without an offload occurring. This number should be zero in a properly sized log stream. Structure such as this can indicate that the volume of data written exceeds the offload capability of the IMS STAP agent to read, process, and delete audited data, and a larger structure size should be considered.

An abundance of Structure Full conditions will result in a degradation of performance when collecting audited DLI call data, and if not rectified, might result in data loss. This condition might result in IXGWRITE 0866 errors being issued in the IMS Control region address space.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Additional Resources

IBM provides a spreadsheet utility to assist in the analysis of the log stream SMF88 data and provide suggestions on how to define the log stream for more efficient use in your environment.

You can access the spreadsheet utility with the following link: ftp://www.redbooks.ibm.com/redbooks/SG246898. Read the disclaimer.txt file before using the tool.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Echoed XML statement definitions

IBM® Guardium® S-TAP® for IMS echoes the XML statements that are produced by the Guardium appliance to represent an Audit Policy. These statements are issued to a physical data set, agent AUILOG DD, or both, as determined by the XML_ECHO_DATASET and XML_ECHO_AUILOG parameters. This topic provides definitions of all XML statements that could be echoed from the appliance by the S-TAP.

XML convention

Start of tag data

=<*tag_name*>
End of tag data
=</*tag_name*>
Null/empty tag
=<*tag_name*/>

See Sample XML file for an example of the XML representation of a valid policy.

IMS-specific statements

Table 1. IMS-specific XML statements

XML statement	Definition
<install-info>	Beginning of relevant policy information.
<artifacts>	Start of IMS definitions.
<ims>	Start of individual IMS-specific information.
<name>	Name of IMS as specified in the Guardium appliance policy.
<agent>	Name of the agent to which IMS is connected.
<description>	Appliance IMS description text.
<version>	Currently a value of zero (0).
<plexname>	Not populated.
<recons>	Start of the IMS-specific RECON data set list.
<recon seq="1">	RECON1 data set name. DSN terminated by </recon>.
<recon seq="2">	RECON2 data set name. DSN terminated by </recon>.
<recon seq="3">	RECON3 data set name. DSN terminated by </recon>.
<reslibs>	Start of IMS-specific RESLIB data sets.
<reslib seq="1">	RESLIB 1 in IMS STEPLIB concatenation. DSN terminated by </reslib>.

Log-specific statements

Table 2. Log-specific XML statements

XML statement	Definition
<dbdlibs/>	Not populated.
<psblibs/>	Not populated.
<thresholds-050i>	Start of message AUII050I message frequency parameters.
<max-count>	Number of DLI calls needed to prompt message AUII050I.
<max-time>	Max time interval (HHMM) between AUII050I messages.
<audit-levels>	Start of IMS Logger and SMF auditing criteria.
<collector name="ims">	Start of IMS Logger auditing criteria. Terminated by </collector>.
<audit-level>	Start of audit level criteria.
<signon-signoff value="true"/>	Audit IMS user sign-ons and sign-offs.
<signon-signoff value="false"/>	Do not audit IMS user sign-ons and sign-offs.
<start-stop value="true"/>	Audit IMS Control Region starts and stops.
<start-stop value="false"/>	Do not audit IMS Control Region starts and stops.
<db-open-close value "true"/>	Audit DBD Opens and Closes.
<db-open-close value "false"/>	Do not audit DBD Opens and Closes.
<dbd-psb value="true/"	Audit DBD/PSB/Dump/Start/Stop/Lock/Unlock
<dbd-psb value="false/"	Audit DBD/PSB/Dump/Start/Stop/Lock/Unlock

SMF-specific statements

Table 3. SMF-specific XML statements

XML statement	Definition
<collector name="smf">	Start of SMF auditing criteria. Terminated by </collector>.
<audit-level>	Start of audit-level criteria.
<read value="true"/>	Audit data sets when they are opened with READ intent.
<read value="false"/>	Do not audit data sets when they are opened with READ intent.
<update value="true"/>	Audit data sets when opened with UPDATE intent.
<update value="false"/>	Do not audit data sets when opened with UPDATE intent.
<delete value="true"/>	Audit data set DELETEs.
<delete value="false"/>	Do not audit data set DELETEs.
<create value="true"/>	Audit data set CREATEs.
<create value="false"/>	Do not audit data set CREATEs.
<alter value="true"/>	Audit VSAM data set ALTERs.
<alter value="false"/>	Do not audit VSAM data set ALTERs.
<racf-violations value "true"/>	Audit RACF security violations against data sets.
<racf-violations value "false"/>	Do not audit RACF security violations against data sets.

Policy-specific statements

Table 4. Policy-specific XML statements

XML statement	Definition

XML statement	Definition
<policies>	Start of policy information.
<collection-profile>	Displays the rules defined to the policy. The collection profile policy name appears in the collection-specific statement <collection> for a given <ims>.
<name>	Policy name. Naming convention is: *policy_IMS_name*.
<description>	Concatenation of descriptions of all policies pushed to the appliance.
<rules>	Start of individual policy rules.
<rule>	Start of rule instance.
<active>	Always a value of true.
<filters>	Start of PSB/USERID/LTERM INCLUDES/EXCLUDES within the rule.
<psb-filter>	PSB instance.
<name>	Name of PSB to be audited or ignored.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).
<lterm-filter>	LTERM instance.
<name>	LTERM to be audited or ignored.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).

Database/segment-specific statements

Table 5. Database/segment-specific XML statements

XML statement	Definition
<targets>	Start of DBD/SEGMENT instances within the rule.
<segment-target>	Start of list of databases/segments to be INCLUDED/EXCLUDED.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).
<database-name>	Database to be audited or ignored.
<segment-name>	Segment to be audited or ignored.
<audit-get>	INCLUDE DLI GET calls.
<audit-insert>	INCLUDE DLI INSERT calls.
<audit-update>	INCLUDE DLI UPDATE (REPL) calls.
<audit-delete>	INCLUDE DLI DELETE (DLET) calls.
<capture-before-image>	INCLUDE link between DLI GH and DLI REPL calls.
<capture-segment-data>	INCLUDE segment data when segment is audited.
<hlvl-filter enabled="false">	Do not report hierarchical parent segment during DLI command calls.
<excluded-regions>	Do not audit DLI calls from these region types.

Collection-specific statements

Table 6. Collection-specific XML statements

XML statement	Definition
<collections>	A grouping of the individual <collection> XML tags.
<ims>	IMS name connection to the collection.
<agent-name>	Agent name connection to the collection.
<name>	IMS name connection to the collection.
<collection-profile>	For each agent name and IMS name, IBM Guardium S-TAP for IMS establishes a connection to the collection profile.
<name>	Constructed name of the policy (*policy_IMS_NAME*).
<dli-status-codes>	Two-character DLI status codes to be audited. Terminated by FF value.

Quarantine information

Quarantine XML is only sent from the appliance when the quarantine is triggered by audited events that are sent to the appliance by the agent, and the quarantine is deemed to be in effect. This causes AI status codes (error opening database) to be returned to the application program in the DLI Status code PCB field (DBPCBSTC), and message AUIJ252W to appear in the IMS region or batch job.

Quarantine only works with full-function DLI calls because the AUI hook for Fast-Path occurs after the DLI call has completed. (The DLI call cannot be preempted.)

Table 7. Quarantine-specific XML statements

XML statement	Definition
<quarantine-lists>	Start of quarantine section.
<quarantine-list agent-name="*xxxxxxxx*" ims-name="*yyyyyyyy*"> >	Agent and IMS name are affected.
<quarantine-item>	Start of quarantine details.
<start-ts>yyyy-mm-dd-hh.mm.ss.000000	Quarantine start date/time.
<end-ts>yyyy-mm-dd-hh.mm.ss.000000	Quarantine end date/time.
<user-id>	User ID to be quarantined.

- **Sample XML file**
  This is an example of a valid audit policy.
- **Additional causes of AUIA060W**
  Warning message AUIA060W can appear if the data set location is incorrect. Review these additional possible causes of the message if the explanation and recommendation provided by AUIA060W do not resolve the warning.

Parent topic: Reference information

Sample XML file

This is an example of a valid audit policy.

```
<install-info>
  <artifacts>
    <ims>
      <name>IMSV14AH</name>
      <agent>AUI15A</agent>
      <description>IMS V14 Test IEACRX AUI10A27</description>
      <version>0</version>
      <plexname></plexname>
      <recons>
        <recon seq="1">IMSEA1.RECON1</recon>
        <recon seq="2">IMSEA1.RECON2</recon>
        <recon seq="3">IMSEA1.RECON3</recon>
      </recons>
      <reslibs>
        <reslib seq="1">IMSEA1.SDFSRESL</reslib>
      </reslibs>
      <dbdlibs/>
      <psblibs/>
      <thresholds-050i>
        <max-count>1K</max-count>
        <max-time>0015</max-time>
      </thresholds-050i>
      <audit-levels>
        <collector name="ims">
          <audit-level>
            <signon-signoff value="true"/>
            <start-stop value="true"/>
            <db-open-close value="true"/>
            <dbd-psb value="true"/>
          </audit-level>
        </collector>
        <collector name="smf">
          <audit-level>
            <read value="true"/>
            <update value="true"/>
            <delete value="true"/>
            <create value="true"/>
            <alter value="true"/>
            <racf-violations value="true"/>
          </audit-level>
        </collector>
      </audit-levels>
    </ims>
  </artifacts>
  <policies>
    <collection-profile>
      <name>policy_IMSV14AH</name>
      <description>---: Log Full Details With Values,Auv - Event All,IEA1_ALL_ST_AH</description>
      <rules>
        <rule>
          <active>true</active>
          <filters/>
          <targets>
            <segment-target>
              <type>include</type>
              <database-name>%</database-name>
              <segment-name>%</segment-name>
              <audit-get>true</audit-get>
              <audit-insert>true</audit-insert>
              <audit-update>true</audit-update>
              <audit-delete>true</audit-delete>
              <capture-before-image>false</capture-before-image>
              <capture-segment-data>true</capture-segment-data>
            </segment-target>
          </targets>
          <audit/>
          <excluded-regions></excluded-regions>
        </rule>
      </rules>
    </collection-profile>
  </policies>
  <collections>
    <collection>
      <ims>
        <agent-name>AUI15A</agent-name>
        <name>IMSV14AH</name>
      </ims>
      <collection-profile>
        <name>policy_IMSV14AH</name>
      </collection-profile>
      <dli-status-codes>FDFWGAGBGDGEGKL2LBLSNIUCUSUXFFFF</dli-status-codes>
    </collection>
  </collections>
  <quarantine-lists/>
</install-info>
```

Parent topic: Echoed XML statement definitions

Additional causes of AUIA060W

Warning message AUIA060W can appear if the data set location is incorrect. Review these additional possible causes of the message if the explanation and recommendation provided by AUIA060W do not resolve the warning.

Data set: <LOCATION> in use

Explanation
: An attempt to dynamically allocate the data set failed because the data set was in use by another process. This warning might be temporary. The agent retries the data set 6 times in 3 seconds before skipping the policy XML echoing.

Response
: If this message occurs several times without successful policy XML echoes, check to see that any running user report program is using the data set correctly or whether a TSO user might be editing the data set.

A dynamic allocation error occurred. Data set <LOCATION>, info code: <info-code>, error code: <error-code>.

Explanation
: An attempt to dynamically allocate the data set failed. The specified information and error codes reflect the return and reason codes from the z/OS dynamic allocation services.

Response
: Use the info code and error code to determine the cause of the dynamic allocation failure by referring to the *z/OS MVS Programming: Authorized Assembler Services Guide* in the IBM Knowledge Center. Correct the error and restart the agent.

Catalog Search Interface: error RC = <rc>, RSN = <rsn>.

Explanation
: Using the z/OS Catalog Search Interface routine, the agent attempted to analyze whether the data set is a Generation Data Group (GDG) data set or a non-VSAM data set. An error occurred while calling the routine.

Response
: Consult the *Return Codes for General Purpose Register 15* section of the *IBM Catalog Search Interface User's Guide* in the IBM Knowledge Center. Contact IBM Support if additional assistance is needed.

Data set "<LOCATION>" could not be deleted, info code: <code>, error code <code>.

Explanation
: An attempt was made to delete and reallocate a non-VSAM non-GDG data set in the catalog.

Response
: Ensure that the agent task has RACF (or other security product) authority to delete a data set that contains a high-level qualifier. Attempt to correct the security problem and restart the agent. If the error persists, contact IBM Support and provide the info and error codes.

XML echo data set <LOCATION> is of an unsupported type

Explanation
: Only non-VSAM and GDG base data sets are supported.

Response
: Ensure that the data set type is either a non-VSAM data set or a Generation Data Group. Restart the agent.

Parent topic: Echoed XML statement definitions

Troubleshooting

Use the following topics to diagnose and correct problems that you experience with IBM Guardium S-TAP for IMS.

- **Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS**

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

This information documents the messages and error codes issued by Security Guardium S-TAP for IMS. Messages are presented in ascending alphabetical and numerical order.

Note: To set a z/OS message alert for messages that begin with AUII, or messages AUIJ250I and AUIJ252W, use single-dash formatting between the message number and message text. For all other messages, use a double-dash. For example:

AUIT031I--Starting the command listener thread
: Format most message alerts with double-dashes between the message number and message text.

AUII056I - ZIIP PROCESSING ENABLED FOR IMS STAP
: Format message alerts for AUII*, AUIJ250I, and AUIJ252W with a single dash between the message number and message text.

- **Error messages and codes: AUIAxxxx**
- **Error messages and codes: AUIBxxxx**
- **Error messages and codes: AUIFxxxx**
- **Error messages and codes: AUIGxxxx**
- **Error messages and codes: AUIIxxxx**
- **Error messages and codes: AUIJxxxx**

- **Error messages and codes: AUILxxxx**
- **Error messages and codes: AUIPxxxx**
- **Error messages and codes: AUIRxxxx**
- **Error messages and codes: AUITxxxx**
- **Error messages and codes: AUIUxxxx**
- **Error messages and codes: AUIXxxxx**
- **Error messages and codes: AUIYxxxx**
- **Error messages and codes: AUIZxxxx**

Parent topic: Troubleshooting

Error messages and codes: AUIAxxxx

The following information is about error messages and codes that begin with AUIA.

- **AUIA003E**
  Address Space *<name>* failed to start successfully on *<LPAR name>*.
- **AUIA004E**
  Address Space *<name> (<job number>)* failed to stop successfully on *<LPAR name>* within the timeout period and was abandoned.
- **AUIA005I**
  Starting address space *<name>* on *<LPAR name>*.
- **AUIA006I**
  Address Space *<name> (<job number>)* is online on *<LPAR name>*.
- **AUIA007I**
  Stopping address space *<name> (<job number>)* on *<LPAR name>*.
- **AUIA008I**
  Address Space *<name> (<job number>)* on *<LPAR name>* is offline.
- **AUIA009E**
  Address space *<name>* is not active.
- **AUIA010E**
  Address Space *<name>* is already active.
- **AUIA021I**
  MODIFY command *<command text>* sent to Address Space *<name>*.
- **AUIA022I**
  <Collector name> collector is disabled: interval is set to *<value>*.
- **AUIA023I**
  <Collector name> collector is disabled: proc name for the collector address space has not been specified in the configuration.
- **AUIA024I**
  <Collector name> collector is disabled: not configured.
- **AUIA027E**
  Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN = *<reason>*.
- **AUIA028S**
  Agent *agent-name* on *PLEX name* for S-TAP version *S-TAP version* is already online. *(ADS_SHM_ID=<Memory Segment ID>)*
- **AUIA029I**
  collector collector is disabled: no Audit IMS Log Events are selected for IMS source *IMS*.
- **AUIA030I**
  collector collector started successfully.
- **AUIA031I**
  collector collector stopped successfully.
- **AUIA033I**
  (GDM) Attempting to establish link with the appliance.
- **AUIA034S**
  (GDM) An attempt to establish the link to the appliance failed.
- **AUIA035W**
  (GDM) Link failed over to a secondary appliance. [host=*host*, port=*port*]
- **AUIA036I**
  (GDM) Link to primary appliance established. [host=*host*, port=*port*]
- **AUIA037I**
  (GDM) Link to primary appliance restored. [host=*host*, port=*port*]
- **AUIA038S**
  (GDM) Link to the appliance lost.
- **AUIA041I**
  Guardium policy processing failed due to prior errors.
- **AUIA042W**
  The Guardium policy is not applicable.
- **AUIA043I**
  The Guardium policy reader thread started.
- **AUIA044I**
  The Guardium policy reader thread is terminating.
- **AUIA045I**
  The guardium policy reader thread is terminating due to prior errors.
- **AUIA048I**
  auiu_taskname is configured to start only on *lpar-name*.
- **AUIA049W**
  auiu_task_name is configured to not start on *lpar_name* but will be started on *lpar_name* because *aui_agent_name* runs on *lpar_name*
- **AUIA050W**
  auiu_task_name is configured to not start on *lpar_name* but no such system exists.
- **AUIA051I**
  auiu_task_name is configured to not start on *lpar_name* and will not be started on *lpar_name*.

- **AUIA052I**
  Discovered <plex-name> system <system-name>.
- **AUIA053I**
  Agent configuration option *<option>* has been updated to *<value>*.
- **AUIA054I**
  Agent configuration option *<option>* is set to *<value>*.
- **AUIA055I**
  The agent is waiting for start-up information from the appliance.
- **AUIA056I**
  Starting the agent collectors.
- **AUIA057I**
  Issuing request to capture agent status.
- **AUIA058I**
  Request to capture agent status has completed successfully.
- **AUIA059I**
  Policy XMl echo
- **AUIA060W**
  Policy XML echo to data set skipped: *<MESSAGE> <LOCATION>*
- **AUIA061I**
  Policy XML echo to data set *<LOCATION>* completed.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIA003E Address Space *<name>* failed to start successfully on *<LPAR name>*.

Explanation

An attempt by the agent to start the named support address space has failed.

User response

Check the named address space logs to identify why it was not able to start. In most cases, this occurs if an address space with that name is already online, there was a JCL error, or there was an issue resolving the loopback address host name. If further assistance is required, contact IBM Software Support.

Parent topic: Error messages and codes: AUIAxxxx

AUIA004E Address Space *<name> (<job number>)* failed to stop successfully on *<LPAR name>* within the timeout period and was abandoned.

Explanation

The specified address space did not stop within the time out period and was consequently abandoned by the master address space.

User response

Check the named address space logs to identify why it did not stop. If further assistance is needed, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA005I Starting address space *<name>* on *<LPAR name>*.

Explanation

The agent has automatically started the support address named.

User response

This is an informational message only.
Parent topic: Error messages and codes: AUIAxxxx

AUIA006I Address Space *<name> (<job number>)* is online on *<LPAR name>*.

Explanation

The agent has successfully started the support address space named.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA007I Stopping address space *<name> (<job number>)* on *<LPAR name>*.

Explanation

The agent has automatically stopped the support address space named.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA008I Address Space *<name> (<job number>)* on *<LPAR name>* is offline.

Explanation

The named address space has successfully stopped.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA009E Address space *<name>* is not active.

Explanation

The specified address space that the master address space was attempting to control is not online.

User response

Correct and retry.

Parent topic: Error messages and codes: AUIAxxxx

AUIA010E Address Space *<name>* is already active.

Explanation

This message indicates that the address space with the specified name is active already and was expected to be. This message occurs when starting the BATCH (or SMF) collector if they are already running.

User response

Verify that the address space is already running. If the address space is not online and the message occurs, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA021I MODIFY command *<command text>* sent to Address Space *<name>*.

Explanation

The MODIFY command *<command text>* sent to address space named.

User response

No action is required.

Parent topic: Error messages and codes: AUIAxxxx

AUIA022I *<Collector name>* collector is disabled: interval is set to *<value>*.

Explanation

Named collector is disabled because the interval value is less than or equal to zero.

User response

If this was not intentional, fix the interval value and restart the agent address space.

Parent topic: Error messages and codes: AUIAxxxx

AUIA023I *<Collector name>* collector is disabled: proc name for the collector address space has not been specified in the configuration.

Explanation

The specified collector is disabled because the procedure name for the collector address space has not been specified in the configuration.

User response

To enable this collector, specify the procedure name for collector address space. If the procedure name is specified and this message still occurs, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA024I *<Collector name>* collector is disabled: not configured.

Explanation

The specified collector is disabled because it has not been configured.

User response

To enable this collector, configure it using the Guardium user interface. If the specified collector is configured and the message still occurs, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA027E Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN = *<reason>*.

Explanation

The Log Stream *log stream* validation failed with abend code *code* and reason code *reason*.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA028S Agent *agent-name* on *PLEX name* for S-TAP version *S-TAP version* is already online. *(ADS_SHM_ID=<Memory Segment ID>)*

Explanation

The specified agent is already online. Agent names must be unique per sysplex.

User response

Change the *agent-name* and restart the agent, or shut down the other agent.
Parent topic: Error messages and codes: AUIAxxxx

AUIA029I *collector* collector is disabled: no Audit IMS Log Events are selected for IMS source *IMS*.

Explanation

An Audit IMS Log Event must be selected for the IMS source *IMS* for the collector to be enabled.

User response

To enable the collector, select an Audit IMS Log Event for the IMS source.
Parent topic: Error messages and codes: AUIAxxxx

AUIA030I *collector* collector started successfully.

Explanation

The specified collector started.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA031I *collector* collector stopped successfully.

Explanation

The specified collector stopped.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA033I (GDM) Attempting to establish link with the appliance.

Explanation

The agent is attempting to establish a connection to one of the appliances specified in the agent configuration.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA034S (GDM) An attempt to establish the link to the appliance failed.

Explanation

The agent could not establish a connection to any of the appliances specified in the configuration.

User response

Contact your network administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA035W (GDM) Link failed over to a secondary appliance. [host=*host*, port=*port*]

Explanation

The agent lost connection to the primary appliance and switched to the specified secondary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA036I (GDM) Link to primary appliance established. [host=*host*, port=*port*]

Explanation

The agent has connected to the specified primary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA037I (GDM) Link to primary appliance restored. [host=*host*, port=*port*]

Explanation

The agent has reconnected to the specified primary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA038S (GDM) Link to the appliance lost.

Explanation

All attempts to connect to the appliances specified in the configuration have failed.

System action

Any new policies defined in the appliance will not be pushed down to the IBM® Guardium® S-TAP® for IMS agent.

User response

Verify network connectivity to the appliance. Contact your network administrator or IBM Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA041I Guardium® policy processing failed due to prior errors.

Explanation

The Guardium policies could not be processed.

User response

Check the log for previous errors.
Parent topic: Error messages and codes: AUIAxxxx

AUIA042W The Guardium® policy is not applicable.

Explanation

One or more of the policy rules cannot be used by the current agent.

User response

Check the log for previous errors to determine why the policy is not applicable and fix the policy definition.
Parent topic: Error messages and codes: AUIAxxxx

AUIA043I The Guardium® policy reader thread started.

Explanation

The Guardium policy reader thread started.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA044I The Guardium® policy reader thread is terminating.

Explanation

The Guardium policy reader thread is stopping.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA045I The guardium policy reader thread is terminating due to prior errors.

Explanation

The policy reader thread is stopping due to previously reported errors.

User response

Check the previously issued messages to determine why the policy reader is terminating.
Parent topic: Error messages and codes: AUIAxxxx

AUIA048I *auiu_taskname* is configured to start only on *lpar-name*.

Explanation

The configuration file pointed to by the AUICONFG DD statement contains an AUIU_EXCLUDE_LPAR statement that has the *ALL parameter supplied as the excluded LPAR name.

System action

The AUIUSTC task is scheduled only on the home LPAR where the agent is running.

User response

To schedule the AUIUSTC task for another LPAR, remove or correct the AUIU_EXCLUDE_LPAR statement.
Parent topic: Error messages and codes: AUIAxxxx

AUIA049W *auiu_task_name* is configured to not start on *lpar_name* but will be started on *lpar_name* because *aui_agent_name* runs on *lpar_name*

Explanation

The AUIU_EXCLUDE_LPAR configuration parameter, found in the AUICONFG SAMPLIB member, was used in an attempt to prevent the AUIU task from executing on the LPAR named.

System action

The request to exclude this LPAR from AUIU processing is ignored because the specified LPAR is also where the agent is executing.

User response

Remove the LPAR name from the AUICONFG samplib member's AUIU_EXCLUDE_LPAR parameter. The change will be implemented at the next restart of the agent.
Parent topic: Error messages and codes: AUIAxxxx

AUIA050W *auiu_task_name* is configured to not start on *lpar_name* but no such system exists.

Explanation

The specified *lpar_name* has been included as part of the LPARS that are specified in the AUIU_EXCLUDE_LPAR configuration keyword. The specified *lpar_name* was not found in the list of members of either the SYSJES or *lpar_name* XCF groups.

System action

Processing continues.

User response

This message might indicate that the lpar_name is not available or that there is an error in the specified lpar_name.
Parent topic: Error messages and codes: AUIAxxxx

AUIA051I *auiu_task_name* is configured to not start on *lpar_name* and will not be started on *lpar_name*.

Explanation

The AUIU_EXCLUDE_LPAR configuration, parameter found in the AUICONFG SAMPLIB member, was used in an attempt to prevent the AUIU task from executing on the specified LPAR.

System action

An instance of the AUIU task is not routed to the excluded LPAR.

User response

None.
Parent topic: Error messages and codes: AUIAxxxx

AUIA052I Discovered <plex-name> system <system-name>.

Explanation

This LPAR name was found as a member of the XCF group when performing a z/OS IXCQUERY on the PLEXNAME of SYSJES XCF GROUPS.

System action

Processing continues

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA053I Agent configuration option <*option*> has been updated to <*value*>.

Explanation

This message indicates that command such as: /f AUIASTC,SET CONFIG <*option*> ON/OFF processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA054I Agent configuration option <*option*> is set to <*value*>.

Explanation

This message indicates that command such as: /f AUIASTC,GET CONFIG <*option*> processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA055I The agent is waiting for start-up information from the appliance.

Explanation

The agent has determined that there is no checkpoint information available for this agent in E/CSA, and is awaiting this data to be sent from the appliance.

System action

The agent waits up to 30 seconds for the checkpoint information, and if none is received, processing continues by using default checkpoint values, such as current blocks from the z/OS log-streams, and SMF and SLDS data sets that were created no earlier than the previous day.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA056I Starting the agent collectors.

Explanation

The agent is starting the auditing threads.

System action

The agent starts the DLIO/DLIB/AUIL/AUIF auditing threads.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA057I Issuing request to capture agent status.

Explanation

A command, such as /f AUIASTC,STATUS, has been issued for processing.

User response

No action is required.

Parent topic: Error messages and codes: AUIAxxxx

AUIA058I Request to capture agent status has completed successfully.

Explanation

A command, such as /f AUIASTC,STATUS has processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA059I Policy XMl echo

Explanation

If the XML_ECHO_AUILOG(Y) keyword exists in the AUICONFG, this message will be followed by the echo of all active XML policies on the AUILOG.

System action

As an example, the first three lines of the echo appear as follows:

```
<?xml version="1.0" encoding="IBM-1047" standalone="yes"?>
<!-- 2019-03-25-13.35.57.354196 -->
<install-info>
```

User response

For more information, see Echoed XML statement definitions.
Parent topic: Error messages and codes: AUIAxxxx

AUIA060W Policy XML echo to data set skipped: *<MESSAGE> <LOCATION>*

Explanation

The XML of the policy that was installed from the Security Guardium® system was not echoed to the specified location due to the specified message. If the &Data_Set_Name parameter contains z/OS system variables, <LOCATION> reflects the data set name after symbol substitution has been done.

<MESSAGE> <LOCATION> can be:

- The installed policy has not been changed. The echo is skipped if the newly installed policy has not changed since it was last installed.
- The data set location is not valid. Incorrect use of a system symbol in the &Data_Set_Name parameter can invalidate the location. Additional requirements:
  - The data set name must not exceed 44 characters.
  - The segment length must be greater than zero and less than or equal to 8.
  - The first character in each segment must be a letter (A – Z), #, @, $, or hyphen.

System action

Processing continues.

User response

Correct the &Data_Set_Name parameter and restart the agent. If the error persists, see Additional causes of AUIA060W .
Parent topic: Error messages and codes: AUIAxxxx

AUIA061I Policy XML echo to data set *<LOCATION>* completed.

Explanation

The agent has completed the XML echo of all active policies that were installed from the Security Guardium® system. *<LOCATION>* is the data set name specified by the &Data_Set_name parameter of the XML_ECHO_DATASET keyword.

System action

The data set name reflects the z/OS system variable substitution and the Generation Data Group extension if either exists in the &Data_Set_name parameter.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

Error messages and codes: AUIBxxxx

The following information is about error messages and codes that begin with AUIB.

- **AUIB300I**
  CONNECTION TO z/OS® SYSTEM *type* LOG STREAM WAS SUCCESSFUL - LOG STREAM NAME: *log_stream_name*, LOG STREAM TYPE: *XCF-BASED|DASD_ONLY*, CHECKPOINT VALUE: *check_point_value*, CHECKPOINT PTR: *address_of_checkpoint*

- **AUIB302I**
  DRAIN REQUEST FOR *type* LOG STREAM HAS COMPLETED. LOG STREAM: *name*.
- **AUIB305I**
  DRAIN COMPLETE FOR LOG STREAM *log-stream name*
- **AUIB306E**
  INVALID RECORD FOUND IN *log-stream* LOG STREAM -RECORD IMAGE SNAPPED TO AUI$NAP DD
- **AUIB700I**
  type: *LOGSTREAM CHECKPOINT INFORMATION* - LOG STREAM NAME: *log-stream-name* - CHECKPOINT VALUE: *check_point_value* - LAST UPDATED (UTC): *date_time*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIB300I CONNECTION TO z/OS® SYSTEM *type* LOG STREAM WAS SUCCESSFUL - LOG STREAM NAME: *log_stream_name*, LOG STREAM TYPE: *XCF-BASED|DASD_ONLY*, CHECKPOINT VALUE: *check_point_value*, CHECKPOINT PTR: *address_of_checkpoint*

Explanation

The connection to the log-stream name (*log_stream_name*) configured to process *log_stream_type* events completed successfully.

System action

Processing continues

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

AUIB302I DRAIN REQUEST FOR *type* LOG STREAM HAS COMPLETED. LOG STREAM: *name*.

Explanation

A DRAIN request, which reads all data from the z/OS® log stream, has completed.

System action

The AUIASTC tasks prepare to terminate.

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

AUIB305I DRAIN COMPLETE FOR LOG STREAM *log-stream name*

Explanation

A DRAIN request used to flush read all existing events from the log-stream-name indicated has completed successfully

System action

The log-stream reader thread will start the termination phase.

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

AUIB306E INVALID RECORD FOUND IN *log-stream* LOG STREAM -RECORD IMAGE SNAPPED TO AUI$NAP DD

Explanation

When reading DLI call audit records from the z/OS System log stream, a malformed audit record was encountered or the version of the audit record was not recognized.

System action

Processing continues after writing a SNAP/DUMP of the offending record to the AUI$NAP DD.

User response

First, verify that the S-TAP version that is running in the IMS Control Region and/or Batch Region is the same as is running in the agent. If adjusting the version does not resolve the issue, forward the AUI$NAP output to IBM Software Support.
Parent topic: Error messages and codes: AUIBxxxx

AUIB700I type: *LOGSTREAM CHECKPOINT INFORMATION* - LOG STREAM NAME: *log-stream-name* - CHECKPOINT VALUE: *check_point_value* - LAST UPDATED (UTC): *date_time*

Explanation

This message provides the highest block ID for the log stream. This is used as the starting checkpoint for processing data from this log stream.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

Error messages and codes: AUIFxxxx

The following information is about error messages and codes that begin with AUIF.

- **AUIF002I**
  SMF log reader interval set to *<n>* minutes.
- **AUIF003E**
  Command *<command>* failed; interval value must be between *<lower-bound>* and *<upper-bound>*.
- **AUIF501I**
  NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: *smf_mask_value*
- **AUIF502I**
  PROCESSING SMF DATA SET: *smf_data_set_name*
- **AUIF503I**
  PROCESSING COMPLETE FOR SMF DATA SET: *smf_data_set_name*
- **AUIF505I**
  SMF AUDITING IS DISABLED AT THE AGENT LEVEL
- **AUIF506I**
  SMF AUDITING IS DISABLED AT THE IMS LEVEL. IMS NAME: *ims_name*
- **AUIF507E**
  PROCESSING FAILED FOR SMF DATA SET: *data set name*
- **AUIF508I**
  SCANNING RECON DATA SETS FOR IMS ARTIFACT DATA SETS. **RECON1:** *recon1_dsn* **RECON2:** *recon2_dsn* **RECON3:** *recon3_dsn*
- **AUIF702I**
  SMF MASK CHECKPOINT INFORMATION - MASK VALUE : *SMF_mask* - LAST DSN READ: *SMF_dsn* - LAST UPDATED (UTC): *date_time*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIF002I SMF log reader interval set to *<n>* minutes.

Explanation

The subtask that reads event data from SMF log data sets is scheduled to perform every <n> minutes.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF003E Command *<command>* failed; interval value must be between *<lower-bound>* and *<upper-bound>*.

Explanation

This message indicates that *<command>* such as:

```
/f AUIASTC,SET INTERVAL <number>
```

failed because of incorrect *<number>* value. Correct value must be between <lower-bound> and <upper-bound>.

User response

Use an interval value between *<lower-bound>* and *<upper-bound>*. If that does not resolve the issue, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIFxxxx

AUIF501I NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: *smf_mask_value*

Explanation

When scanning the z/OS® catalog for new data sets that meet the indicated SMF mask value (*smf_mask_value*) and have not been processed by the product, it was determined that no z/OS data sets meet that criteria.

System action

The process will continue to examine other SMF Mask values.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF502I PROCESSING SMF DATA SET: *smf_data_set_name*

Explanation

Processing has started for a SMF data set.

System action

Events will be obtained from the SMF data set based on collection profile criteria.

User response

None.
Parent topic: Error messages and codes: AUIFxxxx

AUIF503I PROCESSING COMPLETE FOR SMF DATA SET: *smf_data_set_name*

Explanation

Processing of the SMF data set has completed.

System action

Processing continues with other candidate SMF data sets.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF505I SMF AUDITING IS DISABLED AT THE AGENT LEVEL

Explanation

Auditing of SMF events has been disabled at the agent level, as instructed by the settings chosen in the Guardium user interface.

System action

The auditing of events sourced from SMF data sets is not performed.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF506I SMF AUDITING IS DISABLED AT THE IMS LEVEL. IMS NAME: *ims_name*

Explanation

Auditing of SMF events has been disabled at the IMS level for the IMS named (*ims_name*) by use of the Guardium interface and the IMS Auditing Levels editor.

System action

The auditing of events sourced from SMF for the IMS named is not performed.

User response

If this is a desired action, then no response is needed. If SMF events should be audited for this IMS, then the IMS configuration should be modified by using the Guardium interface and the IMS Auditing Levels to select any or all SMF events you want to audit.
Parent topic: Error messages and codes: AUIFxxxx

AUIF507E PROCESSING FAILED FOR SMF DATA SET: *data set name*

Explanation

Processing failed during the reading of the data set, specified by name in the message text.

System action

The collection process terminates.

User response

Determine the cause of the failure and correct it by reviewing previously issued S-TAP and z/OS messages.
Parent topic: Error messages and codes: AUIFxxxx

AUIF508I SCANNING RECON DATA SETS FOR IMS ARTIFACT DATA SETS. RECON1: *recon1_dsn* RECON2: *recon2_dsn* RECON3: *recon3_dsn*

Explanation

The AUIFSTC task has started to scan the RECON data sets looking for database data sets, Image copy data sets and optionally IMS SLDS to be audited using SMF records.

System action

The RECON data sets are read using the specified DSN.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF702I SMF MASK CHECKPOINT INFORMATION - MASK VALUE : *SMF_mask* - LAST DSN READ: *SMF_dsn* - LAST UPDATED (UTC): *date_time*

Explanation

This message provides the SMF data set mask (*SMF_mask*) and the last SMF data set read (*SMF_dsn*) that matched that mask. This information is used as a checkpoint to indicate which SMF data sets have already been processed, and should not be re-read by the AUIFstc tasks.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

Error messages and codes: AUIGxxxx

The following information is about error messages and codes that begin with AUIG.

- **AUIG001S**
  An unexpected error occurred (/path/to/file.c, linenum).
- **AUIG002S**
  An unexpected error occurred with token "token1" (/path/to/file.c,linenum).
- **AUIG003S**
  An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).
- **AUIG004S**
  An unexpected error occurred with tokens "token1", "token2", "token3", and "token4" (/path/to/file.c,linenum).
- **AUIG005S**
  An unexpected error occurred with tokens "token1", "token2", and "token3" (/path/to/file.c,linenum).
- **AUIG006S**
  An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).
- **AUIG014E**
  dataspace create return code = *return-code-hex*, reason = *reason-code-hex*

- **AUIG015W**
  MALLOC: big alloc coming *memory_size* from GDM Read Buffer
- **AUIG016S**
  MALLOC: zero alloc from *<site>*.
- **AUIG017S**
  MALLOC: negative malloc *memory size* at site *site*.
- **AUIG018S**
  MALLOC failed, got NULL for size *<memory_size>* at site *<site>*.
- **AUIG045E**
  Write failed, sd=*bbbb* desired write len *length* buffer at *address*, ret code *xxxx* reason 0x*yyyyzzzz*
- **AUIG046E**
  Failure to resolve address for host *'HOST'*, ret code *return-code*, reason *hex-value*.
- **AUIG047E**
  Set sockopt failed, level = *hex-value*, option = *hex-value*, ret code *return-code*, reason *hex-value*.
- **AUIG048E**
  Get sockopt failed, ret code *return-code*, reason *hex-value*.
- **AUIG049E**
  BPXFCT failed, ret code *<return-code>*; reason *<reason-code>*.
- **AUIG050E**
  Read failed ret code *xxxx* reason 0x*zzzzzzzz*
- **AUIG051I**
  TCP write disabled
- **AUIG052I**
  Write to megabuffer disabled
- **AUIG053I**
  Unexpected payload received *<hexadecimal string>*. Payload ignored.
- **AUIGF120I**
  Trace Settings: Compilation 0, Requested Runtime 0, ECSA Flag 32, Actual Runtime 0...
- **AUIGF201I**
  Valid stage zero filter criteria found.
- **AUIGF202I**
  No valid stage zero filter criteria found.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIG001S An unexpected error occurred (/path/to/file.c, linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG002S An unexpected error occurred with token "token1" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG003S An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG004S An unexpected error occurred with tokens "token1", "token2", "token3", and "token4" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIGxxxx

AUIG005S An unexpected error occurred with tokens "token1", "token2", and "token3" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG006S An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG014E dataspace create return code = *return-code-hex*, reason = *reason-code-hex*

Explanation

An attempt to create a data space for spill usage has failed. Spill capability might not be available.

User response

Examine the return code and reason code, and take appropriate action to ensure that data spaces can be created.
Parent topic: Error messages and codes: AUIGxxxx

AUIG015W MALLOC: big alloc coming *memory_size* from GDM Read Buffer

Explanation

More than 10,485,760 bytes was required in order to process collection policies pushed from the Security Guardium® system.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIG016S MALLOC: zero alloc from *<site>*.

Explanation

Zero bytes was required in order to process collection policies pushed from the Security Guardium® system.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG017S MALLOC: negative malloc *memory size* at site *site*.

Explanation

Negative number of bytes required in order to process collection policies pushed from the Security Guardium® system.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG018S MALLOC failed, got NULL for size *<memory_size>* at site *<site>*.

Explanation

Attempt to allocate memory failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG045E Write failed, sd=*bbbb* desired write len *length* buffer at *address*, ret code *xxxx* reason 0x*yyyyzzzz*

Explanation

An attempt to read or write to a socket has failed. This error might occur if Security Guardium® S-TAP® for IMS is connected to a peer that is offline.

System action

The system attempts to reestablish the connection to the peer in order to read or write the data.

User response

Identify the cause of the failure by using the *z/OS® UNIX System Services Messages and Codes SA23-2284-xx* manual to look up the return and return codes that are provided in the message text, where *bbbb* is an internal code, *xxxx* is the return code, and *yyyyzzzz* is the reason code. Use the *zzzz* value to determine the error code, as described in the Reason codes (errnojrs) section of the *z/OS UNIX System Services Messages and Codes* manual.
Parent topic: Error messages and codes: AUIGxxxx

AUIG046E Failure to resolve address for host *'HOST'*, ret code *return-code*, reason *hex-value*.

