IBM Security QRadar

DSM 構成ガイド

2016 年 12 月

注記

本書および本書で紹介する製品を使用する前に、 1159 ページの『特記事項』に記載されている情報をお読みください。

本書は、本書の更新版に置き換えられない限り、IBM Security QRadar Security Intelligence Platform V7.2.5 および以降のリリースに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

本書は下記原典を翻訳したものです。

原典： IBM Security QRadar
DSM Configuration Guide
December 2016

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

この「DSM 構成ガイド」について

「DSM 構成ガイド」では、サード・パーティー・デバイス (ログ・ソースとも呼びます) からデータを収集する方法について説明します。

ネットワーク上のログ・ソースからイベント・ログを受け入れるように IBM® Security QRadar® を構成することができます。ログ・ソース とは、イベント・ログを作成するデータ・ソースのことです。

対象読者

システム管理者は、QRadar のアクセス権限を保有し、かつ企業ネットワーク・セキュリティーの概念とデバイスの構成を理解している必要があります。

技術資料

IBM Security QRadar の製品資料 (すべての翻訳資料を含む) を Web 上で探すには、IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリー内のより技術的な資料にアクセスする方法については、Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) を参照してください。

お客様サポートへのお問い合わせ

お客様サポートへのお問い合わせについては、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業内および企業外からの不適切なアクセスの防止、検出、およびそれらのアクセスへの対応により、システムおよび情報を保護する必要があります。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、あるいはご使用のシステムの損傷または他のシステムへの攻撃のための利用を含む悪用につながる可能性があります。 完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法かつ包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

注意**:**

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポリシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

第 1 部 QRadar DSM のインストールとログ・ソースの管理

第 1 章 サード・パーティー・デバイスからのイベント収集

サード・パーティー・デバイスからのイベント収集を構成するには、サード・パーティー・デバイスと、QRadar コンソール、イベント・コレクターまたはイベント・プロセッサー上で構成タスクを完了する必要があります。サード・パーティー・デバイスからイベントを収集するために連携するキー・コンポーネントは、ログ・ソース、DSM、および自動更新です。

ログ・ソース

ログ・ソース は、イベントを IBM Security QRadar システムに送信するように構成されているか、または QRadar システムによってイベントが収集されるように構成されている、任意の外部デバイス、外部システム、またはクラウド・サービスです。QRadar は、ログ・ソースからのイベントを「ログ・アクティビティー」タブに表示します。

ログ・ソースからロー・イベントを受信するために、QRadar では複数のプロトコルをサポートしています。これらのプロトコルには、OS、アプリケーション、ファイアウォール、および IPS/IDS からの Syslog、SNMP、SOAP、データベース表およびビューからのデータ用の JDBC があります。QRadar では、Checkpoint の OPSEC/LEA など、ベンダー独自の固有プロトコルもサポートしています。

DSM

デバイス・サポート・モジュール *(DSM)* は、複数のログ・ソースから受信したイベントを解析し、出力として表示できる標準の分類形式にそれらを変換する構成ファイルです。ログ・ソースのタイプごとに、対応する DSM があります。例えば、IBM Fiberlink MaaS360 DSM は、IBM Fiberlink MaaS360 ログ・ソースからのイベントを解析して正規化します。

自動更新

QRadar は、繰り返しスケジュールで、日次および週次の自動更新を行います。週次の自動更新には、新規 DSM リリース、解析問題の修正、およびプロトコル更新が含まれます。自動更新について詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。

サード・パーティー・デバイスのインストール・プロセス

サード・パーティー・デバイスからイベントを収集するには、ログ・ソースとなるデバイスと QRadar システムの両方で、インストールおよび構成ステップを完了する必要があります。一部のサード・パーティー・デバイスには、そのデバイスと QRadar の間の通信を有効にするための証明書を構成するなど、追加の構成ステップが必要になります。

以下のステップは、典型的なインストール・プロセスです。

1. デバイスを統合する方法について、サード・パーティー・デバイスに固有の説明を読みます。

2. サード・パーティー・デバイスの RPM をダウンロードしてインストールします。RPM は、IBM サポート Web サイト (http://www.ibm.com/support/) からダウンロードすることができます。

   ヒント: QRadar システムが自動更新を許可するように構成されている場合、このステップは必要でない場合があります。

3. イベントを QRadarに送信するようサード・パーティー・デバイスを構成します。

   いくつかのイベントを受信した後、QRadar は自動的にサード・パーティー・デバイスを検出し、ログ・ソース構成を作成します。ログ・ソースは、「ログ・ソース」リストにリストされます。ログ・ソースにはデフォルトの情報が含まれています。この情報は、カスタマイズすることができます。

4. QRadar がログ・ソースを自動的に検出しない場合は、手動でログ・ソースを追加します。サポートされている DSM のリストおよびデバイス固有のトピックに、自動的に検出されないサード・パーティー・デバイスが示されています。
5. 構成の変更をデプロイして、Web サービスを再始動します。

サポートされないサード・パーティー・ログ・ソースのユニバーサル DSM

イベントが収集された後、デバイスからの個々のイベントが適切に正規化されるまでは、相関を開始できません。正規化 とは、情報を共通フィールド名 (イベント名、IP アドレス、プロトコル、ポートなど) にマップすることを意味します。エンタープライズ・ネットワークに、QRadar で対応する DSM を提供していないネットワーク・デバイスまたはセキュリティー・デバイスが 1 つ以上ある場合は、ユニバーサル DSM を使用できます。QRadar は、ユニバーサル *DSM* を使用することで、ほとんどのデバイスおよび一般的なあらゆるプロトコル・ソースを統合できます。

ユニバーサル DSM を構成するには、デバイス拡張を使用して、ユニバーサル DSM をデバイスに関連付ける必要があります。「管理」タブの「ログ・ソース」ウィンドウでデバイス拡張情報を定義する前に、ログ・ソース拡張の文書を作成する必要があります。

ユニバーサル DSM について詳しくは、IBM サポート Web サイト (http://www.ibm.com/support) を参照してください。

DSM の追加

システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

制約事項: デバイス・サポート・モジュール (DSM) のアンインストールは、QRadar でサポートされていません。

始める前に

注: インストールするための `rpm -Uvh <rpm_filename>` コマンド・ラインは、`yum -y install <rpm_filename>` コマンドで置換されました。

手順

1. DSM RPM ファイルを IBM サポート Web サイト (http://www.ibm.com/support) からダウンロードします。
2. RPM ファイルを QRadar コンソールにコピーします。
3. SSH を使用して、root ユーザーとして QRadar ホストにログインします。
4. ダウンロードしたファイルが格納されているディレクトリーに移動します。
5. 以下のコマンドを入力します。

   ```
   yum -y install <rpm_filename>
   ```

6. QRadar ユーザー・インターフェースにログインします。
7. 「管理」タブで「変更のデプロイ」をクリックします。
8. 「管理」タブで、「拡張」 > 「**Web** サービスの再始動 **(Restart Web Services)**」を選択します。

関連概念:

83 ページの『第 5 章 3Com Switch 8800』
3Com Switch 8800 用の IBM Security QRadar DSM は、syslog を使用してイベントを受信します。

87 ページの『第 7 章 Akamai Kona』
Akamai KONA 用の IBM Security QRadar DSM は、Akamai KONA サーバーからイベント・ログを収集します。

ログ・ソースの追加

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

このタスクについて

以下の表は、すべてのログ・ソース・タイプに共通のログ・ソース・パラメーターを説明しています。

表 1. ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース ID	ログ・ソースを識別する IPv4 アドレスまたはホスト名。 ネットワークに、単一の管理コンソールに接続された複数のデバイスが含まれる場合、イベントを作成した個々のデバイスの IP アドレスを指定します。それぞれの固有 ID (IP アドレスなど) を指定することにより、イベント検索で管理コンソールがすべてのイベントのソースとして識別されることを回避します。
有効	このオプションが有効にされていない場合、ログ・ソースはイベントを収集しないため、ライセンス制限にカウントされません。

表 1. ログ・ソース・パラメーター (続き)

パラメーター	説明
信頼性	信頼性は、ログ・ソースによって作成されたイベントの整合性または有効性を表します。ログ・ソースに割り当てられている信頼性値は、着信イベントに基づいて増減されたり、ユーザーが作成したイベント規則に対応して調整されたりする場合があります。ログ・ソースからのイベントの信頼性は、オフェンスのマグニチュードの計算に反映され、オフェンスのマグニチュード値を増大または減少させる場合があります。
ターゲット・イベント・コレクター	リモート・ログ・ソースをポーリングする QRadar イベント・コレクターを指定します。 分散デプロイメントでは、コンソールのシステム・パフォーマンスを向上させるために、このパラメーターを使用してポーリング・タスクをイベント・コレクターに移動します。
イベントの統合	同じイベントが短い時間間隔内で複数回発生するとイベント数が増大します。統合されたイベントを使用することで、単一のイベント・タイプが発生する頻度を「ログ・アクティビティー」タブで表示し判別できます。 このチェック・ボックスがクリアされている場合、イベントは個別に表示され、イベントのバンドルは行われません。 自動的に検出された新規のログ・ソースは、「管理」タブの「システム設定」構成から、このチェック・ボックスの値を継承します。このチェック・ボックスを使用して、個々のログ・ソースに対するシステム設定のデフォルトの動作をオーバーライドできます。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. ログ・ソースの共通パラメーターを構成します。
5. ログ・ソースのプロトコル固有のパラメーターを構成します。
6. 「保存」をクリックします。
7. 「管理」タブで「変更のデプロイ」をクリックします。

関連概念:

83 ページの『第 5 章 3Com Switch 8800』

3Com Switch 8800 用の IBM Security QRadar DSM は、syslog を使用してイベ

ントを受信します。

87 ページの『第 7 章 Akamai Kona』
Akamai KONA 用の IBM Security QRadar DSM は、Akamai KONA サーバーからイベント・ログを収集します。

バルク・ログ・ソースの追加

一度に最大 500 個の Microsoft Windows またはユニバーサル DSM のログ・ソースを追加できます。複数のログ・ソースを同時に追加する場合は、QRadar でバルク・ログ・ソースを追加します。バルク・ログ・ソースは、共通の構成を共有する必要があります。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「一括アクション」リストから「一括追加」を選択します。
4. バルク・ログ・ソースのパラメーターを構成します。
   - ファイル・アップロード - 1 行に 1 つのホスト名または IP が含まれるテキスト・ファイルをアップロードします。
   - 手動 - 追加するホストのホスト名または IP を入力します。
5. 「保存」をクリックします。
6. 「続行」をクリックして、ログ・ソースを追加します。
7. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースの構文解析順序の追加

イベントがターゲット・イベント・コレクターで構文解析されるときの順序として、優先順位を割り当てることができます。

このタスクについて

共通の IP アドレスまたはホスト名を共有するログ・ソースに対して構文解析順序を定義することで、ログ・ソースの重要度を指定できます。ログ・ソースの構文解析順序を定義すると、ログ・ソース構成が変更されても、特定のログ・ソースが特定の順序で解析されるようになります。解析順序により、不要な解析が防止され、ログ・ソース構成に対する変更によってシステム・パフォーマンスが影響を受けることがなくなります。解析順序により、より重要なログ・ソースより先に低レベルのイベント・ソースが解析されることがなくなります。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソースの構文解析順序」アイコンをクリックします。
3. ログ・ソースを選択します。
4. オプション: 「選択されたイベント・コレクター」リストから、ログ・ソース構文解析順序を定義するイベント・コレクターを選択します。

5. オプション: 「ログ・ソースのホスト」リストから、ログ・ソースを選択します。
6. ログ・ソースの構文解析順序の優先順位を設定します。
7. 「保存」をクリックします。

第 2 部 ログ・ソース

第 2 章 ログ・ソース管理の概要

ネットワーク上のログ・ソースからイベント・ログを受け入れるように IBM Security QRadar を構成することができます。ログ・ソース とは、イベント・ログを作成するデータ・ソースのことです。

例えば、ファイアウォールや侵入防止システム (IPS) はセキュリティー・ベースのイベントをログに記録し、スイッチやルーターはネットワーク・ベースのイベントをログに記録します。

ログ・ソースからロー・イベントを受信するために、QRadar は多くのプロトコルをサポートしています。パッシブ・プロトコル は、特定のポートでイベントを listen します。アクティブ・プロトコル は、API などの通信手段を使用して、イベントのポーリングと取得を行う外部システムに接続します。

ライセンス制限に応じて、QRadar は、300 件を超えるログ・ソースからイベントを読み取って解釈することができます。

QRadar 用のログ・ソースを構成するには、以下のタスクを実行する必要があります。

1. ログ・ソースをサポートするデバイス・サポート・モジュール (DSM) をダウンロードしてインストールします。*DSM* は、元の形式のイベント・ログを識別して、QRadar が使用できる形式に構文解析するために必要なイベント・パターンを含むソフトウェア・アプリケーションです。
2. DSM の自動ディスカバリーがサポートされている場合は、QRadar が自動的にログ・ソースを構成済みのログ・ソースのリストに追加するまで待ちます。
3. DSM の自動ディスカバリーがサポートされていない場合は、手動でログ・ソース構成を作成します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

7 ページの『バルク・ログ・ソースの追加』
一度に最大 500 個の Microsoft Windows またはユニバーサル DSM のログ・ソースを追加できます。複数のログ・ソースを同時に追加する場合は、QRadar でバルク・ログ・ソースを追加します。バルク・ログ・ソースは、共通の構成を共有する必要があります。

7 ページの『ログ・ソースの構文解析順序の追加』
イベントがターゲット・イベント・コレクターで構文解析されるときの順序として、優先順位を割り当てることができます。

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

ログ・ソースの追加

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

このタスクについて

以下の表は、すべてのログ・ソース・タイプに共通のログ・ソース・パラメーターを説明しています。

表 2. ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース ID	ログ・ソースを識別する IPv4 アドレスまたはホスト名。 ネットワークに、単一の管理コンソールに接続された複数のデバイスが含まれる場合、イベントを作成した個々のデバイスの IP アドレスを指定します。それぞれの固有 ID (IP アドレスなど) を指定することにより、イベント検索で管理コンソールがすべてのイベントのソースとして識別されることを回避します。
有効	このオプションが有効にされていない場合、ログ・ソースはイベントを収集しないため、ライセンス制限にカウントされません。
信頼性	信頼性は、ログ・ソースによって作成されたイベントの整合性または有効性を表します。ログ・ソースに割り当てられている信頼性値は、着信イベントに基づいて増減されたり、ユーザーが作成したイベント規則に対応して調整されたりする場合があります。ログ・ソースからのイベントの信頼性は、オフェンスのマグニチュードの計算に反映され、オフェンスのマグニチュード値を増大または減少させる場合があります。
ターゲット・イベント・コレクター	リモート・ログ・ソースをポーリングする QRadar イベント・コレクターを指定します。 分散デプロイメントでは、コンソールのシステム・パフォーマンスを向上させるために、このパラメーターを使用してポーリング・タスクをイベント・コレクターに移動します。

表 2. ログ・ソース・パラメーター (続き)

パラメーター	説明
イベントの統合	同じイベントが短い時間間隔内で複数回発生するとイベント数が増大します。統合されたイベントを使用することで、単一のイベント・タイプが発生する頻度を「ログ・アクティビティー」タブで表示し判別できます。 このチェック・ボックスがクリアされている場合、イベントは個別に表示され、イベントのバンドルは行われません。 自動的に検出された新規のログ・ソースは、「管理」タブの「システム設定」構成から、このチェック・ボックスの値を継承します。このチェック・ボックスを使用して、個々のログ・ソースに対するシステム設定のデフォルトの動作をオーバーライドできます。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. ログ・ソースの共通パラメーターを構成します。
5. ログ・ソースのプロトコル固有のパラメーターを構成します。
6. 「保存」をクリックします。
7. 「管理」タブで「変更のデプロイ」をクリックします。

関連概念:

83 ページの『第 5 章 3Com Switch 8800』
3Com Switch 8800 用の IBM Security QRadar DSM は、syslog を使用してイベントを受信します。

87 ページの『第 7 章 Akamai Kona』
Akamai KONA 用の IBM Security QRadar DSM は、Akamai KONA サーバーからイベント・ログを収集します。

Blue Coat Web Security Service REST API プロトコルの構成オプション

Blue Coat Web Security Service からイベントを受信するには、Blue Coat Web Security Service REST API プロトコルを使用するようにログ・ソースを構成します。

Blue Coat Web Security Service REST API プロトコルは Blue Coat Web Security Service Sync API を照会して、クラウドから最新のログ・データを取得します。

Blue Coat Web Security Service REST API プロトコルのプロトコル固有のパラメーターを下の表で説明します。

表 3. *Blue Coat Web Security Service REST API* プロトコルのパラメーター

パラメーター	説明
API ユーザー名 (API Username)	Blue Coat Web Security Service での認証に使用される API ユーザー名。API ユーザー名は、Blue Coat Threat Pulse ポータルを使用して構成されます。
パスワード	Blue Coat Web Security Service での認証に使用されるパスワード。
パスワードの確認	「パスワード」フィールドの確認。
プロキシーの使用 (Use Proxy)	プロキシーを構成すると、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Blue Coat Web Security Service にアクセスします。 「プロキシー **IP** またはホスト名 **(Proxy IP or Hostname)**」、「プロキシー・ポート」、「プロキシー・ユーザー名」、および「プロキシー・パスワード」の各フィールドを構成します。プロキシーが認証を必要としない場合、「プロキシー・ユーザー名」フィールドと「プロキシー」「パスワード」フィールドはブランクのままでかまいません。
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	リストから「はい」を選択すると、QRadar は証明書をダウンロードし、ターゲット・サーバーを信頼して使用し始めます。
繰り返し (Recurrence)	ログがいつデータを収集するかを指定できます。フォーマットは、月/時刻/日を表す M/H/D です。デフォルトは 5 M です。
EPS スロットル	1 秒あたりの最大イベント数 (EPS) の上限。デフォルトは 5000 です。

Cisco Firepower eStreamer プロトコルの構成オプション

Cisco Firepower eStreamer プロトコルは、以前は Sourcefire Defense Center eStreamer プロトコルと呼ばれていました。

Cisco Firepower eStreamer (イベント・ストリーマー) サービスからイベントを受信するには、Cisco Firepower eStreamer プロトコルを使用するようにログ・ソースを構成します。

Cisco FireSIGHT Management Center DSM を構成すると、イベント・ファイルが QRadar にストリーミングされて処理されます。

Cisco Firepower eStreamer プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 4. *Cisco Firepower eStreamer* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Cisco Firepower eStreamer**
サーバー・ポート	Cisco Firepower eStreamer の場合に QRadar が使用するデフォルト・ポートは 8302 です。

表 4. *Cisco Firepower eStreamer* プロトコルのパラメーター (続き)

パラメーター	説明
鍵ストア・ファイル名	鍵ストアの秘密鍵と関連証明書のディレクトリー・パスおよびファイル名。デフォルトで、インポート・スクリプトが鍵ストア・ファイルを作成するディレクトリーは `/opt/qradar/conf/estreamer.keystore` です。
トラストストア・ファイル名	トラストストア・ファイルは、クライアントから信頼されている証明書を保持します。デフォルトで、インポート・スクリプトがトラストストア・ファイルを作成するディレクトリーは `/opt/qradar/conf/estreamer.truststore` です。
追加データの要求 (Request Extra Data)	Cisco Firepower eStreamer からの追加データを要求するには、このオプションを選択します。例えば、追加データには、イベントの元の IP アドレスなどがあります。
拡張要求の使用 (Use Extended Requests)	eStreamer ソースからイベントを取得する代替メソッドを使用するには、このオプションを選択します。 拡張要求は、Cisco Firepower eStreamer バージョン 5.0 以降でサポートされます。

Cisco NSEL プロトコルの構成オプション

Cisco Adaptive Security Appliance (ASA) からの NetFlow パケット・フローをモニターするには、Cisco Network Security Event Logging (NSEL) プロトコル・ソースを構成します。

Cisco NSEL を QRadar と統合するには、ログ・ソースを手動で作成して NetFlow イベントを受信する必要があります。QRadar が Cisco NSEL からの Syslog イベントに対してログソースを自動的にディスカバーおよび作成することはありません。

Cisco NSEL プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 5. *Cisco NSEL* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Cisco NSEL**
ログ・ソース ID	ネットワークの中で複数のデバイスが管理コンソールに接続する場合は、イベントを作成した個々のデバイスの IP アドレスを指定できます。それぞれの固有 ID (IP アドレスなど) を指定することにより、イベント検索で管理コンソールがすべてのイベントのソースとして識別されることを回避します。
コレクター・ポート	Cisco ASA が NSEL イベントの転送に使用する UDP ポート番号。QRadar は、QRadar QFlow Collector のフロー・データにポート 2055 を使用します。NetFlow 用に Cisco Adaptive Security Appliance の別の UDP ポートを割り当てる必要があります。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

EMC VMware プロトコルの構成オプション

仮想環境の VMWare Web サービスからイベント・データを受信するには、EMC VMWare プロトコルを使用するようにログ・ソースを構成します。

EMC VMware プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 *6. EMC VMware* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**EMC VMware**
ログ・ソース ID	このパラメーターの値は「**VMware の IP (VMware IP)**」パラメーターに一致している必要があります。
VMware の IP (VMware IP)	VMWare ESXi サーバーの IP アドレス (1.1.1.1 など)。VMware プロトコルは、イベント・データを要求する前に VMware ESXi サーバーの IP アドレスに HTTPS を付加します。

転送プロトコルの構成オプション

デプロイメント内の別のコンソールからイベントを受信するには、転送プロトコルを使用するようにログ・ソースを構成します。

通常、転送プロトコルは、イベントを別の QRadar コンソールに転送するために使用します。例えば、コンソール A でコンソール B がオフサイト・ターゲットとして構成されているとします。自動的にディスカバーされたログ・ソースからのデータはコンソール B に転送されます。コンソール A で手動で作成したログ・ソースも、転送プロトコルを使用してコンソール B にログ・ソースとして追加する必要があります。

IBM BigFix SOAP プロトコル構成オプション

IBM BigFix® アプライアンスからログ拡張イベント・フォーマット (LEEF) 形式のイベントを受信するには、IBM BigFix SOAP プロトコルを使用するログ・ソースを構成します。

このプロトコルは、IBM BigFix バージョン 8.2.x から 9.5.2 と、IBM BigFix 用の Web レポート・アプリケーションを必要とします。

IBM BigFix SOAP プロトコルは、HTTP または HTTPS によって 30 秒間隔でイベントを取得します。イベントを取得すると、IBM BigFix DSM がイベントを解析して分類します。

以下の表では、IBM BigFix SOAP プロトコル用のプロトコル固有のパラメーターについて説明します。

表 7. *IBM BigFix SOAP* プロトコル・パラメーター

パラメーター	説明
プロトコル構成	**IBM BigFix SOAP**
HTTPS の使用	HTTPS で接続するために証明書が必要な場合は、必要な証明書をディレクトリー `/opt/qradar/conf/trusted_certificates` にコピーしてください。ファイル拡張子が `.crt`、`.cert`、または `.der` である証明書がサポートされています。ログ・ソースを保存してデプロイする前に、証明書を信頼証明書ディレクトリーにコピーしてください。
SOAP ポート (SOAP Port)	デフォルトでは、ポート 80 が IBM BigFix と通信するためのポート番号です。ほとんどの構成で、HTTPS 通信にはポート 443 が使用されます。

JDBC プロトコルの構成オプション

QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

JDBC プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 8. *JDBC* プロトコル・パラメーター

パラメーター	説明
データベース・タイプ	イベントが含まれているデータベースのタイプを選択します。
データベース名	データベース名は、「ログ・ソース **ID**」フィールドで指定したデータベース名に一致している必要があります。
ポート	JDBC ポートは、リモート・データベースで構成されている listen ポートに一致している必要があります。データベースは、着信 TCP 接続を許可しなければなりません。MSDE データベース・タイプの場合に「データベース・インスタンス」を使用するとき、管理者は、ログ・ソース構成の「ポート」パラメーターを空白のままにしておく必要があります。
ユーザー名	データベースの QRadar 用ユーザー・アカウント。
パスワード	データベースへの接続に必要なパスワード。
パスワードの確認	データベースへの接続に必要なパスワード。
認証ドメイン (MSDE のみ)	Windows ドメインである MSDE データベースのドメイン。ネットワークがドメインを使用しない場合は、このフィールドを空白のままにしてください。
データベース・インスタンス (MSDE または Informix® のみ)	データベース・インスタンス (必要な場合)。MSDE データベースでは、単一のサーバーに複数の SQL サーバー・インスタンスを含めることができます。 標準以外のポートをデータベースに使用する場合、または SQL データベース解決のためのポート 1434 へのアクセスがブロックされる場合は、ログ・ソース構成の「データベース・インスタンス」パラメーターを空白にする必要があります。

表 8. JDBC プロトコル・パラメーター (続き)

パラメーター	説明
定義済み照会	オプション。ログ・ソースに対する定義済みのデータベース照会を選択します。ログ・ソース・タイプに対して定義済み照会を使用できない場合、管理者は「なし」を選択できます。
テーブル名	イベント・レコードを含む表またはビューの名前。表名に使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、エヌ・ダッシュ (-)、ピリオド (.) です。
選択リスト	表をポーリングしてイベントを照会するときに含めるフィールドのリスト。コンマ区切りのリストを使用できるほか、アスタリスク (*) を入力して、表またはビューにあるすべてのフィールドを選択することができます。コンマ区切りのリストを定義する場合は、「比較フィールド」で定義したフィールドをリストに含める必要があります。
比較フィールド	照会から次の照会までの間に表に追加された新しいイベントを識別する表またはビューにある、数値またはタイム・スタンプのフィールド。重複するイベントが作成されないように、このプロトコルが以前にポーリングしたイベントを識別できるようにします。
準備済みステートメントの使用 (Use Prepared Statements)	準備済みステートメントを使用すると、JDBC プロトコル・ソースで SQL ステートメントをセットアップし、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティー上およびパフォーマンス上の理由により、ほとんどの JDBC プロトコル構成で準備済みステートメントを使用することができます。
開始日時	オプション。データベースのポーリングの開始日時を yyyy-MM-dd HH:mm の形式で入力します。HH は 24 時間形式を使用して指定します。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
ポーリング間隔 (Polling Interval)	イベント・テーブルに対する照会から次の照会までの間の時間。デフォルトのポーリング間隔は 10 秒です。もっと長いポーリング間隔を定義するには、H (時間) または M (分) を数値に追加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を付加せずに数値を入力した場合は、秒単位のポーリングになります。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数。
名前付きパイプ通信の使用 (Use Named Pipe Communication) (MSDE のみ)	MSDE データベースを使用する場合は、「ユーザー名」フィールドおよび「パスワード」フィールドで、データベースのユーザー名とパスワードではなく、Windows 認証のユーザー名とパスワードを使用する必要があります。ログ・ソースの構成では、MSDE データベースのデフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 (Database Cluster Name) (MSDE のみ)	SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

表 8. JDBC プロトコル・パラメーター (続き)

パラメーター	説明
NTLMv2 の使用 (Use NTLMv2) (MSDE のみ)	NTLMv2 認証を必要とする SQL サーバーとの通信時に、MSDE 接続で NTLMv2 プロトコルを使用する場合は、このオプションを選択します。このオプションは、NTLMv2 認証を必要としない MSDE 接続の通信には干渉しません。 NTLMv2 認証を必要としない MSDE 接続の通信には干渉しません。
SSL の使用 (Use SSL) (MSDE のみ)	接続で SSL がサポートされている場合は、このオプションを選択します。このオプションが表示されるのは MSDE の場合のみです。
Oracle 暗号化の使用 (Use Oracle Encryption)	*Oracle* の暗号化とデータ整合性の設定 は、*Oracle Advanced Security* とも呼ばれます。 これを選択した場合、Oracle JDBC 接続では、サーバーが同様の Oracle データ暗号化設定をクライアントとしてサポートすることが必要になります。
データベース・ロケール (Database Locale) (Informix のみ)	多言語インストール済み環境の場合は、このフィールドを使用して、使用する言語を指定します。
コード・セット (Informix のみ)	多言語インストール済み環境の場合は、このフィールドを使用して、使用する文字セットを指定します。

関連情報:

Configuring JDBC Over SSL with a Self-signed Certificate

Configuring JDBC Over SSL with an Externally-signed Certificate

JDBC SiteProtector の構成オプション

Java™ Database Connectivity (JDBC) SiteProtector™ プロトコルを使用してリモート側から IBM Proventia® Management SiteProtector® データベースをポーリングしてイベントを照会するように、ログ・ソースを構成することができます。

JDBC - SiteProtector プロトコルは、ログ・ソース・ペイロードの作成時に SensorData1 表と SensorDataAVP1 表の情報を結合します。SensorData1 表と SensorDataAVP1 表は、IBM Proventia® Management SiteProtector® データベースに存在します。1 回の照会で JDBC - SiteProtector プロトコルがポーリングできる行の最大数は 30,000 行です。

JDBC - SiteProtector プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 9. *JDBC - SiteProtector* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**JDBC - SiteProtector**
データベース・タイプ	リストで、イベント・ソースに使用するデータベースのタイプとして「**MSDE**」を選択します。

表 9. *JDBC - SiteProtector* プロトコルのパラメーター (続き)

パラメーター	説明
データベース名	このプロトコルが接続できるデータベースの名前として `RealSecureDB` と入力します。
IP またはホスト名	データベース・サーバーの IP アドレスまたはホスト名。
ポート	データベース・サーバーが使用するポート番号。JDBC SiteProtector 構成のポートは、データベースのリスナー・ポートに一致する必要があります。データベースでは、着信 TCP 接続を有効にしておく必要があります。データベース・タイプが MSDE のときに「データベース・インスタンス **(Database Instance)**」を定義する場合は、ログ・ソース構成の「ポート」パラメーターを空白のままにする必要があります。
ユーザー名	JDBC プロトコルによるデータベースへのアクセスを追跡する場合は、ご使用の QRadar システムに特定のユーザーを作成できます。
認証ドメイン	MSDE を選択するときに、データベースが Windows 用に構成されている場合は、Windows ドメインを定義する必要があります。 ネットワークがドメインを使用しない場合は、このフィールドを空白のままにしてください。
データベース・インスタンス	MSDE を選択するときに、1 つのサーバーに複数の SQL サーバー・インスタンスがある場合は、接続先インスタンスを定義します。データベース構成で標準以外のポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスがブロックされる場合は、構成で「データベース・インスタンス」パラメーターを空白のままにしておく必要があります。
定義済み照会	ログ・ソースに対する定義済みのデータベース照会。定義済みのデータベース照会は、特別なログ・ソース接続の場合にのみ使用できます。
テーブル名	`SensorData1`
AVP ビュー名 (AVP View Name)	`SensorDataAVP`
応答ビュー名 (Response View Name)	`SensorDataResponse`
選択リスト	テーブルまたはビューのすべてのフィールドを含めるには、`*` を入力します。
比較フィールド	`SensorDataRowID`
準備済みステートメントの使用 (Use Prepared Statements)	準備済みステートメントを使用すると、JDBC プロトコル・ソースで SQL ステートメントをセットアップし、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由で、準備済みステートメントを使用するようにしてください。プリコンパイル・ステートメントを使用しない代替照会手法を使用する場合は、このチェック・ボックスをクリアできます。

表 9. *JDBC - SiteProtector* プロトコルのパラメーター (続き)

パラメーター	説明
監査イベントを含む	監査イベントを IBM SiteProtector® から収集する場合に指定します。
開始日時	オプション。プロトコルがデータベースのポーリングを開始できる開始日時。
ポーリング間隔 (Polling Interval)	イベント・テーブルに対する照会から次の照会までの間の時間。より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。指定子の H および M のない数値の場合は、秒単位のポーリングになります。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数。
データベース・ロケール (Database Locale)	多言語インストール済み環境の場合は、「データベース・ロケール **(Database Locale)**」フィールドを使用して、使用する言語を指定します。
データベースのコード・セット (Database Codeset)	多言語インストール済み環境の場合は、「コード・セット **(Codeset)**」フィールドを使用して、使用する文字セットを指定します。
名前付きパイプ通信の使用 (Use Named Pipe Communication)	データベース・タイプとして MSDE を選択した場合は、このチェック・ボックスを選択して、TCP/IP ポート接続の代替方式を使用します。名前付きパイプ接続を使用する場合は、ユーザー名とパスワードは、データベースのユーザー名とパスワードではなく、Windows 認証の適切なユーザー名とパスワードにする必要があります。ログ・ソースの構成ではデフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 (Database Cluster Name)	名前付きパイプ通信を正常に機能させるためのクラスター名。
NTLMv2 の使用	NTLMv2 認証を必要とする SQL サーバーの場合に、強制的に MSDE 接続で NTLMv2 プロトコルを使用します。「**NTLMv2** の使用」チェック・ボックスを選択しても、NTLMv2 認証を必要としない MSDE 接続の通信には干渉しません。
SSL の使用 (Use SSL)	JDBC プロトコルに対して SSL 暗号化を有効化します。
ログ・ソース言語	ログ・ソースによって生成されるイベントの言語を選択します。ログ・ソース言語により、複数の言語でイベントを作成できる外部のアプライアンスまたはオペレーティング・システムからのイベントをシステムが構文解析できるようになります。

Juniper Networks NSM プロトコルの構成オプション

Juniper Networks NSM および Juniper Networks Secure Service Gateway (SSG) ログ・イベントを受信するには、Juniper Networks NSM プロトコルを使用するようにログ・ソースを構成します。

Juniper Networks Network and Security Manager プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 10. *Juniper Networks NSM* プロトコルのパラメーター

パラメーター	説明
ログ・ソース・タイプ	**Juniper Networks Network and Security Manager**
プロトコル構成	**Juniper NSM**

Juniper Security Binary Log Collector プロトコルの構成オプション

Security Binary Log Collector プロトコルを使用するようにログ・ソースを構成することができます。このプロトコルを使用すると、Juniper アプライアンスが監査イベント、システム・イベント、ファイアウォール・イベント、および侵入防止システム (IPS) イベントをバイナリー形式で QRadar に送信できます。

Juniper SRX または J シリーズ・アプライアンスのバイナリー・ログ形式は、UDP プロトコルを使用してストリーミングされます。バイナリー形式のイベントをストリーミングするための固有のポートを指定する必要があります。標準の Syslog ポート 514 をバイナリー形式のイベントに使用することはできません。Juniper アプライアンスからのストリーミング・バイナリー・イベントの受信用として割り当てられるデフォルト・ポートはポート 40798 です。

Juniper Security Binary Log Collector プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 11. *Juniper Security Binary Log Collector* のプロトコル・パラメーター

パラメーター	説明
プロトコル構成	**Security Binary Log Collector**
XML テンプレート・ファイルのロケーション	Juniper SRX または Juniper J シリーズ・アプライアンスからのバイナリー・ストリームのデコードに使用する XML ファイルのパス。デフォルトでは、バイナリー・ストリームをデコードするための XML ファイルがデバイス・サポート・モジュール (DSM) に含まれています。 この XML ファイルはディレクトリー `/opt/qradar/conf/security_log.xml` にあります。

ログ・ファイル・プロトコルの構成オプション

リモート・ホストからイベントを受信するには、ログ・ファイル・プロトコルを使用するようにログ・ソースを構成します。

ログ・ファイル・プロトコルは、日常イベントのログを書き込むシステムを対象としています。イベント・ファイルに情報を追加するデバイスにログ・ファイル・プロトコルを使用するのは不適切です。

ログ・ファイルは一度に 1 つずつ取得されます。ログ・ファイル・プロトコルは、プレーン・テキスト、圧縮ファイル、またはファイル・アーカイブを管理できます。アーカイブには、一度に 1 行ずつ処理できるプレーン・テキスト・ファイルが含まれている必要があります。ログ・ファイル・プロトコルがイベント・ファイルをダウンロードすると、そのファイルで受信された情報によって「ログ・アクティ

ビティー」タブが更新されます。ダウンロードが完了した後にファイルに追加情報が書き込まれても、その追加情報は処理されません。

ログ・ファイル・プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 12. ログ・ファイル・プロトコルのパラメーター

パラメーター	説明
プロトコル構成	ログ・ファイル
リモート・ポート	リモート・ホストが標準以外のポート番号を使用する場合は、ポートの値を調整してイベントを取得する必要があります。
SSH 鍵ファイル	鍵認証を使用するようにシステムを構成した場合の、SSH 鍵のパス。SSH 鍵ファイルを使用する場合は、「リモート・パスワード」フィールドが無視されます。
リモート・ディレクトリー	FTP の場合に、ログ・ファイルがリモート・ユーザーのホーム・ディレクトリーにある場合は、リモート・ディレクトリーを空白のままにしておくことができます。リモート・ディレクトリーのフィールドを空白にすると、作業ディレクトリーの変更 (CWD) コマンドが制限されているシステムがサポートされます。
再帰的 (Recursive)	このチェック・ボックスを有効にすると、FTP 接続または SFTP 接続を使用して、リモート・ディレクトリーのサブフォルダーを再帰的に検索してイベント・データを取得できます。サブフォルダーから収集するデータは、「FTP ファイル・パターン」の正規表現に一致するかどうかで決まります。「**Recursive**」オプションは、SCP 接続では使用できません。
FTP ファイル・パターン	リモート・ホストからダウンロードするファイルを識別するために必要な正規表現。
FTP 転送モード	FTP 経由で ASCII 転送を行う場合は、「プロセッサー」フィールドで「NONE」を選択し、「イベント・ジェネレーター **(Event Generator)**」フィールドで「LINEBYLINE」を選択する必要があります。
繰り返し (Recurrence)	新しいイベント・ログ・ファイルがあるかどうかリモート・ディレクトリーをスキャンする頻度を決定する時間間隔。時間間隔には時間数 (H)、分数 (M)、または日数 (D) の値を含めることができます。例えば、繰り返しが 2H の場合は、リモート・ディレクトリーを 2 時間ごとにスキャンします。
保存時に実行	ログ・ソース構成を保存した後、直ちにログ・ファイルのインポートを開始します。このチェック・ボックスを選択すると、以前にダウンロードされて処理されたファイルのリストがクリアされます。初回のファイル・インポートの後、ログ・ファイル・プロトコルは、管理者によって定義された開始時刻および繰り返しスケジュールに従います。
EPS スロットル	このプロトコルの上限とする 1 秒当たりのイベント数 (EPS)。

表 12. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
ローカル・ディレクトリーの変更	「ターゲット・イベント・コレクター」でローカル・ディレクトリーを変更してイベント・ログを保管してから処理します。
ローカル・ディレクトリー (Local Directory)	「ターゲット・イベント・コレクター」のローカル・ディレクトリー。ログ・ファイル・プロトコルがイベントの取得を試行する前に、このディレクトリーが存在しなければなりません。
ファイルのエンコード (File Encoding)	ログ・ファイルのイベントで使用する文字エンコード。
フォルダー分離文字 (Folder Separator)	ご使用のオペレーティング・システムでフォルダーの区切りに使用する文字。ほとんどの構成で、「フォルダーの区切り文字 **(Folder Separator)**」フィールドのデフォルト値を使用できます。このフィールドは、別の文字を使用して個別のフォルダーを定義するオペレーティング・システムを対象としています。例えば、メインフレーム・システムの場合にフォルダーを区切るピリオドが該当します。

Microsoft DHCP プロトコルの構成オプション

Microsoft DHCP サーバーからイベントを受信するには、Microsoft DHCP プロトコルを使用するようにログ・ソースを構成します。

ログ・ファイル (管理共有 (C$) を含むフォルダー・パス) を読み取るには、管理共有 (C$) に対する NetBIOS 特権が必要です。ローカルまたはドメインの管理者は、管理共有にあるログ・ファイルにアクセスするための十分な特権を持っています。

ファイル・パスをサポートする Microsoft DHCP プロトコルのフィールドでは、管理者はドライブ名をパス情報付きで定義できます。例えば、管理共有の場合はフィールドに `c$/LogFiles/` ディレクトリーを指定でき、公開共有フォルダー・パスの場合は `LogFiles/` ディレクトリーを指定できますが、`c:/LogFiles` ディレクトリーを指定することはできません。

制約事項: Microsoft 認証プロトコル NTLMv2 は、Microsoft DHCP プロトコルではサポートされていません。

Microsoft DHCP プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 13. *Microsoft DHCP* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Microsoft DHCP**
ドメイン	オプション。
フォルダー・パス	DHCP ログ・ファイルのディレクトリー・パス。

表 13. *Microsoft DHCP* プロトコルのパラメーター (続き)

パラメーター	説明
ファイル・パターン	イベント・ログを識別する正規表現。ログ・ファイルには必ず 3 文字の省略形の曜日が入ります。以下のいずれかのファイル・パターンを使用してください。 • IPv4 ファイルのパターン: `DhcpSrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)¥.log` • IPv6 ファイルのパターン: `DhcpV6SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) ¥.log` • IPv4 と IPv6 が混在するファイルのパターン: `Dhcp.*SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) ¥.log`

Microsoft Exchange プロトコルの構成オプション

SMTP、OWA、Microsoft Exchange 2007 サーバーおよび 2010 サーバーからイベントを受信するには、サポート用の Microsoft Windows Exchange プロトコルを使用するようにログ・ソースを構成します。

ログ・ファイル (管理共有 (C$) を含むフォルダー・パス) を読み取るには、管理共有 (C$) に対する NetBIOS 特権が必要です。ローカルまたはドメインの管理者は、管理共有にあるログ・ファイルにアクセスするための十分な特権を持っています。

ファイル・パスをサポートする Microsoft Exchange プロトコルのフィールドでは、管理者はドライブ名をパス情報付きで定義できます。例えば、管理共有の場合はフィールドに `c$/LogFiles/` ディレクトリーを指定でき、公開共有フォルダー・パスの場合は `LogFiles/` ディレクトリーを指定できますが、`c:/LogFiles` ディレクトリーを指定することはできません。

重要**:** Microsoft Exchange プロトコルは、Microsoft Exchange 2003 および Microsoft 認証プロトコル NTLMv2 セッションをサポートしていません。

Microsoft Exchange プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 14. *Microsoft Exchange* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Microsoft Exchange**
ドメイン	オプション。
SMTP ログ・フォルダーのパス	このフォルダー・パスをクリアすると、SMTP イベント収集が無効になります。
OWA ログ・フォルダーのパス	このフォルダー・パスをクリアすると、OWA イベント収集が無効になります。
MSGTRK ログ・フォルダーのパス	メッセージ・トラッキングを使用できるのは、ハブ・トランスポート、メールボックス、またはエッジ・トランスポート・サーバーのロールが割り当てられている Microsoft Exchange 2007 サーバーまたは 2010 サーバーです。
ファイル・パターン	イベント・ログを識別する正規表現。デフォルトは `.*¥.(?:log|LOG)` です。

表 14. *Microsoft Exchange* プロトコルのパラメーター (続き)

パラメーター	説明
ファイル読み取りの強制 (Force File Read)	このチェック・ボックスをクリアした場合、QRadar が変更時刻またはファイル・サイズの変化を検出した場合にのみログ・ファイルが読み取られます。
スロットル・イベント数/秒	Exchange プロトコルが 1 秒当たり転送できるイベントの最大数。

Microsoft IIS プロトコルの構成オプション

Microsoft IIS プロトコルを使用するようにログ・ソースを構成することができます。このプロトコルは、Microsoft IIS Web サーバーに格納される W3C 形式ログ・ファイルの単一の収集ポイントをサポートします。

ログ・ファイル (管理共有 (C$) を含むフォルダー・パス) を読み取るには、管理共有 (C$) に対する NetBIOS 特権が必要です。ローカルまたはドメインの管理者は、管理共有にあるログ・ファイルにアクセスするための十分な特権を持っています。

ファイル・パスをサポートする Microsoft IIS プロトコルのフィールドでは、管理者はドライブ名をパス情報付きで定義できます。例えば、管理共有の場合はフィールドに `c$/LogFiles/` ディレクトリーを指定でき、公開共有フォルダー・パスの場合は `LogFiles/` ディレクトリーを指定できますが、`c:/LogFiles` ディレクトリーを指定することはできません。

制約事項: Microsoft 認証プロトコル NTLMv2 は、Microsoft IIS プロトコルではサポートされていません。

Microsoft IIS プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 15. *Microsoft IIS* のプロトコル・パラメーター

パラメーター	説明
プロトコル構成	**Microsoft IIS**
ファイル・パターン	イベント・ログを識別する正規表現。
スロットル・イベント数/秒	IIS プロトコルが 1 秒当たり転送できるイベントの最大数。

注: 拡張 IIS ログを使用する場合は、新規ログ定義を作成する必要があります。「ログ定義 (Log Definition)」ウィンドウの「選択されたフィールド **(Selected Fields)**」セクションで、以下のフィールドが選択されていることを確認します。

- 日付 UTC (Date-UTC)
- 時刻 UTC (Time-UTC)
- URI 語幹 (URI-Stem)
- URI 照会ストリング (URI-Querystring)
- コンテンツ・パス (ContentPath)
- Status
- サーバー名 (Server Name)

- リファラー (Referer)
- Win325 状況 (Win325Status)
- 送信バイト数 (Bytes Sent)

Microsoft Security Event Log プロトコルの構成オプション

Microsoft Security Event Log プロトコルを使用するようにログ・ソースを構成することができます。Microsoft Windows Management Instrumentation (WMI) を使用して、カスタマイズしたイベント・ログやエージェントレス Windows イベント・ログを収集することができます。

WMI API では、ファイアウォール構成が、ポート 135 のほか、DCOM に必要なすべての動的ポートで着信外部通信を受け入れる必要があります。以下では、Microsoft Security Event Log プロトコルを使用するログ・ソースの制約について説明します。

- システムでの 1 秒当たりのイベント数 (eps) が 50 を超える場合は、このプロトコルの処理能力を超える可能性があります。50 eps を超えるシステムの場合は、WinCollect を使用してください。
- QRadar をオールインワン・インストールした場合は、Microsoft Security Event Log プロトコルで最大 250 件のログ・ソースをサポートできます。
- 専用のイベント・コレクターは、Microsoft Security Event Log プロトコルを使用して最大 500 件のログ・ソースをサポートできます。

ネットワーク・リンクを経由してリモート・サーバーにアクセスする場合 (例えば、衛星回線や低速な WAN ネットワークなど、システムの往復遅延時間が長い場合) は、Microsoft Security Event Log プロトコルを推奨しません。往復の遅延を確認するには、サーバー ping 間の要求および応答時間を調べます。低速接続によって生じるネットワーク遅延は、これらのリモート・サーバーで使用可能な EPS スループットを低下させます。また、ビジー状態のサーバーやドメイン・コントローラーからのイベント収集が着信イベントに追随するためには、往復遅延時間が短くなければなりません。ネットワークの往復遅延時間を短縮できない場合は、WinCollect を使用して Windows イベントを処理することができます。

Microsoft Security Event Log は、Microsoft Windows Management Instrumentation (WMI) API を備えた以下のソフトウェア・バージョンをサポートしています。

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R3
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7

Microsoft Security Event Log プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 16. *Microsoft Security Event Log* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Windows** セキュリティー・イベント・ログ

MQ プロトコルの構成オプション

メッセージ・キュー (MQ) サービスからメッセージを受信するには、MQ プロトコルを使用するようにログ・ソースを構成します。プロトコル名は、IBM Security QRadar では **MQ JMS** と表示されます。

IBM MQ がサポートされます。

MQ プロトコルは複数のメッセージ・キューをモニターできます (ログ・ソースごとに最大 50 件)。

MQ プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 17. *MQ* プロトコルのパラメーター

パラメーター	説明
プロトコル名 (Protocol Name)	**MQ JMS**
IP またはホスト名	プライマリー・キュー・マネージャーの IP アドレスまたはホスト名。
ポート	プライマリー・キュー・マネージャーとの通信に使用するデフォルト・ポートは 1414 です。
スタンバイ IP またはホスト名 (Standby IP or Hostname)	スタンバイ・キュー・マネージャーの IP アドレスまたはホスト名。
スタンバイ・ポート (Standby Port)	スタンバイ・キュー・マネージャーとの通信に使用するポート。
キュー・マネージャー (Queue Manager)	キュー・マネージャーの名前。
チャネル (Channel)	キュー・マネージャーがメッセージを送信するチャネル。デフォルトのチャネルは `SYSTEM.DEF.SVRCONN` です。
キュー (Queue)	モニター対象のキュー、またはキューのリスト。キューのリストはコンマ区切りのリストで指定します。
ユーザー名	MQ サービスでの認証に使用するユーザー名。
パスワード	**オプション:** MQ サービスでの認証に使用するパスワード。
EPS スロットル	1 秒当たりの最大イベント数 (EPS) の上限。
着信メッセージのエンコード (Incoming Message Encoding)	着信メッセージによって使用される文字エンコード。

Okta REST API プロトコルの構成オプション

Okta からイベントを受信するには、Okta REST API プロトコルを使用するようにログ・ソースを構成します。

Okta REST API プロトコルは、Okta Events and Users API エンドポイントを照会して、組織内のユーザーによって実行されたアクションに関する情報を取得します。

Okta REST API プロトコルのプロトコル固有のパラメーターについて、以下の表で説明します。

表 18. Okta REST API プロトコルのパラメーター

パラメーター	説明
IP またはホスト名	oktaprise.okta.com
認証トークン	Okta コンソールによって生成され、すべての API トランザクションで使用する必要がある単一認証トークン。
プロキシーの使用 (Use Proxy)	プロキシーが構成されている場合は、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Okta にアクセスします。 「プロキシー **IP** またはホスト名 **(Proxy IP or Hostname)**」、「プロキシー・ポート」、「プロキシー・ユーザー名」、および「プロキシー・パスワード」の各フィールドを構成します。プロキシーが認証を必要としない場合、「プロキシー・ユーザー名」フィールドと「プロキシー・パスワード」フィールドはブランクのままでかまいません。
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	リストから「はい」を選択すると、QRadar は証明書をダウンロードし、ターゲット・サーバーを信頼して使用し始めます。
繰り返し (Recurrence)	ログ・ソースがいつデータを収集するかを指定できます。フォーマットは、月/時刻/日を表す M/H/D です。デフォルトは、1 M です。
EPS スロットル	1 秒あたりのイベント数の最大限度。

OPSEC/LEA プロトコルの構成オプション

ポート 18184 でイベントを受信するには、OPSEC/LEA プロトコルを使用するようにログ・ソースを構成します。

OPSEC/LEA プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 19. OPSEC/LEA プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**OPSEC/LEA**
サーバー・ポート	QRadar が OPSEC/LEA プロトコルを使用してポート 18184 で通信できることを確認する必要があります。
統計レポートの間隔	Syslog イベント数が `qradar.log` ファイルに記録される期間を秒数で入力します。

表 19. *OPSEC/LEA* プロトコルのパラメーター (続き)

パラメーター	説明
OPSEC アプリケーション・オブジェクトの SIC 属性 (SIC 名)	SIC (Secure Internal Communications) 名は、アプリケーションの識別名 (DN) です (例えば `CN=LEA,o=fwconsole..7psasx`)。
ログ・ソースの SIC 属性 (SIC エンティティー名)	サーバーの SIC 名 (例えば `cn=cp_mgmt,o=fwconsole..7psasx`)。
OPSEC アプリケーション	証明書要求を実行するアプリケーションの名前。

重要: アップグレード後にエラー・メッセージ「**SSL 証明書をプルできません (Unable to pull SSL certificate)**」を受信した場合は、以下の手順を実行します。

1. 「証明書の指定 **(Specify Certificate)**」チェック・ボックスをクリアします。
2. 「証明書パスワードのプル」のパスワードを再入力します。

Oracle データベース・リスナー・プロトコルの構成オプション

Oracle データベース・サーバーから生成されるログ・ファイルをリモート側で収集するには、Oracle データベース・リスナー・プロトコル・ソースを使用するようにログ・ソースを構成します。

ログ・ファイルを処理のためにモニターするように Oracle データベース・リスナー・プロトコルを構成する前に、Oracle データベースのログ・ファイルのディレクトリー・パスを取得する必要があります。

Oracle データベース・リスナー・プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 20. *Oracle* データベース・リスナー・プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Oracle** データベース・リスナー
ファイル・パターン	イベント・ログを識別する正規表現。

PCAP と Syslog を組み合わせたプロトコルの構成オプション

パケット・キャプチャー (PCAP) データを転送する Juniper Networks SRX シリーズ・アプライアンスからイベントを収集するには、PCAP と Syslog を組み合わせたプロトコルを使用するようにログ・ソースを構成します。

PCAP と Syslog を組み合わせたプロトコルを使用するログ・ソースを構成する前に、Juniper Networks SRX アプライアンスで構成されている発信 PCAP ポートを判別してください。PCAP データをポート 514 に転送することはできません。

注:

QRadar は、イベント・コレクターごとに 1 つの Juniper Networks SRX シリーズ・アプライアンスからの PCAP データのみの受信をサポートします。

PCAP と Syslog を組み合わせたプロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 21. *PCAP* と *Syslog* を組み合わせたプロトコルのパラメーター

パラメーター	説明
ログ・ソース名	ログ・ソースの固有名を入力します。
ログ・ソースの説明	オプション。ログ・ソースの説明を入力します。
ログ・ソース・タイプ	リストから、ログ・ソース・タイプを選択します。
プロトコル構成	リストから、「**PCAP** と **Syslog** の組み合わせ **(PCAP Syslog Combination)**」を選択します。
ログ・ソース ID	Juniper Networks SRX シリーズ・アプライアンスを識別するための IP アドレス、ホスト名、または名前を入力します。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
受信 PCAP ポート	Juniper Networks SRX シリーズ・アプライアンスで発信 PCAP ポートが編集されている場合は、ログ・ソースを編集して、着信 PCAP ポートを更新する必要があります。 着信 PCAP ポートの番号を編集するには、以下の手順を実行します。 1. PCAP データを受信するための新しいポート番号を入力します。 2. 「保存」をクリックします。 3. 「管理」タブで、「拡張」>「すべての構成のデプロイ」を選択します。 **重要:** 管理者が「すべての構成のデプロイ」をクリックすると、システムはすべてのサービスを再始動します。このため、デプロイが完了するまで、イベントとフローのデータ収集にギャップが生じます。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。 このチェック・ボックスがクリアされている場合、ログ・ソースはイベントを収集しないため、ライセンス制限にカウントされません。
信頼性	ログ・ソースの「信頼性」を選択します。範囲は 0 (最低) から 10 (最高) までです。デフォルトの信頼性は 5 です。 信頼性は、ログ・ソースによって作成されたイベントの整合性または有効性を表します。ログ・ソースに割り当てられている信頼性値は、着信イベントに基づいて増減されたり、ユーザーが作成したイベント・ルールに応じて調整されたりする場合があります。ログ・ソースからのイベントの信頼性は、オフェンスのマグニチュードの計算に反映され、オフェンスのマグニチュード値を増大または減少させる場合があります。
ターゲット・イベント・コレクター	ログ・ソースのターゲットを選択します。ログ・ソースがアクティブにリモート・ソースからイベントを収集する場合、このフィールドでイベントをポーリングするアプライアンスが定義されます。 管理者は、このオプションを使用して、コンソール・アプライアンスではなくターゲット・イベント・コレクターでイベントをポーリングして処理することができます。これにより、分散デプロイメントでのパフォーマンスを向上させることができます。

表 21. *PCAP* と *Syslog* を組み合わせたプロトコルのパラメーター (続き)

パラメーター	説明
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 イベントの統合では、同じイベントが短期間に複数回発生するとイベント数が増大します。管理者は、統合されたイベントを使用することで、単一のイベント・タイプが発生する頻度を「ログ・アクティビティー」タブで表示し判別できます。 このチェック・ボックスがクリアされている場合、イベントは個別に表示され、情報はバンドルされません。 自動的に検出された新規のログ・ソースは、「管理」タブの「システム設定」構成から、このチェック・ボックスの値を継承します。管理者はこのチェック・ボックスを使用して、個々のログ・ソースに対するシステム設定のデフォルトの動作をオーバーライドできます。
イベント・ペイロードの保管	ログ・ソースがイベントのペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 自動的に検出された新規のログ・ソースは、「管理」タブの「システム設定」構成から、このチェック・ボックスの値を継承します。管理者はこのチェック・ボックスを使用して、個々のログ・ソースに対するシステム設定のデフォルトの動作をオーバーライドできます。
ログ・ソース言語	ログ・ソースによって生成されるイベントの言語を選択します。 ログ・ソース言語により、複数の言語でイベントを作成できる外部のアプライアンスまたはオペレーティング・システムからのイベントをシステムが構文解析できるようになります。
ログ・ソース拡張	オプション。ログ・ソースに適用する拡張の名前を選択します。 このパラメーターは、ログ・ソース拡張がアップロードされてから使用できるようになります。ログ・ソース拡張とは、デバイス・サポート・モジュール (DSM) で定義されたイベント解析パターンをオーバーライドまたは修復できる、正規表現を含む XML ファイルです。
拡張の使用条件	リスト・ボックスから、ログ・ソース拡張の使用条件を選択します。以下のオプションがあります。 • 解析の機能拡張 - ログ・ソースのほとんどのフィールドが正しく解析される場合に、このオプションを選択します。 • 解析のオーバーライド - ログ・ソースでイベントを正しく解析できない場合に、このオプションを選択します。
グループ	ログ・ソースに対する 1 つ以上のグループを選択します。

SDEE プロトコルの構成オプション

Security Device Event Exchange (SDEE) プロトコルを使用するようにログ・ソースを構成することができます。QRadar はこのプロトコルを使用して、SDEE サーバーを使用するアプライアンスからイベントを収集します。

SDEE プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 22. *SDEE* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**SDEE**
URL	ログ・ソースにアクセスするために必要な HTTP または HTTPS の URL (例えば https://www.mysdeeserver.com/cgi-bin/sdee-server)。 SDEE/CIDEE (Cisco IDS v5.x 以降) の場合は、URL の末尾が `/cgi-bin/sdee-server` でなければなりません。RDEP (Cisco IDS v4.x) を持つ管理者の場合は、URL の末尾が `/cgi-bin/event-server` でなければなりません。
サブスクリプションの強制	このチェック・ボックスを選択すると、プロトコルによって強制的に、サーバーが最もアクティブでない接続をドロップし、新規 SDEE サブスクリプション接続をこのログ・ソース用に受け入れるようになります。
イベントに対するブロックを待機する最大時間	コレクション要求が実行されたが新しいイベントを取得できない場合、このプロトコルではイベント・ブロックが有効になります。ブロックされるため、新しいイベントがなかったリモート・デバイスに対して別のイベント要求を実行できなくなります。このタイムアウトは、システム・リソースを節約することを目的としています。

SMB Tail プロトコルの構成オプション

SMB Tail プロトコルを使用するようにログ・ソースを構成することができます。このプロトコルは、イベント・ログに改行が追加される場合に、リモート側の Samba 共有でのイベントを監視し、Samba 共有からイベントを受信するために使用します。

SMB Tail プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 23. *SMB Tail* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**SMB Tail**
ログ・フォルダー・パス	ログ・ファイルにアクセスするためのディレクトリー・パス。例えば、管理者が管理共有に `c$/LogFiles/` ディレクトリーを使用したり、公開共有フォルダー・パスに `LogFiles/` ディレクトリーを使用したりすることができます。しかし、`c:/LogFiles` ディレクトリーはログ・フォルダーのパスとしてサポートされていません。 ログ・フォルダーのパスに管理共有 (C$) が含まれている場合、その管理共有 (C$) に対する NetBIOS アクセス権を持つユーザーは、ログ・ファイルの読み取りに必要な特権を持っています。 ローカル・システム特権もドメイン管理者特権も、管理共有に存在するログ・ファイルにアクセスするために十分な権限を含んでいます。

表 23. *SMB Tail* プロトコルのパラメーター (続き)

パラメーター	説明
ファイル・パターン	イベント・ログを識別する正規表現。
ファイル読み取りの強制 (Force File Read)	このチェック・ボックスをクリアした場合、QRadar が変更時刻またはファイル・サイズの変化を検出した場合にのみログ・ファイルが読み取られます。
スロットル・イベント数/秒	SMB Tail プロトコルが 1 秒当たり転送するイベントの最大数。

SNMPv2 プロトコルの構成オプション

SNMPv2 プロトコルを使用して SNMPv2 イベントを受信するようにログ・ソースを構成することができます。

SNMPv2 プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 24. *SNMPv2* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**SNMPv3**
コミュニティー	SNMP イベントが含まれているシステムにアクセスするために必要な SNMP コミュニティー名。
イベント・ペイロードに OID を含める (Include OIDs in Event Payload)	イベント・ペイロード形式ではなく、名前と値のペアを使用して SNMP イベント・ペイロードを構成するように指定します。 「ログ・ソース・タイプ」リストから特定のログ・ソースを選択した場合は、SNMPv2 イベントまたは SNMPv3 イベントを処理するためにイベント・ペイロードの OID が必要です。

SNMPv3 プロトコルの構成オプション

SNMPv3 プロトコルを使用して SNMPv3 イベントを受信するようにログ・ソースを構成することができます。

SNMPv3 プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 25. *SNMPv3* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**SNMPv3**
認証プロトコル	SNMP トラップの認証に使用するアルゴリズム。
イベント・ペイロードに OID を含める (Include OIDs in Event Payload)	標準のイベント・ペイロード形式ではなく、名前と値のペアを使用して SNMP イベント・ペイロードを構成するように指定します。「ログ・ソース・タイプ」リストから特定のログ・ソースを選択した場合は、SNMPv2 イベントまたは SNMPv3 イベントを処理するためにイベント・ペイロードの OID が必要です。

Seculert Protection REST API プロトコルの構成オプション

Seculert からイベントを受信するには、Seculert Protection REST API プロトコルを使用するようにログ・ソースを構成します。

Seculert Protection は、アクティブに情報の通信または引き出しを行っているマルウェアの確認済みインシデントに関するアラートを生成します。

Seculert のログ・ソースを構成するには、事前に Seculert Web ポータルから API 鍵を入手する必要があります。

1. Seculert Web ポータルにログインします。
2. ダッシュボードで、「**API**」タブをクリックします。
3. 「**Your API Key**」の値をコピーします。

Seculert Protection REST API プロトコルのプロトコル固有のパラメーターについて、以下の表で説明します。

表 *26. Seculert Protection REST API* プロトコルのパラメーター

パラメーター	説明
API 鍵	Seculert Protection REST API での認証に使用される API 鍵。API 鍵の値は Seculert Web ポータルから入手します。
プロキシーの使用 (Use Proxy)	プロキシーを構成すると、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Seculert Protection REST API にアクセスします。 「プロキシー **IP** またはホスト名 **(Proxy IP or Hostname)**」、「プロキシー・ポート」、「プロキシー・ユーザー名」、および「プロキシー・パスワード」の各フィールドを構成します。プロキシーが認証を必要としない場合、「プロキシー・ユーザー名」フィールドと「プロキシー・パスワード」フィールドはブランクのままでかまいません。
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	リストから「はい」を選択すると、QRadar は証明書をダウンロードし、ターゲット・サーバーを信頼して使用し始めます。
繰り返し (Recurrence)	ログがいつデータを収集するかを指定します。フォーマットは、月/時刻/日を表す M/H/D です。デフォルトは、1 M です。
EPS スロットル	API から受信するイベントの、1 秒当たりの最大イベント数 (eps) の上限。

Sophos Enterprise Console JDBC プロトコルの構成オプション

Sophos Enterprise Console からイベントを受信するには、Sophos Enterprise Console JDBC プロトコルを使用するようにログ・ソースを構成します。

Sophos Enterprise Console JDBC プロトコルは、アプリケーション制御ログ、デバイス制御ログ、データ制御ログ、改ざんからの保護ログ、およびファイアウォール・ログからのペイロード情報を vEventsCommonData 表に結合します。Sophos Enterprise Console が Sophos Reporting Interface を備えていない場合は、標準の JDBC プロトコルを使用してアンチウィルス・イベントを収集できます。

Sophos Enterprise Console JDBC プロトコル用のパラメーターについて、以下の表で説明します。

表 27. *Sophos Enterprise Console JDBC* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Sophos Enterprise Console JDBC**
データベース・タイプ	**MSDE**
データベース名	データベース名は、「ログ・ソース **ID**」フィールドで指定したデータベース名に一致している必要があります。
ポート	Sophos Enterprise Console での MSDE のデフォルト・ポートは 1168 です。JDBC 構成ポートは、QRadar と通信するための Sophos データベースのリスナー・ポートに一致している必要があります。Sophos データベースでは、着信 TCP 接続を有効にしておく必要があります。 MSDE データベース・タイプの場合に「データベース・インスタンス」を使用するときは、「ポート」パラメーターを空白のままにしておく必要があります。
認証ドメイン	ネットワークがドメインを使用しない場合は、このフィールドを空白のままにしてください。
データベース・インスタンス	データベース・インスタンス (必要な場合)。MSDE データベースでは、単一のサーバーに複数の SQL サーバー・インスタンスを含めることができます。 標準以外のポートをデータベースに使用する場合、または管理者が SQL データベース解決のためのポート 1434 へのアクセスをブロックしている場合は、「データベース・インスタンス」パラメーターを空白にする必要があります。
テーブル名	`vEventsCommonData`
選択リスト	*
比較フィールド	`InsertedAt`
準備済みステートメントの使用 (Use Prepared Statements)	準備済みステートメントを使用すると、プロトコル・ソースで SQL ステートメントをセットアップし、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティー上およびパフォーマンス上の理由により、ほとんどの構成で準備済みステートメントを使用することができます。プリコンパイル・ステートメントを使用しない代替照会手法を使用する場合は、このチェック・ボックスをクリアしてください。
開始日時	オプション。プロトコルがデータベースのポーリングを開始できる開始日時。開始時刻が定義されていない場合、このプロトコルは、ログ・ソース構成が保存されてデプロイされた後にイベントをポーリングしようとします。

表 27. *Sophos Enterprise Console JDBC* プロトコルのパラメーター (続き)

パラメーター	説明
ポーリング間隔 (Polling Interval)	ポーリング間隔。データベースに対する照会から次の照会までの時間です。より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。指定子の H および M のない数値の場合は、秒単位のポーリングになります。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数。
名前付きパイプ通信の使用 (Use Named Pipe Communication)	データベース・タイプとして MSDE を構成した場合、管理者はこのチェック・ボックスを選択して、TCP/IP ポート接続の代替方式を使用することができます。 MSDE データベースの名前付きパイプ接続を使用する場合は、「ユーザー名」フィールドおよび「パスワード」フィールドで、データベースのユーザー名とパスワードではなく、Windows 認証のユーザー名とパスワードを使用する必要があります。ログ・ソースの構成では、MSDE データベースのデフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 (Database Cluster Name)	SQL サーバーをクラスター環境で使用する場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにします。
NTLMv2 の使用	NTLMv2 認証を必要とする SQL サーバーの場合に、強制的に MSDE 接続で NTLMv2 プロトコルを使用します。このチェック・ボックスはデフォルトで選択されています。 「**NTLMv2** の使用」チェック・ボックスを選択しても、NTLMv2 認証を必要としない MSDE 接続の通信には干渉しません。

Sourcefire Defense Center eStreamer プロトコルのオプション

Sourcefire Defense Center eStreamer プロトコルは、現在は Cisco Firepower eStreamer プロトコルと呼ばれています。

Syslog リダイレクト・プロトコルの概要

Syslog リダイレクト・プロトコルは、Syslog プロトコルの代わりに使用します。このプロトコルは、イベントを送信した特定のデバイス名を QRadar に識別させる場合に使用します。QRadar は、UDP ポート 517 で Syslog イベントを受動的に listen できます。

Syslog リダイレクト・プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 28. *Syslog* リダイレクト・プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Syslog** リダイレクト

表 28. *Syslog* リダイレクト・プロトコルのパラメーター (続き)

パラメーター	説明
ログ・ソース ID 正規表現 (Log Source Identifier Regex)	`devname=([¥w-]+)`
ログ・ソース ID 正規表現のフォーマット・ストリング (Log Source Identifier Regex Format String)	「ログ・ソース名」フィールドに、Syslog ヘッダーのホスト名を入力します。 キャプチャー・グループを使用して、Syslog ヘッダーのホスト名を置換できます。キャプチャー・グループによる置換は、`¥x` を使用して指定します。ここで、`x` は、正規表現が含まれているグループ番号です。複数のキャプチャー・グループを使用できます。 例えば、ペイロードのソース名が `hostname=(.*?)` で、キャプチャー・グループ 1 の正規表現が `ibm` である場合、ペイロードを次のホスト名にカスタマイズするには、`¥1.`*`hostname`*`.com` と入力します。 `ibm.`*`hostname`*`.com`
Listen ポート	`517`
プロトコル	**UDP**

TCP 複数行 Syslog プロトコルの構成オプション

TCP 複数行 Syslog プロトコルを使用するログ・ソースを構成することができます。単一行イベントを作成するために、このプロトコルは正規表現を使用して、複数行イベントの開始パターンおよび終了パターンを識別します。

複数行イベントの例を以下に示します。

```
06/13/2012 08:15:15 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5156
EventType=0
TaskCategory=Filtering Platform Connection
Keywords=Audit Success
Message=The Windows Filtering Platform permitted a connection.
Process ID: 4
Application Name: System
Direction: Inbound
Source Address: 1.1.1.1
Source Port: 80
Destination Address: 1.1.1.12
Destination Port:444
```

TCP 複数行 Syslog プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 29. *TCP* 複数行 *Syslog* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**TCP** 複数行 **Syslog**
Listen ポート	デフォルトの Listen ポートは 12468 です。

表 29. *TCP* 複数行 *Syslog* プロトコルのパラメーター (続き)

パラメーター	説明
イベント・フォーマッター (Event Formatter)	特に Windows 用に書式設定された複数行イベントの場合は、「**Windows** 複数行 **(Windows Multiline)**」オプションを使用します。
イベント開始パターン (Event Start Pattern)	TCP 複数行イベント・ペイロードの開始を識別するために必要な正規表現。通常、Syslog ヘッダーは日時スタンプで始まります。このプロトコルでは、イベント開始パターン (タイム・スタンプなど) のみに基づく単一行イベントを作成できます。開始パターンしか使用できない場合、このプロトコルは、それぞれの開始値の間にあるすべての情報を取り込んで有効なイベントを作成します。
イベント終了パターン (Event End Pattern)	TCP 複数行イベント・ペイロードの最後のフィールドを識別するために必要な正規表現。Syslog イベントがすべて同じ値で終了する場合は、正規表現を使用してイベントの終了を判別することができます。このプロトコルでは、イベント終了パターンのみに基づくイベントをキャプチャーできます。終了パターンしか使用できない場合、このプロトコルは、それぞれの終了値の間にあるすべての情報を取り込んで有効なイベントを作成します。

TLS Syslog プロトコルの構成オプション

TLS Syslog イベント転送をサポートする最大 50 台のネットワーク・デバイスから暗号化された Syslog イベントを受信するには、TLS Syslog プロトコルを使用するようにログ・ソースを構成します。

ログ・ソースは、着信 TLS Syslog イベントの listen ポートを作成し、ネットワーク・デバイスに対する証明書ファイルを生成します。最大50 台のネットワーク・アプライアンスが、ログ・ソースに対して作成された listen ポートにイベントを転送することができます。50 台を超えるネットワーク・アプライアンスが必要な場合は、追加の listen ポートを作成してください。

TLS Syslog プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 30. *TLS Syslog* プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**TLS Syslog**
TLS listen ポート	デフォルトの TLS listen ポートは 6514 です。
認証モード (Authentication Mode)	TLS 接続が認証されるモード。「**TLS** およびクライアント認証 **(TLS and Client Authentication)**」オプションを選択した場合は、証明書パラメーターを構成する必要があります。
クライアント証明書パス (Client Certificate Path)	ディスク上のクライアント証明書の絶対パス。証明書は、このログ・ソースのコンソールまたはイベント・コレクター (Event Collector)に保管する必要があります。

表 30. TLS Syslog プロトコルのパラメーター (続き)

パラメーター	説明
証明書タイプ (Certificate Type)	認証に使用する証明書のタイプ。「証明書の提供 **(Provide Certificate)**」オプションを選択した場合は、サーバー証明書および秘密鍵のファイル・パスを構成する必要があります。
提供されているサーバー証明書のパス (Provided Server Certificate Path)	サーバー証明書の絶対パス。
提供されている秘密鍵のパス (Provided Private Key Path)	秘密鍵の絶対パス。 **注:** 対応する秘密鍵は、DER エンコードの PKCS8 鍵でなければなりません。他の鍵形式の場合は、構成に失敗します。
最大接続数 (Maximum Connections)	「最大接続数 **(Maximum Connections)**」パラメーターは、各イベント・コレクター (Event Collector)について TLS Syslog プロトコルが許容できる同時接続の数を制御します。各イベント・コレクター (Event Collector)について、すべての TLS Syslog ログ・ソース構成で 1000 接続の制限があります。各デバイス接続のデフォルトは 50 です。 **注:** 別のログ・ソースとリスナーを共有する、自動的にディスカバーされたログ・ソースは、この制限に対して 1 回のみカウントされます。例えば、同一のイベント・コレクターで同一のポートを使用する場合です。

TLS Syslog のユース・ケース

作成できる構成の例を以下のユース・ケースに示します。

クライアント認証
: このプロトコルがクライアント認証に関与できるようにするクライアント証明書を提供できます。このオプションを選択して証明書を提供すると、着信接続がクライアント証明書に照らして検証されます。

ユーザー提供のサーバー証明書
: 専用のサーバー証明書および対応する秘密鍵を構成できます。構成した TLS Syslog プロバイダーは、その証明書と鍵を使用します。着信接続には、自動的に生成された TLS Syslog 証明書ではなく、ユーザー提供の証明書が提示されます。

デフォルト認証
: デフォルト認証方式を使用するには、「認証モード **(Authentication Mode)**」および「証明書タイプ **(Certificate Type)**」の各パラメーターにデフォルト値を使用します。ログ・ソースが保存されると、ログ・ソース・デバイスに対して `syslog-tls` 証明書が作成されます。この証明書を、暗号化された Syslog データを転送するネットワーク上のすべてのデバイスにコピーする必要があります。

UDP 複数行 Syslog プロトコルの構成オプション

単一行 Syslog イベントを複数行イベントから作成するには、UDP 複数行プロトコルを使用するようにログ・ソースを構成します。UDP 複数行 Syslog プロトコルは、正規表現を使用して複数行 Syslog メッセージを識別し、単一のイベント・ペイロードに再組み立てします。

元のイベントに含まれる値が正規表現を繰り返しており、その正規表現によって複数行イベントを識別して再組み立てできる必要があります。例えば、以下のイベントでは特定の値が繰り返されています。

```
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SEARCH RESULT tag=101
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH base="dc=iso-n,dc=com"
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH attr=gidNumber
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=1 SRCH base="dc=iso-n,dc=com"
```

UDP 複数行 Syslog プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 31. UDP 複数行 Syslog プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**UDP Multiline Syslog**
メッセージ ID のパターン	イベント・ペイロード・メッセージをフィルタリングするために必要な正規表現。UDP 複数行イベント・メッセージでは、イベント・メッセージの各行で共通の識別値が繰り返されている必要があります。

ログ・ソースが保存されると、ログ・ソースに対して syslog-tls 証明書が作成されます。この証明書を、暗号化された Syslog を転送するように構成されたネットワーク上のすべてのデバイスにコピーする必要があります。syslog-tls 証明書ファイルおよび TLS listen ポート番号を持つ他のネットワーク・デバイスは、TLS Syslog ログ・ソースとして自動的にディスカバーできます。

VMware vCloud Director プロトコルの構成オプション

VMware vCloud Director 仮想環境からイベントを収集するために、VMware vCloud Director プロトコルを使用するログ・ソースを作成できます。

VMware vCloud Director プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 32. VMware vCloud Director プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**VMware vCloud Director**
vCloud URL	REST API にアクセスするために VMware vCloud アプライアンスで構成されている URL。この URL は、vCloud サーバーの VCD 公開 REST API の基本 URL として構成されているアドレス (`https://1.1.1.1.` など) に一致していなければなりません。

表 32. *VMware vCloud Director* プロトコルのパラメーター (続き)

パラメーター	説明
ユーザー名	vCloud サーバーへのリモート・アクセスに必要なユーザー名 (`console/user@organization` など)。vCloud Director プロトコルとともに使用する読み取り専用のアカウントを構成するには、ユーザーに「コンソール・アクセス専用 (Console Access Only)」権限が必要です。

バルク・ログ・ソースの追加

一度に最大 500 個の Microsoft Windows またはユニバーサル DSM のログ・ソースを追加できます。複数のログ・ソースを同時に追加する場合は、QRadar でバルク・ログ・ソースを追加します。バルク・ログ・ソースは、共通の構成を共有する必要があります。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「一括アクション」リストから「一括追加」を選択します。
4. バルク・ログ・ソースのパラメーターを構成します。
   - ファイル・アップロード - 1 行に 1 つのホスト名または IP が含まれるテキスト・ファイルをアップロードします。
   - 手動 - 追加するホストのホスト名または IP を入力します。
5. 「保存」をクリックします。
6. 「続行」をクリックして、ログ・ソースを追加します。
7. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースの構文解析順序の追加

イベントがターゲット・イベント・コレクターで構文解析されるときの順序として、優先順位を割り当てることができます。

このタスクについて

共通の IP アドレスまたはホスト名を共有するログ・ソースに対して構文解析順序を定義することで、ログ・ソースの重要度を指定できます。ログ・ソースの構文解析順序を定義すると、ログ・ソース構成が変更されても、特定のログ・ソースが特定の順序で解析されるようになります。解析順序により、不要な解析が防止され、ログ・ソース構成に対する変更によってシステム・パフォーマンスが影響を受けることがなくなります。解析順序により、より重要なログ・ソースより先に低レベルのイベント・ソースが解析されることがなくなります。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソースの構文解析順序」アイコンをクリックします。
3. ログ・ソースを選択します。

4. オプション: 「選択されたイベント・コレクター」リストから、ログ・ソース構文解析順序を定義するイベント・コレクターを選択します。
5. オプション: 「ログ・ソースのホスト」リストから、ログ・ソースを選択します。
6. ログ・ソースの構文解析順序の優先順位を設定します。
7. 「保存」をクリックします。

第 3 章 ログ・ソース拡張

拡張文書により、特定のログ・ソースのエレメントを構文解析する方法を拡張したり変更したりすることができます。拡張文書を使用して、構文解析の問題を修正したり、既存の DSM からのイベントに対するデフォルトの構文解析をオーバーライドしたりすることができます。

拡張文書は、ネットワーク内のアプライアンスまたはセキュリティー・デバイスのイベントを解析する DSM が存在しないときにイベントのサポートを提供することもできます。

拡張文書は Extensible Markup Language (XML) 形式の文書であり、一般的な任意のテキスト・エディター、コード・エディター、またはマークアップ・エディターを使用して作成したり編集したりすることができます。複数の拡張文書を作成できますが、1 つのログ・ソースに適用できる拡張文書は 1 つだけです。

XML 形式では、すべての正規表現パターンを文字データ (CDATA) セクションに記述して、正規表現に必要な特殊文字がマークアップ書式に干渉しないようにする必要があります。例として、プロトコルを検出するための正規表現を以下のコードに示します。

```
<pattern id="ProtocolPattern" case-insensitive="true" xmlns="">
<![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
```

`(TCP|UDP|ICMP|GRE)` は正規表現パターンです。

ログ・ソース拡張の構成は、以下のセクションから構成されます。

パターン
: 特定のフィールド名に関連付ける正規表現パターン。パターンは、ログ・ソース拡張ファイル内で何度も参照されます。

比較グループ
: 構文解析される比較グループ内のエンティティー (EventName など)。構文解析のために適切なパターンおよびグループと組み合わせます。拡張文書には任意の数の比較グループを記述できます。

QRadar フォーラムでのログ・ソース拡張の例

サポートされる DSM がないログ・ソースの場合は、ログ・ソース拡張 (LSX) を作成できます。過去に作成した既存の拡張を変更すると、独自のログ・ソース拡張 (DSM 拡張とも呼びます) を簡単に作成できます。

DSM 拡張やカスタム・プロパティーなどの正規表現関連トピックのディスカッション・フォーラム (https://www.ibm.com/developerworks/community/forums/html/forum?id=11111111-0000-0000-0000-000000003046&ps=25) のログ・ソース拡張の例 (https://www.ibm.com/developerworks/community/forums/html/topic?id=d15cac8d-b0fa-4461-bb1e-dc1b291de440&ps=25) にアクセスできます。

IBM Security QRadar のフォーラムはオンラインのディスカッション・サイトであり、ユーザーと対象分野の専門家が共同作業したり情報を共有したりしています。

関連概念:

56 ページの『QRadar 内にデータを取得するためのログ・ソース拡張文書の作成』

ログ・ソースが DSM をサポートしない場合、情報の欠落や誤りがあるイベントを修復する場合、または関連付けた DSM が結果の生成に失敗するときにイベントを構文解析する場合には、ログ・ソース拡張 (LSX) を作成します。

ログ・ソース拡張文書のパターン

正規表現を特定のフィールド名に直接関連付けるのではなく、拡張文書の先頭で別個にパターン (patterns) を宣言します。これらの正規表現パターンは、ログ・ソース拡張ファイルの中で何度でも参照できます。

開始タグ <pattern> と終了タグ </pattern> の間にあるすべての文字が、パターンの構成要素と見なされます。パターンや <CDATA> 表現の内側や前後には余分なスペースや改行を記述しないでください。余分な文字やスペースがあると、意図したパターンに DSM 拡張が一致しなくなる可能性があります。

表 33. パターン・パラメーターの説明

パターン	タイプ	説明
id (必須)	String	拡張文書の中で固有の、通常のストリング。
case-insensitive (オプション)	Boolean	true の場合は、大文字と小文字の違いを無視します。例えば、abc は ABC と同じです。 指定しない場合、このパラメーターはデフォルトで false になります。
trim-whitespace (オプション)	Boolean	true の場合は、ホワイト・スペースおよび改行を無視します。CDATA セクションを複数の行に分割しても、余分なスペースおよび改行がパターンの一部として解釈されることはありません。 指定しない場合、このパラメーターはデフォルトで false になります。

比較グループ

比較グループ (match-group) は、1 つ以上のイベント・タイプを構文解析または変更するために使用する一連のパターンです。

比較機能 は、構文解析される比較グループの中のエンティティー (EventName など) であり、構文解析のために適切なパターンおよびグループと組み合わせます。拡張文書には任意の数の比較グループを記述できます。

表 *34.* 比較グループ・パラメーターの説明

パラメーター	説明
`order` (必須)	比較グループを実行する順序を定義する正の整数。拡張文書の中で固有でなければなりません。
`description` (オプション)	比較グループの説明。任意のストリングを記述できます。この情報はログに出力できます。 指定しない場合、このパラメーターはデフォルトで空になります。
`device-type-id-override` (オプション)	別のデバイス ID を定義して QID をオーバーライドします。特定の比較グループが、指定のデバイスでイベント・タイプを検索できるようにします。有効なログ・ソース・タイプ ID でなければならず、整数で表す必要があります。ログ・ソース・タイプ ID のリストについては、 69 ページの表 41を参照してください。 指定しない場合のこのパラメーターのデフォルトは、拡張を接続するログ・ソースのログ・ソース・タイプです。

比較グループは以下のエンティティーを持つことができます。

- 『比較機能 (matcher)』
- 52 ページの『単一イベント修飾子 (`event-match-single`)』
- 52 ページの『複数イベント修飾子 (`event-match-multiple`)』

比較機能 (matcher)

比較機能エンティティーは、構文解析されるフィールド (EventName など) であり、構文解析のために適切なパターンおよびグループと組み合わせます。

比較機能には順序が関連付けられます。同じフィールド名に対して複数の比較機能が指定された場合は、正常に構文解析されるまで、または構文解析に失敗するまで、記述された順序で比較機能が実行されます。

表 *35.* 比較機能のパラメーターの説明

パラメーター	説明
`field` (必須)	パターンの適用対象フィールド (EventName や SourceIp など)。有効な比較機能フィールド名のリストの表に示した任意のフィールド名を使用できます。

表 35. 比較機能のパラメーターの説明 (続き)

パラメーター	説明
pattern-id (必須)	ペイロードにあるフィールドを構文解析するときに使用するパターン。この値は、以前にパターン ID パラメーター (46 ページの表 33) で定義したパターンの ID パラメーターに (大文字と小文字の違いも含めて) 一致していなければなりません。
order (必須)	同じフィールドに割り当てた比較機能の中で、このパターンを適用する順序。EventName フィールドに 2 つの比較機能を割り当てた場合は、order が最も小さいものが最初に適用されます。
capture-group (オプション)	正規表現における、小括弧 ( ) の内側を参照します。これらのキャプチャーの添字は 1 から始まり、パターンの左から右へ処理されます。capture-group フィールドは、パターンに存在するキャプチャー・グループの数以下の正の整数でなければなりません。デフォルト値は 0 であり、一致全体に相当します。 例えば、送信元 IP アドレスおよびポートに対して単一のパターンを定義できます。この場合、SourceIp という比較機能でキャプチャー・グループ 1 を使用し、SourcePort という比較機能でキャプチャー・グループ 2 を使用することができますが、定義する必要があるパターンは 1 つだけです。 enable-substitutions パラメーターと組み合わせた場合、このフィールドには 2 つの目的が備わります。 例については、拡張文書の例を参照してください。

表 35. 比較機能のパラメーターの説明 (続き)

パラメーター	説明
enable-substitutions (オプション)	Boolean true に設定した場合は、連続したグループ・キャプチャーで適切にフィールドを表記することができません。複数のグループを追加のテキストと組み合わせて値を作成することができます。 このパラメーターにより、capture-group パラメーターの意味が変化します。capture-group パラメーターは新しい値を作成し、¥x (x は 1 から 9 までのグループ番号) を使用してグループ置換が指定されます。グループは何度でも使用でき、自由な形式の任意のテキストを値に挿入することもできます。例として、グループ 1 から値を生成し、その後に下線、グループ 2、@ が続いた後に再度グループ 1 が続く値を生成する場合に適したキャプチャー・グループの構文を以下のコードに示します。 capture-group="¥1_¥2@¥1" 別の例を示します。MAC アドレスはコロンで区切りますが、QRadar では通常 MAC アドレスをハイフンで区切ります。個々の部分を構文解析してキャプチャーする構文を以下の例に示します。 capture-group="¥1:¥2:¥3:¥4:¥5:¥6" 置換が有効であるがキャプチャー・グループでグループが指定されていない場合は、直接テキスト置換が実行されます。 デフォルトは false です。
ext-data (オプション)	拡張で比較機能フィールドが提供できる追加のフィールド情報および書式設定を定義する、追加のデータ・パラメーター。 このパラメーターを使用するフィールドは DeviceTime のみです。 例えば、デバイスが固有のタイム・スタンプを使用してイベントを送信するが、そのイベントを標準のデバイス時刻に書式設定し直したい場合が該当します。このイベントの日時スタンプを書式設定し直すには、DeviceTime フィールドに組み込んだ ext-data パラメーターを使用します。詳しくは、有効な比較機能フィールド名のリストを参照してください。

有効な比較機能フィールド名を以下の表に示します。

表 *36.* 有効な比較機能フィールド名のリスト

フィールド名	説明
EventName (必須)	イベントを識別するための、QID から取得するイベント名。 **注:** このパラメーターは、「ログ・アクティビティー」タブのフィールドとしては表示されません。
EventCategory	event-match-single エンティティーまたは event-match-multiple エンティティーによって処理されないカテゴリーを持つイベントに対するイベント・カテゴリー。 EventCategory は、EventName と組み合わせて QID でイベントを検索するために使用します。QIDmap ルックアップに使用するフィールドでは、既にデバイスが QRadar に認識されているときにオーバーライド・フラグをセットする必要があります。以下に例を示します。 `<event-match-single event-name= "Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity= "OverrideAndNeverSend" />` `force-qidmap-lookup-on-fixup="true"` がフラグのオーバーライドです。 **注:** このパラメーターは、「ログ・アクティビティー」タブのフィールドとしては表示されません。
SourceIp	メッセージの送信元 IP アドレス。
SourcePort	メッセージの送信元ポート。
SourceIpPreNAT	ネットワーク・アドレス変換 (NAT) 実行前のメッセージの送信元 IP アドレス。
SourceIpPostNAT	NAT 実行後のメッセージの送信元 IP アドレス。
SourceMAC	メッセージの送信元 MAC アドレス。
SourcePortPreNAT	NAT 実行前のメッセージの送信元ポート。
SourcePortPostNAT	NAT 実行後のメッセージの送信元ポート。
DestinationIp	メッセージの宛先 IP アドレス。
DestinationPort	メッセージの宛先ポート。
DestinationIpPreNAT	NAT 実行前のメッセージの宛先 IP アドレス。
DestinationIpPostNAT	NAT 実行後のメッセージの宛先 IP アドレス。
DestinationPortPreNAT	NAT 実行前のメッセージの宛先ポート。
DestinationPortPostNAT	NAT 実行後のメッセージの宛先ポート。

表 36. 有効な比較機能フィールド名のリスト (続き)

フィールド名	説明
DestinationMAC	メッセージの宛先 MAC アドレス。
DeviceTime	デバイスで使用する時刻および形式。デバイスによっては、この日時スタンプがイベントの送信時刻を表します。このパラメーターはイベントの受信時刻を表すわけではありません。ext-data の比較機能属性を使用することによって、`DeviceTime` フィールドでイベントのカスタム日時スタンプを使用できます。 `DeviceTime` フィールドで使用できる日時スタンプ形式の例を以下に示します。 • ext-data="dd/MMM/YYYY:hh:mm:ss" 11/Mar/2015:05:26:00 • ext-data="MMM dd YYYY / hh:mm:ss" Mar 11 2015 / 05:26:00 • ext-data="hh:mm:ss:dd/MMM/YYYY" 05:26:00:11/Mar/2015 データおよびタイム・スタンプの形式に使用可能な値について詳しくは、Joda-Time の Web ページ (http://www.joda.org/joda-time/key_format.html) を参照してください。 DeviceTime は、オプション・パラメーター ext-data を使用する唯一のイベント・フィールドです。
Protocol	メッセージのプロトコル (TCP、UDP、ICMP など)。
UserName	メッセージのユーザー名。
HostName	メッセージのホスト名。一般に、このフィールドはアイデンティティー・イベントに関連付けます。
GroupName	メッセージのグループ名。一般に、このフィールドはアイデンティティー・イベントに関連付けます。
IdentityIp	メッセージのアイデンティティー IP アドレス。
IdentityMac	メッセージのアイデンティティー MAC アドレス。
IdentityIpv6	メッセージの IPv6 アイデンティティー IP アドレス。
NetBIOSName	メッセージの NetBIOS 名。一般に、このフィールドはアイデンティティー・イベントに関連付けます。

表 36. 有効な比較機能フィールド名のリスト (続き)

フィールド名	説明
ExtraIdentityData	メッセージのユーザー固有データ。一般に、このフィールドはアイデンティティー・イベントに関連付けます。
SourceIpv6	メッセージの IPv6 送信元 IP アドレス。
DestinationIpv6	メッセージの IPv6 宛先 IP アドレス。

複数イベント修飾子 (event-match-multiple)

複数イベント修飾子 (event-match-multiple) は、pattern-id パラメーターおよび capture-group-index パラメーターでの指定に従って、一定の範囲のイベント・タイプに一致し、そのイベント・タイプを変更します。

この比較はペイロードに対して行われるのではなく、既にペイロードから構文解析された EventName 比較機能の結果に対して行われます。

このエンティティーにより、デバイス・イベント・カテゴリー、重大度、またはイベントがアイデンティティー・イベントの送信に使用する方式を変更して、正常なイベントを変換することができます。capture-group-index は整数値でなければならず (置換はサポートされていません)、pattern-ID は既存のパターン・エンティティーを参照する必要があります。それ以外のプロパティーは、いずれも単一イベント修飾子の対応するプロパティーと同じです。

単一イベント修飾子 (event-match-single)

単一イベント修飾子 (event-match-single) は、必須の EventName パラメーター (大文字と小文字を区別します) の指定に従って 1 つのイベント・タイプのみに一致し、それを変更します。

このエンティティーにより、デバイス・イベント・カテゴリー、重大度、またはアイデンティティー・イベントの送信方式を変更して、正常なイベントを変換することができます。

このイベント名に一致するイベントを構文解析するときには、デバイス・カテゴリー、重大度、およびアイデンティティー・プロパティーを結果イベントに適用します。

event-name 属性を設定する必要があります。この属性の値は **EventName** フィールドの値に一致します。そのほか、event-match-single エンティティーは以下のオプション・プロパティーから構成されます。

表 37. 単一イベント・パラメーターの説明

パラメーター	説明
device-event-category	イベントの QID を検索するための新規カテゴリー。このパラメーターは、一部のデバイスではすべてのイベントに同じカテゴリーが使用されることによる最適化パラメーターです。

表 37. 単一イベント・パラメーターの説明 (続き)

パラメーター	説明
severity	イベントの重大度。このパラメーターは 1 から 10 までの整数値でなければなりません。 1 未満または 10 を超える重大度を指定した場合は、デフォルトで 5 になります。 指定しない場合のデフォルトは、QID で検出した値です。
send-identity	イベントからのアイデンティティー変更情報を送信することを指定します。次のオプションのいずれかを選択してください。 • UseDSMResults DSM がアイデンティティー・イベントを返す場合は、そのイベントが渡されます。DSM がアイデンティティー・イベントを返さない場合、拡張はアイデンティティー情報を作成も変更もしません。 このオプションは、値が指定されていない場合のデフォルト値です。 • SendIfAbsent DSM がアイデンティティー情報を作成する場合、アイデンティティー・イベントは変更されずに渡されます。DSM がアイデンティティー・イベントを生成しないが、アイデンティティー・イベントの作成に十分な情報がイベントに存在する場合は、関連したフィールドがすべて設定されたイベントが生成されます。 • OverrideAndAlwaysSend 十分な情報がある場合は、DSM によって返されたアイデンティティー・イベントを無視し、新しいアイデンティティー・イベントを作成します。 • OverrideAndNeverSend DSM によって返されたアイデンティティー情報をすべて抑止します。アセット更新に渡すイベントを処理しない場合は、このオプションを推奨します。

拡張文書のテンプレート

ここに示す拡張文書の例では、特定のタイプの Cisco FWSM を構文解析し、誤ったイベント名でイベントが送信されないようにする方法を示します。

例として、以下のように session という単語がイベント名の中間に埋め込まれており、その単語を解決する場合を考えます。

```
Nov 17 09:28:26 129.15.126.6 %FWSM-session-0-302015:
Built UDP connection for faddr 38.116.157.195/80
gaddr 129.15.127.254/31696 laddr 10.194.2.196/2157
duration 0:00:00 bytes 57498 (TCP FINs)
```

この状態では DSM がイベントをまったく認識せず、すべてのイベントが構文解析されずに汎用ロガーに関連付けられてしまいます。

QID の検索にはテキスト・ストリングの一部 (302015) しか使用しませんが、イベントが Cisco FWSM から送信されたことはテキスト・ストリング全体 (%FWSM-session-0-302015) で示されています。テキスト・ストリング全体では有効にならないため、DSM はイベントが有効でないと見なします。

特定のイベント・タイプを構文解析するための拡張文書の例

FWSM デバイスには多くのイベント・タイプがあり、多くが固有の形式を持っています。以下の拡張文書の例では、特定のイベント・タイプを構文解析する方法を示します。

注: 構文解析するフィールド名にパターン ID が一致する必要はありません。以下の例ではパターンをコピーしていますが、この場合は SourceIp フィールドおよび SourceIpPreNAT フィールドにまったく同じパターンを使用できます。ただし、すべての FWSM イベントにこの状況が当てはまるとは限りません。

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z¥-]*¥d-(¥d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(tcp|udp|icmp|gre)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(¥d{1,6})]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
      <matcher field="EventName" order="1" pattern-id="EventNameFWSM_Pattern" capture-group="1"/>
      <matcher field="SourceIp" order="1" pattern-id="SourceIp_Pattern" capture-group="1" />
      <matcher field="SourcePort" order="1" pattern-id="SourcePort_Pattern" capture-group="2"/>
      <matcher field="SourceIpPreNAT" order="1" pattern-id="SourceIpPreNAT_Pattern" capture-group="1" />
      <matcher field="SourceIpPostNAT" order="1" pattern-id="SourceIpPostNAT_Pattern" capture-group="1" />
      <matcher field="SourcePortPreNAT" order="1" pattern-id="SourcePortPreNAT_Pattern" capture-group="2" />
      <matcher field="SourcePortPostNAT" order="1" pattern-id="SourcePortPostNAT_Pattern" capture-group="2" />
      <matcher field="DestinationIp" order="1" pattern-id="DestinationIp_Pattern" capture-group="1" />
      <matcher field="DestinationPort" order="1" pattern-id="DestinationIp_Pattern" capture-group="2" />
      <matcher field="Protocol" order="1" pattern-id="Protocol_Pattern" capture-group="1" />
      <matcher field="Protocol" order="2" pattern-id="Protocol_6_Pattern" capture-group="TCP" enable-substitutions=true/>
      <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
   </match-group>
</device-extension>

<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<!-- Do not remove the "allEventNames" value -->
<pattern id="EventName-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceIp-Fakeware_Pattern" xmlns=""><![CDATA[]]</pattern>
<pattern id="SourcePort-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceMAC-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationIp-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationPort-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<pattern id="Protocol-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceIp" order="1" pattern-id="SourceIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="SourcePort" order="1" pattern-id="SourcePort-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceMAC" order="1" pattern-id="SourceMAC-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationIp" order="1" pattern-id="DestinationIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationPort" order="1" pattern-id="SDestinationPort-Fakeware_Pattern" capture-group="1" />
   <matcher field="Protocol" order="1" pattern-id="Protocol-Fakeware_Pattern" capture-group="1" />
   <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
</match-group>
</device-extension>
```

構文解析の基礎

前記の拡張文書の例では、構文解析の基本的な側面のうち、以下のものを示しました。

- IP アドレス
- ポート
- プロトコル
- グループが異なるが同じパターンを使用する複数のフィールド

この例では、指定したパターンに従うすべての FWSM イベントを構文解析します。イベントの内容が異なる場合は、構文解析対象のフィールドがそのイベントに存在しない場合があります。

イベントで使用できなかった、この構成を作成するために必要であった情報は以下のとおりです。

- イベント名は、イベントの `%FWSM-session-0-302015` 部分の末尾 6 桁 (302015) のみです。
- FWSM は、Cisco ファイアウォールのデバイス・イベント・カテゴリーがハードコーディングされたものです。
- FWSM DSM は Cisco Pix QIDmap を使用するため、比較グループで `device-type-id-override="6"` というパラメーターを指定しています。Pix ファイアウォール・ログ・ソース・タイプの ID は 6 です。詳しくは、69 ページの『ログ・ソース・タイプの ID』を参照してください。

注: QID 情報が指定されていない場合や使用できない場合は、イベントのマッピングを変更できます。詳しくは、「*IBM Security QRadar* ユーザー・ガイド」の『イベントのマッピングの変更』を参照してください。

イベント名とデバイス・イベント・カテゴリー

QIDmap の検索時には、イベント名とデバイス・イベント・カテゴリーが必要です。このデバイス・イベント・カテゴリーはデータベース内のグループ化パラメーターであり、デバイス内の類似イベントの定義に役立ちます。比較グループの末尾にある `event-match-multiple` ではカテゴリーをハードコーディングしています。`event-match-multiple` は、構文解析したイベント名に対して EventNameId パターンを使用して 6 桁までの比較を行います。このパターンは、ペイロード全体に対してではなく、EventName フィールドとして構文解析された部分のみに対して実行されます。

EventName パターンはイベントの `%FWSM` 部分を参照します (すべての Cisco FWSM イベントに `%FWSM` 部分が含まれています)。例に示したパターンは、`%FWSM` の後に任意の数 (0 個以上) の英字およびダッシュが続いたものに一致します。このパターン・マッチングにより、イベント名の中間に埋め込まれた単語 `session` を削除する必要がある点が解決されます。イベントの重大度 (Cisco によるもの) の後にダッシュが続き、その後に QRadar が必要とする本当のイベント名が続きます。`(¥d{6})` というストリングは、EventNameFWSM パターンの中のストリングで、唯一キャプチャー・グループを持っています。

イベントの IP アドレスとポートはすべて同じ基本パターンに従っており、IP アドレスの後にコロンとポート番号が続きます。このパターンは、データの 2 つの部分 (IP アドレスとポート) を構文解析し、matcher セクションで異なるキャプチャー・グループを指定しています。

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=¥[(¥d{2}/¥w{3}/¥d{4}:¥d{2}:¥d{2}:¥d{2})¥] </pattern>
<pattern id="Username">(TLSv1)</pattern>
<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1"
       capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username" capture-group="1"/>
</match-group>
</device-extension>
```

IP アドレスとポートのパターン

IP アドレスとポートのパターンは、1 桁から 3 桁の数値 4 組をピリオドで区切ったものの後に、コロンとポート番号を続けたものです。IP アドレスの部分は 1 つのグループになっています。ポート番号も同様ですが、コロンは異なります。これらのフィールドに対する matcher セクションは同じパターン名を参照していますが、別のキャプチャー・グループを参照しています (IP アドレスはグループ 1 であり、ポートはグループ 2 です)。

プロトコルは共通のパターンであり、ペイロードで TCP、UDP、ICMP、または GRE のうち最初のものを検索します。パターンには大文字と小文字を区別しないパラメーターを指定しているため、すべての場合に一致します。

例で使用しているイベントに 2 番目のプロトコル・パターンは出現しませんが、順序を 2 として 2 番目のプロトコル・パターンを定義しています。順序の値が最も小さいプロトコル・パターンが一致しない場合は、次のパターンが適用されます (以後同様)。2 番目のプロトコル・パターンには直接置換も示しています。このパターンに比較グループはありませんが、enable-substitutions パラメーターが有効であるため、protocol=6 の代わりにテキスト TCP を使用できます。

QRadar 内にデータを取得するためのログ・ソース拡張文書の作成

ログ・ソースが DSM をサポートしない場合、情報の欠落や誤りがあるイベントを修復する場合、または関連付けた DSM が結果の生成に失敗するときにイベントを構文解析する場合には、ログ・ソース拡張 (LSX) を作成します。

ログ・ソース拡張を作成する場合

公式な DSM がないログ・ソースの場合は、ユニバーサル DSM (uDSM) を使用してログ・ソースを統合します。それにより、ログ・ソース拡張 (デバイス拡張とも呼びます) が uDSM に適用されて、ログを構文解析するためのロジックが提供されます。LSX は Java 正規表現に基づいており、あらゆるプロトコル・タイプ (Syslog、JDBC、ログ・ファイルなど) に対して使用できます。値をログから抽出して、IBM Security QRadar 内のすべての共通フィールドにマップすることができます。

ログ・ソース拡張を使用してコンテンツの欠落や誤りを修復する場合は、ログ・ソース拡張によって生成されるすべての新規イベントが、元のペイロードの構文解析に失敗したログ・ソースに関連付けられます。拡張を作成すると、不明なイベントや未分類のイベントが QRadar に「不明」として保管されることがなくなります。

ログ・ソース拡張を素早く作成するための DSM エディターの使用

IBM Security QRadar V7.2.8 以降では、ログ・ソース拡張を作成するために DSM エディターを使用できます。DSM エディターには、作成しているログ・ソース拡張に問題があるかどうかを判別するためのリアルタイム・フィードバックが備わっています。DSM エディターを使用して、フィールドの抽出、カスタム・プロパティーの定義、イベントのカテゴリー化、および新規 QID の定義を行います。DSM エディターを使用して独自のログ・ソース・タイプを定義すると、ユニバーサル DSM を使用する必要がなくなります。DSM エディターについて詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。

ログ・ソース拡張を手動で作成するプロセス

代わりの方法として、ログ・ソース拡張を手動で作成するには、以下の手順を実行します。

1. ログ・ソースが QRadar で作成されていることを確認します。

   QRadar でサポートされる DSM としてログ・ソース・タイプがリストされていない場合にソースからイベントを収集するには、ログ・ソース・タイプとしてユニバーサル DSM を使用します。

   IBM Security QRadar V7.2.8 以降では、新規ログ・ソース・タイプを作成するためにユニバーサル DSM を使用する必要はありません。希望する場合は、DSM エディターを使用して新規ログ・ソース・タイプの作成のみを行ってから、ログ・ソースを手動で作成することができます。サポートされるログ・ソース・タイプ (例えば、QRadar でサポートされる DSM としてリストされている Windows、Bluecoat、Cisco など) に LSX を接続できます。
2. 使用可能なフィールドを判別するには、「ログ・アクティビティー」タブを使用してログをエクスポートした上で評価します。
3. 拡張文書のサンプル・テンプレートを使用して、使用できるフィールドを判別します。

   テンプレートにあるフィールドをすべて使用する必要はありません。ログ・ソースに存在し、拡張文書テンプレートのフィールドにマップできる値を判別します。
4. 使用していないフィールドとそれに対応するパターン ID をログ・ソース拡張文書から削除します。
5. 拡張文書をアップロードして、拡張をログ・ソースに適用します。
6. イベントを、QIDmap の対応する要素にマップします。

   「ログ・アクティビティー」タブのこの手動アクションを使用すると、不明なログ・ソース・イベントが既知の QRadar イベントにマップされ、分類と処理が可能になります。

関連概念:

53 ページの『拡張文書のテンプレート』
ここに示す拡張文書の例では、特定のタイプの Cisco FWSM を構文解析し、誤ったイベント名でイベントが送信されないようにする方法を示します。

45 ページの『QRadar フォーラムでのログ・ソース拡張の例』
サポートされる DSM がないログ・ソースの場合は、ログ・ソース拡張 (LSX) を作成できます。過去に作成した既存の拡張を変更すると、独自のログ・ソース拡張 (DSM 拡張とも呼びます) を簡単に作成できます。

関連資料:

1143 ページの『第 149 章 QRadar でサポートされる DSM』
IBM Security QRadar は、デバイス・サポート・モジュール (DSM) と呼ばれるプラグイン・ファイルを使用することにより、セキュリティー製品からのイベントの収集を行うことができます。

ユニバーサル DSM の作成

ユニバーサル DSM を作成するには、まず IBM Security QRadar でログ・ソースを作成します。ログ・ソースを作成するとき、ログは自動的に分類されないため、ログをエクスポートして検討することができます。

手順

1. 「管理」タブで、「ログ・ソース」アイコンをクリックして新しいソースを作成します。
2. 「追加」をクリックします。
3. 「ログ・ソース名」フィールドに名前を指定します。
4. 「ログ・ソース・タイプ」リストで「ユニバーサル **DSM**」を選択します。

   ログ・ソース拡張をまだ QRadar コンソールに適用していないときは、「ログ・ソース拡張」が表示されない場合があります。
5. 「プロトコル構成」リストで、使用するプロトコルを指定します。

   この手段は、サポートされていないログ・ソースからログを取得するために QRadar が使用します。
6. 「ログ・ソース **ID**」に、サポートされていないログ・ソースの IP アドレスまたはホスト名のいずれかを入力します。
7. 「保存」をクリックして新しいログ・ソースを保存し、ウィンドウを閉じます。
8. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

『ログのエクスポート』

ログのエクスポート

ユニバーサル DSM を作成したら、作成されたログをエクスポートします。

このタスクについて

通常、検討のためにはかなりの数のログが必要です。サポートされていないログ・ソースの EPS レートによっては、全体をカバーできるログ・サンプルの取得に数時間かかる場合があります。

QRadar がログ・ソース・タイプを検出できない場合、イベントは収集されますが、構文解析されません。これらの構文解析されないイベントにフィルターを適用して、最後に受信したシステム通知を確認することができます。システム通知を検討した後、その時間フレームに基づいた検索を作成できます。

手順

1. 構文解析されないイベントのみを参照するために、ログをフィルタリングします。
   a. 「ログ・アクティビティー」タブをクリックします。
   b. 「フィルターの追加」をクリックします。
   c. 「未解析のイベント」を選択します。

      ヒント: 「パラメーター」テキスト・ボックスの中に入力して、「未解析のイベント」項目を表示します。
   d. 時間フレームを選択します。
   e. システム通知からの「情報」イベントが表示される場合は、右クリックして除外します。
   f. 「送信元 **IP**」列を確認して、イベントを送信しているデバイスを判別します。

      ロー・イベント・ペイロードを表示できます。通常、製造元では識別可能な製品名をヘッダーに書き込むため、検索を「表示**: Raw Event**」に設定すると、それぞれのイベントを手作業で開かなくてもペイロードを表示できます。ネットワークでソートする方法も、イベントの発信元である特定のデバイスを探すのに有効です。
2. ログをエクスポートするための検索を作成します。
   a. 「ログ・アクティビティー」タブで「検索」 > 「検索の編集」を選択します。
   b. 「時刻範囲」で、ログ・ソース作成からの十分な経過時間 (例えば 6 時間) を指定します。
   c. 「パラメーター」リストの「検索パラメーター」で、「ログ・ソース **(**索引付き**) (Log Source (Indexed))**」を選択し、「演算子」リストで「次と等しい」を選択し、「ログ・ソース・グループ」リストで「その他」を選択し、ユニバーサル DSM の作成時に作成されたログ・ソースを指定します。

注**:** 設定によっては、「パラメーター」リストに「ログ・ソース **(**索引付き**) (Log Source (Indexed))**」ではなく、「ログ・ソース」が表示される場合があります。

d. 「検索」をクリックして結果を表示します。

3. コンソールの結果を検討し、ペイロードを確認します。
4. オプションで、「アクション」 > 「**XML** にエクスポート」 > 「完全エクスポート **(**すべての列**)**」をクリックして結果をエクスポートすることができます。

「**CSV** にエクスポート」は選択しないでください。理由は、ペイロードが複数の列に分割される場合があり、ペイロードの検索が難しくなるためです。イベントの検討に適した形式は XML です。

a. 圧縮ファイルをダウンロードするように指示するプロンプトが出されます。圧縮ファイルを開き、生成されたファイルを開きます。
b. ログを検討します。

イベント・ペイロードは以下のタグの間にあります。

```
<payloadAsUTF>
...
</payloadAsUTF>
```

ペイロードの例を以下のコードに示します。

```
<payloadAsUTF>ecs-ep (pid 4162 4163 4164) is running... </payloadAsUTF>
```

ユニバーサル DSM の作成にあたっては、使いやすさの観点からログを検討することが重要です。少なくとも、イベント名にマップできる値がログに存在しなければなりません。イベント名は、さまざまなログ・タイプを識別できる固有の値でなければなりません。

使用可能なログの例を以下のコードに示します。

```
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root'
from 192.168.50.80:3364
May 20 17:16:26 dropbear[22331]: password auth succeeded for
'root' from 192.168.50.80:3364
May 20 16:42:19 kernel: DROP IN=vlan2 OUT=
MAC=00:01:5c:31:39:c2:08:00 SRC=172.29.255.121
DST=255.255.255.255 PROTO=UDP SPT=67 DPT=68
```

やや使いにくいログを以下のコード例に示します。

```
Oct 26 08:12:08 loopback 1256559128 autotrace[215824]: W: trace:
no map for prod 49420003, idf 010029a2, lal 00af0008
Oct 26 16:35:00 sxpgbd0081 last message repeated 7 times
Nov 24 01:30:00 sxpgbd0081 /usr/local/monitor-rrd/sxpgbd0081/.rrd
(rc=-1, opening '/usr/local/monitor-rrd/sxpgbd0081/.rrd':
No such file or directory)
```

一般的な正規表現

ログ・ソース・ファイルでテキストのパターンを比較するには、正規表現を使用します。メッセージで英字、数字、またはそれら両方の組み合わせのパターンをスキャンできます。例えば、送信元や宛先の IP アドレス、ポート、MAC アドレスなどに一致する正規表現を作成できます。

一般的な正規表現のいくつかを以下のコードに示します。

```
¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3} ¥d{1,5}
(?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2} (TCP|UDP|ICMP|GRE)
¥w{3}¥s¥d{2}¥s¥d{2}:¥d{2}:¥d{2}
¥s ¥t .*?
```

エスケープ文字 ¥ は、リテラル文字を示すために使用します。例えば、. 文字は「任意の 1 文字」を意味し、A、B、1、X などに一致します。. という文字に一致させる (リテラル比較を行う) には、¥. を使用する必要があります。

表 *38.* 一般的な正規表現

タイプ	正規表現
タイプ	¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}
IP アドレス	¥d{1,5}
ポート番号	(?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2}
プロトコル	(TCP|UDP|ICMP|GRE)
デバイス時刻	¥w{3}¥s¥d{2}¥s¥d{2}:¥d{2}:¥d{2}
ホワイト・スペース	¥s
タブ	¥t
すべてのストリングに一致	.*?

ヒント: 誤って別の文字に一致しないように、英数字以外の文字は必ずエスケープしてください。

正規表現パターンの作成

ユニバーサル DSM を作成するには、正規表現を使用して、サポートされていないログ・ソースからのテキスト・ストリングと比較します。

このタスクについて

以下の例に、参照するログ項目をステップに分けて示します。

```
May 20 17:24:59 kernel: DROP MAC=5c:31:39:c2:08:00
SRC=172.29.255.121 DST=10.43.2.10 LEN=351 TOS=0x00 PREC=0x00 TTL=64 ID=9582
PROTO=UDP SPT=67 DPT=68 LEN=331
May 20 17:24:59 kernel: PASS MAC=5c:14:ab:c4:12:59
SRC=192.168.50.10 DST=192.168.10.25 LEN=351 TOS=0x00 PREC=0x00 TTL=64
ID=9583 PROTO=TCP SPT=1057 DPT=80 LEN=331
May 20 17:24:59 kernel: REJECT
MAC=5c:ad:3c:54:11:07 SRC=10.10.10.5 DST=192.168.100.25 LEN=351
TOS=0x00 PREC=0x00 TTL=64 ID=9584 PROTO=TCP SPT=25212 DPT=6881 LEN=331
```

手順

1. サポートされていないログ・ソースを目視で分析し、固有のパターンを見つけ出します。

   それらのパターンを、後で正規表現に変換します。
2. 比較するテキスト・ストリングを探します。

   ヒント: 基本的なエラー検査を実装するには、値の前後の文字を含めて、類似した値が意図せずに一致してしまう事態を防ぎます。後で、実際の値を余分な文字から分離することができます。

3. 比較パターンの疑似コードを作成して、パターンの先頭と末尾を示すスペース文字を含めます。

   引用符は無視して構いません。例に示したログ項目では、イベント名は DROP、PASS、および REJECT です。使用可能なイベント・フィールドを以下に示します。

   - EventName: " kernel: VALUE "
   - SourceMAC: " MAC=VALUE "
   - SourceIp: " SRC=VALUE "
   - DestinationIp: " DST=VALUE "
   - Protocol: " PROTO=VALUE "
   - SourcePort: " SPT=VALUE "
   - DestinationPort: " DPT=VALUE "

4. スペースは ¥s という正規表現で置き換えてください。

   英数字以外の文字には必ずエスケープ文字を使用してください。例えば = は ¥= とし、: は ¥: とします。

5. 疑似コードを正規表現に変換します。

表 *39.* 疑似コードから正規表現への変換

フィールド	疑似コード	正規表現
EventName	" kernel: VALUE "	¥skernel¥:¥s.*?¥s
SourceMAC	" MAC=VALUE "	¥sMAC¥=(?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2}¥s
SourceIP	" SRC=VALUE "	¥sSRC¥=¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥s
DestinationIp	" DST=VALUE "	¥sDST¥=¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥s
Protocol	" PROTO=VALUE "	¥sPROTO¥=(TCP|UDP|ICMP|GRE)¥s
SourcePort	" SPT=VALUE "	¥sSPT¥=¥d{1,5}¥s
DestinationPort	" DPT=VALUE "	¥sDPT¥=¥d{1,5}¥s

6. キャプチャー・グループを指定します。

   キャプチャー・グループは、正規表現の中の特定の値を分離します。

   例えば、前記の例に示した SourcePort パターンでは、スペースおよび SRC=<code> を含んでいるため、値全体を渡すことができません。代わりに、キャプチャー・グループを使用してポート番号のみを指定します。キャプチャー・グループの値は、IBM Security QRadar の関連フィールドに渡される値です。

   以下のように、取り込む値の前後に小括弧を挿入します。

表 *40.* 正規表現からイベント・フィールドのキャプチャー・グループへのマッピング

フィールド	正規表現	キャプチャー・グループ
EventName	¥skernel¥:¥s.*?¥s	¥skernel¥:¥s(.*?)¥s
SourceMAC	¥sMAC¥=(?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2}¥s	¥sMAC¥=((?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2})¥s

表 40. 正規表現からイベント・フィールドのキャプチャー・グループへのマッピング (続き)

フィールド	正規表現	キャプチャー・グループ
SourceIP	¥sSRC¥=¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥s	¥sSRC¥=(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})¥s
Destination IP	¥sDST¥=¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥s	¥sDST¥=(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})¥s
Protocol	¥sPROTO¥=(TCP|UDP|ICMP|GRE)¥s	¥sPROTO¥=((TCP|UDP|ICMP|GRE))¥s
SourcePort	¥sSPT¥=¥d{1,5}¥s	¥sSPT¥=(¥d{1,5})¥s
DestinationPort	¥sDPT¥=¥d{1,5}¥s	¥sDPT¥=(¥d{1,5})¥s

7. パターンおよびキャプチャー・グループをログ・ソース拡張文書に移行します。

   使用する文書の一部を以下のコード・スニペットに示します。

```
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z¥-]*¥d-(¥d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(¥d{1,6})]]></pattern>
```

QRadar への拡張文書のアップロード

複数の拡張文書を作成してアップロードし、さまざまなログ・ソース・タイプに関連付けることができます。それにより、ログ・ソース拡張 (LSX) によるロジックが、サポートされていないログ・ソースからのログを構文解析するために使用されます。

IBM Security QRadar にアップロードするまで、拡張文書は任意の場所に保管しておくことができます。

手順

1. 「管理」タブで「データ・ソース」 > 「ログ・ソース拡張」をクリックします。
2. 「ログ・ソース拡張の追加 (Add Log Source Extensions)」ウィンドウで「追加」をクリックします。
3. 名前を割り当てます。
4. ユニバーサル DSM を使用する場合は、「ログ・ソース・タイプ」のデフォルトとして拡張文書を選択しないでください。

   ユニバーサル DSM をデフォルトとして選択すると、関連付けたすべてのログ・ソースに影響が及びます。ユニバーサル DSM は、複数のカスタム・イベント・ソースおよびサポートされないイベント・ソースの構文解析ロジックを定義するために使用できます。
5. オプション: このログ・ソース拡張を特定のログ・ソース・タイプの複数のインスタンスに適用する場合は、使用可能な「ログ・ソース・タイプ」リストからログ・ソース・タイプを選択し、追加の矢印をクリックしてデフォルトとして設定します。

デフォルトのログ・ソース・タイプを設定すると、そのログ・ソース拡張が特定のログ・ソース・タイプ (および自動的にディスカバーされたログ・ソース) のすべてのイベントに適用されます。

イベントが正しく構文解析されるように、必ず最初にログ・ソース・タイプに対する拡張をテストしてください。

6. 「参照」をクリックして、保存してある LSX を見つけ、「アップロード」をクリックします。

   QRadar は、その文書を内部 XSD に照らして検証し、文書の妥当性を検査してから、拡張文書をシステムにアップロードします。

7. 「保存」をクリックしてウィンドウを閉じます。
8. ログ・ソース拡張をログ・ソースに関連付けます。
   a. 「管理」タブで「データ・ソース」 > 「ログ・ソース」をクリックします。
   b. 拡張文書の作成対象ログ・ソース・タイプをダブルクリックします。
   c. 「ログ・ソース拡張」リストから、作成した文書を選択します。
   d. 「保存」をクリックしてウィンドウを閉じます。

不明なイベントのマッピング

初期状態では、ユニバーサル DSM からのすべてのイベントが、QRadar の「ログ・アクティビティー」タブに「不明」と表示されます。手作業で、不明なすべてのイベントを QID マップの同等のものにマップする必要があります。

ログ・ファイルに表示すると、イベント名 (DROP、DENY、ACCEPT など) が分かりやすい値になっていることがありますが、QRadar は、これらの値が何を表すかを認識できません。QRadar にとってこれらの値は、既知のいずれの値にもマップされていないテキスト・ストリングです。これらの値は想定どおりに出力され、手作業でマップしない限り正規化イベントと見なされます。

侵入検知システム (IDS) や侵入検知防御システム (IDP) など、場合によっては数千件のイベントが存在し、そのマッピングが必要になります。このような場合には、イベント名そのものではなく、イベント名としてカテゴリーをマップすることができます。例えば以下の例では、マップの数を削減するために、イベント名に name フィールドを使用する代わりに category フィールドを使用しています。カスタム・プロパティーを使用すると、イベント名 (Code Red v412) を表示できます。

```
date: "Feb 25 2010 00:43:26"; name: "SQL Slammer v312"; category: "Worm
Activity"; source ip: "100.100.200.200";■date:
"Feb 25 2015 00:43:26"; name: "Code Red v412"; category: "Worm Activity";
source ip: "100.100.200.200"; date: "Feb 25 2015 00:43:26"; name:
"Annoying Toolbar"; category: "Malware"; source ip: "100.100.200.200";
```

イベント名に name フィールドを使用する代わりに、カテゴリー・フィールドを使用します。実際のイベント名 (Code Red v412 など) は、カスタム・プロパティーを使用して表示できます。

始める前に

ログ・ソース拡張文書をアップロードしてユニバーサル DSM に適用しておく必要があります。詳しくは、 63 ページの『QRadar への拡張文書のアップロード』を参照してください。

手順

1. 「ログ・アクティビティー」タブで「検索」 > 「検索の編集」をクリックします。
2. 「時刻範囲」オプションから、ログ・ソース拡張をユニバーサル DSM に適用してからの十分な経過時間 (例えば 15 分) を選択します。
3. 「検索パラメーター」で、「パラメーター」リストから「ログ・ソース **[索引] (Log Source [Index])**」を選択し、「演算子」リストから「次と等しい」を選択し、「ログ・ソース・グループ」および「ログ・ソース・リスト **(Log Source lists)**」から作成したログ・ソースを選択します。
4. 「検索」をクリックして結果を表示します。

   すべてのイベントが「不明」と表示されます。
5. 「不明」の項目をダブルクリックして、イベントの詳細を表示します。
6. ツールバーにある「イベントのマップ」をクリックします。

   値「ログ・ソースのイベント **ID**」に、ログ・ソース拡張にある「**EventName** 値 **(EventName value)**」 (DROP、DENY、ACCEPT など) が表示されます。この値が空白になることはありません。値が空白である場合は、ログ・ソース拡張文書にエラーがあります。
7. 「ログ・ソースのイベント **ID**」として表示された値を、適切な QID にマップします。

   「カテゴリー別に参照 **(Browse By Category)**」、「**QID** の検索」、またはこれら両方を使用して、「ログ・ソースのイベント **ID**」の値に最もよく一致する値を探します。例えば、値 DROP は「**QID** ファイアウォールの拒否 **-** イベント **CRE (QID Firewall Deny - Event CRE)**」にマップできます。

   名前に「イベント CRE」を持つ QID を使用してください。大部分のイベントは、特定のログ・ソース・タイプに固有のものです。例えば、ランダム・ファイアウォールにマップする場合、「拒否 **QID (Deny QID)**」は、ユニバーサル DSM を別のログ・ソース・タイプからのイベントにマップする処理に似ています。「イベント CRE」という名前を含む QID 項目は汎用のものであり、特定のログ・ソース・タイプには結合されません。
8. 不明なすべてのイベントが正常にマップされるまで、上記の手順を繰り返します。

   これ以降は、特定のログ・ソース・イベント ID を含むユニバーサル DSM からのすべてのイベントが、指定した QID として表示されます。QID マッピングより前に受信したイベントは「不明」のままになります。前のイベントを現在の QID にマップする手段はサポートされていません。不明なすべてのイベント・タイプが正常に QID にマップされるまで、この処理を繰り返す必要があります。

構文解析の問題と例

ログ・ソース拡張を作成するときに、構文解析の問題が発生する場合があります。以下の XML 例を使用して、具体的な構文解析の問題を解決していきます。

プロトコルの変換

ペイロードのいずれかの位置で TCP、UDP、ICMP、または GRE を検索する代表的なプロトコル変換を以下の例に示します。この検索パターンは、なんらかの単語境界 (タブ、スペース、行末など) で囲まれています。また、大文字と小文字の違いを無視しています。

```
<pattern id="Protocol" case-insensitive="true" xmlns="">
<![CDATA[¥b(TCP|UDP|ICMP|GRE)¥b]]>
</pattern>
<matcher field="Protocol" order="1" pattern-id="Protocol" capture-group="1" />
```

1 回の置換

送信元 IP アドレスを構文解析し、その結果をオーバーライドして IP アドレスを 100.100.100.100 に設定し、ペイロードにある IP アドレスを無視する置換を以下の例に示します。

この例では、送信元 IP アドレスが SrcAddress=10.3.111.33 のような形式であり、その後にコンマが続くと想定しています。

```
<pattern id="SourceIp_AuthenOK" xmlns="">
<![CDATA[SrcAddress=(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}),]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIp_AuthenOK"
capture-group="100.100.100.100" enable-substitutions="true"/>
```

コロン区切りの MAC アドレスの生成

QRadar は、コロン区切りの形式の MAC アドレスを検出します。すべてのデバイスがこの形式を使用するとは限らないため、以下の例では、その状況に対処する方法について説明します。

```
<pattern id="SourceMACWithDashes" xmlns="">
    <![CDATA[SourceMAC=([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-
    ([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})]]>
</pattern>
 <matcher field="SourceMAC" order="1" pattern-id="
    SourceMACWithDashes" capture-group="¥1:¥2:¥3:¥4:¥5:¥6" />
```

前記の例では、SourceMAC=12-34-56-78-90-AB を 12:34:56:78:90:AB の MAC アドレスに変換します。

パターンからダッシュを削除すると、そのパターンによって MAC アドレスが変換されます (区切り記号なしです)。スペースを挿入すると、パターンによってスペース区切りの MAC アドレスが変換されます。

IP アドレスとポートの結合

通常、IP アドレスとポートは 1 つのフィールドに結合され、コロンによって区切られます。

以下の例では、1 つのパターンで複数のキャプチャー・グループを使用しています。

```
pattern id="SourceIPColonPort" xmlns="">
<! [CDATA[Source=(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}):([¥d]{1,5})]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIPColonPort" capture-group="1" />
<matcher field="SourcePort" order="1" pattern-id="SourceIPColonPort" capture-group="2" />
```

イベント・カテゴリーの変更

デバイス・イベントのカテゴリーをハードコーディングしたり、重大度を調整したりすることができます。

以下の例では、単一のイベント・タイプを対象として重大度を調整します。

```
<event-match-single event-name="TheEvent" device-event-category="Actual
Category" severity="6" send-identity="UseDSMResults" />
```

アイデンティティー変更イベントの抑止

DSM は、アイデンティティー変更イベントを必要以上に送信する場合があります。

アイデンティティー変更イベントが単一のイベント・タイプおよびイベント・グループから送信されないように抑止する方法を以下の例に示します。

```
// Never send identity for the event with an EventName of Authen OK
<event-match-single event-name="Authen OK" device-event-category="ACS"
severity="6" send-identity="OverrideAndNeverSend" />

// Never send any identity for an event with an event name starting with 7,
followed by one to five other digits:
<pattern id="EventNameId" xmlns=""><![CDATA[(7¥d{1,5})]]>
</pattern>

<event-match-multiple pattern-id="EventNameId" capture-group-index="1"
device-event-category="Cisco Firewall" severity="7"
send-identity="OverrideAndNeverSend"/>
```

ログのエンコード

以下のエンコード形式がサポートされています。

- US-ASCII
- UTF-8

US-ASCII 形式にも UTF-8 形式にも合致しないエンコードのログをシステムに転送できます。拡張フラグを構成すると、構文解析および保管の目的で入力を UTF-8 に再エンコードできるようにすることが可能です。

例えば、ソース・ログを SHIFT-JIS (ANSI/OEM 日本語) エンコードで受信したい場合は、以下のコードを入力します。

```
<device-extension source-encoding=SHIFT-JIS xmlns=event_parsing/device_extension>
```

ログは UTF-8 形式で保管されます。

イベント日時スタンプの書式設定

ログ・ソース拡張は、イベントの各種の日時スタンプ形式を検出できます。

デバイスの製造元は標準的な日時スタンプの形式に従っていないため、ext-data というオプション・パラメーターをログ・ソース拡張に組み込んで、DeviceTime を書式設定し直せるようにします。イベントを書式設定し直して日時スタンプの形式を修正する方法を以下の例に示します。

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=¥[(¥d{2}/¥w{3}/¥d{4}:¥d{2}:¥d{2}:¥d{2})¥]</pattern>
<pattern id="Username">(TLSv1)</pattern>

<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1_Pattern" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1_Pattern"
   capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username_Pattern" capture-group="1"/>
</match-group>
</device-extension>
```

単一ログ・ソース内の複数のログ形式

場合によっては、単一のログ・ソース内に複数のログ形式が存在します。

```
May 20 17:15:50 kernel: DROP IN=vlan2 OUT= MAC= SRC=67.149.62.133
DST=239.255.255.250 PROTO=UDP SPT=1900 DPT=1900
May 20 17:16:26 dropbear[22331]: password auth succeeded for 'root' from 192.168.50.80:3364
May 20 17:16:28 dropbear[22331]: exit after auth (root): Exited normally </br>
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root' from 192.168.50.80:3364
```

例えば、ファイアウォール・イベントと認証イベントでログ形式が異なっているとします。このイベントを構文解析するには、複数のパターンを記述しなければなりません。構文解析する順序を指定できます。通常は、頻度の高いイベントを最初に構文解析し、その後に頻度の低いイベントを処理します。すべてのイベントを構文解析するために必要な数のパターンを記述することができます。order 変数により、パターンの比較順序が決定されます。

複数の形式を EventName フィールドと UserName フィールドに指定する例を以下に示します。

固有の各ログ・タイプを構文解析するために、個別のパターンを記述しています。正規化済みフィールドに値を割り当てるときに、両方のパターンが参照されます。

```
<pattern id="EventName-DDWRT-FW_Pattern" xmlns=""><![CDATA[kernel¥:¥s(.*?)¥s]]></pattern>
<pattern id="EventName-DDWRT-Auth_Pattern" xmlns=""><![CDATA[sdrophear¥[¥d{1,5}¥]|:¥s(.*?¥s.*?)¥s]]>
</pattern>

<pattern id="UserName_DDWRT-Auth1__Pattern" xmlns=""><![CDATA[¥sfor¥s¥'(.*?)¥'s]]></pattern>
<pattern id="UserName_DDWRT-Auth2__Pattern" xmlns=""><![CDATA[¥safter¥sauth¥s¥((.*?)¥)¥:]]></pattern>

<match-group order="1" description="DD-WRT Device Extensions xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-DDWRT-FW_Pattern" capture-group="1"/>
   <matcher field="EventName" order="2" pattern-id="EventName-DDWRT-Auth_Pattern" capture-group="1"/>

   <matcher field="UserName" order="1" pattern-id="UserName-DDWRT-Auth1_Pattern" capture-group="1"/>
   <matcher field="UserName" order="2" pattern-id="UserName-DDWRT-Auth2_Pattern" capture-group="1"/>
```

CSV ログ形式の構文解析

CSV 形式のログ・ファイルは、複数のキャプチャー・グループを持つ単一のパーサーを使用できます。このログ・タイプを構文解析する場合、必ずしも複数のパターン ID を作成する必要はありません。

このタスクについて

以下のログ・サンプルを使用します。

```
Event,User,Source IP,Source Port,Destination IP,Destination Port
Failed Login,bjones,192.168.50.100,1024,10.100.24.25,22
Successful Login,nlabadie,192.168.64.76,1743,10.100.24.25,110
Privilege Escalation,bjones,192.168.50.100,1028,10.100.1.100,23
```

手順

1. 前記のパターンを使用して、関連したすべての値に一致するパーサーを作成します。

   ```
   .*?¥,.*?¥,¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}
   ¥,¥d{1,5}¥,¥d{1,3}¥.¥d{1,3} ¥.¥d{1,3}¥.¥d{1,3}¥,¥d{1,5}
   ```

2. それぞれの値を囲むキャプチャー・グループを記述します。

   ```
   (.*?)\,(.*?)¥,(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.
   ¥d{1,3})¥,(¥d{1,5})¥,(¥d{1,3} ¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})¥,(¥d{1,5})
   ```

3. 各キャプチャー・グループのマップ先フィールドを、移動につれて値を増加させながらマップします。

   ```
   1 = Event, 2 = User, 3 = Source IP,
   4 = Source Port, 5 = Destination IP, 6 = Destination Port
   ```

4. キャプチャー・グループを関連イベントにマップすることによって、値をログ・ソース拡張に組み込みます。

   キャプチャー・グループから関連イベントへのマップ例の一部を以下のコードに示します。

   ```
   <pattern id="CSV-Parser_Pattern" xmlns=""><![CDATA 9.*?)\,(.*?)¥,(¥d{1,3}¥.¥{1,3}¥.{1,3}]]></pattern>
   <match-group order="1" description="Log Source Extension xmlns="">
      <matcher field="EventName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="1"/>
      <matcher field="SourceIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="3"/>
      <matcher field="SourcePort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="4"/>
      <matcher field="DestinationIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="5"/>
      <matcher field="DestinationPort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="6"/>
      <matcher field="UserName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="2"/>
   ```

5. ログ・ソース拡張をアップロードします。
6. イベントをマップします。

関連タスク:

64 ページの『不明なイベントのマッピング』

初期状態では、ユニバーサル DSM からのすべてのイベントが、QRadar の「ログ・アクティビティー」タブに「不明」と表示されます。手作業で、不明なすべてのイベントを QID マップの同等のものにマップする必要があります。

ログ・ソース・タイプの ID

IBM Security QRadar は多くのログ・ソースをサポートしており、各ログ・ソースには ID が割り当てられています。ログ・ソース・タイプ ID は `match-group` ステートメントで使用します。

サポートされるログ・ソース・タイプとその ID を以下の表に示します。

表 41. ログ・ソース・タイプの ID

ID	ログ・ソース・タイプ
2	Snort Open Source IDS

表 41. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
3	Check Point Firewall-1
4	構成可能なファイアウォール・フィルター
5	Juniper Networks ファイアウォールおよび VPN
6	Cisco PIX ファイアウォール
7	構成可能な認証メッセージ・フィルター
9	Enterasys Dragon Network IPS
10	Apache HTTP Server
11	Linux OS
12	Microsoft Windows Security Event Log
13	Windows IIS
14	Linux iptables ファイアウォール
15	IBM Proventia Network Intrusion Prevention System (IPS)
17	Juniper Networks 侵入検知防御 (IDP)
19	TippingPoint 侵入防止システム (IPS)
20	Cisco IOS
21	Nortel Contivity VPN スイッチ
22	Nortel Multiprotocol Router
23	Cisco VPN 3000 シリーズ・コンセントレーター
24	Solaris オペレーティング・システム認証メッセージ
25	McAfee IntruShield ネットワーク IPS アプライアンス
26	Cisco CSA
28	Enterasys Matrix E1 スイッチ
29	Solaris オペレーティング・システム sendmail ログ
30	Cisco 侵入防御システム (IDS)
31	Cisco ファイアウォール・サービス・モジュール (FWSM)
33	IBM Proventia Management SiteProtector
35	Cyberguard FW/VPN KS ファミリー
36	Juniper Networks Secure Access (SA) SSL VPN
37	Nortel Contivity VPN スイッチ
38	Top Layer 侵入防止システム (IPS)
39	ユニバーサル DSM
40	Tripwire Enterprise
41	Cisco Adaptive Security Appliance (ASA)

表 41. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager (NSM)
46	Squid Web プロキシー
47	Ambiron TrustWave ipAngel 侵入防止システム (IPS)
48	Oracle RDBMS 監査レコード
49	F5 Networks BIG-IP LTM
50	Solaris オペレーティング・システム DHCP ログ
55	Array Networks SSL VPN アクセス・ゲートウェイ
56	Catalyst スイッチ用 Cisco CatOS
57	ProFTPD サーバー
58	Linux DHCP サーバー
59	Juniper Networks Infranet Controller
64	Juniper JunOS プラットフォーム
68	Enterasys Matrix K/N/S シリーズ・スイッチ
70	Extreme Networks ExtremeWare オペレーティング・システム (OS)
71	Sidewinder G2 Security Appliance
73	Fortinet FortiGate セキュリティー・ゲートウェイ
78	SonicWall UTM/ファイアウォール/VPN デバイス
79	Vericept Content 360
82	Symantec Gateway Security (SGS) Appliance
83	Juniper Steel Belted Radius
85	IBM AIX サーバー
86	Metainfo MetaIP
87	SymantecSystemCenter
90	Cisco ACS
92	Forescout CounterACT
93	McAfee ePolicy Orchestrator
95	Cisco NAC アプライアンス
96	TippingPoint X シリーズ・アプライアンス
97	Microsoft DHCP サーバー
98	Microsoft IAS サーバー
99	Microsoft Exchange Server

表 41. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
100	Trend Interscan VirusWall
101	Microsoft SQL Server
102	MAC OS X
103	Bluecoat SG アプライアンス
104	Nortel Switched Firewall 6000
106	3Com 8800 シリーズ・スイッチ
107	Nortel VPN Gateway
108	Nortel Threat Protection System (TPS) Intrusion Sensor
110	Nortel Application Switch
111	Juniper DX アプリケーション・アクセラレーション・プラットフォーム
112	SNARE Reflector Server
113	Cisco 12000 シリーズ・ルーター
114	Cisco 6500 シリーズ・スイッチ
115	Cisco 7600 シリーズ・ルーター
116	Cisco Carrier Routing System
117	Cisco サービス統合型ルーター
118	Juniper M シリーズ・マルチサービス・エッジ・ルーター
120	Nortel Switched Firewall 5100
122	Juniper MX シリーズ・イーサネット・サービス・ルーター
123	Juniper T シリーズ・コア・プラットフォーム
134	Nortel イーサネット・ルーティング・スイッチ 8300/8600
135	Nortel イーサネット・ルーティング・スイッチ 2500/4500/5500
136	Nortel Secure Router
138	OpenBSD OS
139	Juniper Ex シリーズ・イーサネット・スイッチ
140	Sysmark Power Broker
141	Oracle データベース・リスナー
142	Samhain HIDS
143	Bridgewater Systems AAA サービス・コントローラー
144	名前と値のペア
145	Nortel Secure Network Access Switch (SNAS)
146	Starent Networks Home Agent (HA)

表 41. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
148	IBM AS/400 iSeries
149	Foundry Fastiron
150	Juniper SRX シリーズ・サービス・ゲートウェイ
153	CRYPTOCard CRYPTOShield
154	Imperva Securesphere
155	Aruba モビリティー・コントローラー
156	Enterasys NetsightASM
157	Enterasys HiGuard
158	Motorola SymbolAP
159	Enterasys HiPath
160	Symantec Endpoint Protection
161	IBM RACF
163	RSA Authentication Manager
164	Redback ASE
165	Trend Micro Office Scan
166	Enterasys XSR セキュリティー・ルーター
167	Enterasys スタック可能スイッチおよびスタンドアロン・スイッチ
168	Juniper Networks AVT
169	OS サービスの Qidmap
170	Enterasys A シリーズ
171	Enterasys B2 シリーズ
172	Enterasys B3 シリーズ
173	Enterasys C2 シリーズ
174	Enterasys C3 シリーズ
175	Enterasys D シリーズ
176	Enterasys G シリーズ
177	Enterasys I シリーズ
178	Trend Micro Control Manager
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module (WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	HP Tandem
188	Sentrigo Hedgehog
189	Sybase ASE
191	Microsoft ISA

表 41. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
192	Juniper SRC
193	Radware DefensePro
194	Cisco ACE Firewall
195	IBM DB2
196	Oracle Audit Vault
197	Cicso Firepower eStreamer (旧称 Sourcefire Defense Center)
198	Websense V Series
199	Oracle RDBMS OS 監査レコード
206	Palo Alto PA シリーズ
208	HP ProCurve
209	Microsoft Operations Manager
210	EMC VMWare
211	IBM WebSphere Application Server
213	F5 Networks BIG-IP ASM
214	FireEye
215	Fair Warning
216	IBM Informix
217	CA Top Secret
218	Enterasys NAC
219	System Center Operations Manager
220	McAfee Web Gateway
221	CA Access Control Facility (ACF2)
222	McAfee Application / Change Control
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Cyber-Ark Vault
228	Itron スマート・メーター
230	Bit9 Parity
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper Networks vGW
239	Oracle BEA WebLogic
240	Sophos Web セキュリティー・アプライアンス
241	Sophos Astaro Security Gateway

表 41. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
243	Infoblox NIOS
244	Tropos Control
245	Novell eDirectory
249	IBM Guardium
251	Stonesoft Management Center
252	SolarWinds Orion
254	Great Bay Beacon
255	Damballa Failsafe
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI
263	Digital China Networks DCS および DCRS シリーズ・スイッチ
264	Juniper Security Binary Log Collector
265	Trend Micro Deep Discovery
266	Tivoli Access Manager for e-business
268	Verdasys Digital Guardian
269	Huawei S シリーズ・スイッチ
271	HBGary Active Defense
272	APC UPS
272	Cisco Wireless LAN Controller
276	IBM Customer Information Control System (CICS)
278	Barracuda Spam & Virus Firewall
279	Open LDAP
280	Application Security DbProtect
281	Barracuda Web Application Firewall
283	Huawei AR シリーズ・ルーター
286	IBM AIX 監査
289	IBM Tivoli Endpoint Manager
290	Juniper Junos WebApp Secure
291	Nominum Vantio
292	Enterasys 800 シリーズ・スイッチ
293	IBM zSecure Alert
294	IBM Security Network Protection (XGS)
295	IBM Security Identity Manager
296	F5 Networks BIG-IP AFM
297	IBM Security Network IPS (GX)
298	Fidelis XPS

表 41. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
299	Arpeggio SIFT-IT
300	Barracuda Web Filter
302	Brocade FabricOS
303	ThreatGRID Malware Threat Intelligence Platform
304	IBM Security Access Manager for Enterprise Single Sign-On
306	Venustech Venusense Unified Threat Management
307	Venustech Venusense Firewall
308	Venustech Venusense Network Intrusion Prevention System
309	ObserveIT
311	Pirean Access: One
312	Venustech Venusense Security Platform
313	PostFix MailTransferAgent
314	Oracle ファイングレイン監査
315	VMware vCenter
316	Cisco Identity Services Engine
318	Honeycomb Lexicon File Integrity Monitor
319	Oracle Acme Packet SBC
320	Juniper 無線 LAN
330	Arbor Networks Peakflow SP
331	Zscaler Nss
332	Proofpoint Enterprise Protection/Enterprise Privacy
338	Microsoft Hyper-V
339	Cilasoft QJRN/400
340	Vormetric Data Security
341	SafeNet DataSecure/KeySecure
343	STEALTHbits StealthINTERCEPT
344	Juniper DDoS Secure
345	Arbor Networks Pravail
346	Trusteer Apex
348	IBM Security Directory Server
349	Enterasys A4 シリーズ
350	Enterasys B5 シリーズ
351	Enterasys C5 シリーズ
354	Avaya VPN Gateway
356	DG Technology MEAS
358	CloudPassage Halo

表 41. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
359	CorreLog Agent for IBM zOS
360	WatchGuard Fireware OS
361	IBM Fiberlink MaaS360
362	Trend Micro Deep Discovery Analyzer
363	AccessData InSight
364	IBM Privileged Session Recorder
367	Universal CEF
369	FreeRADIUS
370	Riverbed SteelCentral NetProfiler
372	SSH CryptoAuditor
373	IBM WebSphere DataPower
374	Symantec Critical System Protection
375	Kisco Information Systems SafeNet/i
376	IBM Federated Directory Server
378	Lastline Enterprise
379	genua genugate
383	Oracle Enterprise Manager

第 4 章 ログ・ソース拡張の管理

ログ・ソース拡張を作成すると、特定のデバイスの構文解析ルーチンを拡張したり変更したりすることができます。

ログ・ソース拡張 とは、イベント・ペイロードからのイベントを識別し分類するために必要な正規表現パターンをすべて格納している XML ファイルです。構文解析の問題を修正する必要がある場合や、DSM からのイベントに対するデフォルトの構文解析をオーバーライドする必要がある場合は、拡張ファイルを使用してイベントを構文解析できます。ネットワーク内のアプライアンスまたはセキュリティー・デバイスのイベントを構文解析する DSM が存在しないときは、拡張によってイベントのサポートを提供できます。「ログ・アクティビティー」タブには、以下の基本的なタイプのログ・ソース・イベントが示されます。

- イベントを適切に構文解析するログ・ソース。適切に構文解析されたイベントは、正しいログ・ソース・タイプおよびカテゴリーに割り当てられます。この場合は介入も拡張も不要です。
- イベントを構文解析したが、「ログ・ソース」パラメーターの値が「不明」であるログ・ソース。不明なイベントとは、ログ・ソース・タイプが識別されるが、DSM がペイロード情報を認識できないログ・ソース・イベントのことです。システムが、使用可能な情報からイベント ID を判別してイベントを適切に分類することができません。この場合は、イベントをカテゴリーにマップするか、ログ・ソース拡張を作成して不明なイベントに対するイベント構文解析を修復することができます。
- ログ・ソース・タイプを識別できず、「ログ・ソース」パラメーターの値が「保管」イベントであるログ・ソース。イベントが保管される場合は、DSM ファイルを更新するか、ログ・ソース拡張を作成してイベントを適切に構文解析する必要があります。イベントを構文解析すると、イベントをマップできます。

ログ・ソース拡張を追加するには、拡張文書を作成する必要があります。拡張文書は XML 文書であり、任意の一般的なワード・プロセッサーやテキスト編集アプリケーションで作成できます。複数の拡張文書を作成してアップロードし、さまざまなログ・ソース・タイプに関連付けることができます。拡張文書の形式は、標準の XML スキーマ文書 (XSD) に従わなければなりません。拡張文書を作成するには、XML のコーディングに関する知識と経験が必要です。

ログ・ソース拡張の追加

ログ・ソース拡張を追加すると、特定のデバイスの構文解析ルーチンを拡張したり変更したりすることができます。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース拡張」アイコンをクリックします。
3. 「追加」をクリックします。

4. 「ログ・ソース・タイプ」リストで、以下のいずれかのオプションを選択します。

オプション	説明
使用可能	このオプションは、デバイス・サポート・モジュール (DSM) がログ・ソースのほとんどのフィールドを正しく解析するときに選択します。正しく解析されないフィールドの値は、新しい XML 値で拡張されます。
次の項目のデフォルトに設定	拡張構文解析に追加するログ・ソース、または拡張構文解析から削除するログ・ソースを選択します。ログ・ソースに拡張を追加したり、ログ・ソースから拡張を削除したりすることができます。 ログ・ソース拡張がログ・ソースの「次の項目のデフォルトに設定」に設定されている場合は、同じ「ログ・ソース・タイプ」の新しいログ・ソースがその割り当てられたログ・ソース拡張を使用します。

5. 「参照」をクリックして、ログ・ソース拡張の XML 文書を見つけます。
6. 「アップロード」をクリックします。ログ・ソース拡張の内容が表示されます。適切な拡張ファイルをアップロードしようとしていることを確認します。ファイルのアップロード時には、拡張ファイルにエラーがないか XSD に照らして評価されます。
7. 「保存」をクリックします。

タスクの結果

拡張ファイルにエラーがない場合は、新しいログ・ソース拡張が作成されて有効になります。ログ・ソース拡張をログ・ソースに適用せずにアップロードすることができます。拡張の状況が変化すると、その内容が直ちに適用され、管理対象ホストまたはコンソールでログ・ソース拡張の新しいイベント構文解析パラメーターが適用されます。

次のタスク

「ログ・アクティビティー」タブで、イベントの構文解析パターンが正常に適用されていることを確認します。ログ・ソースがイベントを「保管」に分類している場合は、ログ・ソース拡張の構文解析パターンを調整する必要があります。ログ・ソース・イベントと拡張ファイルを照合することで、イベント構文解析の問題を特定することができます。

第 3 部 DSM

第 5 章 3Com Switch 8800

3Com Switch 8800 用の IBM Security QRadar DSM は、syslog を使用してイベントを受信します。

以下の表は、3Com Switch 8800 DSM の仕様を示しています。

仕様	値
製造元	3Com
DSM 名	Switch 8800 Series
RPM ファイル名	DSM-3ComSwitch_*qradar-version_build-number*.noarch.rpm
サポートされるバージョン	v3.01.30
プロトコル	Syslog
QRadar で記録されるイベント	状況イベントおよびネットワーク状況イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・イベント・プロパティーを含む?	いいえ
その他の情報	3Com Web サイト (http://www.3com.com)

3COM Switch 8800 イベントを QRadarに送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新の 3COM Switch 8800 RPM をダウンロードして QRadar コンソールにインストールしてください。
2. QRadar と通信するように各 3COM Switch 8800 インスタンスを構成します。
3. QRadar が DSM を自動的に検出しない場合、3COM Switch 8800 インスタンスごとに QRadar コンソールでログ・ソースを作成します。すべての必須パラメーターを構成します。固有の値については、以下の表を使用してください。

パラメーター	説明
ログ・ソース・タイプ	3COM Switch 8800
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

84 ページの『3COM Switch 8800 の構成』
Syslog イベントを IBM Security QRadarに転送するように 3COM Switch 8800 を構成します。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプラ

イアンスからイベントを受信するログ・ソースを手動で追加できます。

3COM Switch 8800 の構成

Syslog イベントを IBM Security QRadarに転送するように 3COM Switch 8800 を構成します。

手順

1. 3COM Switch 8800 にログインします。
2. インフォメーション・センターを有効にするために、以下のコマンドを入力します。

   ```
   info-center enable
   ```

3. ログ・ホストを構成するために、以下のコマンドを入力します。

   ```
   info-center loghost QRadar_ip_address facility informational language english
   ```

4. ARP および IP 情報モジュールを構成するために、以下のコマンドを入力します。

   ```
   info-center source arp channel loghost log level informational
   info-center source ip channel loghost log level informational
   ```

第 6 章 AhnLab Policy Center

AhnLab Policy Center 用の IBM Security QRadar DSM は、AhnLab Policy Center がログを保管するために使用している DB2® データベースから、イベントを取得します。

以下の表は、AhnLab Policy Center DSM の仕様を示しています。

表 *42. AhnLab Policy Center DSM* の仕様

仕様	値
製造元	AhnLab
DSM	AhnLab Policy Center
RPM ファイル名	DSM-AhnLabPolicyCenter-*QRadar-Release_Build-Number*.noarch.rpm
サポートされるバージョン	4.0
プロトコル	AhnLabPolicyCenterJdbc
QRadar で記録されるイベント	スパイウェア検出、ウィルス検出、監査
自動的に検出?	いいえ
ID を含む?	はい
その他の情報	Ahnlab Web サイト (https://global.ahnlab.com/)

AhnLab Policy Center DSM を QRadar に統合するには、以下のステップを実行します。

1. 以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - JDBC プロトコル RPM
   - AhnLabPolicyCenterJdbc プロトコル RPM
   - AhnLab Policy Center RPM

   ヒント**:** 詳しくは、DB2 の資料を参照してください。
2. ご使用の AhnLab Policy Center システムが、以下の基準を満たすことを確認してください。
   - DB2 データベースが QRadar からの接続を許可すること。
   - AhnLabPolicyCenterJdbc プロトコル用のポートが、DB2 データベースのリスナー・ポートと一致すること。
   - DB2 データベース上の着信 TCP 接続が、QRadar との通信用に有効にされていること。
3. 統合する AhnLab Policy Center サーバーごとに、QRadar コンソール上でログ・ソースを作成します。以下の表は、Ahnlab 固有のプロトコル値を示しています。

パラメーター	値
ログ・ソース・タイプ	AhnLab Policy Center APC
プロトコル構成	AhnLabPolicyCenterJdbc
アクセス資格情報 (Access credentials)	DB2 サーバーのアクセス資格情報を使用します。
ログ・ソース言語	QRadar v7.2 以降を使用している場合は、ログ・ソース言語を選択する必要があります。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 7 章 Akamai Kona

Akamai KONA 用の IBM Security QRadar DSM は、Akamai KONA サーバーからイベント・ログを収集します。

以下の表は、Akamai KONA DSM の仕様を示しています。

表 43. *Akamai KONA DSM* の仕様

仕様	値
製造元	Akamai
製品	Kona
DSM RPM 名	DSM-AkamaiKona-*QRadar_Version-Build_Number*.noarch.rpm
プロトコル	HTTP レシーバー
QRadar で記録されるイベント	警告ルール・イベント 拒否ルール・イベント
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Akamai Web サイト (http://www.akamai.com/)

Akamai KONA イベントを QRadar に送信するには、以下のステップを実行します。

制約事項: この統合では、受信 Akamai 接続用にファイアウォールで非標準ポートを開く必要があります。受信 Akamai 接続のルーティングには、内部プロキシーを使用します。Akamai データ・ストリームを直接 QRadar コンソールに向けないでください。ファイアウォールで非標準ポートを開く方法について詳しくは、ネットワーク・セキュリティーの担当者に相談してください。

1. 自動更新が有効になっていない場合は、以下の最新バージョンの各 RPM をダウンロードして、QRadar コンソールにインストールします。
   - DSMCommon RPM
   - HTTPReceiver プロトコル RPM
   - Akamai KONA RPM
2. Akamai KONA の各インスタンスで、QRadar と通信するように Akamai KONA システムを 構成します。詳しくは、Akamai にお問い合わせください。
3. 「**HTTPS**」オプションおよび「クライアント認証 **(Client Authentication)**」オプションを使用するようにログ・ソースを構成する場合、Akamai KONA 証明書をターゲット QRadar イベント・コレクター (Event Collector)にコピーします。

4. 統合対象の Akamai KONA サーバーごとに、QRadar コンソールでログ・ソースを作成します。すべての必須パラメーターを構成します。Akamai Kona 固有のパラメーターを構成する際には、以下の表を使用してください。

表 *44. Akamai KONA* ログ・ソース・パラメーター

パラメーター	説明
クライアント証明書パス (Client Certificate Path)	ターゲット QRadar イベント・コレクター (Event Collector)上のクライアント証明書の絶対ファイル・パス。 Akamai KONA 証明書が既にイベント・コレクターにコピーされていることを確認してください。 「**HTTPS**」オプションおよび「クライアント認証 **(Client Authentication)**」オプションを「通信タイプ」リストから選択する場合、**「クライアント証明書パス (Client Certificate Path)」**パラメーターは必須です。
Listen ポート	Akamai KONA システム上に構成された宛先ポート
メッセージ・パターン	`'¥{"type'` は、JSON 形式イベントの**メッセージ・パターン**です。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 8 章 Amazon AWS CloudTrail

IBM Security QRadar DSM for Amazon AWS CloudTrail は、Amazon AWS CloudTrail S3 バケットから監査イベントを収集します。

Amazon AWS CloudTrail DSM の仕様を以下の表に示します。

表 45. *Amazon AWS CloudTrail DSM* の仕様

仕様	値
製造元	Amazon
DSM	Amazon AWS CloudTrail
RPM 名	DSM-AmazonAWSCloudTrail-*QRadar_version-Build_number*.noarch.rpm
サポートされるバージョン	N/A
プロトコル	Amazon AWS S3 REST API
QRadar で記録されるイベント	すべてのバージョン (1.0、1.02、1.03、1.04) のイベント。
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Amazon Cloud Trail の資料 (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/whatisawscloudtrail.html)

Amazon AWS CloudTrail を QRadar に統合するには、以下のステップを実行します。

1. QRadar が Amazon AWS CloudTrail S3 バケットと通信できるようにするための証明書を取得してインストールします。
2. Amazon AWS Identity and Access Management (IAM) ユーザーを作成し、**AmazonS3ReadOnlyAccess** ポリシーを適用します。
3. 以下に示す RPM の最新バージョンを QRadar コンソールにインストールします。
   - プロトコル共通
   - Amazon AWS REST API プロトコル RPM
   - Amazon AWS CloudTrail DSM RPM
4. 「管理」タブをクリックします。
5. 「ログ・ソース」アイコンをクリックします。
6. ナビゲーション・メニューの「追加」をクリックします。
7. QRadar で Amazon AWS CloudTrail ログ・ソースを構成します。すべての必須パラメーターを構成します。以下の表を参考に、Amazon AWS CloudTrail パラメーターの値を決定してください。

表 *46. Amazon AWS CloudTrail* ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース・タイプ	**Amazon AWS CloudTrail**
プロトコル構成	**Amazon AWS S3 REST API**
ログ・ソース ID	ログ・ソースの固有名を入力します。 「ログ・ソース **ID**」には、任意の有効な値を使用でき、特定のサーバーを参照する必要はありません。「ログ・ソース **ID**」は、「ログ・ソース名」と同じ値にすることもできます。複数の Amazon AWS CloudTrail ログ・ソースが構成済みの場合は、最初のログ・ソースを *awscloudtrail1*、2 番目のログ・ソースを *awscloudtrail2*、3 番目のログ・ソースを *awscloudtrail3* として識別できます。
シグニチャー・バージョン	「シグニチャー・バージョン **2 (Signature Version 2)**」または「シグニチャー・バージョン **4 (Signature Version 4)**」 を選択します。 「シグニチャー・バージョン **2 (Signature Version 2)**」では、Amazon AWS の一部のリージョンがサポートされていません。「シグニチャー・バージョン **4 (Signature Version 4)**」のみをサポートするリージョンを使用する場合は、リストで「シグニチャー・バージョン **4 (Signature Version 4)**」を選択する必要があります。
リージョン名	Amazon S3 バケットに関連付けられたリージョン。
サービス名	Amazon Web サービスの名前。
バケット名 (Bucket Name)	ログ・ファイルが格納されている AWS S3 バケットの名前。
アクセス・キー (Access Key)	AWS S3 バケットにアクセスするために必要な公開アクセス・キー。
秘密鍵 (Secret Key)	AWS S3 バケットにアクセスするために必要な秘密アクセス・キー。
プロキシーの使用 (Use Proxy)	プロキシーが構成されている場合は、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Amazon AWS S3 バケットにアクセスします。 「プロキシー・サーバー」、「プロキシー・ポート」、「プロキシー・ユーザー名」、「プロキシー・パスワード」の各フィールドを構成します。プロキシーが認証を必要としない場合、「プロキシー・ユーザー名」フィールドと「プロキシー・パスワード」フィールドはブランクのままでかまいません。

表 46. *Amazon AWS CloudTrail* ログ・ソース・パラメーター (続き)

パラメーター	説明
ディレクトリー接頭部 (Directory Prefix)	CloudTrail ログの取得元である AWS S3 バケットでのルート・ディレクトリーの場所 (例: AWSLogs/<*AccountNumber*>/CloudTrail/us-east-1/)。
ファイル・パターン	.*?¥.json¥.gz
繰り返し (Recurrence)	AWS S3 REST API プロトコルが、新規ファイルの有無を確認して (存在する場合は) 取得するために Amazon クラウド API に接続する頻度。AWS S3 バケットにアクセスするたびに、バケットを所有するアカウントに対してコストが発生します。このため、繰り返しの値を小さくするとコストが上昇します。

8. ログ・ソースの構成に必要な値が入力されたら、「保存」をクリックします。

Amazon AWS CloudTrail DSM のサンプル・イベント・メッセージを次の表に示します。

表 47. *Amazon AWS CloudTrail* によってサポートされる *Amazon AWS CloudTrail* サンプル・メッセージ。

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
コンソール・ログイン	一般監査イベント	{"eventVersion":"1.02", "userIdentity":{"type":"IAMUser", "principalId":"AIDAI56UNJ5SGCUDUOZEE", "arn":"arn:aws:iam::005166929:user/xx.xxccountId": "05166929","userName":"x.x"},"eventTime": "2016-05-04T14:10:58Z","eventSource": "f.amazonaws.com","eventName": "ConsoleLogin","awsRegion": "us-east-1","sourceIPAddress": "1.1.1.1 Agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.1.1 Safari/537.36", "requestParameters":null, "responseElements": {"ConsoleLogin":"Success"}, "additionalEventData": {"LoginTo":"www.webpage.com", "MobileVersion":"No","MFAUsed":"No"}, "eventID":"e1866735-ea8b-4e66-be1a-8067dafe9898", "eventType":"AwsConsoleSignIn", "recipientAccountId":"237005166922"}

Amazon AWS CloudTrail と QRadar の統合に関するトラブルシューティング

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

『IBM Security QRadar と AWS CloudTrail の間の通信の有効化』
QRadar と Amazon AWS CloudTrail の間の HTTP 接続には証明書が必要です。

95 ページの『QRadar との通信のための Amazon AWS CloudTrail の構成』
Amazon 管理者は、Amazon AWS ユーザー・インターフェースでユーザーを作成し、**AmazonS3ReadOnlyAccess** ポリシーを適用する必要があります。これにより、QRadar ユーザーは QRadar でログ・ソースを作成できるようになります。

IBM Security QRadar と AWS CloudTrail の間の通信の有効化

QRadar と Amazon AWS CloudTrail の間の HTTP 接続には証明書が必要です。

手順

1. Amazon AWS CloudTrail S3 バケットにアクセスします。
2. 証明書を DER エンコードのバイナリー証明書としてデスクトップ・システムにエクスポートします。ファイル拡張子は `.DER` でなければなりません。
3. ログ・ソースを構成する予定の QRadar ホスト上の `/opt/QRadar/conf/trusted_certificates` ディレクトリーに証明書をコピーします。

Amazon AWS CloudTrail イベントの受信確認

Amazon AWS CloudTrail S3 バケットからイベント・データを収集していることを確認できます。

手順

1. 管理者として QRadar にログインします。
2. 「ログ・アクティビティー」タブをクリックします。
3. 「フィルターの追加」をクリックします。
4. 「ログ・ソース **[索引](Log Source [Indexed])**」 > 「次と等しい」を選択し、Amazon AWS CloudTrail ログ・ソースの名前を参照します。
5. 「フィルターの追加」をクリックします。
6. 「表示」メニューから、「過去 **15** 分間」または「最後の間隔」を選択します。

タスクの結果

ログ・ソースのパラメーターが正しい場合は、Amazon AWS CloudTrail で Amazon AWS エコシステムから取得したイベントが表示されるはずです。

関連情報:

Amazon AWS CloudTrail の資料 (www.amazon.com)

QRadar: Unable to integrate with Amazon AWS CloudTrail (www.ibm.com/support)

QRadar: Troubleshooting Amazon AWS CloudTrail

Amazon AWS ログ・ソースの統合に関するトラブルシューティング

Amazon AWS ログを収集するように QRadar でログ・ソースを構成しましたが、ログ・ソースのステータスが警告となり、イベントが予期したとおりに生成されません。

症状:

/var/log/qradar.error に示されるエラー:

```
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider2
9154] com.q1labs.semsources.sources.amazonawsrest.utils.web.SimpleRESTFileLister:
[ERROR] [NOT:0000003000]
[x.x.x.x/- -] [-/- -]IOException encountered when trying to list files
from remote Amazon S3 bucket.
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider2
9154] javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException:
Server certificate not recognized
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider2
9154] at com.ibm.jsse2.j.a(j.java:15)
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider2
9154] at com.ibm.jsse2.qc.a(qc.java:728)
```

原因:

このエラーは、正しくない URL から Amazon SSL 証明書をエクスポートしたことが原因と考えられます。

環境:

すべての QRadar バージョン。

問題の診断:

ホワイトリストにある証明書が、接続時に提供されたサーバー証明書と交差していないことを確認してください。Amazon から送信されるサーバー証明書は *.s3.amazonaws.com ドメインを対象とします。お客様は以下の URL の証明書をエクスポートする必要があります。

```
https://<bucketname>.s3.amazonaws.com
```

QRadar のスタック・トレースには、Amazon AWS S3 REST API プロトコルの問題が示されています。以下の例では、QRadar が認証されていない証明書を拒否しています。最も一般的な原因は、証明書が正しい形式でないか、適切な QRadar アプライアンスの適切なディレクトリーに配置されていないことです。

```
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -]
Rejecting SSL/TLS connection because server presented unrecognized certificate.
The chain sent by the server is
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -] Subject =
CN=*.s3.amazonaws.com, O=Amazon.com Inc., L=Seattle, ST=Washington, C=US
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -] Subject =
CN=q1.us.ibm.com, OU=IBM, O=IBM, L=John, ST=Doe, C=IN, EMAILADDRESS=jdoe@us.ibm.com
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -]The current certificate white list is:
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -]
Subject = EMAILADDRESS=q1sales@us.ibm.com,
O=IBM Corp, L=Waltham, ST=Massachusetts, C=US
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -] Subject = O=SyslogTLS_Server, CN=*
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -]
Subject = CN=s3-console-us-standard.console.aws.amazon.com,
O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class
com.q1labs.semsources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN]
[NOT:0000004000][x.x.x.x/- -] [-/- -] To establish trust in this server certificate,
place a copy in /opt/qradar/conf/trusted_certificates
```

問題の解決方法:

.DER 証明書ファイルを正しい QRadar アプライアンスに移動する必要があります。正しい QRadar アプライアンスは、Amazon AWS CloudTrail ログ・ソースの「ターゲット・イベント・コレクター」フィールドで割り当てられています。

注:

証明書の拡張子は .DER である必要があります。.DER 拡張子は大文字と小文字が区別され、大文字である必要があります。小文字の証明書がエクスポートされると、ログ・ソースでイベント・コレクションの問題が発生する場合があります。

1. https://<bucketname>.s3.amazonaws.com の AWS CloudTrail S3 バケットにアクセスします。
2. Firefox を使用して、DER 証明書ファイルとして AWS から SSL 証明書をエクスポートします。Firefox では、.DER 拡張子の必要な証明書を作成することができます。

3. Amazon AWS CloudTrail ログ・ソースを管理する QRadar アプライアンス上の /opt/qradar/conf/trusted_certificates ディレクトリーに DER 証明書ファイルをコピーします。

   注: ログ・ソースを管理する QRadar アプライアンスは、Amazon AWS CloudTrail ログ・ソースの「ターゲット・イベント・コレクター」フィールドで識別されます。Amazon AWS CloudTrail ログ・ソースを管理する QRadar アプライアンスの /opt/qradar/conf/trusted_certificates フォルダーには DER 証明書ファイルのコピーがあります。
4. 管理者として QRadar にログインします。
5. 「管理」タブをクリックします。
6. 「ログ・ソース」アイコンをクリックします。
7. 「**Amazon AWS CloudTrail**」ログ・ソースを選択します。
8. ナビゲーション・メニューで、「有効化/無効化」をクリックして無効にしてから Amazon AWS CloudTrail ログ・ソースを再度有効にします。

   注: ログ・ソースを強制的に無効な状態から有効な状態にすると、ログ・ソースに定義されている Amazon AWS バケットにプロトコルが接続されます。最初の通信時に証明書チェックが行われます。
9. 問題が解決しない場合は、「ログ・ソース ID」フィールドの Amazon AWS バケット名が正しいことを確認します。ログ・ソース構成のリモート・ディレクトリー・パスが正しいことを確認してください。

QRadar との通信のための Amazon AWS CloudTrail の構成

Amazon 管理者は、Amazon AWS ユーザー・インターフェースでユーザーを作成し、**AmazonS3ReadOnlyAccess** ポリシーを適用する必要があります。これにより、QRadar ユーザーは QRadar でログ・ソースを作成できるようになります。

手順

1. ユーザーを作成します。
   a. Amazon AWS ユーザー・インターフェースに管理者としてログインします。
   b. Amazon AWS IAM ユーザーを作成し、**AmazonS3ReadOnlyAccess** ポリシーを適用します。
2. QRadar でログ・ソースを構成するために使用する S3 バケット名とディレクトリー接頭部を見つけます。
   a. 「サービス」をクリックします。
   b. リストで「**CloudTrail**」を選択します。
   c. 「証跡 (Trails)」ページで、証跡の名前をクリックします。
   d. 「**S3 バケット (S3 bucket)**」フィールドに表示される S3 バケットの名前をメモします。
   e. ウィンドウの右側の鉛筆アイコンをクリックします。
   f. 「詳細 **(Advanced)**」**>>**をクリックします。

g. 「ログ・ファイル接頭部 **(Log file prefix)**」フィールドの下に表示される S3 バケットのロケーション・パスをメモします。

次のタスク

QRadar ユーザーが QRadar でログ・ソースを構成する準備ができました。S3 バケット名は、「バケット名 **(Bucket name)**」フィールドの値になります。S3 バケットのロケーション・パスは、「ディレクトリー接頭部 **(Directory Prefix)**」フィールドの値になります。

第 9 章 Ambiron TrustWave ipAngel

IBM Security QRadar DSM for Ambiron TrustWave ipAngel は、ipAngel コンソールから Snort ベースのイベントを受信します。

以下の表は、Ambiron TrustWave ipAngel DSM の仕様を示しています。

表 *48. Ambiron TrustWave ipAngel DSM* の仕様

仕様	値
製造元	Ambiron
DSM 名	Ambiron TrustWave ipAngel
RPM ファイル名	`DSM-AmbironTrustwaveIpAngel-`*`QRadar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	V4.0
プロトコル	Syslog
記録されるイベント・タイプ	Snort ベースのイベント
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Ambiron Web サイト (http://www.apache.org)

Ambiron TrustWave ipAngel イベントを QRadar に送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Ambiron TrustWave ipAngel DSM RPM をダウンロードして QRadar コンソールにインストールしてください。
2. キャッシュおよびアクセス・ログを QRadarに転送するように Ambiron TrustWave ipAngel デバイスを構成します。QRadar へのデバイス・ログの転送について詳しくは、ベンダーの資料を参照してください。
3. QRadar コンソールで Ambiron TrustWave ipAngel ログ・ソースを追加します。以下の表は、固有の値を必要とするパラメーターを示しています。Ambiron TrustWave ipAngel イベントを収集するには、これらの値が必要です。

表 *49. Ambiron TrustWave ipAngel* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Ambiron TrustWave ipAngel 侵入防止システム (IPS)
プロトコル構成	Syslog

第 10 章 APC UPS

IBM Security QRadar DSM for APC UPS は、APC Smart-Uninterruptible Power Supply (UPS) ファミリーの製品から Syslog イベントを受け取ります。

制約事項: RC-Series Smart-UPS からのイベントはサポートされていません。

以下の表は、APC UPS DSM の仕様を示しています。

表 *50. APC UPS DSM* の仕様

仕様	値
製造元	APC
DSM 名	APC UPS
RPM ファイル名	DSM-APCUPS-*Qradar_version-build_number*.noarch.rpm
プロトコル	Syslog
記録されるイベント・タイプ	UPS イベント バッテリー・イベント バイパス・イベント 通信イベント 入力電源イベント 低バッテリー状態イベント SmartBoost イベント SmartTrim イベント
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	APC Web サイト (http://www.apc.com)

APC UPS イベントを QRadar に送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの APC UPS DSM RPM をダウンロードして QRadar コンソールにインストールしてください。
2. QRadar コンソールで APC UPS ログ・ソースを作成します。すべての必須パラメーターを構成します。以下の表を使用して、APC UPS イベントの収集に必要な固有の値を構成していください。

表 *51. APC UPS* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	APC UPS
プロトコル構成	Syslog

3. Syslog イベントを QRadar に転送するように APC UPS デバイスを構成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

『Syslog イベントを転送するように APC UPS を構成』
APC UPS からイベントを収集するには、Syslog イベントを IBM Security QRadar に転送するようにデバイスを構成する必要があります。

Syslog イベントを転送するように APC UPS を構成

APC UPS からイベントを収集するには、Syslog イベントを IBM Security QRadar に転送するようにデバイスを構成する必要があります。

手順

1. APC Smart-UPS Web インターフェースにログインします。
2. ナビゲーション・メニューで、「ネットワーク」>「**Syslog**」をクリックします。
3. 「**Syslog**」リストから「有効」を選択します。
4. 「ファシリティー **(Facility)**」リストから、Syslog メッセージのファシリティー・レベルを選択します。
5. 「**Syslog** サーバー **(Syslog Server)**」フィールドに、QRadar コンソールまたはイベント・コレクターの IP アドレスを入力します。
6. 「重大度」リストから「通知」を選択します。
7. 「適用」をクリックします。

第 11 章 Apache HTTP Server

IBM Security QRadar 用の Apache HTTP Server DSM は、syslog または syslog-ng を使用して Apache イベントを受け入れます。

QRadar は、関連するすべての HTTP 状況イベントを記録します。以下の手順は、UNIX/Linux オペレーティング・システム上で稼動する Apache DSM にのみ該当します。

syslog と syslog-ng の両方を同時に実行しないでください。

以下の構成方法のいずれかを選択します。

- 『syslog での Apache HTTP Server の構成』
- 103 ページの『syslog-ng での Apache HTTP Server の構成』

syslog での Apache HTTP Server の構成

syslog プロトコルでイベントを転送するように Apache HTTP Server を構成できます。

手順

1. Apache をホストしているサーバーに root ユーザーとしてログインします。
2. Apache 構成ファイル `httpd.conf` を編集します。
3. Apache 構成ファイルに以下の情報を追加し、カスタム・ログ・フォーマットを指定します。

   ```
   LogFormat "%h %A %l %u %t ¥"%r¥" %>s %p %b" <log format name>
   ```

   ここで、*<log format name>* は、ログ・フォーマットを定義するために指定する変数名です。
4. Apache 構成ファイルに以下の情報を追加し、syslog イベントのカスタム・パスを指定します。

   ```
   CustomLog "|/usr/bin/logger -t httpd -p <facility>.<priority>" <log
   format name>
   ```

   各部分について以下で説明します。

   - *<facility>* は、syslog ファシリティーです (例えば、local0)。
   - *<priority>* は、syslog 優先順位です (例えば、info や notice)。
   - *<log format name>* は、カスタム・ログ・フォーマットを定義するために指定する変数名です。ログ・フォーマット名は、『syslog での Apache HTTP Server の構成』で定義したログ・フォーマットに一致する必要があります。

   例:

```
CustomLog "|/usr/bin/logger -t httpd -p local1.info" MyApacheLogs
```

5. 以下のコマンドを入力して *hostname* ルックアップを無効にします。

```
HostnameLookups off
```

6. Apache 構成ファイルを保存します。
7. syslog 構成ファイルを編集します。

```
/etc/syslog.conf
```

8. 以下の情報を syslog 構成ファイルに追加します。

```
<facility>.<priority> <TAB><TAB>@<host>
```

各部分について以下で説明します。

- *<facility>* は、syslog ファシリティーです (例えば、local0)。この値は、101 ページの『syslog での Apache HTTP Server の構成』で入力した値に一致する必要があります。
- *<priority>* は、syslog の優先順位です (例: info または notice)。この値は、 101 ページの『syslog での Apache HTTP Server の構成』で入力した値に一致する必要があります。
- <TAB> は、**Tab** キーを押す必要があることを示します。
- *<host>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。

9. syslog 構成ファイルを保存します。
10. 以下のコマンドを入力して syslog サービスを再始動します。

```
/etc/init.d/syslog restart
```

11. Apache を再始動して syslog 構成を完了します。

構成は完了です。Apache HTTP Server からの syslog イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Apache HTTP Server によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

IBM Security QRadar でログ・ソースを構成する

IBM Security QRadar で Apache HTTP Server イベントのログ・ソースを手動で構成できます。

このタスクについて

QRadar は、Apache HTTP Server からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ただし、QRadar 用のログ・ソースを手動で作成して syslog イベントを受信することもできます。以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。

3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Apache HTTP Server**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 52. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Apache インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックしてください。

構成は完了です。Apache について詳しくは、http://www.apache.org/ を参照してください。

syslog-ng での Apache HTTP Server の構成

syslog-ng プロトコルでイベントを転送するように Apache HTTP Server を構成できます。

手順

1. Apache をホストしているサーバーに root ユーザーとしてログインします。
2. Apache 構成ファイルを編集します。

   ```
   /etc/httpd/conf/httpd.conf
   ```

3. Apache 構成ファイルに以下の情報を追加し、**LogLevel** を指定します。

   ```
   LogLevel info
   ```

   LogLevel は既に info レベルに構成されていることがあります。これは、ご使用の Apache インストール済み環境によって異なります。
4. Apache 構成ファイルに以下を追加し、カスタム・ログ・フォーマットを指定します。

   ```
   LogFormat "%h %A %l %u %t ¥"%r¥" %>s %p %b" <log format name>
   ```

   ここで、*<log format name>* は、カスタム・ログ・フォーマットを定義するために指定する変数名です。
5. Apache 構成ファイルに以下の情報を追加し、syslog イベントのカスタム・パスを指定します。

```
CustomLog "|/usr/bin/logger -t 'httpd' -u /var/log/httpd/
apache_log.socket" <log format name>
```

ログ・フォーマット名は、 103 ページの『syslog-ng での Apache HTTP Server の構成』で定義したログ・フォーマットに一致する必要があります。

6. Apache 構成ファイルを保存します。
7. syslog-ng 構成ファイルを編集します。

```
/etc/syslog-ng/syslog-ng.conf
```

8. syslog-ng ファイルで以下の情報を追加して、宛先を指定します。

```
source s_apache {
              unix-stream("/var/log/httpd/apache_log.socket"
              max-connections(512)
              keep-alive(yes));
};
destination auth_destination { <udp|tcp> ("<IP address>" port(514)); };
log{
    source(s_apache);
    destination(auth_destination);
};
```

各部分について以下で説明します。

<IP address> は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。

<udp|tcp> は、syslog イベントを転送するために選択したプロトコルです。

9. syslog-ng 構成ファイルを保存します。
10. 以下のコマンドを入力して syslog-ng を再始動します。

```
service syslog-ng restart
```

11. これで、QRadar でログ・ソースを構成できるようになりました。

構成は完了です。Apache HTTP Server からの syslog イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Apache HTTP Server によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar で Apache HTTP Server イベントのログ・ソースを手動で構成できます。

このタスクについて

QRadar は、Apache HTTP Server からの syslog-ng イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ただし、QRadar 用のログ・ソースを手動で作成して syslog イベントを受信することもできます。以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Apache HTTP Server**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *53. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Apache インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックしてください。

構成は完了です。Apache について詳しくは、http://www.apache.org/ を参照してください。

第 12 章 Apple Mac OS X

Apple Mac OS X 用の IBM Security QRadar DSM は、syslog を使用してイベントを受け入れます。

QRadar は、関連するファイアウォール、Web サーバー・アクセス、Web サーバー・エラー、特権のエスカレーション、および通知イベントをすべて記録します。

Mac OS X イベントを QRadar と統合するには、syslog イベントを受信するログ・ソースを手動で作成する必要があります。

この統合を行うには、まずログ・ソースを構成し、その後で syslog イベントを転送するように Mac OS X を構成する必要があります。Mac OS X デバイスから転送される syslog イベントは自動的に検出されません。Mac OS X からの syslog イベントは、TCP ポート 514 上または UDP ポート 514 上の QRadar に転送できます。

Mac OS X ログ・ソースの構成

IBM Security QRadar では、Apple Mac OS X から転送された Syslog イベントのログ・ソースの検出または作成は自動的に実行されません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Mac OS X**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 「ログ・ソース **ID**」フィールドに、Apple Mac OS X デバイスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。これで、QRadar に Syslog イベントを転送するように Apple Mac OS X デバイスを構成する準備ができました。

Apple Mac OS X での Syslog の構成

Mac OS X オペレーティング・システムが稼働するシステムで syslog を構成できます。

手順

1. SSH を使用して、root ユーザーとして Mac OS X デバイスにログインします。
2. /etc/syslog.conf ファイルを開きます。
3. このファイルの先頭に以下の行を追加します。それ以外の行は変更しないでください。

   ```
   *.* @QRadar_IP_address
   ```

4. ファイルを保存して終了します。
5. ハングアップ・シグナルを syslog デーモンに送信して、すべての変更が確実に適用されるようにします。

   ```
   sudo killall - HUP syslogd
   ```

   syslog の構成は完了です。Apple Mac OS X により IBM Security QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

   Mac OS X の構成について詳しくは、Mac OS X のベンダー資料を参照してください。

第 13 章 Application Security DbProtect

Application Security DbProtect 用の IBM Security QRadar DSM は、インストール済みの DbProtect デバイスから、ログ・イベント拡張フォーマット (LEEF) サービスを使用してイベントを収集します。

以下の表は、Application Security DbProtect DSM の仕様を示しています。

表 54. *Application Security DbProtect DSM* の仕様

仕様	値
製造元	Application Security, Inc
DSM 名	DbProtect
RPM ファイル名	DSM-AppSecDbProtect-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	v6.2 v6.3 v6.3sp1 v6.3.1 v6.4
プロトコル	LEEF
記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Application Security Web サイト (http://www.appsecinc.com/)

Application Security DbProtect イベントを QRadar に送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Application Security DbProtect DSM RPM をダウンロードして、QRadar コンソールにインストールします。
2. QRadar と通信するように Application Security DbProtect デバイスを構成します。以下のステップを実行します。
   a. DbProtect LEEF リレー・モジュールをインストールします。
   b. DbProtect LEEF リレーを構成します。
   c. DbProtect アラートを構成します。

3. QRadar がログ・ソースを自動検出しない場合は、Application Security DbProtect ログ・ソースを QRadar コンソールに追加します。すべての必須パラメーターを構成します。DbProtect 固有の値については、以下の表を使用してください。

表 55. *Application Security DbProtect* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Application Security DbProtect
プロトコル構成	Syslog

DbProtect LEEF Relay モジュールのインストール

DbProtect が IBM Security QRadar と通信できるようにするには、DbProtect LEEF Relay モジュールを DbProtect コンソールと同じサーバーにインストールします。

始める前に

DbProtect LEEF Relay モジュールを Windows 2003 ホストにインストールする前に、Windows Imaging Components をインストールする必要があります。`wic_x86.exe` ファイルに Windows Imaging Components が含まれており、このファイルは Windows Server インストール CD にあります。詳しくは、Windows 2003 オペレーティング・システムの資料を参照してください。

このタスクについて

DbProtect 用の LEEF Relay モジュールは、QRadar 用にデフォルトのイベント・メッセージをログ・イベント拡張フォーマット (LEEF) メッセージに変換します。QRadar でイベントを受信する前に、DbProtect デバイス用に LEEF サービスをインストールし、syslog イベントを転送するように構成する必要があります。DbProtect LEEF Relay では、.NET 4.0 Framework をインストールする必要があります。これは、LEEF Relay のインストールにバンドルされています。

手順

1. DbProtect 用の DbProtect LEEF Relay モジュールを Application Security, Inc. の顧客ポータル (http://www.appsecinc.com) からダウンロードします。
2. セットアップ・ファイルを DbProtect コンソールと同じホストに保存します。
3. 「同意する **(Accept)**」をクリックして Microsoft .NET Framework 4 End-User License Agreement に同意します。
4. 「DbProtect LEEF Relay モジュールのインストール・ウィザード (DbProtect LEEF Relay module installation Wizard)」で「次へ **(Next)**」をクリックします。
5. デフォルトのインストール・パスを選択する場合は、「次へ **(Next)**」をクリックします。

   デフォルトのインストール・ディレクトリーを変更した場合は、ファイルの場所をメモしてください。

6. 「インストールの確認 (Confirm Installation)」ウィンドウで、「次へ **(Next)**」をクリックします。
7. 「閉じる **(Close)**」をクリックします。

次のタスク

『DbProtect LEEF Relay の構成』

DbProtect LEEF Relay の構成

DbProtect LEEF Relay モジュールをインストールした後に、イベントを IBM Security QRadar に転送するようにサービスを構成します。

始める前に

構成値を編集する前に、DbProtect LEEF Relay サービスを停止します。

手順

1. DbProtect LEEF Relay サーバーにログインします。
2. `C:¥Program Files (x86)¥AppSecInc¥AppSecLEEFConverter` ディレクトリーにアクセスします。
3. `AppSecLEEFConverter.exe.config` ファイルを編集します。以下の値を構成します。

パラメーター	説明
SyslogListenerPort	DbProtect LEEF Relay が DbProtect コンソールからの syslog メッセージの listen に使用するポート番号。
SyslogDestinationHost	QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレス。
SyslogDestinationPort	514
LogFileName	DbProtect LEEF Relay がデバッグおよびログ・メッセージを書き込むファイルの名前。DbProtect LEEF Relay サービスを実行する LocalSystem ユーザー・アカウントは、指定したファイル・パスへの書き込み特権を備えている必要があります。

4. 構成変更をファイルに保存します。
5. DbProtect コンソールのデスクトップで「スタート」 > 「ファイル名を指定して実行」を選択します。
6. 以下のコマンドを入力します。

   ```
   services.msc
   ```

7. 「**OK**」をクリックします。
8. 「サービス」ウィンドウの詳細ペインで、「**DbProtect LEEF Relay**」が開始されていて、「自動」スタートアップに設定されていることを確認します。
9. サービスのプロパティーを変更するには、サービス名を右クリックしてから、「プロパティ」をクリックします。
10. 「スタートアップの種類」リストで「自動」を選択します。

11. 「**DbProtect LEEF Relay**」が開始されていない場合は、「開始」をクリックします。

次のタスク

『DbProtect アラートの構成』

DbProtect アラートの構成

アラートを生成するように DbProtect コンソールでセンサーを構成します。

手順

1. DbProtect コンソールにログインします。
2. 「アクティビティー・モニター **(Activity Monitoring)**」タブをクリックします。
3. 「センサー **(Sensors)**」タブをクリックします。
4. センサーを選択し、「再構成 **(Reconfigure)**」をクリックします。
5. データベース・インスタンスを選択し、「再構成 **(Reconfigure)**」をクリックします。
6. 「センサー・マネージャー・ポリシー (Sensor Manager Policy)」ウィンドウが表示されるまで「次へ **(Next)**」をクリックします。
7. 「**Syslog**」チェック・ボックスを選択し、「次へ **(Next)**」をクリックします。
8. 「次の **Syslog** コンソールにアラートを送信 **(Send Alerts to the following Syslog console)**」フィールドで、DbProtect コンソールの IP アドレスを入力します。
9. 「ポート **(Port)**」フィールドに、DbProtect LEEF Relay の「**SyslogListenerPort**」フィールドで構成したポート番号を入力します。

   ヒント**:** デフォルトでは、DbProtect LEEF Relay のデフォルト Syslog listen ポートは 514 です。
10. 「追加」をクリックします。
11. 「センサーにデプロイ (Deploy to Sensor)」ウィンドウに到達するまで「次へ **(Next)**」をクリックします。
12. 「センサーにデプロイ **(Deploy to Sensor)**」をクリックします。

第 14 章 Arbor Networks

さまざまな Arbor Networks DSM を IBM Security QRadar と統合できます。

このセクションでは、以下の DSM についての情報を提供します。

- 『Arbor Networks Peakflow SP』
- 117 ページの『Arbor Networks Pravail』

Arbor Networks Peakflow SP

IBM Security QRadar は、ネットワーク内の Arbor Networks Peakflow SP アプライアンスから syslog イベントを収集し、分類することができます。

Arbor Networks Peakflow SP アプライアンスは、syslog イベントをローカルに保管します。

ローカル syslog イベントを収集するには、syslog イベントをリモート・ホストに転送するように、Peakflow SP アプライアンスを構成する必要があります。QRadar は、Arbor Networks Peakflow SP アプライアンスから転送された syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。QRadar は、Peakflow V5.8 から転送される syslog イベントをサポートします。

Arbor Networks Peakflow SP を構成するには、以下のタスクを実行します。

1. Peakflow SP アプライアンスで、QRadar への通知グループを作成します。
2. Peakflow SP アプライアンスで、グローバル通知設定を構成します。
3. Peakflow SP アプライアンスで、アラート通知ルールを構成します。
4. QRadar システムで、転送されたイベントが自動的に検出されることを確認します。

Arbor Networks Peakflow SP のサポートされるイベント・タイプ

IBM Security QRadar 用の Arbor Networks Peakflow DSM は、さまざまなカテゴリーのイベントを収集します。

各イベント・カテゴリーには下位イベントが含まれ、そのイベント・カテゴリー内で実行されるアクションを記述しています。例えば、認証イベントには、`login successful` または `login failure` という下位カテゴリーを含めることができます。

以下のリストは、QRadar が Peakflow SP アプライアンスから収集するイベント・カテゴリーを定義しています。

- サービス妨害 (DoS) イベント
- 認証イベント
- エクスプロイト・イベント

- 疑わしいアクティビティー・イベント
- システム・イベント

Arbor Networks Peakflow SP でのリモート syslog の構成

イベントを収集するには、新規通知グループを構成するか、既存のグループを編集して IBM Security QRadar をリモート syslog 宛先として追加する必要があります。

手順

1. Peakflow SP 構成インターフェースに管理者としてログインします。
2. ナビゲーション・メニューで「管理 **(Administration)**」 > 「通知 **(Notification)**」 > 「グループ **(Groups)**」を選択します。
3. 「通知グループの追加 **(Add Notification Group)**」をクリックします。
4. 「宛先 **(Destinations)**」フィールドに、QRadar システムの IP アドレスを入力します。
5. 「ポート **(Port)**」フィールドに、syslog 宛先のポートとして 514 と入力します。
6. 「ファシリティー **(Facility)**」リストで syslog ファシリティーを選択します。
7. 「重大度 **(Severity)**」リストで「情報 **(info)**」を選択します。

   「情報 (informational)」重大度では、情報イベント・レベル以上の重大度のすべてのイベント・メッセージが収集されます。
8. 「保存」をクリックします。
9. 「構成のコミット **(Configuration Commit)**」をクリックします。

Arbor Networks Peakflow SP でのアラートのグローバル通知設定の構成

Arbor Networks Peakflow SP のグローバル通知は、ルールに関連付けられていないシステム通知を提供します。

このタスクについて

この手順では、IBM Security QRadar をデフォルト通知グループとして追加し、システム通知を有効にする方法について説明します。

手順

1. Arbor Networks Peakflow SP アプライアンスの構成インターフェースに管理者としてログインします。
2. ナビゲーション・メニューで「管理 **(Administration)**」 > 「通知 **(Notification)**」 > 「グローバル設定 **(Global Settings)**」を選択します。
3. 「デフォルトの通知グループ **(Default Notification Group)**」フィールドで、QRadar syslog イベント用に作成した通知グループを選択します。
4. 「保存」をクリックします。
5. 「構成のコミット **(Configuration Commit)**」をクリックして構成変更を適用します。

6. Arbor Networks Peakflow SP コマンド・ライン・インターフェースに管理者としてログインします。
7. 以下のコマンドを入力して、現在のアラート構成をリストします。

   ```
   services sp alerts system_errors show
   ```
8. オプション: 以下のコマンドを入力して、構成可能なフィールドの名前をリストします。

   ```
   services sp alerts system_errors ?
   ```
9. 以下のコマンドを入力して、システム・アラートの通知を有効にします。

   ```
   services sp alerts system_errors <name> notifications enable
   ```

   ここで、*<name>* は、通知のフィールド名です。
10. 以下のコマンドを入力して、構成変更をコミットします。

    ```
    config write
    ```

Arbor Networks Peakflow SP でのアラート通知ルールの構成

イベントを生成するには、IBM Security QRadar がリモート syslog 宛先として使用する通知グループを使用するためのルールを編集または追加する必要があります。

手順

1. Arbor Networks Peakflow SP 構成インターフェースに管理者としてログインします。
2. ナビゲーション・メニューで「管理 **(Administration)**」 > 「通知 **(Notification)**」 > 「ルール **(Rules)**」を選択します。
3. 次のオプションのいずれかを選択します。
   - 現在のルールをクリックして、ルールを編集します。
   - 「ルールの追加 **(Add Rule)**」をクリックして、新規通知ルールを作成します。
4. 以下の値を構成します。

表 *56. Arbor Networks Peakflow SP* 通知ルールのパラメーター

パラメーター	説明
名前	Peakflow SP インストール済み環境からのイベントの ID として、 IP アドレスまたはホスト名を入力します。 ログ・ソース ID は、固有値でなければなりません。
リソース	CIDR アドレスを入力するか、Peakflow リソースのリストから管理対象オブジェクトを選択します。
重要度 **(Importance)**	ルールの「重要度 **(Importance)**」を選択します。

表 56. *Arbor Networks Peakflow SP* 通知ルールのパラメーター (続き)

パラメーター	説明
通知グループ **(Notification Group)**	syslog イベントを QRadar に転送するために割り当てた「通知グループ **(Notification Group)**」を選択します。

5. 上記ステップを繰り返し、作成する他のルールを構成します。
6. 「保存」をクリックします。
7. 「構成のコミット **(Configuration Commit)**」をクリックして構成変更を適用します。

   QRadar は Arbor Networks Peakflow SP アプライアンスのログ・ソースを自動的に検出および作成します。QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

Arbor Networks Peakflow SP ログ・ソースの構成

IBM Security QRadar は、Arbor Networks Peakflow SP から転送された syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. オプション: 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Arbor Networks Peakflow**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 57. システム・パラメーター

パラメーター	説明
ログ・ソース **ID**	IP アドレスまたはホスト名が、Peakflow SP インストール済み環境からのイベントの ID として使用されます。 ログ・ソース ID は、固有値でなければなりません。

表 57. システム・パラメーター (続き)

パラメーター	説明
信頼性	ログ・ソースの信頼性。送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。
ターゲット・イベント・コレクター	ログ・ソースのターゲットとして使用するイベント・コレクター。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにします。デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」による「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	ログの解析と保管を行うための受信ペイロード・エンコーダー。
イベント・ペイロードの保管	ログ・ソースによるイベント・ペイロード情報の保管を有効にします。 デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」による「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

Arbor Networks Pravail

IBM Security QRadar DSM for Arbor Networks Pravail は、Arbor Networks Pravail サーバーからイベント・ログを受信します。

以下の表は、Arbor Networks Pravail DSM の仕様を示しています。

表 58. *Arbor Networks Pravail DSM* の仕様

仕様	値
製造元	Arbor Networks
DSM	Arbor Networks Pravail
RPM ファイル名	`DSM-ArborNetworksPravail-build_number.noarch.rpm`
プロトコル	Syslog
記録されるイベント	すべての関連イベント

表 58. *Arbor Networks Pravail DSM* の仕様 (続き)

仕様	値
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Arbor Networks Web サイト (www.arbornetworks.com)

Arbor Networks Pravail イベントを QRadar に送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新の Arbor Networks Pravail RPM をダウンロードして QRadar コンソールにインストールしてください。
2. イベントを QRadar に送信するように各 Arbor Networks Pravail システムを構成します。
3. QRadar が Arbor Pravail システムを自動的に検出しない場合、QRadar コンソールでログ・ソースを作成します。必須パラメーターを構成します。Arbor Pravail 固有のパラメーターについては、以下の表を使用してください。

表 59. *Arbor Pravail* パラメーター

パラメーター	値
ログ・ソース・タイプ	Arbor Networks Pravail
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『イベントを IBM Security QRadar に送信するように Arbor Networks Pravail システムを構成』
Arbor Networks Pravail からすべての監査ログおよびシステム・イベントを収集するには、QRadar を Syslog サーバーとして指定する宛先を追加する必要があります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

イベントを IBM Security QRadar に送信するように Arbor Networks Pravail システムを構成

Arbor Networks Pravail からすべての監査ログおよびシステム・イベントを収集するには、QRadar を Syslog サーバーとして指定する宛先を追加する必要があります。

手順

1. Arbor Networks Pravail サーバーにログインします。
2. 「設定とレポート **(Settings & Reports)**」をクリックします。

3. 「管理」 > 「通知 **(Notifications)**」をクリックします。
4. 「通知の構成 (Configure Notifications)」ページで「宛先の追加 **(Add Destinations)**」をクリックします。
5. 「**Syslog**」を選択します。
6. 以下のパラメーターを構成します。

表 *60. Syslog* パラメーター

パラメーター	説明
ホスト	QRadar コンソールの IP アドレス
ポート	514
重大度	通知
アラート・タイプ	QRadar コンソールに送信するアラートのタイプ。

7. 「保存」をクリックします。

第 15 章 Arpeggio SIFT-IT

IBM Security QRadar SIFT-IT DSM は、IBM iSeries 上で実行されている Arpeggio SIFT-IT から、ログ・イベント拡張フォーマット (LEEF) としてフォーマットされた syslog イベントを受け入れます。

QRadar は、IBM iSeries バージョン 5 リビジョン 3 (V5R3) 以降にインストールされた Arpeggio SIFT-IT 3.1 以降のイベントをサポートします。

Arpeggio SIFT-IT は、ジャーナル QAUDJRN の syslog イベント (LEEF 形式) をサポートします。

例:

```
Jan 29 01:33:34 RUFUS LEEF:1.0|Arpeggio|SIFT-IT|3.1|PW_U|sev=3
usrName=ADMIN src=100.100.100.114 srcPort=543 jJobNam=QBASE jJobUsr=ADMIN
jJobNum=1664 jrmtIP=100.100.100.114 jrmtPort=543 jSeqNo=4755 jPgm=QWTMCMNL
jPgmLib=QSYS jMsgId=PWU0000 jType=U jUser=ROOT jDev=QPADEV000F
jMsgTxt=Invalid user id ROOT. Device QPADEV000F.
```

SIFT-IT が QRadar に送信するイベントは、構成ルール・セット・ファイルによって決まります。SIFT-IT にはデフォルトの構成ルール・セット・ファイルがあり、セキュリティー要件または監査要件に合わせて編集できます。ルール・セット・ファイルの構成方法について詳しくは、「*SIFT-IT User Guide*」を参照してください。

SIFT-IT エージェントの構成

Arpeggio SIFT-IT は、SIFT-IT エージェントを使用して、LEEF 形式の syslog イベントを転送できます。

このタスクについて

SIFT-IT エージェント構成は、IBM Security QRadar インストール済み環境の場所、イベント・メッセージのプロトコルとフォーマット設定、および構成ルール・セットを定義します。

手順

1. IBM iSeries にログインします。
2. 以下のコマンドを入力し、Enter キーを押して SIFT-IT をライブラリー・リストに追加します。

   ```
   ADDLIBLE SIFTITLIB0
   ```

3. 以下のコマンドを入力し、Enter キーを押して SIFT-IT メインメニューにアクセスします。

   ```
   GO SIFTIT
   ```

4. メインメニューで「**1. SIFT-IT エージェント定義の処理 (Work with SIFT-IT Agent Definitions)**」を選択します。
5. 1 と入力して QRadar のエージェント定義を追加し、Enter キーを押します。
6. 「**SIFT-IT エージェント名 (SIFT-IT Agent Name)**」フィールドに名前を入力します。

   例: QRadar。
7. 「説明 **(Description)**」フィールドにエージェントの説明を入力します。

   例: `Arpeggio agent for` QRadar。
8. 「サーバーのホスト名または **IP アドレス (Server host name or IP address)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の場所を入力します。
9. 「接続タイプ **(Connection type)**」フィールドに、`*TCP`、`*UDP`、または `*SECURE` のいずれかを入力します。

   `*SECURE` オプションでは TLS プロトコルが必要です。
10. 「リモート・ポート番号 **(Remote port number)**」フィールドに `514` と入力します。

    デフォルトでは、QRadar ではポート 514 で TCP と UDP の両方の syslog メッセージがサポートされます。
11. 「メッセージ・フォーマット・オプション **(Message format options)**」フィールドに *QRadar と入力します。
12. オプション: QRadar 固有ではない属性の追加パラメーターを構成します。

    追加の稼働パラメーターについては、「*SIFT-IT User Guide*」で説明されています。
13. F3 を押して終了して「**SIFT-IT エージェント説明の処理 (Work with SIFT-IT Agents Description)**」メニューに移動します。
14. `9` と入力し、Enter キーを押して QRadar の構成ルール・セットをロードします。
15. 「構成ファイル **(Configuration file)**」フィールドに、QRadar 構成ルール・セット・ファイルのパスを入力します。

    例: `/sifitit/Qradarconfig.txt`
16. F3 を押して終了して「**SIFT-IT エージェント説明の処理 (Work with SIFT-IT Agents Description)**」メニューに移動します。
17. 11 と入力して QRadar エージェントを開始します。

次のタスク

Arpeggio SIFT-IT によって LEEF 形式で転送された syslog イベントは、QRadar によって自動的に検出されます。ほとんどの場合、いくつかのイベントが検出されると、ログ・ソースが QRadar で自動的に作成されます。イベント速度が低い場合、QRadar で Arpeggio SIFT-IT のログ・ソースを手動で作成する必要が生じることがあります。

ログ・ソースが自動的に検出されて識別されるまで、QRadar の「ログ・アクティビティー」タブでイベント・タイプは「不明」と表示されます。自動的に検出されたログ・ソースは、「ログ・ソース」アイコンをクリックすることで、QRadar の「管理」タブに表示できます。

関連概念:

39 ページの『TLS Syslog プロトコルの構成オプション』
TLS Syslog イベント転送をサポートする最大 50 台のネットワーク・デバイスから暗号化された Syslog イベントを受信するには、TLS Syslog プロトコルを使用するようにログ・ソースを構成します。

Arpeggio SIFT-IT ログ・ソースの構成

IBM Security QRadar は Arpeggio SIFT-IT から転送されたシステム認証イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

この手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Arpeggio SIFT-IT**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 「ログ・ソース **ID**」フィールドに、Arpeggio SIFT-IT インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

追加情報

IBM Security QRadar エージェントの定義を作成した後は、Arpeggio SIFT-IT ソフトウェアと QRadar の統合を使用して、セキュリティー要件および監査要件をカスタマイズできます。

以下のようにセキュリティー要件および監査要件をカスタマイズできます。

- イベント属性に基づいたより詳細なフィルタリングを使用する、Arpeggio SIFT-IT のカスタム構成を作成する。

例えば、ジョブ名、ユーザー、ファイル名またはオブジェクト名、システム・オブジェクト、またはポートに基づいたフィルタリング。QRadar での、SIFT-IT から転送されるすべてのイベントおよびイベント・ペイロードの内容の検索が容易になります。

- QRadar でアラートまたはオフェンスを生成するためのルールを構成して、セキュリティー・チームが潜在的なセキュリティーの脅威、データ損失、または侵害をリアルタイムで識別できるようにする。
- IBM iSeries での問題に対してリアルタイムの修復を開始するプロセスを Arpeggio SIFT-IT で構成する。
- QRadar の「オフェンス」タブで、セキュリティー・チームのためのオフェンスを Arpeggio SIFT-IT イベントから作成したり、IBM iSeries 管理者のための E メール・ジョブ・ログを SIFT-IT で構成したりする。
- 特定のセキュリティー・イベントまたは監査イベントを処理するために同時に実行される複数のエージェント用に、複数の構成ルール・セットを作成する。

例えば、ある QRadar エージェントを、すべての IBM iSeries イベントの転送に対応する特定のルール・セットで構成した後に、特定のコンプライアンス目的に合わせた構成ルール・セットを複数開発できます。構成ルール・セットをコンプライアンス規定 (FISMA、PCI、HIPPA、SOX、ISO 27001 など) ごとに容易に管理できます。QRadar エージェントによって転送されるすべてのイベントは、単一のログ・ソースに格納され、分類されて、検索が容易になります。

第 16 章 Array Networks SSL VPN

IBM Security QRadar 用の Array Networks SSL VPN DSM は、syslog を使用して ArrayVPN アプライアンスからイベントを収集します。

QRadar は、TCP ポート 514 または UDP ポート 514 で、syslog を使用して転送される、関連するすべての SSL VPN イベントを記録します。

ログ・ソースの構成

Array Networks SSL VPN イベントを IBM Security QRadar に送信するには、ログ・ソースを手動で作成する必要があります。

このタスクについて

QRadar が Array Networks SSL VPN からの syslog イベントに対して、ログソースを自動的に検出および作成することはありません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Array Networks SSL VPN Access Gateways**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 「ログ・ソース **ID**」フィールドに、ログ・ソースの IP アドレスまたはホスト名を入力します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

これで、リモート syslog イベントを QRadar に転送するように Array Networks SSL VPN アプライアンスを構成する準備ができました。Array Networks SSL VPN アプライアンスの構成について詳しくは、Array Networks の資料を参照してください。

第 17 章 Aruba Networks

さまざまな Aruba DSM を IBM Security QRadar と統合できます。

このセクションでは、以下の DSM についての情報を提供します。

- 『Aruba ClearPass Policy Manager』
- 129 ページの『Aruba モビリティー・コントローラー』

Aruba ClearPass Policy Manager

Aruba ClearPass Policy Manager 用の IBM Security QRadar DSM は、ご使用の Aruba ClearPass Policy Manager サーバーからイベント・ログを収集できます。

以下の表は、Aruba ClearPass Policy Manager DSM の仕様を示しています。

表 61. *Aruba ClearPass Policy Manager DSM* の仕様

仕様	値
製造元	Aruba Networks
DSM 名	ClearPass
RPM ファイル名	DSM-ArubaClearPass-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	6.5.0.71095 以降
イベント・フォーマット	LEEF
記録されるイベント・タイプ	セッション 監査 システム Insight
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Aruba Networks Web サイト (http://www.arubanetworks.com/products/security/)

Aruba ClearPass Policy Manager を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Aruba ClearPass DSM RPM
   - DSMCommon RPM

2. Syslog イベントを QRadar に送信するように Aruba ClearPass Policy Manager デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Aruba ClearPass ログ・ソースを追加してください。以下の表は、Aruba ClearPass Policy Manager イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 62. *Aruba ClearPass Policy Manager* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Aruba ClearPass Policy Manager
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するように Aruba ClearPass Policy Manager を構成

Aruba ClearPass Policy Manager から Syslog イベントを収集するには、QRadar ホスト用に外部の Syslog サーバーを追加する必要があります。次に、Syslog サーバー用に 1 つ以上の Syslog フィルターを作成する必要があります。

始める前に

セッション・イベントおよび Insight イベントの場合、イベントの完全な構文解析は、Aruba ClearPass Policy Manager によって提供されたデフォルト・フィールドに対してのみ機能します。ユーザーによって作成された、フィールドの組み合わせが異なるセッション・イベントおよび Insight イベントは、「不明なセッション・ログ **(Unknown Session Log)**」または「不明な **Insight** ログ **(Unknown Insight Log)**」と表示される場合があります。

手順

1. Aruba ClearPass Policy Manager サーバーにログインします。
2. 管理コンソールを始動します。
3. 「外部サーバー **(External Servers)**」 > 「**Syslog** ターゲット **(Syslog Targets)**」をクリックします。
4. 「追加」をクリックし、QRadar ホストの詳細を構成します。
5. 管理コンソールで、「外部サーバー **(External Servers)**」 > 「**Syslog** エクスポート・フィルター **(Syslog Export Filters)**」をクリックします。
6. 「追加」をクリックします。

7. 「エクスポート・イベントの形式タイプ **(Export Event Format Type)**」として「**LEEF**」を選択し、次に、追加した「**Syslog**サーバー **(Syslog Server)**」を選択します。
8. 「保存」をクリックします。

Aruba モビリティー・コントローラー

IBM Security QRadar 用の Aruba モビリティー・コントローラー DSM は、syslog を使用してイベントを受け入れます。

QRadar は、TCP ポート 514 または UDP ポート 514 で、syslog を使用して転送される、関連するすべてのイベントを記録します。

Aruba モビリティー・コントローラーの構成

syslog イベントを IBM Security QRadar に転送するように Aruba Wireless Networks (モビリティー・コントローラー) デバイスを構成できます。

手順

1. Aruba モビリティー・コントローラーにログインします。
2. トップ・メニューで「構成 **(Configuration)**」を選択します。
3. 「切り替え **(Switch)**」メニューで「管理 **(Management)**」を選択します。
4. 「ロギング **(Logging)**」タブをクリックします。
5. 「ロギング・サーバー **(Logging Servers)**」メニューで「追加 **(Add)**」を選択します。
6. ログを収集する QRadar サーバーの IP アドレスを入力します。
7. 「追加」をクリックします。
8. オプション: 以下のように、モジュールのロギング・レベルを変更します。
   a. ロギング・モジュールの名前の横にあるチェック・ボックスを選択します。
   b. ウィンドウの下部に表示されているリストから変更するロギング・レベルを選択します。
9. 「完了 **(Done)**」をクリックします。
10. 「適用」をクリックします。

ログ・ソースの構成

IBM Security QRadar は、Aruba モビリティー・コントローラーの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。

6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Aruba** モビリティー・コントローラー」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 「ログ・ソース **ID**」フィールドに、ログ・ソースの IP アドレスまたはホスト名を入力します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

第 18 章 Avaya VPN Gateway

Avaya VPN Gateway 用の IBM Security QRadar DSM は、Avaya VPN Gateway サーバーからイベント・ログを収集できます。

以下の表は、Avaya VPN Gateway DSM の仕様を示しています。

表 *63. Avaya VPN Gateway DSM* の仕様

仕様	値
製造元	Avaya Inc.
DSM	Avaya VPN Gateway

RPM ファイル名	`DSM-AvayaVPNGateway-7.1-799033.noarch.rpm`
	
	`DSM-AvayaVPNGateway-7.2-799036.noarch.rpm`

サポートされるバージョン	9.0.7.2
プロトコル	syslog
QRadar で記録されるイベント	OS、システム・コントロール・プロセス、トラフィック処理、始動、構成の再ロード、AAA サブシステム、IPsec サブシステム
自動的に検出?	はい
ID を含む?	はい
その他の情報	http://www.avaya.com

Avaya VPN Gateway DSM 統合プロセス

Avaya VPN Gateway DSM を IBM Security QRadar と統合できます。

このタスクについて

Avaya VPN Gateway DSM を QRadar と統合するには、以下の手順を使用します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Syslog プロトコル RPM
   - DSMCommon RPM
   - Avaya VPN Gateway RPM
2. Avaya VPN Gateway のインスタンスごとに、QRadar との通信を有効にするように Avaya VPN Gateway システムを構成します。
3. QRadar がログ・ソースを自動的に検出した場合、統合する Avaya VPN Gateway サーバーごとに、QRadar コンソールでログ・ソースを作成します。

IBM Security QRadar と通信するための Avaya VPN Gateway システムの構成

Avaya VPN Gateway からすべての監査ログとシステム・イベントを収集するには、QRadar を Syslog サーバーとして指定し、メッセージ・フォーマットを構成する必要があります。

手順

1. Avaya VPN Gateway コマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力します。

   ```
   /cfg/sys/syslog/add
   ```
3. プロンプトで、QRadar システムの IP アドレスを入力します。
4. 構成を適用するには、以下のコマンドを入力します。

   ```
   apply
   ```
5. QRadar システムの IP アドレスがリストされていることを確認するために、以下のコマンドを入力します。

   ```
   /cfg/sys/syslog/list
   ```

IBM Security QRadar での Avaya VPN Gateway のログ・ソースの構成

Avaya VPN Gateway イベントを収集するには、QRadar でログ・ソースを構成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**Avaya VPN Gateway**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。
8. 残りのパラメーターを構成します。
9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

第 19 章 BalaBit IT Security

BalaBit Syslog-ng Agent アプリケーションは、IBM Security QRadar の Microsoft Security Event Log DSM および Microsoft ISA DSM 用に syslog イベントを収集し、転送できます。

Microsoft Windows イベント用の BalaBIt IT Security

IBM Security QRadar の Microsoft Windows Security Event Log DSM は、BalaBit の Syslog-ng Agent からログ・イベント拡張フォーマット (LEEF) のイベントを受け入れることができます。

BalaBit Syslog-ng Agent は、syslog を使用して、以下の Windows イベントを QRadar に転送します。

- Windows セキュリティー
- アプリケーション
- システム
- DNS
- DHCP
- カスタム・コンテナー・イベント・ログ

BalaBit IT Security Syslog-ng Agent からイベントを受信するには、エージェントをインストールして、イベントを転送するように構成する必要があります。

始める前に

BalaBit Syslog-ng Agent を構成する前に、以下の構成ステップを確認してください。

1. BalaBit Syslog-ng Agent を Windows ホストにインストールします。詳しくは、BalaBit Syslog-ng Agent の資料を参照してください。
2. Syslog-ng Agent のイベントを構成します。
3. QRadar を Syslog-ng Agent の宛先として構成します。
4. Syslog-ng Agent サービスを再始動します。
5. オプション。QRadar でログ・ソースを構成します。

Syslog-ng Agent イベント・ソースの構成

イベントを IBM Security QRadar に転送する前に、Syslog-ng Agent が収集する Windows ベースのイベントのタイプを指定する必要があります。

手順

1. 「スタート」メニューから、「すべてのプログラム」 > 「**Syslog-ng Agent for Windows**」 > 「**Syslog-ng Agent for Windows** の構成 **(Configure syslog-ng Agent for Windows)**」を選択します。

「Syslog-ng Agent」ウィンドウが表示されます。

2. 「Syslog-ng Agent の設定 (Syslog-ng Agent Settings)」ペインを展開し、「イベント・ログ・ソース **(Eventlog Sources)**」 を選択します。
3. 「イベント・コンテナー **(Event Containers)**」をダブルクリックします。

   「イベント・コンテナー・プロパティー (Event Containers Properties)」ウィンドウが表示されます。
4. 「イベント・コンテナー (Event Containers)」ペインで「有効にする **(Enable)**」ラジオ・ボタンを選択します。
5. 収集する各イベント・タイプのチェック・ボックスを選択します。
   - アプリケーション **(Application)** - デバイスで Windows アプリケーション・イベント・ログをモニターする場合は、このチェック・ボックスを選択します。
   - セキュリティー **(Security)** - デバイスで Windows セキュリティー・イベント・ログをモニターする場合は、このチェック・ボックスを選択します。
   - システム **(System)** - デバイスで Windows システム・イベント・ログをモニターする場合は、このチェック・ボックスを選択します。

   注**:** BalaBit の Syslog-ng Agent では、カスタム・コンテナーを使用することで、DNS イベントや DHCP イベントなどの他のイベント・タイプもサポートされます。詳しくは、*BalaBit Syslog-ng Agent* の資料 を参照してください。
6. 「適用 **(Apply)**」をクリックしてから、「**OK**」をクリックします。

   BalaBit Syslog-ng Agent のイベント構成は完了です。これで、QRadar を Syslog-ng Agent イベントの宛先として構成する準備ができました。

syslog 宛先の構成

Syslog-ng Agent では、Windows ベースのイベントに対して複数の宛先を構成できます。

このタスクについて

IBM Security QRadar を宛先として構成するには、QRadar の IP アドレスを指定してから、LEEF 形式のメッセージ・テンプレートを構成する必要があります。

手順

1. 「スタート」メニューから、「すべてのプログラム」 > 「**Syslog-ng Agent for Windows**」 > 「**Syslog-ng Agent for Windows** の構成 **(Configure syslog-ng Agent for Windows)**」を選択します。

   「Syslog-ng Agent」ウィンドウが表示されます。
2. 「Syslog-ng Agent の設定 (Syslog-ng Agent Settings)」ペインを展開し、「宛先 **(Destinations)**」をクリックします。
3. 「新規サーバーの追加 **(Add new server)**」をダブルクリックします。

   「サーバー・プロパティー (Server Property)」ウィンドウが表示されます。

4. 「サーバー **(Server)**」タブで「プライマリー・サーバーの設定 **(Set Primary Server)**」をクリックします。
5. 以下のパラメーターを構成します。
   - **Server Name** - QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
   - **Server Port** - QRadar に転送するイベントの TCP ポート番号として 514 と入力します。
6. 「メッセージ **(Messages)**」タブをクリックします。
7. 「プロトコル **(Protocol)**」リストで「**BSD Syslog** のレガシー・プロトコル **(Legacy BSD Syslog Protocol)**」を選択します。
8. 「テンプレート **(Template)**」フィールドに以下を入力して、プロトコルのカスタム・テンプレート・メッセージを定義します。

   ```
   <${PRI}>${BSDDATE} ${HOST} LEEF:${MSG}
   ```

   このフィールドに入力する情報はスペース区切りです。
9. 「イベント・メッセージ・フォーマット **(Event Message Format)**」ペインの「メッセージ・テンプレート **(Message Template**」フィールドに以下のテキストを入力するか、コピーして貼り付けを行って、LEEF イベントのフォーマットを定義します。

   注**:** このテキストは変更しないことをお勧めします。

   ```
   1.0|Microsoft|Windows|2k8r2|${EVENT_ID}|devTime=${R_YEAR}-${R_MONTH}-
   ${R_DAY}T ${R_HOUR}:$ {R_MIN}:${R_SEC}GMT${TZOFFSET}
   devTimeFormat=yyyy-MM-dd'T'HH:mm:ssz cat=${EVENT_TYPE}
   sev=${EVENT_LEVEL} resource=${HOST} usrName=${EVENT_USERNAME}
   application=$ {EVENT_SOURCE} message=${EVENT_MSG}
   ```

   注**:** LEEF 形式では、イベント属性間を区切るために、区切り文字としてタブを使用します。ただし、{Event_ID} の最後のパイプ文字の後までは、区切り文字は開始しません。*devTime*、*devTimeFormat*、*cat*、*sev*、*resource*、*usrName*、*application*、および *message* の各フィールドでは、イベント名の前にタブを含める必要があります。

   テキスト・エディターを使用して、LEEF メッセージ・フォーマットをコピーして「メッセージ・テンプレート **(Message Template)**」フィールドに貼り付ける必要が生じることがあります。
10. 「**OK**」をクリックします。

    宛先の構成は完了です。これで、Syslog-ng Agent サービスを再始動する準備ができました。

Syslog-ng Agent サービスの再始動

Syslog-ng Agent で LEEF 形式のイベントを転送する前に、Windows ホストで Syslog-ng Agent サービスを再始動する必要があります。

手順

1. 「スタート」メニューから「ファイル名を指定して実行」を選択します。

   「ファイル名を指定して実行」ウィンドウが表示されます。
2. 以下のテキストを入力します。

   ```
   services.msc
   ```
3. 「**OK**」をクリックします。

   「サービス」ウィンドウが表示されます。
4. 「名前」列の「**Syslog-ng Agent for Windows**」を右クリックし、「再起動」を選択します。

   Syslog-ng Agent for Windows サービスが再始動したら、構成は完了です。BalaBit Syslog-ng Agent からの syslog イベントは、IBM Security QRadar によって自動的に検出されます。自動的に検出された Windows イベントは、「ログ・アクティビティー」タブで Microsoft Windows セキュリティー・イベント・ログとして表示されます。

ログ・ソースの構成

IBM Security QRadar は、LEEF 形式のメッセージの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドに BalaBit Syslog-ng Agent のログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで Microsoft Windowsの「セキュリティー・イベント・ログ」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 表の以下のパラメーターのいずれかを構成します。

表 *64. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	BalaBit Syslog-ng Agent からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。

12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Microsoft ISA イベントまたは TMG イベント用の BalaBit IT Security

BalaBit Syslog-ng Agent アプリケーションを統合して、IBM Security QRadar に syslog イベントを転送することができます。

BalaBit Syslog-ng Agent は、Microsoft ISA または Microsoft TMG のイベント・ログを読み取り、ログ・イベント拡張フォーマット (LEEF) を使用して syslog イベントを転送します。

BalaBit IT Security が転送するイベントは、QRadar 用の Microsoft Internet and Acceleration (ISA) DSM によって解析され、分類されます。この DSM は、Microsoft ISA イベントおよび Microsoft Threat Management Gateway (TMG) イベントのどちらも受け入れます。

始める前に

BalaBit IT Security Syslog-ng Agent からイベントを受け取るには、エージェントをインストールして、イベントを転送するように構成する必要があります。

注**:** この統合では、BalaBit の Syslog-ng Agent for Windows、および BalaBit の Syslog-ng PE を使用してイベントが解析され、QRadar に転送されて、DSM による解釈が行われます。

BalaBit Syslog-ng Agent を構成する前に、以下の構成ステップを確認してください。

BalaBit Syslog-ng Agent を構成するには、以下のステップを実行する必要があります。

1. BalaBit Syslog-ng Agent を Windows ホストにインストールします。詳しくは、*BalaBit Syslog-ng Agent* のベンダー資料 を参照してください。
2. BalaBit Syslog-ng Agent を構成します。
3. Linux または Unix の場合、BalaBit Syslog-ng PE をリレー・モードでインストールして、イベントを解析し、QRadar に転送します。詳しくは、*BalaBit Syslog-ng PE* のベンダー資料 を参照してください。
4. BalaBit Syslog-ng PE の syslog を構成します。
5. オプション。QRadar でログ・ソースを構成します。

BalaBit Syslog-ng Agent の構成

IBM Security QRadar にイベントを転送するには、Syslog-ng Agent が収集する Microsoft ISA イベントまたは Microsoft TMG イベントのファイル・ソースを指定する必要があります。

Microsoft ISA アプライアンスまたは Microsoft TMG アプライアンスが、Web プロキシー・サーバーおよびファイアウォール・サービスのイベント・ファイルを生成している場合、両方のファイルを追加できます。

BalaBit Syslog-ng Agent ファイル・ソースの構成

BalaBit Syslog-ng Agent ファイル・ソースを使用して、Syslog-ng Agent でモニターするベース・ログ・ディレクトリーおよびファイルを定義します。

手順

1. 「スタート」メニューから、「すべてのプログラム」 > 「**Syslog-ng Agent for Windows**」 > 「**Syslog-ng Agent for Windows** の構成 **(Configure syslog-ng Agent for Windows)**」を選択します。

   「Syslog-ng Agent」ウィンドウが表示されます。
2. 「Syslog-ng Agent の設定 (Syslog-ng Agent Settings)」ペインを展開し、「ファイル・ソース **(File Sources)**」を選択します。
3. 「有効にする **(Enable)**」ラジオ・ボタンを選択します。
4. 「追加 **(Add)**」をクリックして Microsoft ISA イベント・ファイルおよび TMG イベント・ファイルを追加します。
5. 「ベース・ディレクトリー **(Base Directory)**」フィールドで「参照 **(Browse)**」をクリックし、Microsoft ISA ログ・ファイルまたは Microsoft TMG ログ・ファイルのフォルダーを選択します。
6. 「ファイル名フィルター **(File Name Filter)**」フィールドで「参照 **(Browse)**」をクリックし、Microsoft ISA イベントまたは Microsoft TMG イベントが含まれているログ・ファイルを選択します。

   注**:** 「ファイル名フィルター **(File Name Filter)**」フィールドでは、ワイルドカード (*) および疑問符 (?) の文字がサポートされます。これらの文字は、特定のファイル・サイズまたは日付に達したときに、置き換えられたログ・ファイルを検索する際に役立ちます。
7. 「アプリケーション名 **(Application Name)**」フィールドに、アプリケーションを識別するための名前を入力します。
8. 「ログ・ファシリティー **(Log Facility)**」リストで「グローバル設定を使用 **(Use Global Settings)**」を選択します。
9. 「**OK**」をクリックします。

   さらにファイル・ソースを追加する場合は、ステップ 4 から 9 を繰り返します。
10. 「適用 **(Apply)**」をクリックしてから、「**OK**」をクリックします。

    イベント構成は完了です。これで、Microsoft TMG イベントおよび ISA イベントのために syslog 宛先とフォーマット設定を構成する準備ができました。

    Web プロキシー・サービス・イベントおよびファイアウォール・サービス・イベントは、Microsoft ISA と TMG によって個別のファイルに保管されます。

BalaBit Syslog-ng Agent の syslog 宛先の構成

Microsoft ISA または TMG によってキャプチャーされたイベント・ログは BalaBit Syslog-ng Agent for Windows で構文解析できないため、ログを BalaBit Syslog-ng Premium Edition (PE) for Linux/UNIX に転送する必要があります。

このタスクについて

TMG イベント・ログおよび ISA イベント・ログを転送するには、PE Relay の IP アドレスを指定し、LEEF 形式のメッセージ・テンプレートを構成する必要があります。BalaBit Syslog-ng PE は中間 syslog サーバーとして機能して、イベントを構文解析し、情報を IBM Security QRadar に転送します。

手順

1. 「スタート」メニューから、「すべてのプログラム」 > 「**Syslog-ng Agent for Windows**」 > 「**Syslog-ng Agent for Windows** の構成 **(Configure syslog-ng Agent for Windows)**」を選択します。

   「Syslog-ng Agent」ウィンドウが表示されます。
2. 「**Syslog-ng Agent** の設定 **(Syslog-ng Agent Settings)**」ペインを展開し、「宛先 **(Destinations)**」をクリックします。
3. 「新規サーバーの追加 **(Add new server)**」をダブルクリックします。
4. 「サーバー **(Server)**」タブで「プライマリー・サーバーの設定 **(Set Primary Server)**」をクリックします。
5. 以下のパラメーターを構成します。
   - 「サーバー名 **(Server Name)**」に、BalaBit Syslog-ng PE Relay の IP アドレスを入力します。
   - 「サーバー・ポート **(Server Port)**」に、BalaBit Syslog-ng PE Relay に転送されるイベントの TCP ポート番号として 514 と入力します。
6. 「メッセージ **(Messages)**」タブをクリックします。
7. 「プロトコル **(Protocol)**」リストで「**BSD Syslog** のレガシー・プロトコル **(Legacy BSD Syslog Protocol)**」を選択します。
8. 「ファイル・メッセージ・フォーマット (File Message Format)」ペインの「メッセージ・テンプレート **(Message Template)**」フィールドに以下のコードを入力します。

   ```
   ${FILE_MESSAGE}${TZOFFSET}
   ```
9. 「適用 **(Apply)**」をクリックしてから、「**OK**」をクリックします。

   宛先の構成は完了です。これで、イベント・ログからコメント行をフィルタリングする準備ができました。

ログ・ファイルのコメント行のフィルタリング

Microsoft ISA または Microsoft TMG のイベント・ログ・ファイルには、コメント・マーカーが含まれていることがあります。コメントは、イベント・メッセージからフィルタリングする必要があります。

手順

1. 「スタート」メニューから、「すべてのプログラム」 > 「**Syslog-ng Agent for Windows**」 > 「**Syslog-ng Agent for Windows** の構成 **(Configure syslog-ng Agent for Windows)**」を選択します。

   「Syslog-ng Agent」ウィンドウが表示されます。

2. 「Syslog-ng Agent の設定 (Syslog-ng Agent Settings)」ペインを展開し、「宛先 **(Destinations)**」を選択します。
3. IBM Security QRadar の「**Syslog** の宛先 **(Syslog destination)**」を右クリックし、「イベント・フィルター **(Event Filters)**」 > 「プロパティー **(Properties)**」を選択します。

   「グローバル・イベント・フィルターのプロパティー (Global event filters Properties)」ウィンドウが表示されます。
4. 以下の値を構成します。
   - 「グローバル・ファイル・フィルター **(Global file filters)**」ペインで「有効にする **(Enable)**」を選択します。
   - 「フィルター・タイプ **(Filter Type)**」ペインで「ブラック・リストのフィルタリング **(Black List Filtering)**」を選択します。
5. 「**OK**」をクリックします。
6. 「フィルター・リスト **(Filter List)**」メニューで「メッセージ・コンテンツ **(Message Contents)**」をダブルクリックします。

   「メッセージ・コンテンツのプロパティー (Message Contents Properties)」ウィンドウが表示されます。
7. 「メッセージ・コンテンツ (Message Contents)」ペインで「有効にする **(Enable)**」を選択します。
8. 「正規表現 **(Regular Expression)**」フィールドに以下の正規表現を入力します。

   ^#
9. 「追加」をクリックします。
10. 「適用 **(Apply)**」をクリックしてから、「**OK**」をクリックします。

    コメントが付いたイベント・メッセージは転送されなくなりました。

    注**:** syslog の転送を開始するために Syslog-ng Agent for Windows サービスを再始動する必要が生じることがあります。詳しくは、*BalaBit Syslog-ng Agent* の資料 を参照してください。

BalaBit Syslog-ng PE Relay の構成

BalaBit Syslog-ng Agent for Windows は、Microsoft TMG イベント・ログおよび ISA イベント・ログを Balabit Syslog-ng PE インストール済み環境 (リレー・モードで構成されている) に送信します。

このタスクについて

リレー・モードのインストール済み環境は、BalaBit Syslog-ng Agent for Windows からイベント・ログを受信し、イベント・ログを解析して LEEF 形式に変換してから、syslog を使用してイベントを IBM Security QRadar に送信するという処理を行います。

BalaBit Syslog-ng PE Relay を構成するには、以下を行う必要があります。

1. BalaBit Syslog-ng PE for Linux/Unix をリレー・モードでインストールします。詳しくは、BalaBit Syslog-ne PE のベンダー資料を参照してください。
2. Syslog-ng PE Relay で syslog を構成します。

BalaBit Syslog-ng PE は、syslog.conf ファイルの構成に基づいて、TMG イベントおよび ISA イベントを LEEF 形式に設定します。syslog.conf ファイルは、イベント・ログの構文解析と QRadar へのイベントの転送を担います。

手順

1. SSH を使用して、BalaBit Syslog-ng PE Relay コマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のファイルを編集します。

   /etc/syslog-ng/etc/syslog.conf
3. 宛先セクションで、リレー宛先ごとに IP アドレスとポート番号を追加します。

   例: ###### # destinations destination d_messages { file("/var/log/messages"); }; destination d_remote_tmgfw { tcp("QRadar_IP" port(QRadar_PORT) log_disk_fifo_size(10000000) template(t_tmgfw)); }; destination d_remote_tmgweb { tcp("QRadar_IP" port(QRadar_PORT) log_disk_fifo_size(10000000) template(t_tmgweb)); };

   各部分について以下で説明します。 *QRadar_IP* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。

   QRadar_Port は、QRadar が syslog イベントを受信するために必要なポート番号です。デフォルトでは、QRadar は syslog イベントをポート 514 で受信します。
4. syslog 構成変更を保存します。
5. Syslog-ng PE を再始動して、強制的に構成ファイルを読み取ります。

   BalaBit Syslog-ng PE の構成は完了です。BalaBit Syslog-ng Relay から転送された syslog イベントは、「ログ・アクティビティー」タブで Microsoft Windows セキュリティー・イベント・ログとして QRadar によって自動的に検出されます。詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

   注: 複数の syslog 宛先を使用している場合、メッセージは、プライマリー syslog 宛先に正常に到達すると、送達済みと見なされます。

ログ・ソースの構成

IBM Security QRadar は、BalaBit Syslog-ng Relay から提供された LEEF 形式のメッセージの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで Microsoft **ISA** を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   「**Syslog** プロトコル構成 **(Syslog Protocol Configuration)**」が表示されます。
10. 表の以下のパラメーターのいずれかを構成します。

表 *65. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	BalaBit Syslog-ng Agent からの Microsoft ISA イベントまたは Microsoft Threat Management Gateway イベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    Microsoft ISA イベントおよび Microsoft TMG イベント用の BalaBit IT Security の構成は完了です。

第 20 章 Barracuda

IBM Security QRadar は、さまざまな Barracuda デバイスをサポートします。

QRadar がサポートするデバイスは以下のとおりです。

- 『Barracuda Spam & Virus Firewall』
- 144 ページの『Barracuda Web Application Firewall』
- 148 ページの『Barracuda Web Filter』

Barracuda Spam & Virus Firewall

Barracuda Spam & Virus Firewall を IBM Security QRadar と統合できます。

QRadar 用の Barracuda Spam & Virus Firewall DSM は、Barracuda Spam & Virus Firewall アプライアンスから、メール syslog イベントおよび Web syslog イベントの両方を受け入れます。

メール syslog イベントには、ファイアウォールによる E メールの処理時に実行されるイベントとアクションが含まれます。 Web syslog イベントには、ユーザー・アクティビティーについての情報、および Barracuda Spam & Virus Firewall アプライアンスで発生した構成変更が記録されます。

始める前に

syslog メッセージは、UDP ポート 514 を使用して、Barracuda Spam & Virus Firewall から QRadar に送信されます。QRadar と Barracuda Spam & Virus Firewall アプライアンスの間にあるいずれのファイアウォールでもポート 514 での UDP トラフィックが許可されていることを確認してください。

syslog イベントの転送の構成

Barracuda Spam & Virus Firewall 用に syslog の転送を構成できます。

手順

1. Barracuda Spam & Virus Firewall の Web インターフェースにログインします。
2. 「拡張」タブをクリックします。
3. 「拡張 **(Advanced)**」メニューで「拡張ネットワーキング **(Advanced Networking)**」を選択します。
4. 「メール **Syslog (Mail Syslog)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
5. 「追加」をクリックします。
6. 「**Web** インターフェース **Syslog (Web Interface Syslog)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。

7. 「追加」をクリックします。

ログ・ソースの構成

IBM Security QRadar は、Barracuda Spam & Virus Firewall アプライアンスの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「**Barracuda Spam & Virus Firewall**」を選択します。
8. 「プロトコル構成」リストで「**Syslog**」を選択します。
9. 「ログ・ソース **ID**」フィールドに、ログ・ソースの IP アドレスまたはホスト名を入力します。
10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

Barracuda Web Application Firewall

Barracuda Web Application Firewall 用の IBM Security QRadar DSM は、Barracuda Web Application Firewall デバイスから、Syslog LEEF およびカスタム・イベントを収集します。

以下の表は、Barracuda Web Application Firewall DSM の仕様を示しています。

表 *66. Barracuda Web Application Firewall DSM* の仕様

仕様	値
製造元	Barracuda
DSM 名	Web アプリケーション・ファイアウォール
RPM ファイル名	DSM-BarracudaWebApplicationFirewall-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	V7.0.x 以降
プロトコル・タイプ	Syslog

表 66. *Barracuda Web Application Firewall DSM* の仕様 (続き)

仕様	値
QRadar で記録されるイベント・タイプ	システム Web アクセス 監査
自動的に検出?	LEEF フォーマットのペイロードの場合、ログ・ソースは自動的に検出されます。 カスタム・フォーマットのペイロードの場合、ログ・ソースは自動的に検出されません。
ID を含む?	はい
その他の情報	Barracuda Networks Web サイト (https://www.barracudanetworks.com)

Barracuda Web Application Firewall から Syslog イベントを収集するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンを QRadar コンソール コンソールからダウンロードしてください。
   - Barracuda Web Application Firewall DSM RPM
   - DSMCommon RPM
2. Syslog イベントを QRadar に送信するように Barracuda Web Application Firewall デバイスを構成します。
3. QRadar コンソール上で Barracuda Web Application Firewall ログ・ソースを追加します。以下の表は、固有の値を必要とするパラメーターを示しています。Barracuda Web Application Firewall イベントを収集するには、これらの値が必要です。

表 67. *Barracuda Web Application Firewall* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Barracuda Web Application Firewall
プロトコル構成	Syslog

Syslog イベントを QRadar に送信するように Barracuda Web Application Firewall を構成する

Syslog イベントを IBM Security QRadar に送信するように Barracuda Web Application Firewall アプライアンスを構成します。

始める前に

Barracuda アプライアンスと QRadar の間にあるファイアウォールが、ポート 514 で UDP トラフィックを許可することを確認します。

手順

1. Barracuda Web Application Firewall の Web インターフェースにログインします。
2. 「拡張」タブをクリックします。
3. 「拡張」メニューから、「ログのエクスポート」を選択します。
4. 「**Syslog** サーバーの追加 **(Add Syslog Server)**」をクリックします。
5. 以下のパラメーターを構成します。

オプション	説明
名前	QRadar コンソールまたはイベント・コレクターの名前。
Syslog サーバー	QRadar コンソールまたはイベント・コレクターの IP アドレス。
ポート	QRadar コンソールまたはイベント・コレクターの IP アドレスに関連付けられているポート。 Syslog メッセージが UDP によって送信される場合、デフォルト・ポート 514 を使用します。
接続タイプ	Barracuda Web Application Firewall から QRadar コンソールまたはイベント・コレクターにログを送信する接続タイプ。Syslog 通信のデフォルト・プロトコルは UDP です。
サーバー証明書の検証	いいえ

6. 「ログ・フォーマット **(Log Formats)**」ペインのリスト・ボックスから、ログ・タイプごとにフォーマットを選択します。
   - 新しいバージョンの Barracuda Web Application Firewall を使用している場合は、「**LEEF 1.0 (QRadar)**」を選択します。
   - 古いバージョンの Barracuda Web Application Firewall を使用している場合は、「カスタム・フォーマット **(Custom Format)**」を選択します。
7. 「変更の保存 **(Save Changes)**」をクリックします。

LEEF をサポートしないデバイス用に、QRadar に syslog イベントを送信するように Barracuda Web Application Firewall を構成する

ご使用のデバイスで LEEF がサポートされていない場合、Barracuda Web Application Firewall で syslog 転送を構成できます。

手順

1. Barracuda Web Application Firewall の Web インターフェースにログインします。
2. 「拡張」タブをクリックします。

3. 「拡張」メニューから、「ログのエクスポート」を選択します。
4. 「**Syslog** 設定 **(Syslog Settings)**」をクリックします。
5. 以下のオプションの syslog ファシリティー値を構成します。

オプション	説明
Web ファイアウォール・ログ・ファシリティー **(Web Firewall Logs Facility)**	**Local0** と **Local7** の間の syslog ファシリティーを選択します。
アクセス・ログ・ファシリティー **(Access Logs Facility)**	**Local0** と **Local7** の間の syslog ファシリティーを選択します。
監査ログ・ファシリティー **(Audit Logs Facility)**	**Local0** と **Local7** の間の syslog ファシリティーを選択します。
システム・ログ・ファシリティー **(System Logs Facility)**	**Local0** と **Local7** の間の syslog ファシリティーを選択します。

各ログ・タイプに syslog 固有のファシリティーを設定することにより、Barracuda Web Application Firewall でログを複数のファイルに分割できます。

6. 「変更の保存 **(Save Changes)**」をクリックします。
7. 「名前 **(Name)**」フィールドに syslog サーバーの名前を入力します。
8. 「**Syslog**」フィールドに QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
9. 「タイム・スタンプのログ **(Log Time Stamp)**」オプションから「はい **(Yes)**」を選択します。
10. 「ユニット名のログ **(Log Unit Name)**」オプションから「はい **(Yes)**」を選択します。
11. 「追加」をクリックします。
12. 「**Web** ファイアウォール・ログの形式 **(Web Firewall Logs Format)**」リスト・ボックスから「カスタム形式 **(Custom Format)**」を選択します。
13. 「**Web** ファイアウォール・ログの形式 **(Web Firewall Logs Format)**」フィールドに、以下のカスタム・イベント形式を入力します。
`t=%t|ad=%ad|ci=%ci|cp=%cp|au=%au`
14. 「アクセス・ログの形式 **(Access Logs Format)**」リスト・ボックスで「カスタム形式 **(Custom Format)**」を選択します。
15. 「アクセス・ログの形式 **(Access Logs Format)**」フィールドに、以下のカスタム・イベント形式を入力します。 `t=%t|p=%p|s=%s|id=%id|ai=%ai|ap=%ap|ci=%ci|cp=%cp|si=%si|sp=%sp|cu=%cu`
16. 「アクセス・ログの形式 **(Access Logs Format)**」リスト・ボックスで「カスタム形式 **(Custom Format)**」を選択します。
17. 「アクセス・ログの形式 **(Access Logs Format)**」フィールドに、以下のカスタム・イベント形式を入力します。 `t=%t|trt=%trt|an=%an|li=%li|lp=%lp`
18. 「変更の保存 **(Save Changes)**」をクリックします。
19. ナビゲーション・メニューから「基本 **(Basic)**」 > 「管理 **(Administration)**」を選択します。

20. 「システム/再ロード/シャットダウン (System/Reload/Shutdown)」ペインから「再始動 **(Restart)**」をクリックします。

タスクの結果

syslog 構成は Barracuda Web Application Firewall の再始動後に有効になります。 Barracuda Web Application Firewall によって QRadar に転送されたイベントが、「ログ・アクティビティー」タブに表示されます。

Barracuda Web Filter

Barracuda Web Filter アプライアンスのイベントを IBM Security QRadar と統合できます。

IBM Security QRadar 用の Barracuda Web Filter DSM は、Barracuda Web Filter アプライアンスから転送される syslog 形式の Web トラフィック・イベントと Web インターフェース・イベントを受け入れます。

Web トラフィック・イベントには、アプライアンスによる Web トラフィックの処理時に実行されるイベントとアクションが含まれます。Web インターフェース・イベントには、Web Filter アプライアンスへのユーザー・ログイン・アクティビティーと構成変更が含まれます。

始める前に

syslog メッセージは、UDP ポート 514 を使用して、QRadar に転送されます。QRadar と Barracuda Web Filter アプライアンスの間にあるいずれのファイアウォールでもポート 514 での UDP トラフィックが許可されていることを確認してください。

syslog イベントの転送の構成

Barracuda Web Filter 用に syslog の転送を構成します。

手順

1. Barracuda Web Filter の Web インターフェースにログインします。
2. 「拡張」タブをクリックします。
3. 「拡張 **(Advanced)**」メニューで「**Syslog**」を選択します。
4. 「**Web** トラフィック **Syslog (Web Traffic Syslog)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
5. 「追加」をクリックします。
6. 「**Web** インターフェース **Syslog (Web Interface Syslog)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
7. 「追加」をクリックします。

   syslog の構成は完了です。

ログ・ソースの構成

IBM Security QRadar は、Barracuda Web Filter アプライアンスの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Barracuda Web Filter**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下のいずれかのパラメーターを構成します。

表 68. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Barracuda Web Filter アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。 Barracuda Web Filter によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

第 21 章 Bit9

さまざまな Bit9 DSM を IBM Security QRadar と統合できます。

Bit9 Parity

イベントを収集するには、ログ・イベント拡張フォーマット (LEEF) で syslog イベントを 転送するように Bit9 Parity デバイスを構成する必要があります。

手順

1. 管理者特権または PowerUser 特権を使用して Bit9 Parity コンソールにログインします。
2. コンソールの左側にあるナビゲーション・メニューで「管理 **(Administration)**」 > 「システム構成 **(System Configuration)**」を選択します。

   「システム構成 (System Configuration)」ウィンドウが表示されます。
3. 「サーバー状況 **(Server Status)**」をクリックします。

   「サーバー状況 (Server Status)」ウィンドウが表示されます。
4. 「編集」をクリックします。
5. 「**Syslog** アドレス **(Syslog address)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
6. 「**Syslog** 形式 **(Syslog format)**」リストで「**LEEF (Q1Labs)**」を選択します。
7. 「**Syslog** が有効になる **(Syslog enabled)**」チェック・ボックスを選択します。
8. 「更新 **(Update)**」をクリックします。

   構成は完了です。Bit9 Parity イベントが自動的に検出されると、ログ・ソースが IBM Security QRadar に追加されます。Bit9 Parity によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Bit9 Parity からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Bit9 Security Platform**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *69. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Bit9 Parity デバイスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Bit9 Security Platform

Bit9 Parity デバイスからイベントを収集するには、Bit9 Security Platform 用の IBM Security QRadar SIEM DSM を使用します。

以下の表は、Bit9 Security Platform DSM の仕様を示しています。

表 *70. Bit9 Security Platform* の *DSM* 仕様

仕様	値
製造元	Bit9
DSM 名	Bit9 Security Platform
RPM ファイル名	`DSM-Bit9Parity-build_number.noarch.rpm`
サポートされるバージョン	V6.0.2 以降
イベント・フォーマット	Syslog
サポートされるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	はい
その他の情報	Bit9 Web サイト (http://www.bit9.com)

Bit9 Security Platform を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Bit9 Security Platform DSM RPM をダウンロードしてください。
2. QRadar と通信するように Bit9 Security Platform デバイスを構成します。syslog の出力先と転送ポリシーを Bit9 Security Platform デバイス上で作成する必要があります。

3. QRadar が Bit9 Security Platform をログ・ソースとして自動的に検出しない場合は、QRadar コンソール上で Bit9 Security Platform のログ・ソースを作成します。以下に示す Bit9 Security Platform の値を使用して、ログ・ソースのパラメーターを構成してください。

ログ・ソース ID	Bit9 Security Platform デバイスの IP アドレスまたはホスト名
ログ・ソース・タイプ	Bit9 Security Platform
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に Bit9 Security Platform を構成する

イベントを LEEF 形式で IBM Security QRadar に転送するには、Bit9 Security Platform デバイスを構成します。

手順

1. 管理者特権または PowerUser 特権を使用して Bit9 Security Platform コンソールにログインします。
2. ナビゲーション・メニューで、「管理 **(Administration)**」>「システム構成 **(System Configuration)**」を選択します。
3. 「サーバー状況 **(Server Status)**」をクリックして「編集 **(Edit)**」をクリックします。
4. 「**Syslog** アドレス **(Syslog address)**」フィールドに、QRadar コンソールまたはイベント・コレクターの IP アドレスを入力します。
5. 「**Syslog** 形式 **(Syslog format)**」リストで「**LEEF (Q1Labs)**」を選択します。
6. 「**Syslog** が使用可能 **(Syslog enabled)**」チェック・ボックスを選択して「更新 **(Update)**」をクリックします。

Carbon Black

Carbon Black 用の IBM Security QRadar DSM は、Carbon Black サーバーからエンドポイント保護イベントを収集します。

以下の表は、Carbon Black DSM の仕様を示しています。

表 *71. Carbon Black DSM* の仕様

仕様	値
製造元	Carbon Black
DSM 名	Carbon Black

表 71. *Carbon Black DSM* の仕様 (続き)

仕様	値
RPM ファイル名	DSM-CarbonBlackCarbonBlack-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	5.1 以降
プロトコル	Syslog
記録されるイベント・タイプ	監視リスト・ヒット
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Bit9 の Carbon Black Web サイト (https://bit9.com/solutions/carbon-black/)

Carbon Black を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、次の RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Carbon Black DSM RPM
   - DSMCommon RPM
2. Syslog イベントを QRadar に送信するように Carbon Black デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソール で Carbon Black ログ・ソースを追加してください。以下の表は、Carbon Black イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 72. *Carbon Black* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Carbon Black
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するように Carbon Black を構成

Carbon Black からイベントを収集するには、Carbon Black のイベントを IBM Security QRadar に送信するように、cb-event-forwarder を構成する必要があります。

始める前に

準備事項:

Carbon Black Enterprise RPM をインストールし、それが実行中であることを確認します。cb-event-forwarder は、CentOS 6.x を実行中の任意の 64 ビット Linux コンピューターにインストールできます。これは、Carbon Black サーバーと同じコンピューターにも、別のコンピューターにもインストールできます。多くのイベント (すべてのファイル変更、すべてのレジストリー変更、その両方など) を QRadar に転送する場合は、別個のサーバーに `cb-event-forwarder` をインストールしてください。多くのイベントを QRadar に転送しない場合は、Carbon Black サーバーに cb-event-forwarder をインストールしてかまいません。

Carbon Black サーバー以外のコンピューターに cb-event-forwarder をインストールする場合、次のように Carbon Black サーバーを構成する必要があります。

1. Carbon Black サーバー上の Iptables ファイアウォール経由で TCP ポート 5004 を使用できることを確認します。event-forwarder は、Carbon Black サーバー上の TCP ポート 5004 に接続して、Cb メッセージ・バスに接続します。
2. Carbon Black サーバー上の `/etc/cb/cb.conf` ファイルから、RabbitMQ のユーザー名およびパスワードを取得します。RabbitMQUser 変数および RabbitMQPassword 変数を検索し、それらの値を書き留めます。

このタスクについて

GitHub の Web サイト (https://github.com/carbonblack/cb-event-forwarder/) に、次の手順、ソース・コード、およびクイック・スタート・ガイドがあります。

手順

1. まだインストールされていない場合、次のように CbOpenSource リポジトリーをインストールします。

   ```
   cd /etc/yum.repos.d
   curl -O https://opensource.carbonblack.com/release/x86_64/CbOpenSource.repo
   ```

2. 次のように、cb-event-forwarder の RPM をインストールします。

   ```
   yum install cb-event-forwarder
   ```

3. `/etc/cb/integrations/event-forwarder/cb-event-forwarder.conf` ファイルを変更して `udpout=<QRadar_IP_address>:514` を追加し、`output_format=leef` と指定することで、出力形式として LEEF を指定します。
4. Carbon Black サーバー以外のコンピューターにインストールする場合、RabbitMQ のユーザー名およびパスワードを、`/etc/cb/integrations/event-forwarder/cb-event-forwarder.conf` ファイルの *rabbit_mq_username* 変数および *rabbit_mq_password* 変数にコピーします。 *cb_server_hostname* 変数に、Carbon Black サーバーのホスト名または IP アドレスを入力します。
5. 次のように、cb-event-forwarder を検査モードで実行することで、構成が有効であることを確認します。

   ```
   /usr/share/cb/integrations/event-forwarder/cb-event-forwarder -check
   ```

   有効な場合、`Initialized output` というメッセージが表示されます。エラーがある場合、それらのエラーが画面に出力されます。
6. キャプチャー対象のイベントのタイプを選択します。

デフォルトでは、Carbon Black はすべてのフィード・イベントおよび監視リスト・イベントをバス経由で発行します。生のセンサー・イベントやすべての binaryinfo 通知をキャプチャーする場合は、/etc/cb/cb.conf ファイル内でそれらの機能を有効にする必要があります。

- 生のセンサー・イベントをキャプチャーするには、/etc/cb/cb.conf ファイル内の DatastoreBroadcastEventTypes オプションを編集して、エクスポート対象の生のセンサー・イベントのブロードキャストを有効にします。
- バイナリー監視イベントをキャプチャーするには、/etc/cb/cb.conf ファイル内の EnableSolrBinaryInfoNotifications オプションを編集して、True に設定します。

7. /etc/cb/cb.conf 内のいずれかの変数を変更した場合、「service cb-enterprise restart」と入力して Carbon Black サーバーを再始動してください。
8. initctl start cb-event-forwarder と入力して initctl コマンドを使用することで、cb-event-forwarder サービスを開始します。

   注: initctl コマンド initctl stop cb-event-forwarder を使用すると、cb-event-forwarder サービスを停止できます。

第 22 章 BlueCat Networks Adonis

IBM Security QRadar 用の BlueCat Networks Adonis DSM は、BlueCat Proteus で管理される BlueCat Adonis アプライアンスから、syslog を使用してログ・イベント拡張フォーマット (LEEF) で転送されるイベントを受け取ります。

QRadar は、バージョン 6.7.1-P2 以降を使用して、BlueCat Networks Adonis アプライアンスをサポートします。

DNS イベントおよび DHCP イベントを QRadar と統合するには、BlueCat Networks Adonis へのパッチの適用が必要になる場合があります。詳しくは、*KB-4670* および *BlueCat Networks* の資料 を参照してください。

サポートされるイベント・タイプ

IBM Security QRadar は、DNS 照会および DHCP 照会に関連するすべてのイベントを収集できます。

これには、以下のイベントが含まれます。

- DNS IPv4 および IPv6 の照会イベント
- DNS ネーム・サーバー照会イベント
- DNS メール交換照会イベント
- DNS テキスト・レコード照会イベント
- DNS レコード更新イベント
- DHCP 検出イベント
- DHCP 要求イベント
- DHCP 解放イベント

イベント・タイプ・フォーマット

LEEF 形式は、syslog ヘッダー (パイプ (|) 区切り) とイベント・ペイロード (スペース区切り) で構成されます。

例:

```
Aug 10 14:55:30 adonis671-184
LEEF:1.0|BCN|Adonis|6.7.1|DNS_Query|cat=A_record src=10.10.10.10
url=test.example.com
```

BlueCat Adonis アプライアンスから転送された syslog イベントが、上記のサンプルに類似した形式になっていない場合は、デバイス構成を調べてください。LEEF イベント・メッセージは、適切にフォーマットされていると、BlueCat Networks Adonis DSM によって自動的に検出され、ログ・ソースとして IBM Security QRadar に追加されます。

始める前に

イベントをログ・イベント拡張フォーマット (LEEF) で生成し、syslog を使用してイベント出力を QRadar にリダイレクトするように、BlueCat Adonis を構成する必要があります。

BlueCat Networks は、syslog を構成する手助けとなるように、各アプライアンス上でスクリプトを提供しています。syslog のリダイレクトを実行するには、BlueCat Adonis アプライアンスまたは BlueCat Proteus アプライアンスのコマンド・ライン・インターフェースへの管理アクセス権限または root アクセス権限が必要です。アプライアンスに syslog の構成スクリプトがない場合は、BlueCat Networks の営業担当員に連絡してください。

BlueCat Adonis の構成

DNS イベントおよび DHCP イベントを IBM Security QRadar SIEM に転送するように BlueCat Adonis アプライアンスを構成できます。

手順

1. SSH を使用して、BlueCat Adonis アプライアンスにログインします。
2. コマンド・ライン・インターフェースで、以下のコマンドを入力して syslog 構成スクリプトを開始します。

   ```
   /usr/local/bluecat/QRadar/setup-QRadar.sh
   ```
3. QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
4. `yes` または `no` を入力して IP アドレスを確認します。

   成功メッセージが表示されたら、構成は完了です。

   BlueCat Networks Adonis の syslog イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。イベントが自動的に検出されない場合は、手動でログ・ソースを構成できます。

IBM Security QRadar でログ・ソースを構成する

IBM Security QRadar は、BlueCat Networks Adonis からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ただし、QRadar 用のログ・ソースを手動で作成して syslog イベントを受信することもできます。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**BlueCat Networks Adonis**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *73. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	BlueCat Networks Adonis アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 23 章 Blue Coat SG

IBM Security QRadar DSM for Blue Coat SG は、Blue Coat SG アプライアンスからイベントを収集します。

Blue Coat SG DSM の仕様を以下の表に示します。

表 *74. Blue Coat SG DSM* の仕様

仕様	値
製造元	Blue Coat
DSM 名	Blue Coat SG アプライアンス
RPM ファイル名	DSM-BluecoatProxySG-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	SG v4.x 以降
プロトコル	Syslog ログ・ファイル・プロトコル
記録されるイベント・タイプ	すべてのイベント
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	はい
その他の情報	Blue Coat Web サイト (http://www.bluecoat.com)

Blue Coat SG から QRadar にイベントを送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Blue Coat SG DSM RPM をダウンロードして QRadar コンソールにインストールしてください。
2. QRadar と通信するように Blue Coat SG デバイスを構成します。以下のステップを実行します。
   - カスタム・イベント・フォーマットを作成します。
   - ログ・ファシリティーを作成します。
   - アクセス・ロギングを使用可能にします。
   - ログ・ファイル・プロトコルまたは syslog アップロード用に Blue Coat SG を構成します。
3. QRadar コンソールで Blue Coat SG ログ・ソースを追加します。すべての必須パラメーターを構成します。ただし、Blue Coat SG 固有のパラメーターを構成するには、以下の表を使用してください。

表 *75. Blue Coat SG* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Bluecoat SG アプライアンス

表 75. *Blue Coat SG* ログ・ソース・パラメーター (続き)

パラメーター	値
プロトコル構成	「ログ・ファイル」または「Syslog」を選択します。

名前と値のペアのカスタム形式を使用して Blue Coat SG を構成する方法について説明します。ただし、QRadar は次の形式をサポートします。

- カスタム・フォーマット
- SQUID
- NCSA
- main
- IM
- ストリーミング
- smartreporter
- bcereportermain_v1
- bcreporterssl_v1
- p2p
- SSL
- bcreportercifs_v1
- CIFS
- MAPI

関連概念:

170 ページの『追加のカスタム・フォーマットのキー値ペアの作成』

関連タスク:

164 ページの『ログ・ファシリティーの作成』

IBM Security QRadar 用に作成したカスタム・ログ・フォーマットを使用するには、そのカスタム・ログ・フォーマットをファシリティーに関連付ける必要があります。

164 ページの『アクセス・ロギングの有効化』

Blue Coat SG デバイスでアクセス・ロギングを有効にする必要があります。

165 ページの『Blue Coat SG ログ・ソースの構成』

QRadar で、Blue Coat SG ログ・ソースを手動で構成できます。

165 ページの『FTP アップロードに対応する Blue Coat SG の構成』

FTP を使用して Blue Coat SG イベントを収集するには、Blue Coat アップロード・クライアントを使用して FTP サーバーにイベントをアップロードするように Blue Coat SC を構成します。

169 ページの『syslog に対応する Blue Coat SG の構成』

Syslog イベントを収集できるようにするには、Syslog イベントを IBM Security QRadar に転送するように Blue Coat SG アプライアンスを構成する必要があります。

カスタム・イベント・フォーマットの作成

Blue Coat SG からイベントを収集するには、カスタム・イベント・フォーマットを作成します。

手順

1. Blue Coat 管理コンソールにログインします。
2. 「構成」>「アクセス・ロギング **(Access Logging)**」>「フォーマット」を選択します。
3. 「新規」を選択します。
4. カスタム・フォーマットのフォーマット名を入力します。
5. 「カスタム・フォーマット・ストリング **(Custom format string)**」を選択します。
6. 以下のカスタム・フォーマットを入力します。

   重要**:** 以下の各例で改行があると、この構成が失敗する原因となります。コード・ブロックをテキスト・エディターにコピーし、改行を削除してから、「カスタム・フォーマット **(Custom Format)**」列に一行で貼り付けてください。

   ```
   Bluecoat|src=$(c-ip)|srcport=$(c-port)|dst=$(cs-uri-address)
   |dstport=$(cs-uri-port)|username=$(cs-username)|devicetime=$(gmttime)
   |s-action=$(s-action)|sc-status=$(sc-status)|cs-method=$(cs-method)
   |time-taken=$(time-taken)|sc-bytes=$(sc-bytes)|cs-bytes=$(cs-bytes)
   |cs-uri-scheme=$(cs-uri-scheme)|cs-host=$(cs-host)|cs-uri-path=$(cs-uri-path)
   |cs-uri-query=$(cs-uri-query)|cs-uri-extension=$(cs-uri-extension)
   |cs-auth-group=$(cs-auth-group)|rs(Content-Type)=$(rs(Content-Type))
   |cs(User-Agent)=$(cs(User-Agent))|cs(Referer)=$(cs(Referer))
   |sc-filter-result=$(sc-filter-result)|filter-category=$(sc-filter-category)
   |cs-uri=$(cs-uri)
   ```

7. リストから「最後のヘッダーをログに記録 **(Log Last Header)**」を選択します。
8. 「**OK**」をクリックします。
9. 「適用」をクリックします。

   注**:** QRadar のカスタム・フォーマットは、Blue Coat ELFF フォーマットを使用することで、さらに多くのキー値ペアをサポートします。詳しくは、 170 ページの『追加のカスタム・フォーマットのキー値ペアの作成』を参照してください。

次のタスク

Blue Coat デバイスでログ・ファシリティーを作成する準備ができました。

関連タスク:

164 ページの『ログ・ファシリティーの作成』

IBM Security QRadar 用に作成したカスタム・ログ・フォーマットを使用するには、そのカスタム・ログ・フォーマットをファシリティーに関連付ける必要があります。

ログ・ファシリティーの作成

IBM Security QRadar 用に作成したカスタム・ログ・フォーマットを使用するには、そのカスタム・ログ・フォーマットをファシリティーに関連付ける必要があります。

手順

1. 「構成」>「アクセス・ロギング **(Access Logging)**」>「ログ」を選択します。
2. 「新規」をクリックします。
3. 以下のパラメーターを構成します。

パラメーター	説明
ログ名	ログ・ファシリティーの名前。
ログ・フォーマット	作成したカスタム・フォーマット。
説明	ログ・ファシリティーの説明。

4. 「**OK**」をクリックします。
5. 「適用」をクリックします。

関連タスク:

『アクセス・ロギングの有効化』

Blue Coat SG デバイスでアクセス・ロギングを有効にする必要があります。

アクセス・ロギングの有効化

Blue Coat SG デバイスでアクセス・ロギングを有効にする必要があります。

手順

1. 「構成」>「アクセス・ロギング **(Access Logging)**」>「一般 **(General)**」を選択します。
2. 「アクセス・ロギングを有効にする **(Enable Access Logging)**」チェック・ボックスを選択します。
3. オプション: Blue Coat SGOS 6.2.11.2 Proxy Edition を使用している場合は、以下のステップを実行します。
   a. 「構成 **(Config)**」>「ポリシー **(Policy)**」>「ビジュアル・ポリシー・マネージャー **(Visual Policy Manager)**」を選択します。
   b. 「ポリシー」セクションで、「ロギング用 **Web** アクセス・レイヤー **(Web Access Layer for Logging)**」を追加します。
   c. 「アクション」>「編集」を選択し、ログ・ファシリティーに対するロギングを有効にします。
4. 「適用」をクリックします。

関連概念:

170 ページの『追加のカスタム・フォーマットのキー値ペアの作成』

FTP アップロードに対応する Blue Coat SG の構成

FTP を使用して Blue Coat SG イベントを収集するには、Blue Coat アップロード・クライアントを使用して FTP サーバーにイベントをアップロードするように Blue Coat SC を構成します。

手順

1. 「構成」 > 「アクセス・ロギング **(Access Logging)**」 > 「ログ」 > 「アップロード・クライアント **(Upload Client)**」を選択します。
2. 「ログ」リストから、カスタム・フォーマットを含むログを選択します。
3. 「クライアント・タイプ **(Client type)**」リストから、「**FTP** クライアント **(FTP Client)**」を選択します。
4. 「テキスト・ファイル **(text file)**」オプションを選択します。
5. 「設定」をクリックします。
6. 「設定対象 **(Settings For)**」リストから、「プライマリー **FTP** サーバー **(Primary FTP Server)**」を選択します。
7. 以下の値を構成します。

パラメーター	説明
ホスト	Blue Coat イベントを転送する FTP サーバーの IP アドレス。
ポート	FTP ポート番号。
パス	ログ・ファイルのディレクトリー・パス。
ユーザー名	FTP サーバーにアクセスするユーザー名。

8. 「**OK**」をクリックします。
9. 「アップロード・スケジュール **(Upload Schedule)**」タブを選択します。
10. 「アクセス・ログのアップロード **(Upload the access log)**」オプションから、「定期的 **(Periodically)**」を選択します。
11. 「接続試行間の待機時間 **(Wait time between connect attempts)**」オプションを構成します。
12. FTP へのログ・ファイルのアップロードを毎日行うか、間隔に基づいて行うかを選択します。
13. 「適用」をクリックします。

Blue Coat SG ログ・ソースの構成

QRadar で、Blue Coat SG ログ・ソースを手動で構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。

6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソース・タイプ」リストで「**Bluecoat SG** アプライアンス」を選択します。
8. 「プロトコル構成」リストで「ログ・ファイル」オプションを選択します。
9. 以下の値を構成します。

表 *76. Blue Coat SG* ログ・ファイル・プロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。 QRadar が固有のイベント・ソースのログ・ファイルを識別できる、IP アドレスまたはホスト名の入力が推奨されます。
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 オプションは、以下のとおりです。 • FTP - TCP ポート 21 • SFTP - TCP ポート 22 • SCP - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。
SSH 鍵ファイル	サービス・タイプとして「**SCP**」または「**SFTP**」を選択すると、このパラメーターにより、SSH 秘密鍵ファイルを定義することを選択できるようになります。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。

表 *76. Blue Coat SG* ログ・ファイル・プロトコル・パラメーター *(*続き*)*

パラメーター	説明
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。これは、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートするためです。
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」オプションは無視されます。
FTP ファイル・パターン	サービス・タイプとして「**SFTP**」または「**FTP**」を選択した場合、このオプションにより、リモート・ディレクトリーで指定されているファイルのリストをフィルターに掛けるために必要な正規表現 (regex) を構成することを選択できるようになります。一致するすべてのファイルは処理に組み込まれます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。例えば、末尾が `.log` のファイルを収集するには、以下を入力します。 `.*¥.log` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として「**FTP**」を選択した場合にのみ表示されます。「**FTP** 転送モード **(FTP Transfer Mode)**」パラメーターにより、FTP 経由でログ・ファイルを取得するときのファイル転送モードを定義することを選択できるようになります。 リストから、このログ・ソースに適用する転送モードを選択します。 FTP 転送モードとして ASCII を使用するときは、「プロセッサー」パラメーターに「なし」を、「イベント・ジェネレーター (Event Generator)」に「**LINEBYLINE**」を選択する必要があります。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。

表 76. *Blue Coat SG* ログ・ファイル・プロトコル・パラメーター (続き)

パラメーター	説明
開始時刻	処理を開始する時刻を入力します。例えば、午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、00:00 と入力します。 このパラメーターは、「繰り返し (Recurrence)」の値と連携して、リモート・ディレクトリーのファイルをスキャンするタイミングと頻度を設定します。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 (Ignore Previously Processed File)」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リモート・ホストにあるファイルが zip、gzip、tar、または tar+gzip のアーカイブ・フォーマットで保管されている場合は、アーカイブを展開して内容を処理することができるプロセッサーを選択します。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって既に処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが以前に処理されているかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。以前に処理されていないすべてのファイルがダウンロードされます。 このオプションは FTP および SFTP のサービス・タイプにのみ適用されます。

表 76. *Blue Coat SG* ログ・ファイル・プロトコル・パラメーター *(続き)*

パラメーター	説明
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar システム上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスはクリアしたままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー (Local Directory)」フィールドが表示されます。これによりファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、LineByLine を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに追加の処理を適用します。ファイルの各行が、単一イベントです。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

syslog に対応する Blue Coat SG の構成

Syslog イベントを収集できるようにするには、Syslog イベントを IBM Security QRadar に転送するように Blue Coat SG アプライアンスを構成する必要があります。

始める前に

注**:** Syslog イベントを複数の Syslog 宛先に送信する場合、1 つの Syslog 宛先での可用性が中断されると、Blue Coat SG アプライアンスから他の Syslog 宛先へのイベント・ストリームも中断される可能性があります。

手順

1. 「構成」 > 「アクセス・ロギング **(Access Logging)**」 > 「ログ」 > 「アップロード・クライアント **(Upload Client)**」を選択します。
2. 「ログ」リストから、カスタム・フォーマットを含むログを選択します。
3. 「クライアント・タイプ **(Client type)**」リストから、「カスタム・クライアント **(Custom Client)**」を選択します。
4. 「設定」をクリックします。
5. 「設定対象 **(Settings For)**」リストから、「プライマリー・カスタム・サーバー **(Primary Custom Server)**」を選択します。
6. 「ホスト」フィールドに、QRadar システムの IP アドレスを入力します。
7. 「ポート **(Port)**」フィールドに 514 を入力します。
8. 「**OK**」をクリックします。
9. 「アップロード・スケジュール **(Upload Schedule)**」タブを選択します。

10. 「アクセス・ログのアップロード **(Upload the access log)**」リストから、「継続的 **(Continuously)**」を選択します。
11. 「適用」をクリックします。

追加のカスタム・フォーマットのキー値ペアの作成

拡張ログ・ファイル・フォーマット (ELFF) のカスタム・フォーマットを使用して、特定の Blue Coat データまたはイベントを IBM Security QRadar に転送します。

カスタム・フォーマットはパイプ記号で区切った一連のフィールドであり、`Bluecoat|` フィールドで開始し、`$(Blue Coat ELFF)` パラメーターが含まれています。

例:

```
Bluecoat|src=$(c-ip)|srcport=$(c-port)|dst=$(cs-uri-address)|dstport=$(cs-uri-port)|username=$(cs-username)|devicetime=$(gmttime)|s-action=$(s-action)|sc-status=$(sc-status)|cs-method=$(cs-method)
```

表 77. カスタム・フォーマットの例

Blue Coat ELFF パラメーター	**QRadar** カスタム・フォーマットの例
sc-bytes	$(sc-bytes)
rs(Content-type)	$(rs(Content-Type))

使用可能な Blue Coat ELFF パラメーターについて詳しくは、Blue Coat アプライアンスの資料を参照してください。

第 24 章 Blue Coat Web Security Service

Blue Coat Web Security Service 用の IBM Security QRadar DSM は、Blue Coat Web Security Service からイベントを収集します。

以下の表は、Blue Coat Web Security Service DSM の仕様を示しています。

表 *78. Blue Coat Web Security Service DSM* の仕様

仕様	値
製造元	Blue Coat
DSM 名	Blue Coat Web Security Service
RPM ファイル名	DSM-BlueCoatWebSecurityService-*Qradar_version-build_number*.noarch.rpm
イベント・フォーマット	Blue Coat ELFF
記録されるイベント・タイプ	アクセス
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Blue Coat Web サイト (https://www.bluecoat.com)

Blue Coat Web Security Service を QRadar と統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - プロトコル共通 RPM
   - Blue Coat Web Security Service REST API プロトコル RPM
   - Blue Coat Web Security Service DSM RPM
2. Sync API への QRadar のアクセスを許可するように、Blue Coat Web Security Service を構成します。
3. Blue Coat Web Security Service ログ・ソースを QRadar コンソールに追加します。以下の表は、Blue Coat Web Security Service イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 79. *Blue Coat Web Security Service* ログ・ソース・パラメーター

パラメーター	値
プロトコル構成	Blue Coat Web Security Service からイベントを受信するために使用されるプロトコル。以下のプロトコル構成オプションを指定できます。 Blue Coat Web Security Service REST API (推奨) 転送
API ユーザー名 (API Username)	Blue Coat Web Security Service での認証に使用される API ユーザー名。API ユーザー名は、Blue Coat Threat Pulse ポータルを使用して構成されます。
パスワード	Blue Coat Web Security Service での認証に使用されるパスワード。
パスワードの確認	Box 管理者構成の「OAuth2 parameters」ペインに生成されます。
プロキシーの使用 (Use Proxy)	プロキシーを構成すると、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Blue Coat Web Security Service にアクセスします。 「プロキシー **IP** またはホスト名 **(Proxy IP or Hostname)**」、「プロキシー・ポート」、「プロキシー・ユーザー名」、および「プロキシー・パスワード」の各フィールドを構成します。プロキシーが認証を必要としない場合、「プロキシー・ユーザー名」フィールドと「プロキシー」「パスワード」フィールドはブランクのままでかまいません。
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	公開鍵を送信すると、「Public Key Management」ペインに生成されます。
繰り返し (Recurrence)	ログがいつデータを収集するかを指定できます。フォーマットは、月/時刻/日を表す M/H/D です。デフォルトは 5 M です。
EPS スロットル	1 秒あたりの最大イベント数 (EPS) の上限。デフォルトは 5000 です。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

QRadar との通信用に Blue Coat Web Security Service を構成する

Blue Coat Web Security Service からイベントを収集するには、IBM Security QRadar の API 鍵を作成する必要があります。API 鍵が存在する場合は、Blue Coat Web Security Service は既に構成されています。

手順

1. Blue Coat Threat Pulse ポータルにログインします。
2. 「**Service**」モードに切り替えます。
3. 「**Account Maintenance**」 > 「**MDM, API Keys**」をクリックします。
4. 「**Add API key**」をクリックして、API 鍵のユーザー名とパスワードを入力してから、「**Add**」をクリックします。

   ユーザー名とパスワードは、API のログ・ソースを構成する際に必要となります。

第 25 章 Box

Box 用の IBM Security QRadar DSM は、Box エンタープライズ・アカウントからエンタープライズ・イベントを収集します。

以下の表は、Box DSM の仕様を示しています。

表 *80. Box DSM* の仕様

仕様	値
製造元	Box
DSM 名	Box
RPM ファイル名	DSM-BoxBox-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	N/A
プロトコル	Box REST API
イベント・フォーマット	JSON
記録されるイベント・タイプ	管理者イベントとエンタープライズ・イベント
自動的に検出?	いいえ
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Box Web サイト (https://www.box.com/)

Box を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、次の RPM の最新バージョンをリストされている順序でダウンロードして QRadar コンソールにインストールしてください。
   - プロトコル共通 RPM
   - Box REST API プロトコル RPM
   - Box DSM RPM
2. API アクセスに対応するように Box エンタープライズ・アカウントを構成します。
3. 以下の表は、Box イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *81. Box* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Box
プロトコル構成	Box REST API
クライアント ID (Client ID)	Box 管理者構成の「OAuth2 parameters」ペインに生成されます。

表 *81. Box* ログ・ソース・パラメーター *(*続き*)*

パラメーター	値
クライアント秘密鍵 (Client Secret)	Box 管理者構成の「OAuth2 parameters」ペインに生成されます。
鍵 ID (Key ID)	公開鍵を送信すると、「Public Key Management」ペインに生成されます。
エンタープライズ ID (Enterprise ID)	アクセス・トークン要求に使用します。
秘密鍵ファイル名 (Private Key File Name)	QRadar の `/opt/qradar/conf/trusted_certificates/box/` ディレクトリー内の秘密鍵ファイル名。
プロキシーの使用 (Use Proxy)	QRadar がプロキシーを使用して Box API にアクセスする場合、「プロキシーの使用 (Use Proxy)」チェック・ボックスを選択します。 プロキシーが認証を必要とする場合、「プロキシー・サーバー」、「プロキシー・ポート」、「プロキシー・ユーザー名」、「プロキシー・パスワード」の各フィールドを構成します。 プロキシーが認証を必要としない場合、「プロキシー・サーバー」フィールドおよび「プロキシー・ポート」フィールドを構成します。
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	「はい」を選択すると、QRadar は、自動的にサーバー証明書をダウンロードし、ターゲット・サーバーを信頼し始めます。
EPS スロットル	1 秒あたりの最大イベント数。 デフォルトは 5000 です。
繰り返し (Recurrence)	Box API に対する新しいイベントのログ・ソース照会から次のログ・ソース照会までの間の時間間隔。この時間間隔は、時間数 (H)、分数 (M)、または日数 (D) にすることができます。 デフォルトは 10 分です。

Box のサンプル・イベント・メッセージを次の表に示します。

表 82. *Box* エンタープライズのサンプル・イベント・メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
LOGIN	ユーザー・ログイン成功	{"source":{"type":"user","id": "262196057","name":"UserName", "login":"username@ibm.com"}, "created_by":{"type":"user", "id":"262196057","name": "UserName","login": "username@ibm.com"}, "created_at":"2016-01-07T10 :54:30-08:00","event_id": "363714450","event_type":"LOGIN", "ip_address":"127.0.0.1","type" :"event","session_id":null, "additional_details":null}

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するための Box の構成

Box エンタープライズ・アカウントから管理者ログを取得するには、Box および IBM Security QRadar コンソールを構成する必要があります。

始める前に

開発者アカウントを持っている必要があります。

JSON Web トークン (JWT) アサーション用の RSA 秘密鍵/公開鍵ペアを生成します。

1. QRadar コンソールへの SSH セッションを開きます。
   - 秘密鍵の場合、以下のコマンドを入力します。

     ```
     openssl genrsa -out box_private_key.pem 2048
     ```
   - 公開鍵の場合、以下のコマンドを入力します。

     ```
     openssl rsa -pubout -in box_private_key.pem -out box_public_key.pem
     ```

     注:

     公開鍵のコピーを保存します。API アクセスに対応するように Box を構成するときには、公開鍵の内容を「公開鍵の追加 **(Add Public Key)**」テキスト・ボックスに貼り付ける必要があります。
   - 以下のコマンドを 1 行で入力して、秘密鍵を DER に変換します。

     ```
     openssl pkcs8 -topk8 -inform PEM -outform DER
      -in box_private_key.pem -out box_private_key.der -nocrypt
     ```
2. QRadar に秘密鍵を保管します。

a. QRadar の opt/qradar/conf/trusted_certificates/ ディレクトリーに box という名前のディレクトリーを作成します。

b. 作成した opt/qradar/conf/trusted_certificates/box ディレクトリーに秘密鍵 .DER ファイルをコピーします。その他の場所に秘密鍵を保管しないでください。

c. opt/qradar/conf/trusted_certificates/box ディレクトリー内の秘密鍵ファイルのファイル名のみを使用して、ログ・ソースを構成します。ログ・ソースを構成するときには、「秘密鍵ファイル名 **(Private Key File Name)**」フィールドにファイル名を正しく入力してください。

重要**:** ログ・ソースを構成する前に opt/qradar/conf/trusted_certificates/box ディレクトリーに秘密鍵をコピーします。秘密鍵を保管する前にログ・ソースを構成すると、エラー・メッセージが表示されます。

手順

1. Box Developers ポータル (http://developers.box.com/) にログインします。これで、管理コンソールおよび Box コンソールにアクセスできます。

   a. 「**Box** アプリケーションの作成 **(Create a Box Application)**」をクリックして、QRadar アプライアンス用のアプリケーションを作成します。

   b. 「クライアント **ID (client ID)**」、および「OAuth2」パラメーター・ペイン内の「クライアント秘密鍵 **(client secret)**」を記録します。ログ・ソースは、「クライアント **ID (client ID)**」および「クライアント秘密鍵 **(client secret)**」を使用して構成されます。

   c. 「サーバー認証 **(OAuth2.0 with JWT) (Server Authentication (OAuth2.0 with JWT))**」を選択し、「すべてのユーザー **(All Users)**」を選択します。

   d. 「バックエンド (Backend)」パラメーター・ペイン内にある API キーを記録します。API キーは、新規アプリケーションを許可するために必要です。

   e. 「OAuth2」パラメーター・ペインで、「ユーザー・アクセス設定 **(User Access Settings)**」リストから「すべてのユーザー **(All Users)**」を選択し、以下のパラメーターを構成します。

表 *83.* 「ユーザー・アクセス設定 *(User Access Settings)*」パラメーター

パラメーター	値
認証タイプ (Authentication Type):	サーバー認証 (OAuth2.0 with JWT) (Server Authentication (OAuth2.0 with JWT))
ユーザー・アクセス (User Access):	すべてのユーザー (All Users)

表 83. 「ユーザー・アクセス設定 (User Access Settings)」パラメーター (続き)

パラメーター	値
有効範囲 (Scopes):	内容 **(Content)** Box 内に保管されているすべてのファイルおよびフォルダーの読み取り/書き込みを行います。 エンタープライズ **(Enterprise)** 「エンタープライズのプロパティーの管理 **(Manage an enterprise's properties)**」。アプリケーションにエンタープライズ属性とレポートの表示および編集を許可します。デバイス・ピナーの編集および削除を許可します。 **重要:** 正しい有効範囲を選択しないと、Box API がエラー・メッセージを表示します。

2. 公開鍵を送信し、鍵 ID を生成します。
   a. 「公開鍵の管理 (Public Key Management)」ペインで、「公開鍵の追加 **(Add Public Key)**」をクリックします。
   b. QRadar からコピーした公開鍵ファイルを開き、公開鍵ファイルの内容を「公開鍵の追加 **(Add Public Key)**」テキスト・ボックスに貼り付けます。
   c. 「確認 **(Verify)**」をクリックします。
   d. 「保存 **(Save)**」をクリックし、ログ・ソース構成の鍵 ID を記録します。
   e. プロパティーがサーバー上に確実に保管されるように、ページの下部にスクロールし、「保存 **(Save)**」をクリックします。
3. Box エンタープライズ ID を記録します。
   a. 管理コンソールにログインし、「設定 **(Settings)**」をクリックします。
   b. エンタープライズ ID を見つけるには、「アカウント情報 **(Account Info)**」タブをクリックします。
4. アプリケーションを許可します。
   a. Box コンソールにログインし、「設定 **(Settings)**」をクリックします。
   b. 「アプリケーション **(Apps)**」タブをクリックします。
   c. 「カスタム・アプリケーション (Custom Applications)」ペインで、「新規アプリケーションの許可 **(Authorize New App)**」をクリックします。
   d. 「アプリケーションの許可 **(App Authorization)**」ウィンドウで、API キーを入力し、「次へ **(Next)**」をクリックします。アクセス・レベルが「すべてのユーザー **(All Users)**」であることを確認します。
   e. 「許可 **(Authorize)**」をクリックします。

   QRadar と通信するための Box の構成について詳しくは、Box Web サイト (https://docs.box.com/docs/configuring-box-platform) を参照してください。

次のタスク

QRadar が Box DSM からイベントを受信するように構成されていることを確認します。QRadar が正しく構成されている場合は、「ログ・ソースの編集」ウィンドウにエラー・メッセージが表示されません。

第 26 章 Bridgewater

IBM Security QRadar 用の Bridgewater Systems DSM は、syslog を使用してイベントを受け入れます。

QRadar は、syslog を使用して Bridgewater AAA サービス・コントローラー・デバイスから転送される、関連するすべてのイベントを記録します。

Bridgewater Systems 用の Syslog の構成

syslog イベントを IBM Security QRadar に送信するように Bridgewater Systems アプライアンスを構成する必要があります。

手順

1. Bridgewater Systems デバイスのコマンド・ライン・インターフェース (CLI) にログインします。
2. 操作メッセージのログを RADIUS および Diameter サーバーに記録する場合は、以下のファイルを開きます。

   ```
   /etc/syslog.conf
   ```
3. すべての操作メッセージをログに記録する場合は、以下の行のコメントを外します。

   ```
   local1.info /WideSpan/logs/oplog
   ```
4. エラー・メッセージのログのみを記録する場合は、`local1.info /WideSpan/logs/oplog` の行を以下の行に変更します。

   ```
   local1.err /WideSpan/logs/oplog
   ```

   注: RADIUS および Diameter システム・メッセージは、`/var/adm/messages` ファイルに保管されます。
5. 以下の行を追加します。

   `local1.*@<`*IP address*`>`

   ここで、<*IP address*> は、QRadar コンソールの IP アドレスです。
6. RADIUS および Diameter サーバー・システム・メッセージは、`/var/adm/messages` ファイルに保管されます。システム・メッセージについて以下の行を追加します。

   <*facility*>`*@<`*IP address*`>`

   各部分について以下で説明します。

   <*facility*> は、`/var/adm/messages` ファイルにログを記録する際に使用するファシリティーです。

<*IP address*> は、QRadar コンソールの IP アドレスです。

7. ファイルを保存して終了します。
8. ハングアップ・シグナルを syslog デーモンに送信して、すべての変更が確実に適用されるようにします。

```
kill -HUP `cat /var/run/syslog.pid`
```

構成は完了です。Bridgewater Systems アプライアンス・イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Bridgewater Systems アプライアンスによって QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Bridgewater Systems アプライアンスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Bridgewater Systems AAA** サービス・コントローラー」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 84. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Bridgewater Systems アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 27 章 Brocade Fabric OS

IBM Security QRadar は、Fabric OS V7.x を使用する Brocade のスイッチおよびアプライアンスから syslog システム・イベントおよび監査イベントを収集し、分類することができます。

syslog イベントを収集するには、syslog イベントを転送するようにスイッチを構成する必要があります。各スイッチまたは各アプライアンスを、イベントを転送するように構成してください。

Brocade スイッチから転送されるイベントは、自動的に検出されます。ログ・ソースは、QRadar にイベントを転送するスイッチまたはアプライアンスごとに構成されます。

Brocade Fabric OS アプライアンス用の syslog の構成

イベントを収集するには、イベントを IBM Security QRadar に転送するように Brocade アプライアンスで syslog を構成する必要があります。

手順

1. アプライアンスに管理ユーザーとしてログインします。
2. syslog イベントを転送するようにアドレスを構成するには、以下のコマンドを入力します。

   ```
   syslogdipadd <IP address>
   ```

   ここで、*<IP address>* は、QRadar コンソール、イベント・プロセッサー (Event Processor)、イベント・コレクター (Event Collector)、またはオールインワン・システムの IP アドレスです。
3. アドレスを確認するには、以下のコマンドを入力します。

   ```
   syslogdipshow
   ```

タスクの結果

Brocade スイッチがイベントを生成すると、スイッチがイベントを、指定した syslog 宛先に転送します。十分なイベントが Brocade アプライアンスによって転送されると、ログ・ソースが自動的に検出されます。通常、ログ・ソースの自動検出に必要なイベントの最小数は 25 です。

次のタスク

管理者が QRadar コンソールにログインして、QRadar コンソールでログ・ソースが作成されていること、および「ログ・アクティビティー」タブに Brocade アプライアンスからのイベントが表示されていることを確認できます。

第 28 章 CA Technologies

いくつかの CA Technologies DSM を IBM Security QRadar と統合できます。

このセクションでは、以下の DSM についての情報を提供します。

- 『CA ACF2』
- 203 ページの『CA SiteMinder』
- 206 ページの『CA Top Secret』

CA ACF2

IBM Security QRadar は、CA Access Control Facility (ACF2) イベントを統合できます。

以下の 2 つのオプションがあります。

- 『IBM Security zSecure を使用した CA ACF2 と IBM Security QRadar の統合』
- 192 ページの『監査スクリプトを使用した CA ACF2 と IBM Security QRadar の統合』

IBM Security zSecure を使用した CA ACF2 と IBM Security QRadar の統合

CA ACF2 DSM は、IBM z™/OS メインフレーム上の ACF2 イメージからの LEEF イベントを、IBM Security zSecure™ を使用して統合します。

zSecure プロセスを使用すると、System Management Facilities (SMF) からのイベントは、ログ・イベント拡張フォーマット (LEEF) のイベント・ファイルに記録されます。QRadar は、ログ・ファイル・プロトコルを使用して LEEF イベント・ログ・ファイルを取得し、イベントを処理します。ポーリング間隔に基づいてイベントを取得するように QRadar をスケジュールできます。これにより、QRadar は、定義されたスケジュールに基づいてイベントを取得できます。

CA ACF2 イベントを統合するには、以下のようにします。

1. インストール済み環境が、前提条件となるインストール要件をすべて満たしていることを確認します。
2. イベントを LEEF 形式で書き込むように CA ACF2 z/OS® イメージを構成します。詳しくは、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。
3. CA ACF2 が LEEF 形式のイベント・ログを取得するために、QRadar でログ・ソースを作成します。
4. オプション。QRadar で CA ACF2 用のカスタム・イベント・プロパティーを作成します。詳しくは、テクニカル・ノート「IBM Security QRadar *Custom Event Properties for IBM z/OS*」を参照してください。

始める前に

データ収集プロセスを構成する前に、基本の zSecure インストール・プロセスを完了する必要があります。

以下のインストール前提条件が必須です。

- z/OS イメージ上の IBM Security zSecure Audit で parmlib メンバーの IFAPRDxx が有効になっていることを確認する必要があります。
- SCKRLOAD ライブラリーは APF が許可されていなければなりません。
- CKFREEZE と UNLOAD のデータ・セットが定期的に更新されるようにプロセスを構成する必要があります。
- LEEF イベント・ファイルをダウンロードするには、QRadar に対して z/OS イメージ上の SFTP、FTP、または SCP の各サーバーを構成する必要があります。
- QRadar と z/OS イメージの間にあるファイアウォールで SFTP トラフィック、FTP トラフィック、または SCP トラフィックを許可する必要があります。

ソフトウェアをインストールした後に、ポストインストール・アクティビティーを実行して、構成を作成および変更する必要もあります。 zSecure のインストールおよび構成の手順については、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。

IBM Security QRadar での ACF2 のログ・ソースの作成

ログ・ファイル・プロトコルを使用して、イベントを含むアーカイブ・ログ・ファイルをリモート・ホストから取得できます。

このタスクについて

ログ・ファイルは、一度に 1 つずつ、処理のために IBM Security QRadar に転送されます。ログ・ファイル・プロトコルは、プレーン・テキストのイベント・ログや圧縮ファイル、アーカイブを管理できます。アーカイブには、一度に 1 行ずつ処理できるプレーン・テキスト・ファイルが含まれている必要があります。複数行イベント・ログは、ログ・ファイル・プロトコルではサポートされていません。zSecure が含まれた IBM z/OS は、指定されたディレクトリーにログ・ファイルを `gzip` アーカイブとして書き込みます。QRadar は、アーカイブを取り出し、ファイルに 1 行当たり 1 イベントで書き込まれているイベントを処理します。

これらのイベントを取得するには、ログ・ファイル・プロトコルを使用してログ・ソースを作成する必要があります。QRadar は、LEEF 形式のイベント・ファイルをホストするシステムにログインするための資格情報と、ポーリング間隔を要求します。

CA ACF2 用に QRadar でログ・ソースを構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。

5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**CA ACF2**」を選択します。
9. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
10. 以下の値を構成します。

表 85. CA ACF2 ログ・ファイル・パラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。IP アドレスまたはホスト名により、QRadar はログ・ファイルを固有のイベント・ソースに突き合わせることができます。 **例:** ネットワークに複数のデバイス (例えば、複数の z/OS イメージ)、またはすべてのイベント・ログが入っているファイル・リポジトリーが含まれている場合、ログ・ソースを一意的に識別するデバイスの IP アドレスまたはホスト名を指定します。これにより、ファイル・リポジトリーのイベントを識別する代わりに、ネットワーク内のデバイス・レベルでイベントを識別できるようになります。
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 • SFTP - SSH ファイル転送プロトコル • FTP - ファイル転送プロトコル • SCP - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得する基礎のプロトコルでは、「リモート **IP** またはホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。

表 *85. CA ACF2* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 このオプションには、以下のポートがあります。 • FTP - TCP ポート 21 • SFTP - TCP ポート 22 • SCP - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。
SSH 鍵ファイル	「サービス・タイプ」として SCP または SFTP を選択した場合、このパラメーターで SSH 秘密鍵ファイルを定義します。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。これにより、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムがサポートされます。

表 *85. CA ACF2* ログ・ファイル・パラメーター (続き)

パラメーター	説明
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、「再帰的 **(Recursive)**」チェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」オプションは無視されます。
FTP ファイル・パターン	「サービス・タイプ」として SFTP または FTP を選択した場合、このオプションにより、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするための正規表現 (regex) を構成します。一致するすべてのファイルは処理に組み込まれます。 IBM Security zSecure Audit を使用した IBM z/OS メインフレームは、`ACF2.<timestamp>.gz` というパターンを使用してイベント・ファイルを書き込みます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。 **例:** 例えば、先頭が ACF2 で末尾が `.gz` のファイルを収集するには、以下のコマンドを入力します。 `ACF2.*¥.gz` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト *http://download.oracle.com/javase/tutorial/essential/regex/* を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として FTP を選択した場合にのみ表示されます。リストから「バイナリー **(Binary)**」を選択します。 バイナリー転送モードは、`zip`、`gzip`、`tar`、`tar+gzip` アーカイブ・ファイルなど、バイナリー (圧縮) フォーマットで保管されたイベント・ファイルに対して使用します。
SCP リモート・ファイル	サービス・タイプとして「**SCP**」を選択する場合は、リモート・ファイルのファイル名を入力する必要があります。

表 *85. CA ACF2* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
開始時刻	処理を開始する時刻を入力します。 **例:** 午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、`00:00` と入力します。 このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 **例:** リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、`2H` と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「**gzip**」を選択します。 プロセッサーにより、イベント・ファイル・アーカイブを解凍し、内容をイベント用に処理できます。ファイルは、QRadar にダウンロードされた後にのみ処理されます。 QRadar は、`zip`、`gzip`、`tar`、または `tar+gzip` の各アーカイブ・フォーマットのファイルを処理できます。

表 *85. CA ACF2* ログ・ファイル・パラメーター (続き)

パラメーター	説明
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが以前に処理されたかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。以前に処理されていないすべてのファイルがダウンロードされます。 このオプションは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスをクリアのままにしないでください。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。このフィールドでは、ファイルの保管用のローカル・ディレクトリーを構成します。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに複数の処理を適用します。ファイルの各行が、単一イベントです。**例:** ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

CA ACF2 の構成は完了です。構成でカスタム・イベント・プロパティーが必要な場合は、テクニカル・ノート「QRadar *Custom Event Properties for IBM z/OS*」を参照してください。

監査スクリプトを使用した CA ACF2 と IBM Security QRadar の統合

CA Access Control Facility (ACF2) DSM は、ログ・ファイル・プロトコルを使用して IBM メインフレームでのイベントおよび監査トランザクションを収集します。

QexACF2.load.trs は、QEXACF2 プログラムを含む PDS LOADLIB が格納される TERSED ファイルです。TERSED ファイルは、zip ファイルに類似しており、中身を解凍するために、TRSMAIN プログラムを使用する必要があります。TRSMAIN プログラムは、IBM サポート (www.ibm.com/support) から入手できます。

TRS ファイルをワークステーションからアップロードするには、DCB 属性 DSORG=PS、RECFM=FB、LRECL=1024、BLKSIZE=6144 を使用して、ファイルを事前割り振りする必要があります。ファイル転送タイプは、BINARY APPEND でなければなりません。転送タイプが TEXT または TEXT APPEND の場合、ファイルを適切に解凍できません。

ファイルがメインフレームにアップロードされ、割り振られたデータ・セットに格納されると、TRSMAIN ユーティリティーでサンプル JCL (tar パッケージにも含まれています) を使用して TERSED ファイルを解凍できます。TRSMAIN ユーティリティーの戻りコード 0008 は、データ・セットが有効な TERSED ファイルとして認識されていないことを示します。このコード (0008) のエラーは、ファイルが正しい DCB 属性を使用してメインフレームにアップロードされなかったか、転送が BINARY APPEND 転送メカニズムを使用して実行されなかったことが原因として考えられます。

LOADLIB ファイルを正常に解凍したら、サンプル JCL ファイルを使用して QEXACF2 プログラムを実行できます。サンプル JCL ファイルは、tar コレクションに含まれています。QEXACF2 プログラムを実行するには、ローカルの命名規則およびジョブ・カードの要件に合わせて JCL を変更する必要があります。このプログラムが LINKLISTED ライブラリー内に配置されない場合は、STEPLIB DD を使用しなければならない場合もあります。

CA ACF2 イベントを IBM Security QRadar と統合するためのステップは、以下のとおりです。

1. IBM メインフレームが、すべてのセキュリティー・イベントをサービス・マネジメント・フレームワーク (SMF) レコードとしてライブ・リポジトリーに記録します。
2. CA ACF2 データが、SMF ダンプ・ユーティリティーを使用してライブ・リポジトリーから抽出されます。SMF ファイルには、前日のすべてのイベントおよびフィールドが未加工の SMF 形式で格納されています。
3. QexACF2.load.trs プログラムが、SMF 形式ファイルからデータをプルします。QexACF2.load.trs プログラムは、QRadar の関連イベントおよび関連フィールドのみをプルし、互換性を考慮して、その情報を圧縮形式で書き込みます。この情報は、QRadar がアクセスできる場所に保存されます。
4. QRadar は、ログ・ファイル・プロトコル・ソースを使用して、スケジュールに基づいて出力ファイル情報を取得します。次に、QRadar はこのファイルをインポートして、処理します。

IBM Security QRadar と統合するための CA ACF2 の構成

IBM Security QRadar は、スクリプトを使用して CA ACF2 インストール済み環境からのイベントを監査します。これらのイベントは、ログ・ファイル・プロトコルを使用して取得されます。

手順

1. IBM サポート Web サイト (http://www.ibm.com/support) から、以下の圧縮ファイルをダウンロードします。

   `qexacf2_bundled.tar.gz`

2. Linux のオペレーティング・システム上で、以下のファイルを解凍します。

   `tar -zxvf qexacf2_bundled.tar.gz` アーカイブには、以下のファイルが含まれています。

   - `QexACF2.JCL.txt` - ジョブ制御言語ファイル
   - `QexACF2.load.trs` - 圧縮プログラム・ライブラリー (IBM TRSMAIN が必要)
   - `trsmain sample JCL.txt` - TRSMAIN が `.trs` ファイルを圧縮解除するためのジョブ制御言語

3. 以下の方法を使用して、各ファイルを IBM メインフレームにロードします。

   TEXT プロトコルを使用して、サンプルの `QexACF2_trsmain_JCL.txt` ファイルおよび `QexACF2.JCL.txt` ファイルをアップロードします。

4. BINARY モード転送を使用して `QexACF2.load.trs` ファイルをアップロードし、事前割り振りデータ・セットに追加します。`QexACF2.load.trs` ファイルは、実行可能ファイル (メインフレーム・プログラム `QexACF2`) が含まれている簡潔なファイルです。`.trs` ファイルをワークステーションからアップロードするときに、DCB 属性
   DSORG=PS、RECFM=FB、LRECL=1024、BLKSIZE=6144 を使用して、メインフレーム上でファイルを事前割り振りします。ファイル転送タイプは、テキストではなくバイナリー・モードでなければなりません。

   注: `QexACF2` は、TSSUTIL の出力 (EARLOUT データ) を 1 行ずつ読み取る小さな C メインフレーム・プログラムです。`QexACF2` は、イベント情報 (例えば、レコード記述子、日付、時刻) が含まれているヘッダーを各レコードに追加します。このプログラムは各フィールドを出力レコードに書き込み、末尾ブランク文字を抑止し、各フィールドをパイプ文字で区切ります。この出力ファイルは QRadar 用にフォーマット設定されており、ブランクの抑止により、QRadar へのネットワーク・トラフィックが削減されます。このプログラムは、CPU や I/O ディスクのリソースを消費しません。

5. インストール済み環境固有のパラメーターに応じて、`trsmain sample_JCL.txt` ファイルをカスタマイズします。

   例: ジョブ・カード、データ・セット命名規則、出力宛先、保存期間、スペース所要量。

trsmain sample_JCL.txt ファイルは IBM ユーティリティー TRSMAIN を使用して、QexACF2.load.trs ファイルに保管されているプログラムを抽出します。

QexACF2_trsmain_JCL.txt ファイルの例として、以下の情報が含まれています。

```
//TRSMAIN JOB (yourvalidjobcard),Q1labs,
// MSGCLASS=V
//DEL EXEC PGM=IEFBR14
//D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXACF2.LOAD.TRS
// UNIT=SYSDA,
// SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE DD DISP=SHR,DSN=<yourhlq>.QEXACF2.LOAD.TRS
//OUTFILE DD DISP=(NEW,CATLG,DELETE),
// DSN=<yourhlq>.LOAD,
// SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA
//
```

.trs 入力ファイルは、IBM TERSE フォーマットのライブラリーであり、TRSMAIN を呼び出す JCL の実行によって取り出されます。この簡潔なファイルは抽出時に、QexACF2 プログラムをメンバーとして持つ PDS LINKLIB を作成します。

6. STEPLIB をこのライブラリーに対して実行するか、または LINKLST 内にある LINKLIB の 1 つにこのプログラムを移動することを選択できます。このプログラムには許可は必要ありません。
7. アップロード後に、プログラムを既存のリンク・リスト・ライブラリーにコピーするか、またはプログラムを含むことになるライブラリーの、正しいデータ・セット名を持つ STEPLIB DD ステートメントを追加します。
8. QexACF2_jcl.txt ファイルは、サンプル JCL が含まれているテキスト・ファイルです。構成を満たすようにジョブ・カードを構成する必要があります。

   QexACF2_jcl.txt サンプル・ファイルには、以下が含まれています。

```
//QEXACF2 JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXACF2 JCL VERSION 1.0 OCTOBER, 2010
//*
//*************************************************************
//* Change below dataset names to sites specific datasets names*
```

```
//QEXACF2 JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXACF2 JCL VERSION 1.0 OCTOBER, 2010
//*
//*************************************************************
//* Change below dataset names to sites specific datasets names*
//*************************************************************
//SET1 SET SMFIN='MVS1.SMF.RECORDS(0)',
// QEXOUT='Q1JACK.QEXACF2.OUTPUT',
// SMFOUT='Q1JACK.ACF2.DATA'
//*************************************************************
//* Delete old datasets *
//*************************************************************
//DEL EXEC PGM=IEFBR14
```

```
//DD1 DD DISP=(MOD,DELETE),DSN=&SMFOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//DD2 DD DISP=(MOD,DELETE),DSN=&QEXOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//* Allocate new dataset *
//*************************************************************
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DISP=(NEW,CATLG),DSN=&QEXOUT,
// SPACE=(CYL,(100,100)),
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*************************************************************
//* Execute ACFRPTPP (Report Preprocessor GRO) to extract ACF2*
//* SMF records *
//*************************************************************
//PRESCAN EXEC PGM=ACFRPTPP
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//RECMAN1 DD DISP=SHR,DSN=&SMFIN
//SMFFLT DD DSN=&SMFOUT,SPACE=(CYL,(100,100)),DISP=(,CATLG),
// DCB=(RECFM=FB,LRECL=8192,BLKSIZE=40960),
// UNIT=SYSALLDA
//*************************************************************
//* execute QEXACF2 *
//*************************************************************
//EXTRACT EXEC PGM=QEXACF2,DYNAMNBR=10,
// TIME=1440
//STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN DD DUMMY

//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//CFG DD DUMMY
//ACFIN DD DISP=SHR,DSN=&SMFOUT
//ACFOUT DD DISP=SHR,DSN=&QEXOUT
//*************************************************************
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//*
```

9. 出力ファイルの作成後に、以下のいずれかのオプションを選択する必要があります。

   出力ファイルを一時 FTP サーバーに転送するジョブをスケジュールします。ジョブが完了するたびに、出力ファイルが一時 FTP サーバーに転送されます。出力を一時 FTP サーバーに正常に転送するために、サンプル JCL で以下のパラメーターを構成する必要があります。

   例:

```
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
```

```
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

各部分について以下で説明します。

<*IPADDR*> は、出力ファイルを受信するための一時 FTP サーバーの IP アドレスまたはホスト名です。

<*USER*> は、一時 FTP サーバーへのアクセスに必要なユーザー名です。

<*PASSWORD*> は、一時 FTP サーバーへのアクセスに必要なパスワードです。

<*THEIPOFTHEMAINFRAMEDEVICE*> は、出力を受信するメインフレームまたは一時 FTP サーバーの宛先です。

例:

```
PUT 'Q1JACK.QEXACF2.OUTPUT.C320' /192.168.1.101/ACF2/QEXACF2.
OUTPUT.C320
```

<QEXOUTDSN> は、一時 FTP サーバーに保存される出力ファイルの名前です。

これで、QRadar でログ・ソースを作成する準備ができました。詳しくは、218 ページの『ログ・ソースの作成』を参照してください。

10. CA ACF2 から出力ファイルを取得するように QRadar をスケジュールします。

    zOS プラットフォームが FTP または SFTP 経由でファイルを提供するように構成されているか、または SCP を許可するように構成されている場合、一時 FTP サーバーは不要であり、QRadar は出力ファイルをメインフレームから直接プルすることができます。QexACF2_jcl.txt ファイルで、以下のテキストは、//* を使用してコメント化するか削除する必要があります。

```
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

次のタスク

これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの作成

ログ・ファイル・プロトコル・ソースにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

このタスクについて

CA ACF2 DSM は、ログ・ファイル・プロトコル・ソースを使用して、ログ・ファイルの一括ロードをサポートします。ログ・ファイル・プロトコルを使用するように CA ACF2 DSM を構成する際には、CA ACF2 で構成されているホスト名または IP アドレスが、ログ・ファイル・プロトコル構成の**「リモート・ホスト」**パラメーターに構成されているホスト名または IP アドレスと同じになっているようにしてください。

CA ACF2 用に QRadar でログ・ソースを構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**CA ACF2**」を選択します。
9. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
10. 以下の値を構成します。

表 86. CA ACF2 ログ・ファイル・パラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。QRadar によって QRadar がログ・ファイルを固有のイベント・ソースに識別できる IP アドレスまたはホスト名。 **例:** ネットワークに複数のデバイス (例えば、複数の z/OS イメージ)、またはすべてのイベント・ログが入っているファイル・リポジトリーが含まれている場合、ログ・ソースを一意的に識別するデバイスの IP アドレスまたはホスト名を指定する必要があります。この処理により、ファイル・リポジトリーのイベントを識別する代わりに、ネットワーク内のデバイス・レベルでイベントを識別できるようになります。

表 *86. CA ACF2* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 • SFTP - SSH ファイル転送プロトコル • FTP - ファイル転送プロトコル • SCP - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得する基礎のプロトコルでは、「リモート **IP** またはホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 以下のポート番号は、オプションの一部です。 • FTP - TCP ポート 21 • SFTP - TCP ポート 22 • SCP - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。

表 *86. CA ACF2* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
SSH 鍵ファイル	「サービス・タイプ」として SCP または SFTP を選択した場合、このパラメーターで SSH 秘密鍵ファイルを定義します。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。このオプションの目的は、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートすることです。
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」オプションは無視されます。

表 *86. CA ACF2* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
FTP ファイル・パターン	「サービス・タイプ」として SFTP または FTP を選択した場合、このオプションにより、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするための正規表現 (regex) を構成します。一致するすべてのファイルは処理に組み込まれます。 IBM Security zSecure Audit が含まれている IBM z/OS メインフレームは、`zOS.<timestamp>.gz` というパターンでイベント・ファイルを書き込みます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。 **例:** 先頭が zOS で末尾が `.gz` のファイルを収集するには、以下のコマンドを入力します。 `ACF2.*¥.gz` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として FTP を選択した場合にのみ表示されます。リストから「バイナリー **(Binary)**」を選択します。 バイナリー転送モードは、`zip`、`gzip`、`tar`、`tar+gzip` アーカイブ・ファイルなど、バイナリー (圧縮) フォーマットで保管されたイベント・ファイルに対して使用します。
SCP リモート・ファイル	「サービス・タイプ」として SCP を選択した場合は、リモート・ファイルのファイル名を入力する必要があります。

表 *86. CA ACF2* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
開始時刻	処理を開始する時刻を入力します。 **例:** 午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、`00:00` と入力します。 このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、`2H` と入力します。デフォルトは `1H` です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「**gzip**」を選択します。 プロセッサーにより、イベント・ファイル・アーカイブを解凍し、内容をイベント用に処理できます。ファイルは、QRadar にダウンロードされた後にのみ処理されます。QRadar は、`zip`、`gzip`、`tar`、または `tar+gzip` の各アーカイブ・フォーマットのファイルを処理できます。

表 *86. CA ACF2* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが処理されているかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。処理されていないすべてのファイルがダウンロードされます。 このオプションは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスをクリアのままにしないでください。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これにより、ファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに複数の処理を適用します。ファイルの各行が、単一イベントです。**例:** ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

CA ACF2 の構成は完了です。構成でカスタム・イベント・プロパティーが必要な場合は、テクニカル・ノート「QRadar *Custom Event Properties for IBM z/OS*」を参照してください。

CA SiteMinder

CA SiteMinder DSM は、syslog-ng を使用して CA SiteMinder アプライアンスから許可イベントを収集し、分類します。

CA SiteMinder DSM は、`smaccess.log` に記録されているアクセス・イベントおよび許可イベントを受け入れ、syslog-ng を使用してこのイベントを IBM Security QRadar に転送します。

ログ・ソースの構成

IBM Security QRadar を備えた CA SiteMinder は、CA SiteMinder アプライアンスから syslog-ng を使用して転送された許可イベントを自動的に検出することはありません。

このタスクについて

CA SiteMinder ログ・ソースを手動で作成するには、以下のようにします。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
3. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
4. 「ログ・ソース名」フィールドに、CA SiteMinder ログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「**CA SiteMinder**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコルのパラメーターが表示されます。

   注**:** ログ・ファイル・プロトコルは、「プロトコル構成」リストに表示されます。ただし、ログ・ファイルのポーリングは、適切な構成ではありません。
8. 以下の値を構成します。

表 *87. syslog* ログ・ソースの追加

パラメーター	説明
ログ・ソース **ID**	CA SiteMinder アプライアンスの IP アドレスまたはホスト名を入力します。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されています。

表 87. *syslog* ログ・ソースの追加 (続き)

パラメーター	説明
信頼性	リストから、ログ・ソースの信頼性値を入力します。範囲は 0 から 10 です。 信頼性は、送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性を示します。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 自動的に検出されたログ・ソースは、「システム設定」ウィンドウの「イベントの統合」リストで構成されたデフォルト値を使用します。このウィンドウには、「管理」タブからアクセスできます。ただし、新規ログ・ソースを作成するか、自動的に検出されたログ・ソースの構成を更新する際に、各ログ・ソースに対してこのチェック・ボックスを構成することで、デフォルト値をオーバーライドできます。詳しくは、「IBM Security QRadar 管理ガイド」を参照してください。
イベント・ペイロードの保管	QRadar によるイベント・ペイロードの保管を有効または無効にするには、このチェック・ボックスを選択します。 自動的に検出されたログ・ソースは、「システム設定」ウィンドウの「イベント・ペイロードの保管」リストのデフォルト値を使用します。このウィンドウには、「管理」タブからアクセスできます。新規ログ・ソースを作成するか、自動的に検出されたログ・ソースの構成を更新する際に、各ログ・ソースに対してこのチェック・ボックスを構成することで、デフォルト値をオーバーライドできます。詳しくは、「IBM Security QRadar 管理ガイド」を参照してください。

9. 「保存」をクリックします。

   「管理」タブのツールバーでは、ログ・ソースの変更が検出され、変更をデプロイする必要があるときにそれを示すメッセージが表示されます。

10. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

これで、イベントを QRadar に転送するように CA SiteMinder アプライアンスで syslog-ng を構成する準備ができました。

CA SiteMinder 用の Syslog-ng の構成

syslog-ng イベントを QRadar コンソールまたはイベント・コレクター (Event Collector)に転送するように CA SiteMinder アプライアンスを構成する必要があります。

このタスクについて

IBM Security QRadar は、ポート 514 で TCP または UDP syslog ソースからの syslog-ng イベントを収集できます。

CA SiteMinder 用に syslog-ng を構成するには、以下のようにします。

手順

1. SSH を使用して、root ユーザーとして CA SiteMinder アプライアンスにログインします。
2. syslog-ng 構成ファイルを編集します。

   ```
   /etc/syslog-ng.conf
   ```
3. 以下の情報を追加して、syslog-ng のイベント・ファイルとしてアクセス・ログを指定します。

   ```
   source s_siteminder_access
   { file("/opt/apps/siteminder/sm66/siteminder/log/smaccess.log"); };
   ```
4. 以下の情報を追加して、宛先およびメッセージ・テンプレートを指定します。

   ```
   destination d_remote_q1_siteminder {
   udp("<QRadar IP>" port(514) template ("$PROGRAM $MSG¥n"));
   };
   ```

   ここで、<*QRadar IP*> は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
5. 以下のログ項目情報を追加します。

   ```
   log {
   source(s_siteminder_access);
   destination(d_remote_q1_siteminder);
   };
   ```
6. syslog-ng.conf ファイルを保存します。
7. 以下のコマンドを入力して syslog-ng を再始動します。

   ```
   service syslog-ng restart
   ```

   syslog-ng サービスが再始動したら、CA SiteMinder の構成は完了です。CA SiteMinder によって QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

CA Top Secret

IBM Security QRadar は、CA Top Secret イベントを統合します。

以下の 2 つのオプションがあります。

- 『IBM Security zSecure を使用した CA Top Secret と IBM Security QRadar の統合』
- 214 ページの『監査スクリプトを使用した CA Top Secret と IBM Security QRadar の統合』

IBM Security zSecure を使用した CA Top Secret と IBM Security QRadar の統合

CA Top Secret DSM は、IBM z/OS メインフレーム上の Top Secret イメージからの LEEF イベントを、IBM Security zSecure を使用して統合します。

zSecure プロセスを使用すると、System Management Facilities (SMF) からのイベントは、ログ・イベント拡張フォーマット (LEEF) のイベント・ファイルに記録されます。IBM Security QRadar は、ログ・ファイル・プロトコルを使用して LEEF イベント・ログ・ファイルを取得し、イベントを処理します。ポーリング間隔に基づいてイベントを取得するように QRadar をスケジュールできます。これにより、QRadar は、定義されたスケジュールに基づいてイベントを取得できます。

CA Top Secret イベントを統合するには、以下のようにします。

1. インストール済み環境が、前提条件となるインストール要件をすべて満たしていることを確認します。
2. イベントを LEEF 形式で書き込むように CA Top Secret z/OS イメージを構成します。詳しくは、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。
3. CA Top Secret が LEEF 形式のイベント・ログを取得するために、QRadar でログ・ソースを作成します。
4. オプション。QRadar で CA Top Secret 用のカスタム・イベント・プロパティーを作成します。詳しくは、テクニカル・ノート「QRadar *Custom Event Properties for IBM z/OS*」を参照してください。

注**:** 正規化イベントの予期されるフィールドが表示されない場合は、IBM z/OS を構成してください。構文解析の動作の整合性が向上する可能性があります。

始める前に

データ収集プロセスを構成する前に、基本の zSecure インストール・プロセスを完了する必要があります。

以下の前提条件は必須です。

- z/OS イメージ上の IBM Security zSecure Audit で parmlib メンバーの IFAPRDxx が有効になっていることを確認する必要があります。
- SCKRLOAD ライブラリーは APF が許可されていなければなりません。
- CKFREEZE と UNLOAD のデータ・セットが定期的に更新されるようにプロセスを構成する必要があります。

- LEEF イベント・ファイルをダウンロードするには、QRadar に対して z/OS イメージ上の SFTP、FTP、または SCP の各サーバーを構成する必要があります。
- QRadar と z/OS イメージの間にあるファイアウォールで SFTP トラフィック、FTP トラフィック、または SCP トラフィックを許可する必要があります。

ソフトウェアをインストールした後に、構成を作成および変更する必要もあります。zSecure のインストールおよび構成の手順については、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。

関連タスク:

582 ページの『IBM z/OS』

ログ・ファイル・プロトコルにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

CA Top Secret ログ・ソースの構成

ログ・ファイル・プロトコルにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

このタスクについて

ログ・ファイルは、一度に 1 つずつ、処理のために QRadar に転送されます。ログ・ファイル・プロトコルは、プレーン・テキストのイベント・ログや圧縮ファイル、アーカイブを管理できます。アーカイブには、一度に 1 行ずつ処理できるプレーン・テキスト・ファイルが含まれている必要があります。複数行イベント・ログは、ログ・ファイル・プロトコルではサポートされていません。 zSecure が含まれた IBM z/OS は、指定されたディレクトリーにログ・ファイルを gzip アーカイブとして書き込みます。QRadar は、アーカイブを取り出し、ファイルに 1 行当たり 1 イベントで書き込まれているイベントを処理します。

これらのイベントを取得するには、ログ・ファイル・プロトコルを使用してログ・ソースを作成する必要があります。QRadar は、LEEF 形式のイベント・ファイルをホストするシステムにログインするための資格情報と、ポーリング間隔を要求します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。

8. 「ログ・ソース・タイプ」リストで「**CA Top Secret**」を選択します。
9. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
10. 以下の値を構成します。

表 *88. CA Top Secret* ログ・ファイル・パラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。IP アドレスまたはホスト名により、QRadar はログ・ファイルを固有のイベント・ソースに識別できるようになります。 **例:** ネットワークに複数のデバイス (例えば、複数の z/OS イメージ)、またはすべてのイベント・ログが入っているファイル・リポジトリーが含まれている場合、ログ・ソースを一意的に識別するデバイスの IP アドレスまたはホスト名を指定します。これにより、ファイル・リポジトリーのイベントを識別する代わりに、ネットワーク内のデバイス・レベルでイベントを識別できるようになります。
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 • SFTP - SSH ファイル転送プロトコル • FTP - ファイル転送プロトコル • SCP - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP** またはホスト名」フィールドに指定されているサーバーに、有効になっている SFTP サブシステムが含まれている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。

表 *88. CA Top Secret* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 • SFTP - SSH ファイル転送プロトコル • FTP - ファイル転送プロトコル • SCP - セキュア・コピー オプションは、以下のとおりです。 • FTP - TCP ポート 21 • SFTP - TCP ポート 22 • SCP - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。
SSH 鍵ファイル	「サービス・タイプ」として SCP または SFTP を選択した場合、このパラメーターにより、SSH 秘密鍵ファイルを定義することを選択できます。 SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。

表 *88. CA Top Secret* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。これにより、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムがサポートされます。
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」オプションは無視されます。

表 *88. CA Top Secret* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
FTP ファイル・パターン	「サービス・タイプ」として SFTP または FTP を選択した場合、このオプションにより、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 IBM Security zSecure Audit を使用している IBM z/OS メインフレームは、`TSS.<timestamp>.gz` というパターンを使用してイベント・ファイルを書き込みます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。 **例:** 先頭が `TSS` で末尾が `.gz` のファイルを収集するには、以下のコマンドを入力します。 `TSS.*¥.gz` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として FTP を選択した場合にのみ表示されます。リストから「バイナリー **(Binary)**」を選択します。 バイナリー転送モードは、`zip`、`gzip`、`tar`、`tar+gzip` アーカイブ・ファイルなど、バイナリー (圧縮) フォーマットで保管されたイベント・ファイルの場合に必要です。
SCP リモート・ファイル	SCP をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。

表 *88. CA Top Secret* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
開始時刻	処理を開始する時刻を入力します。 **例:** 午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、`00:00` と入力します。 このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 **例:** リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、`2H` と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 (Ignore Previously Processed File)」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「**gzip**」を選択します。 プロセッサーにより、イベント・ファイル・アーカイブを解凍でき、内容がイベント用に処理されます。ファイルは、QRadar にダウンロードされた後にのみ処理されます。QRadar は、`zip`、`gzip`、`tar`、または `tar+gzip` の各アーカイブ・フォーマットのファイルを処理できます。

表 88. CA Top Secret ログ・ファイル・パラメーター (続き)

パラメーター	説明
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが処理されたかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。処理されたすべてのファイルがダウンロードされます。 このオプションは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスはクリアのままにしておきます。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。このフィールドでは、ファイルの保管用に使用するローカル・ディレクトリーを構成します。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに追加の処理を適用します。ファイルの各行が、単一イベントです。**例:** ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

CA Top Secret の構成は完了です。構成でカスタム・イベント・プロパティーが必要な場合は、テクニカル・ノート「QRadar *Custom Event Properties for IBM z/OS*」を参照してください。

監査スクリプトを使用した CA Top Secret と IBM Security QRadar の統合

CA Top Secret DSM は、IBM zOS メインフレームと統合して、イベントおよび監査トランザクションを収集します。

IBM Security QRadar は、イベントからの入手可能な関連情報をすべて記録します。

CA Top Secret イベントを QRadar と統合するためのステップは、以下のとおりです。

1. IBM メインフレームが、すべてのセキュリティー・イベントをサービス・マネジメント・フレームワーク (SMF) レコードとしてライブ・リポジトリーに記録します。
2. 午前 0 時に、CA Top Secret データが、SMF ダンプ・ユーティリティーを使用してライブ・リポジトリーから抽出されます。SMF ファイルには、前日のすべてのイベントおよびフィールドが未加工の SMF 形式で格納されています。
3. qextopsloadlib プログラムが、SMF 形式ファイルからデータをプルします。qextopsloadlib プログラムが、QRadar の関連イベントおよび関連フィールドのみをプルし、互換性を考慮して、その情報を圧縮形式で書き込みます。この情報は、QRadar がアクセスできる場所に保存されます。
4. QRadar は、ログ・ファイル・プロトコル・ソースを使用して、スケジュールに基づいて出力ファイル情報を取得します。次に、QRadar はこのファイルをインポートして、処理します。

IBM Security QRadar と統合するための CA Top Secret の構成

CA Top Secret を IBM Security QRadar と統合できます。

手順

1. IBM サポート Web サイト (http://www.ibm.com/support) から、以下の圧縮ファイルをダウンロードします。

   qextops_bundled.tar.gz
2. Linux のオペレーティング・システム上で、以下のファイルを解凍します。

   tar -zxvf qextops_bundled.tar.gz

   アーカイブには、以下のファイルが含まれています。

   - qextops_jcl.txt
   - qextopsloadlib.trs
   - qextops_trsmain_JCL.txt
3. 任意の端末エミュレーター・ファイル転送方式を使用して、ファイルを IBM メインフレームにロードします。

   TEXT プロトコルを使用して、サンプルの qextops_trsmain_JCL.txt ファイルと qextops_jcl.txt ファイルをアップロードします。

4. BINARY モード転送を使用して、qextopsloadlib.trs ファイルをアップロードします。qextopsloadlib.trs ファイルは、実行可能ファイル (メインフレーム・プログラム qextops) が含まれている簡潔なファイルです。.trs ファイルをワークステーションからアップロードするときに、DCB 属性 DSORG=PS、RECFM=FB、LRECL=1024、BLKSIZE=6144 を使用して、メインフレーム上でファイルを事前割り振りします。ファイル転送タイプは、テキストではなくバイナリー・モードでなければなりません。

   注: Qextops は、TSSUTIL の出力 (EARLOUT データ) を 1 行ずつ読み取る小さな C メインフレーム・プログラムです。Qextops は、イベント情報 (例えば、レコード記述子、日付、時刻) が含まれているヘッダーを各レコードに追加します。このプログラムは各フィールドを出力レコードに書き込み、末尾ブランク文字を抑止し、各フィールドをパイプ文字で区切ります。この出力ファイルは QRadar 用にフォーマット設定されており、ブランクの抑止により、QRadar へのネットワーク・トラフィックが削減されます。このプログラムは、CPU や I/O ディスクのリソースを消費しません。
5. インストール済み環境固有の要件に応じて、qextops_trsmain_JCL.txt ファイルをカスタマイズします。

   qextops_trsmain_JCL.txt ファイルは IBM ユーティリティー TRSMAIN を使用して、qextopsloadlib.trs ファイルに保管されているプログラムを抽出します。

   qextops_trsmain_JCL.txt ファイルの例を以下に示します。