Explanation

An attempt to resolve the given hostname failed.

User response

Verify that the hostname is specified correctly and is resolvable. Contact IBM® Software Support if hostname is correct and resolvable.
Parent topic: Error messages and codes: AUIGxxxx

AUIG047E Set sockopt failed, level = *hex-value*, option = *hex-value*, ret code *return-code*, reason *hex-value*.

Explanation

An attempt to set a socket option failed.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIGxxxx

AUIG048E Get sockopt failed, ret code *return-code*, reason *hex-value*.

Explanation

An attempt to set a socket option failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG049E BPXFCT failed, ret code *<return-code>*; reason *<reason-code>*.

Explanation

The system BPXFCT call failed while attempting to set socket blocking mode.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.
Parent topic: Error messages and codes: AUIGxxxx

AUIG050E Read failed ret code *xxxx* reason 0x*zzzzzzzz*

Explanation

An attempt to read or write to a socket has failed. This error might occur if Security Guardium® S-TAP® for IMS is connected to a peer that is offline.

System action

The system attempts to reestablish the connection to the peer in order to read or write the data.

User response

Identify the cause of the failure by using the z/OS USS Return Codes and Reason Codes to look up the return and reason codes that are provided in the message text, where *xxxx* is the return code and *zzzzzzzz* is the reason code.
Parent topic: Error messages and codes: AUIGxxxx

AUIG051I TCP write disabled

Explanation

TCP/IP processing has been disabled.

System action

The Guardium appliance will not receive data.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIG052I Write to megabuffer disabled

Explanation

TCP/IP buffer has been disabled.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIG053I Unexpected payload received *<hexadecimal string>*. Payload ignored.

Explanation

An unexpected string of data was received by the Security Guardium® S-TAP® for IMS agent from the Guardium appliance or associated firewall. The string does not conform to the format that is normally associated with a pushed-down policy or other expected data.

System action

The string is ignored and normal processing continues.

User response

If this message appears occasionally, no action is required. If this message appears frequently, contact IBM Support to diagnose whether a problem exists with the Guardium appliance or firewall.
Parent topic: Error messages and codes: AUIGxxxx

AUIGF120I Trace Settings: Compilation 0, Requested Runtime 0, ECSA Flag 32, Actual Runtime 0...

Explanation

This message is produced during the compilation of a filter, using the policy information that was specified.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIGF201I Valid stage zero filter criteria found.

Explanation

The collection profile compilation process found that the collection profile criteria will allow for Stage zero filtering of IMS DLI events based on USERIDs or PSB names.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIGF202I No valid stage zero filter criteria found.

Explanation

The collection profile compilation process found that the collection profile criteria is not conducive to providing Stage 0 filtering for IMS DLI events. The reasons may include:

- No USERIDS or PSBS were specified in the selection criteria.
- Multiple RULES were defined and differences in the USERID and/or PSB specifications in each rule were different.

System action

Processing continues without Stage Zero filtering capability.

User response

If Stage 0 filtering is desired, adjust the USERID and PSB specifications in each rule to be the same.
Parent topic: Error messages and codes: AUIGxxxx

Error messages and codes: AUIIxxxx

The following information is about error messages and codes that begin with AUII.

Note: To set a z/OS message alert for messages that begin with AUII, use single-dash formatting between the message number and message text. For example:

```
AUII056I
- ZIIP PROCESSING ENABLED FOR IMS STAP
```

- **AUII017I**
  S-TAP® for V10.1.3 initialization complete using RECON1 DSN: *recon1_dsn*
- **AUII018E**
  IBM® Security Guardium® S-TAP for IMS on z/OS® initialization failed
- **AUII019E**
  IBM Security Guardium S-TAP for IMS on z/OS termination failed
- **AUII020E**
  UNABLE TO FIND RECON1 DATA SET NAME

- **AUII021E**
  BLDL FAILED FOR ACTION MODULE *module_name*
- **AUII022E**
  INSUFFICENT STORAGE AVAILABLE FOR *module_name* ACTION MODULE (*stg_type*)
- **AUII023E**
  IMODULE DIRLOAD FAILED FOR ACTION MODULE *module_name*
- **AUII024E**
  Unable to locate IMS SCD address.
- **AUII025E**
  Unable to locate IMS SSCD Extension address.
- **AUII026E**
  UNABLE TO LOCATE THIS IMS SSCT ADDRESS
- **AUII027E**
  INSUFFICIENT STORAGE AVAILABLE FOR AUIPLOG CONTROL BLOCK
- **AUII028E**
  IMODULE LOAD OF ACTION MODULE *module_name* FAILED
- **AUII029E**
  DFSTCBTB LOCATE SERVICE CALL FAILED
- **AUII031E**
  STAP FOR IMS INTERNAL LOGIC ERROR *(rc)*
- **AUII038E**
  ITASK CREATE FOR ACTION MODULE *module_name* FAILED
- **AUII040E**
  ODBA LOAD OF DFSISSI0 FAILED
- **AUII041E**
  ODBA HOOK POINT NOT FOUND (module_name)
- **AUII042W**
  ZIIP PROCESSOR NOT AVAILABLE ON THIS LPAR
- **AUII043W**
  THIS IMS IS NOT CONNECTED TO WORKLOAD MANAGER
- **AUII044E**
  ZIIP PROCESSING REQUEST HAS BEEN REJECTED
- **AUII046E**
  NAME/TOKEN SERVICE *service-name* SERVICE FAILED (*name value*)
- **AUII049E**
  DEDB CALL ANALYSIS INIT FAILURE RC = *return code*
- **AUII050I**
  S-TAP FOR IMS AUDIT STATISTICS
- **AUII052I**
  `USING IMS STAP V10.1.3 MODULE Module_name APAR# Build_date`
- **AUII055I**
  ZIIP PROCESSING HAS BEEN REQUESTED FOR IMS STAP
- **AUII056I**
  ZIIP PROCESSING ENABLED FOR IMS STAP
- **AUII057I**
  process_type PROCESSING FAILED *RC*: return_code *RSN*: reason_code
- **AUII058A**
  STAP FOR IMS COMPONENT HAS ABENDED
- **AUII060W**
  Potential waited PST=*xxxxxxxx* (PST# = *yyyy*)
- **AUII061I**
  Potential Waited PST xxxxxxxx (PST#= zzzz) RELEASED.
- **AUII120I**
  NO COLLECTIONS ACTIVE FOR THIS IMS INSTANCE
- **AUII172I**
  AUIprogram LOADED EXIT *imsexit* FROM DATA SET: *data set name*
- **AUII173E**
  IMS RELEASE *ims-vrl* IS NOT SUPPORTED
- **AUII174E**
  LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*
- **AUII175I**
  NON_ZERO RC FROM EXIT *exit_name*: RC = *return_code*
- **AUII176E**
  module_name service_type SERVICE ERROR: RC: *return_code* RS: *reason_code*
- **AUII177E**
  module_name FOUND WITH RENT/REUS ATTRIBUTE IN NON_APF ENVIRONMENT
- **AUII178E**
  DATA SET NAME: *dsn*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUII017I S-TAP® for V10.1.3 initialization complete using RECON1 DSN: *recon1_dsn*

Explanation

IBM® Guardium® S-TAP for IMS has initialized in the DLI/DBB batch job or IMS control region environment. For successful auditing to occur, the RECON1 DSN indicated in this message should match the RECON1 DSN associated with the IMS definition you have created.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII018E IBM® Security Guardium® S-TAP® for IMS on z/OS® initialization failed

Explanation

IBM Guardium S-TAP for IMS was unable to initialize in this IMS Control region. The monitoring of IMS databases will not occur.

System action

IMS processing continues without auditing capabilities.

User response

Examine the JES log for other messages to determine the reason for the initialization failure.
Parent topic: Error messages and codes: AUIIxxxx

AUII019E IBM® Security Guardium® S-TAP® for IMS on z/OS® termination failed

Explanation

IBM Guardium S-TAP for IMS was unable to terminate cleanly.

System action

The termination of the IMS online region of DLI/DBB batch job step continues.

User response

This error indicates that an environmental error has occurred. Examine the JES log for other AUI messages to determine the reason for the termination failure.
Parent topic: Error messages and codes: AUIIxxxx

AUII020E UNABLE TO FIND RECON1 DATA SET NAME

Explanation

An attempt to find the RECON1 data set name used by the IMS Online control region or DLI/DBB batch job step has failed. The RECON1 data set name is critical to the determination of the collection profile used to audit IMS events.

System action

IMS processing continues without the IMS auditing feature.

User response

Determine why the RECON1 data set name is not available for this IMS control region or DLI/DBB batch job step. An in-stream RECON1 DD statement must be present in the JCL, or a RECON1 MDALIB member being present in the JOB/STEPLIB DD concatenation is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII021E BLDL FAILED FOR ACTION MODULE *module_name*

Explanation

An attempt to find a required processing module (module_name) has failed.

System action

IMS processing continues without auditing.

User response

Examine the STEPLIB/JOBLIB DD concatenation to ensure the SAUIIMOD product data set is included.
Parent topic: Error messages and codes: AUIIxxxx

AUII022E INSUFFICENT STORAGE AVAILABLE FOR *module_name* ACTION MODULE (*stg_type*)

Explanation

An attempt to obtain storage for the module named (*module_name*) has failed. The storage type field (*stg_type*) indicates if the storage required is 31bit or 24bit based.

System action

IMS processing continues without IMS auditing available.

User response

Increase the region size used by the job step (REGION=).
Parent topic: Error messages and codes: AUIIxxxx

AUII023E IMODULE DIRLOAD FAILED FOR ACTION MODULE *module_name*

Explanation

The DIRLOAD IMS service has failed.

System action

IMS processing continues with auditing.

User response

Determine the cause of the error from the IMS Messages and Codes manual and correct the error. If necessary, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII024E Unable to locate IMS SCD address.

Explanation

An attempt to locate the IMS SCD during product initialization has failed.

System action

IMS processing continues without auditing.

User response

Verify that you are attempting to run the product using a supported IMS release. Contact IBM® Software Support for further assistance.
Parent topic: Error messages and codes: AUIIxxxx

AUII025E Unable to locate IMS SSCD Extension address.

Explanation

An attempt to locate the IMS SSCD Extension address has failed.

System action

IMS processing continues without auditing.

User response

Verify that you are attempting to run the product using a supported IMS release. Contact IBM Software Support for further assistance.
Parent topic: Error messages and codes: AUIIxxxx

AUII026E UNABLE TO LOCATE THIS IMS SSCT ADDRESS

Explanation

The IMS SCCT address cannot be located by the IMS S-TAP initialization process.

System action

IMS processing continues without auditing capabilities.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII027E INSUFFICIENT STORAGE AVAILABLE FOR AUIPLOG CONTROL BLOCK

Explanation

An attempt to obtain E/CSA to hold the AUIPLOG module has failed.

System action

IMS processing continues without auditing.

User response

Investigate E/CSA usage on the LPAR.
Parent topic: Error messages and codes: AUIIxxxx

AUII028E IMODULE LOAD OF ACTION MODULE *module_name* FAILED

Explanation

An attempt to LOAD module module_name using IMS services has failed.

System action

An attempt to LOAD module module_name using IMS services has failed.

User response

Verify that the SAUIIMOD product data set is available in the STEPLIB/JOBLIB data set concatenation. Contact IBM® Software Support for further assistance.
Parent topic: Error messages and codes: AUIIxxxx

AUII029E DFSTCBTB LOCATE SERVICE CALL FAILED

Explanation

A call to the IMS DFSTCBTB service has failed.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII031E STAP FOR IMS INTERNAL LOGIC ERROR *(rc)*

Explanation

Security Guardium® S-TAP® for IMS initialization found a logic error.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII038E ITASK CREATE FOR ACTION MODULE *module_name* FAILED

Explanation

DA call to the DFSCIR IMS service to create an ITASK has failed.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII040E ODBA LOAD OF DFSISSI0 FAILED

Explanation

An attempt to LOAD IMS module DFSISSI0 has failed.

System action

IMS processing with auditing continues. The product will be unable to determine the correct USERID for events driven from ODBA threads.

User response

Contact Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII041E ODBA HOOK POINT NOT FOUND (module_name)

Explanation

An attempt to locate a hook point in the indicated module (module_name) has failed.

System action

IMS processing with auditing continues. The product will be unable to determine the correct USERID for events driven from ODBA threads. An output DD: AUI$NAP is dynamically allocated to SYSOUT, and the area where the hook point was to be located is snapped out to this AUI$NAP DD.

User response

Provide the AUI$NAP output to IBM Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII042W ZIIP PROCESSOR NOT AVAILABLE ON THIS LPAR

Explanation

The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS® System Logger. IMS STAP has determined that zIIP processing is not available on this LPAR.

System action

Processing continues exclusively using general processors.

User response

Remove the AUIZIIP DD statement and restart the IMS sub-system.
Parent topic: Error messages and codes: AUIIxxxx

AUII043W THIS IMS IS NOT CONNECTED TO WORKLOAD MANAGER

Explanation

A request to process DLI call filtering and z/OS® System Logger writes on a zIIP processor has been rejected as the IMS sub-system is not connected to the z/OS Workload Manager.

System action

Processing continues exclusively using general processors.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII044E ZIIP PROCESSING REQUEST HAS BEEN REJECTED

Explanation

A request to process DLI call filtering and z/OS® System Logger writes on a zIIP processor has been rejected.

System action

Processing continues exclusively using general processors.

User response

Review previously issued AUII messages to determine the root cause of the request rejection.
Parent topic: Error messages and codes: AUIIxxxx

AUII046E NAME/TOKEN SERVICE *service-name* SERVICE FAILED (*name value*)

Explanation

An attempt to drive the z/OS® name/token service has failed.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIIxxxx

AUII049E DEDB CALL ANALYSIS INIT FAILURE RC = *return code*

Explanation

An attempt insert product code in the DEDB call analysis area has failed.

System action

IMS processing with DEDB event auditing disabled. An output DD: AUI$NAP is dynamically allocated to SYSOUT, and the area where the code insertion was to be located is snapped out to this AUI$NAP DD.

User response

Provide the AUI$NAP output to IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII050I S-TAP® FOR IMS AUDIT STATISTICS

Explanation

This message provides statistics regarding the number of DLI events which have been processed. This message is issued when:

- The number of DLI calls specified in the message frequency section of the Guardium client's IMS Data Set definition screen has been reached.
- The time specified in the AUII050I message frequency section of the Guardium client's IMS Data Set definition screen has elapsed.
- The collection profile for the IMS is made in active.
- The DLI/DBB batch job or IMS Online Control Region terminates.

The description of values are as follows:

DLI CALLS RECEIVED
: This value indicates the number of IMS DLI calls which had the potential of being audited. This number can be more or less than the number of actual DLI calls performed, because:

  - DLI PATH calls which effect multiple segments within a hierarchical path are treated and counted as individual DLI calls.
  - DLI calls types which are not included in any RULE of the active collection profile are not counted as they are immediately rejected.

DLI CALLS AUDITED
: This value indicates the number of IMS DLI calls which resulted in a DLI event being written to the z/OS® System Logger Log-stream for transmittal to the Guardium® Appliance.

IXGWRITE ERRORS
: This value indicates the number of z/OS System Logger IXGWRITE calls which have failed. One of more AUIJ304E messages will precede the issuance of the AUII050I message if the number of IXGWRITE errors is greater than zero. A non-zero value for the IXGWRITE ERRORS and a zero value for the DLI CALLS LOST DUE TO IXGWRITE ERRORS section of this message indicates that the IXGWRITE errors were subsequently retried and the IXGWRITE calls were then completed successfully.

DLI CALLS LOST DUE TO IXGWRITE ERRORS
: A non-zero value in this section indicates that DLI calls which were audited and either:

  - Could not be placed into a log-stream data buffer (indicated by the issuance of message AUIJ307A).
  - Audited events already in the data buffer could not be written to the z/OS System Logger Log-Stream using the IXGWRITE call and the collection profile for the IMS has been deactivated or the DLI/DBB batch job or IMS Online Control region has been terminated (indicated by the issuance of message AUIJ304E).

System action

Processing continues.

User response

No action is required. This is an informational message only.
Parent topic: Error messages and codes: AUIIxxxx

AUII052I USING IMS STAP V10.1.3 MODULE *Module_name APAR# Build_date*

Explanation

These messages are issued by the IMS S-TAP® code in the IMS Control region during startup to broadcast the maintenance level of the programs that are in use by Security Guardium® S-TAP for IMS.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII055I ZIIP PROCESSING HAS BEEN REQUESTED FOR IMS STAP

Explanation

The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS® System Logger.

System action

IMS STAP attempts to create an environment to support zIIP processing.

User response

If this was not intended, remove the AUIZIIP DD statement and restart the IMS sub-system.
Parent topic: Error messages and codes: AUIIxxxx

AUII056I ZIIP PROCESSING ENABLED FOR IMS STAP

Explanation

The request for zIIP support for IMS STAP and this IMS Control Region has been acted on and all initialization processes have completed successfully.

System action

IMS STAP will schedule DLI call filtering and writes to the z/OS® System Logger as a zIIP eligible enclave SRB.

User response

If this was not intended, remove the AUIZIIP DD statement and restart the IMS sub-system.
Parent topic: Error messages and codes: AUIIxxxx

AUII057I *process_type* PROCESSING FAILED *RC*: return_code *RSN*: reason_code

Explanation

The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS® System Logger. A process (process_type) used to enable zIIP processing has failed.

System action

The request to enable zIIP processing is rejected and general processor will be used.

User response

Review IBM® supplied documentation for the process which failed using the return and reason codes (*return_code/reason_code*) to determine the cause of the failure.
Parent topic: Error messages and codes: AUIIxxxx

AUII058A STAP FOR IMS COMPONENT HAS ABENDED

Explanation

The S-TAP® for IMS component has abnormally ended, causing auditing to disable.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIIxxxx

AUII060W Potential waited PST=*xxxxxxxx* (PST# = *yyyy*)

Explanation

This warning message indicates that IBM® Guardium® S-TAP® for IMS has detected a dependent region that has been waiting for an event to be audited for at least 15 seconds. The dependent region is identified by the PST address *xxxxxxxx*. The PST# value specified as *yyyy* is the region number in hexadecimal format.

System action

IBM Guardium S-TAP for IMS attempts to process the dependent region.

User response

If the dependent region continues processing, then no action is required. If the dependent region remains in a wait state, then it must be stopped or cancelled. Before you stop or cancel the dependent region, take an SVC dump of the IMS Control region and provide it to IBM Software Support for analysis.
Parent topic: Error messages and codes: AUIIxxxx

AUII061I Potential Waited PST xxxxxxxx (PST#= zzzz) RELEASED.

Explanation

This message is a response to message AUII060W (Potential Waited PST xxxxxxxx (PST#= zzzz)). This message indicates that the corresponding IPOST was performed, and the PST is no longer in a WAIT state.

System action

IMS Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII120I NO COLLECTIONS ACTIVE FOR THIS IMS INSTANCE

Explanation

Initialization has completed successfully for Security Guardium® S-TAP® for IMS, but no collections were found that pertain to this batch job or IMS control region.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII172I *AUIprogram* LOADED EXIT *imsexit* FROM DATA SET: *data set name*

Explanation

The *AUIprogram* named found an occurrence of the *imsexit* later within the JOBLIB/STEPLIB concatenation, and has loaded it.

System action

The *imsexit* will be invoked with R13 pointing to the save area originally provided by IMS, as well as its own 512 byte work area, provided in the SXPLAWRK field of the IMS Standard User Exit Parameter list, immediately following each execution of *AUIprogram*.

User response

For the *imsexit* to run, no action is required. If the *imsexit* should not be run in this environment, remove the data set from the JOBLIB/STEPLIB concatenation and restart the IMS control region or batch job.
Parent topic: Error messages and codes: AUIIxxxx

AUII173E IMS RELEASE *ims-vrl* IS NOT SUPPORTED

Explanation

The IMS release being used is not support by this version of the product.

System action

IMS processing continues without auditing.

User response

Review supported IMS releases for the release of this product.
Parent topic: Error messages and codes: AUIIxxxx

AUII174E LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*

Explanation

LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*

User response

Ensure that the SAUIIMOD product data set is included in the STEPLIB/JOBLIB DD concatenation.
Parent topic: Error messages and codes: AUIIxxxx

AUII175I NON_ZERO RC FROM EXIT *exit_name*: RC = *return_code*

Explanation

The *exit_name* indicated returned a non-zero return code value of *return_code* as specified.

System action

The return code value is returned to IMS.

User response

Correct the *exit_name* program if the non-zero value was returned in error. Review the IMS Customization Guide or IMS Exit Routine Reference for more information.
Parent topic: Error messages and codes: AUIIxxxx

AUII176E *module_name service_type* SERVICE ERROR: RC: *return_code* RS: *reason_code*

Explanation

The *service_type* invoked by the specified *module_name* has failed.

System action

IMS processing continues without auditing.

User response

Review all subsequent AUI error messages to diagnose the problem.
Parent topic: Error messages and codes: AUIIxxxx

AUII177E *module_name* FOUND WITH RENT/REUS ATTRIBUTE IN NON_APF ENVIRONMENT

Explanation

Program *module_name* had the RENT/REUS attribute on in a non-APF-Authorized environment. Security Guardium® S-TAP® for IMS is unable to load the program.

System action

Processing continues with the exit cascading feature disabled.

User response

Re-link the exit with the NOREUSE attribute.
Parent topic: Error messages and codes: AUIIxxxx

AUII178E DATA SET NAME: *dsn*

Explanation

This message is issued in conjunction with a previous message (for example, AUII176E) to indicate an associated data set.

User response

Check the log for the previously issued, associated message and take the action that is advised in that message.
Parent topic: Error messages and codes: AUIIxxxx

Error messages and codes: AUIJxxxx

The following information is about error messages and codes that begin with AUIJ.

- **AUIJ005W**
  UNABLE TO LOAD MESSAGE TABLE *table_name* RSN: *reason_code* WILL USE AUIMGENU
- **AUIJ006E**
  LOAD FAILED FOR MESSAGE TABLE *table_name* RSN: *reason_code*
- **AUIJ007E**
  PROGRAM *program_name* IS NOT EXECUTING APF-AUTHORIZED
- **AUIJ008I**
  ATTEMPTING TO CONNECT TO THE GUARDIUM S-TAP® APPLIANCE. **TCP/IP Address:** *ip_address*, **PORT:** *port_number*, **PING RATE:** *ping_rate*
- **AUIJ009E**
  LOAD FAILED FOR MODULE *module_name*. R1: *abend_code* R15: *reason_code*
- **AUIJ010I**
  IMS STAP *ver* HAS STARTED.
- **AUIJ011I**
  function_type CALL TO GUARDUIM S-TAP APPLIANCE SUCCESSFUL
- **AUIJ012I**
  NUMBER OF *event_type* EVENTS SENT TO APPLIANCE: *counter*
- **AUIJ013E**
  stap_call TO GUARDUIM S-TAP APPLIANCE FAILED *(call source)* IP ADDRESS: *ip_address* STAP_RC = *rc1* STAP_RS = *rs1* GDM_RC = *rc2* PB_RC = *rc3* GDML_RC = *rc4* GDML_RS = *rs2*
- **AUIJ014E**
  OPEN FAILED FOR DD *dd_name*
- **AUIJ015E**
  THIS IMS RELEASE IS NOT SUPPORTED. IMS NAME: *ims-name*, VRL: *ims_version*
- **AUIJ016E**
  UNABLE TO INITIALIZE APPLIANCE INTERFACE *(connection_type)*
- **AUIJ017I**
  PRIMARY STAP CONNECTION RESTORED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*
- **AUIJ018W**
  PREVIOUS STAP CONNECTION FAILED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*
- **AUIJ019E**
  STAP CONNECTION FAILED: NO CONNECTIONS AVAILABLE *(connection_type)* - IP ADDRESS: *ip-address* - PORT : *port*
- **AUIJ020I**
  All EVENTS HAVE BEEN WRITTEN FROM SPILL AREA TO APPLIANCE *(connection_type)*
- **AUIJ021W**
  EVENTS ARE BEING WRITTEN TO THE SPILL AREA *(connection_type)*
- **AUIJ022W**
  SPILL AREA IS FULL: EVENT DATA IS BEING LOST *(connection_type)*
- **AUIJ023E**
  SPILL AREA IS NOT AVAILABLE *(connection_type)*
- **AUIJ024W**
  NUMBER OF *type* EVENTS LOST *count*
- **AUIJ042W**
  ZIIP PROCESSING NOT AVAILABLE ON THIS LPAR (type)
- **AUIJ044W**
  ZIIP PROCESSING REQUEST HAS BEEN REJECTED *(connection_type)*
- **AUIJ055I**
  ZIIP PROCESSING REQUESTED FOR *type* PROCESSING
- **AUIJ056I**
  ZIIP PROCESSING ENABLED FOR type PROCESSING, ENCLAVE TOKEN: *value*
- **AUIJ057W**
  ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED DUE TO ERRORS - PROCESSING WILL CONTINUE USING GCPU
- **AUIJ058W**
  ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED - TRACING IS ENABLED BY THE USE OF THE AUI$NAP JCL STATEMENT
- **AUIJ201E**
  VSAM ERROR ENCOUNTERED
- **AUIJ202E**
  VSAM ERROR ENCOUNTERED
- **AUIJ203E**
  VSAM ERROR ENCOUNTERED
- **AUIJ250I**
  AUDITING IMS EVENTS. COLLECTION PROFILE NAME: *collection_profile_name* IMS NAME: *ims_name* AGENT NAME: *agent name* EXCLUDED REGIONS: *region_types*

- **AUIJ251E**
  COMPILED FILTER BUILD FAILED. COLLECTION PROFILE NAME : *collection _profile_name* RC: *return_code* RSN: *reason_code*
- **AUIJ252W**
  GUARDIUM QUARANTINE IS IN EFFECT; DBPCB STATUS CODES OF *AI* MAY OCCUR
- **AUIJ255I**
  AUII050I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ256I**
  AUIJ250I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID : *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ257I**
  AUII120I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ258I**
  AUII052I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ259I**
  JOBNAME *job_name* USING IMS STAP V10.1.3 MODULE: *pgm_name* APAR: *fix_number* DATE: *fix_date*
- **AUIJ303W**
  request_type REQUEST FOR LOG STREAM *log_stream_name* FAILED - RC: *return_code* RS: *reason_code* - WILL CONTINUE TO RETRY
- **AUIJ304A**
  IXGCONN REQUEST FOR LOG_STREAM *log_stream_name* FAILED with RC = *return_code* and RS= *reason_code*
- **AUIJ304E**
  IXGWRITE REQUEST FOR *<log-stream-name>* FAILED - RC: *return_code* RS: *reason_code*
- **AUIJ307A**
  AUDITED EVENTS ARE BEING LOST DUE TO IXGWRITE ERRORS AND/OR BUFFER SHORTAGES
- **AUIJ307E**
  thread_type THREAD IS TERMINATING DUE TO PROCESSING ERRORS.
- **AUIJ330E**
  REQUIRED DATA SET IS NOT CATALOGED. - TYPE: *dsn_type*, DSN: *data_set_name*
- **AUIJ331E**
  service_name SERVICE FAILED - RC: *return_code* - RSN: *reason_code*
- **AUIJ332E**
  DATA SET IS NOT VALID WITHIN CONTEXT USED - TYPE: *data_set_type,* DSN: *data_set_name*, REASON: *reason*
- **AUIJ333E**
  Service *SERVICE FAILED* for *DATA SET*: *dsn - R15: return_code*
- **AUIJ335W**
  dd_name DD IS PRESENT IN THIS JCL, *dsn_types* WILL NOT BE AUDITED
- **AUIJ400E**
  INSUFFICIENT MEMORY - MODULE NAME: *program_name* - MEMORY SEGMENT TYPE: *seg_type*
- **AUIJ401E**
  MODULE *module_name* FAILED DURING ATTACH of *program_name* - RETURN CODE: *return_code*
- **AUIJ402E**
  CATALOG SERVICE REQUEST FAILED - MODULE NAME: *module_name* - RC: *return_code* RSN: *reason_code*
- **AUIJ403E**
  DYNAMIC ALLOCATION FAILURE - FUNCTION : *function_code* - DSN: *data-set-name* - RC: *return_code* RSN: *reason_code*
- **AUIJ404E**
  DYNAMIC ALLOCATION FAILURE - FUNCTION: *function_code* -DDN: *dd_name* - RC: *return_code* RSN: *reason_code*
- **AUIJ406W**
  TOO MANY RULES SPECIFIED IN POLICY, REQUEST HAS BEEN TRUNCATED. POLICY: *policy_name*. RULE LIMIT: *max_number_of rules_allowed*
- **AUIJ407I**
  number DATA SETS ADDED TO POLICY *policy_name* FILTER
- **AUIJ408E**
  POLICY *name* RESULTED IN OVER 102400 DATA SETS TO BE AUDITED; DATA SET RESULT SET HAS BEEN TRUNCATED
- **AUIJ500I**
  STARTING *cycle_type* CYCLE
- **AUIJ501I**
  NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: - *smf_mask_value*
- **AUIJ504I**
  cycle_type CYCLE COMPLETE
- **AUIJ521W**
  CONTROL BLOCK AUIDCCOM NOT FOUND
- **AUIJ510I**
  `ALTERNATE RECON DATA SETS FOUND FOR IMSNAME imsname: RECON1: alt_dsn_1; RECON2: alt_dsn_2, RECON3: alt_dsn_3`
- **AUIJ511E**
  `ALTERNATE RECON DATA SET NOT CATALOGED; DSN:  alt_dsn`
- **AUIJ512E**
  `ALTERNATE RECON DATA SET NOT A VSAM FILE; DSN:  alt_dsn`
- **AUIJ513E**
  `NO VALID ALTERNATE RECON DATA SETS FOUND FOR IMS imsname;  PROCESSING TERMINATED`
- **AUIJ522E**
  INSUFFICIENT E/CSA STORAGE AVAILABLE FOR *control_block* CONTROL BLOCK
- **AUIJ609I**
  event_types ARE BEING EXCLUDED (*excluded_by*)
- **AUIJ800E**
  REQUIRED DD STATEMENT IS MISSING: *dd-name*
- **AUIJ860E**
  VSAM FILE DEFINITION ERROR - DDN: *dd_name* - REASON: *definition_error*
- **AUIJ999E**
  AN INTERNAL LOGIC ERROR HAS OCCURRED - MODULE: module_name RSN: reason_code

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIJ005W UNABLE TO LOAD MESSAGE TABLE *table_name* RSN: *reason_code* WILL USE AUIMGENU

Explanation

An attempt to perform a z/OS® LOAD of the message table named (*table_name*) failed. The reason for the failure is described in the reason code field (*reason_code*). The default U.S. English message table will be used. This message follows the AUI006E message.

System action

Processing continues while using the U.S. English message table.

User response

Determine and correct the cause of the message table load failure.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ006E LOAD FAILED FOR MESSAGE TABLE *table_name* RSN: *reason_code*

Explanation

A z/OS® LOAD attempt failed for the message table (*table_name*) indicated.

System action

If the table name is the U.S. English message table, (AUIMGENU) processing will terminate. Other table names will cause the product to attempt to use the U.S. English message table after issuing the AUIJ005W message continue processing.

User response

Determine and correct the cause of the message table load failure.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ007E PROGRAM *program_name* IS NOT EXECUTING APF-AUTHORIZED

Explanation

The program specified requires APF-Authorization to perform its function.

System action

The program terminates.

User response

Ensure that all data sets included within the STEPLIB DD concatenation of the JCL where this message appeared are APF authorized.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ008I ATTEMPTING TO CONNECT TO THE GUARDIUM S-TAP® APPLIANCE. TCP/IP Address: *ip_address*, PORT: *port_number*, PING RATE: *ping_rate*

Explanation

An attempt is being made to establish a connection with the Guardium® S-TAP appliance using the named TCP/IP address (*ip_address*) and PORT number (*port_number*).

PING RATE (*ping_rate*) indicates how often a message is sent to the appliance to provide the appliance with confirmation that the connection is active. The PINGS are sent at the rate indicated (*ping_rate*) which is shown in hour, minutes, and second (*hh:mm:ss*) format.

System action

The connection to the Guardium S-TAP appliance is attempted.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ009E LOAD FAILED FOR MODULE *module_name*. R1: *abend_code* R15: *reason_code*

Explanation

An attempt to perform a z/OS® LOAD of the named module (module_name) has failed

System action

The function terminates.

User response

Ensure that all required product data sets are included in the STEPLIB DD concatenation of the JCL where this message appeared. The value in R1 (*abend-code*) indicates the ABEND code that would have occurred if the failure had not been trapped by the product. The value in R15 (*reason_code*) indicates the reason code associated with the abend. Documentation regarding the abend codes and possible resolutions can be found in the *IBM® z/OS MVS™ System Code* manual or equivalent.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ010I IMS STAP *ver* HAS STARTED.

Explanation

The Security Guardium® S-TAP® for IMS agent component, using the specified base code level, has started.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ011I *function_type* CALL TO GUARDUIM S-TAP APPLIANCE SUCCESSFUL

Explanation

The function request (*function_type*) to the Guardium® S-TAP® appliance completed successfully. This message usually follows the AUIJ008I message indicating that the connection request has been initiated.

Function request values which can be displayed are:

INIT-DLIB
: Connection request from the tasks which transmits DLI/DBB batch events.

INIT-DLIO
: Connection request from the task which transmits IMS Online DLI events.

INIT_LOG
: Connection request from the task which transmits IMS Archive log events.

INIT-SMF
: Connection request from the task which transmits SMF events.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ012I NUMBER OF *event_type* EVENTS SENT TO APPLIANCE: *counter*

Explanation

By default, this message is issued every 100,000 events sent to the appliance or approximately every 18 minutes. You can modify this frequency by using the agent parameter keyword DLIFREQ. This message provides a status of data being collected and sent to the Guardium® S-TAP® appliance. The count provided (*counter*) is the number of events since the last message was issued. The type of events (*event_type*) can include DLIB (events captured from IMS DLI/DBB batch jobs), DLIO (events captured from IMS Online regions) SMF (events captured from SMF auditing), IMSL (events captured from IMS archive log processing), and MLOG (missing IMS logs found during IMS Archive log processing).

System action

Processing continues.

User response

None action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ013E *stap_call* TO GUARDUIM S-TAP® APPLIANCE FAILED *(call source)* IP ADDRESS: *ip_address* STAP_RC = *rc1* STAP_RS = *rs1* GDM_RC = *rc2* PB_RC = *rc3* GDML_RC = *rc4* GDML_RS = *rs2*

Explanation

The requested call *(call_type)* to the Guardium® S-TAP appliance has failed. A non-zero value GDM_RC field indicates an error.

System action

The process terminates.

User response

Determine the cause of the failure by checking the return and reason code.

- If GDM_RC is not zero, one or more of the PB_RC, GDML_RC and GDML_RS will be set.
- If STAP_RC and STAP_RS are zero but GCM_RC or PB_RC is not zero, an internal error is indicated. Contact IBM® Software Support.
- If STAP_RC and STAP_RS are not zero, contact IBM Software Support.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ014E OPEN FAILED FOR DD *dd_name*

Explanation

A z/OS® OPEN of the data set(s) referenced by the DD named (*dd_name*) failed.

System action

Processing terminates.

User response

Examine the JES log for z/OS issued IEA messages issued regarding this DD statement and take appropriate action.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ015E THIS IMS RELEASE IS NOT SUPPORTED. IMS NAME: *ims-name*, VRL: *ims_version*

Explanation

The IMS named (*ims-name*) was found to be of a release which is not supported by this version of the product.

System action

Processing terminates.

User response

Review the software requirements documented in this user's guide for a list of IMS releases that are supported by this version of the product.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ016E UNABLE TO INITIALIZE APPLIANCE INTERFACE *(connection_type)*

Explanation

An attempt to establish a connection with the appliance has failed.

System action

Processing terminates.

User response

This error is usually due to the TCP/IP address specified in the <appliance-server> parameter of the AUICONFG or other member used in the AUICONFG DD statement used to provide the agent with configuration information being incorrect. This error can also occur if the target of the TCP/IP address is unresponsive.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ017I PRIMARY STAP CONNECTION RESTORED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*

Explanation

Multiple appliances are defined to IBM® Guardium® S-TAP® for IMS, and the primary appliance (ip_address + port) was unavailable for some period of time. This message indicates that the primary appliance has become available and is now being used.

System action

Processing continues sending data to the primary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ018W PREVIOUS STAP CONNECTION FAILED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*

Explanation

Multiple appliances are defined to the IMS STAP the connection to the active appliance has failed. This message indicates that another secondary appliance (ip_address + port) is now active.

System action

Processing continues sending data to the secondary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ019E STAP CONNECTION FAILED: NO CONNECTIONS AVAILABLE *(connection_type)* - IP ADDRESS: *ip-address* - PORT : *port*

Explanation

The connection to the active appliance (ip_address + port) has failed and there are no secondary appliances available for use.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ020I All EVENTS HAVE BEEN WRITTEN FROM SPILL AREA TO APPLIANCE *(connection_type)*

Explanation

All audited events that were buffered to the spill area have been sent to the appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ021W EVENTS ARE BEING WRITTEN TO THE SPILL AREA *(connection_type)*

Explanation

A connection to the appliance has been interrupted, and the spill area is being used to buffer audited events until the appliance connection can be reestablished

System action

Processing continues. Audited events are buffered in the spill area.

User response

Investigate the cause of the appliance connection interruption and correct.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ022W SPILL AREA IS FULL: EVENT DATA IS BEING LOST *(connection_type)*

Explanation

A connection to the appliance was interrupted. The spill area was being used to buffer audited events until the appliance connection can be reestablished. The number of audited events that were generated exceeded the number that could be held in the spill area.

System action

Processing continues. Audited events are discarded.

User response

Investigate the cause of the appliance connection interruption and correct. Look for message AUIJ024W, which is issued at task termination or when a connection is reestablished, for the number of lost events.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ023E SPILL AREA IS NOT AVAILABLE *(connection_type)*

Explanation

An attempt to use the spill area to buffer audited events is unsuccessful.

System action

Processing continues. Audited events are discarded.

User response

Specify a value of 1 through 1024 in the SAUISAMP AUICONFG member <SPILL-SIZE> parameter. Review any z/OS error or warning messages that might indicate why the spill area allocation failed.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ024W NUMBER OF *type* EVENTS LOST *count*

Explanation

Attempts to buffer audited events in the spill area have failed. This message indicates the type of audited events (DLIO, DLIB, SMF etc) which were lost (*type*), and the number that were lost (*count*).

System action

Processing continues. Audited events are discarded.

User response

Investigate the cause of the appliance connection interruption and correct.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ042W ZIIP PROCESSING NOT AVAILABLE ON THIS LPAR (type)

Explanation

A request to process data, using a zIIP enabled enclave, has failed because the Workload Manager feature is not available.

System action

Processing continues, using GCPU (General Central Processor Unit) services.

User response

Remove the ZIIP_AGENT_DLI(Y) keyword from the configuration file that is in use, or change the parameter from Y to N.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ044W ZIIP PROCESSING REQUEST HAS BEEN REJECTED *(connection_type)*

Explanation

An attempt to create a zIIP enabled enclave has failed.

System action

Processing continues using GCPU services.

User response

Determine the cause of the failure by reviewing previously issued AUIJ0331E messages and take corrective action.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ055I ZIIP PROCESSING REQUESTED FOR *type* PROCESSING

Explanation

The use of a zIIP enabled enclave has been requested by the use of the ZIIP_AGENT_DLI(Y) configuration file keyword.

System action

An attempt is made to create the enclave.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ056I ZIIP PROCESSING ENABLED FOR type PROCESSING, ENCLAVE TOKEN: *value*

Explanation

A zIIP enabled enclave has been requested and successfully created.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ057W ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED DUE TO ERRORS - PROCESSING WILL CONTINUE USING GCPU

Explanation

zIIP processing was requested, however due to previously reported errors, this mode of processing could not be enabled.

System action

Processing continues using General Central Processing Unit (GCPU) resources only.