```
//TRSMAIN JOB (yourvalidjobcard),Q1labs,
// MSGCLASS=V
//DEL EXEC PGM=IEFBR14
//D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXTOPS.TRS
// UNIT=SYSDA,
// SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE DD DISP=SHR,DSN=<yourhlq>.QEXTOPS.TRS
//OUTFILE DD DISP=(NEW,CATLG,DELETE),
// DSN=<yourhlq>.LOAD,
// SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA
//
```

   このファイルは、インストール済み環境固有のパラメーター向け情報 (ジョブカード、データ・セット命名規則、出力宛先、保存期間、スペース所要量など) で更新する必要があります。

   .trs 入力ファイルは、IBM TERSE フォーマットのライブラリーであり、TRSMAIN を呼び出す JCL の実行によって取り出されます。この簡潔なファイルは抽出時に、qextops プログラムをメンバーとして持つ PDS LINKLIB を作成します。
6. STEPLIB をこのライブラリーに対して実行するか、または LINKLST 内にある LINKLIB の 1 つにこのプログラムを移動することを選択できます。このプログラムには許可は必要ありません。
7. アップロード後に、プログラムを既存のリンク・リスト・ライブラリーにコピーするか、またはプログラムが含まれるライブラリーの、正しいデータ・セット名を持つ STEPLIB DD ステートメントを追加します。

8. qextops_jcl.txt ファイルは、サンプル JCL が含まれているテキスト・ファイルです。構成を満たすようにジョブ・カードを構成する必要があります。

   qextops_jcl.txt サンプル・ファイルには、以下が含まれています。

```
//QEXTOPS JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXTOPS JCL version 1.0 September, 2010
//*
//*************************************************************
//* Change below dataset names to sites specific datasets names*
//*************************************************************
//SET1 SET TSSOUT='Q1JACK.EARLOUT.ALL',
// EARLOUT='Q1JACK.QEXTOPS.PROGRAM.OUTPUT'
//*************************************************************
//* Delete old datasets *
//*************************************************************//

DEL EXEC PGM=IEFBR14
//DD1 DD DISP=(MOD,DELETE),DSN=&TSSOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//DD2 DD DISP=(MOD,DELETE),DSN=&EARLOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//* Allocate new dataset *
//*************************************************************
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DISP=(NEW,CATLG),DSN=&EARLOUT,
// SPACE=(CYL,(100,100)),
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*************************************************************
//* Execute Top Secret TSSUTIL utility to extract smf records*
//*************************************************************
//REPORT EXEC PGM=TSSUTIL
//SMFIN DD DISP=SHR,DSN=&SMFIN1
//SMFIN1 DD DISP=SHR,DSN=&SMFIN2
//UTILOUT DD DSN=&UTILOUT,
// DISP=(,CATLG),UNIT=SYSDA,SPACE=(CYL,(50,10),RLSE),
// DCB=(RECFM=FB,LRECL=133,BLKSIZE=0)
//EARLOUT DD DSN=&TSSOUT,
// DISP=(NEW,CATLG),UNIT=SYSDA,
// SPACE=(CYL,(200,100),RLSE),
// DCB=(RECFM=VB,LRECL=456,BLKSIZE=27816)
//UTILIN DD *
NOLEGEND
REPORT EVENT(ALL) END
/*
//*************************************************************
//EXTRACT EXEC PGM=QEXTOPS,DYNAMNBR=10,
// TIME=1440
//STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN DD DUMMY
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//CFG DD DUMMY
//EARLIN DD DISP=SHR,DSN=&TSSOUT
//EARLOUT DD DISP=SHR,DSN=&EARLOUT
//*************************************************************
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
```

```
<USER>
<PASSWORD>
PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

9. 出力ファイルの作成後に、以下のいずれかのオプションを選択する必要があります。

   出力ファイルを一時 FTP サーバーに転送するジョブをスケジュールします。ジョブが完了するたびに、出力ファイルが一時 FTP サーバーに転送されます。出力を一時 FTP サーバーに正常に転送するために、サンプル JCL で以下のパラメーターを構成する必要があります。

   例:

   ```
   //FTP EXEC PGM=FTP,REGION=3800K
   //INPUT DD *
   <IPADDR>
   <USER>
   <PASSWORD>
   PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<EARLOUT>
   QUIT
   //OUTPUT DD SYSOUT=*
   //SYSPRINT DD SYSOUT=*
   ```

   各部分について以下で説明します。

   <*IPADDR*> は、出力ファイルを受信するための一時 FTP サーバーの IP アドレスまたはホスト名です。

   <*USER*> は、一時 FTP サーバーへのアクセスに必要なユーザー名です。

   <*PASSWORD*> は、一時 FTP サーバーへのアクセスに必要なパスワードです。

   <*THEIPOFTHEMAINFRAMEDEVICE*> は、出力を受信するメインフレームまたは一時 FTP サーバーの宛先です。

   例:

   ```
   PUT 'Q1JACK.QEXTOPS.OUTPUT.C320' /192.168.1.101/CA/QEXTOPS.OU
   TPUT.C320
   ```

   <QEXOUTDSN> は、一時 FTP サーバーに保存される出力ファイルの名前です。

   これで、ログ・ファイル・プロトコルを構成する準備ができました。 218 ページの『ログ・ソースの作成』を参照してください。

10. CA Top Secret から出力ファイルを取得するように QRadar をスケジュールします。

    zOS プラットフォームが FTP または SFTP 経由でファイルを提供するように構成されているか、または SCP を許可するように構成されている場合、一時 FTP サーバーは不要であり、QRadar は出力ファイルをメインフレームから直接プルすることができます。`qextops_jcl.txt` ファイルで、以下のテキストは、`//*` を使用してコメント化するか削除する必要があります。

```
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<EARLOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

次のタスク

これで、ログ・ファイル・プロトコルを構成する準備ができました。『ログ・ソースの作成』を参照してください。

ログ・ソースの作成

ログ・ファイル・プロトコル・ソースにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。CA Top Secret DSM は、ログ・ファイル・プロトコル・ソースを使用して、ログ・ファイルの一括ロードをサポートします。

このタスクについて

ログ・ファイル・プロトコルを使用するように CA Top Secret DSM を構成する際には、CA Top Secret で構成されているホスト名または IP アドレスが、ログ・ファイル・プロトコル構成の**「リモート・ホスト」**パラメーターに構成されているものと同じになっているようにしてください。

CA Top Secret 用に QRadar でログ・ソースを構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**CA Top Secret**」を選択します。
9. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
10. 以下の値を構成します。

表 89. *CA Top Secret* ログ・ファイル・パラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。IP アドレスまたはホスト名により、QRadar はログ・ファイルを固有のイベント・ソースに識別できるようになります。 **例:** ネットワークに複数のデバイス (例えば、複数の z/OS イメージ)、またはすべてのイベント・ログが入っているファイル・リポジトリーが含まれている場合、ログ・ソースを一意的に識別するデバイスの IP アドレスまたはホスト名を指定します。この処理により、ファイル・リポジトリーのイベントを識別する代わりに、ネットワーク内のデバイス・レベルでイベントを識別できるようになります。
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 • SFTP - SSH ファイル転送プロトコル • FTP - ファイル転送プロトコル • SCP - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得する基礎のプロトコルでは、「リモート **IP** またはホスト名」フィールドに指定されているサーバーに、有効になっている SFTP サブシステムが含まれている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 オプションは、以下のとおりです。 • FTP - TCP ポート 21 • SFTP - TCP ポート 22 • SCP - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。

表 *89. CA Top Secret* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。
SSH 鍵ファイル	「サービス・タイプ」として SCP または SFTP を選択した場合、このパラメーターで SSH 秘密鍵ファイルを定義します。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートするために、リモート・ディレクトリーをブランクのままにすることができます。
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」オプションは無視されます。

表 89. *CA Top Secret* ログ・ファイル・パラメーター (続き)

パラメーター	説明
FTP ファイル・パターン	「サービス・タイプ」として SFTP または FTP を選択した場合、これにより、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成します。一致するすべてのファイルは処理に組み込まれます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。 このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として FTP を選択した場合にのみ表示されます。リストから「バイナリー **(Binary)**」を選択します。 バイナリー転送モードは、`zip`、`gzip`、`tar`、`tar+gzip` アーカイブ・ファイルなど、バイナリー (圧縮) フォーマットで保管されたイベント・ファイルの場合に必要です。
SCP リモート・ファイル	「サービス・タイプ」として SCP を選択した場合は、リモート・ファイルのファイル名を入力する必要があります。
開始時刻	処理を開始する時刻を入力します。 **例:** 午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、`00:00` と入力します。 このパラメーターと「繰り返し **(Recurrence)**」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。

表 *89. CA Top Secret* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 **例:** リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 (Ignore Previously Processed File)」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「**gzip**」を選択します。 プロセッサーにより、イベント・ファイル・アーカイブを解凍し、内容をイベント用に処理できます。ファイルは、QRadar にダウンロードされた後にのみ処理されます。 QRadar は、zip、gzip、tar、または tar+gzip の各アーカイブ・フォーマットのファイルを処理できます。

表 89. CA Top Secret ログ・ファイル・パラメーター (続き)

パラメーター	説明
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって既に処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが以前に処理されたかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。以前に処理されていないすべてのファイルがダウンロードされます。 このオプションは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスはクリアのままにしておきます。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これにより、ファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに複数の処理を実行します。ファイルの各行が、単一イベントです。**例:** ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

CA Top Secret の構成は完了です。構成でカスタム・イベント・プロパティーが必要な場合は、テクニカル・ノート「QRadar *Custom Event Properties for IBM z/OS*」を参照してください。

第 29 章 Check Point

いくつかの Check Point 製品を IBM Security QRadar と統合できます。

以下の製品がサポートされます。

- ファイアウォール
- SmartDefense
- IPS
- Anti Malware
- Anti-Bot
- アンチウィルス
- Mobile Access
- DDoS Protector
- Security Gateway/Management
- Threat Emulation
- URL Filtering
- DLP
- Application Control
- Identity Logging
- VPN
- Endpoint Security

Check Point

いくつかのメソッドのうちの 1 つを採用して、Check Point デバイスと統合するように IBM Security QRadar を構成できます。

以下のいずれかのメソッドを使用します。

- 『OPSEC を使用した Check Point の統合』
- 235 ページの『syslog を使用した Check Point の統合』
- 237 ページの『外部 syslog フォワーダーからの Check Point Firewall イベントの統合』

注: ご使用のオペレーティング・システムに応じて、Check Point デバイス用の手順は異なります。以下は、Check Point SecurePlatform オペレーティング・システムに基づく手順です。

OPSEC を使用した Check Point の統合

このセクションでは、IBM Security QRadar が Open Platform for Security (OPSEC/LEA) を使用して Check Point イベントを受け入れるようにするための方法について説明します。

Check Point OPSEC/LEA を QRadar と統合するには、2 つの Secure Internal Communication (SIC) ファイルを作成し、その情報を Check Point のログ・ソースとして QRadar に入力する必要があります。

Check Point の構成の概要

Check Point を QRadar と統合するには、以下の手順を順序どおりに実行する必要があります。

1. QRadar を Check Point のホストとして追加します。
2. OPSEC アプリケーションを Check Point に追加します。
3. ログ・ソース Secure Internal Communication の DN を特定します。
4. QRadar で、OPSEC LEA プロトコルを構成します。
5. OPSEC/LEA の通信構成を検証します。

Check Point ホストの追加

以下のように、Check Point SmartCenter でホストとして IBM Security QRadar を追加できます。

手順

1. Check Point SmartCenter ユーザー・インターフェースにログインします。
2. 「オブジェクト **(Objects)**」 > 「新規ホスト **(New Host)**」を選択します。
3. Check Point ホストの情報を入力します。
   - オブジェクト名 **(Object Name)**: QRadar
   - **IP** アドレス **(IP address)**: QRadar の IP アドレス
4. 「**OK**」をクリックします。

次のタスク

これで、Check Point 用に OPSEC アプリケーション・オブジェクトを作成する準備ができました。

OPSEC アプリケーション・オブジェクトの作成

Check Point SmartCenter で IBM Security QRadar をホストとして追加した後に、OPSEC アプリケーション・オブジェクトを作成できます。

手順

1. Check Point SmartConsole ユーザー・インターフェースを開きます。
2. 「オブジェクト **(Objects)**」 > 「追加のオブジェクト・タイプ **(More Object Types)**」 > 「サーバー **(Server)**」 > 「**OPSEC** アプリケーション **(OPSEC Application)**」 > 「新規アプリケーション **(New Application)**」を選択します。
3. OPSEC アプリケーションを構成します。
   a. 以下の「**OPSEC** アプリケーション・プロパティー **(OPSEC Application Properties)**」パラメーターを構成します。

表 90. OPSEC アプリケーション・プロパティー (OPSEC Application Properties)

パラメーター	値
名前	QRadar-OPSEC
ホスト	QRadar
クライアント・エンティティー (Client Entities)	LEA

b. 「通信 **(Communication)**」をクリックします。

c. 「ワンタイム・パスワード **(One-time password)**」フィールドに、使用するパスワードを入力します。

d. 「ワンタイム・パスワードの確認 **(Confirm one-time password)**」フィールドに、「ワンタイム・パスワード **(One-time password)**」で使用したパスワードを入力します。

e. 「初期化 **(Initialize)**」をクリックします。

f. 「閉じる **(Close)**」をクリックします。

4. 「メニュー **(Menu)**」 > 「ポリシーのインストール **(Install Policy)**」を選択します。
5. 「公開してインストール **(Publish & Install)**」をクリックします。
6. 「インストール **(Install)**」をクリックします。
7. 「メニュー **(Menu)**」 > 「データベースのインストール **(Install Database)**」を選択します。
8. 「インストール **(Install)**」をクリックします。

注**:** SIC の値は、QRadar での Check Point ログ・ソースの構成時に OPSEC アプリケーション・オブジェクト SIC 属性パラメーターで必要になります。OPSEC アプリケーション・オブジェクトが作成された後で、オブジェクトを表示して、値を確認できます。

OPSEC アプリケーション・オブジェクトは、以下の例のようなものです。

```
CN=QRadar=OPSEC,0=cpmodule..tdfaaz
```

ログ・ソース SIC の検索

OPSEC アプリケーション・オブジェクトを作成した後に、Check Point SmartConsole からログ・ソース SIC を検索できます。

手順

1. 「オブジェクト」 > 「オブジェクト・エクスプローラー」を選択します。
2. 「カテゴリー」ツリーで、「ネットワーク・オブジェクト **(Networks Objects)**」の下の「ゲートウェイとサーバー **(Gateways and Servers)**」を選択します。
3. Check Point ログ・ホスト・オブジェクトを選択します。
4. Secure Internal Communication (SIC) をコピーします。

重要**:** ご使用の Check Point バージョンによっては、「通信 **(Communication)**」ボタンにより、SIC 属性が表示されます。Check Point

Management Server コマンド・ライン・インターフェースから SIC 属性を検索できます。Management Server のコマンド・ライン・インターフェースから **cpca_client lscert** コマンドを使用して、すべての証明書を表示する必要があります。

重要: ログ・ソース SIC 属性は、以下の例のようなものです。
`cn=cp_mgmt,o=cpmodule...tdfaaz`。詳しくは、「*Check Point Command Line Interface Guide*」を参照してください。
ここで、Check Point SmartConsole ユーザー・インターフェースからセキュリティー・ポリシーをインストールする必要があります。

次のタスク

これで、OPSEC LEA プロトコルを構成する準備ができました。

IBM Security QRadar での OPSEC/LEA ログ・ソースの構成

ログ・ソース SIC を検索した後に、以下のように、OPSEC LEA プロトコルを構成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで、「**Check Point**」を選択します。
8. 「プロトコル構成」リストで「**OPSEC/LEA**」を選択します。
9. 以下の値を構成します。

表 *91. OPSEC/LEA* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスを入力します。この値は、「サーバー IP」パラメーターで構成されている値に一致する必要があります。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
サーバー **IP**	Check Point ホストまたは Check Point Management Server IP の IP アドレスを入力します。
サーバー・ポート	OPSEC 通信に使用するポート番号を入力します。 管理者は、既存のファイアウォール・ポリシーで QRadar からの LEA/OPSEC 接続が許可されるようにする必要があります。

表 91. OPSEC/LEA プロトコルのパラメーター (続き)

パラメーター	説明
ログ・ソースにサーバー **IP** を使用	ログ・ソースに管理対象デバイスの IP アドレスではなく LEA サーバーの IP アドレスを使用する場合は、このチェック・ボックスを選択します。QRadar で受信されるすべてのイベントが 1 つのログ・ソースに集められます。Check Point Management Server によって転送されるすべてのイベントを個々のログ・ソースに分散させる場合は、このチェック・ボックスをクリアします。デフォルトでは、このパラメーターは有効になっています。
統計レポートの間隔	syslog イベントの数が QRadar.log ファイルに記録される間隔を秒数で入力します。有効な範囲は 4 から 2,147,483,648、デフォルトは 600 です。
認証タイプ	リストから、当該 LEA 構成で必要な「認証タイプ」を選択します。 オプションは、以下のとおりです。 • sslca (デフォルト) • sslca_clear • clear この値は、Check Point Firewall または Check Point カスタム・ログ管理サーバーで構成されている認証方式に一致する必要があります。
OPSEC アプリケーション・オブジェクトの **SIC** 属性 **(SIC** 名**)**	OPSEC アプリケーション・オブジェクトの Secure Internal Communications (SIC) 名を入力します。 SIC 名は、アプリケーションの識別名 (DN) です (例えば、CN=LEA,o=fwconsole..7psasx)。
ログ・ソースの **SIC** 属性 **(SIC** エンティティー名**)**	ログ・ソースを生成するサーバーの SIC 名を入力します。 例: cn=cp_mgmt,o=fwconsole..7psasx
証明書の指定	当該 LEA 構成の証明書を定義するには、「証明書の指定」チェック・ボックスを選択します。
証明書のファイル名	当該構成で使用する証明書のファイル名を入力します。構成ファイルは、/opt/qradar/conf/trusted_certificates/lea ディレクトリーに配置されている必要があります。
認証局の **IP**	証明書をプルする元の SmartCenter サーバーの IP アドレスを入力します。

表 91. OPSEC/LEA プロトコルのパラメーター (続き)

パラメーター	説明
証明書パスワードのプル	証明書の要求時に使用するパスワードを入力します。
OPSEC アプリケーション	証明書の要求時に使用するアプリケーションの名前を入力します。この値の長さは 255 文字まで可能です。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

これで、Check Point の OPSEC/LEA 通信を確認する準備ができました。

OPSEC 通信構成の編集

このセクションでは、Check Point の構成を変更して、標準以外のポートでの OPSEC 通信を可能にする方法について説明します。

他に、平文の通信を構成する方法、非認証ストリームを構成する方法、および IBM Security QRadar の構成を検証する方法も説明します。

Check Point Custom Log Manager (CLM) の IP アドレスの変更

Check Point の構成に Check Point Custom Log Manager (CLM) が含まれる場合、最終的に CLM の IP アドレスの変更が必要になることがあります。これは、QRadar で自動的に検出される、CLM からのすべての Check Point ログ・ソースに影響を与えます。OPSEC/LEA プロトコルを使用して CLM のログ・ソースを手動で追加すると、CLM にログを転送するすべての Check Point Firewall が QRadar で自動的に検出されます。これらの自動検出されたログ・ソースは編集できません。CLM IP アドレスを変更する場合、OPSEC/LEA プロトコル構成が含まれる元の Check Point CLM ログ・ソースを編集して、サーバー IP アドレスとログ・ソース ID を更新する必要があります。

新しい Check Point CLM IP アドレスでログ・ソースを更新すると、自動検出された Check Point ログ・ソースから報告される新規イベントがすべて更新されます。

重要**:** Check Point CLM、および QRadar で自動検出されたログ・ソースを削除したり、再作成したりしないでください。ログ・ソースを削除してもイベント・データは削除されませんが、以前に記録されたイベントを検索することがより困難になります。

Check Point OPSEC ログ・ソースの更新

Check Point OPSEC ログ・ソースを更新できます。

手順

1. IBM Security QRadar にログインします。
2. 「管理」タブをクリックします。

3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. OPSEC/LEA プロトコル構成が含まれているオリジナルの Check Point CLM ログ・ソースを選択し、「編集」をクリックします。
6. 「ログ・ソース **ID**」フィールドに、Check Point CLM の新規識別名を入力します。
7. 「サーバー **IP**」フィールドに、Check Point CLM の新規 IP アドレスを入力します。
8. 「保存」をクリックします。

IBM Security QRadar での Check Point CLM の IP アドレスの更新は完了です。

OPSEC LEA 通信のデフォルト・ポートの変更

OPSEC LEA が通信するデフォルト・ポート (18184) を変更します。

手順

1. Check Point SmartCenter Server のコマンド・ライン・プロンプトで、以下のコマンドを入力してファイアウォール・サービスを停止します。

```
cpstop
```

2. ご使用の Check Point SmartCenter Server オペレーティング・システムに応じて、以下のファイルを開きます。
   - Linux の場合 - `$FWDIR¥conf¥fwopsec.conf`
   - Windows の場合 - `%FWDIR%¥conf¥fwopsec.conf`

   このファイルのデフォルトのコンテンツは以下のとおりです。

```
# The VPN-1 default settings are:
# # sam_server auth_port 0 # sam_server port 18183
# # lea_server auth_port 18184 # lea_server port 0
# # ela_server auth_port 18187 # ela_server port 0
# # cpmi_server auth_port 18190
# # uaa_server auth_port 19191 # uaa_server port 0 #
```

3. デフォルトの **lea_server auth_port** を 18184 から別のポート番号に変更します。
4. 以下の行からハッシュ・マーク (#) を削除します。

   例:

```
lea_server auth_port 18888 # lea_server port 0
```

5. ファイルを保存して閉じます。
6. 以下のコマンドを入力して、ファイアウォール・サービスを開始します。

```
cpstart
```

非暗号化通信用の OPSEC LEA の構成

以下のように、非暗号化通信用に OPSEC LEA プロトコルを構成できます。

手順

1. Check Point SmartCenter Server のコマンド・ライン・プロンプトで、以下のコマンドを入力してファイアウォール・サービスを停止します。

   ```
   cpstop
   ```

2. ご使用の Check Point SmartCenter Server オペレーティング・システムに応じて、以下のファイルを開きます。
   - Linux の場合 - `$FWDIR¥conf¥fwopsec.conf`
   - Windows の場合 - `%FWDIR%¥conf¥fwopsec.conf`
3. デフォルトの **lea_server auth_port** を 18184 から 0 に変更します。
4. デフォルトの **lea_server port** を 0 から 18184 に変更します。
5. 両方の行からハッシュ・マーク (#) を削除します。

   例:

   ```
   lea_server auth_port 0 lea_server port 18184
   ```

6. ファイルを保存して閉じます。
7. 以下のコマンドを入力して、ファイアウォール・サービスを開始します。

   ```
   cpstart
   ```

Check Point デバイスからイベントを受信するための IBM Security QRadar の構成

Check Point デバイスからイベントを受信するように IBM Security QRadar を構成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで、「**Check Point**」を選択します。
7. 「プロトコル構成」リストで「**OPSEC/LEA**」を選択します。
8. 以下のパラメーターを構成します。

表 92. OPSEC/LEA プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスを入力します。この値は、「サーバー **IP**」パラメーターで構成されている値に一致する必要があります。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
サーバー **IP**	サーバーの IP アドレスを入力します。

表 92. *OPSEC/LEA* プロトコルのパラメーター (続き)

パラメーター	説明
サーバー・ポート	OPSEC 通信に使用するポート番号を入力します。有効な範囲は 0 から 65,536 で、QRadar が使用するデフォルト・ポートは 18184 です。
ログ・ソースにサーバー **IP** を使用	ログ・ソースに管理対象デバイスの IP アドレスではなく、LEA サーバーの IP アドレスを使用する場合は、「ログ・ソースにサーバー **IP** を使用」チェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
統計レポートの間隔	syslog イベントの数が QRadar.log ファイルに記録される間隔を秒数で入力します。有効な範囲は 4 から 2,147,483,648、デフォルトは 600 です。

表 92. *OPSEC/LEA* プロトコルのパラメーター *(*続き*)*

パラメーター	説明
認証タイプ	リストから、当該 LEA 構成で使用する「認証タイプ」を選択します。オプションは、sslca (デフォルト)、sslca_clear、または clear です。この値は、サーバーが使用する認証方式と一致している必要があります。認証タイプとして sslca または sslca_clear を選択する場合は、以下のパラメーターが表示されます。 • **OPSEC** アプリケーション・オブジェクトの **SIC** 属性 **(SIC** 名**) (OPSEC Application Object SIC Attribute (SIC Name))** - OPSEC アプリケーション・オブジェクトの Secure Internal Communications (SIC) 名を入力します。SIC 名は、アプリケーションの識別名 (DN) です (例えば、CN=LEA,o=fwconsole..7psasx)。名前は 255 文字まで可能であり、大/小文字が区別されます。 • ログ・ソースの **SIC** 属性 **(SIC** エンティティー名**)** - サーバーの SIC 名を入力します (例えば、cn=cp_mgmt,o=fwconsole..7psasx)。名前は 255 文字まで可能であり、大/小文字が区別されます。 • 証明書の指定 **(Specify Certificate)** - この LEA 構成の証明書を定義する場合は、このチェック・ボックスを選択します。QRadar は、証明書が必要な場合にこれらのパラメーターを使用して証明書を取得しようとします。 「証明書の指定**(Specify Certificate)**」チェック・ボックスを選択すると、「証明書のファイル名 (Certificate Filename)」パラメーターが表示されます。 • 証明書のファイル名 **(Certificate Filename)** -このオプションは、「証明書の指定 **(Specify Certificate)**」が選択されている場合にのみ表示されます。当該構成で使用する証明書のファイル名を入力します。構成ファイルは、/opt/qradar/conf/trusted_certificates/lea ディレクトリーに配置されている必要があります。 「証明書の指定 **(Specify Certificate)**」チェック・ボックスをクリアすると、以下のパラメーターが表示されます。 • 認証局の **IP (Certificate Authority IP)** - 証明書の取得元 SmartCenter サーバーの IP アドレスを入力します。 • 証明書パスワードのプル - 証明書の要求時に使用するパスワードを入力します。パスワードの最大長は 255 文字です。 • **OPSEC** アプリケーション - 証明書の要求時に使用するアプリケーションの名前を入力します。この値の長さは 255 文字まで可能です。 **重要:** 証明書のプルには、ポート 18210 へのアクセスが必要です。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

syslog を使用した Check Point の統合

このセクションでは、IBM Security QRadar Check Point DSM が syslog を使用して Check Point イベントを受け入れるようにする方法について説明します。

Check Point デバイスと統合するように IBM Security QRadar を構成するには、以下のステップを実行する必要があります。

重要: Check Point SmartCenter が Microsoft Windows にインストールされている場合は、OPSEC を使用して Check Point と QRadar を統合する必要があります。

1. 以下のコマンドを入力し、expert ユーザーとして Check Point コンソールにアクセスします。

   ```
   expert
   ```

   パスワード・プロンプトが表示されます。
2. expert コンソールのパスワードを入力します。Enter キーを押します。
3. 以下のファイルを開きます。

   ```
   /etc/rc.d/rc3.d/S99local
   ```
4. 以下の行を追加します。

   ```
   $FWDIR/bin/fw log -ftn | /usr/bin/logger -p <facility>.<priority>
   /dev/null 2>&1 &
   ```

   各部分について以下で説明します。
   - <*facility*> は、syslog のファシリティーです (例: local3)。
   - <*priority*> は、syslog の優先順位です (例: info)。

   例:

   ```
   $FWDIR/bin/fw log -ftn | /usr/bin/logger -p local3.info > /dev/null
   2>&1 &
   ```
5. ファイルを保存して閉じます。
6. syslog.conf ファイルを開きます。
7. 以下の行を追加します。

   ```
   <facility>.<priority> <TAB><TAB>@<host>
   ```

   各部分について以下で説明します。
   - <*facility*> は、syslog のファシリティーです (例: local3)。この値は、ステップ 4 で入力した値と同じでなければなりません。
   - <*priority*> は、syslog の優先順位です (例: info または notice)。この値は、ステップ 4 で入力した値と同じでなければなりません。

   <TAB> は、Tab キーを押す必要があることを示します。

   <*host*> は、QRadar コンソールまたは管理対象ホストを示します。
8. ファイルを保存して閉じます。

9. 以下のコマンドを入力して syslog を再開します。
   - Linux の場合: `service syslog restart`
   - Solaris の場合: `/etc/init.d/syslog start`
10. 以下のコマンドを入力します。

    ```
    nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p <facility>.<priority>
    > /dev/null 2>&1 &
    ```

    各部分について以下で説明します。
    - *<facility>* は、syslog のファシリティーです (例: local3)。この値は、ステップ 4 で入力した値と同じでなければなりません。
    - *<priority>* は、syslog の優先順位です (例: info)。この値は、ステップ 4 で入力した値と同じでなければなりません。

構成は完了です。Check Point の syslog イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Check Point からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Check Point**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *93. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Check Point アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

外部 syslog フォワーダーからの Check Point Firewall イベントの統合

Check Point Firewall イベントは、IBM Security QRadar にイベントを送信する外部ソース (Splunk Forwarder やその他のサード・パーティー製 syslog 転送機能など) から転送できます。

Check Point Firewall イベントが外部ソースから syslog 形式で提供されると、このイベントを syslog ヘッダー内の IP アドレスで識別します。イベントが標準 syslog プロトコルを使用して処理されると、この識別方法ではイベントが正しく識別されません。syslog リダイレクト・プロトコルは、イベント・ソースを正しく識別するために、イベント・ペイロードからの IP アドレスを syslog ヘッダーに代入する方式を管理者に提供します。

IP アドレスを代入するには、管理者は、適切な IP アドレスを含む、Check Point Firewall イベント・ペイロードの共通フィールドを識別する必要があります。例えば、Splunk Forwarder からのイベントでは、イベント・ペイロードの `orig=` を使用して、Check Point Firewall の元の IP アドレスを識別します。このプロトコルによって適切な IP アドレスが代入され、デバイスがログ・ソースで適切に識別されるようになります。Check Point Firewall イベントが転送されると、QRadar が、固有 IP アドレスごとに新規ログ・ソースを自動的に検出および作成します。

代入は正規表現を使用して実行され、TCP syslog イベントも UDP syslog イベントもサポートできます。プロトコルは、ログ・ソースとポートの初期構成として iptables を自動的に構成します。管理者はポート割り当てを変更することにした場合、「すべての構成のデプロイ」で iptables 構成を更新し、新規ポート割り当てを使用する必要があります。

Check Point 転送イベントのログ・ソースの構成

外部ソースから転送されたロー・イベントを収集するには、イベントが IBM Security QRadar に転送される前にログ・ソースを構成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Check Point**」を選択します。
9. 「プロトコル構成」リストで「**syslog** リダイレクト **(Syslog Redirect)**」を選択します。
10. 以下の値を構成します。

表 *94. syslog* リダイレクト・プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Check Point Firewall イベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。 「ログ・ソース ID」は、固有値でなければなりません。
ログ・ソース **ID** 正規表現 **(Log Source Identifier Regex)**	イベント・ペイロードからの Check Point Firewall IP アドレスを識別するために必要な正規表現 (regex) を入力します。 **例:** 管理者は以下の正規表現を使用して、Splunk Forwarder から提供された Check Point Firewall イベントを構文解析できます。 `orig=(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})`
Listen ポート	QRadar が受信 syslog リダイレクト・イベントを受け入れるために使用するポート番号を入力します。 デフォルトの listen ポートは 517 です。 構成するポート番号は、syslog イベントを転送するアプライアンスで構成されているポートに一致する必要があります。管理者は、このフィールドにポート 514 を指定できません。
プロトコル	リストから、「**UDP**」または「**TCP**」のいずれかを選択します。 syslog リダイレクト・プロトコルでは、任意の数の UDP syslog 接続がサポートされますが、TCP 接続は 2500 に制限されます。syslog ストリームに含まれているログ・ソースが 2500 を超えている場合は、2 つ目の Check Point ログ・ソースと listen ポート番号を入力する必要があります。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
信頼性	リストから、ログ・ソースの「信頼性」を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。

表 94. *syslog* リダイレクト・プロトコルのパラメーター (続き)

パラメーター	説明
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、「イベントの統合」チェック・ボックスを選択します。 デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」による「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	「受信イベント・ペイロード **(Incoming Event Payload)**」リストで、ログの構文解析と保管を行うための受信ペイロード・エンコーダーを選択します。
イベント・ペイロードの保管	ログ・ソースによるイベント・ペイロード情報の保管を有効にするには、「イベント・ペイロードの保管」チェック・ボックスを選択します。 デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」による「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

Check Point Multi-Domain Management (Provider-1)

Check Point Multi-Domain Management (Provider-1) デバイスと統合するように IBM Security QRadar を構成できます。

Check Point Multi-Domain Management (Provider-1) からのすべてのイベントは、Check Point Multi-Domain Management (Provider-1) DSM を使用して解析されます。以下のいずれかの方法で、Check Point Multi-Domain Management (Provider-1) を統合できます。

- 240 ページの『Check Point Multi-Domain Management (Provider-1) のための syslog の統合』

- 241 ページの『Check Point Multi-Domain Management (Provider-1) のための OPSEC の構成』

注: ご使用のオペレーティング・システムに応じて、Check Point Multi-Domain Management (Provider-1) デバイスを使用するための手順が異なります。以下は、Check Point SecurePlatform オペレーティング・システムに基づく手順です。

Check Point Multi-Domain Management (Provider-1) のための syslog の統合

この手順では、IBM Security QRadar 用の Check Point Multi-Domain Management (Provider-1) DSM が syslog を使用して Check Point Multi-Domain Management (Provider-1) イベントを確実に受け入れるようにします。

このタスクについて

QRadar は、すべての関連する Check Point Multi-Domain Management (Provider-1) イベントを記録します。

以下のように、Check Point Multi-Domain Management (Provider-1) デバイスで syslog を構成します。

手順

1. 以下のコマンドを入力して、コンソールに expert ユーザーとしてアクセスします。

   ```
   expert
   ```

   パスワード・プロンプトが表示されます。
2. expert コンソールのパスワードを入力します。Enter キーを押します。
3. 以下のコマンドを入力します。

   ```
   csh
   ```
4. 必要な顧客のログを選択します。

   ```
   mdsenv <customer name>
   ```
5. 以下のコマンドを入力します。

   ```
   # nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p
   <facility>.<priority> 2>&1 &
   ```

   各部分について以下で説明します。

   - *<facility>* は、syslog のファシリティーです (例: local3)。
   - *<priority>* は、syslog の優先順位です (例: info)。

   これで、QRadar でログ・ソースを構成する準備ができました。

   構成は完了です。Check Point Multi-Domain Management Provider-1 の syslog イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Check Point FireWall-1 イベントとしての Check Point Multi-Domain Management (Provider-1) からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。 Point Multi-Domain Management (Provider-1) syslog イベントのログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Check Point Firewall-1**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 95. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Check Point Multi-Domain Management (Provider-1) アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

Check Point Multi-Domain Management (Provider-1) のための OPSEC の構成

この手順では、IBM Security QRadar Check Point FireWall-1 DSM が OPSEC を使用して Check Point Multi-Domain Management (Provider-1) イベントを確実に受け入れるようにします。

このタスクについて

Check Point Multi-Domain Management (Provider-1) Management Domain GUI (MDG) で、QRadar を表すホスト・オブジェクトを作成します。*leapipe* は、Check Point Multi-Domain Management (Provider-1) と QRadar の間の接続です。

Check Point Multi-Domain Management (Provider-1) SmartCenter (MDG) を再構成するには、以下のようにします。

手順

1. ホスト・オブジェクトを作成するために、Check Point SmartDashboard ユーザー・インターフェースを開き、「管理 **(Manage)**」 > 「ネットワーク・オブジェクト **(Network Objects)**」 > 「新規 **(New)**」 > 「ノード **(Node)**」 > 「ホスト **(Host)**」を選択します。
2. 名前と IP アドレスを入力し、必要に応じてコメントを書きます。
3. 「**OK**」をクリックします。
4. 「閉じる **(Close)**」を選択します。
5. OPSEC 接続を作成するために、「管理 **(Manage)**」 > 「サーバーと **OPSEC** アプリケーション **(Servers and OPSEC Applications)**」 > 「新規 **(New)**」 > 「**OPSEC** アプリケーション・プロパティー **(OPSEC Application Properties)**」を選択します。
6. 名前を入力し、必要に応じてコメントを書きます。

   入力する名前は、ステップ 2 で使用した名前と異なるものでなければなりません。
7. 「ホスト **(Host)**」ドロップダウン・メニューから、作成した QRadar ホスト・オブジェクトを選択します。
8. 「アプリケーション・プロパティー **(Application Properties)**」で「ユーザー定義 **(User Defined)**」をベンダー・タイプとして選択します。
9. 「クライアント項目 **(Client Entries)**」から「**LEA**」を選択します。
10. Secure Internal Communication (SIC) 証明書を構成するために、「通信 **(Communication)**」をクリックし、アクティベーション・キーを入力します。
11. 「**OK**」を選択してから、「閉じる **(Close)**」を選択します。
12. ファイアウォールにポリシーをインストールするために、「ポリシー **(Policy)**」 > 「インストール **(Install)**」 > 「**OK**」を選択します。

OPSEC ログ・ソースの構成

以下のように、IBM Security QRadar でログ・ソースを構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

「ログ・ソース」ウィンドウが表示されます。

5. 「追加」をクリックします。

「ログ・ソースの追加」ウィンドウが表示されます。

6. 「ログ・ソース・タイプ」リストで、「**Check Point FireWall-1**」を選択します。
7. 「プロトコル構成」リストで「**OPSEC/LEA**」を選択します。

OPSEC/LEA プロトコルのパラメーターが表示されます。

8. ログ・ソース名 - ログ・ソースの名前を入力します。
9. ログ・ソース **ID** - ログ・ソースの IP アドレスを入力します。この値は、「サーバー **IP**」パラメーターで入力した値に一致する必要があります。
10. サーバー **IP** - Check Point Multi-Domain Management (Provider-1) の IP アドレスを入力します。
11. サーバー・ポート - OPSEC/LEA 用に使用するポート番号を入力します。デフォルトは 18184 です。

既存のファイアウォール・ポリシーで QRadar からの LEA/OPSEC 接続が許可されるようにする必要があります。

12. **OPSEC** アプリケーション・オブジェクトの **SIC** 属性 - OPSEC アプリケーション・オブジェクトの SIC DN を入力します。
13. ログ・ソースの **SIC** 属性 - ログ・ソースを生成するサーバーの SIC 名を入力します。

SIC 属性名は 255 文字まで可能であり、大/小文字が区別されます。

14. 証明書の指定 - 「証明書の指定」チェック・ボックスはクリアされている状態にしてください。
15. 証明書パスワードのプル - アクティベーション・キー・パスワードを入力します。
16. 認証局の **IP** - Check Point Manager Server の IP アドレスを入力します。
17. **OPSEC** アプリケーション - 証明書を要求する *OPSEC* アプリケーション の名前を入力します。

例: 値が `CN=QRadar-OPSEC,O=cpmodule...tdfaaz` の場合、「OPSEC アプリケーション」の値は `QRadar-OPSEC` になります。

18. 「保存」をクリックします。
19. 「管理」タブで「変更のデプロイ」をクリックします。

関連概念:

29 ページの『OPSEC/LEA プロトコルの構成オプション』

ポート 18184 でイベントを受信するには、OPSEC/LEA プロトコルを使用するようにログ・ソースを構成します。

第 30 章 Cilasoft QJRN/400

IBM Security QRadar は、IBM i (AS/400®、iSeries、System i®) 用の Cilasoft QJRN/400 ソフトウェアから、詳細監査イベントを収集します。

イベントを収集するために、管理者は、syslog を使用してイベントを転送するように Cilasoft QJRN/400 を構成するか、オプションで、イベントをファイルに書き込むように統合ファイル・システム (IFS) を構成することができます。syslog により、QRadar にリアルタイム・イベントが提供され、管理者用の自動ログ・ソース検出が行われます。これは、イベント収集の最も簡単な構成方法です。IFS オプションは、イベントをログ・ファイルに書き込むためのオプション構成を提供します。このオプションにより、ログ・ファイル・プロトコルを使用したリモート読み取りが可能になります。QRadar は、Cilasoft QJRN/400 V5.14.K 以降からの syslog イベントをサポートします。

Cilasoft QJRN/400 を構成するには、以下のタスクを実行します。

1. Cilasoft QJRN/400 インストール済み環境で、syslog イベントを QRadar に転送するか、syslog イベントをファイルに書き込むように、Cilasoft Security Suite を構成します。
2. syslog 構成では、管理者は、Cilasoft QJRN/400 によって転送されたイベントが「ログ・アクティビティー」タブで自動的に検出されることを検証できます。

IFS を使用してイベント・ファイルをディスクに書き込む Cilasoft QJRN/400 構成は、管理者が syslog を使用できない場合の代替構成として考えられます。IFS 構成では、管理者が IFS ファイルを特定し、FTP、SFTP、または SCP による通信を許可するようにホスト・システムを構成する必要があります。ログ・ファイル・プロトコルをイベント・ログ・ファイルの場所とともに使用するように、ログ・ソースを構成できます。

Cilasoft QJRN/400 の構成

イベントを収集するには、syslog イベントを IBM Security QRadar に転送するように Cilasoft QJRN/400 で照会を構成する必要があります。

手順

1. Cilasoft Security Suite を開始するには、以下のコマンドを入力します。

   ```
   IJRN/QJRN
   ```

   構成変更を行うために使用するアカウントは、ADM 特権または USR 特権を備えていて、**「拡張アクセス (Extended Access)」**パラメーターを介して特定の照会にアクセスできる必要があります。
2. 出力タイプを構成するには、以下のいずれかのオプションを選択します。

   選択したいくつかの照会を編集するには、`2EV` と入力して実行環境にアクセスし、「出力タイプ **(Output Type)**」フィールドを変更して `SEM` と入力します。

3. 多数の照会を編集するには、コマンド CHGQJQRYA を入力し、「出力タイプ **(Output Type)**」フィールドを変更して SEM と入力します。
4. 「追加パラメーター (Additional Parameters)」画面で、以下のパラメーターを構成します。

表 *96. Cilasoft QJRN/400* の出力パラメーター

パラメーター	説明
フォーマット **(Format)**	*LEEF と入力し、ログ拡張イベント・フォーマット (LEEF) でイベントを書き込むように syslog 出力を構成します。 LEEF は、IBM Security QRadar 用に設計された特殊なイベント・フォーマットです。
出力 **(Output)**	出力タイプを構成するために、以下のいずれかのパラメーターを使用して出力タイプを選択します。 *SYSLOG - syslog プロトコルでイベントを転送する場合は、このパラメーターを入力します。このオプションは、リアルタイムのイベントを提供します。 *IFS - 統合ファイル・システムを使用してイベントをファイルに書き込む場合は、このパラメーターを入力します。このオプションを使用する場合、管理者がログ・ファイル・プロトコルを使用してログ・ソースを構成する必要があります。このオプションでは、イベントをファイルに書き込みます。ファイルは、15 分の間隔でのみ読み取ることができます。
IP アドレス	IBM Security QRadar システムの IP アドレスを入力します。 IBM Security QRadar の IP アドレスが WRKQJVAL コマンドで特殊値として定義されている場合、*CFG と入力できます。 イベントは、QRadar コンソール、イベント・コレクター (Event Collector)、イベント・プロセッサー (Event Processor)、または IBM Security QRadar オールインワン・アプライアンスのいずれかに転送できます。
ポート	syslog イベントのポートとして 514 または *CFG と入力します。 デフォルトでは、*CFG によってポート 514 が自動的に選択されます。
タグ **(Tag)**	このフィールドは、IBM Security QRadar では使用されません。

表 96. *Cilasoft QJRN/400* の出力パラメーター (続き)

パラメーター	説明
ファシリティー **(Facility)**	このフィールドは、IBM Security QRadar では使用されません。
重大度	イベント重大度の値を選択します。 *QRY 宛先に割り当てられる重大度について詳しくは、*Cilasoft* の資料でコマンド **WRKQJFVAL** を参照してください。

Cilasoft の構成パラメーターについて詳しくは、「*Cilasoft QJRN/400 User's Guide*」を参照してください。

IBM Security QRadar に転送された syslog イベントは、「ログ・アクティビティー」タブで表示できます。

Cilasoft QJRN/400 ログ・ソースの構成

IBM Security QRadar は、Cilasoft QJRN/400 から転送された syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. IBM Security QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソース・タイプ」リストで「**Cilasoft QJRN/400**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。

   注**:** *IFS オプションを使用して統合ファイル・システムにイベントを書き込むように Cilasoft QJRN/400 が構成されている場合は、管理者は「ログ・ファイル」を選択して、ログ・ファイル・プロトコルを構成する必要があります。
8. プロトコル値を構成します。

   Syslog プロトコル・パラメーターの詳細**:**

表 97. *syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Cilasoft QJRN/400 インストール済み環境からのイベントの ID として IP アドレスを入力します。 「ログ・ソース **ID**」は、固有値でなければなりません。
有効	ログ・ソースを有効にするには、「有効」チェック・ボックスを選択します。 このチェック・ボックスはデフォルトで選択されます。
信頼性	ログ・ソースの「信頼性」を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的にディスカバーされたログ・ソースは、IBM Security QRadar の「システム設定」による「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	リストから、ログの構文解析と保管を行うための「受信イベント・ペイロード **(Incoming Event Payload)**」エンコーダーを選択します。

表 97. *syslog* プロトコルのパラメーター (続き)

パラメーター	説明
イベント・ペイロードの保管	ログ・ソースによるイベント・ペイロード情報の保管を有効にするには、「イベント・ペイロードの保管」チェック・ボックスを選択します。 デフォルトでは、自動的にディスカバーされたログ・ソースは、IBM Security QRadar の「システム設定」による「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

関連概念:

22 ページの『ログ・ファイル・プロトコルの構成オプション』
リモート・ホストからイベントを受信するには、ログ・ファイル・プロトコルを使用するようにログ・ソースを構成します。

第 31 章 Cisco

さまざまな Cisco DSM を IBM Security QRadar と統合できます。

Cisco ACE Firewall

Cisco ACE Firewall を IBM Security QRadar と統合できます。

QRadar は、syslog を使用して Cisco ACE Firewall から転送されたイベントを受け入れられます。QRadar は、関連するすべてのイベントを記録します。Cisco ACE Firewall と統合するように QRadar を構成するには、すべてのデバイス・ログを QRadar に転送するように Cisco ACE Firewall を構成する必要があります。

Cisco ACE Firewall の構成

Cisco ACE デバイスのログを IBM Security QRadar に転送するには、以下のようにします。

手順

1. Cisco ACE デバイスにログインします。
2. 「シェル・インターフェース (Shell Interface)」で「メインメニュー **(Main Menu)**」 > 「拡張オプション **(Advanced Options)**」 > 「**Syslog** 構成 **(Syslog Configuration)**」を選択します。
3. 「**Syslog** 構成 **(Syslog Configuration)**」メニューは、既に構成されている syslog 宛先ホストがあるかどうかによって異なります。構成されている syslog 宛先がない場合は、「第 **1** サーバーの追加 **(Add First Server)**」オプションを選択して syslog 宛先を作成します。「**OK**」をクリックします。
4. 「第 **1 Syslog** サーバー **(First Syslog Server)**」フィールドに、宛先ホストのホスト名または IP アドレスとポートを入力します。「**OK**」をクリックします。

   システムが新しい設定を使用して再始動します。完了すると、「Syslog サーバー (Syslog server)」ウィンドウに、構成したホストが表示されます。
5. 「**OK**」をクリックします。

   「**Syslog** 構成 **(Syslog Configuration)**」メニューが表示されます。ここで、サーバー構成の編集、サーバーの削除、第 2 サーバーの追加用のオプションが使用可能になっていることに注意してください。
6. 別のサーバーを追加する場合は、「第 **2** サーバーの追加 **(Add Second Server)**」をクリックします。

   いつでも、「**Syslog** オプションの表示 **(View Syslog options)**」をクリックして既存のサーバー構成を表示できます。
7. 「拡張 **(Advanced)**」メニューに戻るために、「戻る **(Return)**」をクリックします。

構成は完了です。Cisco ACE Firewall イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Cisco ACE Firewall アプライアンスによって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Cisco ACE Firewall からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。 QRadar 用のログ・ソースを手動で作成して Syslog イベントを受信することができます。

Cisco ACE Firewall のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco ACE Firewall**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *98. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco ACE Firewall からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Cisco Aironet

Cisco Aironet デバイスを IBM Security QRadar と統合できます。

このタスクについて

Cisco Aironet DSM は、syslog を使用して Cisco Emblem フォーマットのイベントを受け入れます。Cisco Aironet デバイスと統合するように QRadar を構成する前に、syslog イベントを転送するように Cisco Aironet アプライアンスを構成する必要があります。

イベントを転送するように Cisco Aironet を構成するには、以下のようにします。

手順

1. 以下のいずれかの方法を使用して、Cisco Aironet デバイスへの接続を確立します。
   - ワイヤレス・アクセス・ポイントへの Telnet 接続
   - コンソールへのアクセス
2. 以下のコマンドを入力して、特権 EXEC モードにアクセスします。

   ```
   enable
   ```
3. 以下のコマンドを入力して、グローバル構成モードにアクセスします。

   ```
   config terminal
   ```
4. 以下のコマンドを入力して、メッセージ・ロギングを有効にします。

   ```
   logging on
   ```
5. syslog ファシリティーを構成します。デフォルトは local7 です。

   `logging <`*facility*`>`

   ここで、<*facility*> は、例えば local7 です。
6. 以下のコマンドを入力して、メッセージを QRadar のログに記録します。

   `logging <`*IP address*`>`

   ここで、<*IP address*> は、QRadar の IP アドレスです。
7. 以下のように、ログ・メッセージの **timestamp** を有効にします。

   ```
   service timestamp log datatime
   ```
8. 以下のように、特権 EXEC モードに戻ります。

   ```
   end
   ```
9. 以下のように、項目を表示します。

   ```
   show running-config
   ```
10. 以下のように、項目を構成ファイルに保存します。

    ```
    copy running-config startup-config
    ```

構成は完了です。Cisco Aironet イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Cisco Aironet アプライアンスによって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Cisco Aironet の syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。 Cisco Aironet のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco Aironet**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *99. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco Aironet アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Cisco ACS

IBM Security QRadar 用の Cisco ACS DSM は、syslog を使用して syslog ACS イベントを受け入れます。

QRadar は、イベントからの入手可能な関連情報をすべて記録します。以下のいずれかの方法で、Cisco ACS を QRadar と統合できます。

- Cisco ACS v5.x の場合、syslog を直接 QRadar に送信するように Cisco ACS デバイスを構成します。『Cisco ACS v5.x 用の Syslog の構成』を参照してください。
- Cisco ACS v4.x の場合、syslog を直接 QRadar に送信するように Cisco ACS デバイスを構成します。 257 ページの『Cisco ACS v4.x 用の Syslog の構成』を参照してください。
- QRadar WinCollect または QRadar Adaptive Log Exporter を使用するサーバー (Cisco ACS ソフトウェアのバージョン 3.x 以降)。 259 ページの『Adaptive Log Exporter 用の Cisco ACS の構成』を参照してください。

注: QRadar は、ユニバーサル DSM を使用している場合にのみ、バージョン v3.x より前の Cisco ACS をサポートします。

Cisco ACS v5.x 用の Syslog の構成

ソフトウェア・バージョン 5.x の Cisco ACS アプライアンスからの syslog 転送の構成では、いくつかのステップを実行する必要があります。

このタスクについて

以下の作業を行う必要があります。

手順

1. リモート・ログ・ターゲットの作成
2. グローバル・ロギング・カテゴリーの構成
3. ログ・ソースの構成

リモート・ログ・ターゲットの作成

Cisco ACS アプライアンスのリモート・ログ・ターゲットを作成します。

Cisco ACS アプライアンスにログインします。

ナビゲーション・メニューで、「システム管理 **(System Administration)**」 > 「構成 **(Configuration)**」 > 「ログ構成 **(Log Configuration)**」 > 「リモート・ログ・ターゲット **(Remote Log Targets)**」をクリックします。

「リモート・ログ・ターゲット (Remote Log Targets)」ページが表示されます。

「作成」をクリックします。

以下のパラメーターを構成します。

表 100. リモート・ターゲット・パラメーター

パラメーター	説明
名前	リモート syslog ターゲットの名前を入力します。
説明	リモート syslog ターゲットの説明を入力します。
タイプ	「**Syslog**」を選択します。

表 100. リモート・ターゲット・パラメーター (続き)

パラメーター	説明
IP アドレス	QRadar またはイベント・コレクター (Event Collector)の IP アドレスを入力します。

「送信 **(Submit)**」をクリックします。

これで、Cisco ACS アプライアンスでのイベント・ロギング用のグローバル・ポリシーを構成する準備ができました。

グローバル・ロギング・カテゴリーの構成

ログ失敗試行を IBM Security QRadar に転送するように Cisco ACS を構成するには、以下のようにします。

手順

1. ナビゲーション・メニューで「システム管理 **(System Administration)**」 > 「構成 **(Configuration)**」 > 「ログ構成 **(Log Configuration)**」 > 「グローバル **(Global)**」をクリックします。

   「ロギング・カテゴリー (Logging Categories)」ウィンドウが表示されます。
2. 「失敗試行 **(Failed Attempts)**」ロギング・カテゴリーを選択し、「編集 **(Edit)**」をクリックします。
3. 「リモート **Syslog** ターゲット **(Remote Syslog Target)**」をクリックします。
4. 「使用可能なターゲット (Available targets)」ウィンドウから、矢印キーを使用して QRadar の syslog ターゲットを「選択されたターゲット (Selected targets)」ウィンドウに移動します。
5. 「送信 **(Submit)**」をクリックします。

   これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Cisco ACS v5.x からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

ただし、QRadar のログ・ソースを手動で作成して Cisco ACS イベントを受信することもできます。

Cisco ACS のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。

4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース・タイプ」リストで、「**Cisco ACS**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
8. 以下の値を構成します。

表 101. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco ACS イベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Cisco ACS v4.x 用の Syslog の構成

ソフトウェア・バージョン 4.x の Cisco ACS アプライアンスからの syslog 転送の構成では、いくつかのステップを実行する必要があります。

このタスクについて

以下のステップを実行します。

手順

1. syslog 転送の構成
2. ログ・ソースの構成

Cisco ACS v4.x の syslog 転送の構成

syslog イベントを IBM Security QRadar に転送するための ACS デバイスの構成について説明します。

このタスクについて

以下の手順を実行して、syslog イベントを QRadar に転送するように ACS デバイスを構成します。

手順

1. Cisco ACS デバイスにログインします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。

   「システム構成 (System Configuration)」ページが開きます。
3. 「ログの記録」をクリックします。

ロギング構成が表示されます。

4. 「失敗試行 **(Failed Attempts)**」の「Syslog」列で「構成 **(Configure)**」をクリックします。

   「ロギングの有効化 (Enable Logging)」ウィンドウが表示されます。

5. 「**Syslog** 失敗試行レポートに記録 **(Log to Syslog Failed Attempts report)**」チェック・ボックスを選択します。
6. 以下のログ属性を追加します。
   - メッセージ・タイプ **(Message-Type)**
   - ユーザー名 **(User-Name)**
   - **Nas** の **IP** アドレス **(Nas-IP-Address)**
   - 認証失敗コード **(Authen-Failure-Code)**
   - 呼び出し元 **ID (Caller-ID)**
   - **NAS** ポート **(NAS-Port)**
   - 認証データ **(Author-Data)**
   - グループ名 **(Group-Name)**
   - フィルター情報 **(Filter Information)**
   - リモートでログ記録 **(Logged Remotely)**
7. 以下の syslog パラメーターを構成します。

表 *102. Syslog* パラメーター

パラメーター	説明
IP	QRadar の IP アドレスを入力します。
ポート	IBM Security QRadar の syslog ポート番号を入力します。デフォルトはポート 514 です。
最大メッセージ長 **(**バイト**) - タイプ (Max message length (Bytes) - Type)**	最大 syslog メッセージ長として 1024 と入力します。

   注**:** Cisco ACS は、最大で 2 つの syslog サーバーの syslog レポート情報を提供します。

8. 「送信 **(Submit)**」をクリックします。

   これで、QRadar でログ・ソースを構成する準備ができました。

Cisco ACS v4.x のログ・ソースの構成

IBM Security QRadar は、Cisco ACS v4.x からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

Cisco ACS v4.x のログ・ソースを手動で作成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース・タイプ」リストで、「**Cisco ACS**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
8. 以下の値を構成します。

表 103. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco ACS イベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Adaptive Log Exporter 用の Cisco ACS の構成

古いバージョンの Cisco ACS (v3.x など) を使用している場合、Cisco ACS アプライアンスからのイベントをコンマ区切りファイルにログ記録できます。

Adaptive Log Exporter 用の Cisco ACS デバイス・プラグインを使用して、コンマ区切りファイル内のイベントの読み取りおよび IBM Security QRadar への転送を行うことができます。

イベントをログに記録するための Cisco ACS の構成

Cisco ACS アプライアンスは、Adaptive Log Exporter と統合するためにコンマ区切りのイベント・ファイルを書き込むように構成する必要があります。

このタスクについて

Cisco ACS を構成するには、以下の手順を実行します。

手順

1. Cisco ACS アプライアンスにログインします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。

「システム構成 (System Configuration)」ページが開きます。

3. 「ログの記録」をクリックします。

   ロギング構成が表示されます。

4. 「失敗試行用の **CSV** 列 **(CSV column for Failed Attempts)**」で「構成 **(Configure)**」をクリックします。

   「ロギングの有効化 (Enable Logging)」ウィンドウが表示されます。

5. 「**CSV** 失敗試行レポートに記録 **(Log to CSV Failed Attempts report)**」チェック・ボックスを選択します。
6. 以下のログ属性を追加します。
   - メッセージ・タイプ (Message-Type)
   - ユーザー名 (User-Name)
   - Nas の IP アドレス (Nas-IP-Address)
   - 認証失敗コード (Authen-Failure-Code)
   - 呼び出し元 ID (Caller-ID)
   - NAS ポート (NAS-Port)
   - 認証データ (Author-Data)
   - グループ名 (Group-Name)
   - フィルター情報 (Filter Information)
   - リモートでログ記録 (Logged Remotely)
7. Cisco ACS が新しいコンマ区切り値 (CSV) ファイルを生成するように時間フレームを構成します。
8. 「送信 **(Submit)**」をクリックします。

次のタスク

これで、Adaptive Log Exporter を構成する準備ができました。詳しくは、「*Adaptive Log Exporter Users Guide*」を参照してください。

Cisco ASA

Cisco Adaptive Security Appliance (ASA) を IBM Security QRadar と統合できます。

Cisco ASA DSM は、syslog を介してイベントを受け入れるか、NetFlow Security Event Logging (NSEL) を使用して NetFlow を受け入れます。QRadar は、関連するすべてのイベントを記録します。QRadar を構成する前に、syslog イベントまたは NetFlow NSEL イベントを転送するように Cisco ASA デバイスを構成しておく必要があります。

次のオプションのいずれかを選択してください。

- syslog を使用してイベントを QRadar に転送する。 261 ページの『syslog を使用した Cisco ASA の統合』を参照してください。
- NetFlow (NSEL) を使用してイベントを QRadar に転送する。 263 ページの『NSEL を使用した NetFlow 用の Cisco ASA の統合』を参照してください。

syslog を使用した Cisco ASA の統合

syslog を使用した Cisco ASA の統合には、ログ・ソースの構成と syslog 転送の構成が必要です。

syslogを使用して Cisco ASA を統合するには、以下のタスクを実行します。

- 『syslog の転送の構成』
- 262 ページの『ログ・ソースの構成』

syslog の転送の構成

Syslog イベントを転送するように Cisco ASA を構成するには、いくつかの手動構成が必要です。

手順

1. Cisco ASA デバイスにログインします。
2. 以下のコマンドを入力して、特権 EXEC モードにアクセスします。

   ```
   enable
   ```
3. 以下のコマンドを入力して、グローバル構成モードにアクセスします。

   ```
   conf t
   ```
4. 以下のように、ロギングを有効にします。

   ```
   logging enable
   ```
5. 以下のように、ロギング詳細を構成します。

   ```
   logging console warning

   logging trap warning

   logging asdm warning
   ```

   注: Cisco ASA デバイスは、さらに多くのイベントを送信するように、`logging trap informational` を使用して構成することもできます。ただし、この場合は、デバイスのイベント速度 (イベント/秒) が増大します。
6. 以下のコマンドを入力して、IBM Security QRadar へのロギングを構成します。

   `logging host <interface> <IP address>`

   各部分について以下で説明します。

   - *<interface>* は、Cisco Adaptive Security Appliance インターフェースの名前です。
   - *<IP address>* は QRadar の IP アドレスです。

   注: コマンド **show interfaces** を使用すると、Cisco デバイスの使用可能なすべてのインターフェースが表示されます。
7. 以下のように、出力オブジェクト名オプションを無効にします。

   ```
   no names
   ```

出力オブジェクト名オプションを無効にして、ログがオブジェクト名ではなく、IP アドレスを使用するようにしてください。

8. 以下のように、構成を終了します。

```
exit
```

9. 以下のように、変更を保存します。

```
write mem
```

タスクの結果

構成は完了です。Cisco ASA の syslog イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Cisco ASA によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Cisco ASA からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

このタスクについて

Cisco ASA からの syslog イベントに対して、手動でログ・ソースを構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco Adaptive Security Appliance (ASA)**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *104. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	OSSEC インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

NSEL を使用した NetFlow 用の Cisco ASA の統合

NSEL を使用した NetFlow 用の Cisco ASA の統合には、2 つのステップを実行する必要があります。

このセクションには、以下のトピックが含まれます。

- 『NSEL を使用した NetFlow の構成』
- 265 ページの『ログ・ソースの構成』

NSEL を使用した NetFlow の構成

NSEL を使用して NetFlow イベントを転送するように Cisco ASA を構成できます。

手順

1. Cisco ASA デバイスのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力して、特権 EXEC モードにアクセスします。

   ```
   enable
   ```
3. 以下のコマンドを入力して、グローバル構成モードにアクセスします。

   ```
   conf t
   ```
4. 以下のように、出力オブジェクト名オプションを無効にします。

   ```
   no names
   ```
5. 以下のコマンドを入力して、NetFlow エクスポートを有効にします。

   `flow-export destination` *<interface-name> <ipv4-address or hostname> <udp-port>*

   各部分について以下で説明します。

   - *<interface-name>* は、NetFlow コレクター用の Cisco Adaptive Security Appliance インターフェースの名前です。
   - *<ipv4-address or hostname>* は、NetFlow コレクター・アプリケーションが含まれている Cisco ASA デバイスの IP アドレスまたはホスト名です。
   - *<udp-port>* は、NetFlow パケットの送信先の UDP ポート番号です。

注: IBM Security QRadar は通常、QRadar QFlow コレクターで NetFlow イベント・データにポート 2055 を使用します。NSEL を使用して、NetFlow 用の Cisco Adaptive Security Appliance で別の UDP ポートを構成する必要があります。

6. 以下のコマンドを入力して、NSEL class-map を構成します。

   ```
   class-map flow_export_class
   ```

7. 以下のいずれかのトラフィック・オプションを選択します。

   特定のトラフィックに一致するように NetFlow アクセス・リストを構成するには、以下のコマンドを入力します。

   ```
   match access-list flow_export_acl
   ```

8. 任意のトラフィックに一致するように NetFlow を構成するには、以下のコマンドを入力します。

   ```
   match any
   ```

   注: 263 ページの『NSEL を使用した NetFlow の構成』でトラフィック一致オプションを定義する前に、Cisco ASA デバイス上にアクセス制御リスト (ACL) が存在している必要があります。

9. 以下のコマンドを入力して、NSEL policy-map を構成します。

   ```
   policy-map flow_export_policy
   ```

10. 以下のコマンドを入力して、flow-export アクションのクラスを定義します。

    ```
    class flow_export_class
    ```

11. 以下のコマンドを入力して、flow-export アクションを構成します。

    ```
    flow-export event-type all destination <IP address>
    ```

    ここで、<*IP address*> は、QRadar の IP アドレスです。

    注: v8.3 より前のバージョンの Cisco ASA を使用している場合は、デバイスがデフォルトで flow-export 宛先になるため、 263 ページの『NSEL を使用した NetFlow の構成』をスキップできます。詳しくは、ご使用の *Cisco ASA* の資料 を参照してください。

12. 以下のコマンドを入力して、サービス・ポリシーをグローバルに追加します。

    ```
    service-policy flow_export_policy global
    ```

13. 以下のように、構成を終了します。

    ```
    exit
    ```

14. 以下のように、変更を保存します。

    ```
    write mem
    ```

    コレクター・アプリケーションがイベントを相関付けるために「イベント時刻 **(Event Time)**」フィールドを使用していることを確認する必要があります。

ログ・ソースの構成

NetFlow を使用する Cisco ASA を IBM Security QRadar と統合するには、NetFlow イベントを受信するためのログ・ソースを手動で作成する必要があります。

このタスクについて

QRadar が、NetFlow および NSEL を使用する Cisco ASA デバイスからの syslog イベントに対して、ログソースを自動的に検出および作成することはありません。

注**:** NetFlow および NSEL を使用する Cisco ASA デバイスと統合するには、システムで現行バージョンの NSEL プロトコルを実行している必要があります。NSEL プロトコルは、IBM サポート (http://www.ibm.com/support) から、または QRadar での自動更新を使用して入手可能です。

ログ・ソースを構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco Adaptive Security Appliance (ASA)**」を選択します。
9. 「プロトコル構成」リストで「**Cisco NSEL**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 105. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。

表 105. Syslog パラメーター (続き)

パラメーター	説明
コレクター・ポート	Cisco ASA が NSEL イベントの転送に使用する UDP ポート番号を入力します。「コレクター・ポート」パラメーターの有効な範囲は 1 から 65535 です。 QRadar は通常、QRadar QFlow コレクター で NetFlow イベント・データにポート 2055 を使用します。NSEL を使用する NetFlow 用の Cisco Adaptive Security Appliance で別の UDP ポートを定義する必要があります。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。 Cisco ASA によって QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。Cisco ASA デバイスでの NetFlow の構成について詳しくは、ベンダーの資料を参照してください。

Cisco CallManager

IBM Security QRadar 用の Cisco CallManager DSM は、Syslog を使用して Cisco CallManager デバイスから転送されたアプリケーション・イベントを収集します。

QRadar でイベントを受信できるようにするには、イベントを転送するように Cisco Call Manager デバイスを構成する必要があります。Cisco CallManager から Syslog イベントを転送すると、QRadar が Cisco CallManager を自動的に検出し、ログ・ソースとして追加します。

syslog の転送の構成

以下のようにして、Cisco CallManager で syslog を構成することができます。

手順

1. Cisco CallManager インターフェースにログインします。
2. 「システム・エンタープライズ **(System Enterprise)**」 > 「パラメーター **(Parameters)**」を選択します。

   「エンタープライズ・パラメーターの構成 (Enterprise Parameters Configuration)」が表示されます。
3. 「リモート **Syslog** サーバー名 **(Remote Syslog Server Name)**」フィールドに、QRadar コンソールの IP アドレスを入力します。
4. 「リモート **Syslog** メッセージの **Syslog** 重大度 **(Syslog Severity For Remote Syslog messages)**」リストで「情報 **(Informational)**」を選択します。

   「情報 (Informational)」重大度を選択すると、情報レベル以上のすべてのイベントを収集できます。
5. 「保存」をクリックします。

6. 「構成の適用 **(Apply Config)**」をクリックします。

   syslog の構成は完了です。これで、Cisco CallManager の syslog ログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Cisco CallManager デバイスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。 Cisco CallManager の syslog ログ・ソースを手動で構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco Call Manager**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 106. Syslog パラメーター

パラメーター	説明
ログ・ソース ID	Cisco CallManager からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Catalyst スイッチ用 Cisco CatOS

IBM Security QRadar 用の Catalyst スイッチ用 Cisco CatOS DSM は、syslog を使用してイベントを受け入れます。

QRadar は、関連するすべてのデバイス・イベントを記録します。QRadar で Cisco CatOS デバイスを構成する前に、syslog イベントを転送するようにデバイスを構成しておく必要があります。

syslog の構成

syslog イベントを転送するように Cisco CatOS デバイスを構成します。

このタスクについて

以下の手順を実行して、syslog イベントを転送するように Cisco CatOS デバイスを構成します。

手順

1. Cisco CatOS ユーザー・インターフェースにログインします。
2. 以下のコマンドを入力して、特権 EXEC モードにアクセスします。

   ```
   enable
   ```
3. 以下のように、システムで **timestamp** メッセージを構成します。

   ```
   set logging timestamp enable
   ```
4. IBM Security QRadar の IP アドレスを指定して、以下のコマンドを入力します。

   ```
   set logging server <IP address>
   ```
5. 以下のように、重大度レベルを選択して、ログに記録されるメッセージを制限します。

   ```
   set logging server severity <server severity level>
   ```
6. メッセージで使用するファシリティー・レベルを構成します。デフォルトは local7 です。

   ```
   set logging server facility <server facility parameter>
   ```
7. スイッチによる syslog メッセージの QRadar への送信を有効にします。

   ```
   set logging server enable
   ```

   これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Cisco CatOS アプライアンスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

Cisco CatOS の syslog ログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Catalyst** スイッチ用 **Cisco CatOS**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 107. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Catalyst スイッチ用 Cisco CatOS アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Cisco CSA

Cisco Security Agent (CSA) サーバーを IBM Security QRadar と統合できます。

Cisco CSA DSM は、syslog、SNMPv1、および SNMPv2 を使用してイベントを受け入れます。QRadar は、構成済みの Cisco CSA アラートをすべて記録します。

Cisco CSA 用の Syslog の構成

イベントを転送するための Cisco CSA サーバーの構成について説明します。

このタスクについて

以下の手順を実行して、イベントを転送するように Cisco CSA サーバーを構成します。

手順

1. Cisco CSA ユーザー・インターフェースを開きます。
2. 「イベント **(Events)**」 > 「アラート **(Alerts)**」を選択します。
3. 「新規」をクリックします。

   「構成ビュー (Configuration View)」ウィンドウが表示されます。
4. 以下のパラメーターの値を入力します。
   - 名前 **(Name)** - 構成に割り当てる名前を入力します。
   - 説明 **(Description)** - 構成の説明を入力します。このステップは必須ではありません。
5. 「アラートの送信 **(Send Alerts)**」で、アラートを生成するイベント・セットをリストから選択します。
6. 「**SNMP**」チェック・ボックスを選択します。
7. コミュニティー名を入力します。

   CSA ユーザー・インターフェースで入力するコミュニティー名は、IBM Security QRadar で構成されているコミュニティー名に一致する必要があります。このオプションは、SNMPv2 プロトコルの場合にのみ使用可能です。
8. 「マネージャー **IP** アドレス **(Manager IP address)**」パラメーターで、QRadar の IP アドレスを入力します。
9. 「保存」をクリックします。

   これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Cisco CSA アプライアンスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

Cisco CSA の syslog ログ・ソースを手動で構成するには、以下の構成手順 (オプション) を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。

7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco CSA**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 108. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco CSA アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Cisco FireSIGHT Management Center

FireSIGHT Management Center は、以前は Sourcefire Defense Center と呼ばれていました。

Cisco FireSIGHT Management Center 用の IBM Security QRadar DSM では、eStreamer API サービスを使用して FireSIGHT Management Center イベントを受け入れます。

QRadar では、FireSIGHT Management Center v4.8.0.2 から v6.0.0 がサポートされます。

QRadar で FireSIGHT Management Center 5.1.x イベントを収集するには、Cisco FireSIGHT Management Center の Web サイトから次のいずれかのパッチをダウンロードしてインストールする必要があります。

- `Sourcefire_hotfix-v5.1.0-0-build_1.tar`
- `Sourcefire_hotfix-v5.1.1-0-build_1.tar`

ご使用の FireSIGHT アプライアンス用のパッチについて詳しくは、Cisco FireSIGHT Management Center の Web サイトを参照してください。

構成の概要

FireSIGHT Management Center と統合するには、 FireSIGHT Management Center インターフェースで証明書を作成し、eStreamer イベント・データを受信する QRadar アプライアンスにその証明書を追加する必要があります。

デプロイメントに複数の FireSIGHT Management Center アプライアンスが含まれている場合、eStreamerイベントを受信する各アプライアンスに、証明書をコピーする必要があります。証明書に基づき、FireSIGHT Management Center アプライアンスと QRadar コンソール または QRadar イベント・コレクター は、eStreamer API を使用して通信してイベントを収集することができます。

QRadar を FireSIGHT Management Center と統合するには、以下のステップを実行します。

1. FireSIGHT Management Center アプライアンスで eStreamer 証明書を作成します。
2. FireSIGHT Management Center 証明書ファイルを QRadar に追加します。
3. FireSIGHT Management Center アプライアンス用の QRadar でログ・ソースを構成します。

サポートされるイベント・タイプ

QRadar は、FireSIGHT Management Center からの以下のイベント・タイプをサポートしています。

- 侵入イベントおよび追加データ:

  QRadar の Cisco FireSIGHT Management Center DSM で分類される侵入イベントでは、すべての侵入イベントが適切に分類されるように、Snort DSM と同じ QRadar ID (QID) を使用します。

  1,000,000 から 2,000,000 の範囲の侵入イベントは、FireSIGHT Management Center のユーザー定義ルールに分類されます。イベントを生成するユーザー定義ルールは、不明なイベントとして QRadar に追加され、イベント・タイプを説明する追加情報が組み込まれます。例えば、ユーザー定義イベントは「不明: FireSIGHT Management Center のバッファー・オーバーフロー (Unknown:Buffer Overflow for FireSIGHT Management Center)」として識別することができます。
- 相関イベント
- メタデータ・イベント
- ディスカバリー・イベント
- ホスト・イベント
- ユーザー・イベント
- マルウェア・イベント
- ファイル・イベント

Cisco FireSIGHT Management Center DSM のサンプル・イベント・メッセージを次の表に示します。

表 *109. Cisco FireSIGHT Management Center* デバイスによってサポートされる *Cisco FireSIGHT Management Center* サンプル・メッセージ。

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
New_Network_Protocol	情報	DeviceType=Estreamer DeviceAddress =1.1.1.1 CurrentTime=1462455523216 recordType=NEW_NETWORK_PROTOCOL recordLength=42 timestamp=21 Feb 2014 11:18:47 detectionEngineRef=2 ipAddress=2.2.2.2. MACAddress= 00:00:00:00:00:00 hasIPv6=false eventSecond=1392995924 event MicroSecond=464098 eventType=NEW_ NETWORK_PROTOCOL fileNumber=875E0753 filePosition=BF0B0000 protocol. protocolId=2048 protocol.protocol Name=IP

表 109. *Cisco FireSIGHT Management Center* デバイスによってサポートされる *Cisco FireSIGHT Management Center* サンプル・メッセージ。 *(続き)*

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
Intrusion_Event_Record	その他のエクスプロイト	DeviceType=Estreamer DeviceAddress =1.1.1.1 CurrentTime=1462455518176 recordType=INTRUSION_EVENT_RECORD3 recordLength=60 timestamp=18 Feb 2014 10:22:45 detectionEngineRef=3 eventId=133241 eventSecond=13927333 65 eventMicrosecond=739677 rule. generatorId=1 rule.ruleId=18312 rule .ruleRevision=5 rule.rendered SignatureId=18312 rule.message= SERVER-OTHER Subversion 1.0.2 get- dated-rev buffer overflow attempt rule.ruleUUID=439966ABC58A491CB47D2 04EB9A560D8 rule.ruleRevisionUUID= F322B90F2B9311E3B791848F69E36DD2 classification.classificationId=9 classification.name=attempted-user classification.description=Attempted User Privilege Gain classification. classificationUUID=9D0A6F5ECBA211D9 925A005056040501 classification. classificationRevisionUUID=00000000 00000000000000000000000000 priority. priorityId=1 priority.name=high sourceAddress=2.1.2.2 destination Address=2.2.2.2 sourcePortOrICMPType =50594 destinationPortOrICMPCode= 3690 ipProtocolId=6 impactFlags= 00000001 impact=4 blocked=0 vlanId=0

FireSIGHT Management Center 4.x 証明書の作成

IBM Security QRadar では、デプロイメントのすべての Cisco FireSIGHT Management Center アプライアンスについて証明書が必要です。証明書は pkcs12 形式で生成されるため、QRadar アプライアンスで使用可能な鍵ストア・ファイルおよびトラストストア・ファイルに変換する必要があります。

手順

1. FireSIGHT Management Center インターフェースにログインします。
2. 「操作」 > 「構成」 > 「**eStreamer**」を選択します。
3. 「**eStreamer**」タブをクリックします。
4. 「クライアントの作成」をクリックします。
5. FireSIGHT Management Center が QRadar に提供するイベント・タイプのチェック・ボックスを選択します。
6. インターフェースの右側上部にある「**+** クライアントの作成」をクリックします。
7. 「ホスト名」フィールドに、IP アドレスまたはホスト名を入力します。
   - QRadar コンソール またはオールインワン・アプライアンスを使用して eStreamer イベントを収集する場合は、QRadar コンソール の IP アドレスまたはホスト名を入力します。
   - リモート・イベント・コレクターを使用して eStreamer イベントを収集する場合は、リモート・イベント・コレクターの IP アドレスまたはホスト名を入力します。

- 高可用性 (HA) を使用する場合は、仮想 IP アドレスを入力します。

8. 「パスワード」フィールドでは、パスワード・フィールドを空のままにするか、証明書のパスワードを入力して、「保存」をクリックします。

   新しいクライアントが「**eStreamer Client**」リストに追加され、ホストがポート 8302 の eStreamer API と通信できるようになります。

9. 「証明書の場所」列から、作成したクライアントをクリックし、pkcs12 証明書をファイルの場所に保存して「**OK**」をクリックします。

次のタスク

これで、FireSIGHT Management Center 証明書をご使用の QRadar アプライアンスにインポートする準備ができました。

Cisco FireSIGHT Management Center 5.x および 6.x の証明書の作成

証明書は、デプロイメント内の Cisco FireSIGHT Management Center アプライアンスで作成します。

このタスクについて

QRadar では、デプロイメントのすべての FireSIGHT Management Center アプライアンスについて証明書が必要です。証明書は pkcs12 形式で生成されるため、QRadar アプライアンスで使用可能な鍵ストア・ファイルおよびトラストストア・ファイルに変換する必要があります。

手順

1. FireSIGHT Management Center インターフェースにログインします。
2. バージョン 5.x を使用している場合は、「システム」 > 「ローカル」 > 「登録」を選択します。
3. バージョン 6.x を使用している場合は、「システム」 > 「統合」を選択します。
4. 「**eStreamer**」タブをクリックします。
5. FireSIGHT Management Center が QRadar に提供するイベント・タイプのチェック・ボックスを選択して「保存」をクリックします。
6. インターフェースの右側上部にある「**+** クライアントの作成」をクリックします。
7. 「ホスト名」フィールドに、IP アドレスまたはホスト名を入力します。
   - QRadar コンソールまたはオールインワン・アプライアンスを使用して eStreamer イベントを収集する場合は、QRadar コンソールの IP アドレスまたはホスト名を入力します。
   - イベント・コレクターを使用して eStreamer イベントを収集する場合は、イベント・コレクターの IP アドレスまたはホスト名を入力します。
   - 高可用性 (HA) を使用する場合は、仮想 IP アドレスを入力します。
8. 「パスワード」フィールドに証明書のパスワードを入力するか、フィールドを空のままにして、「保存」をクリックします。

新規クライアントが「ストリーマー・クライアント (Streamer Client)」リストに追加され、ホストがポート 8302 の eStreamer API と通信できるようになります。

9. pkcs12 証明書をファイルの場所に保存するためのホストのダウンロード矢印をクリックします。
10. 「**OK**」をクリックして、ファイルをダウンロードします。

次のタスク

これで、FireSIGHT Management Center 証明書をご使用の QRadar アプライアンスにインポートする準備ができました。

QRadar への Cisco FireSIGHT Management Center 証明書のインポート

QRadar の estreamer-cert-import.pl スクリプトは、pkcs12 証明書ファイルを鍵ストア・ファイルおよびトラストストア・ファイルに変換して、その証明書を QRadar アプライアンスの適切なディレクトリーに配置します。QRadar コンソールまたはイベント・コレクターにインポートする必要がある Sourcefire Defense Center pcks12 証明書ごとにこの手順を繰り返します。

始める前に

`estreamer-cert-import.pl` インポート・スクリプトを実行するには、`root` 特権または `su - root` 特権が必要です。

このタスクについて

`estreamer-cert-import.pl` スクリプトは、FireSIGHT Management Center プロトコルのインストール時に QRadar アプライアンスに保管されます。

このスクリプトでは、一度に 1 つずつ、pkcs12 ファイルを変換してインポートします。ユーザーが行う必要があるのは、FireSIGHT Management Center ログ・ソースを管理する QRadar アプライアンスの証明書のインポートだけです。例えば、FireSIGHT Management Center イベントが QRadar デプロイメントでイベント・コレクターによってカテゴリー化および正規化された後で、QRadar コンソールに転送されるとします。このシナリオでは、イベント・コレクターに証明書をインポートします。

新規証明書をインポートすると、QRadar アプライアンス上の既存の FireSIGHT Management Center 証明書は、`estreamer.keystore.old` と `estreamer.truststore.old` に名前変更されます。

手順

1. QRadar コンソールまたはイベント・コレクターに root ユーザーとしてログインします。
2. pkcs12 証明書を FireSIGHT Management Center アプライアンスから以下のディレクトリーにコピーします。

   ```
   /opt/qradar/bin/
   ```

3. pkcs12 ファイルをインポートするには、以下のコマンドと追加パラメーター (ある場合) を入力します。

   ```
   /opt/qradar/bin/estreamer-cert-import.pl -f pkcs12_file_name options
   ```

   追加パラメーターについては以下の表で説明します。

パラメーター	説明
-f	インポートする pkcs12 ファイルのファイル名を識別します。
-o	鍵ストア・ファイルおよびトラストストア・ファイルのデフォルトの Estreamer 名をオーバーライドします。複数の FireSIGHT Management Center デバイスを統合する場合に -o パラメーターを使用します。例えば、/opt/qradar/bin/estreamer-cert-import.pl -f <ファイル名> -o 192.168.1.100 のようになります。 インポート・スクリプトで、以下のファイルが作成されます。 • /opt/qradar/conf/ 192.168.0.100.keystore • /opt/qradar/conf/ 192.168.0.100.truststore
-d	インポート・スクリプトの冗長モードを有効にします。冗長モードは、pkcs12 ファイルが正しくインポートされない場合に、トラブルシューティングの目的でエラー・メッセージを表示するためのものです。
-p	pkcs12 ファイルの生成時にパスワードが誤って入力されている場合に、パスワードを指定します。
-v	インポート・スクリプトのバージョン情報を表示します。
-h	インポート・スクリプトの使用に関するヘルプ・メッセージを表示します。

タスクの結果

インポート・スクリプトにより、以下の場所に鍵ストア・ファイルとトラストストア・ファイルが作成されます。

- /opt/qradar/conf/estreamer.keystore
- /opt/qradar/conf/estreamer.truststore

Cisco FireSIGHT Management Center イベントのログ・ソースの構成

QRadar では Cisco FireSIGHT Management Center イベントを自動的に検出しないため、ログ・ソースを構成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで、「**Cisco FireSIGHT Management Center**」を選択します。
7. 「プロトコル構成」リストで「**Cisco Firepower eStreamer**」を選択します。
8. 以下のパラメーターを構成します。

パラメーター	説明
サーバー・アドレス	FireSIGHT Management Center デバイスの IP アドレスまたはホスト名。
サーバー・ポート	QRadar が FireSIGHT Management Center eStreamer イベントの受信に使用するポート番号。
鍵ストア・ファイル名	鍵ストアの秘密鍵と関連証明書のディレクトリー・パスおよびファイル名。
トラストストア・ファイル名	トラストストア・ファイルのディレクトリー・パスおよびファイル名。クライアントから信頼されている証明書を含むトラストストア・ファイルです。
追加データの要求 **(Request Extra Data)**	FireSIGHT Management Center eStreamer からの追加データを要求するには、このオプションを選択します。例えば、追加データには、イベントの元の IP アドレスなどがあります。
拡張要求の使用 **(Use Extended Requests)**	eStreamer ソースからイベントを取得する代替メソッドを使用するには、このオプションを選択します。 拡張要求は、FireSIGHT Management Center eStreamer バージョン 5.0 以降でサポートされます。

Cisco FWSM

Cisco Firewall Service Module (FWSM) を IBM Security QRadar と統合できます。

QRadar 用の Cisco FWSM DSM は、syslog を使用して FWSM イベントを受け入れます。QRadar は、関連するすべての Cisco FWSM イベントを記録します。

syslog イベントを転送するための Cisco FWSM の構成

Cisco FWSM を IBM Security QRadar と統合するには、syslog イベントを QRadar に転送するように Cisco FWSM アプライアンスを構成する必要があります。

このタスクについて

Cisco FWSM を構成するには、以下のようにします。

手順

1. コンソール接続、telnet、または SSH を使用して、Cisco FWSM にログインします。
2. 以下のように、ロギングを有効にします。

   ```
   logging on
   ```
3. 以下のように、ロギング・レベルを変更します。

   ```
   logging trap <level>
   ```

   ここで、*<level>* は、レベル 1 から 7 の範囲で設定します。デフォルトでは、ロギング・トラップ・レベルは、3 (エラー) に設定されます。
4. 以下のように、メッセージを受信するホストとして QRadar を指定します。

   ```
   logging host [interface] ip_address [tcp[/port] | udp[/port]] [format emblem]
   ```

   例:

   ```
   logging host dmz1 192.168.1.5
   ```

   ここで、192.168.1.5 は、QRadar システムの IP アドレスです。

   これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Cisco FWSM アプライアンスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。 Cisco FWSM の syslog ログ・ソースを手動で構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

「ログ・ソース」ウィンドウが表示されます。

5. 「追加」をクリックします。

「ログ・ソースの追加」ウィンドウが表示されます。

6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco** ファイアウォール・サービス・モジュール **(FWSM)**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

syslog プロトコル構成が表示されます。

10. 以下の値を構成します。

表 110. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco FWSM アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Cisco IDS/IPS

IBM Security QRadar 用の Cisco IDS/IPS DSM は、Security Device Event Exchange (SDEE) プロトコルを使用して、イベントについて Cisco IDS/IPS にポーリングします。

このタスクについて

SDEE 仕様は、Cisco IDS/IPS セキュリティー・デバイスによって生成されたイベントとの通信に使用するメッセージ・フォーマットおよびプロトコルを規定しています。QRadar では、デバイスを制御する管理ソフトウェアではなく、IDS/IPS デバイスに直接ポーリングすることによって SDEE 接続をサポートしています。

注**:** QRadar に接続する前に、デバイスに対するセキュリティー・アクセス権限または Web 認証を備えておく必要があります。

Cisco IDS/IPS デバイスを構成した後に、QRadar で SDEE プロトコルを構成する必要があります。SDEE プロトコルの構成時に、デバイスへのアクセスに必要な URL を定義する必要があります。

例: `https://www.mysdeeserver.com/cgi-bin/sdee-server`

URL では、http または https を使用する必要があります。この URL は、以下のように、ご使用の Cisco IDS バージョンに固有のものです。

- RDEP (Cisco IDS v4.0 の場合) を使用している場合、`/cgi-bin/event-server` が URL の末尾にあることを確認してください。

例: https://www.my-rdep-server.com/cgi-bin/event-server

- SDEE/CIDEE (Cisco IDS v5.x 以降の場合) を使用している場合、/cgi-bin/sdee-server が URL の末尾にあることを確認してください。

  例: https://www.my-sdee-server/cgi-bin/sdee-server

QRadar が Cisco IDS/IPS デバイスからの syslog イベントに対して、ログソースを自動的に検出および作成することはありません。Cisco IDS/IPS デバイスのイベントを QRadar と統合するには、ネットワーク内の各 Cisco IDS/IPS のログ・ソースを手動で作成する必要があります。

SDEE ポーリングを使用して Cisco IDS/IPS ログ・ソースを構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco** 侵入防御システム **(IPS)**」を選択します。
9. 「プロトコル構成」リストで「**SDEE**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *111. SDEE* のパラメーター

パラメーター	説明
ログ・ソース **ID**	SDEE イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。IP アドレスまたはホスト名により、QRadar はログ・ファイルを固有のイベント・ソースに識別できるようになります。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。

表 111. SDEE のパラメーター (続き)

パラメーター	説明
URL	ログ・ソースにアクセスするための URL アドレスを入力します (例えば、https://www.mysdeeserver.com/cgi-bin/sdee-server)。URL では、http または https を使用する必要があります。 以下に、いくつかのオプションを示します。 • SDEE/CIDEE (Cisco IDS v5.x 以降の場合) を使用している場合、/cgi-bin/sdee-server が URL の末尾にあることを確認してください。例: https://www.my-sdee-server/cgi-bin/sdee-server • RDEP (Cisco IDS v4.0 の場合) を使用している場合、/cgi-bin/event-server が URL の末尾にあることを確認してください。例: https://www.my-rdep-server.com/cgi-bin/event-server
ユーザー名	ユーザー名を入力します。このユーザー名は、SDEE URL へのアクセスに使用する SDEE URL ユーザー名に一致する必要があります。ユーザー名の長さは最大で 255 文字までです。
パスワード	ユーザー・パスワードを入力します。このパスワードは、SDEE URL へのアクセスに使用する SDEE URL パスワードに一致する必要があります。パスワードの最大長は 255 文字です。
イベント/照会 **(Events / Query)**	照会ごとに取得する最大イベント数を入力します。有効な範囲は 0 から 501 であり、デフォルトは 100 です。
サブスクリプションの強制	新規 SDEE サブスクリプションを強制する場合は、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。 このチェック・ボックスを選択すると、強制的に、サーバーは最もアクティブでない接続をドロップし、新規 SDEE サブスクリプション接続をこのログ・ソース用に受け入れるようになります。 チェック・ボックスをクリアすると、既存の SDEE サブスクリプションを継続します。
重大度フィルター **(低) (Severity Filter Low)**	重大度レベルを低として構成する場合は、このチェック・ボックスを選択します。 SDEE をサポートするログ・ソースでは、この重大度レベルに一致するイベントのみが返されます。このチェック・ボックスはデフォルトで選択されます。

表 111. SDEE のパラメーター (続き)

パラメーター	説明
重大度フィルター (中) **(Severity Filter Medium)**	重大度レベルを中として構成する場合は、このチェック・ボックスを選択します。 SDEE をサポートするログ・ソースでは、この重大度レベルに一致するイベントのみが返されます。このチェック・ボックスはデフォルトで選択されます。
重大度フィルター (高) **(Severity Filter High)**	重大度レベルを高として構成する場合は、このチェック・ボックスを選択します。 SDEE をサポートするログ・ソースでは、この重大度レベルに一致するイベントのみが返されます。このチェック・ボックスはデフォルトで選択されます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。 Cisco IDS/IPS アプライアンスからポーリングで取得したイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

Cisco IronPort

IBM Security QRadar 用の Cisco IronPort DSM は、E メール・スパム、Web コンテンツのフィルタリング、および企業 E メール・ポリシーの適用に関するイベント情報を提供します。

Cisco IronPort デバイスと統合するように QRadar を構成する前に、ログ・タイプを選択して構成する必要があります。

- IronPort メール・ログを構成するには、『IronPort メール・ログの構成』を参照してください。
- IronPort コンテンツ・フィルタリング・ログを構成するには、 284 ページの『IronPort Web コンテンツ・フィルター』を参照してください。

IronPort メール・ログの構成

IBM Security QRadar Cisco IronPort DSM は、syslog を使用してイベントを受け入れます。

このタスクについて

syslog イベントを QRadar に送信するように IronPort デバイスを構成するには、以下の手順を実行します。

手順

1. Cisco IronPort ユーザー・インターフェースにログインします。

2. 「システム管理 **(System Administration)**」**-**「ログ・サブスクリプション **(Log Subscriptions)**」を選択します。
3. 「ログ・サブスクリプションの追加 **(Add Log Subscription)**」をクリックします。
4. 以下の値を構成します。
   - ログ・タイプ **(Log Type)** - Ironport Text Mail Logs と System Logs の両方のログ・サブスクリプションを定義します。
   - ログ名 **(Log Name)** - ログ名を入力します。
   - ファイル名 **(File Name)** - デフォルト構成値を使用します。
   - 最大ファイル・サイズ **(Maximum File Size)** - デフォルト構成値を使用します。
   - ログ・レベル **(Log Level)** - 「情報 **(Information)**」(デフォルト) を選択します。
   - 取得方式 **(Retrieval Method)** - 「**Syslog** プッシュ **(Syslog Push)**」を選択します。
   - ホスト名 **(Hostname)** - QRadar システムの IP アドレスまたはサーバー名を入力します。
   - プロトコル **(Protocol)** - 「**UDP**」を選択します。
   - ファシリティー **(Facility)** - デフォルト構成値を使用します。この値は、構成されている「ログ・タイプ (Log Type)」によって異なります。
5. サブスクリプションを保存します。

これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

Cisco IronPort を IBM Security QRadar と統合するには、Cisco IronPort イベントを受信するためのログ・ソースを手動で作成する必要があります。QRadar が Cisco IronPort アプライアンスからの syslog イベントに対して、ログ・ソースを自動的に検出および作成することはありません。

このタスクについて

Cisco IronPort イベントのログ・ソースを作成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

「ログ・ソースの追加」ウィンドウが表示されます。

6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco IronPort**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *112. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco IronPort アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    ログ・ソースが QRadar に追加されます。 Cisco IronPort によって QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

IronPort Web コンテンツ・フィルター

IBM Security QRadar 用の Cisco IronPort DSM は、ログ・ファイル・プロトコルを使用して、リモート・ソースから W3C フォーマットで Web コンテンツ・フィルタリング・イベントを取得します。

このタスクについて

Cisco IronPort デバイスと統合するには、システムで現行バージョンのログ・ファイル・プロトコルを実行している必要があります。Web コンテンツ・フィルター・イベントをプッシュするように Cisco IronPort デバイスを構成するには、W3C フォーマットを使用している Web コンテンツ・フィルターのログ・サブスクリプションを構成する必要があります。ログ・サブスクリプションの構成について詳しくは、ご使用の *Cisco IronPort* の資料 を参照してください。

これで、QRadar でログ・ソースおよびプロトコルを構成する準備ができました。

手順

1. 「ログ・ソース・タイプ」ドロップダウン・リスト・ボックスで、「**Cisco IronPort**」を選択します。
2. 「プロトコル構成」リストで「ログ・ファイル」プロトコル・オプションを選択します。
3. Web コンテンツ・フィルター・ログ・ファイルの処理に使用する「イベント・ジェネレーター **(Event Generator)**」として「**W3C**」を選択します。
4. 「**FTP** ファイル・パターン」パラメーターでは、Web コンテンツ・フィルター・ログによって生成されるログ・ファイルに一致する正規表現を使用する必要があります。

関連概念:

22 ページの『ログ・ファイル・プロトコルの構成オプション』
リモート・ホストからイベントを受信するには、ログ・ファイル・プロトコルを使用するようにログ・ソースを構成します。

Cisco IOS

Cisco IOS シリーズ・デバイスを IBM Security QRadar と統合できます。

QRadar 用の Cisco IOS DSM は、syslog を使用して Cisco IOS イベントを受け入れます。QRadar は、関連するすべてのイベントを記録します。以下の Cisco スイッチおよびルーターは、Cisco IOS シリーズ・デバイスとして自動的に検出され、それらのイベントは、Cisco IOS DSM によって解析されます。

- Cisco 12000 シリーズ・ルーター
- Cisco 6500 シリーズ・スイッチ
- Cisco 7600 シリーズ・ルーター
- Cisco Carrier Routing System
- Cisco サービス統合型ルーター

注: すべてのアクセス制御リスト (ACL) を LOG に設定してください。

イベントを転送するための Cisco IOS の構成

イベントを転送するように Cisco IOS ベースのデバイスを構成できます。

このタスクについて

以下の手順を実行して、Cisco デバイスを構成します。

手順

1. Cisco IOS Server、スイッチ、またはルーターにログインします。
2. 以下のコマンドを入力して、privileged-exec でルーターにログインします。

   ```
   enable
   ```
3. 以下のコマンドを入力して、構成モードに切り替えます。

   ```
   conf t
   ```
4. 以下のコマンドを入力します。

   ```
   logging <IP address>
   ```

   ```
   logging source-interface <interface>
   ```

   各部分について以下で説明します。
   - *<IP address>* は、IBM Security QRadar ホストおよび SIM コンポーネントの IP アドレスです。
   - *<interface>* は、インターフェースの名前です (例えば、dmz、lan、ethernet0、ethernet1)。
5. 以下を入力して、優先順位レベルを構成します。

```
logging trap warning
```

```
logging console warning
```

ここで、*warning* は、ログの優先順位設定です。

6. syslog ファシリティーを構成します。

```
logging facility syslog
```

7. ファイルを保存して終了します。
8. 以下のコマンドを入力して、`running-config` を `startup-config` にコピーします。

```
copy running-config startup-config
```

これで、QRadar でログ・ソースを構成する準備ができました。

構成は完了です。Cisco IOS イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Cisco IOS ベースのデバイスによって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Cisco IOS からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。 Cisco IOS ベースのデバイスのログ・ソースを手動で構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

「データ・ソース」ペインが表示されます。

4. 「ログ・ソース」アイコンをクリックします。

「ログ・ソース」ウィンドウが表示されます。

5. 「追加」をクリックします。

「ログ・ソースの追加」ウィンドウが表示されます。

6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、以下のいずれかのデバイスを選択します。
   - Cisco IOS
   - Cisco 12000 シリーズ・ルーター

- Cisco 6500 シリーズ・スイッチ
- Cisco 7600 シリーズ・ルーター
- Cisco Carrier Routing System
- Cisco サービス統合型ルーター

9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。

10. 以下の値を構成します。

表 113. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco IOS ベースのデバイスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Cisco Identity Services Engine

IBM Security QRadar 用の Cisco Identity Services Engine (ISE) DSM は、UDP Multiline プロトコルを使用するように構成されたログ・ソースを使用して Cisco ISE アプライアンスからの syslog イベントを受け入れます。

QRadar は、Cisco ISE バージョン 1.1 から転送される syslog イベントをサポートします。Cisco ISE アプライアンスを構成する前に、QRadar に転送するように Cisco ISE で構成するロギング・カテゴリーを検討します。各ロギング・カテゴリーは syslog 重大度が構成されていて、Cisco ISE から QRadar へのイベント転送を許可するリモート・ターゲットとして含める必要があります。

QRadar で構成するログ・ソースは、Cisco ISE から転送されるイベントを受信し、正規表現を使用して Multiline Syslog イベントを QRadar が読み取り可能なイベントにアセンブルします。

Cisco ISE イベントを QRadar と統合するには、以下のタスクを実行します。

1. Cisco ISE アプライアンスがイベントを QRadar に転送するために、ログ・ソースを QRadar で構成します。
2. Cisco ISE アプライアンスで、QRadar のリモート・ロギング・ターゲットを作成します。
3. Cisco ISE アプライアンスで、ロギング・カテゴリーを構成します。

サポートされるイベント・ロギング・カテゴリー

IBM Security QRadar 用の Cisco ISE DSM は、さまざまなイベント・ロギング・カテゴリーの syslog イベントを受信できます。

以下の表に、Cisco ISE DSM のサポートされるイベント・ロギング・カテゴリーを示します。

表 *114. Cisco ISE* イベント・ロギング・カテゴリー

イベント・ロギング・カテゴリー
AAA 監査 (AAA audit)
失敗した試行 (Failed attempts)
成功した認証 (Passed authentication)
AAA 診断 (AAA diagnostics)
管理者の認証と許可 (Administrator authentication and authorization)
認証フロー診断 (Authentication flow diagnostics)
ID ストア診断 (Identity store diagnostics)
ポリシー診断 (Policy diagnostics)
Radius 診断 (Radius diagnostics)
ゲスト (Guest)
アカウンティング (Accounting)
Radius アカウンティング (Radius accounting)
管理および操作の監査 (Administrative and operational audit)
ポスチャおよびクライアント プロビジョニングの監査 (Posture and client provisioning audit)
ポスチャおよびクライアント プロビジョニングの診断 (Posture and client provisioning diagnostics)
プロファイラ (Profiler)
システム診断 (System diagnostics)
分散管理 (Distributed management)
内部操作診断 (Internal operations diagnostics)
システム統計 (System statistics)

IBM Security QRadar での Cisco ISE ログ・ソースの構成

syslog イベントを収集するには、UDP Multiline Syslog プロトコルを使用するように QRadar で Cisco ISE のログ・ソースを構成する必要があります。

このタスクについて

イベントを QRadar に転送する個別 Cisco ISE アプライアンスごとに、ログ・ソースを構成します。ただし、すべての Cisco ISE アプライアンスが、構成した QRadar 上の同じ listen ポートにイベントを転送できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。

8. 「ログ・ソース・タイプ」リストで、「**Cisco Identity Services Engine**」を選択します。
9. 「プロトコル構成」リストで「**UDP** 多重回線 **Syslog (UDP Multiline Syslog)**」を選択します。
10. 以下の値を構成します。

表 115. Cisco ISE ログ・ソースのパラメーター

パラメーター	説明
ログ・ソース **ID**	UDP Multiline Syslog イベントを QRadar に提供するログ・ソースまたはアプライアンスを識別するための IP アドレスを入力します。
Listen ポート	着信 UDP 多重回線 Syslog イベントを受け取るために QRadar が使用するポート番号として 517 と入力します。有効なポート範囲は、1 から 65535 です。 **注:** UDP Multiline Syslog イベントは、ポート 514 以外の任意の未使用ポートに割り当てることができます。UDP Multiline プロトコルに割り当てられているデフォルト・ポートは、UDP ポート 517 です。ネットワークでポート 517 が使用されている場合は、QRadar によって使用されているポートのリストを「IBM Security QRadar Common Ports Technical Note」(http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/CommonPorts.pdf) で参照してください。 保存済みの構成を編集して新しいポート番号を使用するには、以下のようにします。 「**listen** ポート **(Listen Port)**」フィールドに、UDP 多重回線 Syslog イベント受信用の新しいポート番号を入力します。 1. 「保存」をクリックします。 2. 「管理」タブで、「拡張」 > 「すべての構成のデプロイ」を選択します。 全デプロイメントが完了すると、QRadar は、更新された listen ポートでイベントを受信できるようになります。 「すべての構成のデプロイ」をクリックすると、QRadar はすべてのサービスを再開します。このため、デプロイが完了するまで、イベントとフローのデータ収集にギャップが生じます。
メッセージ **ID** のパターン	イベント・ペイロード・メッセージをフィルタリングするために必要な以下の正規表現 (regex) を入力します。 `CISE_¥S+ (¥d{10})`

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

これで、リモート・ロギング・ターゲットを使用して Cisco ISE アプライアンスを構成する準備ができました。

Cisco ISE でのリモート・ロギング・ターゲットの作成

syslog イベントを IBM Security QRadar に転送するには、リモート・ロギング・ターゲットを使用して Cisco ISE アプライアンスを構成する必要があります。

手順

1. Cisco ISE 管理インターフェースにログインします。
2. ナビゲーション・メニューで「管理 **(Administration)**」 > 「システム **(System)**」 > 「ロギング **(Logging)**」 > 「リモート・ロギング・ターゲット **(Remote Logging Targets)**」を選択します。
3. 「追加」をクリックします。
4. 「名前 **(Name)**」フィールドに、リモート・ターゲット・システムの名前を入力します。
5. 「説明 **(Description)**」フィールドに説明を入力します。
6. 「**IP** アドレス **(IP Address)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
7. 「ポート **(Port)**」フィールドで、517 と入力するか、QRadar の Cisco ISE ログ・ソースで指定したポート値を使用します。
8. 「ファシリティー・コード **(Facility Code)**」リストで、イベントのロギングで使用する syslog ファシリティーを選択します。
9. 「最大長 **(Maximum Length)**」フィールドに、UDP syslog メッセージに許可される最大パケット長として 1024 と入力します。
10. 「送信 **(Submit)**」をクリックします。

    リモート・ロギング・ターゲットが QRadar 用に作成されました。

次のタスク

これで、Cisco ISE によって QRadar に転送されるロギング・カテゴリーを構成する準備ができました。

Cisco ISE ロギング・カテゴリーの構成

Cisco ISE アプライアンスによってどのイベントが転送されるかを定義するには、各ロギング・カテゴリーを構成する必要があります。

このタスクについて

Cisco ISE の事前定義イベント・ロギング・カテゴリーのリストについては、 287 ページの『サポートされるイベント・ロギング・カテゴリー』を参照してください。

syslog 重大度とリモート・ロギング・ターゲットを使用して、各ロギング・カテゴリーを構成します。以下の手順を実行して、イベント・ロギング・カテゴリーを構成します。

手順

1. ナビゲーション・メニューで「管理 **(Administration)**」 > 「システム **(System)**」 > 「ロギング **(Logging)**」 > 「ロギング・カテゴリー **(Logging Categories)**」を選択します。
2. ロギング・カテゴリーを選択し、「編集 **(Edit)**」をクリックします。
3. 「ログ重大度 **(Log Severity)**」リストから、ロギング・カテゴリーの重大度を選択します。
4. 「ターゲット **(Target)**」フィールドで、IBM Security QRadar のリモート・ロギング・ターゲットを「選択 **(Select)**」ボックスに追加します。
5. 「保存」をクリックします。
6. QRadar に転送するロギング・カテゴリーごとに、このプロセスを繰り返します。

構成は完了です。Cisco ISE によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

Cisco NAC

IBM Security QRadar 用の Cisco NAC DSM は、syslog を使用してイベントを受け入れます。

QRadar は、関連するすべてのイベント (監査、エラー、失敗、検疫、および感染システムの各イベント) を記録します。Cisco NAC デバイスを QRadar で構成する前に、syslog イベントを転送するようにデバイスを構成しておく必要があります。

イベントを転送するための Cisco NAC の構成

syslog イベントを転送するように Cisco NAC を構成することができます。

手順

1. Cisco NAC ユーザー・インターフェースにログインします。
2. 「モニタリング (Monitoring)」セクションで「イベント・ログ **(Event Logs)**」を選択します。
3. 「**Syslog** 設定 **(Syslog Settings)**」タブをクリックします。
4. 「**Syslog** サーバー・アドレス **(Syslog Server Address)**」フィールドに、IBM Security QRadar の IP アドレスを入力します。
5. 「**Syslog** サーバー・ポート **(Syslog Server Port)**」フィールドに、syslog ポート番号を入力します。デフォルトは 514 です。
6. 「システム・ヘルス・ログの間隔 **(System Health Log Interval)**」フィールドに、システム統計ログ・イベントの頻度を分単位で入力します。
7. 「更新 **(Update)**」をクリックします。

これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

Cisco NAC イベントを IBM Security QRadar と統合するには、Cisco NAC イベントを受信するためのログ・ソースを手動で作成する必要があります。

このタスクについて

QRadar が Cisco NAC アプライアンスからの syslog イベントに対して、ログソースを自動的に検出および作成することはありません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco NAC** アプライアンス」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 116. syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco NAC アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。 Cisco NAC により QRadar に転送されるイベントは、「ログ・アクティビティー」タブに表示されます。

Cisco Nexus

IBM Security QRadar 用の Cisco Nexus DSM は、Cisco NX-OS デバイスからのアラートをサポートします。

syslog は、イベントを Cisco Nexus から QRadar に転送するために使用されます。イベントを QRadar と統合するには、syslog イベントを転送するように Cisco Nexus デバイスを構成する必要があります。

イベントを転送するための Cisco Nexus の構成

Cisco Nexus サーバーで syslog を構成してイベントを転送することができます。

手順

1. 以下のコマンドを入力して、構成モードに切り替えます。

   ```
   config t
   ```

2. 以下のコマンドを入力します。

   ```
   logging server <IP address> <severity>
   ```

   各部分について以下で説明します。

   - *<IP address>* は、QRadar コンソールの IP アドレスです。
   - *<severity>* は、イベント・メッセージの重大度レベルです。値の範囲は 0 から 7 です。

   例えば、`logging server 100.100.10.1 6` の場合、情報レベル (6) の syslog メッセージが 100.100.10.1 に転送されます。

3. 以下のコマンドを入力して、syslog イベントを送信するためにインターフェースを構成します。

   ```
   logging source-interface loopback
   ```

4. 以下のコマンドを入力して、現在の構成を始動構成として保存します。

   ```
   copy running-config startup-config
   ```

   構成は完了です。Cisco Nexus イベントが自動的に検出されると、ログ・ソースが IBM Security QRadar に追加されます。Cisco Nexus によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Cisco Nexus の syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。 Cisco Nexus のログ・ソースを手動で構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。

4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。

5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。

6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco Nexus**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *117. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco Nexus アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。Cisco Nexus デバイスでの Virtual Device Context (VDC) の構成について詳しくは、ベンダーの資料を参照してください。

Cisco Pix

Cisco Pix セキュリティー・アプライアンスを IBM Security QRadar と統合できます。

QRadar 用の Cisco Pix DSM は、syslog を使用して Cisco Pix イベントを受け入れます。QRadar は、関連するすべての Cisco Pix イベントを記録します。

イベントを転送するための Cisco Pix の構成

イベントを転送するように Cisco Pix を構成することができます。

手順

1. コンソール接続、telnet、または SSH を使用して、Cisco PIX アプライアンスにログインします。
2. 以下のコマンドを入力して、特権モードにアクセスします。

   ```
   enable
   ```
3. 以下のコマンドを入力して、構成モードにアクセスします。

   ```
   conf t
   ```
4. 以下のように、ロギングを有効にし、ログにタイム・スタンプを付けます。

   ```
   logging on

   logging timestamp
   ```
5. 以下のように、ログ・レベルを設定します。

   ```
   logging trap warning
   ```
6. 以下のように、IBM Security QRadar へのロギングを構成します。

```
logging host <interface> <IP address>
```

各部分について以下で説明します。

- *<interface>* は、インターフェースの名前です (例えば、DMZ、LAN、ethernet0、ethernet1)。
- *<IP address>* は、QRadar ホストの IP アドレスです。

構成は完了です。Cisco Pix ファイアウォール・イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Cisco Pix ファイアウォールによって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Cisco PIX ファイアウォールの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

Cisco Pix のログ・ソースを手動で構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco PIX** ファイアウォール」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 118. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco Pix ファイアウォールからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Cisco VPN 3000 Concentrator

IBM Security QRadar 用の Cisco VPN 3000 Concentrator DSM は、syslog を使用して、Cisco VPN Concentrator イベントを受け入れます。

このタスクについて

QRadar は、関連するすべてのイベントを記録します。Cisco VPN Concentrator と統合する前に、syslog イベントを QRadar に転送するようにデバイスを構成しておく必要があります。

Cisco VPN 3000 Concentrator を構成するには、以下のようにします。

手順

1. Cisco VPN 3000 Concentrator のコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力して、syslog サーバーを構成に追加します。

   ```
   set logging server <IP address>
   ```

   ここで、*<IP address>* は、QRadar またはイベント・コレクターの IP アドレスです。
3. 以下のコマンドを入力して、構成した syslog サーバーへのシステム・メッセージのログの記録を有効にします。

   ```
   set logging server enable
   ```
4. 以下のように、syslog サーバー・メッセージのファシリティーおよび重大度レベルを設定します。
   - ```
     set logging server facility <server_facility_parameter>
     ```
   - ```
     set logging server severity <server_severity_level>
     ```

   構成は完了です。Cisco VPN Concentrator イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Cisco VPN 3000 シリーズ Concentrator からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

ログ・ソースを手動で構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco VPN 3000** シリーズ **Concentrator (Cisco VPN 3000 Series Concentrator)**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 119. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco VPN 3000 シリーズ Concentrator からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Cisco Wireless Services Module

Cisco Wireless Services Module (WiSM) デバイスを IBM Security QRadar と統合できます。

QRadar 用の Cisco WiSM DSM は、syslog を使用してイベントを受け入れます。QRadar を Cisco WiSM デバイスと統合する前に、syslog イベントを転送するように Cisco WiSM を構成する必要があります。

イベントを転送するための Cisco WiSM の構成

syslog イベントを IBM Security QRadar に転送するように Cisco WiSM を構成できます。

このタスクについて

以下の手順を実行して、syslog イベントを転送するように Cisco WiSM を構成します。

手順

1. Cisco Wireless LAN Controller ユーザー・インターフェースにログインします。
2. 「管理 **(Management)**」 > 「ログ **(Logs)**」 > 「構成 **(Config)**」をクリックします。

   「Syslog 構成 (Syslog Configuration)」ウィンドウが表示されます。
3. 「**Syslog** サーバー **IP** アドレス **(Syslog Server IP Address)**」フィールドに、syslog メッセージを受信する QRadar ホストの IP アドレスを入力します。
4. 「追加」をクリックします。
5. 「**Syslog** レベル **(Syslog Level)**」リストを使用して、以下のいずれかの重大度レベルを使用して、syslog サーバーへの syslog メッセージをフィルタリングするための重大度レベルを設定します。
   - 緊急 **(Emergencies)** - 重大度レベル 0
   - アラート **(Alerts)** - 重大度レベル 1 (デフォルト)
   - 重大 **(Critical)** - 重大度レベル 2
   - エラー **(Errors)** - 重大度レベル 3
   - 警告 **(Warnings)** - 重大度レベル 4
   - 通知 **(Notifications)** - 重大度レベル 5
   - 情報 **(Informational)** - 重大度レベル 6
   - デバッグ **(Debugging)** - 重大度レベル 7

   syslog レベルを設定した場合、選択した syslog レベル以下の重大度レベルのメッセージのみが syslog サーバーに送信されます。例えば、syslog レベルを「警告 **(Warnings)**」(重大度レベル 4) に設定した場合、重大度が 0 から 4 のメッセージのみが syslog サーバーに送信されます。
6. 「**Syslog** ファシリティー **(Syslog Facility)**」リストから、以下のいずれかのファシリティー・レベルを使用して、syslog サーバーへの送信 syslog メッセージのファシリティーを設定します。
   - カーネル **(Kernel)** - ファシリティー・レベル 0
   - ユーザー・プロセス **(User Process)** - ファシリティー・レベル 1
   - メール **(Mail)** - ファシリティー・レベル 2
   - システム・デーモン **(System Daemons)** - ファシリティー・レベル 3
   - 許可 **(Authorization)** - ファシリティー・レベル 4
   - **Syslog** - ファシリティー・レベル 5 (デフォルト値)

- ライン・プリンター **(Line Printer)** - ファシリティー・レベル 6
- **USENET** - ファシリティー・レベル 7
- **UNIX** 間のコピー **(Unix-to-Unix Copy)** - ファシリティー・レベル 8
- クーロン **(Cron)** - ファシリティー・レベル 9
- **FTP** デーモン **(FTP Daemon)** - ファシリティー・レベル 11
- システム使用 **1 (System Use 1)** - ファシリティー・レベル 12
- システム使用 **2 (System Use 2)** - ファシリティー・レベル 13
- システム使用 **3 (System Use 3)** - ファシリティー・レベル 14
- システム使用 **4 (System Use 4)** - ファシリティー・レベル 15
- ローカル使用 **0 (Local Use 0)** - ファシリティー・レベル 16
- ローカル使用 **1 (Local Use 1)** - ファシリティー・レベル 17
- ローカル使用 **2 (Local Use 2)** - ファシリティー・レベル 18
- ローカル使用 **3 (Local Use 3)** - ファシリティー・レベル 19
- ローカル使用 **4 (Local Use 4)** - ファシリティー・レベル 20
- ローカル使用 **5 (Local Use 5)** - ファシリティー・レベル 21
- ローカル使用 **6 (Local Use 6)** - ファシリティー・レベル 22
- ローカル使用 **7 (Local Use 7)** - ファシリティー・レベル 23

7. 「適用」をクリックします。
8. 「バッファーに入れられたログ・レベル **(Buffered Log Level)**」リストおよび「コンソール・ログ・レベル **(Console Log Level)**」リストから、以下のいずれかの重大度レベルを使用して、コントローラー・バッファーおよびコンソールに送信されるログ・メッセージの重大度レベルを選択します。
   - 緊急 **(Emergencies)** - 重大度レベル 0
   - アラート **(Alerts)** - 重大度レベル 1
   - 重大 **(Critical)** - 重大度レベル 2
   - エラー **(Errors)** - 重大度レベル 3 (デフォルト値)
   - 警告 **(Warnings)** - 重大度レベル 4
   - 通知 **(Notifications)** - 重大度レベル 5
   - 情報 **(Informational)** - 重大度レベル 6
   - デバッグ **(Debugging)** - 重大度レベル 7

   ロギング・レベルを設定した場合、重大度がそのレベル以下のメッセージのログのみがコントローラーによってログに記録されます。例えば、ロギング・レベルを「警告 **(Warnings)**」(重大度レベル 4) に設定した場合、重大度が 0 から 4 のメッセージのログのみがログに記録されます。
9. ソース・ファイルに関する情報をメッセージ・ログに含める場合、「ファイル情報 **(File Info)**」チェック・ボックスを選択します。デフォルト値では、有効になっています。
10. プロセス情報をメッセージ・ログに含める場合、「プロセス情報 **(Proc Info)**」チェック・ボックスを選択します。デフォルト値では、無効になっています。

11. トレースバック情報をメッセージ・ログに含める場合、「トレース情報 **(Trace Info)**」チェック・ボックスを選択します。デフォルト値では、無効になっています。
12. 「適用 **(Apply)**」をクリックして変更をコミットします。
13. 「構成の保存 **(Save Configuration)**」をクリックして変更を保存します。

構成は完了です。Cisco WiSM イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Cisco WiSM によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Cisco WiSM からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

Cisco WiSM のログ・ソースを手動で構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

「データ・ソース」ペインが表示されます。

4. 「ログ・ソース」アイコンをクリックします。

「ログ・ソース」ウィンドウが表示されます。

5. 「追加」をクリックします。

「ログ・ソースの追加」ウィンドウが表示されます。

6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco Wireless Services Module (WiSM)**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

syslog プロトコル構成が表示されます。

10. 以下の値を構成します。

表 120. syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco WiSM アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Cisco ワイヤレス LAN コントローラー

IBM Security QRadar 用の Cisco ワイヤレス LAN コントローラー DSM は、syslog または SNMPv2 を使用して Cisco ワイヤレス LAN コントローラー・デバイスから転送されたイベントを収集します。

このセクションには、以下のトピックが含まれます。

- 『Cisco Wireless LAN Controller 用の syslog の構成』
- 303 ページの『Cisco Wireless LAN Controller 用の SNMPv2 の構成』

始める前に

Cisco ワイヤレス LAN コントローラーからイベントを収集する場合、ご使用の構成に最もふさわしい収集方法を選択してください。QRadar 用の Cisco ワイヤレス LAN コントローラー DSM は、syslog イベントおよび SNMPv2 イベントのどちらもサポートします。ただし、syslog は使用可能な Cisco ワイヤレス LAN コントローラー・イベントをすべて提供するのに対し、SNMPv2 は限られたセキュリティー・イベントのセットのみを QRadar に送信します。

Cisco Wireless LAN Controller 用の syslog の構成

syslog イベントを IBM Security QRadar に転送するように Cisco Wireless LAN Controller を構成できます。

手順

1. Cisco Wireless LAN Controller インターフェースにログインします。
2. 「管理 **(Management)**」タブをクリックします。
3. メニューで「ログ **(Logs)**」 > 「構成 **(Config)**」を選択します。
4. 「**Syslog** サーバー **IP** アドレス **(Syslog Server IP Address)**」フィールドに、QRadar コンソールの IP アドレスを入力します。
5. 「追加」をクリックします。
6. 「**Syslog** レベル **(Syslog Level)**」リストから、ロギング・レベルを選択します。

   「情報 **(Information)**」ロギング・レベルを選択すると、「デバッグ **(Debug)**」ロギング・レベルより上のすべての Cisco Wireless LAN Controller イベントを収集できます。
7. 「**Syslog** ファシリティー **(Syslog Facility)**」リストから、ファシリティー・レベルを選択します。
8. 「適用」をクリックします。
9. 「構成の保存 **(Save Configuration)**」をクリックします。

次のタスク

これで、Cisco Wireless LAN Controller の syslog ログ・ソースを構成する準備ができました。

IBM Security QRadar での syslog ログ・ソースの構成

QRadar が Cisco Wireless LAN Controller からの受信 syslog イベントを自動的に検出することはありません。syslog イベントを QRadar に提供する Cisco Wireless LAN Controller ごとにログ・ソースを作成する必要があります。

このタスクについて

QRadar でログ・ソースを構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco Wireless LAN Controller**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 121. syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco Wireless LAN Controller からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。
有効	ログ・ソースを有効にするには、「有効」チェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
信頼性	リストから、ログ・ソースの信頼性を選択します。範囲は 0 から 10 です。送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 自動的に検出されたログ・ソースは、QRadar の「設定」ウィンドウの「管理」タブにある「イベントの統合」ドロップダウン・リストで構成されたデフォルト値を使用します。ただし、新規ログ・ソースを作成するか、自動的に検出されたログ・ソースの構成を更新する際に、各ログ・ソースに対してこのチェック・ボックスを構成することで、デフォルト値をオーバーライドできます。設定について詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。

表 121. *syslog* プロトコルのパラメーター (続き)

パラメーター	説明
受信イベント・ペイロード **(Incoming Event Payload)**	リストから、ログの解析と保管を行うための受信ペイロード・エンコーダーを選択します。
イベント・ペイロードの保管	QRadar によるイベント・ペイロードの保管を有効または無効にするには、このチェック・ボックスを選択します。 自動的に検出されたログ・ソースは、QRadar の「設定」ウィンドウの「管理」タブにある「イベント・ペイロードの保管」ドロップダウン・リストのデフォルト値を使用します。ただし、新規ログ・ソースを作成するか、自動的に検出されたログ・ソースの構成を更新する際に、各ログ・ソースに対してこのチェック・ボックスを構成することで、デフォルト値をオーバーライドできます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Cisco Wireless LAN Controller 用の SNMPv2 の構成

Cisco Wireless LAN Controller の SNMP イベント収集により、IBM Security QRadar 用にイベントをキャプチャーできます。

このタスクについて

以下のイベントが収集されます。

- SNMP 構成イベント
- bsn 認証エラー
- LWAPP 鍵復号エラー

手順

1. Cisco Wireless LAN Controller インターフェースにログインします。
2. 「管理 **(Management)**」タブをクリックします。
3. メニューで「**SNMP**」 > 「コミュニティー **(Communities)**」を選択します。

   作成済みのデフォルト・コミュニティーのいずれかを使用するか、新規コミュニティーを作成することができます。
4. 「新規」をクリックします。
5. 「コミュニティー名 **(Community Name)**」フィールドに、ご使用のデバイスのコミュニティーの名前を入力します。
6. 「**IP** アドレス **(IP Address)**」フィールドに、QRadar の IP アドレスを入力します。

   指定する IP アドレスおよび IP マスクは、Cisco Wireless LAN Controller が SNMP 要求を受け入れるアドレスです。これらの値は、SNMP 要求のアクセス・リストとして扱うことができます。

7. 「**IP** マスク **(IP Mask)**」フィールドに、サブネット・マスクを入力します。
8. 「アクセス・モード **(Access Mode)**」リストから、「読み取り専用 **(Read Only)**」または「読み取り/書き込み **(Read/Write)**」を選択します。
9. 「状況 **(Status)**」リストから「有効にする **(Enable)**」を選択します。
10. 「構成の保存 **(Save Configuration)**」をクリックして変更を保存します。

次のタスク

これで、SNMPv2 トラップ・レシーバーを作成する準備ができました。

Cisco Wireless LAN Controller 用のトラップ・レシーバーの構成

Cisco Wireless LAN Controller で構成されたトラップ・レシーバーは、デバイスが SNMP トラップ・メッセージを送信できる場所を定義します。

このタスクについて

Cisco Wireless LAN Controller でトラップ・レシーバーを構成するには、以下の手順を実行します。

手順

1. 「管理 **(Management)**」タブをクリックします。
2. メニューで「**SNMP**」 > 「トラップ・レシーバー **(Trap Receivers)**」を選択します。
3. 「トラップ・レシーバー名 **(Trap Receiver Name)**」フィールドに、トラップ・レシーバーの名前を入力します。
4. 「**IP** アドレス **(IP Address)**」フィールドに、IBM Security QRadar の IPアドレスを入力します。

   指定する IP アドレスは、Cisco Wireless LAN Controller が SNMP メッセージを送信する先のアドレスです。イベント・コレクター (Event Collector)でこのログ・ソースを構成する予定の場合は、イベント・コレクター (Event Collector)・アプライアンスの IP アドレスを指定できます。
5. 「状況 **(Status)**」リストから「有効にする **(Enable)**」を選択します。
6. 「適用 **(Apply)**」をクリックして変更をコミットします。
7. 「構成の保存 **(Save Configuration)**」をクリックして設定を保存します。

次のタスク

これで、QRadar で SNMPv2 ログ・ソースを作成する準備ができました。

SNMPv2 を使用する Cisco Wireless LAN Controller のログ・ソースの構成

IBM Security QRadar が、Cisco Wireless LAN Controller からの SNMP イベント・データのログ・ソースを自動的に検出および作成することはありません。SNMPv2 イベントを提供する Cisco Wireless LAN Controller ごとにログ・ソースを作成する必要があります。

このタスクについて

以下の手順を実行して、Cisco Wireless LAN Controller のログ・ソースを作成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Cisco Wireless LAN Controller**」を選択します。
9. 「プロトコル構成」リストで「**SNMPv2**」を選択します。
10. 以下の値を構成します。

表 122. SNMPv2 プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Cisco Wireless LAN Controller からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。
コミュニティー **(Community)**	SNMP イベントが含まれているシステムにアクセスするために必要な SNMP コミュニティー名を入力します。デフォルトは Public です。
イベント・ペイロードに **OID** を含める **(Include OIDs in Event Payload)**	「イベント・ペイロードに **OID** を含める **(Include OIDs in Event Payload)**」チェック・ボックスを選択します。 このオプションにより、標準イベント・ペイロード・フォーマットではなく、名前と値のペアを使用して SNMP イベント・ペイロードを構成できます。イベント・ペイロード内の OID は、特定の DSM からの SNMPv2 または SNMPv3 イベントを処理するために必要です。
有効	ログ・ソースを有効にするには、「有効」チェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
信頼性	リストから、ログ・ソースの信頼性を選択します。範囲は 0 から 10 です。送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。

表 *122. SNMPv2* プロトコルのパラメーター *(*続き*)*

パラメーター	説明
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 自動的に検出されたログ・ソースは、QRadar の「設定」ウィンドウの「管理」タブにある「イベントの統合」ドロップダウンで構成されたデフォルト値を使用します。ただし、新規ログ・ソースを作成するか、自動的に検出されたログ・ソースの構成を更新する際に、各ログ・ソースに対してこのチェック・ボックスを構成することで、デフォルト値をオーバーライドできます。設定について詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。
イベント・ペイロードの保管	QRadar によるイベント・ペイロードの保管を有効または無効にするには、このチェック・ボックスを選択します。 自動的に検出されたログ・ソースは、QRadar の「設定」ウィンドウの「管理」タブにある「イベント・ペイロードの保管」ドロップダウンのデフォルト値を使用します。ただし、新規ログ・ソースを作成するか、自動的に検出されたログ・ソースの構成を更新する際に、各ログ・ソースに対してこのチェック・ボックスを構成することで、デフォルト値をオーバーライドできます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。Cisco Wireless LAN Controller によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

第 32 章 Citrix

Citrix NetScaler DSM および Citrix Access Gateway DSM。

IBM Security QRadar 用の Citrix NetScaler DSM は、syslog を使用して、関連するすべての監査ログ・イベントを受け入れます。

Citrix Access Gateway DSM は、syslog を使用して Citrix Access Gateway アプライアンスから転送されるアクセス、監査、および診断の各イベントを受け入れます。

Citrix NetScaler

Citrix NetScaler イベントを IBM Security QRadar と統合するには、syslog イベントを転送するように Citrix NetScaler を構成する必要があります。

手順

1. SSH を使用して、root ユーザーとして Citrix NetScaler デバイスにログインします。
2. 以下のコマンドを入力して、リモート syslog サーバーを追加します。

   ```
   add audit syslogAction <ActionName> <IP Address> -serverPort 514
   -logLevel Info -dateFormat DDMMYYYY
   ```

   各部分について以下で説明します。

   <*ActionName*> は、syslog サーバー・アクションの記述名です。

   <*IP Address*> は、QRadar コンソールの IP アドレスまたはホスト名です。

   例:

   ```
   add audit syslogAction action-QRadar 10.10.10.10 -serverPort 514
   -logLevel Info -dateFormat DDMMYYYY
   ```

3. 以下のコマンドを入力して、監査ポリシーを追加します。

   ```
   add audit syslogPolicy <PolicyName> <Rule> <ActionName>
   ```

   各部分について以下で説明します。

   <*PolicyName*> は、syslog ポリシーの記述名です。

   <*Rule*> は、ポリシーが使用するルールまたは式です。サポートされる値は、`ns_true` のみです。

   <*ActionName*> は、syslog サーバー・アクションの記述名です。

   例:

   ```
   add audit syslogPolicy policy-QRadar ns_true action-QRadar
   ```

4. 以下のコマンドを入力して、ポリシーをグローバルにバインドします。

   ```
   bind system global <PolicyName> -priority <Integer>
   ```

   各部分について以下で説明します。

   <*PolicyName*> は、syslog ポリシーの記述名です。

   <*Integer*> は、syslog を使用して通信している複数のポリシーのメッセージ優先順位をランク付けするために使用する数値です。

   例:

   ```
   bind system global policy-QRadar -priority 30
   ```

   複数のポリシーに (割り当てられた数値によって表される) 優先順位が設定されている場合、数値が低い方が数値が高い方より先に評価されます。
5. 以下のコマンドを入力して、Citrix NetScaler 構成を保存します。

   ```
   save config
   ```
6. 以下のコマンドを入力して、ポリシーが構成に保存されているかを確認します。

   ```
   sh system global
   ```

   注: Citrix NetScaler ユーザー・インターフェースを使用した syslog の構成については、http://support.citrix.com/article/CTX121728 またはベンダーの資料を参照してください。

   構成は完了です。Citrix NetScaler イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Citrix NetScaler によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

Citrix NetScaler ログ・ソースの構成

IBM Security QRadar は、Citrix NetScaler からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

この手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Citrix NetScaler**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

10. 以下の値を構成します。

表 *123. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Citrix NetScaler デバイスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

Citrix Access Gateway

イベントを QRadar コンソールまたはイベント・コレクター (Event Collector)に転送するための Citrix Access Gateway における syslog の構成について説明します。

手順

1. Citrix Access Gateway の Web インターフェースにログインします。
2. 「**Access Gateway** クラスター **(Access Gateway Cluster)**」タブをクリックします。
3. 「ロギング**/**設定 **(Logging/Settings)**」を選択します。
4. 「サーバー **(Server)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
5. 「ファシリティー **(Facility)**」リストで syslog ファシリティー・レベルを選択します。
6. 「ブロードキャスト間隔 **(**分**) (Broadcast interval (mins))**」で、syslog イベントを継続的に QRadar に転送するために `0` と入力します。
7. 「送信 **(Submit)**」をクリックして変更を保存します。

タスクの結果

構成は完了です。Citrix Access Gateway イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Citrix Access Gateway によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

Citrix Access Gateway のログ・ソースの構成

IBM Security QRadar は、Citrix Access Gateway アプライアンスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

この手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。

3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Citrix Access Gateway**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *124. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Citrix Access Gateway アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

第 33 章 Cloudera Navigator

Cloudera Navigator 用の IBM Security QRadar DSM は、Cloudera Navigator からイベントを収集します。

以下の表は、Cloudera Navigator DSM の仕様を示しています。

表 *125. Cloudera Navigator DSM* の仕様

仕様	値
製造元	Cloudera
DSM 名	Cloudera Navigator
RPM ファイル名	DSM-ClouderaNavigator-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	v2.0
プロトコル	Syslog
記録されるイベント・タイプ	HDFS、HBase、Hive、Hue、Cloudera Impala、Sentry に対する監査イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Cloudera Navigator の Web サイト (www.cloudera.com)

Cloudera Navigator を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Cloudera Navigator DSM RPM
2. Syslog イベントを QRadar に送信するように Cloudera Navigator デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Cloudera Navigator ログ・ソースを追加してください。以下の表は、Cloudera Navigator イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *126. Cloudera Navigator* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Cloudera Navigator
プロトコル構成	Syslog
ログ・ソース ID	Syslog ヘッダー内の IP アドレスまたはホスト名。Syslog ヘッダーに IP アドレスやホスト名が含まれていない場合、パケット IP アドレスを使用します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するように Cloudera Navigator を構成

JSON 形式の Syslog イベントを IBM Security QRadar に送信するように Cloudera Navigator を構成できます。

始める前に

Cloudera Navigator が、QRadar システム上のポート 514 にアクセスできることを確認します。

このタスクについて

Cloudera Navigator をインストールすると、すべての監査ログが自動的に収集されます。ただし、Syslog を使用して監査ログを QRadar に送信するには、Cloudera Navigator を構成する必要があります。

手順

1. 次のいずれかのタスクを実行します。
   - 「クラスター」 > 「**Cloudera Management Service**」 > 「**Cloudera Management Service**」をクリックします。
   - 「ホーム」ページの「状況」タブで、「**Cloudera Management Service**」テーブルの「**Cloudera Management Service**」リンクをクリックします。
2. 「構成 **(Configuration)**」タブをクリックします。
3. **Navigator Audit Server Logging Advanced Configuration Snippet** を見つけます。
4. 形式のタイプに応じて、「値」フィールドに次のいずれかの値を入力します。
   - `log4j.logger.auditStream = TRACE,SYSLOG`
   - `log4j.appender.SYSLOG = org.apache.log4j.net.SyslogAppender`
   - `log4j.appender.SYSLOG.SyslogHost = <QRadar Hostname>`
   - `log4j.appender.SYSLOG.Facility = Local2`
   - `log4j.appender.SYSLOG.FacilityPrinting = true`
   - `log4j.additivity.auditStream = false`
5. 「変更の保存 **(Save Changes)**」をクリックします。

第 34 章 CloudPassage Halo

IBM Security QRadar 用の CloudPassage Halo DSM は、CloudPassage Halo アカウントからイベント・ログを収集することができます。

以下の表は、CloudPassage Halo DSM の仕様を示しています。

表 *127. CloudPassage Halo DSM* の仕様

仕様	値
製造元	CloudPassage
DSM 名	CloudPassage Halo
RPM ファイル名	DSM-CloudPassageHalo-*build_number*.noarch.rpm
サポートされるバージョン	すべて
イベント・フォーマット	Syslog、ログ・ファイル
QRadar で記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	CloudPassage Web サイト (www.cloudpassage.com)

CloudPassage Halo を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードしてください。
   - DSMCommon RPM
   - CloudPassage Halo RPM
2. QRadar と通信できるように CloudPassage Halo を構成します。
3. QRadar が CloudPassage Halo をログ・ソースとして自動的に検出しない場合は、QRadar コンソール上で CloudPassage Halo のログ・ソースを作成します。

QRadar との通信用に CloudPassage Halo を構成する

CloudPassage Halo イベントを収集するには、 CloudPassage Halo Event Connector スクリプトをダウンロードし、QRadar に Syslog イベントを送信するようにこのスクリプトを構成します。

始める前に

Event Connector を構成する前に、読み取り専用の CloudPassage API 鍵を作成する必要があります。読み取り専用鍵を作成するには、CloudPassage ポータルにログインし、「サイトの管理 (Site Administration)」ウィンドウで「新しい鍵の追加 **(Add New Key)**」をクリックします。

このタスクについて

Event Connector スクリプトを実行するには、Event Connector スクリプトを実行するホストに Python 2.6 以降がインストールされている必要があります。Event Connector は、CloudPassage Events API (すべての Halo サブスクライバーが使用可能) の呼び出しを行います。

注**:** CloudPassage Halo Event Collect がイベントをファイルに書き込んで、QRadar がログ・ファイル・プロトコルを使用して取得できるように構成することができますが、この方法は推奨されません。

手順

1. CloudPassage ポータルにログインします。
2. 「設定 **(Settings)**」**>**「サイトの管理 **(Site Administration)**」に移動します。
3. 「**API** 鍵 **(API Keys)**」タブをクリックします。
4. 使用したい鍵の「表示 **(Show)**」をクリックします。
5. 鍵 ID と秘密鍵をテキスト・ファイルにコピーします。

   このファイルには、鍵 ID と秘密鍵を縦線/パイプ (|) で区切った値を 1 行で指定する必要があります。例えば、「**鍵 ID|秘密鍵**」のように指定します。複数の Halo アカウントからイベントを取得する場合は、アカウントごとに行を追加してください。
6. このファイルを `haloEvents.auth` として保存します。
7. Event Connector スクリプトと関連ファイルを https://github.com/cloudpassage/halo-event-connector-python からダウンロードします。
8. 以下のファイルを、Python 2.6 以降がインストールされている Linux システムまたは Windows システムにコピーします。
   - haloEvents.py
   - cpapi.py
   - cputils.py
   - remote_syslog.py (このスクリプトを使用するのは、Event Connector を Windows にデプロイしており、syslog を使用してイベントを送信する場合のみです)
   - haloEvents.auth
9. 以下のようにして、Linux システムまたは Windows システムで環境変数を設定します。
   - Linux の場合は、Python インタープリターの絶対パスを PATH 環境変数で指定します。
   - Windows の場合は、以下の変数を設定します。
     - PATH 変数を、haloEvents.py と Python インタープリターの場所を含めるように設定します。
     - PYTHONPATH 変数を、Python ライブラリーと Python インタープリターの場所を含めるように設定します。

10. Event Connector が Windows システム上にデプロイされている場合に syslog 経由でイベントを送信するには、以下のように **--leefsyslog=<QRadar の IP>** スイッチを指定して haloEvents.py スクリプトを実行します。

    ```
    haloEvents.py --leefsyslog=1.2.3.4
    ```

    デフォルトでは、Event Connector は初回接続時に既存のイベントを受信します。それ以降は、新しいイベントだけを受信します。起動時にすべての履歴イベントを受信するのではなく、特定の日付を開始日として指定してそれ以降のイベントを取得するには、以下のように **--starting=<date>** スイッチを使用します。日付は YYYY-MM-DD の形式で指定します。

    ```
    haloEvents.py --leefsyslog=1.2.3.4 --starting=2014-04-02
    ```

11. syslog 経由でイベントを送信し、Event Connector を Linux システムにデプロイするには、ローカル・ロガー・デーモンを構成します。
    a. システムで使用されるロガーを確認するには、以下のコマンドを入力します。

       ```
       ls -d /etc/*syslog*
       ```

       使用している Linux ディストリビューションによっては、以下のファイルがリストされる場合があります。

       - rsyslog.conf
       - syslog-ng.conf
       - syslog.conf

    b. ご使用の環境に関連する情報を使用して、該当する .conf ファイルを編集します。

       syslog-ng の構成例を以下に示します。

       ```
       source s_src {
             file("/var/log/leefEvents.txt");
       };
       destination d_qradar {
            udp("qradar_hostname" port(514));
       };
       log {
            source(s_src); destination(d_qradar);
       };
       ```

    c. **leeffile=<ファイル・パス>** スイッチを使用して haloEvents.py スクリプトを実行するには、以下のコマンドを入力します。

       ```
       haloEvents.py --leeffile=/var/log/leefEvents.txt
       ```

       --starting=YYYY-MM-DD スイッチを使用すると、初回起動時におけるイベント収集の開始日を指定することができます。

       注: syslog を使用する代わりに、イベントをファイルに書き込み、QRadar がログ・ファイル・プロトコルを使用して取得できるように構成できます。Windows システムまたは Linux システム上で、代替方法とし

てイベントをファイルに書き込むには、**--leeffile=<ファイル名>** スイッチを使用して、書き込み先のファイルを指定します。

QRadar で CloudPassage Halo のログ・ソースを構成する

CloudPassage Halo イベントを収集するには、QRadar でログ・ソースを構成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで、「**CloudPassage Halo**」を選択します。
7. 「プロトコル構成」リストで、「**Syslog**」または「ログ・ファイル **(Log File)**」を選択します。
8. 残りのパラメーターを構成します。
9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

第 35 章 CloudLock Cloud Security Fabric

IBM Security QRadar DSM for CloudLock Cloud Security Fabric は、CloudLock Cloud Security Fabric サービスからイベントを収集します。

以下の表は、CloudLock Cloud Security Fabric DSM の仕様を示しています。

表 *128. CloudLock Cloud Security Fabric DSM* の仕様

仕様	値
製造元	CloudLock
DSM 名	CloudLock Cloud Security Fabric
RPM ファイル名	DSM-CloudLockCloudSecurityFabric-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	該当なし
プロトコル	Syslog
イベント・フォーマット	ログ・イベント拡張フォーマット (LEEF)
記録されるイベント・タイプ	インシデント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Cloud Cybersecurity (https://www.cloudlock.com/products/)

CloudLock Cloud Security Fabric を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、次の RPM の最新バージョンをリストされている順序でダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - CloudLock Cloud Security Fabric DSM RPM
2. Syslog イベントを QRadar に送信するように CloudLock Cloud Security Fabric サービスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで CloudLock Cloud Security Fabric ログ・ソースを追加してください。以下の表は、CloudLock Cloud Security Fabric イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *129. CloudLock Cloud Security Fabric* ログ・ソースのパラメーター

パラメーター	値
ログ・ソース・タイプ	CloudLock Cloud Security Fabric
プロトコル構成	Syslog

CloudLock Cloud Security Fabric DSM のサンプル・イベント・メッセージを次の表に示します。

表 130. *CloudLock Cloud Security Fabric* サービスによってサポートされる *CloudLock Cloud Security Fabric* サンプル・メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
新しいインシデント	疑わしいアクティビティー	LEEF: 1.0|Cloudlock|API|v2|Incidents| match_count=2 sev=1 entity_id=ebR4q6DxvA entity_origin _type=document group=None url=https://drive.google.com/ a/cloudlockplus.com/file/d/0B3FwRBjOyR6wS0M1VUdaLWxQODg/ view?usp=drivesdk CloudLockID=NOpzejQ3v2 updated_at= 2016¬01-20T15:42:15.128356+0000 entity_owner_email= admin@cloudlockplus.com cat=NEW entity_origin_id= 0B3FwRBjOyR6wS0M1VUdaLWxQODg entity_mime_type=text/ plain devTime=2016¬01-20T15:42:14.913178+0000 policy=Custom Regex resource=confidential.txt usrName= Admin Admin realm=google policy_id=EW9zMXxNBY devTimeFormat=yyyy¬MM-dd'T'HH:mm:ss.SSSSSSZ

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するための CloudLock Cloud Security Fabric の構成

Python スクリプトを使用することで、QRadar と通信するように CloudLock Cloud Security Fabric を構成できます。

始める前に

- CloudLock からインシデントを収集するには、CloudLock API 呼び出しを行うスクリプトが必要です。このスクリプトは、インシデントを収集し、それらをログ・イベント拡張フォーマット (LEEF) に変換します。
- Python が必要です。

手順

1. CloudLock API トークンを生成します。CloudLock で API トークンを生成するには、「設定」を開きます。「統合 **(Integrations)**」パネルに移動します。ページに表示されたアクセス・トークンをコピーします。
2. CloudLock Support Web サイト (https://www.cloudlock.com/support/) に移動します。`cl_sample_incidents.py` ファイルを取得するためのサポート・ケースを開いて、イベント収集のためにそのスクリプトをスケジュールします。

第 36 章 Correlog Agent for IBM z/OS

IBM Security QRadar 用の CorreLog Agent for IBM z/OS DSM は、IBM z/OS サーバーからイベント・ログを収集することができます。

以下の表は、CorreLog Agent for IBM z/OS DSM の仕様を示しています。

仕様	値
製造元	CorreLog
DSM 名	CorreLog Agent for IBM z/OS
RPM ファイル名	DSM-CorreLogzOSAgent_*qradar-version_build-number*.noarch.rpm
サポートされるバージョン	7.1 7.2
プロトコル	Syslog LEEF
QRadar で記録されるイベント	すべてのイベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・イベント・プロパティーを含む	いいえ
その他の情報	Correlog Web サイト (https://correlog.com/solutions-and-services/sas-correlog-mainframe.html)

CorreLog Agent for IBM z/OS DSM を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新の CorreLog Agent for IBM z/OS RPM をダウンロードして QRadar コンソールにインストールしてください。
2. CorreLog Agent インスタンスごとに、CorreLog Agent システムを構成して QRadar との通信を有効にします。
3. QRadar が DSM を自動的に検出しない場合は、統合する CorreLog Agent システムごとに、QRadar コンソール上でログ・ソースを作成します。すべての必須パラメーターを構成しますが、固有の Correlog 値については、以下の表を使用します。

パラメーター	説明
ログ・ソース・タイプ	CorreLog Agent for IBM zOS
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に CorreLog Agent システムを構成する

QRadar と通信するように CorreLog Agent システムを構成する手順については、CorreLog から Agent for z/OS ソフトウェア配布と一緒に受け取った CZA - CorreLog Agent for z/OS のマニュアルを参照してください。

このタスクについて

CZA - CorreLog Agent for z/OS のマニュアルの以下のセクションを使用します。

- 「**Section 1: Introduction**」の一般考慮事項。
- 「**Section 2: Installation**」の手順。
- 「**Section 3: Configuration**」の手順。

  必ず、『**Tailoring the Installation for a Proprietary Syslog Extension/IBM Security QRadar instructions**』の手順を完了してください。

  CorreLog エージェントを始動しても、QRadar が z/OS イベントを収集しない場合は、セクション **3** のトラブルシューティングに関するトピックを参照してください。
- オプションの CorreLog Agent パラメーター・ファイルをカスタマイズするには、「**Appendix G: Fields**」に記載されている QRadar 正規化イベント属性を検討してください。

第 37 章 CrowdStrike Falcon Host

CrowdStrike Falcon Host 用の IBM Security QRadar DSM は、Falcon SIEM Connector によって転送される LEEF イベントを収集します。

以下の表では、CrowdStrike Falcon Host DSM の仕様について説明しています。

表 131. *CloudStrike Falcon Host DSM* の仕様

仕様	値
製造元	CrowdStrike
DSM 名	CrowdStrike Falcon Host
RPM ファイル名	`DSM-CrowdStrikeFalconHost-`*`QRadar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	N/A
プロトコル	Syslog
イベント・フォーマット	LEEF
記録されるイベント・タイプ	Falcon Host 検出サマリー Falcon Host 認証ログ Falcon Host 検出状況更新ログ カスタマー IOC 検出イベント ハッシュ拡散イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	CrowdStrike の Web サイト (https://www.crowdstrike.com/products/falcon-host/

CrowdStrike Falcon Host を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードし、記載されている順に QRadar コンソールでインストールしてください。
   - DSMCommon RPM
   - CrowdStrike Falcon Host DSM RPM
2. Falcon SIEM Connector をインストールし、QRadar にイベントを送信するように構成します。
3. QRadar がログ・ソースを自動的に検出しない場合は、QRadar コンソール で CrowdStrike Falcon Host ログ・ソースを追加してください。以下の表では、CrowdStrike Falcon Host イベントの収集用に固有の値を必要とするパラメーターについて説明しています。

表 132. *CrowdStrike Falcon Host* ログ・ソースのパラメーター

パラメーター	値
ログ・ソース・タイプ	CrowdStrike Falcon Host
プロトコル構成	Syslog
ログ・ソース ID	Falcon SIEM Connector がインストールされている場所の IP アドレスまたはホスト名。

以下の表は、CrowdStrike Falcon Host からのサンプル・イベント・メッセージを示しています。

表 133. *CrowdStrike Falcon Host* サンプル・メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
疑わしいアクティビティー	疑わしいアクティビティー	LEEF:1.0|CrowdStrike|FalconHost|1.0|Suspicious Activity| devTime=2016-06-09 02:57:28 src=<ipv4> srcPort=49220 dst=<ipv4> domain=INITECH cat=NetworkAccesses usrName=<username> devTimeFormat=yyyy-MM-dd HH:mm:ss connDir=0 dstPort=443 resource=CS-SE-WB-INITEC proto=TCP url=https://falcon.crowdstrike.com/detects/-4366619238013284776

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するための CloudStrike Falcon Host の構成

CloudStrike Falcon Host から IBM Security QRadar に LEEF イベントを送信するには、Falcon SIEM Connector をインストールして構成する必要があります。

始める前に

Falcon Streaming API への管理者特権付きのアクセス権限を持っている必要があります。アクセスを可能にするには、Crowdstrike のサポート (support@crowdstrike.com) にお問い合わせください。

手順

1. SIEM Connector を構成するための API 鍵と UUID を取得します。
   a. Falcon ユーザー・インターフェースにログインします。

b. 「**People App**」を選択し、「**Customer**」タブをクリックします。
「**People App**」オプションが表示されるのは管理者ユーザーのみです。

c. 「**Generate new API key**」をクリックします。

d. API 鍵および UUID のコピーを作成します。

2. Falcon SIEM Connector をインストールします。

注**:** Falcon SIEM Connector は、CentOS または RHEL 6.x-7.x のいずれかが実行されているシステム上のオンプレミスにデプロイする必要があります。CrowdStrike Cloud へのインターネット接続も必要です。

注**:** 管理者 **(root)** 特権が必要です。

- 提供される RPM を使用して Falcon SIEM Connector をインストールします。

```
rpm -Uhv /path/to/file/cs.falconhoseclient-<build_version>.<OS_version>.rpm
```

Falcon SIEM Connector は、デフォルトで `/opt/crowdstrike/` ディレクトリーにインストールされます。

サービスは、`/etc/init.d/cs.falconhoseclientd/` ディレクトリーに作成されます。

3. LEEF イベントを QRadar に転送するように SIEM Connector を構成します。構成ファイルは `/opt/crowdstrike/etc/` ディレクトリーにあります。

- LEEF 構成設定用に、`cs.falconhoseclient.leef.cfg` を `cs.falconhoseclient.cfg` に名前変更します。SIEM Connector は、デフォルトで `cs.falconhoseclient.cfg` 構成を使用します。

以下の表では、LEEF イベントを QRadar に転送するためのキー・パラメーター値のいくつかを説明しています。

表 *134.* キー・パラメーター値

キー	説明	値
version	使用する認証のバージョン。個の場合、API 鍵認証のバージョンです。	2
api_url	SIEM Connector は、このエンドポイント URL に接続します。	https://firehose.crowdstrike.com/sensors/entities/datafeed/v1
app_id	Falcon Streaming API に接続するための任意のストリング ID。	任意のストリング。例: FHAPI-LEEF
api_key	クライアント検証で資格情報として API 鍵が使用されます。	ステップ 1 で取得済み
api_uuid	クライアント検証で資格情報として UUID が使用されます。	ステップ 1 で取得済み

表 134. キー・パラメーター値 (続き)

キー	説明	値
send_to_syslog_server	Syslog サーバーへの Syslog プッシュを有効または無効にするには、このフラグを true または false に設定します。	true
host	SIEM の IP またはホスト名。	Connector が LEEF イベントを転送している QRadar SIEM の IP またはホスト名。
header_delim	ヘッダー接頭部とフィールドが、この値で区切られます。	値は等号 (=) でなければなりません。
field_delim	キー値ペアを分離するために使用される区切り文字の値。	値はタブ (¥t) でなければなりません。
time_fields	この日時フィールドの値は、指定された時刻形式に変換されます。	デフォルト・フィールドは、devTime (デバイス時刻) です。デバイス時刻の設定にカスタム LEEF キーが使用される場合は、別のフィールド名を使用してください。

4. 以下のコマンドを入力して、SIEM Connector サービスを開始します。

```
service cs.falconhoseclientd start
```

   a. サービスを停止するには、以下のコマンドを入力します。

```
service cs.falconhoseclientd stop
```

   b. サービスを再始動するには、以下のコマンドを入力します。

```
service cs.falconhoseclientd restart
```

次のタスク

Falcon SIEM Connector がイベントを QRadar に送信するように構成されていることを確認します。

第 38 章 CRYPTOCard CRYPTO-Shield

QRadar 用の IBM Security QRadar CRYPTOCard CRYPTO-Shield DSM は、syslog を使用してイベントを受け入れます。

CRYPTOCard CRYPTO-Shield イベントを QRadar と統合するには、syslog イベントを受信するために、手動でログ・ソースを作成する必要があります。

QRadar でイベントを受信するには、ログ・ソースを構成してから、syslog イベントを転送するように CRYPTOCard CRYPTO-Shield を構成する必要があります。CRYPTOCard CRYPTO-Shield デバイスから転送された syslog イベントは自動的に検出されません。QRadar は、syslog イベントを TCP ポート 514 および UDP ポート 514 の両方で受信できます。

ログ・ソースの構成

IBM Security QRadar が CRYPTOCard CRYPTO-Shield デバイスからの syslog イベントに対して、ログソースを自動的に検出および作成することはありません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**CRYPTOCard CRYPTOShield**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *135. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	CRYPTOCard CRYPTO-Shield デバイスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

CRYPTOCard CRYPTO-Shield 用の syslog の構成

syslog イベントを転送するように CRYPTOCard CRYPTO-Shield デバイスを構成するには、以下のようにします。

手順

1. CRYPTOCard CRYPTO-Shield デバイスにログインします。
2. 以下のシステム構成パラメーターを構成します。

   重要: システム構成パラメーターにアクセスするには、割り当てられているデフォルトの Super-Operator システム・ロールを備えた CRYPTOCard Operator 権限が必要です。

   - `log4j.appender.<protocol>` - ログを syslog ホストに送信します。ここで、
     - *<protocol>* は、保管用のログの送信先を決定する、ログ・アペンダーのタイプです。
       オプションは、ACC、DBG、または LOG です。このパラメーターには、以下の項目を入力します。
       `org.apache.log4j.net.SyslogAppender`
   - `log4j.appender.<protocol>.SyslogHost <IP address>` - syslog サーバーの IP アドレスまたはホスト名を入力します。ここで、
     - *<Protocol>* は、保管用のログの送信先を決定する、ログ・アペンダーのタイプです。オプションは、ACC、DBG、または LOG です。
     - *<IP address>* は、ログ送信先の IBM Security QRadar ホストの IP アドレスです。

   IP address パラメーターは、`log4j.apender.<protocol>` パラメーターの構成後に指定します。

   構成は完了です。CRYPTOCard CRYPTO-Shield によって QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

第 39 章 CyberArk

IBM Security QRadar は複数の CyberArk DSM をサポートしています。

CyberArk Privileged Threat Analytics

CyberArk Privileged Threat Analytics 用の IBM Security QRadar DSM は、CyberArk Privileged Threat Analytics デバイスからイベントを収集します。

以下の表は、CyberArk Privileged Threat Analytics DSM の仕様を示しています。

表 136. *CyberArk Privileged Threat Analytics DSM* の仕様

仕様	値
製造元	CyberArk
DSM 名	CyberArk Privileged Threat Analytics
RPM ファイル名	DSM-CyberArkPrivilegedThreatAnalytics-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	V3.1
プロトコル	Syslog
記録されるイベント・タイプ	検出されたセキュリティー・イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	CyberArk の Web サイト (http://www.cyberark.com)

CyberArk Privileged Threat Analytics を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - CyberArk Privileged Threat Analytics DSM RPM
   - DSMCommon RPM
2. Syslog イベントを QRadar に送信するように CyberArk Privileged Threat Analytics デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで CyberArk Privileged Threat Analytics ログ・ソースを追加してください。以下の表は、CyberArk Privileged Threat Analytics イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 137. *CyberArk Privileged Threat Analytics* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	CyberArk Privileged Threat Analytics

表 137. *CyberArk Privileged Threat Analytics* ログ・ソース・パラメーター (続き)

パラメーター	値
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に CyberArk Privileged Threat Analytics を構成する

CyberArk Privileged Threat Analytics からすべてのイベントを収集するには、Syslog サーバーとして IBM Security QRadar を指定し、Syslog フォーマットを構成する必要があります。CyberArk Privileged Threat Analytics デバイスは、ログ・イベント拡張フォーマット (LEEF) としてフォーマットされた Syslog イベントを送信します。

手順

1. CyberArk Privileged Threat Analytics マシンで、`/opt/tomcat/diamond-resources/local/` ディレクトリーに移動し、`systemparm.properties` ファイルを vi などのテキスト・エディターで開きます。
2. `syslog_outbound` プロパティーのコメントを外して、以下のパラメーターを編集します。

パラメーター	値
ホスト	QRadar システムのホスト名または IP アドレス。
ポート	514
プロトコル	UDP
フォーマット	QRadar

例: syslog_outbound プロパティーの例を次に示します。