User response

Review the processing log looking for error and warning messages that were issued prior to this message to help determine why zIIP processing could not be initiated.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ058W ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED - TRACING IS ENABLED BY THE USE OF THE AUI$NAP JCL STATEMENT

Explanation

Event tracing has been enabled through the addition of the AUI$NAP DD SYSOUT=* JCL statement in the agent JCL. The use of zIIP processing has been disabled because event tracing cannot coexist with the zIIP environment.

System action

All processing continues with event tracing on. Processing occurs on the General Central Processing Unit (GCPU).

User response

If the addition of the AUI$NAP DD statement was not intentional, remove it from the agent JCL.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ201E VSAM ERROR ENCOUNTERED

Explanation

FUNCTION

vsam_function
RPL/RECORD TYPE
rpl/record_value
R15
return_code
R0
reason_code
CSI-CALL
function_call
SUBRTN
pgm_routine

While accessing the VSAM repository, an internal logic error was encountered.

System action

Processing terminates.

User response

There are no user actions available for this failure. Contact IBM® Software Support with the content of this message.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ202E VSAM ERROR ENCOUNTERED

Explanation

While accessing the VSAM repository, an internal logic error was encountered.

FUNCTION:
vsam_function
R15:
return_code
ACBOFLGS:
acboflag_value
CSI-CALL:
function_call
SUBRTN:
pgm_routine

System action

Processing terminates.

User response

There are no user actions available for this failure. Contact IBM® Software Support with the content of this message.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ203E VSAM ERROR ENCOUNTERED

Explanation

While accessing the VSAM repository, an internal logic error was encountered.

FUNCTION:
vsam_function
RPL/RECORD TYPE
rpl/record_value
FDBWD:
rpl_fdbwd
OPTCD:
rpl_optcd
CSI-CALL:
function_call
SUBRTN:
pgm_routine

System action

Processing terminates.

User response

There are no user actions available for this failure. Contact IBM Software Support with the content of this message.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ250I AUDITING IMS EVENTS. COLLECTION PROFILE NAME: *collection_profile_name* IMS NAME: *ims_name* AGENT NAME: *agent name* EXCLUDED REGIONS: *region_types*

Explanation

The auditing of IMS events proceeds by using the collection profile (*collection_profile_name*) that is associated with the IMS definition (*ims_name*). The agent name indicates which agent is processing the audited data. Various region types might have been excluded from auditing, such as AER, BMP, CICS, DBCTL, IFP, MPP, ODBA, or NONE.

System action

Auditing continues.

User response

No action is required.
Note: To set a z/OS message alert for this message, use single-dash formatting between the message number and message text; for example, AUIJ250I - AUDITING IMS EVENTS.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ251E COMPILED FILTER BUILD FAILED. COLLECTION PROFILE NAME : *collection_profile_name* RC: *return_code* RSN: *reason_code*

Explanation

An attempt at building a compiled filter using the collection profile named (*collection_profile_name*) failed.

System action

Processing terminates, auditing will not be performed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ252W GUARDIUM QUARANTINE IS IN EFFECT; DBPCB STATUS CODES OF *AI* MAY OCCUR

Explanation

The Guardium appliance has detected a list of users for whom access is to be restricted for a period of time. This list is based on policy rules and criteria that are set by the Guardium administrator who maintains the auditing rules in your environment.

System action

Processing continues. If a user in the list of quarantined user IDs attempts to issue DB/DLI calls, the DLI call fails. A DB PCB status code of AI, or an AIB return/reason code of 110/C, is returned to the application program.

User response

If access to IMS databases terminate with a DB PCB status code of AI, or an AIB return/reason code of 110/C, contact the Guardium administrator who maintains the auditing rules in your environment to obtain the reason for the quarantine.
Note: To set a z/OS message alert for this message, use single-dash formatting between the message number and message text; for example, AUIJ252W - GUARDIUM QUARANTINE IS IN EFFECT
Parent topic: Error messages and codes: AUIJxxxx

AUIJ255I AUII050I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUII050I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUII050I for details regarding the available output fields.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ256I AUIJ250I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID : *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUIJ250I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUIJ250I for details regarding the available output fields.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ257I AUII120I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUII120I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUII120I for details regarding the available output fields.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ258I AUII052I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUII052I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUII052I for details regarding the available output fields.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ259I JOBNAME *job_name* USING IMS STAP V10.1.3 MODULE: *pgm_name* APAR: *fix_number* DATE: *fix_date*

Explanation

This message echoes message AUII052I, which is generated by the S-TAP code, and can appear in the IMS control region. This message appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ303W *request_type* REQUEST FOR LOG STREAM *log_stream_name* FAILED - RC: *return_code* RS: *reason_code* - WILL CONTINUE TO RETRY

Explanation

A request (*request_type*) made to the indicated log stream (*log_stream_name*) has failed. This is a recoverable situation and the request will be retried.

System action

Processing will continue with the request being retried.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ304A IXGCONN REQUEST FOR LOG_STREAM *log_stream_name* FAILED with RC = *return_code* and RS= *reason_code*

Explanation

An attempt to connect to the z/OS System Logger log-stream, by using the IXGCONN function, has failed.

System action

Auditing is disabled, but IMS continues processing.

User response

Correct the issue that has caused the IXGCONN failure; then, uninstall and reinstall the policy to cause IMS to reattempt the connection. Or, correct the issue; then, stop and restart the Security Guardium® S-TAP® for IMS agent to cause IMS to reattempt the IXGCONN call.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ304E IXGWRITE REQUEST FOR *<log-stream-name>* FAILED - RC: *return_code* RS: *reason_code*

Explanation

An attempt to write to the z/OS® System Logger log-stream using the IXGWRITE function has failed.

System action

One occurrence of this message is issued once per error type (RC + RSN) within the each issuance of message AUII050I. IXGWRITE calls continues until the collection policy for the IMS system is uninstalled, or the DLI/DBB batch job or IMS control region terminates.

User response

Examine the description of the IXGWRITE error using the RC and RSN codes provided in the IBM® z/OS MVS™ Programming: Assembler Services Reference, Vol. 2 (IAR-XCT) or equivalent, under the IXGWRITE Macro description, and take corrective action. The most common reason for the appearance of this message is the volume and the rate (number of events per second) of DLI events exceeds the capacity of the current z/OS System Logger log stream definition.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ307A AUDITED EVENTS ARE BEING LOST DUE TO IXGWRITE ERRORS AND/OR BUFFER SHORTAGES

Explanation

A number of attempts to write audited events to the z/OS® System Logger Log-stream have failed which has caused has resulted in available space in the data buffers being exhausted. This has resulted in DLI events which are to be audited to be discarded.

System action

DLI events continue to be audited at attempts to write exiting data buffers to the z/OS System Logger Log-stream until. The number of DLI events which were rejected are noted in subsequent AUII050I message.

User response

Review any AUIJ304E messages which have been issued to determine the cause of the z/OS System Logger Log-stream Write failures.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ307E *thread_type* THREAD IS TERMINATING DUE TO PROCESSING ERRORS.

Explanation

The agent has determined that a fatal error or abend occurred in the thread type indicated.

System action

Processing that is associated with this thread will not occur.

User response

Examine previously issued error or abend messages to determine the corrective action to be taken. Then, restart the agent.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ330E REQUIRED DATA SET IS NOT CATALOGED. - TYPE: *dsn_type*, DSN: *data_set_name*

Explanation

The data set name indicated (data_set_name) was not found in the z/OS® catalog.

System action

Processing terminates

User response

Specify the name of a cataloged data set.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ331E *service_name* SERVICE FAILED - RC: *return_code* - RSN: *reason_code*

Explanation

A z/OS® service (*service_name*) failed when executed.

System action

Processing terminates.

User response

Determine the cause of the failure by using the return and reason codes provided. Contact IBM® Software Support for additional assistance.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ332E DATA SET IS NOT VALID WITHIN CONTEXT USED - TYPE: *data_set_type,* DSN: *data_set_name*, REASON: *reason*

Explanation

The data set indicated (*data_set_name*) is not of a type valid for use where it is defined. The reason for the rejection of this data set is found in the REASON field (*reason*).

System action

Processing terminates

User response

Specify a data set of the correct type.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ333E Service *SERVICE FAILED* for *DATA SET*: *dsn - R15: return_code*

Explanation

A z/OS LOCATE or OBTAIN service failed when it was run against the specified data set dsn.

System action

Processing terminates.

User response

Ensure that the data set names exists, and has not been migrated. Determine the cause of the failure by examining the LOCATE/OBTAIN MACRO return codes found in the *IBM DFSMSdfp Advanced Services* manual. Contact IBM Software Support for additional assistance
Parent topic: Error messages and codes: AUIJxxxx

AUIJ335W *dd_name* DD IS PRESENT IN THIS JCL, *dsn_types* WILL NOT BE AUDITED

Explanation

The AUIF*stc* task has encountered a DD in the JCL that prevents a specific type of data set from being audited by SMF.

System action

Accesses to the data set types that are specified in the text of this message are not audited.

User response

If you want to audit accesses to these types of data sets, remove the DD statement. See the Data sets and DD DUMMY statements table in the SMF records section of this user's guide for information on which DDs affect which data set types.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ400E INSUFFICIENT MEMORY - MODULE NAME: *program_name* - MEMORY SEGMENT TYPE: *seg_type*

Explanation

An attempt at obtaining memory in program (*module_name*) has failed due to insufficient memory being available.

System action

Processing terminates

User response

Increase the region size of the started task where this message appeared. Restart the started task and retry the request.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ401E MODULE *module_name* FAILED DURING ATTACH of *program_name* - RETURN CODE: *return_code*

Explanation

An attempt to perform a z/OS® ATTACH of the program_name by module module_name has failed.

System action

Processing terminates.

User response

Determine the cause of the failure by using the return code (*return_code*) provided. Correct and restart the task that issued the message. Contact IBM® Software Support for further assistance if need.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ402E CATALOG SERVICE REQUEST FAILED - MODULE NAME: *module_name* - RC: *return_code* RSN: *reason_code*

Explanation

An attempt use the catalog interface has failed.

System action

Processing terminates

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ403E DYNAMIC ALLOCATION FAILURE - FUNCTION : *function_code* - DSN: *data-set-name* - RC: *return_code* RSN: *reason_code*

Explanation

An attempt to issue a dynamic allocation function (*function_code*) using the data set name indicated (*data_set_name*) has failed.

System action

Processing terminates.

User response

Using the *return_code* and *reason_code* determine the cause for the failure. Correct and retry the request.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ404E DYNAMIC ALLOCATION FAILURE - FUNCTION: *function_code* -DDN: *dd_name* - RC: *return_code* RSN: *reason_code*

Explanation

An attempt to issue a dynamic allocation function (*function_code*) using the DD name indicated (*dd_name*) has failed.

System action

Processing terminates.

User response

Using the *return_code* and *reason_code* determine the cause for the failure. Correct and retry the request.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ406W TOO MANY RULES SPECIFIED IN POLICY, REQUEST HAS BEEN TRUNCATED. POLICY: *policy_name*. RULE LIMIT: *max_number_of rules_allowed*

Explanation

Preprocessing of the rules associated with the indicated policy (*policy_name*) determined that the number of rules that were specified in the policy exceeded the rule limit of *max_number_of rules_allowed*. Allowing an excessive number of rules causes memory constraint and performance issues.

System action

The contents of subsequent rules are discarded. Processing continues using all previous rule content.

User response

Review the rules that are included in the policy, and edit the policy to combine the rule content where permissible. If the resulting policy still requires a greater number of rules than the rule limit permits, contact IBM Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ407I *number* DATA SETS ADDED TO POLICY *policy_name* FILTER

Explanation

This message provides the number of data set names that are used as input when building the compiled filter for SMF processing.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ408E POLICY *name* RESULTED IN OVER 102400 DATA SETS TO BE AUDITED; DATA SET RESULT SET HAS BEEN TRUNCATED

Explanation

The specified policy has found over 102,400 data sets to audit based on the databases that are specified in the policy rules and the IMS system log data set (SLDS) and recovery log data set (RLDS) RECON entries. Due to memory constraints, the data set occurrence limit per policy is 102,400 per IMS definition.

System action

Remaining data set names for the database description (DBD) that is being processed are included in the list to be audited, which might cause the 102,400 data set limit to be slightly exceeded. The process that determines the DBD and DSN pairings ends, no additional rules within the policy are processed, and a filter is created for the policy based on the 102,400 (or more) data set names. Normal processing continues.

User response

- Change the policy rules to audit fewer databases, or modify the rules to reduce or avoid multiple rules from auditing the same databases.
- Review the IMS RECON data set that is looking for IMS SLDS and RLDS, database image copy data sets, or database data set group (DSG)/area data sets, which no longer physically exist but remain listed in the RECON. Delete the RECON references that are no longer needed.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ500I STARTING *cycle_type* CYCLE

Explanation

The task is starting the processing cycle specified.

System action

Processing starts for the cycle specified.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ501I NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: - *smf_mask_value*

Explanation

The SMF processing cycle has determined that no new, unprocessed data sets which meet the SMF mask value have been found.

System action

The task waits for the start of the next cycle.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ504I *cycle_type* CYCLE COMPLETE

Explanation

The cycle has completed.

System action

The task waits for the start of the next cycle.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ521W CONTROL BLOCK AUIDCCOM NOT FOUND

Explanation

A critical E/CSA control block was not found.

System action

Processing terminates.

User response

Contact Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ510I ALTERNATE RECON DATA SETS FOUND FOR IMSNAME *imsname*: RECON1: *alt_dsn_1*; RECON2: *alt_dsn_2*, RECON3: *alt_dsn_3*

Explanation

The AUIARCN DD was found in the JCL. The *imsname* that was used when installing the active IMS policy was found in the AUIARCN file, along with alternate RECON data sets names (*alt_dsn_1/2/3*).

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ511E ALTERNATE RECON DATA SET NOT CATALOGED; DSN: *alt_dsn*

Explanation

When attempting to validate the *alt_dsn* value, the data set was not found in the catalog.

System action

Processing continues to validate other specified data set names.

User response

Correct the data set name or catalog the data set.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ512E ALTERNATE RECON DATA SET NOT A VSAM FILE; DSN: *alt_dsn*

Explanation

When attempting to validate the *alt_dsn* value, the data set was found to in a format invalid for processing. The data set name must be in VSAM format.

System action

Processing continues to validate other specified data set names.

User response

Correct the data set name or catalog the data set.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ513E NO VALID ALTERNATE RECON DATA SETS FOUND FOR IMS *imsname*; PROCESSING TERMINATED

Explanation

The data set validation was completed, and no valid alternate RECON data set names found for the IMSNAME.

System action

Processing terminates.

User response

Add or correct valid RECON data set names.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ522E INSUFFICIENT E/CSA STORAGE AVAILABLE FOR *control_block* CONTROL BLOCK

Explanation

Insufficient E/CSA storage was available to hold the specified control block.

System action

Processing terminates.

User response

Determine the cause of the E/CSA shortage.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ609I *event_types* ARE BEING EXCLUDED (*excluded_by*)

Explanation

If the *excluded_by* value is AGENT, then the reporting of *event_types* is excluded due to the specification of certain configuration keywords. If the *excluded_by* value is IMS, these events are excluded as directed by the IMS definition.

System action

Occurrences of these event types are not reported.

User response

If you want to view reports of this event type, review and modify the agent configuration file (SMF_AUDIT_LEVELS or IMSL_AUDIT_LEVELS keywords) or the Guardium system IMS definition, using the Auditing Levels tab.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ800E REQUIRED DD STATEMENT IS MISSING: *dd-name*

Explanation

A critical error has occurred due to a missing DD statement.

System action

Processing terminates.

User response

This message occurs if a product JCL has been edited and a DD statement has been deleted or omitted. If this is not the case, check for any dynamic allocation error messages. If none are present, or are not user resolvable, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ860E VSAM FILE DEFINITION ERROR - DDN: *dd_name* - REASON: *definition_error*

Explanation

When validating the VSAM repository, an allocation definition error was found.

System action

Processing terminates.

User response

The VSAM repository requires specific values for the attribute, LRECL, key length and key position. Review the SAUISAMP product distribution data set member AUISJ001 for the correct file definition specifications.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ999E AN INTERNAL LOGIC ERROR HAS OCCURRED - MODULE: module_name RSN: reason_code

Explanation

An internal logic error has occurred.

System action

Processing terminates

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

Error messages and codes: AUILxxxx

The following information is about error messages and codes that begin with AUIL.

- **AUIL002I**
  Archive log reader interval set to *<number> <time interval in hours/minutes>*.
- **AUIL003E**
  Command *<command-text>*failed; interval value must be between *<lower-bound>* and *<upper-bound>*.
- **AUIL600I**
  NO NEW CATALOGED IMS LOG DATA SETS FOUND
- **AUIL601I**
  PROCESSING IMS LOG DATA SET: *ims_log_data_set_name*
- **AUIL602I**
  PROCESSING COMPLETE FOR IMS LOG DATA SET: *ims_log_data_set_name*
- **AUIL603I**
  SCANNING RECON DATA SETS FOR IMS LOGS TO PROCESS. RECON1: *recon1_dsn* - RECON2: *recon2_dsn* - RECON3: *recon3_dsn*
- **AUIL605I**
  RECON DATA SET SCAN COMPLETE
- **AUIL606W**
  RECON HAS NOCATDS SPECIFIED, RESULTS MAY NOT BE ACCURATE
- **AUIL607W**
  THERE ARE NO ACTIVE IMS POLICIES FOR AGENT *agent_name*
- **AUIL701I**
  IMS LOG CHECKPOINT INFORMATION - IMSID: *IMS_name_from_policy* - RECON1 DSN: *dsn_of_RECON1* - CREATING SSID: *SSID_from_PRILOG* - LAST DSN READ: *dsn_of_SLDS* - LAST UPDATED (UTC): *date_time*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIL002I Archive log reader interval set to *<number> <time interval in hours/minutes>*.

Explanation

The Archive log reader is scheduled to process archive logs as specified.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL003E Command *<command-text>*failed; interval value must be between *<lower-bound>* and *<upper-bound>*.

Explanation

This message indicates that *<command>*, such as: /f AUILSTC,SET INTERVAL number failed because of incorrect *number* value. Correct values must be between *<lower-bound>* and *<upper-bound>*.

User response

Use an interval value between *<lower-bound>* and *<upper-bound>*. If that does not resolve the issue, contact IBM® Software Support.
Parent topic: Error messages and codes: AUILxxxx

AUIL600I NO NEW CATALOGED IMS LOG DATA SETS FOUND

Explanation

After examining the RECON data sets, it has been determined that no new IMS SLDS data sets were found that have yet to be processed by the product.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL601I PROCESSING IMS LOG DATA SET: *ims_log_data_set_name*

Explanation

Processing has started for the IMS SLDS data set indicated (*ims_log_data_set_name*)

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL602I PROCESSING COMPLETE FOR IMS LOG DATA SET: *ims_log_data_set_name*

Explanation

Processing of the IMS SLDS data set has completed.

System action

Processing continues with other candidate IMS SLDS data sets.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL603I SCANNING RECON DATA SETS FOR IMS LOGS TO PROCESS. RECON1: *recon1_dsn* - RECON2: *recon2_dsn* - RECON3: *recon3_dsn*

Explanation

To determine the candidate IMS SLDS data sets to be read, the IMS RECON data sets must be queried. This message indicates that this query process has started.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL605I RECON DATA SET SCAN COMPLETE

Explanation

This message follows the AUIL603I message and indicates that the scan of the RECON data sets is complete.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL606W RECON HAS NOCATDS SPECIFIED, RESULTS MAY NOT BE ACCURATE

Explanation

When examining the RECON data sets the NOCATDS option was found to be on, meaning any log data sets found might not be cataloged.

System action

Processing continues.

User response

The function that produces this message relies on the log data sets existing in the z/OS® catalog or having been in the z/OS catalog at one time. Having the NOCATDS option on in the RECON data sets might negate the validity of further processing, if the SLDS data sets are not cataloged.
Parent topic: Error messages and codes: AUILxxxx

AUIL607W THERE ARE NO ACTIVE IMS POLICIES FOR AGENT *agent_name*

Explanation

A request to query the RECON data sets of IMS systems defined under the named agent found that there were no IMS systems audited by the agent with an active profile. The function that produces this message relies on having at least one IMS system with an active collection policy.

System action

Processing terminates.

User response

Install a collection policy for an IMS under of the control the agent.
Parent topic: Error messages and codes: AUILxxxx

AUIL701I IMS LOG CHECKPOINT INFORMATION - IMSID: *IMS_name_from_policy* - RECON1 DSN: *dsn_of_RECON1* - CREATING SSID: *SSID_from_PRILOG* - LAST DSN READ: *dsn_of_SLDS* - LAST UPDATED (UTC): *date_time*

Explanation

This message provides the name of the IMS SLDS that was last read when processing data for the SSID (*SSID_from_PRILOG*) found in the set of the DBRC RECON data sets (*dsn_of_RECON1*). This information is used as a checkpoint to indicate which SLDS data sets have already been processed, and should not be re-read by the AUILstc tasks.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

Error messages and codes: AUIPxxxx

The following information is about error messages and codes that begin with AUIP.

- **AUIP001E**
  A protobuf message schema violation was detected; value *value* is not a valid boolean value.
- **AUIP002E**
  A protobuf message schema violation was detected; value *value* is not a valid double value.
- **AUIP003E**
  A protobuf message schema violation was detected; value *value* is not a valid integer value.
- **AUIP004E**
  A protobuf message schema violation was detected; required message *message* property *property* is not present.
- **AUIP005E**
  A protobuf message schema violation was detected; required message *message* sub-message *submessage* is not present.
- **AUIP006S**
  A severe error occurred during protobuf message parsing; an unknown exception occurred.
- **AUIP007E**
  A protobuf message schema violation was detected; property name *property* is invalid.
- **AUIP008E**
  A protobuf message schema violation was detected; property *property* value *value* is invalid.
- **AUIP009E**
  A protobuf message schema violation was detected; message name 'name' is invalid.
- **AUIP010E**
  A protobuf message schema violation was detected; message name *name* is invalid (expected *expected name*).
- **AUIP011E**
  A protobuf message schema violation was detected; value *value* is not a valid bytes value.
- **AUIP012E**
  A protobuf message schema violation was detected; value *value* is not a valid unsigned integer value.
- **AUIP013E**
  An error occurred while parsing item text: String is empty.
- **AUIP014E**
  An error occurred while parsing item text: text.
- **AUIP015E**
  Failed to send error message to appliance: *host/port*.
- **AUIP016E**
  Policy rule <rule> was ignored: IMS name is empty.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIP001E A protobuf message schema violation was detected; value *value* is not a valid boolean value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP002E A protobuf message schema violation was detected; value *value* is not a valid double value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP003E A protobuf message schema violation was detected; value *value* is not a valid integer value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP004E A protobuf message schema violation was detected; required message *message* property *property* is not present.

Explanation

The specified message property is not present.

User response

Contact your administrator or IBM® Software Support
Parent topic: Error messages and codes: AUIPxxxx

AUIP005E A protobuf message schema violation was detected; required message *message* sub-message *submessage* is not present.

Explanation

The specified message submessage is not present.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP006S A severe error occurred during protobuf message parsing; an unknown exception occurred.

Explanation

An error occurred while parsing a protobuf message.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP007E A protobuf message schema violation was detected; property name *property* is invalid.

Explanation

The specified property name is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP008E A protobuf message schema violation was detected; property *property* value *value* is invalid.

Explanation

The specified property value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP009E A protobuf message schema violation was detected; message name 'name' is invalid.

Explanation

The specified message name is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP010E A protobuf message schema violation was detected; message name *name* is invalid (expected *expected name*).

Explanation

The specified message name is not valued.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP011E A protobuf message schema violation was detected; value *value* is not a valid bytes value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP012E A protobuf message schema violation was detected; value *value* is not a valid unsigned integer value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP013E An error occurred while parsing item text: String is empty.

Explanation

A policy message contained an item field with an empty value.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP014E An error occurred while parsing item text: text.

Explanation

A policy message contained an item field with a value *text* could not be parsed successfully.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP015E Failed to send error message to appliance: *host/port*.

Explanation

The IBM® Guardium® S-TAP® for IMS agent was unable to send the error message to the specified appliance.

User response

Contact your administrator or IBM Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP016E Policy rule <rule> was ignored: IMS name is empty.

Explanation

The specified policy rule was ignored because it does not apply to any IMS subsystem, or the IMS name is empty.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

Error messages and codes: AUIRxxxx

The following information is about error messages and codes that begin with AUIR.

- **AUIR002E**
  The provided *parameter 'value'* is too long; should be less than or equal to *maximum length* characters.
- **AUIR004E**
  A maximum of *maximum* data sets are allowed for the *names* libs and a total of *libs-count* were specified.
- **AUIR006E**
  The parameter *parameter* can't be empty.
- **AUIR007W**
  Policy_rule_item *<item-name>* for Policy_rule *<rule-name>* has conflicting *<value-name>* values.
- **AUIR008W**
  IMS 050i Max Time threshold was changed from "2460" to "2359".

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIR002E The provided *parameter 'value'* is too long; should be less than or equal to *maximum length* characters.

Explanation

The value of the specified *parameter* exceeds the maximum length *maximum length*.

User response

Specify a shorter value that does not exceed the specified limit for the parameter.
Parent topic: Error messages and codes: AUIRxxxx

AUIR004E A maximum of *maximum* data sets are allowed for the *names* libs and a total of *libs-count* were specified.

Explanation

The maximum number of data sets was exceeded for the libs specified.

User response

Limit the number of data sets for the specified libs to *maximum*.
Parent topic: Error messages and codes: AUIRxxxx

AUIR006E The parameter *parameter* can't be empty.

Explanation

The parameter value must be specified in the agent configuration.

User response

Update agent configuration, or contact your administrator.
Parent topic: Error messages and codes: AUIRxxxx

AUIR007W Policy_rule_item *<item-name>* for Policy_rule *<rule-name>* has conflicting *<value-name>* values.

Explanation

The Guardium policy was processed but there are conflicting fields in the definition. Only one of the policies has been applied.

User response

Check the policy definition, and change the specified values to eliminate the conflict.
Parent topic: Error messages and codes: AUIRxxxx

AUIR008W IMS 050i Max Time threshold was changed from "2460" to "2359".

Explanation

An invalid time value was supplied through the use of the Message AUII050I Frequency field of the IMS definition screen of the Guardium® appliance. The invalid value was automatically corrected by the agent.

System action

Processing continues.

User response

When convenient, update the invalid time value in the IMS definition to a value within the range of 00:10 -- 23:59.
Parent topic: Error messages and codes: AUIRxxxx

Error messages and codes: AUITxxxx

The following information is about error messages and codes that begin with AUIT.

- **AUIT001E**
  The specified user ID *userid* is not defined or does not have an OMVS segment defined.
- **AUIT006S**
  The product is not properly configured to authenticate users.
- **AUIT008E**
  The configuration file *filename* is invalid; the root element *element* is not <agent-config>.
- **AUIT010E**
  An error occurred while opening the configuration file *filename message text*
- **AUIT012I**
  Performing discovery of available locations.
- **AUIT013I**
  Security Guardium® S-TAP® for IMS agent is terminating.
- **AUIT014I**
  Connected to server *<host>* on port *<port>*.
- **AUIT015I**
  Attempting connection to server *<host>* on port *<port>*.
- **AUIT017I**
  Discovered subsystem *subsystem-id*.
- **AUIT019I**
  Security Guardium S-TAP for IMS agent started on *<lpar _name> (<lpar_ip>)*.
- **AUIT020I**
  Starting the socket selector thread (thread *thread id*).
- **AUIT023I**
  Received shutdown request.
- **AUIT025I**
  The socket selector thread is terminating.
- **AUIT028E**
  An error occurred while authenticating user *user-id error-text*.
- **AUIT031I**
  Starting the command listener thread (thread *thread-id*).
- **AUIT032I**
  Received stop command: *command-text*.
- **AUIT033I**
  Received modify command: *command-text*.
- **AUIT034S**
  Security Guardium S-TAP for IMS agent is terminating due to hard stop request.
- **AUIT044E**
  The connection to the server has been lost.
- **AUIT047E**
  IBM® Security Guardium S-TAP for IMS on z/OS® agent ended with RC = *[rc]*.
- **AUIT048I**
  Issuing request to capture service dump.
- **AUIT049I**
  Request to capture service dump has completed successfully.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIT001E The specified user ID *userid* is not defined or does not have an OMVS segment defined.

Explanation

You specified a user ID that is not defined or does not have an OMVS segment defined.

User response

Security Guardium® S-TAP® for IMS was unable to authenticate the specified user. Either specify a valid user ID, or if the user ID is valid, see your security administrator to have an OMVS segment defined for the user ID.

Parent topic: Error messages and codes: AUITxxxx

AUIT006S The product is not properly configured to authenticate users.

Explanation

Security Guardium® S-TAP® for IMS is not properly configured to authenticate users.

User response

An error occurred while authenticating a remote user request. The error code indicates that the installation configuration required to allow this authentication has not been completed. See IBM Guardium S-TAP for IMS agent for more information about how to complete the required configuration.
Parent topic: Error messages and codes: AUITxxxx

AUIT008E The configuration file *filename* is invalid; the root element *element* is not <agent-config>.

Explanation

The configuration file identified in the message is invalid.

User response

The contents of the specified configuration file are invalid. Correct the file contents to specify <agent-config> as the root XML element.

Parent topic: Error messages and codes: AUITxxxx

AUIT010E An error occurred while opening the configuration file *filename message text*

Explanation

An error occurred while opening the configuration file identified in the message. Additional error information is also contained within the message.

User response

Use the specified message text to diagnose the error that occurred. Specify a valid configuration file that is not in use by any other process.

Parent topic: Error messages and codes: AUITxxxx

AUIT012I Performing discovery of available locations.

Explanation

The Security Guardium® S-TAP® for IMS agent is looking for available locations.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT013I Security Guardium® S-TAP® for IMS agent is terminating.

Explanation

The Security Guardium S-TAP for IMS agent is terminating.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT014I Connected to server *<host>* on port *<port>*.

Explanation

The Security Guardium® S-TAP® for IMS agent task has connected to the S-TAP to the specified host and port.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT015I Attempting connection to server *<host>* on port *<port>*.

Explanation

The Security Guardium® S-TAP® for IMS agent is attempting to connect to the specified host and port number.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT017I Discovered subsystem *subsystem-id*.

Explanation

The Security Guardium® S-TAP® for IMS agent has discovered the identified subsystem.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT019I Security Guardium® S-TAP® for IMS agent started on *<lpar _name> (<lpar_ip>)*.

Explanation

The IBM® Guardium S-TAP for IMS agent has started.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT020I Starting the socket selector thread (thread *thread id*).

Explanation

The Security Guardium® S-TAP® for IMS agent is starting the identified socket selector thread.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT023I Received shutdown request.

Explanation

The Security Guardium® S-TAP® for IMS agent has received a shutdown request.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT025I The socket selector thread is terminating.

Explanation

The Security Guardium® S-TAP® for IMS agent socket selector thread is terminating.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT028E An error occurred while authenticating user *user-id error-text*.

Explanation

An unexpected return code was returned by the *pthread_security_np()* callable service.

User response

Ensure that the configuration required to use this service has been completed. See IBM Guardium S-TAP for IMS agent for more information about the required configuration. Check the agent job log for additional messages which might be generated.

Parent topic: Error messages and codes: AUITxxxx

AUIT031I Starting the command listener thread (thread *thread-id*).

Explanation

The Security Guardium® S-TAP® for IMS agent is starting the command listener thread.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT032I Received stop command: *command-text*.

Explanation

The Security Guardium® S-TAP® for IMS agent received a STOP command.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT033I Received modify command: *command-text*.

Explanation

The Security Guardium® S-TAP® for IMS agent received a MODIFY command.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT034S Security Guardium® S-TAP® for IMS agent is terminating due to hard stop request.

Explanation

Security Guardium S-TAP for IMS agent is terminating due to a user /MODIFY FORCE command.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT044E The connection to the server has been lost.

Explanation

The Security Guardium® S-TAP® for IMS agent task is unable to communicate with the Security Guardium S-TAP for IMS agent.

User response

Resolve any network connectivity issues, then try logging in again.
Parent topic: Error messages and codes: AUITxxxx

AUIT047E IBM® Security Guardium® S-TAP® for IMS on z/OS® agent ended with RC = *[rc]*.

Explanation

Due to a prior error, the agent has ended with the specified return code.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUITxxxx

AUIT048I Issuing request to capture service dump.

Explanation

A command, such as /f AUIASTC,DUMP/DDX, has been issued for processing.

User response

No action is required.
Parent topic: Error messages and codes: AUITxxxx

AUIT049I Request to capture service dump has completed successfully.

Explanation

A command, such as /f AUIASTC,DUMP/DDX has processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUITxxxx

Error messages and codes: AUIUxxxx

The following information is about error messages and codes that begin with AUIU.

- **AUIUR002I**
  Migrate Utility for IBM® Security Guardium® S-TAP® for IMS on z/OS® started.
- **AUIUR003I**
  Agent record *<agent name>* was not found in the repository.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIUR002I Migrate Utility for IBM® Security Guardium® S-TAP® for IMS on z/OS® started.

Explanation

The utility to migrate the configuration of an older version of the product to the current product version has started.

User response

No action is required.
Parent topic: Error messages and codes: AUIUxxxx

AUIUR003I Agent record *<agent name>* was not found in the repository.

Explanation

An attempt to read an agent record from the repository while migration failed as the record was not found.

System action

The agent record migration fails, processing continues.

User response

Check the configuration file for agent and repository names and use the Guardium user interface to verify that the specified agent definition is presented in specified repository.
Parent topic: Error messages and codes: AUIUxxxx

Error messages and codes: AUIXxxxx

The following information is about error messages and codes that begin with AUIX.

- **AUIX013E**
  A shared memory error occurred on "*service name*": *error message*.
- **AUIX014E**
  An XML schema violation was detected; value *value* is not a valid boolean value.
- **AUIX015E**
  An XML schema violation was detected; value *value* is not a valid double value.
- **AUIX016E**
  An XML schema violation was detected; value *value* is not a valid integer value.
- **AUIX017E**
  An XML syntax error was detected at offset *offset*; expected *expected-value*, found *found-value*.
- **AUIX018E**
  An XML schema violation was detected; required element *element* attribute *attribute*\" is not present.

- **AUIX019E**
  An XML schema violation was detected; required element *<element>* child *<child-element>* is not present.
- **AUIX020E**
  Memory allocation failed (*number* bytes).
- **AUIX021E**
  An XML schema violation was detected; element *element* child *child-number* has wrong type.
- **AUIX022E**
  An XML syntax error was detected; character reference *character-reference* is invalid.
- **AUIX023E**
  An XML syntax error was detected; entity reference *entity-reference* is invalid.
- **AUIX024E**
  An XML syntax error was detected; more than one element was found at the root of the document.
- **AUIX025E**
  An XML syntax error was detected; no element was found at the root of the document.
- **AUIX026E**
  An XML syntax error was detected; text was found at the root of the document.
- **AUIX027S**
  A severe error occurred during XML parsing; an unknown exception occurred.
- **AUIX028E**
  The command line option *<option name>* is invalid.
- **AUIX034S**
  A severe error occurred during command line processing; an unknown exception occurred.
- **AUIX035E**
  The operation completed successfully.
- **AUIX036E**
  The address family is not supported by the protocol family (*socket-return-code*).
- **AUIX037E**
  The operation is still in progress (*socket-return-code*).
- **AUIX038E**
  Permission is denied (*socket-return-code*).
- **AUIX039E**
  The network is down (*socket-return-code*).
- **AUIX040E**
  No buffer space is available (*socket-return-code*).
- **AUIX041E**
  Too many sockets have been opened (*socket-return-code*).
- **AUIX042E**
  The protocol is not supported (*socket-return-code*).
- **AUIX043E**
  The WSAStartup routine was not called (*socket-return-code*).
- **AUIX044E**
  The protocol is the wrong type for the socket (*socket-return-code*).
- **AUIX045E**
  The socket type is not supported (*socket-return-code*).
- **AUIX046E**
  The destination network is unreachable (*socket-return-code*).
- **AUIX047E**
  The socket handle is invalid (*socket-return-code*).
- **AUIX048E**
  The address is already in use (*socket-return-code*).
- **AUIX049E**
  The function call was interrupted (*socket-return-code*
- **AUIX050E**
  The requested address is not available (*socket-return-code*).
- **AUIX051E**
  The connection was aborted (*socket-return-code*).
- **AUIX052E**
  The connection was refused by the partner (*socket-return-code*).
- **AUIX053E**
  The connection was reset by the partner (*socket-return-code*).
- **AUIX054E**
  The network message is too long (*socket-return-code*).
- **AUIX055E**
  The network dropped the connection when reset (*socket-return-code*).
- **AUIX056E**
  An invalid parameter was specified (*socket-return-code*).
- **AUIX057E**
  The socket is not connected (*socket-return-code*).
- **AUIX058E**
  The operation is not supported (*socket-return-code*).
- **AUIX059E**
  The socket has been closed (*socket-return-code*).
- **AUIX060E**
  The socket is already connected (*socket-return-code*).
- **AUIX061S**
  An unknown error occurred (*socket-return-code*).
- **AUIX062E**
  A socket error occurred on *socket-operation* with RC = *return code*: *message-text*.
- **AUIX063E**
  A socket select error occurred: *message-text*.

- **AUIX064E**
  An XML schema violation was detected; expected root element *element-expected*, but found *element-found* instead.
- **AUIX066E**
  An XML schema violation was detected; element *element* value *value* is invalid.
- **AUIX067E**
  An XML schema violation was detected; element name *element* is invalid.
- **AUIX068E**
  An XML schema violation was detected; element name *element-found* is invalid (expected *element-expected*).
- **AUIX074E**
  An abend occurred: *<abend code>*.
- **AUIX076E**
  An XML schema violation was detected; element *element* attribute *attribute* value *value* is invalid.
- **AUIX085E**
  A dynamic allocation error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX086E**
  A dynamic concatenation error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX087E**
  A dynamic free error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX088E**
  An invalid dynamic allocation parameter was specified: code = *parm-code*.
- **AUIX093S**
  An unexpected error occurred (*file-name*, *line-number*).
- **AUIX094S**
  An unexpected error occurred with token *token*, (*file-name*, *line-number*).
- **AUIX095S**
  An unexpected error occurred with tokens *token* and *token* (*file-name*, *line-number*).
- **AUIX096S**
  An unexpected error occurred with tokens *token*, *token* and *token* (*file-name*, *line-number*).
- **AUIX097S**
  An unexpected error occurred with tokens *token*, *token*, *token*, and *token* (*file-name*, *line-number*.
- **AUIX098E**
  A thread error occurred on *thread-operation* : *message-text*.
- **AUIX101E**
  An event error occurred on *event-operation* : *message-text*.
- **AUIX104E**
  A mutex error occurred on *mutex-operation* : *message-text*.
- **AUIX109E**
  A semaphore error occurred on *semaphore-operation* : *message-text*.
- **AUIX110I**
  The network connection has been disconnected.
- **AUIX114E**
  A dynamic allocation query error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX115E**
  An input command error occurred on \"*command-operation*\": *message-text*.
- **AUIX116I**
  Received input command: *command-text*.
- **AUIX122I**
  Build date *component* = *date*.
- **AUIX123W**
  The action was cancelled.
- **AUIX124S**
  The task is not running APF-authorized.
- **AUIX126E**
  A DLL error occurred on *dll-operation* : *message-text*
- **AUIX127S**
  An error occurred while opening log file *file-name*.
- **AUIX142E**
  An XML schema violation was detected; element *element* value *value* is invalid: expected min *<min-value>* and max *<max value>*.
- **AUIX143E**
  An XML schema violation was detected; element *element* attribute *value* value *value* is invalid: expected min *<minimum>* and max *<maximum>*.
- **AUIX149E**
  Data set *[data set]* is not cataloged.
- **AUIX150E**
  Invalid data set *'data set'*: Data set name must not exceed 44 characters.
- **AUIX151E**
  Invalid data set *{'data set'}*: The segment length must be greater than 0 and less than or equal to 8.
- **AUIX152E**
  Invalid data set *'name'*: The first character in each segment must be alphabetic (A-Z) or national (#, @, $).
- **AUIX153E**
  Invalid data set *'<data set>'*: The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.
- **AUIX154E**
  Invalid data set *'<data set>'*: The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).
- **AUIX155E**
  Data set *<data set>* is not APF-authorized.
- **AUIX156E**
  Invalid data set *'<data set>'*: The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).
- **AUIX160E**
  A dynamic allocation query error occurred: info code = *<info-code>*, error code = *<error-code>*, DD name = *<dd-name>*.

- **AUIX183E**
  The number of file descriptors (sockets) has exceeded maximum = <*number*>.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIX013E A shared memory error occurred on "*service name*": *error message*.

Explanation

This error can occur in the primary agent address space. When the error occurs, the primary agent address space will shut down with a CC of 12. This startup error indicates that attempts to create a shared memory segment failed because of an already existing shared memory segment that never belonged to, or currently does not belong to, the primary agent address space.

This message can occur in the secondary address space if the <id> elements in the ADS_SHM_ID and ADS_LISTENER_PORT parameters do not match in the AUICONFG configuration member that is used by the agent primary address space and the secondary address spaces.

User response

Edit SAUISAMP member AUICONFG (or the customized AUICONFG) and specify the correct <id> elements in the ADS_SHM_ID and ADS_LISTENER_PORT parameters.
Parent topic: Error messages and codes: AUIXxxxx

AUIX014E An XML schema violation was detected; value *value* is not a valid boolean value.

Explanation

An XML schema violation was detected; value value is not a valid boolean value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX015E An XML schema violation was detected; value *value* is not a valid double value.

Explanation

An XML schema violation was detected; value *value* is not a valid double value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX016E An XML schema violation was detected; value *value* is not a valid integer value.

Explanation

An XML schema violation was detected; value value is not a valid integer value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX017E An XML syntax error was detected at offset *offset*; expected *expected-value*, found *found-value*.

Explanation

An XML syntax error was detected at offset offset; expected expected-value, found found-value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX018E An XML schema violation was detected; required element *element* attribute *attribute*\" is not present.

Explanation

An XML schema violation was detected; required element element attribute attribute is not present.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX019E An XML schema violation was detected; required element *<element>* child *<child-element>* is not present.

Explanation

The XML schema must contain the specified elements.

User response

Correct the XML schema and retry.
Parent topic: Error messages and codes: AUIXxxxx

AUIX020E Memory allocation failed (*number* bytes).

Explanation

Memory allocation failed (number bytes).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX021E An XML schema violation was detected; element *element* child *child-number* has wrong type.

Explanation

An XML schema violation was detected; element element child child-number has wrong type.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX022E An XML syntax error was detected; character reference *character-reference* is invalid.

Explanation

An XML syntax error was detected; character reference character-reference is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX023E An XML syntax error was detected; entity reference *entity-reference* is invalid.

Explanation

An XML syntax error was detected; entity reference entity-reference is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX024E An XML syntax error was detected; more than one element was found at the root of the document.

Explanation

An XML syntax error was detected; more than one element was found at the root of the document.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX025E An XML syntax error was detected; no element was found at the root of the document.

Explanation

An XML syntax error was detected; no element was found at the root of the document.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX026E An XML syntax error was detected; text was found at the root of the document.

Explanation

An XML syntax error was detected; text was found at the root of the document.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX027S A severe error occurred during XML parsing; an unknown exception occurred.

Explanation

A severe error occurred during XML parsing; an unknown exception occurred.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX028E The command line option *<option name>* is invalid.

Explanation

The command line option, which is specified in the message text, is invalid.

User response

Correct the command line option and retry the operation. Review the IBM® Guardium® S-TAP® for IMS client/server environment information for valid options.

Parent topic: Error messages and codes: AUIXxxxx

AUIX034S A severe error occurred during command line processing; an unknown exception occurred.

Explanation

A severe error occurred during command line processing; an unknown exception occurred.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX035E The operation completed successfully.

Explanation

The operation completed successfully.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX036E The address family is not supported by the protocol family (*socket-return-code*).

Explanation

The address family is not supported by the protocol family (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX037E The operation is still in progress (*socket-return-code*).

Explanation

The operation is still in progress (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX038E Permission is denied (*socket-return-code*).

Explanation

Permission is denied (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX039E The network is down (*socket-return-code*).

Explanation

The network is down (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX040E No buffer space is available (*socket-return-code*).

Explanation

No buffer space is available (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX041E Too many sockets have been opened (*socket-return-code*).

Explanation

Too many sockets have been opened (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX042E The protocol is not supported (*socket-return-code*).

Explanation

The protocol is not supported (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX043E The WSAStartup routine was not called (*socket-return-code*).

Explanation

The WSAStartup routine was not called (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX044E The protocol is the wrong type for the socket (*socket-return-code*).

Explanation

The protocol is the wrong type for the socket (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX045E The socket type is not supported (*socket-return-code*).

Explanation

The socket type is not supported (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX046E The destination network is unreachable (*socket-return-code*).

Explanation

The destination network is unreachable (socket-return-code).

User response

Specify the correct host name or IP address.

Parent topic: Error messages and codes: AUIXxxxx

AUIX047E The socket handle is invalid (*socket-return-code*).

Explanation

The socket handle is invalid (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX048E The address is already in use (*socket-return-code*).

Explanation

The address is already in use (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX049E The function call was interrupted (*socket-return-code*

Explanation

The function call was interrupted (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX050E The requested address is not available (*socket-return-code*).

Explanation

The requested address is not available (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX051E The connection was aborted (*socket-return-code*).

Explanation

The connection was aborted (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX052E The connection was refused by the partner (*socket-return-code*).

Explanation

The connection was refused by the partner (socket-return-code).

User response

Verify that the correct port number was specified, and that the partner application has been started and is available.

Parent topic: Error messages and codes: AUIXxxxx

AUIX053E The connection was reset by the partner (*socket-return-code*).

Explanation

The connection was reset by the partner (socket-return-code).

User response

The partner application ended the network connection. If this is unexpected, diagnose the partner application failure. Otherwise, no action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX054E The network message is too long (*socket-return-code*).

Explanation

The network message is too long (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX055E The network dropped the connection when reset (*socket-return-code*).

Explanation

The network dropped the connection when reset (socket-return-code

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX056E An invalid parameter was specified (*socket-return-code*).

Explanation

An invalid parameter was specified (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX057E The socket is not connected (*socket-return-code*).

Explanation

The socket is not connected (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX058E The operation is not supported (*socket-return-code*).

Explanation

The operation is not supported (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX059E The socket has been closed (*socket-return-code*).

Explanation

The socket has been closed (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX060E The socket is already connected (*socket-return-code*).

Explanation

The socket is already connected (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX061S An unknown error occurred (*socket-return-code*).

Explanation

An unknown error occurred (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX062E A socket error occurred on *socket-operation* with RC = *return code*: *message-text*.

Explanation

A socket error occurred.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX063E A socket select error occurred: *message-text*.

Explanation

A socket select error occurred.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX064E An XML schema violation was detected; expected root element *element-expected*, but found *element-found* instead.

Explanation

An XML schema violation was detected; expected root element element-expected , but found element-found instead.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX066E An XML schema violation was detected; element *element* value *value* is invalid.

Explanation

An XML schema violation was detected; element element value value is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX067E An XML schema violation was detected; element name *element* is invalid.

Explanation

An XML schema violation was detected; element name element is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX068E An XML schema violation was detected; element name *element-found* is invalid (expected *element-expected*).

Explanation

An XML schema violation was detected; element name element-found is invalid (expected element-expected).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX074E An abend occurred: *<abend code>*.

Explanation

This message indicates a callable service abend has occurred. Additional diagnostic information might be present in the message when applicable.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIXxxxx

AUIX076E An XML schema violation was detected; element *element* attribute *attribute* value *value* is invalid.

Explanation

An XML schema violation was detected; element element attribute attribute value value is invalid.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX085E A dynamic allocation error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic allocation error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX086E A dynamic concatenation error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic concatenation error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX087E A dynamic free error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic free error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX088E An invalid dynamic allocation parameter was specified: code = *parm-code*.

Explanation

An invalid dynamic allocation parameter was specified: code = parm-code.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX093S An unexpected error occurred (*file-name*, *line-number*).

Explanation

An unexpected error occurred (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX094S An unexpected error occurred with token *token*, (*file-name*, *line-number*).

Explanation

An unexpected error occurred with token token, (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX095S An unexpected error occurred with tokens *token* and *token* (*file-name*, *line-number*).

Explanation

An unexpected error occurred with tokens token and token (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX096S An unexpected error occurred with tokens *token*, *token* and *token* (*file-name*, *line-number*).

Explanation

An unexpected error occurred with tokens token, token and token (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX097S An unexpected error occurred with tokens *token*, *token*, *token*, and *token* (*file-name*, *line-number*.

Explanation

An unexpected error occurred with tokens token, token, token, and token (file-name, line-number.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX098E A thread error occurred on *thread-operation* : *message-text*.

Explanation

A thread error occurred on thread-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX101E An event error occurred on *event-operation* : *message-text*.

Explanation

An event error occurred on event-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX104E A mutex error occurred on *mutex-operation* : *message-text*.

Explanation

A mutex error occurred on mutex-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX109E A semaphore error occurred on *semaphore-operation* : *message-text*.

Explanation

A semaphore error occurred on semaphore-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX110I The network connection has been disconnected.

Explanation

The network connection has been disconnected.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX114E A dynamic allocation query error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic allocation query error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified info and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX115E An input command error occurred on \"*command-operation*\": *message-text*.

Explanation

An input command error occurred on \"command-operation\": message-text.

User response

Contact IBM® Customer Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX116I Received input command: *command-text*.

Explanation

Received input command: command-text.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX122I Build date *component* = *date*.

Explanation

Build date component = date.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX123W The action was cancelled.

Explanation

The action was cancelled.

User response

No action is required. The operation was cancelled due to user or administrator request.

Parent topic: Error messages and codes: AUIXxxxx

AUIX124S The task is not running APF-authorized.

Explanation

The task is not running APF-authorized.

User response

The Security Guardium® S-TAP® for IMS load library, and the load libraries for all of the IMS subsystems accessed, must be APF-authorized. See IBM Guardium S-TAP for IMS agent for more information about the required configuration steps.

Parent topic: Error messages and codes: AUIXxxxx

AUIX126E A DLL error occurred on *dll-operation* : *message-text*

Explanation

A DLL error occurred on dll-operation : message-text

User response

Contact IBM® Customer Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX127S An error occurred while opening log file *file-name*.

Explanation

An error occurred while opening log file file-name.

User response

Contact IBM® Customer Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX142E An XML schema violation was detected; element *element* value *value* is invalid: expected min *<min-value>* and max *<max value>*.

Explanation

The *element-value* given for *element-name* is out of the range and must be within *min-value* and *max-value*.

User response

Correct the value for the *element-name* in the configuration.

Parent topic: Error messages and codes: AUIXxxxx

AUIX143E An XML schema violation was detected; element *element* attribute *value* value *value* is invalid: expected min *<minimum>* and max *<maximum>*.

Explanation

The element attribute value is not valid.

User response

If the error occurred while reading the agent configuration file, update the configuration. Otherwise, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIXxxxx

AUIX149E Data set *[data set]* is not cataloged.

Explanation

The data set specified in the message text has not been cataloged.

User response

Allocate the data set.
Parent topic: Error messages and codes: AUIXxxxx

AUIX150E Invalid data set *'data set'*: Data set name must not exceed 44 characters.

Explanation

MVS™ data sets cannot exceed 44 characters.

User response

Correct the data set entry, then retry.
Parent topic: Error messages and codes: AUIXxxxx

AUIX151E Invalid data set *{'data set'}*: The segment length must be greater than 0 and less than or equal to 8.

Explanation

The specified data set name has one or more segments that are not between 1 and 8 characters.

User response

Specify a data set where each segment contains more than 0 characters and 8 or fewer characters.
Parent topic: Error messages and codes: AUIXxxxx

AUIX152E Invalid data set *'name'*: The first character in each segment must be alphabetic (A-Z) or national (#, @, $).

Explanation

The data set name provided does not is not a valid name and does not satisfy the MVS™ data set naming requirements.

User response

Correct the data set name and try again.
Parent topic: Error messages and codes: AUIXxxxx

AUIX153E Invalid data set *'<data set>'*: The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.

Explanation

The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.

User response

Specify a data set where non-first characters in the segments is alphabetic (A-Z), numeric, national (#, @, $), or hyphen.
Parent topic: Error messages and codes: AUIXxxxx

AUIX154E Invalid data set '*<data set>*': The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).

Explanation

The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).

User response

Specify a data set where non-first characters in the SMF segments is alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).
Parent topic: Error messages and codes: AUIXxxxx

AUIX155E Data set *<data set>* is not APF-authorized.

Explanation

The specified data set requires APF authorization.

User response

The specified data set must be APF-authorized. See Configuration overview for more information about the required configuration steps.
Parent topic: Error messages and codes: AUIXxxxx

AUIX156E Invalid data set '*<data set>*': The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).

Explanation

The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).

User response

Specify a data set where first character in SMF segments must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).
Parent topic: Error messages and codes: AUIXxxxx

AUIX160E A dynamic allocation query error occurred: info code = *<info-code>*, error code = *<error-code>*, DD name = *<dd-name>*.

Explanation

A dynamic allocation query error occurred with the specified information code, error code, and DD name.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified info and error codes.
Parent topic: Error messages and codes: AUIXxxxx

AUIX183E The number of file descriptors (sockets) has exceeded maximum = *<number>*.

Explanation

The active program holds too many file or socket descriptors and exceeded system maximum = *<number>*.

User response

Contact your system administrator or IBM Software Support.
Parent topic: Error messages and codes: AUIXxxxx

Error messages and codes: AUIYxxxx

The following information is about error messages and codes that begin with AUIY.

- **AUIY001E**
  A callable services abend *abend* has occurred.
- **AUIY002E**
  GPRS *number-number*: *hex-value hex-value hex-value hex-value*
- **AUIY003E**
  Active module not found.
- **AUIY004E**
  Active module = *module-name*, load point = *hex-address*, offset = *hex-address*
- **AUIY005E**
  PSW = *string string*
- **AUIY006E**
  Callable service invocation failed with return code = *return-code* and reason code = *reason-code*
- **AUIY007I**
  Invoking callable service *callable service*.
- **AUIY008I**
  Returned from callable service *service-name*
- **AUIY009E**
  Invalid data set mask: *data set mask*.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIY001E A callable services abend *abend* has occurred.

Explanation

This message indicates a callable service abend has occurred. Additional diagnostic information is be present in the message when applicable.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIYxxxx

AUIY002E GPRS *number-number*: *hex-value hex-value hex-value hex-value*

Explanation

This message indicates an CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY003E Active module not found.

Explanation

This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY004E Active module = *module-name*, load point = *hex-address*, offset = *hex-address*

Explanation

This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY005E PSW = *string string*

Explanation

This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY006E Callable service invocation failed with return code = *return-code* and reason code = *reason-code*

Explanation

A service requested by the agent task has failed.

User response

View the JES log of the agent task to determine the data set name and reason for the error. Contact IBM® Software Support if you are unable to resolve the error.
Parent topic: Error messages and codes: AUIYxxxx

AUIY007I Invoking callable service *callable service*.

Explanation

The specified callable service has been invoked successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY008I Returned from callable service *service-name*

Explanation

Returned from a callable service that is identified in the message.

User response

No action is required.

Parent topic: Error messages and codes: AUIYxxxx

AUIY009E Invalid data set mask: *data set mask*.

Explanation

The specified data set mask is not valid.

User response

Enter a valid data set mask and retry.
Parent topic: Error messages and codes: AUIYxxxx

Error messages and codes: AUIZxxxx

The following information is about error messages and codes that begin with AUIZ.

- **AUIZ002E**
  dd-name DD has already been allocated.
- **AUIZ003W**
  Attached to existing shared memory segment.
- **AUIZ004S**
  Shared memory segment key verification failed ('*key-value*').
- **AUIZ005S**
  Shared memory segment eyecatcher 'value' invalid.
- **AUIZ007S**
  The master address space failed to respond to a connect request.
- **AUIZ008W**
  IBM® Security Guardium® S-TAP® for IMS on z/OS® agent failed to shut down properly last time.
- **AUIZ009S**
  Attempts to attach to shared memory segment *segment key* failed.
- **AUIZ010W**
  Configuration value for <*parameter*> is set below the allowed minimum of <*limit*>.
- **AUIZ011W**
  Configuration value for <*parameter*> is set above the allowed maximum of <*limit*>.

- **AUIZ012I**
  Log-server: listening on port *<port>*.
- **AUIZ013E**
  Log-server: no available port was found in the range *<min-port>-<max-port>*.
- **AUIZ014W**
  Log-server: invalid data received from client *<client-ip>* (*<header-data>*).
- **AUIZ020W**
  Configuration parameter *parameter-name* was ignored: duplicate value specified *specified-value*.
- **AUIZ021E**
  Configuration parameter *option* can't be empty.
- **AUIZ022E**
  At least one active appliance is required.
- **AUIZ023E**
  Duplicate appliance specified: *host/port*.
- **AUIZ024E**
  Duplicate appliance priority specified: *priority*.
- **AUIZ025E**
  Spill size can't be zero if more than one appliance is enabled.
- **AUIZ026E**
  Configuration parameter *<option>* value *<value>* is invalid; expected list *<value-list>*.
- **AUIZ027W**
  Host name can't be resolved *<host-name>*.
- **AUIZ028E**
  Configuration parameter *element-name* value *element-value* is invalid: expected min *value-min* and max *value-max*.
- **AUIZ029E**
  Property *property-name* not found in config.
- **AUIZ030E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid long value.
- **AUIZ031E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned long value.
- **AUIZ032E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid short value.
- **AUIZ033E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned short value.
- **AUIZ034E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid boolean value.
- **AUIZ035E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid double value.
- **AUIZ036E**
  Configuration parameter *element-name* value *element-value* length is invalid: expected min *length-min* and max *length-max* characters.
- **AUIZ037I**
  Collection profile *profile* uninstalled successfully.
- **AUIZ038I**
  Collection profile *profile* installed successfully.
- **AUIZ039I**
  Guardium policy processing started.
- **AUIZ040I**
  Guardium policy processing finished [active = *<number1>*, installed = *<number2>*, uninstalled = *<number3>*].
- **AUIZ041E**
  Profile for IMS source *ims_name* was ignored: unknown IMS.
- **AUIZ041W**
  Profile for IMS source *ims_name* was ignored: unknown IMS.
- **AUIZ042W**
  IMS artifact *ims-name* was ignored: invalid IMS definition.
- **AUIZ043E**
  XCF callable service invocation failed: function *function-name*, RC = *nn*, reason code = *hhhhhhhh*, AUIU proc name = *proc-name*, ADS_SHR_MEM ID = *nn*.
- **AUIZ044S**
  Shared memory segment version *S-TAP version found* is not compatible with expected *expected version*.
- **AUIZ045E**
  AUICONFG DD must be allocated.
- **AUIZ046E**
  module-name callable service invocation failed: RC = *return-code*, reason code = *reason-code*.
- **AUIZ047E**
  Specified spill file *data_set_name* does not exist.
- **AUIZ048E**
  Problem encountered for *<spill>*, *<problem area>*: required *<req>*, received *<res>*.
- **AUIZ049E**
  z/OS call failure for *<spill>*, *<problemarea>*: RC= *<rc>*, RSN= *<rsn>*.
- **AUIZ050E**
  Specified Log Stream 'xxx.xxx.xxx' does not exist
- **AUIZ051E**
  Problem encountered while validating *log-stream-name*. Function: *request: CONNECT*, RC = *xx*, RSN = *zzzz*.
- **AUIZ052E**
  Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN=*<reason>*.
- **AUIZ053E**
  Logging subsystem failed to initialize successfully.
- **AUIZ054E**
  The Batch DLI log Stream and Online DLI log stream names must be different.
- **AUIZ055E**
  Shared memory segment ID *<shm-id>* is not available for use.

- **AUIZ056E**
  Shared memory segment ID *segment_id* is owned by agent *agent_name* and cannot be attached.
- **AUIZ057E**
  A configuration syntax error was detected at line *<number>*; expected "*<token1>*", found "*<token2>*".
- **AUIZ058I**
  Collection profile *<profile-name>* updated successfully.
- **AUIZ059E**
  Configuration parameter *<option>* value *<value>* is invalid: the first character must be alphabetic.
- **AUIZ060E**
  The master address space did not respond within 60 seconds.
- **AUIZ061I**
  AUIHOST file has been detected.
- **AUIZ062I**
  AUIHOST file LPAR name/DNS name overrides in use: CVTS_LPAR_NAME(DNS_NAME)
- **AUIZ063E**
  AUIHOST file format is invalid. RECFM must be FB; LRECL must be 80.
- **AUIZ064E**
  AUIHOST file contains invalid syntax *<line number and string>*
- **AUIZ065W**
  IMS STAP *<name>* TCP/IP streaming disabled due to user settings.
- **AUIZ066E**
  Configuration parameter "DLIFREQ" value *value* is invalid: expected 10K-999K, 1M-10M.
- **AUIZ067W**
  Configuration parameter *<parameter>* value *<wrong value>* is not valid. *<Value>* will be used instead.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIZ002E *dd-name* DD has already been allocated.

Explanation

The *dd-name* DD needed for the task, has been previously allocated.

System action

The task terminates with a return code of 12.

User response

dd-name DD is dynamically allocated. Ensure that the *dd-name* DD is not present in the task JCL. If the *dd-name* is not present in the JCL, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ003W Attached to existing shared memory segment.

Explanation

This message corresponds to message AUIZ008W. This message indicates that the memory segment has been cleaned, and is being reused.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ004S Shared memory segment key verification failed ('*key-value*').

Explanation

Shared memory segment validation failed. This usually implies that the shared memory segment is owned by another product or system.

User response

Change shared memory segment id and restart the agent:

```
ADS_SHR_MEM_ID
```

Parent topic: Error messages and codes: AUIZxxxx

AUIZ005S Shared memory segment eyecatcher 'value' invalid.

Explanation

Shared memory segment validation failed. This implies that the shared memory segment is owned by another product or system.

User response

Change shared memory segment ID and restart the agent:

```
ADS_SHR_MEM_ID
```

Parent topic: Error messages and codes: AUIZxxxx

AUIZ007S The master address space failed to respond to a connect request.

Explanation

A secondary address space failed to connect to the master address space.

User response

Check the listener-port in the address-space-manager-config section of the configuration and verify that it matches in both AUICONFG and members of the primary address space and secondary address spaces.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ008W IBM® Security Guardium® S-TAP® for IMS on z/OS® agent failed to shut down properly last time.

Explanation

When the agent is restarting, the persistent memory object indicates that the agent was abnormally cancelled or terminated without going through the proper clean-up routines, for example, Estae processing. This message might also indicate that another instance of the agent is currently executing.

User response

Verify that there is only one instance of this agent running.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ009S Attempts to attach to shared memory segment *segment key* failed.

Explanation

This error message always occurs in conjunction with error message AUIX013E.

This startup error indicates that attempts to create a shared memory segment failed because of an already existing shared memory segment that never belonged to, or currently does not belong to, the primary agent address space.

This message can occur in the secondary address space if the <id> elements in the <address-space-manager-config> parameters of the AUICONFG config member that is used by the agent primary address space and the secondary address spaces(s) do not match.

User response

Edit SAUISAMP member AUICONFG (or the customized AUICONFG) and specify a different <id> element in the <address-space-manager-config> section.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ010W Configuration value for *<parameter>* is set below the allowed minimum of *<limit>*.

Explanation

Configuration parameter is not valid: *<parameter>* should be not less than *<limit>*.

User response

Change the parameter to comply with the requirements.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ011W Configuration value for *<parameter>* is set above the allowed maximum of *<limit>*.

Explanation

Configuration parameter is not valid: <parameter> should exceed the *<limit>*.

User response

Change the parameter to correspond to the requirements.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ012I Log-server: listening on port *<port>*.

Explanation

Identifies the port number that the Log-server is listening to.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ013E Log-server: no available port was found in the range *<min-port>-<max-port>*.

Explanation

No available port was found in specified range. This usually implies that the range of ports is used by other installations or products.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ014W Log-server: invalid data received from client *<client-ip>* (*<header-data>*).

Explanation

This message indicates that an unexpected connection occurred from *<client-ip>* to log-server port.

System action

The connection is refused, and processing continues.

User response

This warning message can be produced during a system-level port security scan. If you do not want to receive this message, suppress it by using the configuration parameters LOG_FILTER(E) and LOG_FILTER_MSGS_ID(AUIZ014W).

If a port scan was not active when this message was received, it indicates that an unknown message was received by the log-server port. Contact IBM Software Support.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ020W Configuration parameter *parameter-name* was ignored: duplicate value specified *specified-value*.

Explanation

The specified configuration parameter *parameter-name* cannot contain a value that has already been specified for a related parameter.

User response

Fix the duplicate value *specified-value* and restart the agent.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ021E Configuration parameter *option* can't be empty.

Explanation

The configuration parameter *option* contains an invalid value.

User response

Check the valid values for the *option* and correct the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ022E At least one active appliance is required.

Explanation

No appliances were specified in the agent configuration, or all specified appliances were disabled.

User response

Check agent configuration and add enabled appliances to configuration.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ023E Duplicate appliance specified: *host/port*.

Explanation

Specified appliance (*host/port*) are duplicates of another appliance specified in the configuration.

User response

Update or remove duplicate appliances in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ024E Duplicate appliance priority specified: *priority*.

Explanation

Two or more appliances with duplicate priority (*priority*) were specified.

User response

Update or remove appliances with duplicate priorities in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ025E Spill size can't be zero if more than one appliance is enabled.

Explanation

Spill size should be greater than zero if two or more active appliances are specified.

User response

Specify a valid spill size.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ026E Configuration parameter *<option>* value *<value>* is invalid; expected list *<value-list>*.

Explanation

The configuration parameter *<option>* contains an invalid value.

User response

Check the valid values for the *<option>* and correct the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ027W Host name can't be resolved *<host-name>*.

Explanation

An attempt was made to determine the IP address of the host name that was indicated through the use of the z/OS *getaddrinfo* service. The attempt failed.

System action

If the host name is not the local LPAR, processing continues. The TCP/IP address for any events that occur on this LPAR will not be sent to the appliance for reporting. If the host name is the local LPAR where the agent (AUIAstc task) is running, the local host name and IP address will be used for INTER and INTRA task communications.

User response

The z/OS network administrator must verify that the LPAR name exists in the DNS table.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ028E Configuration parameter *element-name* value *element-value* is invalid: expected min *value-min* and max *value-max*.

Explanation

The *element-value* given for *element-name* is out of the range and must be within *min-value* and *max-value*.

User response

Correct the value for the *element-name* in the configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ029E Property *property-name* not found in config.

Explanation

A required property *property-name* could not be loaded from the configuration file because it has been incorrectly specified, specified multiple times, or not specified at all.

User response

Update configuration file and add *property-name* with an appropriate value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ030E Configuration parameter *parameter-name* value *parameter-value* is not valid long value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *long*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ031E Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned long value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *unsigned long*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ032E Configuration parameter *parameter-name* value *parameter-value* is not valid short value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *short*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ033E Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned short value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *unsigned short*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ034E Configuration parameter *parameter-name* value *parameter-value* is not valid boolean value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *boolean*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ035E Configuration parameter *parameter-name* value *parameter-value* is not valid double value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *double*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ036E Configuration parameter *element-name* value *element-value* length is invalid: expected min *length-min* and max *length-max* characters.

Explanation

The *element-value* given for *element-name* is too long and its length must be within *length-min* and *length-max*.

User response

Correct the value for the *element-name* in the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ037I Collection profile *profile* uninstalled successfully.

Explanation

The specified collection profile uninstalled.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ038I Collection profile *profile* installed successfully.

Explanation

The specified collection profile installed.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ039I Guardium® policy processing started.

Explanation

The agent has received a policy message from the appliance and has started to process it.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ040I Guardium® policy processing finished [active = *<number1>*, installed = *<number2>*, uninstalled = *<number3>*].

Explanation

The Guardium policy has been processed. The active, installed, and uninstalled values indicate the number of processed collection profiles.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ041E Profile for IMS source *ims_name* was ignored: unknown IMS.

Explanation

The agent received an IMS policy from the Security Guardium® system which does not relate to this agent instance.

System action

The policy is ignored by this agent.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ041W Profile for IMS source *ims_name* was ignored: unknown IMS.

Explanation

The agent received an IMS policy from the Security Guardium® system which does not relate to this agent instance.

System action

The policy is ignored by this agent.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ042W IMS artifact *ims-name* was ignored: invalid IMS definition.

Explanation

During policy pushdown, an *ims-name* was specified for one of the rules that does not exist in the Guardium® appliance.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ043E XCF callable service invocation failed: function *function-name*, RC = *nn*, reason code = *hhhhhhhh*, AUIU proc name = *proc-name*, ADS_SHR_MEM ID = *nn*.

Explanation

An error occurred attempting to retrieve AUIU tokens from the CF.

User response

If the LPAR is not a sysplex member, no action is necessary. If the LPAR is a sysplex member, please contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ044S Shared memory segment version *S-TAP version found* is not compatible with expected *expected version*.

Explanation

An attempt to attach to a shared memory segment failed because of version mismatch. This might indicate that the shared memory segment that is identified by ADS_SHR_MEM_ID is already in use by an older version of the product, or another product.

User response

Verify and change the ADS_SHR_MEM_ID that is specified in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ045E AUICONFG DD must be allocated.

Explanation

The address space requires an AUICONFG DD to be specified in the JCL.

User response

Update the JCL for the address space to include an AUICONFG DD.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ046E *module-name* callable service invocation failed: RC = *return-code*, reason code = *reason-code*.

Explanation

Invocation of the specified module failed due to the specified *return-code* and *reason-code*.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ047E Specified spill file *data_set_name* does not exist.

Explanation

During agent startup, the SMF spill file that is named in the configuration parameter SMF_SPILL_FILE(dsn) was not found.

System action

The agent terminates.

User response

Determine why the file cannot be located. Correct any errors, and restart the agent.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ048E Problem encountered for *<spill>*, *<problem area>*: required *<req>*, received *<res>*.

Explanation

This spill data set *<spill>* could not be validated. The *<problem area>* with the parameters *<req>* and *<res>* gives additional details.

User response

Fix the issue in the *<problem area>* using the required *<req>* value. If necessary, contact IBM® Software Support for additional help.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ049E z/OS call failure for *<spill>*, *<problemarea>*: RC= *<rc>*, RSN= *<rsn>*.

Explanation

An attempt to validate the spill data set has caused an error with the z/OS services. A *<problemarea>* value with return code *<rc>* and reason code *<rsn>* are returned. If the *<problemarea>* value is *OBTAIN*, and the *<rc>* value is 4, the spill database in question might have been migrated. In that case, the spill database should be recalled before processing continues.

User response

If a migrated data set is not the problem, contact IBM Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ050E Specified Log Stream 'xxx.xxx.xxx' does not exist

Explanation

The z/OS log stream name that was specified in the LOG_STREAM_DLIO or LOG_STREAM_DLIB AUICONFG DD input stream does not exist.

System action

The agent address space terminates.

User response

Correct the log stream name that you provided, or customize and run the AUILSTRx Log Stream definition jobs that are located in the SAUISAMP product data set.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ051E Problem encountered while validating *log-stream-name*. Function: *request: CONNECT*, RC = *xx*, RSN = *zzzz*.

Explanation

There was a failed attempt to validate the z/OS® System Logger Log-Stream, through the use of an IXGCONN call.

System action

Processing terminates.

User response

Determine the cause of the failure by examining the return and reason codes for the IXGCONN macro. These can be found in the manual, *IBM® MVS™ Programming: Authorized Assembler Services References*.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ052E Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN= *<reason>*.

Explanation

The Log Stream *<log stream>* validation failed with abend code *<code>* and reason code *<reason>*.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ053E Logging subsystem failed to initialize successfully.

Explanation

This error can occur for several reasons. It is preceded by the specific occurrence that caused the logging subsystem to fail during initialization.

User response

Review previously issued error messages to determine the cause of the logging failure.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ054E The Batch DLI log Stream and Online DLI log stream names must be different.

Explanation

The log stream name specified for LOG_STREAM_DLIO and LOG_STREAM_DLIB must be different.

User response

Specify different log streams for batch and online in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ055E Shared memory segment ID *<shm-id>* is not available for use.

Explanation

The shared memory segment ID *<shm-id>* that is specified in the configuration file is not available, or is used by another task.

User response

Check the available *<shm-id>* and update the confugration files. Contact IBM® Software Support if *<shm-id>* is set correctly.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ056E Shared memory segment ID *segment_id* is owned by agent *agent_name* and cannot be attached.

Explanation

The shared memory segment that was identified by the <id> parameter within the address-space-manager-config section of the agent configuration file is already used by the specified agent, *agent_name*.

System action

The agent terminates because it is unable to use the shared memory segment.

User response

To avoid a collision with other agents running on the LPAR, change or include the <id> value in the address-space-manager_config section of the agent configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ057E A configuration syntax error was detected at line *<number>*; expected "*<token1>*", found "*<token2>*".

Explanation

An invalid value was found in the AUICONFG file and the indicated line.

System action

Processing terminates.

User response

Review Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent for information about permissible configuration values. Correct the syntax error and restart the agent.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ058I Collection profile *<profile-name>* updated successfully.

Explanation

The active collection profile *<profile-name>* has been updated during policy installation.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ059E Configuration parameter *<option>* value *<value>* is invalid: the first character must be alphabetic.

Explanation

The configuration parameter *<option>* contains an invalid value.

User response

Review the valid values for the *<option>* and correct the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ060E The master address space did not respond within 60 seconds.

Explanation

The IBM® Guardium® S-TAP® for IMS agent did not send the policy report to the Memory Management Utility (AUIU*STC*) task within 60 seconds of establishing the connection.

System action

The AUIU*STC* task terminates with RC=12.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ061I AUIHOST file has been detected.

Explanation

The AUIHOST DD statement has been detected in the JCL.

System action

The IP address for participating LPARs are resolved by the information contained in this file and described by message AUIxxxI.

User response

If this was not intended, remove the DD statement.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ062I AUIHOST file LPAR name/DNS name overrides in use: CVTS_LPAR_NAME(DNS_NAME)

Explanation

The AUIHOST DD has provided an override for the host named.

System action

The DNS_NAME is the value that is used to perform the gethostbyname call in order to obtain the relevant IP address.

User response

Verify that the supplied LPAR_NAME and DNS_NAME values are correct.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ063E AUIHOST file format is invalid. RECFM must be FB; LRECL must be 80.

Explanation

The file format that was provided by using the AUIHOST DD is incorrect.

System action

The address space terminates.

User response

Verify that the supplied file is a Fixed Block (FB) sequential file, has a logical record length (LRECL) of 80 bytes, and is a either a sequential file or a member of a Partitioned Data Set (PDS or PDS/E). Correct the error and restart the address space.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ064E AUIHOST file contains invalid syntax *<line number and string>*

Explanation

The AUIHOST file supplied contains a record with invalid syntax.

System action

The address space terminates.

User response

Review the Overriding the TCP/IP DNS resolver table topic to verify the required syntax. Correct the record and restart the address space.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ065W IMS STAP <*name*> TCP/IP streaming disabled due to user settings.

Explanation

Simulation mode is on because the STAP_STREAM_EVENTS parameter has been set to N.

System action

Events will not be streamed to the Guardium® system.

User response

To stream events to the Guardium system, set the STAP_STREAM_EVENTS parameter to Y.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ066E Configuration parameter "DLIFREQ" value *value* is invalid: expected 10K-999K, 1M-10M.

Explanation

In the AUICONFG file, the DLIFREQ parameter value is outside of the permitted range. Valid values for the DLIFREQ parameter are 10K -- 999K, or 1M -- 10M.

System action

The AUIA*xxx* task terminates.

User response

Correct the DLIFREQ parameter value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ067W Configuration parameter <*parameter*> value <*wrong value*> is not valid. <*Value*> will be used instead.

Explanation

Configuration parameter is not valid: <*parameter*> should match <*value*>.

User response

Change the parameter to correspond to the requirements.
Parent topic: Error messages and codes: AUIZxxxx

IBM Security Guardium S-TAP for Data Sets on z/OS

These topics describe how to use IBM Security Guardium S-TAP for Data Sets on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for Data Sets). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Data Sets collects and correlates data access information from a variety of resources to produce a comprehensive view of business activity for auditors.

About these topics

This information is designed to help database administrators, system programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for Data Sets
- Install and operate IBM Guardium S-TAP for Data Sets
- Configure the IBM Guardium S-TAP for Data Sets environment
- Diagnose and recover from IBM Guardium S-TAP for Data Sets problems

A PDF of this User's Guide is also available here.

- **IBM Security Guardium S-TAP for Data Sets on z/OS overview**
  IBM Security Guardium S-TAP for Data Sets on z/OS (also referred to as IBM Guardium S-TAP for Data Sets) collects and correlates data access information from System Management Facilities (SMF) records and realtime system events to produce a comprehensive view of data set access activity for auditors.
- **Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3**
  Review the software and authorization prerequisites for installing IBM Guardium S-TAP for Data Sets V10.1.3.
- **Configuring the IBM Guardium S-TAP for Data Sets agent**
  You must configure the IBM Guardium S-TAP for Data Sets agent.
- **IBM Guardium S-TAP for Data Sets administration**
  You must configure the Guardium system to communicate with the IBM Guardium S-TAP for Data Sets agent.
- **Reference information**
  This section provides IBM Guardium S-TAP for Data Sets reference information.
- **Troubleshooting**
  Use these topics to diagnose and correct problems that you might experience with IBM Guardium S-TAP for Data Sets.

Parent topic: S-TAP for z/OS V10.1.3 User's Guide

IBM Security Guardium S-TAP for Data Sets on z/OS overview

IBM Security Guardium S-TAP for Data Sets on z/OS (also referred to as IBM Guardium S-TAP for Data Sets) collects and correlates data access information from System Management Facilities (SMF) records and realtime system events to produce a comprehensive view of data set access activity for auditors.

IBM Guardium S-TAP for Data Sets enables you to collect many different types of information, including:

- Access to VSAM and non-VSAM data sets and security violations that are recorded by SMF.
- Data set operations that are performed against VSAM data sets, such as delete or rename events, recorded by SMF.
- Access to specific records within VSAM data sets, including key-sequenced data sets (KSDS) or relative record data sets (RRDS), captured as they occur.
- Transaction information that is associated with a VSAM KSDS or RRDS logical record operation, performed within a transaction that runs on the Customer Information Control System (CICS) Transaction Server.
- Access to read and update events for a particular VSAM cluster (consisting of one or more physical data sets) for actions performed on the data set as a whole, or actions performed at the individual level for records within the data set.

- **What's new in IBM Guardium S-TAP for Data Sets V10.1.3?**
  Speed and monitoring enhancements are now provided in V10.1.3.
- **IBM Guardium S-TAP for Data Sets components**
  IBM Guardium S-TAP for Data Sets consists of its data collection agent and the Security Guardium system. The IBM Guardium S-TAP for Data Sets agent collects data set access information that is obtained from the SMF record exit interface, as well as record access information that is obtained from individual I/O requests. The Guardium system is a server-based component that provides the product user interface.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

What's new in IBM Guardium S-TAP for Data Sets V10.1.3?

Speed and monitoring enhancements are now provided in V10.1.3.

Enhanced reporting of partitioned data sets (PDS) and extended partitioned data sets (PDSE) member activity
: IBM Guardium S-TAP for Data Sets can now report on the following types of activity:

  - Member Adds
  - Member Replaces
  - Member Renames
  - Member Deletes
  - STOW Initialization (PDSE directory clearing)

New Simulation option
: Enabling Simulation mode enables you to assess the impact of data collection processing without streaming data to the Guardium appliance.

Increased CICS transaction server support
: IBM Guardium S-TAP for Data Sets supports collection of:

  - CICS Transaction Server 5.3 to capture Record Level Monitoring (RLM) data
  - 8-character CICS local unit of work (with CICS Transaction Server 4.2 and later, until end of service)
  - Dynamic starting and stopping of RLM data collection with new IBM Guardium S-TAP for Data Sets SAMPLIB members

Ability to restrict reporting of sensitive data
: When enabled, the FORCE_LOG_LIMITED parameter enables you to restrict Personally Identifiable Identification (PII) from being sent to the Guardium system.

Reporting of FTP activity
: In addition to monitoring of JES2, JES3, ASCH, TSO, and STC address spaces, IBM Guardium S-TAP for Data Sets provides OMVS address space monitoring. This enables reporting of FTP activity.