```
syslog_outbound=[{"host": "SIEM_MACHINE_ADDRESS", "port": 514, "format":
"QRadar", "protocol": "UDP"}]
```

例: 次に、複数の Syslog 宛先をコンマ区切りで指定している syslog_outbound プロパティーの例を示します。

```
syslog_outbound=[{"host": "SIEM_MACHINE_ADDRESS", "port": 514, "format":
"QRadar", "protocol": "UDP"} , {"host": "SIEM_MACHINE_ADDRESS1", "port":
514, "format": "QRadar", "protocol": "UDP"} , ...]
```

3. `systemparm.properties` 構成ファイルを保存して、ファイルを閉じます。

4. CyberArk Privileged Threat Analytics を再始動します。

CyberArk Vault

IBM Security QRadar 用の CyberArk Vault DSM は、syslog を使用して、ログ・イベント拡張フォーマット (LEEF) 形式のイベントを受け入れます。

QRadar は、CyberArk Vault からのユーザー・アクティビティーおよびセーフ・アクティビティーの両方を監査イベント・ログに記録します。CyberArk Vault は QRadar と統合し、syslog を使用して監査ログを転送して、特権アカウント・アクティビティーの詳細なログを作成します。

イベント・タイプ・フォーマット

イベントをログ・イベント拡張フォーマット (LEEF) で生成し、syslog を使用して転送するように、CyberArk Vault を構成する必要があります。LEEF 形式は、syslog ヘッダー (パイプ (|) 区切り) とログ・ペイロード・セクション (タブ区切りフィールド) から構成されます。

CyberArk Vault からの syslog イベントが適切にフォーマットされていない場合は、デバイス構成またはソフトウェアのバージョンを調べて、アプライアンスが LEEF をサポートしていることを確認してください。LEEF イベント・メッセージは、適切にフォーマットされていると、自動的に検出され、ログ・ソースとして QRadar に追加されます。

CyberArk Vault 用の syslog の構成

syslog イベントを IBM Security QRadar に転送するように CyberArk Vault を構成するには、以下のようにします。

手順

1. CyberArk デバイスにログインします。
2. `DBParm.ini` ファイルを編集します。
3. 以下のパラメーターを構成します。

表 *138. Syslog* パラメーター

パラメーター	説明
SyslogServerIP	QRadar の IP アドレスを入力します。
SyslogServerPort	QRadar への接続に使用する UDP ポートを入力します。デフォルト値は 514 です。
SyslogMessageCodeFilter	CyberArk Vault から QRadar にどのメッセージ・コードが送信されるかを構成します。特定のメッセージ番号または番号の範囲を定義できます。デフォルトでは、ユーザー・アクティビティーと安全アクティビティーのすべてのメッセージ・コードが送信されます。 **例:** メッセージ・コード 1、2、3、30、および 5 から 10 を定義するには、`1,2,3,5-10,30` と入力する必要があります。

表 138. Syslog パラメーター (続き)

パラメーター	説明
SyslogTranslatorFile	LEEF.xsl 変換プログラム・ファイルのファイル・パスを入力します。変換プログラム・ファイルは、syslog プロトコルの CyberArk 監査レコード・データを構文解析するために使用されます。

4. LEEF.xsl を、DBParm.ini ファイル内の **SyslogTranslatorFile** パラメーターで指定されている場所にコピーします。

タスクの結果

構成は完了です。CyberArk Vault イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。CyberArk Vault によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

CyberArk Vault のログ・ソースの構成

IBM Security QRadar は、CyberArk Vault の syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**CyberArk Vault**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 139. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	CyberArk Vault アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

第 40 章 CyberGuard Firewall/VPN Appliance

IBM Security QRadar 用の CyberGuard Firewall VPN Appliance DSM は、syslog を使用して CyberGuard イベントを受け入れます。

QRadar は、syslog を使用して転送される CyberGuard KS シリーズ・アプライアンスの関連するすべての CyberGuard イベントを記録します。

syslog イベントの構成

syslog イベントを転送するように CyberGuard デバイスを構成するには、以下のようにします。

手順

1. CyberGuard ユーザー・インターフェースにログインします。
2. 「拡張 (Advanced)」ページを選択します。
3. 「システム・ログ **(System Log)**」で「リモート・ロギングを有効にする **(Enable Remote Logging)**」を選択します。
4. IBM Security QRadar の IP アドレスを入力します。
5. 「適用」をクリックします。

構成は完了です。CyberGuard イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。CyberGuard アプライアンスによって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、CyberGuard アプライアンスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**CyberGuard TSP** ファイアウォール**/VPN**」を選択します。

9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 「ログ・ソース **ID**」パラメーターに、CyberGuard アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

第 41 章 Damballa Failsafe

IBM Security QRadar 用の Failsafe DSM は、ログ・イベント拡張フォーマット (LEEF) を使用して syslog イベントを受け入れるため、関連するすべての Damballa Failsafe イベントを QRadar が記録できます。

イベントをログ・イベント拡張フォーマット (LEEF) で生成し、syslog を使用して転送するように Damballa Failsafe を構成する必要があります。LEEF 形式は、syslog ヘッダー (パイプ (|) 区切り) とログ・イベント・ペイロード (タブ区切りフィールド) から構成されます。

Damballa Failsafe から転送される syslog イベントが LEEF 形式で適切にフォーマットされていない場合は、デバイス構成またはソフトウェアのバージョンを調べて、アプライアンスが LEEF をサポートしていることを確認してください。LEEF イベント・メッセージは、適切にフォーマットされていると、自動的に検出され、ログ・ソースとして QRadar に追加されます。

Damballa Failsafe 用の syslog の構成

イベントを収集するには、syslog イベントを IBM Security QRadar に転送するように Damballa Failsafe デバイスを構成する必要があります。

手順

1. Damballa Failsafe 管理コンソールにログインします。
2. ナビゲーション・メニューで「セットアップ **(Setup)**」 > 「統合設定 **(Integration Settings)**」を選択します。
3. 「QRadar」タブをクリックします。
4. 「IBM Security QRadar への公開を有効にする (Enable Publishing to IBM Security QRadar)」を選択します。
5. 以下のオプションを構成します。
   - ホスト名 **(Hostname)** - QRadar コンソールの IP アドレスまたは完全修飾名 (FQN) を入力します。
   - 宛先ポート **(Destination Port)** - 514 と入力します。デフォルトでは、QRadar は、syslog イベントを受信するためのポートとしてポート 514 を使用します。
   - 送信元ポート **(Source Port)** - この入力は必須ではありません。Damballa Failsafe デバイスが syslog イベントの送信に使用する送信元ポートを入力します。
6. 「保存」をクリックします。

構成は完了です。Damballa Failsafe イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Damballa Failsafe によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Damballa Failsafe デバイスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Damballa Failsafe**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *140. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Damballa Failsafe デバイスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 42 章 DG Technology MEAS

DG Technology MEAS 用の IBM Security QRadar DSM では、DG Technology MEAS サーバーからイベント・ログを収集できます。

以下の表は、DG Technology MEAS DSM の仕様を示しています。

表 *141. DG Technology MEAS* の *DSM* 仕様

仕様	値
製造元	DG Technology
ログ・ソース・タイプ	DG Technology MEAS
RPM ファイル名	DSM-DGTechnologyMEAS-*build_number*.noarch.rpm
サポートされるバージョン	8.x
プロトコル構成	LEEF Syslog
サポートされるイベント・タイプ	メインフレーム・イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・イベント・プロパティーを含む	いいえ
その他の情報	DG Technology Web サイト (http://www.dgtechllc.com)

DG Technology MEAS DSM を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、最新の DG Technology MEAS RPM をダウンロードして QRadar コンソールにインストールしてください。
2. DG Technology MEAS のインスタンスごとに、DG Technology MEAS システムを構成して QRadar と通信できるようにします。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に DG Technology MEAS システムを構成する

DG Technology MEAS からすべての監査ログとシステム・イベントを収集するには、QRadar を Syslog サーバーとして指定する必要があります。

手順

1. DG Technology MEAS サーバーにログインします。
2. 以下のコマンドを入力します。

   ```
   java meas/MeasServer 41000 m=qwl lo=IP_address_of_QRadar_host
   ```

タスクの結果

QRadar が DG Technology MEAS からイベントを受信すると、自動的にログ・ソースが作成されて、「ログ・ソース」ウィンドウにリストされます。

第 43 章 Digital China Networks (DCN)

IBM Security QRadar 用の Digital China Networks (DCN) DCS/DCRS シリーズ DSM は、syslog を使用して Digital China Networks (DCN) スイッチからイベントを受け入れることができます。

IBM Security QRadarは、DCN スイッチから転送される、関連するすべての IPv4 イベントを記録します。ご使用のデバイスを QRadar と統合するには、ログ・ソースを構成してから、syslog イベントを転送するように DCS スイッチまたは DCRS スイッチを構成する必要があります。

サポートされるアプライアンス

DSM は以下の DCN DCS/DCRS シリーズのスイッチをサポートします。

- DCS - 3650
- DCS - 3950
- DCS - 4500
- DCRS - 5750
- DCRS - 5960
- DCRS - 5980
- DCRS - 7500
- DCRS - 9800

ログ・ソースの構成

IBM Security QRadar が DCN DCS/DCRS シリーズ・スイッチからの受信 syslog イベントを自動的に検出することはありません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**DCN DCS/DCRS** シリーズ」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 142. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	DCN DCS/DCRS シリーズ・スイッチの ID として使用する、ログ・ソースの IP アドレス、ホスト名、または名前を入力します。 DCN DCS/DCRS シリーズ・スイッチ用に作成した各ログ・ソースには、IP アドレスやホスト名などの固有 ID が含まれます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。これで、イベントを QRadar に転送するように Digital China Networks DCS または DCRS シリーズ・スイッチを構成する準備ができました。

DCN DCS/DCRS シリーズ・スイッチの構成

イベントを収集するには、IBM Security QRadar で DCN DCS/DCRS シリーズ・スイッチを構成する必要があります。

手順

1. DCN DCS/DCRS シリーズ・スイッチのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力して、管理モードにアクセスします。

   ```
   enable
   ```

3. 以下のコマンドを入力して、グローバル構成モードにアクセスします。

   ```
   構成
   ```

   コマンド・ライン・インターフェースに、以下の構成モード・プロンプトが表示されます。

   ```
   Switch(Config)#
   ```

4. 以下のコマンドを入力して、スイッチのログ・ホストを構成します。

   ```
   logging <IP address> facility <local> severity <level>
   ```

   各部分について以下で説明します。

   - *<IP address>* は、QRadar コンソールの IP アドレスです。
   - *<local>* は、syslog ファシリティーです (例えば、local0)。
   - *<level>* は、syslog イベントの重大度です (例えば、informational)。値 informational を指定した場合、すべての情報レベル・イベントおよびそれより上の (情報レベルより重大度が高い) イベント (通知、警告、エラー、重大、アラート、緊急など) が転送されます。

   例:

   ```
   logging 10.10.10.1 facility local0 severity informational
   ```

5. 以下のコマンドを入力して、構成変更を保存します。

   `write` 構成は完了です。「ログ・アクティビティー」タブでイベントを表示することで、QRadar に転送されたイベントを確認できます。

第 44 章 Enterprise-IT-Security.com SF-Sherlock

Enterprise-IT-Security.com SF-Sherlock 用の IBM Security QRadar DSM は、ご使用の Enterprise-IT-Security.com SF-Sherlock サーバーからログを収集します。

以下の表は、Enterprise-IT-Security.com SF-Sherlock DSM の仕様を示しています。

表 143. *Enterprise-IT-Security.com SF-Sherlock DSM* の仕様

仕様	値
製造元	Enterprise-IT-Security.com
DSM 名	Enterprise-IT-Security.com SF-Sherlock
RPM ファイル名	DSM-EnterpriseITSecuritySFSherlock-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	v8.1 以降
イベント・フォーマット	ログ・イベント拡張フォーマット (LEEF)
記録されるイベント・タイプ	All_Checks, DB2_Security_Configuration, JES_Configuration, Job_Entry_System_Attack, Network_Parameter, Network_Security, No_Policy, Resource_Access_Viol, Resource_Allocation, Resource_Protection, Running_System_Change, Running_System_Security, Running_System_Status, Security_Dbase_Scan, Security_Dbase_Specialty, Security_Dbase_Status, Security_Parm_Change, Security_System_Attack, Security_System_Software, Security_System_Status, SF-Sherlock, Sherlock_Diverse, Sherlock_Diverse, Sherlock_Information, Sherlock_Specialties, Storage_Management, Subsystem_Scan, Sysplex_Security, Sysplex_Status, System_Catalog, System_File_Change, System_File_Security, System_File_Specialty, System_Log_Monitoring, System_Module_Security, System_Process_Security, System_Residence, System_Tampering, System_Volumes, TSO_Status, UNIX_OMVS_Security, UNIX_OMVS_System, User_Defined_Monitoring, xx_Resource_Prot_Templ
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Enterprise-IT-Security の Web サイト (http://www.enterprise-it-security.com)

Enterprise-IT-Security.com SF-Sherlock を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、次の RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Enterprise-IT-Security.com SF-Sherlock DSM RPM
   - DSM 共通 RPM
2. Syslog イベントを QRadar に送信するように Enterprise-IT-Security.com SF-Sherlock デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Enterprise-IT-Security.com SF-Sherlock ログ・ソースを追加してください。以下の表は、Enterprise-IT-Security.com SF-Sherlock イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *144. Enterprise-IT-Security.com SF-Sherlock* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Enterprise-IT-Security.com SF-Sherlock
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するように Enterprise-IT-Security.com SF-Sherlock を構成

SF-Sherlock のイベントと評価の詳細を QRadar に送信するには、SF-Sherlock 2 QRadar 接続キットを実装します。

このタスクについて

QRadar に送信される情報は、詳細に定義および選択できます。選択する転送方法に関係なく、すべての情報が LEEF 形式のレコードとして QRadar に到達します。

手順

1. 対応する SHERLOCK.SSHKSAMP データ・セット・メンバーを使用することで、UMODQR01 および UMODQR02 という SF-Sherlock SMP/E ユーザー変更をインストールします。
2. SF-Sherlock の LEEF レコードを QRadar の Syslog デーモンに送信する方法 (一般的に推奨される転送方法) を採用する場合、z/OS の USS 環境に SF-Sherlock の汎用 Syslog メッセージ・ルーターをインストールする必要があります。SHERLOCK.SSHKSAMP データ・セットの UNIXCMDL メンバーにすべてのインストール詳細があります。
3. オプション: FTP や別の手法を使用してログを転送する場合は、UMODQR01 ユーザー変更を調整する必要があります。

4. SF-Sherlock の `init-deck` パラメーター構成ファイルの QRADARSE メンバーに、QRadar LEEF Syslog サーバーの IP アドレス、転送方法 (UDP または TCP)、およびポート番号 (514) を入力します。
5. SHERLOCK.SSHKSAMP データ・セットの ALLOCQRG ジョブを使用して、QRadar 関連のログ・データ・セットを割り振ります。これは、SHERLOCK 開始プロシージャー (STC) が、QRadar に転送されるすべての QRadar LEEF レコードを保持するために使用されます。
6. SHERLOCK.SSHKSAMP データ・セットの QRDARTST メンバーを使用して、SF-Sherlock 2 QRadar メッセージのルーティング接続をテストできます。QRadar がテスト・イベントを受信した場合、実装は正常に完了しています。
7. $BUILD00 マスター制御メンバー内に既に準備されている `ADD QRADARxx` ステートメントを使用して、QRADAR00 (イベント・モニター) メンバーと、オプションで QRADAR01 (評価の詳細) `init-deck` メンバーをアクティブ化することで、SF-Sherlock インストール済み環境内の SF-Sherlock 2 QRadar 接続を有効にします。
8. SHERLOCK 開始プロシージャーをリフレッシュまたはリサイクルして、SF-Sherlock から QRadar への接続を有効にする新しいマスター制御メンバーをアクティブ化します。

第 45 章 Epic SIEM

Epic SIEM 用の IBM Security QRadar DSM は、Epic SIEM からイベント・ログを収集できます。

以下の表は、Epic SIEM DSM の仕様を示しています。

表 *145. Epic SIEM DSM* の仕様

仕様	値
製造元	Epic
DSM 名	Epic SIEM
RPM ファイル名	DSM-EpicSIEM*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	Epic 2014
イベント・フォーマット	LEEF
記録されるイベント・タイプ	監査 認証
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Epic Web サイト (http://www.epic.com/)

Epic SIEM DSM を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、次の RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Epic SIEM DSM RPM
   - DSMCommon RPM
2. Syslog イベントを QRadar に送信するように Epic SIEM デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Epic SIEM ログ・ソースを追加してください。以下の表は、Epic SIEM イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *146. Epic SIEM* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Epic SIEM
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するように Epic SIEM を構成

Epic SIEM から Syslog イベントを収集するには、IBM Security QRadar ホスト用に外部の Syslog サーバーを追加する必要があります。

手順

1. すべての Web サービスが Interconnect のインスタンスに対して有効になっていない場合、必須の **SendSIEMSyslogAudit** サービスを実行するために次の手順を実行します。
   a. **Interconnect Configuration Editor** にアクセスするために、「スタート」 > 「**Epic 2014**」 > 「**Interconnect**」 > 「***your_instance***」 > 「**Configuration Editor**」をクリックします。
   b. 「**Configuration Editor**」で、「**Business Services**」フォームを選択します。
   c. 「**Service Category**」タブで、「**SendSIEMSyslogAudit**」をクリックします。
   d. 「保存」をクリックします。
2. Epic サーバーにログインします。
3. 「**Epic System Definitions (%ZeUSTBL)**」 > 「**Security**」 > 「**Auditing Options**」 > 「**SIEM Syslog Settings**」 > 「**SIEM Syslog Configuration**」をクリックします。
4. 次の表を使用して、パラメーターを構成します。

パラメーター	説明
SIEM ホスト	QRadar アプライアンスのホスト名または IP アドレス。
SIEM ポート	514
SIEM 形式	LEEF (ログ・イベント拡張フォーマット)。

5. 「**SIEM Syslog Settings**」メニューで、「**SIEM Syslog**」をクリックし、それを enabled に設定します。

   SIEM Syslog 送信デーモンは、環境が **runlevel Up** に設定されるか、**SIEM Syslog** を有効にすると自動的に開始されます。
6. このデーモンを停止する場合は、「**SIEM Syslog Settings**」メニューで、「**SIEM Syslog**」をクリックし、それを disabled に設定します。

   重要**:** Syslog 設定が enabled のときにデーモンを停止すると、システムでは、データをパージすることなくログへの記録を続行します。Syslog 設定が enabled のときにデーモンを停止する場合は、Epic 社の担当者、またはシステム管理者に連絡してください。

第 46 章 Exabeam

Exabeam 用の IBM Security QRadar DSM は、Exabeam デバイスからイベントを収集します。

以下の表は、Exabeam DSM の仕様を示しています。

表 *147. Exabeam DSM* の仕様

仕様	値
製造元	Exabeam
DSM 名	Exabeam
RPM ファイル名	DSM-ExabeamExabeam-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	v1.7 および v2.0
記録されるイベント・タイプ	重要 異常
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Exabeam の Web サイト (http://www.exabeam.com)

Exabeam を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Exabeam DSM RPM をダウンロードして、QRadar コンソールにインストールします。
2. Syslog イベントを QRadar に送信するように Exabeam デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Exabeam ログ・ソースを追加してください。以下の表は、Exabeam イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *148. Exabeam* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Exabeam
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するように Exabeam を構成

Exabeam から Syslog イベントを収集するには、Syslog サーバーとして QRadar を指定する宛先を追加する必要があります。

手順

1. Exabeam ユーザー・インターフェース (https://<*Exabeam_IP*>:8484) にログインします。
2. `https://<Exabeam_IP>:8484` を選択し、URL アドレスの末尾に `#setup` と入力します。 `https://<Exabeam_IP>:8484/#setup`
3. 「Navigation」ペインで、「**Incident Notification**」をクリックします。
4. 「**Send via Syslog**」を選択し、次の Syslog パラメーターを構成します。

パラメーター	説明
IP アドレスまたはホスト名	QRadar イベント・コレクター (Event Collector) の IP アドレス。
プロトコル	TCP
ポート	514
Syslog の重大度レベル	緊急

第 47 章 Extreme

IBM Security QRadar は、さまざまな Extreme DSM からイベントを受け入れます。

Extreme 800 シリーズ・スイッチ

IBM Security QRadar用の Extreme 800 シリーズ・スイッチ DSM は、syslog を使用してイベントを受け入れます。

QRadar は、関連するすべてのイベント (監査、認証、システム、およびスイッチの各イベント) を記録します。Extreme 800 シリーズ・スイッチを QRadar で構成する前に、syslog イベントを転送するようにスイッチを構成しておく必要があります。

Extreme 800 シリーズ・スイッチ

syslog イベントを転送するように Extreme 800 シリーズ・スイッチを構成します。

このタスクについて

Extreme 800 シリーズ・スイッチを手動で構成するには、以下のようにします。

手順

1. Extreme 800 シリーズ・スイッチのコマンド・ライン・インターフェースにログインします。

   以下の構成ステップを実行するには、システム管理者またはオペレーター・レベルのユーザーでなければなりません。
2. 以下のコマンドを入力して、syslog を有効にします。

   ```
   enable syslog
   ```
3. 以下のコマンドを入力して、イベントを QRadar に転送するための syslog アドレスを作成します。

   ```
   create syslog host 1 <IP address> severity informational facility local7
   udp_port 514 state enable
   ```

   ここで、*<IP address>* は、QRadar コンソールまたはイベント・コレクターの IP アドレスです。
4. オプション: 以下のコマンドを入力し、IP インターフェース・アドレスを使用して syslog イベントを転送します。

   ```
   create syslog source_ipif <name> <IP address>
   ```

   各部分について以下で説明します。

   - *<name>* は、IP インターフェースの名前です。

- *<IP address>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。

構成は完了です。Extreme 800 シリーズ・スイッチのイベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Extreme 800 シリーズ・スイッチによって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Extreme 800 シリーズ・スイッチの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。ログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Extreme 800** シリーズ・スイッチ」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 149. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Extreme 800 シリーズ・スイッチからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Extreme Dragon

IBM Security QRadar 用の Extreme Dragon DSM は、syslog または SNMPv3 のいずれかを使用して Extreme イベントを受け入れ、該当するすべての Extreme Dragon イベントを記録します。

このタスクについて

QRadar Extreme Dragon DSM を構成するには、以下の手順を使用します。

手順

1. SNMPv3 通知ルールを使用して Alarm Tool ポリシーを作成します。『SNMPv3 用の Alarm Tool ポリシーの作成』を参照してください。
2. Syslog 通知ルールを使用して Alarm Tool ポリシーを作成します。 353 ページの『Syslog 用のポリシーの作成』を参照してください。
3. QRadar 内でログ・ソースを構成します。 356 ページの『ログ・ソースの構成』を参照してください。
4. syslog メッセージを転送するように Dragon Enterprise Management Server (EMS) を構成します。 356 ページの『syslog メッセージを転送するための EMS の構成』を参照してください。

SNMPv3 用の Alarm Tool ポリシーの作成

この手順では、SNMPv3 通知ルールを使用して Alarm Tool ポリシーを構成する方法について説明します。PDATA バイナリー・データ・エレメントを転送する必要がある場合は、SNMPv3 通知ルールを使用します。

このタスクについて

SNMPv3 通知ルールを使用して Alarm Tool ポリシーで Extreme Dragon を構成するには、以下のようにします。

手順

1. Extreme Dragon EMS にログインします。
2. 「**Alarm Tool**」アイコンをクリックします。
3. 以下のように、Alarm Tool ポリシーを構成します。

   「**Alarm Tool** ポリシー・ビュー **(Alarm Tool Policy View)**」 > 「カスタム・ポリシー **(Custom Policies)**」メニュー・ツリーで右クリックして「**Alarm Tool** ポリシーの追加 **(Add Alarm Tool Policy)**」を選択します。

   「Alarm Tool ポリシーの追加 (Add Alarm Tool Policy)」ウィンドウが表示されます。
4. 「**Alarm Tool** ポリシーの追加 **(Add Alarm Tool Policy)**」フィールドにポリシー名を入力します。

   例:

   QRadar
5. 「**OK**」をクリックします。
6. メニュー・ツリーで、『SNMPv3 用の Alarm Tool ポリシーの作成』のステップで入力したポリシー名を選択します。
7. 以下のように、イベント・グループを構成します。

   「イベント・グループ **(Events Group)**」タブをクリックします。

8. 「新規」をクリックします。

「イベント・グループ・エディター (Event Group Editor)」が表示されます。

9. モニターするイベント・グループまたは個別のイベントを選択します。
10. 「追加」をクリックします。

プロンプトが表示されます。

11. 「はい」をクリックします。
12. 「イベント・グループ・エディター **(Event Group Editor)**」の右側の列に `Dragon-Events` と入力します。
13. 「**OK**」をクリックします。
14. 以下のように、SNMPv3 通知ルールを構成します。

「通知ルール **(Notification Rules)**」タブをクリックします。

15. 「新規」をクリックします。
16. 「名前 (name)」フィールドに、QRadar-`Rule` と入力します。
17. 「**OK**」をクリックします。
18. 「通知ルール (Notification Rules)」ペインで、「QRadar-**Rule**」を選択します。
19. 「**SNMP V3**」タブをクリックします。
20. 「新規」をクリックします。
21. 必要に応じて、以下のように SNMP V3 の値を更新します。
    - サーバー **IP** アドレス **(Server IP Address)** - QRadar の IP アドレスを入力します。

    注**:** OID は変更しないでください。
    - 情報提供 **(Inform)** - 「情報提供 **(Inform)**」チェック・ボックスを選択します。
    - セキュリティー名 **(Security Name)** - SNMPv3 ユーザー名を入力します。
    - 認証パスワード **(Auth Password)** - 該当するパスワードを入力します。
    - プライバシー・パスワード **(Priv Password)** - 該当するパスワードを入力します。
    - メッセージ **(Message)** - 以下を 1 行で入力します。

```
Dragon Event: %DATE%,,%TIME%,,%NAME%,,%SENSOR%,,%PROTO%,,%SIP%,,
%DIP%,,%SPORT%,,%DPORT%,,%DIR%,,%DATA%,,<<<%PDATA%>>>
```

    注**:** セキュリティー・パスワードおよびプロトコルが、SNMP 構成で構成されているデータに一致していることを確認してください。
22. 「**OK**」をクリックします。
23. 以下のように、通知イベントが別個のイベントとしてログに記録されていることを確認します。

「グローバル・オプション **(Global Options)**」タブをクリックします。

24. 「メイン **(Main)**」タブをクリックします。

25. 「イベントの連結 **(Concatenate Events)**」が選択されていないことを確認します。
26. 以下のように、SNMP のオプションを構成します。

    「グローバル・オプション **(Global Options)**」タブをクリックします。
27. 「**SNMP**」タブをクリックします。
28. SNMP トラップを送信する EMS サーバーの IP アドレスを入力します。
29. 以下のように、アラーム情報を構成します。

    「アラーム **(Alarms)**」タブをクリックします。
30. 「新規」をクリックします。
31. 以下のパラメーターの値を入力します。
    - 名前 **(Name)** - QRadar-Alarm と入力します。
    - タイプ **(Type)** - 「リアルタイム **(Real Time)**」を選択します。
    - イベント・グループ **(Event Group)** - 「**Dragon-Events**」を選択します。
    - 通知グループ **(Notification Rule)** - 「QRadar-**Rule**」チェック・ボックスを選択します。
32. 「**OK**」をクリックします。
33. 「コミット **(Commit)**」をクリックします。
34. 「エンタープライズ・ビュー (Enterprise View)」に移動します。
35. 「**Alarm Tool**」を右クリックし、「**Alarm Tool** ポリシーを関連付ける **(Associate Alarm Tool Policy)**」を選択します。
36. 「QRadar ポリシー (QRadar policy)」を選択します。「**OK**」をクリックします。
37. 「エンタープライズ **(Enterprise)**」メニューで右クリックし、「デプロイ **(Deploy)**」を選択します。

    これで、QRadar でログ・ソース SNMP プロトコルを構成する準備ができました。

Syslog 用のポリシーの作成

この手順では、ログ・イベント拡張フォーマット (LEEF) メッセージ形式の syslog 通知ルールを使用して Alarm Tool ポリシーを構成する方法について説明します。

このタスクについて

LEEF は、通知レートが高いときまたは IPv6 アドレスが表示されているときに通知を Dragon Network Defense に送信するための推奨メッセージ・フォーマットです。LEEF 形式の syslog 通知を使用しない場合は、詳細について *Extreme Dragon* の資料 を参照してください。

注**:** バイナリー・データ・エレメントである PDATA を転送する必要がある場合は、SNMPv3 通知ルールを使用します。syslog 通知ルールは使用しないでください。

syslog 通知ルールを使用して Alarm Tool ポリシーで Extreme Dragon を構成するには、以下のようにします。

手順

1. Extreme Dragon EMS にログインします。
2. 「**Alarm Tool**」アイコンをクリックします。
3. 以下のように、Alarm Tool ポリシーを構成します。

   「**Alarm Tool** ポリシー・ビュー **(Alarm Tool Policy View)**」 > 「カスタム・ポリシー **(Custom Policies)**」メニュー・ツリーで右クリックして「**Alarm Tool** ポリシーの追加 **(Add Alarm Tool Policy)**」を選択します。

   「Alarm Tool ポリシーの追加 (Add Alarm Tool Policy)」ウィンドウが表示されます。
4. 「**Alarm Tool** ポリシーの追加 **(Add Alarm Tool Policy)**」フィールドにポリシー名を入力します。

   例:

   QRadar
5. 「**OK**」をクリックします。
6. メニュー・ツリーで「**QRadar**」を選択します。
7. 以下のように、イベント・グループを構成します。

   「イベント・グループ **(Events Group)**」タブをクリックします。
8. 「新規」をクリックします。

   「イベント・グループ・エディター (Event Group Editor)」が表示されます。
9. モニターするイベント・グループまたは個別のイベントを選択します。
10. 「追加」をクリックします。

    プロンプトが表示されます。
11. 「はい」をクリックします。
12. 「イベント・グループ・エディター (Event Group Editor)」の右側の列に `Dragon-Events` と入力します。
13. 「**OK**」をクリックします。
14. 以下のように、Syslog 通知ルールを構成します。

    「通知ルール **(Notification Rules)**」タブをクリックします。
15. 「新規」をクリックします。
16. 「名前 (name)」フィールドに、`QRadar-RuleSys` と入力します。
17. 「**OK**」をクリックします。
18. 「通知ルール (Notification Rules)」ペインで、新しく作成した「QRadar**-RuleSys**」項目を選択します。
19. 「**Syslog**」タブをクリックします。
20. 「新規」をクリックします。

「Syslog エディター (Syslog Editor)」が表示されます。

21. 以下の値を更新します。
    - ファシリティー **(Facility)** - 「ファシリティー **(Facility)**」リストを使用して、ファシリティーを選択します。
    - レベル **(Level)** - 「レベル **(Level)**」リストを使用して、「通知 **(notice)**」を選択します。
    - メッセージ **(Message)** - 「タイプ **(Type)**」リストを使用して、「**LEEF**」を選択します。

    ```
    LEEF:Version=1.0|Vendor|Product|ProductVersion|eventID|devTime|
    proto|src|sensor|dst|srcPort|dstPort|direction|eventData|
    ```

    LEEF メッセージ・フォーマットでは、各キーワード間にパイプ区切り文字を使用してフィールドを区切ります。
22. 「**OK**」をクリックします。
23. 以下のように、通知イベントが別個のイベントとしてログに記録されていることを確認します。

    「グローバル・オプション **(Global Options)**」タブをクリックします。
24. 「メイン **(Main)**」タブをクリックします。
25. 「イベントの連結 **(Concatenate Events)**」が選択されていないことを確認します。
26. 以下のように、アラーム情報を構成します。

    「アラーム **(Alarms)**」タブをクリックします。
27. 「新規」をクリックします。
28. 以下のように、パラメーターの値を入力します。
    - 名前 **(Name)** - QRadar**-Alarm** と入力します。
    - タイプ **(Type)** - 「リアルタイム **(Real Time)**」を選択します。
    - イベント・グループ **(Event Group)** - 「**Dragon-Events**」を選択します。
    - 通知グループ **(Notification Rule)** - 「QRadar**-RuleSys**」チェック・ボックスを選択します。
29. 「**OK**」をクリックします。
30. 「コミット **(Commit)**」をクリックします。
31. 「エンタープライズ・ビュー (Enterprise View)」に移動します。
32. 「**Alarm Tool**」を右クリックし、「**Alarm Tool** ポリシーを関連付ける **(Associate Alarm Tool Policy)**」を選択します。
33. 新しく作成した「QRadar ポリシー **(QRadar policy)**」を選択します。「**OK**」をクリックします。
34. 「企業 **(Enterprise)**」メニューでポリシーを右クリックし、「デプロイ **(Deploy)**」を選択します。

これで、QRadar で syslog ログ・ソースを構成する準備ができました。

ログ・ソースの構成

これで、IBM Security QRadar でログ・ソースを構成する準備ができました。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Extreme Dragon Network IPS**」を選択します。
9. 「プロトコル構成」リストで「**SNMPv3**」または「**Syslog**」のいずれかのオプションを選択します。

   Extreme Dragon デバイスについて詳しくは、*Extreme Dragon* の資料 を参照してください。

   注**:** 「ログ・アクティビティー」タブのイベント・マッピング・ツールを使用して、正規化されたイベントまたはロー・イベントを上位および下位のカテゴリー (QID) にマップできます。ただし、イベント・マッピング・ツールを使用して、Dragon メッセージの組み合わせをマップすることはできません。詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

関連概念:

34 ページの『SNMPv3 プロトコルの構成オプション』

SNMPv3 プロトコルを使用して SNMPv3 イベントを受信するようにログ・ソースを構成することができます。

syslog メッセージを転送するための EMS の構成

Dragon Enterprise Management Server (EMS) v7.4.0 アプライアンス以降、イベントを IBM Security QRadar などのセキュリティーおよび情報マネージャーに転送するには、syslog-ng を使用する必要があります。

Dragon EMS v7.4.0 以降、syslogd は syslog-ng に置き換わりました。

syslog メッセージを転送するように EMS を構成するには、以下のいずれかを選択する必要があります。

- syslog-ng および Extreme Dragon EMS v7.4.0 以降を使用している場合は、357 ページの『Extreme Dragon EMS v7.4.0 以降を使用した syslog-ng の構成』を参照してください。
- syslogd および Extreme Dragon EMS v7.4.0 以前を使用している場合は、357 ページの『Extreme Dragon EMS v7.4.0 以下を使用した syslogd の構成』を参照してください。

Extreme Dragon EMS v7.4.0 以降を使用した syslog-ng の構成

このセクションでは、syslog メッセージを IBM Security QRadar に転送するように、syslogd および非暗号化モードの syslog-ng を構成する手順について説明します。

このタスクについて

暗号化 syslog-ng を使用している場合は、*Extreme* の資料 を参照してください。

syslog-ng と syslogd の両方を同時に実行しないでください。

非暗号化モードの syslog-ng を構成するには、以下のようにします。

手順

1. EMS システムで以下のファイルを開きます。

   ```
   /opt/syslog-ng/etc/syslog-ng.conf
   ```

2. Syslog 通知ルールの **Facility** フィルターを構成します。

   例えば、**facility** として local1 を選択した場合、以下のようにします。

   ```
   filter filt_facility_local1 {facility(local1); };
   ```

3. Syslog 通知ルールの **Level** フィルターを構成します。

   例えば、**level** として notice を選択した場合、以下のようにします。

   ```
   filter filt_level_notice {level(notice); };
   ```

4. QRadar 用に destination ステートメントを構成します。

   例えば、QRadar の IP アドレスが 10.10.1.1 で、syslog ポート 514 を使用する場合、以下を入力します。

   ```
   destination siem { tcp("10.10.1.1" port(514)); };
   ```

5. 以下のように、通知ルールの log ステートメントを追加します。

   ```
   log { source(s_local); filter (filt_facility_local1); filter
   (filt_level_notice); destination(siem); };
   ```

6. ファイルを保存し、syslog-ng を再始動します。

   ```
   cd /etc/rc.d ./rc.syslog-ng stop ./rc.syslog-ng start
   ```

7. Extreme Dragon EMS の構成は完了です。

Extreme Dragon EMS v7.4.0 以下を使用した syslogd の構成

アプライアンスで Dragon Enterprise Management Server (EMS) が v7.4.0 より前のバージョンを使用している場合、IBM Security QRadar などのセキュリティーおよび情報マネージャーにイベントを転送するために syslogd を使用する必要があります。

このタスクについて

syslogd を構成するには、以下を行う必要があります。

手順

1. Dragon EMS システムで以下のファイルを開きます。

   ```
   /etc/syslog.conf
   ```

2. syslog 通知ルールで構成した **facility** および **level** を QRadar に転送するための行を追加します。

   例えば、**facility** として local1 および **level** として notice を定義するには、以下のようにします。

   ```
   local1.notice @<IP address>
   ```

   各部分について以下で説明します。

   <IP address> は、QRadar システムの IP アドレスです。

3. ファイルを保存し、syslogd を再始動します。

   ```
   cd /etc/rc.d ./rc.syslog stop ./rc.syslog start
   ```

   Extreme Dragon EMS の構成は完了です。

Extreme HiGuard Wireless IPS

IBM Security QRadar 用の Extreme HiGuard Wireless IPS DSM は、syslog を使用して、関連するすべてのイベントを記録します。

Extreme HiGuard Wireless IPS デバイスを QRadar で構成する前に、syslog イベントを転送するようにデバイスを構成しておく必要があります。

Enterasys HiGuard の構成

syslog イベントを転送するようにデバイスを構成するには、以下のようにします。

手順

1. HiGuard Wireless IPS ユーザー・インターフェースにログインします。
2. 左側のナビゲーション・ペインで「**Syslog**」をクリックします。これにより、管理サーバーがイベントを指定 syslog レシーバーに送信できるようになります。

   「Syslog 構成 (Syslog Configuration)」ペインが表示されます。

3. 「システム統合状況 **(System Integration Status)**」セクションで、syslog 統合を有効にします。

   syslog 統合を有効にすると、管理サーバーが、構成した syslog サーバーにメッセージを送信できるようになります。デフォルトでは、管理サーバーで syslog は有効になっています。

「現在の状況 **(Current Status)**」フィールドに、syslog サーバーの状況が表示されます。選択項目は「実行中 **(Running)**」または「停止済み **(Stopped)**」です。以下のいずれかが発生した場合、エラー状況が表示されます。

- 構成されていて有効になっている syslog サーバーのいずれかに、解決できないホスト名が含まれている。
- 管理サーバーが停止している。
- 内部エラーが発生した。このエラーが発生した場合は、Enterasys テクニカル・サポートにお問い合わせください。

4. 「**Syslog** サーバーの管理 **(Manage Syslog Servers)**」から、「追加 **(Add)**」をクリックします。

   「Syslog 構成 (Syslog Configuration)」ウィンドウが表示されます。
5. 以下のパラメーターの値を入力します。
   - **Syslog** サーバー **(IP** アドレス**/**ホスト名**) (Syslog Server (IP Address/Hostname))** - イベントが送信される syslog サーバーの IP アドレスまたはホスト名を入力します。

   注**:** 構成した syslog サーバーは、HWMH Config Shell の「サーバーの初期化とセットアップ・ウィザード (Server initialization and Setup Wizard)」で構成された DNS 名および DNS サフィックスを使用します。
   - ポート番号 **(Port Number)** - HWMH がイベントを送信する先の syslog サーバーのポート番号を入力します。デフォルトは 514 です。
   - メッセージ・フォーマット **(Message Format)** - イベントを送信するためのフォーマットとして「プレーン・テキスト **(Plain Text)**」を選択します。
   - 有効にする **(Enabled?)** - イベントを当該 syslog サーバーに送信する場合は、「有効にする **(Enabled?)**」を選択します。
6. 構成を保存します。

   構成は完了です。HiGuard イベントが自動的に検出されると、ログ・ソースが IBM Security QRadar に追加されます。Enterasys HiGuard によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Extreme HiGuard の syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。 Extreme HiGuard のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Extreme HiGuard**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *150. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Extreme HiGuard からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Extreme HiPath Wireless Controller

IBM Security QRadar 用の Extreme HiPath Wireless Controller DSM は、syslog を使用して、関連するすべてのイベントを記録します。

QRadar は、以下の Extreme HiPath Wireless Controller イベントをサポートします。

- ワイヤレス・アクセス・ポイント・イベント
- アプリケーション・ログ・イベント
- サービス・ログ・イベント
- 監査ログ・イベント

HiPath Wireless Controller の構成

Extreme HiPath Wireless Controller イベントを IBM Security QRadar と統合するには、syslog イベントを転送するようにデバイスを構成する必要があります。

このタスクについて

syslog イベントを QRadar に転送するには、以下のようにします。

手順

1. HiPath Wireless Assistant にログインします。
2. 「**Wireless Controller** の構成 **(Wireless Controller Configuration)**」をクリックします。

   「Wireless Controller の構成 (Wireless Controller Configuration)」ウィンドウが表示されます。
3. メニューで「システム保守 **(System Maintenance)**」をクリックします。

4. 「**Syslog** セクション **(Syslog section)**」から、「**Syslog** サーバー **IP (Syslog Server IP)**」チェック・ボックスを選択し、syslog メッセージを受信するデバイスの IP アドレスを入力します。
5. 「**Wireless Controller** ログ・レベル **(Wireless Controller Log Level)**」リストを使用して、「情報 **(Information**」を選択します。
6. 「**Wireless AP** ログ・レベル **(Wireless AP Log Level)**」リストを使用して、「メジャー **(Major)**」を選択します。
7. 「アプリケーション・ログ **(Application Logs)**」リストを使用して、「**local.0**」を選択します。
8. 「サービス・ログ **(Service Logs)**」リストを使用して、「**local.3**」を選択します。
9. 「監査ログ **(Audit Logs)**」リストを使用して、「**local.6**」を選択します。
10. 「適用」をクリックします。

これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Extreme HiPath からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

このタスクについて

Extreme HiPath のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Extreme HiPath**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 151. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Extreme HiPath からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。Extreme HiPath Wireless Controller デバイスについて詳しくは、ベンダーの資料を参照してください。

Extreme Matrix Router

IBM Security QRadar 用の Extreme Matrix Router DSM は、SNMPv1、SNMPv2、SNMPv3、および syslog を使用して、Extreme Matrix イベントを受け入れます。

このタスクについて

Extreme Matrix Router バージョン 3.5 を QRadar と統合できます。QRadar は、すべての SNMP イベント、syslog のログイン、ログアウト、およびログイン失敗の各イベントを記録します。Extreme Matrix と統合するように QRadar を構成する前に、以下の手順を実行する必要があります。

手順

1. 特権ユーザーとしてスイッチ/ルーターにログインします。
2. 以下のコマンドを入力します。

   `set logging server <server number> description <description> facility <facility> ip_addr <IP address> port <port> severity <severity>` 各部分について以下で説明します。

   - *<server number>* は、1 から 8 の値のサーバー番号です。
   - *<description>* は、サーバーの説明です。
   - *<facility>* は、syslog ファシリティーです (例えば、local0)。
   - *<IP address>* は、syslog メッセージを受信するサーバーの IP アドレスです。
   - *<port>* は、クライアントがサーバーへのメッセージの送信に使用するデフォルト UDP ポートです。別途記載がない限り、ポート 514 を使用してください。
   - *<severity>* は、値が 1 から 9 のサーバー重大度レベルです。1 は緊急を指示し、8 はデバッグ・レベルです。

   例えば、以下のようにします。

   ```
   set logging server 5 description ourlogserver facility local0 ip_addr
   1.2.3.4 port 514 severity 8
   ```

3. これで、QRadar でログ・ソースを構成する準備ができました。

   「ログ・ソース・タイプ」リストで「**Extreme Matrix E1** スイッチ」を選択します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Extreme Matrix K/N/S シリーズ・スイッチ

IBM Security QRadar 用の Extreme Matrix シリーズの DSM は、syslog を使用してイベントを受け入れます。QRadar は、該当するすべての Matrix K シリーズ、N シリーズ、または S シリーズのスタンドアロン・デバイスのイベントを記録します。

このタスクについて

Matrix K シリーズ、N シリーズ、または S シリーズと統合するように QRadar を構成する前に、以下の手順を実行します。

手順

1. Extreme Matrix デバイスのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力します。
   a. `set logging server 1 ip-addr <IP Address of Event Processor> state enable`
   b. `set logging application RtrAcl level 8`
   c. `set logging application CLI level 8`
   d. `set logging application SNMP level 8`
   e. `set logging application Webview level 8`
   f. `set logging application System level 8`
   g. `set logging application RtrFe level 8`
   h. `set logging application Trace level 8`
   i. `set logging application RtrLSNat level 8`
   j. `set logging application FlowLimt level 8`
   k. `set logging application UPN level 8`
   l. `set logging application AAA level 8`
   m. `set logging application Router level 8`
   n. `set logging application AddrNtfy level 8`
   o. `set logging application OSPF level 8`
   p. `set logging application VRRP level 8`
   q. `set logging application RtrArpProc level 8`
   r. `set logging application LACP level 8`
   s. `set logging application RtrNat level 8`
   t. `set logging application RtrTwcb level 8`
   u. `set logging application HostDoS level 8`
   v. `set policy syslog extended-format enable`

   Matrix シリーズのルーターやスイッチの構成について詳しくは、ベンダーの資料を参照してください。
3. これで、QRadar でログ・ソースを構成する準備ができました。

Extreme Matrix シリーズのデバイスからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**Extreme Matrix K/N/S**シリーズ・スイッチ」を選択します。

関連タスク:

5 ページの『ログ・ソースの追加』

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Extreme NetSight Automatic Security Manager

IBM Security QRadar 用の Extreme NetSight Automatic Security Manager DSM は、syslog を使用してイベントを受け入れます。

このタスクについて

QRadar は、関連するすべてのイベントを記録します。QRadar で Extreme NetSight Automatic Security Manager デバイスを構成する前に、syslog イベントを転送するようにデバイスを構成しておく必要があります。

Syslog イベントを QRadar に送信するようにデバイスを構成するには、以下のようにします。

手順

1. Automatic Security Manager ユーザー・インターフェースにログインします。
2. 「自動化セキュリティー・マネージャー **(Automated Security Manager)**」アイコンをクリックして、「自動化セキュリティー・マネージャーの構成 (Automated Security Manager Configuration)」ウィンドウにアクセスします。

   注**:** 「自動化セキュリティー・マネージャーの構成 (Automated Security Manager Configuration)」ウィンドウには、「ツール **(Tool)**」メニューからもアクセスできます。
3. 左側のナビゲーションで「ルール定義 **(Rule Definitions)**」を選択します。
4. 次のオプションのいずれかを選択してください。

   ルールを構成する場合、ルールを強調表示します。「編集」をクリックします。
5. 新規ルールを作成するために、「作成 **(Create)**」をクリックします。
6. 「通知 **(Notifications)**」チェック・ボックスを選択します。
7. 「編集」をクリックします。

   「通知の編集 (Edit Notifications)」ウィンドウが表示されます。
8. 「作成」をクリックします。

   「通知の作成 (Create Notification)」ウィンドウが表示されます。
9. 「タイプ **(Type)**」リストを使用して、「**Syslog**」を選択します。

10. 「**Syslog** サーバーの **IP/**名前 **(Syslog Server IP/Name)**」フィールドに、syslog トラフィックを受信するデバイスの IP アドレスを入力します。
11. 「適用」をクリックします。
12. 「閉じる **(Close)**」をクリックします。
13. 「通知 **(Notification)**」リストで、構成した通知を選択します。
14. 「**OK**」をクリックします。
15. これで、QRadar でログ・ソースを構成する準備ができました。

Extreme NetSight Automatic Security Manager デバイスからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**Extreme NetsightASM**」を選択します。

Extreme NetSight Automatic Security Manager デバイスについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Extreme NAC

IBM Security QRadar 用の Extreme NAC DSM は、syslog を使用してイベントを受け入れます。QRadar は、関連するすべてのイベントを記録します。

syslog 用の Extreme NAC アプライアンスの構成について詳しくは、ベンダー資料を参照してください。Extreme NAC アプライアンスが syslog イベントを QRadar に転送したら、構成は完了です。Extreme NAC イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Extreme NAC アプライアンスによって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Extreme NAC からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。 Extreme NAC のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。

7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Extreme NAC**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *152. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Extreme NAC アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Extreme スタック可能スイッチおよびスタンドアロン・スイッチ

IBM Security QRadar 用の Extreme スタック可能スイッチおよびスタンドアロン・スイッチの DSM は、syslog を使用してイベントを受け入れます。

このタスクについて

QRadar は、関連するすべてのイベントを記録します。QRadar で Extreme スタック可能スイッチおよびスタンドアロン・スイッチのデバイスを構成する前に、syslog イベントを転送するようにデバイスを構成しておく必要があります。

syslog イベントを QRadar に転送するようデバイスを構成するには、以下のようにします。

手順

1. Extreme スタック可能スイッチおよびスタンドアロン・スイッチのデバイスにログインします。
2. 以下のコマンドを入力します。

   `set logging server <index> [ip-addr <IP address>] [facility <facility>] [severity <severity>] [descr <description>] [port <port] [state <enable | disable>]` 各部分について以下で説明します。

   - *<index>* は、当該サーバーのサーバー表索引番号 (1 から 8) です。
   - *<IP address>* は、syslog メッセージを送信するサーバーの IP アドレスです。IP アドレスの入力は必須ではありません。IP アドレスを定義しなかった場合、指定した索引番号を使用して Syslog サーバー表内の項目が作成され、IP アドレスが割り当てられていないことを示すメッセージが表示されます。
   - *<facility>* は、syslog ファシリティーです。有効な値は、local0 から local7 です。ファシリティー値の入力は必須ではありません。値を指定しなかった場合、**set logging** デフォルト・コマンドで構成されたデフォルト値が適用されます。

- <*description*> は、ファシリティー/サーバーの説明です。説明の入力は必須ではありません。
- <*port*> は、クライアントがサーバーへのメッセージの送信に使用するデフォルト UDP ポートです。指定しなかった場合、**set logging** デフォルト・コマンドで構成されたデフォルト値が適用されます。ポート値の入力は必須ではありません。
- <enable | disable> により、当該ファシリティー/サーバー構成を有効または無効にします。オプションの選択は必須ではありません。状態を指定しなかった場合、enable と disable のいずれにもデフォルトで設定されません。
- <*severity*> は、サーバーがメッセージをログに記録するサーバー重大度レベルです。有効な範囲は、1 から 8 です。指定しなかった場合、**set logging** デフォルト・コマンドで構成されたデフォルト値が適用されます。重大度値の入力は必須ではありません。以下に、有効な値を示します。
- 1: 緊急 (システムが使用不可)
- 2: アラート (即時アクションが必要)
- 3: 重大な状態
- 4: エラー状態
- 5: 警告状態
- 6: 通知 (有意状態)
- 7: 情報メッセージ
- 8: デバッグ・メッセージ

3. これで、QRadar でログ・ソースを構成する準備ができました。

Extreme スタック可能スイッチおよびスタンドアロン・スイッチのデバイスからイベントを受信するように QRadar を構成するには、以下のようにします。

「ログ・ソース・タイプ」リストで、以下のいずれかのオプションを選択します。

- **Extreme** スタック可能スイッチおよびスタンドアロン・スイッチ
- **Extreme A** シリーズ
- **Extreme B2** シリーズ
- **Extreme B3** シリーズ
- **Extreme C2** シリーズ
- **Extreme C3** シリーズ
- **Extreme D** シリーズ
- **Extreme G** シリーズ
- **Extreme I** シリーズ

Extreme スタック可能スイッチおよびスタンドアロン・スイッチについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプラ

イアンスからイベントを受信するログ・ソースを手動で追加できます。

Extreme Networks ExtremeWare

IBM Security QRadar 用の Extreme Networks ExtremeWare DSM は、syslog を使用して、関連するすべてのイベント (Extreme Networks の ExtremeWare デバイスおよび Extremeware XOS デバイスのイベント) を記録します。

QRadar を ExtremeWare デバイスと統合するには、ログ・ソースを QRadar で構成してから、syslog イベントを転送するように Extreme Networks の ExtremeWare デバイスおよび Extremeware XOS デバイスを構成します。QRadar は、ExtremeWare アプライアンスからの syslog イベントに対して、ログソースを自動的に検出および作成することはありません。

ログ・ソースの構成

IBM Security QRadar と統合するには、QRadar に転送された受信 ExtremeWare イベントを受け取るためのログ・ソースを手動で作成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Extreme Networks ExtremeWare** オペレーティング・システム **(OS)**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 153. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	ExtremeWare アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。 Extreme Networks ExtremeWare アプライアンスによって QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

Extremeware アプライアンス用の syslog 転送の構成については、ベンダーの資料を参照してください。

Extreme XSR Security Router

IBM Security QRadar 用の Extreme XSR Security Router DSM は、syslog を使用してイベントを受け入れます。

このタスクについて

QRadar は、関連するすべてのイベントを記録します。QRadar で Extreme XSR Security Router を構成する前に、syslog イベントを転送するようにデバイスを構成しておく必要があります。

syslog イベントを QRadar に送信するようにデバイスを構成するには、以下のようにします。

手順

1. Telnet または SSH を使用して、XSR Security Router のコマンド・ライン・インターフェースにログインします。
2. 以下のコマンドを入力して、構成モードにアクセスします。
   a. `enable`
   b. `config`
3. 以下のコマンドを入力します。

   ```
   logging <IP address> low
   ```

   ここで、<*IP address*> は、QRadar の IP アドレスです。
4. 構成モードを終了します。

   ```
   exit
   ```
5. 以下のように、構成を保存します。

   ```
   copy running-config startup-config
   ```
6. これで、QRadar でログ・ソースを構成する準備ができました。

   「ログ・ソース・タイプ」リストで「**Extreme XSR Security Router**」を選択します。

   Extreme XSR Security Router について詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 48 章 F5 Networks

IBM Security QRadar は、さまざまな F5 Networks DSM からイベントを受け入れます。

F5 Networks BIG-IP AFM

IBM Security QRadar 用の F5 Networks BIG-IP Advanced Firewall Manager (AFM) DSM は、F5 Networks BIG-IP AFM システムから名前と値のペアのフォーマットで転送された syslog イベントを受け入れます。

このタスクについて

QRadar は、Advanced Firewall Manager が含まれている F5 BIG-IP アプライアンスから以下のイベントを収集できます。

- ネットワーク・イベント
- ネットワークのサービス妨害 (DoS) イベント
- プロトコル・セキュリティー・イベント
- DNS イベント
- DNS のサービス妨害 (DoS) イベント

Advanced Firewall Manager を構成する前に、BIG-IP アプライアンスがライセンス交付を受けていて、Advanced Firewall Manager を含めるようにプロビジョンされていることを確認する必要があります。

手順

1. BIG-IP アプライアンスの管理インターフェースにログインします。
2. ナビゲーション・メニューで「システム **(System)**」 > 「ライセンス **(License)**」を選択します。
3. 「ライセンスの状況 **(License Status)**」列で、Advanced Firewall Manager がライセンス交付を受けていて有効になっていることを確認します。
4. Advanced Firewall Manager を有効にするには、「システム **(System)**」 > 「リソース **(Resource)**」 > 「プロビジョニング **(Provisioning)**」を選択します。
5. 「プロビジョニング **(Provisioning)**」列で、チェック・ボックスを選択し、リストから「公称 **(Nominal)**」を選択します。
6. 「送信 **(Submit)**」をクリックして変更を保存します。

ロギング・プールの構成

ロギング・プールを使用して、syslog イベントを受信するサーバーのプールを定義します。プールには、指定した IP アドレス、ポート、およびノード名が含まれます。

手順

1. ナビゲーション・メニューで「ローカル・トラフィック **(Local Traffic)**」 > 「プール **(Pools)**」 を選択します。
2. 「作成」をクリックします。
3. 「名前 **(Name)**」フィールドに、ロギング・プールの名前を入力します。

   例: Logging_Pool
4. 「ヘルス・モニター **(Health Monitor)**」フィールドの「使用可能 **(Available)**」リストで「**TCP**」を選択し、「**<<**」をクリックします。

   このクリック・アクションにより、「TCP」オプションが「使用可能 (Available)」リストから「選択済み (Selected)」リストに移動します。
5. 「リソース (Resource)」ペインの「ノード名 **(Node Name)**」リストで、「**Logging_Node**」または 371 ページの『ロギング・プールの構成』で定義した名前を選択します。
6. 「アドレス **(Address)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
7. 「サービス・ポート **(Service Port)**」フィールドに 514 と入力します。
8. 「追加」をクリックします。
9. 「終了」をクリックします。

高速ログ宛先の作成

BIG-IP AFM 用にロギングを構成するプロセスでは、高速ロギング宛先を作成する必要があります。

手順

1. ナビゲーション・メニューで「システム **(System)**」 > 「ログ **(Logs)**」 > 「構成 **(Configuration)**」 > 「ログ宛先 **(Log Destinations)**」を選択します。
2. 「作成」をクリックします。
3. 「名前 **(Name)**」フィールドに、宛先の名前を入力します。

   例: Logging_HSL_dest
4. 「説明 **(Description)**」フィールドに説明を入力します。
5. 「タイプ **(Type)**」リストから「リモート高速ログ **(Remote High-Speed Log)**」を選択します。
6. 「プール名 **(Pool Name)**」リストで、リモート・ログ・サーバーのリストからロギング・プールを選択します。

   例: Logging_Pool
7. 「プロトコル **(Protocol)**」リストから「**TCP**」を選択します。
8. 「終了」をクリックします。

フォーマット設定されたログ宛先の作成

フォーマット設定されたログ宛先を使用して、高速ロギング宛先に転送されるイベントで必要とされる特殊フォーマットを指定します。

手順

1. ナビゲーション・メニューで「システム **(System)**」 > 「ログ **(Logs)**」 > 「構成 **(Configuration)**」 > 「ログ宛先 **(Log Destinations)**」を選択します。
2. 「作成」をクリックします。
3. 「名前 **(Name)**」フィールドに、ロギング・フォーマット宛先の名前を入力します。

   例: Logging_Format_dest
4. 「説明 **(Description)**」フィールドに説明を入力します。
5. 「タイプ **(Type)**」リストから「リモート **Syslog (Remote Syslog)**」を選択します。
6. 「**Syslog** フォーマット **(Syslog Format)**」リストから「**Syslog**」を選択します。
7. 「高速ログ宛先 **(High-Speed Log Destination)**」リストから高速ロギング宛先を選択します。

   例: Logging_HSL_dest
8. 「終了 **(Finished)**」をクリックします。

ログ・パブリッシャーの作成

パブリッシャーを作成すると、BIG-IP アプライアンスがフォーマット設定されたログ・メッセージをローカル syslog データベースにパブリッシュできるようになります。

手順

1. ナビゲーション・メニューで「システム **(System)**」 > 「ログ **(Logs)**」 > 「構成 **(Configuration)**」 > 「ログ・パブリッシャー **(Log Publishers)**」を選択します。
2. 「作成」をクリックします。
3. 「名前 **(Name)**」フィールドに、パブリッシャーの名前を入力します。

   例: Logging_Pub
4. 「説明 **(Description)**」フィールドに説明を入力します。
5. 「宛先 **(Destinations)**」フィールドの「使用可能 (Available)」リストで、 371 ページの『ロギング・プールの構成』で作成したログ宛先名を選択し、「**<<**」をクリックして項目を「選択済み (Selected)」リストに追加します。

   このクリック・アクションにより、ロギング・フォーマット宛先が「使用可能 (Available)」リストから「選択済み (Selected)」リストに移動します。パブリッシャー構成にローカル・ロギングを含めるために、「**local-db**」および「**local-syslog**」を「選択済み (Selected)」リストに追加できます。

ロギング・プロファイルの作成

ロギング・プロファイルを使用して、Advanced Firewall Manager が生成するイベントのタイプを構成し、これらのイベントをロギング宛先に関連付けます。

手順

1. ナビゲーション・メニューで「セキュリティー **(Security)**」 > 「イベント・ログ **(Event Logs)**」 > 「ロギング・プロファイル **(Logging Profile)**」を選択します。
2. 「作成」をクリックします。
3. 「名前 **(Name)**」フィールドに、ログ・プロファイルの名前を入力します。

   例: Logging_Profile
4. 「ネットワーク・ファイアウォール **(Network Firewall)**」フィールドで「有効 **(Enabled)**」チェック・ボックスを選択します。
5. 「パブリッシャー **(Publisher)**」リストから、構成したログ・パブリッシャーを選択します。

   例: Logging_Pub
6. 「ログ・ルールのマッチング **(Log Rule Matches)**」フィールドで、「受け入れ **(Accept)**」、「除去 **(Drop)**」、および「拒否 **(Reject)**」の各チェック・ボックスを選択します。
7. 「**Log IP** エラー **(Log IP Errors)**」フィールドで「有効 **(Enabled)**」チェック・ボックスを選択します。
8. 「**Log TCP** エラー **(Log TCP Errors)**」フィールドで「有効 **(Enabled)**」チェック・ボックスを選択します。
9. 「**Log TCP** イベント **(Log TCP Events)**」フィールドで「有効 **(Enabled)**」チェック・ボックスを選択します。
10. 「ストレージ・フォーマット **(Storage Format)**」フィールドのリストから「フィールド・リスト **(Field-List)**」を選択します。
11. 「区切り文字 **(Delimiter)**」フィールドに、イベントの区切り文字として **,** (コンマ) を入力します。
12. 「ストレージ・フォーマット **(Storage Format)**」フィールドで、「使用可能な項目 **(Available Items)**」リストのすべてのオプションを選択し、「**<<**」をクリックします。

    このクリック・アクションにより、すべての「フィールド・リスト (Field-List)」オプションが「使用可能 **(Available)**」リストから「選択済み **(Selected)**」リストに移動します。
13. 「IP インテリジェンス (IP Intelligence)」ペインの「パブリッシャー **(Publisher)**」リストから、構成したログ・パブリッシャーを選択します。

    例: Logging_Pub
14. 「終了 **(Finished)**」をクリックします。

仮想サーバーへのプロファイルの関連付け

作成したログ・プロファイルは、「セキュリティー・ポリシー **(Security Policy)**」タブで仮想サーバーに関連付ける必要があります。この関連付けにより、仮想サーバーがローカル・トラフィックとともにネットワーク・ファイアウォール・イベントを処理できるようになります。

このタスクについて

以下の手順を実行して、プロファイルを仮想サーバーに関連付けます。

手順

1. ナビゲーション・メニューで「ローカル・トラフィック **(Local Traffic)**」 > 「仮想サーバー **(Virtual Servers)**」を選択します。
2. 変更する仮想サーバーの名前をクリックします。
3. 「セキュリティー **(Security)**」タブで「ポリシー **(Policies)**」を選択します。
4. 「ログ・プロファイル **(Log Profile)**」リストから「有効 **(Enabled)**」を選択します。
5. 「プロファイル **(Profile)**」フィールドの「使用可能 **(Available)**」リストで「ロギング・プロファイル **(Logging_Profile)**」または 373 ページの『ロギング・プロファイルの作成』で指定した名前を選択し、「**<<**」をクリックします。

   このクリック・アクションにより、「ロギング・プロファイル (Logging_Profile)」オプションが「使用可能 **(Available)**」リストから「選択済み **(Selected)**」リストに移動します。
6. 「更新 **(Update)**」をクリックして変更を保存します。

   構成は完了です。F5 Networks BIG-IP AFM の syslog イベントが自動的に検出されると、ログ・ソースが IBM Security QRadar に追加されます。F5 Networks BIG-IP AFM によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、F5 Networks BIG-IP AFM の syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ただし、QRadar 用のログ・ソースを手動で作成して syslog イベントを受信することもできます。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**F5 Networks BIG-IP AFM**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *154. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	F5 BIG-IP AFM アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

F5 Networks BIG-IP APM

IBM Security QRadar 用の F5 Networks BIG-IP Access Policy Manager (APM) DSM は、syslog を使用して、BIG-IP APM デバイスからアクセス・イベントおよび認証セキュリティー・イベントを収集します。

syslog イベントをリモート syslog ソースに転送するように BIG-IP LTM デバイスを構成するには、BIG-IP APM ソフトウェアの以下のバージョンを選択します。

- 『F5 BIG-IP APM 11.x 用のリモート syslog の構成』
- 377 ページの『F5 BIG-IP APM 10.x 用のリモート syslog の構成』

F5 BIG-IP APM 11.x 用のリモート syslog の構成

F5 BIG-IP APM 11.x 用に syslog を構成できます。

このタスクについて

F5 BIG-IP APM 11.x 用にリモート syslog を構成するには、以下の手順を実行します。

手順

1. F5 BIG-IP デバイスのコマンド・ラインにログインします。
2. 以下のコマンドを入力して、単一のリモート syslog サーバーを追加します。

   `tmsh syslog remote server {<Name> {host <IP address>}}` 各部分について以下で説明します。

   - *<Name>* は、F5 BIG-IP APM syslog ソースの名前です。
   - *<IP address>* は、QRadar コンソールの IP アドレスです。

   例:

   ```
   bigpipe syslog remote server {BIGIP_APM {host 10.100.100.101}}
   ```
3. 以下を入力して、構成変更を保存します。

   ```
   tmsh save sys config partitions all
   ```

   構成は完了です。F5 Networks BIG-IP APM の イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。F5 Networks BIG-IP APM によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

F5 BIG-IP APM 10.x 用のリモート syslog の構成

F5 BIG-IP APM 10.x 用に syslog を構成できます。

このタスクについて

F5 BIG-IP APM 10.x 用にリモート syslog を構成するには、以下の手順を実行します。

手順

1. F5 BIG-IP デバイスのコマンド・ラインにログインします。
2. 以下のコマンドを入力して、単一のリモート syslog サーバーを追加します。

   `bigpipe syslog remote server {<Name> {host <IP address>}}` 各部分について以下で説明します。

   - *<Name>* は、F5 BIG-IP APM syslog ソースの名前です。
   - *<IP address>* は、QRadar コンソールの IP アドレスです。

   例:

   ```
   bigpipe syslog remote server {BIGIP_APM {host 10.100.100.101}}
   ```

3. 以下を入力して、構成変更を保存します。

   ```
   bigpipe save
   ```

   構成は完了です。F5 Networks BIG-IP APM の イベントが自動的に検出されると、ログ・ソースが IBM Security QRadar に追加されます。F5 Networks BIG-IP APM によって QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、F5 Networks BIG-IP APM アプライアンスの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**F5 Networks BIG-IP APM**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

10. 以下の値を構成します。

syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	F5 Networks BIG-IP APM アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

F5 Networks BIG-IP ASM の構成

IBM Security QRadar F5 Networks BIG-IP Application Security Manager (ASM) DSM は、syslog を使用して、BIG-IP ASM アプライアンスから Web アプリケーション・セキュリティー・イベントを収集します。

このタスクについて

syslog イベントを F5 Networks BIG-IP ASM アプライアンスから QRadar に転送するには、ロギング・プロファイルを構成する必要があります。

ロギング・プロファイルを使用して、syslog イベント用のリモート・ストレージを構成できます。syslog イベントは、QRadar に直接転送できます。

手順

1. F5 Networks BIG-IP ASM アプライアンスのユーザー・インターフェースにログインします。
2. ナビゲーション・ペインで「アプリケーション・セキュリティー **(Application Security)**」 > 「オプション **(Options)**」 を選択します。
3. 「ロギング・プロファイル **(Logging Profiles)**」をクリックします。
4. 「作成」をクリックします。
5. 「構成 **(Configuration)**」リストから「拡張 **(Advanced)**」を選択します。
6. 「プロファイル名」プロパティーの記述名を入力します。
7. オプション: 「プロファイルの説明」を入力します。

   ローカルとリモートの両方にデータを記録しない場合は、「ローカル・ストレージ **(Local Storage)**」チェック・ボックスをクリアします。
8. 「リモート・ストレージ **(Remote Storage)**」チェック・ボックスを選択します。
9. 「タイプ **(Type)**」リストから「レポート作成サーバー **(Reporting Server)**」を選択します。
10. 「プロトコル **(Protocol)**」リストから「**TCP**」を選択します。
11. 「**IP** アドレス」フィールドに QRadar コンソールの IP アドレスを入力し、「ポート」フィールドにポート値 514 を入力します。

12. 「ロギングを保証する **(Guarantee Logging)**」チェック・ボックスを選択します。

    注**:** 「ロギングを保証する **(Guarantee Logging)**」オプションを有効にすると、ロギング・ユーティリティーがシステム・リソースについて競合している場合でも、システム・ログ要求が Web アプリケーションに対して確実に続行します。「ロギングを保証する **(Guarantee Logging)**」オプションを有効にすると、関連 Web アプリケーションへのアクセスが遅くなることがあります。
13. 「検出された異常を報告 **(Report Detected Anomalies)**」チェック・ボックスを選択して、システムが詳細をログに記録できるようにします。
14. 「作成」をクリックします。

    最新表示が行われ、新しいロギング・プロファイルが示されます。F5 Networks BIG-IP ASM のイベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。F5 Networks BIG-IP ASM によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、F5 Networks BIG-IP ASM アプライアンスの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**F5 Networks BIG-IP ASM**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 155. syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	F5 Networks BIG-IP ASM アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

F5 Networks BIG-IP LTM

IBM Security QRadar 用の F5 Networks BIG-IP Local Traffic Manager (LTM) DSM は、syslog を使用して、BIG-IP デバイスからネットワーク・セキュリティー・イベントを収集します。

QRadar でイベントを受信するには、QRadar でログ・ソースを構成してから、syslog イベントを転送するように BIG-IP LTM デバイスを構成する必要があります。QRadar は、F5 BIG-IP LTM アプライアンスからの syslog イベントに対して、ログソースを自動的に検出および作成することはないため、イベントが転送される前に、ログ・ソースを作成しておきます。

ログ・ソースの構成

F5 BIG-IP LTM を IBM Security QRadar と統合するには、ログ・ソースを手動で作成して syslog イベントを受信する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**F5 Networks BIG-IP LTM**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 156. syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	BIG-IP LTM アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

これで、syslog イベントを QRadar に転送するように BIG-IP LTM アプライアンスを構成する準備ができました。

BIG-IP LTM での syslog 転送の構成

syslog イベントを転送するように BIG-IP LTM デバイスを構成できます。

以下の BIG-IP LTM ソフトウェアのバージョンで syslog を構成できます。

- 『F5 BIG-IP LTM 11.x 用のリモート syslog の構成』
- 『F5 BIG-IP LTM 10.x 用のリモート syslog の構成』
- 382 ページの『F5 BIG-IP LTM 9.4.2 から 9.4.8 用のリモート syslog の構成』

F5 BIG-IP LTM 11.x 用のリモート syslog の構成

F5 BIG-IP LTM 11.x 用に syslog を構成できます。

このタスクについて

F5 BIG-IP LTM 11.x 用に syslog を構成するには、以下の手順を実行します。

手順

1. F5 BIG-IP デバイスのコマンド・ラインにログインします。
2. Traffic Management Shell (tmsh) にログインするために、以下のコマンドを入力します。

   ```
   tmsh
   ```

3. syslog サーバーを追加するために、以下のコマンドを入力します。

   ```
   modify /sys syslog remote-servers add {<Name> {host <IP address>
   remote-port 514}}
   ```

   各部分について以下で説明します。

   - <*Name*> は、BIG-IP LTM アプライアンスで syslog サーバーを識別するために割り当てる名前です。
   - <*IP address*> は、IBM Security QRadar の IP アドレスです。

   例:

   ```
   modify /sys syslog remote-servers add {BIGIPsyslog {host 10.100.100.100
   remote-port 514}}
   ```

4. 以下のように、構成変更を保存します。

   ```
   save /sys config
   ```

   F5 Networks BIG-IP LTM アプライアンスから転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

F5 BIG-IP LTM 10.x 用のリモート syslog の構成

F5 BIG-IP LTM 10.x 用に syslog を構成できます。

このタスクについて

F5 BIG-IP LTM 10.x 用に syslog を構成するには、以下の手順を実行します。

手順

1. F5 BIG-IP デバイスのコマンド・ラインにログインします。
2. 以下のコマンドを入力して、単一のリモート syslog サーバーを追加します。

`bigpipe syslog remote server {<Name> {host <IP address>}}` 各部分について以下で説明します。

- *<Name>* は、F5 BIG-IP LTM syslog ソースの名前です。
- *<IP address>* は、IBM Security QRadar の IP アドレスです。

例:

```
bigpipe syslog remote server {BIGIPsyslog {host 10.100.100.100}}
```

3. 以下のように、構成変更を保存します。

```
bigpipe save
```

注: F5 Networks により、BIG-IP v10.x の syslog 出力フォーマットが変更され、syslog ヘッダーのホスト名の前に `local/` の使用が組み込まれました。`local/` が含まれている syslog ヘッダー・フォーマットは QRadar ではサポートされませんが、syslog ヘッダーを修正する回避策が使用可能です。詳しくは、http://www.ibm.com/support を参照してください。

F5 Networks BIG-IP LTM アプライアンスから転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

F5 BIG-IP LTM 9.4.2 から 9.4.8 用のリモート syslog の構成

F5 BIG-IP LTM 9.4.2 から 9.4.8 用に syslog を構成できます。

このタスクについて

F5 BIG-IP LTM 9.4.2 から 9.4.8 用に syslog を構成するには、以下の手順を実行します。

手順

1. F5 BIG-IP デバイスのコマンド・ラインにログインします。
2. 以下のコマンドを入力して、単一のリモート syslog サーバーを追加します。

```
bigpipe syslog remote server <IP address>
```

ここで、*<IP address>* は IBM Security QRadar の IP アドレスです。 例えば、以下のようにします。

```
bigpipe syslog remote server 10.100.100.100
```

3. 以下を入力して、構成変更を保存します。

```
bigpipe save
```

構成は完了です。F5 Networks BIG-IP LTM アプライアンスから転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

F5 Networks FirePass

IBM Security QRadar 用の F5 Networks FirePass DSM は、syslog を使用して、F5 FirePass SSL VPN デバイスからシステム・イベントを収集します。

F5 Networks FirePass デバイスでは、デフォルトでリモート・ロギングが無効になっており、有効にする必要があります。QRadar でイベントを受信するには、システム・イベントをリモート syslog サーバーとして QRadar に転送するように F5 Networks FirePass デバイスを構成する必要があります。

F5 FirePass 用の syslog 転送の構成

syslog イベントを F5 Networks BIG-IP FirePass SSL VPN アプライアンスから IBM Security QRadar に転送するには、リモート・ログ・サーバーを構成して有効にする必要があります。

このタスクについて

リモート・ログ・サーバーは、QRadar コンソールまたはデプロイメント内の任意のイベント・コレクター (Event Collector)にイベントを直接転送できます。

手順

1. F5 Networks FirePass 管理コンソールにログインします。
2. ナビゲーション・ペインで「デバイス管理 **(Device Management)**」 > 「保守 **(Maintenance)**」 > 「ログ **(Logs)**」を選択します。
3. 「システム・ログ **(System Logs)**」メニューで「リモート・ログ・サーバーを有効にする **(Enable Remote Log Server)**」チェック・ボックスを選択します。
4. 「システム・ログ **(System Logs)**」メニューで「拡張システム・ログを有効にする **(Enable Extended System Logs)**」チェック・ボックスをクリアします。
5. 「リモート・ホスト **(Remote host)**」パラメーターに、QRadarの IP アドレスまたはホスト名を入力します。
6. 「ログ・レベル **(Log Level)**」リストから「情報 **(Information)**」を選択します。

   「ログ・レベル **(Log Level)**」パラメーターは、アプリケーション・レベルのシステム・メッセージをモニターします。
7. 「カーネル・ログ・レベル **(Kernel Log Level)**」リストから「情報 **(Information)**」を選択します。

   「カーネル・ログ・レベル **(Kernel Log Level)**」パラメーターは、Linux カーネル・システム・メッセージをモニターします。
8. 「システム・ログの変更を適用 **(Apply System Log Changes)**」をクリックします。

   変更が適用され、構成は完了です。F5 Networks FirePass のイベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。F5 Networks BIG-IP ASM によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、F5 Networks FirePass アプライアンスの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**F5 Networks FirePass**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *157. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	F5 Networks FirePass アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 49 章 Fair Warning

IBM Security QRadar 用の Fair Warning DSM は、ログ・ファイル・プロトコルを使用して、リモート・ソースからイベント・ファイルを取得します。

QRadar は、患者のプライバシーや医療記録に対するセキュリティーの脅威に関連するユーザー・アクティビティーについての Fair Warning ログ・ファイルからイベント・カテゴリーを記録します。Fair Warning からログ・ファイルを取得するには、イベント・ログを生成するようにデバイスが構成されていることを確認する必要があります。イベント・ログを生成するための手順は、*Fair Warning* の資料 で確認できます。

ログ・ファイル・プロトコルの構成時には、Fair Warning システムに構成されたホスト名または IP アドレスが、ログ・ファイル・プロトコル構成内の **Remote Host** パラメーターで構成されたものと同じであることを確認します。

ログ・ソースの構成

Fair Warning デバイスからイベント・ログをダウンロードするように IBM Security QRadar を構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リスト・ボックスで、「**Fair Warning**」を選択します。
9. 「プロトコル構成」リストから「ログ・ファイル」オプションを選択します。
10. 「**FTP** ファイル・パターン」フィールドに、Fair Warning システムで生成されるログ・ファイルに一致する正規表現を入力します。
11. 「リモート・ディレクトリー」フィールドに、Fair Warning デバイスからのログが含まれるディレクトリーのパスを入力します。
12. 「イベント・ジェネレーター **(Event Generator)**」リストで、「**Fair Warning**」を選択します。
13. 「保存」をクリックします。
14. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。ログ・ファイル・プロトコルの完全なパラメーターについて詳しくは、「*IBM Security QRadar IBM Security QRadar Managing Log Sources Guide*」を参照してください。

Fair Warning の構成について詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 50 章 Fidelis XPS

IBM Security QRadar 用の Fidelis XPS DSM は、syslog を使用して、Fidelis XPS アプライアンスからログ・イベント拡張フォーマット (LEEF) で転送されるイベントを受け入れます。

QRadar は、Fidelis XPS アプライアンスに構成されたポリシー違反およびルール違反でトリガーされる、関連するすべてのアラートを収集できます。

イベント・タイプ・フォーマット

イベントをログ・イベント拡張フォーマット (LEEF) で生成し、syslog を使用して転送するように、Fidelis XPS を構成する必要があります。LEEF 形式は、syslog ヘッダー (パイプ (|) 区切り) とイベント・ペイロード (タブ区切りフィールド) から構成されます。

Fidelis XPS から転送される syslog イベントが LEEF 形式でない場合は、デバイス構成またはソフトウェアのバージョンを調べて、アプライアンスが LEEF をサポートしていることを確認してください。 LEEF イベント・メッセージは、適切にフォーマットされていると、自動的に検出され、ログ・ソースとして QRadar に追加されます。

Fidelis XPS の構成

Fidelis XPS アプライアンスからのアラートの syslog 転送を構成できます。

手順

1. CommandPost にログインして、Fidelis XPS アプライアンスを管理します。
2. ナビゲーション・メニューで「システム **(System)**」 > 「エクスポート **(Export)**」を選択します。

   使用可能なエクスポートのリストが表示されます。エクスポート機能の初回使用時には、リストは空です。
3. 次のオプションのいずれかを選択します。
   - 「新規 **(New)**」をクリックして、Fidelis XPS アプライアンス用の新規エクスポートを作成します。
   - エクスポート名の横にある「編集 **(Edit)**」をクリックして、Fidelis XPS アプライアンス上の既存のエクスポートを編集します。

   「エクスポート・エディター (Export Editor)」が表示されます。
4. 「エクスポート方式 **(Export Method)**」リストから「**Syslog LEEF**」を選択します。
5. 「宛先 **(Destination)**」フィールドに、IBM Security QRadar の IP アドレスまたはホスト名を入力します。

   例: `10.10.10.100:::514`

「宛先 **(Destination)**」フィールドでは、非 ASCII 文字はサポートされません。

6. 「アラートのエクスポート **(Export Alerts)**」から、以下のいずれかのオプションを選択します。
   - すべてのアラート **(All alerts)** - すべてのアラートを QRadarにエクスポートする場合は、このオプションを選択します。このオプションはリソースを多く消費し、すべてのアラートをエクスポートするのに時間がかかることがあります。
   - 条件別アラート **(Alerts by Criteria)** - 特定のアラートを QRadar にエクスポートする場合は、このオプションを選択します。このオプションでは、アラート条件を定義できる新規フィールドが表示されます。
7. 「マルウェア・イベントのエクスポート **(Export Malware Events)**」から「なし **(None)**」を選択します。
8. 「エクスポート頻度 **(Export Frequency)**」から「アラート/マルウェアごと **(Every Alert / Malware)**」を選択します。
9. 「名前を付けて保存 **(Save As)**」フィールドに、エクスポートの名前を入力します。
10. 「保存」をクリックします。
11. オプション: イベントが QRadar に転送されていることを確認するために、「今すぐ実行する **(Run Now)**」をクリックできます。

    「今すぐ実行する **(Run Now)**」は、条件で選択されたアラートが Fidelis アプライアンスからエクスポートされていることを確認するためのテスト・ツールとして設計されています。 387 ページの『Fidelis XPS の構成』ですべてのイベントをエクスポートすることを選択した場合、このオプションは使用できません。

    構成は完了です。Fidelis XPS の syslog イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Fidelis XPS によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Fidelis XPS からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ただし、QRadar 用のログ・ソースを手動で作成して syslog イベントを受信することもできます。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。

5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Fidelis XPS**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *158. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Fidelis XPS アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 51 章 FireEye

IBM Security QRadar DSM for FireEye は、ログ・イベント拡張フォーマット (LEEF) および共通イベント・フォーマット (CEF) の Syslog イベントを受け取ります。

この DSM は、FireEye CMS、MPS、EX、AX、NX、FX、および HX の各アプライアンスに適用されます。QRadar は、FireEye アプライアンスから送信されたすべての関連通知アラートを記録します。

以下の表は、FireEye DSM の仕様を示しています。

表 *159. FireEye DSM* の仕様

仕様	値
製造元	FireEye
DSM 名	FireEye MPS
サポートされるバージョン	CMS、MPS、EX、AX、NX、FX、および HX
RPM ファイル名	DSM-FireEyeMPS-*QRadar_version-Build_number*.noarch.rpm
プロトコル	Syslog
QRadar で記録されるイベント・タイプ	すべての関連イベント
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	FireEye Web サイト (www.fireeye.com)

FireEye を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、DSM Common および FireEye MPS RPM をダウンロードして QRadar コンソールにインストールしてください。
2. デプロイメント環境内の FireEye のインスタンスごとに、QRadar にイベントを転送するように FireEye システムを構成します。
3. FireEye のインスタンスごとに、QRadar コンソール上で FireEye のログ・ソースを作成します。

関連タスク:

392 ページの『QRadar との通信用に FireEye HX システムを構成する』
FireEye HX が IBM Security QRadar と通信できるようにするために、Syslog イベントを転送するように FireEye HX アプライアンスを構成します。

392 ページの『QRadar との通信用に FireEye システムを構成する』
FireEye が IBM Security QRadar と通信できるようにするために、Syslog イベントを転送するように FireEye アプライアンスを構成します。

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインスト

ールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に FireEye システムを構成する

FireEye が IBM Security QRadar と通信できるようにするために、Syslog イベントを転送するように FireEye アプライアンスを構成します。

手順

1. CLI を使用して FireEye アプライアンスにログインします。
2. 構成モードをアクティブにするには、以下のコマンドを入力します。

   ```
   enable

   configure terminal
   ```
3. rsyslog 通知を有効にするには、以下のコマンドを入力します。

   ```
   fenotify rsyslog enable
   ```
4. QRadar を rsyslog 通知コンシューマーとして追加するには、以下のコマンドを入力します。

   ```
   fenotify rsyslog trap-sink QRadar
   ```
5. rsyslog トラップ・シンク通知を受信する QRadar システムの IP アドレスを指定するには、以下のコマンドを入力します。

   ```
   fenotify rsyslog trap-sink QRadar address <QRadar の IP アドレス>
   ```
6. rsyslog イベント・フォーマットを定義するには、以下のコマンドを入力します。

   ```
   fenotify rsyslog trap-sink QRadar prefer message format leef
   ```
7. FireEye アプライアンスの構成に対する変更内容を保存するには、以下のコマンドを入力します。

   ```
   write memory
   ```

関連タスク:

『QRadar との通信用に FireEye HX システムを構成する』
FireEye HX が IBM Security QRadar と通信できるようにするために、Syslog イベントを転送するように FireEye HX アプライアンスを構成します。

QRadar との通信用に FireEye HX システムを構成する

FireEye HX が IBM Security QRadar と通信できるようにするために、Syslog イベントを転送するように FireEye HX アプライアンスを構成します。

手順

1. CLI を使用して FireEye HX アプライアンスにログインします。
2. 構成モードをアクティブにするには、以下のコマンドを入力します。

   ```
   enable

   configure terminal
   ```

3. リモート Syslog サーバーの宛先を追加するために、次のコマンドを入力します。

   ```
   logging <remote_IP_address> trap none

   logging <remote_IP_address> trap override class cef priority info
   ```

4. FireEye HX アプライアンスの構成に対する変更内容を保存するには、以下のコマンドを入力します。

   ```
   write mem
   ```

QRadar で FireEye のログ・ソースを構成する

IBM Security QRadar コンソールが FireEye イベントを受信すると、QRadar は自動的にログ・ソースを作成します。QRadar が FireEye イベントを自動的に検出しない場合は、イベント・ログの収集元となるインスタンスごとにログ・ソースを手動で追加します。

このタスクについて

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**FireEye**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。
8. 「ログ・ソース **ID**」フィールドに、FireEye アプライアンスの IP アドレスまたはホスト名を入力します。
9. 残りのパラメーターを構成します。
10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

第 52 章 Forcepoint

IBM Security QRadar は Forcepoint DSM を幅広くサポートしています。

Forcepoint は、以前は Websense と呼ばれていました。

関連概念:

1137 ページの『第 147 章 Websense』

QRadar は Websense DSM を幅広くサポートしています。

Forcepoint TRITON

IBM Security QRadar 用の Forcepoint V-Series Content Gateway DSM は、複数の Forcepoint TRITON ソリューション (Web Security、Web Security Gateway、Web Security Gateway Anywhere、V-Series アプライアンスなど) からの Web コンテンツのイベントをサポートします。

このタスクについて

Forcepoint TRITON は、Forcepoint Multiplexer コンポーネントを使用して QRadar へのイベント情報の収集およびストリーミングを行います。QRadar を構成する前に、LEEF 形式の syslog イベントを提供するように Forcepoint TRITON ソリューションを構成しておく必要があります。

イベントを QRadar に転送するように Forcepoint TRITON Web Security ソリューションを構成するには、デプロイメントに Forcepoint Multiplexer が含まれていることを確認してください。

Forcepoint Multiplexer は、Windows、Linux、および Forcepoint V-Series アプライアンスでサポートされます。

Forcepoint Triton または V-Series アプライアンスで Forcepoint Multiplexer を構成するには、以下の手順を実行します。

手順

1. ネットワーク内の Forcepoint Policy Server コンポーネントごとに、Forcepoint Multiplexer のインスタンスをインストールします。
   - Microsoft Windows の場合 - Windows に Forcepoint Multiplexer をインストールするには、TRITON Unified Installer を使用します。Triton Unified Installer は、http://www.myforcepoint.com からダウンロードできます。
   - Linux の場合 - Linux に Forcepoint Multiplexer をインストールするには、Web Security Linux Installer を使用します。Web Security Linux Installer は、http://www.myforcepoint.com からダウンロードできます。

ソフトウェアのインストール環境への Forcepoint Multiplexer の追加について詳しくは、「*Forcepoint Security Information Event Management (SIEM) Solutions*」の資料を参照してください。

2. 完全ポリシー・ソースまたはユーザー・ディレクトリーおよびフィルタリング・アプライアンスとして構成された V-Series アプライアンス上で Forcepoint Multiplexer を有効にします。
   a. Forcepoint TRITON Web Security コンソールまたは V-Series アプライアンスにログインします。
3. Appliance Manager で、「管理 **(Administration)**」 > 「ツールボックス **(Toolbox)**」 > 「コマンド・ライン・ユーティリティー **(Command Line Utility)**」を選択します。
4. 「**Forcepoint Web Security**」タブをクリックします。
5. 「コマンド **(Command)**」リストで「マルチプレクサー **(multiplexer)**」を選択してから、「有効 **(enable)**」コマンドを使用します。
6. 395 ページの『Forcepoint TRITON』 を繰り返して、ネットワーク内のポリシー・サーバー・インスタンスごとに Multiplexer インスタンスを 1 つずつ有効化します。

   1 つの ポリシー・サーバーに複数の Multiplexer がインストールされている場合は、最後にインストールされた Forcepoint Multiplexer のインスタンスのみが使用されます。各 Forcepoint Multiplexer インスタンスの構成はそのポリシー・サーバーによって保管されます。

次のタスク

これで、LEEF 形式 の syslog イベントを QRadar に転送するように Forcepoint TRITON アプライアンスを構成できるようになりました。

Forcepoint TRITON 用の syslog の構成

イベントを収集するには、Forcepoint TRITON の syslog 転送を構成する必要があります。

手順

1. Forcepoint TRITON Web Security コンソールにログインします。
2. 「設定 **(Settings)**」タブで、「一般 **(General)**」 > 「**SIEM** 統合 **(SIEM Integration)**」を選択します。
3. 「このポリシー・サーバーの **SIEM** 統合を有効にする **(Enable SIEM integration for this Policy Server)**」チェック・ボックスを選択します。
4. 「**IP** アドレスまたはホスト名 **(IP address or hostname)**」フィールドに、QRadar の IP アドレスを入力します。
5. 「ポート **(Port)**」フィールドに 514 を入力します。
6. 「トランスポート・プロトコル **(Transport protocol)**」リストで、「**TCP**」または「**UDP**」のプロトコル・オプションのいずれかを選択します。

   QRadar は、ポート 514 で TCP プロトコルおよび UDP プロトコルの syslog イベントをサポートします。

7. 「**SIEM format**」リストで、「**syslog/LEEF (QRadar)**」を選択します。
8. 「**OK**」をクリックして、すべての変更内容をキャッシュに入れます。
9. 「デプロイ **(Deploy)**」をクリックして、Forcepoint TRITON のセキュリティー・コンポーネントまたは V-Series アプライアンスを更新します。

Forcepoint Multiplexer は Forcepoint Filtering Service に接続して、QRadar にイベント・ログ情報が送信されることを確認します。

Forcepoint TRITON 用のログ・ソースの構成

IBM Security QRadar は、Forcepoint TRITON アプライアンスおよび V-Series アプライアンスからの LEEF 形式の syslog イベントに対して、ログ・ソースの検出および作成を自動的に実行します。

このタスクについて

ログ・ソースを作成するための構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Forcepoint V** シリーズ」を選択します。

   注**:** Forcepoint TRITON は、Forcepoint V Series Content Gateway DSM を使用してイベントを解析します。Forcepoint TRITON 用の QRadar に手動でログ・ソースを追加するときは、「**Forcepoint V Series**」を選択する必要があります。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *160. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Forcepoint TRITON アプライアンスまたは V-Series アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。

Forcepoint V シリーズ Data Security Suite

IBM Security QRadar 用の Forcepoint V-Series Data Security Suite DSM は、Forcepoint V シリーズ・アプライアンスおよび Data Security Suite (DSS) ソフトウェアをサポートしています。

Forcepoint V シリーズ Data Security Suite 用の syslog の構成

Forcepoint V-Series Data Security Suite DSM は、syslog を使用してイベントを受け入れます。IBM Security QRadar を統合するには、Data Security Suite (DSS) 管理コンソールで Forcepoint V-Series アプライアンスが syslog イベントを転送できるようにする必要があります。

手順

1. 「ポリシー **(Policies)**」 > 「ポリシー・コンポーネント **(Policy Components)**」 > 「通知テンプレート **(Notification Templates)**」を選択します。
2. 既存の通知テンプレートを選択するか、新規テンプレートを作成します。
3. 「一般 **(General)**」タブをクリックします。
4. 「**Syslog** メッセージの送信 **(Send Syslog Message)**」をクリックします。
5. 「オプション **(Options)**」 > 「設定 **(Settings)**」 > 「**Syslog**」を選択して「Syslog」ウィンドウにアクセスします。

   「Syslog」ウィンドウでは、管理者が組織の syslog のIP アドレス/ホスト名およびポート番号を定義できます。定義された syslog は Forcepoint Data Security Suite DSS Manager からインシデント・メッセージを受信します。
6. syslog は以下のフィールドで構成されます。

   ```
   DSS Incident|ID={value}|action={display value - max}|
   urgency= {coded}|
   policy categories={values,,,}|source={value-display name}|
   destinations={values...}|channel={display name}|
   matches= {value}|detaills={value}
   ```

   - 「policy categories」の最大長は 200 文字です。
   - 「destinations」の最大長は 200 文字です。
   - 「detaills」および「source」は 30 文字に短縮されます。
7. 「接続のテスト **(Test Connection)**」をクリックして、syslog にアクセス可能であることを確認します。

次のタスク

これで、QRadar でログ・ソースを構成できるようになりました。構成は完了です。OSSEC イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。OSSEC によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

Forcepoint V シリーズ Data Security Suite 用のログ・ソースの構成

IBM Security QRadar は、Forcepoint V-Series Data Security Suite からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Forcepoint V シリーズ**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 161. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Forcepoint V-Series Data Security Suite DSM からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Forcepoint V シリーズ Content Gateway

IBM Security QRadar 用の Forcepoint V シリーズ Content Gateway DSM は、Content Gateway ソフトウェアを備えた Forcepoint V シリーズ・アプライアンスの Web コンテンツに関するイベントをサポートしています。

Forcepoint V シリーズ Content Gateway DSM は、syslog を使用してイベントをストリーミングしたり、ログ・ファイル・プロトコルを使用してイベントを QRadar に提供したりすることでイベントを受け取ります。アプライアンスを QRadar と統合するには、以下のいずれかの構成方法を選択する必要があります。

- Forcepoint V-Series に対する Syslog を構成するには、『Forcepoint V シリーズ Content Gateway 用の syslog の構成』を参照してください。

- Forcepoint V-Series に対するログ・ファイル・プロトコルを構成するには、『Forcepoint V シリーズ Content Gateway 用のログ・ファイル・プロトコル』を参照してください。

Forcepoint V シリーズ Content Gateway 用の syslog の構成

Forcepoint V シリーズ DSM は、Linux ソフトウェア・インストール済み環境で Forcepoint Content Gateway を実行する Forcepoint V シリーズ・アプライアンスをサポートしています。

IBM Security QRadar を構成する前に、LEEF 形式の syslog イベントを提供するように Forcepoint Content Gateway を構成する必要があります。

Forcepoint V-Series Content Gateway 用の管理コンソールの構成

Content Gateway Manager でイベント・ロギングを構成できます。

手順

1. Forcepoint Content Gateway Manager にログインします。
2. 「構成 **(Configure)**」タブをクリックします。
3. 「サブシステム **(Subsystems)**」 > 「ロギング **(Logging)**」を選択します。

   一般ロギング構成 (General Logging Configuration)」ウィンドウが表示されます。
4. 「トランザクションとエラーをログに記録 **(Log Transactions and Errors)**」を選択します。
5. 「ログ・ディレクトリー **(Log Directory)**」を選択して、保管されるイベント・ログ・ファイルのディレクトリー・パスを指定します。

   定義するディレクトリーが存在している必要があり、また、Forcepoint ユーザーは指定したディレクトリーに対する読み取り/書き込み権限を持っている必要があります。

   デフォルトのディレクトリーは、`/opt/WGC/logs` です。
6. 「適用」をクリックします。
7. 「カスタム **(Custom)**」タブをクリックします。
8. 「カスタム・ログ・ファイル定義 **(Custom Log File Definitions)**」ウィンドウで、以下の LEEF 形式のテキストを入力します。

```
<LogFormat>
             <Name = "leef"/>
             <Format = "LEEF:1.0|Forcepoint|WCG|7.6|
             %<wsds>|cat=%<wc>
             src=%<chi> devTime=%<cqtn>
             devTimeFormat=dd/MMM/yyyy:HH:mm:ss Z
             http-username=%<caun> url=%<cquc>
             method=%<cqhm> httpversion=%<cqhv>
             cachecode=%<crc>dstBytes=%<sscl> dst=%<pqsi>
             srcBytes=%<pscl> proxy-status-code=%<pssc>
             server-status-code=%<sssc> usrName=%<wui>
             duration=%<ttms>"/>
        </LogFormat>
```

```
<LogObject>
             <Format = "leef"/>
             <Filename = "leef"/>
         </LogObject>
```

注**:** LEEF 形式ストリングのフィールドはタブ区切り です。テキスト・エディターに LEEF 形式で入力し、次に、Web ブラウザーにカット・アンド・ペーストして、タブ区切りを保持することが必要な場合があります。定義ファイルでは、余分なホワイト・スペース、ブランク行、およびすべてのコメントが無視されます。

9. 「有効にする **(Enabled)**」を選択して、カスタム・ロギング定義を有効にします。
10. 「適用」をクリックします。

次のタスク

これで、Forcepoint Content Gateway のイベント・ロギングを有効化できるようになりました。

Forcepoint V-Series Content Gateway のイベント・ロギングの有効化

Forcepoint V-Series アプライアンスを使用している場合、この機能を有効にするには、Forcepoint のテクニカル・サポートに問い合わせる必要があります。

手順

1. Forcepoint Content Gateway を実行しているサーバーのコマンド・ライン・インターフェース (CLI) にログインします。
2. `/etc/rc.local` ファイルの末尾に以下の行を追加します。

   ```
   ( while [ 1 ] ; do tail -n1000 -F /opt/WCG/logs/leef.log |
   nc <IP Address> 514 sleep 1 done ) &
   ```

   ここで、*<IP Address>* は、IBM Security QRadar の IP アドレスです。
3. ロギングをすぐに開始するには、以下のコマンドを入力します。

   ```
   nohup /bin/bash -c "while [ 1 ] ; do
   tail -F /opt/WCG/logs/leef.log | nc <IP Address> 514;
   sleep 1; done" &
   ```

   注**:** 『Forcepoint V-Series Content Gateway のイベント・ロギングの有効化』のロギング・コマンドを入力するか、このコマンドをテキスト・エディターにコピーして引用符を解釈することが必要であると考えられます。

   構成は完了です。Forcepoint V-Series Content Gateway からの syslog イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Forcepoint V-Series Content Gateway によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

Forcepoint V-Series Content Gateway 用のログ・ソースの構成

QRadar は、Forcepoint V-Series Content Gateway からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Forcepoint V** シリーズ」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 162. Syslog パラメーター

パラメーター	説明
ログ・ソース ID	Forcepoint V-Series Content Gateway アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Forcepoint V シリーズ Content Gateway 用のログ・ファイル・プロトコル

ログ・ファイル・プロトコルにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

Forcepoint V シリーズ DSM は、ログ・ファイル・プロトコルを使用してスケジュールされた一定の間隔でイベントを提供することにより、Forcepoint V シリーズ Content Gateway からのログ・ファイルの一括ロードをサポートしています。ログ・ファイルには、Forcepoint V シリーズ Content Gateway のトランザクションおよびエラー・イベントが記録されます。

Forcepoint V-Series Content Gateway 用の Content 管理コンソールの構成

Content 管理コンソールでのイベント・ロギングの構成

手順

1. Forcepoint Content Gateway インターフェースにログインします。
2. 「構成 **(Configure)**」タブをクリックします。

3. 「サブシステム **(Subsystems)**」 > 「ロギング **(Logging)**」を選択します。
4. 「トランザクションとエラーをログに記録 **(Log Transactions and Errors)**」を選択します。
5. 「ログ・ディレクトリー **(Log Directory)**」を選択して、保管されるイベント・ログ・ファイルのディレクトリー・パスを指定します。

   定義するディレクトリーが存在している必要があり、また、Forcepoint ユーザーは指定したディレクトリーに対する読み取り/書き込み権限を持っている必要があります。

   デフォルトのディレクトリーは `/opt/WGC/logs` です。
6. 「適用」をクリックします。
7. 「フォーマット **(Formats)**」タブをクリックします。
8. フォーマット・タイプとして「**Netscape** 拡張フォーマット **(Netscape Extended Format)**」を選択します。
9. 「適用」をクリックします。

次のタスク

これで、Forcepoint V-Series Content Gateway のイベント・ロギングを有効化できるようになりました。

Forcepoint V-Series Content Gateway 用のログ・ファイル・プロトコルのログ・ソースの構成

ログ・ファイル・プロトコルを使用するように Forcepoint V-Series DSM を構成するときは、Forcepoint V-Series に構成されているホスト名または IP アドレスを、ログ・ファイル・プロトコル構成の「リモート・ホスト」パラメーターに構成するようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Forcepoint V Series**」を選択します。
9. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
10. 「サービス・タイプ」リストで「**Secure File Transfer Protocol (SFTP)**」オプションを選択します。
11. 「**FTP** ファイル・パターン」フィールドに `extended.log_.*.old` と入力します。
12. 「リモート・ディレクトリー」フィールドに `/opt/WCG/logs` と入力します。

これは、 402 ページの『Forcepoint V-Series Content Gateway 用の Content 管理コンソールの構成』で指定した、Forcepoint V-Series ログ・ファイルを保管するためのデフォルトのディレクトリーです。

13. 「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LINEBYLINE)**」を選択します。
14. 「保存」をクリックします。
15. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。 .

第 53 章 ForeScout CounterACT

IBM Security QRadar 用の ForeScout CounterACT DSM は、syslog を使用して、CounterACT からログ・イベント拡張フォーマット (LEEF) のイベントを受け入れます。

QRadar は、以下の ForeScout CounterACT イベントを記録します。

- サービス妨害 (DoS)
- 認証
- エクスプロイト (Exploit)
- 疑わしい振る舞い
- システム

ログ・ソースの構成

ForeScout CounterACT を IBM Security QRadar と統合するには、ポリシー・ベースの syslog イベントを受信するためのログ・ソースを手動で作成する必要があります。

このタスクについて

QRadar が ForeScout CounterACT アプライアンスからの syslog イベントに対して、ログソースを自動的に検出および作成することはありません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**ForeScout CounterACT**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 163. syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	ForeScout CounterACT アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。

ForeScout CounterACT プラグインの構成

IBM Security QRadar を構成する前に、ForeScout CounterACT アプライアンス用のプラグインをインストールし、syslog イベントを QRadar に転送するように ForeScout CounterACT を構成する必要があります。

このタスクについて

QRadar を ForeScout CounterACT と統合するには、CounterACT 用のプラグインをダウンロードし、インストールして構成する必要があります。プラグインは ForeScout CounterACT を拡張し、LEEF イベントを QRadar に転送するためのフレームワークを提供します。

手順

1. ForeScout の Web サイトから、ForeScout CounterACT 用のプラグインをダウンロードします。
2. ForeScout CounterACT アプライアンスにログインします。
3. CounterACT コンソールのツールバーで「オプション **(Options)**」 > 「プラグイン **(Plugins)**」 > 「インストール **(Install)**」を選択します。プラグイン・ファイルの場所を選択します。

   プラグインがインストールされ、「プラグイン (Plug-ins)」ペインに表示されます。
4. 「プラグイン (Plug-ins)」ペインで QRadar プラグインを選択し、「構成 **(Configure)**」をクリックします。

   「QRadar の追加 (Add QRadar)」ウィザードが表示されます。
5. 「サーバー・アドレス **(Server Address)**」フィールドに、QRadar の IP アドレスを入力します。
6. 「ポート **(Port)**」リストで「**514**」を選択します。
7. 「次へ」をクリックします。
8. 「割り当てられた CounterACT (Assigned CounterACT)」ペインで、以下のいずれかのオプションを選択します。
   - デフォルト・サーバー **(Default Server)** - 当該 ForeScout CounterACT のすべてのデバイスがイベントを QRadar に転送するようにする場合は、このオプションを選択します。
   - **CounterACT** デバイスの割り当て **(Assign CounterACT devices)** - ForeScout CounterACT で実行されている個別デバイスのどれがイベントを QRadar に転送するかを割り当てる場合は、このオプションを選択します。「CounterACT デバイスの割り当て (Assign CounterACT devices)」オプションは、ForeScout CounterACT サーバーが 1 つ以上ある場合にのみ使用可能です。

9. 「終了」をクリックします。

   プラグイン構成は完了です。これで、ForeScout CounterACT ポリシーによって QRadar に転送されるイベントを定義する準備ができました。

ForeScout CounterACT ポリシーの構成

ForeScout CounterACT ポリシーは、アプライアンスでの管理アクションおよび修復アクションをトリガーするための条件をテストします。

このタスクについて

プラグインは、ポリシーで syslog を使用して IBM Security QRadar にイベントを転送するための追加アクションを提供します。イベントを QRadar に転送するには、QRadar 更新アクションが含まれた CounterACT ポリシーを定義する必要があります。

QRadar へのイベントの送信を開始するには、ポリシー条件が少なくとも 1 回満たされる必要があります。記録するイベントについて QRadar に更新を送信するように各ポリシーを構成する必要があります。

手順

1. ForeScout CounterACT のポリシーを選択します。
2. 「アクション・ツリー (Actions tree)」で「監査 **(Audit)**」 > 「更新の送信 **(Send Updates)**」(QRadar Server を対象) を選択します。
3. 「内容 **(Contents)**」タブで以下の値を構成します。

   「ホスト・プロパティーの結果を送信 **(Send host property results)**」チェック・ボックスを選択します。
4. ポリシーで転送するイベントのタイプのいずれかを以下から選択します。
   - すべて送信 **(Send All)** - ポリシーで検出されたすべてのプロパティーを QRadar に含める場合は、このオプションを選択します。
   - 特定のものを送信 **(Send Specific)** - ポリシーで特定のプロパティーのみを選択して QRadar に送信する場合は、このオプションを選択します。
5. 「ポリシー状況を送信 **(Send policy status)**」チェック・ボックスを選択します。
6. 「トリガー **(Trigger)**」タブで、QRadar へのイベントの転送に ForeScout CounterACT が使用する間隔を以下から選択します。
   - アクションの開始時に送信 **(Send when the action starts)** - ポリシーの条件が満たされたときに単一のイベントを QRadar に送信する場合は、このチェック・ボックスを選択します。
   - 情報の更新時に送信 **(Send when information is updated)** - 「内容 **(Contents)**」タブで指定されているホスト・プロパティーが変更されたときにレポートを送信する場合は、このチェック・ボックスを選択します。
   - 定期的に送信 **(Send periodically every)** - ポリシー条件が満たされたときに一定間隔で繰り返しイベントを QRadar に送信する場合は、このチェック・ボックスを選択します。

7. 「**OK**」をクリックしてポリシー変更を保存します。
8. このプロセスを繰り返し、QRadar に更新を送信するアクションを使用して追加ポリシーを構成します。

構成は完了です。ForeScout CounterACT によって転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

第 54 章 Fortinet FortiGate

Fortinet 用の IBM Security QRadar SIEM は、Fortinet FortiGate および FortiAnalyzer 製品からイベントを収集します。

以下の表は、Fortinet FortiGate DSM の仕様を示しています。

表 *164. Fortinet FortiGate DSM* の仕様

仕様	値
製造元	Fortinet
DSM 名	Fortinet FortiGate
RPM ファイル名	`DSM-FortinetFortiGate-`*`QRadar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	FortiOS v2.5
プロトコル	Syslog Syslog リダイレクト
記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	はい
その他の情報	Fortinet Web サイト (http://www.fortinet.com)

Fortinet FortiGate DSM を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、Fortinet FortiGate RPM の最新バージョンを QRadar コンソールにダウンロードしてください。
2. Fortigate FortiAnalyzer を介してイベントを収集するために、Syslog Redirect プロトコルの RPM をダウンロードし、インストールします。Syslog Redirect プロトコルを使用すると、QRadar は、イベントを送信した特定の Fortigate ファイアウォールを識別できます。
3. Fortinet FortiGate のインスタンスごとに、Syslog イベントを QRadar に送信するように Fortinet FortiGate システムを構成します。

4. QRadar が Fortinet FortiGate のログ・ソースを自動的に検出しない場合は、手動でログ・ソースを追加できます。プロトコル構成として「**Syslog**」を選択し、次にパラメーターを構成します。
5. QRadar が Fortinet FortiAnalyzer からイベントを受信するようにするには、ログ・ソースを手動で追加します。プロトコル構成として「**Syslog** リダイレクト」を選択し、次にパラメーターを構成します。

   Fortinet FortiAnalyzer イベントの収集に必要な特定のパラメーター値を次の表にリストします。

パラメーター	値
ログ・ソース ID 正規表現 (Log Source Identifier Regex)	**devname=([¥w-]+)**
Listen ポート	**517**
プロトコル	**UDP**

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

『Fortinet FortiGate デバイスでの Syslog 宛先の構成』
FortiGate イベントを IBM Security QRadar に転送するには、Syslog 宛先を構成する必要があります。

411 ページの『Fortinet FortiAnalyzer デバイスでの Syslog 宛先の構成』
FortiGate イベントを IBM Security QRadar に転送するには、Syslog 宛先を構成する必要があります。

Fortinet FortiGate デバイスでの Syslog 宛先の構成

FortiGate イベントを IBM Security QRadar に転送するには、Syslog 宛先を構成する必要があります。

手順

1. Fortinet FortiGate アプライアンスで、コマンド・ライン・インターフェースにログインします。
2. 次のコマンドを順に入力し、環境に適合する値で変数を置換します。

```
config log syslogd setting
set csv {disable | enable}
set facility <facility_name>
set port <port_integer>
set reliable enable
set server <IP_address>
set status enable
end
```

次のタスク

デプロイメント環境に、イベント・ログを FortiAnalyzer に送信するように構成されている複数の FortiGate インスタンスが存在する可能性があります。FortiAnalyzer イベントを QRadar に送信する場合は、『Fortinet FortiAnalyzer デバイスでの Syslog 宛先の構成』を参照してください。

Fortinet FortiAnalyzer デバイスでの Syslog 宛先の構成

FortiGate イベントを IBM Security QRadar に転送するには、Syslog 宛先を構成する必要があります。

手順

1. FortiAnalyzer デバイスにログインします。
2. 「拡張 **(Advanced)**」ツリー・メニューで、「**Syslog** サーバー **(Syslog Server)**」を選択します。
3. ツールバーで「新規作成 **(Create New)**」をクリックします。
4. 以下の「**Syslog** サーバー **(Syslog Server)**」の各パラメーターを構成します。

パラメーター	説明
ポート	デフォルトのポートは 514 です。

5. 「**OK**」をクリックします。

第 55 章 Foundry FastIron

Foundry FastIron デバイスを IBM Security QRadar と統合すると、syslog を使用して、関連するすべてのイベントを収集できます。

これを行うには、syslog とログ・ソースを構成する必要があります。

Foundry FastIron 用の syslog の構成

IBM Security QRadar を Foundry FastIron RX デバイスと統合するには、syslog イベントを転送するようにアプライアンスを構成する必要があります。

手順

1. Foundry FastIron デバイスのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力して、ロギングを有効にします。

   ```
   logging on
   ```

   これで、以下のデフォルトを使用してローカル syslog が有効になりました。
   - すべての syslog レベル (緊急からデバッグまで) のログが記録されます。
   - 最大で 50 件のメッセージがローカル syslog バッファーに保持されます。
   - syslog サーバーは指定されていません。
3. 以下のコマンドを入力して、syslog サーバーの IP アドレスを定義します。

   ```
   logging host <IP Address>
   ```

   ここで *<IP Address>* は、QRadar の IP アドレスです。

   これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

QRadar は、Foundry FastIron からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「Foundry FastIron」を選択します。

9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース ID	Foundry FastIron アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 56 章 FreeRADIUS

IBM Security QRadar DSM for FreeRADIUS は、FreeRADIUS デバイスからイベントを収集します。

FreeRADIUS DSM の仕様を以下の表に示します。

表 *165. FreeRADIUS DSM* の仕様

仕様	値
製造元	FreeRADIUS
DSM 名	FreeRADIUS
RPM ファイル名	DSM-FreeRADIUS-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	V2.x
イベント・フォーマット	Syslog
記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	FreeRADIUS Web サイト (http://freeradius.org)

FreeRADIUS から QRadar にログを送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの FreeRADIUS DSM RPM をダウンロードして QRadar コンソールにインストールしてください。
2. Syslog イベントを QRadar に送信するように FreeRADIUS デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで FreeRADIUS ログ・ソースを追加してください。以下の表は、FreeRADIUS イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *166. FreeRADIUS* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	FreeRADIUS
プロトコル構成	Syslog

QRadar との通信のための FreeRADIUS デバイスの構成

ホストの syslog デーモンにログを送信するように FreeRADIUS を構成し、QRadar にイベントを送信するようにデーモンを構成します。

始める前に

syslog 構成および Linux ディストリビューションの作業知識が必要です。

このタスクについて

FreeRADIUS には複数のディストリビューションがあります。以下の手順で説明するように、ファイルが同一の場所にない場合があります。例えば、FreeRADIUS の始動スクリプトの場所はディストリビューションに基づいています。概念的には、構成ステップはすべてのディストリビューションで同じです。

手順

1. FreeRADIUS をホストしているシステムにログインします。
2. /etc/freeradius/radius.conf ファイルを編集します。
3. ファイル内のテキストを以下の行に一致するように変更します。

```
logdir = syslog
Log_destination = syslog
log{
    destination = syslog
    syslog_facility = daemon
    stripped_names = no
    auth = yes
    auth_badpass = no
    auth_goodpass = no
}
```

4. /etc/syslog.conf ファイルを編集します。
5. ログ・オプションを構成するには、以下のテキストを追加します。

   # .=notice は、認証メッセージ **(L_AUTH)** をログに記録します。

   ```
   # <facility_name>.=notice
   @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>
   ```

   # .=err は、**FreeRADIUS** のモジュール・エラーをログに記録します。

   ```
   #<facility_name>.=err
   @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>
   ```

   # .* は、同じターゲットへのメッセージをログに記録します。

   ```
   # <facility_name>.*
   @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>
   ```

   syslog ファシリティー名の例としては、*local1* があります。この名前は変更可能です。

   ログ・オプションを構成するには、@ シンボルを含むアクティブ行のいずれかからコメント・タグ (#) を削除します。
6. 構成変更が自動的にロードされない場合は、syslog デーモンを再始動します。syslog デーモンの再始動方法は、使用しているディストリビューションによって異なります。以下の表に、可能な方法を示します。

オペレーティング・システムの配布	デーモンを再始動するコマンド
Red Hat Enterprise Linux	service syslog restart
Debian Linux または **Ubuntu Linux**	/etc/init.d/syslog restart
FreeBSD オペレーティング・システム	/etc/rc.d/syslogd restart

7. 以下のオプションを FreeRADIUS 始動スクリプトに追加します。
   - -l syslog

- `-g <facility_name>`

  `-g` 値は、ステップ 5 のファシリティー名と一致している必要があります。

8. FreeRADIUS を再始動します。

第 57 章 汎用

IBM Security QRadar は、さまざまな汎用 DSM をサポートしています。

汎用認証サーバー

IBM Security QRadar 用の汎用認証サーバー DSM は、syslog を使用して、関連するすべての汎用認証サーバーのイベントを記録します。

受信汎用認証サーバー・イベントを解釈するように QRadar を構成し、手動でログ・ソースを作成する必要があります。

イベント・プロパティーの構成

受信汎用認証イベントを解釈するように IBM Security QRadar を構成するには、以下のようにします。

手順

1. すべての認証サーバー・ログを QRadar システムに転送します。

   QRadar への認証サーバー・ログの転送については、汎用認証サーバーのベンダー資料 を参照してください。

2. 以下のファイルを開きます。

   ```
   /opt/QRadar/conf/genericAuthServer.conf
   ```

   イベント・コレクター (Event Collector)および QRadar コンソールをホストしているシステムにこのファイルをコピーしてください。

3. 以下のように、Tomcat サーバーを再始動します。

   ```
   service tomcat restart
   ```

   Tomcat サーバーが再始動されたことを示すメッセージが表示されます。

4. **regex_enabled** プロパティーを設定して、パターンでの正規表現を有効または無効にします。デフォルトでは、正規表現は無効になっています。 例えば、以下のようにします。

   ```
   regex_enabled=false
   ```

   regex_enabled プロパティーを `false` に設定すると、システムは、ログから対応するデータ値を取得しようとする際に、入力したタグに基づいて、正規表現 (regex) を生成します。

   regex_enabled プロパティーを `true` に設定した場合、パターンを制御するためのカスタム正規表現を定義できます。この正規表現構成は、ログに直接適用され、最初にキャプチャーされたグループが返されます。カスタムの正規表現パターンを定義する場合は、Java プログラミング言語で規定されている正規表

現のルールに従う必要があります。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。

汎用許可サーバーを QRadar と統合する場合は、事前定義のクラスを使用するのではなく、クラスを直接指定するようにしてください。例えば、数字クラス (/¥d/) は、/[0-9]/ になります。また、数値修飾子を使用するのではなく、プリミティブな修飾子 (/?/、/*/、および /+/) を使用するように表現を書き直してください。

5. 以下のように、ファイルを確認して、ログイン成功のパターンを判別します。

   例えば、受け入れられたパケットに対して認証サーバーで以下のログ・メッセージが生成される場合を考えます。

   ```
   Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from
   10.100.100.109 port 1727 ssh2
   ```

   ログイン成功のパターンは、以下のとおりです。

   ```
   Accepted password.
   ```

6. 以下の項目をファイルに追加します。

   ```
   login_success_pattern=<login success pattern>
   ```

   ここで、*<login success pattern>* は、 419 ページの『イベント・プロパティーの構成』で判別したパターンです。

   例:

   ```
   login_success_pattern=Accepted password
   ```

   すべての項目で、大/小文字が区別されません。

7. 以下のように、ファイルを確認して、ログイン失敗のパターンを判別します。

   例えば、認証サーバーでログイン失敗に対して以下のログ・メッセージが生成される場合を考えます。

   ```
   Jun 27 12:58:33 expo sshd[20627]: Failed password for root from
   10.100.100.109 port 1849 ssh2
   ```

   ログイン失敗のパターンは、「Failed password」です。

8. 以下をファイルに追加します。

   ```
   login_failed_pattern=<login failure pattern>
   ```

   ここで、*<login failure pattern>* は、ログイン失敗について判別したパターンです。

   例:

   ```
   login_failed_pattern=Failed password
   ```

すべての項目で、大/小文字が区別されません。

9. 以下のように、ファイルを確認して、ログアウトのパターンを判別します。

   例えば、認証サーバーでログアウトに対して以下のログ・メッセージが生成される場合を考えます。

   ```
   Jun 27 13:00:01 expo su(pam_unix)[22723]: session closed for user
   genuser
   ```

   ログアウトのパターンは、「session closed」です。

10. 以下を genericAuthServer.conf ファイルに追加します。

    ```
    logout_pattern=<logout pattern>
    ```

    ここで、<*logout pattern*> は、 419 ページの『イベント・プロパティーの構成』でログアウトについて判別したパターンです。

    例:

    ```
    logout_pattern=session
    ```

    すべての項目で、大/小文字が区別されません。

11. ファイルを確認して、送信元 IP アドレスおよび送信元ポートのパターンを判別します (存在する場合)。

    例えば、認証サーバーで以下のログ・メッセージが生成される場合を考えます。

    ```
    Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from
    10.100.100.109 port 1727 ssh2
    ```

    送信元 IP アドレスのパターンは from であり、送信元ポートのパターンは port です。

12. 以下のように、送信元 IP アドレスおよび送信元ポートの項目をファイルに追加します。

    ```
    source_ip_pattern=<source IP pattern>
    ```

    ```
    source_port_pattern=<source port pattern>
    ```

    ここで、<*source IP pattern*> および <*source port pattern*> は、送信元 IP アドレスおよび送信元ポートについて 419 ページの『イベント・プロパティーの構成』で特定したパターンです。

    例:

    ```
    source_ip_pattern=from
    ```

    ```
    source_port_pattern=port
    ```

13. ファイルを確認して、ユーザー名のパターンが存在するかどうかを判別します。

例:

```
Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from
10.100.100.109 port 1727 ssh2
```

ユーザー名のパターンは `for` です。

14. 以下のように、ユーザー名パターンの項目をファイルに追加します。

例:

```
user_name_pattern=for
```

これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

汎用認証アプライアンスのイベントを IBM Security QRadar と統合するには、イベントを受信するためのログ・ソースを手動で作成する必要があります。これは、QRadar が汎用認証アプライアンスからのイベントのログ・ソースを自動的に検出および作成することがないためです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「構成可能な認証」メッセージ・フィルターを選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *167. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	汎用認証アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。汎用認証アプライアンスによって QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

汎用ファイアウォール

IBM Security QRadar 用の汎用ファイアウォール・サーバー DSM は、syslog を使用してイベントを受け入れます。QRadar は、関連するすべてのイベントを記録します。

受信汎用ファイアウォール・イベントを解釈するように QRadar を構成し、手動でログ・ソースを作成します。

イベント・プロパティーの構成

受信汎用ファイアウォール・イベントを解釈するための IBM Security QRadar の構成について説明します。

このタスクについて

以下の手順を使用して、イベント・プロパティーを構成します。

手順

1. すべてのファイアウォール・ログを QRadar に転送します。

   汎用ファイアウォールから QRadar へのファイアウォール・ログの転送については、ファイアウォールのベンダー資料を参照してください。
2. 以下のファイルを開きます。

   ```
   /opt/QRadar/conf/genericFirewall.conf
   ```

   イベント・コレクター (Event Collector)および QRadar コンソールをホストしているシステムにこのファイルをコピーしてください。
3. 以下のように、Tomcat サーバーを再始動します。

   ```
   service tomcat restart
   ```

   Tomcat サーバーが再始動されたことを示すメッセージが表示されます。
4. **regex_enabled** プロパティーを設定して、パターンでの正規表現を有効または無効にします。デフォルトでは、正規表現は無効になっています。

   例:

   ```
   regex_enabled=false
   ```

   regex_enabled プロパティーを `false` に設定すると、システムは、ログから対応するデータ値を取得しようとする際に、入力したタグに基づいて、正規表現を生成します。

   regex_enabled プロパティーを `true` に設定した場合、パターンを制御するためのカスタム正規表現を定義できます。この正規表現構成は、ログに直接適用され、最初にキャプチャーされたグループが返されます。カスタムの正規表現パターンを定義する場合は、Java プログラミング言語で規定されている正規表現のルールに従う必要があります。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。

汎用ファイアウォールを QRadar と統合する場合は、事前定義のクラスを使用するのではなく、クラスを直接指定するようにしてください。例えば、数字クラス (/¥d/) は、/[0-9]/ になります。また、数値修飾子を使用するのではなく、プリミティブな修飾子 (/?/、/*/、および /+/) を使用するように表現を書き直してください。

5. 以下のように、ファイルを確認して、パケット受け入れのパターンを判別します。

   例えば、受け入れられたパケットに対してデバイスで以下のログ・メッセージが生成される場合を考えます。

   ```
   Aug. 5, 2005 08:30:00 Packet accepted. Source IP: 192.168.1.1 Source
   Port: 80 Destination IP: 192.168.1.2 Destination Port: 80 Protocol: tcp
   ```

   パケット受け入れのパターンは、「Packet accepted」です。

6. 以下をファイルに追加します。

   ```
   accept_pattern=<accept pattern>
   ```

   ここで、*<accept pattern>* は、 423 ページの『イベント・プロパティーの構成』で判別したパターンです。例:

   ```
   accept pattern=Packet accepted
   ```

   パターンでは、大/小文字が区別されません。

7. 以下のように、ファイルを確認して、パケット拒否のパターンを判別します。

   例えば、拒否されたパケットに対してデバイスで以下のログ・メッセージが生成される場合を考えます。

   ```
   Aug. 5, 2005 08:30:00 Packet denied. Source IP: 192.168.1.1 Source
   Port: 21 Destination IP: 192.168.1.2 Destination Port: 21 Protocol: tcp
   ```

   パケット拒否のパターンは、「Packet denied」 です。

8. 以下をファイルに追加します。

   ```
   deny_pattern=<deny pattern>
   ```

   ここで、*<deny pattern>* は、 423 ページの『イベント・プロパティーの構成』で判別したパターンです。

   パターンでは、大/小文字が区別されません。

9. ファイルを確認して、以下のパラメーターのパターンを判別します (存在する場合)。
   - 送信元 IP (source ip)
   - 送信元ポート (source port)
   - 宛先 IP (destination ip)
   - 宛先ポート (destination port)
   - プロトコル (protocol)

例えば、デバイスで以下のログ・メッセージが生成される場合を考えます。

```
Aug. 5, 2005 08:30:00 Packet accepted. Source IP: 192.168.1.1 Source
Port: 80 Destination IP: 192.168.1.2 Destination Port: 80 Protocol: tcp
```

送信元 IP のパターンは、「Source IP」です。

10. 以下をファイルに追加します。
    - source_ip_pattern=<*source ip pattern*>
    - source_port_pattern=<*source port pattern*>
    - destination_ip_pattern=<*destination ip pattern*>
    - destination_port_pattern=<*destination port pattern*>
    - protocol_pattern=<*protocol pattern*>

    ここで、<*source ip pattern*>、<*source port pattern*>、<*destination ip pattern*>、<*destination port pattern*>、および <*protocol pattern*> は、423 ページの『イベント・プロパティーの構成』で特定した対応するパターンです。

    注: パターンでは大/小文字が区別されず、また複数のパターンを追加できます。複数のパターンを使用する場合は、# 記号を使用して区切ってください。
11. ファイルを保存して終了します。

これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

汎用許可ファイアウォールを IBM Security QRadar と統合するには、イベントを受信するためのログ・ソースを手動で作成する必要があります。これは、QRadar が汎用ファイアウォール・アプライアンスからのイベントのログ・ソースを自動的に検出および作成することがないためです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「構成可能なファイアウォール・フィルター」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

syslog プロトコル構成が表示されます。

10. 以下の値を構成します。

表 *168. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	汎用ファイアウォール・アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。汎用ファイアウォールによって QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

第 58 章 genua genugate

IBM Security QRadar DSM for genua genugate は、genua genugate デバイスからイベントを収集します。

genua genugate は、サード・パーティーのソフトウェア (openBSD や sendMail など) からログを生成します。genua genugate DSM により、これらのサード・パーティー・デバイスから取得したログに対して基本的な構文解析を実行できます。それらのログを厳密に構文解析するには、そのデバイスに固有の DSM をインストールしてください。

genua genugate DSM の仕様を以下の表に示します。

表 169. genua genugate DSM の仕様

仕様	値
製造元	genua
DSM 名	genua genugate
RPM ファイル名	DSM-GenuaGenugate-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	8.2 以降
プロトコル	Syslog
記録されるイベント・タイプ	一般的なエラー・メッセージ 高可用性 汎用リレー・メッセージ リレー固有のメッセージ genua プログラム/デーモン EPSI アカウンティング・デーモン - gg/src/acctd Configfw FWConfig ROFWConfig ユーザー・インターフェース Web サーバー
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ

表 169. genua genugate DSM の仕様 (続き)

仕様	値
その他の情報	genua Web サイト (https://www.genua.de/en/solutions/high-resistance-firewall-genugate.html)

genua genugate イベントを QRadar に送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - genua genugate DSM RPM
2. Syslog イベントを QRadar に送信するように genua genugate デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで genua genugate ログ・ソースを追加してください。すべての必須パラメーターを構成します。以下の表を使用して、genua genugate に固有の値を識別してください。

表 170. genua genugate ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	genua genugate
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『イベントを QRadar に送信するように genua genugate を構成する』
イベントを IBM Security QRadar に送信するように genua genugate を構成します。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

イベントを QRadar に送信するように genua genugate を構成する

イベントを IBM Security QRadar に送信するように genua genugate を構成します。

手順

1. genua genugate にログインします。
2. 「システム」 > 「システム管理 **(Sysadmin)**」 > 「ロギング・ページ **(Logging page)**」をクリックします。

3. IBM QRadar の「**IP** アドレス」フィールドに、QRadar コンソールまたはイベント・コレクターの IP アドレスを入力します。
4. 「外部に対するアカウンティング **(Accounting to External)**」チェック・ボックスを選択します。
5. 「**OK**」をクリックします。

第 59 章 Great Bay Beacon

IBM Security QRadar 用の Great Bay Beacon DSM は、Great Bay Beacon Endpoint Profiler からの syslog アラートをサポートします。

QRadar は、関連するすべての Endpoint セキュリティー・イベントを記録します。Great Bay Beacon と QRadar を統合するには、syslog イベント・メッセージを QRadar に転送するように Great Bay Beacon Endpoint Profiler を構成する必要があります。

Great Bay Beacon 用の syslog の構成

syslog イベントを転送するように Great Bay Beacon Endpoint Profiler を構成できます。

手順

1. Great Bay Beacon Endpoint Profiler にログインします。
2. イベントを作成するために、「構成 **(Configuration)**」 > 「イベント **(Events)**」 > 「イベントの作成 **(Create Events)**」を選択します。

   現在構成されているイベントのリストが表示されます。
3. 「イベント送達方式 (Event Delivery Method)」ペインで「**Syslog**」チェック・ボックスを選択します。
4. 変更を適用するために、「構成変更の適用 **(Configuration Apply Changes)**」 > 「モジュールの更新 **(Update Modules)**」を選択します。
5. 『Great Bay Beacon 用の syslog の構成』を繰り返し、IBM Security QRadar でモニターするすべてのイベントを構成します。
6. Great Bay Beacon Endpoint Profiler の外部ログ・ソースとして QRadar を構成します。

   外部ログ・ソースとしての QRadar の構成については、「*Great Bay Beacon Endpoint Profiler Configuration Guide*」を参照してください。

   これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Great Bay Beacon からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Great Bay Beacon**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *171. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Great Bay Beacon アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 60 章 HBGary Active Defense

IBM Security QRadar 用の HBGary Active Defense DSM は、HBGary Active Defense デバイスから転送される、いくつかのイベント・タイプ (アクセス、システム、システム構成、ポリシーの各イベントなど) を受け入れます。

Active Defense からのイベントは、syslog を使用して、ログ・イベント拡張フォーマット (LEEF) で QRadar に転送されます。QRadar を構成するには、HBGary Active Defense デバイスがイベントを syslog 宛先に転送する経路を構成しておく必要があります。

HBGary Active Defense の構成

QRadar 用に Active Defense で syslog イベントの経路を構成できます。

手順

1. Active Defense 管理コンソールにログインします。
2. ナビゲーション・メニューで「設定 **(Settings)**」 > 「アラート **(Alerts)**」を選択します。
3. 「経路の追加 **(Add Route)**」をクリックします。
4. 「経路名 **(Route Name)**」フィールドに、Active Defense に追加する syslog 経路の名前を入力します。
5. 「経路タイプ **(Route Type)**」リストから「**LEEF (Q1 Labs)**」を選択します。
6. 「設定 (Settings)」ペインで以下の値を構成します。
   - ホスト **(Host)** - QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスまたはホスト名を入力します。
   - ポート **(Port)** - ポート番号として 514 を入力します。
7. 「イベント (Events)」ペインで、QRadar に転送するイベントを選択します。
8. 「**OK**」をクリックして構成変更を保存します。

   Active Defense デバイスの構成は完了です。これで、ログ・ソースを QRadar で構成することができます。Active Defense での経路の構成について詳しくは、「*HBGary Active Defense User Guide*」を参照してください。

ログ・ソースの構成

IBM Security QRadar は、Active Defense から転送された LEEF 形式からの syslog イベントに対して、ログソースを自動的に検出および作成します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**HBGary Active Defense**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *172. HBGary Active Defense* の *syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	HBGary Active Defense デバイスの IP アドレスまたはホスト名を入力します。 IP アドレスまたはホスト名により、QRadar での固有のイベント・ソースとして HBGary Active Defense デバイスが識別されます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

HBGary Active Defense の構成は完了です。

第 61 章 H3C Technologies

IBM Security QRadar は、さまざまな H3C Technologies DSM からイベントを受け取ります。

H3C Comware Platform

H3C Comware Platform 用の IBM Security QRadar DSM は、H3C Technologies のさまざまなネットワーク・デバイスからイベントを収集します。QRadar は、H3C スイッチ、H3C ルーター、H3C ワイヤレス LAN デバイス、および H3C IP セキュリティー・デバイスをサポートしています。

以下の表は、H3C Comware Platform DSM の仕様を示しています。

表 *173. H3C Comware Platform DSM* の仕様

仕様	値
製造元	H3C Technologies Co., Limited
DSM 名	H3C Comware Platform、H3C スイッチ、H3C ルーター、H3C ワイヤレス LAN デバイス、および H3C IP セキュリティー・デバイス。
RPM ファイル名	DSM-H3CComware-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	V7
プロトコル	Syslog
イベント・フォーマット	NVP
記録されるイベント・タイプ	システム
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	H3C Technologies (http://www.h3c.com)

H3C Comware Platform、H3C スイッチ、H3C ルーター、H3C ワイヤレス LAN デバイス、または H3C IP セキュリティー・デバイスを QRadar と統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの H3C Comware Platform DSM RPM をダウンロードして QRadar コンソールにインストールしてください。
2. Syslog イベントを QRadar に送信するように H3C Comware Platform のルーターまたはデバイスを構成します。

3. QRadar がログ・ソースを自動的に検出しない場合は、QRadar コンソールで H3C Comware Platform ログ・ソースを追加してください。以下の表は、H3C Comware Platform イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *174. H3C Comware Platform* ログ・ソースのパラメーター

パラメーター	値
ログ・ソース・タイプ	H3C Comware Platform
プロトコル構成	Syslog

H3C Comware Platform DSM のサンプル Syslog イベント・メッセージを次の表に示します。

表 *175. H3C Comware Platform* のサンプル *Syslog* メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
ユーザーの AAA 要求が拒否されました	AAA セッション拒否	<188>Jun 14 17:11:11 2013 HP %%10AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain =domain1-Service=login-UserName=cwf@system; AAA is failed.

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信のための H3C Comware Platform の構成

H3C Comware Platform イベントを収集するには、Syslog 設定を有効にして、ログ・ホストを構成します。 H3C スイッチ、H3C ルーター、H3C ワイヤレス LAN デバイス、および H3C IP セキュリティー・デバイスが QRadar によってサポートされています。

手順

1. コンソール・ポートを使用するか、または Telnet あるいは SSH を使用して、コマンド・ライン・インターフェースにログインします。 ログインの方法について詳しくは、ご使用の H3C デバイスの構成ガイドの『*CLI* へのログイン』セクションを参照してください。
2. システム・ビューにアクセスするために、`<system_name> system-view` コマンドを入力します。
3. Syslog 設定を有効にするには、以下のコマンドを、リストされている順序で入力します。
   a. `info-center source default loghost deny`
   b. `info-center source AAA loghost level informational`
   c. `info-center source ACL loghost level informational`

d. info-center source FIPS loghost level informational
e. info-center source HTTPD loghost level informational
f. info-center source IKE loghost level informational
g. info-center source IPSEC loghost level informational
h. info-center source LOGIN loghost level informational
i. info-center source LS loghost level informational
j. info-center source PKI loghost level informational
k. info-center source PORTSEC loghost level informational
l. info-center source PWDCTL loghost level informational
m. info-center source RADIUS loghost level informational
n. info-center source SHELL loghost level informational
o. info-center source SNMP loghost level informational
p. info-center source SSHS loghost level informational
q. info-center source TACACS loghost level informational
r. info-center loghost <*QRadar Event Collector IP*> 514

4. システム・ビューを終了するには、quit <*system_name*> コマンドを入力します。

第 62 章 Honeycomb Lexicon File Integrity Monitor (FIM)

IBM Security QRadar と Honeycomb Lexicon File Integrity Monitor (FIM) DSM を使用して、ネットワークから詳細ファイル保全性イベントを収集できます。

QRadar は、Lexicon mesh v3.1 以降を使用している Lexicon File Integrity Monitor インストール済み環境から転送される syslog イベントをサポートします。Lexicon FIM から転送される syslog イベントは、Lexicon mesh サービスによって、ログ・イベント拡張フォーマット (LEEF) のイベントとしてフォーマットされます。

Lexicon FIM イベントを QRadar と統合するには、以下のタスクを実行する必要があります。

1. Honeycomb インストール済み環境で、syslog イベントを LEEF で生成するように Lexicon mesh サービスを構成します。
2. Honeycomb インストール済み環境で、Honeycomb データ・コレクターが FIM イベントを QRadar コンソールまたはイベント・コレクター (Event Collector)に転送するようにすべての FIM ポリシーを構成します。
3. QRadar コンソールで、Lexicon FIM ログ・ソースが作成され、イベントが「ログ・アクティビティー」タブに表示されていることを確認します。
4. オプション。Honeycomb データ・コレクターと、イベントを受信する QRadar コンソールまたはイベント・コレクター (Event Collector)との間の通信がファイアウォール・ルールによってブロックされていないことを確認してください。

QRadar によるログ記録でサポートされる Honeycomb FIM イベント・タイプ

IBM Security QRadar 用の Honeycomb FIM DSM は、さまざまなイベント・カテゴリーからイベントを収集できます。

各イベント・カテゴリーには下位イベントが含まれ、そのイベント・カテゴリー内で実行されるアクションを記述しています。例えば、ファイル名の変更イベントには、file rename successful または file rename failed という下位カテゴリーを含めることが考えられます。

以下のリストは、QRadar が収集する、Honeycomb ファイル保全性イベントのイベント・カテゴリーを定義しています。

- ベースライン・イベント
- ファイルのオープン・イベント
- ファイルの作成イベント
- ファイル名の変更イベント
- ファイルの変更イベント
- ファイルの削除イベント
- ファイルの移動イベント

- ファイル属性の変更イベント
- ファイル所有者の変更イベント

QRadar は、Honeycomb Lexicon から転送される Windows やその他のログ・ファイルも収集できます。ただし、ファイル保全性イベント以外の任意のイベントでは、QRadar でユニバーサル DSM またはログ・ソースの拡張による特別な処理が必要になる場合があります。

Lexicon mesh service の構成

IBM Security QRadar との互換性があるフォーマットでイベントを収集するには、LEEF で syslog イベントを生成するように Lexicon mesh service を構成する必要があります。

手順

1. ネットワーク・デプロイメントで dbContact システムとして構成されている Honeycomb LexCollect システムにログインします。
2. `installImage` ディレクトリーの Honeycomb インストール・ディレクトリーの場所を探索します。

   例: `c:¥Program Files¥Honeycomb¥installImage¥data`
3. `mesh.properties` ファイルを開きます。

   デプロイメントに Honeycomb LexCollect が含まれていない場合は、`mesh.properties` を手動で編集できます。

   例: `c:¥Program Files¥mesh`
4. syslog イベントを LEEF でエクスポートするために、「フォーマッター **(formatter)**」フィールドを編集します。

   例: `formatter=leef`
5. 変更を保存します。

   メッシュ・サービスが、LEEF イベントを出力するように構成されました。Lexicon mesh service については、*Honeycomb* の資料 を参照してください。

QRadar での Honeycomb Lexicon FIM のログ・ソースの構成

IBM Security QRadar は、Honeycomb Lexicon File Integrity Monitor から転送されたファイル保全性イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。

3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. オプション: 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Honeycomb Lexicon File Integrity Monitor**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 176. syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Honeycomb Lexicon FIM インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。 「ログ・ソース **ID**」は、固有値でなければなりません。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
信頼性	リストから、ログ・ソースの「信頼性」を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」による「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	リストから、ログの解析と保管を行うための受信ペイロード・エンコーダーを選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」による「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

11. 「保存」をクリックします。

12. 「管理」タブで「変更のデプロイ」をクリックします。

QRadar に転送された Honeycomb Lexicon File Integrity Monitor イベントは、「ログ・アクティビティー」タブに表示されます。

第 63 章 Hewlett Packard (HP)

IBM Security QRadar は、いくつかの Hewlett Packard (HP) DSM と統合できます。

HP Network Automation

HP Network Automation 用の IBM Security QRadar DSM は HP Network Automation ソフトウェアからイベントを収集します。

以下の表は、HP Network Automation DSM の仕様を示しています。

表 *177. HP Network Automation DSM* の仕様

仕様	値
製造元	Hewlett Packard
DSM 名	HP Network Automation
RPM ファイル名	DSM-HPNetworkAutomation-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	V10.11
プロトコル	Syslog
イベント・フォーマット	LEEF
記録されるイベント・タイプ	すべての操作可能な構成ネットワーク・イベント。
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Hewlett Packard Network Automation (http://www.hpe.com/software/na)

HP Network Automation ソフトウェアを QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下の RPM の最新バージョンをリストされている順に QRadar コンソールにダウンロードします。
   - DSMCommon DSM RPM
   - HP Network Automation DSM RPM
2. LEEF イベントを QRadar に送信するように HP Network Automation ソフトウェアを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで HP Network Automation ログ・ソースを追加してください。以下の表は、HP Network Automation イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 178. *HP Network Automation* ログ・ソースのパラメーター

パラメーター	値
ログ・ソース・タイプ	HP Network Automation
プロトコル構成	Syslog
ログ・ソース ID	QRadar が HP Network Automation イベントを収集するデバイスの IP アドレスまたはホスト名。

以下の表は、HP Network Automation DSM の LEEF メッセージのサンプルを示しています。

表 179. *HP Network Automation* ソフトウェアでサポートされる *HP Network Automation* のサンプル・メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
デバイス・スナップショット	情報	LEEF:1.0|HP|Network Automation|v10|Device Snapshot| devTime=Wed Jul 06 08:26:45 UTC 2016 devTimeFormat=EEE MMM dd HH:mm:ss Z yyyy src=127.0.0.1 eventId=11111111 usrName=UserName eventText=Snapshot of configuration taken

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信のための HP Network Automation ソフトウェアの構成

LEEF イベントを IBM Security QRadar に送信するように HP Network Automation ソフトウェアを構成します。

始める前に

HP Network Automation ソフトウェアのユーザー・インターフェースに対する管理者権限が必要です。

手順

1. HP Network Automation ソフトウェアのユーザー・インターフェースにログインします。
2. 「管理者」メニューで「イベント通知と応答ルール **(Event Notification & Response Rules)**」を選択します。
3. 「新規イベント通知と応答ルール **(New Event Notification & Respone Rule)**」をクリックします。

4. HP Network Automation のパラメーターを構成します。

   以下の表は、LEEF イベントを QRadar に送信する場合のパラメーター値を示しています。

パラメーター	値
指定された **E** メールとイベント・ルールの追加 **(Add Email and Event Rule named)**	任意のストリングを使用できます。例: QRadar_logs。
このアクションの実行方法 **(To take this action)**	リストから「**Syslog** メッセージを送信 **(Send Syslog Message)**」を選択します。
次のイベントが発生した場合 **(When the following events occur)**	1. すべてのイベントを選択します。 2. 「任意の重要度 **(of any importance)**」ボタンを有効にします。 3. ポリシー非準拠イベントに対するアクションを実行するには、「すべてのポリシー **(for all policies)**」ボタンを有効にします。
ルール・ステータス	「アクティブ」ボタンを有効にします。
Syslog ホスト名 **(Syslog Hostname)**	QRadar のホスト名または IP アドレス。
Syslog ポート **(Syslog Port)**	514
Syslog メッセージ	LEEF:1.0|HP|Network Automation|v10| $EventType$|devTime= $EventDate$ devTimeFormat=EE E MMM dd HH:mm:ss Z yyyy src=$IPAddress$ eventId=$EventID$ usrName=$EventUserName$ eventText= $EventText$ **注:** イベント属性はすべてタブで区切られます。例えば、devTime、devTimeFormat などとなります。「**Syslog** メッセージ」の値をテキスト・エディターにコピーしてから、属性がタブで区切られていることを確認し、改行文字をすべて削除します。 **注:** LEEF ヘッダーのバージョン番号 v10 を HP Network Automation ソフトウェアの正確なバージョンに置き換えることができます。フォーマット・ストリングの他のコンポーネントを変更すると、イベントが正規化されないか、あるいは不明なイベントが発生する場合があります。

5. 「保存」をクリックします。

HP ProCurve

HP ProCurve デバイスを IBM Security QRadar と統合し、syslog を使用して、関連するすべての HP Procurve イベントを記録できます。

このタスクについて

以下の手順を実行して、syslog イベントを QRadar に転送するように HP ProCurve デバイスを構成します。

手順

1. HP ProCurve デバイスにログインします。
2. 以下のコマンドを入力して、グローバル構成レベルの変更を行います。

   ```
   config
   ```

   成功した場合、CLI が以下のプロンプトに変化します。

   ```
   ProCurve(config)#
   ```
3. 以下のコマンドを入力します。

   ```
   logging <syslog-ip-addr>
   ```

   ここで、*<syslog-ip-addr>* は、QRadar の IP アドレスです。
4. 構成モードを終了するために、CTRL+Z を押します。
5. コマンド `write mem` を入力して、ご使用の HP ProCurve デバイスの開始構成に現在の構成を保存します。

   これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Active Defense から転送された LEEF 形式からの syslog イベントに対して、ログソースを自動的に検出および作成します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**HP ProCurve**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *180. HP ProCurve* の *syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	HP ProCurve デバイスの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

HP Tandem

HP Tandem デバイスを IBM Security QRadar と統合できます。HP Tandem デバイスは、ログ・ファイル・プロトコル・ソースを使用して、SafeGuard Audit ファイル・イベントを受け入れます。

このタスクについて

ログ・ファイル・プロトコル・ソースにより、QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。HP Tandem DSM は、ログ・ファイル・プロトコル・ソースを使用して、ログ・ファイルの一括ロードをサポートします。

ログ・ファイル・プロトコルを使用するように HP Tandem デバイスを構成する際には、HP Tandem デバイスで構成されているホスト名または IP アドレスが、「リモート・ホスト」パラメーターに構成されているものと同じになっているようにしてください。

SafeGuard Audit ファイル名は、以下の形式を使用します。

```
Annnnnnn
```

単一の英字 `A` の後に、7 桁の 10 進整数 `nnnnnnn` が続きます。この整数は、名前が同じ監査プールで生成されるたびに 1 ずつ増分されます。

これで、QRadar でログ・ソースおよびプロトコルを構成する準備ができました。

手順

1. 「ログ・ソース・タイプ」リストで「**HP Tandem**」を選択します。
2. ログ・ファイル・プロトコルを構成するために、「プロトコル構成」リストで「ログ・ファイル」を選択します。
3. 「イベント・ジェネレーター **(Event Generator)**」リストで、「**HPTANDEM**」を選択します。

   注**:** HP Tandem デバイスと統合するには、システムで現行バージョンのログ・ファイル・プロトコルを実行している必要があります。

   HP Tandem について詳しくは、ベンダーの資料を参照してください。

Hewlett Packard UNIX (HP-UX)

HP-UX デバイスを IBM Security QRadar と統合できます。HP-UX DSM は、syslog を使用してイベントを受け入れます。

このタスクについて

イベントを QRadar に転送するように HP-UX デバイスで syslog を構成できます。

手順

1. HP-UX デバイスのコマンド・ライン・インターフェースにログインします。
2. 以下のファイルを開きます。

   ```
   /etc/syslog.conf
   ```
3. 以下の行を追加します。

   ```
   <facility>.<level><destination>
   ```

   各部分について以下で説明します。
   - *<facility>* は auth です。
   - *<level>* は info です。
   - *<destination>* は、QRadar の IP アドレスです。
4. ファイルを保存して終了します。
5. 以下のコマンドを入力して、syslogd が `syslog.conf` ファイルに対する変更を適用するようにします。

   ```
   kill -HUP `cat /var/run/syslog.pid`
   ```

   注: 逆引用符をコマンド・ラインで使用します。

   これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、HP-UX から転送された syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。

7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Hewlett Packard UniX**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *181. HP-UX syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Hewlett Packard UNIX デバイスの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 64 章 Huawei

IBM Security QRadar は、いくつかの Huawei DSM と統合できます。

Huawei AR シリーズ・ルーター

IBM Security QRadar 用の Huawei AR シリーズ・ルーター DSM は、syslog を使用して、Huawei AR シリーズ・ルーターからイベントを受け入れることができます。

QRadarは、Huawei AR シリーズ・ルーターから転送される、関連するすべての IPv4 イベントを記録します。ご使用のデバイスを QRadar と統合するには、ログ・ソースを作成してから、syslog イベントを転送するように AR シリーズ・ルーターを構成する必要があります。

サポートされるルーター

DSM は、以下の Huawei AR シリーズ・ルーターからのイベントをサポートします。

- AR150
- AR200
- AR1200
- AR2200
- AR3200

ログ・ソースの構成

IBM Security QRadar が Huawei AR シリーズ・ルーターからの受信 syslog イベントを自動的に検出することはありません。

このタスクについて

イベントが自動的に検出されない場合は、QRadar の「管理」タブからログ・ソースを手動で作成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Huawei AR** シリーズ・ルーター」を選択します。

9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Huawei AR シリーズ・ルーターの ID として、ログ・ソースの IP アドレス、ホスト名、または名前を入力します。 Huawei AR シリーズ・ルーター用に作成した各ログ・ソースには、IP アドレスやホスト名などの固有 ID が含まれている必要があります。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。これで、イベントを QRadar に転送するように Huawei AR シリーズ・ルーターを構成する準備ができました。

Huawei AR シリーズ・ルーターの構成

syslog イベントを IBM Security QRadar に転送するには、Huawei AR シリーズ・ルーターをインフォメーション・センターとして構成してから、ログ・ホストを構成する必要があります。

このタスクについて

Huawei AR シリーズ・ルーター用に作成したログ・ホストは、イベントを QRadar コンソールまたはイベント・コレクター (Event Collector)に転送できます。

手順

1. Huawei AR シリーズ・ルーターのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力して、システム・ビューにアクセスします。

```
system-view
```

3. 以下のコマンドを入力して、インフォメーション・センターを有効にします。

```
info-center enable
```

4. 以下のコマンドを入力して、情報レベルのログ・メッセージをデフォルト・チャネルに送信します。

```
info-center source default channel loghost log level informational debug
state off trap state off
```

5. オプション: Huawei AR シリーズ・ルーターのソース構成を確認するために、以下のコマンドを入力します。

```
display channel loghost
```

6. 以下のコマンドを入力して、スイッチのログ・ホストとして QRadar の IP アドレスを構成します。

   ```
   info-center loghost <IP address> facility <local>
   ```

   各部分について以下で説明します。

   - *<IP address>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
   - *<local>* は、syslog ファシリティーです (例えば、local0)。

   例:

   ```
   info-center loghost 10.10.10.1 facility local0
   ```

7. 以下のコマンドを入力して、構成を終了します。

   ```
   quit
   ```

   構成は完了です。「ログ・アクティビティー」タブでイベントを表示することで、QRadar に転送されたイベントを確認できます。

Huawei S シリーズ・スイッチ

IBM Security QRadar 用の Huawei S シリーズ・スイッチ DSM は、syslog を使用して、Huawei S シリーズ・スイッチ・アプライアンスからイベントを受け入れることができます。

QRadar は、Huawei S シリーズ・スイッチから転送される、関連するすべての IPv4 イベントを記録します。ご使用のデバイスを QRadar と統合するには、ログ・ソースを構成してから、syslog イベントを転送するように S シリーズ・スイッチを構成する必要があります。

サポートされるスイッチ

DSM は、以下の Huawei S シリーズ・スイッチからのイベントをサポートします。

- S5700
- S7700
- S9700

ログ・ソースの構成

IBM Security QRadar が Huawei S シリーズ・スイッチからの受信 syslog イベントを自動的に検出することはありません。

このタスクについて

イベントが自動的に検出されない場合は、QRadar の「管理」タブからログ・ソースを手動で作成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Huawei S** シリーズ・スイッチ」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *182. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Huawei S シリーズ・スイッチの ID として、ログ・ソースの IP アドレス、ホスト名、または名前を入力します。 Huawei S シリーズ・スイッチ用に作成した各ログ・ソースには、IP アドレスやホスト名などの固有 ID が含まれている必要があります。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。これで、イベントを QRadar に転送するように Huawei S シリーズ・スイッチを構成する準備ができました。

Huawei S シリーズ・スイッチの構成

syslog イベントを IBM Security QRadar に転送するには、Huawei S シリーズ・スイッチをインフォメーション・センターとして構成してから、ログ・ホストを構成する必要があります。

このタスクについて

Huawei S シリーズ・スイッチ用に作成したログ・ホストは、イベントを QRadar コンソールまたはイベント・コレクター (Event Collector)に転送できます。

手順

1. Huawei S シリーズ・スイッチのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力して、システム・ビューにアクセスします。

```
system-view
```

3. 以下のコマンドを入力して、インフォメーション・センターを有効にします。

```
info-center enable
```

4. 以下のコマンドを入力して、情報レベルのログ・メッセージをデフォルト・チャネルに送信します。

   ```
   info-center source default channel loghost log level informational debug state off trap state off
   ```

5. オプション: Huawei S シリーズ・スイッチのソース構成を確認するために、以下のコマンドを入力します。

   ```
   display channel loghost
   ```

6. 以下のコマンドを入力して、スイッチのログ・ホストとして QRadar の IP アドレスを構成します。

   ```
   info-center loghost <IP address> facility <local>
   ```

   各部分について以下で説明します。

   - <*IP address*> は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
   - <*local*> は、syslog ファシリティーです (例えば、local0)。

   例:

   ```
   info-center loghost 10.10.10.1 facility local0
   ```

7. 以下のコマンドを入力して、構成を終了します。

   ```
   quit
   ```

   構成は完了です。「ログ・アクティビティー」タブでイベントを表示することで、QRadar に転送されたイベントを確認できます。

第 65 章 HyTrust CloudControl

IBM Security QRadar DSM for HyTrust CloudControl は、HyTrust CloudControl デバイスからイベントを収集します。

HyTrust CloudControl DSM の仕様を以下の表に示します。

表 *183. HyTrust CloudControl DSM* の仕様

仕様	値
製造元	Hytrust
DSM 名	HyTrust CloudControl
RPM ファイル名	DSM-HyTrustCloudControl-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	V3.0.2 から V3.6.0 まで
プロトコル	Syslog
記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Hytrust Web サイト (http://www.hytrust.com)

HyTrust CloudControl イベントを収集するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - HyTrust CloudControl DSM RPM
2. Syslog イベントを QRadar に送信するように HyTrust CloudControl デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで HyTrust CloudControl ログ・ソースを追加してください。以下の表は、固有の値を必要とするパラメーターを示しています。HyTrust CloudControl イベントを収集するには、これらの値が必要です。

表 *184. HyTrust CloudControl* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	HyTrust CloudControl
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『QRadar と通信するように HyTrust CloudControl を構成』
HyTrust CloudControl イベントを収集するには、イベントを IBM Security QRadar に送信するようにサード・パーティー・デバイスを構成する必要があります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するように HyTrust CloudControl を構成

HyTrust CloudControl イベントを収集するには、イベントを IBM Security QRadar に送信するようにサード・パーティー・デバイスを構成する必要があります。

手順

1. HyTrust CloudControl にログインします。
2. 「HTA Management Console (HTA 管理コンソール)」で、「構成 **(Configuration)**」 > 「ロギング **(Logging)**」を選択します。
3. 「**HTA** ロギング集計オプション **(HTA Logging Aggregation options**」で、「外部 **(External)**」を選択します。
4. 「ロギング集計テンプレート・タイプ **(Logging Aggregation Template Type)**」のオプションから、「プロプラエタリー **(Proprietary)**」または「**CEF**」を選択します。
5. 「**HTA Syslog** サーバー **(HTA Syslog Servers)**」フィールドに、QRadar の IP アドレスを入力します。

第 66 章 IBM

IBM Security QRadar は複数の IBM DSM をサポートしています。

IBM AIX DSM

IBM Security QRadarには、IBM AIX® デバイスからの監査イベントまたはオペレーティング・システム・イベントを収集して構文解析するための IBM AIX 監査 DSM および IBM AIX サーバー DSM が用意されています。

IBM AIX サーバー DSM の概要

IBM AIX サーバー DSM は、IBM AIX アプライアンスと対話したり、IBM AIX アプライアンスにログインしたりするユーザーのために、Syslog を使用してオペレーティング・システム・イベントおよび認証イベントを収集します。

以下の表は、IBM AIX DSM サーバーの仕様を示しています。

表 *185. IBM AIX* サーバー *DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM AIX Server
RPM ファイル名	DSM-IBMAIXServer-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	V5.X、V6.X、および V7.X
プロトコル・タイプ	Syslog
QRadar で記録されるイベント・タイプ	ログイン・イベントまたはログオフ・イベント セッションのオープン・イベントまたはセッションのクローズ・イベント パスワードの受け入れイベントおよびパスワード失敗イベント オペレーティング・システム・イベント
自動的に検出?	はい
ID を含む?	はい
その他の情報	IBM Web サイト (http://www.ibm.com/)

IBM AIX サーバー・イベントを QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの IBM AIX サーバー DSM をダウンロードしてください。

2. Syslog イベントを QRadar に送信するように IBM AIX サーバー・デバイスを構成します。
3. IBM AIX サーバー・デバイスの Syslog ベースのログ・ソースを構成します。以下のプロトコル固有のパラメーターを使用します。

パラメーター	説明
ログ・ソース・タイプ	IBM AIX サーバー
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『Syslog イベントを QRadar に送信するように IBM AIX サーバー・デバイスを構成する』

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Syslog イベントを QRadar に送信するように IBM AIX サーバー・デバイスを構成する

手順

1. root ユーザーとして、IBM AIX アプライアンスにログインします。
2. /etc/syslog.conf ファイルを開きます。
3. システム認証ログを QRadar に転送するために、以下の行をファイルに追加します。

   ```
   auth.info @QRadar_IP_address
   ```

   タブで auth.info と QRadar の IP アドレスを区切る必要があります。 例えば、以下のようにします。

   ```
   ##### begin /etc/syslog.conf
   mail.debug /var/adm/maillog
   mail.none /var/adm/maillog
   auth.notice /var/adm/authlog
   lpr.debug /var/adm/lpd-errs
   kern.debug /var/adm/messages
   *.emerg;*.alert;*.crit;*.warning;*.err;*.notice;*.info /var/adm/messages
   auth.info            @<10.100.100.1>
   ##### end /etc/syslog.conf
   ```
4. ファイルを保存して終了します。
5. syslog サービスを再起動します。

   ```
   refresh -s syslogd
   ```

IBM AIX Audit DSM の概要

IBM AIX Audit DSM は、IBM AIX アプライアンスで発生したイベントの詳細な監査情報を収集します。

以下の表は、IBM AIX Audit DSM の仕様を示しています。

表 *186. IBM AIX Audit DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM AIX 監査
RPM ファイル名	DSM-IBMAIXAudit-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	V6.1 および V7.1
プロトコル・タイプ	Syslog ログ・ファイル・プロトコル
QRadar で記録されるイベント・タイプ	監査イベント
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	IBM Web サイト (http://www.ibm.com/)

IBM AIX 監査イベントを QRadar に統合するには、以下のステップを実行します。

1. 最新バージョンのIBM AIX 監査 DSM をダウンロードします。
2. Syslog イベントの場合、以下のステップを実行します。
   a. QRadar に Syslog イベントを送信するように、IBM AIX 監査デバイスを構成します。 463 ページの『Syslog イベントを QRadar に送信するように IBM AIX 監査 DSM を構成する』を参照してください。
   b. QRadar がログ・ソースを自動的に検出しない場合は、IBM AIX 監査のログ・ソースを追加します。ログ・ソース構成では、IBM AIX 監査に固有の以下の値を使用します。

パラメーター	値
ログ・ソース・タイプ	IBM AIX 監査
プロトコル構成	Syslog

3. ログ・ファイル・プロトコル・イベントの場合、以下のステップを実行します。
   a. 監査ログをログ・ファイル・プロトコル・フォーマットに変換するように IBM AIX 監査デバイスを構成します。
   b. IBM AIX 監査デバイスのログ・ファイル・プロトコル・ベースのログ・ソースを構成します。ログ・ソース構成では、プロトコルに固有の以下の値を使用します。

パラメーター	値
ログ・ソース・タイプ	IBM AIX 監査

パラメーター	値
プロトコル構成	ログ・ファイル
サービス・タイプ	リモート・サーバーからログ・ファイルを取得するためのプロトコル。 **重要:** サービス・タイプとして SCP および SFTP を選択する場合、「リモート **IP/**ホスト名」パラメーターに指定されているサーバーの SFTP サブシステムが有効になっていることを確認します。
リモート・ポート	イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合、ポート値を調整します。
SSH 鍵ファイル	サービス・タイプとして SCP または SFTP を選択する場合、このパラメーターを使用して SSH 秘密鍵ファイルを定義します。SSH 鍵ファイルを指定すると、「リモート・パスワード **(Remote Password)**」パラメーターは無視されます。
リモート・ディレクトリー	ファイルを取得するリモート・ホスト上のディレクトリーの場所。ログインするために使用しているユーザー・アカウントに関連する場所を指定します。 **制約事項:** FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートするために、リモート・ディレクトリーをブランクのままにします。
FTP ファイル・パターン	FTP ファイル・パターンは、監査スクリプトの **-n** パラメーターで AIX 監査ファイルに割り当てた名前と一致する必要があります。例えば、名前が AIX_AUDIT で始まり、タイム・スタンプ値で終わるファイルを収集するには、`AIX_Audit_*` と入力します。
FTP 転送モード	ログ・ファイル・プロトコルで FTP を使用して取得されるテキスト・イベント・ログには、ASCII が必要です。
プロセッサー	NONE
ローカル・ディレクトリーの変更	このチェック・ボックスはクリアのままにしておきます。

パラメーター	値
イベント・ジェネレーター **(Event Generator)**	LineByLine イベント・ジェネレーターは、取得されたイベント・ファイルに複数の処理を適用します。ファイルの各行が、単一イベントです。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『Syslog イベントを QRadar に送信するように IBM AIX 監査 DSM を構成する』
IBM AIX 監査デバイスから Syslog 監査イベントを収集するには、監査ログ出力を IBM AIX デバイスから IBM Security QRadar コンソールまたはイベント・コレクターにリダイレクトします。

464 ページの『ログ・ファイル・プロトコル・イベントを QRadar に送信するように IBM AIX 監査 DSM を構成する』
IBM AIX 監査ログを QRadar で読み取り可能なイベント・ログ・フォーマットに変換する必要があるたびに実行する、audit.pl スクリプトを構成します。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Syslog イベントを QRadar に送信するように IBM AIX 監査 DSM を構成する

IBM AIX 監査デバイスから Syslog 監査イベントを収集するには、監査ログ出力を IBM AIX デバイスから IBM Security QRadar コンソールまたはイベント・コレクターにリダイレクトします。

このタスクについて

IBM AIX アプライアンス上で、監査構成に含まれるクラスを有効または無効にすることができます。IBM AIX のデフォルト・クラスは、多数の監査イベントをキャプチャーします。パフォーマンスの問題を回避するために、IBM AIX アプライアンスを調整して、収集されるクラスの数を減らすことができます。監査クラスについて詳しくは、ご使用の IBM AIX アプライアンスの資料を参照してください。

手順

1. IBM AIX アプライアンスにログインします。
2. 監査構成ファイルを開きます。

   ```
   /etc/security/audit/config
   ```

3. 「開始」セクションを編集して、**binmode** エレメントを無効にし、**streammode** エレメントを有効にします。

```
binmode = off
streammode = on
```

4. 「クラス (Classes)」セクションを編集して、監査対象のクラスを指定します。
5. 構成変更を保存します。
6. streamcmds ファイルを開きます。

   ```
   /etc/security/audit/streamcmds
   ```

7. 以下の行をファイルに追加します。

   ```
   /usr/sbin/auditstream | /usr/sbin/auditselect -m -e "command != logger
   && command != auditstream && command != auditpr && command !=
   auditselect"|auditpr -t0 -h eclrRdi -v |sed -e :a -e '$!N;s/¥n / /;ta'
   -e 'P;D'| /usr/bin/logger -p local0.debug -r &
   ```

8. 構成変更を保存します。
9. Syslog 構成ファイルを編集して、デバッグ項目と QRadar コンソールまたはイベント・コレクターの IP アドレスを指定します。

   ```
   *.debug @ip_address
   ```

   ヒント: タブで *.debug と IP アドレスを区切る必要があります。
10. 構成変更を保存します。
11. Syslog 構成を再ロードします。

    ```
    refresh -s syslogd
    ```

12. IBM AIX アプライアンスで監査スクリプトを開始します。

    ```
    audit start
    ```

次のタスク

IBM AIX 監査 DSM は、IBM AIX から QRadar に転送された Syslog 監査イベントを自動的に検出し、ログ・ソースを作成します。イベントが自動的に検出されない場合は、手動でログ・ソースを構成できます。

ログ・ファイル・プロトコル・イベントを QRadar に送信するように IBM AIX 監査 DSM を構成する

IBM AIX 監査ログを QRadar で読み取り可能なイベント・ログ・フォーマットに変換する必要があるたびに実行する、audit.pl スクリプトを構成します。

始める前に

監査スクリプトを使用するには、バージョン 5.8 以降の Perl を IBM AIX アプライアンスにインストールする必要があります。

このタスクについて

この手順では、以下の 2 つのファイルを構成する必要があります。

監査構成ファイル
: 監査構成ファイルは、監査対象のイベント・クラスと、IBM AIX アプライ

アンス上のイベント・ログ・ファイルの場所を識別します。IBM AIX のデフォルト・クラスは、多数の監査イベントをキャプチャーします。パフォーマンスの問題を回避するために、これらのクラスを監査構成ファイルに構成できます。監査クラスの構成について詳しくは、IBM AIX の資料を参照してください。

監査スクリプト

監査スクリプトは、監査構成ファイルを使用して、読み取る監査ログを識別し、バイナリー・ログを QRadar で読み取り可能な単一行のイベントに変換します。これにより、ログ・ファイル・プロトコルが IBM AIX アプライアンスからイベント・ログを取得して、イベントを QRadar にインポートできるようになります。監査スクリプトは、バイナリー監査レコードを QRadar で読み取り可能なイベント・ログ・ファイルに変換するために、audit.pr ファイルを使用します。

監査レコードを読み取り可能なイベントに変換する必要がある場合は、毎回監査スクリプトを実行します。クーロン・ジョブを使用すると、このプロセスを自動化できます。例えば、`0 * * * * /audit.pl` を追加すると、監査スクリプトを 1 時間ごとに実行できます。詳しくは、システムの資料を参照してください。

手順

1. IBM AIX アプライアンスにログインします。
2. 監査構成ファイルを構成します。
   a. 監査構成ファイルを開きます。

      ```
      etc/security/audit/config
      ```

   b. 「開始」セクションを編集して、**binmode** エレメントを有効にします。

      ```
      binmode = on
      ```

   c. 「開始」セクションの構成を編集して、バイナリー監査ログを格納するディレクトリーを決定します。 IBM AIX 監査のデフォルト構成では、バイナリー・ログは以下のディレクトリーに書き込まれます。

      ```
      trail = /audit/trail
      bin1 = /audit/bin1
      bin2 = /audit/bin2
      binsize = 10240
      cmds = /etc/security/audit/bincmds
      ```

      通常は、bin1 および bin2 ディレクトリー内のバイナリー・ファイルを編集する必要はありません。

   d. 「クラス (Classes)」セクションの構成を編集し、監査対象のクラスを決定します。クラスの構成については、IBM AIX の資料を参照してください。
   e. 構成変更を保存します。
3. IBM AIX システムで監査を開始するには、以下のようにします。

   ```
   audit start
   ```

4. 監査スクリプトをインストールします。
   a. IBM サポート Web サイト (http://www.ibm.com/support) にアクセスします。

b. audit.pl.gz ファイルをダウンロードします。

c. 監査スクリプトを、IBM AIX アプライアンス上のフォルダーにコピーします。

d. ファイルを解凍します。

```
tar -zxvf audit.pl.gz
```

e. 監査スクリプトを開始します。

```
./audit.pl
```

以下のパラメーターを追加することで、コマンドを修正できます。

パラメーター	説明
-r	監査スクリプトが QRadar のイベント・ログ・ファイルの書き込み先とする結果ディレクトリーを定義します。 結果ディレクトリーを指定しない場合、スクリプトは、イベントを /audit/results/ ディレクトリーに書き込みます。結果ディレクトリーは、「リモート・ディレクトリー **(Remote Directory)**」パラメーターで使用されます。ログ・ソース構成では、このパラメーターの値を使用します。エラーを回避するために、結果ディレクトリーが IBM AIX システム上に存在することを確認してください。
-n	監査スクリプトによって生成されるイベント・ログ・ファイルの固有の名前を定義します。ログ・ソース構成の「**FTP** ファイル・パターン **(FTP File Pattern)**」パラメーターは、この名前を使用して、ログ・ソースが QRadar 内から取得しなければならないイベント・ログを識別します。
-l	最終レコード・ファイルの名前を定義します。
-m	IBM AIX システムで保持する監査ファイルの最大数を定義します。デフォルトでは、スクリプトは 30 個の監査ファイルを保持します。監査ファイルの数が **-m** パラメーターの値を超えると、スクリプトは最も古いタイム・スタンプを持つ監査ファイルを削除します。
-t	監査証跡ファイルを格納するディレクトリーを定義します。デフォルトのディレクトリーは /audit/trail です。

次のタスク

IBM AIX 監査 DSM は、IBM AIX から QRadar に転送されたログ・ファイル・プロトコル監査イベントを自動的に検出し、ログ・ソースを作成します。イベントが自動的に検出されない場合は、手動でログ・ソースを構成できます。

IBM AS/400 iSeries DSM

IBM Security QRadar DSM for IBM AS/400 iSeries は、IBM AS/400 iSeries デバイスから監査レコードおよびイベント情報を収集します。

以下の表は、IBM AS/400 iSeries DSM の仕様を示しています。

表 *187. IBM AS/400 iSeries DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM AS/400 iSeries
サポートされるバージョン	V5R4 以降
RPM ファイル名	DSM-IBMiSeries-*Qradar_version-build_number*.noarch.rpm
プロトコル	ログ・ファイル・プロトコル Syslog
記録されるイベント・タイプ	レコードおよびイベントの監査
自動的に検出?	いいえ
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	IBM Web サイト (http://www.ibm.com/)

IBM AS/400 iSeries デバイスからイベントを収集するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの IBM AS/400 iSeries DSM RPM をダウンロードして QRadar コンソールにインストールしてください。
2. QRadar と通信するように IBM AS/400 iSeries デバイスを構成します。
3. 次の表を使用して、IBM AS/400 iSeries のイベントを収集するために必要なパラメーターを構成することで、QRadar コンソールに IBM AS/400 iSeries ログ・ソースを追加します。

表 *188. IBM AS/400 iSeries* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	IBM AS/400 iSeries

表 188. IBM AS/400 iSeries ログ・ソース・パラメーター (続き)

パラメーター	値
プロトコル構成	ログ・ファイル PowerTech Interact または LogAgent for System i ソフトウェアを使用して CEF 形式の syslog メッセージを収集する場合は、「**Syslog**」オプションを選択する必要があります。
サービス・タイプ	セキュア・ファイル転送プロトコル (SFTP)

関連タスク:

『IBM Security QRadar と統合するための IBM i の構成』
IBM i を IBM Security QRadar と統合できます。

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

472 ページの『QRadar と統合するように Townsend Security Alliance LogAgent を構成』
Townsend Security Alliance LogAgent から、すべての監査ログおよびシステム・イベントを収集できます。IBM Security QRadar の LEEF 用に Alliance LogAgent を構成し、Syslog サーバーとして QRadar を指定する宛先を構成する必要があります。

IBM Security QRadar と統合するための IBM i の構成

IBM i を IBM Security QRadar と統合できます。

手順

1. IBM Fix Central (http://www.ibm.com/support/fixcentral) から、次のファイルをダウンロードします。

   ```
   AJLIB.SAVF
   ```

2. AJLIB.SAVF ファイルを、IBM i に FTP でアクセスできるコンピューターまたは端末にコピーします。
3. 以下のコマンドを入力して、IBM i で汎用オンライン SAVF ファイルを作成します。

   ```
   CRTSAVF QGPL/SAVF
   ```

4. コンピューターまたは端末で FTP を使用して、IBM i の汎用 SAVF ファイルを、ダウンロードした AJLIB.SAVF ファイルに置き換えます。

   以下のコマンドを入力します。

```
bin
cd qgpl
lcd c:¥
put ajlib.savf savf
quit
```

別の IBM i システムから SAVF ファイルを転送する場合、GET ステートメントまたは PUT ステートメントの前に、FTP サブコマンド・モード BINARY を配置します。

5. 次のコマンドを入力することで、IBM i 上の AJLIB ファイルを復元します。

   ```
   RSTLIB SAVLIB(AJLIB) DEV(*SAVF) SAVF(QGPL/AJLIB)
   ```

   AJLIB は、IBM i の監査ジャーナル項目を QRadar に送信するために必要なマッピングおよびデータ転送のサポートを提供します。

6. **AJLIB/SETUP** を実行します。

   セットアップ画面は、処理された項目を受信するための FTP、SFTP、またはローカル・パス用に AJLIB を構成するために使用します。

   FTP や SFTP にはサーバーのユーザー ID が、FTP にはパスワードが必要です。FTP は行区切り文字の変換を処理しますが、SFTP 転送を受信するシステムのタイプについては、改行はユーザーが予期する値に設定します。

7. SFTP を使用する場合、**AJLIB/GENKEY** を実行します。

   このコマンドにより、SFTP 認証に必要な SSH 鍵ペアが生成されます。この鍵ペアが存在する場合、置き換えられることはありません。新しい鍵ペアを生成する場合、このコマンドを実行する前に、/ajlib/.ssh ディレクトリーから既存の鍵ファイルを削除してください。

   IBM i 上での SSH 鍵ペア構成について詳しくは、http://www-01.ibm.com/support/docview.wss?uid=nas8N1012710 を参照してください。

8. 鍵ペアの生成後、次の手順を使用して、サーバー上での鍵ペアの使用を有効にします。
   a. id_rsa.pub ファイルを、/ajlib ディレクトリーから SSH サーバーにコピーし、該当するフォルダーにインストールします。
   b. **AJLIB/AUDITJRN** コマンドを実行するユーザー・プロファイルの known_hosts ファイルに、SSH サーバーが追加されていることを確認します。

9. 該当のユーザー・プロファイルを使用して、次の手順を実行します。
   a. 次のコマンドを入力することで、PASE (ポータブル・アプリケーション・ソリューション環境) シェルを開始します。

      ```
      call qp2term
      ```

   b. 次のコマンドを入力することで、SSH サーバーとのセッションを開始します。

      ```
      ssh -T <user>@<serveraddress>
      ```

   c. プロンプトが表示されたら、システム・キーを受け入れ、パスワードを入力します。

d. exit と入力して SSH セッションを終了します。

AJLIB/AUDITRN コマンドを実行するのとは異なる IBM i プロファイルでこれらの手順を実行する場合は、このコマンドを実行するプロファイルのホーム・ディレクトリーに、.ssh ディレクトリー、および known_hosts ファイルをコピーします。

10. 特定の項目タイプのフィルター処理を構成するには、**AJLIB/SETENTTYP** コマンドを使用します。
11. 次のコマンドを入力することで、監査ジャーナル・ライブラリー (AJLIB) のデータ収集の開始日時をセットアップします。

    AJLIB/DATETIME

    監査ジャーナル収集プログラムを開始すると、失敗メッセージが QSYSOPR に送信されます。

    セットアップ機能により、監査ジャーナルからのデータ収集のデフォルト開始日時が、現在の日の 08:00:00 に設定されます。

    前のインストールの前の開始日時の情報を保持するには、**AJLIB/DATETIME** を実行する必要があります。前の開始日時を記録し、**AJLIB/SETUP** を実行する際に、それらの値を入力します。開始日時には、6 文字のシステム日付およびシステム時刻フォーマットの有効な日時が含まれていなければなりません。終了日時は、有効な日時であるか、空白のままにする必要があります。
12. **AJLIB/AUDITJRN** を実行します。

    監査ジャーナルの収集プログラムが開始し、レコードをリモート FTP サーバーに送信します。FTP サーバーへの転送に失敗すると、メッセージが QSYSOPR に送信されます。**AJLIB/AUDITJRN** を開始するプロセスは、通常、定期的にレコードを収集する IBM i のジョブ・スケジューラーによって自動化されています。

    FTP 転送が成功した場合、現在の日時情報が **AJLIB/DATETIME** の開始時刻に書き込まれて、収集時間が更新されます。終了時刻は、空白に設定されます。FTP 転送が失敗した場合、エクスポート・ファイルが消去され、収集日時の更新は行われません。

IBM AS/400 iSeries のジャーナル項目の手動での抽出

監査ジャーナル・レシーバー・チェーンが破損している場合は、DSPJRN コマンドを実行して、IBM AS/400 iSeries のジャーナル項目を抽出できます。

このタスクについて

ALJIB/DATETIME コマンドを実行して、開始日を *OUTF に設定します。このコマンドは、日時を使用する代わりに構文解析用の事前作成 QTEMP/AUDITJRN outfile を使用してジャーナル項目を抽出するように、処理プログラムに強制します。構文解析プログラム・コマンド AJLIB/AUDITJRN を実行した後で、DATETIME は新しい処理日に設定されます。

手順

1. IBM AS/400 iSeries デバイスのコマンド・ライン・インターフェース (CLI) にログインします。
2. **DSPJRN** を実行します。

   以下の例で変更可能なパラメーターは、**RCVRNG** および **ENTTYP** のみです。その他のコマンド・パラメーターは変更しないでください。**ENTTP** が **AJLIB/SETENTTYP** コマンド設定と一致していることを確認してください。

   ```
   DSPJRN JRN(QSYS/QAUDJRN) RCVRNG(AUDRCV0001 AUDRCV0003)
   JRNCDE((T)) ENTTYP(*ALL)
   OUTPUT(*OUTFILE) OUTFILFMT(*TYPE5) OUTFILE(QTEMP/AUDITJRN)
   ENTDTALEN(*VARLEN 16000 100)
   ```

3. outfile ***OUTF** サポートを使用するように「日時 **(Date Time)**」を設定するには、**AJLIB/DATETIME** コマンドを実行します。

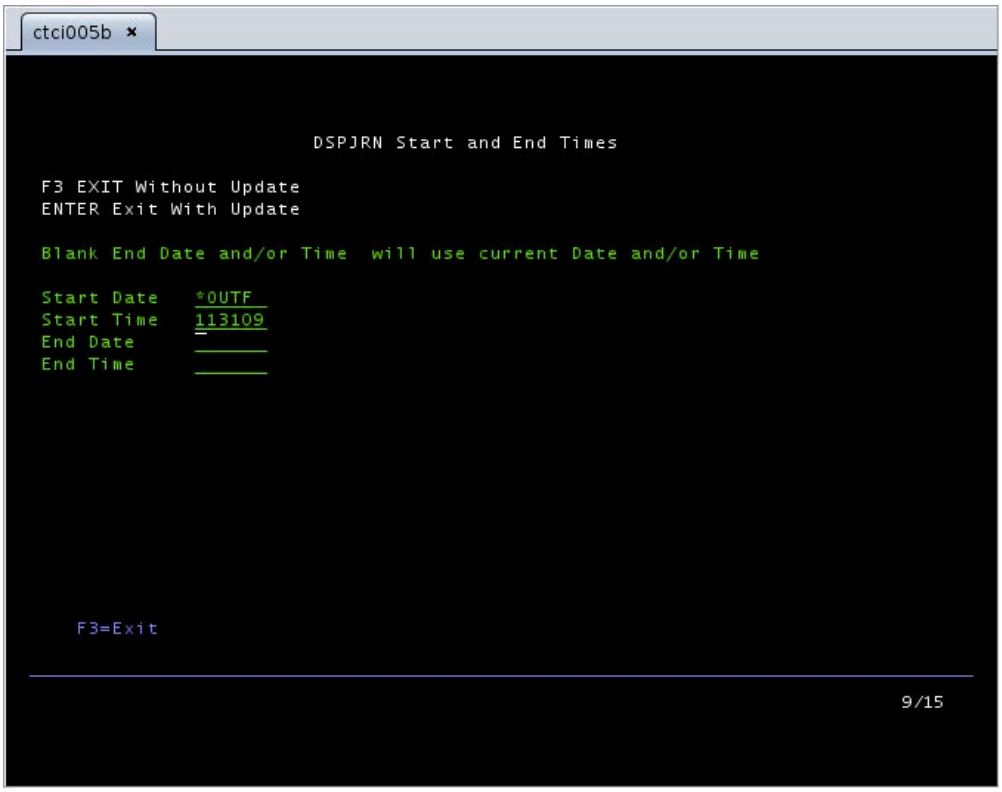

図 *1. DSPJRN* の開始時刻および終了時刻

4. **AJLIB/AUDITJRN** を実行します。

タスクの結果

DATETIME は次の開始日に設定されます。

ログ・ファイル・プロトコルを使用したデータのプル

以下のように、IBM AS/400 iSeries をログ・ソースとして構成し、IBM Security QRadar でログ・ファイル・プロトコルを使用するように構成できます。

手順

1. IBM AS/400 iSeries からイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「IBM AS/400 iSeries」オプションを選択する必要があります。
2. IBM AS/400 iSeries DSM 用にログ・ファイル・プロトコルを構成するには、「プロトコル構成」リストで「ログ・ファイル」オプションを選択し、FTP サーバー接続設定の場所を定義する必要があります。

   注**:** PowerTech Interact または LogAgent for System i ソフトウェアを使用して CEF フォーマットの syslog メッセージを収集する場合は、「プロトコル構成」リストで「**Syslog**」オプションを選択する必要があります。
3. ファイルの転送にセキュア・プロトコル (Secure File Transfer Protocol (SFTP) など) を選択したログ・ファイル・プロトコル・オプションを使用します。

QRadar と統合するように Townsend Security Alliance LogAgent を構成

Townsend Security Alliance LogAgent から、すべての監査ログおよびシステム・イベントを収集できます。IBM Security QRadar の LEEF 用に Alliance LogAgent を構成し、Syslog サーバーとして QRadar を指定する宛先を構成する必要があります。

手順

1. Townsend Security Alliance LogAgent アプライアンスにログインします。
2. コマンド **addlible allsy1100** を入力することで、ライブラリー・リストに「**ALLSYL100**」を追加します。
3. メインメニューを表示するには、「**go symain**」を選択します。
4. 構成のためのオプションを選択します。
5. 「**Configure Alliance LogAgent**」を選択し、次のパラメーターを構成します。

パラメーター	説明
Interface version	4=IBM QRadar LEEF
Transmit	1=Yes
Data queue control	1=Yes
フォーマット	4=IBM QRadar LEEF

6. 構成メニューで、「**Work With TCP Clients**」を選択します。
7. オプション 2 を選択して、「**SYSLOGD**」クライアントを変更し、次のパラメーターを構成します。

パラメーター	説明
Status	1=Active
Autostart client	1=Yes
Remote IP address	QRadar の IP アドレス
Remote port number	514

8. 「**Configuration**」メニューで、「**Start LogAgent Subsystem**」を選択します。イベントが QRadar に流れます。

次のタスク

TCP サービスが開始したら、IPL QSTRUP プログラムに次のステートメントを含めることで、Alliance LogAgent サブシステムを自動的に始動することを検討してください。

```
/* START ALLIANCE LOGAGENT */
QSYS/STRSBS ALLSYL100/ALLSYL100
MONMSG MSGID(CPF0000)
```

「**Independent Auxiliary Storage Pool**」操作用のインストール方法および構成方法、およびイベントのフィルター・オプションについて詳しくは、ベンダーの資料を参照してください。

IBM BigFix

IBM Security QRadar 用の IBM BigFix DSM は、IBM BigFix から取得するシステム・イベントをログ・イベント拡張フォーマット (LEEF) で受け入れます。

IBM BigFix は、以前は IBM Tivoli® Endpoiont Manager と呼ばれていました。

QRadar は、IBM BigFix SOAP プロトコルを使用して 30 秒間隔でイベントを取得します。イベントを取得すると、IBM BigFix DSM が QRadar 用にイベントを解析して分類します。IBM BigFix の SOAP API は、Web レポート・アプリケーションをインストールしてある場合にのみ使用できます。IBM BigFix の Web レポート・アプリケーションは、IBM BigFix のシステム・イベント・データを取得し、QRadar と統合するために必要です。

注**:** QRadar は、IBM BigFix バージョン 8.2.x から 9.5.2 をサポートします。

IBM BigFix を QRadar に統合するには、ログ・ソースを手動で構成する必要があります。IBM BigFix のイベントは自動的に検出されません。

- QRadar にログインします。
- 「管理」タブをクリックします。
- 「ログ・ソース」アイコンをクリックします。
- 「追加」をクリックします。
- 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
- 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
- 「ログ・ソース・タイプ」リストから「**BigFix**」を選択します。
- 「プロトコル構成」リストから「**BigFix SOAP**」を選択します。

以下の値を構成します。

IBM BigFix SOAP プロトコル構成

パラメーター	説明
ログ・ソース **ID**	IBM BigFix アプライアンスの IP アドレスまたはホスト名を入力します。 IP アドレスまたはホスト名により、IBM BigFix が QRadar 内で固有のイベント・ソースとして識別されます。
ポート	SOAP API を使用して IBM BigFix に接続するために使用するポート番号を入力します。 デフォルトでは、ポート 80 が IBM BigFix と通信するためのポート番号です。HTTPS を使用する場合、このフィールドをご使用のネットワークの HTTPS ポート番号に更新する必要があります。ほとんどの構成で、HTTPS 通信にはポート 443 が使用されます。
HTTPS の使用	HTTPS を使用して接続するには、このチェック・ボックスを選択します。 このチェック・ボックスを選択すると、指定したホスト名または IP アドレスは HTTPS を使用して IBM BigFix に接続します。HTTPS を使用して接続するために証明書が必要な場合、QRadar コンソールまたは管理対象ホストで要求される証明書を以下のディレクトリーにコピーします。 `/opt/qradar/conf/trusted_certificates` QRadar は、ファイル拡張子 `.crt`、`cert`、または `.der` を持つ証明書をサポートします。必要なすべての証明書をトラステッド証明書ディレクトリーにコピーしてから、変更内容を保存し、デプロイします。
ユーザー名	IBM BigFix へのアクセスに必要なユーザー名を入力します。
パスワード	IBM BigFix へのアクセスに必要なパスワードを入力します。
パスワードの確認	IBM BigFix へのアクセスに必要なパスワードを確認します。

IBM BigFix 脆弱性評価情報をインポートするように QRadar を構成する方法について詳しくは、「*IBM Security QRadar Vulnerability Assessment* 構成ガイド」を参照してください。

「保存」をクリックします。

「管理」タブで「変更のデプロイ」をクリックします。

関連概念:

16 ページの『IBM BigFix SOAP プロトコル構成オプション』

IBM BigFix アプライアンスからログ拡張イベント・フォーマット (LEEF) 形式のイベントを受信するには、IBM BigFix SOAP プロトコルを使用するログ・ソースを構成します。

IBM Bluemix プラットフォーム

IBM Bluemix プラットフォーム用の IBM Security QRadar DSM は、ご使用の Bluemix プラットフォームからイベント・ログを収集します。

以下の表は、Bluemix Platform DSM の仕様を示しています。

表 *189. Bluemix Platform DSM* の仕様

仕様	値
製造元	IBM
DSM 名	Bluemix Platform
RPM ファイル名	DSM-IBMBluemixPlatform-*7.x-xxxxxxx*.noarch.rpm
サポートされるバージョン	N/A
プロトコル	Syslog、TLS Syslog
記録されるイベント・タイプ	すべてのシステム (Cloud Foundry) イベント、一部のアプリケーション・イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Bluemix の IBM Web サイト (Bluemix の IBM Web サイト)

Bluemix Platform を QRadar に統合するには、以下の手順を実行します。

インストール、サード・パーティー構成、および QRadar 構成手順を、この順序で実行する必要があります。インストールは常に最初に行う必要がありますが、その他の 2 つの手順の順序は逆転させることができます。場合によっては、サード・パーティー構成には何のアクションも必要ではないことがあり、この手順を省略できます。

1. 自動更新が有効になっていない場合は、最新バージョンの Bluemix Platform DSM RPM をダウンロードして、QRadar コンソールにインストールします。
2. Syslog イベントを QRadar に送信するように Bluemix Platform デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Bluemix Platform ログ・ソースを追加してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に Bluemix Platform を構成する

Bluemix プラットフォーム・イベントを収集するには、イベントを QRadar に送信するようにサード・パーティー製のインスタンスを構成する必要があります。

始める前に

ログ・ドレーンを作成するには、Bluemix でアプリケーションが実行中である必要があります。

手順

1. Cloud Foundry コマンド・ライン・インターフェースで、次のコマンドを入力してドレーンを作成します。

   ```
   cf cups drain_name -l syslog://QRadar_IP_Address:514
   ```

   別の方法としては、次のコマンドを使用します。

   ```
   cf cups drain_name -l syslog-tls://QRadar_IP_Address:1513
   ```

   1513 は、QRadar と通信するために使用するポートです。
2. 次のコマンドを使用して、サービス・インスタンスをバインドします。

   ```
   cf bind-service BusinessApp_name drain_name
   ```

QRadar との Bluemix プラットフォームの統合

ほとんどのインストール済み環境には、RPM のみがあります。複数の RPM (PROTOCOL RPM と DSMCommon RPM など) が必要なインストール済み環境では、RPM の依存関係をインストールの順序に反映するようにしてください。

手順

1. 必要に応じて、QRadar コンソールに最新の TLS Syslog RPM をダウンロードしてインストールします。 DSM を手動でインストール手順を使用することで、プロトコルをインストールできます。プロトコル更新をインストールするように自動更新が構成されている場合、この手順は不要です。
2. 最新の DSMCommon RPM をQRadar コンソール にダウンロードしてインストールします。DSM 更新をインストールするように自動更新が構成されている場合、この手順は不要です。
3. 最新の Bluemix Platform RPM をQRadar コンソール にダウンロードしてインストールします。DSM 更新をインストールするように自動更新が構成されている場合、この手順は不要です。

次のタスク

Syslog または Syslog TLS を使用することで、QRadar 内に Bluemix ログ・ソースを構成する必要があります。

Syslog を使用するように Bluemix ログ・ソースを構成

IBM Security QRadar で Bluemix ログ・ソースを構成できます。

手順

1. 「**Syslog**」を使用するために、QRadar にログインします。

2. 「管理」タブで「データ・ソース」 > 「ログ・ソース」 > 「追加」をクリックします。
3. 「ログ・ソース・タイプ」リストで、「**Bluemix** プラットフォーム **(Bluemix Platform)**」を選択します。
4. 「プロトコル構成」リストで「**Syslog**」を選択します。
5. 「ログ・ソース **ID**」フィールドに、Bluemix Loggregator の IP アドレスを入力します。

   重要**:** ログ・ソース ID として、IP アドレスおよびポートを含めることが必要な場合があります。例: `1.1.1.1:1234`。
6. 「ログ・ソース」ウィンドウ内の残りのフィールドを必要に応じて構成し、「保存」をクリックします。
7. 「管理」タブのツールバーで「変更のデプロイ」をクリックします。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

TLS Syslog を持つ Bluemix ログ・ソースの構成

IBM Security QRadar で、TLS Syslog を使用する Bluemix ログ・ソースを構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブで「データ・ソース」 > 「ログ・ソース」 > 「追加」をクリックします。
3. 「ログ・ソース・タイプ」リストで、「**Bluemix** プラットフォーム **(Bluemix Platform)**」を選択します。
4. 「プロトコル構成」リストで「**TLS Syslog**」を選択します。
5. 「ログ・ソース **ID**」フィールドに、Bluemix Loggregator の IP アドレスを入力します。
6. 「**TLS listen** ポート **(TLS Listen Port)**」フィールドに、ポート番号を入力します。
7. 「認証モード **(Authentication Mode)**」リストで、「**TLS**」を選択します。
8. 「証明書タイプ **(Certificate Type)**」リストで、「証明書を提供 **(Provide Certificate)**」を選択します。
9. 「提供されたサーバー証明書のパス **(Provided Server Certificate Path)**」フィールドに、サーバー証明書への絶対パスを入力します。例:

   ```
   syslog-tls.cert
   ```
10. 「提供された秘密鍵のパス **(Provided Private Key Path)**」フィールドに、秘密鍵への絶対パスを入力します。

秘密鍵は、DER エンコードの PKCS8 鍵である必要があります。

11. 「ログ・ソース」ウィンドウ内の残りのフィールドを必要に応じて構成し、「保存」をクリックします。
12. 「管理」タブのツールバーで「変更のデプロイ」をクリックします。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

IBM CICS

IBM CICS® DSM により、IBM z/OS® メインフレームの IBM 顧客情報管理システム (CICS) からのイベントを、IBM Security zSecure を使用して統合できます。

zSecure プロセスを使用すると、System Management Facilities (SMF) からのイベントは、ログ・イベント拡張フォーマット (LEEF) のイベント・ファイルに記録されます。IBM Security QRadar は、ログ・ファイル・プロトコルを使用して LEEF イベント・ログ・ファイルを取得し、イベントを処理します。ポーリング間隔に基づいてイベントを取得するように QRadar をスケジュールできます。これにより、QRadar は、定義されたスケジュールに基づいてイベントを取得できます。

IBM CICS イベントを統合するには、以下のようにします。

1. インストール済み環境が、前提条件となるインストール要件をすべて満たしていることを確認します。
2. イベントを LEEF 形式で書き込むように IBM z/OS イメージを構成します。詳しくは、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。
3. IBM CICS が LEEF 形式のイベント・ログを取得するために、QRadar でログ・ソースを作成します。詳しくは、 479 ページの『ログ・ソースの作成』を参照してください。
4. オプション。QRadar で IBM CICS 用のカスタム・イベント・プロパティーを作成します。詳しくは、テクニカル・ノート「*IBM Security QRadar Custom Event Properties for IBM z/OS*」を参照してください。

始める前に

データ収集プロセスを構成する前に、基本の zSecure インストール・プロセスを完了する必要があります。

以下の前提条件は必須です。

- z/OS イメージ上の IBM Security zSecure Audit で parmlib メンバーの IFAPRDxx が有効になっていることを確認する必要があります。
- SCKRLOAD ライブラリーは APF が許可されていなければなりません。

- CKFREEZE と UNLOAD のデータ・セットが定期的に更新されるようにプロセスを構成する必要があります。
- LEEF イベント・ファイルをダウンロードするには、QRadar に対して z/OS イメージ上の SFTP、FTP、または SCP の各サーバーを構成する必要があります。
- QRadar と z/OS イメージの間にあるファイアウォールで SFTP トラフィック、FTP トラフィック、または SCP トラフィックを許可する必要があります。

ソフトウェアをインストールしたら、ポストインストール・アクティビティーを実行して、構成を作成および変更します。 zSecure のインストールおよび構成の手順については、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。

ログ・ソースの作成

ログ・ファイル・プロトコルにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

このタスクについて

ログ・ファイルは、一度に 1 つずつ、処理のために QRadar に転送されます。ログ・ファイル・プロトコルは、プレーン・テキストのイベント・ログや圧縮ファイル、アーカイブを管理できます。アーカイブには、一度に 1 行ずつ処理できるプレーン・テキスト・ファイルが含まれている必要があります。複数行イベント・ログは、ログ・ファイル・プロトコルではサポートされていません。 zSecure が含まれた IBM z/OS は、指定されたディレクトリーにログ・ファイルを `gzip` アーカイブとして書き込みます。QRadar は、アーカイブを取り出し、ファイルに 1 行当たり 1 イベントで書き込まれているイベントを処理します。

これらのイベントを取得するには、ログ・ファイル・プロトコルを使用するログ・ソースを作成する必要があります。QRadar は、LEEF 形式のイベント・ファイルをホストするシステムにログインするための資格情報と、ポーリング間隔を要求します。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「IBM CICS」を選択します。
7. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
8. 以下の値を構成します。

表 *190. IBM CICS* ログ・ファイル・プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。 QRadar がログ・ファイルを固有のイベント・ソースに識別できるようになるので、IP アドレスまたはホスト名が推奨されます。 例えば、ネットワークに複数のデバイス (例えば、複数の z/OS イメージ)、またはすべてのイベント・ログが入っているファイル・リポジトリーが含まれている場合、IBM CICS ログ・ソースのイベントを一意に識別する、イメージまたは場所の名前、IP アドレス、またはホスト名を指定する必要があります。この指定により、ユーザーが識別可能なネットワークのイメージ・レベルまたは場所のレベルで、イベントを識別できるようになります。
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 • SFTP - SSH ファイル転送プロトコル • FTP - ファイル転送プロトコル • SCP - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 オプションには、以下のポートがあります。 • FTP - TCP ポート 21 • SFTP - TCP ポート 22 • SCP - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているシステムにログインするために必要なユーザー名またはユーザー ID を入力します。 • ログ・ファイルが IBM z/OS イメージ上にある場合は、IBM z/OS にログインするために必要なユーザー ID を入力します。ユーザー ID の長さは 8 文字まで可能です。 • ログ・ファイルがファイル・リポジトリー上にある場合は、ファイル・リポジトリーにログインするために必要なユーザー名を入力します。ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。

表 *190. IBM CICS* ログ・ファイル・プロトコルのパラメーター *(*続き*)*

パラメーター	説明
SSH 鍵ファイル	「サービス・タイプ」として「**SCP**」または「**SFTP**」を選択した場合、このパラメーターにより、SSH 秘密鍵ファイルを定義できます。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」オプションは無視されます。
FTP ファイル・パターン	「サービス・タイプ」として「**SFTP**」または「**FTP**」を選択した場合、これを選択することで、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 IBM Security zSecure Audit を使用する IBM z/OS メインフレームは、`CICS.<timestamp>.gz` というパターンを使用してイベント・ファイルを書き込みます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。例えば、先頭が `zOS` で末尾が `.gz` のファイルを収集するには、以下のコードを入力します。 `CICS.*¥.gz` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として「**FTP**」を選択した場合にのみ表示されます。リストから「バイナリー **(Binary)**」を選択します。 バイナリー転送モードは、`zip`、`gzip`、`tar`、`tar+gzip` アーカイブ・ファイルなど、バイナリー (圧縮) フォーマットで保管されたイベント・ファイルの場合に必要です。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。

表 *190. IBM CICS* ログ・ファイル・プロトコルのパラメーター *(*続き*)*

パラメーター	説明
開始時刻	処理を開始する時刻を入力します。例えば、午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、00:00 と入力します。 このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 (Ignore Previously Processed File)」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「**gzip**」を選択します。 プロセッサーにより、イベント・ファイル・アーカイブを解凍でき、内容がイベント用に処理されます。ファイルは、QRadar にダウンロードされた後にのみ処理されます。QRadar は、zip、gzip、tar、または tar+gzip の各アーカイブ・フォーマットのファイルを処理できます。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって既に処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが以前に処理されているかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。以前に処理されていないすべてのファイルがダウンロードされます。 このオプションは FTP および SFTP のサービス・タイプにのみ適用されます。

表 190. IBM CICS ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスはクリアしたままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これによりファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに複数の処理を適用します。各行が、単一イベントです。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

IBM CICS の構成は完了です。IBM CICS でカスタム・イベント・プロパティーが必要な場合は、テクニカル・ノート「*IBM Security QRadar Custom Event Properties for IBM z/OS*」を参照してください。

IBM DB2

IBM Security QRadar には、IBM DB2 からのイベントを統合するための 2 つのオプションがあります。

以下のトピックを参照してください。

- 『IBM DB2 と LEEF イベントの統合』
- 488 ページの『IBM DB2 監査イベントの統合』

IBM DB2 と LEEF イベントの統合

IBM DB2 DSM により、IBM z/OS® メインフレームからの LEEF 形式の DB2 イベントを、IBM Security zSecure を使用して統合できます。

zSecure プロセスを使用すると、System Management Facilities (SMF) からのイベントは、ログ・イベント拡張フォーマット (LEEF) のイベント・ファイルに記録されます。IBM Security QRadar は、ログ・ファイル・プロトコルを使用して LEEF イベント・ログ・ファイルを取得し、イベントを処理します。ポーリング間隔に基づいてイベントを取得するように QRadar をスケジュールできます。

IBM DB2 イベントを統合するには、以下のようにします。

1. インストール済み環境が、前提条件となるインストール要件をすべて満たしていることを確認します。詳しくは、 484 ページの『始める前に』を参照してください。

2. イベントを LEEF 形式で書き込むように IBM DB2 イメージを構成します。詳しくは、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。
3. IBM DB2 が LEEF 形式のイベント・ログを取得するために、QRadar でログ・ソースを作成します。詳しくは、『IBM DB2 用のログ・ソースの作成』を参照してください。
4. オプション。QRadar で、IBM DB2 用のカスタム・イベント・プロパティーを作成します。詳しくは、テクニカル・ノート「*IBM Security QRadar Custom Event Properties for IBM z/OS*」を参照してください。

始める前に

データ収集プロセスを構成する前に、基本の zSecure インストール・プロセスを完了する必要があります。

以下の前提条件は必須です。

- IBM DB2 z/OS イメージ上の IBM Security zSecure Audit で parmlib メンバーの IFAPRDxx が有効になっていることを確認する必要があります。
- SCKRLOAD ライブラリーは APF が許可されていなければなりません。
- CKFREEZE と UNLOAD のデータ・セットが定期的に更新されるようにプロセスを構成する必要があります。
- LEEF イベント・ファイルをダウンロードするには、QRadar に対して z/OS イメージ上の SFTP、FTP、または SCP の各サーバーを構成する必要があります。
- QRadar と z/OS イメージの間にあるファイアウォールで SFTP トラフィック、FTP トラフィック、または SCP トラフィックを許可する必要があります。

ソフトウェアをインストールした後に、ポストインストール・アクティビティーを実行して、構成を作成および変更する必要があります。zSecure のインストールおよび構成の手順については、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。

IBM DB2 用のログ・ソースの作成

ログ・ファイル・プロトコル・ソースにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

このタスクについて

IBM DB2 DSM は、ログ・ファイル・プロトコル・ソースを使用して、ログ・ファイルの一括ロードをサポートします。ログ・ファイル・プロトコルを使用するように IBM DB2 を構成する際には、IBM DB2 システムで構成されているホスト名または IP アドレスが、ログ・ファイル・プロトコル構成の「リモート・ホスト」パラメーターに構成されているものと同じになっているようにしてください。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。

4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「IBM DB2」を選択します。
8. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
9. 以下の値を構成します。

表 *191. IBM DB2* ログ・ファイル・プロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。 QRadar がログ・ファイルを固有のイベント・ソースに識別できるようになるので、IP アドレスまたはホスト名の使用が推奨されます。 例えば、ネットワークに複数のデバイス (例えば、複数の z/OS イメージ)、またはすべてのイベント・ログが入っているファイル・リポジトリーが含まれている場合、IBM DB2 ログ・ソースのイベントを一意に識別する、イメージまたは場所の名前、IP アドレス、またはホスト名を指定します。このアドレス指定により、ユーザーが識別可能なネットワークのイメージ・レベルまたは場所のレベルで、イベントを識別できるようになります。
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 このオプションには、以下のポートがあります。 • **FTP** - TCP ポート 21 • **SFTP** - TCP ポート 22 • **SCP** - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。

表 *191. IBM DB2* ログ・ファイル・プロトコル・パラメーター *(*続き*)*

パラメーター	説明
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。
SSH 鍵ファイル	「サービス・タイプ」として「**SCP**」または「**SFTP**」を選択した場合、このパラメーターにより、SSH 秘密鍵ファイルを定義できます。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。このオプションにより、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートできます。
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 **SCP** をサービス・タイプとして構成する場合は、「再帰的 **(Recursive)**」オプションは無視されます。
FTP ファイル・パターン	「サービス・タイプ」として「**SFTP**」または「**FTP**」を選択した場合、このオプションにより、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。例えば、末尾が `.del` のコンマ区切りファイルを収集するには、以下のコードを入力します。 `.*.del` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	ASCII FTP ファイル転送モードを必要とするコンマ区切り、テキスト、または ASCII の各ログ・ソースに対して、リストから「**ASCII**」を選択します。 このオプションは、「サービス・タイプ」として「**FTP**」を選択した場合にのみ表示されます。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。

表 191. IBM DB2 ログ・ファイル・プロトコル・パラメーター (続き)

パラメーター	説明
開始時刻	処理を開始する時刻を入力します。例えば、午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、00:00 と入力します。 このパラメーターと「繰り返し **(Recurrence)**」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「なし」を選択します。 プロセッサーにより、イベント・ファイル・アーカイブを解凍し、内容をイベント用に処理できます。ファイルは、QRadar にダウンロードされた後にのみ処理されます。QRadar は、zip、gzip、tar、または tar+gzip の各アーカイブ・フォーマットのファイルを処理できます。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって既に処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが以前に処理されているかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。以前に処理されていないすべてのファイルがダウンロードされます。 このオプションは、「**FTP**」および「**SFTP**」のサービス・タイプにのみ適用されます。

表 191. IBM DB2 ログ・ファイル・プロトコル・パラメーター (続き)

パラメーター	説明
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスはクリアしたままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これにより、ファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに複数の処理を適用します。ファイルの各行が、単一イベントです。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

関連概念:

22 ページの『ログ・ファイル・プロトコルの構成オプション』
リモート・ホストからイベントを受信するには、ログ・ファイル・プロトコルを使用するようにログ・ソースを構成します。

IBM DB2 監査イベントの統合

IBM DB2 DSM により、分析のために DB2 監査ログを IBM Security QRadar と統合できます。

db2audit コマンドは、拡張子が「.del」の一連のコンマ区切りテキスト・ファイルを作成します。監査が構成され、有効になっている場合、これらのファイルは QRadar の監査データの有効範囲を定義します。db2audit コマンドで作成されるコンマ区切りファイルとして、以下のものがあります。

- audit.del
- checking.del
- context.del
- execute.del
- objmaint.del
- secmaint.del
- sysadmin.del
- validate.del

IBM DB2 DSM を QRadar と統合するには、以下を実行する必要があります。

1. db2audit コマンドを使用して IBM DB2 がセキュリティー・イベントを記録するようにします。詳しくは、「*IBM DB2* のベンダー資料」を参照してください。

2. IBM DB2 のバージョンに応じて、インスタンスに格納された、イベントの DB2 監査データをログ・ファイルに抽出します。

   DB2 v9.5 以降を使用している場合は、『監査データの抽出: DB2 v9.5 以降』を参照してください。または

   DB2 v8.x から v9.4 を使用している場合は、 490 ページの『監査データの抽出 : DB2 v8.x から v9.4』を参照してください。
3. ログ・ファイル・プロトコル・ソースを使用して出力インスタンス・ログ・ファイルをプルし、スケジュールに基づいてその情報を QRadar に送信します。次に、QRadar はこのファイルをインポートして、処理します。 484 ページの『IBM DB2 用のログ・ソースの作成』を参照してください。

注: IBM DB2 DSM は、IBM z/OS メインフレーム・オペレーティング・システムをサポートしません。

監査データの抽出: DB2 v9.5 以降

IBM DB2 v9.5 以降を使用している場合は、監査データを抽出できます。

手順

1. SYSADMIN 特権を使用して DB2 アカウントにログインします。
2. 以下のように、データベース・インスタンスの監査レコードを監査ログに移動します。

   ```
   db2audit flush
   ```

   例えば、flush コマンドの応答の出力は、以下のようになります。

   ```
   AUD00001 操作が成功しました。(Operation succeeded.)
   ```
3. 以下のように、アクティブ・インスタンスをアーカイブし、後から抽出するために新しい場所に移動します。

   ```
   db2audit archive
   ```

   例えば、archive コマンドの応答の出力は、以下のようになります。

   ```
   ノード AUD がアーカイブされました、または一時ログ・ファイル・メッセージ
   (Node AUD Archived or Interim Log File Message)
   ---- --- ----------------------------
   - 0 AUD00001 dbsaudit.instance.log.0.20091217125028 AUD00001 操作が成功しました。
   (Operation succeeded.)
   ```

   注: DB2 v9.5 以降では、archive コマンドによって prune コマンドが置き換えられています。

   archive コマンドはアクティブ監査ログを新しい場所に移動します。結果として、すべての非アクティブ・レコードがログから除去されます。抽出を実行する前に archive コマンドが完了している必要があります。
4. 以下のように、アーカイブされた監査ログからデータを抽出し、そのデータを .del ファイルに書き込みます。

   ```
   db2audit extract delasc from files db2audit.instance.log.0.200912171528
   ```

例えば、archive コマンドの応答の出力は、以下のようになります。

```
AUD00001 操作が成功しました。(Operation succeeded.)
```

注: ASCII ファイルのデフォルトのテキスト区切り文字として二重引用符 (") が使用されます。区切り文字を変更しないでください。

5. IBM Security QRadar がファイルをプルできるストレージ・ロケーションに .del ファイルを移動します。コンマ区切りファイル (.del) の移動は、QRadar でのファイル・プル間隔に同期させる必要があります。

これで、DB2 ログ・ファイルを受信するように QRadar を構成する準備ができました。 484 ページの『IBM DB2 用のログ・ソースの作成』を参照してください。

監査データの抽出: DB2 v8.x から v9.4

IBM DB2 v8.x から v9.4 を使用している場合は、監査データを抽出できます。

手順

1. SYSADMIN 特権を使用して DB2 アカウントにログインします。
2. 以下の start コマンドを入力してデータベース・インスタンスを監査します。

```
db2audit start
```

例えば、start コマンドの応答の出力は、以下のようになります。

```
AUD00001 操作が成功しました。(Operation succeeded.)
```

3. 以下のように、インスタンスの監査レコードを監査ログに移動します。

```
db2audit flush
```

例えば、flush コマンドの応答の出力は、以下のようになります。

```
AUD00001 操作が成功しました。(Operation succeeded.)
```

4. 以下のように、アーカイブされた監査ログからデータを抽出し、そのデータを .del ファイルに書き込みます。

```
db2audit extract delasc
```

例えば、archive コマンドの応答の出力は、以下のようになります。

```
AUD00001 操作が成功しました。(Operation succeeded.)
```

注: ASCII ファイルのデフォルトのテキスト区切り文字として二重引用符 (") が使用されます。区切り文字を変更しないでください。

5. 以下のように、非アクティブなレコードを削除します。

```
db2audit prune all
```

6. IBM Security QRadar がファイルをプルできるストレージ・ロケーションに .del ファイルを移動します。コンマ区切りファイル (.del) の移動は、QRadar でのファイル・プル間隔に同期させる必要があります。

これで、DB2 ログ・ファイルを受信するためのログ・ソースを QRadar で作成する準備ができました。

IBM DB2 用のログ・ソースの作成

ログ・ファイル・プロトコル・ソースにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

このタスクについて

IBM DB2 DSM は、ログ・ファイル・プロトコル・ソースを使用して、ログ・ファイルの一括ロードをサポートします。ログ・ファイル・プロトコルを使用するように IBM DB2 を構成する際には、IBM DB2 システムで構成されているホスト名または IP アドレスが、ログ・ファイル・プロトコル構成の「リモート・ホスト」パラメーターに構成されているものと同じになっているようにしてください。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「IBM DB2」を選択します。
8. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
9. 以下の値を構成します。

表 192. IBM DB2 ログ・ファイル・プロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。 QRadar がログ・ファイルを固有のイベント・ソースに識別できるようになるので、IP アドレスまたはホスト名の使用が推奨されます。 例えば、ネットワークに複数のデバイス (例えば、複数の z/OS イメージ)、またはすべてのイベント・ログが入っているファイル・リポジトリーが含まれている場合、IBM DB2 ログ・ソースのイベントを一意に識別する、イメージまたは場所の名前、IP アドレス、またはホスト名を指定します。このアドレス指定により、ユーザーが識別可能なネットワークのイメージ・レベルまたは場所のレベルで、イベントを識別できるようになります。

表 *192. IBM DB2* ログ・ファイル・プロトコル・パラメーター *(*続き*)*

パラメーター	説明
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 このオプションには、以下のポートがあります。 • **FTP** - TCP ポート 21 • **SFTP** - TCP ポート 22 • **SCP** - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。
SSH 鍵ファイル	「サービス・タイプ」として「**SCP**」または「**SFTP**」を選択した場合、このパラメーターにより、SSH 秘密鍵ファイルを定義できます。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。このオプションにより、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートできます。

表 192. IBM DB2 ログ・ファイル・プロトコル・パラメーター (続き)

パラメーター	説明
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 **SCP** をサービス・タイプとして構成する場合は、「再帰的 **(Recursive)**」オプションは無視されます。
FTP ファイル・パターン	「サービス・タイプ」として「**SFTP**」または「**FTP**」を選択した場合、このオプションにより、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。例えば、末尾が `.del` のコンマ区切りファイルを収集するには、以下のコードを入力します。 `.*.del` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	ASCII FTP ファイル転送モードを必要とするコンマ区切り、テキスト、または ASCII の各ログ・ソースに対して、リストから「**ASCII**」を選択します。 このオプションは、「サービス・タイプ」として「**FTP**」を選択した場合にのみ表示されます。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。
開始時刻	処理を開始する時刻を入力します。例えば、午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、`00:00` と入力します。 このパラメーターと「繰り返し **(Recurrence)**」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、`2H` と入力します。デフォルトは 1H です。

表 *192. IBM DB2* ログ・ファイル・プロトコル・パラメーター *(*続き*)*

パラメーター	説明
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「なし」を選択します。 プロセッサーにより、イベント・ファイル・アーカイブを解凍し、内容をイベント用に処理できます。ファイルは、QRadar にダウンロードされた後にのみ処理されます。QRadar は、`zip`、`gzip`、`tar`、または `tar+gzip` の各アーカイブ・フォーマットのファイルを処理できます。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって既に処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが以前に処理されているかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。以前に処理されていないすべてのファイルがダウンロードされます。 このオプションは、「**FTP**」および「**SFTP**」のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスはクリアしたままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これにより、ファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに複数の処理を適用します。ファイルの各行が、単一イベントです。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

関連概念:

22 ページの『ログ・ファイル・プロトコルの構成オプション』
リモート・ホストからイベントを受信するには、ログ・ファイル・プロトコルを使用するようにログ・ソースを構成します。

IBM DataPower

IBM Security QRadar DSM は、IBM DataPower® システムからイベント・ログを収集します。

IBM DataPower は、以前は IBM WebSphere® DataPower と呼ばれていました。

以下の表は、IBM DataPower DSM の仕様を示しています。

表 *193. IBM DataPower DSM* の仕様

仕様	値
製造元	IBM
DSM 名	DataPower
RPM ファイル名	DSM-IBMDataPower-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	FirmwareV6 および V7
プロトコル	Syslog
QRadar で記録されるイベント・タイプ	すべてのイベント
QRadar UI でのログ・ソース・タイプ	IBM DataPower
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
詳細情報	IBM Web ページ (http://www.ibm.com/)

IBM DataPower から QRadar にイベントを送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの IBM DataPower DSM をダウンロードして QRadar コンソール にインストールしてください。
2. IBM DataPower のインスタンスごとに、QRadar と通信するよう IBM DataPower システムを構成します。
3. QRadar が IBM DataPower を自動的に検出しない場合は、QRadar コンソール上の IBM DataPower のインスタンスごとにログ・ソースを作成します。以下の IBM DataPower 固有の値を使用します。

パラメーター	値
ログ・ソース・タイプ	IBM DataPower
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインスト

ールしなければならないことがあります。

『QRadar との通信のための IBM DataPower の構成』
IBM DataPower イベントを収集するには、イベントを IBM Security QRadar に送信するようにサード・パーティー・システムを構成します。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信のための IBM DataPower の構成

IBM DataPower イベントを収集するには、イベントを IBM Security QRadar に送信するようにサード・パーティー・システムを構成します。

始める前に

DataPower ロギング資料を確認して、ご使用のデプロイメントに適したロギング構成変更を判断してください。IBM Knowledge Center (http://www-01.ibm.com/support/knowledgecenter/SS9H2Y_7.0.0/com.ibm.dp.xi.doc/logtarget_logs.html?lang=en) を参照してください。

手順

1. IBM DataPower システムにログインします。
2. 左側のナビゲーション・メニューにある検索ボックスに、`Log Target` と入力します。
3. 一致する結果を選択します。
4. 「追加」をクリックします。
5. 「メイン」タブで、ログ・ターゲットの名前を入力します。
6. 「ターゲット・タイプ」リストから、「**syslog**」を選択します。
7. 「ローカル **ID**」フィールドに、QRadar ユーザー・インターフェースの「**Syslog** イベント・ペイロード **(Syslog event payloads)**」パラメーターに表示する ID を入力します。
8. 「リモート・ホスト」フィールドに、QRadar コンソールまたはイベント・コレクターの IP アドレスまたはホスト名を入力します。
9. 「リモート・ポート」フィールドに `514` を入力します。
10. 「イベント・サブスクリプション」の下に、以下のパラメーターとともに基本ロギング構成を追加します。

パラメーター	値
イベント・カテゴリー	`all`
最小イベント優先順位	`warning` **重要:** システム・パフォーマンスの低下を防ぐため、「最小イベント優先順位」パラメーターに 2 語以上使用しないでください。

11. ログ・ターゲットに変更を適用します。
12. 構成の変更を確認して保存します。

IBM Federated Directory Server

IBM Security QRadar DSM は、IBM Federated Directory Server システムからイベントを収集します。

以下の表は、IBM Federated Directory Server DSM の仕様を示しています。

表 194. *IBM Federated Directory Server DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM Federated Directory Server
RPM ファイル名	DSM-IBMFederated DirectoryServer-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	V7.2.0.2 以降
イベント・フォーマット	LEEF
記録されるイベント・タイプ	FDS 監査
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	IBM Knowledge Center の Security Directory Server 情報 (http://www-01.ibm.com/support/knowledgecenter/SSVJJU/welcome)

IBM Federated Directory Server から QRadar にイベントを送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンを QRadar コンソール コンソールからダウンロードしてください。
   - DSMCommon RPM
   - IBM Federated Directory Server DSM RPM
2. IBM Federated Directory Server デバイスで QRadar モニターを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで IBM Federated Directory Server ログ・ソースを追加してください。以下の表は、IBM Federated Directory Server イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 195. *IBM Federated Directory Serve* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	IBM Federated Directory Server
プロトコル構成	Syslog
ログ・ソース ID	IBM Federated Directory Server の送信元 IP またはホスト名。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインスト

ールしなければならないことがあります。

『セキュリティー・イベントをモニターするように IBM Federated Directory Server を構成』
セキュリティー・イベントをモニターするように IBM Federated Directory Server を構成します。これらのセキュリティー・イベントは、項目の追加、変更、または削除がターゲットで行われたときに生成されます。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

セキュリティー・イベントをモニターするように IBM Federated Directory Server を構成

セキュリティー・イベントをモニターするように IBM Federated Directory Server を構成します。これらのセキュリティー・イベントは、項目の追加、変更、または削除がターゲットで行われたときに生成されます。

手順

1. IBM Federated Directory Server にログインします。
2. ナビゲーション・ペインの「共通設定 **(Common Settings)**」で、「モニター **(Monitoring)**」をクリックします。
3. 「モニター (Monitoring)」ページで QRadar タブをクリックします。
4. セキュリティー・イベントをモニターすることを示すために、QRadar ページで「有効」を選択します。
5. パラメーターを構成します。
6. 「マップ・ファイル」フィールドに、イベントの各種 QRadar LEEF 属性を構成するマップ・ファイルのパスとファイル名を指定します。
7. 「選択」をクリックして、マップ・ファイルを参照します。デフォルト値では、`LDAPSync/QRadar.map` ファイルが指定されています。
8. 「日付形式マスク」フィールドで、マップ対象の LEEF 属性に書き込まれる日付値に使用する標準の Java `SimpleDateFormat` マスクを指定します。

   この値により、**devTimeFormat** 属性の値と、イベントの日付値のフォーマットの両方が制御されます。デフォルト値は ISO 8601 規格のマスク `MMM dd yy HH:mm:ss` であり、`Oct 16 12 15:15:57` などのストリングが作成されます。

IBM Fiberlink MaaS360

IBM Security QRadar 用の IBM Fiberlink® MaaS360® DSM は、Fiberlink MaaS360 コンソールからイベント・ログを収集することができます。

以下の表は、IBM Fiberlink MaaS360 DSM の仕様を示しています。

表 *196. IBM Fiberlink MaaS360 DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM Fiberlink MaaS360

表 196. IBM Fiberlink MaaS360 DSM の仕様 (続き)

仕様	値
RPM ファイル名	DSM-IBMFiberlinkMaaS360
サポートされるバージョン	N/A
イベント・フォーマット	LEEF
QRadar で記録されるイベント・タイプ	コンプライアンス・ルール・イベント デバイス登録イベント アクション履歴イベント
自動的に検出?	いいえ
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Fiberlink MaaS360 Web サイト (http://www.maas360.com/)

IBM Fiberlink MaaS360 を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードしてください。
   - DSMCommon RPM
   - IBM Fiberlink REST API プロトコル RPM
   - IBM Fiberlink MaaS360 RPM
2. QRadar と通信できるように Fiberlink MaaS360 インスタンスを構成します。
3. QRadar コンソール上で IBM Fiberlink MaaS360 のログ・ソースを作成します。

RPM の手動インストール

QRadar コンソールで自動更新が有効になっていない場合や、QRadar コンソールがインターネットに接続できない場合は、IBM サポート Web サイトから DSM、プロトコル、スキャナーの RPM をダウンロードしてください。その後、コマンド・ライン・インターフェースを使用してこれらの RPM をインストールすることができます。RPM をアンインストールする場合は、カスタマー・サポートにお問い合わせください。

始める前に

注: インストールするための `rpm -Uvh <rpm_filename>` コマンド・ラインは、`yum -y install <rpm_filename>` コマンドで置換されました。

手順

1. IBM サポート Web サイト (http://www.ibm.com/support) にアクセスします。
2. QRadar コンソールをホストしているシステムに RPM ファイルをダウンロードします。
3. SSH を使用して、root ユーザーとして QRadar にログインします。

4. ダウンロードしたファイルが格納されているディレクトリーに移動します。
5. 以下のコマンドを入力します。

   ```
   yum -y install <rpm_filename>
   ```
6. QRadar ユーザー・インターフェースにログインします。
7. 「管理」タブで「変更のデプロイ」をクリックします。

   重要: プロトコルの RPM をインストールする場合は、コンソールの出力に記載されているインストール後のステップを実行してください (コンソールの出力からインストールが開始されます)。

QRadar で IBM Fiberlink MaaS360 のログ・ソースを構成する

IBM Fiberlink MaaS360 イベントを収集するには、QRadar でログ・ソースを構成します。

始める前に

IBM Fiberlink MaaS360 が QRadar と通信できるようにするには、REST API を有効にする必要があります。Fiberlink カスタマー・サービスに問い合わせて、ご使用の Fiberlink MaaS360 アカウントに対して REST API を使用可能にします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**IBM Fiberlink MaaS360**」を選択します。
7. 「プロトコル構成」リストで「**IBM Fiberlink REST API**」を選択します。
8. 以下に示す IBM Fiberlink REST API のパラメーターを構成します。

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの固有 ID を入力します。 「ログ・ソース **ID**」には、任意の有効な値を設定でき、特定のサーバーを参照する必要はありません。「ログ・ソース **ID**」は、「ログ・ソース名」と同じ値にすることもできます。複数の IBM Fiberlink MaaS360 ログ・ソースが構成済みの場合は、最初のログ・ソースを *fiberlink1*、2 番目のログ・ソースを *fiberlink2*、3 番目のログ・ソースを *fiberlink3* として識別できます。
ログイン **URL (Login URL)**	Fiberlink MaaS360 REST サーバーの URL。

パラメーター	説明
ユーザー名	MaaS360 API にアクセスするために使用するユーザー名。 次の管理者役割のユーザーが、API にアクセスできます。 • サービス管理者 • 管理者 • 管理者 - レベル 2
パスワード	MaaS360 API にアクセスするために使用するパスワード。
秘密鍵 **(Secret Key)**	REST API を使用可能にしたときに Fiberlink カスタマー・サービスから受け取った秘密鍵。
アプリケーション **ID (App ID)**	REST API を使用可能にしたときに Fiberlink カスタマー・サービスから受け取ったアプリケーション ID。
請求 **ID (Billing ID)**	Fiberlink MaaS360 アカウントの請求 ID。
プラットフォーム **(Platform)**	Fiberlink MaaS360 コンソールのプラットフォーム・バージョン。
アプリケーションのバージョン **(App Version)**	REST API アカウントに対応するアプリケーションのバージョン。
プロキシーの使用 **(Use Proxy)**	QRadar がプロキシーを使用して Fiberlink MaaS360 API にアクセスする場合、「プロキシーの使用 **(Use Proxy)**」チェック・ボックスを選択します。 プロキシーが認証を必要とする場合、「プロキシー・サーバー」、「プロキシー・ポート」、「プロキシー・ユーザー名」、「プロキシー・パスワード」の各フィールドを構成します。 プロキシーが認証を必要としない場合、「プロキシー・サーバー」フィールドおよび「プロキシー・ポート」フィールドを構成します。
サーバー証明書を自動的に獲得 **(Automatically Acquire Server Certificate(s))**	「はい」オプションを選択すると、QRadar は、自動的にサーバー証明書をダウンロードし、ターゲット・サーバーを信頼し始めます。

9. 残りのパラメーターを構成します。
10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Guardium

IBM Guardium® は、システム管理者が複数のデータベース・プラットフォームにわたる詳細監査イベントを取得するためのデータベース・アクティビティーおよびデータベース監査のトラッキング・ツールです。

以下の手順では、InfoSphere® Guardium の 8.2p45 フィックスをインストールする必要があります。このフィックスについて詳しくは、Fix Central Web サイト (http://www.ibm.com/support/fixcentral/) を参照してください。

IBM Security QRadar は、syslog を使用して、IBM Guardium から通知、エラー、アラート、および警告を収集します。IBM Security QRadar は、IBM Guardium Policy Builder イベントをログ・イベント拡張フォーマット (LEEF) で受信します。

QRadar は、IBM Guardium の出荷時のデフォルト・ポリシーのイベントのみを自動的に検出してマップできます。ユーザーが構成した必要なイベントはすべて、不明であると QRadar に表示され、これらの不明イベントを手動でマップする必要があります。

構成の概要

IBM Guardium を QRadar と統合するために必要なプロセスの概要を以下にリストします。

1. ポリシー違反イベントの syslog 宛先を作成します。詳しくは、『イベント用の syslog 宛先の作成』を参照してください。
2. syslog イベントを生成するように既存のポリシーを構成します。詳しくは、504 ページの『syslog イベントを生成するためのポリシーの構成』を参照してください。
3. IBM Guardium にポリシーをインストールします。詳しくは、 504 ページの『IBM Guardium ポリシーのインストール』を参照してください。
4. QRadar でログ・ソースを構成します。詳しくは、 505 ページの『ログ・ソースの構成』を参照してください。
5. QRadar で不明ポリシー・イベントを特定し、マップします。詳しくは、 506 ページの『IBM Guardium イベント用のイベント・マップの作成』を参照してください。

イベント用の syslog 宛先の作成

IBM Guardium で該当するイベントの syslog 宛先を作成するには、コマンド・ライン・インターフェース (CLI) にログインし、IBM Security QRadar の IP アドレスを定義する必要があります。

手順

1. SSH を使用して、IBM Guardium に root ユーザーとしてログインします。

   ユーザー名: *<username>*

   パスワード: *<password>*
2. 以下のコマンドを入力して、情報イベントの syslog 宛先を構成します。

```
store remote add daemon.info <IP address>:<port> <tcp|udp>
```

例:

```
store remote add daemon.info 10.10.1.1:514 tcp
```

各部分について以下で説明します。

- *<IP address>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
- *<port>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)との通信に使用する syslog ポート番号です。
- <tcp|udp> は、QRadar コンソールまたはイベント・コレクター (Event Collector)との通信に使用するプロトコルです。

3. 以下のコマンドを入力して、警告イベントの syslog 宛先を構成します。

```
store remote add daemon.warning <IP address>:<port> <tcp|udp>
```

各部分について以下で説明します。

- *<IP address>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
- *<port>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)との通信に使用する syslog ポート番号です。
- <tcp|udp> は、QRadar コンソールまたはイベント・コレクター (Event Collector)との通信に使用するプロトコルです。

4. 以下のコマンドを入力して、エラー・イベントの syslog 宛先を構成します。

```
store remote add daemon.err <IP address>:<port> <tcp|udp>
```

各部分について以下で説明します。

- *<IP address>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
- *<port>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)との通信に使用する syslog ポート番号です。
- <tcp|udp> は、QRadar コンソールまたはイベント・コレクター (Event Collector)との通信に使用するプロトコルです。

5. 以下のコマンドを入力して、アラート・イベントの syslog 宛先を構成します。

```
store remote add daemon.alert <IP address>:<port> <tcp|udp>
```

各部分について以下で説明します。

- *<IP address>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
- *<port>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)との通信に使用する syslog ポート番号です。
- <tcp|udp> は、QRadar コンソールまたはイベント・コレクター (Event Collector)との通信に使用するプロトコルです。

これで、IBM InfoSphere Guardium 用にポリシーを構成する準備ができました。

syslog イベントを生成するためのポリシーの構成

IBM Guardium のポリシーは、イベントへの対応とイベント情報の IBM Security QRadar への転送を担います。

手順

1. 「ツール」タブをクリックします。
2. 左側のナビゲーションで「ポリシー・ビルダー」を選択します。
3. 「ポリシー・ファインダー」ペインで既存のポリシーを選択し、「ルールの編集」をクリックします。
4. 「このルールの個別編集」をクリックします。

   「アクセス・ルール定義」が表示されます。
5. 「アクションの追加」をクリックします。
6. 「アクション」リストから以下のいずれかのアラート・タイプを選択します。
   - 一致ごとにアラート - ポリシー違反ごとに通知が提供されます。
   - 毎日アラート - 当該日に初めてポリシー違反が発生したときに通知が提供されます。
   - セッションごとに **1** 回アラート - ユニーク・セッションのポリシー違反ごとに通知が提供されます。
   - 時間間隔ごとにアラート - 選択した時間フレームごとに通知が提供されます。
7. 「メッセージ・テンプレート」リストで QRadar を選択します。
8. 「通知タイプ」リストから「**SYSLOG**」を選択します。
9. 「追加」をクリックし、「適用」をクリックします。
10. 「保存」をクリックします。
11. QRadar に転送するポリシー内のすべてのルールについて、『syslog イベントを生成するためのポリシーの構成』を繰り返します。

    ポリシーの構成について詳しくは、*IBM InfoSphere Guardium* のベンダー資料を参照してください。すべてのポリシーの構成が終わったら、IBM Guardium システムでポリシーをインストール準備ができています。

    注**:** ポリシーが構成可能であるため、QRadar が自動的に検出するのは、デフォルト・ポリシー・イベントのみです。イベントを QRadar に転送するポリシーをカスタマイズした場合は、該当するイベントをキャプチャーするためのログ・ソースを手動で作成する必要があります。

IBM Guardium ポリシーのインストール

更新したアラート・アクションまたはルールの変更を行うには、その前に、IBM Guardium の新規ポリシーまたは編集したポリシーをインストールする必要があります。

手順

1. 「管理コンソール」タブをクリックします。
2. 左側のナビゲーションで、「構成」 > 「ポリシー・インストール」を選択します。
3. 「ポリシー・インストーラー」ペインで、 504 ページの『syslog イベントを生成するためのポリシーの構成』で変更したポリシーを選択します。
4. ドロップダウン・リストから「インストールおよびオーバーライド」を選択します。

   すべての検査エンジンにポリシーをインストールするかに関する確認が表示されます。
5. 「**OK**」をクリックします。

   ポリシーのインストールについて詳しくは、*IBM InfoSphere Guardium* のベンダー資料を参照してください。すべてのポリシーをインストールしたら、IBM Security QRadar でログ・ソースを構成する準備ができています。

ログ・ソースの構成

IBM Security QRadar は、IBM Guardium からのデフォルト・ポリシー・イベントのみを自動的に検出します。

このタスクについて

ポリシーは構成可能であるため、IBM Guardium 用にログ・ソースを手動で構成することをお勧めします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「**IBM Guardium**」を選択します。
8. 「プロトコル構成」リストで「**Syslog**」を選択します。
9. 以下の値を構成します。

表 197. IBM Guardium の syslog 構成

パラメーター	説明
ログ・ソース **ID**	IBM InfoSphere Guardium アプライアンスの IP アドレスまたはホスト名を入力します。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Guardium イベント用のイベント・マップの作成

多数の IBM Guardium イベントで、イベント・マッピングが必要です。ポリシー・ルールはカスタマイズ可能であるため、デフォルト・ポリシー・イベントを除くほとんどのイベントには、セキュリティー・イベントをカテゴリー化するための事前定義の IBM Security QRadar ID (QID) マップが含まれていません。

このタスクについて

デバイスの各イベントは、個別に QRadar のイベント・カテゴリーにマップすることができます。イベントをマップすることで、QRadar は、ネットワーク・デバイスからの繰り返しイベントを識別、統合、および追跡できます。イベントをマップしない限り、IBM Guardium の「ログ・アクティビティー」タブで表示されるイベントはすべて「不明」に分類されます。不明なイベントは「イベント名」列に示され、「下位カテゴリー」列に「不明」と表示されるため、簡単に分かります。

デバイスから QRadar にイベントを転送すると、イベント・ソース・アプライアンスまたはソフトウェアが一部のイベントを即時に生成しないことがあるため、デバイスのすべてのイベントの分類に時間がかかる場合があります。不明イベントを迅速に検索する方法を把握しておくと有益です。不明イベントの検索方法が分かっている場合は、ほとんどのイベントが識別されて満足できる状態になるまで、この検索を繰り返すことをお勧めします。

手順

1. QRadar にログインします。
2. 「ログ・アクティビティー」タブをクリックします。
3. 「フィルターの追加」をクリックします。
4. 最初のリストから「ログ・ソース」を選択します。
5. 「ログ・ソース・グループ」リストから、ログ・ソース・グループまたは「その他」を選択します。

   グループに割り当てられていないログ・ソースは「その他」に分類されます。
6. 「ログ・ソース」リストで IBM Guardium ログ・ソースを選択します。
7. 「フィルターの追加」をクリックします。

   「ログ・アクティビティー」タブに、ログ・ソース用のフィルターが表示されます。
8. 「表示」リストから「過去 **1** 時間」を選択します。

   IBM Guardium DSM によって過去 1 時間に生成されたイベントがすべて表示されます。「イベント名」列、または「下位カテゴリー」列に「不明」として表示されているイベントについては、QRadar でのイベント・マッピングが必要です。

   注**:** 「条件の保存」をクリックすると、既存の検索フィルターを保存することができます。

   これで、イベント・マップを変更する準備ができました。

イベント・マップの変更

イベント・マップを変更する際に、イベントを IBM Security QRadar ID (QID) マップに手動で分類できます。ログ・ソースに分類された任意のイベントを、新しい QRadar ID (QID) に再マップできます。

このタスクについて

ログ・ソースが定義されていない IBM Guardium イベント・マップのイベントは、イベントにマップできません。ログ・ソースのないイベントの場合、「ログ・ソース」列に「**SIM 汎用ログ (SIM Generic Log)**」と表示されます。

手順

1. 「イベント名」列で、IBM Guardium の不明イベントをダブルクリックします。

   詳細なイベント情報が表示されます。
2. 「イベントのマップ」をクリックします。
3. 「QID の参照 (Browse for QID)」ペインから、以下のいずれかの検索オプションを選択して、QRadar ID (QID) のイベント・カテゴリーを絞り込みます。
   - 「上位カテゴリー」リストから、上位イベント・カテゴリーを選択します。
   - 上位イベント・カテゴリーと下位イベント・カテゴリーの全リストおよびカテゴリーの定義については、「*IBM Security QRadar* 管理ガイド」の『イベント・カテゴリー』セクションを参照してください。
   - 「下位カテゴリー」リストから、下位イベント・カテゴリーを選択します。
   - 「ログ・ソース・タイプ」リストから、ログ・ソース・タイプを選択します。

   「ログ・ソース・タイプ」リストでは、他のログ・ソースからの QID を検索できます。イベントが既存の別のネットワーク・デバイスからのイベントに類似している場合、ログ・ソースで QID を検索すると便利です。例えば、IBM Guardium がポリシー・イベントを提供する場合、類似するイベントをキャプチャーする可能性のある別の製品を選択できます。
4. 名前で QID を検索するには、「**QID/**名前」フィールドに名前を入力します。

   「**QID/**名前」フィールドでは、特定の単語 (例: policy) で QID の完全なリストをフィルタリングできます。
5. 「検索」をクリックします。

   QID のリストが表示されます。
6. 不明イベントに関連付ける QID を選択します。
7. 「**OK**」をクリックします。

   QRadar は、イベント・ペイロードに一致する 同じ QID を持つデバイスから転送されるすべての追加イベントをマップします。QRadar によってイベントが識別されるたびに、イベントの数が増加します。

新しい QRadar ID (QID) マップでイベントを更新する場合、QRadar に保管されている過去のイベントは更新されません。新しいイベントだけが新しい QID によって分類されます。

IBM IMS

IBM Security QRadar 用の IBM Information Management System (IMS™) DSM により、IBM メインフレームを使用して、イベントの収集および IMS データベース・トランザクションの監査を行うことができます。

IBM IMS イベントを QRadar と統合するには、IBM IMS イベントをログ・ファイルに書き込むことができるようにするスクリプトをダウンロードする必要があります。

イベント収集プロセスの概要

1. IBM メインフレームが、すべてのセキュリティー・イベントをサービス・マネジメント・フレームワーク (SMF) レコードとしてライブ・リポジトリーに記録します。
2. IBM IMS データが、SMF ダンプ・ユーティリティーを使用してライブ・リポジトリーから抽出されます。SMF ファイルには、前日のすべてのイベントおよびフィールドが未加工の SMF 形式で格納されています。
3. `qeximsloadlib.trs` プログラムが、SMF 形式ファイルからデータをプルします。`qeximsloadlib.trs` プログラムは QRadar の関連イベントおよび関連フィールドのみをプルし、互換性を考慮して、その情報を圧縮形式で書き込みます。この情報は、QRadar がアクセスできる場所に保存されます。
4. QRadar は、ログ・ファイル・プロトコル・ソースを使用して、スケジュールに基づいて QRadar 用の出力ファイル情報を取得します。次に、QRadar はこのファイルをインポートして、処理します。

IBM IMS の構成

IBM IMS を QRadar と統合できます。

手順

1. IBM サポート Web サイト (http://www.ibm.com/support) から、以下の圧縮ファイルをダウンロードします。

   `QexIMS_bundled.tar.gz`

2. Linux ベースのオペレーティング・システム上で、以下のファイルを解凍します。

   ```
   tar -zxvf qexims_bundled.tar.gz
   ```

   アーカイブには、以下のファイルが含まれています。

   - `qexims_jcl.txt` - ジョブ制御言語ファイル
   - `qeximsloadlib.trs` - 圧縮プログラム・ライブラリー (IBM TRSMAIN が必要)
   - `qexims_trsmain_JCL.txt` - TRSMAIN が `.trs` ファイルを圧縮解除するためのジョブ制御言語

3. 以下の方法を使用して、各ファイルを IBM メインフレームにロードします。

   TEXT プロトコルを使用して、サンプルの qexims_trsmain_JCL.txt ファイルと qexims_jcl.txt ファイルをアップロードします。

4. BINARY モード転送を使用して qeximsloadlib.trs ファイルをアップロードし、事前割り振りデータ・セットに追加します。qeximsloadlib.trs ファイルは、実行可能ファイル (メインフレーム・プログラム QexIMS) が含まれている簡潔なファイルです。.trs ファイルをワークステーションからアップロードするときに、DCB 属性
   DSORG=PS、RECFM=FB、LRECL=1024、BLKSIZE=6144 を使用して、メインフレーム上でファイルを事前割り振りします。ファイル転送タイプは、テキストではなくバイナリー・モードでなければなりません。

   注: QexIMS は、IMS ログ・ファイルの出力 (EARLOUT データ) を 1 行ずつ読み取る小さな C メインフレーム・プログラムです。QexIMS は、イベント情報 (例えば、レコード記述子、日付、時刻) が含まれているヘッダーを各レコードに追加します。このプログラムは各フィールドを出力レコードに書き込み、末尾ブランク文字を抑止し、各フィールドをパイプ文字で区切ります。この出力ファイルは QRadar 用にフォーマット設定されており、ブランクの抑止により、QRadar へのネットワーク・トラフィックが削減されます。このプログラムは、CPU や I/O ディスクのリソースをあまり多く必要としません。

5. パラメーターのインストール済み環境固有の情報に応じて、qexims_trsmain_JCL.txt ファイルをカスタマイズします。

   例えば、ジョブ・カード、データ・セット命名規則、出力宛先、保存期間、スペース所要量です。

   qexims_trsmain_JCL.txt ファイルは IBM ユーティリティー TRSMAIN を使用して、qeximsloadlib.trs ファイルに保管されているプログラムを抽出します。

   qexims_trsmain_JCL.txt ファイルの例を以下に示します。

```
//TRSMAIN JOB (yourvalidjobcard),Q1labs,
// MSGCLASS=V
//DEL EXEC PGM=IEFBR14 //D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXIMS.TRS
// UNIT=SYSDA, // SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE DD DISP=SHR,DSN=<yourhlq>.QEXIMS.TRS
//OUTFILE DD DISP=(NEW,CATLG,DELETE),
// DSN=<yourhlq>.LOAD, // SPACE=(CYL,(1,1,5),RLSE),UNIT=SYSDA
//
```

   .trs 入力ファイルは、IBM TERSE フォーマットのライブラリーであり、TRSMAIN を呼び出す JCL の実行によって取り出されます。この簡潔なファイルは抽出時に、qexims プログラムをメンバーとして持つ PDS LINKLIB を作成します。

6. STEPLIB をこのライブラリーに対して実行するか、または LINKLST 内にある LINKLIB の 1 つにこのプログラムを移動することを選択できます。このプログラムには許可は必要ありません。

7. qexims_jcl.txt ファイルは、サンプル JCL が含まれているテキスト・ファイルです。構成を満たすようにジョブ・カードを構成する必要があります。

   qexims_jcl.txt サンプル・ファイルには、以下が含まれています。

```
//QEXIMS JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M //* //*QEXIMS JCL VERSION 1.0 FEBRUARY 2011
//*
//*************************************************************
//* Change dataset names to site specific dataset names *

//*************************************************************
//SET1 SET IMSOUT='Q1JACK.QEXIMS.OUTPUT',
// IMSIN='Q1JACK.QEXIMS.INPUT.DATA'
//*************************************************************
//* Delete old datasets *
//*************************************************************
//DEL EXEC PGM=IEFBR14 //DD1 DD DISP=(MOD,DELETE),DSN=&IMSOUT,
// UNIT=SYSDA, // SPACE=(CYL,(10,10)), // DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//* Allocate new dataset
//*************************************************************
//ALLOC EXEC PGM=IEFBR14 //DD1 DD DISP=(NEW,CATLG),DSN=&IMSOUT,
// SPACE=(CYL,(21,2)),
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//EXTRACT EXEC PGM=QEXIMS,DYNAMNBR=10,
// TIME=1440 //STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN DD DUMMY
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=* //IMSIN DD DISP=SHR,DSN=&IMSIN
//IMSOUT DD DISP=SHR,DSN=&IMSOUT
//*FTP EXEC PGM=FTP,REGION=3800K //*INPUT DD *
//*<target server>
//*<USER>
//*<PASSWORD>
//*ASCII //*PUT '<IMSOUT>' /TARGET DIRECTORY>/<IMSOUT>
//*QUIT
//*OUTPUT DD SYSOUT=* //*SYSPRINT DD SYSOUT=*
//*
```

8. 出力ファイルの作成後に、以下のいずれかを選択する必要があります。
   - 出力ファイルを一時 FTP サーバーに転送するジョブをスケジュールします。
   - ジョブが完了するたびに、出力ファイルが一時 FTP サーバーに転送されます。出力を一時 FTP サーバーに正常に転送するために、サンプル JCL で以下のパラメーターを構成する必要があります。

   例:

```
//*FTP EXEC PGM=FTP,REGION=3800K
//*INPUT DD *
//*<target server>
//*<USER>
//*<PASSWORD> //*ASCII //*PUT '<IMSOUT>'
/TARGET DIRECTORY>/<IMSOUT>
//*QUIT //*OUTPUT DD SYSOUT=*
//*SYSPRINT DD SYSOUT=*
```

   各部分について以下で説明します。

   - <*target server*> は、出力ファイルを受信するための一時 FTP サーバーの IP アドレスまたはホスト名です。
   - <*USER*> は、一時 FTP サーバーへのアクセスに必要なユーザー名です。

- <*PASSWORD*> は、一時 FTP サーバーへのアクセスに必要なパスワードです。
- <*IMSOUT*> は、一時 FTP サーバーに保存される出力ファイルの名前です。

例:

```
PUT 'Q1JACK.QEXIMS.OUTPUT.C320' /192.168.1.101/IMS/QEXIMS.OUTPUT.C320
```

注**:** スクリプトが出力ファイルを一時 FTP サーバーに正しく転送できるようにするために、//* で始まるコメント行を削除する必要があります。

これで、ログ・ファイル・プロトコルを構成する準備ができました。

9. IBM IMS から出力ファイルを取得するように QRadar をスケジュールします。

メインフレームが FTP または SFTP 経由でファイルを提供するように構成されているか、または SCP を許可するように構成されている場合、一時 FTP サーバーは不要であり、QRadar は出力ファイルをメインフレームから直接プルすることができます。qexims_jcl.txt ファイルで、以下のテキストは、//* を使用してコメント化するか削除する必要があります。

```
//*FTP EXEC PGM=FTP,REGION=3800K //*INPUT DD *
//*<target server>
//*<USER> //*<PASSWORD> //*ASCII
//*PUT '<IMSOUT>'
/<TARGET DIRECTORY>/<IMSOUT>
//*QUIT //*OUTPUT DD SYSOUT=*
//*SYSPRINT DD SYSOUT=*
```

これで、ログ・ファイル・プロトコルを構成する準備ができました。

ログ・ソースの構成

ログ・ファイル・プロトコルのソースにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取得することができます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「ログ・ソース・タイプ」リストで「IBM IMS」を選択します。
5. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
6. 以下のパラメーターを構成します。

表 *198.* ログ・ファイル・プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。

表 198. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
サービス・タイプ	リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを、リストから選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	IBM IMS システムの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。サービス・タイプを **FTP** として構成する場合、デフォルトは 21 です。「サービス・タイプ」を「**SFTP**」または「**SCP**」として構成する場合、デフォルトは 22 です。 有効な範囲は、1 から 65535 です。
リモート・ユーザー	IBM IMS システムにログインするのに必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	IBM IMS システムにログインするのに必要なパスワードを入力します。
パスワードの確認	IBM IMS システムにログインするためのリモート・パスワードを確認します。
SSH 鍵ファイル	**SCP** または **SFTP** を「サービス・タイプ **(Service Type)**」フィールドから選択する場合、SSH 秘密鍵ファイルへのディレクトリー・パスを定義できます。SSH 秘密鍵ファイルを使用する場合、「リモート・パスワード」フィールドは無視できます。
リモート・ディレクトリー	ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。デフォルトでは、newauditlog.sh スクリプトは、人間が理解できるログ・ファイルを `/var/log/` ディレクトリーに書き込みます。
再帰的 **(Recursive)**	サブフォルダーからもファイル・パターンを検索したい場合は、このチェック・ボックスを選択します。「**SCP**」を「サービス・タイプ」として構成する場合は、「再帰的 **(Recursive)**」パラメーターは使用されません。デフォルトでは、このチェック・ボックスはクリアされています。

表 198. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
FTP ファイル・パターン	「サービス・タイプ」として「**SFTP**」または「**FTP**」を選択した場合、これにより、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするために使用する正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 例えば、*<starttime>.<endtime>.<hostname>*`.log` というフォーマットのファイルをすべて取得する場合、`¥d+¥.¥d+¥.¥w+¥.log` という項目を使用します。 このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として「**FTP**」を選択した場合にのみ表示されます。「**FTP** 転送モード」パラメーターにより、FTP を介してログ・ファイルを取得するときのファイル転送モードを定義できます。 リストから、このログ・ソースに適用する転送モードを選択します。 • バイナリー - バイナリー・データ・ファイル、または圧縮された `.zip`、`.gzip`、`.tar`、`.tar+gzip` のアーカイブ・ファイルを必要とするログ・ソースには、「バイナリー」を選択します。 • **ASCII** - ASCII FTP ファイル転送を必要とするログ・ソースには、「**ASCII**」を選択します。「ASCII」を転送モードとして使用する場合、「プロセッサー」フィールドには「なし」を選択し、「イベント・ジェネレーター **(Event Generator)**」フィールドには「**1** 行ずつ **(LineByLine)**」を選択する必要があります。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。
開始時刻	処理を開始する時刻を入力します。このパラメーターと「繰り返し **(Recurrence)**」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、ディレクトリーを 2 時間おきにスキャンする場合は、`2H` と入力します。デフォルトは 1H です。

表 198. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リモート・ホストにあるファイルが `.zip`、`.gzip`、`.tar`、または `tar+gzip` の各アーカイブ・フォーマットで保管されている場合、アーカイブを解凍して内容を処理することができるプロセッサーを選択します。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	処理済みのファイルを追跡し、ファイルの再度の処理を希望しない場合は、このチェック・ボックスを選択します。これは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar システム上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。このチェック・ボックスはクリアしたままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これにより、ファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。

7. 「保存」をクリックします。

構成は完了です。ログ・ファイル・プロトコルを使用して取得されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

IBM Informix Audit

IBM Informix Audit DSM により、IBM Security QRadar は、分析のために IBM Informix 監査ログを QRadar と統合できます。

QRadar は、ログ・ファイル・プロトコル構成を使用して、リモート・ホストから IBM Informix アーカイブ監査ログ・ファイルを取得します。QRadar は、構成済みのすべての IBM Informix Audit イベントを記録します。

ログ・ファイル・プロトコルを使用するように IBM Informix を構成する場合、IBM Informix に構成されたホスト名または IP アドレスが、ログ・ファイル・プロトコル構成内の **`Remote Host`** パラメーターで構成されたものと同じであることを確認します。

これで、QRadar でログ・ソースとプロトコルを構成する準備ができました。

- IBM Informix デバイスからイベントを受信するように QRadar を構成するには、IBM Informix Audit オプションを「ログ・ソース・タイプ」リストから選択する必要があります。
- ログ・ファイル・プロトコルを構成するには、「プロトコル構成」リストから「ログ・ファイル」オプションを選択する必要があります。

ファイル転送には、セキュア・ファイル転送プロトコル (SFTP) などの安全なプロトコルを使用してください。

関連概念:

22 ページの『ログ・ファイル・プロトコルの構成オプション』
リモート・ホストからイベントを受信するには、ログ・ファイル・プロトコルを使用するようにログ・ソースを構成します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

IBM Lotus Domino

IBM Lotus® Domino® デバイスを IBM Security QRadar と統合できます。IBM Lotus Domino デバイスは、SNMP を使用してイベントを受け入れます。

SNMP サービスのセットアップ

IBM Lotus Domino Server で SNMP サービスをセットアップするには、以下のようにします。

手順

1. Lotus Domino SNMP Agent をサービスとしてインストールします。コマンド・プロンプトで Lotus¥Domino ディレクトリーに移動し、以下のコマンドを入力します。

   ```
   Insnmp -SC
   ```

2. Microsoft SNMP サービスがインストールされていることを確認します。
3. SNMP サービスおよび LNSNMP サービスを開始します。コマンド・プロンプトで以下のコマンドを入力します。
   - `net start snmp`
   - `net start lnsnmp`
4. 「スタート」 > 「プログラム」 > 「管理ツール」 > 「サービス」を選択して、サービス MMC を開きます。
5. 「**SNMP**」サービスをダブルクリックし、「トラップ」タブを選択します。

6. 「コミュニティ名」フィールドに public と入力し、「一覧に追加」をクリックします。
7. 「トラップ送信先」セクションで「追加」をクリックし、IBM Security QRadar の IP アドレスを入力します。「追加」をクリックします。
8. 「**OK**」をクリックします。
9. 両方の SNMP エージェントが、サーバーのブート時に実行されるように「自動」に設定されていることを確認します。

AIX での SNMP のセットアップ

始める前に

TCP/IP および SNMP がサーバー上で適切にインストールおよび構成されていることを確認してください。

root ユーザーとしてログインする必要があります。

手順

1. 以下のコマンドを使用して、LNSNMP サービスを停止します。

   ```
   lnsnmp.sh stop
   ```

2. 以下のコマンドを使用して、SNMP サブシステムを停止します。

   ```
   stopsrc -s snmpd
   ```

3. SNMP が LNSNMP を SMUX ピアとして受け入れるように構成します。/etc/snmpd.peers に以下の行を追加します。

   ```
   "Lotus Notes Agent" 1.3.6.1.4.1.334.72 "NotesPasswd"
   ```

4. SNMP が LNSNMP からの SMUX の関連付けを受け入れるように構成します。/etc/snmpd.conf または /etc/snmpdv3.conf に以下の行を追加します。

   ```
   smux 1.3.6.1.4.1.334.72 NotesPasswd
   ```

5. 以下のコマンドを使用して、SNMP サブシステムを開始します。

   ```
   startsrc -s snmpd
   ```

6. 以下のコマンドを使用して、LNSNMP サービスを開始します。

   ```
   lnsnmp.sh start
   ```

7. LNSNMP スクリプトへのリンクを作成します。

   ```
   ln -f -s /opt/ibm/lotus/notes/latest/ibmpow/lnsnmp.sh /etc/lnsnmp.rc
   ```

8. LNSNMP サービスがシステム再始動中に開始されるように構成します。/etc/rc.tcpip の末尾に以下の行を追加します。

   ```
   /etc/lnsnmp.rc start
   ```

IBM Domino Server アドイン・タスクの開始

SNMP サービスを構成した後に、IBM Domino Server アドイン・タスクを開始する必要があります。

このタスクについて

Domino 区画ごとに以下の手順を使用します。

手順

1. IBM Domino Server のコンソールにログインします。
2. Domino イベントで SNMP トラップをサポートするために、以下のコマンドを入力して Event Interceptor アドイン・タスクを開始します。

   ```
   load intrcpt
   ```

3. Domino 統計しきい値トラップをサポートするために、以下のコマンドを入力して Statistic Collector アドイン・タスクを開始します。

   ```
   load collect
   ```

4. IBM Domino の次回再始動時にアドイン・タスクが自動的に再始動されるように調整します。IBM Domino の `NOTES.INI` ファイル内の *ServerTasks* 変数に **`intrcpt`** および **`collect`** を追加します。

SNMP サービスの構成

SNMP サービスを構成できます。

このタスクについて

構成は、ご使用の環境によって異なることがあります。詳しくは、ベンダーの資料を参照してください。

手順

1. IBM Domino Administrator ユーティリティーを開き、管理資格情報を使用して認証します。
2. 「ファイル」タブをクリックし、「**Monitoring Configuration**」(`events4.nsf`) 資料をクリックします。
3. 「DDM 設定」ツリーを展開し、「タイプ別 **DDM** 調査 **(DDM Probes By Type)**」を選択します。
4. 「調査を有効にする」を選択してから、「ビュー内のすべての調査を有効にする」を選択します。

   注**:** このアクションを実行すると、警告を受け取ることがあります。一部の調査をさらに構成する必要があるため、この警告は正常な結果です。

5. 「**DDM** フィルタ」を選択します。

   新規 DDM フィルターを作成するか、既存の DDM デフォルト・フィルターを編集できます。

6. DDM フィルターを拡張イベントおよびシンプル・イベントに適用します。すべてのイベント・タイプをログに記録することを選択します。
7. 環境によっては、フィルターの適用先をドメイン内のすべてのサーバーにするか、特定のサーバーのみにするかを選択できます。
8. 「保存」をクリックします。完了したら閉じます。

9. 「イベントハンドラ」ツリーを展開し、「サーバー別イベントハンドラ **(Event Handlers By Server)**」を選択します。
10. 「新規イベントハンドラ」を選択します。
11. 以下のパラメーターを構成します。
    - 基本 - モニターするサーバー: ドメイン内のすべてのサーバーをモニターするか、特定のサーバーのみをモニターするかを選択します。
    - 基本 - 通知トリガー:「検索条件に合ったイベント」。
    - イベント - 検索条件:「すべての種類のイベント」。
    - イベント - 検索条件:「指定した優先順位のイベント (Events must be one of these priorities)」(すべてのボックスにチェック・マークを付けます)。
    - イベント - 検索条件:「すべてのイベントメッセージ」。
    - アクション - 通知方法:「SNMP トラップ」。
    - アクション - 有効/無効:「有効」。
12. 「保存」をクリックします。完了したら閉じます。

これで、IBM Security QRadar でログ・ソースを構成する準備ができました。

QRadar との通信のための IBM Lotus Domino デバイスの構成

IBM Security QRadar が IBM Lotus Domino デバイスからの受信 syslog イベントを自動的に検出することはありません。

このタスクについて

QRadar の「管理」タブで、ログ・ソースを手動で作成する必要があります。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで「IBM Lotus Domino」を選択します。
6. 「プロトコル構成」リストで、「**SNMPv2**」を選択します。
7. 以下の値を構成します。

表 199. SNMPv2 プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	SNMPv2 イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。 QRadar が固有のイベント・ソースのログ・ファイルを識別できる、IP アドレスまたはホスト名の入力が推奨されます。
コミュニティー **(Community)**	SNMP イベントが含まれているシステムにアクセスするために必要な SNMP コミュニティー名を入力します。

表 199. SNMPv2 プロトコルのパラメーター (続き)

パラメーター	説明
イベント・ペイロードに **OID** を含める **(Include OIDs in Event Payload)**	このチェック・ボックスの値をクリアします。 このオプションが選択されている場合、標準イベント・ペイロード・フォーマットではなく、名前と値のペアを使用して SNMP イベントが構成されます。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Privileged Session Recorder

IBM Privileged Session Recorder 用の IBM Security QRadar DSM は、IBM Privileged Session Recorder デバイスからイベント・ログを収集することができます。

IBM Privileged Session Recorder DSM の仕様を以下の表に示します。

表 200. IBM Privileged Session Recorder の仕様

仕様	値
製造元	IBM
DSM 名	Privileged Session Recorder
RPM ファイル名	DSM-IBMPrivilegedSessionRecorder
プロトコル	JDBC
QRadar で記録されるイベント・タイプ	コマンド実行監査イベント
自動的に検出?	いいえ
ID を含む?	いいえ
その他の情報	IBM Web サイト (http://www.ibm.com/)

IBM Privileged Session Recorder のイベントを収集するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM をダウンロードして QRadar コンソールにインストールしてください。
   - Protocol-JDBC RPM
   - IBM Privileged Session Recorder DSM RPM
2. IBM Security Privileged Identity Manager ダッシュボードで、Privileged Session Recorder データ・ストアのデータベース情報を取得し、着信 TCP 接続を許可するように IBM Privileged Session Recorder DB2 データベースを構成します。
3. IBM Privileged Session Recorder のインスタンスごとに、QRadar コンソール上で IBM Privileged Session Recorder のログ・ソースを作成します。Imperva SecureSphere パラメーターを定義するには以下の表の内容を使用します。

表 201. *IBM Privileged Session Recorder* ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース・タイプ	IBM Privileged Session Recorder
プロトコル構成	JDBC
ログ・ソース ID	*DATABASE@HOSTNAME*
データベース・タイプ	DB2
データベース名	IBM Privileged Identity Manager ダッシュボードで構成した Session Recorder データ・ストアの名前。
IP またはホスト名	Session Recorder データベース・サーバーのアドレス。
ポート	IBM Privileged Identity Manager ダッシュボードで指定したポート。
ユーザー名	DB2 データベースのユーザー名
パスワード	DB2 データベースのパスワード。
定義済み照会	IBM Privileged Session Recorder
準備済みステートメントの使用 (Use Prepared Statements)	このオプションは必ず選択します。
開始日時	JDBC 取得の初回日時。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『QRadar との通信のための IBM Privileged Session Recorder の構成』
IBM Privileged Session Recorder で IBM Security QRadar 用にログ・ソースを構成するには、事前に Privileged Session Recorder データ・ストアのデータベース情報を取得します。また、QRadar からの着信 TCP 接続を許可するように IBM Privileged Session Recorder DB2 データベースを構成する必要があります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信のための IBM Privileged Session Recorder の構成

IBM Privileged Session Recorder で IBM Security QRadar 用にログ・ソースを構成するには、事前に Privileged Session Recorder データ・ストアのデータベース情報を取得します。また、QRadar からの着信 TCP 接続を許可するように IBM Privileged Session Recorder DB2 データベースを構成する必要があります。

IBM Privileged Session Recorder は、IBM Security Privileged Identity Manager のコンポーネントです。

手順

1. IBM Security Privileged Identity Manager Web ユーザー・インターフェースにログインします。

2. 「**Privileged Identity Manager** の構成 **(Configure Privileged Identity Manager)**」タブを選択します。
3. 「外部エンティティーの管理」セクションで「データベース・サーバーの構成」を選択します。
4. テーブル内で、「データベース・サーバーの構成」列の「セッション記録データ・ストア」行をダブルクリックします。
5. QRadar でログ・ソースを構成する際に使用する以下のパラメーターを記録します。

IBM Privileged Session Recorder フィールド	**QRadar** ログ・ソースのフィールド
ホスト名	IP またはホスト名
ポート	ポート
データベース名	データベース名
データベース管理者 **ID**	ユーザー名

IBM Privileged Session Recorder のログ・ソースの構成

QRadar は、IBM Privileged Session Recorder イベントを自動的に検出することはありません。IBM Privileged Session Recorder のイベント・データを統合するには、イベント・ログの収集元となるインスタンスごとにログ・ソースを作成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「IBM **Privileged Session Recorder**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. 「定義済み照会 **(Predefined Query)**」リストで「IBM **Privileged Session Recorder**」を選択します。
9. 「準備済みステートメント **(Prepared Statement)**」チェック・ボックスを選択します。
10. 残りのパラメーターを構成します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Proventia

IBM Security QRadar は複数の IBM Proventia DSM をサポートしています。

QRadar は、以下の複数の IBM Proventia DSM をサポートしています。

IBM Proventia Management SiteProtector

IBM Security QRadar 用の IBM Proventia® Management SiteProtector DSM は、SiteProtector データベースをポーリングして SiteProtector イベントを受け入れます。

この DSM により、QRadar は、IBM SiteProtector データベースからの侵入防御システム (IPS) イベントと監査イベントを直接記録できます。

注: IBM Proventia Management SiteProtector DSM は、監査イベントを収集するために、最新の JDBC プロトコルを必要とします。

IBM Security QRadar 用の IBM Proventia Management SiteProtector DSM は、プライマリー SensorData1 テーブルの情報を読み取ることで、詳細 SiteProtector イベントを受け入れることができます。SensorData1 テーブルは、IBM SiteProtector データベース内の他の複数のテーブルからの情報で生成されます。イベント収集では SensorData1 が常にプライマリー・テーブルになります。

IDP イベントには、SensorData1 からの情報とともに、以下のテーブルからの情報が含まれます。

- SensorDataAVP1
- SensorDataReponse1

監査イベントには、以下のテーブルからの情報が含まれます。

- AuditInfo
- AuditTrail

監査イベントはデフォルトで収集されません。「監査イベントを含む」チェック・ボックスを選択した場合、AuditInfo テーブルと AuditTrail テーブルに別個に照会を行ってください。SiteProtector データベースのテーブルについて詳しくは、ベンダー資料を参照してください。

QRadar を SiteProtector と統合するように構成する前に、SiteProtector で QRadar 用にデータベースのユーザー・アカウントとパスワードを作成しておくことをお勧めします。

QRadar ユーザーは、SiteProtector イベントを保管する SensorData1 テーブルに対する読み取り権限が必要です。JDBC と SiteProtector の間のプロトコルにより、QRadar がデータベースにログインし、イベントをポーリングできます。QRadar のアカウントを作成することは必須ではありませんが、イベント・データのトラッキングおよび保護という点で推奨されます。

注: SiteProtector コンソールと QRadar の間の通信がファイアウォール・ルールによってブロックされていないことを確認してください。

ログ・ソースの構成

IBM SiteProtector イベントについてポーリングするように IBM Security QRadar を構成できます。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで「IBM **Proventia Management** SiteProtector」を選択します。
6. 「プロトコル構成」リストを使用して、「**JDBC - SiteProtector**」を選択します。
7. 以下の値を構成します。

表 *202. JDBC - SiteProtector* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は、以下の形式で定義する必要があります。 <*database*>@<*hostname*> 各部分について以下で説明します。 • <*database*> は、**「データベース名」**パラメーターで定義されているデータベース名です。database (データベース名) は必須です。 • <*hostname*> は、「**IP** またはホスト名」パラメーターで定義されている、ログ・ソースのホスト名または IP アドレスです。hostname は必須です。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
データベース・タイプ	リストで、イベント・ソースに使用するデータベースのタイプとして「**MSDE**」を選択します。
データベース名	接続先データベースの名前を入力します。デフォルトのデータベース名は RealSecureDB です。
IP またはホスト名	データベース・サーバーの IP アドレスまたはホスト名を入力します。

表 202. JDBC - SiteProtector プロトコルのパラメーター (続き)

パラメーター	説明
ポート	データベース・サーバーが使用するポート番号を入力します。表示されるデフォルトは、選択した「データベース・タイプ」によって異なります。有効な範囲は 0 から 65536 です。MSDE のデフォルトはポート 1433 です。 JDBC 構成のポートは、データベースのリスナー・ポートに一致する必要があります。データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 すべてのオプションのデフォルトのポート番号は次のとおりです。 • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Oracle - 1521 • Sybase - 1521 データベース・タイプとして MSDE を使用する際にデータベース・インスタンスを定義する場合、構成で「ポート」パラメーターをブランクのままにする必要があります。
ユーザー名	データベース・ユーザー名を入力します。ユーザー名は、英数字で最大 255 文字までです。ユーザー名には下線 (_) も使用できます。
パスワード	データベース・パスワードを入力します。 パスワードの最大長は 255 文字です。
パスワードの確認	データベースにアクセスするためのパスワードを確認します。
認証ドメイン	「データベース・タイプ」として **MSDE** を選択し、データベースが Windows 用に構成されている場合は、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。 認証ドメインには、英数字を含める必要があります。ドメインに使用できる特殊文字は、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
データベース・インスタンス	「**MSDE**」を「データベース・タイプ」として選択し、1 つのサーバーに複数の SQL サーバー・インスタンスがある場合、接続先にするインスタンスを定義します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックした場合は、構成内で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードが含まれるビューの名前を入力します。デフォルトのテーブル名は SensorData1 です。
AVP ビュー名 (AVP View Name)	イベント属性が含まれるビューの名前を入力します。デフォルトのテーブル名は SensorDataAVP です。

表 202. *JDBC - SiteProtector* プロトコルのパラメーター (続き)

パラメーター	説明
応答ビュー名 **(Response View Name)**	応答イベントが含まれるビューの名前を入力します。デフォルトのテーブル名は SensorDataResponse です。
選択リスト	テーブルまたはビューのすべてのフィールドを含めるには、* を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	テーブルへの照会から次の照会までの間に追加された新規イベントを識別するには、`SensorDataRowID` と入力します。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。指定子の H および M のない数値の場合は、秒単位のポーリングになります。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「**MSDE**」を「データベース・タイプ」として選択した場合は、このチェック・ボックスを選択して、TCP/IP ポート接続の代替方式を使用します。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。
監査イベントを含む	監査イベントを IBM SiteProtector から収集する場合は、このチェック・ボックスを選択します。 デフォルトでは、このチェック・ボックスはクリアされています。
NTLMv2 の使用	NTLMv2 認証を必要とする SQL サーバーとの通信時に MSDE 接続で NTLMv2 プロトコルを使用するように強制する場合は、「**NTLMv2** の使用」チェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されています。 「**NTLMv2** の使用」チェック・ボックスを選択した場合でも、NTLMv2 認証を必要としない SQL サーバーへの MSDE 接続には影響しません。

表 202. JDBC - SiteProtector プロトコルのパラメーター (続き)

パラメーター	説明
SSL の使用 **(Use SSL)**	接続で SSL 通信がサポートされている場合は、このチェック・ボックスを選択します。
ログ・ソース言語	ログ・ソース・イベントの言語を選択します。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

IBM ISS Proventia

IBM Security QRadar 用の IBM Integrated Systems Solutions® (ISS) Proventia DSM は、SNMP を使用して、関連するすべての IBM Proventia® イベントを記録します。

手順

1. Proventia Manager ユーザー・インターフェースのナビゲーション・ペインで、「システム・ノード **(System node)**」を展開します。
2. 「システム **(System)**」を選択します。
3. 「サービス **(Services)**」を選択します。

   「サービス構成 (Service Configuration)」ページが表示されます。
4. 「**SNMP**」タブをクリックします。
5. 「**SNMP** トラップが有効 **(SNMP Traps Enabled)**」を選択します。
6. 「トラップ・レシーバー **(Trap Receiver)**」フィールドに、受信 SNMP トラップをモニターする QRadar の IP アドレスを入力します。
7. 「トラップ・コミュニティー **(Trap Community)**」フィールドに、該当するコミュニティー名を入力します。
8. 「トラップ・バージョン **(Trap Version)**」リストでトラップ・バージョンを選択します。
9. 「変更の保存 **(Save Changes)**」をクリックします。

   これで、SNMP トラップを受信するように QRadar を構成する準備ができました。
10. ISS Proventia デバイスからイベントを受信するように QRadar を構成するには、以下のようにします。「ログ・ソース・タイプ」リストで「IBM **Proventia Network Intrusion Prevention System (IPS)**」を選択します。

    ISS Proventia デバイスについて詳しくは、ベンダーの資料を参照してください。

関連概念:

34 ページの『SNMPv2 プロトコルの構成オプション』
SNMPv2 プロトコルを使用して SNMPv2 イベントを受信するようにログ・ソースを構成することができます。

34 ページの『SNMPv3 プロトコルの構成オプション』
SNMPv3 プロトコルを使用して SNMPv3 イベントを受信するようにログ・ソースを構成することができます。

IBM RACF

IBM Security QRadar には、IBM RACF® からのイベントを統合するための 2 つのオプションがあります。

以下のオプションを参照してください。

- 532 ページの『監査スクリプトを使用した IBM RACF と IBM Security QRadar の統合』
- 『IBM Security zSecure を使用した IBM RACF と IBM Security QRadar の統合』

IBM Security zSecure を使用した IBM RACF と IBM Security QRadar の統合

IBM RACF DSM により、IBM Security zSecure を使用して、IBM z/OS® メインフレームからのイベントを統合できます。

zSecure プロセスを使用すると、System Management Facilities (SMF) からのイベントは、ログ・イベント拡張フォーマット (LEEF) のイベント・ファイルに記録されます。QRadar は、ログ・ファイル・プロトコルを使用して LEEF イベント・ログ・ファイルを取得し、イベントを処理します。ポーリング間隔に基づいてイベントを取得するように QRadar をスケジュールできます。これにより、QRadar は定義されたスケジュールに基づいてイベントを取得できます。

IBM RACF LEEF イベントを統合するには、以下のようにします。

1. インストール済み環境が、前提条件となるインストール要件をすべて満たしていることを確認します。詳しくは、『始める前に』を参照してください。
2. イベントを LEEF 形式で書き込むように IBM z/OS イメージを構成します。詳しくは、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。
3. IBM RACF が LEEF 形式のイベント・ログを取得するために、QRadar でログ・ソースを作成します。詳しくは、 528 ページの『IBM Security QRadar での IBM RACF ログ・ソースの作成』を参照してください。
4. オプション。QRadar で IBM RACF 用のカスタム・イベント・プロパティーを作成します。詳しくは、テクニカル・ノート「*IBM Security QRadar Custom Event Properties for IBM z/OS*」を参照してください。

始める前に

データ収集プロセスを構成する前に、基本の zSecure インストール・プロセスを完了する必要があります。

以下の前提条件は必須です。

- z/OS イメージ上の IBM Security zSecure Audit で parmlib メンバーの IFAPRDxx が有効になっていることを確認する必要があります。

- SCKRLOAD ライブラリーは APF が許可されていなければなりません。
- CKFREEZE と UNLOAD のデータ・セットが定期的に更新されるようにプロセスを構成する必要があります。
- LEEF イベント・ファイルをダウンロードするには、QRadar に対して z/OS イメージ上の SFTP、FTP、または SCP の各サーバーを構成する必要があります。
- QRadar と z/OS イメージの間にあるファイアウォールで SFTP トラフィック、FTP トラフィック、または SCP トラフィックを許可する必要があります。

ソフトウェアをインストールしたら、ポストインストール・アクティビティーを実行して、構成を作成および変更する必要があります。zSecure のインストールおよび構成の手順については、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。

IBM Security QRadar での IBM RACF ログ・ソースの作成

ログ・ファイル・プロトコルにより、QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

このタスクについて

ログ・ファイルは、一度に 1 つずつ、処理のために QRadar に転送されます。ログ・ファイル・プロトコルは、プレーン・テキストのイベント・ログや圧縮ファイル、アーカイブを管理できます。アーカイブには、一度に 1 行ずつ処理できるプレーン・テキスト・ファイルが含まれている必要があります。複数行イベント・ログは、ログ・ファイル・プロトコルではサポートされていません。 zSecure が含まれた IBM z/OS は、指定されたディレクトリーにログ・ファイルを `gzip` アーカイブとして書き込みます。QRadar は、アーカイブを取り出し、ファイルに 1 行当たり 1 イベントで書き込まれているイベントを処理します。

これらのイベントを取得するには、ログ・ファイル・プロトコルを使用してログ・ソースを作成する必要があります。QRadar は、LEEF 形式のイベント・ファイルをホストするシステムにログインするための資格情報と、ポーリング間隔を要求します。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「IBM **Resource Access Control Facility**」(RACF) を選択します。
7. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
8. 以下の値を構成します。

表 *203. IBM RACF* ログ・ファイル・プロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。 QRadar がログ・ファイルを固有のイベント・ソースに識別できるようになるので、IP アドレスまたはホスト名が推奨 ID です。 例えば、ネットワークに複数のデバイス (例えば、複数の z/OS イメージ)、またはすべてのイベント・ログが入っているファイル・リポジトリーが含まれている場合、IBM RACF ログ・ソースのイベントを一意に識別する、イメージまたは場所の名前、IP アドレス、またはホスト名を指定します。この指定により、ユーザーが識別可能なネットワークのイメージ・レベルまたは場所のレベルで、イベントを識別できるようになります。
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 このオプションには、以下のポートがあります。 • **FTP** - TCP ポート 21 • **SFTP** - TCP ポート 22 • **SCP** - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名またはユーザー ID を入力します。 • ログ・ファイルが IBM z/OS イメージ上にある場合は、IBM z/OS にログインするために必要なユーザー ID を入力します。ユーザー ID の長さは 8 文字まで可能です。 • ログ・ファイルがファイル・リポジトリー上にある場合は、ファイル・リポジトリーにログインするために必要なユーザー名を入力します。ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。

表 *203. IBM RACF* ログ・ファイル・プロトコル・パラメーター *(*続き*)*

パラメーター	説明
SSH 鍵ファイル	「サービス・タイプ」として「**SCP**」または「**SFTP**」を選択した場合、このパラメーターにより、SSH 秘密鍵ファイルを定義できます。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 **SCP** をサービス・タイプとして構成する場合は、「再帰的 **(Recursive)**」オプションは無視されます。
FTP ファイル・パターン	「サービス・タイプ」として「**SFTP**」または「**FTP**」を選択した場合、このオプションにより、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 IBM Security zSecure Audit を使用する IBM z/OS メインフレームは、`RACF.<timestamp>.gz` というパターンを使用してイベント・ファイルを書き込みます。 指定する「**FTP** ファイル・パターン」は、イベント・ファイルに割り当てた名前に一致する必要があります。例えば、先頭が zOS で末尾が `.gz` のファイルを収集するには、以下のコードを入力します。 `RACF.*¥.gz` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「`FTP`」を「**サービス・タイプ**」として選択した場合にのみ表示されます。 バイナリー転送モードは、`zip`、`gzip`、`tar`、`tar+gzip` アーカイブ・ファイルなど、バイナリー (圧縮) フォーマットで保管されたイベント・ファイルの場合に必要です。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。
開始時刻	処理を開始する時刻を入力します。例えば、午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、`00:00` と入力します。 このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。

表 *203. IBM RACF* ログ・ファイル・プロトコル・パラメーター *(*続き*)*

パラメーター	説明
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 (Ignore Previously Processed File)」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「**gzip**」を選択します。 プロセッサーにより、イベント・ファイル・アーカイブを解凍し、内容をイベント用に処理できます。ファイルは、QRadar にダウンロードされた後にのみ処理されます。QRadar は、zip、gzip、tar、または tar+gzip の各アーカイブ・フォーマットのファイルを処理できます。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって処理された、以前に処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが処理されたかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。以前に処理されていないすべてのファイルがダウンロードされます。 このオプションは、「**FTP**」および「**SFTP**」の「サービス・タイプ」にのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスはクリアのままにしておきます。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。このフィールドでは、ファイルの保管用に使用するローカル・ディレクトリーを構成できます。

表 203. IBM RACF ログ・ファイル・プロトコル・パラメーター (続き)

パラメーター	説明
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに複数の処理を適用します。ファイルの各行が、単一イベントです。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

IBM RACF の構成が完了します。IBM RACF でカスタム・イベント・プロパティーが必要な場合は、テクニカル・ノート「*IBM Security QRadar Custom Event Properties for IBM z/OS*」を参照してください。

監査スクリプトを使用した IBM RACF と IBM Security QRadar の統合

IBM Security QRadar 用の IBM Resource Access Control Facility (RACF®) DSM により、IBM RACF を使用して、トランザクションの監査のために IBM z/OS メインフレームと統合できます。

QRadar は、イベントからの入手可能な関連情報をすべて記録します。

注**:** zSecure 統合は、カスタム・イベントをログ・ソースに提供する唯一の統合です。カスタム・イベントは、ネイティブの QEXRACF 統合を使用してイベントを収集するときにも表示できます。

IBM RACF イベントを QRadar と統合するには、以下の手順を使用します。

1. IBM メインフレーム・システムは、すべてのセキュリティー・イベントを、ライブ・リポジトリー内にサービス・マネジメント・フレームワーク (SMF) レコードとして記録します。
2. 午前 0 時に、IBM RACF データが、SMF ダンプ・ユーティリティーを使用してライブ・リポジトリーから抽出されます。RACFICE ユーティリティーの IRRADU00 (IBM ユーティリティーの 1 つ) は、前日のすべてのイベントおよびフィールドを含むログ・ファイルを、SMF レコード形式で作成します。
3. QEXRACF プログラムが、SMF 形式ファイルからデータをプルします。プログラムは QRadar の関連イベントおよび関連フィールドのみをプルし、互換性を考慮して、その情報を圧縮形式で書き込みます。この情報は、QRadar がアクセスできる場所にも保存されます。
4. QRadar は、ログ・ファイル・プロトコル・ソースを使用して QEXRACF 出力ファイルをプルし、スケジュールに基づいて情報を取得します。次に、QRadar はこのファイルをインポートして処理します。

IBM Security QRadar と統合するための IBM RACF の構成

IBM メインフレーム RACF は、QRadar と以下のように統合できます。

手順

1. qexracf_bundled.tar.gz を IBM サポートの Web サイトからダウンロードします。
2. Linux ベースのオペレーティング・システムで、以下のコマンドを使用してファイルを解凍します。

   ```
   tar -zxvf qexracf_bundled.tar.gz
   ```

   アーカイブには、以下のファイルが含まれています。

   - qexracf_jcl.txt
   - qexracfloadlib.trs
   - qexracf_trsmain_JCL.txt
3. 任意の端末エミュレーター・ファイル転送方式を使用して、ファイルを IBM メインフレームにロードします。

   TEXT プロトコルを使用して、qexracf_trsmain_JCL.txt ファイルと qexracf_jcl.txt ファイルをアップロードします。

   バイナリー・モードを使用して QexRACF loadlib.trs ファイルをアップロードし、事前割り振りデータ・セットに追加します。 QexRACF loadlib.trs ファイルは、実行可能プログラム (メインフレーム・プログラム QEXRACF) が含まれている簡潔なファイルです。

   .trs ファイルをワークステーションからアップロードするときに、DCB 属性 DSORG=PS、RECFM=FB、LRECL=1024、BLKSIZE=6144 を使用して、メインフレーム上でファイルを事前割り振りします。ファイル転送タイプは、テキストではなくバイナリー・モードでなければなりません。
4. インストール済み環境固有の要件に応じて、qexracf_trsmain_JCL.txt ファイルをカスタマイズします。

   qexracf_trsmain_JCL.txt ファイルは、IBM ユーティリティーの Trsmain を使用して、QexRACF loadlib.trs ファイルに保管されているプログラムを圧縮解除します。

   qexracf_trsmain_JCL.txt ファイルの例を次に示します。以下のコードが含まれています。

   ```
   //TRSMAIN JOB (yourvalidjobcard),Q1labs,
   // MSGCLASS=V //DEL EXEC PGM=IEFBR14
   //D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXRACF.TRS // UNIT=SYSDA,
   // SPACE=(CYL,(10,10))
   //TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
   //SYSPRINT DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
   //INFILE DD DISP=SHR,DSN=<yourhlq>.QEXRACF.TRS
   //OUTFILE DD DISP=(NEW,CATLG,DELETE),
   // DSN=<yourhlq>.LOAD,
   // SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA //
   ```

   このファイルは、インストール済み環境固有のパラメーター向け情報 (ジョブ・カード、データ・セット命名規則、出力宛先、保存期間、スペース所要量など) で更新する必要があります。

.trs 入力ファイルは、IBM TERSE フォーマットのライブラリーであり、TRSMAIN を呼び出す JCL の実行によって取り出されます。この簡潔なファイルは抽出時に、QEXRACF プログラムをメンバーとして持つ PDS LINKLIB を作成します。

5. STEPLIB をこのライブラリーに対して実行するか、または LINKLST 内にある LINKLIB の 1 つにこのプログラムを移動することを選択できます。このプログラムには許可は必要ありません。
6. アップロードの完了後に、プログラムを既存のリンク・リスト・ライブラリーにコピーするか、またはプログラムを含むことになるライブラリーの、正しいデータ・セット名を持つ STEPLIB DD ステートメントを追加します。
7. qexracf_jcl.txt ファイルは、IBM IRRADU00 ユーティリティーの実行に必要な JCL を提供するための、サンプル JCL デックが含まれているテキスト・ファイルです。これにより、QRadar は必要な IBM RACF イベントを取得できます。ローカル規格を満たすようにジョブ・カードを構成します。

   qexracf_jcl.txt ファイルの例として、以下のコードが含まれています。

```
//QEXRACF JOB (<your valid jobcard>),Q1LABS,
// MSGCLASS=P, // REGION=0M //*
//*QEXRACF JCL version 1.0 April 2009 //*
//*************************************************************
//* Change below dataset names to sites specific datasets names *
//*************************************************************
//SET1 SET SMFOUT='<your hlq>.CUSTNAME.IRRADU00.OUTPUT',
// SMFIN='<your SMF dump ouput dataset>',
// QRACFOUT='<your hlq>.QEXRACF.OUTPUT'
//*************************************************************
//* Delete old datasets *
//*************************************************************
//DEL EXEC PGM=IEFBR14 //DD2 DD DISP=(MOD,DELETE),DSN=&QRACFOUT,
// UNIT=SYSDA, // SPACE=(TRK,(1,1)), // DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//* Allocate new dataset *
//*************************************************************
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DISP=(NEW,CATLG),DSN=&QRACFOUT,
// SPACE=(CYL,(1,10)),UNIT=SYSDA,
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*************************************************************
//* Execute IBM IRRADU00 utility to extract RACF smf records *
//*************************************************************
//IRRADU00 EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//ADUPRINT DD SYSOUT=*
//OUTDD DD DSN=&SMFOUT,SPACE=(CYL,(100,100)),DISP=(,CATLG),
// DCB=(RECFM=FB,LRECL=8192,BLKSIZE=40960),
// UNIT=SYSALLDA
//SMFDATA DD DISP=SHR,DSN=&SMFIN
//SMFOUT DD DUMMY
//SYSIN DD *INDD(SMFDATA,OPTIONS(DUMP))
OUTDD(SMFOUT,TYPE(30:83)) ABEND(NORETRY)
USER2(IRRADU00) USER3(IRRADU86) /*
//EXTRACT EXEC PGM=QEXRACF,DYNAMNBR=10,
// TIME=1440
//*STEPLIB DD DISP=SHR,DSN=
<the loadlib containing the QEXRACF program if not in LINKLST>
//SYSTSIN DD DUMMY //SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//RACIN DD DISP=SHR,DSN=&SMFOUT
//RACOUT DD DISP=SHR,DSN=&QRACFOUT //
```

```
//*************************************************************
//* FTP Output file from C program (Qexracf) to an FTP server *
//* QRadar will go to that FTP Server to get file *
//* Note you need to replace <user>, <password>,<serveripaddr>*
//* <THEIPOFTHEMAINFRAMEDEVICE> and <QEXRACFOUTDSN> *
//*************************************************************
//*FTP EXEC PGM=FTP,REGION=3800K //*INPUT DD *
//*<FTPSERVERIPADDR>
//*<USER>
//*<PASSWORD>
//*ASCII //*PUT '<QEXRACFOUTDSN>'
/<THEIPOFTHEMAINFRAMEDEVICE>/<QEXRACFOUTDSN>
//*QUIT //*OUTPUT DD SYSOUT=*
//*SYSPRINT DD SYSOUT=* //* //*
```

8. 出力ファイルを作成した後に、このファイルを FTP サーバーに送信する必要があります。 このアクションにより、ユーティリティーを実行するたびに、出力ファイルはスクリプトの終了時に、処理のために特定の FTP サーバーに必ず送信されます。 z/OS プラットフォームが FTP または SFTP 経由でファイルを提供するように構成されているか、または SCP を許可するように構成されている場合、一時サーバーは不要であり、QRadar はそれらのファイルをメインフレームから直接プルすることができます。一時 FTP サーバーが必要な場合、QRadar は、各 IBM RACF ログ・ソースに固有の IP アドレスを必要とします。固有の IP アドレスが指定されない場合、それらの複数のログ・ソースは、1 つのシステムとして結合されます。

IBM RACF ログ・ソースの作成

ログ・ファイル・プロトコルにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

このタスクについて

ログ・ファイルは、一度に 1 つずつ、処理のために QRadar に転送されます。ログ・ファイル・プロトコルは、プレーン・テキストのイベント・ログや圧縮ファイル、アーカイブを管理できます。アーカイブには、一度に 1 行ずつ処理できるプレーン・テキスト・ファイルが含まれている必要があります。複数行イベント・ログは、ログ・ファイル・プロトコルではサポートされていません。 IBM RACF は QRadar と統合し、監査スクリプトを使用して、指定のディレクトリーにログ・ファイルをプレーン・テキスト・ファイルとして書き込みます。QRadar は、ファイルに 1 行当たり 1 イベントで書き込まれているイベントを処理します。 QRadar は、アーカイブを取り出し、ファイルに 1 行当たり 1 イベントで書き込まれているイベントを処理します。

これらのイベントを取得するには、ログ・ファイル・プロトコルを使用してログ・ソースを作成する必要があります。 QRadar は、イベント・ファイルをホスティングするシステムにログインするための資格情報と、ポーリング間隔を要求します。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。

5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「IBM **Resource Access Control Faclilty**」(RACF) を選択します。
7. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
8. 以下の値を構成します。

表 *204. IBM RACF* ログ・ファイル・プロトコル・パラメーター

パラメーター	説明
ログ・ソース ID	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。QRadar が固有のイベント・ソースのログ・ファイルを識別できる、IP アドレスまたはホスト名の入力が推奨されます。 例えば、ネットワークに、複数の z/OS イメージなどの複数のデバイスや、すべてのイベント・ログを含むファイル・リポジトリーが含まれている場合、IBM RACF ログ・ソースのイベントを一意に識別する、イメージまたは場所の名前、IP アドレス、またはホスト名を指定する必要があります。これにより、ユーザーが識別可能なネットワークのイメージ・レベルまたは場所のレベルで、イベントが識別されるようになります。
サービス・タイプ	リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを、リストから選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート IP またはホスト名	イベント・ログ・ファイルを保管しているデバイスの IP アドレスまたはホスト名を入力します。

表 *204. IBM RACF* ログ・ファイル・プロトコル・パラメーター *(*続き*)*

パラメーター	説明
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 以下のオプションがあります。 • **FTP** - TCP ポート 21 • **SFTP** - TCP ポート 22 • **SCP** - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、それに応じてポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれるホストにログインするために必要なユーザー名またはユーザー ID を入力します。 • ログ・ファイルが IBM z/OS イメージ上にある場合は、IBM z/OS にログインするために必要なユーザー ID を入力します。ユーザー ID の長さは 8 文字まで可能です。 • ログ・ファイルがファイル・リポジトリー上にある場合は、ファイル・リポジトリーにログインするために必要なユーザー名を入力します。ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。
SSH 鍵ファイル	サービス・タイプとして SCP または SFTP を選択する場合、このパラメーターを使用して SSH 秘密鍵ファイルを定義できます。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。

表 *204. IBM RACF* ログ・ファイル・プロトコル・パラメーター (続き)

パラメーター	説明
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。これは、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートするためです。
再帰的 (Recursive)	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」オプションは無視されます。
FTP ファイル・パターン	SFTP または FTP をサービス・タイプとして選択する場合、このオプションによって、リモート・ディレクトリーで指定されたファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。例えば、先頭が zOS で末尾が .gz のファイルを収集するには、以下を入力します。 このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。

表 *204. IBM RACF* ログ・ファイル・プロトコル・パラメーター *(*続き*)*

パラメーター	説明
FTP 転送モード	このオプションは、FTP をサービス・タイプとして選択した場合にのみ表示されます。 リストから、このログ・ソースに適用する転送モードを選択します。 • バイナリー - バイナリー・データ・ファイル、または圧縮された zip、gzip、tar、tar + gzip のアーカイブ・ファイルを必要とするログ・ソースには、「バイナリー」を選択します。 • **ASCII** - ASCII FTP ファイル転送を必要とするログ・ソースには、ASCII を選択します。
SCP リモート・ファイル	SCP をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。
開始時刻	処理を開始する時刻を入力します。例えば、午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、00:00 と入力します。 このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し (Recurrence)	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。

表 204. IBM RACF ログ・ファイル・プロトコル・パラメーター (続き)

パラメーター	説明
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 (Ignore Previously Processed File)」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	なし。
以前に処理したファイルを無視 (Ignore Previously Processed File(s))	ログ・ファイル・プロトコルによって既に処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが以前に処理されているかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。以前に処理されていないすべてのファイルがダウンロードされます。 このオプションは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar システム上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスはクリアしたままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー (Local Directory)」フィールドが表示されます。これによりファイルの保管に使用するローカル・ディレクトリーを構成できます。

表 204. IBM RACF ログ・ファイル・プロトコル・パラメーター (続き)

パラメーター	説明
イベント・ジェネレーター (Event Generator)	「イベント・ジェネレーター **(Event Generator)**」リストで、LineByLine を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに追加の処理を適用します。ファイルの各行が、単一イベントです。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

IBM RACF の構成が完了します。IBM RACF でカスタム・イベント・プロパティーが必要な場合は、テクニカル・ノート「*IBM Security QRadar Custom Event Properties for IBM z/OS*」を参照してください。

IBM Security Access Manager for Enterprise Single Sign-On

IBM Security QRadar 用の IBM Security Access Manager for Enterprise Single Sign-On DSM で、syslog を使用して転送されるイベントを受信できます。

QRadar は、IBM Security Access Manager for Enterprise Single Sign-On バージョン 8.1 または 8.2 からイベントを収集できます。

IBM Security Access Manager for Enterprise Single Sign-On によって転送されるイベントには、監査、システム、および認証の各イベントがあります。

イベントは以下のデータベース・テーブルから読み取られ、syslog を使用して転送されます。

- IMSLOGUserService
- IMSLOGUserAdminActivity
- IMSLOGUserActivity

IBM Security Access Manager for Enterprise Single Sign-On から QRadar に転送されるすべてのイベントは、syslog のフィールド区切り記号として ### を使用します。IBM Security Access Manager for Enterprise Single Sign-On は、UDP ポート 514 を使用して、イベントを QRadar に転送します。

始める前に

イベントの syslog 転送を構成する際に IMS 構成ユーティリティーにアクセスするには、管理者であるか、または使用するユーザー・アカウントに資格情報を含める必要があります。

IBM Security Access Manager for Enterprise Single Sign-On と QRadar の間に構成されるファイアウォールは、ポート 514 の UDP 通信を許可するように構成することが理想的です。この構成では、IBM Security Access Manager for Enterprise Single Sign-On アプライアンスの再始動が必要です。

ログ・サーバー・タイプの構成

IBM Security Access Manager for Enterprise Single Sign-On アプライアンスでは、以下のように、syslog フォーマットのイベントを転送するようにログ・サーバー・タイプを構成する必要があります。

手順

1. IMS Configuration Utility for IBM Security Access Manager for Enterprise Single Sign-On にログインします。

   例: https://localhost:9043/webconf
2. ナビゲーション・メニューで「詳細設定 **(Advanced Settings)**」>「IMS **Server**」>「ロギング **(Logging)**」>「ログ・サーバー情報 **(Log Server Information)**」を選択します。
3. 「ログ・サーバー・タイプ **(Log server types)**」リストで「**syslog**」を選択します。
4. 「追加」をクリックします。
5. 「更新 **(Update)**」をクリックして構成を保存します。

syslog の転送の構成

このタスクについて

イベントを QRadar に転送するには、IBM Security Access Manager for Enterprise Single Sign-On アプライアンスで syslog の宛先を構成する必要があります。

手順

1. ナビゲーション・メニューで「詳細設定 **(Advanced Settings)**」**>**「IMS **Server**」「ロギング **(Logging)**」「**Syslog**」を選択します。
2. 以下のオプションを構成します。

表 *205. Syslog* パラメーター

フィールド	説明
syslog を使用可能にする **(Enable syslog)**	「使用可能なテーブル **(Available Tables)**」リストから以下のテーブルを選択し、「追加 **(Add)**」をクリックする必要があります。 • **logUserService** • **logUserActivity** • **logUserAdminActivity**
Syslog サーバー・ポート **(Syslog server port)**	イベントを QRadar に転送するために使用するポート番号として 514 と入力します。

表 205. *Syslog* パラメーター (続き)

フィールド	説明
Syslog サーバーのホスト名 **(Syslog server hostname)**	QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスまたはホスト名を入力します。
Syslog ロギング・ファシリティー **(Syslog logging facility)**	QRadar に転送されるイベントのファシリティーを指定する整数値を入力します。デフォルト値は 20 です。
Syslog フィールド分離文字 **(Syslog field-separator)**	syslog ペイロード内の名前と値のペアの項目を区切るために使用する文字として ### と入力します。

3. 「更新 **(Update)**」をクリックして構成を保存します。
4. IBM Security Access Manager for Enterprise Single Sign-On アプライアンスを再始動します。

   syslog の構成は完了です。IBM Security Access Manager for Enterprise Single Sign-On の syslog イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

IBM Security QRadar でログ・ソースを構成する

QRadar は、IBM Security Access Manager for Enterprise Single Sign-On からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の手順はオプションです。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで「**IBM Security Access Manager for Enterprise Single Sign-On**」を選択します。
6. 「プロトコル構成」リストで「**Syslog**」を選択します。
7. 以下の値を構成します。

表 206. *Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	IBM Security Access Manager for Enterprise Single Sign-On アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

表 206. Syslog パラメーター (続き)

パラメーター	説明
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。 このチェック・ボックスはデフォルトで選択されます。
信頼性	ログ・ソースの「信頼性」を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	ログ・ソースのターゲットとして使用する「イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」による「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	「受信イベント・ペイロード **(Incoming Event Payload)**」リストで、ログの構文解析と保管を行うための受信ペイロード・エンコーダーを選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的にディスカバーされたログ・ソースは、QRadar の「システム設定」による「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Security Access Manager for Mobile

IBM Security Access Manager for Mobile 用の IBM Security QRadar DSM は、IBM Security Access Manager for Mobile デバイス、および IBM Identity as a Service (IDaaS) デバイスからログを収集します。

以下の表は、IBM Security Access Manager for Mobile DSM の仕様を示しています。

表 207. IBM Security Access Manager for Mobile DSM の仕様

仕様	値
製造元	IBM
DSM 名	IBM Security Access Manager for Mobile

表 207. *IBM Security Access Manager for Mobile DSM* の仕様 (続き)

仕様	値
RPM ファイル名	DSM-IBMSecurityAccessManagerForMobile-7.x -*Qradar_version*-*Buildbuild_number*.noarch.rpm
サポートされるバージョン	IBM Security Access Manager for Mobile v8.0.0 IBM IDaaS v2.0
イベント・フォーマット	Common Base Event 形式 ログ・イベント拡張フォーマット (LEEF)
記録されるイベント・タイプ	IBM_SECURITY_AUTHN IBM_SECURITY_TRUST IBM_SECURITY_RUNTIME IBM_SECURITY_CBA_AUDIT_MGMT IBM_SECURITY_CBA_AUDIT_RTE IBM_SECURITY_RTSS_AUDIT_AUTHZ IBM_SECURITY_SIGNING CloudOE Operations 使用法 IDaas Appliance Audit IDaaS Platform Audit
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	www.ibm.com/software (http://www-03.ibm.com/software/products/en/access-mgr-mobile)

IBM Security Access Manager for Mobile を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンを QRadar コンソール コンソールからダウンロードしてください。

   TLS Syslog プロトコル RPM

   IBM Security Access Manager for Mobile DSM RPM
2. Syslog イベントを QRadar に送信するように IBM Security Access Manager for Mobile デバイスを構成します。

3. QRadar がログ・ソースを自動的に検出しない場合は、QRadar コンソールに IBM Security Access Manager for Mobile ログ・ソースを追加します。IBM Security Access Manager for Mobile および IBM Identity as a Service のイベント収集のために特定の値を必要とするパラメーターについて、次の表で説明します。

表 208. *IBM Security Access Manager for Mobile* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	IBM Security Access Manager for Mobile または IBM Identity as a Service
プロトコル構成	TLS Syslog
ログ・ソース ID	Syslog ヘッダー内の IP アドレスまたはホスト名。Syslog ヘッダーに IP アドレスやホスト名が含まれていない場合、パケット IP アドレスを使用します。
TLS listen ポート	着信 TLS Syslog イベントを受け入れるポート番号を入力します。

4. ログ・ソースを保存すると、着信 TLS Syslog イベント用の listen ポートが作成され、ネットワーク・デバイスの証明書が生成されます。この証明書は、ネットワーク上の、暗号化された Syslog を転送できるすべてのデバイスにコピーする必要があります。syslog-tls 証明書ファイル、および該当 TLS listen ポート番号を持つ追加のネットワーク・デバイスは、QRadar で、TLS Syslog ログ・ソースとして自動的に検出されます。

QRadar との通信のための IBM Security Access Manager for Mobile の構成

TLS Syslog 経由で IBM Security QRadar に監査ログを送信するように IBM Security Access Manager Mobile を構成します。

始める前に

IBM Security Access Manager for Mobile に、TLS Syslog 通信のための QRadar へのアクセス権限があることを確認します。

手順

1. 「モニター - 分析および診断」 > 「ログ」 > 「監査構成」を選択します。
2. 「**Syslog**」タブをクリックして、次の表にある情報を入力します。

フィールド	値
監査ログを有効にする	「監査ログを有効にする」をクリックします。

フィールド	値
詳細監査イベントを有効にする	「詳細監査イベントを有効にする」をクリックします。 冗長ではない監査イベントには、ユーザー・アクティビティーの詳細を格納する JSON ペイロードは含まれません。
syslog サーバーの場所	「リモート **syslog** サーバー」を選択します。
ホスト	QRadar サーバーのホスト名または IP。
ポート	QRadar が着信 TLS Syslog イベントを受け入れるために使用するポート番号。
プロトコル	「**TLS**」を選択します。
証明書データベース **(**トラストストア**)**	Syslog サーバー証明書を検証するトラストストア。
クライアント証明書認証を有効にする	「クライアント証明書認証を有効にする」をクリックします。 クライアントは、サーバー要求に対する SSL ハンドシェーク中にクライアント証明書認証を実行できます。
証明書データベース (鍵ストア)	クライアント証明書認証用の鍵ストア。
証明書ラベル	クライアント証明書認証用の個人証明書。
ディスク・フェイルオーバーを有効にする	「ディスク・フェイルオーバーを有効にする」をクリアします。

3. 「保存」をクリックします。
4. 「変更を確認する場合、または変更をシステムに適用する場合は、ここをクリックしてください」をクリックして、保留中の変更を確認します。
5. 「変更のデプロイ」をクリックします。

   新しい変更内容のいずれかが再始動を必要とする場合は、ランタイム・サーバーが自動的に再始動されます。

QRadar との通信のための IBM IDaaS Platform の構成

IBM IDaaS コンソール上で、IBM IDaaS プラットフォームの監査イベントの LEEF 形式での生成を有効にできます。

始める前に

WAS コンソールに IBM IDaaS プラットフォームがインストールおよび構成されていることを確認します。

手順

1. WAS コンソール上の IDaas プラットフォームの構成ファイルにアクセスします。*<WAS_home>*/profiles/*<profile_name>*/config/idaas/platform.cofig.properties

2. platform.config.properties ファイルに、監査プロパティーのセットが含まれていない場合は、次のオプションを構成します。

プロパティー	説明
audit.enabled=true	監査プロパティーを有効にします。
audit.syslog.message.format=leef audit.syslog.server=10.108.122.107	有効なタイプは LEEF です。
audit.syslog.transport=TRANSPORT_UDP audit.syslog.server.port=514	トランスポート値は TRANSPORT_UDP および TRANSPORT_TLS です。

3. WAS コンソール上の IBM IDaaS プラットフォーム・アプリケーションを再始動します。

QRadar との通信のための IBM IDaaS コンソールの構成

IBM IDaaS コンソール上で、監査イベントの LEEF Syslog 形式での生成を有効にできます。

始める前に

IBM IDaaS コンソールがインストールおよび構成されていることを確認します。

手順

1. 「セキュア・アクセス制御 **(Secure Access Control)**」 > 「拡張構成」を選択します。
2. 「フィルター」テキスト・ボックスで、idaas.audit.event と入力します。デフォルトの形式は Syslog です。
3. 「編集」をクリックします。
4. 「**LEEFSyslog**」を選択します。
5. 「保存」をクリックします。
6. 「変更のデプロイ」をクリックします。

IBM Security Directory Server

IBM Security Directory Server 用の IBM Security QRadar DSM は、IBM Security Directory Server からイベント・ログを収集できます。

以下の表は、IBM Security Directory Server DSM の仕様を示しています。

表 *209. IBM Security Directory Server DSM* の仕様

仕様	値
製造元	IBM
DSM	IBM Security Directory Server
RPM ファイル名	DSM-IBMSecurityDirectoryServer-*build_number*.noarch.rpm

表 209. IBM Security Directory Server DSM の仕様 (続き)

仕様	値
サポートされるバージョン	6.3.1 以降
プロトコル	Syslog (LEEF)
QRadar で記録されるイベント	すべての関連イベント
自動的に検出?	はい
ID を含む?	はい
詳細情報	IBM Web サイト (https://www.ibm.com)

IBM Security Directory Server の統合プロセス

IBM Security Directory Server を IBM Security QRadar と統合できます。

以下の手順を使用します。

1. 自動更新が有効になっていない場合は、以下の最新バージョンの各 RPM をダウンロードして、QRadar コンソールにインストールします。
   - DSMCommon RPM
   - IBM Security Directory Server DSM RPM
2. ネットワーク内の各 IBM Security Directory Server システムを、QRadar と通信できるように構成します。

QRadar と IBM Security Directory Server との間の通信を有効にする方法について詳しくは、IBM の Web サイト (https://www.ibm.com) を参照してください。

1. QRadar がログ・ソースを自動的に検出しない場合は、ネットワーク上の IBM Security Directory Server ごとに、QRadar コンソールでログ・ソースを作成します。

IBM Security QRadar での IBM Security Directory Server ログ・ソースの構成

QRadar でログ・ソースを構成すると、IBM Security Directory Server イベントを収集できます。

このタスクについて

`DSM-IBMSecurityDirectoryServer-build_number.noarch.rpm` ファイルが QRadar ホストでインストールおよびデプロイされていることを確認します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。

3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「IBM **Security Directory Server**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。
8. 残りのパラメーターを構成します。
9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Security Identity Governance

IBM Security Identity Governance 用の IBM Security QRadar DSM は、IBM Security Governance サーバーから監査イベントを収集します。

以下の表は、IBM Security Identity Governance DSM の仕様を示しています。

表 *210. IBM Security Identity Governance (ISIG) DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM Security Identity Governance
RPM ファイル名	`DSM-IBMSecurityIdentityGovernance-`*`Qradar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	IBM Security Identity Governance v5.1.1
プロトコル	JDBC
イベント・フォーマット	NVP
記録されるイベント・タイプ	監査
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	IBM Web サイト (http://www.ibm.com)

IBM Security Identity Governance を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。複数の DSM RPM が必要な場合、統合の順序は DSM RPM の依存関係を反映したものでなければなりません。
   - IBM Security Identity Governance (ISIG) DSM RPM
   - JDBC プロトコル RPM
2. IBM Security Identity Governance データベースからイベントをポーリングするように JDBC ログ・ソースを構成します。

3. QRadar と IBM Security Identity Governance に関連付けられているデータベースとの間の通信を、ファイアウォール・ルールがブロックしないことを確認します。
4. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで IBM Security Identity Governance ログ・ソースを追加してください。以下の表は、IBM Security Identity Governance イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *211. IBM Security Identity Governance* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	IBM Security Identity Governance
プロトコル構成	JDBC
ログ・ソース ID	*DATABASE@HOSTNAME*
データベース・タイプ	イベント・ソースとして使用するデータベースとして「**Oracle**」または「**DB2**」を選択します。
データベース名	IBM Security Identity Governance データベースの名前。これは、**ログ・ソース ID** に対する「データベース」の名前と同じである必要があります。
IP またはホスト名	IBM Security Governance データベースの IP アドレスまたはホスト名。これは、**ログ・ソース ID** の「ホスト名」と同じである必要があります。
ポート	データベース・サーバーが使用するポート番号。デフォルトは、**Oracle: 1521** と **DB2: 50000** です。表示されるデフォルトは、選択したデータベース・タイプによって異なります。
ユーザー名	データベース・ユーザー名。
パスワード	データベース・パスワード。
定義済み照会	デフォルトは、「なし」です。
テーブル名	AUDIT_LOG
選択リスト	*
比較フィールド	ID
準備済みステートメントの使用 (Use Prepared Statements)	チェック・ボックスを有効にします。
開始日時	データベース・ポーリングの最初の日時。
ポーリング間隔 (Polling interval)	データベース表への照会と照会の間の時間 (秒)。デフォルトのポーリング間隔は 10 秒です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数。デフォルトは 20000 EPS です。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

IBM Security Identity Governance データベースと通信するように QRadar を構成

IBM Security Identity Governance データベースから IBM Security QRadar に監査ログを転送するには、ログ・ソースを追加する必要があります。ログ・ソースは自動的には検出されません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで、「**IBM Security Identity Governance**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. パラメーターを構成します。
9. 「保存」をクリックします。

IBM Security Identity Manager

IBM Security QRadar 用の IBM Security Identity Manager DSM は、IBM Security Identity Manager アプライアンスから監査イベント、再認証イベント、およびシステム・イベントを受け入れます。

このタスクについて

QRadar でイベントを収集するには、IBM Security Identity Manager JDBC プロトコルがインストールされている必要があります。このプロトコルにより、QRadarがITIMDB データベース内のイベント情報についてポーリングできるようになります。IBM Security Identity Manager イベントは、データベースのいくつかの他のテーブルとともに監査テーブルから生成されます。

IBM Security Identity Manager と統合するように QRadar を構成する前に、IBM Security Identity Manager for QRadar でデータベースのユーザー・アカウントおよびパスワードを作成します。QRadar ユーザーは、IBM Security Identity Manager イベントが保管される ITIMDB データベースに対する読み取り許可を備えている必要があります。

IBM Security Identity Manager プロトコルにより、QRadar はデータベースにログインして、データベースからのイベントについてポーリングすることができます。QRadar アカウントの作成は不要ですが、イベント・データを追跡して保護するために作成することをお勧めします。

注**:** IBM Security Identity Manager アプライアンスと QRadar の間の通信がファイアウォール・ルールによってブロックされていないことを確認してください。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「IBM **Security Identity Manager**」を選択します。
7. 「プロトコル構成」リストを使用して、「IBM **Security Identity Manager JDBC**」を選択します。
8. 以下の値を構成します。

表 *212. IBM Security Identity Manager JDBC* のパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は、以下の形式で定義する必要があります。 `ITIMDB@<hostname>` ここで、*<hostname>* は、IBM Security Identity Manager アプライアンスの IP アドレスまたはホスト名です。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
データベース・タイプ	「データベース・タイプ」リストで、イベント・ソースとして使用するデータベースを選択します。 オプションには、以下のデータベースがあります。 • DB2 - IBM Security Identity Manager アプライアンスで DB2 がデータベース・タイプの場合は、このオプションを選択します。DB2 は、デフォルトのデータベース・タイプです。 • **MSDE** - IBM Security Identity Manager アプライアンスで MSDE がデータベース・タイプの場合は、このオプションを選択します。 • **Oracle** - IBM Security Identity Manager アプライアンスで Oracle がデータベース・タイプの場合は、このオプションを選択します。

表 212. *IBM Security Identity Manager JDBC* のパラメーター (続き)

パラメーター	説明
データベース名	接続先データベースの名前を入力します。デフォルトのデータベース名は ITIMDB です。 テーブル名は、英数字で最大 255 文字までです。テーブル名には、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、およびピリオド (.) の各特殊文字を含めることができます。
IP またはホスト名	IBM Security Identity Manager アプライアンスの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。表示されるデフォルトは、選択した「データベース・タイプ」によって異なります。有効な範囲は 0 から 65536 です。DB2 のデフォルトはポート 50000 です。 JDBC 構成のポートは、データベースのリスナー・ポートに一致する必要があります。データベースには、QRadar との通信に使用可能な着信 TCP 接続が必要です。 すべてのオプションのデフォルト・ポート番号には、以下のものがあります。 • DB2 - 50000 • MSDE - 1433 • Oracle - 1521 データベース・タイプとして MSDE を使用する際にデータベース・インスタンスを定義する場合は、構成で「ポート」パラメーターをブランクのままにしておく必要があります。
ユーザー名	データベース・ユーザー名を入力します。ユーザー名は、英数字で最大 255 文字までです。ユーザー名には下線 (_) も使用できます。
パスワード	データベース・パスワードを入力します。 パスワードの最大長は 255 文字です。
パスワードの確認	データベースにアクセスするためのパスワードを確認します。
テーブル名	イベント・レコードを含むテーブルまたはビューの名前として、`ITIMUSER.AUDIT_EVENT` と入力します。このフィールドの値をデフォルトから変更した場合、IBM Security Identity Manager JDBC プロトコルがイベントを正しく収集できなくなります。 テーブル名は、英数字で最大 255 文字までです。テーブル名には、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、およびピリオド (.) の各特殊文字を含めることができます。

表 212. IBM Security Identity Manager JDBC のパラメーター (続き)

パラメーター	説明
選択リスト	テーブルまたはビューのすべてのフィールドを含めるには、* を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	タイム・スタンプによってテーブルへの照会から次の照会までの間に追加された新規イベントを識別するには、TIMESTAMP を入力します。 比較フィールドは、英数字で最大 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
開始日時	オプション。データベース・ポーリングの開始日時を構成します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (データベース・テーブルへの照会から次の照会までの間の時間) を秒単位で入力します。デフォルトのポーリング間隔は 30 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。指定子の H および M のない数値の場合は、秒単位のポーリングになります。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
認証ドメイン	「**MSDE**」を「データベース・タイプ」として選択した場合、「認証ドメイン」フィールドが表示されます。ドメイン資格情報でユーザーを検証するようにネットワークが構成されている場合、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。 認証ドメインには、英数字を含める必要があります。ドメインには、下線 (_)、en ダッシュ (-)、およびピリオド (.) の各特殊文字を含めることができます。

表 212. *IBM Security Identity Manager JDBC* のパラメーター (続き)

パラメーター	説明
データベース・インスタンス	「**MSDE**」を「データベース・タイプ」として選択した場合、「データベース・インスタンス」フィールドが表示されます。 1 つのサーバーに複数の SQL サーバー・インスタンスがある場合は、接続先のインスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスがブロックされる場合は、構成で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「**MSDE**」を「データベース・タイプ」として選択した場合、「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスが表示されます。デフォルトでは、このチェック・ボックスはクリアされています。 TCP/IP ポート接続の代替方式を使用する場合は、このチェック・ボックスを選択します。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
NTLMv2 の使用	「**MSDE**」を「データベース・タイプ」として選択した場合、「**NTLMv2** の使用」チェック・ボックスが表示されます。 NTLMv2 認証を必要とする SQL サーバーとの通信時に MSDE 接続で NTLMv2 プロトコルを使用するように強制する場合は、「**NTLMv2** の使用」チェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されています。 「**NTLMv2** の使用」チェック・ボックスを選択した場合でも、NTLMv2 認証を必要としない SQL サーバーへの MSDE 接続には影響しません。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

IBM Security Network IPS (GX)

IBM Security QRadar 用の IBM Security Network IPS (GX) DSM は、syslog プロトコルを使用して、IBM Security Network IPS アプライアンスから LEEF ベースのイベントを収集します。

以下の表は、IBM Security Network IPS (GX) DSM の仕様を示しています。

パラメーター	値
製造元	IBM
DSM	Security Network IPS (GX)
RPM ファイル名	DSM-IBMSecurityNetworkIPS-*QRadar バージョン-Build_number*.noarch.rpm
サポートされるバージョン	v4.6 以降 (UDP) v4.6.2 以降 (TCP)
プロトコル	syslog (LEEF)
QRadar で記録されるイベント	セキュリティー・アラート (IPS と SNORT を含む) 正常性アラート システム・アラート IPS イベント (セキュリティー・イベント、接続イベント、ユーザー定義イベント、および OpenSignature ポリシー・イベントを含む)
自動的に検出?	はい
ID を含む?	いいえ

IBM Security Network IPS (GX) アプライアンスを QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、IBM Security Network IPS (GX) RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
2. IBM Security Network IPS (GX) のインスタンスごとに IBM Security Network IPS (GX) アプライアンスを構成して、QRadar と通信できるようにします。
3. QRadar がログ・ソースを自動的に検出しない場合は、ネットワーク上の IBM Security Network IPS (GX) のインスタンスごとにログ・ソースを作成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に IBM Security Network IPS (GX) アプライアンスを構成する

QRadar を使用してイベントを収集するには、IBM Security Network IPS (GX) アプライアンスを構成して LEEF イベントの syslog 転送を有効にする必要があります。

始める前に

IBM Security Network IPS (GX) アプライアンスと QRadar との通信がファイアウォール・ルールによってブロックされていないことを確認してください。

手順

1. IPS ローカル管理インターフェースにログインします。
2. ナビゲーション・メニューで、「システム設定の管理 **(Manage System Settings)**」 > 「アプライアンス **(Appliance)**」 > 「**LEEF** ログ転送 **(LEEF Log Forwarding)**」を選択します。
3. 「ローカル・ログを使用可能にする **(Enable Local Log)**」チェック・ボックスを選択します。
4. 「最大ファイル・サイズ **(Maximum File Size)**」フィールドで、LEEF ログ・ファイルの最大ファイル・サイズを構成します。
5. 「リモート Syslog サーバー (Remote Syslog Servers)」ペインで「有効 **(Enable)**」チェック・ボックスを選択します。
6. 「**Syslog** サーバー **IP/**ホスト **(Syslog Server IP/Host)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
7. 「**TCP** ポート」フィールドで、LEEF ログ・イベントを転送するためのポート番号として `514` を入力します。

   注**:** v4.6.1 以前のバージョンを使用する場合は、「**UDP** ポート」フィールドを使用してください。
8. イベント・タイプのリストで、QRadar に転送されるイベント・タイプを有効にします。
9. TCP ポートを使用する場合は、以下の手順で **`crm.leef.fullavp`** 調整パラメーターを構成します。
   a. ナビゲーション・メニューで、「システム設定の管理 **(Manage System Settings)**」 > 「アプライアンス **(Appliance)**」 > 「調整パラメーター **(Tuning Parameters)**」を選択します。
   b. 「調整パラメーターの追加 **(Add Tuning Parameters)**」をクリックします。
   c. 「名前」フィールドに `crm.leef.fullavp` と入力します。
   d. 「値」フィールドに `true` と入力します。
   e. 「**OK**」をクリックします。

QRadar で IBM Security Network IPS (GX) のログ・ソースを構成する

QRadar は、IBM Security Network IPS (GX) アプライアンスの Syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ただし、QRadar 用のログ・ソースを手動で作成して Syslog イベントを受信することもできます。

このタスクについて

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで「**IBM Security Network IPS (GX)**」を選択します。
6. 「プロトコル構成」リストで「**Syslog**」を選択します。
7. 以下のパラメーターを構成します。

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名。IBM Security Network IPS (GX) アプライアンスから受信したイベントの ID として使用されます。
信頼性	送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにします。
受信イベント・ペイロード **(Incoming Event Payload)**	ログの解析と保管を行うための受信ペイロード・エンコーダー。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Security Network Protection (XGS)

IBM Security Network Protection (XGS) DSM は、ログ・イベント拡張フォーマット (LEEF) を使用してイベントを受け入れます。これにより、IBM Security QRadar がすべての関連イベントを記録できます。

以下の表は、IBM Security Network Protection (XGS) DSM の仕様を示しています。

表 *213. IBM Security Network Protection (XGS)* の仕様

仕様	値
製造元	IBM

表 213. IBM Security Network Protection (XGS) の仕様 (続き)

仕様	値
DSM	Security Network Protection (XGS)
RPM ファイル名	
サポートされるバージョン	v5.0 フィックスパック 7
プロトコル	syslog (LEEF)
QRadar で記録されるイベント	関連するすべてのシステム・イベント、アクセス・イベント、およびセキュリティー・イベント
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	IBM Network Security Protection (XGS) Web サイト (http://pic.dhe.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.alps.doc/tasks/alps_configuring_system_alerts.htm)

Network Security Protection (XGS) アプライアンスを QRadar で構成する前に、IBM Security Network Protection (XGS) のルールまたはポリシーがイベントを QRadar に転送するように、リモート syslog アラートを構成しておく必要があります。

IBM Security Network Protection (XGS) アラートの構成

LEEF 対応のリモート syslog アラート・オブジェクトを使用して、すべてのイベント・タイプが IBM Security QRadar に送信されます。

このタスクについて

リモート syslog アラート・オブジェクトは、イベントが生成された各コンテキストから作成、編集、および削除できます。Network Security Protection (XGS) ローカル管理インターフェースに管理者としてログインし、リモート syslog アラート・オブジェクトを構成して、以下のメニューのいずれかに移動します。

- 「管理」 > 「システムの設定」 > 「システム・アラート」 (システム・イベント)
- 「セキュア」 > 「ネットワーク・アクセス・ポリシー」 (アクセス・イベント)
- 「セキュア」 > 「**IPS** イベント・フィルター・ポリシー」 (セキュリティー・イベント)
- 「セキュア」 > 「**IPS** ポリシー」 (セキュリティー・イベント)
- 「セキュア」 > 「ネットワーク・アクセス・ポリシー」 > 「インスペクション」 > 「**IPS** ポリシー」

「IPS オブジェクト」の「ネットワーク・オブジェクト」ペインまたは「システム・アラート」ページで、以下の手順を実行します。

手順

1. 「新規」 > 「アラート」 > 「リモート **Syslog**」をクリックします。
2. 既存のリモート syslog アラート・オブジェクトを選択してから、「編集」をクリックします。

3. 以下のオプションを構成します。

表 *214. Syslog* 構成パラメーター

オプション	説明
名前	syslog アラート構成の名前を入力します。
リモート **Syslog** コレクター	QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
リモート **Syslog** コレクター・ポート	「リモート **Syslog** コレクター・ポート」には、514 と入力します。
リモート **LEEF** が有効 **(Remote LEEF Enabled)**	LEEF 形式のイベントを有効にする場合は、このチェック・ボックスを選択します。これは必須フィールドです。 このオプションが表示されない場合は、IBM Security Network Protection アプライアンスにソフトウェア・バージョン 5.0 およびフィックスパック 7 がインストールされていることを確認してください。
コメント	syslog 構成のコメントの入力はオプションです。

4. 「構成の保存 **(Save Configuration)**」をクリックします。

   アラートが「使用可能なオブジェクト」リストに追加されます。
5. IBM Security Network Protection (XGS) アプライアンスを更新するために、「適用」をクリックします。
6. QRadar 用の LEEF アラート・オブジェクトを以下の場所に追加します。
   - ポリシー内の 1 つ以上のルール
   - 「システム・アラート」ページの「追加されたオブジェクト」ペイン
7. 「適用」をクリックします。

   Network Security Protection (XGS) デバイスについて詳しくは、Network Security Protection (XGS) ローカル管理インターフェースのブラウザー・クライアント・ウィンドウの「ヘルプ」をクリックするか、オンラインの *Network Security Protection (XGS)* の資料 にアクセスしてください。

IBM Security QRadar でログ・ソースを構成する

QRadar は、IBM Security Network Protection (XGS) からの LEEF 対応 syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで「IBM **Security Network Protection (XGS)**」を選択します。
6. 「プロトコル構成」リストで「**Syslog**」を選択します。

7. 以下の値を構成します。

表 215. *Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	IBM Security Network Protection (XGS) からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Security Privileged Identity Manager

IBM Security QRadar DSM for IBM Security Privileged Identity Manager は、IBM Security Privileged Identity Manager デバイスからイベントを収集します。

以下の表は、IBM Security Privileged Identity Manager DSM の仕様を示しています。

表 216. *IBM Security Privileged Identity Manager DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM Security Privileged Identity Manager
RPM ファイル名	`DSM-IBMSecurityPrivilegedIdentityManager-`*`Qradar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	V2.0
プロトコル	JDBC
記録されるイベント・タイプ	監査 認証 システム
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	IBM Security Privileged Identity Manager Web サイト (http://www-03.ibm.com/software/products/en/pim/)

IBM Security Privileged Identity Manager からイベントを収集するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - JDBC プロトコル RPM
   - IBM Security Privileged Identity Manager DSM RPM

2. IBM Security Privileged Identity Manager Web ユーザー・インターフェースから情報を収集します。
3. QRadar コンソールで IBM Security Privileged Identity Manager ログ・ソースを追加します。以下の表は、IBM Security Privileged Identity Manager イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 217. *IBM Security Privileged Identity Manager* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	IBM Security Privileged Identity Manager
プロトコル構成	JDBC
ログ・ソース ID	*<DATABASE@HOSTNAME>*
データベース・タイプ	DB2
データベース名	IBM Security Privileged Identity Manager の「データベース名」フィールドの値に一致する必要があります。
IP またはホスト名	IBM Security Privileged Identity Manager の「ホスト名」フィールドの値に一致する必要があります。
ポート	IBM Security Privileged Identity Manager の「ポート」フィールドの値に一致する必要があります。
ユーザー名	IBM Security Privileged Identity Manager の「データベース管理者 **ID**」フィールドの値に一致する必要があります。
定義済み照会	なし
テーブル名	*DB2ADMIN*.V_PIM_AUDIT_EVENT *DB2ADMIN* は、IBM Security Privileged Identity Manager の「データベース管理者 ID」パラメーターに指定されている実際のデータベース・スキーマ名に置き換えてください。
選択リスト	*
比較フィールド	TIMESTAMP
準備済みステートメントの使用 (Use Prepared Statements)	このチェック・ボックスを選択します。
開始日時	JDBC 取得の初回日時。
ポーリング間隔 (Polling Interval)	10
EPS スロットル	20000

IBM Security Privileged Identity Manager の構成

IBM Security QRadar でログ・ソースを構成するには、IBM Security Privileged Identity Manager から一部の情報を記録する必要があります。

始める前に

QRadar と通信するには、IBM Security Privileged Identity Manager DB2 データベースで着信 TCP 接続を有効にしておく必要があります。

手順

1. IBM Security Privileged Identity Manager にログインします。
2. 「**Privileged Identity Manager** の構成 **(Configure Privileged Identity Manager)**」タブをクリックします。
3. 「外部エンティティーの管理」ペインで、「データベース・サーバーの構成」を選択します。
4. 「データベース・サーバーの構成」列の「**ID** データ・ストア」行をダブルクリックします。
5. 以下のパラメーターの値を記録します。
   - ホスト名
   - ポート
   - データベース名
   - データベース管理者 ID
6. 「データベース管理者 ID」パラメーターに指定したのと同じスキーマで、IBM Security Privileged Identity Manager DB2 データベースにビューを作成するには、以下の SQL ステートメントを実行します。