Reporting of FTP transmission of non-VSAM data sets
: IBM Guardium S-TAP for Data Sets enables you to audit FTP transmission of non-VSAM data sets to and from monitored systems.

New filtering criteria for data set accesses
: For VSAM and non-VSAM Data Sets Close events, you can filter by input-only, output-only, or both input and output events.

Support for Internet Protocol version 6 (IPV6)
: PH16991 introduces IPV6 support and new subsystem configuration option, PREFER_IPV4_STACK.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS overview

IBM Guardium S-TAP for Data Sets components

IBM Guardium S-TAP for Data Sets consists of its data collection agent and the Security Guardium system. The IBM Guardium S-TAP for Data Sets agent collects data set access information that is obtained from the SMF record exit interface, as well as record access information that is obtained from individual I/O requests. The Guardium system is a server-based component that provides the product user interface.

Guardium system and S-TAP agent communication

Communication between the Guardium system and the agent uses a TCP/IP connection. The collection policies that you create, by using the Guardium system user interface, tell the agent what types of data to collect. The policies specify filter information, such as which jobs and data sets to monitor for data accesses.

Guardium system

Use the Guardium system to gather and generate reports on information from multiple agents that are running on multiple z/OS® systems. The Guardium system:

- Provides the user interface, which processes your requests and displays the resulting information.
- Enables you to create collection policies, which specify the types of data that are to be collected by the agent.

- Stores the collected data.

Agent

The agent collects data from a single z/OS system. Monitoring can be performed at both the data set and record level:

- For data set level monitoring, data is collected directly from SMF records, as presented to various SMF exits with which the agent interfaces.
- For record level monitoring, data is collected when VSAM records are read or written.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS overview

Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3

Review the software and authorization prerequisites for installing IBM Guardium S-TAP for Data Sets V10.1.3.

- **Software prerequisites**
  IBM Guardium S-TAP for Data Sets requires z/OS Version 2 Release 2 or later, until end of service.
- **User ID authority requirements**
  To install the product, you must have the necessary z/OS user ID authorities.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Software prerequisites

IBM Guardium S-TAP for Data Sets requires z/OS® Version 2 Release 2 or later, until end of service.

Customer Information Control System (CICS®) Transaction Server support requires IBM CICS Transaction Server for z/OS V4 Release 2 or later, until end of service.

Parent topic: Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3

User ID authority requirements

To install the product, you must have the necessary z/OS® user ID authorities.

Your z/OS user ID must have the authority to:

- Define the appropriate SMF record collection parameters in the SMFPRMxx PARMLIB member and APF authorize the load library for the product.
- Update the appropriate procedure library to include the agent started task.

If you choose to enable CICS support, you must also have the authority to:

- Update CICS parameters.
- Add CICS program definitions.
- Update or create CICS system initialization and termination program list tables for startup and shutdown.

If necessary, contact your system administrator to obtain the required authorities.
Parent topic: Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3

Configuring the IBM Guardium S-TAP for Data Sets agent

You must configure the IBM Guardium S-TAP for Data Sets agent.

Configuration overview

To configure the product, complete the required steps.

- Security: Review and establish the security requirements. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.
- Review the required resource authorizations information, including:
  - APF authorizing the load library
  - Authorizing the z/OS agent started task for the control data set
  - Defining an OMVS segment
- Planning your configuration: Review the steps that are required to plan your configuration.
  - Job cards for the sample JCL in the sample library: Provide valid job cards.
  - Allocating auxiliary storage: Ensure that data will not be lost in the event of an overflow.
- Configuring the SMFPRMxx parameter library member: Ensure a complete audit by configuring the SMFPRMxx parameter library to collect the required SMF record types.
- IAM and ACF2 collection considerations: Review information about capturing IAM data set activity and ACF2 access failures.
- Creating the control data set: Generate the initial partitioned data set members.
- Specifying subsystem options: Review the subsystem changes that you can make to the options member in the control data set.
- Configuring the started task JCL: Determine the location of the started task control job language (JCL), and follow configuration steps and tips.
- CICS Transaction Server support: Review the requirements for enabling the CICS Transaction Server, and follow the instructions for Configuring CICS Transaction Server support.

- **Security**
  IBM Guardium S-TAP for Data Sets requires access to various z/OS data sets and system components. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.

- **Planning your configuration**
  Use this planning list to determine necessary information before continuing. Then, provide a valid job card, and allocate auxiliary storage if necessary, as described in the following sections.
- **Configuring the SMFPRMxx parameter library member**
  To ensure a complete audit, you must configure the active SMFPRMxx member of the z/OS system PARMLIB to collect the required SMF record types needed by IBM Guardium S-TAP for Data Sets.
- **IAM and ACF2 collection considerations**
  IBM Guardium S-TAP for Data Sets can capture IAM data set activity and ACF2 access failures. Learn how to enable IBM Guardium S-TAP for Data Sets to collect this information, and be aware of the following collection considerations. These products implement the collection of SMF data in a nonstandard way and require special consideration.
- **Creating the control data set**
  Complete these steps to create the control data set and generate the initial partitioned data set (PDS) members. These members contain required information, and must be added to the newly created data set for the agent to work correctly.
- **Specifying subsystem options**
  To configure IBM Guardium S-TAP for Data Sets, you must specify a four-character IBM Guardium S-TAP for Data Sets subsystem ID (SUBSYS) to associate with this particular instance of IBM Guardium S-TAP for Data Sets. The SUBSYS identifies the IBM Guardium S-TAP for Data Sets subsystem in messages that are generated by the product.
- **Configuring the started task JCL**
  You must configure the started task JCL statements with values that provide the system with information that is specific to your environment. Follow these steps to configure the started task JCL.
- **CICS Transaction Server support**
  IBM Guardium S-TAP for Data Sets CICS Transaction Server support enables you to filter and capture CICS transaction information.
- **Configuring CICS signon reporting**
  IBM Guardium S-TAP for Data Sets can identify the CICS signon that was used for a specific file access event. Configure the product to enable the agent to send the CICS signon information to the Guardium system.
- **Starting the product**
  Start IBM Guardium S-TAP for Data Sets before starting products that perform similar functions.
- **Sample library members**
  The following sample library members are included for your use in installing and configuring IBM Guardium S-TAP for Data Sets. The following table lists them by type and description.
- **Verifying the installation**
  After you install and configure the IBM Guardium S-TAP for Data Sets agent, verify that the agent is properly installed. Use the JCL that is provided in the AUVJIVP member of the SAUVSAMP sample library.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Security

IBM Guardium S-TAP for Data Sets requires access to various z/OS® data sets and system components. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.

To provide IBM Guardium S-TAP for Data Sets with access to the necessary z/OS data sets and system components, you must APF authorize the load library, authorize the z/OS started task for the control data set, and define an OMVS segment to your security product, as described in the following sections.

Security products can include various software tools that are currently available, such as IBM Resource Access Control Facility (RACF®), Computer Associates International Top Secret, and Computer Associates International Access Control Facility (ACF2).

- **APF authorizing the load library**
  IBM Guardium S-TAP for Data Sets requires certain data sets to be accessible and APF authorized on the system on which the agent started task will run. SMF data will be collected by the agent.
- **Authorizing the z/OS agent started task for the control data set**
  The z/OS agent started task must be authorized to read and update the control data set. The control data set is a partitioned data set that contains various members that define options and operating parameters for the product. IBM Guardium S-TAP for Data Sets uses a control data set that is defined in the agent started task.
- **Defining an OMVS segment**
  You must define an OMVS segment to your security product to make use of TCP/IP connectivity and UNIX System Services. An OMVS segment specifies the user ID to be used, the home directory, and the shell program name.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

APF authorizing the load library

IBM Guardium S-TAP for Data Sets requires certain data sets to be accessible and APF authorized on the system on which the agent started task will run. SMF data will be collected by the agent.

The product data set SAUVLOAD, which contains the product load modules that are required for operation, must be APF authorized on the system on which IBM Guardium S-TAP for Data Sets will be run.

Refer to the z/OS MVS Programming Authorized Assembler Services Guide for guidelines and instructions for using APF.

Parent topic: Security

Authorizing the z/OS agent started task for the control data set

The z/OS® agent started task must be authorized to read and update the control data set. The control data set is a partitioned data set that contains various members that define options and operating parameters for the product. IBM Guardium S-TAP for Data Sets uses a control data set that is defined in the agent started task.

Refer to your security product documentation for more information on authorizing the agent started task.

Parent topic: Security

Defining an OMVS segment

You must define an OMVS segment to your security product to make use of TCP/IP connectivity and UNIX System Services. An OMVS segment specifies the user ID to be used, the home directory, and the shell program name.

If you are using IBM RACF, refer to z/OS UNIX System Services Planning for guidelines and instructions about OMVS segment definitions. If you are using a security product other than RACF, refer to your product's instructions on how to define an OMVS segment.

Parent topic: Security

Planning your configuration

Use this planning list to determine necessary information before continuing. Then, provide a valid job card, and allocate auxiliary storage if necessary, as described in the following sections.

Before configuration, you must determine:

- The user who will configure the product
- The user ID that will be used to run the agent
- Where the Guardium system and the S-TAP agent will run

- **Job cards for the sample JCL in the sample library**
  Some JCL members that are included with the product sample library, SAUVSAMP, have a sample card for the job card. Provide a valid job card that conforms to the JCL standards of your site before submitting any of the JCL members.
- **Allocating auxiliary storage**
  z/OS auxiliary storage consists of DASD space that is allocated to the local page data sets. It is used as temporary backup storage for programs and data located in virtual and physical memory. IBM Guardium S-TAP for Data Sets can allocate auxiliary storage space if the OUTAGE_SPILLAREA_SIZE parameter is set in accordance with the following requirements.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Job cards for the sample JCL in the sample library

Some JCL members that are included with the product sample library, SAUVSAMP, have a sample card for the job card. Provide a valid job card that conforms to the JCL standards of your site before submitting any of the JCL members.

Parent topic: Planning your configuration

Allocating auxiliary storage

z/OS auxiliary storage consists of DASD space that is allocated to the local page data sets. It is used as temporary backup storage for programs and data located in virtual and physical memory. IBM Guardium S-TAP for Data Sets can allocate auxiliary storage space if the OUTAGE_SPILLAREA_SIZE parameter is set in accordance with the following requirements.

- The OUTAGE_SPILLAREA_SIZE parameter option instructs the address space to allocate a data space equal in size to the value that you set for OUTAGE_SPILLAREA_SIZE.
- Verify that the current local page space can accommodate a new data space.

Example

Specifying OUTAGE_SPILLAREA_SIZE=64 instructs the address space to allocate 64 MB of data space.

Refer to the z/OS® MVS™ Initialization and Tuning guide for more information about sizing local page data sets.
Parent topic: Planning your configuration

Configuring the SMFPRMxx parameter library member

To ensure a complete audit, you must configure the active SMFPRMxx member of the z/OS® system PARMLIB to collect the required SMF record types needed by IBM Guardium S-TAP for Data Sets.

The record types can be collected at the subsystem or system level. Maximum auditing of VSAM and non-VSAM data set activity can be achieved by ensuring that all defined subsystems record all of the SMF record types that are required by the product.

The defaults used at the system level for those subsystems that are not explicitly defined should also specify collection of the required SMF record types. The required SMF record types are 14, 15, 17, 18, 30, 42, 60, 61, 62, 64, 65, 66, and 80. If any required SMF record types are not defined for collection, message AUV1450W alerts you to define them.

If the appropriate exit is not defined for the operating system level, SMF records will not be collected. Specify the SMF exits as follows:

- For z/OS Version 2 Release 2 and earlier, specify the IEFU83, IEFU84, and IEFU85 SMF exits.
- For z/OS Version 2 Release 3 and later, specify the IEFU86 SMF exit.

These exits can be defined at either the subsystem or system level in a manner consistent with the SMF record type specifications.

For more information about setting up and managing SMF, refer to the z/OS MVS™ System Management Facility (SMF) manual.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Related reference

- SMF record types and contexts

IAM and ACF2 collection considerations

IBM Guardium S-TAP for Data Sets can capture IAM data set activity and ACF2 access failures. Learn how to enable IBM Guardium S-TAP for Data Sets to collect this information, and be aware of the following collection considerations. These products implement the collection of SMF data in a nonstandard way and require special consideration.

Innovation Access Method (IAM) from Innovation Data Processing provides capabilities beyond standard VSAM. IAM replaces VSAM access with a proprietary non-VSAM access that simulates VSAM. Because the underlying data sets are non-VSAM, accesses to the IAM-simulated VSAM data sets do not generate VSAM SMF records, such as the SMF type 62 (VSAM OPEN) and SMF type 64 (VSAM CLOSE).

For IAM data sets, IBM Guardium S-TAP for Data Sets does not report the following items:

- Context records for OPEN and UPDATE for IAM data sets (because of the lack of the SMF type 62 records).
- IAM simulation of alternate index and path processing (because of the lack of an IAM SMF CLOSE record).

The CLOSE record counters will report IAM data sets differently from native VSAM processing. Although the IAM CLOSE SMF record offers an extensive array of counters, those corresponding to the VSAM SMF Type 64 record are included in the accumulated counts within the CLOSE context record.

Computer Associates International ACF2 considerations

Unlike some security products, ACF2 does not offer a unique authorization failure code to identify a CONTROL access failure. Instead, it reports these as UPDATE access failures. In ACF2 facilities, no CONTROL context records will be reported.

- **Enabling Innovations Data Processing IAM reporting**
  IAM provides a unique, user-specified record ID, which is written during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access:
- **Enabling Computer Associates International ACF2 reporting**
  Access Control Facility (ACF2) from Computer Associates International records access failures to a unique, user-specified record ID. For IBM Guardium S-TAP for Data Sets to report these failures:

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Enabling Innovations Data Processing IAM reporting

IAM provides a unique, user-specified record ID, which is written during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access:

Procedure

1. Determine the user-specified SMF record ID that was selected for IAM.
2. Specify that value in the IBM Guardium S-TAP for Data Sets control data set IAM_SMF_RECORD_ID option.

Parent topic: IAM and ACF2 collection considerations

Enabling Computer Associates International ACF2 reporting

Access Control Facility (ACF2) from Computer Associates International records access failures to a unique, user-specified record ID. For IBM Guardium S-TAP for Data Sets to report these failures:

Procedure

1. Determine the user-specified SMF record ID that was selected for ACF2.
2. Specify that value in the IBM Guardium S-TAP for Data Sets control data set ACF_SMF_RECORD_ID option.

Parent topic: IAM and ACF2 collection considerations

Creating the control data set

Complete these steps to create the control data set and generate the initial partitioned data set (PDS) members. These members contain required information, and must be added to the newly created data set for the agent to work correctly.

Before you begin

Refer to the high-level qualifier that you specified when configuring the started task JCL. The same high-level qualifier must be used in step 1 of the control data set creation procedure.

About this task

The options and definitions that determine how IBM Guardium S-TAP for Data Sets performs processing in your environment are contained in the control data set.

Procedure

1. The JCL to create the control data set is located in the AUVJCNTL member of the SAUVSAMP library. Configure the AUVJCNTL member by replacing AUV.V10R1M3 with the high-level qualifier of the installed IBM Guardium S-TAP for Data Sets load library.
2. Submit the JCL to create the control data set.
   The JCL creates the control data set and populates the data set with these initial members: subsystem options (OPTIONS) and policy rule definition members (RULEDEFS and RULEDEFB).
   Important:
   - Do not modify the contents of the RULEDEFS or RULEDEFB member.
   - Do not modify the value of the default INITIAL_RULEDEF option in the RULEDEFS or RULEDEFB members.
3. Specify the APPLIANCE_SERVER and AUDIT parameters in the OPTIONS member to enable the product to function properly.
4. Optional: Consider whether allocating the control data set as an extended partitioned data set (PDSE) is appropriate for your environment.
   A PDSE dynamically manages internal space, drastically reducing the need to perform the space compressions that are required for a nonextended partitioned data set (PDS). The AUVJCNTL member includes statements that can be used to change the allocation to a PDSE.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Specifying subsystem options

To configure IBM Guardium S-TAP for Data Sets, you must specify a four-character IBM Guardium S-TAP for Data Sets subsystem ID (SUBSYS) to associate with this particular instance of IBM Guardium S-TAP for Data Sets. The SUBSYS identifies the IBM Guardium S-TAP for Data Sets subsystem in messages that are generated by the product.

How to use subsystem options

Use either the *keyword=value* or *keyword(value)* format to specify values for these option members.

Option members and descriptions

The IBM Guardium S-TAP for Data Sets subsystem options are in the OPTIONS member of the IBM Guardium S-TAP for Data Sets control data set that is generated by the AUVJCNTL member JCL. These options are the global definitions and general operation options that determine where and how IBM Guardium S-TAP for Data Sets performs its functions.

To specify IBM Guardium S-TAP for Data Sets subsystem options, modify the contents of the OPTIONS member as described.

ACF_SMF_RECORD_ID
: If you are using Access Control Facility (ACF2) from Computer Associates International, you must provide product-specific information for your SMF data to be processed. ACF2 records access failures to a unique record ID. Determine the user-specified SMF record ID that is selected for ACF2 and specify that ID in the IBM Guardium S-TAP for Data Sets CONTROL data set ACF_SMF_RECORD_ID option if you want the product to report these failures.
  ACF2 writes SMF access failure data to a user-defined SMF record ID. Specify a numeric value that identifies the SMF record identification number used by ACF2.
  For ACF2 installations, contact your ACF2 administrator to determine the appropriate numeric value to include with this parameter.
  Note:

  - For z/OS Version 2 Release 3 and later, valid values are 128 – 1151.
  - For z/OS Version 2 Release 2 and earlier, valid values are 128 – 255.

  There is no product default value, however, the SAMPLIB member AUVSOPTS includes a default specification of 230.

APPLIANCE_CONNECT_RETRY_COUNT
: Specify a numeric value that defines the number of times to retry communicating with the Guardium system when an error is encountered during initialization. If the communication is still not successful after the number of retries as specified by this value has been completed, the communication is abandoned and no data is sent. The process also terminates if the number of retries specified is reached with no successful connection.
  Valid values are 0 -- 65535. The default value is 20.

APPLIANCE_NETWORK_REQUEST_TIMEOUT
: Specify a numeric value that defines the number of seconds that must transpire before a timeout is recognized.
  Valid values are 0 -- 65535. The default value, in seconds, is 0.

APPLIANCE_PING_RATE
: Specify a numeric value that defines the number of seconds between pings to the Guardium system. The ping signals the Guardium system that the S-TAP is active and available for communications.
  Valid values are 1 -- 65535. The default value, in seconds, is 5.

APPLIANCE_PORT
: Specify a numeric value that defines the TCP/IP port number for communication with the Guardium system by IBM Guardium S-TAP for Data Sets. Use port 16022 for the V10.1.3 system protocol.
  The default value is 16022.
  If port 16023 is used, encryption support is required for the connection to the appliance.
  Note: Specifying this keyword and parameter designates the port on which the Guardium appliance is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS® by another application.
  Valid values are 16022 and 16023.

APPLIANCE_RETRY_INTERVAL
: Specify a numeric value that defines the number of seconds between retries when an error is encountered during an initial attempt to connect to the Guardium system.
  Valid values are 0 -- 65535. The default value, in seconds, is 10.

APPLIANCE_SERVER
: Specify the TCP/IP address for the Guardium system with which IBM Guardium S-TAP for Data Sets is to communicate. In multistream processing scenarios, this address specifies the first Guardium appliance that is to be used.
  The address can be specified as a host name (*security.guardiumvsam.net*) or as four numbers separated by periods (for example, 188.128.6.42).
  Maximum length is 53 characters. There is no default.

APPLIANCE_SERVER_[1-5]
: Specify alternative TCP/IP addresses to use for failover recovery processing and multistream Guardium appliance destinations. Up to five alternative TCP/IP addresses are supported.
  To specify one or more entries, include this parameter with a numeric suffix from 1 - 5. Provide a unique TCP/IP address for each entry.
  The option syntax is as follows:

- APPPLIANCE_SERVER_1=*addr*

or

- APPPLIANCE_SERVER_1(*addr*)

where 1 can be 1, 2, 3, 4, or 5.
Valid values are any valid TCP/IP address. There are no default values. If initialization does not detect this parameter, it does not activate the failover process.
Both the APPLIANCE_SERVER_[1-5] and APPLIANCE _SERVER_FAILOVER_[1-5] parameters can be used to designate servers for multistreaming or failover. Use the APPLIANCE_SERVER_LIST parameter to designate how these parameters are used.
Maximum length is 51 characters.

APPLIANCE_SERVER_FAILOVER_[1-5]

Specify alternative TCP/IP addresses to use for failover and recovery processing. The product supports up to five alternative TCP/IP addresses. To specify one or more entries, include this parameter with a numeric suffix from 1 - 5, each time providing a unique TCP/IP address.
The option syntax is as follows:

```
APPPLIANCE_SERVER_FAILOVER_1=addr
```

or

```
APPPLIANCE_SERVER_FAILOVER_1(addr)
```

where *1* can be 1, 2, 3, 4, or 5.
Valid values are any valid TCP/IP address. There are no default values. If initialization does not detect this parameter, it does not activate the failover process.
Both the APPLIANCE _SERVER_FAILOVER_[1-5] and APPLIANCE_SERVER_[1-5] parameters can be used to designate servers for multistreaming or failover. Use the APPLIANCE_SERVER_LIST parameter to designate how these parameters are used.
Maximum length is 42 characters.

APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER|HOT_FAILOVER)

Set APPLIANCE_SERVER_LIST to *MULTI_STREAM* for a Guardium appliance connection to be established for each server that is identified by the APPLIANCE_SERVER_n or APPLIANCE_SERVER_FAILOVER_n parameters.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *FAILOVER* for one Guardium appliance connection to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the APPLIANCE_SERVER_n or APPLIANCE_SERVER_FAILOVER_n parameter.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *HOT_FAILOVER* to keep each connected Guardium appliance active via pings. If the primary Guardium appliance (which is set by the APPLIANCE_SERVER parameter) becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.
With all settings of APPLIANCE_SERVER_LIST, if all connections fail, and a spill file is specified (parameter OUTAGE_SPILLAREA_SIZE), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.
The default is *FAILOVER*.

AUDIT

Specify a character string from one through 26 characters that defines the name of this IBM Guardium S-TAP for Data Sets agent.
There is no default.

CICS_SUPPORT

Enabling CICS® Transaction Server support activates additional reporting of CICS-specific information on record level events, including:

- CICS File ID
- CICS Function Code
- CICS Program ID
- CICS Region ID
- CICS Terminal ID
- CICS Transaction ID
- CICS User ID
- CICS Logical Unit of Work

Enable or disable CICS support by specifying `ENABLE` or `DISABLE`.
The default is *DISABLE*.
If you enable CICS support, you must also configure CICS for record level monitoring events to be captured for CICS. For more information about CICS support, see CICS Transaction Server support.

FORCE_LOG_LIMITED

Record level monitoring enables you to monitor VSAM file access based on key values. The VSAM key can contain Personally Identifying Information, such as account number, last name, or Social Security number. When the FORCE_LOG_LIMITED option is enabled, IBM Guardium S-TAP for Data Sets does not monitor any record level data. If the file is being monitored by a policy, then only file access is reported; monitoring and reporting of access to specific keys is suppressed.
Specify *Y* to prevent Personally Identifiable Identification (PII) data from being sent to the Guardium system. Data that is sent as part of Record Level Monitoring and CICS is considered PII. This data will not be sent to the Guardium system if FORCE_LOG_LIMITED(*Y*) is specified.
The default is *N*.

IAM_SMF_RECORD_ID

If you are using Innovation Access Method (IAM) from Innovation Data Processing, you must provide product-specific information for your SMF data to be processed. IAM provides a unique user-specified record ID, which it writes during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access, determine the user SMF record ID for IAM, and specify that value in the IBM Guardium S-TAP for Data Sets control data set IAM_SMF_RECORD_ID option.
IAM writes SMF statistical data to a user-defined SMF record ID. Specify a numeric value that identifies the SMF record identification number used by IAM.
For IAM installations, consult your IAM administrator to determine the appropriate numeric value to include with this parameter.
Note:

- For z/OS Version 2 Release 3 and later, valid values are 128 – 1151.
- For z/OS Version 2 Release 2 and earlier, valid values are 128 – 255.

There is no product default value; however, the SAMPLIB member AUVSOPTS includes a default specification of 201.

INTERNAL_BUFFER_SIZE

Specify the size of the internal buffer used.

To improve performance, data is stored in an internal buffer that is sent when the buffer is full or during a ping request. If the buffer reaches the INTERNAL_BUFFER_SIZE, data is sent without waiting for the next ping request.

Specifying an INTERNAL_BUFFER_SIZE value that is too large for your environment can cause connection problems that are due to timing out while trying to send a large amount of data. Specifying too small a value might cause unnecessary I/O requests.

Tip: Performance varies based on system load, network load, and the load on the Guardium system, so the correct value for your environment cannot be predetermined. Begin with the default value, and make minor, incremental adjustments to improve performance, if necessary.

Valid values are 0 -- 2047 megabytes. The default is 8.

INITIAL_RULEDEF

You must not change this subsystem option unless IBM Software Support instructs you to do so. If instructed to modify this subsystem option, specify the name of the rule definitions member to use at startup. The default rule definitions member name is RULEDEFS.

MEGABUFFER_COUNT

Specify the number of IBM Guardium S-TAP for Data Sets audit events that are buffered, prior to the product attempting a TCP/IP send operation.

The megabuffer is flushed when either of two conditions is met:

- At regular intervals, based on the APPLIANCE_PING_RATE
- When the number of audit events that are held in the megabuffer reaches the count that is specified by this parameter

When MULTI_STREAM mode is enabled by parameter APPLIANCE_SERVER_LIST, and a megabuffer flush occurs, the audit event data stream is switched to the next available Guardium appliance. The event data stream will switch from appliance to appliance in a round-robin sequence as each megabuffer is sent.

Valid values are 1 -- 8192. The default is 200.

OUTAGE_SPILLAREA_SIZE

Specify the size of the spill file to be used when a connection cannot be made.

If the product includes a spill file, and no secondary APPLIANCE_SERVER_FAILOVER address is specified, or none of the secondary APPLIANCE_SERVER_FAILOVER addresses respond, it writes to the spill file. The spill file is meant for short-term outages only, because when a connection is restored to any Guardium system, it clears the spill file content before continuing to send data.

Valid values are 0 -- 1024 megabytes. If a valid value is not specified, a spill file is not created.

PREFER_IPV4_STACK

Specify the request for an IPV4 address to be issued from the Domain Name Server (DNS). The default value is N.

- Y causes a request to be issued to the DNS for an IPV4 address for the hostname that is specified in the APPLIANCE_SERVER parameter:
  - The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
  - If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
  - If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.
- N or omitting this option from configuration causes a request for an IPV6 address to be issued to the DNS for the hostname that is specified by the APPLIANCE_SERVER parameter.
  - The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
  - If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
  - If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this option is specified, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for Data Sets started task will terminate.

RLM

Specify the initial status of RLM processing by setting the RLM parameter to either *ENABLE* or *DISABLE*. *ENABLE* enables record level monitoring. *DISABLE* disables record level monitoring.

The default value is *ENABLE*.

SOCKET_CONNECT_TIMEOUT

Specify the length of time for socket connection attempts before failure or timeout.

Setting this value too low results in connection failures when the Guardium system is slow to respond. Setting this value too high causes problems in failover scenarios.

Tip: Performance varies based on system load, network load, and the load on the Guardium system, so the correct value for your environment cannot be predetermined. Begin with the default value, and make minor, incremental adjustments to improve performance, if necessary.

Valid values are 1 -- 65535. The default value, in seconds, is 3.

STAP_STREAM_EVENTS

Specify the initial streaming status by setting the STAP_STREAM_EVENTS parameter to either *Y* or *N*.

- Y indicates that the IBM Guardium S-TAP for Data Sets agent address space will send data to the server in a manner that is consistent with the active policy.
- N indicates that the agent address space will not send data to the server. It will perform all data collection processing in a manner that is consistent with the active policy. The agent address space will issue message AUV1070I at startup: TCP/IP STREAMING DISABLED DUE TO USER SETTING. See Simulation mode for more information.

The default value is *Y*.

SUBSYS

Choose any four-character alphanumerical subsystem ID to identify this particular instance of IBM Guardium S-TAP for Data Sets. For example, `AUV1`, `AUV2`, and so on.

Choose a unique SSID for each agent.

The default subsystem ID is *VTAP*.

SUPPRESS_INCOMPLETE_EVENTS

Enables SMF records without identifying characteristics to either be suppressed or sent to the appliance. Specify the SMF event filtering preference for SMF records with missing identifying characteristics, where:

- *N* indicates that missing field values in SMF records should always pass policy rule filters.
- *Y* indicates that missing field values should not pass the filters and the corresponding events should not be sent to the appliance.

The default value is *N*.
For more information, see SMF record identification considerations.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Configuring the started task JCL

You must configure the started task JCL statements with values that provide the system with information that is specific to your environment. Follow these steps to configure the started task JCL.

About this task

The IBM Guardium S-TAP for Data Sets started task JCL is located in the AUVJSTC member of the IBM Guardium S-TAP for Data Sets sample library (SAUVSAMP).
Note: Do not start the started task until you finish configuring IBM Guardium S-TAP for Data Sets. Attempting to start the started task before completing configuration can cause the started task to fail.

Procedure

1. Copy the IBM Guardium S-TAP for Data Sets started task JCL to your system PROCLIB from sample data set member AUVJSTC.
   Tip: Name the IBM Guardium S-TAP for Data Sets started task member AUVSTAPV. This name is easily identifiable with the IBM Guardium S-TAP for Data Sets product.
2. Verify that the statement: //AUVSTAPV PROC OPTSMBR=OPTIONS points to the default member name OPTIONS.
   The default member name OPTIONS was created during creation of the control data set.
3. Configure the started task JCL that you copied to your system PROCLIB by replacing AUV.V10R1M3 with the high-level qualifier of the installed IBM Guardium S-TAP for Data Sets load library.
   Note: For operation of the product, policy activation, and correct processing of data, the following conditions must be met:
   - A DD statement with the DDNAME OPTIONS must be in the IBM Guardium S-TAP for Data Sets started task. This DD statement points to the subsystem OPTIONS member of the IBM Guardium S-TAP for Data Sets control data set, which contains the global settings for the product. When the started task is initiated, it references the data in the subsystem options member to establish global settings, including the subsystem identifier for this specific instance of IBM Guardium S-TAP for Data Sets.
     - By default, the OPTIONS DD statement uses the same data set as the RULEDEFS and RULEDEFB DD statements. If necessary, you can specify a different data set for the OPTIONS DD statement other than that which is used for the DD statements RULEDEFS and RULEDEFB. The OPTIONS member must be present in the data set that is specified for the OPTIONS DD statement.
   - A DD statement with a DDNAME of CONTROL must be in the IBM Guardium S-TAP for Data Sets started task. For example: //CONTROL DD DSN=AUV.V10R1M3.CONTROL,DISP=SHR. This DD statement points to the IBM Guardium S-TAP for Data Sets control data set that contains the collection policy in the RULEDEFS member.
   - The two DD statements with the DDNAMES RULEDEFS and RULEDEFB must be present and must point to the same control data set name that was specified in the CONTROL DD statement. The member names RULEDEFS and RULEDEFB must not be changed. If DDNAMES RULEDEFS and RULEDEFB are not present, are changed, or do not point to the correct data set name, then the agent does not initiate correctly and is unable to collect data.
   - The high-level qualifier you specify for the control data set JCL when allocating the control data set must match the high-level qualifier you specify in the started task JCL.
   - The started task must have the authority to read and update the control data set and load library.
4. After you configure the started task JCL, add it to the z/OS® PROCLIB data set for started task initiation.
   Note:

   IBM Guardium S-TAP for Data Sets accommodates the use of multistream and improves support for large policies by providing a default started task JCL region size of 96 megabytes. When multistream is enabled, a buffer is created for each appliance, based on the INTERNAL_BUFFER_SIZE value. (Valid values are 0 - 2047 megabytes. The default value is 8.) The default started task JCL region size of 96 megabytes can accommodate large policies by providing space for up to six connected appliances with a default INTERNAL_BUFFER_SIZE of 8 megabytes and approximately 150,000 values in a policy.

   You might need to increase the started task JCL region size if:
   - the value specified for INTERNAL_BUFFER_SIZE is greater than 8 megabytes
   - an installed policy contains more than 150,000 values

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

CICS Transaction Server support

IBM Guardium S-TAP for Data Sets CICS® Transaction Server support enables you to filter and capture CICS transaction information.

IBM Guardium S-TAP for Data Sets must be running before CICS is started. If changes to a policy are made while a CICS file is open, the file must be closed and reopened for RLM-related policy changes to take effect.

Verify that the agent is running and correctly configured, and the appropriate work area storage is available.

- To capture data on files that are referenced within a transaction, the IBM Guardium S-TAP for Data Sets agent must be running and correctly configured to monitor each system image on which data sets reside.
- CICS support uses the XFCFROUT Global User Exit (GLUE).
- The GLUE acquires an above-the-line work area from the extended CICS dynamic storage area (ECDSA) of approximately 1412 bytes for each active or suspended transaction that performs at least one VSAM file operation. The work area is released at the end of the transaction.

- **Configuring CICS Transaction Server support**
  For CICS related information to be captured, you must configure CICS Transaction Server support.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Configuring CICS Transaction Server support

For CICS® related information to be captured, you must configure CICS Transaction Server support.

About this task

If you configure CICS Transaction Server support, you can capture CICS transaction information that is associated with record level monitoring of logical record activities that occur within a CICS transaction for KSDS and RRDS data sets. Remember to start IBM Guardium S-TAP for Data Sets before starting CICS. If changes to a policy are made while a CICS file is open, the file must be closed and reopened for any RLM-related policy changes to take effect.

Procedure

1. Configure the CICS system options.
   a. Specify the CICS_SUPPORT=ENABLE option, by using the subsystem options that are located in the OPTIONS member of the control data set.
2. Configure the CICS system initialization and system termination program list tables (PLTs), as shown in the example at the end of this topic.
   a. Enter the program AUVPLTPI after the DFHDELIM PLT entry.
   b. Enter the program AUVPLTPS before the DFHDELIM PLT entry.
   c. After creating or modifying the CICS system initialization and system termination PLTs, you must assemble and link them. For more information about creating a PLT, see the CICS Transaction Server for z/OS® Resource Definition Guide.
3. Specify autoinstall in the CICS system initialization parameters to automatically install the AUVPLTPI, AUVPLTPS, and AUVFROUT programs.
   If you do not specify autoinstall in the CICS system initialization parameters, you must define AUVPLTPI, AUVPLTPS, and AUVFROUT in the CICS system definition file (CSD). To install the program definitions in batch, sample JCL has been provided in member AUVCSDUP of the IBM Guardium S-TAP for Data Sets SAUVSAMP library that can be modified and used for the CICS program DFHCSDUP. Alternatively, the CICS CEDA Resource Definition Online transaction can also be used to perform the install of the program definitions. See the CICS Transaction Server for z/OS Resource Definition Guide for more information about installing resource definitions.
   a. Define the following attributes:
      - LANGUAGE (ASSEMBLER)
      - STATUS (ENABLED)
      - CEDF (NO)
      - DATALOCATION (BELOW)
      - EXECKEY (CICS)
      - EXECUTIONSET (FULLAPI)
      - RELOAD (NO)

      For the load modules to be located, the AUVPLTPI, AUVPLTPS, and AUVFROUT programs must be located in a load library located in the CICS DFHRPL concatenation within the CICS startup JCL.
4. Optional: The CICS facilities that implement RLM support, outside of normal CICS PLT initialization, can be enabled and disabled. To do so, define CICS transactions accordingly by using the batch CICS program DFHCSDUP or the CICS CEDA Resource Definition Online transaction.

   To enable the CICS facilities that are used to implement CICS RLM support, the following attributes must be assigned to the transaction:

   - TRANSACTION (*tran*, where *tran* is your chosen transaction ID)
   - PROGRAM (AUVPLTPI)
   - TASKDATAKEY (CICS)
   - TASKDATALOC (ANY)

   To disable the CICS facilities that are used to implement CICS RLM support, the following attributes must be assigned to the transaction:
   - TRANSACTION (*tran*, where *tran* is your chosen transaction ID)
   - PROGRAM (AUVPLTPS)
   - TASKDATAKEY (CICS)
   - TASKDATALOC (ANY)
5. Reference the program initialization and termination PLTs in parameters PLTPI and PLTPSD, as described in the topic, Using CICS system initialization parameters.

Results

If you have configured CICS support, message AUV3004I is displayed during CICS initialization to indicate that the Global User Exit AUVPLTPI XFCFROUT was installed and enabled.

Example

Enter the program AUVPLTPI after the DFHDELIM PLT entry in the CICS system initialization PLT:

```
*
*   CICS PROGRAM LIST TABLE FOR CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=INITIAL,SUFFIX=I1
*
*  ENTRIES AHEAD OF DFHDELIM ARE EXECUTED IN FIRST PASS OF PLTPI
*  DURING THE SECOND PHASE OF CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
*
*  ENTRIES AFTERF DFHDELIM ARE EXECUTED IN SECOND PASS OF PLTPI
*  DURING THE THIRD PHASE OF CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=ENTRY,PROGRAM=AUVPLTPI
*
         DFHPLT TYPE=FINAL
*
         END
```

Enter the program AUVPLTS before the DFHDELIM PLT entry in the CICS system termination PLT:

```
*
*   CICS PROGRAM LIST TABLE FOR CICS SYSTEM TERMINATION
*
         DFHPLT TYPE=INITIAL,SUFFIX=T1
*
```

```
*  ENTRIES AHEAD OF DFHDELIM ARE EXECUTED IN FIRST PASS OF PLTPSD
*  DURING THE FIRST PHASE OF CICS SYSTEM TERMINATION
*
       DFHPLT TYPE=ENTRY,PROGRAM=AUVPLTPS
*
       DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
*
*  ENTRIES AFTERF DFHDELIM ARE EXECUTED IN SECOND PASS OF PLTSD
*  DURING THE SECOND PHASE OF CICS SYSTEM TERMINATION
*
*
        DFHPLT TYPE=FINAL
*
        END
```

- **Using CICS system initialization parameters**
  If you created program initialization and termination program list tables to use with IBM Guardium S-TAP for Data Sets, they must be referenced in the CICS system initialization parameters PLTPI and PLTSD.

Parent topic: CICS Transaction Server support

Using CICS system initialization parameters

If you created program initialization and termination program list tables to use with IBM Guardium S-TAP for Data Sets, they must be referenced in the CICS® system initialization parameters PLTPI and PLTSD.

- The suffix of the table that was created as the program initialization PLT must be referenced in the PLTPI parameter.
- The suffix of the table that was created as the program termination PLT must be referenced in the PLTSD parameter.

Here is a sample set of system initialization parameters that specifies the PLTPI and PLTSD suffixes:

```
AICONS=YES,
XRF=NO,
AUXTR=OFF,
AUXTRSW=NO,
APPLID=CICSSYSA,
FCT=NO,
    ...
PLTPI=I1,
PLTSD=T1,
    ...
SYSIDNT=SYSA
```

Parent topic: Configuring CICS Transaction Server support

Configuring CICS signon reporting

IBM Guardium S-TAP for Data Sets can identify the CICS® signon that was used for a specific file access event. Configure the product to enable the agent to send the CICS signon information to the Guardium system.

About this task

Remember: CICS signon records do not indicate a security failure. They are an indication that the identified user successfully accessed the named file or data set.
By default, IBM Guardium S-TAP for Data Sets reports only the CICS address SAF user ID for data set level events and failed security violations. However, for RACF® environments, both CICS and RACF can be configured for the S-TAP agent to report all of the following:

- the CICS signon
- the file or data set name that was accessed
- the access context (ALTER, CONTROL, UPDATE, or READ)

Note:

- Implementation of this facility requires changes to both CICS and RACF. After implementation, the resulting change to SMF type 80 processing results in the SMF80USR field containing the CICS signon for specific file accesses. Consult your CICS and RACF security administrator when considering the implementation of this facility.
- This facility does not report the data set activity, only the security level for the requested access event.
- The following steps are also documented in the *RACF Security Guide*. For more information, see the CICS Transaction Server for z/OS® RACF Security Guide.