```
CREATE view V_PIM_AUDIT_EVENT
AS
SELECT
ae.ID, ae.itim_event_category as event_category, ae.ENTITY_NAME, service.NAME service_name,
ae.ENTITY_DN, ae.ENTITY_TYPE,
ae.ACTION, ae.INITIATOR_NAME, ae.INITIATOR_DN, ae.CONTAINER_NAME, ae.CONTAINER_DN,
ae.RESULT_SUMMARY, ae.TIMESTAMP,
lease.POOL_NAME, lease.LEASE_DN, lease.LEASE_EXPIRATION_TIME, lease.JUSTIFICATION,
ae.COMMENTS, ae.TIMESTAMP2, ae.WORKFLOW_PROCESS_ID
FROM AUDIT_EVENT ae
LEFT OUTER JOIN AUDIT_MGMT_LEASE lease ON (ae.id = lease.event_id)
LEFT OUTER JOIN SA_EVALUATION_CREDENTIAL cred ON (LOWER(ae.entity_dn) = LOWER(cred.DN))
LEFT OUTER JOIN V_SA_EVALUATION_SERVICE service ON (LOWER(cred.service_dn) = LOWER(service.dn));
```

次のタスク

5 ページの『ログ・ソースの追加』

IBM Security Trusteer Apex Advanced Malware Protection

IBM Security Trusteer® Trusteer Apex™ Advanced Malware Protection DSM は、Trusteer Apex Advanced Malware Protection システムからイベント・データを収集します。

IBM Security QRadar は、Trusteer Apex Advanced Malware Protection システムから次の項目を収集できます。

- Syslog イベント
- ログ・ファイル (システムのフラット・フィード・ファイルをホストする仲介サーバー経由)

以下の表は、IBM Security Trusteer Apex Advanced Malware Protection DSM の仕様を示しています。

表 218. *IBM Security Trusteer Apex Advanced Malware Protection DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM Security Trusteer Apex Advanced Malware Protection
RPM ファイル名	`DSM-TrusteerApex-`*`QRadar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	Syslog/LEEF イベントの収集: Apex Local Manager 2.0.45 LEEF: `ver_1303.1` フラット・ファイル・フィード: v1、v3、および v4
プロトコル	Syslog/TLS Syslog/LEEF ログ・ファイル
記録されるイベント・タイプ	マルウェア検出 エクスプロイト検出 データ引き出し検出 Java イベントのロックダウン ファイル検査イベント Apex 停止イベント Apex アンインストール・イベント ポリシー変更イベント ASLR 違反イベント ASLR 適用イベント パスワード保護イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	IBM Security Trusteer Apex Advanced Malware Protection Web サイト (http://www-03.ibm.com/software/products/en/trusteer-apex-adv-malware)

IBM Security Trusteer Apex Advanced Malware Protection イベント収集を構成するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - ログ・ファイル・プロトコル RPM
   - TLS Syslog プロトコル RPM
   - IBM Security Trusteer Apex Advanced Malware Protection DSM RPM
2. 次のオプションのいずれかを選択してください。
   - Syslog イベントを QRadar に送信するには、 568 ページの『QRadar に syslog イベントを送信するための IBM Security Trusteer Apex Advanced Malware Protection の構成』を参照してください。
   - 仲介サーバーを介して IBM Security Trusteer Apex Advanced Malware Protection からログ・ファイルを収集するには、 569 ページの『フラット・ファイル・フィード・サービスの構成』を参照してください。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで IBM Security Trusteer Apex Advanced Malware Protection ログ・ソースを追加してください。

   以下の表は、IBM Security Trusteer Apex Advanced Malware Protection syslog イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *219. syslog* 用の *IBM Security Trusteer Apex Advanced Malware Protection* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	IBM Security Trusteer Apex Advanced Malware Protection
プロトコル構成	**Syslog**
ログ・ソース **ID**	Syslog ヘッダーに格納されている IP アドレスまたはホスト名。syslog ヘッダーに IP アドレスまたはホスト名が含まれない場合は、パケット IP アドレスを使用します。

   以下の表は、IBM Security Trusteer Apex Advanced Malware Protection TLS syslog イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *220. TLS syslog* 用の *IBM Security Trusteer Apex Advanced Malware Protection* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	IBM Security Trusteer Apex Advanced Malware Protection
プロトコル構成	**TLS Syslog**
ログ・ソース **ID**	syslog ヘッダー内の IP アドレスまたはホスト名。syslog ヘッダーに IP アドレスまたはホスト名が含まれない場合は、パケット IP アドレスを使用します。

重要**:** TLS Syslog を使用し、かつ FQDN を使用してシステムにアクセスするときは、リスナーに対して独自の証明書を生成し、それを TLS Syslog 構成で指定する必要があります。

以下の表は、IBM Security Trusteer Apex Advanced Malware Protection ログ・ファイルの収集用に固有の値を必要とするパラメーターを示しています。

表 *221.* ログ・ファイル・プロトコル用の *IBM Security Trusteer Apex Advanced Malware Protection* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	IBM Security Trusteer Apex Advanced Malware Protection
プロトコル構成	ログ・ファイル
ログ・ソース **ID**	フラット・フィード・ファイルをホストするサーバーの IP アドレスまたはホスト名。
サービス・タイプ	**SFTP**
リモート **IP** またはホスト名	フラット・フィード・ファイルをホストするサーバーの IP アドレスまたはホスト名。
リモート・ポート	22
リモート・ユーザー	フラット・フィード・ファイルをホストするサーバー上で QRadar 用に作成したユーザー名。
SSH 鍵ファイル	パスワードを使用する場合は、このフィールドをブランクにすることができます。
リモート・ディレクトリー	フラット・フィード・ファイルを保存するログ・ファイル・ディレクトリー。
再帰的 **(Recursive)**	このオプションを選択しないでください。
FTP ファイル・パターン	"trusteer_feeds_.*?_[0-9]{8}_[0-9]*?¥.csv"
開始時刻	ログ・ファイル・プロトコルにログ・ファイル収集を開始させる時刻。
繰り返し **(Recurrence)**	ログ・ファイル取得のポーリング間隔。
保存時に実行	有効にする必要があります。
プロセッサー	なし
以前に処理したファイルを無視 **(Ignore Previously Processed Files)**	有効にする必要があります。
イベント・ジェネレーター **(Event Generator)**	**LINEBYLINE**
ファイルのエンコード **(File Encoding)**	**UTF-8**

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

568 ページの『QRadar に syslog イベントを送信するための IBM Security Trusteer Apex Advanced Malware Protection の構成』
IBM Security QRadar に syslog イベントを送信するように IBM Security

Trusteer Apex Advanced Malware Protection を構成します。

569 ページの『フラット・ファイル・フィード・サービスの構成』
IBM Security QRadar で IBM Security TrusteerApex Advanced Malware Protection からログ・ファイルを取得するには、SFTP が有効な仲介サーバー上でフラット・ファイル・フィード・サービスをセットアップする必要があります。このサービスによって、IBM Security TrusteerApex Advanced Malware Protection から受け取るフラット・ファイルをホストする仲介サーバーが使用可能になり、外部デバイスから接続できるようになるため、QRadar はログ・ファイルを取得できます。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar に syslog イベントを送信するための IBM Security Trusteer Apex Advanced Malware Protection の構成

IBM Security QRadar に syslog イベントを送信するように IBM Security Trusteer Apex Advanced Malware Protection を構成します。

始める前に

ご使用の Trusteer Management Application™ (TMA) に Apex Local Manager をインストールします。

QRadar との通信用に IBM Security Trusteer Apex Advanced Malware Protection を構成する方法について詳しくは、IBM Knowledge Center にある以下の資料を参照してください。

- *IBM Security Trusteer Apex Advanced Malware Protection Local Manager - Hybrid Solution Reference Guide*
- *IBM Security Trusteer Apex Advanced Malware Protection Feeds Reference Guide*

SSL/TLS 認証はサポートされていません。

手順

1. Trusteer Management Application (TMA) にログインします。
2. 「**Apex Local Manager**」&「**SIEM** 設定 **(SIEM Settings)**」を選択します。
3. オプション: Apex Local Manager ウィザードが自動的に表示されない場合は、「追加」をクリックします。
4. Apex Local Manager の名前を入力します。
5. 「有効」ボックスにチェック・マークを付けて「次へ」をクリックします。
6. QRadar のサーバー設定を入力し、「次へ」をクリックします。
7. オプション: Apex Local Manager システム・イベント用に別個の syslog サーバーを使用する場合は、その設定を入力します。
8. 「終了」をクリックします。

フラット・ファイル・フィード・サービスの構成

IBM Security QRadar で IBM Security TrusteerApex Advanced Malware Protection からログ・ファイルを取得するには、SFTP が有効な仲介サーバー上でフラット・ファイル・フィード・サービスをセットアップする必要があります。このサービスによって、IBM Security TrusteerApex Advanced Malware Protection から受け取るフラット・ファイルをホストする仲介サーバーが使用可能になり、外部デバイスから接続できるようになるため、QRadar はログ・ファイルを取得できます。

仲介サーバーにフラット・ファイル・フィードを送信するように IBM Security TrusteerApex Advanced Malware Protection を構成するには、IBM Trusteer サポートに連絡してください。

このタスクについて

フラット・ファイル・フィードでは CSV 形式を使用します。各フィード項目はファイルの個別の行に書き込まれ、各行には複数のコンマ区切りフィールドが含まれます。各フィールドにはフィード項目を説明するデータが含まれます。各フィード行の最初のフィールドには、フィード・タイプが含まれます。

手順

1. SFTP が有効なサーバーを使用可能にし、外部デバイスから接続できることを確認します。
2. SFTP が有効なサーバーにログオンします。
3. サーバー上で IBM Security Trusteer Apex Advanced Malware Protection のユーザー・アカウントを作成します。
4. QRadar のユーザー・アカウントを作成します。
5. オプション: SSH 鍵ベースの認証を有効にします。

次のタスク

仲介サーバーをセットアップしたら、以下の詳細情報を記録します。

- ターゲット SFTP サーバー名および IP アドレス
- SFTP サーバー・ポート (標準ポートは 22)
- ターゲット・ディレクトリーのファイル・パス
- SFTP ユーザー名 (SSH 認証が構成されていない場合)
- アップロード頻度 (1 分から 24 時間)
- RSA 形式の SSH 公開鍵

IBM Trusteer サポートは、フラット・フィード・ファイルを送信するように IBM Security TrusteerApex Advanced Malware Protection を構成するときに、仲介サーバーの詳細情報を使用します。

IBM Security Trusteer Apex Local Event Aggregator

IBM Security QRadar は、Trusteer Apex Local Event Aggregator からマルウェア、エクスプロイト、およびデータ引き出し検出のイベントを収集して分類することができます。

syslog イベントを収集するには、syslog イベントを QRadar に転送するように Trusteer Apex Local Event Aggregator を構成する必要があります。管理者は、Apex L.E.A. の管理コンソール・インターフェースを使用してイベントの syslog ターゲットを構成することができます。QRadar は、Trusteer Apex Local Event Aggregator アプライアンスから転送された syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。QRadar は、Trusteer Apex Local Event Aggregator V1304.x 以降からの syslog イベントをサポートしています。

イベントを QRadar と統合するには、管理者が以下の作業を実行します。

1. Trusteer Apex Local Event Aggregator アプライアンスで syslog サーバーを構成します。
2. QRadar システムで、転送されたイベントが自動的に検出されることを確認します。

Trusteer Apex Local Event Aggregator 用の syslog の構成

イベントを収集するには、syslog イベントを転送するように Trusteer Apex Local Event Aggregator で syslog サーバーを構成する必要があります。

手順

1. Trusteer Apex L.E.A. 管理コンソールにログインします。
2. ナビゲーション・メニューから「構成」を選択します。
3. 現在の Trusteer Apex Local Event Aggregator の構成をエクスポートするために、「エクスポート」をクリックして、ファイルを保存します。
4. 構成ファイルをテキスト・エディターで開きます。
5. `syslog.event_targets` セクションで、以下の情報を追加します。

   ```
   {

   host": "<QRadar IP address>", "port": "514", "proto": "tcp"

   }
   ```
6. 構成ファイルを保存します。
7. ナビゲーション・メニューから「構成」を選択します。
8. 「ファイルの選択 **(Choose file)**」をクリックして、イベント・ターゲットの IP アドレスが含まれる新規構成ファイルを選択します。
9. 「インポート」をクリックします。

   Trusteer Apex Local Event Aggregator で syslog イベントが生成されると、構成ファイルで指定したターゲットに転送されます。十分な数のイベントが QRadar に転送された後、ログ・ソースが自動的に検出されます。通常、ログ・ソースの自動検出に必要なイベントの最小数は 25 です。

次のタスク

管理者は QRadar コンソールにログインして、ログ・ソースが作成されていることを確認できます。「ログ・アクティビティー」タブには、Trusteer Apex Local Event Aggregator からのイベントが表示されます。

IBM Sense

IBM Sense 用の IBM Security QRadar DSM は、Sense イベントを生成するローカル・システムまたは外部システムから、顕著なイベントを収集します。

以下の表は、IBM Sense DSM の仕様を示しています。

表 *222. IBM Sense DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM Sense
RPM ファイル名	DSM-IBMSense-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	1
プロトコル	Syslog
イベント・フォーマット	LEEF
記録されるイベント・タイプ	ユーザーの振る舞い ユーザーの地域 ユーザー時間 ユーザー・アクセス ユーザー特権 ユーザー・リスク Sense オフェンス リソースのリスク
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	IBM Web サイト (http://www.ibm.com)

IBM Sense を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - IBM Sense DSM RPM
   - DSMCommon RPM

IBM Sense のサンプル・イベント・メッセージを次の表に示します。

表 223. *IBM Sense* のサンプル・メッセージ。

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
振る舞いの変更	ユーザーの振る舞い	LEEF:2.0|IBM|Sense|1.0|Behavior Change|cat=User Behavior description= score= scoreType= confidence= primaryEntity= primaryEntityType= additionalEntity= additionalEntityType= beginningTimestamp= endTimestamp= sensorDomain= referenceId1= referenceId2= referenceId3= referenceId4= referenceURL= originalSenseEventName=

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

QRadar との通信のための IBM Sense の構成

User Behavior Analytics (UBA) アプリケーションは、IBM Sense DSM を使用して、ユーザーのリスク・スコアとオフェンスを QRadar に追加します。アプリケーションをインストールすると、アプリケーションによって、IBM Sense ログ・ソースが自動的に作成および構成されます。ユーザーによる入力や構成は不要です。

IBM SmartCloud Orchestrator

IBM SmartCloud Orchestrator 用の IBM Security QRadar DSM は、IBM SmartCloud Orchestrator システムから監査ログを収集します。

以下の表は、IBM SmartCloud Orchestrator DSM の仕様を示しています。

表 224. *IBM SmartCloud Orchestrator* の仕様

仕様	値
製造元	IBM
DSM 名	IBM SmartCloud Orchestrator
RPM ファイル名	DSM-IBMSmartCloudOrchestrator-*Qradar_version_build number*.noarch.rpm
サポートされるバージョン	V2.3 FP1 以降
プロトコル・タイプ	IBM SmartCloud Orchestrator REST API
QRadar で記録されるイベント・タイプ	監査レコード
QRadar UI でのログ・ソース・タイプ	IBM SmartCloud Orchestrator
自動的に検出?	いいえ
ID を含む?	はい
カスタム・プロパティーを含む	いいえ

表 224. *IBM SmartCloud Orchestrator* の仕様 (続き)

仕様	値
その他の情報	http://ibm.com

IBM SmartCloud Orchestrator を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - IBM SmartCloud Orchestrator RPM
   - IBM SmartCloud Orchestrator RESTAPI プロトコル RPM
2. QRadar コンソール上で IBM SmartCloud Orchestrator のログ・ソースを作成します。IBM SmartCloud 固有のパラメーターには、以下の値を使用します。

パラメーター	説明
ログ・ソース・タイプ	IBM SmartCloud Orchestrator
プロトコル構成	IBM SmartCloud Orchestrator REST API
IP またはホスト名	IBM SmartCloud Orchestrator の IP アドレスまたはサーバー名

IBM SmartCloud Orchestrator システムでは、アクションは不要です。ログ・ソースを作成した後、QRadar は、IBM SmartCloud Orchestrator からログを収集し始めます。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

IBM SmartCloud Orchestrator のインストール

IBM SmartCloud Orchestrator を IBM Security QRadar に統合します。

手順

1. 最新の DSMCommon RPM をQRadar コンソールにダウンロードしてインストールします。DSM 更新をインストールするように自動更新が構成されている場合、このステップは不要です。
2. 最新の IBM SmartCloud Orchestrator RESTAPI プロトコル RPM を QRadar コンソールにダウンロードしてインストールします。
3. 最新の IBM SmartCloud Orchestrator RPM を QRadar コンソールにダウンロードしてインストールします。DSM 更新をインストールするように自動更新が構成されている場合、このステップは不要です。

QRadar で IBM SmartCloud Orchestrator のログ・ソースを構成する

IBM SmartCloud Orchestrator を IBM Security QRadar に統合できるようにするには、ログ・ソースを追加します。

手順

1. QRadar にログインします。
2. 「管理」タブを選択します。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックし、「追加」をクリックします。
5. 「ログ・ソース・タイプ」リストで「**IBM SmartCloud Orchestrator**」を選択します。
6. 「プロトコル構成」リストで「**IBM SmartCloud Orchestrator REST API**」を選択します。
7. 以下のパラメーターを構成します。

オプション	説明
IP またはホスト名	IBM SmartCloud Orchestrator の IP アドレスまたはサーバー名
ユーザー名	IBM SmartCloud Orchestrator コンソール・ユーザーのユーザー名。
パスワード	IBM SmartCloud Orchestrator コンソール・ユーザーのパスワード。
パスワードの確認	パスワードが正しく入力されたことを確認します。
EPS スロットル	このログ・ソースの 1 秒あたりの最大イベント数 (デフォルトは 5000)。
繰り返し **(Recurrence)**	ログ・ソースがデータの取得を試行する頻度。分単位、時間単位、日単位で指定できます (デフォルトは 5 分)。

IBM Tivoli Access Manager for e-business

IBM Security QRadar 用の IBM Tivoli Access Manager for e-business DSM は、IBM Tivoli Access Manager から転送されたアクセス、監査、および HTTP の各イベントを受け入れます。

QRadar は、syslog を使用して、IBM Tivoli Access Manager for e-business から監査、アクセス、および HTTP の各イベントを収集します。QRadar を構成するには、イベントを syslog 宛先に転送するように Tivoli Access Manager for e-business を構成しておく必要があります。

Tivoli Access Manager for e-business の構成

Tivoli Access Manager for e-business でイベントを転送するように syslog を構成できます。

手順

1. Tivoli Access Manager の IBM Security Web Gateway にログインします。
2. ナビゲーション・メニューで「セキュア・リバース・プロキシー設定 **(Secure Reverse Proxy Settings)**」 > 「管理」 > 「リバース・プロキシー **(Reverse Proxy)**」を選択します。

   「リバース・プロキシー (Reverse Proxy)」ペインが表示されます。
3. 「インスタンス」列でインスタンスを選択します。
4. 「管理」リストをクリックし、「構成」 > 「拡張」を選択します。

   WebSEAL 構成ファイルのテキストが表示されます。
5. 許可 API のロギング構成を見つけます。

   リモート syslog 構成は、`logcfg` で開始します。

   例えば、許可イベントをリモート syslog サーバーに送信するには、以下のようにします。

   ```
   # logcfg = audit.azn:rsyslog server=<IP address>,port=514,log_id=<log name>
   ```
6. リモート syslog 構成 (`logcfg`) を新しい行にコピーします。ただし、コメント・マーカー (`#`) は削除します。
7. リモート syslog 構成を編集します。

   例:

   ```
   logcfg = audit.azn:rsyslog server=<IP address>,port=514,log_id=<log name> logcfg = audit.authn:rsyslog server=<IP address>,port=514,log_id=<log name> logcfg = http:rsyslog server=<IP address>,port=514,log_id=<log name>
   ```

   各部分について以下で説明します。

   - *<IP address>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
   - *<Log name>* は、QRadar に転送されるログに割り当てる名前です。例: `log_id=WebSEAL-log`
8. 「送信 **(Submit)**」をクリックします。

   ナビゲーション・メニューに「適用 **(Deploy)**」ボタンが表示されます。
9. ナビゲーション・メニューの「適用 **(Deploy)**」をクリックします。
10. 「適用 **(Deploy)**」をクリックします。

    続行するには、リバース・プロキシー・インスタンスを再始動する必要があります。
11. 「インスタンス」列でインスタンス構成を選択します。
12. 「管理」リストをクリックし、「コントロール」 > 「再始動」を選択します。

再始動が完了すると、状況メッセージが表示されます。syslog の宛先の構成について詳しくは、*IBM Tivoli Access Manager for e-business* のベンダー資料を参照してください。これで、ログ・ソースを QRadar で構成することができます。

ログ・ソースの構成

QRadar Risk Manager は syslog の監査イベントとアクセス・イベントを自動的に検出しますが、IBM Tivoli Access Manager for e-business から転送された HTTP イベントを自動的に検出することはありません。

このタスクについて

QRadar が監査イベントおよびアクセス・イベントを自動的に検出するため、ログ・ソースを作成する必要はありません。ただし、QRadar が IBM Tivoli Access Manager for e-business の syslog イベントを受信するために手動でログ・ソースを作成することもできます。以下のログ・ソースを作成する構成ステップはオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「IBM Tivoli **Access Manager for e-business**」を選択します。
8. 「プロトコル構成」リストで「**Syslog**」を選択します。
9. 以下の値を構成します。

表 *225. IBM Tivloi Access Manager for e-business の syslog の構成*

パラメーター	説明
ログ・ソース **ID**	IBM Tivoli Access Manager for e-business アプライアンスの IP アドレスまたはホスト名を入力します。 IP アドレスまたはホスト名により、QRadar での固有のイベント・ソースとして IBM Tivoli Access Manager for e-business が識別されます。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Tivoli Endpoint Manager

IBM Tivoli® Endpoint Manager は、現在は IBM BigFix と呼ばれています。

関連概念:

473 ページの『IBM BigFix』
IBM Security QRadar 用の IBM BigFix DSM は、IBM BigFix から取得するシステム・イベントをログ・イベント拡張フォーマット (LEEF) で受け入れます。

IBM WebSphere Application Server

IBM Security QRadar 用の IBM WebSphere® Application Server DSM は、ログ・ファイル・プロトコル・ソースを使用してイベントを受け入れます。

QRadar は、WebSphere Application Server ログ・ファイルからの関連するすべてのアプリケーション・イベントおよびセキュリティー・イベントを記録します。

IBM WebSphere の構成

IBM Security QRadar 用に IBM WebSphere Application Server のイベントを構成できます。

手順

1. Web ブラウザーを使用して、IBM WebSphere 管理コンソールにログインします。
2. 「環境」 > 「**WebSphere** 変数」をクリックします。
3. 変数の有効範囲レベルとして「セル」を定義します。
4. 「新規」をクリックします。
5. 以下の値を構成します。
   - 名前 - セル変数の名前を入力します。
   - 説明 - 変数の説明を入力します (オプション)。
   - 値 - ログ・ファイルのディレクトリー・パスを入力します。

   例:

   ```
   {QRADAR_LOG_ROOT} = /opt/IBM/WebSphere/AppServer/profiles/Custom01/logs/
   QRadar
   ```

   続行する前に、『IBM WebSphere の構成』で指定したターゲット・ディレクトリーを作成する必要があります。
6. 「**OK**」をクリックします。
7. 「保存」をクリックします。
8. 構成変更を保存するために、WebSphere Application Server を再始動する必要があります。

   注**:** 作成した変数がセルに影響する場合は、続行する前に、セル内のすべての WebSphere Application Server を再始動する必要があります。

次のタスク

これで、IBM WebSphere Application Server DSM 用にロギング・オプションをカスタマイズする準備ができました。

ロギング・オプションのカスタマイズ

WebSphere が使用する各アプリケーション・サーバー用にロギング・オプションをカスタマイズし、JVM ログ (Java 仮想マシン・ログ) の設定を変更する必要があります。

手順

1. 「サーバー」 > 「アプリケーション・サーバー」を選択します。
2. WebSphere Application Server を選択し、サーバー・プロパティーをロードします。
3. 「ロギングおよびトレース」 > 「**JVM** ログ」を選択します。
4. JVM ログ・ファイルの名前を構成します。

   例:

   System.Out ログ・ファイル名:

   ```
   ${QRADAR_LOG_ROOT}/${WAS_SERVER_NAME}-SystemOut.log
   ```

   System.Err ログ・ファイル名:

   ```
   ${QRADAR_LOG_ROOT}/${WAS_SERVER_NAME}-SystemErr.log
   ```
5. ログ・ファイルをターゲット・ディレクトリーに保存する時刻を選択します。
6. 「**OK**」をクリックします。
7. 構成変更を保存するために、WebSphere Application Server を再始動する必要があります。

   注**:** JVM ログの変更がセルに影響する場合は、続行する前に、セル内のすべての WebSphere Application Server を再始動する必要があります。

   これで、ログ・ファイル・プロトコルを使用してファイルを IBM Security QRadar にインポートする準備ができました。

ログ・ソースの作成

ログ・ファイル・プロトコルにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。IBM WebSphere Application Server DSM は、ログ・ファイル・プロトコルのソースを使用して、ログ・ファイルの一括ロードをサポートします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「IBM WebSphere **Application Server**」を選択します。

8. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
9. 以下の値を構成します。

表 226. ログ・ファイル・パラメーター

パラメーター	説明
ログ・ソース **ID**	QRadar で IBM WebSphere Application Server をイベント・ソースとして識別するための IP アドレス、ホスト名、または名前を入力します。QRadar が固有のイベント・ソースのログ・ファイルを識別できる、IP アドレスまたはホスト名の入力が推奨されます。 例えば、ネットワークに、ログをファイル・リポジトリーに提供する IBM WebSphere Application Server が複数含まれている場合は、イベント・ログを作成したイベントの IP アドレスまたはホスト名を指定します。これにより、ファイル・リポジトリーを識別する代わりに、ネットワーク内のデバイス・レベルでイベントを識別できるようになります。
サービス・タイプ	リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを、リストから選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管する IBM WebSphere Application Server の IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 オプションには、以下の FTP ポートがあります。 • **FTP** - TCP ポート 21 • **SFTP** - TCP ポート 22 • **SCP** - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。

表 226. ログ・ファイル・パラメーター (続き)

パラメーター	説明
SSH 鍵ファイル	「サービス・タイプ」として「**SCP**」または「**SFTP**」を選択した場合、このパラメーターにより、SSH 秘密鍵ファイルを定義できます。 SSH 鍵ファイルを指定した場合、「リモート・パスワード」フィールドは無視されます。
リモート・ディレクトリー	577 ページの『IBM WebSphere の構成』で指定したセルおよびファイル・パスの、リモート・ホスト上のディレクトリーの場所を入力します。これは、IBM WebSphere Application Server イベント・ファイルが含まれる、作成したディレクトリーです。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。これは、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートするためです。
再帰的 **(Recursive)**	ファイル・パターンでサブフォルダーを検索する場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 **SCP** をサービス・タイプとして構成する場合は、「再帰的 **(Recursive)**」オプションは無視されます。
FTP ファイル・パターン	「サービス・タイプ」として「**SFTP**」または「**FTP**」を選択した場合、このオプションにより、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするための正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 指定する FTP ファイル・パターンは、 578 ページの『ロギング・オプションのカスタマイズ』で JVM ログに割り当てた名前に一致する必要があります。例えば、システム・ログを収集するには、以下のコードを入力します。 `System.*¥.log` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。

表 226. ログ・ファイル・パラメーター (続き)

パラメーター	説明
FTP 転送モード	このオプションは、「サービス・タイプ」として「**FTP**」を選択した場合にのみ表示されます。「**FTP** 転送モード」パラメーターにより、FTP を介してログ・ファイルを取得する際のファイル転送モードを定義できます。 リストから、このログ・ソースに適用する転送モードを選択します。 • バイナリー - バイナリー・データ・ファイル、または圧縮された zip、gzip、tar、tar + gzip のアーカイブ・ファイルを必要とするログ・ソースには、「バイナリー」を選択します。 • **ASCII** - ASCII FTP ファイル転送を必要とするログ・ソースには、**ASCII** を選択します。 「**FTP** 転送モード」として「ASCII」を使用する場合、「プロセッサー」パラメーターには「なし」を選択し、「イベント・ジェネレーター **(Event Generator)**」パラメーターには「**1** 行ずつ **(LineByLine)**」を選択する必要があります。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。
開始時刻	処理を開始する時刻を入力します。このパラメーターと「繰り返し **(Recurrence)**」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。例えば、ディレクトリーを 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。 ログ・ファイル・プロトコルのスケジュール時に、スケジュールされている WebSphere Application Server ログ・ファイルの書き込み間隔よりも短い、ログ・ファイル・プロトコルの繰り返し時間を選択します。これにより、新しいログ・ファイルが古いイベント・ログを上書きしてしまう前に、WebSphere イベントがログ・ファイル・プロトコルによって確実に収集されるようになります。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 **「保存時に実行」**が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 **「保存時に実行」**を選択すると、「以前に処理したファイルを無視 (Ignore Previously Processed File)」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。

表 226. ログ・ファイル・パラメーター (続き)

パラメーター	説明
プロセッサー	リモート・ホストにあるファイルが zip、gzip、tar、または tar+gzip のアーカイブ・フォーマットで保管されている場合、アーカイブを解凍して内容を処理することができるプロセッサーを選択します。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	処理済みのファイルを追跡する場合は、このチェック・ボックスを選択します。以前に処理されたファイルは、再度処理されません。 このチェック・ボックスは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。このチェック・ボックスはクリアしたままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これによりファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで「WebSphere **Application Server**」を選択します。 イベント・ジェネレーターは、IBM WebSphere Application Server イベントの取得されたイベント・ファイルに固有の追加処理を適用します。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。IBM WebServer Application Server について詳しくは、ベンダーの資料を参照してください。

IBM WebSphere DataPower

IBM WebSphere DataPower は、今は IBM Datapower と呼ばれています。

関連概念:

495 ページの『IBM DataPower』

IBM Security QRadar DSM は、IBM DataPower システムからイベント・ログを収集します。

IBM z/OS

ログ・ファイル・プロトコルにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。

このタスクについて

ログ・ファイルは、一度に 1 つずつ、処理のために QRadar に転送されます。ログ・ファイル・プロトコルは、プレーン・テキストのイベント・ログや圧縮ファイル、アーカイブを管理できます。アーカイブには、一度に 1 行ずつ処理できるプレ

ーン・テキスト・ファイルが含まれている必要があります。複数行イベント・ログは、ログ・ファイル・プロトコルではサポートされていません。 zSecure が含まれた IBM z/OS は、指定されたディレクトリーにログ・ファイルを gzip アーカイブとして書き込みます。QRadar は、アーカイブを取り出し、ファイルに 1 行当たり 1 イベントで書き込まれているイベントを処理します。

これらのイベントを取得するには、ログ・ファイル・プロトコルを使用してログ・ソースを作成する必要があります。QRadar は、LEEF 形式のイベント・ファイルをホストするシステムにログインするための資格情報と、ポーリング間隔を要求します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「IBM **z/OS**」を選択します。
8. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
9. 以下の値を構成します。

表 *227. z/OS* ログ・ファイル・パラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。 QRadar がログ・ファイルを固有のイベント・ソースに識別できるようになるので、IP アドレスまたはホスト名の使用が推奨されます。 ネットワークに複数のデバイス (例えば、複数の z/OS イメージ)、またはすべてのイベント・ログが入っているファイル・リポジトリーが含まれている場合、IBM z/OS ログ・ソースのイベントを一意に識別する、イメージまたは場所の名前、IP アドレス、またはホスト名を指定します。これにより、ユーザーが識別可能なネットワークのイメージ・レベルまたは場所のレベルで、イベントを識別できるようになります。

表 227. *z/OS* ログ・ファイル・パラメーター (続き)

パラメーター	説明
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。 オプションには、以下のポートがあります。 • **FTP** - TCP ポート 21 • **SFTP** - TCP ポート 22 • **SCP** - TCP ポート 22 イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名またはユーザー ID を入力します。 • ログ・ファイルが IBM z/OS イメージ上にある場合は、IBM z/OS にログインするために必要なユーザー ID を入力します。ユーザー ID の長さは 8 文字まで可能です。 • ログ・ファイルがファイル・リポジトリー上にある場合は、ファイル・リポジトリーにログインするために必要なユーザー名を入力します。ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワードを入力します。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。
SSH 鍵ファイル	「サービス・タイプ」として「**SCP**」または「**SFTP**」を選択した場合、このパラメーターにより、SSH 秘密鍵ファイルを定義できます。SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。

表 227. z/OS ログ・ファイル・パラメーター (続き)

パラメーター	説明
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 **SCP** をサービス・タイプとして構成する場合は、「再帰的 **(Recursive)**」オプションは無視されます。
FTP ファイル・パターン	「サービス・タイプ」として「**SFTP**」または「**FTP**」を選択することで、「リモート・ディレクトリー」で指定したファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成するオプションが有効になります。一致するすべてのファイルは処理に組み込まれます。 IBM Security zSecure Audit を使用する IBM z/OS メインフレームは、`z0S.<timestamp>.gz` というパターンを使用してイベント・ファイルを書き込みます。 指定する FTP ファイル・パターンは、イベント・ファイルに割り当てた名前に一致する必要があります。例えば、先頭が zOS で末尾が `.gz` のファイルを収集するには、以下のコードを入力します。 `z0S.*¥.gz` このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、FTP をサービス・タイプとして選択した場合にのみ表示されます。リストから「バイナリー **(Binary)**」を選択します。 バイナリー転送モードは、`zip`、`gzip`、`tar`、`tar+gzip` アーカイブ・ファイルなど、バイナリー (圧縮) フォーマットで保管されたイベント・ファイルに対して使用します。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。

表 227. *z/OS* ログ・ファイル・パラメーター (続き)

パラメーター	説明
開始時刻	処理を開始する時刻を入力します。例えば、午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、00:00 と入力します。 このパラメーターと「繰り返し **(Recurrence)**」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、リモート・ディレクトリーを開始時刻から 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「**gzip**」を選択します。 プロセッサーにより、イベント・ファイル・アーカイブを解凍し、内容をイベント用に処理できます。ファイルは、QRadar にダウンロードされた後にのみ処理されます。QRadar は、zip、gzip、tar、または tar+gzip の各アーカイブ・フォーマットのファイルを処理できます。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	ログ・ファイル・プロトコルによって処理済みのファイルを追跡および無視するには、このチェック・ボックスを選択します。 QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが以前に処理されたかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。まだ処理されていないすべてのファイルがダウンロードされます。 このオプションは FTP および SFTP のサービス・タイプにのみ適用されます。

表 227. z/OS ログ・ファイル・パラメーター (続き)

パラメーター	説明
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスは、クリアしたままにすることをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これにより、ファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LineByLine)**」を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに複数の処理を適用します。ファイルの各行が、単一イベントです。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

IBM zSecure を使用する IBM z/OS の構成は完了です。IBM z/OS for zSecure でカスタム・イベント・プロパティーが必要な場合は、テクニカル・ノート「*IBM Security QRadar Custom Event Properties for IBM z/OS*」を参照してください。

IBM z/Secure® Audit

IBM Security QRadar 用の IBM z/OS® DSM により、IBM Security zSecure を使用して IBM z/OS メインフレームと統合し、セキュリティー、許可、および監査の各イベントを収集することができます。

zSecure プロセスを使用すると、System Management Facilities (SMF) からのイベントは、ログ・イベント拡張フォーマット (LEEF) のイベント・ファイルに記録されます。QRadar は、ログ・ファイル・プロトコルを使用して LEEF イベント・ログ・ファイルを取得し、イベントを処理します。ポーリング間隔に基づいてイベントを取得するように QRadar をスケジュールできます。これにより、QRadar は定義されたスケジュールに基づいてイベントを取得できます。

IBM Security zSecure Audit からの IBM z/OS イベントを QRadar と統合するには、以下のようにします。

1. インストール済み環境が、前提条件となるインストール要件をすべて満たしていることを確認します。
2. IBM z/OS イメージを構成します。詳しくは、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。

3. IBM z/OS が LEEF 形式のイベント・ログを取得するために、QRadar でログ・ソースを作成します。詳しくは、 582 ページの『IBM z/OS』を参照してください。
4. オプション。QRadar で、IBM z/OS 用のカスタム・イベント・プロパティーを作成します。詳しくは、テクニカル・ノート「*IBM Security QRadar Custom Event Properties for IBM z/OS*」を参照してください。

始める前に

データ収集プロセスを構成する前に、基本の zSecure インストール・プロセスを完了する必要があります。

以下の前提条件は必須です。

- z/OS イメージ上の IBM Security zSecure Audit で parmlib メンバーの IFAPRDxx が有効になっていることを確認する必要があります。
- SCKRLOAD ライブラリーは APF が許可されていなければなりません。
- CKFREEZE と UNLOAD のデータ・セットが定期的に更新されるようにプロセスを構成する必要があります。
- LEEF イベント・ファイルをダウンロードするには、QRadar に対して z/OS イメージ上の SFTP、FTP、または SCP の各サーバーを構成する必要があります。
- QRadar と z/OS イメージの間にあるファイアウォールで SFTP トラフィック、FTP トラフィック、または SCP トラフィックを許可する必要があります。

ソフトウェアをインストールした後に、ポストインストール・アクティビティーを実行して、構成を作成および変更します。 zSecure のインストールおよび構成の手順については、「*IBM Security zSecure Suite: CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。

IBM zSecure Alert

IBM Security QRadar 用の IBM zSecure Alert DSM は、syslog を使用してアラート・イベントを受け入れます。これにより、QRadar は、アラート・イベントをリアルタイムで受信できるようになります。

このタスクについて

IBM zSecure Alert アプライアンスでのアラート構成により、モニターして QRadar に転送するアラート条件が決定されます。QRadar でイベントを収集するには、QRadar の IP アドレスを宛先として使用して、UNIX syslog イベント・フォーマットでイベントを転送するように IBM zSecure Alert アプライアンスを構成する必要があります。UNIX syslog アラートおよび宛先の構成については、「*IBM Security zSecure Alert* ユーザー・リファレンス・マニュアル」を参照してください。

QRadar は、IBM zSecure Alert からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ただし、QRadar 用のログ・ソースを手動で作成して syslog イベントを受信することもできます。以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「IBM zSecure **Alert**」を選択します。
8. 「プロトコル構成」リストで「**Syslog**」を選択します。
9. 以下の値を構成します。

表 228. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	IBM zSecure Alert からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 67 章 ISC Bind

Internet System Consortium (ISC) BIND デバイスを IBM Security QRadar と統合できます。ISC BIND デバイスは、syslog を使用してイベントを受け入れます。

このタスクについて

イベントを QRadar に転送するように ISC BIND デバイスで syslog を構成できます。

手順

1. ISC BIND デバイスにログインします。
2. 以下のファイルを開いて、logging 節を追加します。

```
named.conf

logging {

channel <channel_name> {

syslog <syslog_facility>;

 severity <critical | error | warning | notice | info | debug [level ] |
dynamic >;

print-category yes;

print-severity yes;

print-time yes;

};

category queries {

<channel_name>;

};

category notify {

<channel_name>;

};

category network {

<channel_name>;

};
```

```
category client {

<channel_name>;

};

};

例:

logging {

channel QRadar {

syslog local3;

severity info;

};

category queries {

QRadar;

};

category notify {

QRadar;

};

category network {

QRadar;

};

category client {

QRadar;

};

};
```

3. ファイルを保存して終了します。
4. 591 ページの『第 67 章 ISC Bind』で選択したファシリティーを使用して QRadar にログを記録するように syslog 構成を編集します。

   ```
   <syslog_facility>.* @<IP Address>
   ```

   ここで *<IP Address>* は、QRadar の IP アドレスです。

   例えば、以下のようにします。

```
local3.* @192.16.10.10
```

注: QRadar は、重大度レベルが info 以上のログのみを構文解析します。

5. 以下のサービスを再始動します。

```
service syslog restart

service named restart
```

次のタスク

これで、QRadar でログ・ソースを構成できるようになりました。

ログ・ソースの構成

IBM Security QRadar は、ISC BIND の syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**ISC BIND**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *229. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	ISC BIND アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 68 章 Imperva SecureSphere

Imperva SecureSphere 用の IBM Security QRadar DSM は、ご使用の Imperva SecureSphere デバイスからすべての関連 Syslog イベントを収集します。

Imperva SecureSphere DSM の仕様を以下の表に示します。

表 *230. Imperva SecureSphere DSM*

仕様	値
製造元	Imperva
DSM 名	SecureSphere
RPM ファイル名	`DSM-ImpervaSecuresphere-QRadar-version-Build_number.noarch.rpm`
サポートされるバージョン	v6.2 および v7.x リリースの Enterprise Edition (Syslog) v9.5 から v11.5 (LEEF)
イベント・フォーマット	syslog LEEF
QRadar で記録されるイベント・タイプ	ファイアウォール・ポリシー・イベント
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Imperva の Web サイト (http://www.imperva.com)

Imperva SecureSphere デバイスから QRadar にイベントを送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Imperva SecureSphere DSM RPM をダウンロードして QRadar コンソールにインストールしてください。
2. Imperva SecureSphere のインスタンスごとに、QRadar と通信する Imperva SecureSphere アプライアンスを構成します。Imperva SecureSphere アプライアンスで、次の手順を実行します。
   a. アラート・アクションを構成します。
   b. システム・イベント・アクションを構成します。
3. QRadar が Imperva SecureSphere ログ・ソースを自動的に検出しない場合は、ネットワーク上の Imperva SecureSphere のインスタンスごとにログ・ソースを作成します。Imperva SecureSphere 固有のパラメーターを定義するには以下の表の内容を使用します。

表 231. *Imperva SecureSphere* ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース・タイプ	Imperva SecureSphere
プロトコル構成	Syslog

関連タスク:

『Imperva SecureSphere のアラート・アクションの構成』
ファイアウォール・ポリシー・アラートの syslog イベントを QRadar に転送するように Imperva SecureSphere アプライアンスを構成します。

598 ページの『Imperva SecureSphere のシステム・イベント・アクションの構成』
syslog システム・ポリシー・イベントを QRadar に転送するように Imperva SecureSphere アプライアンスを構成します。

600 ページの『QRadar にデータベース監査レコードを送信するための Imperva SecureSphere V11.0 の構成』
Imperva SecureSphere V11.0 から IBM Security QRadar にデータベース監査レコードを送信するには、カスタム・アクション・セットを作成し、アクション・インターフェースを追加し、監査ポリシーを構成します。

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『Imperva SecureSphere のアラート・アクションの構成』
ファイアウォール・ポリシー・アラートの syslog イベントを QRadar に転送するように Imperva SecureSphere アプライアンスを構成します。

598 ページの『Imperva SecureSphere のシステム・イベント・アクションの構成』
syslog システム・ポリシー・イベントを QRadar に転送するように Imperva SecureSphere アプライアンスを構成します。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Imperva SecureSphere のアラート・アクションの構成

ファイアウォール・ポリシー・アラートの syslog イベントを QRadar に転送するように Imperva SecureSphere アプライアンスを構成します。

このタスクについて

次のリストを使用して、転送するイベント・タイプごとに「メッセージ」フィールドにメッセージ・ストリングを定義します。

重要**:** これらのコード例で改行があると、この構成が失敗する原因になる可能性があります。各アラートで、コード・ブロックをテキスト・エディターにコピーし、改行を削除してから、「カスタム・フォーマット **(Custom Format)**」列に一行で貼り付けてください。

データベース・アラート **(V9.5** から **v11.5)**

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|
${Alert.alertType}${Alert.immediateAction}|Alert ID=${Alert.dn}
|devTimeFormat=[see note]|devTime=${Alert.createTime}
|Alert type=${Alert.alertType}|src=${Alert.sourceIp}|usrName=$
{Event.struct.user.user}|Application name=${Alert.applicationName}
|dst=${Event.destInfo.serverIp}|Alert Description=${Alert.description}
|Severity=${Alert.severity}|Immediate Action=${Alert.immediateAction}
|SecureSphere Version=${SecureSphereVersion}
```

ファイル・サーバー・アラート **(V9.5** から **v11.5)**

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|
${Alert.alertType} ${Alert.immediateAction}|Alert ID={Alert.dn}
|devTimeFormat=[see note] |devTime=${Alert.createTime}
|Alert type=${Alert.alertType}|src=${Alert.sourceIp} |usrName=
${Event.struct.user.username}|Domain=${Event.struct.user.domain}
|Application name=${Alert.applicationName}|dst=${Event.destInfo.serverIp}
|Alert Description=${Alert.description}|Severity=${Alert.severity}
|Immediate Action=${Alert.immediateAction} |SecureSphere
Version=${SecureSphereVersion}
```

Web アプリケーション・ファイアウォール・アラート **(V9.5** から **v11.5)**

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|
${Alert.alertType} ${Alert.immediateAction}|Alert ID=${Alert.dn}
|devTimeFormat=[see note]|devTime=${Alert.createTime}
|Alert type=${Alert.alertType}|src=${Alert.sourceIp}
|usrName=${Alert.username}|Application name=${Alert.applicationName}
|Service name=${Alert.serviceName}|Alert Description=${Alert.description}
|Severity=${Alert.severity}|Simulation Mode=${Alert.simulationMode}
|Immediate Action=${Alert.immediateAction}
```

すべてのアラート **(v6.2** および **v7.x** リリースの **Enterprise Edition)**

```
DeviceType=ImpervaSecuresphere Alert|an=$!{Alert.alertMetadata.
alertName}|at=SecuresphereAlert|sp=$!{Event.sourceInfo.sourcePort}
|s=$!{Event.sourceInfo.sourceIp}|d=$!{Event.destInfo.serverIp}|dp=$!
{Event.destInfo.serverPort}|u=$!{Alert.username}|g=$!
{Alert.serverGroupName}|ad=$!{Alert.description}
```

注**:** 時刻形式は SecureSphere アプライアンスで構成できるため、**devTimeFormat** パラメーターには値が含まれていません。SecureSphere アプライアンスの時刻形式を確認し、適切な時刻形式を指定します。

手順

1. 管理特権を使用して、SecureSphere にログインします。
2. 「ポリシー **(Policies)**」タブをクリックします。
3. 「アクション・セット **(Action Sets)**」タブをクリックします。
4. SecureSphere デバイスが生成する各アラートに対して、次のようにイベントを生成します。
   a. 「**New**」をクリックして、アラートに対する新しいアクション・セットを作成します。
   b. アクションを「選択したアクション **(Selected Actions)**」リストに移動します。
   c. 「システム・ログ **(System Log)**」アクション・グループを展開します。
   d. 「アクション名 **(Action Name)**」フィールドにアラート・アクションの名前を入力します。
   e. 「**Apply to event type**」リストで、「**Any event type**」を選択します。

f. 以下のパラメーターを構成します。
   - 「**Syslog host**」フィールドに、イベントの送信先の QRadar アプライアンスの IP アドレスを入力します。
   - 「**Syslog ログ・レベル (Syslog log level)**」リストで、「情報 **(INFO)**」を選択します。
   - 「メッセージ **(Message)**」フィールドで、イベント・タイプのメッセージ・ストリングを定義します。

g. 「**Facility**」フィールドに、syslog と入力します。

h. 「すべてのイベントで実行 **(Run on Every Event)**」チェック・ボックスを選択します。

i. 「保存」をクリックします。

5. Syslog イベントをトリガーするには、次のように、各ファイアウォール・ポリシーをアラート・アクションに関連付けます。

   a. ナビゲーション・メニューから、「ポリシー **(Policies)**」>「セキュリティー **(Security)**」>「ファイアウォール・ポリシー **(Firewall Policy)**」をクリックします。

   b. アラート・アクションに使用するポリシーを選択します。

   c. 「ポリシー **(Policy)**」タブをクリックします。

   d. 「**Followed Action**」リストで、新しいアクションを選択し、パラメーターを構成します。

      ヒント**:** 確立した接続を、ブロック、インバウンド、またはアウトバウンドとして構成します。該当するサービス・ポートを常に許可します。

   e. ポリシーが使用可能として構成され、適切なサーバー・グループに適用されていることを確認します。

   f. 「保存」をクリックします。

Imperva SecureSphere のシステム・イベント・アクションの構成

syslog システム・ポリシー・イベントを QRadar に転送するように Imperva SecureSphere アプライアンスを構成します。

このタスクについて

次のリストを使用して、転送するイベント・タイプごとに「メッセージ」フィールドにメッセージ・ストリングを定義します。

重要**:** これらのコード例で改行があると、この構成が失敗する原因になる可能性があります。各アラートで、コード・ブロックをテキスト・エディターにコピーし、改行を削除してから、「カスタム・フォーマット **(Custom Format)**」列に一行で貼り付けてください。

システム・イベント **(V9.5** から **v11.5)**

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|${Event.eventType}
|Event ID=${Event.dn}|devTimeFormat=[see note]|devTime=${Event.createTime}
|Event Type=${Event.eventType}|Message=${Event.message}
|Severity=${Event.severity.displayName}|usrName=${Event.username}
|SecureSphere Version=${SecureSphereVersion}
```

データベース監査レコード **(V9.5** から **v11.5)**

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}
|${Event.struct.eventType}|Server Group=${Event.serverGroup}
|Service Name=${Event.serviceName}|Application Name=$
{Event.applicationName}|Source Type=${Event.sourceInfo.eventSourceType}
|User Type=${Event.struct.user.userType}|usrName=$
{Event.struct.user.user}|User Group=${Event.struct.userGroup}
|Authenticated=${Event.struct.user.authenticated}|App User=$
{Event.struct.applicationUser}|src=${Event.sourceInfo.sourceIp}
|Application=${Event.struct.application.application}|OS User=
${Event.struct.osUser.osUser}|Host=${Event.struct.host.host}
|Service Type=${Event.struct.serviceType}|dst=$
{Event.destInfo.serverIp}|Event Type=${Event.struct.eventType}
|Operation=${Event.struct.operations.name}|Operation type=
${Event.struct.operations.operationType}|Object name=$
{Event.struct.operations.objects.name}|Object type=$
{Event.struct.operations.objectType}|Subject=
${Event.struct.operations.subjects.name}|Database=$
{Event.struct.databases.databaseName}|Schema=
${Event.struct.databases.schemaName}|Table Group=$
{Event.struct.tableGroups.displayName}|Sensitive=
${Event.struct.tableGroups.sensitive}|Privileged=$
{Event.struct.operations.privileged}|Stored Proc=$
{Event.struct.operations.storedProcedure}|Completed Successfully
=${Event.struct.complete.completeSuccessful}|Parsed Query=$
{Event.struct.query.parsedQuery}|Bind Vaiables=$
{Event.struct.rawData.bindVariables}|Error=$
{Event.struct.complete.errorValue}|Response Size=$
{Event.struct.complete.responseSize}|Response Time=$
{Event.struct.complete.responseTime}|Affected Rows=
${Event.struct.query.affectedRows}| devTimeFormat=[see note]
|devTime=${Event.createTime}
```

すべてのアラート **(v6.2** および **v7.x** リリースの **Enterprise Edition)**

```
DeviceType=ImpervaSecuresphere Event|et=$!{Event.eventType}
|dc=Securesphere System Event|sp=$!{Event.sourceInfo.sourcePort}
|s=$!{Event.sourceInfo.sourceIp}|d=$!{Event.destInfo.serverIp}
|dp=$!{Event.destInfo.serverPort}|u=$!{Event.username}|t=$!
{Event.createTime}|sev=$!{Event.severity}|m=$!{Event.message}
```

注**:** 時刻形式は SecureSphere アプライアンスで構成できるため、**devTimeFormat** パラメーターには値が含まれていません。SecureSphere アプライアンスの時刻形式を確認し、適切な時刻形式を指定します。

手順

1. 管理特権を使用して、SecureSphere にログインします。
2. 「ポリシー **(Policies)**」タブをクリックします。
3. 「アクション・セット **(Action Sets)**」タブをクリックします。
4. SecureSphere デバイスが生成する各アラートに対して、次のようにイベントを生成します。
   a. 「**New**」をクリックして、アラートに対する新しいアクション・セットを作成します。
   b. 新しいアクション・セットの名前を入力します。
   c. アクションを「選択したアクション **(Selected Actions)**」リストに移動します。
   d. 「システム・ログ **(System Log)**」アクション・グループを展開します。

e. 「アクション名 **(Action Name)**」フィールドにアラート・アクションの名前を入力します。

f. 「**Apply to event type**」リストで、「**Any event type**」を選択します。

g. 以下のパラメーターを構成します。

- 「**Syslog host**」フィールドに、イベントの送信先の QRadar アプライアンスの IP アドレスを入力します。
- 「**Syslog ログ・レベル (Syslog log level)**」リストで、「情報 **(INFO)**」を選択します。
- 「メッセージ **(Message)**」フィールドで、イベント・タイプのメッセージ・ストリングを定義します。

h. 「**Facility**」フィールドに、`syslog` と入力します。

i. 「すべてのイベントで実行 **(Run on Every Event)**」チェック・ボックスを選択します。

j. 「保存」をクリックします。

5. Syslog イベントをトリガーするには、次のように、各システム・イベント・ポリシーをアラート・アクションに関連付けます。

a. ナビゲーション・メニューで、「**Policies**」>「**System Events**」をクリックします。

b. アラート・アクションに対して使用するシステム・イベント・ポリシーを選択または作成します。

c. 「フォロー・アクション **(Followed Action)**」タブをクリックします。

d. 「**Followed Action**」リストで、新しいアクションを選択し、パラメーターを構成します。

ヒント**:** 確立した接続を、ブロック、インバウンド、またはアウトバウンドとして構成します。該当するサービス・ポートを常に許可します。

e. 「保存」をクリックします。

QRadar にデータベース監査レコードを送信するための Imperva SecureSphere V11.0 の構成

Imperva SecureSphere V11.0 から IBM Security QRadar にデータベース監査レコードを送信するには、カスタム・アクション・セットを作成し、アクション・インターフェースを追加し、監査ポリシーを構成します。

手順

1. カスタム・アクション・セットを作成します。

a. Imperva SecureSphere システムにログインします。

b. 「メイン **(Main)**」ワークスペースで、「ポリシー **(Policies)**」 > 「アクション・セット **(Action Sets)**」を選択します。

c. 「アクション・セット (Action Sets)」ペインで、緑色の正符号アイコンをクリックします。

d. 「アクション・セット **(Action Set)**」テキスト・ボックスに、アクション・セットの名前を入力します。例: `QRadar SIEM`。

e. 「適用先のイベント・タイプ **(Apply to event type)**」リストで、「監査 **(Audit)**」を選択します。

f. 「作成」をクリックします。

2. アクション・セットの一部にするアクション・インターフェースを「選択したアクション **(Selected Actions)**」ペインに追加します。

a. 緑色の上矢印アイコンをクリックし、「ゲートウェイ・システム・ログ **(Gateway System Log)**」 > 「システム・ログに監査イベントを記録 **(**ゲートウェイ・システム・ログ**) (log audit event to System Log (Gateway System Log))**」を選択します。

b. 以下のアクション・インターフェース・パラメーターを構成します。

パラメーター	値
名前	アクション・セット用に作成した名前を入力します。例: QRadar SIEM。
プロトコル (Protocol)	「**UDP**」を選択します。
ホスト	イベントを送信する対象の QRadar アプライアンスの IP アドレスまたはホスト名を入力します。
ポート	514
Syslog ログ・レベル (Syslog Log Level)	通知
ファシリティー (Facility)	syslog
メッセージ (Message)	**重要:** コード例にある改行は、この構成が失敗する原因になる可能性があります。各アラートで、以下のコード・ブロックをテキスト・エディターにコピーし、改行を削除してから、「メッセージ **(Message)**」フィールドに一行で貼り付けてください。 `LEEF:1.0|Imperva|Secure Sphere|${SecureSphereVersion}| ${Alert.alertType}${Alert.immediate Action}|Alert ID=${Alert.dn}\|devTime Format=devTimeFormat=yyyy-MM-dd HH:mm:ss.S\|devTime=${Alert.createTime} |Alert type=${Alert.alertType}\|src=$ {Alert.sourceIp}|usrName=${Event. struct.user.user}|Application name= ${Alert.applicationName}\|dst=${Event. destInfo.serverIp}|Alert Description= ${Alert.description}\|Severity=${Alert. severity}|Immediate Action=${Alert. immediateAction}\|SecureSphere Version=$ {SecureSphereVersion}`

a. 「すべてのイベントで実行 **(Run on Every Event)**」チェック・ボックスを選択します。

3. QRadar に送信するイベントの監査ポリシーを構成します。

a. 「メイン (Main)」ワークスペースで、「ポリシー **(Policies)**」 > 「監査 **(Audit)**」をクリックします。

b. 「**DB** サービスの作成 **(Create DB Service)**」をクリックします。

c. ポリシーの名前を入力します。

d. 「既存の使用 **(Use Existing)**」を選択し、リストからポリシーを選択します。
e. 「基準の一致 **(Match Criteria)**」タブをクリックし、ポリシーの基準を入力します。
f. 「適用先 **(Apply To)**」タブをクリックし、サーバー・グループを選択します。
g. 「外部ロガー **(External Logger)**」タブをクリックします。
h. 「**Syslog**」リストで、構成した「**QRadar SIEM**」を選択します。
i. オプション: 「**Syslog**」リストで事前定義のポリシーを選択した場合は、「適用先 **(Apply To)**」フィールドおよび「外部ロガー **(External Logger)**」フィールドを構成します。
j. 「保存」をクリックします。

次のタスク

QRadar に送信する監査イベントのタイプごとに、監査ポリシーを定義するか、事前定義のポリシーを構成する必要があります。

第 69 章 Infoblox NIOS

IBM Security QRadar 用の Infoblox NIOS DSM は、syslog を使用してイベントを受け入れることで、QRadar が Infoblox NIOS デバイスから関連イベントをすべて記録できるようにします。

QRadar を構成する前に、syslog イベントを QRadar に送信するように Infoblox NIOS デバイスを構成します。Infoblox NIOS デバイスのログの構成について詳しくは、ご使用の *Infoblox NIOS* のベンダー資料を参照してください。

以下の表は、Infoblox NIOS DSM の仕様を示しています。

Infoblox NIOS DSM の仕様

仕様	値
製造元	Infoblox
DSM	NIOS
バージョン	v6.x
受け入れられたイベント	Syslog
QRadar で記録されるイベント	• ISC Bind イベント • Linux DHCP イベント • Linux サーバー・イベント • Apache イベント
QRadar でのオプション	Infoblox NIOS
自動的に検出	いいえ
ID を含む?	はい
詳細情報	http://www.infoblox.com

ログ・ソースの構成

IBM Security QRadar が Infoblox NIOS アプライアンスからの syslog イベントに対して、ログソースを自動的に検出および作成することはありません。Infoblox NIOS アプライアンスを QRadar と統合するには、Infoblox NIOS イベントを受信するためのログ・ソースを手動で作成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。

6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Infoblox NIOS**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 残りのパラメーターを構成します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

第 70 章 iT-CUBE agileSI

IBM Security QRadar 用の iT-CUBE agileSI DSM は、ご使用の SAP システムに統合されている agileSI インストール済み環境からセキュリティー・ベースの SAP イベントおよび監査 SAP イベントを受け入れます。

QRadar は、ご使用の SAP 環境でセキュリティー・リスクとして定義されているイベント・データを使用してオフェンスを生成し、セキュリティー・チームのためにイベント・データを相関させます。SAP セキュリティー・イベントは、agileSI によって生成されたログ・ファイルにログ・イベント拡張フォーマット (LEEF) で書き込まれます。QRadar は、SMB Tail プロトコルを使用して新規イベントを取得します。agileSI からイベントを取得するには、SMB Tail プロトコルを使用してログ・ソースを作成し、ログインして LEEF 形式の agileSI イベント・ファイルをポーリングするための QRadar 資格情報を提供します。QRadar は、SMB Tail プロトコルが新規 SAP イベントのイベント・ファイルをポーリングするたびに新規イベントで更新されます。

イベントを転送するための agileSI の構成

agileSI を構成するには、イベントの論理ファイル名を作成し、agileSI イベント・ログのパスを使用してコネクター設定を構成する必要があります。

このタスクについて

LEEF 形式のイベント・ファイルの場所は、Samba で表示可能で、かつ IBM Security QRadar でログ・ソースに対して構成した資格情報を使用してアクセス可能な場所でなければなりません。

手順

1. agileSI コア・システム・インストール済み環境で、SAP セキュリティー・イベントが含まれる出力ファイルの論理ファイル名を定義します。

   SAP は、アプリケーション・プログラムでプラットフォームに依存しない論理ファイル名を使用できるようにする概念を備えています。組織の要件に従って、トランザクション「FILE」(論理ファイル・パス定義) を使用して、論理ファイルの名前とパスを作成します。
2. agileSI にログインします。

   例: `http://<sap-system-url:port>/sap/bc/webdynpro/itcube/ccf?sap-client=<client>&sap-language=EN`

   各部分について以下で説明します。

   - *<sap-system-url>* は、SAP システムの IP アドレスとポート番号です (10.100.100.125:50041 など)。
   - *<client>* は、agileSI デプロイメント内のエージェントです。

3. メニューで「表示/変更 **(Display/Change)**」をクリックして、agileSI の変更モードを有効にします。
4. ツールバーで「ツール **(Tools)**」 > 「コア・コンシューマー・コネクター設定 **(Core Consumer Connector Settings)**」 を選択します。

   「コア・コンシューマー・コネクター設定 (Core Consumer Connector Settings)」が表示されます。
5. 以下の値を構成します。

   「コア・コンシューマー **(Consumer Connector)**」リストで「**Q1 Labs**」を選択します。
6. 「アクティブ **(Active)**」チェック・ボックスを選択します。
7. 「コネクター・タイプ **(Connector Type)**」リストで「ファイル **(File)**」を選択します。
8. 「論理ファイル名 **(Logical File Name)**」フィールドに、 605 ページの『イベントを転送するための agileSI の構成』で構成した論理ファイル名のパスを入力します。

   例: `/ITCUBE/LOG_FILES`

   agileSI イベント用に作成されるファイルのラベルは、`LEEFYYYYDDMM.TXT` になります。ここで、`YYYYDDMM` は、年、日、月です。抽出が実行されるたびに、現在の日のイベント・ファイルに新規イベントが追加されます。*iT-CUBE* agileSI は、毎日、SAP イベント用の新規 LEEF ファイルを作成します。
9. 「保存」をクリックします。

   コネクターの構成が保存されます。agileSI の構成を完了する前に、抽出を使用して、agileSI の変更をデプロイする必要があります。
10. ツールバーで「ツール **(Tools)**」 > 「抽出の管理 **(Extractor Management)**」を選択します。

    「抽出の管理 (Extractor Management)」設定が表示されます。
11. 「すべてをデプロイ **(Deploy all)**」をクリックします。

    agileSI イベントの構成は完了です。これで、ログ・ソースを QRadar で構成することができます。

agileSI ログ・ソースの構成

SMB Tail プロトコルを使用してログインおよびイベント・ファイルのポーリングを行うように IBM Security QRadar を構成する必要があります。

このタスクについて

SMB Tail プロトコルにより、ログインし、agileSI によって `LEEFYYYYDDMM.txt` ファイルにログが記録されたイベントを取得します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**iT-CUBE agileSI**」を選択します。
9. 「プロトコル構成」リストで「**SMB Tail**」を選択します。
10. 以下の値を構成します。

表 *232. SMB Tail* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	*iT-CUBE* agileSI イベントの ID として、ログ・ソースの IP アドレス、ホスト名、または名前を入力します。
サーバー・アドレス	*iT-CUBE* agileSI サーバーの IP アドレスを入力します。
ドメイン	*iT-CUBE* agileSI サーバーのドメインを入力します。 サーバーがドメイン内にない場合は、このパラメーターはオプションです。
ユーザー名	*iT-CUBE* agileSI サーバーにアクセスするために必要なユーザー名を入力します。 指定するユーザー名とパスワードは、agileSI イベントについて `LEEFYYYYDDMM.txt` ファイルを読み取ることができる必要があります。
パスワード	*iT-CUBE* agileSI サーバーにアクセスするために必要なパスワードを入力します。
パスワードの確認	*iT-CUBE* agileSI サーバーにアクセスするために必要なパスワードを確認します。
ログ・フォルダーのパス **(Log Folder Path)**	`LEEFYYYYDDMM.txt` ファイルにアクセスするためのディレクトリー・パスを入力します。 ファイル・パスをサポートするパラメーターでは、パス情報でドライブ名を定義できます。例えば、管理共有に `c$/LogFiles/` を使用したり、公開共有フォルダー・パスに `LogFiles/` を使用したりすることができますが、`c:/LogFiles` は使用できません。 ログ・フォルダー・パスに管理共有 (`C$`) が含まれる場合、管理共有 (`C$`) に対する NetBIOS 権限を備えたユーザーは、ログ・ファイルの読み取りに必要である適切なアクセス権限を備えています。ローカルまたはドメインの管理者は、管理共有上にあるログ・ファイルにアクセスするための十分な特権を備えています。

表 232. *SMB Tail* プロトコルのパラメーター (続き)

パラメーター	説明
ファイル・パターン	ファイル名のフィルタリングに必要な正規表現 (regex) を入力します。QRadar がイベントについてポーリングすると、一致するすべてのファイルが処理対象として含まれます。 例えば、末尾が `txt` であるすべてのファイルをリストする場合、`.*¥.txt` という入力を使用します。このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://docs.oracle.com/javase/tutorial/essential/regex/ を参照してください。
ファイル読み取りの強制 **(Force File Read)**	プロトコルにログ・ファイルの読み取りを強制するには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。 このチェック・ボックスをクリアした場合、QRadar が変更時刻またはファイル・サイズの変更を検出すると、イベント・ファイルが読み取られます。
再帰的 **(Recursive)**	ファイル・パターンでサブフォルダーを検索する場合は、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
ポーリング間隔 **(秒)**	ポーリング間隔 (新規データを確認するためのログ・ファイルに対する照会から次の照会までの間の秒数) を入力します。 最小ポーリング間隔は 10 秒、最大ポーリング間隔は 3,600 秒です。デフォルトは 10 秒です。
スロットル・イベント数/秒	SMB Tail プロトコルが 1 秒あたり転送する最大イベント数を入力します。 最小値は 100 EPS、最大値は 20,000 EPS です。デフォルトは 100 EPS です。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。*iT-CUBE* agileSI ログ・ソースが新規イベントを取得すると、QRadar の「ログ・アクティビティー」タブが更新されます。

第 71 章 Itron スマート・メーター

IBM Security QRadar 用の Itron スマート・メーターの DSM は、syslog を使用して、Itron Openway スマート・メーターからイベントを収集します。

このタスクについて

Itron Openway スマート・メーターは、ポート 514 を使用して、syslog イベントを QRadar に送信します。syslog 用のメーターの構成について詳しくは、*Itron Openway* スマート・メーター の資料を参照してください。

QRadar は、Itron Openway スマート・メーターからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ただし、QRadar 用のログ・ソースを手動で作成して syslog イベントを受信することもできます。以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Itron** スマート・メーター」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *233. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース ID	Itron Openway スマート・メーター・インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 72 章 Juniper Networks

IBM Security QRadar はさまざまな Juniper Networks DSM をサポートします。

Juniper Networks AVT

IBM Security QRadar 用の Juniper Networks Application Volume Tracking (AVT) DSM は、Java Database Connectivity (JDBC) プロトコルを使用してイベントを受け入れます。

このタスクについて

QRadar は、関連するすべてのイベントを記録します。Juniper Networks NSM AVT データを統合するには、Juniper Networks NSM サーバーのデータベースでビューを作成する必要があります。また Juniper Networks NSM サーバー上で Postgres データベースを構成し、データベースへの接続を許可する必要があります。これは、デフォルトではローカル接続だけが許可されているためです。

注**:** この手順はガイドラインとして提供されます。具体的な手順については、ベンダーの資料を参照してください。

手順

1. Juniper Networks AVT デバイスのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のファイルを開きます。

   ```
   /var/netscreen/DevSvr/pgsql/data/pg_hba.conf file
   ```

3. このファイルの終わりに以下の行を追加します。

   ```
   host all all <IP address>/32 trust
   ```

   ここで、*<IP address>* はデータベースに接続する QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
4. 以下のようにして、Postgres サービスを再ロードします。

   ```
   su - nsm -c "pg_ctl reload -D /var/netscreen/DevSvr/pgsql/data"
   ```

5. Juniper Networks NSM ユーザーとして、以下の入力を使用してビューを作成します。

   ```
   create view strm_avt_view as SELECT a.name, a.category,
   v.srcip,v.dstip,v.dstport, v."last", u.name as userinfo,
   v.id, v.device, v.vlan,v.sessionid, v.bytecnt,v.pktcnt,
   v."first" FROM avt_part v JOIN app a ON v.app =a.id
   JOIN userinfo u ON v.userinfo = u.id;
   ```

   ビューが作成されました。

   これで、QRadar でログ・ソースを構成する準備ができました。

Juniper Networks AVT デバイスからイベントを受信するための IBM Security QRadar の構成

Juniper Networks AVT デバイスからイベントを受信するように QRadar を構成できます。

手順

1. 「ログ・ソース・タイプ」リストで「**Juniper Networks AVT**」を選択します。
2. ログ・ソースに対して JDBC プロトコルを構成する必要もあります。JDBC プロトコルを構成するには、以下のパラメーターを使用します。

表 *234. JDBC* プロトコル・パラメーター

パラメーター	説明
データベース・タイプ	「データベース・タイプ」リストで「**Postgres**」を選択します。
データベース名	`profilerDb`
IP またはホスト名	Juniper Networks NSM システムの IP アドレスを入力します
ポート	`5432` を入力します
ユーザー名	profilerDb データベースのユーザー名を入力します
パスワード	profilerDB データベースのパスワードを入力します
テーブル名	`strm_avt_view` を入力します。
選択リスト	`*` を入力します
比較フィールド	`id` を入力します
準備済みステートメントの使用 **(Use Prepared Statements)**	「準備済みステートメントの使用 **(Use Prepared Statements)**」チェック・ボックスが選択されていない状態である必要があります。 Juniper Networks AVT DSM では準備済みステートメントはサポートされていません。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔として `10` を入力します。

注**:** パラメーター「データベース名」と「テーブル名」では、大/小文字が区別されます。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Juniper Networks DDoS Secure

IBM Security QRadar 用の Juniper DDoS Secure DSM は、ログ・イベント拡張フォーマット (LEEF) の Syslog を使用して Juniper DDoS Secure デバイスからイベントを受信します。QRadar は、関連する状況とネットワーク状態イベントをすべて記録します。

手順

1. Juniper DDoS Secure にログインします。
2. 「構造化 Syslog サーバー (Structured Syslog Server)」ウィンドウに移動します。
3. 「サーバーの **IP** アドレス **(Server IP Address(es))**」フィールドに、QRadar コンソールの IP アドレスを入力します。
4. 「フォーマット **(Format)**」リストで「**LEEF**」を選択します。
5. オプション: 「ファシリティー **(Facility)**」フィールドでデフォルトの `local0` を使用しない場合は、ファシリティー値を入力します。
6. 「優先順位」リストで、組み込む Syslog 優先レベルを選択します。選択した Syslog 優先レベルに一致するかまたはこのレベルを超えるイベントが、QRadar に転送されます。
7. QRadar にログインします。
8. 「管理」タブをクリックします。
9. ナビゲーション・メニューで「データ・ソース」をクリックします。
10. 「ログ・ソース」アイコンをクリックします。
11. 「追加」をクリックします。
12. 「ログ・ソース・タイプ」リストで「**Juniper DDoS Secure**」オプションを選択します。
13. パラメーターを構成します。
14. 「保存」をクリックします。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Juniper Networks DX Application Acceleration Platform

IBM Security QRadar 用の Juniper DX Application Acceleration Platform DSM は、Syslog を使用してイベントを受信します。QRadar は、関連する状況とネットワーク状態イベントをすべて記録します。QRadar を構成する前に、Syslog イベントを転送するように Juniper デバイスを構成する必要があります。

手順

1. Juniper DX のユーザー・インターフェースにログインします。
2. 必要なクラスター構成 (「サービス - クラスター名 (Services - Cluster Name)」)、「ロギング (Logging)」セクションを参照します。
3. 「ロギングの有効化 **(Enable Logging)**」チェック・ボックスを選択します。
4. ログ・フォーマットを選択します。

QRadar では、共通フォーマットと perf2 フォーマットのみを使用して Juniper DX ログがサポートされています。

5. ログの区切り文字の形式を選択します。

   QRadar ではコンマで区切られているログだけがサポートされています。

6. 「ログ・ホスト **(Log Host)**」セクションで、QRadar システムの IP アドレスを入力します。
7. 「ログ・ポート **(Log Port)**」セクションで、ログをエクスポートする UDP ポートを入力します。
8. これで、QRadar でログ・ソースを構成する準備ができました。

Juniper DX アプリケーション・アクセラレーション・プラットフォームからイベントを受信するための IBM Security QRadar の構成

このタスクについて

Juniper DX アプリケーション・アクセラレーション・プラットフォームからイベントを受信するように QRadar を構成できます。

手順

「ログ・ソース・タイプ」リストで「**Juniper DX** アプリケーション・アクセラレーション・プラットフォーム」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Juniper Networks EX シリーズ・イーサネット・スイッチ

IBM Security QRadar 用の Juniper シリーズ・イーサネット・スイッチ DSM は、Syslog を使用してイベントを受け取ります。

このタスクについて

Juniper EX Series Ethernet Switch DSM では、Juno OS が稼働する Juniper EX シリーズ・イーサネット・スイッチがサポートされます。Juniper EX シリーズ・イーサネット・スイッチと QRadar を統合する前に、Syslog イベントを転送するように Juniper EX シリーズ・イーサネット・スイッチを構成する必要があります。

手順

1. Juniper EX シリーズ・イーサネット・スイッチのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力します。

```
configure
```

3. 以下のコマンドを入力します。

```
set system syslog host <IP address> <option> <level>
```

各部分について以下で説明します。

- <*IP address*> は、QRadar の IP アドレスです。
- <*level*> は、info、error、warning、または any です。
- <*option*> は、表 235 の以下のオプションのいずれかです。

表 *235. Juniper Networks EX* シリーズ・スイッチのオプション

オプション	説明
any	すべてのファシリティー
authorization	許可システム
change-log	構成変更ログ
conflict-log	構成競合ログ
daemon	各種システム・プロセス
dfc	ダイナミック・フロー・キャプチャー
explicit-priority	優先順位とファシリティーをメッセージに含めます
external	ローカルの外部アプリケーション
facility-override	リモート・ホストへのロギングのための代替ファシリティー
firewall	ファイアウォール・フィルター・システム
ftp	FTP プロセス
interactive-commands	UI により実行されるコマンド
kernel	カーネル
log-prefix	このホストへのすべてのロギングのプレフィックス
match	ログに記録する行の正規表現
pfe	パケット転送エンジン

表 235. *Juniper Networks EX* シリーズ・スイッチのオプション (続き)

オプション	説明
user	ユーザー・プロセス

例:

```
set system syslog host 10.77.12.12 firewall info
```

この例のコマンドは、情報 (info) メッセージをファイアウォール・フィルター・システムから QRadar に送信するように Juniper EX シリーズ・イーサネット・スイッチを構成します。

4. ステップ 1 から 3 を繰り返し、追加の Syslog 宛先とオプションを構成します。追加する各オプションは、個別の Syslog 宛先構成を使用して識別する必要があります。
5. これで、QRadar で Juniper EX シリーズ・イーサネット・スイッチを構成する準備ができました。

Juniper EX シリーズ・イーサネット・スイッチからイベントを受信するための IBM Security QRadar の構成

Juniper EX シリーズ・イーサネット・スイッチからイベントを受信するように QRadar を構成できます。

手順

「ログ・ソース・タイプ」リストで「**Juniper EX** シリーズ・イーサネット・スイッチ」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Juniper Networks IDP

IBM Security QRadar 用の Juniper IDP DSM は、Syslog を使用してイベントを受け取ります。QRadar は、関連するすべての Juniper IDP イベントを記録します。

このタスクについて

Syslog サーバーにログを送信するように Juniper IDP 上のセンサーを構成できます。

手順

1. Juniper NSM のユーザー・インターフェースにログインします。
2. NSM で「デバイス・マネージャー **(Device Manager)**」の「センサー **(Sensor)**」をダブルクリックします。
3. 「グローバル設定 **(Global Settings)**」を選択します。
4. 「**Syslog** を有効にする **(Enable Syslog)**」を選択します。
5. イベントを QRadar に転送する Syslog サーバーの IP アドレスを入力します。
6. 「**OK**」をクリックします。
7. 「デバイスの更新 **(Update Device)**」を使用して、新しい設定を IDP センサーにロードします。

   IDP センサーにより送信される Syslog メッセージのフォーマットを次に示します。

   ```
   <day id>, <record id>, <timeReceived>,
   <timeGenerated>, <domain>, <domainVersion>,
   <deviceName>, <deviceIpAddress>, <category>,
   <subcategory>,<src zone>, <src intface>,
   <src addr>, <src port>, <nat src addr>,
   <nat src port>, <dstzone>, <dst intface>,
   <dst addr>, <dst port>, <nat dst addr>,
   <nat dst port>,<protocol>, <rule domain>,
   <rule domainVersion>, <policyname>, <rulebase>,
   <rulenumber>, <action>, <severity>,
   <is alert>, <elapsed>, <bytes in>,
   <bytes out>, <bytestotal>, <packet in>,
   <packet out>, <packet total>, <repeatCount>,
   <hasPacketData>,<varData Enum>, <misc-str>,
   <user str>, <application str>, <uri str>
   ```

   以下の Syslog の例を参照してください。

   ```
   [syslog@juniper.net dayId="20061012" recordId="0"
   timeRecv="2006/10/12 21:52:21"
   timeGen="2006/10/12 21:52:21" domain="" devDomVer2="0" device_ip="10.209.83.4"
   cat="Predefined" attack="TROJAN:SUBSEVEN:SCAN" srcZn="NULL" srcIntf="NULL"
   srcAddr="192.168.170.20" srcPort="63396" natSrcAddr="NULL" natSrcPort="0"
   dstZn="NULL" dstIntf="NULL" dstAddr="192.168.170.10" dstPort="27374"
   natDstAddr="NULL" natDstPort="0" protocol="TCP" ruleDomain="" ruleVer="5"
   policy="Policy2" rulebase="IDS" ruleNo="4" action="NONE" severity="LOW"
   alert="no" elaspedTime="0" inbytes="0" outbytes="0" totBytes="0" inPak="0"
   outPak="0" totPak="0" repCount="0" packetData="no" varEnum="31"
   misc="<017>'interface=eth2" user="NULL" app="NULL" uri="NULL"]
   ```

ログ・ソースの構成

Juniper NSM は、Juniper IDP の中央管理サーバーです。中央 NSM から着信次第 Juniper IDP アラートを収集して表示するように IBM Security QRadar を構成することができます。または、QRadar は個別の Juniper IDP デバイスから syslog を収集することができます。

Juniper Networks Secure Access デバイスからイベントを受信するように QRadar を構成するには、以下のようにします。

「ログ・ソース・タイプ」リストで、「**Juniper Networks Intrusion Detection and Prevention (IDP)**」を選択します。

. Juniper IDP について詳しくは、「*Network and Security Manager*」の資料を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Juniper Networks Infranet Controller

IBM Security QRadar 用の Juniper Networks Infranet Controller DSM は、Syslog を使用して DHCP イベントを受け取ります。QRadar は、Juniper Networks Infranet Controller からの関連するすべてのイベントを記録します。

このタスクについて

Juniper Networks Infranet Controller と統合するように QRadar を構成する前に、サーバーで Syslog を構成する必要があります。 Juniper Networks Infranet Controller の構成について詳しくは、ベンダーの資料を参照してください。

Juniper Infranet Controller の Syslog を構成したら、QRadar でログ・ソースを構成できます。

Juniper Networks Infranet Controller からイベントを受信するように QRadar を構成するには、以下のようにします。

手順

「ログ・ソース・タイプ」リストで「**Juniper Networks Infranet Controller**」を選択します。
デバイスの構成について詳しくは、「*IBM Security QRadar IBM Security QRadar Managing Log Sources Guide*」を参照してください。

Juniper Networks ファイアウォールおよび VPN

IBM Security QRadar 用の Juniper Networks Firewall and VPN DSM は、UDP Syslog を使用して Juniper ファイアウォールおよび VPN イベントを受け取ります。

このタスクについて

QRadar は、関連するファイアウォールおよび VPN イベントをすべて記録します。

注**:** TCP Syslog はサポートされていません。UDP Syslog を使用する必要があります。

イベントを QRadar にエクスポートするように Juniper Networks ファイアウォールおよび VPN デバイスを構成できます。

手順

1. Juniper Networks ファイアウォールおよび VPN のユーザー・インターフェースにログインします。
2. 「構成 **(Configuration)**」 > 「レポート設定 **(Report Settings)**」 > 「**Syslog**」を選択します。
3. 「**Syslog** メッセージを有効にする **(Enable Syslog Messages)**」チェック・ボックスを選択します。
4. QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
5. 「適用」をクリックします。

これで、QRadar でログ・ソースを構成する準備ができました。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

イベントを受信するための IBM Security QRadar の構成

このタスクについて

Juniper Networks ファイアウォールおよび VPN デバイスからイベントを受信するように QRadar を構成できます。

手順

「ログ・ソース・タイプ」リストで「**Juniper Networks** ファイアウォールおよび **VPN**」を選択します。
Juniper Networks ファイアウォールおよび VPN デバイスについて詳しくは、Juniper の資料を参照してください。

Juniper Networks Junos OS

IBM Security QRadar 用の Juniper Junos OS Platform DSM は、Syslog、構造化データ Syslog、または PCAP (SRX シリーズのみ) を使用するイベントを受け取ります。QRadar は、有効なすべての Syslog イベントまたは構造化データ Syslog イベントを記録します。

このタスクについて

Juniper Junos OS Platform DSM では、Junos OS が稼働する以下の Juniper デバイスがサポートされています。

- Juniper M シリーズ・マルチサービス・エッジ・ルーター

- Juniper MX シリーズ・イーサネット・サービス・ルーター
- Juniper T シリーズ・コア・プラットフォーム
- Juniper SRX シリーズ・サービス・ゲートウェイ

Juniper Networks SRX シリーズ・アプライアンスを使用する PCAP データの構成について詳しくは、 624 ページの『PCAP プロトコルの構成』を参照してください。

注: 構造化データ Syslog について詳しくは、Internet Engineering Task Force (http://www.ietf.org/) の RFC 5424 を参照してください。

Juniper デバイスと統合するように QRadar を構成する前に、Syslog または構造化データ Syslog を使用してデータを QRadar に転送する必要があります。

手順

1. Juniper プラットフォームのコマンド・ライン・インターフェース (CLI) にログインします。
2. `set system` 階層レベルで以下の Syslog ステートメントを組み込みます。

   ```
   [set system] syslog {host (hostname) {facility <severity>;
   explicit-priority; any any; authorization any; firewall any;

   } source-address source-address; structured-data {brief;} }
   ```

   次の表で、Syslog ステートメントに入力する構成設定変数を説明します。

Syslog 構成設定変数のリスト

パラメーター	説明
host	QRadar の IP アドレスまたは完全修飾ホスト名を入力します。
Facility	指定されたファシリティーに属し、このファシリティーとペアになっているメッセージの重大度を定義します。有効な重大度レベルは次のとおりです。 • すべて • なし • 緊急 • アラート • 重要 • エラー • 警告 • 注意 • 通知 指定された重大度レベル以上のメッセージがログに記録されます。emergency から info までの重大度レベルは、最も高いレベルから最も低いレベルの順に示されています。

Syslog 構成設定変数のリスト

パラメーター	説明
Source-address	ルーター・インターフェースの 1 つでシステム・ロギングの目的で構成されている有効な IP アドレスを入力します。 Source-address は、QRadar に送信される Syslog メッセージの送信元として記録されます。この IP アドレスは、`set system syslog` 階層レベルで **host** host name ステートメントに指定されます。ただし、これは他のルーティング・エンジン、またはルーティング・マトリックス内の TX Matrix プラットフォームに出力されるメッセージのものではありません。
structured-data	データに構造化データ Syslog を挿入します。

これで、QRadar でログ・ソースを構成できるようになりました。

QRadar により Juniper Junos OS プラットフォーム・デバイスとして自動的に検出されるデバイスを以下に示します。

- Juniper M シリーズ・マルチサービス・エッジ・ルーター
- Juniper MX シリーズ・イーサネット・サービス・ルーター
- Juniper SRX シリーズ
- Juniper EX シリーズ・イーサネット・スイッチ
- Juniper T シリーズ・コア・プラットフォーム

注**:** JunOS ファミリーのさまざまなデバイスでのロギングの類似性が原因で、デバイスが自動的にディスカバーされた場合に、予期したイベントが正しいログ・ソース・タイプで受信されないことがあります。デバイスに対して自動的に作成されたログ・ソースを確認して、手動で構成を調整してください。欠落したログ・ソース・タイプを追加できます。また、誤って追加されたログ・ソース・タイプを削除することもできます。

関連概念:

39 ページの『TLS Syslog プロトコルの構成オプション』
TLS Syslog イベント転送をサポートする最大 50 台のネットワーク・デバイスから暗号化された Syslog イベントを受信するには、TLS Syslog プロトコルを使用するようにログ・ソースを構成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Juniper Networks Network and Security Manager

IBM Security QRadar 用の Juniper Networks Network and Security Manager (NSM) DSM は、Juniper Networks NSM ログと Juniper Networks Secure

Service Gateway (SSG) ログを受け入れます。すべての Juniper SSG ログは Juniper NSM を介して QRadar に転送される必要があります。その他すべての Juniper デバイスのログは QRadar に直接転送できます。

Juniper Networks NSM ログの拡張フィルタリングについて詳しくは、ご使用の *Juniper Networks* のベンダー資料を参照してください。

Juniper Networks NSM デバイスを QRadar と統合するには、以下のタスクを実行する必要があります。

- 『Syslog にログをエクスポートするための Juniper Networks NSM の構成』
- 『Juniper Networks NSM のログ・ソースの構成』

Syslog にログをエクスポートするための Juniper Networks NSM の構成

Juniper Networks NSM は、Syslog サーバーを使用して該当するログ項目を Syslog にエクスポートします。

このタスクについて

管理システムの Syslog 設定を構成する場合、管理システムの Syslog 設定だけが定義されます。個々のデバイスからログはエクスポートされません。管理システムがログを Syslog にエクスポートできるように設定できます。

手順

1. Juniper Networks NSM のユーザー・インターフェースにログインします。
2. 「アクション・マネージャー **(Action Manager)**」メニューから「アクション・パラメーター **(Action Parameters)**」を選択します。
3. 該当するログの送信先とする Syslog サーバーの IP アドレスを入力します。
4. 該当するログの送信先とする Syslog サーバーの Syslog サーバー・ファシリティーを入力します。
5. 「デバイス・ログ・アクションの条件 **(Device Log Action Criteria)**」ノードで「アクション **(Actions)**」タブを選択します。
6. 「カテゴリー **(Category)**」、「重大度 **(Severity)**」、「アクション **(Action)**」で「**Syslog** を有効にする **(Syslog Enable)**」を選択します。

   これで、IBM Security QRadar でログ・ソースを構成する準備ができました。

Juniper Networks NSM のログ・ソースの構成

IBM Security QRadar で Juniper Networks NSM のログ・ソースを構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。

5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**Juniper Networks Network and Security Manager**」を選択します。
7. 「プロトコル構成」リストで「**Juniper NSM**」を選択します。
8. Juniper NSM プロトコルの以下の値を構成します。

表 *236. Juniper NSM* のプロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。 「ログ・ソース **ID**」は、ログ・ソース・タイプに対して固有でなければなりません。
IP	Juniper Networks NSM サーバーの IP アドレスまたはホスト名を入力します。
インバウンド・ポート	Juniper Networks NSM が通信を送信するインバウンド・ポートを入力します。有効な範囲は 0 から 65536 です。デフォルトは 514 です。
リダイレクション **Listen** ポート **(Redirection Listen Port)**	トラフィックの転送先ポートを入力します。有効な範囲は 0 から 65,536 です。デフォルトは 516 です。
ログ・ソースに **NSM** アドレスを使用	ログ・ソースの IP アドレスではなく Juniper NSM 管理サーバーの IP アドレスを使用する場合は、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。

注**:** QRadar インターフェースで、Juniper NSM プロトコル構成の「**Use NSM Address for Log Source**」チェック・ボックスを選択することで Juniper Networks NSM IP アドレスを使用することを選択できます。送信元の IP アドレスを使用するように構成を変更する場合 (このチェック・ボックスをクリアする場合)、QRadar コンソールに root ユーザーとしてログインし、コンソール (オールインワン・システムの場合) を再起動するか、または **shutdown -r now** コマンドを使用してログ・ソースをホストする イベント・コレクター (Event Collector) (分散環境の場合) を再起動する必要があります。

Juniper Junos OS プラットフォーム・デバイスからイベントを受信するための QRadar の構成

Juniper Junos OS プラットフォーム・デバイスからイベントを受信するように IBM Security QRadar を手動で構成できます。

手順

「ログ・ソース・タイプ」リストで、以下のいずれかのオプションを選択します。

- **Juniper JunOS** プラットフォーム
- **Juniper M** シリーズ・マルチサービス・エッジ・ルーター
- **Juniper MX** シリーズ・イーサネット・サービス・ルーター
- **Juniper SRX** シリーズ

- **Juniper T** シリーズ・コア・プラットフォーム

Juniper デバイスについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

PCAP プロトコルの構成

Juniper SRX Series のアプライアンスはパケット・キャプチャー (PCAP) および syslog データの IBM Security QRadar への転送をサポートします。

Syslog データは、ポート 514 の QRadar に転送されます。IP アドレスと発信 PCAP ポート番号は Juniper Networks SRX Series アプライアンス・インターフェースに構成されています。 Juniper Networks SRX Series アプライアンスは、PCAP データを転送するために以下の形式で構成されている必要があります。

<IP アドレス>:<ポート>

ここで、各項目は次のとおりです。

- *<IP Address>* は QRadar の IP アドレスです。
- <ポート> は PCAP データの発信ポート・アドレスです。

注:

QRadar は、イベント・コレクターごとに 1 つの Juniper Networks SRX シリーズ・アプライアンスからの PCAP データのみの受信をサポートします。

パケット・キャプチャーの構成の詳細については、ご使用の *Juniper Networks Junos OS* の資料 を参照してください。

これで、QRadar で新しい Juniper Networks SRX ログ・ソースと PCAP プロトコルを構成する準備ができました。

関連タスク:

『PCAP を使用した新規 Juniper Networks SRX ログ・ソースの構成』
Juniper Networks SRX シリーズ・アプライアンスは、IBM Security QRadar により Juniper Junos OS プラットフォームとして自動的に検出されます。

PCAP を使用した新規 Juniper Networks SRX ログ・ソースの構成

Juniper Networks SRX シリーズ・アプライアンスは、IBM Security QRadar により Juniper Junos OS プラットフォームとして自動的に検出されます。

始める前に

オペレーティング・システムによっては、ログ・ソースが自動的に検出されたときに予期されるイベントが受信されない場合があります。ログ・ソースを手動で構成できます。

このタスクについて

QRadar は Syslog データを検出し、ログ・ソースを自動的に追加します。PCAP と Syslog を組み合わせたプロトコルを使用して、 PCAP データを Juniper SRX シリーズ・サービス・ゲートウェイのログ・ソースとして QRadar に追加できます。QRadar により Junos OS Syslog データが自動的に検出された後で「**PCAP と Syslog の組み合わせ (PCAP Syslog Combination)**」プロトコルを追加すると、ログ・ソースが既存のログ・ソース制限に追加されます。既存の Syslog 項目を削除してから「**PCAP と Syslog の組み合わせ (PCAP Syslog Combination)**」プロトコルを追加すると、Syslog データと PCAP データの両方が 1 つのログ・ソースとして追加されます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**Juniper SRX シリーズ・サービス・ゲートウェイ**」を選択します。
7. 「プロトコル構成」リストで「**PCAP と Syslog の組み合わせ (PCAP Syslog Combination)**」を選択します。
8. 「ログ・ソース **ID**」に入力します。
9. 「着信 **PCAP** ポート **(Incoming PCAP Port)**」を入力します。

   ログ・ソースで「着信 **PCAP** ポート **(Incoming PCAP Port)**」パラメーターを構成するには、Juniper Networks SRX シリーズ・アプライアンスのインターフェースで構成した PCAP データの出力ポート・アドレスを入力します。.
10. 「保存」をクリックします。
11. Juniper Networks SRX シリーズ・アプライアンスの自動検出 Syslog のみの Junos OS ログ・ソースを選択します。
12. 「削除」をクリックします。

    ログ・ソース削除の確認ウィンドウが表示されます。
13. 「はい」をクリックします。

    Junos OS Syslog ログ・ソースが「ログ・ソース」リストから削除されます。「**PCAP と Syslog の組み合わせ (PCAP Syslog Combination)**」プロトコルがログ・ソース・リストに表示されます。
14. 「管理」タブで「変更のデプロイ」をクリックします。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Juniper Networks Secure Access

IBM Security QRadar 用の Juniper Networks Secure Access DSM は、syslog を使用してログインとセッションの情報を WebTrends Enhanced Log File (WELF) 形式で受け入れます。

QRadar を使用して Juniper SA と Juniper IC を統合することができます。

注**:** ご使用の Juniper デバイスがリリース 5.5R3-HF2 から 6.1 以上を実行している場合、ロギングには WELF:WELF 形式を使用することを推奨します。ご使用のデバイスとライセンスが WELF:WELF 形式でのロギングをサポートしているかどうかを判断するには、ベンダー資料を参照してください。

この資料では、以下のいずれかの形式を使用して Juniper Secure Access デバイスを統合する情報を提供します。

- WELF:WELF 形式については、『WELF:WELF フォーマットの使用』を参照してください。
- Syslog については、 629 ページの『Syslog フォーマットの使用』を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

WELF:WELF フォーマットの使用

WELF:WELF フォーマットを使用して、Juniper Networks Secure Access デバイスと IBM Security QRadar を統合できます。

手順

1. Juniper デバイス管理ユーザー・インターフェースにログインします。

   ```
   https://10.xx.xx.xx/admin
   ```

   イベントの Syslog サーバー情報を構成するには、以下の手順に従います。
2. 左側のペインから「システム **(System)**」 > 「ログ**/**モニタリング **(Log/Monitoring)**」 > 「イベント **(Events)**」 > 「フィルター **(Filter)**」を選択します。
3. 「新規フィルター **(New Filter)**」をクリックします。

4. 「**WELF**」を選択します。
5. 「変更の保存 **(Save Changes)**」をクリックします。
6. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「イベント **(Events)**」 > 「設定 **(Settings)**」を選択します。
7. 「ログに記録するイベントの選択 (Select Events to Log)」ペインで、ログに記録するイベントを選択します。
8. 「サーバー名/**IP (Server name/IP)**」フィールドに、Syslog サーバーの名前または IP アドレスを入力します。
9. 「ファシリティー **(Facility)**」リストでファシリティーを選択します。
10. 「フィルター **(Filter)**」リストで「**WELF:WELF**」を選択します。
11. 「追加 **(Add)**」をクリックし、「変更の保存 **(Save Changes)**」をクリックします。

    ユーザー・アクセスの Syslog サーバー情報を構成するには、以下の手順に従います。
12. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「ユーザー・アクセス **(User Access)**」 > 「フィルター **(Filter)**」を選択します。
13. 「新規フィルター **(New Filter)**」をクリックします。
14. 「**WELF**」を選択します。「変更の保存 **(Save Changes)**」をクリックします。
15. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「ユーザー・アクセス **(User Access)**」 > 「設定 **(Settings)**」を選択します。
16. 「ログに記録するイベントの選択 (Select Events to Log)」ペインで、ログに記録するイベントを選択します。
17. 「サーバー名/**IP (Server name/IP)**」フィールドに、Syslog サーバーの名前または IP アドレスを入力します。
18. 「ファシリティー (Facility)」リストでファシリティーを選択します。
19. 「フィルター **(Filter)**」リストで「**WELF:WELF**」を選択します。
20. 「追加 **(Add)**」をクリックし、「変更の保存 **(Save Changes)**」をクリックします。

    管理者アクセスの Syslog サーバー情報を構成するには、以下の手順に従います。
21. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「管理者アクセス **(Admin Access)**」 > 「フィルター **(Filter)**」を選択します。
22. 「新規フィルター **(New Filter)**」をクリックします。
23. 「**WELF**」を選択します。
24. 「変更の保存 **(Save Changes)**」をクリックします。

25. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「管理者アクセス **(Admin Access)**」 > 「設定 **(Settings)**」を選択します。
26. 「ログに記録するイベントの選択 (Select Events to Log)」ペインで、ログに記録するイベントを選択します。
27. 「サーバー名/**IP (Server name/IP)**」フィールドに、Syslog サーバーの名前または IP アドレスを入力します。
28. 「ファシリティー **(Facility)**」リストでファシリティーを選択します。
29. 「フィルター **(Filter)**」リストで「**WELF:WELF**」を選択します。
30. 「追加 **(Add)**」をクリックし、「変更の保存 **(Save Changes)**」をクリックします。

    クライアント・ログの Syslog サーバー情報を構成するには、以下の手順に従います。
31. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「クライアント・ログ **(Client Logs)**」 > 「フィルター **(Filter)**」を選択します。

    「フィルター **(Filter)**」メニューが表示されます。
32. 「新規フィルター **(New Filter)**」をクリックします。
33. 「**WELF**」を選択します。「変更の保存 **(Save Changes)**」をクリックします。
34. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「クライアント・ログ **(Client Logs)**」 > 「設定 **(Settings)**」を選択します。
35. 「ログに記録するイベントの選択 (Select Events to Log)」ペインで、ログに記録するイベントを選択します。
36. 「サーバー名/**IP (Server name/IP)**」フィールドに、Syslog サーバーの名前または IP アドレスを入力します。
37. 「ファシリティー **(Facility)**」リストでファシリティーを選択します。
38. 「フィルター (Filter)」リストで「**WELF:WELF**」を選択します。
39. 「追加 **(Add)**」をクリックし、「変更の保存 **(Save Changes)**」をクリックします。

    これで、ログ・ソースを構成することができます。

Juniper Networks Secure Access デバイスからイベントを受信するための QRadar の構成

Juniper Networks Secure Access デバイスからイベントを受信するように IBM Security QRadar を構成できます。

手順

「ログ・ソース・タイプ」リストで「**Juniper Networks Secure Access (SA) SSL VPN**」を選択します。
Juniper デバイスについて詳しくは、ベンダーの資料を参照してください。

Syslog フォーマットの使用

Syslog 形式を使用して Juniper Networks Secure Access デバイスと IBM Security QRadar を統合できます。

手順

1. Juniper デバイス管理ユーザー・インターフェースにログインします。

   ```
   https://10.xx.xx.xx/admin
   ```

   イベントの Syslog サーバー情報を構成するには、以下の手順に従います。
2. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「イベント **(Events)**」 > 「設定 **(Settings)**」を選択します。
3. 「ログに記録するイベントの選択 **(Select Events to Log)**」セクションで、ログに記録するイベントを選択します。
4. 「サーバー名/**IP (Server name/IP)**」フィールドに、Syslog サーバーの名前または IP アドレスを入力します。

   ユーザー・アクセスの Syslog サーバー情報を構成するには、以下の手順に従います。
5. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「ユーザー・アクセス **(User Access)**」 > 「設定 **(Settings)**」を選択します。
6. 「ログに記録するイベントの選択 **(Select Events to Log)**」セクションで、ログに記録するイベントを選択します。
7. 「サーバー名/**IP (Server name/IP)**」フィールドに、Syslog サーバーの名前または IP アドレスを入力します。

   管理者アクセスの Syslog サーバー情報を構成するには、以下の手順に従います。
8. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「管理者アクセス **(Admin Access)**」 > 「設定 **(Settings)**」を選択します。
9. 「ログに記録するイベントの選択 **(Select Events to Log)**」セクションで、ログに記録するイベントを選択します。
10. 「サーバー名/**IP (Server name/IP)**」フィールドに、Syslog サーバーの名前または IP アドレスを入力します。

    クライアント・ログの Syslog サーバー情報を構成するには、以下の手順に従います。
11. 左側のペインから「システム **(System)**」 > 「ログ/モニタリング **(Log/Monitoring)**」 > 「クライアント・ログ **(Client Logs)**」 > 「設定 **(Settings)**」を選択します。
12. 「ログに記録するイベントの選択 **(Select Events to Log)**」セクションで、ログに記録するイベントを選択します。
13. 「サーバー名/**IP (Server name/IP)**」フィールドに、Syslog サーバーの名前または IP アドレスを入力します。

次のタスク

これで、QRadar でログ・ソースを構成する準備ができました。

Juniper Networks Security Binary Log Collector

IBM Security QRadar 用の Juniper Security Binary Log Collector DSM は、Juniper SRX アプライアンスまたは Juniper Networks J Series アプライアンスから、監査、システム、ファイアウォール、および侵入防止システム (IPS) の各イベントをバイナリー形式で受け入れることができます。

Juniper Networks バイナリー・ログ・ファイルの形式は、大量のデータがイベント・ログに送信される際のパフォーマンスの向上が意図されています。ご使用のデバイスを QRadar と統合するには、バイナリー形式のイベントをストリームするようにご使用の Juniper アプライアンスを構成してから、QRadar のログ・ソースを構成する必要があります。

以下のトピックを参照してください。

- 『Juniper Networks バイナリー・ログ・フォーマットの構成』
- 631 ページの『ログ・ソースの構成』

Juniper Networks バイナリー・ログ・フォーマットの構成

Juniper SRX または J シリーズ・アプライアンスのバイナリー・ログ・フォーマットは、UDP プロトコルを使用して IBM Security QRadar にストリーミングされます。QRadar の標準 Syslog ポートはバイナリー・フォーマットのイベントを認識できないため、バイナリー・フォーマットのイベントのストリーミングのために固有のポートを指定する必要があります。

このタスクについて

Juniper アプライアンスからのストリーミング・バイナリー・イベントの受信用として QRadar に割り当てられているデフォルト・ポートは、ポート 40798 です。

注: Juniper Binary Log Collector DSM では、ストリーム・モードで転送されたイベントだけがサポートされます。イベント・モードはサポートされていません。

手順

1. コマンド・ライン・インターフェース (CLI) を使用して Juniper SRX または J シリーズにログインします。
2. 以下のコマンドを入力して、デバイス構成を編集します。

   ```
   configure
   ```

3. 以下のコマンドを入力して、ストリーミング・バイナリー・フォーマットのイベントのための IP アドレスとポート番号を構成します。

   ```
   set security log stream <Name> host <IP address> port <Port>
   ```

   各部分について以下で説明します。

   - *<Name>* は、ストリームに割り当てられる名前です。

- *<IP address>* は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
- *<Port>* は、ストリーミング・バイナリー・フォーマットのイベント用として QRadar に割り当てられる固有のポート番号です。デフォルトでは、QRadar はポート 40798 でバイナリー・ストリーミング・データを listen します。*QRadar* が使用するポートのリストについては、IBM Security QRadar の「*Common Ports List technical note*」を参照してください。

4. 以下のコマンドを入力して、セキュリティー・ログ・フォーマットをバイナリーに設定します。

   ```
   set security log stream <Name> format binary
   ```

   ここで *<Name>* は、 630 ページの『Juniper Networks バイナリー・ログ・フォーマットの構成』でバイナリー・フォーマット・ストリームに指定した名前です。
5. 以下のコマンドを入力して、セキュリティー・ログ・ストリーミングを有効にします。

   ```
   set security log mode stream
   ```
6. 以下のコマンドを入力して、イベント・ストリームの送信元 IP アドレスを設定します。

   ```
   set security log source-address <IP address>
   ```

   ここで *<IP address>* は、Juniper SRX シリーズまたは Juniper J シリーズ・アプライアンスの IP アドレスです。
7. 以下のコマンドを入力して、構成の変更内容を保存します。

   ```
   commit
   ```
8. 以下のコマンドを入力して、構成モードを終了します。

   ```
   exit
   ```

次のタスク

Juniper SRX または J シリーズ・アプライアンスの構成は完了です。これで、QRadar でログ・ソースを構成できるようになりました。

ログ・ソースの構成

IBM Security QRadar では、Juniper SRX または Juniper J シリーズ・アプライアンスから受信する Juniper Security Binary Log Collector イベントは自動的に検出されません。

このタスクについて

イベントが自動的に検出されない場合は、QRadar の「管理」タブを使用してログ・ソースを手動で作成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Juniper Security Binary Log Collector**」を選択します。
9. 「プロトコル構成」リストで「**Juniper Security Binary Log Collector**」を選択します。
10. 以下の値を構成します。

表 *237. Juniper Security Binary Log Collector* のプロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースを識別する IP アドレスまたはホスト名を入力します。識別子アドレスは、バイナリー・イベント・ストリームを生成する Juniper SRX または J シリーズ・アプライアンスです。
バイナリー・コレクター・ポート	Juniper Networks SRX または J シリーズ・アプライアンスが着信バイナリー・データを QRadar に転送するために使用するポート番号を指定します。バイナリー・データ用の UDP ポート番号は、 630 ページの『Juniper Networks バイナリー・ログ・フォーマットの構成』で構成するポートと同じです。 Juniper Networks SRX または J シリーズ・アプライアンスからのバイナリー・イベント・ストリーム用の出力ポート番号を編集する場合、Juniper ログ・ソースを編集し、QRadar の「バイナリー・コレクター・ポート **(Binary Collector Port)**」パラメーターを更新する必要もあります。 ポートを編集するには、以下のようにします。 1. 「バイナリー・コレクター・ポート **(Binary Collector Port)**」フィールドに、バイナリー・イベント・データ受信用の新しいポート番号を入力します。 2. 「保存」をクリックします。 3. 「管理」タブで「拡張」 > 「すべての構成のデプロイ」をクリックします。 ポートの更新が完了し、新しいポート番号でイベント収集が開始されます。 QRadar を完全にデプロイするまで、ログ・ソースのイベント収集は停止されます。 4. 「すべての構成のデプロイ」をクリックすると、QRadar はすべてのサービスを再開します。このため、デプロイが完了するまで、イベントとフローのデータ収集にギャップが生じます。

表 237. *Juniper Security Binary Log Collector* のプロトコル・パラメーター (続き)

パラメーター	説明
XML テンプレート・ファイルのロケーション	Juniper SRX または Juniper J シリーズ・アプライアンスからのバイナリー・ストリームのデコードに使用する XML ファイルのパスを入力します。 デフォルトでは、QRadar ではバイナリー・ストリームのデコード用 XML テンプレート・ファイルが以下のディレクトリーに格納されています。 `/opt//conf/security_log.xml`

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。「ログ・アクティビティー」タブでイベントを表示して、QRadar に転送されたイベントを確認できます。

Juniper Networks Steel-Belted Radius

IBM Security QRadar 用の Juniper Steel-Belted Radius DSM は、Windows または Linux 上で WinCollect ユーティリティーまたは Adaptive Log Exporter ユーティリティーを実行するクライアントからの syslog イベントを syslog を使用して受け入れます。

QRadar は、成功したログイン試行も失敗したログイン試行もすべて記録します。以下のいずれかのメソッドを使用することで、Juniper Networks Steel-Belted Radius を QRadar と統合できます。

- Microsoft Windows オペレーティング・システム上で WinCollect または Adaptive Log Exporter を使用するように Juniper Steel Belted-Radius を構成します。詳しくは、『Adaptive Log Exporter での Juniper Steel-Belted Radius の構成』または「*IBM Security QRadar WinCollect* ユーザー・ガイド」を参照してください。
- Linux ベースのオペレーティング・システム上で syslog を使用することで Juniper Steel-Belted Radius を構成します。詳しくは、 635 ページの『Syslog 用の Juniper Steel-Belted Radius の構成』を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Adaptive Log Exporter での Juniper Steel-Belted Radius の構成

Adaptive Log Exporter を使用して Juniper Steel-Belted Radius DSM を IBM Security QRadar と統合できます。

手順

1. 「スタート」メニューで「プログラム」 > 「**Adaptive Log Exporter**」 > 「**Adapter Log Exporter** の構成 **(Configure Adapter Log Exporter)**」をクリックします。

   Adaptive Log Exporter は Juniper SBR システムと同じシステムにインストールされている必要があります。Juniper SBR デバイス・プラグインを組み込むため、Adaptive Log Exporter を更新する必要があります。詳細については、「*Adaptive Log Exporter Users Guide*」を参照してください。
2. 「デバイス **(Devices)**」タブをクリックします。
3. 「**Juniper SBR**」を選択し、右クリックして「デバイスの追加 **(Add Device)**」を選択します。

   「Juniper SBR の新規プロパティー (New Juniper SBR Properties)」ウィンドウが表示されます。
4. 以下のパラメーターを構成します。

表 *238. Juniper SBR* のプロパティー

パラメーター	説明
名前	デバイスの名前を入力します。この名前には、英数字と下線 (_) を使用できます。
説明	このデバイスの説明を入力します。
デバイス・アドレス (Device Address)	デバイスの IP アドレスまたはホスト名を入力します。この IP アドレスまたはホスト名を使用して、QRadar に転送される Syslog メッセージでデバイスが識別されます。このアドレスは、QRadar に示される IP アドレスまたはホスト名です。
ルート・ログ・ディレクトリー (Root Log Directory)	Juniper SBR がログ・ファイルを保存する場所を指定します。レポート・ログ・ファイルは Steel-Belted Radius のディレクトリー `<radiusdir>¥authReports` にあります。Adaptive Log Exporter はルート・ログ・ディレクトリーをモニターし、ファイル名のタイム・スタンプが現在の日付に一致する `.CSV` ファイルを検出します。

5. 「**Adaptive Log Exporter**」ツールバーで「保存 **(Save)**」をクリックします。
6. 「**Adaptive Log Exporter**」ツールバーで「デプロイ **(Deploy)**」をクリックします。

   注**:** Juniper Steel-Belted Radius アプライアンスではログ・ファイル・ヘッダーにデフォルト値を使用する必要があります。ログ・ファイル・ヘッダーがデフォルト値以外の値に変更されており、QRadar が SBR イベントを適切に解析しない場合は、お客様サポートにご連絡ください。
7. これで、QRadar でログ・ソースを構成する準備ができました。

   Adaptive Log Exporter から受信する Juniper SBR イベントは、QRadar により自動的に検出されます。Juniper Steel-Belted Radius からのイベントを受信するように QRadar を手動で構成するには、以下の手順に従います。

「ログ・ソース・タイプ」ドロップダウン・ボックスで「**Juniper Steel-Belted Radius**」オプションを選択します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Syslog 用の Juniper Steel-Belted Radius の構成

Linux ベースのオペレーティング・システムで syslog を使用して Juniper Steel-Belted Radius DSM を IBM Security QRadar と統合できます。

手順

1. SSH を使用して、root ユーザーとして Juniper Steel-Belted Radius デバイスにログインします。
2. 以下のファイルを編集します。

   ```
   /etc/syslog.conf
   ```
3. 以下の情報を追加します。

   ```
   <facility>.<priority>@<IP address>
   ```

   各部分について以下で説明します。

   - *<facility>* は、syslog のファシリティーです (例: local3)。
   - *<priority>* は、syslog の優先順位です (例: info)。
   - *<IP address>* は QRadar の IP アドレスです。
4. ファイルを保存します。
5. コマンド・ラインで、以下のコマンドを入力して syslog を再始動します。

   ```
   service syslog restart
   ```
6. これで、QRadar でログ・ソースを構成できるようになりました。

   Juniper Steel-Belted Radius からイベントを受信するように QRadar を構成するには、以下のようにします。

   「ログ・ソース・タイプ」リストで「**Juniper Steel-Belted Radius**」オプションを選択します。

   Steel-Belted Radius サーバーの構成について詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Juniper Networks vGW Virtual Gateway

IBM Security QRadar 用の Juniper Networks vGW Virtual Gateway DSM は、vGW 管理サーバーまたはファイアウォールから NetFlow と Syslog を使用してイベントを受け取ります。

このタスクについて

QRadar は、すべての関連イベント (管理、ポリシー、IDS ログ、ファイアウォール・イベントなど) を記録します。QRadar で Juniper Networks vGW Virtual Gateway を構成する前に、Syslog イベントを転送するように vGW を構成する必要があります。

手順

1. Juniper Networks vGW のユーザー・インターフェースにログインします。
2. 「設定 **(Settings)**」を選択します。
3. 「セキュリティー設定 **(Security Settings)**」から「グローバル **(Global)**」を選択します。
4. 「外部ロギング **(External Logging)**」から次のいずれかのオプションを選択します。
   - **vGW** 管理サーバーから **Syslog** を送信する **(Send Syslog from vGW management server)** - 管理サーバーから提供される Syslog イベントを中央でログに記録します。
   - ファイアウォールから **Syslog** を送信する **(Send Syslog from Firewalls)** - Syslog イベントを提供する各ファイアウォール・セキュリティー VM を使用して分散型でロギングを実行します。

   「**vGW** 管理サーバーから **Syslog** を送信する **(Send Syslog from vGW management server)**」オプションを選択すると、QRadar に転送されるすべてのイベントには、vGW 管理サーバーの IP アドレスが含まれます。
5. 以下のパラメーターの値を入力します。

表 *239. Syslog* パラメーター

パラメーター	説明
Syslog サーバー	「**vGW** 管理サーバーから **Syslog** を送信する **(Send Syslog from vGW management server)**」を選択した場合は、vGW 管理サーバーの IP アドレスを入力します。「ファイアウォールから **Syslog** を送信する **(Send Syslog from Firewalls)**」を選択した場合は、QRadar の IP アドレスを入力します。
Syslog サーバー・ポート **(Syslog Server Port)**	Syslog のポート・アドレスを入力します。通常、このポートは 514 です。

6. 「外部ロギング (External Logging)」ペインで「保存 **(Save)**」をクリックします。

「保存 **(Save)**」をクリックすると、「外部ロギング **(External Logging)**」セクションで行った変更だけが保存されます。NetFlow に対して行った変更はすべて、「**NetFlow** 構成 **(NetFlow Configuration)**」セクション内のボタンを使用して保存する必要があります。

7. 「NetFlow 構成 (NetFlow Configuration)」ペインで、「有効 **(enable)**」チェック・ボックスを選択します。

   NetFlow では、vGW 管理サーバーからの中央でのロギングはサポートされていません。「外部ロギング **(External Logging)**」セクションで、「ファイアウォールから **Syslog** を送信する **(Send Syslog from Firewalls)**」オプションを選択する必要があります。

8. 以下のパラメーターの値を入力します。

表 240. Netflow パラメーター

パラメーター	説明
NetFlow コレクター・アドレス **(NetFlow collector address)**	QRadar の IP アドレスを入力します。
Syslog サーバー・ポート **(Syslog Server Port)**	NetFlow イベントのポート・アドレスを入力します。

   注**:** QRadar は通常、QFlow Collector の NetFlow イベント・データにポート 2055 を使用します。Juniper Networks vGW Series Virtual Gateway for NetFlow では異なる NetFlow コレクター・ポートを構成する必要があります。

9. 「**NetFlow** 構成 **(NetFlow Configuration)**」で「保存 **(Save)**」をクリックします。
10. これで、QRadar でログ・ソースを構成できるようになりました。

    QRadar は、Juniper Networks vGW から転送された Syslog イベントを自動的に検出します。Syslog イベントを受信するように QRadar を手動で構成するには、以下の手順に従います。

    「ログ・ソース・タイプ」リストで「**Juniper vGW**」を選択します。

    詳しくは、*Juniper Networks vGW* の資料を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Juniper Networks Junos WebApp Secure

IBM Security QRadar 用の Juniper WebApp Secure DSM は、Juniper Junos WebApp Secure アプライアンスから転送されたイベントを syslog を使用して受け入れます。

Juniper Junos WebApp Secure は、QRadar に対してインシデント・ロギング・イベントおよびアクセス・ロギング・イベントを提供します。QRadar でイベントを受信する前に、ご使用の Juniper Junos WebApp Secure でイベント転送を構成してから、転送するイベントを定義する必要があります。

Syslog の転送の構成

Juniper Junos WebApp Secure のリモート Syslog サーバーを構成するには、SSH を使用して構成インターフェースに接続する必要があります。構成インターフェースを使用して、Juniper Junos WebApp Secure アプライアンスのセットアップまたはコア設定の構成を行うことができます。

手順

1. ポート 2022 で SSH を使用して、Juniper Junos WebApp デバイスにログインします。

   `https://<IP address>:<port>`

   各部分について以下で説明します。

   - *<IP address>* は、Juniper Junos WebApp Secure アプライアンスの IP アドレスです。
   - *<Port>* は、Juniper Junos WebApp Secure アプライアンスの構成インターフェースのポート番号です。

   デフォルトの SSH 構成ポートは 2022 です。
2. 「ツールの選択 **(Choose a Tool)**」メニューで「ロギング **(Logging)**」を選択します。
3. 「ツールの実行 **(Run Tool)**」をクリックします。
4. 「ログの宛先 **(Log Destination)**」メニューで「リモート **Syslog** サーバー **(Remote Syslog Server)**」を選択します。
5. 「**Syslog** サーバー **(Syslog Server)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
6. 「保存」をクリックします。
7. 「ツールの選択 **(Choose a Tool)**」メニューで「終了 **(Quit)**」を選択します。
8. `Exit` と入力して SSH セッションを終了します。

次のタスク

これで、Juniper Junos WebApp Secure アプライアンスでイベント・ロギングを構成する準備ができました。

イベント・ロギングの構成

IBM Security QRadar に転送するログを決定するように Juniper Junos WebApp Secure アプライアンスを構成する必要があります。

手順

1. Web ブラウザーを使用して Juniper Junos WebApp Secure アプライアンスの構成サイトにログインします。

   `https://<IP address>:<port>`

   各部分について以下で説明します。

   - *<IP address>* は、Juniper Junos WebApp Secure アプライアンスの IP アドレスです。
   - *<Port>* は、Juniper Junos WebApp Secure アプライアンスのポート番号です。

     デフォルトの構成ではポート番号 5000 が使用されます。
2. ナビゲーション・メニューで、「構成マネージャー **(Configuration Manager)**」を選択します。
3. 構成メニューで「基本モード **(Basic Mode)**」を選択します。
4. 「グローバル構成 **(Global Configuration)**」タブをクリックし、「ロギング **(Logging)**」を選択します。
5. 「詳細オプションを表示 **(Show Advanced Options)**」リンクをクリックします。
6. 以下のパラメーターを構成します。

表 241. Juniper Junos WebApp Secure のロギング・パラメーター

パラメーター	説明
アクセス・ロギング: ログ・レベル **(Access logging: Log Level)**	アクセス・ロギングが有効な場合にログに記録する情報のレベルを構成するには、このオプションをクリックします。 このオプションには次のレベルがあります。 • **0** - アクセス・ロギングは無効です。 • **1** - 基本ロギング。 • **2** - ヘッダーを含む基本ロギング。 • **3** - ヘッダーと本文を含む基本ロギング。 **注:** アクセス・ロギングはデフォルトでは無効になっています。アクセス・ロギングはデバッグ目的でのみ有効にすることをお勧めします。詳しくは、*Juniper Junos WebApp Secure* の資料を参照してください。
アクセス・ロギング: 処理前に要求をログに記録する **(Access logging: Log requests before processing)**	このオプションをクリックして「**True**」を選択すると、要求が処理前にログに記録され、その後イベントが QRadar に転送されます。

表 241. *Juniper Junos WebApp Secure* のロギング・パラメーター (続き)

パラメーター	説明
アクセス・ロギング: 処理後に要求をアクセス・ログに記録する **(Access logging: Log requests to access log after processing)**	このオプションを選択して「**True**」を選択すると、要求が処理後にログに記録されます。Juniper Junos WebApp Secure によりイベントが処理された後で、イベントが QRadar に転送されます。
アクセス・ロギング: 処理後に応答をアクセス・ログに記録する **(Access logging: Log responses to access log after processing)**	このオプションを選択して「**True**」を選択すると、応答が処理後にログに記録されます。Juniper Junos WebApp Secure によりイベントが処理された後で、イベントが QRadar に転送されます。
アクセス・ロギング: 処理前に応答をアクセス・ログに記録する **(Access logging: Log responses to access log before processing)**	このオプションをクリックして「**True**」を選択すると、応答が処理前にログに記録され、その後イベントが QRadar に転送されます。
インシデント重大度ログ・レベル **(Incident severity log level)**	ログに記録するインシデント・イベントの重大度を定義するには、このオプションをクリックします。定義したレベル以上のインシデントはすべて QRadar に転送されます。 このオプションには次のレベルがあります。 • **0** - 「通知 (Informational)」レベル以上のインシデント・イベントがログに記録され、転送されます。 • **1** - 「疑わしい振る舞い (Suspicious)」レベル以上のインシデント・イベントがログに記録され、転送されます。 • **2** - 「低 (Low)」レベル以上のインシデント・イベントがログに記録され、転送されます。 • **3** - 「中 (Medium)」レベル以上のインシデント・イベントがログに記録され、転送されます。 • **4** - 「高 (High)」レベル以上のインシデント・イベントがログに記録され、転送されます。
Syslog にインシデントを記録する **(Log incidents to the syslog)**	このオプションをクリックして「はい **(Yes)**」を選択すると、QRadar への Syslog の転送が有効になります。

構成は完了です。Juniper Junos WebApp Secure イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Juniper Junos WebApp Secure により QRadar に転送されるイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は Juniper Junos WebApp Secure からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

手順

1. IBM Security QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Juniper Junos WebApp Secure**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 242. Syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Juniper Junos WebApp Secure アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

Juniper Networks WLC シリーズ無線 LAN コントローラー

IBM Security QRadar は、Juniper Networks WLC シリーズ無線 LAN コントローラーからの syslog イベントを収集して分類することができます。

syslog イベントを収集するには、syslog イベントを QRadar に転送するようにご使用の Juniper Networks 無線 LAN コントローラーを構成する必要があります。管理者は RingMaster インターフェースまたはコマンド・ラインインターフェースのいずれかを使用して、Juniper Networks 無線 LAN コントローラー・アプライアンスの syslog 転送を構成できます。QRadar は、Juniper Networks WLC 士リース無線 LAN コントローラーから転送された syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。QRadar は、Mobility System Software (MSS) V7.6 上で実行される Juniper WLAN デバイスからの syslog イベントをサポートします。

Juniper WLC イベントを QRadar と統合するために、管理者は以下のタスクを実行できます。

1. ご使用の Juniper WLAN アプライアンスで、syslog サーバーを構成します。
2. 以下のいずれかのメソッドを使用します。

- RingMaster ユーザー・インターフェースを使用して syslog サーバーを構成するには、『Juniper WLC ユーザー・インターフェースからの Syslog サーバーの構成』を参照してください。
- コマンド・ライン・インターフェースを使用して syslog サーバーを構成するには、 643 ページの『Juniper WLC のコマンド・ライン・インターフェースを使用した Syslog サーバーの構成』を参照してください。

3. QRadar システムで、転送されたイベントが自動的に検出されることを確認します。

Juniper WLC ユーザー・インターフェースからの Syslog サーバーの構成

イベントを収集するには、Juniper WLC システムで Syslog サーバーが Syslog イベントを IBM Security QRadar に転送するように構成する必要があります。

手順

1. RingMaster ソフトウェアにログインします。
2. 「オーガナイザー **(Organizer)**」パネルで、無線 LAN コントローラーを選択します。
3. 「システム (System)」パネルで「ログ **(Log)**」を選択します。
4. 「タスク (Task)」パネルで「**Syslog** サーバーの作成 **(Create Syslog Server)**」を選択します。
5. 「**Syslog** サーバー **(Syslog Server)**」フィールドに、QRadar システムの IP アドレスを入力します。
6. 「ポート **(Port)**」フィールドに 514 を入力します。
7. 「重大度フィルター **(Severity Filter)**」リストで重大度を選択します。

   重大度がデバッグのイベントをログに記録すると、Juniper WLC アプライアンスのシステム・パフォーマンスに悪影響を及ぼす可能性があります。管理者は、エラーまたは警告の重大度レベルでイベントをログに記録し、必要なデータを取得するためにレベルを徐々に上げていくことが推奨されます。デフォルトの重大度レベルはエラーです。
8. 「ファシリティー・マッピング **(Facility Mapping)**」リストで、local 0 から local 7 までのいずれかのファシリティーを選択します。
9. 「終了」をクリックします。

   Juniper WLC アプライアンスにより生成されたイベントは、指定した Syslog 宛先に転送されます。十分な数のイベントが QRadar に転送された後、ログ・ソースが自動的に検出されます。通常、ログ・ソースの自動検出に必要なイベントの最小数は 25 です。

次のタスク

管理者は QRadar コンソールにログインして、QRadar コンソールでログ・ソースが作成されていることを確認できます。「ログ・アクティビティー」タブに、Juniper WLC アプライアンスからのイベントが表示されます。

Juniper WLC のコマンド・ライン・インターフェースを使用した Syslog サーバーの構成

イベントを収集するには、Juniper WLC システムで Syslog サーバーが Syslog イベントを IBM Security QRadar に転送するように構成します。

手順

1. Juniper WLC アプライアンスのコマンド・ライン・インターフェースにログインします。
2. Syslog サーバーを構成するため、以下のコマンドを入力します。
3. 構成を保存するため、以下のコマンドを入力します。

   ```
   save configuration
   ```

   Juniper WLC アプライアンスにより生成されたイベントは、指定した Syslog 宛先に転送されます。十分な数のイベントが QRadar に転送された後、ログ・ソースが自動的に検出されます。通常、ログ・ソースの自動検出に必要なイベントの最小数は 25 です。

次のタスク

管理者は QRadar コンソールにログインして、ログ・ソースが作成されていることを確認できます。「ログ・アクティビティー」タブに、Juniper WLC アプライアンスからのイベントが表示されます。

第 73 章 Kaspersky Security Center

IBM Security QRadar DSM for Kaspersky Security Center は、Kaspersky Security Center アプライアンスのデータベースから直接イベントを取得できるほか、syslog を使用してアプライアンスからイベントを受信することもできます。

以下の表は、Kaspersky Security Center DSM の仕様を示しています。

表 243. *Kaspersky Security Center DSM* の仕様

仕様	値
製造元	Kaspersky
DSM 名	Kaspersky Security Center
RPM ファイル名	`DSM-KasperskySecurityCenter-`*`Qradar_version-build_number`*`.noarch.rpm`
プロトコル	JDBC: バージョン 9.2-10.1 Syslog LEEF: バージョン 10.1 以降
記録されるイベント・タイプ	アンチウィルス サーバー 監査
自動的に検出?	JDBC プロトコルを使用する場合は行われません。 syslog プロトコルを使用する場合は行われます。
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Kaspersky Web サイト (http://www.kaspersky.com)

Kaspersky Security Center イベントを QRadar に送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - Kaspersky Security Center DSM
2. 次のオプションのいずれかを選択してください。
   - syslog を使用する場合は、イベントを QRadar に転送するように Kaspersky Security Center を構成します。
   - JDBC プロトコルを使用する場合は、Kaspersky Security Center デバイスにデータベース・ビューを作成します。

3. QRadar コンソールで、Kaspersky Security Center ログ・ソースを作成します。すべての必須パラメーターを構成します。以下の表を使用して、Kaspersky Security Center イベントの収集に必要な固有の値を構成してください。
   - syslog を使用する場合は、以下のパラメーターを構成します。

表 244. *Kaspersky Security Center の syslog* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Kaspersky Security Center
プロトコル構成	Syslog

   - JDBC を使用する場合は、以下のパラメーターを構成します。

表 245. *Kaspersky Security Center JDBC* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Kaspersky Security Center
プロトコル構成	JDBC
ログ・ソース ID	以下の形式を使用します。 <*Kaspersky_Database*>@<*Server_Address*> ここで、<*Server_Address*> は Kaspersky データベース・サーバーの IP アドレスまたはホスト名です。
データベース・タイプ	MSDE
データベース名	KAV
IP またはホスト名	Kaspersky Security Center データベースをホストする SQL サーバーの IP アドレスまたはホスト名。
ポート	MSDE のデフォルト・ポートは 1433 です。有効化して、「ポート」フィールドで指定したポートを使用して通信できることを確認する必要があります。 JDBC 構成のポートは Kaspersky データベースのリスナー・ポートに一致していなければなりません。QRadar と通信できるように、Kaspersky データベースで着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして MSDE を使用するデータベース・インスタンスを定義する場合は、構成の「ポート」パラメーターをブランクのままにしておいてください。
テーブル名	dbo.events

関連概念:

17 ページの『JDBC プロトコルの構成オプション』
QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Kaspersky Security Center のデータベース・ビューの作成

監査イベント・データを収集するには、IBM Security QRadar がアクセスできる Kaspersky サーバーにデータベース・ビューを作成する必要があります。

このタスクについて

データベース・ビューを作成するには、 Kaspersky から入手できる `klsql2.zip` ツールをダウンロードするか、またはデータベース・ビューを作成できる他のプログラムを使用します。以下の手順では、Kaspersky Labs ツールを使用して `dbo.events` ビューを作成するために必要なステップを説明します。

手順

1. Kaspersky Labs Web サイトから `klsql2.zip` ファイルをダウンロードします。

   http://support.kaspersky.com/9284
2. `klsql2.zip` を Kaspersky Security Center 管理サーバーにコピーします。
3. `klsql2.zip` を任意のディレクトリーに解凍します。
4. 以下のファイルが含まれています。
   - `klsql2.exe`
   - `src.sql`
   - `start.cmd`
5. 任意のテキスト・エディターで、`src.sql` ファイルを編集します。
6. `src.sql` ファイルの内容を消去します。
7. `dbo.events` データベース・ビューを作成する以下の Transact-SQL ステートメントを入力します。

   ```
   create view dbo.events as select e.nId, e.strEventType as 'EventId',
   e.wstrDescription as 'EventDesc', e.tmRiseTime as 'DeviceTime',
   h.nIp as 'SourceInt', e.wstrPar1, e.wstrPar2, e.wstrPar3,
   e.wstrPar4, e.wstrPar5, e.wstrPar6, e.wstrPar7, e.wstrPar8,
   e.wstrPar9 from dbo.v_akpub_ev_event e,
   dbo.v_akpub_host h where e.strHostname = h.strName;
   ```
8. `src.sql` ファイルを保存します。
9. コマンド・ラインから `klsql2` のファイルが格納されている場所にナビゲートします。
10. 以下のコマンドを入力して、Kaspersky Security Center アプライアンス上にビューを作成します。

    ```
    klsql2 -i src.sql -o result.xml
    ```

dbo.events ビューが作成されます。これで、Kaspersky Security Center イベントの確認のためにビューをポーリングするように QRadar でログ・ソースを構成することができます。

注: Kaspersky Security Center データベース管理者は、QRadar がイベントを確認するため、TCP ポート 1433 またはログ・ソースに対して設定されているポートを使用して、データベースをポーリングできるようにする必要があります。データベースではデフォルトでプロトコル接続が無効になっていることがよくあります。その場合、イベント・ポーリング用の接続を許可するために、追加の構成ステップが必要になります。Kaspersky Security Center と QRadar の間にファイアウォールが導入されている場合、イベント・ポーリング用のトラフィックを許可するようにそのファイアウォールを構成する必要もあります。

IBM Security QRadar でのログ・ソースの構成

QRadar では、Kaspersky Security Center データベースで作成したビューにアクセスするための適切な資格情報が割り当てられているユーザー・アカウントが必要です。

このタスクについて

Kaspersky Security Center データベースから監査データを適切にポーリングするには、新規ユーザーを作成するか、または dbo.events ビューからの読み取りのための既存のユーザー資格情報をログ・ソースに指定する必要があります。ユーザー・アカウントの作成について詳しくは、*Kaspersky Security Center* の資料を参照してください。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「**Kaspersky Security Center**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. 以下の値を構成します。

表 246. JDBC プロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<Kaspersky Database>@<Kaspersky Database Server IP or Host Name>* 各部分について以下で説明します。 • *<Kaspersky Database>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<Kaspersky Database Server IP or Host Name>* は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	Kaspersky Security Center データベースの名前として KAV を入力します。
IP またはホスト名	Kaspersky Security Center データベースをホストする SQL サーバーの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。 MSDE のデフォルト・ポートは 1433 です。ポートを使用可能にして、「ポート」フィールドで指定するポートを使用して通信できることを確認する必要があります。 JDBC 構成のポートは Kaspersky データベースのリスナー・ポートに一致していなければなりません。Kaspersky データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして「MSDE」を使用するときに「データベース・インスタンス **(Database Instance)**」を定義する場合は、構成の「ポート」パラメーターをブランクのままにする必要があります。
ユーザー名	ログ・ソースが Kaspersky データベースへのアクセスに使用できるユーザー名を入力します。
パスワード	ログ・ソースが Kaspersky データベースへのアクセスに使用できるパスワードを入力します。 パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」フィールドに入力したパスワードと同一である必要があります。
認証ドメイン	「データベース・タイプ」として「**MSDE**」を選択し、データベースが Windows 用に構成されている場合は、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。

表 246. JDBC プロトコル・パラメーター (続き)

パラメーター	説明
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックした場合は、構成内で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを含むテーブルまたはビューの名前として `dbo.events` と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに `*` を入力します。 ご使用の構成で必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	比較フィールドに `nld` と入力します。比較フィールドを使用して、テーブルに対する照会から次の照会までの間に追加されたい新しいイベントを特定できます。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
準備済みステートメントの使用 **(Use Prepared Statements)**	「準備済みステートメントの使用 **(Use Prepared Statements)**」チェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (作成したビューに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。

表 246. JDBC プロトコル・パラメーター (続き)

パラメーター	説明
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

注: 「信頼性」パラメーターに 5 よりも大きい値を選択すると、Kaspersky Security Center ログ・ソースに対し、QRadar の他のログ・ソースよりも高い重要度が設定されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

Kaspersky Security Center の構成は完了です。JDBC プロトコルを使用して収集されるイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

Kaspersky Security Center から QRadar への Syslog のエクスポート

Syslog イベントを IBM Security QRadar コンソールまたはイベント・コレクターに転送するように Kaspersky Security Center を構成します。

このタスクについて

Kaspersky Security Center は、管理サーバー、管理コンソール、およびネットワーク・エージェント・アプライアンスに登録されているイベントを転送できます。

手順

1. Kaspersky Security Center にログインします。
2. コンソール・ツリーで、「レポートと通知 **(Reports and notifications)**」フォルダーを展開します。
3. 「イベント」を右クリックして、「プロパティー」を選択します。
4. 「エクスポート・イベント」ペインで、「自動的にイベントを **SIEM** システム・データベースにエクスポートする **(Automatically export events to SIEM system database)**」チェック・ボックスを選択します。
5. 「**SIEM** システム **(SIEM system)**」リストで、「**QRadar**」を選択します。

6. QRadar コンソールまたはイベント・コレクターの IP アドレスとポートを入力します。
7. オプション: 履歴データを QRadar に転送するには、「アーカイブのエクスポート **(Export archive)**」をクリックし、履歴データをエクスポートします。
8. 「**OK**」をクリックします。

第 74 章 Kisco Information Systems SafeNet/i

Kisco Information Systems SafeNet/i 用の IBM Security QRadar DSM は、IBM iSeries システムからイベント・ログを収集します。

以下の表は、Kisco Information Systems SafeNet/i DSM の仕様を示しています。

表 247. *Kisco Information Systems SafeNet/i DSM* の仕様

仕様	値
製造元	Kisco Information Systems
DSM 名	Kisco Information Systems SafeNet/i
RPM ファイル名	DSM-KiscoInformationSystemsSafeNetI-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	V10.11
プロトコル	ログ・ファイル
記録されるイベント・タイプ	すべてのイベント
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Kisco Information Systems Web サイト (http://www.kisco.com/safenet/summary.htm)

Kisco Information Systems SafeNet/i イベントを収集するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - ログ・ファイル・プロトコル RPM
   - Kisco Information Systems SafeNet/i DSM RPM
2. QRadar と通信するように Kisco Information Systems SafeNet/i デバイスを構成します。
3. QRadar コンソールで、Kisco Information Systems SafeNet/i ログ・ソースを追加します。以下の表は、Kisco Information Systems SafeNet/i イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 248. *Kisco Information Systems SafeNet/i* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Kisco Information Systems SafeNet/i
プロトコル構成	ログ・ファイル
サービス・タイプ	FTP

表 248. *Kisco Information Systems SafeNet/i* ログ・ソース・パラメーター (続き)

パラメーター	値
リモート IP またはホスト名	Kisco Information Systems SafeNet/i デバイスの IP またはホスト名。
リモート・ポート	21
リモート・ユーザー	Kisco Information Systems SafeNet/i に QRadar 用に作成した iSeries ユーザー ID。
リモート・ディレクトリー	このフィールドは空のままにします。
FTP ファイル・パターン	.*
FTP 転送モード	BINARY
プロセッサー	NONE
イベント・ジェネレーター (Event Generator)	LINEBYLINE
ファイルのエンコード (File Encoding)	US-ASCII

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『QRadar との通信のための Kisco Information Systems SafeNet/i の構成』
SafeNet/i イベントを収集するには、Kisco Information Systems SafeNet/i を介して QRadar から FTP GET 要求を受け取るように IBM iSeries システムを構成します。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信のための Kisco Information Systems SafeNet/i の構成

SafeNet/i イベントを収集するには、Kisco Information Systems SafeNet/i を介して QRadar から FTP GET 要求を受け取るように IBM iSeries システムを構成します。

このタスクについて

FTP アクセス設定を構成するときには以下の表を使用します。

表 249. *FTP* アクセス設定

パラメーター	値
初期名前フォーマット (Initial Name Format)	*PATH
初期リスト・フォーマット (Initial List Format)	*UNIX
初期ライブラリー (Initial Library)	*USRPRF
初期ホーム・ディレクトリー・パス (Initial Home Directory Path)	IFS ディレクトリー

手順

1. IBM iSeries システム上に IFS ディレクトリーを作成します。
   a. IBM iSeries システムにログインします。
   b. Kisco Information Systems SafeNet/i QRadar アラート・ファイルを保持するための IFS ディレクトリーを作成します。

      例: `/SafeNet/QRadar/`
   c. SafeNet/i を介して IFS ディレクトリーに FTP でファイル転送するために使用する、QRadar のユーザー・プロファイルをセットアップします。

      例: `QRADARUSER`
2. QRadar ユーザー・プロファイルの FTP アクセスを構成します。
   a. Kisco Information Systems SafeNet/i にログインします。
   b. **GO SN7** と入力し、「サーバー・セキュリティーに対するユーザーを処理 **(Work with User to Server Security)**」を選択します。
   c. QRadar 用に作成したユーザー・プロファイル名 (`QRADARUSER` など) を入力します。
   d. **FTP Server Request Validation *FTPSERVER** サーバーと **FTP Server Logon *FTPLOGON3** サーバーについて 1 と入力します。
   e. F3 を押して、「**FTP** ステートメント・セキュリティーに対するユーザーを処理 **(Work with User to FTP Statement Security)**」を選択し、ユーザー・プロファイル名をもう一度入力します。
   f. 「ファイルのリスト **(List Files)**」および「ファイルの受信 **(Receiving Files)**」の FTP 操作タイプについて、1 と入力します。
   g. F4 を押して、ユーザーの FTP アクセス・パラメーターを構成します。654 ページの表 249を参照してください。
   h. F3 を押して、「長いパスに対するユーザーを処理 **(Work with User to Long Paths)**」を選択します。
   i. F6 を押して、IFS ディレクトリーのパスを指定します。

      パスの末尾にアスタリスクがあることを確認してください (例えば、`/SafeNet/QRadar/*`)。
   j. **R** 列の下に `X` と入力します。
   k. F3 を押して終了します。
3. `CHGRDRSET` と入力してから、F4 を押します。
4. 以下のパラメーターを構成します。

パラメーター	値
QRADAR 統合をアクティブにする **(Activate QRADAR Integration)**	はい
このホスト **ID (This Host Identifier)**	IBM iSeries デバイスの IP アドレスまたはホスト名。

パラメーター	値
QRADAR アラート・ファイルの **IFS** パス **(IFS Path to QRADAR Alert File)**	次の形式を使用します: `/SafeNet/QRadar/`

5. `CHGNOTIFY` と入力して、F4 を押します。
6. 以下のパラメーターを構成します。

パラメーター	値
アラート通知状況 **(Alert Notification Status)**	オン
アラートを要約する**? (Summarized Alerts?)**	はい

第 75 章 Lastline Enterprise

IBM Security QRadar DSM for Lastline Enterprise は、Lastline Enterprise システムからアンチマルウェア・イベントを受信します。

以下の表は、Lastline Enterprise DSM の仕様を示しています。

表 250. *Lastline Enterprise DSM* の仕様

仕様	値
製造元	Lastline
DSM 名	Lastline Enterprise
RPM ファイル名	`DSM-LastlineEnterprise-`*`Qradar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	6.0
プロトコル	LEEF
記録されるイベント・タイプ	アンチマルウェア
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Lastline Web サイト (http://www.lastline.com/platform/enterprise)

Lastline Enterprise イベントを QRadar に送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - Lastline Enterprise DSM RPM
2. Syslog イベントを QRadar に送信するように Lastline Enterprise デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Lastline Enterprise ログ・ソースを追加してください。以下の表は、固有の値を必要とするパラメーターを示しています。Lastline Enterprise イベントを収集するには、これらの値が必要です。

表 251. *Lastline Enterprise* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Lastline Enterprise
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインスト

ールしなければならないことがあります。

『QRadar と通信するように Lastline Enterprise を構成』
Lastline Enterprise システムにおいて、通知インターフェースで SIEM 設定を使用して、Lastline がイベントを送信できる SIEM アプライアンスを指定します。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するように Lastline Enterprise を構成

Lastline Enterprise システムにおいて、通知インターフェースで SIEM 設定を使用して、Lastline がイベントを送信できる SIEM アプライアンスを指定します。

手順

1. Lastline Enterprise システムにログインします。
2. サイドバーで「管理」をクリックします。
3. 「レポート **(Reporting)**」>「通知 **(Notifications)**」をクリックします。
4. 通知を追加するために、「通知の追加 **(Add a notification)**」 (+) アイコンをクリックします。
5. 「通知タイプ **(Notification Type)**」リストから「**SIEM**」を選択します。
6. 「SIEM サーバー設定 (SIEM Server Settings)」ペインで、QRadar コンソールまたはイベント・コレクターのパラメーターを構成します。「**SIEM** ログ・フォーマット **(SIEM Log Format)**」リストから「**LEEF**」を選択する必要があります。
7. 通知のトリガーを構成します。
   a. リスト内の既存のトリガーを編集するには、「トリガーの編集 **(Edit trigger)**」アイコンをクリックし、パラメーターを編集し、「トリガーの更新 **(Update Trigger)**」をクリックします。
   b. リストにトリガーを追加するには、「トリガーの追加 **(Add Trigger)**」 (+) アイコンをクリックしてパラメーターを構成し、「トリガーの追加 **(Add Trigger)**」をクリックします。
8. 「保存」をクリックします。

第 76 章 Lieberman Random Password Manager

Lieberman Random Password Manager DSM では、ログ拡張イベント・フォーマット (LEEF) の Syslog を使用して、IBM Security QRadar を Lieberman Enterprise Random Password Manager および Lieberman Random Password Manager ソフトウェアと統合できます。

このタスクについて

Lieberman Random Password Manager はポート 514 を使用して Syslog イベントを QRadar に転送します。QRadar は、関連するすべてのパスワード管理イベントを記録します。Syslog 転送の構成について詳しくは、ベンダーの資料を参照してください。

QRadar は、Lieberman Random Password Manager および Lieberman Enterprise Random Password Manager デバイスから転送された Syslog イベントを自動的に検出します。ただしこれらのデバイスからのイベントを受信するように QRadar を手動で構成する場合は、以下の手順に従います。

手順

「ログ・ソース・タイプ」リストで「**Lieberman Random Password Manager**」を選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 77 章 Linux

IBM Security QRadar は Linux DSM を幅広くサポートしています。

Linux DHCP

IBM Security QRadar 用の Linux DHCP Server DSM は、syslog を使用して DHCP イベントを受け入れます。

QRadar は、Linux DHCP サーバーのすべての関連イベントを記録します。Linux DHCP サーバーと統合するように QRadar を構成する前に、Linux DHCP サーバー内で syslog を構成して syslog イベントを QRadar に転送するようにする必要があります。

Linux DHCP サーバーの構成について詳しくは、man ページまたは DHCP デーモンの関連資料を調べてください。

ログ・ソースの構成

IBM Security QRadar は、Linux DHCP サーバーに転送されたイベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドに、Linux DHCP サーバーの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「Linux **DHCP** サーバー」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *252. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Linux DHCP サーバーからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Linux IPtables

IBM Security QRadar 用の Linux IPtables DSM は、syslog を使用することでファイアウォールの IPtables イベントを受け入れます。

QRadar は、syslog イベントに「受け入れ」、「ドロップ」、「拒否」、または「拒否」のいずれかの単語が含まれる Linux IPtables からすべての関連イベントを記録します。イベント・ペイロードにカスタマイズしたログ接頭辞を作成すると、QRadar が IPtables の動作を簡単に識別できるようになります。

IPtables の構成

IPtables は、Linux カーネル・ファイアウォールでトラフィック・ルーティングのためのルールを作成するときに使用する強力なツールです。

このタスクについて

IPtables を構成するには、既存のルールを調べ、イベントをログに記録するためのルールを変更し、IBM Security QRadar により識別可能なログ ID を IPtables ルールに割り当てる必要があります。このプロセスは、QRadar によりログに記録されるルールを決定するために使用されます。QRadar には、単語 accept、drop、reject、または deny がイベント・ペイロードに含まれている記録済みイベントが含まれています。

手順

1. SSH を使用して、root ユーザーとして Linux サーバーにログインします。
2. 以下のディレクトリーにある IPtables ファイルを編集します。

   ```
   /etc/iptables.conf
   ```

   注: IPtables ルールが含まれているファイルは、構成する Linux オペレーティング・システムに応じて異なることがあります。例えば Red Hat Enterprise を使用するシステムでは、このファイルは `/etc/sysconfig/iptables` ディレクトリーにあります。IPtables の構成について詳しくは、*Linux* オペレーティング・システムの資料を参照してください。
3. ファイルを調べ、ログに記録する IPtables ルールを決定します。

   例えば項目によって定義されるルールをログに記録するには、以下を使用します。

   ```
   -A INPUT -i eth0 --dport 31337 -j DROP
   ```
4. ログに記録する各ルールの直前に、対応するルールを挿入します。

   ```
   -A INPUT -i eth0 --dport 31337 -j DROP -A INPUT -i eth0 --dport 31337
   -j DROP
   ```
5. ログに記録するルールごとに、新しいルールのターゲットを LOG に変更します。次に例を示します。

```
-A INPUT -i eth0 --dport 31337 -j LOG -A INPUT -i eth0 --dport 31337 -j
DROP
```

6. LOG ターゲットのログ・レベルを SYSLOG 優先レベル (info、notice など) に設定します。

```
-A INPUT -i eth0 --dport 31337 -j LOG --log-level info -A INPUT -i eth0
--dport 31337 -j DROP
```

7. ルールの動作を指定するログ接頭部を構成します。ログ接頭部パラメーターを次のように設定します。

```
Q1Target=<rule>
```

ここで *<rule>* は **fw_accept**、**fw_drop**、**fw_reject**、**fw_deny** のいずれかです。

例えば、ファイアウォールによりログに記録されるルールのターゲットがドロップ・イベントである場合、ログ接頭部の設定は以下のようになります。

```
Q1Target=fw_drop
-A INPUT -i eth0 --dport 31337 -j LOG --log-level info --log-prefix
 "Q1Target=fw_drop " -A INPUT -i eth0 --dport 31337 -j DROP
```

注: 終了引用符の前に末尾のスペースが 1 つ必要です。

8. ファイルを保存して終了します。
9. 以下のコマンドを使用して IPtables を再始動します。

```
/etc/init.d/iptables restart
```

10. syslog.conf ファイルを開きます。
11. 以下の行を追加します。

```
kern.<log level>@<IP address>
```

各部分について以下で説明します。

- *<log level>* は、以前に設定されたログ・レベルです。
- *<IP address>* は QRadar の IP アドレスです。

12. ファイルを保存して終了します。
13. 以下のコマンドを使用して Syslog デーモンを再始動します。

```
/etc/init.d/syslog restart
```

Syslog デーモンの再始動後に、イベントが QRadar に転送されます。Linux サーバーから転送される IPtable イベントは自動的に検出され、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Linux サーバーから転送された IPtables Syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下のログ・ソースの構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドに、Linux DHCP サーバーの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「Linux **iptables** ファイアウォール **(Linux iptables Firewall)**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *253. Syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Linux サーバーから転送される IPtables イベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。Linux サーバーから転送される IPtables イベントは自動的に検出され、QRadar の「ログ・アクティビティー」タブに表示されます。

Linux サーバーでの IPtables の構成について詳しくは、マニュアル・ページまたは関連する Linux 資料を参照してください。

Linux OS

IBM Security QRadar 用の Linux OS DSM は、Linux オペレーティング・システム・イベントを記録し、syslog または syslog-ng を使用してそのイベントを転送します。

UNIX ホストで syslog を使用している場合は、標準の syslog を syslog-ng などの最新バージョンにアップグレードしてください。

注**:** syslog と syslog-ng の両方を同時に実行しないでください。

Linux OS を QRadar と統合するには、イベント収集用に以下のいずれかのsyslog構成を選択します。

- 665 ページの『Linux OS での Syslog の構成』
- 665 ページの『Linux OS での syslog-ng の構成』

また、QRadar に監査ログを送るように Linux オペレーティング・システムを構成することも可能です。詳しくは、 666 ページの『監査ログを送信するための Linux OS の構成』を参照してください。

サポートされるイベント・タイプ

Linux OS DSM は以下のイベント・タイプをサポートします。

- cron
- HTTPS
- FTP
- NTP
- Simple Authentication Security Layer (SASL)
- SMTP
- SNMP
- SSH
- ユーザー切り替え (SU)
- Pluggable Authentication Module (PAM) イベント

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Linux OS での Syslog の構成

Linux OS で Syslog プロトコルを構成します。

手順

1. root ユーザーとして Linux OS デバイスにログインします。
2. `/etc/syslog.conf` ファイルを開きます。
3. 以下のファシリティー情報を追加します。

   ```
   authpriv.*@<IP address>
   ```

   ここで、*<IP address>* は IBM Security QRadar の IP アドレスです。
4. ファイルを保存します。
5. 以下のコマンドを使用して Syslog を再始動します。