To implement security for files managed by the CICS file control:

Procedure

1. Specify `RESSEC(YES)` in the CSD resource definition of the transactions that access the files.
2. Using the CICS file names for identification, define the profiles to RACF in the FCICSFCT or HCICSFCT resource classes, or their equivalent if you have a user-defined resource class names.
   a. For example, use the following commands to define files in the FCICSFCT class, and authorize users to read from or write to the files:

```
RDEFINE FCICSFCT (file1, file2, .., filen)
                UACC(NONE) NOTIFY(sys_admin_userid)
PERMIT file1 CLASS(FCICSFCT)
                ID(group1, group2) ACCESS(UPDATE)
PERMIT file2 CLASS(FCICSFCT)
                ID(group1, group2) ACCESS(READ)
```

3. To define files as members of a profile in the CICS file resource group class with an appropriate access list, use the following commands:

```
RDEFINE HCICSFCT (file_groupname)
                UACC(NONE) ADDMEM(filea, fileb, .., filez)
                NOTIFY(sys_admin_userid)
PERMIT file_groupname
                CLASS(HCICSFCT)
                ID(group_userid) ACCESS(UPDATE)
```

4. Specify `SEC=YES` as a CICS system initialization parameter, or `SECPRFX` if you define profiles with a prefix.
5. Specify `XFCT=YES` for the default resource class names of FCICSFCT and HCICSFCT, or XFCT=class_name for user-defined resource class names.

Results

RACF SMF type 80 records contain the CICS user signon in the SMF80USR field. The data is reported to the Guardium system records User ID field.
Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Starting the product

Start IBM Guardium S-TAP for Data Sets before starting products that perform similar functions.

Product initialization errors might occur if other products, which are known to intercept processing at the point of open, close, or record management functions for VSAM data sets, are started before IBM Guardium S-TAP for Data Sets. Message AUV1196E will warn you of a product initialization order conflict.

If you receive this error at startup:

1. Shut down IBM Guardium S-TAP for Data Sets and any similar products, including the previous version of this product
2. Close any data sets that are open under IBM Guardium S-TAP for Data Sets.
3. Start IBM Guardium S-TAP for Data Sets before starting similar products. IBM Guardium S-TAP for Data Sets must be running before CICS is started.

- **Starting and stopping the agent started task**
  Follow these steps to start and stop the IBM Guardium S-TAP for Data Sets agent started task.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Starting and stopping the agent started task

Follow these steps to start and stop the IBM Guardium S-TAP for Data Sets agent started task.

1. Start the agent started task by issuing the START command from the operator console, for example: START AUVSTAPV
2. Stop the agent started task by issuing the STOP command from the operator console, for example: STOP AUVSTAPV

You can configure the agent started task to start automatically during the z/OS® initial program load (IPL). To set automatic startup, add the appropriate command to the COMMNDxx member in SYS1.PARMLIB, or contact your system administrator.
Parent topic: Starting the product

Sample library members

The following sample library members are included for your use in installing and configuring IBM Guardium S-TAP for Data Sets. The following table lists them by type and description.

Table 1. Sample library members, types, and descriptions

Member	Type	Description
AUVCSDUP	JCL	Sample JCL to create CICS resource definition lists, groups, and program definitions with the CICS DFHCSDUP utility.
AUVJCNTL	JCL	Sample JCL to allocate and initially populate the control data set.
AUVJIVP	JCL	Sample JCL to verify installation.
AUVJSTC	JCL	Sample PROC to start the IBM Guardium S-TAP for Data Sets agent address space.
AUVSOPTS	Data	Initial data used to populate the control data set OPTIONS member.
AUVSRDEF	Data	Initial data used to populate the control data set RULEDEFS and RULEDEFB members.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Verifying the installation

After you install and configure the IBM® Guardium® S-TAP® for Data Sets agent, verify that the agent is properly installed. Use the JCL that is provided in the AUVJIVP member of the SAUVSAMP sample library.

Before you begin

Before you begin, complete all required tasks for Configuring the IBM Guardium S-TAP for Data Sets agent.

Procedure

1. You must install a policy on the IBM Guardium system with the characteristics listed below. Remember to replace <HLQ> with a valid high-level qualifier.

```
Job Name.....: AUVJIVP
Data Set Name: <HLQ>.AUVIVP.%%
DB Type......: DATA SET COLLECTION PROFILE
Data Set Type: ALL
```

```
Data Set Event: ALL
Actions......: z/OS AUDIT
```

Note: To see specific records on the IBM Guardium system, you might need to install a policy on the appliance in the first position that specifies Actions: LOG FULL DETAILS WITH VALUES.

2. Create a query on the IBM Guardium system that will report the events received from IBM Guardium S-TAP for Data Sets. Query characteristics are as follows:

```
Domain........: Access
Main Entity...: FULL SQL
Recommended Fields: IMS/DATA SET Event time
IMS/DATA SET Job Name
IMS/DATA SET Step Name
IMS/DATA SET Program Name
IMS/DATA SET Previous DSN
IMS/DATA SET Set Type
IMS/DATA SET Context
```

3. Start the IBM Guardium S-TAP for Data Sets started task.
4. Verify that the required SMF record types are enabled. Message AUV1450W in the Data Sets agent JESMSGLG log will alert you if any SMF record types are not defined.
5. Verify that the IBM Guardium S-TAP for Data Sets agent is connected to the intended appliance. Message AUV2182I in the Data Sets agent JESMSGLG log indicates a successful connection between the agent and the appliance.
6. Make the following modifications to the installation verification JCL in SAUVSAMP member AUVJIVP:
   a. Add a valid job card.
   b. Replace all occurrences of <HLQ> with the same high-level qualifier that was used in the policy as described in Step 1.
7. Submit the modified JCL in SAUVSAMP member AUVJIVP.

Results

Verify that the following data sets contexts appear on the appliance:

Table 1. Data set contexts for installation verification

Step	Description	Data set contexts
GENDATA	Generate input data for subsequent job steps	None
VSAM	Define, load, rename and delete ESDS, KSDS, and RRDS data sets	DATA SET ALTER DATA SET CLOSE DATA SET CREATE DATA SET DELETE DATA SET OPEN DATA SET RENAME DATA SET UPDATE
PDS	Create a PDS and write to a new PDS member	DATA SET CLOSE DATA SET CREATE Member Add
PDSCOPY	Copy a PDS member to another PDS member	DATA SET CLOSE Member Add
PDSREPL	Copy over an existing PDS member	DATA SET CLOSE Member Replace
PDSTEST	Rename a PDS member, create an alias, delete all PDS members, rename the PDS, and delete the PDS	DATA SET CLOSE DATA SET DELETE DATA SET RENAME Member Add Member Delete Member Rename STOW Initialize

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

IBM Guardium S-TAP for Data Sets administration

You must configure the Guardium system to communicate with the IBM Guardium S-TAP for Data Sets agent.

- **Communicating with the Guardium system**
  The Guardium system and the S-TAP for Data Sets agent need to communicate policy rules and collected data by using a TCP/IP connection. For the IBM Guardium S-TAP for Data Sets to communicate with the Guardium system, the following conditions must be met:
- **Communicating with the IBM Guardium S-TAP for Data Sets started task**
  IBM Guardium S-TAP for Data Sets operator commands enable authorized users to perform selected operations. Several types of operator commands can be used to display the status of IBM Guardium S-TAP for Data Sets, to enable and disable certain functions, and to dynamically alter processing without stopping or quiescing the product.

- **Data collection**
  IBM Guardium S-TAP for Data Sets collects data from multiple sources. This section describes the data collection process, as well as filtering stages and their performance impacts.
- **Record level and SMF data set monitoring options**
  You can reduce z/OS CPU and storage usage by setting options for Record level and SMF data set monitoring.
- **Policy pushdown**
  Policy pushdown is a method of controlling the data that is collected by the IBM Guardium S-TAP for Data Sets agent. Policy pushdown enables the agent to evaluate the filtering criteria that you specified.
- **Data set collection filtering parameters**
  Use the following filtering parameters to collect data set event data.
- **CICS collection filtering parameters**
  Use the following filtering parameters to collect transaction data from CICS®.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Communicating with the Guardium system

The Guardium system and the S-TAP for Data Sets agent need to communicate policy rules and collected data by using a TCP/IP connection. For the IBM Guardium S-TAP for Data Sets to communicate with the Guardium system, the following conditions must be met:

- The IBM Guardium S-TAP for Data Sets TCP/IP connection must be configured.
- At least one agent per z/OS® image must be specified. When you are configuring an agent instance:
  - Specify the host name or IP address on which the Guardium system is running. This value is specified by the APPLIANCE_SERVER element in the agent configuration file. The complete name of this CONTROL member is OPTIONS.

  When the agent is started, it uses the specified configuration information to connect to the Guardium system.

- **Streaming audit data to multiple systems**
  Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).
- **Keeping connections active when HOT_FAILOVER is enabled**
  When the *HOT_FAILOVER* feature is enabled by the APPLIANCE_SERVER_LIST parameter, each connected Guardium appliance is kept active via pings.

Parent topic: IBM Guardium S-TAP for Data Sets administration

Streaming audit data to multiple systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).

IBM Guardium S-TAP for Data Sets sends events to a single appliance until a ping occurs, or the number of records that is specified by MEGABUFFER_COUNT is reached.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the APPLIANCE_SERVER_LIST parameter in the OPTIONS member of the CONTROL data set. Parameters APPLIANCE_SERVER and APPLIANCE_SERVER_[1-5] specify the appliances to which you intend to stream events. The appliance that is specified by APPLIANCE_SERVER provides the policy that is used for event matching.

For more information about OPTIONS member parameters, see Specifying subsystem options.

Parent topic: Communicating with the Guardium system

Keeping connections active when HOT_FAILOVER is enabled

When the *HOT_FAILOVER* feature is enabled by the APPLIANCE_SERVER_LIST parameter, each connected Guardium appliance is kept active via pings.

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Parent topic: Communicating with the Guardium system

Communicating with the IBM Guardium S-TAP for Data Sets started task

IBM Guardium S-TAP for Data Sets operator commands enable authorized users to perform selected operations. Several types of operator commands can be used to display the status of IBM Guardium S-TAP for Data Sets, to enable and disable certain functions, and to dynamically alter processing without stopping or quiescing the product.

- **IBM Guardium S-TAP for Data Sets started task commands**
  If you are an authorized user, you can enter commands to display the status of IBM Guardium S-TAP for Data Sets enable and disable certain functions, and dynamically alter processing without shutting down or quiescing the system.

Parent topic: IBM Guardium S-TAP for Data Sets administration

IBM Guardium S-TAP for Data Sets started task commands

If you are an authorized user, you can enter commands to display the status of IBM Guardium S-TAP for Data Sets enable and disable certain functions, and dynamically alter processing without shutting down or quiescing the system.

Commands

Enter operator commands from an MVS™ operator console, or by using a facility that issues MVS commands, such as SDSF.

The command format is MODIFY*stcname*, where *stcname* is the name of the started task, followed by the DISPLAY command.

For example, for record level monitoring, you can enter: MODIFY*stcname*,DISPLAY RLM. You can also use the shorthand for MODIFY, which is F to enter F*stcname*,DISPLAY RLM.

The following table summarizes the commands for displaying monitoring status and for enabling or disabling monitoring:

Table 1. Started task commands and descriptions

Command	Description
DISPLAY RLM	Indicates whether record level monitoring is enabled or disabled
DISPLAY SMFM	Indicates whether SMF monitoring is enabled or disabled
ENABLE RLM	Enables record level monitoring
DISABLE RLM	Disables record level monitoring
ENABLE SMFM	Enables SMF monitoring
DISABLE SMFM	Disables SMF monitoring
DISPLAY STREAM	Indicates whether audit records are being sent to the appliance
DIAG	Displays diagnostic information about the agent. Also displays the counters, which record the number of SMF-based and RLM-based audit records that are created as well as the number of audit records that are sent to the appliance.

Parent topic: Communicating with the IBM Guardium S-TAP for Data Sets started task

Data collection

IBM Guardium S-TAP for Data Sets collects data from multiple sources. This section describes the data collection process, as well as filtering stages and their performance impacts.

Record level and SMF event monitoring

Event information is gathered at run time through record level and SMF event monitoring. For both record level and SMF event monitoring, the filtering options you specify can minimize overhead, and control the performance of the data collection and reporting phases of processing. IBM Guardium S-TAP for Data Sets uses the filtering criteria you define to dynamically tune its processing path for optimal performance.

With few exceptions, you can use the same filtering criteria for both record level and SMF event monitoring.

- Specify the minimal filtering criteria necessary for your policy. Filtering only on the data you require minimizes:
  - Data collection overhead
  - Event processing
  - Event reporting
  - CPU time
  - Memory usage

  Record level monitoring creates the potential for the collection and reporting of large amounts of data. When constructing a policy and specifying filtering criteria, carefully consider the potential amount of data to be collected and processed.
- In the user interface, you can specify lists of elements for some filters, and use generic characters (wildcards) to create more flexibility in your filtering criteria. Generic characters act as placeholders in the specification of a character-based operand, representative of one or more valid characters for the entity on which an operation is performed.
- The use of generic characters can reduce the total number of policy rules required, but an overly inclusive set of selected entities can ultimately reduce efficiency. Excessive use of generic characters can increase the scope of selectivity during the qualification of records for processing, and dramatically reduce efficiency and increase overhead.
- SMF event monitoring can be controlled at a higher level through the specifications in the SMFPRMxx z/OS® system PARMLIB member.

Note:

- Record level monitoring support for a data set is detected, filtered, and activated at OPEN time. Files that are open at the time of an initial or updated policy activation will not be intercepted for RLM processing unless the application permits closing and reopening the file. This is of particular importance for CICS, which typically opens files at initialization or at first-use of a file. If a policy is updated after a CICS file has already been opened, it must be closed and reopened to be eligible for RLM processing.
- Record level monitoring enables you to monitor VSAM file access based on key values. The VSAM key can contain Personally Identifying Information, such as account number, last name, or Social Security number. When the FORCE_LOG_LIMITED option is enabled, IBM Guardium S-TAP for Data Sets does not monitor any record level data. If the file is being monitored by a policy, then only file access is reported; monitoring and reporting of access to specific keys is suppressed.

Filtering stages

Both record level and SMF event monitoring are performed in stages. If a collected event does not pass the lowest filtering stage (0), further processing of that event is not performed. Otherwise, the event is reevaluated during the next stage of filter processing, and IBM Guardium S-TAP for Data Sets determines whether the event should be auditing and reporting.

Stage 0 filtering

Stage 0 filtering should only be used by advanced users. An understanding of each SMF record type is required.
Stage 0 filtering can be performed for SMF event monitoring only. Only SMF events being recorded by SMF can be monitored for processing.
SMF record types to be monitored must be defined in the SMFPRMxx z/OS System Initialization PARMLIB member. If one or more SMF record types to be monitored are not specified, data collection cannot be performed. See the *SMF record types collected by IBM Guardium S-TAP for Data Sets* section of this user's guide for

details on the record types and the associated data collected with each record type.

Stage 1 filtering

Stage 1 filtering can be performed with both record level and SMF event monitoring.
Filter out as much data as possible to achieve the best possible performance.
The filtering criteria specified in the policy associated with this level of filtering include:

- Data set name
- Data set type
- DD name
- Job name
- Job type
- Program name
- Security system user ID
- Security system group ID
- SMF system ID
- Subsystem ID
- Sysplex name
- VSAM record organization*

*VSAM record organization is only available as a filtering criterion for record level monitoring. Only key-sequenced data set (KSDS) and relative record data set (RRDS) organizations are supported.
Some of the possible filtering criteria for Stage 1 filtering include a wider scope of data than others. For example, a user ID can require a much larger subset of data for processing than a data set name requires. You can define the minimum amount of data to be monitored, collected, and reported on by including or excluding selection criteria, creating lists of elements, and specifying relational operators for most criteria.
Stage 1 filtering for record level monitoring: For record level monitoring, Stage 1 filtering occurs at OPEN time for KSDS and RRDS VSAM data sets.
Stage 1 filtering for SMF event monitoring: For SMF event monitoring, Stage 1 filtering occurs in the IBM Guardium S-TAP for Data Sets address space immediately after a monitored SMF record type is obtained by the collector, located at the SMF User Exit collection point.

Stage 2 filtering

Stage 2 filtering for record level and SMF event monitoring applies to the following event types:

- Data set open
- Data set close
- Data set create
- Data set alter
- Data set update
- Data set delete
- Data set rename
- Data set SAF alter
- Data set SAF control
- Data set SAF define
- Data set SAF read
- Data set SAF update
- Member add
- Member replace
- Member rename
- Member delete
- STOW initialize

Default or specified event types are collected and passed on to the Guardium system.
Stage 2 filtering for record level monitoring can be based on the type of logical record access as well as one or more values for the key of the VSAM data set. The types of record level access that can filtered on in Stage 2 are:

- Record insert
- Record delete
- Record update
- Record read

You can use a key value or list of key values, as well as a key range or list of key ranges, to further limit the amount and scope of data collected. The key data can be specified in normal printable characters or in hexadecimal by using the EBCDIC character set.
For key values, you can use generic characters in the specification of the keys. Only those records that pass Stage 2 filtering are collected and passed on to the Guardium system.
If CICS® support is enabled, you can filter the record level monitoring event data that is captured within a CICS transaction. CICS transaction data can be filtered by:

- CICS user ID
- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS region ID
- CICS terminal ID
- CICS function code

Stage 3 filtering

Stage 3 filtering is performed by IBM Guardium S-TAP for Data Sets based on Stage 2 filtering criteria that you define. During policy pushdown and activation, an analysis of the policy filtering criteria is performed. This analysis enables prefiltering processing determinations that can be performed across the product. Stage 3 prefiltering can be very efficient in eliminating certain types of data collection, and ultimately reducing the path length through the product to provide optimal processing performance.
Examples:

- **Record level monitoring:** If no record level monitoring event types are specified in the policy, Stage 2 filtering is eliminated, which reduces overhead significantly.
- **SMF event monitoring:** The exclusion of certain SMF event monitoring types from your filtering criteria allows IBM Guardium S-TAP for Data Sets to bypass collection very early in the SMF User Exit data collection, and eliminates all downstream processing for that SMF record type.

Exclusions

IBM Guardium S-TAP for Data Sets does not collect information on the following types of activities:

On IBM Db2® subsystems
: Activity within address spaces whose STC names have the following endings:

- MSTR (example: QA1XMSTR)
- DIST (example: QA1XDIST)
- IRLM (example: QA1XIRLM)
- DBM1 (example: QA1XDBM1)

On IBM IMS subsystems
: Accesses performed by the following program names:

- DFSMVRC0
- CQSINIT0
- HWSHWS00
- IRTRRC00
- DFSRRC00
- DFSUARC0
- DSPCINT0
- DSPURI00

SMF record identification considerations

In certain cases, such as when an SMF record is generated before the issuing job is run, SMF records can have zeros in the fields that the agent uses for record identification. When this happens, the agent is unable to find a RULEDEFS match for the record by using this field or any dependent fields. To avoid data loss, the agent still sends these records to the appliance even if the policy rule is set to filter out those fields. If one or more identifying fields are empty, you can use the Guardium appliance to highlight them, for example, by marking them with a specific color. The data set audit fields that can be affected by this consideration are:

- Job name
- Job number
- Program name
- DD name
- User ID
- Group ID
- Job type
- Step name
- Step number

To optionally suppress incomplete events from being sent to the appliance, use the SUPPRESS_INCOMPLETE_EVENTS parameter as described in Specifying subsystem options.

Parent topic: IBM Guardium S-TAP for Data Sets administration

Record level and SMF data set monitoring options

You can reduce z/OS® CPU and storage usage by setting options for Record level and SMF data set monitoring.

Record level monitoring performance

During record level monitoring, data is collected when VSAM records are read or written. Record level monitoring can affect performance, TCP/IP traffic, and system load. Record level monitoring intercepts VSAM accesses at the record level, so excessive monitoring of logical record requests can result in large volumes of data being transferred to the Guardium system from the TCP/IP telecommunications link, along with a corresponding increase in CPU and storage use within z/OS. Even in a moderately-sized installation that uses VSAM files, hundreds of millions, if not billions, of logical record requests can be made to VSAM daily. Attempting to monitor and report on all VSAM requests can result in huge volumes of data that can increase system load on z/OS and data traffic on communication links.

To provide flexibility in controlling the impact of record level monitoring, policy options can be used to limit the scope of monitoring. Carefully consider these options with the goal of limiting record level monitoring to the logical record requests in specific data sets that must be monitored in your environment.

Record level monitoring filter options

You can use the record level monitoring to filter based on:

- Data set name
- Data set type
- Job name
- Job type
- Program name
- Security system user ID
- Security system group ID
- SMF system ID
- Subsystem ID
- Sysplex name
- VSAM record organization
- DD name

If CICS® support is enabled you can also filter based on:

- CICS user ID

- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS region ID
- CICS terminal ID
- CICS function code

You can also limit the monitoring of records to particular keys or key ranges:

VSAM KSDS and RRDS data sets
: For KSDS data sets, the key used is defined when the data set is created through an IDCAMS DEFINE.
For RRDS data sets, the key is a relative record number within the data set.
For individual keys, a list of keys is permitted with which a comparison operator can be used. In situations where the key contains unprintable characters, you can define the keys or key ranges by using hexadecimal notation.

Limit the monitoring of record level requests by the type of logical requests, including:

- Record read events
- Update write events
- Insertions
- Deletions

Remember: Each monitored record that matches the various policy filters results in the processing, creation, and transmission of a record monitoring data element to the Guardium system. Use the Guardium system interface to establish as restrictive a set of policy filters as possible. IBM Guardium S-TAP for Data Sets dynamically tunes and minimizes processing based on the filtering criteria chosen. Effectively chosen filters allows for maximum efficiency of record level monitoring processing.

Activating record level monitoring

You must define a policy that includes rules that specify one or more of the record level request filters (reads, update writes, insertions, or deletions) in order to activate record level monitoring.

- If a policy does not contain any of these filters, no additional overhead occurs at the logical record request level.
- If a particular policy rule contains one or more of these filters, only the specific data set defined in the rule (or data sets associated with other policy filters defined in the rule) incurs any additional monitoring overhead.
- Record level monitoring is only valid for use with VSAM data sets (KSDS and RRDS only).

SMF data set monitoring performance and filtering

Use filtering criteria to limit the amount of VSAM data set monitoring to only particular events. By using policy filters, SMF data set monitoring performance is enhanced by reducing CPU usage, storage usage, and TCP/IP traffic to the Guardium system.

Filter down to each specific VSAM data set event with the following filters:

- Data Set Open
- Data Set Update
- Data Set Close
- Data Set Close (input-only)
- Data Set Close (output-only)
- Data Set Delete
- Data Set Rename
- Data Set Create
- Data Set Alter
- Data Set SAF Alter
- Data Set SAF Update
- Data Set SAF Read
- Data Set SAF Define
- Data Set SAF Control

Filter down to each specific non-VSAM data set event with the following filters:

- Data Set Close
- Data Set Close (input-only)
- Data Set Close (output-only)
- Data Set Delete
- Data Set Rename
- Data Set Create
- Data Set SAF Alter
- Data Set SAF Update
- Data Set SAF Read
- Data Set SAF Define
- Data Set SAF Control
- Member Add
- Member Delete
- Member Rename
- Member Replace
- STOW Initialize

You can achieve optimal record level monitoring and SMF data set monitoring performance when you create and use a policy that defines only those events that are required by your organization.

Parent topic: IBM Guardium S-TAP for Data Sets administration

Policy pushdown

Policy pushdown is a method of controlling the data that is collected by the IBM Guardium S-TAP for Data Sets agent. Policy pushdown enables the agent to evaluate the filtering criteria that you specified.

Evaluating a match

When the product is searching for a match for the filtering criteria that you have specified, an evaluation is performed through each data set level. Access rules are used for processing a data set, when the filtering criteria of the following access types match the data:

- Job name
- Program
- Data set name
- Data set type
- DD name
- User ID
- Group ID
- SYSPLEX
- SSID
- SYS ID
- RECORG*
- Job type

*RECORG is valid only for the processing of VSAM record level monitoring.
The following values are not used to evaluate for a match on an access rule. They are used as subfiltering criteria after a match on a data set is found:

- Key
- Key range
- Data set event
- RLM event
- CICS® user ID
- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS region ID
- CICS terminal ID
- CICS function code

Multiple values are allowed in an access rule, as shown in the following example with two access rules:

```
Access Rule 1
        Rule Type = INCLUDE
        Job Name = JOBA
        Key = "111111"
        RLM Event = ALL
Access Rule 2
        Rule Type = INCLUDE
        Job Name = JOBA
        Key = "222222"
        RLM Event = ALL
```

When a match is found on Access Rule 1 for job JOBA, no further scanning of the Access Rules occurs. The keyword *Key* is not used as part of the Access Rule match. To filter on keys "111111" and "222222" for a job that is named JOBA, code the Access Rules as follows:

```
Access Rule 1
        Rule Type = INCLUDE
        Job Name = JOBA
        Key = "111111","222222"
        RLM Event = ALL
```

This rule searches for a match on the job name JOBA. If a match on JOBA is found, the RLM Event and Key values are matched.
Parent topic: IBM Guardium S-TAP for Data Sets administration

Data set collection filtering parameters

Use the following filtering parameters to collect data set event data.

All the fields are optional and most have a default behavior as described. All fields apply to both VSAM and non-VSAM monitoring, unless otherwise specified.

Rule Type
: Indicates whether this rule indicates inclusion or exclusion for events that match the criteria.
Allowed values are: INCLUDE|EXCLUDE: Include collects events that satisfy the specified criteria; exclude does not collect those events. If nothing is specified, then INCLUDE is used.

Job Type
: Indicates the type of jobs that should be considered for a match.
If nothing is specified, all types are collected. You can specify the following values, separated by a comma (,): JOB|STC|TSU|APPC|OMVS, where:

  JOB
  : Jobs

  STC

Started Task

TSU
: Time Sharing User

APPC
: Advanced Program-To-Program Communication

OMVS
: Open MVS access to non-VSAM data sets, particularly that performed by FTP

SYS ID
: Indicates the SMF System IDs to use when searching for a match.
1 - 4 character SMF System ID to match.
Can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Valid wildcards are supported at any position. They are:

- Percent sign (%) for zero or more characters
- Question mark (?) for a single character match

If left blank, then all SMF System IDs are considered a match.
Examples:

SS01
: Matches events that occur on SS01

SS01,EQ
: Matches that occur on SS01

SS%,EQ
: Matches that occur on systems with SS as the first 2 characters in the SMF system ID

RECORG
: Indicates the record organization type to match.
Applies only to VSAM record level monitoring collection.
Can contain zero or more of the following values, separated by a comma (,): KSDS|RRDS, where:

KSDS
: Key-sequenced data set

RRDS
: Relative record data set

If left blank, all record organization types for record level monitoring are considered a match.
Examples:

KSDS
: Matches key-sequenced data set events

KSDS,RRDS
: Matches key-sequenced data set, and relative record data set events

User ID
: Indicates the user ID to use when searching for a match.
1 - 8 character user ID to match.
Can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all user IDs are considered a match.
Examples:

PDUSER01
: Matches events that are caused by user *PDUSER01*

PDUSER01,EQ
: Matches events that are caused by user *PDUSER01*

PDUSER%,EQ
: Matches events that are caused by users with the prefix *PDUSER*

SSID
: Indicates the AUV ID to use when searching for a match.
1 - 4 character AUV ID optionally followed by a comma (,) and a relational operator. If no relational operator is provided EQ is assumed.
Wildcards are supported.
If left blank, activities for all SSID are considered a match.
Examples:

AUV1
: Matches events from systems with AUV ID of AUV1

AUV1,EQ
: Matches events from systems with AUV ID of AUV1

AUV%,EQ
: Matches events from systems with AUV ID prefix of AUV

SYSPLEX
: Indicates the z/OS sysplex name to use when searching for a match.
The specific 1 - 8 character z/OS sysplex name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, then activities for all SYSPLEX are considered a match.
Examples:

SYSPLEX1
: Matches events from systems on SYSPLEX1

SYSPLEX1,EQ
Matches events from systems on SYSPLEX1
SYSPLEX%,EQ
Matches events from systems on a plex beginning with SYSPLEX

Program
Indicates the program name to use when searching for a match.
1 - 8 character program name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, activities from all programs are considered a match.
Examples:

IDCAMS
Matches events that are accessed from IDCAMS
IDCAMS,EQ
Matches events that are accessed from IDCAMS
IDCAM%,EQ
Matches events that are accessed from programs beginning with IDCAM

Group ID
Indicates the group ID to use when searching for a match.
1 - 8 character representing the security system group ID optionally followed by a comma (,) and a relational operator. If no relational operator is provided EQ is assumed.
Wildcards are supported.
If left blank, then activities from all groups are considered a match.
Examples:

GROUP1
Matches events that are caused by someone within GROUP1
GROUP1,EQ
Matches events that are caused by someone within GROUP1
GROUP%,EQ
Matches events that are caused by someone within a group ID beginning with GROUP

Data Set Name
Indicates the data set name to use when searching for a match.
1 - 44 character that represents the data set name for which activity is collected, optionally followed by the comma character (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, all data set names are considered a match.
Examples:

HLQ1.MLQ1.LLQ1
Matches events on HLQ1.MLQ1.LLQ1
HLQ1.MLQ1.LLQ1,EQ
Matches events on HLQ1.MLQ1.LLQ1
HLQ%.MLQ%.LLQ%.EQ
Matches events with the data set name mask HLQ%.MLQ%.LLQ%
%.%%,EQ
Matches all data sets with more than one qualifier
%,EQ
Matches all data sets with one qualifier

DD Name
Indicates the DD name to use when searching for a match.
1 - 8 character DD name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, activities for all DD names are considered a match.
Examples:

PAYFILE
Matches events that are accessed by DD name *PAYFILE*
PAYFILE,EQ
Matches events that are accessed by DD name *PAYFILE*
PAYFIL%,EQ
Matches events that are accessed by DD names beginning with *PAYFIL*

Job Name
Indicates the job name to use when searching for a match.
1 - 8 character name representing the job for which activity must be collected, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, then activities from all jobs are considered a match.
Examples:

AUVJOB01
Matches events that result from a job name AUVJOB01
AUVJOB01,EQ
Matches events that result from a job name AUVJOB01
AUVJOB%,EQ
Matches events that result from any job beginning with AUVJOB

Key

Indicates the keys to consider when searching for a match.
Only applies to VSAM record level monitoring collection.
One or more keys in plain text or hexadecimal format, representing the key for which to match event data during record level monitoring processing.
Multiple keys must be delimited by a comma (,) optionally followed by the comma character (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Plain text keys can be 1 - 255 characters long.
Hexadecimal keys can be 2 - 510 characters long and must always have an even number of characters.
An individual key must be surrounded in double quotation marks ("").
If the key is in hexadecimal format, it must be prefixed with x' and suffixed with a single quotation mark (') . It must be placed inside double quotation marks, for example: "x'F0F0F1'"
A backslash (\) can precede any character to escape the character. For example:

`"\x'0123'"`
: Matches the plain text key "x'0123'" instead of a hexadecimal key. Both types can be supplied together.

Wildcards are supported. If a wildcard is supplied with a hexadecimal key, the wildcard must be in hexadecimal (6C for `'%'`, 6E for `'?'`).
If a provided key is greater than the actual length of the VSAM key, the key will be truncated. If the key provided is shorter than the VSAM key, it will be padded with hex zeroes.
If the Key and Key Range fields are blank, activities for all keys are considered a match.
Examples:

`"KEY01"`
: Matches record level monitoring events with a key of KEY01

`"KEY01","KEY02"`
: Matches record level monitoring events with a key of KEY01 or KEY02

`"x'F0F0'"`
: Matches record level monitoring events with a key that contains the hexadecimal value F0F0

`"x'F0F0'","x'F0F1'"`
: Matches record level monitoring events with a key that contains the hexadecimal value of F0F0 or F0F1

`"KEY01","x'F0F1'"`
: Matches record level monitoring events with a key of KEY01 or a key with the hexadecimal value of F0F1

`"KEY0%"`
: Matches record level monitoring events with a key beginning with KEY0.

`"x'F06C'″`
: Matches record level monitoring events with a key with a hexadecimal value beginning with F0

`"\x'F06C'″`
: Matches record level monitoring events with a key of x'F06C'

Key Range

Indicates the range of keys to consider when searching for a match.
Only applies to VSAM record level monitoring collection.
A pair of keys in plain text, or a pair of keys in hexadecimal, representing the range to match for record level monitoring. This must be specified as <key1>,<key2>.
A pair of keys must both be in plain text, or both be in hexadecimal. Each plain text key in a plain text key pair can be 1 - 255 characters long. Each hexadecimal key in a hexadecimal key pair can be 2 - 510 characters long and must have an even number of characters.
If the keys are in hexadecimal, they must begin with x' and end with a single quotation mark (') . All keys must be enclosed in double quotation marks.
A backslash (\) can precede any characters to escape the character.
There must be an even number of keys in this field.
All key pairs must have the smaller key in the first value and the larger key in the second value; otherwise the key pairs will be rejected.
Wildcards are not supported in this field.
If the provided key is greater than the actual length of the VSAM key, the provided key will be truncated. If the key provided is shorter than the VSAM key, it will be padded with hex zeroes.
If the Key Range and Key fields are blank, activities for all keys are considered a match.
Examples:

`"KEY01","KEY09″`
: Matches record level monitoring events where the key is between KEY01 and KEY09

`"KEY01","KEY09","KEY11","KEY19″`
: Matches record level monitoring events where the key is between KEY01 and KEY09 or between KEY11 and KEY19

`"x'F0F0'","x'F0F9'″`
: Matches record level monitoring events where the key has a hexadecimal value between F0F0 and F0F9

`"x'F0F0'","x'F0F9'","x'F1F0'","x'F1F9'"`
: Matches record level monitoring events where the key has a hexadecimal value between F0F0 and F0F9 or between F1F0 and F1F9

`"\x'F0F0'","\x'F0F9'″`
: Matches record level monitoring events where the key is between x'F0F0' and x'F0F9'

RLM Event

Indicates what type of record level monitoring events should be considered for a match.
Only applies to VSAM record level monitoring collection.
Must contain zero or more of the following values, separated by a comma (,): RINS|RDEL|RWRT|RGET|ALL|SKIP, where:

RINS
: A record insert within a data set of a supported type

RDEL
: A record delete within a data set of a supported type

RWRT
: A record level update within a record of a supported type

RGET
: A record level that is read within a data set of a supported type

`ALL`

: Returns all record level events

SKIP

Returns no record level events

If left blank, then SKIP is the default and nothing is considered a match
Examples:

RINS
: Matches record level monitoring events where the operation was a record insert

RINS,RDEL
: Matches record level monitoring events where the operation was a record insert or a record delete

Data Set Event
: Indicates what type of SMF Data Set Events should be considered for a match.
Must contain zero or more of the following values, separated by a comma (,):

```
DSCLI | DSCLO | DSOP | DSCL | DSUP | DSDL | DSRN | DSCR | DSALT | DSRAL | DSRCN | DSRRD |
DSRUP | DSRDF | MADD | MREP | MREN | STOWI | ALL | SKIP
```

where:

DSOP
: An OPEN event against a supported data set type

DSCL
: A CLOSE event against a supported data set type

DSCLI
: A CLOSE event against a supported data set type that was opened for input

DSCLO
: A CLOSE event against a supported data sets type that was opened for output

DSUP
: An UPDATE event against a supported data set type

DSDL
: A DELETE event against a supported data set type

DSRN
: A RENAME event against a supported data set type

DSCR
: A DEFINE or NEW ALLOCATION event of a supported data set type

DSALT
: An ALTER of the attributes of a supported data set type

DSRAL
: A security facility ALTER access of a supported data set type

DSRCN
: A security facility CONTROL access of a supported data set type

DSRRD
: A security facility READ access of a supported data set type

DSRUP
: A security facility UPDATE access of a supported data set type

DSRDF
: A security facility DEFINE access of a supported data set type

MADD
: A member add event against a supported data set type

MREP
: A member replace event against a supported data set type

MREN
: A member rename event against a supported data set type

MDEL
: A member delete event against a supported data set type

STOWI
: A STOW initialize event against a supported data set type

ALL
: Returns all data set level events

SKIP
: Returns no data set level events

If left blank, ALL is the default and all types are considered a match.
Examples:

DSOP
: Matches data set events where an open occurred.

DSOP,DSCL
: Matches data set events where an open or a close occurred.

Valid relational operators are:

- EQ (Equals)
- NE (Does not equal)
- GE (Greater than or equal to)
- LE (Less than or equal to)
- GT (Greater than)
- LT (Less than)

Note:

- If you are using a relational operator with the Group of Values list, you must ensure that the operator is appended to the last field in the list, otherwise it will be treated as an additional value for that field.

- To use individual values along with those listed in the Group of Values list, the relational operator must be appended to the last field in the Group of Values list, rather than to the individual field.

String comparisons are performed in lexicographical order. Because the strings are in EBCDIC, the order is lowercase, uppercase, and then numeric. Special character positions depend on the hexadecimal value of the special character itself in relation to the other characters.

Data Set Type

Indicates the type of data sets that should be considered for a match.
Must contain zero or one of the following values:

VSAM|NONVSAM|ALL, where:

VSAM
: VSAM data sets

NONVSAM
: Non-VSAM data sets

All
: Both VSAM and non-VSAM data sets

If nothing is specified, then only VSAM data set types are collected.

Parent topic: IBM Guardium S-TAP for Data Sets administration

CICS collection filtering parameters

Use the following filtering parameters to collect transaction data from CICS®.

CICS User ID

Indicates the CICS logon user ID to use when searching for a match
1 - 8 character CICS logon user ID to match
The user ID can be followed by a comma (,) and a relational operator. If no relational operator is specified, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS logon user IDs are considered a match

Examples:

CICUSR01
: Matches events that are caused by CICS logon user CICUSR01

CICUSR01,EQ
: Matches events that are caused by CICS logon user CICUSR01

CICUSR%,EQ
: Matches events that are caused by CICS logon users with the prefix CICUSR

CICS Transaction ID

Indicates the CICS transaction ID to use when searching for a match
1 - 4 character CICS transaction ID to match
The transaction ID can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS transaction IDs are considered a match.

Examples:

VTAP
: Matches events that occur within CICS transaction ID VTAP

VTAP,EQ
: Matches events that occur within CICS transaction ID VTAP

VT%,EQ
: Matches events that occur within CICS transaction IDs starting with the prefix VT

CICS Terminal ID

Indicates the CICS terminal ID to use when searching for a match
1 - 4 character CICS terminal ID to match
The terminal ID can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS terminal IDs are considered a match.

Examples

VTAP
: Matches events that occur within CICS transaction ID VTAP

VTAP,EQ
: Matches events that occur within CICS transaction ID VTAP

VT%,EQ
: Matches events that occur within CICS transaction IDs starting with the prefix VT

CICS Region ID

Indicates the CICS region ID to use when searching for a match. The Region ID is defined in the CICS Transaction Server System Initialization Table parameter SYSIDNT.
1 - 4 character CICS region ID to match
The region ID can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS region IDs are considered a match.

Examples:

CICA
: Matches events that occur within the CICS region with an ID of CICA

CICA,EQ
: Matches events that occur within the CICS region with an ID of CICA

CIC%,EQ
: Matches events that occur within the CICS regions with a prefix of CIC

CICS Program Name
: Indicates the CICS program name to use when searching for a match.
1 - 8 character CICS program name to match.
The program name can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS program names are considered a match.

Examples:

PAYROLLA
: Matches events that occur under control of the program that is named PAYROLLA

PAYROLLA,EQ
: Matches events that occur under control of the program that is named PAYROLLA

PAYROLL%,EQ
: Matches events that occur under control of program names that are prefixed with PAYROLL

CICS File ID
: Indicates the CICS file ID to use when searching for a match.
1 - 8 character CICS file ID to match.
The file ID can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS file IDs are considered a match.