   ```
   service syslog restart
   ```
6. QRadar ユーザー・インターフェースにログインします。
7. Linux OS ログ・ソースを追加します。
8. 「管理」タブで「変更のデプロイ」をクリックします。

   Syslog について詳しくは、*Linux* オペレーティング・システムの資料を参照してください。

Linux OS での syslog-ng の構成

syslog-ng プロトコルを使用するように Linux OS を構成します。

手順

1. root ユーザーとして Linux OS デバイスにログインします。
2. /etc/syslog-ng/syslog-ng.conf ファイルを開きます。
3. 以下のファシリティー情報を追加します。

```
filter auth_filter{ facility(authpriv); };

destination auth_destination { tcp("<IP address>" port(514)); };

log{

 source(<Sourcename>);

 filter(auth_filter);

 destination(auth_destination);

};
```

   各部分について以下で説明します。
   - *<IP address>* は IBM Security QRadar の IP アドレスです。
   - *<Source name>* は、構成ファイルで定義されているソースの名前です。
4. ファイルを保存します。
5. 以下のコマンドを使用して Syslog-ng を再始動します。

```
service syslog-ng restart
```

6. QRadar ユーザー・インターフェースにログインします。
7. Linux OS ログ・ソースを追加します。
8. 「管理」タブで「変更のデプロイ」をクリックします。

   syslog-ng について詳しくは、*Linux* オペレーティング・システムの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

監査ログを送信するための Linux OS の構成

監査ログを QRadar に送信するように Linux OS を構成します。

このタスクについて

このタスクは、Red Hat Enterprise Linux v6 オペレーティング・システムに適用されます。

SUSE、Debian、または Ubuntu オペレーティング・システムをご使用の場合は、オペレーティング・システム固有の手順をベンダーの資料で参照してください。

手順

1. root ユーザーとして Linux OS デバイスにログインします。
2. 以下のコマンドを入力します。

   ```
   yum install audit service auditd start chkconfig auditd on
   ```
3. 以下のファイルを開きます。

   ```
   /etc/audisp/plugins.d/syslog.conf
   ```
4. パラメーターが以下の値に一致していることを確認します。

   ```
   active = yes direction = out path = builtin_syslog type = builtin args
   = LOG_LOCAL6 format = string
   ```
5. 以下のファイルを開きます。

   ```
   /etc/rsyslog.conf
   ```
6. このファイルの終わりに以下の行を追加します。

   ```
   local6.* @@QRadar_Collector_IP_address
   ```
7. QRadar ユーザー・インターフェースにログインします。
8. Linux OS ログ・ソースを追加します。
9. 「管理」タブで「変更のデプロイ」をクリックします。
10. root ユーザーとして QRadar にログインします。
11. 以下のコマンドを入力します。

    ```
    service auditd restart service syslog restart
    ```

関連タスク:

5 ページの『ログ・ソースの追加』

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 78 章 LOGbinder

イベント・ログを IBM Security QRadar に送信するように LOGbinder システムを構成します。

以下の LOGbinder システムがサポートされます。

- Microsoft Exchange Server からの LOGbinder EX イベント収集。
- Microsoft SharePoint からの LOGbinder SP イベント収集。
- Microsoft SQL Server からの LOGbinder SQL イベント収集。

Microsoft Exchange Server からの LOGbinder EX イベント収集

Microsoft Exchange Server 用の IBM Security QRadar DSM では、LOGbinder EX V2.0 のイベントを収集できます。

以下の表は、LOGbinder EX イベントを収集するログ・ソースを構成する場合の Microsoft Exchange Server DSM の仕様を示しています。

表 *254. Microsoft Exchange Server* 用の *LOGbinder*

仕様	値
製造元	Microsoft
DSM 名	Microsoft Exchange Server
RPM ファイル名	DSM-MicrosoftExchange-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	LOGbinder EX V2.0
プロトコル・タイプ	Syslog LEEF
QRadar で記録されるイベント・タイプ	管理 メールボックス
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	Microsoft Exchange Web サイト (http://www.office.microsoft.com/en-us/exchange/)

Microsoft Exchange Server DSM では、他のタイプのイベントも収集できます。他の Microsoft Exchange Server イベント・フォーマットの構成方法について詳しくは、「*IBM Security QRadar DSM Configuration Guide*」の Microsoft Exchange Server に関するトピックを参照してください。

Microsoft Exchange Server から LOGbinder イベントを収集するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードしてください。
   - DSMCommon RPM
   - Microsoft Exchange Server DSM RPM
2. Microsoft Exchange Server イベント・ログを QRadar に送信するように LOGbinder EX システムを構成します。
3. ログ・ソースが自動的に作成されない場合、QRadar コンソール上で Microsoft Exchange Server DSM ログ・ソースを追加します。以下の表は、固有の値を必要とするパラメーターを示しています。LOGbinder EX イベントを収集するには、これらの値が必要です。

表 255. *LOGbinder* イベント収集用の *Microsoft Exchange Server* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Microsoft Exchange Server
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Microsoft Exchange イベント・ログを QRadar に送信するように LOGbinder EX システムを構成する

Microsoft Exchange LOGbinder イベントを収集するには、イベントを IBM Security QRadar に送信するように LOGbinder EX システムを構成する必要があります。

始める前に

Microsoft Exchange Server からイベントを収集するように LOGbinder EX を構成します。詳しくは、LOGbinder EX の資料を参照してください。

手順

1. 「LOGbinder EX 制御パネル (LOGbinder EX Control Panel)」を開きます。
2. 「構成」ペインで「出力 **(Output)**」をダブルクリックします。
3. 次のオプションのいずれかを選択してください。
   - 汎用 Syslog の出力の構成
     a. 「出力 (Outputs)」ペインで**>**「汎用 **Syslog (Syslog-Generic)**」をダブルクリックします。
     b. 「出力を汎用 **Syslog** に送信 **(Send output to Syslog-Generic)**」チェック・ボックスを選択してから、QRadar コンソールまたはイベント・コレクターの IP アドレスおよびポートを入力します。

- Syslog-LEEF 出力の構成:
  a. 「出力」ペインで「**Syslog-LEEF**」をダブルクリックします。
  b. 「出力を **Syslog-LEEF** に送信 **(Send output to Syslog-LEEF)**」チェック・ボックスを選択してから、QRadar コンソールまたはイベント・コレクターの IP アドレスおよびポートを入力します。

4. 「**OK**」をクリックします。
5. LOGbinder サービスを再始動するには、「再始動」アイコンをクリックします。

Microsoft SharePoint からの LOGbinder SP イベント収集

Microsoft SharePoint の IBM Security QRadar DSM では、LOGbinder SP イベントを収集できます。

以下の表は、LOGbinder SP イベントを収集するログ・ソースを構成する場合の Microsoft SharePoint DSM の仕様を示しています。

表 *256. Microsoft SharePoint* 用の *LOGbinder* の仕様

仕様	値
製造元	Microsoft
DSM 名	Microsoft SharePoint
RPM ファイル名	`DSM-MicrosoftSharePoint-QRadar_version-build_number.noarch.rpm`
サポートされるバージョン	LOGbinder SP V4.0
プロトコル・タイプ	Syslog LEEF
QRadar で記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	*http://office.microsoft.com/en-sg/sharepoint/* (http://office.microsoft.com/en-sg/sharepoint/) *http://www.logbinder.com/products/logbindersp/* (http://www.logbinder.com/products/logbindersp/)

Microsoft SharePoint DSM では、他のタイプのイベントも収集できます。他の Microsoft SharePoint イベント・フォーマットについて詳しくは、「*IBM Security QRadar DSM Configuration Guide*」の Microsoft SharePoint に関するトピックを参照してください。

Microsoft SharePoint から LOGbinder イベントを収集するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードしてください。

- DSMCommon RPM
- Microsoft SharePoint DSM RPM

2. Microsoft SharePoint イベント・ログを QRadar に送信するように LOGbinder SP システムを構成します。
3. ログ・ソースが自動的に作成されない場合、QRadar コンソール上で Microsoft SharePoint DSM ログ・ソースを追加します。以下の表は、固有の値を必要とするパラメーターを示しています。LOGbinder イベントを収集するには、これらの値が必要です。

表 257. *LOGbinder* イベント収集用の *Microsoft SharePoint* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Microsoft SharePoint
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『Microsoft SharePoint イベント・ログを QRadar に送信するように LOGbinder SP システムを構成する』
Microsoft SharePoint LOGbinder イベントを収集するには、イベントを IBM Security QRadar に送信するように LOGbinder SP システムを構成する必要があります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Microsoft SharePoint イベント・ログを QRadar に送信するように LOGbinder SP システムを構成する

Microsoft SharePoint LOGbinder イベントを収集するには、イベントを IBM Security QRadar に送信するように LOGbinder SP システムを構成する必要があります。

手順

1. 「LOGbinder SP 制御パネル (LOGbinder SP Control Panel)」を開きます。
2. 「構成」ペインで「出力 **(Output)**」をダブルクリックします。
3. 次のオプションのいずれかを選択してください。
   - 汎用 Syslog の出力の構成
     a. 「出力 (Outputs)」ペインで**>**「汎用 **Syslog (Syslog-Generic)**」をダブルクリックします。
     b. 「出力を汎用 **Syslog** に送信 **(Send output to Syslog-Generic)**」チェック・ボックスを選択してから、QRadar コンソールまたはイベント・コレクターの IP アドレスおよびポートを入力します。
   - Syslog-LEEF 出力の構成:
     a. 「出力」ペインで「**Syslog-LEEF**」をダブルクリックします。

b. 「出力を **Syslog-LEEF** に送信 **(Send output to Syslog-LEEF)**」チェック・ボックスを選択してから、QRadar コンソールまたはイベント・コレクターの IP アドレスおよびポートを入力します。

4. 「**OK**」をクリックします。
5. LOGbinder サービスを再始動するには、「再始動」アイコンをクリックします。

Microsoft SQL Server からの LOGbinder SQL イベント収集

Microsoft SQL Server 用の IBM Security QRadar DSM では、LOGbinder SQL イベントを収集できます。

以下の表は、LOGbinder SQL イベントを収集するようにログ・ソースを構成する場合の Microsoft SQL Server DSM の仕様を示しています。

表 *258. Microsoft SQL Server* 用の *LOGbinder* の仕様

仕様	値
製造元	Microsoft
DSM 名	Microsoft SQL Server
RPM ファイル名	`DSM-MicrosoftSQL-`*`QRadar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	LOGBinder SQL V2.0
プロトコル・タイプ	Syslog
QRadar で記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	はい
その他の情報	LogBinder SQL Web サイト (http://www.logbinder.com/products/logbindersql/) Microsoft SQL Server Web サイト (http://www.microsoft.com/en-us/server-cloud/products/sql-server/)

Microsoft SQL Server DSM では、他のタイプのイベントも収集できます。他の Microsoft SQL Server イベント・フォーマットについて詳しくは、「*IBM Security QRadar DSM Configuration Guide*」の Microsoft SQL Server に関するトピックを参照してください。

Microsoft SQL Server から LOGbinder イベントを収集するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードしてください。
   - DSMCommon RPM
   - Microsoft SQL Server DSM RPM
2. Microsoft SQL Server イベント・ログを QRadar に送信するように LOGbinder SQL システムを構成します。

3. ログ・ソースが自動的に作成されない場合、QRadar コンソール上で Microsoft SQL Server DSM ログ・ソースを追加します。以下の表は、固有の値を必要とするパラメーターを示しています。LOGbinder イベントを収集するには、これらの値が必要です。

表 259. *LOGbinder* イベント収集用の *Microsoft SQL Server* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Microsoft SQL Server
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Microsoft SQL Server イベント・ログを QRadar に送信するように LOGbinder SQL システムを構成する

Microsoft SQL LOGbinder イベントを収集するには、イベントを IBM Security QRadar に送信するように LOGbinder SQL システムを構成する必要があります。

始める前に

Microsoft SQL Server からイベントを収集するように LOGbinder SQL を構成します。詳しくは、LOGbinder SQL の資料を参照してください。

手順

1. 「LOGbinder SQL 制御パネル (LOGbinder SQL Control Panel)」を開きます。
2. 「構成」ペインで「出力 **(Output)**」をダブルクリックします。
3. 次のオプションのいずれかを選択してください。
   - 汎用 Syslog の出力の構成
     a. 「出力 (Outputs)」ペインで**>**「汎用 **Syslog (Syslog-Generic)**」をダブルクリックします。
     b. 「出力を汎用 **Syslog** に送信 **(Send output to Syslog-Generic)**」チェック・ボックスを選択してから、QRadar コンソールまたはイベント・コレクターの IP アドレスおよびポートを入力します。
   - Syslog-LEEF 出力の構成:
     a. 「出力」ペインで「**Syslog-LEEF**」をダブルクリックします。
     b. 「出力を **Syslog-LEEF** に送信 **(Send output to Syslog-LEEF)**」チェック・ボックスを選択してから、QRadar コンソールまたはイベント・コレクターの IP アドレスおよびポートを入力します。
4. 「**OK**」をクリックします。

5. LOGbinder サービスを再始動するには、「再始動」アイコンをクリックします。

第 79 章 McAfee

IBM Security QRadar は、さまざまな McAfee 製品をサポートしています。

McAfee Application / Change Control

McAfee Application / Change Control DSM for IBM Security QRadar は、Java Database Connectivity (JDBC) を使用して変更制御イベントを受け取ります。QRadar は、関連するすべての McAfee Application / Change Control イベントを記録します。この資料では、JDBC プロトコルを使用してイベントが格納されているデータベースにアクセスするように QRadar を構成する手順を説明します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース・タイプ」リストで「**McAfee Application / Change Control**」を選択します。
6. 「プロトコル構成」リストで「**JDBC**」を選択します。

   QRadar で McAfee Application / Change Control DSM を設定するときには、Application / Change Control Management Console で「データベース設定の構成 *(Configure Database Settings)*」を参照する必要があります。
7. 以下の値を構成します。

表 260. *McAfee Application / Change Control* の *JDBC* プロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<McAfee Change Control Database>@<Change Control Database Server IP or Host Name>* 各部分について以下で説明します。 • *<McAfee Change Control Database>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<Change Control Database Server IP or Host Name>* は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。 「ログ・ソース **ID**」の名前を定義する際には、ePO Management Console から McAfee Change Control Database の値と Database Server の IP アドレスまたはホスト名の値を使用する必要があります。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	McAfee Application / Change Control データベースの正確な名前を入力します。
IP またはホスト名	McAfee Application / Change Control SQL サーバーの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。MSDE のデフォルト・ポートは 1433 です。 JDBC 構成のポートは、McAfee Application / Change Control データベースのリスナー・ポートに一致していなければなりません。McAfee Application / Change Control データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして「MSDE」を使用するときに「データベース・インスタンス **(Database Instance)**」を定義する場合は、構成の「ポート」パラメーターをブランクのままにする必要があります。
ユーザー名	データベースへのアクセスに必要なユーザー名を入力します。
パスワード	データベースへのアクセスに必要なパスワードを入力します。パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」パラメーターに入力したパスワードと同じでなければなりません。

表 260. *McAfee Application / Change Control* の *JDBC* プロトコル・パラメーター (続き)

パラメーター	説明
認証ドメイン	「データベース・タイプ」として「**MSDE**」を選択し、データベースが Windows 用に構成されている場合は、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックした場合は、構成内で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを含むテーブルまたはビューの名前として `SCOR_EVENTS` と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに `*` を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	比較フィールドとして `AutoID` を入力します。比較フィールドを使用して、テーブルに対する照会から次の照会までの間に追加されたい新しいイベントを特定できます。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。

表 260. *McAfee Application / Change Control* の *JDBC* プロトコル・パラメーター *(*続き*)*

パラメーター	説明
準備済みステートメントの使用 **(Use Prepared Statements)**	準備済みステートメントを使用する場合は、このチェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、そのステートメントを別のパラメーターで何度も使用できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

注**:** 「信頼性」パラメーターに 5 よりも大きい値を選択すると、McAfee Application / Change Control ログ・ソースに対し、QRadar の他のログ・ソースよりも高い重要度が設定されます。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

McAfee ePolicy Orchestrator

IBM Security QRadar for McAfee ePolicy Orchestrator で、McAfee ePolicy Orchestrator デバイスからイベント・ログを収集できます。

以下の表は、McAfee ePolicy Orchestrator DSM の仕様を示しています。

表 *261. McAfee ePolicy Orchestrator*

仕様	値
製造元	McAfee
DSM 名	McAfee ePolicy Orchestrator
RPM ファイル名	DSM-McAfeeEpo-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	V3.5 から V5.x
プロトコル・タイプ	JDBC SNMPv2 SNMPv3
QRadar で記録されるイベント・タイプ	アンチウィルス・イベント
自動的に検出?	いいえ
ID を含む?	いいえ
その他の情報	http://www.mcafee.com (http://www.mcafee.com)

McAfee ePolicy Orchestrator を QRadar と統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの McAfee ePolicy Orchestrator DSM RPM をダウンロードしてください。
2. QRadar と通信できるように McAfee ePolicy Orchestrator DSM デバイスを構成します。以下のいずれかのオプションを使用します。
   - 統合
3. QRadar コンソール上で McAfee ePolicy Orchestrator DSM のログ・ソースを作成します。

JDBC プロトコルを使用した McAfee ePO ログ・ソースの構成

JDBC プロトコルを使用して ePolicy Orchestrator (McAfee ePO) データベースにアクセスするように、IBM Security QRadar を構成します。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドに McAfee ePolicy Orchestrator のログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで、「**McAfee ePolicy Orchestrator**」を選択します。
6. 「プロトコル構成」リストで「**JDBC**」を選択します。
7. 以下のログ・ソース・パラメーターを構成します。

オプション	説明
ログ・ソース **ID**	次の形式を使用します: `<McAfee_ePO_Database>@ <McAfee_ePO_Database_Server_IP_or_Host_Name>` ePO Management Console から McAfee ePO Database の値および Database Server の IP アドレスまたはホスト名の値を使用する必要があります。
データベース・タイプ	MSDE
データベース名	McAfee ePolicy Orchestrator データベースの名前。
IP またはホスト名	McAfee ePolicy Orchestrator SQL Server の IP アドレスまたはホスト名。
ポート	データベース・サーバーが使用するポート番号。このポートは、McAfee ePolicy Orchestrator データベースのリスナー・ポートと一致している必要があります。McAfee ePolicy Orchestrator データベースには、QRadar との通信に使用可能な着信 TCP 接続が必要です。 データベース・タイプ・リストから MSDE を選択する場合は、ポート・パラメーターを空のままにしておいてください。
ユーザー名	ユーザー名は、英数字で最大 255 文字までであり、アンダースコアー文字 (_) を含めることができます。 監査目的でデータベース・アクセスを追跡するには、QRadar 用のデータベースに特定のユーザーを作成します。
パスワード	パスワードの最大長は 255 文字です。
認証ドメイン **(MSDE** のみ**)**	データベース・タイプ・リストから MSDE を選択し、データベースが Windows 用に構成されている場合は、このパラメーターを定義する必要があります。それ以外の場合は、このパラメーターを空のままにしておいてください。

オプション	説明
データベース・インスタンス **(MSDE** または **Informix** のみ**)**	データベース・サーバーに複数の SQL サーバー・インスタンスがある場合のオプション。データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックした場合は、構成内でこのパラメーターを空のままにしておく必要があります。
定義済み照会	オプション。ログ・ソース・タイプに対して定義済み照会を使用できない場合、管理者は「なし」を選択できます。
テーブル名	次のようなイベント・レコードを含むテーブルまたはビュー。 • ePO 3.x の場合は、Events と入力。 • ePO 4.x の場合は、EPOEvents と入力。 • ePO 5.x の場合は、EPOEvents と入力。
選択リスト	テーブルまたはビューのすべてのフィールドに * を入力します。コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義します。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。
比較フィールド	テーブルの照会の間に追加された新規イベントを識別するには、AutoID を入力します。
準備済みステートメントの使用 **(Use Prepared Statements)**	JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度も実行できるようになります。セキュリティーおよびパフォーマンス上の理由で、準備済みステートメントを使用するようにしてください。このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用してください。
開始日時	オプション。データベースのポーリングについては、HH を 24 時間形式で指定した yyyy-MM-dd HH:mm の形式を使用します。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔。イベント・テーブルへの照会から次の照会までの間の時間です。デフォルトのポーリング間隔は 10 秒です。もっと長いポーリング間隔を定義するには、H (時間) または M (分) を数値に追加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力する数値は、秒数のポーリング間隔です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数。

オプション	説明
名前付きパイプ通信の使用 **(Use Named Pipe Communication) (MSDE** のみ**)**	MSDE データベースを使用する場合は、「ユーザー名」フィールドおよび「パスワード」フィールドで、データベースのユーザー名とパスワードではなく、Windows 認証のユーザー名とパスワードを使用する必要があります。ログ・ソースの構成では、MSDE データベースのデフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name) (MSDE** のみ**)**	SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。
NTLMv2 の使用 **(Use NTLMv2) (MSDE** のみ**)**	接続が NTLMv2 をサポートする場合は、これが必要なくてもこのパラメーターを有効にする必要があります。このオプションを選択すると、NTLMv2 認証を必要とする SQL サーバーとの通信時に、MSDE 接続で NTLMv2 プロトコルが強制的に使用されます。 NTLMv2 認証を必要としない MSDE 接続の通信には干渉しません。
SSL の使用 **(Use SSL) (MSDE** のみ**)**	接続が SSL をサポートする場合は、これが必要なくてもこのパラメーターを有効にする必要があります。このオプションを選択する場合は、データベースに追加の構成が必要であり、管理者が両方のアプライアンスで証明書を構成する必要があります。
データベース・ロケール **(Database Locale) (Informix** のみ**)**	データベースで使用されるロケールと一致するロケールを選択します。
コード・セット **(Informix** のみ**)**	ロケールをデフォルトに設定しない場合は、データベースに使用するコード・セットを選択します。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

関連情報:

Configuring JDBC Over SSL with a Self-signed Certificate

Configuring JDBC Over SSL with an Externally-signed Certificate

SNMP イベントの転送用の ePO の構成

SNMP イベントを転送するように ePO を構成するには、McAfee ePolicy Orchestrator デバイスで SNMP トラップ通知を送信し、その通知を QRadar で受信するように構成する必要があります。

このタスクについて

手順

1. 登録済みサーバーを追加します。
2. ePO デバイスで SNMP トラップ通知を構成します。
3. QRadar でログ・ソースとプロトコルを構成します。

4. オプション: 上位 SNMP 復号アルゴリズムの Java Cryptography Extension をインストールします。

McAfee ePO への登録済みサーバーの追加

ePO で SNMP イベントを転送するように構成するには、登録済みサーバーを McAfee EPO に追加する必要があります。

手順

1. McAfee ePolicy Orchestrator コンソールにログインします。
2. 「メニュー」>「構成」>「登録済みサーバー」を選択します。
3. 「新規サーバー」をクリックします。
4. 「サーバー・タイプ」メニューから、「**SNMP** サーバー」を選択します。
5. SNMP サーバーの名前と追加メモを入力して「次へ」をクリックします。
6. 「アドレス」リストから、使用中のサーバー・アドレスのタイプを選択して名前または IP アドレスを入力します。
7. 「**SNMP** バージョン」リストから、使用する SNMP バージョンを選択します。
   - SNMPv2c を使用する場合は、コミュニティー名を指定する必要があります。
   - SNMPv3 を使用する場合は、SNMPv3 セキュリティーの詳細を指定する必要があります。
8. SNMP 構成を検査するには、「テスト・トラップの送信」をクリックします。
9. 「保存」をクリックします。

McAfee ePO での SNMP 通知の構成

SNMP イベントを転送するように ePO を構成するには、ご使用の McAfee ePO システムで SNMP 通知を構成する必要があります。

始める前に

McAfee ePO に登録済みサーバーを追加する手順を完了する必要があります。

手順

1. 「メニュー」 > 「自動化 **(Automation)**」 > 「自動応答 **(Automatic Responses)**」を選択します。
2. 「新規応答 **(New Responses)**」をクリックします。
3. 以下の値を構成します。
   a. 応答の名前を入力します。
   b. 応答の説明を入力します。
   c. 「イベント・グループ **(Event group)**」リストから「**ePO** 通知イベント **(ePO Notification Events)**」を選択します。
   d. 「イベント・タイプ **(Event type)**」リストから「脅威 **(Threats)**」を選択します。
   e. 「ステータス **(Status)**」リストで「有効 **(Enabled)**」を選択します。
4. 「次へ」をクリックします。

5. 「値 **(Value)**」列でシステムの選択に使用する値を入力するか、省略符号アイコンをクリックします。
6. オプション: 「使用可能なプロパティー **(Available Properties)**」リストからさらにフィルターを選択して、応答結果を絞り込みます。
7. 「次へ」をクリックします。
8. 「すべてのイベントでこの応答をトリガー **(Trigger this response for every event)**」を選択し、「次へ」をクリックします。

   McAfee ePO 応答に対して集約を構成する場合は、スロットルを有効にしないでください。
9. 「アクション **(Actions)**」リストから「**SNMP** トラップの送信 **(Send SNMP Trap)**」を選択します。
10. 以下の値を構成します。
    a. SNMP サーバーのリストから、登録済みサーバーを追加したときに登録した SNMP サーバーを選択します。
    b. 「使用可能なタイプ **(Available Types)**」リストから「すべての値のリスト **(List of All Values)**」を選択します。
    c. **>>** をクリックして、ご使用の McAfee ePolicy Orchestrator バージョンに関連付けられているイベント・タイプを追加します。以下の表をガイドとして参照してください。

使用可能なタイプ	選択されたタイプ	**ePO** バージョン
検出された UTC	{listOfDetectedUTC}	4.5, 5.1
受け取った UTC	{listOfReceivedUTC}	4.5, 5.1
製品 IPv4 アドレスの検出	{listOfAnalyzerIPV4}	4.5, 5.1
製品 IPv6 アドレスの検出	{listOfAnalyzerIPV6}	4.5, 5.1
製品 MAC アドレスの検出	{listOfAnalyzerMAC}	4.5, 5.1
ソース IPv4 アドレス	{listOfSourceIPV4}	4.5, 5.1
送信元 IPv6 アドレス	{listOfSourceIPV6}	4.5, 5.1
送信元 MAC アドレス	{listOfSourceMAC}	4.5, 5.1
送信元ユーザー名	{listOfSourceUserName}	4.5, 5.1
ターゲット IPv4 アドレス	{listOfTargetIPV4}	4.5, 5.1
ターゲット IPv6 アドレス	{listOfTargetIPV6}	4.5, 5.1
ターゲット MAC	{listOfTargetMAC}	4.5, 5.1
ターゲット・ポート	{listOfTargetPort}	4.5, 5.1
脅威のイベント ID	{listOfThreatEventID}	4.5, 5.1
脅威のイベント ID	{listOfThreatEventID}	4.5, 5.1
脅威の重大度	{listOfThreatSeverity}	4.5, 5.1
SourceComputers		4.0
AffectedComputerIPs		4.0
EventIDs		4.0
TimeNotificationSent		4.0

11. 「次へ」をクリックします。

12. 「保存」をクリックします。

SNMP イベントの転送用の ePO の構成

SNMP イベントを転送するように ePO を構成するには、McAfee ePolicy Orchestrator デバイスで SNMP トラップ通知を送信し、その通知を QRadar で受信するように構成する必要があります。

このタスクについて

手順

1. 登録済みサーバーを追加します。
2. ePO デバイスで SNMP トラップ通知を構成します。
3. QRadar でログ・ソースとプロトコルを構成します。
4. オプション: 上位 SNMP 復号アルゴリズムの Java Cryptography Extension をインストールします。

SNMP プロトコルを使用した McAfee ePO ログ・ソースの構成

SNMP プロトコルを使用して ePO データベースにアクセスするように、QRadar を構成します。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドに McAfee ePolicy Orchestrator のログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで、「**McAfee ePolicy Orchestrator**」を選択します。
6. 「プロトコル構成」リストで「**SNMPv2**」または「**SNMPv3**」のいずれかを選択します。
7. SNMPv2 を選択した場合は、以下のログ・ソース・パラメーターを構成します。

オプション	説明
ログ・ソース **ID**	ログ・ソースの固有の IP アドレス。
コミュニティー	SNMPv2 プロトコルの SNMP コミュニティー・ストリング (Public など)。
イベント・ペイロードに **OID** を含める **(Include OIDs in Event Payload)**	標準のイベント・ペイロード形式ではなく、名前と値のペアで McAfee ePO イベント・ペイロードを構成できるようにするには、「イベント・ペイロードに **OID** を含める **(Include OIDs in Event Payload)**」チェック・ボックスを有効にします。 **重要:** McAfee ePO では、SNMPv2 イベントまたは SNMPv3 イベントを処理するためには、イベント・ペイロードに OID を含める必要があります。

8. SNMPv3 を選択した場合は、以下のログ・ソース・パラメーターを構成します。

オプション	説明
ログ・ソース **ID**	ログ・ソースの固有の IP アドレス。
認証プロトコル	SNMPv3 トラップの認証に使用するアルゴリズム: • **SHA**。認証プロトコルとして Secure Hash Algorithm (SHA) を使用します。 • **MD5**。認証プロトコルとして Message Digest 5 (MD5) を使用します。
認証パスワード	SNMPv3 を認証するパスワード。認証パスワードには、8 文字以上を含める必要があります。
復号プロトコル **(Decryption Protocol)**	SNMPv3 トラップの暗号化解除に使用するアルゴリズムを選択します。 • DES • AES128 • AES192 • AES256 **注:** 復号アルゴリズムとして AES192 または AES256 を選択する場合は、Java Cryptography Extension をインストールする必要があります。McAfee ePO への Java Cryptography Extension のインストール方法について詳しくは、Java Cryptography Extension のインストールを参照してください。
復号パスワード **(Decryption Password)**	SNMPv3 トラップを復号するパスワード。復号パスワードには 8 文字以上を含める必要があります。
ユーザー	このプロトコルのユーザー・アクセス。
イベント・ペイロードに **OID** を含める **(Include OIDs in Event Payload)**	標準のイベント・ペイロード形式ではなく、名前と値のペアで McAfee ePO イベント・ペイロードを構成できるようにするには、「イベント・ペイロードに **OID** を含める **(Include OIDs in Event Payload)**」チェック・ボックスを有効にします。 **重要:** McAfee ePO では、SNMPv2 イベントまたは SNMPv3 イベントを処理するためには、イベント・ペイロードに OID を含める必要があります。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

McAfee ePO への Java Cryptography Extension のインストール

Java™ Cryptography Extension (JCE) は、QRadar で AES192 または AES256 の拡張暗号化アルゴリズムを復号するために必要な Java フレームワークです。以下の情報では、Oracle JCE を McAfee ePO アプライアンスにインストールする方法を説明します。

手順

1. 以下の Web サイトから最新バージョンの JavaTM Cryptography Extension をダウンロードします。

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

   JavaTM Cryptography Extension のバージョンは、McAfee ePO アプライアンスにインストールされている Java™ のバージョンと一致している必要があります。
2. McAfee ePO アプライアンスの以下のディレクトリーに JCE 圧縮ファイルをコピーします。

   `<installation path to McAfee ePO>/jre/lib/security`

QRadar への Java Cryptography Extension のインストール

Java™ Cryptography Extension (JCE) は、QRadar で AES192 または AES256 の拡張暗号化アルゴリズムを復号するために必要な Java フレームワークです。以下の情報では、 Oracle JCE を QRadar アプライアンスにインストールする方法を説明します。

手順

1. 以下の Web サイトから最新バージョンの JavaTM Cryptography Extension をダウンロードします。

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

   JavaTM Cryptography Extension のバージョンは、QRadar にインストールされている Java™ のバージョンと一致している必要があります。
2. JCE ファイルを解凍します。

   JCE ダウンロードには以下の Java アーカイブ (JAR) ファイルが含まれています。

   - local_policy.jar
   - US_export_policy.jar
3. QRadar コンソールまたはイベント・コレクターに root ユーザーとしてログインします。
4. QRadar コンソールまたはイベント・コレクターの以下のディレクトリーに JCE jar ファイルをコピーします。

   `/usr/java/latest/jre/lib/`

タスクの結果

McAfee ePolicy Orchestrator から AES192 または AE256 暗号化ファイルを受信するシステムにのみ JCE jar ファイルがコピーされます。

McAfee Firewall Enterprise

McAfee Firewall Enterprise は、以前は Secure Computing Sidewinder と呼ばれていました。McAfee Firewall Enterprise 用の IBM Security QRadar DSM は、McAfee Firewall Enterprise デバイスからログを収集します。

以下の表は、McAfee Firewall Enterprise DSM の仕様を示しています。

表 *262. McAfee Firewall Enterprise DSM* の仕様

仕様	値
製造元	McAfee
DSM 名	McAfee Firewall Enterprise
RPM ファイル名	`DSM-McAfeeFirewallEnterprise-`*`Qradar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	v6.1
イベント・フォーマット	Syslog
記録されるイベント・タイプ	Firewall Enterprise イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	McAfee の Web サイト (https://www.McAfee.com)

McAfee Firewall Enterprise を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - McAfee Firewall Enterprise DSM RPM
2. Syslog イベントを QRadar に送信するように McAfee Firewall Enterprise デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで McAfee Firewall Enterprise ログ・ソースを追加してください。以下の表は、McAfee Firewall Enterprise イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *263. McAfee Firewall Enterprise* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	McAfee Firewall Enterprise
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプラ

イアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するように McAfee Firewall Enterprise を構成

McAfee Firewall Enterprise 用の IBM Security QRadar DSM は、syslog を使用してイベントを収集します。

このタスクについて

Firewall Enterprise デバイスと統合するように QRadar SIEM を構成する前に、McAfee Firewall Enterprise デバイス内で syslog を構成する必要があります。Syslog イベントを QRadar SIEM に転送するように McAfee Firewall Enterprise デバイスを構成する際に、ログを SEF フォーマット (Sidewinder Export Format) でエクスポートしてください。

手順

McAfee Firewall Enterprise の構成について詳しくは、ベンダーの資料を参照してください。

次のタスク

イベントが QRadar SIEM に転送されるように syslog を構成すると、QRadar SIEM でログ・ソースを構成する準備が整います。

McAfee Intrushield

IBM Security QRadar McAfee Intrushield DSM は、syslog を使用するイベントを受け入れます。QRadar は、関連するすべてのイベントを記録します。

McAfee Intrushield デバイスと統合するように QRadar を構成する前に、McAfee Intrushield のバージョンを選択する必要があります。

- McAfee Intrushield V2.x から V5.x のアラート・イベントを収集するには、『McAfee Intrushield V2.x から V5.x のアラート・イベントの構成』を参照してください。
- McAfee Intrushield V6.x から V7.x のアラート・イベントを収集するには、693 ページの『McAfee Intrushield V6.x および V7.x のアラート・イベントの構成』を参照してください。
- McAfee Intrushield V6.x から V7.x の障害通知イベントを収集するには、 695 ページの『McAfee Intrushield V6.x および V7.x の障害通知イベントの設定』を参照してください。

McAfee Intrushield V2.x から V5.x のアラート・イベントの構成

McAfee Intrushield からアラート通知イベントを収集するには、IBM Security QRadar にイベントを送信するように、管理者が Syslog 転送機能を構成する必要があります。

手順

1. McAfee Intrushield Manager のユーザー・インターフェースにログインします。
2. ダッシュボードで「構成 **(Configure)**」をクリックします。
3. 「リソース・ツリー **(Resource Tree)**」でルート・ノード (Admin-Domain-Name) をクリックします。
4. 「アラート通知 **(Alert Notification)**」 > 「**Syslog** 転送機能 **(Syslog Forwarder)**」を選択します。
5. Syslog サーバーの詳細情報を入力します。

   「**Syslog** 転送機能を有効にする **(Enable Syslog Forwarder)**」が「はい (Yes)」に設定されている必要があります。

   「ポート **(Port)**」は 514 に設定されている必要があります。
6. 「編集」をクリックします。
7. 以下のいずれかのバージョンを選択します。

表 *264. McAfee Intrushield V2.x* から *V5.x* のカスタム・メッセージ・フォーマット

パラメーター	説明
パッチ未適用の McAfee Intrushield V2.x システム (Unpatched McAfee Intrushield V2.x systems)	|$ALERT_ID$|$ALERT_TYPE$|$ATTACK_TIME$|"$ATTACK_NAME$" $ATTACK_ID$|$ATTACK_SEVERITY$|$ATTACK_SIGNATURE$ $ATTACK_CONFIDENCE$|$ADMIN_DOMAIN$|$SENSOR_NAME$ $INTERFACE$|$SOURCE_IP$|$SOURCE_PORT$|$DESTINATION_IP$ $DESTINATION_PORT$|
V3.x から V5.x への更新のためにパッチが適用されている McAfee Intrushield (McAfee Intrushield that has patches applied to update to V3.x - V5.x)	|IV_ALERT_ID|IV_ALERT_TYPE|IV_ATTACK_TIME "IV_ATTACK_NAME" IV_ATTACK_ID|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$ $IV_ATTACK_CONFIDENCE$ IV_ADMIN_DOMAIN|IV_SENSOR_NAME|$IV_INTERFACE$ IV_SOURCE_IP|IV_SOURCE_PORT $IV_DESTINATION_IP$|$IV_DESTINATION_PORT$|

   注**:** カスタム・メッセージ・ストリングは、改行やスペースを使用せずに 1 行で入力する必要があります。ソフトウェア・パッチが適用されていない McAfee Intrushield アプライアンスでは、パッチが適用されているシステムとは異なるメッセージ・ストリングが使用されます。McAfee Intrushield では、各アラート・エレメントの前後に区切り文字としてドル記号 ($) を使用したカスタム・メッセージのフォーマットが必要です。エレメントのドル記号がないと、アラート・イベントが正しくフォーマットされない可能性があります。

   使用するイベント・メッセージ・フォーマットがわからない場合は、McAfee のお客様サポートにお問い合わせください。
8. 「保存」をクリックします。

   McAfee Intrushield により生成されたイベントは、指定した Syslog 宛先に転送されます。十分な数のイベントが McAfee Intrushield アプライアンスによっ

て転送されると、ログ・ソースが自動的に検出されます。通常、ログ・ソースの自動検出に必要なイベントの最小数は 25 です。

次のタスク

管理者は QRadar コンソールにログインして、QRadar コンソールでログ・ソースが作成されていることと、「ログ・アクティビティー」タブに McAfee Intrushield アプライアンスからのイベントが表示されていることを確認できます。

McAfee Intrushield V6.x および V7.x のアラート・イベントの構成

McAfee Intrushield からアラート通知イベントを収集するには、IBM Security QRadar にイベントを送信するように、管理者が Syslog 転送機能を構成する必要があります。

手順

1. McAfee Intrushield Manager のユーザー・インターフェースにログインします。
2. 「**Network Security Manager**」ダッシュボードで「構成 **(Configure)**」をクリックします。
3. 「リソース・ツリー **(Resource Tree)**」を展開し、「**IPS** 設定 **(IPS Settings)**」ノードを展開します。
4. 「アラート通知 **(Alert Notification)**」タブをクリックします。
5. 「アラート通知 **(Alert Notification)**」メニューで「**Syslog**」タブをクリックします。
6. アラート通知イベントを転送するため、以下のパラメーターを構成します。

表 *265. McAfee Intrushield v6.x* および *7.x* のアラート通知パラメーター

パラメーター	説明
Syslog 通知を有効にする **(Enable Syslog Notification)**	McAfee Intrushield の Syslog 通知を有効にするには「はい **(Yes)**」を選択します。イベントを QRadar に転送するには、このオプションを有効にする必要があります。
管理ドメイン **(Admin Domain)**	以下のいずれかのオプションを選択します。 • 「現行 **(Current)**」 - 現行ドメインのアラートの Syslog 通知を送信するには、このチェック・ボックスを選択します。このオプションはデフォルトで選択されています。 • 「子 **(Children)**」 - 現行ドメイン内の子ドメインのアラートの Syslog 通知を送信するには、このチェック・ボックスを選択します。
サーバー名または **IP** アドレス **(Server Name or IP Address)**	QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。このフィールドでは、IPv4 アドレスと IPv6 アドレスの両方がサポートされています。
UDP ポート **(UDP Port)**	Syslog イベントの UDP ポートとして 514 を入力します。
ファシリティー **(Facility)**	Syslog ファシリティー値を選択します。

表 265. *McAfee Intrushield v6.x* および *7.x* のアラート通知パラメーター *(*続き*)*

パラメーター	説明
重大度マッピング **(Severity Mappings)**	アラート通知レベル **informational**、**low**、**medium**、および **high** を Syslog 重大度にマップするための値を選択します。 このオプションには次のレベルがあります。 • 緊急 **(Emergency)** - システムが停止しているかまたは使用不可の状態です。 • アラート **(Alert)** - システムはユーザーによる即時の入力または介入を必要としています。 • 重大 **(Critical)** - システムの重大な状態を修正する必要があります。 • エラー **(Error)** - 緊急ではない障害がシステムで発生しています。 • 警告 **(Warning)** - システムに、エラーが発生する可能性を示す警告メッセージがあります。 • 注意 **(Notice)** - システムに通知があります。即時アクションは不要です。 • 通知 **(Informational)** - 通常の運用メッセージです。
通知送信の条件 **(Send Notification If)**	以下のチェック・ボックスを選択します。 • 攻撃定義でこの通知オプションが明示的に有効化されている **(The attack definition has this notification option explicitly enabled)** • 次の通知フィルターに一致する **(The following notification filter is matched)**」。リストから「重大度**:** 通知以上 **(Severity Informational and later)**」を選択します。
IPS 検疫アラートの通知 **(Notify on IPS Quarantine Alert)**	IPS 検疫の通知のオプションとして「いいえ **(No)**」を選択します。
メッセージ設定 **(Message Preference)**	「カスタマイズ **(Customized)**」オプションを選択します。

7. 「メッセージ設定 **(Message Preference)**」フィールドで「編集 **(Edit)**」をクリックし、カスタム・メッセージ・フィルターを追加します。
8. アラート通知を正しくフォーマットするため、以下のメッセージ文字列を入力します。

```
|$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$
"$IV_ATTACK_NAME$"|$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$
$IV_ATTACK_SIGNATURE$|$IV_ATTACK_CONFIDENCE$|$IV_ADMIN_DOMAIN$
$IV_SENSOR_NAME$|$IV_INTERFACE$|$IV_SOURCE_IP$|$IV_SOURCE_PORT$
$IV_DESTINATION_IP$|$IV_DESTINATION_PORT$|$IV_DIRECTION$
$IV_SUB_CATEGORY$
```

注**:** カスタム・メッセージ・ストリングは、改行やスペースを使用せずに 1 行で入力する必要があります。 McAfee Intrushield では、各アラート・エレメントの前後に区切り文字としてドル記号 ($) を使用したカスタム・メッセージのフォーマットが必要です。エレメントのドル記号がないと、アラート・イベントが正しくフォーマットされない可能性があります。

テキスト・エディターで、カスタム・メッセージ文字列を 1 行で入力し、適切にフォーマットする必要があります。

9. 「保存」をクリックします。

McAfee Intrushield により生成されたアラート・イベントは、指定した Syslog 宛先に転送されます。十分な数のイベントが McAfee Intrushield アプライアンスによって転送されると、ログ・ソースが自動的に検出されます。通常、ログ・ソースの自動検出に必要なイベントの最小数は 25 です。

次のタスク

管理者は QRadar コンソールにログインして、QRadar コンソールでログ・ソースが作成されていることと、「ログ・アクティビティー」タブに McAfee Intrushield アプライアンスからのイベントが表示されていることを確認できます。

McAfee Intrushield V6.x および V7.x の障害通知イベントの設定

McAfee Intrushield に障害通知を統合するには、障害通知イベントを転送するように McAfee Intrushield を構成する必要があります。

手順

1. McAfee Intrushield Manager のユーザー・インターフェースにログインします。
2. 「**Network Security Manager**」ダッシュボードで「構成 **(Configure)**」をクリックします。
3. 「リソース・ツリー **(Resource Tree)**」を展開し、「**IPS** 設定 **(IPS Settings)**」ノードを展開します。
4. 「障害通知 **(Fault Notification)**」タブをクリックします。
5. 「アラート通知 **(Alert Notification)**」メニューで「**Syslog**」タブをクリックします。
6. 障害通知イベントを転送するため、以下のパラメーターを構成します。

表 *266. McAfee Intrushield v6.x* および *7.x* の障害通知パラメーター

パラメーター	説明
Syslog 通知を有効にする **(Enable Syslog Notification)**	McAfee Intrushield の Syslog 通知を有効にするには「はい **(Yes)**」を選択します。イベントを QRadar に転送するには、このオプションを有効にする必要があります。
管理ドメイン **(Admin Domain)**	以下のいずれかのオプションを選択します。 • 「現行 **(Current)**」 - 現行ドメインのアラートの Syslog 通知を送信するには、このチェック・ボックスを選択します。このオプションはデフォルトで選択されています。 • 「子 **(Children)**」 - 現行ドメイン内の子ドメインのアラートの Syslog 通知を送信するには、このチェック・ボックスを選択します。

表 266. *McAfee Intrushield v6.x* および *7.x* の障害通知パラメーター (続き)

パラメーター	説明
サーバー名または **IP** アドレス **(Server Name or IP Address)**	QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。このフィールドでは、IPv4 アドレスと IPv6 アドレスの両方がサポートされています。
ポート	Syslog イベントのポートとして **514** を入力します。
ファシリティー **(Facilities)**	Syslog ファシリティー値を選択します。
重大度マッピング **(Severity Mappings)**	アラート通知レベル **informational**、**low**、**medium**、および **high** を Syslog 重大度にマップするための値を選択します。 このオプションには次のレベルがあります。 • 緊急 **(Emergency)** - システムが停止しているかまたは使用不可の状態です。 • アラート **(Alert)** - システムはユーザーによる即時の入力または介入を必要としています。 • 重大 **(Critical)** - システムの重大な状態を修正する必要があります。 • エラー **(Error)** - 緊急ではない障害がシステムで発生しています。 • 警告 **(Warning)** - システムに、エラーが発生する可能性を示す警告メッセージがあります。 • 注意 **(Notice)** - システムに通知があります。即時アクションは不要です。 • 通知 **(Informational)** - 通常の運用メッセージです。
障害を転送する重大度レベル **(Forward Faults with severity level)**	「通知以上 **(Informational and later)**」を選択します。
メッセージ設定 **(Message Preference)**	「カスタマイズ **(Customized)**」オプションを選択します。

7. 「メッセージ設定 **(Message Preference)**」フィールドで「編集 **(Edit)**」をクリックし、カスタム・メッセージ・フィルターを追加します。
8. 障害通知を正しくフォーマットするため、以下のメッセージ・ストリングを入力します。

   ```
   |%INTRUSHIELD-FAULT|$IV_FAULT_NAME$|$IV_FAULT_TIME$|
   ```

   注**:** カスタム・メッセージ・ストリングは、改行を使用せずに 1 行で入力する必要があります。 McAfee Intrushield では、各エレメントの前後にドル記号 ($) の区切り文字を使用したカスタム・メッセージ・フォーマットが必要です。エレメントのドル記号がないと、イベントが正しく解析されない可能性があります。
9. 「保存」をクリックします。

McAfee Intrushield により生成された障害イベントは、指定した Syslog 宛先に転送されます。

次のタスク

管理者は QRadar コンソールにログインして、「ログ・アクティビティー」タブに McAfee Intrushield アプライアンスからの障害イベントが表示されていることを確認できます。

McAfee Web Gateway

IBM Security QRadar と統合するように McAfee Web Gateway を構成することができます。

以下のいずれかのメソッドを使用します。

- 698 ページの『QRadar と通信するための McAfee Web Gateway の構成 (syslog)』
- 700 ページの『IBM Security QRadar と通信するための McAfee Web Gateway の構成 (ログ・ファイル・プロトコル)』

注: McAfee Web Gateway は、以前は McAfee WebWasher と呼ばれていました。

以下の表は、McAfee Web Gateway DSM の仕様を示しています。

表 *267. McAfee Web Gateway DSM* の仕様

仕様	値
製造元	McAfee
DSM	McAfee Web Gateway
RPM ファイル名	`DSM-McAfeeWebGateway-qradarversion-buildnumber.noarch`
サポートされるバージョン	v6.0.0 以降
プロトコル	syslog、ログ・ファイル・プロトコル
QRadar 記録されるイベント	すべての関連イベント
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	McAfee の Web サイト (http://www.mcafee.com)

McAfee Web Gateway DSM の統合プロセス

McAfee Web Gateway DSM を IBM Security QRadar と統合することができます。

以下の手順を使用します。

- ご使用の QRadar コンソールに最新バージョンの McAfee Web Gateway DSM RPM をダウンロードしてインストールします。

- McAfee Web Gateway の各インスタンスごとに、McAfee Web Gateway VPN システムを構成して QRadar との通信を有効にします。
- QRadar がログ・ソースを自動で検出しない場合は、統合する McAfee Web Gateway サーバーごとに、QRadar コンソール上でログ・ソースを作成します。
- McAfee Web Gateway v7.0.0 以降を使用する場合は、イベント・マップを作成します。

関連タスク

『QRadar と通信するための McAfee Web Gateway の構成 (syslog)』

700 ページの『IBM Security QRadar と通信するための McAfee Web Gateway の構成 (ログ・ファイル・プロトコル)』

701 ページの『McAfee Web Gateway イベント用のイベント・マップの作成』

QRadar と通信するための McAfee Web Gateway の構成 (syslog)

McAfee Web Gateway からすべてのイベントを収集するには、Syslog サーバーとして IBM Security QRadar を指定し、メッセージ・フォーマットを構成する必要があります。

手順

1. McAfee Web Gateway コンソールにログインします。
2. 「ツールバー **(Toolbar)**」で「構成 **(Configuration)**」をクリックします。
3. 「ファイル・エディター **(File Editor)**」タブをクリックします。
4. 「アプライアンス・ファイル **(Appliance Files)**」を展開し、`/etc/rsyslog.conf` ファイルを選択します。

   ファイル・エディターに、編集のために `rsyslog.conf` ファイルが表示されます。
5. `rsyslog.conf` ファイルを変更して、以下の情報を追加します。

   ```
   # send access log to qradar *.info;
   daemon.!=info;
   mail.none;authpriv.none;
   cron.none -/var/log/messages *.info;mail.none;
   authpriv.none;
   cron.none
   @<IP Address>:<Port>
   ```

   各部分について以下で説明します。

   - *<IP Address>* は QRadar の IP アドレスです。
   - *<Port>* は Syslog ポート番号 (514 など) です。
6. 「変更の保存 **(Save Changes)**」をクリックします。

   これで、McAfee Web Gateway アプライアンスで Syslog ハンドラーのポリシーをインポートする準備ができました。詳しくは、 699 ページの『Syslog ログ・ハンドラーのインポート』を参照してください。

Syslog ログ・ハンドラーのインポート

このタスクについて

Syslog ハンドラーのポリシー・ルール・セットをインポートするには、以下のようにします。

手順

1. サポート Web サイトから以下の圧縮ファイルをダウンロードします。

   ```
   log_handlers-1.1.tar.gz
   ```

2. ファイルを解凍します。

   解凍ファイルに含まれている XML ファイルは、ご使用の McAfee Web Gateway アプライアンスのバージョンに依存します。

表 268. McAfee Web Gateway に必要なログ・ハンドラー・ファイル

バージョン	必要な **XML** ファイル
McAfee Web Gateway V7.0	syslog_loghandler_70.xml
McAfee Web Gateway V7.3	syslog_loghandler_73.xml

3. McAfee Web Gateway コンソールにログインします。
4. メニュー・ツールバーで「ポリシー **(Policy)**」をクリックします。
5. 「ログ・ハンドラー **(Log Handler)**」をクリックします。
6. メニュー・ツリーを使用して「デフォルト **(Default)**」を選択します。
7. 「追加 **(Add)**」リストから「ライブラリーのルール・セット **(Rule Set from Library)**」を選択します。
8. 「ファイルからインポート **(Import from File)**」ボタンをクリックします。
9. ダウンロードした syslog_handler ファイルが含まれているディレクトリーにナビゲートし、インポートするファイルとして **syslog_loghandler.xml** を選択します。

   注**:** McAfee Web Gateway アプライアンスがルール・セットとの競合を検出した場合は、競合を解決する必要があります。詳しくは、*McAfee Web Gateway* の資料 を参照してください。
10. 「**OK**」をクリックします。
11. 「変更の保存 **(Save Changes)**」をクリックします。
12. これで、QRadar でログ・ソースを構成する準備ができました。

    QRadar は、McAfee Web Gateway アプライアンスからの Syslog イベントを自動的に検出します。

    Syslog イベントを受け取るように QRadar を手動で構成する場合は、「ログ・ソース・タイプ」リストから「McAfee Web Gateway」を選択します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

IBM Security QRadar と通信するための McAfee Web Gateway の構成 (ログ・ファイル・プロトコル)

McAfee Web Gateway アプライアンスでは、QRadar が取得できるように、中間ファイル・サーバーへイベント・ログ・ファイルを転送することができます。

手順

1. サポート Web サイトから以下のファイルをダウンロードします。

   `log_handlers-1.1.tar.gz`
2. ファイルを解凍します。

   これにより、McAfee Web Gateway アプライアンスを構成するために必要なアクセス・ハンドラー・ファイルが使用可能になります。

   `access_log_file_loghandler.xml`
3. McAfee Web Gateway コンソールにログインします。
4. メニュー・ツールバーで「ポリシー **(Policy)**」をクリックします。

   注**:** McAfee Web Gateway アプライアンスに既存のアクセス・ログ構成がある場合は、`access_log_file_loghandler.xml` を追加する前に、「ルール・セット・ライブラリー **(Rule Set Library)**」から既存のアクセス・ログを削除する必要があります。
5. 「ログ・ハンドラー **(Log Handler)**」をクリックします。
6. メニュー・ツリーを使用して「デフォルト **(Default)**」を選択します。
7. 「追加 **(Add)**」リストから「ライブラリーのルール・セット **(Rule Set from Library)**」を選択します。
8. 「ファイルからインポート **(Import from File)**」ボタンをクリックします。
9. ダウンロードした `access_log_file_loghandler.xml` ファイルが含まれているディレクトリーにナビゲートし、インポートするファイルとして `syslog_loghandler.xml` を選択します。

   `access_log_file_loghandler.xml` のルール・セットのインポート時に、現在の構成にはアクセス・ログ構成が既に存在していることを示す競合が発生し、競合解決策が表示されることがあります。
10. アクセス・ログ構成が既に存在することが McAfee Web Gateway アプライアンスによって検出された場合は、ルール・セットの解決のために表示される「競合解決: 名前の変更 **(Conflict Solution: Change name)**」オプションを選択します。

    競合の解決について詳しくは、*McAfee Web Gateway* のベンダー資料 を参照してください。

    自動ローテーションで `access.log` ファイルが中間サーバーにプッシュされるように構成する必要があります。ファイルを中間サーバーにプッシュする条件

は、access.log ファイルの時刻またはサイズのいずれでもかまいません。自動ローテーションについて詳しくは、*McAfee Web Gateway* のベンダー資料 を参照してください。

注**:** 生成される access.log ファイルのサイズから、McAfee Web Gate アプライアンスでのローテーション後にオプションの GZIP ファイルを選択することをお勧めします。

11. 「**OK**」をクリックします。
12. 「変更の保存 **(Save Changes)**」をクリックします。

注**:** デフォルトでは、McAfee Web Gateway はアクセス・ログを /opt/mwg/log/user-defined-logs/access.log/ ディレクトリーに書き込むように構成されます。

次のタスク

これで、McAfee Web Gateway から access.log ファイルを受信するように QRadar を構成する準備ができました。詳しくは、『ログ・ファイル・プロトコルを使用したデータのプル』を参照してください。

ログ・ファイル・プロトコルを使用したデータのプル

ログ・ファイル・プロトコル・ソースにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。McAfee Web Gateway DSM は、ログ・ファイル・プロトコル・ソースを使用した access.log ファイルの一括ロードをサポートしています。McAfee Web Gateway アクセス・ログのデフォルト・ディレクトリーは /opt/mwg/log/user-defined-logs/access.log/ ディレクトリーです。

このタスクについて

QRadar でログ・ソースとプロトコルを構成できます。

手順

1. McAfee Web Gateway アプライアンスからイベントを受け取るように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**McAfee Web Gateway**」を選択します。
2. プロトコルを構成するため、「プロトコル構成」リストから「ログ・ファイル」オプションを選択する必要があります。
3. 「ファイル・パターン」パラメーターを構成するため、access.log ファイルの正規表現文字列 (access[0-9]+¥.log など) を入力する必要があります。

注**:** access.log ファイルを **GZIP** で圧縮することを選択した場合は、「ファイル・パターン」フィールドに access[0-9]+¥.log¥.gz と入力し、「プロセッサー」リストから「**GZIP**」を選択する必要があります。

McAfee Web Gateway イベント用のイベント・マップの作成

McAfee Web Gateway v7.0.0 以降から収集したイベントはすべて、イベント・マッピングが必要です。

デバイスの各イベントは、個別に IBM Security QRadar のイベント・カテゴリーにマップすることができます。イベントをマップすることで、QRadar は、ネットワーク・デバイスからの繰り返しイベントを識別、統合、および追跡できます。イベントをマップしない限り、McAfee Web Gateway の「ログ・アクティビティー」タブに表示される一部のイベントは不明として分類され、一部のイベントは既存の QID マップに既に割り当てられている場合があります。不明なイベントは「イベント名」列に示され、「下位カテゴリー」列に「不明」と表示されるため、簡単に分かります。

不明イベントの検出

この手順では、すべてのイベント・タイプをマップしており、頻繁に生成されないイベントが欠落していないことを確認できます。この手順は、一定期間にわたって繰り返し実行します。

手順

1. QRadar にログインします。
2. 「ログ・アクティビティー」タブをクリックします。
3. 「フィルターの追加」をクリックします。
4. 最初のリストから「ログ・ソース」を選択します。
5. 「ログ・ソース・グループ」リストから、ログ・ソース・グループまたは「その他」を選択します。

   グループに割り当てられていないログ・ソースは「その他」に分類されます。
6. 「ログ・ソース」リストで McAfee Web Gateway ログ・ソースを選択します。
7. 「フィルターの追加」をクリックします。

   「ログ・アクティビティー」タブに、ログ・ソース用のフィルターが表示されます。
8. 「表示」リストから「過去 **1** 時間」を選択します。

   過去 1 時間に McAfee Web Gateway DSM により生成されたすべてのイベントが表示されます。「イベント名」列、または「下位カテゴリー」列に「不明」として表示されているイベントについては、イベント・マッピングが必要です。

   注**:** 「条件の保存」をクリックすると、既存の検索フィルターを保存することができます。

   これで、イベント・マップを変更する準備ができました。

イベント・マップの変更

イベント・マップを変更し、イベントを QRadar ID (QID) マップに手動で分類します。

このタスクについて

ログ・ソースに分類されたイベントはすべて、新しい QRadar ID (QID) に再マップできます。

注: ログ・ソースが定義されていないイベントは、イベントにマップできません。ログ・ソースのないイベントの場合、「ログ・ソース」列に「SIM 汎用ログ (SIM Generic Log)」と表示されます。

手順

1. 「イベント名」列で、McAfee Web Gateway の不明イベントをダブルクリックします。

   詳細なイベント情報が表示されます。
2. 「イベントのマップ」をクリックします。
3. 「QRadar ID の参照 (Browse for QRadar ID)」ペインから、以下のいずれかの検索オプションを選択して、QRadar ID (QID) のイベント・カテゴリーを絞り込みます。
   - 「上位カテゴリー」リストから、上位イベント・カテゴリーを選択します。
   - 「下位カテゴリー」リストから、下位イベント・カテゴリーを選択します。
   - 「ログ・ソース・タイプ」リストから、ログ・ソース・タイプを選択します。

   「ログ・ソース・タイプ」リストでは、他のログ・ソースからの QID を検索できます。イベントが既存の別のネットワーク・デバイスからのイベントに類似している場合、ログ・ソースで QID を検索すると便利です。例えば、McAfee Web Gateway がポリシー・イベントを提供する場合、類似するイベントをキャプチャーする可能性のある別の製品を選択することがあります。

   名前で QID を検索するには、「**QID/**名前」フィールドに名前を入力します。

   「**QID/**名前」フィールドでは、特定の単語 (例: policy) で QID の完全なリストをフィルタリングできます。
4. 「検索」をクリックします。

   QID のリストが表示されます。
5. 不明なイベントに関連付ける QID を選択します。
6. 「**OK**」をクリックします。

   QRadar は、イベント・ペイロードに一致する 同じ QID を持つデバイスから転送されるすべての追加イベントをマップします。QRadar によってイベントが識別されるたびに、イベントの数が増加します。

   新しい QRadar ID (QID) マップでイベントを更新する場合、QRadar に保管されている過去のイベントは更新されません。新しいイベントだけが新しい QID によって分類されます。

第 80 章 MetaInfo MetaIP

MetaInfo MetaIP DSM for IBM Security QRadar は、Syslog を使用して MetaIP イベントを受け取ります。

このタスクについて

QRadar は、イベントからの入手可能な関連情報をすべて記録します。QRadar で MetaIP デバイスを構成する前に、Syslog イベントを転送するようにデバイスを構成する必要があります。MetaInfo MetaIP アプライアンスの構成について詳しくは、ベンダーの資料を参照してください。

MetaInfo MetaIP アプライアンスを構成したら、QRadar の構成は完了です。QRadar は、MetaInfo MetaIP アプライアンスから転送される Syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ただし、QRadar 用のログ・ソースを手動で作成して Syslog イベントを受信することもできます。以下の構成手順はオプションです。

MetaInfo MetaIP のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Metainfo MetaIP**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   Syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 269. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	MetaInfo MetaIP アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。

12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 81 章 Microsoft

IBM Security QRadar は、さまざまな Microsoft 製品をサポートしています。

Microsoft Azure

Microsoft Azure 用の IBM Security QRadar DSM は、Azure アクティビティー・ログからイベントを収集します。

以下の表では、Microsoft Azure DSM の仕様について説明しています。

表 270. *Microsoft Azure DSM* の仕様

仕様	値
製造元	Microsoft
DSM 名	Microsoft Azure
RPM ファイル名	DSM-MicrosoftAzure-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	N/A
プロトコル	Syslog
イベント・フォーマット	LEEF
記録されるイベント・タイプ	Authorization Classic Compute Classic Storage Compute Insights KeyVault SQL Storage
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Microsoft Azure の Web サイト (https://azure.microsoft.com)

Azure アクティビティー・ログを QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードし、QRadar コンソールでインストールしてください。
   - DSMCommon RPM

- Microsoft Azure DSM RPM

2. Syslog イベントを QRadar に送信するように Microsoft Azure Log Integration サービスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合は、QRadar コンソール で Microsoft Azure ログ・ソースを追加してください。以下の表では、Microsoft Azure イベントの収集用に固有の値を必要とするパラメーターについて説明しています。

表 271. *Microsoft Azure* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Microsoft Azure
プロトコル構成	Syslog
ログ・ソース ID	Microsoft Azure イベントを QRadar に送信するデバイスの IP アドレスまたはホスト名。

以下の表は、Microsoft Azure DSM のサンプル Syslog イベント・メッセージを記載しています。

表 272. *Microsoft Azure* のサンプル *Syslog* メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
仮想マシンの再起動。	開始アクティビティーが試行されました	LEEF:1.0|Microsoft|Azure Resource Manager|1.0| MICROSOFT.CLASSICCOMPUTE /VIRTUALMACHINES/RESTART/ ACTION|devTime=Jun 07 2016 17:04:26 devTimeFormat =MMM dd yyyy HH:mm:ss cat=Compute src= 10.0.0.2 usrName =erica@example.com sev=4 resource= testvm resourceGroup=Test Resource Group description =Restart a Virtual Machine

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信のための Microsoft Azure の構成

Microsoft Azure からイベントを収集するには、Microsoft Azure Log Integration サービスをインストールする必要があります。インストール先のマシンはオンプレミスでも Cloud 内でもかまいませんが、64 ビット Windows OS を実行している、.Net 4.5.1 を備えたマシンである必要があります。

手順

1. 以前のバージョンの Microsoft Azure Log Integration サービスがインストールされている場合、以前のバージョンはアンインストールする必要があります。アンインストールすると、登録済みのソースがすべて削除されます。Microsoft Azure Log Integration サービスをアンインストールするには、以下のステップを実行します。
   a. Windows コマンド・ライン・インターフェースを管理者として開き、以下のコマンドを記載されている順に入力します。
      - `cd C:¥Program Files¥Microsoft Azure Log Integration¥`
      - `azlog removeazureid`
   b. 「コントロール パネル」で、「プログラムの追加と削除」 > 「**Microsoft Azure Log Integration**」 > 「アンインストール」をクリックします。
2. Microsoft Azure Log Integration サービス (`AzureLogIntegration.msi`) を Microsoft の Web サイト (https://azure.microsoft.com/en-us/documentation/articles/security-azure-log-integration-get-started/) から取得してインストールします。
3. Windows コマンド・ライン・インターフェースを管理者として開きます。
4. Microsoft Azure Log Integration サービスを構成するには、コマンド `cd C:¥Program Files¥Microsoft Azure Log Integration¥` を実行してディレクトリーを移動してから、以下のステップを実行します。
   a. コマンド `azlog.exe powershell` を入力して Azure PowerShell を実行します。
   b. 「PowerShell」で、コマンド `Add-AzLogEventDestination -Name <QRadar_Console_name> -SyslogServer <IP_address> -SyslogFormat LEEF` を入力します。

      QRadar の Syslog リスナーがデフォルト・ポート上にない場合は、**SyslogPort** を指定できます。デフォルトは 514 です。例:

      ```
      Add-AzLogEventDestination -Name <QRadar_Console_name> -SyslogServer
      <IP_address> -SyslogPort <port_number> -SyslogFormat LEEF
      ```
   c. コマンド `.¥azlog.exe createazureid` を実行し、プロンプトに Azure ログイン資格情報を入力します。
   d. サブスクリプションに読み取り権限を割り当てるには、コマンド `.¥azlog authorize <Subscription_ID>` を入力します。

Microsoft DHCP Server

Microsoft DHCP Server DSM for IBM Security QRadar は、Microsoft DHCP サーバー・プロトコルまたは WinCollect を使用して DHCP イベントを受け取ります。

このタスクについて

Microsoft DHCP サーバーを QRadar と統合する前に、監査ロギングを有効にする必要があります。

Microsoft DHCP サーバーを構成するには、以下のようにします。

手順

1. DHCP サーバー管理ツールにログインします。
2. DHCP サーバー管理ツールで DHCP サーバーを右クリックし、「プロパティ」を選択します。

   「プロパティ」ウィンドウが表示されます。
3. 「一般 **(General)**」タブをクリックします。

   「全般」ペインが表示されます。
4. 「**DHCP** 監査ログを記録する」をクリックします。

   監査ログ・ファイルは午前 0 時に作成されます。このファイルには、3 文字の曜日の省略形が含まれている必要があります。

表 *273. Microsoft DHCP* ログ・ファイルの例

ログ・タイプ	例
IPv4	`DhcpSrvLog-Mon.log`
IPv6	`DhcpV6SrvLog-Wed.log`

   デフォルトでは、Microsoft DHCP は監査ログを `%WINDIR%¥system32¥dhcp¥` ディレクトリーに書き込むように構成されています。
5. DHCP サービスを再始動します。
6. QRadar でログ・ソースとプロトコルを構成できます。
   a. Microsoft DHCP サーバーからイベントを受け取るように QRadar を構成するには、「ログ・ソース・タイプ」リストで「Microsoft **DHCP** サーバー」オプションを選択する必要があります。
   b. プロトコルを構成するには、「プロトコル構成」リストから「Microsoft DHCP」オプションを選択する必要があります。

      注**:** WinCollect を使用して Microsoft DHCP Server バージョン 2000/2003 を QRadar と統合するには、「*IBM Security QRadar WinCollect* ユーザー・ガイド」を参照してください。

関連概念:

24 ページの『Microsoft DHCP プロトコルの構成オプション』
Microsoft DHCP サーバーからイベントを受信するには、Microsoft DHCP プロトコルを使用するようにログ・ソースを構成します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Microsoft Endpoint Protection

IBM Security QRadar 用の Microsoft Endpoint Protection DSM は、マルウェア検出イベントを収集できます。

QRadar でマルウェア検出イベントを取得するには、JDBC プロトコルを構成します。マルウェア検出イベントを QRadar に追加すると、デプロイメント内をモニターし、マルウェアに感染したコンピューターを検出できるようになります。

マルウェア検出イベントには、次のイベント・タイプがあります。

- マルウェアが検出されたサイト名と送信元。
- 脅威名、脅威 ID、および重大度。
- 脅威に関連付けられたユーザー ID。
- イベント・タイプ、タイム・スタンプ、およびマルウェアに対して実行したクリーンアップ・アクション。

構成の概要

Microsoft Endpoint Protection DSM は、JDBC を使用して SQL データベースをポーリングし、マルウェア検出イベント・データを収集します。この DSM は、自動検出は行いません。Microsoft EndPoint Protection を QRadar と統合するには、以下の手順を実行します。

1. マルウェア検出イベント・データの SQL データベース・ビューを QRadar 用に作成します。
2. Microsoft EndPoint Protection データベースからイベントをポーリングするように JDBC ログ・ソースを構成します。
3. Microsoft EndPoint Protection に関連付けられたデータベースと QRadar との間の通信をブロックするようなファイアウォール・ルールがないことを確認します。

データベース・ビューの作成

Microsoft EndPoint Protection は、SQL Server Management Studio (SSMS) を使用して EndPoint Protection SQL データベースを管理します。

手順

1. Microsoft EndPoint Protection SQL データベースをホストしているシステムにログインします。
2. 「スタート」メニューから「ファイル名を指定して実行」を選択します。
3. 以下のコマンドを入力します。

   ```
   ssms
   ```
4. 「**OK**」をクリックします。
5. Microsoft Endpoint Protection データベースにログインします。
6. 「オブジェクト エクスプローラー」で「データベース」を選択します。
7. データベースを選択し、「ビュー」をクリックします。
8. ナビゲーション・メニューで「新しいクエリ」をクリックします。
9. 「クエリ」ペインで、データベース・ビューを作成する以下の Transact-SQL ステートメントを入力します。

   ```
   create view dbo.MalwareView as select n.Type
   , n.RowID , n.Name , n.Description , n.Timestamp
   , n.SchemaVersion , n.ObserverHost , n.ObserverUser
   ```

```
, n.ObserverProductName , n.ObserverProductversion
, n.ObserverProtectionType , n.ObserverProtectionVersion
, n.ObserverProtectionSignatureVersion , n.ObserverDetection
, n.ObserverDetectionTime , n.ActorHost , n.ActorUser
, n.ActorProcess , n.ActorResource , n.ActionType
, n.TargetHost , n.TargetUser , n.TargetProcess
, n.TargetResource , n.ClassificationID
, n.ClassificationType , n.ClassificationSeverity
, n.ClassificationCategory , n.RemediationType
, n.RemediationResult , n.RemediationErrorCode
, n.RemediationPendingAction , n.IsActiveMalware
, i.IP_Addresses0 as 'SrcAddress'

from v_AM_NormalizedDetectionHistory n,
System_IP_Address_ARR i, v_RA_System_ResourceNames s,
Network_DATA d where n.ObserverHost = s.Resource_Names0
and s.ResourceID = d.MachineID and d.IPEnabled00 = 1
and d.MachineID = i.ItemKey and i.IP_Addresses0 like '%.%.%.%';
```

10. 「クエリ」ペインで右クリックして、「実行」を選択します。

    ビューが作成されると、結果ペインに以下のメッセージが表示されます。

    コマンドは正常に完了しました。

次のタスク

これで、ログ・ソースを IBM Security QRadar で構成することができます。

ログ・ソースの構成

IBM Security QRadar では、Microsoft EndPoint Protection データベースで作成したビューにアクセスするための適切な資格情報が設定されたユーザー・アカウントが必要です。

このタスクについて

Microsoft EndPoint Protection データベースからマルウェア検出イベントを正常にポーリングするには、新規ユーザーを作成するか、または作成したデータベース・ビューからの読み取りのための既存のユーザー資格情報をログ・ソースに指定する必要があります。ユーザー・アカウントの作成について詳しくは、ベンダーの資料を参照してください。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストから、「Microsoft **EndPoint Protection**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. 以下の値を構成します。

表 274. *Microsoft EndPoint Protection* の *JDBC* パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 <*Database*>@<*Database Server IP or Host Name*> 各部分について以下で説明します。 • <*Database*> は、「データベース名」パラメーターに入力するデータベース名です。 • <*Database Server IP or Host Name*> は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	Microsoft EndPoint Protection データベースの名前を入力します。 この名前は、 711 ページの『データベース・ビューの作成』 でビューを作成するときに選択するデータベース名と一致している必要があります。
IP またはホスト名	Microsoft EndPoint Protection SQL サーバーの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。 MSDE のデフォルト・ポートは 1433 です。 JDBC 構成のポートは、Microsoft EndPoint Protection データベースのリスナー・ポートに一致していなければなりません。 Microsoft EndPoint Protection データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして「MSDE」を使用するときに「データベース・インスタンス」を定義する場合は、構成の「ポート」パラメーターをブランクのままにしておく必要があります。
ユーザー名	ログ・ソースが Microsoft EndPoint Protection データベースへのアクセスに使用できるユーザー名を指定します。
パスワード	ログ・ソースが Microsoft EndPoint Protection データベースへのアクセスに使用できるパスワードを入力します。 パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」フィールドに入力したパスワードと同一である必要があります。
認証ドメイン	「データベース・タイプ」で *MSDE* を選択し、データベースが Windows 用に構成されている場合は、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。

表 274. *Microsoft EndPoint Protection* の *JDBC* パラメーター (続き)

パラメーター	説明
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックする場合は、構成内で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを含むテーブルまたはビューの名前として `dbo.MalwareView` と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに * を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	比較フィールドとして `Timestamp` と入力します。比較フィールドを使用して、テーブルに対する照会から次の照会までの間に追加されたい新しいイベントを特定できます。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
準備済みステートメントの使用 **(Use Prepared Statements)**	「準備済みステートメントの使用 **(Use Prepared Statements)**」チェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、そのステートメントを別のパラメーターで何度も使用できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (作成したビューに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。

表 274. *Microsoft EndPoint Protection の JDBC パラメーター (続き)*

パラメーター	説明
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。
NTLMv2 の使用	「**NTLMv2** の使用 **(Use NTLMv2)**」チェック・ボックスを選択します。 このオプションを選択すると、NTLMv2 認証を必要とする SQL サーバーとの通信時に、MSDE 接続で NTLMv2 プロトコルが強制的に使用されます。このチェック・ボックスはデフォルトで選択されています。 「**NTLMv2** の使用」チェック・ボックスを選択した場合でも、NTLMv2 認証を必要としない SQL サーバーへの MSDE 接続には影響しません。

注**:** 「信頼性」パラメーターに 5 よりも大きい値を選択すると、Microsoft EndPoint Protection ログ・ソースに対し、QRadar の他のログ・ソースよりも高い重要度が設定されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

Microsoft EndPoint Protection の構成は完了です。

Microsoft SQL Server

Microsoft SQL Server 用の IBM Security QRadar DSM は、syslog プロトコル、WinCollect Microsoft SQL プロトコル、または JDBC プロトコルを使用して、SQL イベントを収集します。

以下の表は、Microsoft SQL Server DSM の仕様を示しています。

表 275. *Microsoft SQL Server DSM*

仕様	値
製造元	Microsoft
DSM 名	SQL Server

表 275. *Microsoft SQL Server DSM (続き)*

仕様	値
RPM ファイル名	DSM-MicrosoftSQL-><*QRadar-version-Build_number*>.noarch.rpm
サポートされるバージョン	2008、2012、および 2014 (Enterprise Edition のみ)
イベント・フォーマット	syslog、JDBC、WinCollect
QRadar で記録されるイベント・タイプ	SQL エラー・ログ・イベント
自動的に検出?	はい
ID を含む?	はい
その他の情報	Microsoft Web サイト (http://www.microsoft.com/en-us/server-cloud/products/sql-server/)

以下に示すいずれかの方法で、Microsoft SQL Server を QRadar に統合することができます。

JDBC Microsoft SQL Server Enterprise は、JDBC プロトコルを使用して監査イベントを取得することができます。取得された監査イベントはテーブル・ビューに格納されます。監査イベントを使用できるのは、Microsoft SQL Server 2008、2012、2014 Enterprise だけです。

WinCollect

Microsoft SQL Server が管理するデータベースから ERRORLOG メッセージを収集する WinCollect を使用することにより、Microsoft SQL Server 2000、2005、2008、2012、2014 を QRadar に統合することができます。詳しくは、WinCollect の資料を参照してください。

Microsoft SQL Server DSM を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Microsoft SQL Server RPM をダウンロードして QRadar コンソールにインストールしてください。
2. Microsoft SQL Server のインスタンスごとに、Microsoft SQL Server アプライアンスを構成して、QRadar と通信できるようにします。
3. QRadar が Microsoft SQL Server ログ・ソースを自動的に検出しない場合は、ネットワーク上の Microsoft SQL Server のインスタンスごとにログ・ソースを作成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に Microsoft SQL Server を準備する

QRadar との通信用に Microsoft SQL Server を準備するには、監査オブジェクト、監査仕様、データベース・ビューを作成する必要があります。

Microsoft SQL Server 監査オブジェクトの作成

監査イベントを保管するには、監査オブジェクトを作成します。

手順

1. Microsoft SQL Server Management Studio にログインします。
2. ナビゲーション・メニューで、「セキュリティ」>「監査」を選択します。
3. 「監査」を右クリックして「新しい監査」を選択します。
4. 「監査名」フィールドに、新しい監査ファイルの名前を入力します。
5. 「監査の出力先」リストで「ファイル」を選択します。
6. 「ファイル パス」フィールドに、Microsoft SQL Server 監査ファイルのディレクトリー・パスを入力します。
7. 「**OK**」をクリックします。
8. 監査オブジェクトを右クリックして「監査の有効化」を選択します。

Microsoft SQL Server 監査仕様の作成

監査ファイルに書き込まれる監査イベントのレベルを定義するには、監査仕様を作成します。

始める前に

監査オブジェクトを作成する必要があります。『Microsoft SQL Server 監査オブジェクトの作成』を参照してください。

このタスクについて

監査仕様は、サーバー・レベルで作成することも、データベース・レベルで作成することもできます。要件によっては、サーバーとデータベースの両方で監査仕様が必要になる場合があります。

手順

1. Microsoft SQL Server Management Studioの ナビゲーション・メニューで、以下に示すいずれかのオプションを選択します。
   - 「セキュリティ」>「サーバー監査の仕様」
   - <データベース> >「セキュリティ」>「データベース監査の仕様」
2. 「サーバー監査の仕様」を右クリックし、以下に示すいずれかのオプションを選択します。
   - 新しいサーバー監査の仕様
   - 新しいデータベース監査の仕様
3. 「名前」フィールドに、新しい監査ファイルの名前を入力します。
4. 「監査」リストで、作成した監査オブジェクトを選択します。
5. 「アクション」ペインで、サーバー監査にアクションとオブジェクトを追加します。

6. 「**OK**」をクリックします。
7. サーバー監査の仕様を右クリックし、以下に示すいずれかのオプションを選択します。
   - サーバー監査の仕様の有効化
   - データベース監査の仕様の有効化

Microsoft SQL Server データベース・ビューの作成

JDBC プロトコルを使用してデータベース表からの監査イベントを QRadar でポーリングできるようにするには、dbo.AuditData データベース・ビューを作成します。このデータベース・ビューには、サーバー監査仕様とデータベース監査仕様からの監査イベントが格納されます。

手順

1. Microsoft SQL Server Management Studio のツールバーで「新しいクエリ」をクリックします。
2. 以下の Transact-SQL ステートメントを入力します。

```
create view dbo.AuditData as
     SELECT * FROM sys.fn_get_audit_file
     ('<Audit File Path and Name>',default,default);
     GOa
```

   例えば、以下のようにします。

```
create view dbo.AuditData as
     SELECT * FROM sys.fn_get_audit_file
     ('C:¥inetpub¥logs¥SQLAudits*',default,default);
     GO
```

3. 標準ツールバーで「実行」をクリックします。

Microsoft SQL Server のログ・ソースの構成

QRadar コンソールが Microsoft Windows セキュリティー・イベントのログ・ソースを自動的に検出しなかった場合は、以下の手順を実行します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」ボタンをクリックします。
5. 「ログ・ソース・タイプ」リストで、「**Microsoft SQL Server**」を選択します。
6. 「プロトコル構成」リストで「**JDBC**」または「**WinCollect**」を選択します。
7. **オプション。JDBC** のイベントを構成する場合は、以下に示す Microsoft SQL Server ログ・ソース・パラメーターを構成します。

パラメーター	説明
ログ・ソース **ID**	以下の形式のログ・ソースの ID を入力します。 `<SQL Database>@<SQL DB Server IP or Host Name>` 各部分について以下で説明します。 `<SQL Database>` は、「データベース名」パラメーターに入力するデータベース名です。 <SQL DB Server IP or Host Name> は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	Microsoft SQL データベースの名前として、`Master` と入力します。
IP またはホスト名	Microsoft SQL Server の IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。MSDE のデフォルト・ポートは 1433 です。 JDBC 構成のポートは Microsoft SQL データベースのリスナー・ポートに一致していなければなりません。Microsoft SQL データベースには、QRadar との通信に使用可能な着信 TCP 接続が必要です。 **重要:** 「データベース・タイプ」として MSDE を使用する場合に「データベース・インスタンス」を定義するときは、構成の「ポート」パラメーターをブランクのままにする必要があります。
ユーザー名	SQL データベースにアクセスするユーザー名を入力します。
パスワード	SQL データベースにアクセスするパスワードを入力します。
パスワードの確認	SQL データベースにアクセスするパスワードを入力します。
認証ドメイン	「データベース・タイプ」として MSDE を選択し、データベースが Windows 用に構成されている場合は、**Window** 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。

パラメーター	説明
データベース・インスタンス	**オプション:** データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 **重要:** データベース構成に標準でないポートがある場合、または SQL データベース解決用のポート 1434 へのアクセスがブロックされている場合は、「データベース・インスタンス」パラメーターをブランクのままにする必要があります。
テーブル名	監査イベント・レコードを含むテーブルまたはビューの名前として、`dbo.AuditData` と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに `*` を入力します。 コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。このコンマ区切りリストの最大長は 255 文字です。ドル記号 ($)、番号記号 (#)、アンダースコアー (_)、en ダッシュ (-)、ピリオド (.) の各特殊文字を使用できます。
比較フィールド	「比較フィールド」パラメーターには `event_time` と入力します。「比較フィールド」によって、照会と照会の間に追加される新規イベントがテーブル内で特定されます。
開始日時	**オプション:** データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、`yyyy-MM-dd HH:mm` の形式で入力する必要があります (`HH` は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。

パラメーター	説明
準備済みステートメントの使用 **(Use Prepared Statements)**	準備済みステートメントを使用する場合は、このチェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで SQL ステートメントをセットアップし、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔の数値を入力できます。ポーリング間隔とは、イベント・テーブルに対する照会から次の照会までの間の時間です。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、`H` (時間) または `M` (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。`H` または `M` を付加せずに数値を入力した場合は、秒単位のポーリングになります。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名とパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義します。

8. **オプション。WinCollect** のイベントを構成する場合は、「*IBM Security QRadar WinCollect* ユーザー・ガイド」を参照してください。
9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

Microsoft Exchange Server

Microsoft Exchange Server 用の IBM Security QRadar DSM は、イベント・ログ・ファイルを対象にポーリングすることによって、Exchange イベントを収集します。

以下の表は、Microsoft Exchange Server DSM の仕様を示しています。

表 276. *Microsoft Exchange Server*

仕様	値
製造元	Microsoft
DSM 名	Exchange Server
RPM ファイル名	DSM-MicrosoftExchange-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	Microsoft Exchange 2003 Microsoft Exchange 2007 Microsoft Exchange 2010 Microsoft Exchange 2013 Microsoft Exchange 2016
プロトコル・タイプ	Microsoft Exchange 2003 用の WinCollect Microsoft Exchange 2007、2010、2013、および 2016 用の Microsoft Exchange プロトコル
QRadar で記録されるイベント・タイプ	Outlook Web Access のイベント (OWA) Simple Mail Transfer Protocol のイベント (SMTP) Message Tracking Protocol のイベント (MSGTRK)
自動的に検出?	いいえ
ID を含む?	いいえ
その他の情報	Microsoft Web サイト (http://www.microsoft.com)

Microsoft Exchange Server を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Microsoft Exchange Server DSM RPM をダウンロードしてください。
2. QRadar と通信できるように Microsoft Exchange Server DSM デバイスを構成します。
3. QRadar コンソール上で Microsoft Exchange Server DSM のログ・ソースを作成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に Microsoft Exchange Server を構成する

始める前に

Exchange Server とリモート・ホストの間にあるファイアウォールが、以下のポートでトラフィックを許可することを確認します。

- Microsoft エンドポイント・マッパー用の TCP ポート 135。
- NetBIOS ネーム・サービス用の UDP ポート 137。
- NetBIOS データグラム・サービス用の UDP ポート 138。
- NetBIOS セッション・サービス用の TCP ポート 139。
- Microsoft ディレクトリー・サービスが Windows 共有でファイルを転送するためのTCP ポート 445。

手順

1. OWA ログを構成します。
2. SMTP ログを構成します。
3. MSGTRK ログを構成します。

Microsoft Exchange Server 上での OWA ログの構成

IBM Security QRadar と通信するように Microsoft Exchange Server を準備するには、Outlook Web Access (OWA) イベント・ログを構成します。

手順

1. Microsoft Internet Information System (IIS) Manager にログインします。
2. デスクトップで、「スタート」>「実行」を選択します。
3. 以下のコマンドを入力します。

```
inetmgr
```

4. 「**OK**」をクリックします。
5. メニュー・ツリーで、「ローカル コンピューター」を展開します。

6. Microsoft Server 2003 用 IIS 6.0 Manager を使用している場合は、以下のステップを実行します。
   a. 「**Web** サイト」を展開します。
   b. 「既定の **Web** サイト」を右クリックして、「プロパティ」を選択します。
   c. 「アクティブ ログ形式」リストから「**W3C**」を選択します。
   d. 「プロパティ」をクリックします。
   e. 「拡張」タブをクリックします。
   f. プロパティーのリストで、「メソッド **(cs-method)**」および「プロトコル バージョン **(cs-version)**」チェック・ボックスを選択します。
   g. 「**OK**」をクリックします。
7. Microsoft Server 2008 R2 用 IIS 7.0 Manager、または Microsoft Server 2012 R2 用 IIS 8.5 を使用している場合は、次の手順を実行します。
   a. 「ログの記録」をクリックします。
   b. 「形式」リストから「**W3C**」を選択します。
   c. 「フィールドの選択」をクリックします。
   d. プロパティーのリストで、「メソッド **(cs-method)**」および「プロトコル バージョン **(cs-version)**」チェック・ボックスを選択します。
   e. 「**OK**」をクリックします。

Microsoft Exchange Server 2003、2007、および 2010 での SMTP ログの有効化

Microsoft Exchange Server 2003、2007、および 2010 が IBM Security QRadar と通信できるように準備するには、SMTP イベント・ログを有効にします。

手順

1. Exchange Management Console を始動します。
2. *receive connector* を構成するには、以下のいずれかのオプションを選択します。
   - エッジ・トランスポート・サーバーの場合は、コンソール・ツリーで「エッジ・トランスポート **(Edge Transport)**」を選択し、「受信コネクター **(Receive Connectors)**」タブをクリックします。
   - ハブ・トランスポート・サーバーの場合は、コンソール・ツリーで「サーバー・トランスポート **(Server Transport)**」>「ハブ・トランスポート **(Hub Transport)**」を選択し、「受信コネクター **(Receive Connectors)**」タブをクリックします。
3. 受信コネクターを選択し、「プロパティー」をクリックします。
4. 「一般 **(General)**」タブをクリックします。
5. 「プロトコルのロギング・レベル **(Protocol logging level)**」リストで「詳細」を選択します。
6. 「適用」をクリックします。
7. 「**OK**」をクリックします。
8. *send connector* を構成するには、以下のいずれかのオプションを選択します。

- エッジ・トランスポート・サーバーの場合は、コンソール・ツリーで「エッジ・トランスポート **(Edge Transport)**」を選択し、「送信コネクター **(Send Connectors)**」タブをクリックします。
- ハブ・トランスポート・サーバーの場合は、コンソール・ツリーで「組織構成 **(Organization Configuration)**」>「ハブ・トランスポート **(Hub Transport)**」を選択し、サーバーを選択してから「送信コネクター **(Send Connectors)**」タブをクリックします。

9. 送信コネクターを選択し、「プロパティー」をクリックします。
10. 「一般 **(General)**」タブをクリックします。
11. 「プロトコルのロギング・レベル **(Protocol logging level)**」リストで「詳細」を選択します。
12. 「適用」をクリックします。
13. 「**OK**」をクリックします。

Microsoft Exchange Server 2013 および 2016 での SMTP ログの有効化

Microsoft Exchange Server 2013 および 2016 が IBM Security QRadar と通信できるように準備するには、SMTP イベント・ログを有効にします。

手順

1. Exchange 管理センターを開始します。
2. *receive connector* を構成するには、「メール・フロー **(Mail Flow**」 > 「受信コネクター **(Receive Connectors)**」を選択します。
3. 受信コネクターを選択し、「編集」をクリックします。
4. 「一般 **(General)**」タブをクリックします。
5. 「プロトコルのロギング・レベル **(Protocol logging level)**」リストで「詳細」を選択します。
6. 「保存」をクリックします。
7. *send connector* を構成するには、「メール・フロー **(Mail Flow**」 > 「送信コネクター **(Send Connectors)**」を選択します。
8. 送信コネクターを選択し、「編集」をクリックします。
9. 「一般 **(General)**」タブをクリックします。
10. 「プロトコルのロギング・レベル **(Protocol logging level)**」リストで「詳細」を選択します。
11. 「保存」をクリックします。

Microsoft Exchange 2003、2007、および 2010 用の MSGTRK ログの構成

Microsoft Exchange Server によって作成されるメッセージ追跡ログには、Microsoft Exchange Server で発生した、メッセージ・パス情報を含むメッセージ・アクティビティーの詳細が記録されます。

このタスクについて

MSGTRK ログは、Microsoft Exchange 2007 または Exchange 2010 インストール済み環境ではデフォルトで有効になっています。以下の構成手順はオプションです。

MSGTRK イベント・ログを有効にするには、以下のようにします。

手順

1. Exchange Management Console を始動します。
2. サーバー・タイプに応じて受信コネクターを構成します。
   - エッジ・トランスポート・サーバー - コンソール・ツリーで「エッジ トランスポート」を選択し、「プロパティ」をクリックします。
   - ハブ・トランスポート・サーバー - コンソール・ツリーで「サーバーの構成」 > 「ハブ トランスポート」を選択し、サーバーを選択して「プロパティ」をクリックします。
3. 「ログの設定」タブをクリックします。
4. 「メッセージ追跡ログの有効化」チェック・ボックスを選択します。
5. 「適用」をクリックします。
6. 「**OK**」をクリックします。

   Exchange Server で MSGTRK イベントが有効になりました。

Exchange 2013 および 2016 用の MSGTRK ログの構成

Microsoft Exchange Server によって作成されるメッセージ追跡ログには、Exchange Server で発生した、メッセージ・パス情報を含むメッセージ・アクティビティーの詳細が記録されます。

手順

1. Exchange 管理センターを開始します。
2. 「サーバー」 > 「サーバー」をクリックします。
3. 構成するメールボックス・サーバーを選択し、「編集」をクリックします。
4. 「トランスポート ログ」をクリックします。
5. 「メッセージ追跡ログ」セクションで、次のパラメーターを構成します。

パラメーター	説明
メッセージ追跡ログを有効にする	サーバーで、メッセージ追跡を有効または無効にします。
メッセージ追跡ログのパス	指定する値は、ローカルの Exchange サーバーに存在する必要があります。フォルダーが存在しない場合、「保存」をクリックしたときに作成されます。

6. 「保存」をクリックします。

Microsoft Exchange のログ・ソースの構成

IBM Security QRadar は、Microsoft Exchange イベントを自動的に検出することはありません。Microsoft Exchange のイベント・データを統合するには、イベント・ログの収集元となるインスタンスごとにログ・ソースを作成する必要があります。

始める前に

Exchange Server 上のログ・フォルダー・パスに管理共有 (C$) が含まれている場合、NetBIOS アクセス権を持つユーザーにローカルまたはドメインの管理者権限が付与されていることを確認します。

このタスクについて

OWA、SNMP、および MSGTRK のフォルダー・パス・フィールドは、ドライブ名とパス情報を使用してデフォルトのファイル・パスを定義します。Microsoft Exchange Server 上のログ・ファイルの場所を変更した場合は、必ずログ・ソース構成に正しいファイル・パスを指定してください。Microsoft Exchange プロトコルは、イベント・ログの OWA、SMTP、および MSGTRK フォルダーのサブディレクトリーを読み取ることができます。

ディレクトリー・パスは、以下の形式で指定できます。

- 正 - `c$/LogFiles/`
- 正 - `LogFiles/`
- 誤 - `c:/LogFiles`
- 誤 - `c$¥LogFiles`

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで、「**Microsoft Exchange Server**」を選択します。
7. 「プロトコル構成」リストで「**Microsoft Exchange**」を選択します。
8. ログ・ソース・パラメーターを構成します。

Microsoft Exchange ログ・ソース・パラメーターの詳細**:**

パラメーター	説明
ログ・ソース ID	QRadar ユーザー・インターフェース内の Windows Exchange イベント・ソースを識別する IP アドレスまたはホスト名。
サーバー・アドレス	Microsoft Exchange Server の IP アドレス。

パラメーター	説明
SMTP ログ・フォルダーのパス	SMTP ログ・ファイルにアクセスするためのディレクトリー・パス。以下のいずれかのディレクトリー・パスを使用します。 • Microsoft Exchange 2003 の場合は、c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/ を使用します。 • Microsoft Exchange 2007 の場合は、c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/ を使用します。 • Microsoft Exchange 2010 の場合は、c$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/ProtocolLog/ を使用します。 • Microsoft Exchange 2013 の場合は、c$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/ProtocolLog/ を使用します。 • Microsoft Exchange 2016 の場合は、c$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/ProtocolLog/ を使用します。
OWA ログ・フォルダーのパス	OWA ログ・ファイルにアクセスするためのディレクトリー・パス。以下のいずれかのディレクトリー・パスを使用します。 • Microsoft Exchange 2003 の場合は、c$/WINDOWS/system32/LogFiles/W3SVC1/ を使用します。 • Microsoft Exchange 2007 の場合は、c$/WINDOWS/system32/LogFiles/W3SVC1/ を使用します。 • Microsoft Exchange 2010 の場合は、c$/inetpub/logs/LogFiles/W3SVC1/ を使用します。 • Microsoft Exchange 2013 の場合は、c$/inetpub/logs/LogFiles/W3SVC1/ を使用します。 • Microsoft Exchange 2016 の場合は、c$/inetpub/logs/LogFiles/W3SVC1/ を使用します。

パラメーター	説明
MSGTRK ログ・フォルダーのパス	メッセージ・トラッキング・ログ・ファイルにアクセスするためのディレクトリー・パス。メッセージ・トラッキングを使用できるのは、ハブ・トランスポート、メールボックス、またはエッジ・トランスポート・サーバーのロールが割り当てられている Microsoft Exchange 2007 サーバーのみです。以下のいずれかのディレクトリー・パスを使用します。 • Microsoft Exchange 2007 の場合は、`c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/MessageTracking/` を使用します。 • Microsoft Exchange 2010 の場合は、`c$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/MessageTracking/` を使用します。 • Microsoft Exchange 2013 の場合は、`c$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/MessageTracking/` を使用します。 • Microsoft Exchange 2016 の場合は、`c$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/MessageTracking/` を使用します。
ファイル読み取りの強制 (Force File Read)	プロトコルにログ・ファイルの読み取りを強制します。このチェック・ボックスはデフォルトで選択されます。このチェック・ボックスをクリアすると、ログ・ファイルの読み取りは、ログ・ファイル変更日時またはファイル・サイズの属性が変更された場合に行われます。

9. 残りのパラメーターを構成します。
10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

Microsoft Hyper-V

Microsoft Hyper-V 用の IBM Security QRadar DSM は、Microsoft Hyper-V サーバーからのイベント・ログを収集できます。

以下の表は、Microsoft Hyper-V Server DSM の仕様を示しています。

表 *277. Microsoft Hyper-V DSM* の仕様

仕様	値
製造元	Microsoft

表 277. *Microsoft Hyper-V DSM* の仕様 (続き)

仕様	値
DSM	Microsoft Hyper-V
RPM ファイル名	`DSM-MicrosoftHyperV-build_number.rpm`
サポートされるバージョン	v2008 および v2012
プロトコル	WinCollect
QRadar で記録されるイベント	すべての関連イベント
自動的に検出?	いいえ
ID を含む?	いいえ
その他の情報	http://technet.microsoft.com/en-us/windowsserver/dd448604.aspx

Microsoft Hyper-V DSM 統合プロセス

Microsoft Hyper-V DSM を IBM Security QRadar と統合できます。

以下の手順を実行します。

1. 最新の WinCollect RPM をダウンロードして、QRadar コンソールにインストールします。
2. Hyper-V システムか、または Hyper-V システムへの経路を持つ別のシステムに WinCollect エージェントをインストールします。既存の WinCollect エージェントを使用することもできます。詳しくは、「*IBM Security QRadar WinCollect* ユーザー・ガイド」を参照してください。
3. 自動更新が有効になっていない場合は、Microsoft Hyper-V 用の DSM RPM をダウンロードして、QRadar コンソールにインストールします。RPM は 1 回だけインストールする必要があります。
4. 統合する Microsoft Hyper-V サーバーごとに、QRadar コンソール上でログ・ソースを作成します。

関連タスク

『QRadar での Microsoft Hyper-V ログ・ソースの構成』

QRadar での Microsoft Hyper-V ログ・ソースの構成

Microsoft Hyper-V イベントを収集するには、IBM Security QRadar でログ・ソースを構成します。

このタスクについて

Microsoft Hyper-V サーバーの現行資格情報があり、WinCollect エージェントがサーバーにアクセスできることを確認します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。

3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「Microsoft **Hyper-V**」を選択します。
7. 「プロトコル構成」リストで「**WinCollect**」を選択します。
8. 「アプリケーションまたはサービスのログ・タイプ **(Application or Service Log Type)**」リストで、「Microsoft **Hyper-V**」を選択します。
9. 「**WinCollect** エージェント **(WinCollect Agent)**」リストから、Microsoft Hyper-V サーバーにアクセスする WinCollect エージェントを選択します。
10. 残りのパラメーターを構成します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

Microsoft IAS サーバー

Microsoft IAS Server DSM for IBM Security QRadar は、Syslog を使用して RADIUS イベントを受け取ります。

このタスクについて

WinCollect を使用して、インターネット認証サービス (IAS) またはネットワーク・ポリシー・サーバー (NPS®) のログを QRadar と統合できます。詳しくは、「*IBM Security QRadar WinCollect* ユーザー・ガイド」を参照してください。

これで、QRadar でログ・ソースを構成できるようになりました。

Microsoft Windows IAS サーバーからイベントを受信するように QRadar を構成するには、以下のようにします。

手順

「ログ・ソース・タイプ」リストで「Microsoft **IAS Server**」オプションを選択します。
ご使用のサーバーについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Microsoft IIS サーバー

IBM Security QRadar 用の Microsoft Internet Information Services (IIS) Server DSM は、syslog を使用して FTP、HTTP、NNTP、および SMTP のイベントを受け取ります。

以下に示すいずれかの方法で、Microsoft IIS サーバーを QRadar と統合することができます。

- IIS プロトコルを使用して QRadar が Microsoft IIS サーバーに接続するように構成します。IIS プロトコルは、Microsoft IIS サーバーから HTTP イベントを収集します。詳しくは、『IIS プロトコルを使用した Microsoft IIS の構成』を参照してください。
- イベント情報を QRadar に転送するように、Microsoft IIS サーバーで Snare エージェントを構成します。詳しくは、 735 ページの『Snare Agent を使用した Microsoft IIS の構成』を参照してください。
- IIS イベントを QRadar に転送するように、WinCollect を構成します。詳しくは、 737 ページの『Adaptive Log Exporter を使用した Microsoft IIS の構成』を参照してください。

詳しくは、「*IBM Security QRadar WinCollect* ユーザー・ガイド」を参照してください。

表 *278. Microsoft IIS* でサポートされるログ・タイプ

バージョン	サポートされるログ・タイプ	インポートの方法
Microsoft IIS 6.0	SMTP, NNTP, FTP, HTTP	IIS プロトコル
Microsoft IIS 6.0	SMTP, NNTP, FTP, HTTP	WinCollect または Snare
Microsoft IIS 7.0	HTTP	IIS プロトコル
Microsoft IIS 7.0	SMTP, NNTP, FTP, HTTP	WinCollect または Snare
Microsoft IIS 8.x	HTTP	IIS プロトコル
Microsoft IIS 8.x	SMTP, NNTP, FTP, HTTP	WinCollect または Snare

IIS プロトコルを使用した Microsoft IIS の構成

IIS プロトコルを使用して QRadar と通信するように Microsoft IIS プロトコルを構成できます。

始める前に

Microsoft IIS プロトコルを使用して IBM Security QRadar を構成する前に、正しいログ形式を生成するように Microsoft IIS サーバーを構成する必要があります。

このタスクについて

Microsoft IIS プロトコルでは、W3C 拡張ログ・ファイル・フォーマットのみがサポートされています。Microsoft 認証プロトコル NTLMv2 セッションは、Microsoft IIS プロトコルではサポートされていません。

手順

1. Microsoft インターネット・インフォメーション・サービス (IIS) マネージャーにログインします。
2. 「**IIS** マネージャー」 > 「ローカル コンピューター」 > 「サイト」を展開します。

3. 「**Web** サイト」を選択します。
4. 「ログの記録」アイコンをダブルクリックします。
5. 「ログ ファイル」ウィンドウからログ・ファイル・フォーマットとして「**W3C**」を選択します。
6. 「フィールドの選択」プッシュボタンをクリックします。
7. プロパティーのリストから、以下の W3C プロパティーのチェック・ボックスを選択します。

表 279. IIS イベント・ログの必須プロパティー

IIS 6.0 の必須プロパティー	**IIS 7.0** の必須プロパティー
日付 **(date)**	日付 **(date)**
時刻 **(time)**	時刻 **(time)**
クライアント **IP** アドレス **(c-ip)**	クライアント **IP** アドレス **(c-ip)**
ユーザー名 **(cs-username)**	ユーザー名 **(cs-username)**
サーバー **IP** アドレス **(s-ip)**	サーバー **IP** アドレス **(s-ip)**
サーバー ポート **(s-port)**	サーバー ポート **(s-port)**
メソッド **(cs-method)**	メソッド **(cs-method)**
URI Stem (cs-uri-stem)	**URI Stem (cs-uri-stem)**
URI クエリ **(cs-uri-query)**	**URI** クエリ **(cs-uri-query)**
プロトコル ステータス **(sc-status)**	プロトコル ステータス **(sc-status)**
プロトコル バージョン **(cs-version)**	ユーザー エージェント **(cs(User-Agent))**
ユーザー エージェント **(cs(User-Agent))**	

8. 「**OK**」をクリックします。

次のタスク

これで、QRadar でログ・ソースを構成する準備ができました。

IBM Security QRadar での Microsoft IIS プロトコルの構成

QRadar で Microsoft IIS のログ・ソースを構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース・タイプ」リストで「Microsoft IIS サーバー」を選択します。
7. 「プロトコル構成」リストで「Microsoft **IIS**」を選択します。

8. 以下の値を構成します。

表 280. *Microsoft IIS* のプロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。
サーバー・アドレス	Microsoft IIS サーバーの IP アドレスを入力します。
ユーザー名	Microsoft IIS サーバーへのアクセスに必要なユーザー名を入力します。
パスワード	Microsoft IIS サーバーへのアクセスに必要なパスワードを入力します。
パスワードの確認	Microsoft IIS サーバーへのアクセスに必要なパスワードを確認します。
ドメイン	Microsoft IIS サーバーへのアクセスに必要なドメインを入力します。
フォルダー・パス	IIS ログ・ファイルにアクセスするためのディレクトリー・パスを入力します。デフォルトは `/WINDOWS/system32/LogFiles/W3SVC1/` です。 ファイル・パスをサポートしているパラメーターでは、パス情報でドライブ名を定義できます。例えば管理共有用の `c$/LogFiles/` や公開共有フォルダー・パス用の `LogFiles/` を使用できますが、`c:/LogFiles` は使用できません。 ログ・フォルダー・パスに管理共有 (`C$`) が含まれている場合、その管理共有 (**C$**) に対する NetBIOS アクセス権限を持つユーザーには、ログ・ファイルの読み取りに必要な適切なアクセス権限があります。 ローカルまたはドメインの管理者は、管理共有上にあるログ・ファイルにアクセスするための十分な特権を持っています。
ファイル・パターン	ファイル名をフィルタリングするために必要な正規表現 (regex) を入力します。一致するすべてのファイルは処理に組み込まれます。デフォルトは `(?:u_)?ex.*¥.(?:log|LOG)` です。 例えば、log という単語で始まり 1 つ以上の数字が続き、`tar.gz` で終わるファイルをすべてリストするには、`log[0-9]+¥.tar¥.gz` を使用します。このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
再帰的 **(Recursive)**	ファイル・パターンでサブフォルダーを検索する場合は、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
ポーリング間隔 **(秒) (Polling Interval (s))**	ポーリング間隔 (新規データを確認するためのログ・ファイルに対する照会から次の照会までの間の秒数) を入力します。デフォルトは 10 秒です。

9. 「保存」をクリックします。
10. Microsoft IIS プロトコルの構成は完了です。

Snare Agent を使用した Microsoft IIS の構成

Snare Agent を使用して Microsoft IIS サーバーを IBM Security QRadar と統合する前に、イベントを転送するように Snare Agent を構成する必要があります。

このタスクについて

QRadar で Snare Agent を使用して Microsoft IIS を構成するには、以下の手順を実行する必要があります。

1. 『Snare 用の Microsoft IIS サーバーの構成』
2. 736 ページの『Snare Agent の構成』
3. 736 ページの『Microsoft IIS ログ・ソースの構成』

Snare 用の Microsoft IIS サーバーの構成

Microsoft IIS サーバーを IBM Security QRadar と統合するために Snare エージェントを構成できます。

手順

1. Microsoft インターネット・インフォメーション・サービス (IIS) マネージャーにログインします。
2. 「**IIS** マネージャー」メニュー・ツリーで、「ローカル コンピューター」を展開します。
3. 「**Web** サイト」を選択します。
4. 「既定の **Web** サイト」を右クリックして、「プロパティ」を選択します。

   「既定の Web サイトのプロパティ」ウィンドウが表示されます。
5. 「**Web** サイト」タブを選択します。
6. 「ログの記録を有効にする」チェック・ボックスを選択します。
7. 「アクティブ ログ形式」リストから「**W3C** 拡張ログ ファイル形式」を選択します。
8. 「ログの記録を有効にする」ペインで「プロパティ」をクリックします。

   「ログ プロパティ」ウィンドウが表示されます。
9. 「拡張」タブをクリックします。
10. プロパティーのリストから、以下の W3C プロパティーのチェック・ボックスを選択します。

表 281. IIS イベント・ログの必須プロパティー

IIS 6.0 の必須プロパティー	**IIS 7.0** の必須プロパティー
日付 **(date)**	日付 **(date)**
時刻 **(time)**	時刻 **(time)**
クライアント **IP** アドレス **(c-ip)**	クライアント **IP** アドレス **(c-ip)**
ユーザー名 **(cs-username)**	ユーザー名 **(cs-username)**
サーバー **IP** アドレス **(s-ip)**	サーバー **IP** アドレス **(s-ip)**
サーバー ポート **(s-port)**	サーバー ポート **(s-port)**
メソッド **(cs-method)**	メソッド **(cs-method)**

表 281. IIS イベント・ログの必須プロパティー (続き)

IIS 6.0 の必須プロパティー	IIS 7.0 の必須プロパティー
URI Stem (cs-uri-stem)	**URI Stem (cs-uri-stem)**
URI クエリ (cs-uri-query)	**URI クエリ (cs-uri-query)**
プロトコル ステータス **(sc-status)**	プロトコル ステータス **(sc-status)**
プロトコル バージョン **(cs-version)**	ユーザー エージェント **(cs(User-Agent))**
ユーザー エージェント **(cs(User-Agent))**	

11. 「**OK**」をクリックします。
12. これで、Snare Agent を構成する準備ができました。

Snare Agent の構成

Snare Agent を構成できます。

手順

1. InterSect Alliance Web サイトにアクセスします。

   http://www.intersectalliance.com/
2. オープン・ソース Snare Agent for IIS バージョン 1.2 をダウンロードします。

   ```
   SnareIISSetup-1.2.exe
   ```
3. オープン・ソース Snare Agent for IIS をインストールします。
4. Snare Agent で「監査の構成 **(Audit Configuration)**」を選択します。

   「監査サービスの構成 (Audit Service Configuration)」ウィンドウが表示されます。
5. 「ターゲット・ホスト **(Target Host)**」フィールドに QRadar の IP アドレスを入力します。
6. 「ログ・ディレクトリー **(Log Directory)**」フィールドに、IIS ファイルの場所を入力します。

   ```
   ¥%SystemRoot%¥System32¥LogFiles¥
   ```

   デフォルトでは、Snare for IIS は `C:¥WINNT¥System32¥LogFiles¥` でログを検索するように構成されます。
7. 「宛先 **(Destination)**」で「**Syslog**」を選択します。
8. 「区切り文字 **(Delimiter)**」で「タブ **(TAB)**」を選択します。
9. 「**IIS** ヘッダー情報を表示する **(Display IIS Header Information)**」チェック・ボックスを選択します。
10. 「**OK**」をクリックします。

Microsoft IIS ログ・ソースの構成

IBM Security QRadar は、Snare Agent から転送された Microsoft IIS からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

このタスクについて

QRadar で Microsoft IIS ログ・ソースを手動で作成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース・タイプ」リストで「Microsoft IIS サーバー」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。
8. 以下の値を構成します。

表 *282. Microsoft IIS Syslog* の構成

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

Adaptive Log Exporter を使用した Microsoft IIS の構成

WinCollect は、デバイス・ログまたはアプリケーション・イベント・データを IBM Security QRadar または QRadar Log Manager と統合することができるスタンドアロン・アプリケーションです。

このタスクについて

Adaptive Log Exporter を Microsoft IIS と統合するには、以下のようにします。

手順

1. Microsoft インターネット・インフォメーション・サービス (IIS) マネージャーにログインします。
2. 「**IIS** マネージャー」メニュー・ツリーで、「ローカル コンピューター」を展開します。
3. 「**Web** サイト」を選択します。
4. 「既定の **Web** サイト」を右クリックして、「プロパティ」を選択します。

   「Web サイトのプロパティ」ウィンドウが表示されます。

5. 「アクティブ ログ形式」リストから、以下のいずれかのオプションを選択します。
   - 「**NCSA**」を選択します。その場合は、 737 ページの『Adaptive Log Exporter を使用した Microsoft IIS の構成』に進みます。
   - 「**IIS**」を選択します。その場合は、 737 ページの『Adaptive Log Exporter を使用した Microsoft IIS の構成』に進みます。
   - 「**W3C**」を選択します。その場合は、 737 ページの『Adaptive Log Exporter を使用した Microsoft IIS の構成』に進みます。
6. 「プロパティ」をクリックします。

   「プロパティ」ウィンドウが表示されます。
7. 「拡張」タブをクリックします。
8. プロパティーのリストから、Microsoft IIS イベント・ログに適用するすべてのイベント・プロパティーを選択します。選択するプロパティーでは、次の項目を選択する必要があります。
   a. 「メソッド **(cs-method)**」チェック・ボックスを選択します。
   b. 「プロトコル バージョン **(cs-version)**」チェック・ボックスを選択します。
9. 「**OK**」をクリックします。

次のタスク

これで、Adaptive Log Exporter を構成する準備ができました。Microsoft IIS のインストールと Adaptive Log Exporter に対応した構成について詳しくは、「*Adaptive Log Exporter User Guide*」を参照してください。

Microsoft ISA

IBM Security QRadar 用の Microsoft Internet and Acceleration (ISA) DSM は syslog を使用してイベントを受け取ります。

WinCollect を使用して Microsoft ISA Server を QRadar と統合できます。詳しくは、「*IBM Security QRadar WinCollect* ユーザー・ガイド」を参照してください。

注**:** Microsoft ISA DSM は、WinCollect を使用して Microsoft Threat Management Gateway からのイベントもサポートします。

Microsoft Office 365

Microsoft Office 365 用のIBM Security QRadar DSM は、Microsoft Office 365 オンライン・サービスからイベントを収集します。

以下の表は、Microsoft Office 365 DSM の仕様を示しています。

表 *283. Microsoft Office 365 DSM* の仕様

仕様	値
製造元	Microsoft
DSM 名	Microsoft Office 365

表 283. *Microsoft Office 365 DSM* の仕様 (続き)

仕様	値
RPM ファイル名	DSM-MicrosoftOffice365-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	N/A
プロトコル	Office 365 REST API
イベント・フォーマット	JSON
記録されるイベント・タイプ	Exchange 監査、SharePoint 監査、Azure Active Directory 監査、サービス通信
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Microsoft Web サイト (https://www.microsoft.com)

Microsoft Office 365 を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - プロトコル共通 RPM
   - Office 365 REST API プロトコル RPM
   - Microsoft Office 365 DSM RPM
2. Azure Active Directory にアプリケーションを登録します。
3. QRadar コンソールで、Microsoft Office 365 ログ・ソースを追加します。以下の表は、Microsoft Office 365 イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 284. *Microsoft Office 365* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Microsoft Office 365
プロトコル構成	Office 365 REST API
ログ・ソース ID	ログ・ソースの固有 ID。 「ログ・ソース **ID**」には、任意の有効な値を使用でき、特定のサーバーを参照する必要はありません。「ログ・ソース **ID**」は、「ログ・ソース名」と同じ値にすることもできます。複数の Microsoft Office 365 ログ・ソースを構成した場合は、最初のログ・ソースを MSOffice365-1、2 番目のログ・ソースを MSOffice365-2、3 番目のログ・ソースを MSOffice365-3 として識別できます。
クライアント ID (Client ID)	Azure Active Directory のアプリケーション構成で、このパラメーターは「クライアント **ID (Client ID)**」の下にあります。

表 284. *Microsoft Office 365* ログ・ソース・パラメーター (続き)

パラメーター	値
クライアント秘密鍵 (Client Secret)	Azure Active Directory のアプリケーション構成で、このパラメーターは「鍵 **(Keys)**」の下にあります。
テナント ID (Tenant ID)	Azure AD 認証に使用します。
イベント・フィルター (Event Filter)	Microsoft Office から取得する監査イベントのタイプ。 • Azure Active Directory • Exchange • SharePoint • サービス通信
プロキシーの使用 (Use Proxy)	QRadar が Office 365 Management API にアクセスする場合、ログ・ソースのすべてのトラフィックが構成済みのプロキシーを経由します。 「プロキシー・サーバー」、「プロキシー・ポート」、「プロキシー・ユーザー名」、「プロキシー・パスワード」の各フィールドを構成します。 プロキシーが認証を必要としない場合、「プロキシー・ユーザー名」フィールドおよび「プロキシー・パスワード」フィールドはブランクのままにします。
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	選択すると、サーバー証明書を自動的にダウンロードし、ターゲット・サーバーを信頼して使用し始めます。
EPS スロットル	1 秒あたりの最大イベント数。 デフォルトは 5000 です。

Microsoft Office 365 DSM のサンプル・イベント・メッセージを次の表に示します。

表 285. *Microsoft Office 365* サービスによってサポートされる *Microsoft Office 365* サンプル・メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
ユーザーの更新 - 失敗	更新アクティビティーが失敗しました	{"CreationTime":"2016-05-05T08:53:46","Id":"8c1-b601-446b-accd-5db1bb544200","Operation":"Update user.","OrganizationId":"d3fc05f9-1eb4-4a92-bd0b-220dc6614f75","RecordType":8,"ResultStatus":"fail","UserKey":"NotAvailable","UserType":6,"Workload":"AzureActiveDirectory","ObjectId":"10033FFF9706BDBF","UserId":"e5-f79d-4402-916f-46a467ce1140","AzureActiveDirectoryEventType":1,"ExtendedProperties":[{"Name":"MethodExecutionResult.","Value":"Microsoft.Online.Workflows.ValidationException"}],"Actor":[{"ID":"5-f79d-4402-916f-46a467ce1140","Type":4},{"ID":"ncipal_b0c7c0a8-203a-4dbc-b76c-78f82d0c96f4","Type":2}],"ActorContextId":"d3fc05f9-1eb4-4a92-bd0b-220dc6614f75","InterSystemsId":"72021b83-22b2-4f7f-ac80-774efca27742","IntraSystemId":"e546cb1d-f0f2-4488-853e-c1c6928287f6","Target":[{"ID":"5-d9f4-4761-b70a-3128d3b43700","Type":2},{"ID":"sql@cis.secu.com","Type":1},{"ID":"1706BDBF","Type":3}],"TargetContextId":"d3fc05f9-1eb4-4a92-bd0b-220dc6614f75"}
サイト権限の変更	更新アクティビティーが成功しました	{"CreationTime":"2015-10-20T15:54:05","Id":"ea3942ca-3096-4487-f59e-08d2d966af07","Operation":"SitePermissionsModified","OrganizationId":"d3fc05f9-1eb4-4a92-bd0b-220dc6614f75","RecordType":4,"UserKey":"(empty)","UserType":0,"Workload":"SharePoint","ClientIP":"32.97.110.60","ObjectId":"https://ibmsecurity-my.sharepoint.com/personal/qradar_admin_ibmsecurity_onmicrosoft_com","UserId":"SHAREPOINT¥¥system","EventSource":"SharePoint","ItemType":"Web","Site":"308d9383-a3de-4f38-837d-50ac91fa5588","UserAgent":"Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0"}

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に Microsoft Office 365 を構成する

Microsoft Office 365 のログ・ソースを構成するには、「テナント **ID (Tenant ID)**」のコンテンツ・サブスクリプションを有効にするように Microsoft に要求しておく必要が生じる場合があります。コンテンツ・サブスクリプションを有効化することで、QRadar は管理アクティビティー API からデータを取得できます。

始める前に

「テナント **ID (Tenant ID)**」、「クライアント **ID (Client ID)**」、および「クライアント秘密鍵 **(Client Secret)**」が必要です。

手順

1. Azure Active Directory PowerShell コマンドレットを実行します。詳しくは、Azure PowerShell のインストールおよび構成方法 (https://azure.microsoft.com/ja-jp/documentation/articles/powershell-install-configure/) を参照してください。
2. Microsoft Office 365 に加入したテナントの「テナント **ID (Tenant ID)**」を取得するために、以下のコマンドを入力します。

```
import-module MSOnline

$userCredential = Get-Credential

Connect-MsolService -Credential $userCredential

Get-MsolAccountSku | % {$_.AccountObjectID}
```

3. Azure 管理ポータルを使用して、Azure Active Directory にアプリケーションを登録します。
   a. Azure 管理ポータルにログインするには、Microsoft Office 365 に加入したテナントの資格情報を使用します。
   b. 「**Active Directory**」をクリックします。
   c. 新規アプリケーションが登録された場所のディレクトリー名を選択します。
   d. そのディレクトリーのページで、「アプリケーション」を選択します。
   e. 「追加」をクリックします。
   f. 「組織で開発中のアプリケーションを追加」を選択します。
   g. アプリケーションの名前を入力します。
   h. タイプについては、「**Web** アプリケーションや **Web API**」を選択します。
   i. 「サインオン **URL**」フィールドには、以下を入力します。

```
http://localhost
```

j. 「アプリケーション **ID URL (App ID URL)**」には、そのアプリケーション用に URL の形式で固有 ID を入力します。 URL http://*company_name*.onmicrosoft.com/QRadarApp は固有 ID の例です。

4. アプリケーション・プロパティーを構成します。
   a. Azure AD で新しく作成したアプリケーションを選択します。
   b. 「構成」を選択します。
   c. 「アプリケーションはマルチテナントです」オプションが「いいえ **(NO)**」に設定されていることを確認します。
   d. 将来使用する目的で、クライアント ID をコピーします。
   e. 構成を保存します。
5. アプリケーションのクライアント秘密鍵を生成します。
   a. 「鍵 **(Keys)**」の下で、「期間の選択」をクリックします。
   b. 1 年または 2 年を選択します。
   c. 構成を保存します。

   クライアント秘密鍵は、構成の保存後に表示されます。クライアント秘密鍵は一度だけ表示され、取得することができないため、クライアント秘密鍵をコピーして、保管します。
6. アプリケーションが Office 365 Management API にアクセスするために必要とする許可を指定します。
   a. 「他のアプリケーションに対するアクセス許可」の下で、「アプリケーションの追加」を選択します。
   b. 「**Office 365 Management API**」を選択します。
   c. チェック・マークをクリックして、その選択を保存します。
   d. 「アプリケーションのアクセス許可」および「デリゲートされたアクセス許可」の下で、以下のオプションを選択します。
      - 「組織のアクティビティー・データの読み取り **(Read Activity data for your organization)**」
      - 「組織のサービス正常性の情報の読み取り **(Read service health information for your organization)**」
      - 「組織のアクティビティー・レポートの読み取り **(Read activity reports for your organization)**」
   e. 構成を保存します。

   Azure AD のアプリケーション構成は、完了です。QRadar 内で Microsoft Office 365 のログ・ソースを作成できます。詳しくは、Getting started with Office 365 Management API (https://msdn.microsoft.com/EN-US/library/office/dn707383.aspx) を参照してください。

Microsoft Operations Manager

Microsoft Operations Manager DSM for IBM Security QRadar は、OnePoint データベースをポーリングすることで Microsoft Operations Manager (MOM) イベントを受け取ります。これにより、QRadar は関連イベントを記録できます。

このタスクについて

Microsoft Operations Manager と統合するように QRadar を構成する前に、MOM OnePoint SQL サーバー・データベースにアクセスするための適切な権限を使用してデータベース・ユーザー・アカウントが構成されていることを確認する必要があります。OnePoint データベース SDK ビューへのアクセスは、MOM SDK View User データベース・ロールを使用して管理されます。詳しくは、*Microsoft Operations Manager* の資料 を参照してください。

注**:** QRadar と、MOM に関連付けられている SQL サーバー・データベースの間の通信が、ファイアウォール・ルールによってブロックされていないことを確認します。SQL サーバー・データベースに個別の専用コンピューターを使用する MOM インストール済み環境では、MOM が稼働しているシステムではなく、データベース・システムで SDKEventView ビューに対して照会が実行されます。

MOM イベントを受信するように QRadar を構成するには、以下のようにします。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
3. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
4. 「ログ・ソース・タイプ」リストで「Microsoft Operations Manager」を選択します。
5. 「プロトコル構成」リストで「**JDBC**」を選択します。

   JDBC プロトコル・パラメーターが表示されます。
6. 以下の値を構成します。

表 *286. Microsoft Operations Manager* の *JDBC* パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<MOM Database>@<MOM Database Server IP or Host Name>* 各部分について以下で説明します。 • *<MOM Database>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<MOM Database Server IP or Host Name>* は、「IP またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。

表 286. *Microsoft Operations Manager の JDBC パラメーター (続き)*

パラメーター	説明
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	Microsoft Operations Manager データベースの名前として `OnePoint` を入力します。
IP またはホスト名	Microsoft Operations Manager SQL サーバーの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。MSDE のデフォルト・ポートは 1433 です。 JDBC 構成のポートは、Microsoft Operations Manager データベースのリスナー・ポートに一致していなければなりません。Microsoft Operations Manager データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして「MSDE」を使用するときに「データベース・インスタンス」を定義する場合は、構成の「ポート」パラメーターをブランクのままにしておく必要があります。
ユーザー名	データベースへのアクセスに必要なユーザー名を入力します。
パスワード	データベースへのアクセスに必要なパスワードを入力します。パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」パラメーターに入力したパスワードと同じでなければなりません。
認証ドメイン	「データベース・タイプ」として「**MSDE**」を選択し、データベースが Windows 用に構成されている場合は、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックする場合は、構成内で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを含むテーブルまたはビューの名前として `SDKEventView` と入力します。

表 286. *Microsoft Operations Manager の JDBC パラメーター (続き)*

パラメーター	説明
選択リスト	テーブルまたはビューのすべてのフィールドに * を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	比較フィールドとして `TimeStored` を入力します。比較フィールドを使用して、テーブルに対する照会から次の照会までの間に追加されたい新しいイベントを特定できます。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH:mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
準備済みステートメントの使用 **(Use Prepared Statements)**	準備済みステートメントを使用する場合は、このチェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。

表 286. Microsoft Operations Manager の JDBC パラメーター (続き)

パラメーター	説明
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

注: 「信頼性」パラメーターに 5 よりも大きい値を選択すると、Microsoft Operations Manager ログ・ソースに対し、QRadar の他のログ・ソースよりも高い重要度が設定されます。

7. 「保存」をクリックします。
8. 「管理」タブで「変更のデプロイ」をクリックします。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Microsoft SharePoint

IBM Security QRadar 用の Microsoft SharePoint DSM は、JDBC を使用して監査イベントを対象に SQL データベースをポーリングすることにより、SharePoint データベースから監査イベントを収集します。

監査イベントにより、Microsoft SharePoint で管理されているサイト、ファイル、およびコンテンツに対して行われた変更を追跡できます。

Microsoft SharePoint 監査イベントには、以下のエレメントが含まれます。

- イベントが発生したサイト名と送信元
- 項目 ID、項目名、およびイベントのロケーション
- イベントに関連付けられたユーザー ID。
- イベント・タイプ、タイム・スタンプ、およびイベント・アクション

Microsoft SharePoint データベース・イベントの収集には、2 つのログ・ソース構成を使用できます。

1. JDBC プロトコルを使用してイベントをポーリングする SharePoint データベースのデータベース・ビューを作成します。『監査イベントを収集するためのデータベース・ビューの構成』を参照してください。
2. JDBC ログ・ソースを作成し、定義済みのデータベース照会を使用して SharePoint イベントを収集します。このオプションは、管理者によるデータベース・ビューの作成を必要としません。 753 ページの『定義済みデータベース照会の SharePoint ログ・ソースの構成』を参照してください。

注**:** Microsoft Sharepoint イベントの収集は、管理者によるデータベース・ビューの作成を必要とする代わりに、定義済み照会を使用するようになりました。管理者は、既存の Microsoft Sharepoint ログ・ソースが Microsoft Sharepoint 定義済み照会を使用するように、そのログ・ソースを更新できます。

監査イベントを収集するためのデータベース・ビューの構成

Microsoft SharePoint イベントを IBM Security QRadar と統合する前に、3 つの作業を完了しておく必要があります。

このタスクについて

以下の手順を使用します。

手順

1. 収集する Microsoft SharePoint の監査イベントを構成します。
2. Microsoft SharePoint で QRadar の SQL データベース・ビューを作成します。
3. Microsoft SharePoint から監査イベントを収集するようにログ・ソースを構成します。

   注**:** QRadar と、Microsoft SharePoint に関連付けられているデータベースの間の通信が、ファイアウォール・ルールによってブロックされていないことを確認します。

Microsoft SharePoint 監査イベントの構成

Microsoft SharePoint の監査設定では、Microsoft SharePoint により管理されるサイトごとに追跡するイベントを定義できます。

手順

1. Microsoft SharePoint サイトにログインします。
2. 「サイト操作」リストから「サイトの設定」を選択します。
3. 「サイト コレクションの管理」リストで「サイト コレクションの監査設定」をクリックします。
4. 「ドキュメント、アイテム」セクションで、監査するドキュメントとアイテムの監査イベントのチェック・ボックスを選択します。
5. 「リスト、ライブラリ、サイト」セクションで、有効にする各コンテンツ監査イベントのチェック・ボックスを選択します。

6. 「**OK**」をクリックします。

これで、IBM Security QRadar が Microsoft SharePoint イベントをポーリングするためのデータベース・ビューを作成する準備ができました。

Microsoft SharePoint のデータベース・ビューの作成

Microsoft SharePoint は、SQL Server Management Studio (SSMS) を使用して SharePoint SQL データベースを管理します。監査イベント・データを収集するには、IBM Security QRadar がアクセスできる Microsoft SharePoint サーバーにデータベース・ビューを作成する必要があります。

始める前に

ビューの名前やテーブルの名前にピリオド(.) を使用しないでください。ビュー名やテーブル名にピリオドを使用した場合、JDBC はそのビュー内のデータにアクセスできず、アクセスが拒否されます。ピリオド (.) より後にあるものはすべて子オブジェクトとして扱われます。

手順

1. Microsoft SharePoint SQL データベースをホストしているシステムにログインします。
2. 「スタート」メニューから「ファイル名を指定して実行」を選択します。
3. 以下のコマンドを入力します。

   ```
   ssms
   ```
4. 「**OK**」をクリックします。

   Microsoft SQL Server 2008 に「サーバーへの接続」ウィンドウが表示されます。
5. Microsoft SharePoint データベースにログインします。
6. 「接続」をクリックします。
7. SharePoint データベースの「オブジェクト エクスプローラー」で「データベース」 > 「**WSS_Logging**」 > 「ビュー」をクリックします。
8. ナビゲーション・メニューで「新しいクエリ」をクリックします。
9. 「クエリ」ペインで、AuditEvent データベース・ビューを作成する以下の Transact-SQL ステートメントを入力します。

   ```
   create view dbo.AuditEvent as select a.siteID
   ,a.ItemId ,a.ItemType ,u.tp_Title as "User"
   ,a.MachineName ,a.MachineIp ,a.DocLocation
   ,a.LocationType ,a.Occurred as "EventTime"
   ,a.Event as "EventID" ,a.EventName
   ,a.EventSource ,a.SourceName ,a.EventData
   from WSS_Content.dbo.AuditData a,
   WSS_Content.dbo.UserInfo u
   where a.UserId = u.tp_ID
   and a.SiteId = u.tp_SiteID;
   ```
10. 「クエリ」ペインで右クリックして、「実行」を選択します。

    ビューが作成されると、結果ペインに以下のメッセージが表示されます。

コマンドは正常に完了しました。

dbo.AuditEvent ビューが作成されました。これで、監査イベントの確認のためにビューをポーリングするように QRadar でログ・ソースを構成する準備ができました。

データベース・ビューの SharePoint ログ・ソースの構成

IBM Security QRadar では Microsoft SharePoint データベースで作成したビューにアクセスするための適切な資格情報が設定されたユーザー・アカウントが必要です。

このタスクについて

Microsoft SharePoint データベースから監査データを適切にポーリングするには、新規ユーザーを作成するか、または AuditEvent ビューからの読み取りのための既存のユーザー資格情報をログ・ソースに指定する必要があります。ユーザー・アカウントの作成について詳しくは、ベンダーの資料を参照してください。

SharePoint イベントを受信するように QRadar を構成するには、以下のようにします。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「Microsoft SharePoint」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. 以下の値を構成します。

表 *287. Microsoft SharePoint の JDBC パラメーター*

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<SharePoint Database>@<SharePoint Database Server IP or Host Name>* 各部分について以下で説明します。 • *<SharePoint Database>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<SharePoint Database Server IP or Host Name>* は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	Microsoft SharePoint データベースの名前として `WSS_Logging` を入力します。

表 287. *Microsoft SharePoint の JDBC パラメーター (続き)*

パラメーター	説明
IP またはホスト名	Microsoft SharePoint SQL サーバーの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。MSDE のデフォルト・ポートは 1433 です。 JDBC 構成のポートは、Microsoft SharePoint データベースのリスナー・ポートに一致していなければなりません。Microsoft SharePoint データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして「**MSDE**」を使用するときに「データベース・インスタンス **(Database Instance)**」を定義する場合は、構成の「ポート」パラメーターをブランクのままにする必要があります。
ユーザー名	ログ・ソースが Microsoft SharePoint データベースへのアクセスに使用できるユーザー名を入力します。
パスワード	ログ・ソースが Microsoft SharePoint データベースへのアクセスに使用できるパスワードを入力します。 パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」フィールドに入力したパスワードと同一である必要があります。
認証ドメイン	「データベース・タイプ」として「**MSDE**」を選択し、データベースが Windows 用に構成されている場合は、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックする場合は、構成内で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを含むテーブルまたはビューの名前として `AuditEvent` と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに `*` を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。

表 287. *Microsoft SharePoint* の *JDBC* パラメーター (続き)

パラメーター	説明
比較フィールド	比較フィールドとして EventTime を入力します。比較フィールドを使用して、テーブルに対する照会から次の照会までの間に追加されたい新しいイベントを特定できます。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
準備済みステートメントの使用 **(Use Prepared Statements)**	「準備済みステートメントの使用 **(Use Prepared Statements)**」チェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (作成した AuditEvent ビューに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
NTLMv2 の使用	「**NTLMv2** の使用 **(Use NTLMv2)**」チェック・ボックスを選択します。 このオプションを選択すると、NTLMv2 認証を必要とする SQL サーバーとの通信時に、MSDE 接続で NTLMv2 プロトコルが強制的に使用されます。このチェック・ボックスはデフォルトで選択されています。 「**NTLMv2** の使用」チェック・ボックスを選択した場合でも、NTLMv2 認証を必要としない SQL サーバーへの MSDE 接続には影響しません。

表 287. Microsoft SharePoint の JDBC パラメーター (続き)

パラメーター	説明
SSL の使用 **(Use SSL)**	接続で SSL 通信がサポートされている場合は、このチェック・ボックスを選択します。このオプションを選択する場合は、SharePoint データベースに追加の構成が必要であり、また管理者が両方のアプライアンスで証明書を構成する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

注**:** 「信頼性」 に 5 よりも大きいパラメーター値を選択すると、Microsoft SharePoint ログ・ソースに対し、QRadar の他のログ・ソースよりも高い重要度が設定されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

定義済みデータベース照会の SharePoint ログ・ソースの構成

ポリシー制限のためにデータベース・ビューを作成する権限がない管理者は、定義済み照会を使用するログ・ソースを使用して Microsoft SharePoint イベントを収集できます。

このタスクについて

定義済み照会は、データベースが JDBC プロトコルによりポーリングされるときに個別のテーブルのデータを結合できるカスタマイズされたステートメントです。Microsoft SharePoint データベースから監査データを適切にポーリングするには、新しいユーザーを作成するか、または既存のユーザー資格情報をログ・ソースに指定する必要があります。ユーザー・アカウントの作成について詳しくは、ベンダーの資料を参照してください。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「**Microsoft SharePoint**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. 以下の値を構成します。

表 *288. Microsoft SharePoint* の *JDBC* パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<SharePoint Database>@<SharePoint Database Server IP or Host Name>* 各部分について以下で説明します。 • *<SharePoint Database>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<SharePoint Database Server IP or Host Name>* は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	Microsoft SharePoint データベースの名前として `WSS_Logging` を入力します。
IP またはホスト名	Microsoft SharePoint SQL サーバーの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。MSDE のデフォルト・ポートは 1433 です。 JDBC 構成のポートは、Microsoft SharePoint データベースのリスナー・ポートに一致していなければなりません。 Microsoft SharePoint データベースでは、IBM Security QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして「**MSDE**」を使用するときに「データベース・インスタンス **(Database Instance)**」を定義する場合は、構成の「ポート」パラメーターをブランクのままにする必要があります。
ユーザー名	ログ・ソースが Microsoft SharePoint データベースへのアクセスに使用できるユーザー名を入力します。
パスワード	ログ・ソースが Microsoft SharePoint データベースへのアクセスに使用できるパスワードを入力します。 パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」フィールドに入力したパスワードと同一である必要があります。
認証ドメイン	「データベース・タイプ」として「**MSDE**」を選択し、データベースが Windows 用に構成されている場合は、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。

表 288. *Microsoft SharePoint* の *JDBC* パラメーター (続き)

パラメーター	説明
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックする場合は、構成内で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
定義済み照会	リストで「**Microsoft SharePoint**」を選択します。
準備済みステートメントの使用 **(Use Prepared Statements)**	「準備済みステートメントの使用 **(Use Prepared Statements)**」チェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 開始日または開始時刻が選択されていない場合は、ポーリングが即時に開始され、指定のポーリング間隔で繰り返されます。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (作成した AuditEvent ビューに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 (Use Named Pipe Communication)」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。

表 288. *Microsoft SharePoint の JDBC パラメーター (続き)*

パラメーター	説明
NTLMv2 の使用	「**NTLMv2** の使用 **(Use NTLMv2)**」チェック・ボックスを選択します。 このオプションを選択すると、NTLMv2 認証を必要とする SQL サーバーとの通信時に、MSDE 接続で NTLMv2 プロトコルが強制的に使用されます。このチェック・ボックスはデフォルトで選択されています。 「**NTLMv2** の使用」チェック・ボックスを選択した場合でも、NTLMv2 認証を必要としない SQL サーバーへの MSDE 接続には影響しません。
SSL の使用 **(Use SSL)**	接続で SSL 通信がサポートされている場合は、このチェック・ボックスを選択します。このオプションを選択する場合は、SharePoint データベースに追加の構成が必要であり、また管理者が両方のアプライアンスで証明書を構成する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 (Use Named Pipe Communication)」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

注**:** 「信頼性」 に 5 よりも大きいパラメーター値を選択すると、Microsoft SharePoint ログ・ソースに対し、QRadar の他のログ・ソースよりも高い重要度が設定されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

Microsoft System Center Operations Manager

QRadar Microsoft System Center Operations Manager (SCOM) DSM は、OperationsManager データベースをポーリングすることで SCOM イベントを受け取ります。これにより、QRadar が関連イベントを記録できるようになります。

このタスクについて

Microsoft SCOM と統合するように QRadar を構成する前に、SCOM OperationsManager SQL サーバー・データベースにアクセスするための適切な権限を使用してデータベース・ユーザー・アカウントが構成されていることを確認してください。SQL サーバーのプロパティーのセキュリティー設定で、適切な認証モードを有効にする必要があります。詳しくは、Microsoft SCOM の資料を参照してください。

注**:** QRadar と、SCOM に関連付けられている SQL サーバー・データベースの間の通信をブロックするファイアウォール・ルールがないことを確認します。SQL サーバー・データベースに個別の専用コンピューターを使用する SCOM インストー

ル済み環境では、SCOM が稼働しているシステムではなく、データベース・システムで EventView ビューに対して照会が実行されます。

SCOM イベントを受信するように QRadar を構成するには、以下のようにします。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
3. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
4. 「ログ・ソース・タイプ」リストで「Microsoft SCOM」を選択します。
5. 「プロトコル構成」リストで「**JDBC**」を選択します。

   JDBC プロトコルが表示されます。
6. 以下の値を構成します。

表 *289. Microsoft SCOM の JDBC パラメーター*

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<SCOM Database>@<SCOM Database Server IP or Host Name>* 各部分について以下で説明します。 • *<SCOM Database>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<SCOM Database Server IP or Host Name>* は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	Microsoft SCOM データベースの名前として OperationsManager と入力します。
IP またはホスト名	Microsoft SCOM SQL サーバーの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。 MSDE のデフォルト・ポートは 1433 です。 JDBC 構成のポートは、Microsoft SCOM データベースのリスナー・ポートに一致していなければなりません。Microsoft SCOM データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして「MSDE」を使用するときに「データベース・インスタンス」を定義する場合は、構成の「ポート」パラメーターをブランクのままにしておく必要があります。
ユーザー名	データベースへのアクセスに必要なユーザー名を入力します。

表 289. *Microsoft SCOM の JDBC パラメーター (続き)*

パラメーター	説明
パスワード	データベースへのアクセスに必要なパスワードを入力します。パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」パラメーターに入力したパスワードと同じでなければなりません。
認証ドメイン	「データベース・タイプ」として **MSDE** を選択し、データベースが Windows 用に構成されている場合は、Window 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックする場合は、構成内で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを含むテーブルまたはビューの名前として EventView と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに * を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	比較フィールドとして **TimeAdded** を入力します。比較フィールドを使用して、テーブルに対する照会から次の照会までの間に追加されたい新しいイベントを特定できます。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH:mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。

表 289. Microsoft SCOM の JDBC パラメーター (続き)

パラメーター	説明
準備済みステートメントの使用 **(Use Prepared Statements)**	準備済みステートメントを使用する場合は、このチェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 (Use Named Pipe Communication)」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

注**:** 「信頼性」パラメーターに 5 よりも大きい値を選択すると、Microsoft SCOM ログ・ソースに対し、QRadar の他のログ・ソースよりも高い重要度が設定されます。

7. 「保存」をクリックします。
8. 「管理」タブで「変更のデプロイ」をクリックします。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプラ

イアンスからイベントを受信するログ・ソースを手動で追加できます。

Microsoft Windows セキュリティー・イベント・ログ

IBM Security QRadar DSM for Microsoft Windows セキュリティー・イベント・ログは、Microsoft Windows システムから syslog イベントを受け取ります。

Microsoft オペレーティング・システムからのイベント収集用に、QRadar では以下のプロトコルがサポートされています。

- MSRPC (MSRPC 経由の Microsoft セキュリティー・イベント・ログ)
- Syslog (Snare、BalaBit、およびその他のサード・パーティー Windows ソリューションが対象)
  - 共通イベント・フォーマット (CEF) もサポートされています。
- WMI (Microsoft セキュリティー・イベント・ログ)。これは、レガシー・プロトコルです。
- WinCollect。WinCollect ユーザー・ガイド (http://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.4/QRadar/EN/b_wincollect.pdf) を参照してください。

関連タスク:

『Windows ホスト上での MSRPC の有効化』
MSRPC を介した Windows ホストと IBM Security QRadar との間の接続を有効にするには、Microsoft Remote Procedure Calls (MSRPC) プロトコル用に Windows ホスト上でリモート・プロシージャー・コール (RPC) 設定を構成します。

765 ページの『Windows ホスト上での Snare Agent の有効化』
Windows ホストと IBM Security QRadar との間の通信を有効にするには、Snare Agent を使用して Windows イベントを転送します。

766 ページの『Windows ホスト上での WMI の有効化』
Windows ホストと IBM Security QRadar との間の通信を有効にするために、Windows Management Instrumentation (WMI) を使用できます。

Windows ホスト上での MSRPC の有効化

MSRPC を介した Windows ホストと IBM Security QRadar との間の接続を有効にするには、Microsoft Remote Procedure Calls (MSRPC) プロトコル用に Windows ホスト上でリモート・プロシージャー・コール (RPC) 設定を構成します。

始める前に

Windows ホストと QRadar アプライアンスとの間の MSRPC を介した通信を有効にするには、管理者グループのメンバーでなければなりません。

このタスクについて

128 GB の RAM および 40 コア (Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80 GHz) を搭載した IBM Security QRadar QRadar Event Processor 1628 アプライアンスでのパフォーマンス・テストによると、1 秒あたり 8500 イベント (eps) の

速度が正常に達成されたと同時に、他の 非 Windows システムからのログの受け取りおよび処理が行われました。ログ・ソース制限は 500 です。

仕様	値
製造元	Microsoft
プロトコル・タイプ	イベントの収集のための、オペレーティング・システム依存のリモート・プロシージャー・プロトコルのタイプ。 「プロトコル・タイプ **(Protocol Type)**」リストから、次のオプションのいずれかを選択します。 **MS-EVEN6** 新しいログ・ソースのデフォルトのプロトコル・タイプ。 QRadar が Windows Vista や Windows Server 2008 以降と通信するために使用するプロトコル・タイプ。 **MS-EVEN (XP/2003 の場合)** QRadar が Windows XP や Windows Server 2003 と通信するために使用するプロトコル・タイプ。 Windows XP と Windows Server 2003 は、Microsoft ではサポートされていません。このオプションを使用すると正常に動作しない可能性があります。 自動検出 **(**レガシー構成用**)** Microsoft Windows セキュリティー・イベント・ログ DSM に対する従来のログ・ソース構成は、「自動検出 **(**レガシー構成用**)**」プロトコル・タイプを使用しています。 「**MS_EVEN6**」プロトコル・タイプまたは「**MS-EVEN (Windows XP/2003** の場合**)**」プロトコル・タイプにアップグレードしてください。

仕様	値
サポートされるバージョン	Windows 2012 (最新) Windows Server 2008 (最新) Windows 8.1 Windows 8 Windows 7 Windows Vista
対象用途	ログ・ソースあたり 100 EPS をサポート可能な Windows オペレーティング・システムに対するエージェントレス・イベント収集。
サポートされるログ・ソースの最大数	管理対象ホスト (16xx または 18xx アプライアンス) ごとに 500 MSRPC プロトコル・ログ・ソース
全体の MSRPC の最大 EPS 速度	管理対象ホストごとに 8500 EPS
特殊機構	デフォルトで暗号化イベントがサポートされます。
必要な権限	ログ・ソース・ユーザーは、「**Event Log Readers**」グループのメンバーでなければなりません。このグループがまだ構成されていない場合は、ドメイン間で Windows イベント・ログをポーリングするためにドメイン管理特権が必要になることがほとんどです。場合によっては、Microsoft グループ・ポリシー・オブジェクトの構成方法に応じて、「**Backup Operators**」グループも使用できる場合があります。 Windows XP および 2003 オペレーティング・システム・ユーザーは、以下のレジストリー・キーに対する読み取り権限が必要です。 • `HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥services¥eventlog` • `HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Nls¥Language` • `HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft Windows¥CurrentVersion`

仕様	値
サポートされるイベント・タイプ	アプリケーション システム セキュリティー DNS サーバー ファイル複製 ディレクトリー・サービスのログ
Windows のサービス条件	Windows Server 2008 および Windows Vista の場合、以下のサービスを使用します。 • リモート・プロシージャー・コール (RPC) • RPC エンドポイント・マッパー Windows 2003 の場合、リモート・レジストリーおよびリモート・サーバーを使用します。
Windows のポート条件	以下のポートでの着信 TCP 接続および発信 TCP 接続が許可されるように、Windows ホストと QRadar アプライアンスとの間の外部ファイアウォールが構成されていることを確認します。 Windows Server 2008 および Windows Vista の場合、以下のポートを使用します。 • TCP ポート 135 • RPC 用に動的に割り振られる、49152 より大きい TCP ポート Windows 2003 の場合、以下のポートを使用します。 • TCP ポート 445 • TCP ポート 139
自動的に検出?	いいえ
ID を含む?	はい
カスタム・プロパティーを含む?	Windows カスタム・イベント・プロパティーを含むセキュリティー・コンテンツ・パックは、IBM Fix Central で入手できます。
必要な RPM ファイル	PROTOCOL-WindowsEventRPC-*QRadar_release-Build_number*.noarch.rpm DSM-MicrosoftWindows-*QRadar_release-Build_number*.noarch.rpm DSM-DSMCommon-*QRadar_release-Build_number*.noarch.rpm

仕様	値
その他の情報	Microsoft サポート (http://support.microsoft.com/)
使用可能なトラブルシューティング・ツール	MSRPC テスト・ツールは MSRPC プロトコル RPM の一部です。MSRPC プロトコル RPM をインストールすると、MSRPC テスト・ツールは /opt/qradar/jars に保管されます。

手順

1. 管理者として QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース・タイプ」リストで「**Microsoft Windows** セキュリティー・イベント・ログ」を選択します。
6. 「プロトコル構成」リストで「**Microsoft Security Event Log over MSRPC**」を選択します。
7. 「ログ・ソース **ID**」リストで、イベントのポーリング対象の Windows システムの IP アドレスまたはホスト名を入力します。ホスト名は、完全修飾ドメイン名 (FQDN) を入力する必要があります (myhost.example.com など)。
8. 「ドメイン」フィールドに、Windows システムのドメインを入力します。
9. ログ・ソースのユーザー名パラメーターおよびパスワード・パラメーターを構成します。
10. オプション: 「ポーリング間隔」フィールドを構成します。

    注**:** 「ポーリング間隔 **(**秒**)(Polling Interval (Sec))**」フィールドは、WinCollect ログ・ソースのように、ログ・ソース・パフォーマンスを調整することはありません。低いイベント速度システムを制限された帯域幅でポーリングするには、ネットワーク使用量を削減するためにポーリング間隔を大きくします。
11. 「イベント・スロットル **(Event Throttle)**」フィールドを構成します。
12. 「プロトコル・タイプ」リストで、オペレーティング・システムに対するプロトコル・タイプを選択します。
13. 「標準ログ・タイプ **(Standard Log Types)**」チェック・ボックスを 1 つ以上選択します。

    重要**: Microsoft** セキュリティー・イベント・ログ・プロトコルまたは **MSRPC** 経由の **Microsoft** セキュリティー・イベント・ログ・プロトコルを使用する場合は、ターゲット Windows ホストでサポートされるログ・タイプのみを選択します。
14. 「イベント・タイプ **(Event Types)**」チェック・ボックスを 1 つ以上選択します。
15. 「保存」をクリックします。
16. 「管理」タブで「変更のデプロイ」をクリックします。

Windows ホスト上での Snare Agent の有効化

Windows ホストと IBM Security QRadar との間の通信を有効にするには、Snare Agent を使用して Windows イベントを転送します。

このタスクについて

Windows イベントの Syslog 収集は、多数のソースから行われる可能性があります。このガイドに示す説明では、Intersect Alliance による Snare のフリー・バージョンの構成を概説します。他のいくつかのサード・パーティー製品が Syslog プロトコルを使用できます。

仕様	値
製造元	Microsoft
プロトコル・タイプ	Syslog
サポートされるバージョン	ご使用のベンダーの資料を参照してください。
この DSM をよく使用する製品	Snare Adaptive Log Exporter BalaBit 転送された Splunk イベント Snare Epilogue
サポートされるイベント・タイプ	セキュリティー システム、アプリケーション DNS サーバー ファイル複製 ディレクトリー・サービス
対象用途	パートナー製品およびサード・パーティー製品からの Windows イベントを解析および収集するためのエージェント・ソリューション。
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	Windows カスタム・イベント・プロパティーを含むセキュリティー・コンテンツ・パックは、IBM Fix Central で入手できます。
必要な RPM ファイル	DSM-MicrosoftWindows-*QRadar_release-Build_number*.noarch.rpm DSM-DSMCommon-*QRadar_release-Build_number*.noarch.rpm
その他の情報	Microsoft サポート (support.microsoft.com/)

仕様	値
使用可能なトラブルシューティング・ツール	QRadar アプライアンス上で tcpdump ユーティリティーを使用して、イベントが受信されていることを確認できます。

手順

1. Windows ホストにログインします。
2. Snare の Web サイトから Snare Agent をダウンロードしてインストールします。
3. ナビゲーション・メニューで、「ネットワーク構成」を選択します。
4. 「宛先 **Snare** サーバー **(Destination Snare Server)**」アドレス・フィールドに、QRadar システムの IP アドレスを入力します。
5. 「**SYSLOG** ヘッダーを有効にする **(Enable SYSLOG Header)**」チェック・ボックスを選択します。
6. 「構成変更」をクリックします。
7. ナビゲーション・メニューで、「目的の構成 **(Objectives Configuration)**」を選択します。
8. 「キャプチャーするイベント・タイプの識別 **(Identify the event types to be captured)**」フィールドで、QRadar に転送するイベント・タイプを定義するチェック・ボックスを選択します。

   ヒント**:** Microsoft Windows イベント・ログ用の DSM では、通知、警告、エラー、監査の成功、および監査の失敗の各イベント・タイプがサポートされます。
9. 「イベント・ログの識別 **(Identify the event logs)**」フィールドで、QRadar に転送するイベント・ログを定義するチェック・ボックスを選択します。

   ヒント**:** Microsoft Windows Event Log DSM では、セキュリティー、システム、アプリケーション、DNS サーバー、ファイル複製、およびディレクトリー・サービスのログ・タイプがサポートされます。
10. 「構成変更」をクリックします。
11. ナビゲーション・メニューで、「最新の監査構成を適用 **(Apply the Latest Audit Configuration)**」を選択します。
12. 「ホスト名検出のオーバーライド値 **(override host name detection with)**」フィールド内の値を記録します。この値は、QRadar ログ・ソースで構成されているデバイスに割り当てられている IP アドレスまたはホスト名に一致する必要があります。

タスクの結果

QRadar が約 35 イベントを受け取ると、ログ・ソースが自動的に作成され、イベントが「ログ・アクティビティー」タブに表示されます。

Windows ホスト上での WMI の有効化

Windows ホストと IBM Security QRadar との間の通信を有効にするために、Windows Management Instrumentation (WMI) を使用できます。

始める前に

WMI/DCOM Windows ホストと QRadar アプライアンスを構成するには、リモート・コンピューター上で管理者グループのメンバーでなければなりません。

このタスクについて

50 EPS を超えるイベント収集が必要な場合や、低速のネットワーク接続を介するサーバー (サテライト・ネットワークや低速な WAN ネットワークなど) には、Microsoft セキュリティー・イベント・ログ・プロトコル (WMI) は推奨されません。低速接続によるネットワーク遅延は、リモート・サーバーで使用可能な EPS スループットを低下させます。高速接続では、代わりに MSRPC を使用できます。ネットワークの往復遅延時間を短縮できない場合、WinCollect などのエージェントを使用することをお勧めします。

仕様	値
製造元	Microsoft
DSM 名	Windows セキュリティー・イベント・ログ
サポートされるバージョン	Windows Server 2003 (最新) Windows Server 2008 (最新) Windows 2012 (最新) Windows 7 Windows 8 (64 ビット・バージョン) Windows Vista Windows XP
特殊機構	デフォルトで暗号化イベントがサポートされます。
対象用途	ログ・ソースあたり 50 EPS をサポート可能な WMI を介する Windows オペレーティング・システムに対するエージェントレス・イベント収集。 **重要:** これは、レガシー・プロトコルです。ほとんどの場合、新規ログ・ソースは、MSRPC 経由の Microsoft セキュリティー・イベント・ログ・プロトコルを使用して構成する必要があります。
特殊な構成の説明	Configuring DCOM and WMI to Remotely Retrieve Windows 7 Events (http://www.ibm.com/support/docview.wss?uid=swg21678809) Configuring to Remotely Retrieve Windows 8 and Windows 2012 Events (http://www.ibm.com/support/docview.wss?uid=swg21681046)

仕様	値
Windows のポート条件	以下のポートでの着信 TCP 接続および発信 TCP 接続が許可されるように、Windows ホストと QRadar アプライアンスとの間の外部ファイアウォールが構成されていることを確認する必要があります。 • TCP ポート 135 (すべてのオペレーティング・システムのバージョン) • 動的に割り振られる、49152 より大きい TCP ポート (Vista 以上のオペレーティング・システムに必須) • 動的に割り振られる、1024 より大きい TCP ポート (Windows XP および 2003 に必須) • TCP ポート 445 (Windows XP および 2003 に必須) • TCP ポート 139 (Windows XP および 2003 に必須)
Windows のサービス条件	自動的に始動するには、以下のサービスを構成する必要があります。 • リモート・プロシージャー・コール (RPC) • リモート・プロシージャー・コール (RPC) ロケーター • RPC エンドポイント・マッパー • リモート・レジストリー • サーバー • Windows Management Instrumentation
ログ・ソースの権限	ログ・ソース・ユーザーは、「**Event Log Readers**」グループのメンバーでなければなりません。このグループがまだ構成されていない場合は、ドメイン間で Windows イベント・ログをポーリングするためにドメイン管理特権が必要になることがほとんどです。場合によっては、Microsoft グループ・ポリシー・オブジェクトの構成方法に応じて、「**Backup Operators**」グループも使用できる場合があります。 ログ・ソース・ユーザーには、以下のコンポーネントへのアクセス権限が必要です。 • Window イベント・ログ・プロトコルの DCOM コンポーネント • Windows イベント・ログ・プロトコルの名前空間 • リモート・レジストリー・キーへの適切なアクセス権限

仕様	値
サポートされるイベント・タイプ	アプリケーション システム セキュリティー DNS サーバー ファイル複製 ディレクトリー・サービスのログ
自動的に検出?	いいえ、手動でログ・ソースを作成する必要があります。
ID を含む?	はい
カスタム・プロパティーを含む?	Windows カスタム・イベント・プロパティーを含むセキュリティー・コンテンツ・パックは、IBM Fix Central で入手できます。
必要な RPM ファイル	PROTOCOL-WinCollectWindowsEventLog-*QRadar_release-Build_number*.noarch.rpm DSM-MicrosoftWindows-*QRadar_release-Build_number*.noarch.rpm DSM-DSMCommon-*QRadar_release-Build_number*.noarch.rpm
その他の情報	Microsoft サポート (support.microsoft.com/)
使用可能なトラブルシューティング・ツール	はい、WMI テスト・ツールは /opt/qradar/jars で入手できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「ログ・ソース・タイプ」リストで「**Microsoft Windows** セキュリティー・イベント・ログ」を選択します。
5. 「プロトコル構成」リストで「**Microsoft** セキュリティー・イベント・ログ **(Microsoft Security Event Log)**」を選択します。
6. 「ログ・ソース **ID**」フィールドに、イベントのポーリング対象である Windows システムの IP アドレスまたはホスト名を入力します。ホスト名は、完全修飾ドメイン名 (FQDN) を入力する必要があります (myhost.example.com など)。
7. 「ドメイン」フィールドに、Windows システムのドメインを入力します。
8. ログ・ソースのユーザー名パラメーターおよびパスワード・パラメーターを構成します。
9. 「標準ログ・タイプ **(Standard Log Types)**」チェック・ボックスを 1 つ以上選択します。

重要**: Microsoft** セキュリティー・イベント・ログ・プロトコルまたは **MSRPC** 経由の **Microsoft** セキュリティー・イベント・ログ・プロトコルを使用する場合は、ターゲット Windows ホストでサポートされるログ・タイプのみを選択します。

10. 「イベント・タイプ **(Event Types)**」チェック・ボックスを 1 つ以上選択します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

第 82 章 Motorola Symbol AP

IBM Security QRadar 用の Motorola Symbol AP DSM は、syslog を使用して Motorola Symbol AP デバイスから転送された関連イベントをすべて記録します。

ログ・ソースの構成

Motorola SymbolAP を IBM Security QRadar と統合する場合、イベントを受信するために、手動でログ・ソースを作成する必要があります。

このタスクについて

QRadar は、Motorola SymbolAP アプライアンスからの syslog イベントのログ・ソースの検出や作成を自動的に行うことはありません。ログ・ソースが自動的に検出されない場合は、QRadar にイベントを転送する前にログ・ソースを作成することをお勧めします。

ログ・ソースを構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Motorola SymbolAP**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 290. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Motorola SymbolAP アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。