Examples:

HRKSDS01
: Matches events that occur for CICS file ID HRKSDS01

HRKSDS01,EQ
: Matches events that occur for CICS file ID HRKSDS01

HRKSDS%,EQ
: Matches events that occur for CICS file IDs prefixed with HRKSDS

CICS Function Code
: Indicates the CICS function code to use when searching for a match. The function code is defined in the CICS Transaction Server Customization Guide. Search for "File control domain exits, XFCFRIN and XFCFROUT." See the description for the XFCFROUT parameter UEP_FC_FUNCTION. The hex values for the UEP_FC_FUNCTION symbolic names are defined in the DFHUEXIT macro in the CICS SDFHMAC macro library.
Two hex characters represent the single character CICS function code.
The function code can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are not supported.
If left blank, then all CICS function codes are considered a match.

Examples

01
: Matches events that occur with the CICS function code defined by the hex character 01

01,EQ
: Matches events that occur with the CICS function code defined by the hex character 01

Parent topic: IBM Guardium S-TAP for Data Sets administration

Reference information

This section provides IBM® Guardium® S-TAP® for Data Sets reference information.

- **Simulation mode**
  Simulation mode enables you to simulate agent processing. IBM Guardium S-TAP for Data Sets uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.
- **VSAM and non-VSAM data set types and events**
  IBM Guardium S-TAP for Data Sets agent performs data set and record level monitoring for VSAM and non-VSAM data sets. The data set types, as well as the type of events that IBM Guardium S-TAP for Data Sets collects, are described here.
- **SMF record types and contexts**
  SMF records are correlated to IBM Guardium S-TAP for Data Sets contexts, as shown in the following table.
- **Time-to-reporting considerations**
  Learn about the benefits, considerations, and exceptions that apply to the time-to-reporting feature.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Simulation mode

Simulation mode enables you to simulate agent processing. IBM® Guardium® S-TAP® for Data Sets uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by

using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.

When STAP_STREAM_EVENTS is set to *N*, the parameter stops the agent TCP/IP data transmission process. The agent performs all data collection processes but does not send the audit record to the Guardium appliance.

The DISPLAY STREAM command display whether the TCP/IP stream of data to the appliance is enabled or disabled. Use this command to verify whether the agent is sending data to the Guardium appliance.

The DIAG command displays the number of created SMF-based records, RLM-based records, and the number of records sent to the appliance. When the agent is in simulation mode (STAP_STREAM_EVENTS=N), the SMF and RLM counters increment with each record created, but the number of records sent to the appliance remains zero. When the agent is not in simulation mode (STAP_STREAM_EVENTS=Y), all counters increment.

Parent topic: Reference information

VSAM and non-VSAM data set types and events

IBM Guardium S-TAP for Data Sets agent performs data set and record level monitoring for VSAM and non-VSAM data sets. The data set types, as well as the type of events that IBM Guardium S-TAP for Data Sets collects, are described here.

Data set level monitoring

The IBM Guardium S-TAP for Data Sets agent collects SMF data for the following data set organizations:

VSAM

ESDS
: Entry sequence data set

KSDS
: Key-sequenced data set

RRDS
: Relative record data set

VRRDS
: Variable length relative record data set

LDS
: Linear data set

Non-VSAM

PS
: Physical sequential

PO
: Partitioned organization

DA
: Direct access

PDSE
: Partitioned organization-extended

The agent audits these data set types by correlating data from a combination of SMF record types to construct one of the following audit events.

VSAM

DATA SET CREATE (DSCR)
: A DEFINE or New Allocation event of a supported data set type

DATA SET OPEN (DSOP)
: An OPEN event against a supported data set type

DATA SET CLOSE (DSCL)
: A CLOSE event against a supported data set type

DATA SET CLOSE INPUT (DSCLI)
: A CLOSE event against a supported data set type that was opened for input

DATA SET CLOSE OUTPUT (DSCLO)
: A CLOSE event against a supported data set type that was opened for output

DATA SET UPDATE (DSUP)
: An UPDATE event against a supported data set type

DATA SET RENAME (DSRN)
: A RENAME event of a supported data set type

DATA SET ALTER (DSALT)
: An ALTER of the attributes of a supported data set type

DATA SET DELETE (DSDL)
: A DELETE event of a supported data set type

Security facility DEFINE violation (DSRDF)
: A security facility DEFINE violation of a supported data set type

Security facility READ violation (DSRRD)
: A security facility READ violation of a supported data set type

Security facility UPDATE violation (DSRUP)
: A security facility UPDATE violation of a supported data set type

Security facility ALTER violation (DSRAL)
: A security facility ALTER violation of a supported data set type

Security facility CONTROL violation (DSRCN)
: A security facility CONTROL violation of a supported data set type

Non-VSAM

DATA SET CREATE (DSCR)
: A DEFINE or New Allocation event of a supported data set type
: For non-SMS data sets, a RENAME event also produces a DATA SET CREATE context record, in addition to a DATA SET RENAME context record.

DATA SET CLOSE (DSCL)
: A CLOSE event against a supported data set type

DATA SET CLOSE INPUT (DSCLI)
: A CLOSE event against a supported data set type that was opened for input

DATA SET CLOSE OUTPUT (DSCLO)
: A CLOSE event against a supported data set type that was opened for output

DATA SET DELETE (DSDL)
: A DELETE event of a supported data set type

DATA SET RENAME (DSRN)
: A RENAME event of a supported data set type

Member add (MADD)
: A member ADD event against a supported data set type

Member replace (MREP)
: A member REPLACE event against a supported data set type

Member rename (MREN)
: A member RENAME event against a supported data set type

Member delete (MDEL)
: A member DELETE event against a supported data set type

STOW initialize (STOWI)
: A STOW initialize event against a supported data set type

Security facility DEFINE violation (DSRDF)
: A security facility DEFINE violation of a supported data set type

Security facility READ violation (DSRRD)
: A security facility READ violation of a supported data set type

Security facility UPDATE violation (DSRUP)
: A security facility UPDATE violation of a supported data set type

Security facility ALTER violation (DSRAL)
: A security facility ALTER violation of a supported data set type

Security facility CONTROL violation (DSRCN)
: A security facility CONTROL violation of a supported data set type

Note: For partitioned organization data sets (PDS and PDSE) that are processed by using EXCP:

- Member additions, updates, and deletions are reported by z/OS® as updates to the base data set.
- IBM Guardium S-TAP for Data Sets reports member additions, updates, and deletions as CLOSE events with an access of OUTPUT.

Record level monitoring

The IBM Guardium S-TAP for Data Sets agent collects record access information for the following VSAM data set types:

KSDS
: Key-sequenced data set

RRDS
: Relative record data set

VRRDS
: Variable length relative record data sets

The agent audits these record level monitoring events:

RECORD INSERT
: A record insert within a data set of a supported type

RECORD DELETE
: A record delete within a data set of a supported type

RECORD READ
: A record read within a data set of a supported type

RECORD UPDATE
: A record update within a data set of a supported type

Parent topic: Reference information

SMF record types and contexts

SMF records are correlated to IBM Guardium S-TAP for Data Sets contexts, as shown in the following table.

Table 1. SMF record types, subtypes, and contexts

Record number	Record subtype	Purpose	SMF context
14		Collecting non-VSAM file activity	CLOSE (non-VSAM input)
15		Collecting non-VSAM file activity	CLOSE (non-VSAM output)
17		Collecting Delete activity	DELETE (non-VSAM)
18		Collecting Rename activity	RENAME (non-VSAM)
30	4, 5	Collecting Job/Step activity	Accounting
42	6	Collecting VSAM type information	Accounting (VSAM)
42	20	Collecting PDS/PDSE member activity	STOW initialization (PDSE directory clearing)
42	21	Collecting PDS/PDSE member activity	DELETE (PDS/PDSE member)
42	24	Collecting PDS/PDSE member activity	ADD/REPLACE (PDS/PDSE member)

Record number	Record subtype	Purpose	SMF context
42	25	Collecting PDS/PDSE member activity	RENAME (PDS/PDSE member)
60*		Collecting VVDS update activity	Data Set ALTER, Data Set CREATE
61*		Collecting DEFINE/CATLG activity	Data Set CREATE
62		Collecting VSAM file activity	OPEN (VSAM)
64		Collecting VSAM I/O statistics	CLOSE (VSAM)
65		Collecting Delete activity	DELETE (VSAM)
66*		Collecting Rename activity	RENAME, ALTER (VSAM)
80		Collecting CICS sign-on security violations	Security Violation

*For more information, see the SMF records section of the *IBM z/OS MVS System Management Facilities (SMF)* documentation, available in the IBM Knowledge Center.

Note:

- There is not a one-to-one correlation between SMF records and context events reported. If more than one SMF record is encountered within a step for a single event, then subsequent records are considered duplicates.
- Audit records for data set events are produced as they occur.
- Data Set CREATE context can appear for RENAME requests of non-SMS, non-VSAM data sets, because the RENAME process generates an SMF type 61 record.

Parent topic: Reference information

Related reference

- Configuring the SMFPRMxx parameter library member

Time-to-reporting considerations

Learn about the benefits, considerations, and exceptions that apply to the time-to-reporting feature.

IBM Guardium S-TAP for Data Sets provides faster real-time reporting for data set level events. When possible, the S-TAP agent immediately delivers data set level information to the Guardium system. The agent presents the data as it occurs, giving you up-to-the-minute results without waiting for jobs to end or SMF type 30 records to be generated.

Benefits

Immediate reporting
: No need to wait for a CICS® address space to terminate, or a TSO user logs off.

Reduced storage usage
: The agent immediately reports data set events to the Guardium system, which substantially reduces the agent storage requirement. The data set event record is complete and ready for transmission to the Guardium system as soon as z/OS® MVS™ creates the source SMF record.

Considerations

Additional event records
: A notable difference as a result of this enhancement is the appearance of data set event records that were not identified in previous versions of this product. Collecting the data set event records in preparation for the SMF type 30 record caused seemingly similar records to merge. For example, a Close event could be reported for a KSDS event, although z/OS DFSMSdfp actually records this as two separate events (one for the Cluster Data component, and one for the Cluster Index component). Improved time-to-reporting now more accurately reflects data set events.

Events Span Data Set Types
: With this feature, and the V10.0 addition of non-VSAM reporting, data set event records might span data set types. For example, when you delete a VSAM KSDS event, z/OS DFSMSdfp deletes a VSAM and a non-VSAM collection of components. Use the DS_TYPE policy filter to adjust this reporting.

Exceptions

To avoid waiting for the SMF type 30 record, the agent scans various z/OS system control blocks in the address space when z/OS is writing the data set SMF record. There are instances when these control blocks are unavailable because of the state of the address space. Before this scan is run, the agent assesses the state of the address space for compatibility. If the address space is not in a compatible state, the agent waits for the SMF type 30 record, which delays reporting of the event until the address space has terminated.

Parent topic: Reference information

Troubleshooting

Use these topics to diagnose and correct problems that you might experience with IBM Guardium S-TAP for Data Sets.

- **Messages and codes**

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Messages and codes

This information documents the messages and error codes issued by IBM Guardium S-TAP for Data Sets. Messages are presented in ascending alphabetical and numerical order.

- **Error message code descriptions**

Parent topic: Troubleshooting

Error message code descriptions

IBM Guardium S-TAP for Data Sets error messages adhere to the following format: AUV*nnnx*

Where:

AUV
: Indicates that the message was issued by IBM Guardium S-TAP for Data Sets.

nnn
: Indicates the message identification number.

x
: Indicates the severity of the message:

Table 1. Error message severity codes

Severity Code	Description
A	Indicates that operator intervention is required before processing can continue.
E	Indicates that an error occurred, which might or might not require operator intervention.
I	Indicates that the message is informational only.
W	Indicates that the message is a warning to alert you to a possible error condition.

- **AUV1001I**
  RULEDEFS ACTIVATION SUCCESSFUL –*ssss*
- **AUV1002E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV1003E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV1004E**
  UNABLE TO LOCATE REQUIRED DDNAME - CONTROL
- **AUV1005E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME CONTROL, RC=*rrrrrrrr*
- **AUV1006E**
  UNABLE TO LOCATE REQUIRED DDNAME - OPTIONS
- **AUV1007E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME OPTIONS, RC=*rrrrrrrr*
- **AUV1008I**
  RULEDEFS NOT ACTIVATED –*ssss*
- **AUV1009E**
  OPEN FAILED FOR PROCESSING OPTIONS MEMBER; DEFAULT OPTIONS USED
- **AUV1012E**
  ATTACH FOR AUVMAIN FAILED, RC=*rrrrrrrr*
- **AUV1013I**
  PRODUCT TERMINATION IS COMPLETE
- **AUV1014E**
  INVALID START PARAMETERS SPECIFIED; IGNORED
- **AUV1015E**
  INVALID PARM SPECIFIED - *parm*
- **AUV1016E**
  DELIMITER "=" IS MISSING - *parm*
- **AUV1017I**
  START PARAMETER SPECIFIED - *parm*
- **AUV1018E**
  INVALID VALUE SPECIFIED FOR PARAMETER - *parm*
- **AUV1019I**
  START PARAMETER SPECIFIED - *parm*
- **AUV1020E**
  VALUE SPECIFIED FOR PARAMETER - *parm*
- **AUV1021E**
  INVALID OPTION SPECIFIED - *pppppppp*
- **AUV1022E**
  INVALID KEYWORD/DELIMITER - *pppppppp*
- **AUV1023E**
  INVALID VALUE SPECIFIED FOR OPTION - *pppppppp*
- **AUV1024I**
  PROCESSING OPTION SET - SUBSYS=*ssss*
- **AUV1025E**
  INVALID VALUE SPECIFIED FOR OPTION - SUBSYS=*ssss*
- **AUV1026I**
  PROCESSING OPTION SET - INITIAL_RULEDEF=*rrrrrrrr*
- **AUV1027E**
  INVALID VALUE SPECIFIED FOR OPTION -INITIAL_RULEDEF=*rrrrrrrr*
- **AUV1028I**
  PROCESSING OPTION SET - PORT=*nnnnn*
- **AUV1029E**
  INVALID VALUE SPECIFIED FOR OPTION - PORT=*nnnnn*
- **AUV1030I**
  PROCESSING OPTION SET – APPLIANCE_PING_RATE=*nnnnn*
- **AUV1031E**
  INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_PING_RATE=*nnnnn*

- **AUV1032I**
  PROCESSING OPTION SET – APPLIANCE_RETRY_INTERVAL=*nnnnn*
- **AUV1033E**
  VALUE SPECIFIED FOR OPTION – APPLIANCE_RETRY_INTERVAL=*nnnnn*
- **AUV1034E**
  ERROR IN NAME/TOKEN RETRIEVAL PROCESSING, RC=*rrrrrrrr*
- **AUV1035E**
  NAME/TOKEN ALREADY EXISTS, BUT TOKEN IS ZERO
- **AUV1036E**
  NAME/TOKEN ALREADY EXISTS, BUT TOKEN DOES NOT POINT TO A VALID PRODUCT BLOCK
- **AUV1038E**
  UNABLE TO OBTAIN STORAGE FOR PRODUCT CONTROL BLOCK, RC=*rrrrrrrr*
- **AUV1040E**
  ERROR IN NAME/TOKEN CREATE PROCESSING, RC=*rrrrrrrr*
- **AUV1041I**
  PRODUCT INTERCEPTS HAVE BEEN ESTABLISHED
- **AUV1042E**
  UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*
- **AUV1043E**
  BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*
- **AUV1044E**
  UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*
- **AUV1046E**
  PRIVATE LOAD FAILED FOR *mmmmmmmm*
- **AUV1047E**
  COMMON LOAD FAILED FOR *mmmmmmmm*
- **AUV1048I**
  PROCESSING OPTION SET: APPLIANCE_CONNECT_RETRY_COUNT
- **AUV1049E**
  INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_CONNECT_RETRY_COUNT=*nnnnn*
- **AUV1050E**
  UNABLE TO ESTABLISH *NNNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*
- **AUV1052E**
  UNABLE TO DELETE *NNNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*
- **AUV1054E**
  GSSB IS NOT PRESENT
- **AUV1055E**
  GSSB CONTROL BLOCK ID IS INVALID
- **AUV1056I**
  PROCESSING OPTION SET – APPLIANCE_NETWORK_REQUEST_TIMEOUT=*nnnnn*
- **AUV1058E**
  UNABLE TO LOCATE LPDE FOR IGC0005E
- **AUV1058I**
  PROCESSING OPTION SET – APPLIANCE_SERVER=*a**
- **AUV1059E**
  INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER=*a**
- **AUV1060I**
  PROCESSING OPTION SET – AUDIT=*a**
- **AUV1061E**
  VALUE SPECIFIED FOR OPTION – AUDIT=*a**
- **AUV1062I**
  PROCESSING OPTION SET – CICS_SUPPORT=*nnnnnnn*
- **AUV1063E**
  INVALID VALUE SPECIFIED FOR OPTION – CICS_SUPPORT=*nnnnnnn*
- **AUV1064W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **AUV1065E**
  UNABLE TO LOCATE LPDE FOR IDA0192A
- **AUV1066E**
  UNABLE TO LOCATE IDA0192A
- **AUV1067E**
  PAGE SERVICE LIST EXHAUSTED FOR *xx* INTERCEPT
- **AUV1068E**
  UNABLE TO OBTAIN STORAGE FOR *xx* INTERCEPT, RC=*rrrrrrrr*
- **AUV1069E**
  UNABLE TO LOCATE IDA0200T
- **AUV1070I**
  TCP/IP STREAMING DISABLED DUE TO USER SETTING
- **AUV1073W**
  MAXIMUM ACTIVE SUBSYSTEMS EXCEEDED (1)
- **AUV1074E**
  DUPLICATE SUBSYSTEM FOUND FOR SSID=*ssss*
- **AUV1077I**
  PII DATA NOT BEING TRANSMITTED DUE TO USER SETTING
- **AUV1080E**
  ERROR IN NAME/TOKEN DELETE PROCESSING, RC=*rrrrrrrr*
- **AUV1081E**
  GETMAIN FAILED FOR JSPB VECTOR TABLE, RC=*rrrrrrrr*
- **AUV1082W**
  IEFU86 EXIT IS NOT DEFINED

- **AUV1100E**
  ACRONYM CHECK FAILED FOR GSSB
- **AUV1101E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV1102E**
  ERROR OCCURRED IN CROSS-MEMORY INITIALIZATION
- **AUV1103E**
  ATTACH FOR AUVPING FAILED, RC=*rrrrrrrr -ssss*
- **AUV1105E**
  ATTACH FOR AUVSSRP FAILED, RC=*rrrrrrrr -ssss*
- **AUV1105I**
  SUBSYSTEM IS ACTIVE AND ENABLED
- **AUV1106I**
  SUBSYSTEM INITIALIZATION IS COMPLETE
- **AUV1107I**
  PRODUCT TERMINATION HAS BEEN REQUESTED
- **AUV1111E**
  UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*
- **AUV1112E**
  BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*
- **AUV1113E**
  UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*
- **AUV1115E**
  INITIAL LOAD FAILED FOR *mmmmmmmm*
- **AUV1116E**
  DIRECTED LOAD FAILED FOR *mmmmmmmm*
- **AUV1117E**
  NON-ZERO RETURN CODE FROM SYSEVENT, RC=*rrrrrrrr -ssss*
- **AUV1122E**
  INVALID COMMAND SPECIFIED - *cccccccc -ssss*
- **AUV1123E**
  INVALID COMMAND SPECIFIED - *cccccccc -ssss*
- **AUV1123W**
  ACTIVE SUBSYSTEM DETECTED; PRODUCT-LEVEL MODULE NOT RE-INITIALIZED
- **AUV1124E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1125E**
  INSUFFICIENT OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1126E**
  INVALID OPERAND SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1127I**
  SUBSYSTEM IS ACTIVE | INACTIVE AND ENABLED | DISABLED *-ssss*
- **AUV1128E**
  INVALID COMMAND SPECIFIED - *command*
- **AUV1129I**
  THERE ARE CURRENTLY NO SUBSYSTEMS *-ssss*
- **AUV1130I**
  SUBSYSTEM xxxx IS ACTIVE | INACTIVE AND ENABLED | DISABLED *-ssss*
- **AUV1131I**
  RULEDEFS ACTIVATED ON *mm/dd/yyyy* AT *hh:mm:ss* FROM MEMBER *mmmmmmmm -ssss*
- **AUV1132I**
  RULEDEFS NOT ACTIVATED *-ssss*
- **AUV1136I**
  PRODUCT-LEVEL TRACING IS ENABLED | DISABLED *-ssss*
- **AUV1137I**
  SUBSYSTEM-LEVEL TRACING IS ENABLED | DISABLED *-ssss*
- **AUV1138E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1140I**
  SMF MONITORING SUCCESSFULLY ENABLED – *SSSS*
- **AUV1141I**
  SUBSYSTEM IS NOW ENABLED *-ssss*
- **AUV1142I**
  TCP/IP STREAM SUCCESSFULLY ENABLED *-ssss*
- **AUV1143I**
  SMF MONITORING SUCCESSFULLY DISABLED –*SSSS*
- **AUV1144I**
  TRACING FOR PRODUCT IS NOW ENABLED *-ssss*
- **AUV1145I**
  TRACING FOR SUBSYSTEM IS NOW ENABLED *-ssss*
- **AUV1146E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1147I**
  TCP/IP STREAM IS *EEEEEEEE -ssss*
- **AUV1149I**
  SUBSYSTEM IS NOW DISABLED *-ssss*
- **AUV1150I**
  TCP/IP STREAM SUCCESSFULLY DISABLED *-ssss*
- **AUV1151E**
  SMF MONITORING DISABLE NOT SUCCESSFUL –*SSSS*

- **AUV1152I**
  TRACING FOR PRODUCT IS NOW DISABLED -*ssss*
- **AUV1153I**
  TRACING FOR SUBSYSTEM IS NOW DISABLED -*ssss*
- **AUV1154E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc* -*ssss*
- **AUV1155E**
  SMF MONITORING ENABLE FAILED –*SSSS*
- **AUV1156E**
  SMF MONITORING ALREADY ENABLED –*SSSS*
- **AUV1157E**
  OPERANDS SPECIFIED FOR COMMAND - *command*
- **AUV1158E**
  SMF MONITORING ALREADY DISABLED –*SSSS*
- **AUV1175I**
  DDDDDDDD MEMBER ACTIVATION SUCCESSFUL –*SSSS*
- **AUV1176E**
  DDDDDDDD MEMBER ACTIVATION FAILED – SEE JESYSMSG FOR DETAILS –*SSSS*
- **AUV1176I**
  dddddddd MEMBER *mmmmmmmm* ACTIVATION FAILED - SEE JESYSMSG FOR DETAILS -*ssss*
- **AUV1177I**
  dddddddd MEMBER *mmmmmmmm* ACTIVATION FAILED - FAILURE CODE *cccc* -*ssss*
- **AUV1179E**
  DDDDDDDD MEMBER ACTIVATION FAILED - FAILURE CODE *CCCCCCCC* –*SSSS*
- **AUV1184E**
  COMMAND VERB NOT UNIQUE - cccccccc -ssss
- **AUV1185E**
  INVALID COMMAND SYNTAX SPECIFIED - *ssss*
- **AUV1191E**
  INVALID MODULE NAME SPECIFIED - *cccccccc*
- **AUV1192I**
  MODULE *mmmmmmmm vvvv ffffffff dddddddd ttttt*
- **AUV1193I**
  MODULE *mmmmmmmm* LOCATED AT *aaaaaaaa* (*stgloc*)
- **AUV1195E**
  ERROR OCCURRED DURING FREEMAIN FOR GPB, RC=*rrrrrrrr*
- **AUV1196E**
  UNEXPECTED VCON COUNT FOR *xx* INTERCEPT; EXPECTED=*eee*, FOUND=*fff*
- **AUV1200E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1202E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1203E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1204E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1213E**
  ERROR RETRIEVING SSRE
- **AUV1214E**
  UNEXPECTED SSRE QUEUE ERROR
- **AUV1215E**
  UNEXPECTED SSRE QUEUE ERROR
- **AUV1400I**
  RECORD LEVEL MONITORING IS *EEEEEEEE* -*SSSS*
- **AUV1401I**
  RECORD LEVEL MONITORING INTERCEPTS ARE *EEEEEEEE* -*SSSS*
- **AUV1402I**
  CURRENT POLICY *EEE* -*SSSS*
- **AUV1405I**
  RECORD LEVEL MONITORING SUCCESSFULLY ENABLED -*SSSS*
- **AUV1406W**
  RECORD LEVEL MONITORING SUCCESSFULLY ENABLED, BUT NO RLM FILTERS EXIST IN CURRENT POLICY -*SSSS*
- **AUV1408W**
  POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*
- **AUV1410I**
  PROCESSING OPTION SET - SOCKET_CONNECT_TIMEOUT=*nnnnn*
- **AUV1411E**
  INVALID VALUE SPECIFIED FOR OPTION - SOCKET_CONNECT_TIMEOUT=*nnnnn*
- **AUV1412I**
  PROCESSING OPTION SET - OUTAGE_SPILLAREA_SIZE=*nnnnnnn*
- **AUV1413E**
  INVALID VALUE SPECIFIED FOR OPTION – OUTAGE_SPILLAREA_SIZE=*nnnnnnn*
- **AUV1414I**
  PROCESSING OPTION SET - INTERNAL_BUFFER_SIZE=*nnnnnnn*
- **AUV1415E**
  INVALID VALUE SPECIFIED FOR OPTION INTERNAL_BUFFER_SIZE=*nnnnnnn*
- **AUV1416I**
  PROCESSING OPTION SET - APPLIANCE_SERVER_FAILOVER=a*
- **AUV1417E**
  INVALID VALUE SPECIFIED FOR OPTION - *keyword*=a*

- **AUV1418I**
  PROCESSING OPTION SET - IAM_SMF_RECORD_ID = *nnn*
- **AUV1419E**
  INVALID VALUE SPECIFIED FOR OPTION - IAM_SMF_RECORD_ID = *nnn*
- **AUV1420I**
  PROCESSING OPTION SET - ACF_SMF_RECORD_ID = *nnn*
- **AUV1421E**
  INVALID VALUE SPECIFIED FOR OPTION - ACF_SMF_RECORD_ID = *nnn*
- **AUV1422I**
  PROCESSING OPTION SET - APPLIANCE_SERVER_LIST(*nnn*)
- **AUV1423E**
  INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER_LIST(*nnn*)
- **AUV1424I**
  PROCESSING OPTION SET - MEGABUFFER_COUNT =*nnnnnnn*
- **AUV1425E**
  INVALID VALUE SPECIFIED FOR OPTION MEGABUFFER_COUNT =*nnnnnnn*
- **AUV1438I**
  SMF MONITORING IS *EEEEEEEE -SSSS*
- **AUV1439I**
  SMF MONITORING EXITS ARE *EEE -SSSS*
- **AUV1450W**
  SMF RECORDING TEST FAILED, RC=*cc*, TYPE=*nnnn*, SUBSYSTEM=*ssss*
- **AUV1747E**
  SUBSYSTEM IS NOT ACTIVE OR ENABLED
- **AUV1748W**
  POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*
- **AUV2000E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV2030E**
  UNRECOGNIZED INTERCEPT ID ENCOUNTERED (*XX*)
- **AUV2040E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JCT, RC=*rrrrrrrr*
- **AUV2041E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR SCT, RC=*rrrrrrrr*
- **AUV2042E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JMR, RC=*rrrrrrrr*
- **AUV2097I**
  JCT UNAVAILABLE FOR JSPB LOOK-UP FOR ASID *xxxx*
- **AUV2098I**
  ASID *xxxx* EXCEEDS GJVT MAX; ASVTMAXU=*xxxxxxxx*
- **AUV2104E**
  ERROR OCCURRED IN FREEMAIN OF AUVSMFX1, RC=*RRRRRRRR*
- **AUV2170I**
  ATTEMPTING TO CONNECT TO THE GUARDIUM APPLIANCE
- **AUV2171I**
  CALL TO GUARDIUM APPLIANCE SUCCESSFUL
- **AUV2172E**
  function CALL TO GUARDIUM APPLIANCE FAILED
- **AUV2173E**
  function CALL TO GUARDIUM APPLIANCE FAILED, RC = *rc* RC_STP= *rc* RS_STP= *rs* RC_GDM= *rc* RC_PB = *rc* RC_LST= *rc* RS_LST= *rs*
- **AUV2174E**
  SPILL FILE FULL, DATA LOSS MIGHT OCCUR
- **AUV2175E**
  CONNECTION LOST WITH NO SPILL FILE, DATA LOSS MIGHT OCCUR
- **AUV2176E**
  UNABLE TO OBTAIN STORAGE, DATA LOSS MIGHT OCCUR
- **AUV2177E**
  RULEDEF NOT ACTIVATED - CHECK SYSPRINT FOR REASON
- **AUV2178I**
  SPILL FILE IS *xx*% FULL
- **AUV2179E**
  UNABLE TO OBTAIN REQUESTED STORAGE FOR INTERNAL_BUFFER_SIZE: dddd. PROCESSING CONTINUES.
- **AUV2180W**
  WRITING TO SPILL FILE
- **AUV2181I**
  NO LONGER WRITING TO SPILL FILE
- **AUV2182I**
  CONNECTION ESTABLISHED TO *x*
- **AUV2183W**
  STORAGE SHORTAGE DETECTED; ONE OR MORE EVENTS NOT RECORDED
- **AUV2184W**
  STORAGE SHORTAGE RELIEVED; EVENT RECORDING RESUMED. EVENTS LOST=????????
- **AUV2185I**
  UNEXPECTED PRODUCT STATE DETECTED. ATTEMPTING RESTART.
- **AUV2186E**
  UNABLE TO RESOLVE HOST NAME *a**
- **AUV2900E**
  INVALID STORAGE REQUEST FOR CONTROL BLOCK *nnnn -ssss*
- **AUV2901E**
  INSUFFICIENT VIRTUAL STORAGE FOR CONTROL BLOCK *nnnn -ssss*

- **AUV2902E**
  ACRONYM CHECK FAILED WHILE ATTEMPTING TO FREE *nnnn*, DATA=*dddd -ssss*
- **AUV2903E**
  FAILURE OCCURRED DURING FREEMAIN FOR *nnnn -ssss*
- **AUV3000E**
  ERROR ENABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3001E**
  ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNN*
- **AUV3003E**
  ERROR STARTING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3004I**
  AUVPLTPI XFCFROUT GLOBAL USER EXIT SUCCESSFULLY ENABLED AND STARTED
- **AUV3005E**
  ERROR STOPPING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3006E**
  ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNN*
- **AUV3008E**
  ERROR DISABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3009I**
  AUVPLTPS XFCFROUT GLOBAL USER EXIT SUCCESSFULLY STOPPED AND DISABLED
- **AUV3010W**
  CICS PLTPI INSTALLED BUT CICS_SUPPORT NOT SPECIFIED IN OPTIONS

Parent topic: Messages and codes

AUV1001I RULEDEFS ACTIVATION SUCCESSFUL –*ssss*

Explanation

This message is issued to the operator console following successful activation of rule definitions using the ACTIVATE RULEDEFS operator command.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1002E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

Product initialization was unable to obtain the required above-the-line storage.

User response

Increase the amount of available above-the-line storage and attempt to restart the product. If this is not successful, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1003E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

Product initialization was unable to obtain the required below-the-line storage.

User response

Increase the amount of available below-the-line storage and attempt to restart the product. If this is not successful, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1004E UNABLE TO LOCATE REQUIRED DDNAME - CONTROL

Explanation

During product initialization, the CONTROL DD statement was unable to be located in the product started task procedure.

User response

The CONTROL DD statement is required. Add the CONTROL DD statement to the product started task procedure and retry.
Parent topic: Error message code descriptions

AUV1005E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME CONTROL, RC=*rrrrrrrr*

Explanation

An internal error (*rrrrrrrr*) occurred while processing the CONTROL DD statement during product initialization.

User response

Make sure that the CONTROL DD statement points to a valid partitioned data set and retry. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1006E UNABLE TO LOCATE REQUIRED DDNAME - OPTIONS

Explanation

During product initialization, the OPTIONS DD statement was unable to be located in the product started task procedure.

User response

The OPTIONS DD statement is required. Add the OPTIONS DD statement to the product started task procedure and retry.
Parent topic: Error message code descriptions

AUV1007E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME OPTIONS, RC=*rrrrrrrr*

Explanation

An internal error (*rrrrrrrr*) occurred while processing the OPTIONS DD statement during product initialization.

User response

Make sure that the OPTIONS DD statement points to a valid data set and retry. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1008I RULEDEFS NOT ACTIVATED –*ssss*

Explanation

This message is issued in response to the DISPLAY RULEDEFS operator command when no rule definitions have been activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1009E OPEN FAILED FOR PROCESSING OPTIONS MEMBER; DEFAULT OPTIONS USED

Explanation

Open processing was unsuccessful for the OPTIONS member so the default options were used.

User response

Make sure that the OPTIONS DD statement points to a valid data set and retry. If the error continues, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1012E ATTACH FOR AUVMAIN FAILED, RC=*rrrrrrrr*

Explanation

During product initialization, the startup of an internal task failed. The value *rrrrrrrr* identifies the internal error code.

User response

Examine other error messages that might have occurred at the same time as this message to aid in determining the cause of the failure. If no cause can be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1013I PRODUCT TERMINATION IS COMPLETE

Explanation

This message is issued in response to the product shutdown command at completion of termination processing.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1014E INVALID START PARAMETERS SPECIFIED; IGNORED

Explanation

An invalidly constructed parameter was specified on the START command for the started task; it will be ignored.

User response

Correct the START command parameter and restart the started task.
Parent topic: Error message code descriptions

AUV1015E INVALID PARM SPECIFIED - *parm*

Explanation

An unrecognized parameter was specified on the START command for the started task where parm is the unrecognized parameter.

User response

Correct the START command parameter and restart the started task.
Parent topic: Error message code descriptions

AUV1016E DELIMITER "=" IS MISSING - *parm*

Explanation

The START parameter specified by parm requires an equal sign followed by a keyword value; no equal sign was found.

User response

Correct the START command parameter and restart the started task.
Parent topic: Error message code descriptions

AUV1017I START PARAMETER SPECIFIED - *parm*

Explanation

The TRACING START parameter specified by parm was successfully recognized and processed.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1018E INVALID VALUE SPECIFIED FOR PARAMETER - *parm*

Explanation

The TRACING START parameter keyword value for the parameter specified by *parm* was invalid.

User response

Correct the START parameter keyword value and restart the started task.
Parent topic: Error message code descriptions

AUV1019I START PARAMETER SPECIFIED - *parm*

Explanation

The KEY START parameter specified by parm was successfully recognized and processed.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1020E VALUE SPECIFIED FOR PARAMETER - *parm*

Explanation

The KEY START parameter keyword value for the parameter specified by parm was invalid.

User response

Correct the START parameter keyword value and restart the started task.
Parent topic: Error message code descriptions

AUV1021E INVALID OPTION SPECIFIED - *pppppppp*

Explanation

During product initialization, an invalid keyword was encountered when processing the subsystem options in the OPTIONS member. The value *pppppppp* is the invalid option encountered — or the value "(NONE)" if blank options were specified.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1022E INVALID KEYWORD/DELIMITER - *pppppppp*

Explanation

During product installation, while processing the subsystem options in the OPTIONS member, an invalid keyword or delimiter was encountered. The value *pppppppp* indicates the associated keyword.

User response

Correct the specified option keyword or delimiter and restart the product.
Parent topic: Error message code descriptions

AUV1023E INVALID VALUE SPECIFIED FOR OPTION - *pppppppp*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, a keyword was encountered with an invalid value. The value *pppppppp* indicates the option with the incorrect value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1024I PROCESSING OPTION SET - SUBSYS=*ssss*

Explanation

This message is issued during product initialization to display the value (*ssss*) set for the SUBSYS keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1025E INVALID VALUE SPECIFIED FOR OPTION - SUBSYS=*ssss*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SUBSYS option. The value *ssss* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1026I PROCESSING OPTION SET - INITIAL_RULEDEF=*rrrrrrrr*

Explanation

This message is issued during product initialization to display the value (*rrrrrrrr*) specified for the INITIAL_RULEDEF keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1027E INVALID VALUE SPECIFIED FOR OPTION -INITIAL_RULEDEF=*rrrrrrrr*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the INITIAL_RULEDEF option. The value *rrrrrrrr* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1028I PROCESSING OPTION SET - PORT=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) specified for the PORT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1029E INVALID VALUE SPECIFIED FOR OPTION - PORT=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the PORT option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1030I PROCESSING OPTION SET – APPLIANCE_PING_RATE=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) specified for the APPLIANCE_PING_RATE keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1031E INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_PING_RATE=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_PING_RATE option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.

Parent topic: Error message code descriptions

AUV1032I PROCESSING OPTION SET – APPLIANCE_RETRY_INTERVAL=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) specified for the APPLIANCE_RETRY_INTERVAL keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1033E VALUE SPECIFIED FOR OPTION – APPLIANCE_RETRY_INTERVAL=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_RETRY_INTERVAL option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1034E ERROR IN NAME/TOKEN RETRIEVAL PROCESSING, RC=*rrrrrrrr*

Explanation

During product initialization, an internal system error (*rrrrrrrr*) was encountered in establishing the product.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1035E NAME/TOKEN ALREADY EXISTS, BUT TOKEN IS ZERO

Explanation

During product initialization, an internal system error was encountered in establishing the product.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1036E NAME/TOKEN ALREADY EXISTS, BUT TOKEN DOES NOT POINT TO A VALID PRODUCT BLOCK

User response

IPL the system before starting the product. If this does not resolve the problem, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1038E UNABLE TO OBTAIN STORAGE FOR PRODUCT CONTROL BLOCK, RC=*rrrrrrrr*

Explanation

During product initialization, above-the-line CSA storage was unable to be obtained a product control block as indicated by the internal return code *rrrrrrrr*.

User response

Investigate and correct the shortage of above-the-line CSA storage and restart the product. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1040E ERROR IN NAME/TOKEN CREATE PROCESSING, RC=*rrrrrrrr*

Explanation

During product initialization, an internal system error (*rrrrrrrr*) was encountered in establishing the product.

User response

Please contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1041I PRODUCT INTERCEPTS HAVE BEEN ESTABLISHED

Explanation

This message is issued when all intercepts have been successfully established.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1042E UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*

Explanation

During product initialization, above-the-line CSA storage was unable to be obtained for loading a required product routine as detailed by the internal return code *rrrrrrrr*.

User response

Investigate and correct the shortage of above-the-line CSA storage and restart the product. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1043E BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*

Explanation

During product initialization, a required load module was unable to be successfully located. The value *mmmmmmmm* identifies the load module and the value *rrrrrrrr* specifies the internal return code in error.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product.
Parent topic: Error message code descriptions

AUV1044E UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*

Explanation

During product initialization while processing the product load module *mmmmmmmm* an error was encountered.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and restart the product.
Parent topic: Error message code descriptions

AUV1046E PRIVATE LOAD FAILED FOR *mmmmmmmm*

Explanation

During product initialization, the processing of a product load module *(mmmmmmm*) to be located in above-the-line private storage failed.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line private storage available for the product started task. After correcting the problem, restart the product. If the error cannot be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1047E COMMON LOAD FAILED FOR *mmmmmmmm*

Explanation

During product initialization, the processing of a product load module (*mmmmmmm*) to be located in above-the-line common storage, failed.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line common storage available for the product started task. After correcting the problem, restart the product. If the error cannot be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1048I PROCESSING OPTION SET: APPLIANCE_CONNECT_RETRY_COUNT

Explanation

This message is issued during product initialization to display the value set (*nnnnn*) specified for the APPLIANCE_CONNECT_RETRY_COUNT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1049E INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_CONNECT_RETRY_COUNT=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_CONNECT_RETRY_COUNT option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1050E UNABLE TO ESTABLISH *NNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*

Explanation

During started task initialization or as a result of the ENABLE SMFEXIT1 operator command, an error was encountered attempting to establish the SMF exit named *NNNNNNNNNNNNNNN*. The return code encountered is specified by *RRRRRRRR* and the reason code is specified by *SSSSSSSS*.

This message might be caused by having more than one agent active on a single z/OS image. Only one agent per z/OS image is required.

User response

Verify that no more than one agent is active per z/OS image. If that does not resolve the error, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1052E UNABLE TO DELETE *NNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*

Explanation

During started task termination or as a result of the DISABLE SMFEXIT1 operator command, an error was encountered attempting to delete the SMF exit named *NNNNNNNNNNNNNNN*. The return code encountered is specified by *RRRRRRRR* and the reason code is specified by *SSSSSSSS*.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1054E GSSB IS NOT PRESENT

Explanation

During activation of a policy RULEDEFS member, a necessary Security Guardium® S-TAP® for Data Sets control block could not be located.

User response

Ensure that the Security Guardium S-TAP for Data Sets started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1055E GSSB CONTROL BLOCK ID IS INVALID

Explanation

During activation of a policy RULEDEFS member, a necessary Security Guardium® S-TAP® for Data Sets control block was located but it is not valid.

User response

Ensure that the Security Guardium S-TAP for Data Sets started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1056I PROCESSING OPTION SET – APPLIANCE_NETWORK_REQUEST_TIMEOUT=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) that is specified for the APPLIANCE_NETWORK_REQUEST_TIMEOUT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1058E UNABLE TO LOCATE LPDE FOR IGC0005E

Explanation

During product initialization, a required pointer to an operating system module could not be located.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1058I PROCESSING OPTION SET – APPLIANCE_SERVER=*a**

Explanation

This message is issued during product initialization to display the value (*a**) specified for the APPLIANCE_SERVER keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1059E INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER=*a**

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_SERVER option. The value *a** indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1060I PROCESSING OPTION SET – AUDIT=*a**

Explanation

This message is issued during product initialization to display the value (*a**) specified for the AUDIT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1061E VALUE SPECIFIED FOR OPTION – AUDIT=*a**

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the AUDIT option. The value *a** indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1062I PROCESSING OPTION SET – CICS_SUPPORT=*nnnnnnn*

Explanation

This message is issued during product initialization to display the value *nnnnnnn* that was specified for the CICS_SUPPORT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1063E INVALID VALUE SPECIFIED FOR OPTION – CICS_SUPPORT=*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the CICS_SUPPORT option. The value *nnnnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.

Parent topic: Error message code descriptions

AUV1064W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022 or 16023. If APPLIANCE_PORT is specified with a value other than 16022 or 16023, message AUV1064W is issued and port 16022 is used instead.

User response

Change the APPLIANCE_PORT parameter setting to one of the supported values, or remove the parameter.
Parent topic: Error message code descriptions

AUV1065E UNABLE TO LOCATE LPDE FOR IDA0192A

Explanation

During Record level monitoring initialization, a required pointer to an operating system module could not be located.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1066E UNABLE TO LOCATE IDA0192A

Explanation

During Record level monitoring initialization, a required operating system module could not be located.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1067E PAGE SERVICE LIST EXHAUSTED FOR *xx* INTERCEPT

Explanation

During Record level monitoring initialization, an unexpected internal error occurred during an attempt to establish a product intercept. The intercept, identified by *xx*, is “O1” for open-intercept one, or “C1” for close-intercept one.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1068E UNABLE TO OBTAIN STORAGE FOR *xx* INTERCEPT, RC=*rrrrrrrr*

Explanation

During Record level monitoring initialization, an error specified as *rrrrrrrr* was encountered during an attempt to obtain common storage for a product control block. The intercept, identified by *xx*, is “O1” for open-intercept one, or “C1” for close-intercept one.

User response

Investigate a potential shortage of common storage and restart the product. If the problem continues, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1069E UNABLE TO LOCATE IDA0200T

Explanation

During Record level monitoring initialization, a required operating system module could not be located.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1070I TCP/IP STREAMING DISABLED DUE TO USER SETTING

Explanation

This message indicates that the STAP_STREAM_EVENTS parameter is set to a value of `N`.

System action

The agent address space will not send data to the server. This feature is also referred to as Simulation Mode. The agent address space will perform all processing necessary to collect data consistent with the active policy.

User response

No action is required. To instruct the agent to stream data to the server, change the STAP_STREAM_EVENTS parameter value to *Y*.
Parent topic: Error message code descriptions

AUV1073W MAXIMUM ACTIVE SUBSYSTEMS EXCEEDED (1)

Explanation

The current iteration of the product being started would exceed the limit of one concurrently active subsystems on a single z/OS® system. Startup for the current iteration is terminated.

User response

If the current iteration of the product is needed, shut down one of the already active subsystems and then restart the current iteration. To display all currently active subsystems use the "`display,subsystems,all`" command.

Parent topic: Error message code descriptions

AUV1074E DUPLICATE SUBSYSTEM FOUND FOR SSID=*ssss*

Explanation

During product initialization, a duplicate product control block was encountered for the subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1077I PII DATA NOT BEING TRANSMITTED DUE TO USER SETTING

Explanation

This message indicates that the FORCE_LOG_LIMITED parameter is set to a value of `Y`.

System action

When FORCE_LOG_LIMITED is set to `Y`, the S-TAP agent address space does not collect or send Personally Identifiable Identification (PII) data to the Guardium server. Record Level Monitoring (RLM) and CICS data is considered PII; therefore, it is not collected when FORCE_LOG_LIMITED is set to `Y`.

User response

No action is required. To collect and stream PII data, change the FORCE_LOG_LIMITED parameter value to `N`.
Parent topic: Error message code descriptions

AUV1080E ERROR IN NAME/TOKEN DELETE PROCESSING, RC=*rrrrrrrr*

Explanation

During product initialization, an error occurred that required product termination. During termination, an attempt was made to delete the product's NAME/TOKEN, but the NAME/TOKEN DELETE service encountered an error. *rrrrrrrr* contains the value returned in register 15.

System action

Product termination continues.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1081E GETMAIN FAILED FOR JSPB VECTOR TABLE, RC=*rrrrrrrr*

Explanation

During product initialization, the specified error *rrrrrrrr* occurred while attempting to obtain common storage for a product control block.

User response

Investigate a potential shortage of above-the-line common storage and restart the product. If the problem continues, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1082W IEFU86 EXIT IS NOT DEFINED

Explanation

The Security Guardium® S-TAP® for Data Sets address space issues this message if it detects an inadequacy in the SMF exit definitions in z/OS V2.3 and later environments. During initialization, Security Guardium S-TAP for Data Sets verifies that the required SMF exit IEFU86 is defined to the system.

For z/OS V2.3 and later, IEFU86 must be defined in the SMFPRMxx system, at the system level of the PARMLIB member, or at the various subsystem levels for Security Guardium S-TAP for Data Sets to collect data set level auditing events.

User response

To audit data set level events, configure z/OS SMF to define the require SMF exits for the appropriate z/OS level. For more information, refer to Configuring the SMFPRMxx parameter library member.
Parent topic: Error message code descriptions

AUV1100E ACRONYM CHECK FAILED FOR GSSB

Explanation

An internal error occurred within the product during product initialization.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1101E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

Main task startup was unable to obtain enough above-the-line private storage to initialize.

User response

Increase the amount of above-the-line private storage. If the problem persists, contact IBM® Support.

Parent topic: Error message code descriptions

AUV1102E ERROR OCCURRED IN CROSS-MEMORY INITIALIZATION

Explanation

An internal error occurred during main task startup.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1103E ATTACH FOR AUVPING FAILED, RC=*rrrrrrrr -ssss*

Explanation

During initialization of the Security Guardium® S-TAP® for Data Sets started task, an error was encountered during the attach of the subtask named AUVPING for the subsystem *SSSS*. The return code encountered is specified by *RRRRRRRR*.

User response

Ensure that the STEPLIB for the started task contains all of the load modules included with Security Guardium S-TAP for Data Sets. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1105E ATTACH FOR AUVSSRP FAILED, RC=*rrrrrrrr -ssss*

Explanation

During initialization of the Security Guardium® S-TAP® for Data Sets started task, an error was encountered during the attach of the subtask named AUVSSRP for the subsystem *SSSS*. The return code encountered is specified by *RRRRRRRR*.

User response

Ensure that the STEPLIB for the started task contains all of the load modules Included with Security Guardium S-TAP for Data Sets. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1105I SUBSYSTEM IS ACTIVE AND ENABLED

Explanation

This message indicates that the main product task has successfully started and is now active.

User response

No action is required.

Parent topic: Error message code descriptions

AUV1106I SUBSYSTEM INITIALIZATION IS COMPLETE

Explanation

This message is issued when the main product task has successfully completed initialization processing.

User response

No action is required.

Parent topic: Error message code descriptions

AUV1107I PRODUCT TERMINATION HAS BEEN REQUESTED

Explanation

This message is issued when the main product task has initiated subsystem shutdown processing, either due to a command request or because of an unrecoverable error condition.

User response

No action is required if this is due to a command request. If this is due to an unrecoverable error, restart the subsystem address space. Contact IBM® Software Support if the problems persist.

Parent topic: Error message code descriptions

AUV1111E UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*

Explanation

Product subsystem initialization was unable to obtain a sufficient amount of storage to load a required module.

User response

Check and increase the amount available above- and below-the-line storage and restart the product. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1112E BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*

Explanation

During product subsystem initialization, a required load module was unable to be successfully located. The value *mmmmmmmm* identifies the load module and the value *rrrrrrr* specifies the internal return code in error.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product.
Parent topic: Error message code descriptions

AUV1113E UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*

Explanation

An error was encountered during product subsystem initialization while processing the product load module *mmmmmmmm*.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product
Parent topic: Error message code descriptions

AUV1115E INITIAL LOAD FAILED FOR *mmmmmmmm*

Explanation

During product subsystem initialization, a required load module (*mmmmmmmm*) did not load successfully.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line private storage available for the product started task. After correcting the problem restart the product. If the error cannot be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1116E DIRECTED LOAD FAILED FOR *mmmmmmmm*

Explanation

During product subsystem initialization, a required load module (*mmmmmmmm*) did not load successfully.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product.
Parent topic: Error message code descriptions

AUV1117E NON-ZERO RETURN CODE FROM SYSEVENT, RC=*rrrrrrrr -ssss*

Explanation

During product subsystem initialization, an error (*rrrrrrrr*) was encountered when attempting to make the product started task address space non-swappable for subsystem *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1122E INVALID COMMAND SPECIFIED - *cccccccc -ssss*

Explanation

The product subsystem command parser received an error while processing the command (*cccccccc*) issued to the started task for subsystem ID *ssss*.

User response

Correct and re-issue the command.
Parent topic: Error message code descriptions

AUV1123E INVALID COMMAND SPECIFIED - *cccccccc -ssss*

Explanation

An invalid or null product subsystem command (*cccccccc*) was issued to the started task for subsystem ID *ssss*.

User response

Correct and re-issue the command.
Parent topic: Error message code descriptions

AUV1123W ACTIVE SUBSYSTEM DETECTED; PRODUCT-LEVEL MODULE NOT RE-INITIALIZED

Explanation

While a version of the product subsystem was active, an attempt was made to initiate the same product subsystem. The subsequent attempt to start the subsystem fails. Only one instance of the subsystem is allowed on a z/OS® image at a time.

User response

No action required. If you are attempting to initiate a new version of the subsystem, first shut down the currently executing version of the subsystem.
Parent topic: Error message code descriptions

AUV1124E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the DISPLAY command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1125E INSUFFICIENT OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

The command entered contains fewer operands than the minimum required. The command entered is *cccccccc*. The subsystem ID is *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1126E INVALID OPERAND SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

The command entered contains an invalid operand. The command entered is *cccccccc*. The subsystem ID is *ssss*.

User response

Correct the invalid operand and re-issue the command.
Parent topic: Error message code descriptions

AUV1127I SUBSYSTEM IS ACTIVE | INACTIVE AND ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY SUBSYSTEM or DISPLAY ALL operator command and shows the ACTIVE or INACTIVE status of the product subsystem and whether or not the subsystem is ENABLED or DISABLED for the subsystem *ssss*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1128E INVALID COMMAND SPECIFIED - *command*

Explanation

An unrecognized Security Guardium® S-TAP® for Data Sets operator command was issued to the started task where command is the unrecognized command.

User response

Issue a valid operator command to the started task.
Parent topic: Error message code descriptions

AUV1129I THERE ARE CURRENTLY NO SUBSYSTEMS -*ssss*

Explanation

This message is issued in response to the product operator command DISPLAY SUBSYSTEM ALL when no subsystems are located.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1130I SUBSYSTEM xxxx IS ACTIVE | INACTIVE AND ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY SUBSYSTEM ALL operator command issued to subsystem *ssss* and shows the ACTIVE or INACTIVE status of each product subsystem as identified by *xxxx* and whether or not the subsystem is ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1131I RULEDEFS ACTIVATED ON *mm/dd/yyyy* AT *hh:mm:ss* FROM MEMBER *mmmmmmmm -ssss*

Explanation

This message is issued in response to the DISPLAY RULEDEFS operator command to subsystem ID *ssss* and shows the date *mm/dd/yyyy* and time *hh:mm:ss* at which the active set of RULEDEFS was last activated as well as the member name (*mmmmmmmm*) from which they were activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1132I RULEDEFS NOT ACTIVATED -*ssss*

Explanation

This message is issued in response to the DISPLAY RULEDEFS operator command to subsystem ID *ssss* when no RULEDEFS were found to have been activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1136I PRODUCT-LEVEL TRACING IS ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY TRACING operator command to subsystem ID *ssss* and shows whether or not the product tracing facility is ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1137I SUBSYSTEM-LEVEL TRACING IS ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY TRACING operator command to subsystem ID *ssss* and shows whether or not the subsystem tracing facility is ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1138E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the ENABLE command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1140I SMF MONITORING SUCCESSFULLY ENABLED – *SSSS*

Explanation

The ENABLE SMFM command was processed for the specified subsystem *SSSS*. The required SMF monitoring exits have been loaded and enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1141I SUBSYSTEM IS NOW ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE SUBSYSTEM operator command and indicates that the subsystem *ssss* was successfully enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1142I TCP/IP STREAM SUCCESSFULLY ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE INTERCEPTS operator command for subsystem *ssss* were successfully enabled.

System action

The agent address space will send data to the server in a manner that is consistent with the active policy.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1143I SMF MONITORING SUCCESSFULLY DISABLED –*SSSS*

Explanation

The DISABLE SMFM command was processed for the specified subsystem *SSSS*. The required SMF monitoring exits have been disabled and unloaded.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1144I TRACING FOR PRODUCT IS NOW ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE TRACING or ENABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that product level tracing is now enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1145I TRACING FOR SUBSYSTEM IS NOW ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that subsystem level tracing is now enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1146E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the DISABLE command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1147I TCP/IP STREAM IS *EEEEEEEE -ssss*

Explanation

This message is issued in response to the operator command DISPLAY STREAM for subsystem *ssss*. The value *EEEEEEEE* indicates ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1149I SUBSYSTEM IS NOW DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE SUBSYSTEM operator command and indicates that the subsystem *ssss* was successfully disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1150I TCP/IP STREAM SUCCESSFULLY DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE STREAM operator command for subsystem *ssss*.

System action

The agent address space will not send data to the server. It will perform the steps that are necessary for data collection to be performed in a manner that is consistent with the active policy.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1151E SMF MONITORING DISABLE NOT SUCCESSFUL –*SSSS*

Explanation

The DISABLE SMFM command could not be processed for the specified subsystem *SSSS*. The SMF monitoring exits are still loaded and enabled.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1152I TRACING FOR PRODUCT IS NOW DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE TRACING or DISABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that product level tracing is now disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1153I TRACING FOR SUBSYSTEM IS NOW DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that subsystem level tracing is now disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1154E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the ACTIVATE command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1155E SMF MONITORING ENABLE FAILED –*SSSS*

Explanation

The ENABLE SMFM command failed to process for the specified *SSSS*. The SMF monitoring exits are not loaded or enabled.

User response

Ensure that the STEPLIB for the started task contains all of the load modules required for the product. If no error can be found, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1156E SMF MONITORING ALREADY ENABLED –*SSSS*

Explanation

The ENABLE SMFM command was issued for the specified subsystem *SSSS* but the SMFEXIT1 exits are already enabled. The SMF exits are still loaded and enabled.

User response

No response is required.
Parent topic: Error message code descriptions

AUV1157E OPERANDS SPECIFIED FOR COMMAND - *command*

Explanation

An operator command as identified by command was issued to the started task for subsystem *SSSS*, but more operands were specified than are permitted for the particular command.

User response

Correct and reissue the operator command.
Parent topic: Error message code descriptions

AUV1158E SMF MONITORING ALREADY DISABLED –*SSSS*

Explanation

The DISABLE SMFM command was issued for the specified subsystem *SSSS* but the SMF monitoring exits are already disabled.

User response

No response is required.
Parent topic: Error message code descriptions

AUV1175I *DDDDDDDD* MEMBER ACTIVATION SUCCESSFUL –*SSSS*

Explanation

A policy member as identified by DDDDDDDD for subsystem SSSS was successfully activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1176E *DDDDDDDD* MEMBER ACTIVATION FAILED – SEE JESYSMSG FOR DETAILS –*SSSS*

Explanation

A policy member as identified by *DDDDDDDD* for subsystem *SSSS* could not be successfully activated. The JESYSMSG output data set for the started task contains details of the error(s) encountered.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1176I *dddddddd* MEMBER *mmmmmmmm* ACTIVATION FAILED - SEE JESYSMSG FOR DETAILS -*ssss*

Explanation

This message is issued in response to the ACTIVATE RULEDEFS operator command or the initial RULEDEFS activation (as indicated from the OPTIONS member for subsystem ID *ssss*) to show that the activation of the RULEDEFS from member *mmmmmmmm* was not successful due to syntax errors.

User response

Review the error messages in the JES SYSMSG output for the product started task, and then correct the errors and re-activate the RULEDEFS.
Parent topic: Error message code descriptions

AUV1177I *dddddddd* MEMBER *mmmmmmmm* ACTIVATION FAILED - FAILURE CODE *cccc -ssss*

Explanation

This message is issued in response to the ACTIVATE RULEDEFS operator command, or the initial RULEDEFS activation (as indicated from the OPTIONS member for subsystem ID *ssss)* to show that the activation of the RULEDEFS from member *mmmmmmmm* was not successful due to an internal error as denoted by *cccc*.

User response

Review any error messages in the JES SYSMSG output or the console log for the product started task to determine the possible cause of the error, then correct the errors and re-activate the RULEDEFS. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1179E *DDDDDDDD* MEMBER ACTIVATION FAILED - FAILURE CODE *CCCCCCCC –SSSS*

Explanation

A policy member as identified by *DDDDDDDD* for subsystem *SSSS* could not be successfully activated. The failure code is identified by *CCCCCCCC*.

User response

Contact IBM® Technical Support.
Parent topic: Error message code descriptions

AUV1184E COMMAND VERB NOT UNIQUE - cccccccc -ssss

Explanation

More than one command exists that matches the abbreviation specified (*cccccccc*) for the command verb. The product subsystem processing the command was *ssss*.

User response

Re-issue the command, using a command verb abbreviation that more uniquely specifies the intended command.
Parent topic: Error message code descriptions

AUV1185E INVALID COMMAND SYNTAX SPECIFIED - *ssss*

Explanation

The command entered contains invalid syntax. The product subsystem processing the command was *ssss*.

User response

Review the command entered and correct the syntax.
Parent topic: Error message code descriptions

AUV1191E INVALID MODULE NAME SPECIFIED - *cccccccc*

Explanation

The command entered specifies an invalid module name. The command entered is *cccccccc*.

User response

Re-issue the command with a correct module name.
Parent topic: Error message code descriptions

AUV1192I MODULE *mmmmmmmm vvvv ffffffff dddddddd ttttt*

Explanation

Module header information is displayed, where *mmmmmmmm* is the name of the module, *vvvv* is the version, *ffffffff* is the FMID *dddddddd* is the assembly date and *ttttt* is the assembly time.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1193I MODULE *mmmmmmmm* LOCATED AT *aaaaaaaa* (*stgloc*)

Explanation

The module address (with offset if specified) is displayed, where *mmmmmmmm* is the name of the module, *aaaaaaaa* is the virtual storage address, and *stgloc* is the storage location ("PRIVATE" or "COMMON").

User response

No action is required.
Parent topic: Error message code descriptions

AUV1195E ERROR OCCURRED DURING FREEMAIN FOR GPB, RC=*rrrrrrrr*

Explanation

During initialization, the product encountered an error and determined that termination was necessary. As part of termination, an attempt was made to freemain the product control block, but the FREEMAIN service encountered an error. *rrrrrrrr* contains the value returned in register 15. Product termination continues.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1196E UNEXPECTED VCON COUNT FOR *xx* INTERCEPT; EXPECTED=*eee*, FOUND=*fff*

Explanation

While setting product intercept *xx*, An unexpected VCON count was encountered for a particular csect. The expected VCON count is *eee* and the actual VCON count is *fff*. This does not necessarily indicate a problem, but a problem is possible.

System action

An SVC memory dump is taken. Depending upon the particular intercept, product initialization might continue or terminate.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1200E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response

Increase the amount of above-the-line storage for the product task. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1202E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response

Increase the amount of above-the-line storage for the product task. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1203E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A product module was unable to obtain the required amount of above-the-line virtual storage.

User response

Increase the amount of above-the-line storage for the Security Guardium® S-TAP® for Data Sets started task and restart. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1204E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response

Increase the amount of above-the-line storage for the Security Guardium® S-TAP® for Data Sets started task. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1213E ERROR RETRIEVING SSRE

Explanation

An internal error was encountered.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1214E UNEXPECTED SSRE QUEUE ERROR

Explanation

An internal error was encountered.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1215E UNEXPECTED SSRE QUEUE ERROR

Explanation

An internal error was encountered.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1400I RECORD LEVEL MONITORING IS *EEEEEEEE -SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY RLM for subsystem *SSSS*. The value *EEEEEEEE* indicates *ENABLED* or *DISABLED*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1401I RECORD LEVEL MONITORING INTERCEPTS ARE *EEEEEEEE* -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY RLM for subsystem *SSSS*. The value *EEEEEEEE* indicates ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1402I CURRENT POLICY *EEE* -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY RLM for subsystem *SSSS*. The value *EEE* indicates either CONTAINS RLM FILTERS or DOES NOT CONTAIN RLM FILTERS.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1405I RECORD LEVEL MONITORING SUCCESSFULLY ENABLED -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command ENABLE RLM for subsystem *SSSS*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1406W RECORD LEVEL MONITORING SUCCESSFULLY ENABLED, BUT NO RLM FILTERS EXIST IN CURRENT POLICY -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command ENABLE RLM for subsystem *SSSS*. The enable action was successful, but no filters specifying record level monitoring processing exist in the currently activated policy.

System action

Record level monitoring will not be performed.

User response

To perform record level monitoring, add record level monitoring definitions to the policy and activate it.
Parent topic: Error message code descriptions

AUV1408W POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command ENABLE RLM for subsystem SSSS. The policy activation containing record level monitoring filters was successful, but record level monitoring processing is currently disabled.

System action

Record level monitoring will not be performed.

User response

To perform record level monitoring, issue the ENABLE RLM command for subsystem *SSSS*.
Parent topic: Error message code descriptions

AUV1410I PROCESSING OPTION SET - SOCKET_CONNECT_TIMEOUT=*nnnnn*

Explanation

This message is issued during product initialization to display the value (nnnnn) specified for the SOCKET_CONNECT_TIMEOUT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1411E INVALID VALUE SPECIFIED FOR OPTION - SOCKET_CONNECT_TIMEOUT=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SOCKET_CONNECT_TIMEOUT option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1412I PROCESSING OPTION SET - OUTAGE_SPILLAREA_SIZE=*nnnnnnn*

Explanation

This message is issued during product initialization to display the value (nnnnnnn) specified for the OUTAGE_SPILLAREA_SIZE keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1413E INVALID VALUE SPECIFIED FOR OPTION – OUTAGE_SPILLAREA_SIZE=*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the OUTAGE_SPILLAREA_SIZE option. The value *nnnnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1414I PROCESSING OPTION SET - INTERNAL_BUFFER_SIZE=*nnnnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnnnn*) specified for the INTERNAL_BUFFER_SIZE keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1415E INVALID VALUE SPECIFIED FOR OPTION INTERNAL_BUFFER_SIZE=*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the INTERNAL_BUFFER_SIZE option. The value *nnnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1416I PROCESSING OPTION SET - APPLIANCE_SERVER_FAILOVER=a*

Explanation

This message is issued during product initialization to display the value a* specified for the APPLIANCE_SERVER_FAILOVER keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1417E INVALID VALUE SPECIFIED FOR OPTION - *keyword*=a*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the keyword. The *keyword* value indicates APPLIANCE_SERVER_FAILOVER_*n*, or its alternate specification, APPLIANCE_SERVER_*n*, where *n* is 1, 2, 3, 4, or 5. The value *a** indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1418I PROCESSING OPTION SET - IAM_SMF_RECORD_ID = *nnn*

Explanation

This message is issued during product initialization to display the value *nnn* that is specified for the IAM_SMF_RECORD_ID keyword in the OPTIONS member. This keyword identifies the SMF record ID for the IAM records.

User response

For Security Guardium® S-TAP® for Data Sets to report IAM access, specify the value *nnn* in the control data set IAM_SMF_RECORD_ID option.
Parent topic: Error message code descriptions

AUV1419E INVALID VALUE SPECIFIED FOR OPTION - IAM_SMF_RECORD_ID = *nnn*

Explanation

While processing the subsystem options in the OPTIONS member during product initialization, an incorrect value was encountered for the IAM_SMF_RECORD_ID option. The value *nnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1420I PROCESSING OPTION SET - ACF_SMF_RECORD_ID = *nnn*

Explanation

This message is issued during product initialization to display the value specified for the ACF_SMF_RECORD_ID keyword in the OPTIONS member. This keyword identifies the SMF record ID for the ACF2 records.

User response

For Security Guardium® S-TAP® for Data Sets to report access failures to a unique record ID, specify the value *nnn* in the control data set ACF_SMF_RECORD_ID option.
Parent topic: Error message code descriptions

AUV1421E INVALID VALUE SPECIFIED FOR OPTION - ACF_SMF_RECORD_ID = *nnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the ACF_SMF_RECORD_ID option. The value nnn indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1422I PROCESSING OPTION SET - APPLIANCE_SERVER_LIST(*nnn*)

Explanation

This message is issued during product initialization to display the value specified for the APPLIANCE_SERVER_LIST keyword in the OPTIONS member. This value *nnn* identifies one of the following selected options:

FAILOVER
: One appliance connection is active at a time. If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The appliance attempts to reconnect to the primary server at intervals of 12 times the PING_RATE.

MULTI_STREAM
: An appliance connection is established for each server that is listed by the APPLIANCE_SERVER_n or APPLIANCE_SERVER_FAILOVER_n parameter. When a connection is lost, Security Guardium® S-TAP® for Data Sets audit events continue to be spread over the remaining appliance connections. Any lost connections are retried at regular intervals of 12 times the PING_RATE.

HOT_FAILOVER
: Keeps each connected Guardium appliance active via pings. If the primary Guardium appliance becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1423E INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER_LIST(*nnn*)

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_SERVER_LIST option. The value *nnn* indicates the incorrect value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1424I PROCESSING OPTION SET - MEGABUFFER_COUNT =*nnnnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnnnn*) that is specified for the MEGABUFFER_COUNT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1425E INVALID VALUE SPECIFIED FOR OPTION MEGABUFFER_COUNT =*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the MEGABUFFER_COUNT option. The value *nnnnnnn* indicates the incorrect value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1438I SMF MONITORING IS *EEEEEEEE -SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY SMFEXIT1 for subsystem *SSSS*. The value *EEEEEEEE* indicates *ENABLED* or *DISABLED*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1439I SMF MONITORING EXITS ARE *EEE -SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY SMFM for subsystem *SSSS*. The value *EEE* indicates ACTIVE/LOADED or NOT ACTIVE/LOADLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1450W SMF RECORDING TEST FAILED, RC=*cc*, TYPE=*nnnn*, SUBSYSTEM=*ssss*

Explanation

The Security Guardium® S-TAP® for Data Sets address space issues this message if it detects an inadequacy in the SMF environment. During initialization,Security Guardium S-TAP for Data Sets tests z/OS® MVS™ SMF to determine if SMF is collecting the record types that are necessary for data set level auditing. The S-TAP address space issues this message for each SMF record type *nnnn*, and z/OS MVS subsystem *ssss*, for which the test fails. RC *cc* identifies one of the following return codes:

16
: SMF is not active or has ended abnormally.

36
: Information for the specified record type is not being recorded.

User response

To audit data set level events, configure z/OS MVS SMF to collect the required SMF records. For more information, refer to Configuring the SMFPRMxx parameter library member.
Parent topic: Error message code descriptions

AUV1747E SUBSYSTEM IS NOT ACTIVE OR ENABLED

Explanation

This message is issued when, during the activation of a policy, the Security Guardium® S-TAP® for Data Sets subsystem is found to be disabled or inactive. The policy is not activated.

User response

Ensure that the Security Guardium S-TAP for Data Sets started task has been started and that the subsystem is enabled and the hooks are active. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1748W POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets policy pushdown operation for subsystem *SSSS*. The policy pushdown containing record level monitoring filters was successful, but record level monitoring processing is currently disabled.

System action

Record level monitoring will not be performed.

User response

To perform record level monitoring, issue the ENABLE RLM command for subsystem *SSSS*.
Parent topic: Error message code descriptions

AUV2000E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

During an attempt to intercept an OPEN/CLOSE event, Security Guardium® S-TAP® for Data Sets was unable to obtain enough virtual storage to perform processing.

User response

Increase the amount of virtual storage for the job. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2030E UNRECOGNIZED INTERCEPT ID ENCOUNTERED (*XX*)

Explanation

Security Guardium® S-TAP® for Data Sets received control with unexpected intercept parameters.

User response

This is an unexpected internal condition. If product maintenance was recently applied, ensure that all steps in the HOLDDATA were performed. If they were, record the ID *XX* and contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2040E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JCT, RC=*rrrrrrrr*

Explanation

During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* occurred while attempting to access a system control block.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2041E ERROR OCCURRED DURING SWAREQ PROCESSING FOR SCT, RC=*rrrrrrrr*

Explanation

During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* was encountered while attempting to access a system control block.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2042E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JMR, RC=*rrrrrrrr*

Explanation

During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* occurred while attempting to access a system control block.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2097I JCT UNAVAILABLE FOR JSPB LOOK-UP FOR ASID *xxxx*

Explanation

During interception of an OPEN or CLOSE event, Security Guardium® S-TAP® for Data Sets was unable to locate a product control block for the address space with the ASID *xxxx*.

System action

Processing is bypassed for the current job.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2098I ASID *xxxx* EXCEEDS GJVT MAX; ASVTMAXU=*xxxxxxxx*

Explanation

During interception of an OPEN or CLOSE event, Security Guardium® S-TAP® for Data Sets detected an unexpected error for the address space with the ASID *xxxx*. The system value for ASVTMAX *xxxxxxxx* is also displayed.

System action

Processing is bypassed for the current job.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2104E ERROR OCCURRED IN FREEMAIN OF AUVSMFX1, RC=*RRRRRRRR*

Explanation

During termination processing of the Security Guardium® S-TAP® for Data Sets started task or during the DISABLE of the SMFEXIT1 exits, the storage occupied by the module AUVSMFX1 could not be successfully freed. The error code encountered is specified by *RRRRRRRR*.

User response

No noticeable effect on system operations should be noticed as, although the module is located in Extended CSA, it consumes only a few kilobytes of storage. However, the cause of the error should be investigated by contacting IBM® Software Support.
Parent topic: Error message code descriptions

AUV2170I ATTEMPTING TO CONNECT TO THE GUARDIUM APPLIANCE

Explanation

This is an informational message issued during product initialization indicating initialization progress.

User response

None required.
Parent topic: Error message code descriptions

AUV2171I CALL TO GUARDIUM APPLIANCE SUCCESSFUL

Explanation

This is an informational message issued during product initialization indicating that the z/OS® host component of successfully connected to Guardium® system.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2172E *function* CALL TO GUARDIUM APPLIANCE FAILED

Explanation

An attempt to communicate with the Guardium® system failed. Before reporting the failure, the agent retried the request the number of times specified on the APPLIANCE_RETRY_INTERVAL parameter for the number of iterations specified on the APPLIANCE_CONNECT_RETRY_COUNT parameter. The *function* will be one of the following:

INIT
: Guardium system initialization, which occurs when the started task starts.

PING
: Cyclical pings to the system that report the agent's status.

SEND-SMF
: Agent transmission of the audit records to the Guardium system.

If any one of these service requests fail, the agent address space is terminated.

User response

Correct any communications issue causing this failure and restart the agent started task. Contact IBM® Software Support for further assistance.
Parent topic: Error message code descriptions

AUV2173E *function* CALL TO GUARDIUM APPLIANCE FAILED, RC = *rc* RC_STP= *rc* RS_STP= *rs* RC_GDM= *rc* RC_PB = *rc* RC_LST= *rc* RS_LST= *rs*

Explanation

An attempt to communicate with the Guardium® system failed. Before reporting the failure, the agent retried the request the number of times specified on the APPLIANCE_RETRY_INTERVAL parameter for the number of iterations specified on the APPLIANCE_CONNECT_RETRY_COUNT parameter. The function will be one of the following:

INIT
: Guardium system initialization, which occurs at started task initialization.

PING
: Cyclical pings to the system that reports the agent's status.

SEND-SMF
: Agent transmission of the audit records to the Guardium system. If any one of these service requests fail, the agent address space is terminated.

The *rc* and *rs* text is replaced with numeric values that can assist IBM® Support with problem diagnosis, if the problem persists.

User response

Correct any communications issue causing this failure and restart the agent started task. Contact IBM Support for further assistance.
Parent topic: Error message code descriptions

AUV2174E SPILL FILE FULL, DATA LOSS MIGHT OCCUR

Explanation

Connection to the Guardium® system has unexpectedly terminated and the spill file with SPILL_BUFFER size is now full. Data loss can occur if this condition continues.

User response

Ensure that the Guardium system is communicating. Increase the SPILL_BUFFER value to increase the amount of data that can be written to the spill file.
Parent topic: Error message code descriptions

AUV2175E CONNECTION LOST WITH NO SPILL FILE, DATA LOSS MIGHT OCCUR

Explanation

The connection to the Guardium® system has unexpectedly terminated. SPILL_BUFFER was not specified in the configuration member.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be re-established. To minimize data loss, specify a SPILL_BUFFER.
Parent topic: Error message code descriptions

AUV2176E UNABLE TO OBTAIN STORAGE, DATA LOSS MIGHT OCCUR

Explanation

An attempt to allocate storage for additional data failed.

User response

Ensure that a sufficient region size is provided in the started task JCL.
Parent topic: Error message code descriptions

AUV2177E RULEDEF NOT ACTIVATED - CHECK SYSPRINT FOR REASON

Explanation

An attempt to process a policy pushdown failed. No RULEDEF was activated as a result.

User response

Check the SYSPRINT for the detailed reason on what caused the failure. Correct the issue, and reissue a policy pushdown.
Parent topic: Error message code descriptions

AUV2178I SPILL FILE IS *xx*% FULL

Explanation

This message is issued while the spill file is in use. It indicates that the spill file has been filled to the percentage indicated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2179E UNABLE TO OBTAIN REQUESTED STORAGE FOR INTERNAL_BUFFER_SIZE: dddd. PROCESSING CONTINUES.

Explanation

An attempt to allocate storage for the internal buffer has failed. The started task remains up, but data processing does not run as efficiently.

User response

Ensure that a sufficient region size is provided in the started task JCL, or decrease the amount specified for INTERNAL_BUFFER_SIZE in the OPTIONS member. If the problem persists, contact IBM Software Support.
Parent topic: Error message code descriptions

AUV2180W WRITING TO SPILL FILE

Explanation

The connection to the Guardium system has been lost. All data is now being written to a spill file. The data in the spill file will be written to the Guardium system when the connection is restored.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be re-established.
Parent topic: Error message code descriptions

AUV2181I NO LONGER WRITING TO SPILL FILE

Explanation

The connection to the Guardium system has been restored, and the agent is no longer writing to the spill file.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2182I CONNECTION ESTABLISHED TO *x*

Explanation

An attempt to connect to the Guardium system was successful, where *x* is the system with which a connection has been made.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2183W STORAGE SHORTAGE DETECTED; ONE OR MORE EVENTS NOT RECORDED

Explanation

An attempt to allocate virtual storage for an internal product control block failed. Without the control block, the data for the event cannot be captured.

User response

Ensure that a sufficient region size is provided in the started task JCL. A region size of at least 96M is recommended when a large number of events are being monitored.

If the problem persists, evaluate the amount of data that is being captured as defined by the policy. Monitoring a very large number of events can cause storage shortages, especially when Record Level Monitoring (RLM) is being used.

Parent topic: Error message code descriptions

AUV2184W STORAGE SHORTAGE RELIEVED; EVENT RECORDING RESUMED. EVENTS LOST=????????

Explanation

A previous virtual storage shortage was resolved, allowing event recording to be resumed. EVENTS LOST=*????????* indicates the number of events that could not be recorded.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2185I UNEXPECTED PRODUCT STATE DETECTED. ATTEMPTING RESTART.

Explanation

Indicators in product control blocks conflict with the current product state. This could be caused by a non-standard product shutdown or an unexpected product termination. The product will attempt to correct the environment and continue to re-initialize.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2186E UNABLE TO RESOLVE HOST NAME *a**

Explanation

During product initialization, one of the host names (*a**) specified for the APPLIANCE_SERVER or APPLIANCE_SERVER_n option could not be resolved to a valid IP address.

User response

Ensure that all the host names specified in the OPTIONS member are correct and can be resolved to IP addresses. Correct the configuration if needed and restart.
Parent topic: Error message code descriptions

AUV2900E INVALID STORAGE REQUEST FOR CONTROL BLOCK *nnnn -ssss*

Explanation

An internal error occurred while attempting to obtain a control block identified by *nnnn* subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2901E INSUFFICIENT VIRTUAL STORAGE FOR CONTROL BLOCK *nnnn -ssss*

Explanation

Sufficient storage was not available to obtain a required control block identified by *nnnn* subsystem ID *ssss*.

User response

Attempt to increase above-the-line or below-the-line storage for the job receiving the error message. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2902E ACRONYM CHECK FAILED WHILE ATTEMPTING TO FREE *nnnn*, DATA=*dddd -ssss*

Explanation

An internal error occurred while attempting to free a control block identified by *nnnn* with the invalid data identified by *dddd* for subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2903E FAILURE OCCURRED DURING FREEMAIN FOR *nnnn -ssss*

Explanation

An internal error occurred while attempting to free a control block identified by *nnnn* subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV3000E ERROR ENABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered attempting to enable the XFCFROUT Global User Exit program AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3001E ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered regarding an attempt to obtain the address of the Global Work area. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3003E ERROR STARTING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered regarding an attempt to start the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3004I AUVPLTPI XFCFROUT GLOBAL USER EXIT SUCCESSFULLY ENABLED AND STARTED

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, the XFCFROUT Global User Exit AUVFROUT was successfully enabled and started.

User response

No action is required.
Parent topic: Error message code descriptions

AUV3005E ERROR STOPPING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to stop the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3006E ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to obtain the address of the Global Work area. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation that is provided in the CICS Transaction Server System Programming Reference manual, Appendix B. EXEC interface block (EIB) response and function codes. Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3008E ERROR DISABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*

Explanation

While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to disable the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3009I AUVPLTPS XFCFROUT GLOBAL USER EXIT SUCCESSFULLY STOPPED AND DISABLED

Explanation

While running the Program List Table Program Termination module AUVPLTPS, the XFCFROUT Global User Exit AUVFROUT was successfully stopped and disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV3010W CICS PLTPI INSTALLED BUT CICS_SUPPORT NOT SPECIFIED IN OPTIONS

Explanation

The CICS Support Program List Table Program Initialization program AUVPLTPI was defined to CICS, but the CICS_SUPPORT parameter was not enabled in the OPTIONS start-up parameters for the Security Guardium® S-TAP® for Data Sets started task.

User response

To use full CICS support within the product, you must specify CICS_SUPPORT=ENABLE in the OPTIONS parameters defined to the started task. Make the necessary changes to the OPTIONS parameters and restart the product.
Parent topic: Error message code descriptions