12. 「管理」タブで「変更のデプロイ」をクリックします。

    ログ・ソースが QRadar に追加されます。

Motorola Symbol AP の syslog イベントの構成

syslog イベントを IBM Security QRadar に転送するようにデバイスを構成できます。

手順

1. Symbol AP デバイスのユーザー・インターフェースにログインします。
2. メニューから、「システム構成 **(System Configuration)**」 > 「ロギング構成 **(Logging Configuration)**」を選択します。

   「アクセス・ポイント (Access Point)」ウィンドウが表示されます。
3. 「ロギング・レベル **(Logging Level)**」リストを使用して、システム・イベントの追跡に必要なログ・レベルを選択します。オプションは以下のとおりです。

   0 - 緊急

   1- アラート

   2 - 重要

   3 - エラー

   4 - 警告

   5 - 注意

   6 - 通知。これはデフォルトです。

   7 - デバッグ
4. 「外部 syslog サーバーへのロギングを有効にする (Enable logging to an external syslog server)」チェック・ボックスを選択します。
5. 「**syslog** サーバーの **IP** アドレス **(Syslog Server IP Address)**」フィールドに QRadar などの外部 Syslog サーバーの IP アドレスを入力します。

   これは、QRadar への syslog イベントの経路指定に必須です。
6. 「適用」をクリックします。
7. 「ログアウト **(Logout)**」をクリックします。

   確認ウィンドウが表示されます。
8. 「**OK**」をクリックして、アプリケーションを終了します。

   構成は完了です。QRadar に転送されたイベントは、「ログ・アクティビティー」タブに表示されます。

第 83 章 Name Value Pair

Name Value Pair DSM を使用すると、通常は Syslog ログを送信しないようなデバイスを IBM Security QRadar と統合することを選択できます。

Name Value Pair DSM には、QRadar にログを送信することを選択できるログ形式が用意されています。例えば、本来は syslog によるログのエクスポートを行わないデバイスの場合、スクリプトを作成し、このスクリプトにより、QRadar でサポートされないデバイスからログをエクスポートし、ログを Name Value Pair ログ・フォーマットの形式にして、syslog を使用してそのログを QRadar に送信することができます。

これにより、QRadar で構成された Name Value Pair DSM ログ・ソースがログを受信し、データを解析できるようになります。ログが、Name Value Pair ログ・フォーマットで届くからです。

注**:** Name Value Pair DSM のイベントは、QRadar で自動的には検出されません。

Name Value Pair DSM は、syslog を使用してイベントを受け取ります。QRadar は、関連するすべてのイベントを記録します。Name Value Pair DSM のログ・フォーマットは、タブ区切りの、`Name=Parameter` の単一行のリストでなければなりません。Name Value Pair DSM では、有効な syslog ヘッダーは必要ありません。

注**:** Name Value Pair DSM は、Name Value Pair フォーマットの syslog を使用して QRadar にログを送信するためのカスタム・スクリプトを作成できること、またはご使用のデバイス機能についての十分な知識が前提となっています。

Name Value Pair DSM が解析できるタグを以下に示します。

表 *291. Name Value Pair* ログ・フォーマット・タグ

タグ	説明
DeviceType	「**DeviceType**」として `NVP` と入力します。これにより、ログのフォーマットが名前と値のペアのログ・メッセージとして識別されます。 これは必須パラメーターであり、`DeviceType=NVP` はリストの 1 番目のペアとして指定する必要があります。

表 291. *Name Value Pair* ログ・フォーマット・タグ (続き)

タグ	説明
EventName	イベント・マッピング機能を使用する場合に、Events インターフェースでイベントを識別するために使用するイベント名を入力します。イベント・マッピングについて詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。 これは必須パラメーターです。
EventCategory	「イベント」インターフェースでイベントを識別するために使用するイベント・カテゴリーを入力します。この値がログ・メッセージに含まれていない場合、 `NameValuePair` 値が使用されます。
SourceIp	メッセージの送信元 IP アドレスを入力します。
SourcePort	メッセージの送信元ポートを入力します。
SourceIpPreNAT	ネットワーク・アドレス変換 (NAT) の実行前のメッセージの送信元 IP アドレスを入力します。
SourceIpPostNAT	NAT 実行後のメッセージの送信元 IP アドレスを入力します。
SourceMAC	メッセージの送信元 MAC アドレスを入力します。
SourcePortPreNAT	NAT 実行前のメッセージの送信元ポートを入力します。
SourcePortPostNAT	NAT 実行後のメッセージの送信元ポートを入力します。
DestinationIp	メッセージの宛先 IP アドレスを入力します。
DestinationPort	メッセージの宛先ポートを入力します。
DestinationIpPreNAT	NAT 実行前のメッセージの宛先 IP アドレスを入力します。
DestinationIpPostNAT	NAT 実行後のメッセージの宛先 IP アドレスを入力します。
DestinationPortPreNAT	NAT 実行前のメッセージの宛先ポートタイプを入力します。

表 291. *Name Value Pair* ログ・フォーマット・タグ (続き)

タグ	説明
DestinationPortPostNAT	NAT 実行後のメッセージの宛先ポートを入力します。
DestinationMAC	メッセージの宛先 MAC アドレスを入力します。
DeviceTime	デバイスに基づいて、イベントの送信時刻を入力します。フォーマットは YY/MM/DD hh:mm:ss です。特定の時刻が指定されない場合は、Syslog ヘッダーまたは **DeviceType** パラメーターが適用されます。
UserName	イベントに関連付けられているユーザー名を入力します。
HostName	イベントに関連付けられているホスト名を入力します。一般に、このパラメーターはアイデンティティー・イベントにのみ関連付けられています。
GroupName	イベントに関連付けられているグループ名を入力します。一般に、このパラメーターはアイデンティティー・イベントにのみ関連付けられています。
NetBIOSName	イベントに関連付けられている NetBIOS 名を入力します。一般に、このパラメーターはアイデンティティー・イベントにのみ関連付けられています。
Identity	このイベントでアイデンティティー・イベントを生成するかどうかを示すため、TRUE または FALSE を入力します。 ログ・メッセージに、**SourceIp** (**IdentityUseSrcIp** パラメーターが TRUE に設定されている) または **DestinationIp** (**IdentityUseSrcIp** パラメーターが FALSE に設定されている) のいずれかと、**UserName**、**SourceMAC**、**HostName**、**NetBIOSName**、**GroupName** パラメーターのいずれか 1 つが含まれている場合に、アイデンティティー・イベントが生成されます。

表 291. *Name Value Pair* ログ・フォーマット・タグ (続き)

タグ	説明
IdentityUseSrcIp	TRUE または FALSE (デフォルト) を入力します。 TRUE は、アイデンティティーに送信元 IP アドレスを使用することを指定します。FALSE は、アイデンティティーに宛先 IP アドレスを使用することを指定します。このパラメーターを使用するのは、Identity パラメーターが TRUE に設定されている場合だけです。

例 1

以下の例では、すべてのフィールドを構文解析します。

```
DeviceType=NVP EventName=Test
DestinationIpPostNAT=172.16.45.10
DeviceTime=2007/12/14 09:53:49
SourcePort=1111 Identity=FALSE SourcePortPostNAT=3333
DestinationPortPostNAT=6666 HostName=testhost
DestinationIpPreNAT=172.16.10.10 SourcePortPreNAT=2222
DestinationPortPreNAT=5555 SourceMAC=AA:15:C5:BF:C4:9D
SourceIp=172.16.200.10 SourceIpPostNAT=172.16.40.50
NetBIOSName=testbois DestinationMAC=00:41:C5:BF:C4:9D
EventCategory=Accept DestinationPort=4444
GroupName=testgroup SourceIpPreNAT=172.16.70.87
UserName=root DestinationIp=172.16.30.30
```

例 2

以下の例では、宛先 IP アドレスを使用してアイデンティティーを提供します。

```
<133>Apr 16 12:41:00 172.16.10.10 namevaluepair:
DeviceType=NVP EventName=Test EventCategory=Accept
Identity=TRUE SourceMAC=AA:15:C5:BF:C4:9D
SourceIp=172.15.210.113 DestinationIp=172.16.10.10
UserName=root
```

例 3

以下の例では、送信元 IP アドレスを使用してアイデンティティーを提供します。

```
DeviceType=NVP EventName=Test
EventCategory=Accept DeviceTime=2007/12/14 09:53:49
SourcePort=5014 Identity=TRUE IdentityUseSrcIp=TRUE
SourceMAC=AA:15:C5:BF:C4:9D SourceIp=172.15.210.113
DestinationIp=172.16.10.10
DestinationMAC=00:41:C5:BF:C4:9D UserName=root
```

例 4

以下は、アイデンティティーを提供しない項目の例です。

```
DeviceType=NVP EventName=Test
EventCategory=Accept DeviceTime=2007/12/14 09:53:49
SourcePort=5014 Identity=FALSE
SourceMAC=AA:15:C5:BF:C4:9D
```

```
SourceIp=172.15.210.113
DestinationIp=172.16.10.10
DestinationMAC=00:41:C5:BF:C4:9D
UserName=root
```

第 84 章 NetApp Data ONTAP

IBM Security QRadar は、Adaptive Log Exporter とともにインストールされる Windows エージェントからの Syslog イベントを受け取ります。

このタスクについて

Adaptive Log Exporter は外部イベント収集エージェントです。Adaptive Log Exporter では、NetApp Data ONTAP プラグインを使用してイベントを収集できます。Adaptive Log Exporter は、NetApp Data ONTAP デバイスで Common Internet File System (CIFS) 監査から生成されるイベント・ログ・メッセージを読み取りおよび処理し、イベントを転送することができます。

Adaptive Log Exporter の使用法について詳しくは、「*Adaptive Log Exporter Users Guide*」を参照してください。

注**:** Adaptive Log Exporter 用の NetApp Data ONTAP プラグインでは CIFS だけがサポートされています。NetApp Data ONTAP デバイスでの CIFS の構成については、ベンダーの資料を参照してください。

QRadar は、Adaptive Log Exporter からの NetApp Data ONTAP イベントを自動的に検出します。NetApp Data ONTAP からイベントを受信するように QRadar を手動で構成するには、以下のようにします。

「ログ・ソース・タイプ」リストで「**NetApp Data ONTAP**」オプションを選択します。

第 85 章 Netskope Active

IBM Security QRadar DSM for Netskope Active は、Netskope Active サーバーからイベントを収集します。

以下の表は、Netskope Active DSM の仕様を示しています。

表 292. *Netskope Active DSM* の仕様

仕様	値
製造元	Netskope
DSM 名	Netskope Active
RPM ファイル名	DSM-NetskopeActive-*Qradar_version-build_number*.noarch.rpm
プロトコル	Netskope Active REST API
記録されるイベント・タイプ	アラート、すべて
自動的に検出?	いいえ
ID を含む?	はい
その他の情報	Netskope Active の Web サイト (www.netskope.com)

Netskope Active DSM を QRadar に統合するには、以下のステップを実行します。

注: 複数の DSM RPM が必要な場合、統合の順序は DSM RPM の依存関係を反映したものでなければなりません。

1. 自動更新が有効になっていない場合は、以下に示す DSM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Netskope Active DSM RPM
   - Netskope Active REST API プロトコル RPM
   - プロトコル共通 RPM
2. 必須パラメーターを構成します。Netskope Active ログ・ソース固有のパラメーターについては、以下の表を使用してください。

表 293. *Netskope Active* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Netskope Active
プロトコル構成	Netskope Active REST API

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『Netskope Active システムからイベントを収集するための QRadar の構成』
すべての監査ログとシステム・イベントを Netskope Active サーバーから収集するには、Netskope Active システムから監査ログとシステム・イベントを収集するように QRadar を構成する必要があります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Netskope Active システムからイベントを収集するための QRadar の構成

すべての監査ログとシステム・イベントを Netskope Active サーバーから収集するには、Netskope Active システムから監査ログとシステム・イベントを収集するように QRadar を構成する必要があります。

このタスクについて

以下の表に、Netskope Active イベントを収集するために必要なパラメーターを示します。

表 294. *Netskope Active DSM* ログ・ソース・パラメーター

パラメーター	説明
IP またはホスト名	partners.goskope.com
認証トークン	認証トークンは、Netskope WebUI で生成され、**Netskope Active REST API** の使用に必要な唯一の資格情報となります。Netskope WebUI のトークン生成オプションにアクセスするには、「設定」 > 「**REST API**」を選択します。
サーバー証明書を自動的に獲得 **(Automatically Acquire Server Certificates)**	ドロップダウン・リストから「はい」を選択すると、QRadar は証明書を自動的にダウンロードし、ターゲット・サーバーを信頼して使用し始めます。正しいサーバーを、「**IP** またはホスト名」フィールドに入力する必要があります。
スロットル **(Throttle)**	1 秒あたりの最大イベント数。デフォルトは 5000 です。
繰り返し **(Recurrence)**	ログ・ソースがデータの取得を試行するタイミングを指定できます。フォーマットは、月/時刻/日を表す M/H/D です。デフォルトは、1 M です。
収集タイプ **(Collection Type)**	すべてのイベント すべてのイベントの収集を選択します。 アラートのみ アラートのみの収集を選択します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**Netskope Active**」を選択します。
7. 「プロトコル構成」リストで、「**Netskope Active REST API**」を選択します。
8. パラメーターを構成します。
9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

第 86 章 Niara

Niara 用の IBM Security QRadar DSM は、Niara Analyzer デバイスからイベントを収集します。

以下の表は、Niara DSM の仕様を示しています。

表 *295. Niara DSM* の仕様

仕様	値
製造元	Niara
DSM 名	Niara
RPM ファイル名	DSM-NiaraNiara-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	1.6
プロトコル	Syslog
イベント・フォーマット	名前と値のペア (NVP)
記録されるイベント・タイプ	セキュリティー システム 内部アクティビティー 引き出し 感染 コマンドと制御
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Niara Web サイト (https://www.niara.com)

Niara を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードし、記載されている順に QRadar コンソールでインストールしてください。
   - DSMCommon RPM
   - Niara DSM RPM
2. Syslog イベントを QRadar に送信するように Niara デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Niara ログ・ソースを追加してください。以下の表は、Niara イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 296. *Niara* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Niara
プロトコル構成	Syslog
ログ・ソース ID	ログ・ソースの固有 ID。

4. QRadar が正しく構成されていることを確認するには、以下の表を参照して、構文解析されたイベント・メッセージの例を確認してください。

   Niara のサンプル・イベント・メッセージを次の表に示します。

表 297. *Niara* のサンプル・イベント・メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
クラウド引き出し	疑わしいアクティビティー	May 6 20:04:38 lab-an-node.niara .com May 7 03:04:38 lab-an-node msg_type=alert detection_time= "2016-05-06 20:04:23 -07:00" alert_name="Large DropBox Upload" alert_type="Cloud Exfiltration" alert_category= "Network Access" alert_severity=60 alert_confidence=20 attack_stage =Exfiltration user_name=kramer src_host_name=lab36.niara.com src_ip=10.43.3.72 dest_ip=45. 58.74.1,108.160.173.65,45.58 .74.129,... description="User kramer on host lab36.niara.com uploaded 324.678654 MB to Dropbox on May 05, 2016; compared with users in the whole Enterprise who uploaded an average of 22.851 KB during the same day" alert_id=35f2173 edef00000000000200010000084fcdc 17d0d3_1462590263066675_Large _DropBox_Upload

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するための Niara の構成

IBM Security QRadar が Niara からイベントを収集できるようにするには、QRadar にイベントを送信するように Niara を構成する必要があります。

手順

1. Niara Analyzer にログインします。
2. 転送を構成します。

a. 「システム構成 **(System Configuration)**」 > 「**Syslog** 宛先 **(Syslog Destinations)**」をクリックします。

b. 以下の転送パラメーターを構成します。

表 *298. Niara Analyzer* 転送パラメーター

パラメーター	値
Syslog 宛先 (Syslog Destination)	QRadar イベント・コレクター (Event Collector)の IP またはホスト名。
プロトコル (Protocol)	TCP または UDP
ポート	514

3. 通知を構成します。

a. 「システム構成 **(System Configuration)**」 > 「セキュリティー・アラート **/ E** メール **(Security Alerts / Emails)**」 > 「新規の追加 **(Add New)**」をクリックします。

b. 以下の通知パラメーターを構成します。

表 *299. Niara Analyzer* 通知パラメーター

パラメーター	値
アラート Syslog 転送を有効にする (Enable Alert Syslog Forwarding)	「アラート **Syslog** 転送を有効にする **(Enable Alert Syslog Forwarding)**」チェック・ボックスを有効にします。
通知の送信 (Sending Notification)	「アラートが生成されるごとに送信する (As Alerts are produced)」。 ライブ・ストリームではなくバッチで送信するように、この設定をカスタマイズできます。
タイム・ゾーン (TimeZone)	ローカル・タイム・ゾーン。

注: すべてのアラートを送信するには、「照会 **(Query)**」、「重大度 **(Severity)**」、および「信頼性 **(Confidence)**」の値をデフォルトのままにしておきます。アラートをフィルターに掛けて、QRadar にアラートのサブセットのみを送信するように、これらの値をカスタマイズできます。

次のタスク

トラブルシューティングに役立てるために、`/var/log/notifier.log` ファイル内の転送ログを参照できます。

新しい通知が作成されるときには、ステップ 3 で説明されているように、「照会 **(Query)**」、「重大度 **(Severity)**」、および「信頼性 **(Confidence)**」の各フィールドと一致する過去 1 週間のアラートが送信されます。

第 87 章 Niksun

IBM Security QRadar 用の Niksun DSM は、syslog を使用して関連するすべての Niksun イベントを記録します。

NetDetector/NetVCR2005 バージョン 3.2.1sp1_2 を QRadar と統合できます。Niksun デバイスと統合するように QRadar を構成する前に、ログ・ソースを構成し、Niksun アプライアンスで syslog 転送を有効にする必要があります。Niksun の構成方法について詳しくは、*Niksun* アプライアンスの資料 を参照してください。

ログ・ソースの構成

IBM Security QRadar に Niksun を統合するには、イベントを受信するためにログ・ソースを手動で作成する必要があります。

このタスクについて

QRadar では、Niksun アプライアンスから転送された Syslog イベントに対して、ログ・ソースの検出と作成は自動的に実行されません。ログ・ソースが自動的に検出されない場合、QRadar にイベントを転送する前にログ・ソースを作成することをお勧めします。

ログ・ソースを構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Niksun 2005 v3.5**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   Syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *300. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Niksun アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。

第 88 章 Nokia Firewall

Check Point Firewall-1 DSM を使用すると、Nokia Firewall アプライアンスから送信された Check Point ベースのファイアウォール・イベントを、Syslog または OPSEC プロトコルを使用することで IBM Security QRadar で受け入れるようにできます。

syslog の使用による Nokia Firewall との統合

この方法では、Nokia Firewall アプライアンスから転送された Check Point の syslog イベントを受け入れるように Nokia Firewall を構成するという選択肢が提供されます。

Nokia Firewall デバイスと統合するように IBM Security QRadar を構成するには、以下の手順を実行します。

1. QRadar コンソールまたはイベント・コレクター (Event Collector)で、Nokia Firewall からの syslog イベントを受け取るように iptables を構成します。
2. syslog イベント・データを転送するように Nokia Firewall を構成します。
3. Nokia Firewall によってログに記録されるイベントを構成します。
4. オプション。QRadar でログ・ソースを構成します。

IPtables の構成

Nokia ファイアウォールでは、Syslog イベントを転送する前に IBM Security QRadar からポート 256 経由で TCP リセット (`rst`) または TCP 応答 (`ack`) を受け取る必要があります。

このタスクについて

Nokia ファイアウォール TCP 要求は、QRadar がオンラインであり Syslog イベントを受信できることを確認することを目的としたオンライン状況要求です。有効なリセットまたは応答を QRadar から受信すると、Nokia ファイアウォールはイベントを UDP ポート 514 で QRadar に転送します。デフォルトでは、QRadar は TCP ポート 256 から受信したすべてのオンライン状況要求に応答しません。

Nokia ファイアウォールから Check Point イベントを受信するすべての イベント・コレクター (Event Collector)または QRadar コンソールで、オンライン状況要求に応答するように IPtables を構成する必要があります。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。

   ログイン: `root`

   パスワード: *<password>*
2. 以下のコマンドを入力して、IPtables ファイルを編集します。

```
vi /opt/qradar/conf/iptables.pre
```

IPtables 構成ファイルが表示されます。

3. 以下のコマンドを入力して、QRadar に対し、Nokia ファイアウォールに対してポート 256 で TCP リセットを使用して応答するように指示します。

```
-A INPUT -s <IP address> -p tcp --dport 256 -j REJECT --reject-with
tcp-reset
```

<*IP address*> は Nokia ファイアウォールの IP アドレスです。QRadar コンソールまたはイベント・コレクター (Event Collector)にイベントを送信する各 Nokia ファイアウォールの IP アドレスに対する TCP リセットを組み込む必要があります。例を以下に示します。

- -A INPUT -s 10.10.100.10/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset
- -A INPUT -s 10.10.110.11/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset
- -A INPUT -s 10.10.120.12/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset

4. IPtables の構成を保存します。
5. 以下のコマンドを入力して、QRadar で IPtables を更新します。

```
./opt/qradar/bin/iptables_update.pl
```

6. ステップ 1 から 5 を繰り返し、Nokia ファイアウォールから Syslog イベントを受信する追加の QRadar イベント・コレクター を構成します。

これで、QRadar にイベントを転送するように Nokia ファイアウォールを構成する準備ができました。

Syslog の構成

IBM Security QRadar に Syslog イベントを転送するように Nokia ファイアウォールを構成するには、以下のようにします。

手順

1. Nokia Voyager にログインします。
2. 「構成 **(Config)**」をクリックします。
3. 「システム構成 (System Configuration)」ペインで「システム・ロギング **(System Logging)**」をクリックします。
4. 「記録先の新しいリモート **IP** アドレスを追加する **(Add new remote IP address to log to)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
5. 「適用」をクリックします。
6. 「保存」をクリックします。

これで、Nokia ファイアウォールによりロガーに記録されるイベントを構成する準備ができました。

ログに記録されるイベントのカスタム・スクリプトの構成

Nokia ファイアウォールによりログに記録され、IBM Security QRadar に転送されるイベントを構成するには、Nokia ファイアウォール用のカスタム・スクリプトを構成する必要があります。

手順

1. SSH を使用して、管理ユーザーとして Nokia ファイアウォールにログインします。

   Nokia ファイアウォールに接続できない場合は、SSH が有効になっているかどうかを確認してください。Nokia Voyager Web インターフェースを使用してコマンド・ラインを有効にするか、またはシリアル接続を使用して直接接続する必要があります。詳しくは、*Nokia Voyager* の資料 を参照してください。
2. 以下のコマンドを入力して、Nokia ファイアウォールの `rc.local` を編集します。

   ```
   vi /var/etc/rc.local
   ```
3. 以下のコマンドを `rc.local` ファイルに追加します。

   ```
   $FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &
   ```
4. `rc.local` ファイルの変更内容を保存します。

   「ターミナル (terminal)」が表示されます。
5. ロギングをすぐに開始するには、以下のコマンドを入力します。

   ```
   nohup $FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &
   ```

   これで、QRadar でログ・ソースを構成できるようになりました。

ログ・ソースの構成

Nokia ファイアウォールにより転送されるイベントは、Check Point Firewall-1 DSM により自動的に検出されます。自動検出処理により、Nokia Firewall アプライアンスからの syslog イベントに対してログ・ソースが作成されます。

このタスクについて

以下の手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。

8. 「ログ・ソース・タイプ」リストで、「**Check Point Firewall-1**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

Syslog プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Nokia ファイアウォール・アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

Nokia ファイアウォールから Check Point イベントを Syslog 経由で受信するための Syslog 構成は完了です。Nokia ファイアウォールからの Check Point イベントは、IBM Security QRadar の「ログ・アクティビティー」タブに表示されます。

OPSEC の使用による Nokia Firewall との統合

IBM Security QRadar は、OPSEC/LEA プロトコルを使用して構成された Check Point FireWall-1 DSM により、Nokia Firewall からの Check Point FireWall-1 イベントを受け入れることができます。

Nokia Firewall デバイスと統合するように QRadar を構成する前に、以下を実行する必要があります。

1. OPSEC を使用して Nokia Firewall を構成します。『OPSEC 用の Nokia ファイアウォールの構成』を参照してください。
2. OPSEC LEA プロトコルを使用して Nokia Firewall 用に QRadar でログ・ソースを構成します。 795 ページの『OPSEC ログ・ソースの構成』を参照してください。

OPSEC 用の Nokia ファイアウォールの構成

OPSEC を使用して Nokia ファイアウォールを構成できます。

手順

1. IBM Security QRadar のホスト・オブジェクトを作成するには、Check Point SmartDashboard GUI を開き、「管理 **(Manage)**」 > 「ネットワーク・オブジェクト **(Network Objects)**」 > 「新規 **(New)**」 > 「ノード **(Node)**」 > 「ホスト **(Host)**」を選択します。
2. QRadar の名前、IP アドレスを入力し、オプションでコメントを入力します。
3. 「**OK**」をクリックします。
4. 「閉じる **(Close)**」を選択します。

5. OPSEC 接続を作成するために、「管理 **(Manage)**」 > 「サーバーと **OPSEC** アプリケーション **(Servers and OPSEC Applications)**」 > 「新規 **(New)**」 > 「**OPSEC** アプリケーション・プロパティー **(OPSEC Application Properties)**」を選択します。
6. 名前を入力し、オプションでコメントを入力します。

   入力する名前は、 794 ページの『OPSEC 用の Nokia ファイアウォールの構成』での名前とは異なる必要があります。
7. 「ホスト **(Host)**」ドロップダウン・メニューから、作成した QRadar ホスト・オブジェクトを選択します。
8. 「アプリケーション・プロパティー **(Application Properties)**」から、「ベンダー・タイプとしてユーザー定義 **(User Defined as the Vendor Type)**」を選択します。
9. 「クライアント項目 **(Client Entries)**」から「**LEA**」を選択します。
10. 「通信 **(Communication)**」を選択し、Secure Internal Communication (SIC) 証明書を構成するためアクティベーション・キーを入力します。
11. 「**OK**」を選択し、次に「閉じる **(Close)**」を選択します。
12. ファイアウォールにポリシーをインストールするために、「ポリシー **(Policy)**」 > 「インストール **(Install)**」 > 「**OK**」を選択します。

    ポリシーについて詳しくは、ベンダーの資料を参照してください。これで、QRadar で Nokia ファイアウォールのログ・ソースを構成できるようになりました。

OPSEC ログ・ソースの構成

IBM Security QRadar では OPSEC/LEA ログ・ソースは自動的に検出されないため、イベント収集のために OPSEC ログ・ソースを作成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Check Point FireWall-1**」を選択します。
9. 「プロトコル構成」リストで「**OPSEC/LEA**」を選択します。
10. 以下の値を構成します。

表 *301. OPSEC/LEA* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。 IP アドレスまたはホスト名では、QRadar がログ・ファイルを固有のイベント・ソースと突き合わせることができるため、IP アドレスまたはホスト名を使用することをお勧めします。
サーバー **IP**	サーバーの IP アドレスを入力します。
サーバー・ポート	OPSEC 通信に使用するポートを入力します。有効な範囲は 0 から 65,536、デフォルトは 18184 です。
ログ・ソースにサーバー **IP** を使用	ログ・ソースに管理対象デバイスの IP アドレスではなく LEA サーバーの IP アドレスを使用する場合は、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
統計レポートの間隔	Syslog イベントが `qradar.log` ファイルに記録される期間を秒数で入力します。 有効な範囲は 4 から 2,147,483,648、デフォルトは 600 です。

表 *301. OPSEC/LEA* プロトコルのパラメーター *(*続き*)*

パラメーター	説明
認証タイプ	リストから、当該 LEA 構成で使用する「認証タイプ」を選択します。オプションは **sslca** (デフォルト)、**sslca_clear**、または **clear** です。この値は、サーバーが使用する認証方式と一致している必要があります。認証タイプとして **sslca** または **sslca_clear** を選択する場合は、以下のパラメーターが表示されます。 • **OPSEC** アプリケーション・オブジェクトの **SIC** 属性 **(SIC** 名**) (OPSEC Application Object SIC Attribute (SIC Name))** - OPSEC アプリケーション・オブジェクトの Secure Internal Communications (SIC) 名を入力します。SIC 名はアプリケーションの識別名 (DN) です (例: `CN=LEA, o=fwconsole..7psasx`)。この名前の最大長は 255 文字であり、大/小文字が区別されます。 • ログ・ソースの**/ SIC** 属性 **(SIC** エンティティー名**) (Log Source SIC Attribute (Entity SIC Name))** - サーバーの SIC 名を入力します (例: `cn=cp_mgmt,o=fwconsole..7psasx`)。名前の最大長は 255 文字で、大/小文字が区別されます。 • 証明書の指定 **(Specify Certificate)** - この LEA 構成の証明書を定義する場合は、このチェック・ボックスを選択します。QRadar は、証明書が必要な場合にこれらのパラメーターを使用して証明書の取得を試行します。 「証明書の指定 **(Specify Certificate)**」チェック・ボックスを選択すると、「証明書のファイル名 **(Certificate Filename)**」パラメーターが表示されます。 • 証明書のファイル名 **(Certificate Filename)** -このオプションは、「証明書の指定 **(Specify Certificate)**」が選択されている場合にのみ表示されます。当該構成で使用する証明書のファイル名を入力します。構成ファイルは、`/opt/qradar/conf/trusted_certificates/lea` ディレクトリーに配置されている必要があります。 「証明書の指定 **(Specify Certificate)**」チェック・ボックスをクリアすると、以下のパラメーターが表示されます。 • 認証局の **IP (Certificate Authority IP)** - 証明書の取得元 SmartCenter サーバーの IP アドレスを入力します。 • 証明書パスワードのプル **(Pull Certificate Password)** - 証明書を要求するときに使用するパスワードを入力します。パスワードの最大長は 255 文字です。 • **OPSEC** アプリケーション **(OPSEC Application)** - 証明書を要求するときに使用するアプリケーションの名前を入力します。この値の長さは 255 文字まで可能です。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。受信したイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

第 89 章 Nominum Vantio

IBM Security QRadar 用の Nominum Vantio DSM は、Nominum Vantio LEEF アダプターがインストールされている Nominum Vantio エンジンから転送されたログ・イベント拡張フォーマット (LEEF) の syslog イベントを受け入れます。

QRadar は、Nominum Vantio から転送されたすべての関連イベントを受け入れます。

Vantio LEEF アダプターは、Lightweight View Policy (LVP) 一致に基づいて LEEF メッセージを作成します。Vantio LEEF アダプターが処理する LVP 一致を生成するには、Vantio エンジン用の Lightweight View および LVP モニターを構成する必要があります。LVP は、Nominum Vantio 製品のオプションのライセンス・コンポーネントです。LVP の構成方法について詳しくは、「*Vantio Administrator's Manual*」を参照してください。

Nominum Vantio イベントを QRadar と統合するには、事前に Vantio LEEF アダプターをインストールして構成する必要があります。Vantio LEEF アダプターを入手する場合、または追加情報を請求する場合は、Nominum に E メール (アドレス: leefadapter@nominum.com) を送信してください。

Vantio LEEF Adapter の構成

Vantio LEEF Adapter をインストールして構成できます。

手順

1. SSH を使用して、Vantio エンジン・サーバーにログインします。
2. Vantio LEEF Adapter をインストールします。

   ```
   sudo rpm -I VantioLEEFAdapter-0.1-a.x86_64.rpm
   ```
3. Vantio LEEF Adapter 構成ファイルを編集します。

   ```
   usr/local/nom/sbin/VantioLEEFAdapter
   ```
4. LEEF イベントを IBM Security QRadar に転送するように Vantio LEEF Adapter を構成します。

   ```
   -qradar-dest-addr=<IP Address>
   ```

   ここで、*<IP Address>* は QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
5. Vantio LEEF 構成ファイルを保存します。
6. 以下のコマンドを入力して、Vantio Adapter を開始します。

   ```
   usr/local/nom/sbin/VantioLEEFAdapter &
   ```

構成は完了です。Nominum Vantio イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。Vantio LEEF Adapter により QRadar に転送されるイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Vantio LEEF Adapter からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

このタスクについて

Nominum Vantio のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Nominum Vantio**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   Syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	Nominum Vantio からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

第 90 章 Nortel Networks

さまざまな Nortel Networks DSM を IBM Security QRadar と統合できます。

Nortel Multiprotocol Router

Nortel Multiprotocol Router DSM for IBM Security QRadar は、Syslog を使用して関連するすべての Nortel Multiprotocol Router イベントを記録します。

このタスクについて

Nortel Multiprotocol Router デバイスと統合するように QRadar を構成する前に、以下の手順を実行する必要があります。

手順

1. Nortel Multiprotocol Router デバイスにログインします。
2. プロンプトで以下のコマンドを入力します。

   ```
   bcc
   ```

   Bay Command Console プロンプトが表示されます。

   ```
   Welcome to the Bay Command Console!

   * To enter configuration mode, type config

   * To list all system commands, type ?

   * To exit the BCC, type exit

   bcc>
   ```
3. 以下のコマンドを入力して、構成モードにアクセスします。

   ```
   config
   ```
4. 以下のコマンドを入力して、Syslog 構成にアクセスします。

   ```
   syslog
   ```
5. 以下のコマンドを入力します。

   ```
   log-host address <IP address>
   ```

   ここで *<IP address>* は、QRadar の IP アドレスです。
6. QRadar の現在のデフォルト設定を表示します。

   ```
   info
   ```

   例:

   ```
   log-host/10.11.12.210# info
   ```

```
address 10.11.12.210

log-facility local0

state enabled
```

7. 801 ページの『Nortel Multiprotocol Router』で入力したコマンドの出力に、状態が enabled ではないことが示される場合は、以下のコマンドを入力して Syslog ホストの転送を有効にします。

```
state enable
```

8. ログ・ファシリティー・パラメーターを構成します。

```
log-facility local0
```

9. ハードウェア・スロットが Syslog イベントを転送できるようにするため、ハードウェア・スロットのフィルターを作成します。以下のコマンドを入力して、WILDCARD という名前のフィルターを作成します。

```
filter name WILDCARD entity all
```

10. slot-upper bound パラメーターを構成します。

```
slot-upper bound <number of slots>
```

ここで *<number of slots>* は、デバイスで使用可能なスロットの数です。このパラメーターでは、ご使用の Nortel Multiprotocol Router デバイスのバージョンに応じて異なる構成が必要となることがあります。これにより、デバイスで使用可能なスロットの最大数が決定します。

11. QRadar に送信する Syslog メッセージのレベルを構成します。

```
severity-mask all
```

12. このフィルターの現在の設定を表示します。

```
info
```

例えば、以下のようにします。

```
filter/10.11.12.210/WILDCARD# info

debug-map debug

entity all

event-lower-bound 0

event-upper-bound 255

fault-map critical

info-map info

name WILDCARD

severity-mask {fault warning info trace debug}
```

```
slot-lower-bound 0

slot-upper-bound 1

state enabled

trace-map debug

warning-map warning
```

13. Syslog フィルターの現在構成されている設定を表示します。

    ```
    show syslog filters
    ```

    syslog パラメーターと filter パラメーターが正しく構成されている場合、「Operational State」は up を示します。

    例:

    ```
    syslog# show syslog filters

    show syslog filters Sep 15, 2008 18:21:25 [GMT+8]
    ```

表 302. *Syslog* フィルター

Host IP address	Filter Name	Entity Name	Entity Code	Configured State	Operational State
10.11.12.130	WILDCARD	all	255	enabled	up
10.11.12.210	WILDCARD	all	255	enabled	up

14. 現在構成されている Syslog ホスト情報を表示します。

    ```
    show syslog log-host
    ```

    ホスト・ログに、さまざまな Syslog ホストに送信されるパケットの数が表示されます。

    例:

    ```
    syslog# show syslog log-host

    show syslog log-host Sep 15, 2008 18:21:32 [GMT+8]
    ```

表 303. *Syslog* ホストのログ

Host IP address	Configured State	Operational State	Time Sequencing	UDP Port	Facility Code	#Messages Sent
10.11.12.130	enabled	up	disabled	514	local0	1402
10.11.12.210	enabled	up	disabled	514	local0	131

15. コマンド・ライン・インターフェースを終了します。

a. 現在のコマンド・ラインを終了して bcc コマンド・ラインに戻ります。

```
exit
```

16. bbc コマンド・ラインを終了します。

```
exit
```

17. コマンド・ライン・セッションを終了します。

```
logout
```

18. これで、QRadar でログ・ソースを構成できるようになりました。

Nortel Multiprotocol Router デバイスからイベントを受信するように QRadar を構成するには、以下のようにします。

a. 「ログ・ソース・タイプ」リストで「**Nortel Multiprotocol Router**」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel Application Switch

Nortel Application Switch は、レイヤー 4 から 7 の情報を使用してレイヤー 2 の速度でトラフィックを転送することで、ルーティングとスイッチングを統合します。

このタスクについて

Nortel Application Switch DSM for IBM Security QRadar は、Syslog を使用してイベントを受け取ります。QRadar は、関連する状況とネットワーク状態イベントをすべて記録します。QRadar で Nortel Application Switch デバイスを構成する前に、Syslog イベントを QRadar に送信するようにデバイスを構成する必要があります。

Syslog イベントを QRadar に送信するようにデバイスを構成するには、以下のようにします。

手順

1. Nortel Application Switch のコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力します。

```
/cfg/sys/syslog/host
```

3. 以下のプロンプトで、QRadar の IP アドレスを入力します。

Enter new syslog host: <*IP address*>

ここで *<IP address>* は、QRadar の IP アドレスです。

4. 構成を適用します。

   ```
   apply
   ```

5. 新しい構成の適用後に、構成を保存します。

   ```
   save
   ```

6. 構成をフラッシュに保存することを確認するためのプロンプトで y と入力します。 以下の例を参照してください。

   ```
   Confirm saving to FLASH [y/n]: y

   New config successfully saved to FLASH
   ```

   次に、Nortel Application Switch からイベントを受信するように QRadar を構成する必要があります。

7. QRadar でログ・ソースを構成します。「ログ・ソース・タイプ」リストで「**Nortel Application Switch**」オプションを選択します。

   Nortel Application Switch について詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel Contivity

QRadar Nortel Contivity DSM は、Syslog を使用して関連するすべての Nortel Contivity イベントを記録します。

このタスクについて

Nortel Contivity デバイスと統合するように QRadar を構成する前に、以下の手順を実行します。

手順

1. Nortel Contivity のコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力します。

   enable *<password>*

   ここで *<password>* は Nortel Contivity デバイス管理パスワードです。

3. 以下のコマンドを入力します。

   ```
   config t
   ```

4. ロギング情報を構成します。

   ```
   logging <IP address> facility-filter all level all
   ```

ここで、*<IP address>* は QRadar の IP アドレスです。

5. 以下のコマンドを入力して、コマンド・ラインを終了します。

   ```
   exit
   ```

   次に、Nortel Contivity デバイスからイベントを受信するように QRadar を構成する必要があります。

6. これで、QRadar でログ・ソースを構成できるようになりました。「ログ・ソース・タイプ」リストで「**Nortel Contivity VPN スイッチ (Nortel Contivity VPN Switch)**」オプションを選択します。

   Nortel Contivity デバイスについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel イーサネット・ルーティング・スイッチ 2500/4500/5500

IBM Security QRadar Nortel イーサネット・ルーティング・スイッチ (ERS) 2500/4500/5500 DSM は、Syslog を使用して関連するすべてのルーティング・スイッチ・イベントを記録します。

このタスクについて

QRadar で Nortel ERS 2500/4500/5500 デバイスを構成する前に、Syslog イベントを QRadar に送信するようにデバイスを構成する必要があります。

Syslog イベントを QRadar に送信するようにデバイスを構成するには、以下のようにします。

手順

1. Nortel ERS 2500/4500/5500 のユーザー・インターフェースにログインします。
2. 以下のコマンドを入力して、グローバル構成モードにアクセスします。

   ```
   ena

   config term
   ```

3. リモート・サーバーに送信するログの重大度レベルとして `informational` を入力します。

   例: `logging remote level {critical|informational|serious|none}`

   ```
   logging remote level informational
   ```

重大度レベル `informational` では、すべてのログが Syslog サーバーに送信されます。

4. ホストを有効にします。

   ```
   host enable
   ```

5. リモート・ロギング・アドレスを入力します。

   ```
   logging remote address <IP address>
   ```

   ここで、*<IP address>* は QRadar システムの IP アドレスです。

6. リモート・ロギングが有効であることを確認します。

   `logging remote enable` これで、QRadar でログ・ソースを構成できるようになりました。

7. Nortel ERS 2500/4500/5500 デバイスからイベントを受信するように構成するには、「ログ・ソース・タイプ」リストで「**Nortel** イーサネット・ルーティング・スイッチ **2500/4500/5500 (Nortel Ethernet Routing Switch 2500/4500/5500)**」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel イーサネット・ルーティング・スイッチ 8300/8600

IBM Security QRadar Nortel Ethernet Routing Switch (ERS) 8300/8600 DSM は、Syslog を使用して関連するすべてのイベントを記録します。

このタスクについて

QRadar で Nortel ERS 8600 デバイスを構成する前に、Syslog イベントを QRadar に送信するようにデバイスを構成する必要があります。

Syslog イベントを QRadar に送信するようにデバイスを構成するには、以下のようにします。

手順

1. Nortel ERS 8300/8600 のコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力します。

   ```
   config sys syslog host <ID>
   ```

   ここで *<ID>* は、Syslog イベントを QRadar に送信するように構成するホストの ID です。

Syslog ホスト ID の有効範囲は、1 から 10 です。

3. QRadar システムの IP アドレスを入力します。

   address <*IP address*>

   ここで <IP address> は、QRadar システムの IP アドレスです。

4. Syslog ホストにアクセスするためのファシリティーを入力します。

   ```
   host <ID> facility local0
   ```

   ここで、<*ID*> は 807 ページの『Nortel イーサネット・ルーティング・スイッチ 8300/8600』で指定した ID です。

5. ホストを有効にします。

   ```
   host enable
   ```

6. 送信する Syslog メッセージの重大度レベルを入力します。

   ```
   host <ID> severity info
   ```

   ここで、<*ID*> は 807 ページの『Nortel イーサネット・ルーティング・スイッチ 8300/8600』で指定した ID です。

7. Syslog メッセージ送信機能を有効にします。

   ```
   state enable
   ```

8. ホストの Syslog 構成を検証します。

   ```
   sylog host <ID> info
   ```

   出力は次のようになります。

   ```
   ERS-8606:5/config/sys/syslog/host/1# info Sub-Context: Current Context:
   address : 10.10.10.1 create : 1 delete : N/A facility : local6 host :
   enable mapinfo : info mapwarning : warning maperror : error mapfatal :
   emergency severity : info|warning|error|fatal udp-port : 514
   ERS-8606:5/config/sys/syslog/host/1#
   ```

   これで、QRadar でログ・ソースを構成できるようになりました。

9. Nortel ERS 8300/8600 デバイスからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Nortel** イーサネット・ルーティング・スイッチ **8300/8600 (Nortel Ethernet Routing Switch 8300/8600)**」オプションを選択します。

関連タスク:

5 ページの『ログ・ソースの追加』

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel Secure Router

IBM Security QRadar Nortel Secure Router DSM は、Syslog を使用して関連するすべてのルーター・イベントを記録します。

このタスクについて

QRadar で Nortel Secure Router デバイスを構成する前に、Syslog イベントを QRadar に送信するようにデバイスを構成する必要があります。

Syslog イベントを QRadar に送信するようにデバイスを構成するには、以下のようにします。

手順

1. Nortel Secure Router のコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のように入力して、グローバル構成モードにアクセスします。

   ```
   config term
   ```
3. 以下のコマンドを入力します。

   ```
   system logging syslog
   ```
4. Syslog サーバー (QRadar システム) の IP アドレスを入力します。

   ```
   host_ipaddr <IP address>
   ```

   ここで、*<IP address>* は QRadar システムの IP アドレスです。
5. リモート・ロギングが有効であることを確認します。

   ```
   enable
   ```
6. ロギング・レベルが正しく構成されていることを確認します。

   ```
   show system logging syslog
   ```

   以下のコードは出力例です。

   ```
   ----------------------------------- Syslog Setting

   ----------------------------------- Syslog:

   Enabled Host IP Address: 10.10.10.1 Host UDP Port: 514

   Facility Priority Setting:

   facility priority

   ======== ========

   auth: info

   bootp: warning

   daemon: warning

   domainname: warning

   gated: warning
   ```

```
kern: info

mail: warning

ntp: warning

system: info

fr: warning

ppp: warning

ipmux: warning

bundle: warning

qos: warning

hdlc: warning

local7: warning

vpn: warning

firewall: warning
```

これで、QRadar でログ・ソースを構成できるようになりました。

7. Nortel Secure Router デバイスからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Nortel Secure Router**」オプションを選択します。

関連タスク:

5 ページの『ログ・ソースの追加』

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel Secure Network Access Switch

IBM Security QRadar Nortel Secure Network Access Switch (SNAS) DSM は、Syslog を使用して関連するすべてのスイッチ・イベントを記録します。

このタスクについて

QRadar で Nortel SNAS デバイスを構成する前に、以下の手順を実行します。

手順

1. Nortel SNAS ユーザー・インターフェースにログインします。
2. 「構成 **(Config)**」タブを選択します。
3. 「ナビゲーション (Navigation)」ペインで「セキュア・アクセス・ドメインおよび **Syslog (Secure Access Domain and Syslog)**」を選択します。

   「セキュア・アクセス・ドメイン (Secure Access Domain)」ウィンドウが表示されます。

4. 「セキュア・アクセス・ドメイン **(Secure Access Domain)**」リストで「セキュア・アクセス・ドメイン **(secure access domain)**」を選択します。「最新表示 **(Refresh)**」をクリックします。
5. 「追加」をクリックします。

   「新規リモート・サーバーの追加 **(Add New Remote Server)**」ウィンドウが表示されます。
6. 「更新 **(Update)**」をクリックします。

   セキュア・アクセス・ドメイン・テーブルにサーバーが表示されます。
7. ツールバーを使用して「適用 **(Apply)**」をクリックし、Nortel SNAS に現在の変更内容を送信します。

   これで、QRadar でログ・ソースを構成する準備ができました。
8. Nortel SNAS デバイスからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Nortel Secure Network Access Switch (SNAS)**」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel Switched Firewall 5100

IBM Security QRadar Nortel Switched Firewall 5100 DSM は、syslog または OPSEC を使用してすべての関連するファイアウォール・イベントを記録します。

QRadar で Nortel Switched Firewall デバイスを構成する前に、QRadar にイベントを送信するようにデバイスを構成する必要があります。

以下のいずれかの方法を使用して Nortel Switched Firewall を構成する方法についての情報を参照してください。

- 『Syslog を使用した Nortel Switched Firewall の統合』
- 812 ページの『OPSEC の使用による Nortel Switched Firewall との統合』

Syslog を使用した Nortel Switched Firewall の統合

この手順では、IBM Security QRadar Nortel Switched Firewall 5100 DSM が Syslog を使用してイベントを確実に受け入れるようにします。

このタスクについて

Nortel Switched Firewall 5100 を構成するには、以下のようにします。

手順

1. Nortel Switched Firewall デバイスのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力します。

   ```
   /cfg/sys/log/syslog/add
   ```
3. 以下のプロンプトで QRadar システムの IP アドレスを入力します。

   ```
   Enter IP address of syslog server:
   ```

   重大度レベルを構成するためのプロンプトが表示されます。
4. 重大度レベルとして **info** を構成します。

   例: `Enter minimum logging severity`

   `(emerg | alert | crit | err | warning | notice | info | debug): info`

   ファシリティーを構成するためのプロンプトが表示されます。
5. ローカル・ファシリティーとして **auto** を構成します。

   例: `Enter the local facility (auto | local0-local7): auto`
6. 構成を適用します。

   ```
   apply
   ```
7. クラスター内のファイアウォールごとにこの手順を繰り返します。

   これで、QRadar でログ・ソースを構成する準備ができました。
8. Nortel Switched Firewall 5100 デバイスから Syslog を使用してイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Nortel Switched Firewall 5100**」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

OPSEC の使用による Nortel Switched Firewall との統合

この手順では、IBM Security QRadar Nortel Switched Firewall 5100 DSM が OPSEC を使用して Check Point FireWall-1 イベントを確実に受け入れるようにします。

Check Point SmartCenter Server 用の手順は、オペレーティング・システムによって異なります。以下は、Check Point SecurePlatform オペレーティング・システムに基づく手順です。

Nortel Switched Firewall を QRadar と統合できるようにするには、以下の手順を実行します。

1. Check Point SmartCenter Server を再構成します。
2. QRadar でログ・ソースを構成します。

ログ・ソースの構成

QRadar でログ・ソースを構成します。

手順

1. OPSEC を使用する Nortel Switched Firewall 5100 デバイスからイベントを受け取るように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**Nortel Switched Firewall 5100**」オプションを選択する必要があります。
2. OPSEC LEA を使用する Check Point SmartCenter Server からイベントを受け取るように QRadar を構成するには、プロトコルの構成時に「プロトコル構成」リストから「**LEA**」オプションを選択する必要があります。

関連概念:

29 ページの『OPSEC/LEA プロトコルの構成オプション』
ポート 18184 でイベントを受信するには、OPSEC/LEA プロトコルを使用するようにログ・ソースを構成します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel Switched Firewall 6000

IBM Security QRadar Nortel Switched Firewall 6000 DSM は、syslog または OPSEC を使用してすべての関連するファイアウォール・イベントを記録します。

QRadar で Nortel Switched Firewall デバイスを構成する前に、QRadar にイベントを送信するようにデバイスを構成する必要があります。

以下は、Nortel Switched Firewall 6000 デバイスおよび QRadar を構成する方法についての情報です。以下のいずれかの方法を使用してください。

- 『Nortel Switched Firewall 用の Syslog の構成』
- 814 ページの『Nortel Switched Firewall の OPSEC の構成』

Nortel Switched Firewall 用の Syslog の構成

この手順では、IBM Security QRadar Nortel Switched Firewall 6000 DSM が Syslog を使用してイベントを確実に受け入れるようにします。

このタスクについて

Nortel Switched Firewall 6000 を構成するには、以下のようにします。

手順

1. Nortel Switched Firewall デバイスのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力します。

   ```
   /cfg/sys/log/syslog/add
   ```

3. 以下のプロンプトで QRadar システムの IP アドレスを入力します。

   ```
   Enter IP address of syslog server:
   ```

   重大度レベルを構成するためのプロンプトが表示されます。
4. 重大度レベルとして **info** を構成します。

   例: `Enter minimum logging severity`

   `(emerg | alert | crit | err | warning | notice | info | debug): info`

   ファシリティーを構成するためのプロンプトが表示されます。
5. ローカル・ファシリティーとして **auto** を構成します。

   例: `Enter the local facility (auto | local0-local7): auto`
6. 構成を適用します。

   ```
   apply
   ```

   これで、QRadar でログ・ソースを構成できるようになりました。
7. Nortel Switched Firewall 6000 デバイスからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Nortel Switched Firewall 6000**」オプションを選択します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel Switched Firewall の OPSEC の構成

この手順では、IBM Security QRadar Nortel Switched Firewall 6000 DSM が OPSEC を使用して Check Point FireWall-1 イベントを確実に受け入れるようにします。

このタスクについて

Check Point SmartCenter Server 用の手順は、オペレーティング・システムによって異なります。以下は、Check Point SecurePlatform オペレーティング・システムに基づく手順です。

Nortel Switched Firewall を QRadar と統合できるようにするには、以下の手順を実行します。

手順

1. Check Point SmartCenter Server を再構成します。『Check Point SmartCenter Server の再構成』を参照してください。
2. QRadar で OPSEC LEA プロトコルを構成します。

   OPSEC LEA を使用する Check Point SmartCenter Server からイベントを受け取るように QRadar を構成するには、LEA の構成時に「プロトコル構成」リストから「**LEA**」オプションを選択する必要があります。
3. QRadar でログ・ソースを構成します。

   OPSEC を使用する Nortel Switched Firewall 6000 デバイスからイベントを受け取るように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**Nortel Switched Firewall 6000**」オプションを選択する必要があります。

関連概念:

29 ページの『OPSEC/LEA プロトコルの構成オプション』
ポート 18184 でイベントを受信するには、OPSEC/LEA プロトコルを使用するようにログ・ソースを構成します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Check Point SmartCenter Server の再構成

Check Point SmartCenter Server では、IBM Security QRadar システムを表すホスト・オブジェクトを作成できます。*leapipe* は、Check Point SmartCenter Server と QRadar の間の接続です。

このタスクについて

Check Point SmartCenter Server を再構成するには、以下のようにします。

手順

1. ホスト・オブジェクトを作成するために、Check Point SmartDashboard ユーザー・インターフェースを開き、「管理 **(Manage)**」 > 「ネットワーク・オブジェクト **(Network Objects)**」 > 「新規 **(New)**」 > 「ノード **(Node)**」 > 「ホスト **(Host)**」を選択します。
2. ホストの名前、IP アドレスを入力し、必要に応じてホストのコメントを入力します。
3. 「**OK**」をクリックします。
4. 「閉じる **(Close)**」を選択します。
5. OPSEC 接続を作成するために、「管理 **(Manage)**」 > 「サーバーと **OPSEC** アプリケーション **(Servers and OPSEC applications)**」 > 「新規 **(New)**」 > 「**OPSEC** アプリケーション・プロパティー **(OPSEC Application Properties)**」を選択します。
6. 名前を入力し、必要に応じてコメントを入力します。

入力する名前は、 815 ページの『Check Point SmartCenter Server の再構成』での名前とは異なる必要があります。

7. 「ホスト **(Host)**」ドロップダウン・メニューから、 815 ページの『Check Point SmartCenter Server の再構成』で作成したホスト・オブジェクトを選択します。
8. 「アプリケーション・プロパティー **(Application Properties)**」から、ベンダーとして「ユーザー定義 **(User Defined)**」を選択します。
9. 「クライアント項目 **(Client Entries)**」から「**LEA**」を選択します。
10. 「通信 **(Communication)**」をクリックして Secure Internal Communication (SIC) 証明書を生成し、アクティベーション・キーを入力します。
11. 「**OK**」をクリックし、次に「閉じる **(Close)**」をクリックします。
12. ファイアウォールにセキュリティー・ポリシーをインストールするため、「ポリシー **(Policy)**」 > 「インストール」 > 「**OK**」をクリックします。

構成は完了です。

Nortel Threat Protection System (TPS)

IBM Security QRadar Nortel Threat Protection System (TPS) DSM は、Syslog を使用して関連する脅威イベントとシステム・イベントをすべて記録します。

このタスクについて

QRadar で Nortel TPS デバイスを構成する前に、以下の手順を実行します。

手順

1. Nortel TPS ユーザー・インターフェースにログインします。
2. 「ポリシーと応答 **(Policy & Response)**」 > 「侵入センサー **(Intrusion Sensor)**」 > 「検出と保護 **(Detection & Prevention)**」を選択します。

   「検出と保護 (Detection & Prevention)」ウィンドウが表示されます。
3. アラート・オプションを構成する侵入ポリシーの横の「編集 **(Edit)**」をクリックします。

   「ポリシーの編集 (Edit Policy)」ウィンドウが表示されます。
4. 「アラート設定 **(Alerting)**」をクリックします。

   「アラート設定 (Alerting)」ウィンドウが表示されます。
5. 「**Syslog** の構成 **(Syslog Configuration)**」で「状態の次にオン **(on next to State)**」を選択し、*Syslog* アラート を有効にします。
6. リストからファシリティーと優先レベルを選択します。
7. オプション: 「ロギング・ホスト **(Logging Host)**」フィールドに、QRadar システムの IP アドレスを入力します。これにより、QRadar システムがロギング・ホストとして構成されます。複数のホストはコンマで区切って指定します。
8. 「保存」をクリックします。

Syslog アラート 構成が保存されます。

9. 適切な検出エンジンにポリシーを適用します。

   これで、QRadar でログ・ソースを構成できるようになりました。

10. Nortel TPS デバイスからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Nortel Threat Protection System (TPS) Intrusion Sensor**」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Nortel VPN Gateway

IBM Security QRadar Nortel VPN Gateway DSM は、Syslog を使用してイベントを受け取ります。

このタスクについて

QRadar は、関連するオペレーティング・システム (OS)、システム制御、トラフィック処理、起動、構成の再ロード、AAA、および IPsec イベントをすべて記録します。QRadar で Nortel VPN Gateway デバイスを構成する前に、Syslog イベントを QRadar に送信するようにデバイスを構成しておく必要があります。

Syslog イベントを QRadar に送信するようにデバイスを構成するには、以下のようにします。

手順

1. Nortel VPN Gateway コマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力します。

   ```
   /cfg/sys/syslog/add
   ```

3. プロンプトで、QRadar システムの IP アドレスを入力します。

   ```
   Enter new syslog host: <IP address>
   ```

   ここで、*<IP address>* は QRadar システムの IP アドレスです。

4. 構成を適用します。

   ```
   apply
   ```

5. システム構成に現在追加されているすべての Syslog サーバーを表示します。

   ```
   /cfg/sys/syslog/list
   ```

   これで、QRadar でログ・ソースを構成できるようになりました。

6. Nortel VPN Gateway デバイスからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Nortel VPN Gateway**」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 91 章 Novell eDirectory

IBM Security QRadar 用の Novell eDirectory DSM は、syslog を使用して Novell eDirectory からの監査イベントを受け取ります。

Novell eDirectory DSM を使用するには、以下のコンポーネントをインストールする必要があります。

- Novell eDirectory v8.8 (サービス・パック 6 (sp6))
- Novell Audit プラグイン
- Novell iManager v2.7
- XDASv2

Novell eDirectory を QRadar とともに構成するには、以下を実行する必要があります。

1. イベントを QRadar に転送するように XDASv2 プロパティー・ファイルを構成します。
2. ご使用の Linux または Windows オペレーティング・システムに XDASv2 モジュールをロードします。
3. Novell iManager に Novell Audit プラグインをインストールします。
4. Novell iManager を使用して監査を構成します。
5. QRadar を構成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

イベント転送のための XDASv2 の構成

デフォルトでは、XDASv2 はイベントをファイルに記録するように構成されています。イベントを XDASv2 から QRadar に転送するには、`xdasconfig.properties.template` を編集し、Syslog を転送するようにこのファイルを構成する必要があります。

このタスクについて

監査イベントは、ファイルに記録するのではなく、Syslog から QRadar に転送する必要があります。

Syslog イベントを転送するように XDASv2 を構成するには、以下のようにします。

手順

1. Novell eDirectory をホストするサーバーにログインします。
2. 編集する以下のファイルを開きます。
   - Windows - C:¥Novell¥NDS¥xdasconfig.properties.template
   - Linux または Solaris - etc/opt/novell/eDirectory/conf/xdasconfig.properties.template
3. ルート・ロガーを設定するには、以下の行でコメント・マーカー (#) を削除します。

   ```
   log4j.rootLogger=debug, S, R
   ```
4. アペンダーを設定するには、以下の行でコメント・マーカー (#) を削除します。

   ```
   log4j.appender.S=org.apache.log4j.net.SyslogAppender
   ```
5. Syslog 宛先の IP アドレスを構成するには、以下の行でコメント・マーカー (#) を削除して編集します。

   ```
   log4j.appender.S.Host=<IP address> log4j.appender.S.Port=<Port>
   ```

   ここで、各項目は次のとおりです。

   <IP address> は、QRadar の IP アドレスまたはホスト名です。

   <Port> は、UDP または TCP プロトコル用のポート番号です。QRadar やイベント・コレクターに対する Syslog 通信のデフォルト・ポートはポート **514** です。
6. Syslog プロトコルを構成するには、以下の行でコメント・マーカー (#) を削除し、使用するプロトコル (UDP、TCP、または SSL) を入力します。

   ```
   log4j.appender.S.Protocol=TCP
   ```

   QRadar では暗号化プロトコル SSL はサポートされていません。
7. イベントのロギングのための重大度レベルを設定するには、以下の行でコメント・マーカー (#) を削除します。

   ```
   log4j.appender.S.Threshold=INFO
   ```

   デフォルト値 INFO は、イベントの適切な重大度レベルです。
8. イベントのロギングのためのファシリティーを設定するには、以下の行でコメント・マーカー (#) を削除します。

   ```
   log4j.appender.S.Facility=USER
   ```

   デフォルト値の USER は、イベントの適切なファシリティー値です。
9. イベントのロギングのためのファシリティーを設定するには、以下の行でコメント・マーカー (#) を削除します。

   ```
   log4j.appender.R.MaxBackupIndex=10
   ```
10. xdasconfig.properties.template ファイルを保存します。

XDASv2 イベントの Syslog プロパティーの構成が完了したら、XDASv2 モジュールをロードすることができます。

XDASv2 モジュールのロード

Novell iManager でイベントを構成する前に、XDASv2 モジュールに対して行った変更をロードする必要があります。

このタスクについて

XDASv2 モジュールをロードするには、ご使用のオペレーティング・システムを選択します。

- Linux で XDASv2 をロードするには、『Linux オペレーティング・システムでの XDASv2 のロード』を参照してください。
- Windows で XDASv2 をロードするには、『Windows オペレーティング・システムでの XDASv2 のロード』を参照してください。

重要: Novell eDirectory に Novell Module Authentication Service (NMAS) がインストールされており、NMAS 監査が有効な場合、XDASv2 モジュールに対して行った変更内容は自動的にロードされます。NMAS がインストールされている場合、イベント監査を構成する必要があります。イベント監査の構成について詳しくは、822 ページの『Novell iManager を使用したイベント監査の構成』を参照してください。

Linux オペレーティング・システムでの XDASv2 のロード

XDASv2 を Linux オペレーティング・システムにロードできます。

手順

1. Novell eDirectory をホストする Linux サーバーに、root ユーザーとしてログインします。
2. 以下のコマンドを入力します。

```
ndstrace -c "load xdasauditds"
```

次のタスク

これで、Novell eDirectory でイベント監査を構成する準備ができました。詳しくは、822 ページの『Novell iManager を使用したイベント監査の構成』を参照してください。

Windows オペレーティング・システムでの XDASv2 のロード

XDASv2 を Windows オペレーティング・システムにロードできます。

手順

1. Novell eDirectory をホストする Windows サーバーにログインします。
2. デスクトップで、「スタート」>「ファイル名を指定して実行」をクリックします。

「ファイル名を指定して実行」ウィンドウが表示されます。

3. 以下のように入力します。

```
C:¥Novell¥NDS¥ndscons.exe
```

これは、Windows オペレーティング・システムでのデフォルトのインストール・パスです。Novell eDirectory を異なるディレクトリーにインストールした場合は、正しいパスが必要です。

4. 「**OK**」をクリックします。

Novell Directory Service コンソールに、使用可能なモジュールのリストが表示されます。

5. 「サービス **(Services)**」タブで「**xdasauditds**」を選択します。
6. 「開始 **(Start)**」をクリックします。

Novell eDirectory の xdasauditds サービスが開始します。

7. 「スタートアップ **(Startup)**」をクリックします。

「サービス (Service)」ウィンドウが表示されます。

8. 「スタートアップの種類 **(Startup Type)**」パネルで「自動 **(Automatic)**」チェック・ボックスを選択します。
9. 「**OK**」をクリックします。
10. 「Novell eDirectory サービス (Novell eDirectory Services)」ウィンドウを閉じます。

次のタスク

これで、Novell eDirectory でイベント監査を構成する準備ができました。詳しくは、『Novell iManager を使用したイベント監査の構成』を参照してください。

Novell iManager を使用したイベント監査の構成

Novell iManager で XDASv2 のイベント監査を構成できます。

手順

1. Novell iManager コンソール・ユーザー・インターフェースにログインします。
2. ナビゲーション・バーで「ロールとタスク **(Roles and Tasks)**」をクリックします。
3. 左側のナビゲーションで「**eDirectory** 監査 **(eDirectory Auditing)**」 > 「監査の構成 **(Audit Configuration)**」をクリックします。

「監査の構成 (Audit Configuration)」パネルが表示されます。

4. 「**NPC** サーバー名 **(NPC Server name)**」フィールドに、NPC サーバーの名前を入力します。
5. 「**OK**」をクリックします。

「NPC サーバーの監査構成 (Audit Configuration for the NPC Server)」が表示されます。

6. 以下のパラメーターを構成します。
   a. 「コンポーネント **(Components)**」パネルで、以下のいずれかまたは両方を選択します。

      DS - eDirectory オブジェクトの XDASv2 イベントを監査するには、このチェック・ボックスを選択します。

      LDAP - Lightweight Directory Access Protocol (LDAP) オブジェクトの XDASv2 イベントを監査するには、このチェック・ボックスを選択します。
7. 「イベントの大きな値をログに記録する **(Log Event's Large Values)**」パネルで、以下のいずれかを選択します。

   大きな値をログに記録する **(Log Large Values)** - 768 バイトよりも大きなイベントをログに記録するには、このオプションを選択します。

   大きな値をログに記録しない **(Don't Log Large Values)** - 768 バイトよりも小さいイベントをログに記録するには、このオプションを選択します。768 バイトを超える値の場合、イベントは切り捨てられます。
8. 「**XDAS** イベントの構成 **(XDAS Events Configuration)**」で、XDAS がキャプチャーして IBM Security QRadar に転送するイベントのチェック・ボックスを選択します。
9. 「適用」をクリックします。
10. 「**XDAS**」タブで「**XDASRoles**」をクリックします。

    「XDAS ロールの構成 (XDAS Roles Configuration)」パネルが表示されます。
11. 以下のロール・パラメーターを構成します。
    a. イベント収集をサポートする各オブジェクト・クラスのチェック・ボックスを選択します。
12. 「使用可能な属性 **(Available Attribute(s))**」リストで任意の属性を選択し、矢印をクリックします。選択した属性が「選択した属性 **(Selected Attribute(s))**」リストに追加されます。
13. オブジェクト属性を追加したら、「**OK**」をクリックします。
14. 「適用」をクリックします。
15. 「**XDAS**」タブで「**XDASAccounts**」をクリックします。

    「XDAS アカウントの構成 (XDAS Accounts Configuration)」パネルが表示されます。
16. 以下のアカウント・パラメーターを構成します。
    a. 「使用可能なクラス **(Available Classes)**」リストで任意のクラスを選択し、矢印をクリックします。選択したクラスが「選択した属性 **(Selected Attribute(s))**」リストに追加されます。
17. オブジェクト属性を追加したら、「**OK**」をクリックします。

18. 「適用」をクリックします。

次のタスク

これで、QRadar を構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar では Novell eDirectory からの Syslog イベントが自動的に検出されます。この構成手順はオプションです。

手順

「ログ・ソース・タイプ」リストで「Novell eDirectory」を選択します。
Novell eDirectory、Novell iManager、または XDASv2 について詳しくは、ベンダーの資料を参照してください。

第 92 章 ObserveIT JDBC

ObserveIT JDBC 用の IBM Security QRadar DSM は、ObserveIT から JDBC イベントを収集します。

以下の表は、ObserveIT JDBC DSM の仕様を示しています。

表 *304. ObserveIT JDBC DSM* の仕様

仕様	値
製造元	ObserveIT
製品	ObserveIT JDBC
DSM RPM 名	`DSM-ObserveIT-`*`QRadar_Version-Build_Number`*`.noarch.rpm`
サポートされるバージョン	v5.7 以降
プロトコル	ObserveIT JDBC ログ・ファイル・プロトコル
QRadar で記録されるイベント	以下のイベント・タイプが ObserveIT JDBC によってサポートされています。 • アラート • ユーザー・アクティビティー • システム・イベント • セッション・アクティビティー • DBA アクティビティー このログ・ファイル・プロトコルでは、LEEF ログ内でユーザー・アクティビティーがサポートされます。
自動的に検出?	いいえ
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	ObserveIT の Web サイト (http://www.observeit-sys.com)

ObserveIT JDBC イベントを収集するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下の最新バージョンの各 RPM をダウンロードして、QRadar コンソールにインストールします。
   - ObserveIT JDBC DSM RPM
   - DSMCommon DSM RPM
   - ObserveIT JDBC PROTOCOL RPM
   - JDBC PROTOCOL RPM
2. ObserveIT システムがインストールされていて、SQL Server データベースがネットワーク経由でアクセス可能であることを確認してください。

3. 統合対象の ObserveIT サーバーごとに、QRadar コンソールでログ・ソースを作成します。すべての必須パラメーターを構成します。ObserveIT 固有のパラメーターを構成する際には、以下の表を使用してください。

表 *305. ObserveIT JDBC* ログ・ソースのパラメーター

パラメーター	説明
ログ・ソース・タイプ	ObserveIT
プロトコル構成	**DATABASE@HOSTNAME**。ここで、**DATABASE** は「データベース名」フィールドに入力したテキストと一致するストリングで、かつ **@** 記号が含まれていない必要があります。**HOSTNAME** は「**IP**」フィールドまたは「ホスト名」フィールドに入力したテキストと一致するストリングで、かつ **@** 記号が含まれていない必要があります。
データベース名	ObserveIT
IP またはホスト名	ObserveIT システムの IP アドレスまたはホスト名。
ポート	ObserveIT ホスト上のポート。デフォルトは 1433 です。
ユーザー名	ObserveIT MS SQL データベースに接続するために必要なユーザー名。
パスワード	ObserveIT MS SQL データベースに接続するために必要なパスワード。
開始日時	yyyy-MM-dd HH: mm 形式を使用します。
ポーリング間隔 (Polling Interval)	データベースをポーリングする頻度。
EPS スロットル	イベント速度スロットル (イベント/秒)。

表 *306.* ログ・ファイル・プロトコルのパラメーター

パラメーター	説明
プロトコル構成	ログ・ファイル
ログ・ソース ID	ログ・ソースの IP アドレス。この値は、「サーバー **IP**」パラメーターで構成されている値に一致する必要があります。「ログ・ソース **ID**」は、ログ・ソース・タイプに対して固有でなければなりません。

表 306. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
サービス・タイプ	リストから、リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを選択します。デフォルトは SFTP です。 SFTP - SSH ファイル転送プロトコル FTP - ファイル転送プロトコル SCP - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得する基礎のプロトコルでは、「リモート **IP**」または「ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート IP またはホスト名	イベント・ログ・ファイルを保管するデバイスの IP アドレスまたはホスト名。
リモート・ポート	リモート・ホストが非標準のポート番号を使用する場合、イベントを取得するにはポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名。ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ホストにログインするために必要なパスワード。
パスワードの確認	ホストにログインするために必要なパスワードの確認。
SSH 鍵ファイル	SSH 鍵へのパス (鍵認証を使用するようにシステムが構成されている場合)。SSH 鍵ファイルを使用するときは、「リモート・パスワード **(Remote Password)**」フィールドは無視されます。
リモート・ディレクトリー	FTP について、ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合、リモート・ディレクトリーをブランクのままにしておくことができます。ブランクの「リモート・ディレクトリー **(remote directory)**」フィールドにより、作業ディレクトリーの変更 (CWD) コマンドが制限されるシステムがサポートされます。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択した場合は、リモート・ファイルのファイル名を入力する必要があります。
再帰的 (Recursive)	このオプションは、SCP ファイル転送では無視されます。

表 306. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
FTP ファイル・パターン	リモート・ホストからダウンロードするファイルを特定するために必要な正規表現 (regex)。
FTP 転送モード	FTP 経由の ASCII 転送については、「プロセッサー」フィールドに「なし」を、「イベント・ジェネレーター **(Event Generator)**」フィールドに「**LINEBYLINE**」を選択する必要があります。
開始時刻	処理を開始する時刻。例えば、午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、`12:00 AM` と入力します。このパラメーターは、「繰り返し **(Recurrence)**」の値と連携して、リモート・ディレクトリーのファイルをスキャンするタイミングと頻度を設定します。12 時間クロックに基づいて、`HH:MM` *<AM/PM>* の形式で「開始時刻」を入力します。
繰り返し (Recurrence)	リモート・ディレクトリーをスキャンして新しいイベント・ログ・ファイルを検索する頻度を決定する時間間隔。この時間間隔には、時間数 (H)、分数 (M)、または日数 (D) の値を含めることができます。例えば、繰り返しが 2H の場合、2 時間ごとにリモート・ディレクトリーがスキャンされます。
保存時に実行	ログ・ソース構成の保存後すぐにログ・ファイルのインポートを開始します。このチェック・ボックスを選択すると、前にダウンロードして処理したファイルのリストがクリアされます。最初のファイルのインポート後、ログ・ファイル・プロトコルは、管理者によって定義されている開始時刻および繰り返しスケジュールに従います。
EPS スロットル	このプロトコルが超えないようにするイベント/秒 (EPS) の数。
プロセッサー	プロセッサーにより、QRadar はイベント・ファイルのアーカイブを拡張し、イベント用にコンテンツを処理できるようになります。QRadar は、ファイルがダウンロードされた後にのみそれらのファイルを処理します。QRadar は、`zip`、`gzip`、`tar`、または `tar+gzip` の各アーカイブ・フォーマットのファイルを処理できます。

表 306. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
以前に処理したファイルを無視 (Ignore Previously Processed File(s))	ログ・ファイル・プロトコルによって処理されたファイルを追跡および無視します。QRadar は、リモート・ディレクトリー内にあるログ・ファイルを調べて、ログ・ファイル・プロトコルによってファイルが以前に処理されたかどうかを判別します。以前に処理されたファイルが検出されると、ログ・ファイル・プロトコルはそのファイルを処理のためにダウンロードすることはしません。前に処理されなかったすべてのファイルがダウンロードされます。このオプションは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	イベント・ログの処理前にそれらを格納するターゲット・イベント・コレクターのローカル・ディレクトリーを変更します。
ローカル・ディレクトリー (Local Directory)	ターゲット・イベント・コレクターのローカル・ディレクトリー。このディレクトリーは、ログ・ファイル・プロトコルがイベントを取得しようとする前に存在する必要があります。
ファイルのエンコード (File Encoding)	ログ・ファイル内のイベントによって使用される文字エンコード。
フォルダー分離文字 (Folder Separator)	オペレーティング・システムのフォルダーを分離するために使用される文字。ほとんどの構成では、「フォルダー分離文字 **(Folder Separator)**」フィールドのデフォルト値を使用できます。このフィールドは、分離フォルダーの定義に異なる文字を使用するオペレーティング・システム向けです。例えば、メインフレーム・システムでフォルダーを分離するピリオドがあります。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 93 章 Okta

Okta 用の IBM Security QRadar DSM は、Okta REST API を使用してイベントを収集します。

以下の表は、Okta DSM の仕様を示しています。

表 *307. Okta DSM* の仕様

仕様	値
製造元	Okta
DSM 名	Okta
RPM ファイル名	DSM-OktaIdentityManagement-*QRadar_version-build_number*.noarch.rpm
プロトコル	Okta REST API
イベント・フォーマット	JSON
記録されるイベント・タイプ	すべて
自動的に検出?	いいえ
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Okta の Web サイト (https://www.okta.com/)

Okta を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - プロトコル共通
   - Okta REST API プロトコル RPM
   - Okta DSM RPM

   複数の DSM RPM が必要な場合、統合の順序は DSM RPM の依存関係を反映したものでなければなりません。
2. Okta ログ・ソース固有のパラメーター用の以下の表を使用して、必須パラメーターを構成します。

表 *308. Okta DSM* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Okta
プロトコル構成	Okta REST API
IP またはホスト名	oktaprise.okta.com
認証トークン	Okta コンソールによって生成され、すべての API トランザクションで使用する必要がある単一認証トークン。

表 *308. Okta DSM* ログ・ソース・パラメーター *(*続き*)*

パラメーター	値
プロキシーの使用 (Use Proxy)	プロキシーが構成されている場合は、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Okta にアクセスします。 「プロキシー **IP** またはホスト名 **(Proxy IP or Hostname)**」、「プロキシー・ポート」、「プロキシー・ユーザー名」、および「プロキシー・パスワード」の各フィールドを構成します。プロキシーが認証を必要としない場合、「プロキシー・ユーザー名」フィールドと「プロキシー・パスワード」フィールドはブランクのままでかまいません。
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	リストから「はい」を選択すると、QRadar は証明書をダウンロードし、ターゲット・サーバーを信頼して使用し始めます。
繰り返し (Recurrence)	ログ・ソースがいつデータを収集するかを指定できます。フォーマットは、月/時刻/日を表す M/H/D です。デフォルトは、1 M です。
EPS スロットル	1 秒あたりのイベント数の最大限度。

Okta DSM のサンプル・イベント・メッセージを次の表に示します。

表 *309. Okta* デバイスによってサポートされる *Okta* サンプル・メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
コア・ユーザーの認証 ログイン成功	ユーザー・ログイン成功	{"eventId":"teveLnptWDqSfKg 2Gq8oO-eVg146522980aaaa"," sessionId":"101V8yTdKXcQ9a9pj a1uzaaaa","requestId":"V1Wh6 MUxWNbrLROUi3K0jAaaaa", "published":"2016-04-06T16: 16:40.000Z","action":{ "message":"Sign-in successful","categories": ["Sign-in Success"],"object Type":"core.user_auth.login _success","requestUri":"/api /v1/authn"},"actors":[{"id": "00uzysse4pPSPXWNaaaa", "displayName":"User","login": "account@oktaprise.com", "objectType":"User"},{"id": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/ 20100101 Firefox/45.0", "displayName":"FIREFOX", "ipAddress":"1.2.3.4", "objectType":"Client"}], "targets":[{"id":"00uzysse 4pPSPXWNaaaa","displayName": "User","login":"account@ oktaprise.com","objectType": "User"}]}

表 309. *Okta* デバイスによってサポートされる *Okta* サンプル・メッセージ (続き)

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
コア・ユーザーの認証ログイン失敗	ユーザー・ログイン失敗	{"eventId":"tev7UdwtYhTSkGVA_rmMJgeJQ1440004117000","sessionId":"","requestId":"VdS4FTWJxk6c4mX2wB1-@wAAA9I","published":"2015-08-19T17:08:37.000Z","action":{"message":"Sign-in Failed - Not Specified","categories":["Sign-in Failure","Suspicious Activity"],"objectType":"core.user_auth.login_failed","requestUri":"/login/do-login"},"actors":[{"id":"Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko","displayName":"x x","ipAddress":"1.1.1.1","objectType":"Client"}],"targets":[{"id":"","objectType":"User"}]}

関連概念:

29 ページの『Okta REST API プロトコルの構成オプション』
Okta からイベントを受信するには、Okta REST API プロトコルを使用するようにログ・ソースを構成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 94 章 Onapsis Security Platform

Onapsis Security Platform デバイス用の IBM Security QRadar DSM は、Onapsis Security Platform からログを収集します。

以下の表は、Onapsis Security Platform DSM の仕様を示しています。

表 *310. Onapsis Security Platform DSM* の仕様

仕様	値
製造元	Onapsis
DSM 名	Onapsis Security Platform
RPM ファイル名	DSM-OnapsisIncOnapsisSecurityPlatform-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	1.5.8 以降
イベント・フォーマット	ログ・イベント拡張フォーマット (LEEF)
記録されるイベント・タイプ	評価 アタック・シグニチャー 相関 コンプライアンス
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Onapsis Web サイト (https://www.onapsis.com)

Onapsis Security Platform を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Onapsis Security Platform DSM RPM
   - DSM 共通 RPM
2. Syslog イベントを QRadar に送信するように Onapsis Security Platform デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソール で Onapsis Security Platform ログ・ソースを追加してください。以下の表は、Onapsis Security Platform イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *311. Onapsis Security Platform* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Onapsis Security Platform

表 311. *Onapsis Security Platform* ログ・ソース・パラメーター (続き)

パラメーター	値
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に Onapsis Security Platform を構成する

Onapsis Security Platform からイベントを収集するには、コネクターおよびアラーム・プロファイルを追加する必要があります。

このタスクについて

アラーム・プロファイルは、インシデントが監視されているときに、自動的にアクションを実行するように Onapsis Security Platform を構成します。

手順

1. Onapsis Security Platform にログインします。
2. 「**Gear**」アイコンをクリックします。
3. 「設定」をクリックします。
4. 「**Connectors Settings**」から、「**Add**」をクリックして、新規コネクターを含めます。
5. 「**Respond**」 > 「**Alarm Profiles**」をクリックします。
6. 新規アラーム・プロファイルを追加します。
   a. 「**Alarm Type**」および「**Severity**」を選択します。
   b. 名前と説明を入力します。
   c. 「**Assets List**」または「**Tags List**」からターゲットを選択します。 これらのリストは、同時には使用できません。
   d. いつアラームをトリガーするかについて条件を追加します。
   e. アラームがトリガーされたときに実行するアクションを追加するには、「**Action**」をクリックします。
   f. ステップ 4 で作成した QRadar コネクターを選択します。

第 95 章 OpenBSD

IBM Security QRadar 用の OpenBSD DSM は、syslog を使用してイベントを受け取ります。

QRadar は、OpenBSD オペレーティング・システムから転送されるすべての関連情報、認証、およびシステム・レベルのイベントを記録します。

ログ・ソースの構成

IBM Security QRadar に OpenBSD イベントを統合するには、ログ・ソースを手動で作成する必要があります。QRadar では、OpenBSD オペレーティング・システムからの Syslog イベントに対し、ログ・ソースの検出と作成は自動的に実行されません。

このタスクについて

OpenBSD のログ・ソースを作成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**OpenBSD OS**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   Syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 312. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	OpenBSD アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。

12. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

ログ・ソースが QRadar に追加されます。これで、Syslog イベントを転送するように OpenBSD アプライアンスを構成する準備ができました。

OpenBSD 用の Syslogの構成

Syslog イベントを転送するように OpenBSD を構成できます。

手順

1. SSH を使用して、root ユーザーとして OpenBSD デバイスにログインします。
2. /etc/syslog.conf ファイルを開きます。
3. このファイルの先頭に以下の行を追加します。それ以外の行は変更しないでください。

   ```
   *.* @<IP address>
   ```

   ここで *<IP address>* は、IBM Security QRadar の IP アドレスです。
4. ファイルを保存して終了します。
5. ハングアップ・シグナルを syslog デーモンに送信し、すべての変更が適用されるようにします。

   ```
   kill -HUP `cat /var/run/syslog.pid`
   ```

   注: このコマンド・ラインでは逆引用符文字 (`) が使用されています。ほとんどのキーボード・レイアウトでは、逆引用符文字は数字 1 の左側にあります。

   構成は完了です。OpenBSD により QRadar に転送されるイベントは、「ログ・アクティビティー」タブに表示されます。

第 96 章 Open LDAP

IBM Security QRadar 用の Open LDAP DSM は、ロギング・レベル 256 を使用して統計イベントをログに記録するように構成された Open LDAP インストール済み環境からの UDP Multiline Syslog イベントを受け入れます。

Open LDAP イベントはポート 514 を使用して QRadar に転送されますが、UDP Multiline プロトコルで構成されたポートにリダイレクトされなければなりません。iptable を使用するこのリダイレクトが必要になるのは、標準の listen ポートでの UDP Multiline Syslog が QRadar でサポートされていないためです。

注: UDP Multiline Syslog イベントは、ポート 514 以外の任意のポートに割り当てることができます。UDP Multiline プロトコルに割り当てられているデフォルト・ポートは、UDP ポート 517 です。ネットワークでポート 517 を使用している場合は、「*IBM Security QRadar Common Ports Technical Note*」を参照してください。QRadar で使用されるポートのリストが記載されています。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

ログ・ソースの構成

IBM Security QRadar は、UDP 多重回線フォーマットで転送される Open LDAP イベントを自動的に検出しません。統合を完了するには、QRadar の「管理」タブを使用して UDP 多重回線 Syslog プロトコルのログ・ソースを手動で作成する必要があります。ログ・ソースを作成することで、QRadar が着信 Open LDAP 多重回線イベントに対して listen ポートを確立できます。

このタスクについて

QRadar で Open LDAP ログ・ソースを構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。

5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Open LDAP** ソフトウェア **(Open LDAP Software)**」を選択します。
9. 「プロトコル構成」リストで「**UDP** 多重回線 **Syslog (UDP Multiline Syslog)**」を選択します。
10. 以下の値を構成します。

表 *313. UDP* 多重回線プロトコルの構成

パラメーター	説明
ログ・ソース **ID**	Open LDAP サーバーからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。
Listen ポート	着信 UDP 多重回線 Syslog イベントを受け取るために QRadar が使用するポート番号を入力します。有効な範囲は 1 から 65536 です。 デフォルトの UDP 多重回線 Syslog listen ポートは 517 です。 「**Listen** ポート **(Listen Port)**」フィールドが表示されない場合は、QRadar で Tomcat を再始動する必要があります。 「**listen** ポート **(Listen Port)**」の番号を編集するには、以下のようにします。 QRadar コンソールまたはイベント・コレクター (Event Collector) で、IPtables を新しい UDP 多重回線 Syslog ポート番号で更新します。詳しくは、 841 ページの『多重回線 UDP Syslog イベント用の IPtables の構成』を参照してください。 「**listen** ポート **(Listen Port)**」フィールドに、UDP 多重回線 Syslog イベント受信用の新しいポート番号を入力します。 「保存」をクリックします。 「管理」タブで、「拡張」 > 「すべての構成のデプロイ」を選択します。 「すべての構成のデプロイ」をクリックすると、QRadar はすべてのサービスを再開します。このため、デプロイが完了するまで、イベントとフローのデータ収集にギャップが生じます。

表 313. UDP 多重回線プロトコルの構成 (続き)

パラメーター	説明
メッセージ **ID** のパターン	イベント・ペイロード・メッセージをフィルタリングするために必要な正規表現 (regex) を入力します。Open LDAP イベントの処理時に、一致するすべてのイベントが含まれます。 Open LDAP イベント向けに推奨される正規表現は以下のとおりです。 `conn=(¥d+)` 例えば Open LDAP では、接続メッセージは *conn* という単語で始まり、残りのイベント・ペイロードがその後に続きます。このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

Open LDAP イベントのログ・ソースが作成されました。これで、QRadar が Open LDAP イベントを QRadar コンソールまたはイベント・コレクター (Event Collector)の適切な UDP 多重回線 Syslog ポートにリダイレクトするように IPtables を構成する準備ができました。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

多重回線 UDP Syslog イベント用の IPtables の構成

Open LDAP では、Open LDAP サーバーのポート 514 から UDP 多重回線プロトコル用の別の IBM Security QRadar ポートにイベントをリダイレクトする必要があります。QRadar コンソール、または Open LDAP サーバーから多重回線 UDP Syslog イベントを受信する各 QRadar イベント・コレクター で、IPtables を構成する必要があります。

このタスクについて

多重回線 UDP Syslog イベントをリダイレクトするように QRadar を構成するには、以下のようにします。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。

   ログイン: *<root>*

   パスワード: *<password>*

2. 以下のコマンドを入力して、IPtables ファイルを編集します。

   ```
   vi /opt/qradar/conf/iptables-nat.post
   ```

   IPtables NAT 構成ファイルが表示されます。

3. 以下のコマンドを入力して、QRadar に対し、UDP ポート 514 から UDP ポート 517 に Syslog イベントをリダイレクトするように指示します。

   ```
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port
   <new-port> -s <IP address>
   ```

   各部分について以下で説明します。

   <*IP address*> は、Open LDAP サーバーの IP アドレスです。

   <*New port*> は、Open LDAP 用に UDP 多重回線プロトコルで構成されているポート番号です。

   QRadar コンソールまたはイベント・コレクター (Event Collector)にイベントを送信する Open LDAP IP アドレスごとに、リダイレクトを組み込む必要があります。例えば、Event Collect と通信する Open LDAP サーバーが 3 つある場合は、以下のコードを入力します。

   ```
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517
   -s 10.10.10.10 -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517
   -s 10.10.10.11 -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517
   -s 10.10.10.12
   ```

4. IPtables NAT 構成を保存します。

   これで、Open LDAP サーバーからのイベントを受け取るように QRadar コンソールまたはイベント・コレクター (Event Collector)で IPtables を構成することができます。

5. 以下のコマンドを入力して、IPtables ファイルを編集します。

   ```
   vi /opt/qradar/conf/iptables.post
   ```

   IPtables 構成ファイルが表示されます。

6. 以下のコマンドを入力して、QRadar に対し、Open LDAP サーバーからの通信を許可するように指示します。

   ```
   -I QChain 1 -m udp -p udp --src <IP address> --dport <New port> -j
   ACCEPT
   ```

   各部分について以下で説明します。

   <*IP address*> は、Open LDAP サーバーの IP アドレスです。

   <*New port*> は、Open LDAP 用に UDP 多重回線プロトコルで構成されているポート番号です。

   QRadar コンソールまたはイベント・コレクター (Event Collector)にイベントを送信する Open LDAP IP アドレスごとに、リダイレクトを組み込む必要があります。例えば、Event Collect と通信する Open LDAP サーバーが 3 つある場合は、以下のコードを入力します。

```
-I QChain 1 -m udp -p udp --src 10.10.10.10 --dport 517
-j ACCEPT -I QChain 1 -m udp -p udp --src 10.10.10.11 --dport 517
-j ACCEPT -I QChain 1 -m udp -p udp --src 10.10.10.12 --dport 517
-j ACCEPT
```

7. 以下のコマンドを入力して、QRadar で IPtables を更新します。

   ```
   ./opt/qradar/bin/iptables_update.pl
   ```

例

Open LDAP サーバーから Syslog イベントを受信する別の QRadar コンソールまたはイベント・コレクター (Event Collector)を構成する必要がある場合は、上記の手順を繰り返します。

次のタスク

これで、QRadar へイベントを転送するように Open LDAP サーバーを構成できるようになりました。

Open LDAP のイベント転送の設定

Open LDAP での syslog 転送を構成できます。

手順

1. Open LDAP サーバーのコマンド・ライン・インターフェースにログインします。
2. 以下のファイルを編集します。

   ```
   /etc/syslog.conf
   ```

3. Syslog 構成ファイルに以下の情報を追加します。

   ```
   <facility>@<IP address>
   ```

   各部分について以下で説明します。

   <facility> は Syslog ファシリティーです (例: local4)。

   <IP address> は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。

   例:

   ```
   #Logging for SLAPD local4.debug /var/log/messages local4.debug @10.10.10.1
   ```

   注: Open LDAP サーバーで `/var/log/messages` 以外のディレクトリーにイベント・メッセージを保存している場合は、ディレクトリー・パスを編集する必要があります。

4. Syslog 構成ファイルを保存します。
5. 以下のコマンドを入力して syslog サービスを再始動します。

   ```
   /etc/init.d/syslog restart
   ```

Open LDAP の構成は完了です。QRadar に転送される UDP Multiline イベントは、「ログ・アクティビティー」タブに表示されます。

第 97 章 オープン・ソース SNORT

IBM Security QRadar 用のオープン・ソース SNORT DSM は、syslog を使用して、関連するすべての SNORT イベントを記録します。

登録済み SNORT ユーザーに対する SourceFire VRT 認証済みルールがサポートされています。Bleeding Edge や Emerging Threat のルール・セットをはじめとするベンダー・ルール・セットは、オープン・ソース SNORT DSM によって完全にサポートされていない場合があります。

オープン・ソース SNORT の構成

オープン・ソース SNORT デバイスで syslog を構成するには、以下を実行します。

このタスクについて

以下の手順は、Red Hat Enterprise を実行するシステムに該当します。他のオペレーティング・システムでは、手順が異なる場合があります。

手順

1. リモート・システムで SNORT を構成します。
2. snort.conf ファイルを開きます。
3. 以下の行のコメントを外します。

   ```
   output alert_syslog:LOG_AUTH LOG_INFO
   ```
4. ファイルを保存して終了します。
5. 以下のファイルを開きます。

   ```
   /etc/init.d/snortd
   ```
6. 例に示すように、以下の行に -s を追加します。

   ```
   daemon /usr/sbin/snort $ALERTMODE
   $BINARY_LOG $NO PACKET_LOG $DUMP_APP -D
   $PRINT_INTERFACE -i $i -s -u $USER -g
   $GROUP $CONF -i $LOGIR/$i $PASS_FIRST

   daemon /usr/sbin/snort $ALERTMODE
   $BINARY_LOG $NO_PACKET_LOG $DUMP_APP -D
   $PRINT_INTERFACE $INTERFACE -s -u $USER -g
   $GROUP $CONF -i $LOGDIR
   ```
7. ファイルを保存して終了します。
8. 以下のコマンドを入力して、SNORT を再始動します。

   ```
   /etc/init.d/snortd restart
   ```
9. syslog.conf ファイルを開きます。
10. 以下のコードが反映されるようにファイルを更新します。

    ```
    auth.info@<IP Address>
    ```

ここで、*<IP Address>* は、ログの送信先とするシステムです。

11. ファイルを保存して終了します。
12. syslog を再始動します。

```
/etc/init.d/syslog restart
```

次のタスク

これで、QRadar でログ・ソースを構成できるようになりました。

ログ・ソースの構成

IBM Security QRadar は、オープン・ソース SNORT の syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

QRadar でログ・ソースを作成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストから、「**Open Source IDS**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 314. Syslog パラメーター

パラメーター	説明
ログ・ソース **ID**	オープン・ソース SNORT イベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

SNORT について詳しくは、SNORT の資料 (http://www.snort.org/docs/) を参照してください。

第 98 章 OpenStack

IBM Security QRadar DSM for OpenStack は、OpenStack デバイスからイベント・ログを収集します。

以下の表は、OpenStack DSM の仕様を示しています。

表 *315. OpenStack DSM* の仕様

仕様	値
製造元	OpenStack
DSM 名	OpenStack
RPM ファイル名	`DSM-OpenStackCeilometer-Qradar_version-build_number.noarch.rpm`
サポートされるバージョン	v 2015.1
プロトコル	HTTP レシーバー
記録されるイベント・タイプ	監査イベント
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	OpenStack Web サイト (http://www.openstack.org/)

OpenStack から QRadar にイベントを送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - PROTOCOL-HTTPReceiver RPM
   - OpenStack DSM RPM
2. QRadar コンソールで OpenStack ログ・ソースを追加します。以下の表に、OpenStack イベントを収集するために必要なパラメーターを示します。

表 *316. OpenStack* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	**OpenStack**
プロトコル構成	**HTTPReceiver**
通信タイプ	**HTTP**
Listen ポート	OpenStack が QRadar と通信するために使用するポート番号。 **重要:** 標準以外のポートを使用してください。このポートは OpenStack デバイスの構成に必要になるため、メモしておいてください。
メッセージ・パターン	`^¥{"typeURI`

3. QRadar と通信するように OpenStack デバイスを構成します。

OpenStack DSM のサンプル・イベント・メッセージを次の表に示します。

表 317. *OpenStack* デバイスによってサポートされる *OpenStack* サンプル・メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
すべてのサーバーの詳細をリスト	読み取りアクティビティーが試行されました	{"typeURI": "http://schemas .dmtf.org/cloud/audit/1.0/event", "eventTime": "2014-12-09T00:18:52. 063878+0000", "target": {"typeURI": "service/compute/servers/detail", "id": "openstack:4b2eb8813bc243038 cbbb307b7daaaaa", "name": "nova", "addresses": [{"url": "http://1.2. 3.4:8774/v2/c99506ed278e49f49080ff 1a8a5aaaaa", "name": "admin"}, {"url": "http://1.2.3.4:8774/v2/ c99506ed278e49f49080ff1a8a5aaaaa", "name": "private"}, {"url": "http: //1.2.3.4:8774/v2/c99506ed278e49f 49080ff1a8a5aaaaa", "name": "public"}]}, "observer": {"id": "target"}, "tags": ["correlation_ id?value=openstack:d0837d49-688d- 4fe0-a166-f362d09caaaa"], "eventType": "activity", "initiator": {"typeURI": "service/security/account/user", "name": "admin", "credential": {"token": "74c0 xxxxxxxx aaaa", "identity_status": "Confirmed"}, "host": {"agent": "python- novaclient", "address": "1.2.3.4"}, "project_id": "openstack:c99506ed 278e49f49080ff1a8a5aaaaa", "id": "openstack:460d1061b1ad4e3cb492 e22e5daaaaa"}, "action": "read/list", "outcome": "pending", "id": "openstack:0400ce73-2058-4bcd- bd1b-cbbba9faaaaa",

関連タスク:

『QRadar と通信するように OpenStack を構成』
OpenStack イベントを収集するには、QRadar からの接続を許可するように OpenStack デバイスを構成する必要があります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

QRadar と通信するように OpenStack を構成

OpenStack イベントを収集するには、QRadar からの接続を許可するように OpenStack デバイスを構成する必要があります。

重要: OpenStack は、各種のディストリビューションを備えたオープン・ソースの製品で、各種のオペレーティング・システムでセットアップできます。この手順は、ご使用の環境では異なる場合があります。

手順

1. OpenStack デバイスにログインします。
2. /etc/nova/api-paste.ini ファイルを編集します。
3. ファイルの最後に、以下のテキストを追加します。

```
[filter:audit]
paste.filter_factory = pycadf.middleware.audit:AuditMiddleware.factory
audit_map_file = /etc/nova/api_audit_map.conf
```

4. [composite:openstack_compute_api_v2] 設定を確認し、値が以下のサンプルと一致しているか検査します。

```
[composite:openstack_compute_api_v2]
use = call:nova.api.auth:pipeline_factory
noauth = faultwrap sizelimit noauth ratelimit osapi_compute_app_v2
keystone = faultwrap sizelimit authtoken keystonecontext ratelimit audit osapi_compute_app_v2
keystone_nolimit = faultwrap sizelimit authtoken keystonecontext audit osapi_compute_app_v2
```

5. api_audit_map.conf ファイルを /etc/nova/ ディレクトリーにコピーします。
6. API サービスを再始動します。

   API サービスを再始動するコマンドは、OpenStack ノードをホストしているオペレーティング・システムによって異なります。Redhat Enterprise Linux システムでは、このコマンドは service openstack-nova-api restart です。
7. OpenStack インストール・ディレクトリーの egg-info サブディレクトリーで entry_points.txt ファイルを開きます。

   PackStack インストールでは、このファイル・パスは次のようになります: /usr/lib/python2.7/site-packages/ceilometer-2014.2-py2.7.egg-info/entry_points.txt.
8. http ディスパッチャーを [ceilometer.dispatcher] セクションに追加します。

```
[ceilometer.dispatcher]
file = ceilometer.dispatcher.file:FileDispatcher
database = ceilometer.dispatcher.database:DatabaseDispatcher
http = ceilometer.dispatcher.http:HttpDispatcher
```

9. 提供されている http.py スクリプトを、Ceilometer インストール・ディレクトリーの dispatcher サブディレクトリーにコピーします。

   正確な場所は、ご使用のオペレーティング・システムおよび OpenStack ディストリビューションによって異なります。OpenStack の Redhat Enterprise Linux ディストリビューションでは、このディレクトリーは /usr/lib/python2.7/site-packages/ceilometer/dispatcher/ です。
10. /etc/ceilometer/ceilometer.conf ファイルを編集します。
11. [default] セクションの下に dispatcher=http を追加します。
12. ファイルの下部に、次のセクションを追加します。

```
[dispatcher_http]
target = http://<QRadar-IP>:<QRadar-Port>
cadf_only = True
```

    QRadar システムでログ・ソースを作成したときに OpenStack に対して構成したポートを使用します。
13. ceilometer コレクター・サービスと notification サービスを再始動します。

ceilometer コレクター・サービスと notification サービスを再始動するコマンドは、OpenStack デバイスをホストしているオペレーティング・システムによって異なります。Redhat Enterprise Linux オペレーティング・システムを使用するデバイスでは、以下のコマンドを使用します。

```
service openstack-ceilometer-collector restart
service openstack-ceilometer-notification restart
```

第 99 章 Oracle

IBM Security QRadar は複数の Oracle DSM をサポートしています。

Oracle Acme Packet Session Border Controller

IBM Security QRadar を使用して、ネットワーク内の Oracle Acme Packet Session Border Controller (SBC) インストール済み環境からのイベントを収集できます。

Oracle Acme Packet SBC インストール済み環境では、syslog および SNMP トラップからのイベントが生成されます。SNMP トラップ・イベントは syslog に変換され、すべてのイベントが syslog を使用して QRadar に転送されます。QRadar は、Oracle Communications SBC から転送された syslog イベントを自動的には検出しません。QRadar では、Oracle Acme Packet SBC V6.2 以降からの syslog イベントがサポートされています。

Oracle Acme Packet SBC イベントを収集するには、以下のタスクを実行する必要があります。

1. QRadar システムで、Oracle Acme Packet Session Border Controller DSM を使用してログ・ソースを構成します。
2. Oracle Acme Packet SBC インストール済み環境で、SNMP を有効にし、syslog イベントの宛先 IP アドレスを構成します。
3. Oracle Acme Packet SBC インストール済み環境で、media-manager オブジェクトに対する syslog 設定を有効にします。
4. Oracle Acme Packet SBC インストール済み環境を再始動します。
5. オプション。Oracle Acme Packet SBC インストール済み環境と、 QRadar コンソールまたは syslog イベントを収集する管理対象ホストとの間の syslog 通信がファイアウォール・ルールによってブロックされないことを確認します。

IBM Security QRadar でログに記録される、サポートされる Oracle Acme Packet イベント・タイプ

QRadar 用の Oracle Acme Packet SBC DSM は、イベント・カテゴリーが許可イベントおよびシステム・モニター・イベントの syslog イベントを収集できます。

各イベント・カテゴリーには、そのイベント・カテゴリー内で実行されたアクションを記述する下位イベントが含まれる場合があります。例えば、許可イベントには、下位カテゴリー `login success` または `login failed` が存在する場合があります。

Oracle Acme Packet SBC ログ・ソースの構成

Oracle Acme Packet SBC から Syslog イベントを収集するには、IBM Security QRadar でログ・ソースを構成する必要があります。QRadar では、Oracle Acme Packet SBC Syslog イベントは自動的に検出されません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. オプション: 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Oracle Acme Packet SBC**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *318. Syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Oracle Acme Packet SBC インストール済み環境からのイベントの ID として、IP アドレスまたはホスト名を入力します。 ログ・ソース ID は、固有値でなければなりません。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
信頼性	ログ・ソースの「信頼性」を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	ログ・ソースのターゲットとして使用する「イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	リストから、ログの解析と保管を行うための受信ペイロード・エンコーダーを選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

次のタスク

これで、Oracle Acme Packet SBC インストール済み環境を構成できるようになりました。

Oracle Acme Packet SBC での SNMP から Syslog への変換の構成

IBM Security QRadar と互換性のあるフォーマットのイベントを収集するには、SNMP から Syslog への変換を有効にし、Syslog 宛先を構成する必要があります。

手順

1. SSH を使用して、管理者として Oracle Acme Packet SBC インストール済み環境のコマンド・ライン・インターフェースにログインします。
2. 以下のコマンドを入力して、構成モードを開始します。

   ```
   config t
   ```
3. 以下のコマンドを入力して、システム構成を開始します。

   ```
   (configure)# system (system)# (system)# system-config (system-config)#
   sel
   ```

   システム構成オブジェクトの単一インスタンスを選択するため、**sel** コマンドが使用されています。
4. 以下のコマンドを入力して、QRadar システムを Syslog 宛先として構成します。

   ```
   (system-config)# syslog-servers (syslog-config)# address <QRadar IP
   address> (syslog-config)# done
   ```
5. 以下のコマンドを入力して、SNMP トラップと SNMP トラップ通知の Syslog 変換を有効にします。

   ```
   (system-config)# enable-snmp-auth-traps enabled (system-config)
   # enable-snmp-syslog-notify enabled (system-config)
   # enable-snmp-monitor-traps enabled (system-config)
   # ids-syslog-facility 4 (system-config)# done
   ```
6. 以下のコマンドを入力して、構成モードに戻ります。

   ```
   (system-config)# exit (system)# exit (configure)#
   ```

media manager オブジェクトでの Syslog 設定の有効化

media-manager オブジェクトの構成により、侵入検知システム (IDS) が IP アドレスに対するアクションを完了した時点での Syslog 通知を有効にできます。イベントに対して使用可能なアクションは、ご使用のファームウェア・バージョンによって異なります。

手順

1. 以下のコマンドを入力して、Oracle Acme Packet SBC インストール済み環境のファームウェア・バージョンをリストします。

   ```
   (configure)# show ver

   ACME Net-Net OSVM Firmware SCZ 6.3.9 MR-2 Patch 2 (Build 465) Build
   Date=03/12/13
   ```

   ファームウェアのメジャー・バージョン番号とマイナー・バージョン番号を示す下線付きテキストが表示されます。
2. 以下のコマンドを入力して、media-manager オブジェクトを構成します。

   ```
   (configure)# media-manager (media-manager)# (media-manager)#
   media-manager (media-manager)# sel (media-manager-config)#
   ```

   media-manager オブジェクトの単一のインスタンスを選択するため、**sel** コマンドが使用されています。
3. 以下のコマンドを入力して、侵入検知システム (IDS) により IP が拒否キューに降格された時点での Syslog メッセージを有効にします。

   ```
   (media-manager-config)# syslog-on-demote-to-deny enabled
   ```
4. ファームウェア・バージョン C6.3.0 以降では、以下のコマンドを入力して、セッションが拒否された時点での Syslog メッセージを有効にします。

   ```
   (media-manager-config)# syslog-on-call-reject enabled
   ```
5. ファームウェア・バージョン C6.4.0 以降では、以下のコマンドを入力して、IP が信頼されないキューに降格された時点での Syslog メッセージを有効にします。

   ```
   (media-manager-config)# syslog-on-demote-to-untrusted enabled
   ```
6. 以下のコマンドを入力して、構成モードに戻ります。

   ```
   (media-manager-config)# done (media-manager-config)# exit
   (media-manager)# exit (configure)# exit
   ```
7. 以下のコマンドを入力して、構成を保存してアクティブにします。

   ```
   # save Save complete # activate
   ```
8. reboot と入力して、Oracle Acme Packet SBC インストール済み環境を再始動します。

   システム再始動後に、イベントが IBM Security QRadar に転送され、「ログ・アクティビティー」タブに表示されます。

Oracle Audit Records

Oracle データベースは、ユーザーのログイン/ログアウト、許可の変更、表の作成と削除、およびデータベース挿入などの監査イベントを追跡できます。

IBM Security QRadar は、Oracle Audit DSM を使用することにより、相関とレポートの目的でこれらのイベントを収集できます。詳しくは、Oracle の資料を参照してください。

注: Oracle の監査ログには、2 つのモードがあります。QRadar では、ファイングレイン監査はサポートされません。

始める前に

syslog を使用する場合、Oracle RDBMS は Linux でのみサポートされます。JDBC を使用してデータベース監査表を参照する場合、Microsoft Windows ホストおよび Linux がサポートされます。Microsoft Windows ホストを使用する場合は、データベース監査表が使用可能になっていることを確認してください。これらの手順は単なるガイドラインと見なしてください。本資料の手順を実行する前に Oracle DBA の経験があることが推奨されます。詳しくは、ベンダーの資料を参照してください。

QRadar で Oracle RDBMS インスタンスからの Oracle Audit イベントを収集できるようにするには、その前に、そのインスタンスが監査レコードを syslog またはデータベース監査表に書き込むように構成されている必要があります。監査の構成方法についての詳しい説明については、ベンダーの資料を参照してください。

注: Oracle の一部のバージョンでは、syslog を使用して監査イベントを送信できません。Oracle v9i および 10g リリース 1 では、監査イベントをデータベースへのみ送信できます。Oracle v10g リリース 2 および Oracle v11g では、データベースまたは syslog に監査イベントを書き込むことができます。v10g リリース 1 または v9i を使用している場合は、JDBC ベースのイベントを使用する必要があります。Oracle v10g リリース 2 を使用している場合は、syslog または JDBC ベースのイベントを使用できます。

Oracle Audit デバイスが監査ログを QRadar に書き込むように構成するには、『Oracle 監査ログの構成』を参照してください。サイズの大きな Oracle 監査表 (1 GB を超える) がシステムにある場合は、 859 ページの『大規模な監査テーブルでのパフォーマンスの向上』を参照してください。

Oracle 監査ログの構成

監査ログを書き込むようにデバイスを構成できます。

手順

1. Oracle ホストに Oracle ユーザーとしてログインします (このユーザーは、Oracle のインストールに使用したユーザー (例: oracle) です。)
2. 環境変数 *ORACLE_HOME* と *ORACLE_SID* が、ご使用のデプロイメントに対応して適切に構成されていることを確認します。
3. 以下のファイルを開きます。

   ```
   ${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora
   ```

4. 次のオプションのいずれかを選択してください。
   a. データベース監査証跡の場合、以下のコマンドを入力します。

```
*.audit_trail='DB'
```

b. Syslog の場合、以下のコマンドを入力します。

```
*.audit_trail='os'

*.audit_syslog_level='local0.info'
```

Oracle ホストの Syslog デーモンが、監査ログを QRadar に転送するように構成されていることを確認する必要があります。Red Hat Enterprise を実行するシステムでは、/etc/syslog.conf ファイルの以下の行が転送に影響します。

```
local0.info @qradar.domain.tld
```

ここで *qradar.domain.tld* は、イベントを受信する QRadar のホスト名です。 (上記の) コマンドを認識させるには、Syslog 構成を再ロードする必要があります。Red Hat Enterprise を実行するシステムで、Syslog 構成を再ロードする以下の行を入力します。

```
kill -HUP /var/run/syslogd.pid
```

5. ファイルを保存して終了します。
6. データベースを再始動するために、SQLplus に接続して sysdba としてログインします。:

例:

```
Enter user-name: sys as sysdba
```

7. データベースをシャットダウンします。

```
shutdown immediate
```

8. データベースを再始動します。

```
startup
```

9. Oracle v9i または Oracle v10g リリース 1 を使用している場合は、SQLplus を使用してビューを作成し、QRadar 統合を有効にする必要があります。Oracle 10g リリース 2 以降を使用している場合は、このステップを省略できます。

```
CREATE VIEW qradar_audit_view
AS SELECT CAST(dba_audit_trail.timestamp AS TIMESTAMP)
AS qradar_time, dba_audit_trail.* FROM dba_audit_trail;
```

JDBC プロトコルを使用する場合、QRadar 内で JDBC プロトコルを構成する際に、以下の固有のパラメーターを使用します。

表 *319.* ログ・ソース・パラメーターの構成

パラメーター名	**Oracle v9i** または **10g** リリース **1** での値	**Oracle v10g** リリース **2** および **v11g** での値
テーブル名	QRadar_audit_view	dba_audit_trail
選択リスト	*	*
比較フィールド	QRadar_time	extended_timestamp

表 319. ログ・ソース・パラメーターの構成 (続き)

パラメーター名	**Oracle v9i** または **10g** リリース **1** での値	**Oracle v10g** リリース **2** および **v11g** での値
データベース名	サポートされているすべてのバージョンの Oracle では、「データベース名」は、Oracle *listener* が使用するサービス名でなければなりません。使用可能なサービス名を表示するには、Oracle ホストで **lsnrctl status** コマンドを実行します。	

注**:** QRadar が監査ログ・テーブルのイベントを照会するときに使用するデータベース・ユーザーに、Table Name オブジェクトに対する適切なアクセス権があることを確認してください。

10. Oracle データベースからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Oracle RDBMS** 監査レコード **(Oracle RDBMS Audit Record)**」オプションを選択します。

関連概念:

17 ページの『JDBC プロトコルの構成オプション』
QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

大規模な監査テーブルでのパフォーマンスの向上

Oracle 監査テーブルのサイズは、IBM Security QRadar が DBA_AUDIT_TRAIL ビューの処理に必要とする時間に影響します。

このタスクについて

sys.sud$ テーブルが大きい (約 1 GB 以上) 場合、処理時間を延長する必要があります。 QRadar が大きな sys.sud$ テーブルを迅速に処理できるようにするには、索引と新しいビューを作成する必要があります。

SQL_BIND フィールドおよび SQL_TEXT フィールドの最大文字数は 2000 です。

注**:** 監査が大規模であるか、データベース・サーバーがアクティブな場合、以下の手順を実行するにはデータベースをシャットダウンする必要があることがあります。

索引または新しいビューを作成するには、以下のようにします。

手順

1. 以下の Web サイトに移動してファイルをダウンロードします。

   http://www.ibm.com/support
2. 「ソフトウェア **(Software)**」タブで「スクリプト **(Scripts)**」を選択します。
3. ご使用の Oracle のバージョンに対応した適切なファイルをダウンロードします。

a. Oracle 9i または 10g リリース 1 を使用している場合は、以下のファイルをダウンロードします。

```
oracle_9i_dba_audit_view.sql
```

b. Oracle v10g リリース 2 および v11g を使用している場合は、以下のファイルをダウンロードします。

```
oracle_alt_dba_audit_view.sql
```

4. ダウンロードしたファイルをローカル・ディレクトリーにコピーします。
5. 859 ページの『大規模な監査テーブルでのパフォーマンスの向上』でファイルをコピーしたディレクトリーに移動します。
6. SQLPlus に sysdba としてログインします。

```
sqlplus / as sysdba
```

7. SQL プロンプトで、ご使用の Oracle Audit のバージョンに応じて以下のいずれかのコマンドを入力します。

索引を作成する場合、ファイルが既に使用中である可能性があります。この場合は排他的アクセスを取得する必要があります。

a. Oracle 9i または 10g リリース 1 を使用している場合は、以下のコマンドを入力します。

```
@oracle_9i_dba_audit_view.sql
```

b. Oracle v10g リリース 2 および v11g を使用している場合は、以下のコマンドを入力します。

```
@oracle_alt_dba_audit_view.sql
```

8. QRadar で構成されているデータベース・ユーザーに、このビューに対する SELECT 権限が付与されていることを確認します。

例えばユーザーが USER1 の場合は以下のようにします。

```
grant select on sys.alt_dba_audit_view to USER1;
```

9. SQLPlus からログアウトします。
10. QRadar にログインします。
11. この項目の JDBC プロトコル構成を更新し、次の項目を追加します。
    - テーブル名 **(Table Name)** - テーブル名を `DBA_AUDIT_TRAIL` から `sys.alt_dba_audit_view` に更新します。
    - 比較フィールド **(Compare Field)** - このフィールドを `entended_timestamp` から `ntimestamp` に更新します。
12. 「保存」をクリックします。

関連概念:

17 ページの『JDBC プロトコルの構成オプション』

QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

Oracle Audit Vault

IBM Security QRadar 用の Oracle Audit Vault DSM は、Java Database Connectivity (JDBC) を使用して JDBC プロトコルに対するアラートにアクセスすることにより、Oracle v10.2.3.2 以降のイベントを受け入れます。

QRadar は、ソース・データベースからの Oracle Audit Vault アラートを記録し、Oracle 監査ポリシー設定により構成されたイベントをキャプチャーします。イベントが発生すると、avsys.av$alert_store 表にアラートが保管されます。AV_AUDITOR 許可を持つユーザーによって、カスタマイズされたイベントが Oracle Audit Vault 内で作成されます。

Oracle Audit Vault での Oracle 監査ポリシー設定の構成については、ベンダーの資料を参照してください。

Oracle Audit Vault では、アラート名は QRadar ID (QID) マップされません。QRadar の「イベント」インターフェースの「イベントのマップ」機能を使用すると、正規化されたイベントまたはロー・イベントを上位または下位のカテゴリー (QID) に手動でマップできます。Oracle Audit Vault DSM を使用すると、上位または下位のカテゴリーのアラートをペイロードのアラート名 (**ALERT_NAME** フィールド) に直接マップすることにより、カテゴリー・マッピングを実行できます。「イベント」インターフェースについて詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

ログ・ソースの構成

JDBC プロトコルを使用して Oracle Audit Vault データベースにアクセスするように QRadar ログ・ソースを構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストを使用して、「**Oracle Audit Vault**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. 以下の値を構成します。
   a. データベース・タイプ **(Database Type)**: Oracle
   b. データベース名: <*Audit Vault* データベース名>
   c. テーブル名 **(Table Name)**: avsys.av$alert_store
   d. 選択リスト **(Select List)**: *
   e. 比較フィールド **(Compare Field)**: ALERT_SEQUENCE

f. **IP** またはホスト名 **(IP or Hostname)**: <*Oracle Audit Vault Server* の場所>

g. ポート: <デフォルト・ポート>

h. ユーザー名: <*AV_AUDITOR* ロールを持つデータベース・アクセス・ユーザー名>

i. パスワード: <パスワード>

j. ポーリング間隔 **(Polling Interval)**: <デフォルトの間隔>

JDBC プロトコル構成を保存する前に、AV_AUDITOR パスワードを正しく入力していることを確認してください。ログイン試行が繰り返し失敗したことが原因で、Oracle Audit Vault がユーザー・アカウントをロックすることがあります。

AV_AUDITOR アカウントがロックされると、`avsys.av$alert_store` のデータにアクセスできなくなります。このユーザー・アカウントのロックを解除するには、プロトコル構成でパスワード項目を修正する必要があります。次に、Oracle `sqlplus` プロンプトで *avadmindva* ユーザーとして Oracle Audit Vault にログインし、alter user <*AV_AUDITOR USER*> account unlock コマンドを実行します。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

古いバージョンの JDBC プロトコルでは、QRadar に対し、ローカル・タイム・ゾーン変換に依存する Oracle タイム・スタンプがサポートされていません。このため、JDBC プロトコルが更新されるまでは、ペイロードの **AV_ALERT_TIME**、**ACTUAL_ALERT_TIME**、および **TIME_CLEARED** フィールドには、オブジェクト ID のみが表示されます。

Oracle BEA WebLogic

Oracle BEA WebLogic DSM により、IBM Security QRadar はアーカイブされているサーバー・ログと監査ログをリモート・ホスト (Oracle BEA WebLogic サーバーなど) から取得できます。

このタスクについて

QRadar はログ・ファイル・プロトコルを使用して Oracle BEA WebLogic サーバーからイベントを取得し、ドメインまたは単一サーバーで発生したアプリケーション・イベントに関する情報を提供します。

Oracle BEA WebLogic イベントを統合するには、以下のようにします。

1. Oracle BEA WebLogic サーバーで監査を有効にします。
2. Oracle BEA WebLogic サーバーでドメイン・ロギング を構成します。
3. Oracle BEA WebLogic サーバーでアプリケーション・ロギング を構成します。
4. Oracle BEA WebLogic 用の監査プロバイダーを構成します。

5. Oracle BEA WebLogic からログ・ファイルを取得するように QRadar を構成します。

イベント・ログの有効化

デフォルトでは、Oracle BEA WebLogic のイベント・ロギングは有効になっていません。

このタスクについて

Oracle WebLogic コンソールでイベント・ロギングを有効にするには、以下のようにします。

手順

1. Oracle WebLogic コンソール・ユーザー・インターフェースにログインします。
2. 「ドメイン **(Domain)**」 > 「構成 **(Configuration)**」 > 「一般 **(General)**」を選択します。
3. 「詳細 **(Advanced)**」をクリックします。
4. 「構成監査タイプ **(Configuration Audit Type)**」リストで「変更ログおよび監査 **(Change Log and Audit)**」を選択します。
5. 「保存」をクリックします。

次のタスク

これで、Oracle BEA WebLogic のドメイン・ログ収集を構成できるようになりました。

ドメイン・ロギングの構成

Oracle BEA WebLogic では複数インスタンスがサポートされています。インスタンスからのイベント・メッセージは、Oracle BEA WebLogic サーバーのドメイン全体の単一ログに収集されます。

このタスクについて

ドメインのログ・ファイルを構成するには、以下のようにします。

手順

1. Oracle WebLogic コンソールで、「ドメイン **(Domain)**」 > 「構成 **(Configuration)**」 > 「ロギング **(Logging)**」を選択します。
2. 「ログ・ファイル名 **(Log file name)**」パラメーターに、ドメイン・ログのディレクトリー・パスとファイル名を入力します。

   例えば `OracleDomain.log` などです。
3. オプション: 追加のドメイン・ログ・ファイル・ローテーション・パラメーターを構成します。
4. 「保存」をクリックします。

次のタスク

これで、サーバーのアプリケーション・ロギング を構成できるようになりました。

アプリケーション・ロギングの構成

Oracle BEA WebLogic のアプリケーション・ロギングを構成できます。

手順

1. Oracle WebLogic コンソールで、「サーバー **(Server)**」 > 「ロギング **(Logging)**」 > 「一般 **(General)**」を選択します。
2. 「ログ・ファイル名 **(Log file name)**」パラメーターに、アプリケーション・ログのディレクトリー・パスとファイル名を入力します。

   例えば `OracleDomain.log` などです。
3. オプション: 追加のアプリケーション・ログ・ファイルのローテーション・パラメーターを構成します。
4. 「保存」をクリックします。

次のタスク

これで、Oracle BEA WebLogic の監査プロバイダーを構成できるようになりました。

監査プロバイダーの構成

監査プロバイダーを構成できます。

手順

1. 「セキュリティー・レルム **(Security Realms)**」 > 「レルム名 **(Realm Name)**」 > 「プロバイダー **(Providers)**」 > 「監査 **(Auditing)**」を選択します。
2. 「新規」をクリックします。
3. 作成する監査プロバイダーの名前を入力して、監査プロバイダーを構成します。
4. 「タイプ **(Type)**」リストで「**DefaultAuditor**」を選択します。
5. 「**OK**」をクリックします。

   「設定 (Settings)」ウィンドウが表示されます。
6. 『監査プロバイダーの構成』で作成した監査プロバイダーをクリックします。
7. 「プロバイダー固有の情報 **(Provider Specific)**」タブをクリックします。
8. 必要な「アクティブなコンテキスト・ハンドラー項目 **(Active Context Handler Enteries)**」項目を追加します。
9. 「重大度 **(Severity)**」リストから「通知 **(Information)**」を選択します。
10. 「保存」をクリックします。

次のタスク

これで、Oracle BEA WebLogic からログ・ファイルをプルするように IBM Security QRadar を構成できるようになりました。

ログ・ソースの構成

Oracle BEA WebLogic からログ・ファイルを取得するように IBM Security QRadar を構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「ログ・ソース・タイプ」リストで「**Oracle BEA WebLogic**」を選択します。
6. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
7. 以下のパラメーターを構成します。

表 *320.* ログ・ファイル・パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。この値は、「リモート・ホストの **IP** またはホスト名 **(Remote Host IP or Hostname)**」パラメーターで構成した値と一致している必要があります。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
サービス・タイプ	リストから、ファイルの取得に使用するファイル転送プロトコル **(FTP)**を選択します。「**SSH** ファイル転送プロトコル **(SFTP) (SSH File Transfer Protocol (SFTP))**」、「ファイル転送プロトコル **(FTP) (File Transfer Protocol (FTP))**」、または「セキュア・コピー **(SCP) (Secure Copy (SCP))**」を選択できます。デフォルトは **SFTP** です。
リモート **IP** またはホスト名	受信するファイルの送信元ホストの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。サービス・タイプを **FTP** として構成する場合、デフォルトは 21 です。「サービス・タイプ」を「**SFTP**」または「**SCP**」として構成する場合、デフォルトは 22 です。 有効な範囲は、1 から 65535 です。
リモート・ユーザー	選択した「サービス・タイプ **(Service Type)**」を実行するホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。

表 320. ログ・ファイル・パラメーター (続き)

パラメーター	説明
リモート・パスワード	選択した「サービス・タイプ **(Service Type)**」を実行するホストにログインするために必要なパスワードを入力します。
パスワードの確認	選択した「サービス・タイプ **(Service Type)**」を実行するホストにログインするための「リモート・パスワード **(Remote Password)**」を確認します。
SSH 鍵ファイル	「サービス・タイプ」として「**SCP**」または「**SFTP**」を選択した場合、このパラメーターにより、SSH 秘密鍵ファイルを定義できます。また、SSH 鍵ファイルを指定すると、「リモート・パスワード **(Remote Password)**」オプションは無視されます。
リモート・ディレクトリー	ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。
再帰的 **(Recursive)**	サブフォルダーからもファイル・パターンを検索したい場合は、このチェック・ボックスを選択します。「**SCP**」を「サービス・タイプ」として構成する場合は、「再帰的 **(Recursive)**」パラメーターは使用されません。デフォルトでは、このチェック・ボックスはクリアされています。
FTP ファイル・パターン	「サービス・タイプ」として「**SFTP**」または「**FTP**」を選択すると、「リモート・ディレクトリー」で指定されたファイルのリストのフィルタリングに必要な正規表現 (regex) を構成するオプションを使用できます。一致するすべてのファイルは処理に組み込まれます。 例えば、server という単語で始まり 1 つ以上の数字が続き、`.log` で終わるファイルをすべてリストするには、`server[0-9]+¥.log` を使用します。このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://docs.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として「**FTP**」を選択した場合にのみ表示されます。「**FTP** 転送モード」パラメーターにより、FTP を介してログ・ファイルを取得するときのファイル転送モードを定義できます。 リストから、このログ・ソースに適用する転送モードを選択します。 • バイナリー **(Binary)** - バイナリー・データ・ファイル、または `.zip`、`.gzip`、`.tar`、`.tar+gz` 圧縮アーカイブ・ファイルを必要とするログ・ソースの場合、バイナリー FTP 転送モードを選択します。 • **ASCII** - ASCII FTP ファイル転送を必要とするログ・ソースには、**ASCII** を選択します。「FTP 転送モード」として「ASCII」を使用する場合、「プロセッサー」パラメーターには「なし」を選択し、「イベント・ジェネレーター **(Event Generator)**」パラメーターには「**1** 行ずつ **(LineByLine)**」を選択する必要があります。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。

表 320. ログ・ファイル・パラメーター (続き)

パラメーター	説明
開始時刻	処理を開始する時刻を入力します。このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、ディレクトリーを 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リモート・ホストにあるファイルが .zip、.gzip、.tar、または .tar.gz アーカイブ・フォーマットで保管されている場合は、アーカイブを展開して内容を処理することができるプロセッサーを選択します。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	既に処理済みのファイルを追跡し、これらのファイルの 2 回目の処理を希望しない場合は、このチェック・ボックスを選択します。これは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar システム上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。チェック・ボックスは選択されていない状態のままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これにより、ファイルの保管先ローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで「**Oracle BEA WebLogic**」 を選択します。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Oracle DB リスナー

Oracle データベース・リスナー・アプリケーションは、データベース・サーバーにログを格納します。

IBM Security QRadar に Oracle DB リスナーを統合するには、以下のいずれかのイベント収集方法を選択します。

- 『Oracle データベース・リスナー・プロトコルを使用したイベントの収集』
- 870 ページの『Perl を使用した Oracle データベース・イベントの収集』

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Oracle データベース・リスナー・プロトコルを使用したイベントの収集

Oracle データベース・リスナー・プロトコル・ソースにより、IBM Security QRadar は Oracle リスナー・データベースから生成されるログ・ファイルをモニターできます。ログ・ファイルを処理のためにモニターするように Oracle データベース・リスナー・プロトコルを構成する前に、Oracle リスナー・データベースのログ・ファイルのディレクトリー・パスを取得する必要があります。

始める前に

Oracle データベース・リスナー・プロトコルを使用しているときにイベントを適切に取得するには、Samba サービスが宛先サーバーで実行されている必要があります。

このタスクについて

Oracle データベース・リスナーからのログ・ファイルをモニターするように QRadar を構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「ログ・ソース・タイプ」リストで「**Oracle** データベース・リスナー **(Oracle Database Listener)**」を選択します。

6. 「プロトコル構成」リストで「**Oracle** データベース・リスナー」を選択します。
7. 以下のパラメーターを構成します。

表 *321. Oracle* データベース・リスナーのパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。
サーバー・アドレス	Oracle データベース・リスナーの IP アドレスを入力します。
ドメイン	Oracle データベース・リスナーにアクセスするために必要なドメインを入力します。このパラメーターはオプションです。
ユーザー名	Oracle データベース・リスナーを実行するホストにアクセスするために必要なユーザー名を入力します。
パスワード	Oracle データベース・リスナーを実行するホストにアクセスするために必要なパスワードを入力します。
パスワードの確認	Oracle データベース・リスナーにアクセスするために必要なパスワードを確認します。
ログ・フォルダーのパス **(Log Folder Path)**	Oracle データベース・リスナーのログ・ファイルにアクセスするためのディレクトリー・パスを入力します。
ファイル・パターン	ファイル名をフィルタリングするために必要な正規表現 (regex) を入力します。一致するすべてのファイルは処理に組み込まれます。デフォルトは `listener¥.log` です。 このパラメーターでは、ワイルドカードまたはグロビング・パターンを正規表現で使用することはできません。例えば、log という単語で始まり 1 つ以上の数字が続き、`tar.gz` で終わるファイルをすべてリストするには、`log[0-9]+¥.tar¥.gz` を使用します。このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://docs.oracle.com/javase/tutorial/essential/regex/ を参照してください。
ファイル読み取りの強制 **(Force File Read)**	ポーリング間隔のタイミングが指定されている場合にプロトコルにログ・ファイルの読み取りを強制するには、このチェック・ボックスを選択します。 このチェック・ボックスが選択されている場合、最終変更時刻属性またはファイル・サイズ属性に関係なく、指定されたポーリング間隔で常にログ・ファイル・ソースが検査されます。 このチェック・ボックスが選択されていない場合、最終変更時刻属性またはファイル・サイズ属性が変更されると、ポーリング間隔でログ・ファイル・ソースが検査されます。

表 321. *Oracle* データベース・リスナーのパラメーター (続き)

パラメーター	説明
再帰的 **(Recursive)**	サブフォルダーからもファイル・パターンを検索したい場合は、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
ポーリング間隔 **(秒)**	ポーリング間隔 (新規データを確認するためのログ・ファイルに対する照会から次の照会までの間の秒数) を入力します。最小ポーリング間隔は 10 秒、最大ポーリング間隔は 3,600 秒です。デフォルトは 10 秒です。
スロットル・イベント数/秒	Oracle データベース・リスナー・プロトコルによる 1 秒あたりの転送イベント最大数を入力します。最小値は 100 EPS、最大値は 20,000 EPS です。デフォルトは 100 EPS です。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

Perl を使用した Oracle データベース・イベントの収集

Oracle データベース・リスナー・アプリケーションは、データベース・サーバーにログを格納します。Oracle サーバーからこれらのログを IBM Security QRadar に転送するには、Oracle サーバーで Perl スクリプトを構成する必要があります。この Perl スクリプトはリスナー・ログ・ファイルをモニターし、複数行のログ項目を結合して 1 つのログ項目にし、Syslog (UDP) を使用してログを QRadar に送信します。

このタスクについて

ログは、QRadar に送信される前に処理および再フォーマットされます。これにより、ログは行単位 (ログ・ファイルのフォーマット) で転送されません。関連情報はすべて維持されます。

注**:** Oracle DB リスナー用に作成された Perl スクリプトは、Linux/UNIX サーバーでのみ機能します。Windows Perl スクリプトはサポートされていません。

Perl スクリプトをインストールして構成するには、以下のようにします。

手順

1. 以下の Web サイトに移動して必要なファイルをダウンロードします。

   http://www.ibm.com/support
2. 「ソフトウェア **(Software)**」タブで「スクリプト **(Scripts)**」を選択します。
3. Oracle DB リスナー・イベントを転送するスクリプトをダウンロードします。

   ```
   oracle_dblistener_fwdr.pl.gz
   ```
4. ファイルを解凍します。

   ```
   gzip -d oracle_dblistener_fwdr.pl.gz
   ```

5. Perl スクリプトを、Oracle サーバーをホストするサーバーにコピーします。

   注: Oracle サーバーをホストするデバイスに Perl 5.8 をインストールする必要があります。

6. listener.log ファイルと /var/run ディレクトリーに対する読み取り/書き込み権限が付与されているアカウントを使用して、Oracle サーバーにログインします。

7. 以下のコマンドを入力します。Oracle DB リスナー・スクリプトを開始するための追加コマンド・パラメーターを指定します。

   ```
   oracle_dblistener_fwdr.pl -h <IP address> -t "tail -F listener.log"
   ```

   ここで、*<IP address>* は QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。

表 322. コマンド・パラメーター

パラメーター	説明
-D	**-D** パラメーターは、スクリプトをフォアグラウンドで実行することを定義します。 デフォルトでは、スクリプトはデーモンとして実行され、すべての内部メッセージがローカル Syslog サービスに記録されます。
-t	**-t** パラメーターは、コマンド・ラインを使用してログ・ファイルをテールすること (リスナーからの新しい出力をすべてモニターすること) を定義します。Oracle データベースのバージョンによってログ・ファイルは異なります。以下に例を示します。 Oracle 9i: <install_directory>/product/9.2/network/log /listener.log Oracle 10g: <install_directory>/product/10.2.0/db_1/network/log /listener.log Oracle 11g: <install_directory>/diag/tnslsnr/qaoracle11/listener/trace/listener.log
-f	**-f** パラメーターは、**syslog facility.priority** をログの先頭に組み込むことを定義します。 何も指定されていない場合は、user.info が使用されます。
-H	**-H** パラメーターは、Syslog ヘッダーのホスト名または IP アドレスを定義します。スクリプトが実行される Oracle サーバーの IP アドレスを指定することをお勧めします。
-h	**-h** パラメーターは、受信 Syslog ホスト (ログの受信に使用されるイベント・コレクターのホスト名または IP アドレス) を定義します。
-p	**-p** パラメーターは、着信 UDP Syslog ポートを定義します。 ポートが指定されない場合は、514 が使用されます。
-r	**-r** パラメーターは、.pid ファイルを作成するディレクトリーの名前を定義します。デフォルトは /var/run です。**-D** が指定されている場合、このパラメーターは無視されます。

表 322. コマンド・パラメーター (続き)

パラメーター	説明
-l	**-I** パラメーターは、ロック・ファイルの作成先ディレクトリーの名前を定義します。デフォルトは /var/lock です。**-D** が指定されている場合、このパラメーターは無視されます。

例えば、IP アドレスが 192.168.12.44 の Oracle 9i サーバーでリスナー・ログをモニターし、IP アドレスが 192.168.1.100 の QRadar にイベントを転送するには、以下のコードを入力します。

```
oracle_dblistener_fwdr.pl -t tail -f <install_directory>/product/9.2/
network/log/listener.log -f user.info -H 192.168.12.44 -h 192.168.1.100
-p 514
```

このセットアップのサンプル・ログは次のようになります。

```
<14>Apr 14 13:23:37 192.168.12.44 AgentDevice=OracleDBListener
Command=SERVICE_UPDATE DeviceTime=18-AUG-2006 16:51:43 Status=0
SID=qora9
```

注: スクリプト・パラメーターを再構成する必要がある場合や、スクリプトによる QRadar へのイベント送信を停止する必要がある場合には、**kill** コマンドを使用してスクリプトを停止できます。例:

```
kill -QUIT `cat /var/run/oracle_dblistener_fwdr.pl.pid`
```

このコマンド例では、逆引用符文字 (`) が使用されています。ほとんどのキーボード・レイアウトでは、逆引用符文字は数字 1 の左側にあります。

次のタスク

これで、QRadar 内で Oracle データベース・リスナーを構成することができます。

QRadar 内での Oracle データベース・リスナーの構成

IBM Security QRadar 内で Oracle データベース・リスナーを構成できます。

手順

1. 「ログ・ソース・タイプ」リストで「**Oracle** データベース・リスナー **(Oracle Database Listener)**」を選択します。
2. 「プロトコル構成」リストで「**Syslog**」を選択します。
3. 「ログ・ソース **ID**」フィールドに、 870 ページの『Perl を使用した Oracle データベース・イベントの収集』で -H オプションを使用して指定した Oracle データベースの IP アドレスを入力します。

Oracle データベース・リスナー・プロトコルの構成は完了です。Oracle データベース・リスナーについて詳しくは、ベンダーの資料を参照してください。

Oracle Directory Server の概要

Oracle Directory Server は、以前は Sun ONE LDAP と呼ばれていました。

関連概念:

1013 ページの『Sun ONE LDAP』

QRadar 用の Sun ONE LDAP DSM は、Sun ONE Directory Server からの複数行の UDP アクセス・イベントおよび LDAP イベントを受け入れます。

Oracle Enterprise Manager

IBM Security QRadar DSM for Oracle Enterprise Manager は、Oracle Enterprise Manager デバイスからイベントを収集します。イベントは、Oracle Enterprise Manager のコンプライアンスのリアルタイム監視機能によって生成されます。

Oracle Enterprise Manager DSM の仕様を以下の表に示します。

表 323. *Oracle Enterprise Manager DSM* の仕様

仕様	値
製造元	Oracle
DSM 名	Oracle Enterprise Manager
RPM ファイル名	`DSM-OracleEnterpriseManager-`*`Qradar_version`*`-`*`Buildbuild_number`*`.noarch.rpm`
サポートされるバージョン	Oracle Enterprise Manager Cloud Control 12c
プロトコル	JDBC
記録されるイベント・タイプ	監査 コンプライアンス
自動的に検出?	いいえ
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Oracle Enterprise Manager (http://www.oracle.com/jp/products/enterprise-manager/index.html) イベントの元のフォーマットは、Oracle Enterprise Manager データベース・ビュー (`sysman.mgmt$ccc_all_observations`) 内の行です。QRadar は、このビューで新規の行をポーリングし、それらの行を使用してイベントを生成します。詳しくは、Compliance Views (http://docs.oracle.com/cd/E24628_01/doc.121/e57277/ch5_complianceviews.htm#BABBIJAA) を参照してください。

Oracle Enterprise Manager からイベントを収集するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Oracle Enterprise Manager DSM RPM をダウンロードして QRadar コンソールにインストールしてください。
2. Oracle Enterprise Manager システムが、外部デバイスからの接続を受け入れるように構成されていることを確認してください。
3. QRadar コンソールで Oracle Enterprise Manager ログ・ソースを追加します。以下の表は、Oracle Enterprise Manager イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *324. Oracle Enterprise Manager* ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース・タイプ	Oracle Enterprise Manager
プロトコル構成	JDBC
データベース・タイプ	Oracle
データベース名	Oracle Enterprise Manager データベースのサービス名。 使用可能なサービス名を表示するには、Oracle ホストで `lsnrctl status` コマンドを実行します。
IP またはホスト名	Oracle Enterprise Manager データベースのホストの IP アドレスまたはホスト名。
ポート	Oracle Enterprise Manager データベースが使用するポート。
ユーザー名	`sysman.mgmt$ccc_all_observations` テーブルにアクセスする権限を持つアカウントのユーザー名。
定義済み照会	none
テーブル名	`sysman.mgmt$ccc_all_observations`
選択リスト	*
比較フィールド	ACTION_TIME
準備済みステートメントの使用 (Use Prepared Statements)	True

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Oracle ファイングレイン監査

Oracle ファイングレイン監査 DSM は、Java Database Connectivity (JDBC) プロトコルを使用して、Oracle 9i 以降からのデータベース監査イベントをポーリングできます。

イベントを収集するには、管理者が Oracle データベースでファイングレイン監査を有効にする必要があります。ファイングレイン監査では、ソース・データベースで発生した select、update、delete、および insert の各操作のイベントと、データが変更されたレコードが提供されます。管理者が監査ポリシーを有効にしている場合、いずれかのデータベース表で変更が発生するたびに、新規行が挿入されてデータベース表 `dba_fga_audit_trail` が更新されます。

Oracle のファイングレイン監査を構成するために、管理者は以下のタスクを実行できます。

1. Oracle データベースでポリシー・モニターを必要とするすべての表で監査を構成します。
2. Oracle ファイングレイン監査 DSM が Oracle データベースをポーリングしてイベントを収集するように、ログ・ソースを構成します。
3. ポーリングされて収集されたイベントが IBM Security QRadar の 「ログ・アクティビティー」タブに表示されることを確認します。

ログ・ソースの構成

データベース管理者がデータベース・ポリシーを構成した後で、JDBC プロトコルを使用して Oracle データベースにアクセスするようにログ・ソースを構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストを使用して、「**Oracle** ファイングレイン監査」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. 以下の値を構成します。

表 325. *Oracle* ファイングレイン監査の *JDBC* パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソース ID は以下の形式で入力します。 <*database*>@<*hostname*> または <*table name*>|<*database*>@<*hostname*> 各部分について以下で説明します。 • <*table name*> は、イベント・レコードが含まれているデータベースのテーブルまたはビューの名前です。このパラメーターはオプションです。テーブル名を指定する場合は、パイプ文字 (|) を指定する必要があります。また、テーブル名は「テーブル名」パラメーターと一致している必要があります。 • <*database*> は、「データベース名」パラメーターで定義されているデータベース名です。データベース名は必須パラメーターです。 • <*hostname*> は、「**IP** またはホスト名」パラメーターで定義されている、ログ・ソースのホスト名または IP アドレスです。ホスト名は必須パラメーターです。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
データベース・タイプ	データベース・タイプとして「**MSDE**」を選択します。
データベース名	接続先データベースの名前を入力します。 テーブル名は、英数字で最大 255 文字までです。テーブル名に使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
IP またはホスト名	データベースの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。表示されるデフォルトは、選択した「データベース・タイプ」によって異なります。有効な範囲は 0 から 65536 です。 JDBC 構成のポートは、データベースのリスナー・ポートに一致する必要があります。データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 すべてのオプションのデフォルトのポート番号は次のとおりです。 • DB2 - 50000 • MSDE - 1433 • Oracle - 1521 データベース・タイプとして「MSDE」を使用するときに**「データベース・インスタンス」**を定義する場合は、構成の「ポート」パラメーターをブランクのままにしておく必要があります。
ユーザー名	データベース・ユーザー名を入力します。 ユーザー名は、英数字で最大 255 文字までです。ユーザー名には下線 (_) も使用できます。

表 325. *Oracle* ファイングレイン監査の *JDBC* パラメーター (続き)

パラメーター	説明
パスワード	データベース・パスワードを入力します。 パスワードの最大長は 255 文字です。
パスワードの確認	データベースにアクセスするためのパスワードを確認します。
認証ドメイン	「**MSDE**」を「データベース・タイプ」として選択した場合、「認証ドメイン」フィールドが表示されます。ドメイン資格情報でユーザーを検証するようにネットワークが構成されている場合、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。 認証ドメインには、英数字を含める必要があります。ドメインに使用できる特殊文字は、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
データベース・インスタンス	「MSDE」を「**データベース・タイプ**」として選択した場合、「データベース・インスタンス」フィールドが表示されます。 1 つのサーバー上に複数の SQL サーバー・インスタンスがある場合は、接続するインスタンスのタイプを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックする場合は、構成内で「**データベース・インスタンス**」パラメーターをブランクのままにしておく必要があります。
定義済み照会	リストから「なし」を選択します。
テーブル名	イベント・レコードを含むテーブルの名前として `dba_fga_audit_trail` と入力します。このフィールドの値をデフォルト以外に変更すると、JDBC プロトコルがイベントを適切に収集できなくなります。
選択リスト	テーブルまたはビューのすべてのフィールドを含めるには、`*` を入力します。 ご使用の構成で必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	テーブルに対する照会から次の照会までの間に追加された新しいイベントをそのタイム・スタンプによって特定するため、`extended_timestamp` を入力します。
準備済みステートメントの使用 **(Use Prepared Statements)**	「準備済みステートメントの使用 **(Use Prepared Statements)**」チェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。

表 325. *Oracle* ファイングレイン監査の *JDBC* パラメーター (続き)

パラメーター	説明
開始日時	オプション。データベース・ポーリングの開始日時を構成します。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (データベース・テーブルへの照会から次の照会までの間の時間) を秒単位で入力します。デフォルトのポーリング間隔は 30 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。指定子の H および M のない数値の場合は、秒単位のポーリングになります。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「**MSDE**」を「データベース・タイプ」として選択した場合、「名前付きパイプ通信の使用 **(Use Named Pipe Communications)**」チェック・ボックスが表示されます。デフォルトでは、このチェック・ボックスはクリアされています。 TCP/IP ポート接続の代替方式を使用する場合は、このチェック・ボックスを選択します。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
NTLMv2 の使用	「**MSDE**」を「データベース・タイプ」として選択した場合、「**NTLMv2** の使用」チェック・ボックスが表示されます。 NTLMv2 認証を必要とする SQL サーバーとの通信時に MSDE 接続で NTLMv2 プロトコルを使用するように強制する場合は、「**NTLMv2** の使用」チェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されています。 「**NTLMv2** の使用」チェック・ボックスを選択した場合でも、NTLMv2 認証を必要としない SQL サーバーへの MSDE 接続には影響しません。
SSL の使用 **(Use SSL)**	接続で SSL 通信がサポートされている場合は、このチェック・ボックスを選択します。このオプションを選択する場合は、SharePoint データベースに追加の構成が必要であり、また管理者が両方のアプライアンスで証明書を構成する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにします。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

Oracle OS Audit

Oracle OS Audit DSM for IBM Security QRadar は、ローカル・オペレーティング・システム・ファイルに保管されている監査レコードをモニターできるようにします。

このタスクについて

監査イベント・ファイルがローカル・オペレーティング・システム・ディレクトリーで作成または更新されると、Perl スクリプトが変更を検出し、データを QRadar に転送します。この Perl スクリプトは監査ログ・ファイルをモニターし、複数行のログ項目をすべて結合して 1 つのログ項目にすることで、ログが行単位 (ログ・ファイルのフォーマット) で転送されないようにします。その後 Syslog を使用してログが QRadar に送信されます。Oracle OS Audit 用に作成された Perl スクリプトは、Linux/UNIX サーバーでのみ機能します。Windows ベースの Perl のインストールはサポートされていません。

Oracle OS Audit DSM を QRadar と統合するには、以下のようにします。

手順

1. 以下の Web サイトに移動して必要なファイルをダウンロードします。

   http://www.ibm.com/support
2. 「ソフトウェア **(Software)**」タブで「スクリプト **(Scripts)**」を選択します。
3. Oracle OS Audit スクリプトをダウンロードします。

   `×oracle_osauditlog_fwdr_5.3.tar.gz`
4. 以下のコマンドを入力して、ファイルを解凍します。

   ```
   tar -zxvf oracle_osauditlog_fwdr_5.3.tar.gz
   ```
5. Perl スクリプトを、Oracle サーバーをホストするサーバーにコピーします。

   注**:** Oracle サーバーをホストするデバイスに Perl 5.8 をインストールする必要があります。Perl 5.8 がインストールされていない場合は、Oracle OS Audit スクリプトを開始しようとすると、ライブラリー・ファイルが欠落していることが示されます。続行する前に、Perl 5.8 がインストールされていることを確認することをお勧めします。
6. Oracle ホストに、SYS または root 権限を持つ Oracle ユーザーとしてログインします。
7. 環境変数 *ORACLE_HOME* と *ORACLE_SID* がご使用のデプロイメントに対応して適切に構成されていることを確認します。
8. 以下のファイルを開きます。

   ```
   ${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora
   ```
9. Syslog の場合、以下の行をファイルに追加します。

   ```
   *.audit_trail=os *.audit_syslog_level=local0.info
   ```
10. 以下のディレクトリーに対する読み取り/書き込み権限がアカウントにあることを確認します。

/var/lock/ /var/run/

11. Oracle データベース・インスタンスを再始動します。
12. OS Audit DSM スクリプトを開始します。

```
oracle_osauditlog_fwdr_5.3.pl -t target_host -d logs_directory
```

表 *326. Oracle OS Audit* のコマンド・パラメーター

パラメーター	説明
-t	**-t** パラメーターは、監査ログ・ファイルを受信するリモート・ホストを定義します。
-d	**-d** パラメーターは、DDL および DML ログ・ファイルのディレクトリー・ロケーションを定義します。 指定するディレクトリー・ロケーションは、ルート・ディレクトリーを基準にした絶対パスである必要があります。
-H	**-H** パラメーターは、Syslog ヘッダーのホスト名または IP アドレスを定義します。スクリプトが実行される Oracle サーバーの IP アドレスを指定することをお勧めします。
-D	**-D** パラメーターは、スクリプトをフォアグラウンドで実行することを定義します。 デフォルトでは、スクリプトはデーモンとして (バックグラウンドで) 実行され、すべての内部メッセージがローカル Syslog サービスに記録されます。
-n	**-n** パラメーターは、新しいログを処理し、既存のログ・ファイルで処理する変更があるかどうかをモニタリングします。 **-n** オプション文字列が指定されていない場合、スクリプトの実行時に既存のログ・ファイルがすべて処理されます。
-u	**-u** パラメーターは UDP を定義します。
-f	**-f** パラメーターは、**syslog facility.priority** をログの先頭に組み込むことを定義します。 値を入力しない場合、user.info が使用されます。
-r	**-r** パラメーターは、.pid ファイルの作成先ディレクトリーの名前を定義します。デフォルトは /var/run です。**-D** が指定されている場合、このパラメーターは無視されます。
-l	**-I** パラメーターは、ロック・ファイルの作成先ディレクトリーの名前を定義します。デフォルトは /var/lock です。**-D** が指定されている場合、このパラメーターは無視されます。
-h	**-h** パラメーターは、ヘルプ・メッセージを表示します。

表 326. Oracle OS Audit のコマンド・パラメーター (続き)

パラメーター	説明
-v	**-v** パラメーターを指定すると、スクリプトのバージョン情報が表示されます。

Oracle サーバーを再始動するとき場合は、スクリプトを再始動する必要があります。

```
oracle_osauditlog_fwdr.pl -t target_host -d logs_directory
```

次のタスク

これで、QRadar 内でログ・ソースを構成できるようになりました。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar 内での Oracle OS Audit のログ・ソースの構成

IBM Security QRadar 内でログ・ソースを構成できます。

手順

1. 「ログ・ソース・タイプ」リストで「**Oracle RDBMS OS 監査レコード (Oracle RDBMS OS Audit Record)**」を選択します。
2. 「プロトコル構成」リストで「**Syslog**」を選択します。
3. 「ログ・ソース **ID**」フィールドに、 879 ページの『Oracle OS Audit』で **-H** オプションを使用して指定したアドレスを入力します。

Oracle 監査レコードについて詳しくは、ベンダーの資料を参照してください。

第 100 章 OSSEC

IBM Security QRadar 用の OSSEC DSM は、syslog を使用して OSSEC インストール済み環境から転送されたイベントを受け取ります。

OSSEC はオープン・ソースのホスト・ベース侵入検知システム (HIDS) であり、侵入イベントを QRadar に提供できます。OSSEC エージェントをインストールしてある場合は、OSSEC 管理サーバーで syslog を構成する必要があります。OSSEC をローカル環境に (スタンドアロンで) インストールしてある場合は、syslog イベントを QRadar に転送するように各スタンドアロン OSSEC で syslog を構成する必要があります。

OSSEC の構成

スタンドアロン・インストール済み環境または管理サーバーで OSSEC の Syslog を構成できます。

手順

1. SSH を使用して、OSSEC デバイスにログインします。
2. OSSEC の ossec.conf 構成ファイルを編集します。

   <インストール・ディレクトリー>/ossec/etc/ossec.conf
3. 以下の Syslog 構成を追加します。

   注: **alerts** 項目と **localfile** 項目の間に Syslog 構成を追加します。

   ```
   </alerts>

   <syslog_output> <server>(QRadar IP Address)</server> <port>514</port>
   </syslog_output>

   <localfile>
   ```

   例:

   ```
   <syslog_output> <server>10.100.100.2</server> <port>514</port>
   </syslog_output>
   ```
4. OSSEC 構成ファイルを保存します。
5. 以下のコマンドを入力して、Syslog デーモンを有効にします。

   ```
   <installation directory>/ossec/bin/ossec-control enable client-syslog
   ```
6. 以下のコマンドを入力して、Syslog デーモンを再始動します。

   ```
   <installation directory>/ossec/bin/ossec-control restart
   ```

構成は完了です。OSSEC イベントが自動的に検出されると、ログ・ソースが IBM Security QRadar に追加されます。OSSEC によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、OSSEC からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

OSSEC のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**OSSEC**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   Syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *327. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	OSSEC インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

第 101 章 Palo Alto Networks PA シリーズ

Palo Alto PA シリーズのデバイスからイベントを収集するには、Palo Alto PAシリーズ用の IBM Security QRadar DSM を使用します。

以下の表は、Palo Alto PA シリーズ DSM の仕様を示しています。

表 328. *Palo Alto PA* シリーズ用の *DSM* の仕様

仕様	値
製造元	Palo Alto Networks
DSM 名	Palo Alto PA シリーズ
RPM ファイル名	DSM-PaloAltoPaSeries-*QRadar_version-build_number*.noarch.rpm
サポートされるバージョン	PAN-OS v3.0 から v7.1
イベント・フォーマット	Syslog LEEF PAN-OS v4.0 から v6.1 の CEF
QRadar で記録されるイベント・タイプ	Traffic Threat Config System HIP Match
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Palo Alto Networks Web サイト (http://www.paloaltonetworks.com)

イベントを Palo Alto PA シリーズから QRadar に送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Palo Alto PA シリーズ DSM RPM をダウンロードしてください。
2. QRadar と通信するように Palo Alto PA シリーズ・デバイスを構成します。syslog の出力先と転送ポリシーを Palo Alto PA シリーズ・デバイス上で作成する必要があります。
3. QRadar が Palo Alto PA シリーズをログ・ソースとして自動的に検出しない場合は、QRadar コンソール上で Palo Alto PA シリーズのログ・ソースを作成します。以下に示す Palo Alto の値を使用して、ログ・ソースのパラメーターを構成してください。

パラメーター	説明
ログ・ソース ID	Palo Alto PA シリーズ・デバイスの IP アドレスまたはホスト名。
ログ・ソース・タイプ	Palo Alto PA シリーズ
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『Palo Alto PA シリーズ・デバイスでの Syslog 宛先の作成』
Palo Alto PA シリーズ・イベントを IBM Security QRadar に送信するには、Palo Alto PA シリーズ・デバイス上で Syslog 宛先を作成します。

888 ページの『Palo Alto PA シリーズ・デバイスに対する転送ポリシーの作成』
IBM Security QRadar コンソールまたはイベント・コレクター (Event Collector) が、Palo Alto PA シリーズ・デバイスとは異なるセキュリティー・ゾーンに含まれる場合、転送ポリシー・ルールを作成します。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

889 ページの『Palo Alto PA シリーズ Networks のファイアウォール・デバイスでの ArcSight CEF 形式の Syslog イベントの作成』
ArcSight CEF 形式の Syslog イベントを IBM Security QRadar に送信するように Palo Alto Networks のファイアウォールを構成できます。

Palo Alto PA シリーズ・デバイスでの Syslog 宛先の作成

Palo Alto PA シリーズ・イベントを IBM Security QRadar に送信するには、Palo Alto PA シリーズ・デバイス上で Syslog 宛先を作成します。

手順

1. Palo Alto Networks インターフェースにログインします。
2. 「デバイス **(Device)**」タブをクリックします。
3. 「サーバー・プロファイル」>「**Syslog**」をクリックします。
4. 「追加」をクリックします。
5. syslog の出力先を作成します。
   a. 「**Syslog** サーバー・プロファイル **(Syslog Server Profile)**」ダイアログ・ボックスで「追加」をクリックします。
   b. Syslog サーバーとして使用する QRadar システムの名前、サーバー IP アドレス、ポート、およびファシリティーを指定します。
   c. 「**OK**」をクリックします。
6. LEEF イベントを構成します。

   注**:** Syslog を使用している場合は、デフォルト・オプションを選択してください。

重要**:** 以下の各例で改行があると、この構成が失敗する原因となります。各サブステップで、コード・ブロックをテキスト・エディターにコピーし、改行を削除してから、「カスタム・フォーマット **(Custom Format)**」列に一行で貼り付けてください。

a. 「カスタム・ログ・フォーマット **(Custom Log Format)**」タブをクリックします。

b. 以下のテキストをコピーして、「構成」ログ・タイプの「カスタム・フォーマット **(Custom Format)**」列に貼り付けます。

PAN-OS v3.0 から **v6.1**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$result|cat=$type|usrName
=$admin|src=$host|devTime=$cef-formatted-receive_time|client=$client|sequence=
$seqno|serial=$serial|msg=$cmd
```

PAN-OS v7.1

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version
|$result|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|devTime=$cef
-formatted-receive_time|src=$host|VirtualSystem=$vsys|msg=$cmd|usrName=$admin|
client=$client|Result=$result|ConfigurationPath=$path|sequence=$seqno|ActionFlags
=$actionflags|BeforeChangeDetail=$before-change-detail||AfterChangeDetail=$after-
change-detail|DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_
hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_
hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name
```

c. 以下のテキストをコピーして、「システム」ログ・タイプの「カスタム・フォーマット **(Custom Format)**」列に貼り付けます。

PAN-OS v3.0 から **v6.1**

```
LEEF:1.0|PaloAlto Networks|PAN-OS Syslog Integration|4.0|$eventid
|cat=$type|subtype=$subtype|devTime=$cef-formatted-receive_time|sev=$severity|
Severity=$number-of-severity|msg=$opaque|Filename=$object
```

PAN-OS v7.1

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version
|$eventid| ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|subtype=$subtype
|devTime=$cef-formatted-receive_time|VirtualSystem=$vsys|Filename=$object| Module=
$module|sev=$number-of-severity|Severity=$severity|msg=$opaque| sequence=$seqno|
ActionFlags=$actionflags|DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2
=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_
hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name
```

d. 以下のテキストをコピーして、「脅威」ログ・タイプの「カスタム・フォーマット **(Custom Format)**」列に貼り付けます。

PAN-OS v3.0 から **v6.1**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$threatid|cat=$type
|subtype=$subtype|src=$src|dst=$dst|srcPort=$sport|dstPort=$dport|proto=$proto
|usrName=$srcuser|SerialNumber=$serial|srcPostNAT=$natsrc|dstPostNAT=$natdst
|RuleName=$rule|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app
|VirtualSystem=$vsys|SourceZone=$fromDestinationZone=$to|IngressInterface=$inbound_if
|EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid
|RepeatCount=$repeatcnt|srcPostNATPort=$natsport|dstPostNATPort=$natdport
|Flags=$flags|URLCategory=$category|sev=$severity|Severity=$number-of-severity
|Direction=$direction|ContentType=$contenttype|action=$action|Miscellaneous=$misc
```

PAN-OS v7.1

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender
_sw_version|$threatid|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type
|subtype=$subtype|devTime=$cef-formatted-receive_time|src=$src|dst=$dst|srcPostNAT
=$natsrc|dstPostNAT=$natdst|RuleName=$rule|usrName=$srcuser|SourceUser=$srcuser|
DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|SourceZone=$from|
DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|
LogForwardingProfile=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|srcPort
=$sport|dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=
$flags|proto=$proto|action=$action|Miscellaneous=$misc|ThreatID=$threatid|
URLCategory=$category|sev=$number-of-severity|Severity=$severity|Direction=$
direction|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=$srcloc
|DestinationLocation=$dstloc|ContentType=$contenttype|PCAP_ID=$pcap_id|FileDigest
=$filedigest|Cloud=$cloud|URLIndex=$url_idx|UserAgent=$user_agent|FileType=
$filetype|identSrc=$xff|Referer=$referer|Sender=$sender|Subject=$subject|Recipient
=$recipient|ReportID=$reportid|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name
```

e. 以下のテキストをコピーして、「トラフィック」ログ・タイプの「カスタム・フォーマット **(Custom Format)**」列に貼り付けます。

PAN-OS v3.0 から **v6.1**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$action|cat=$type|src=$src
|dst=$dst|srcPort=$sport|dstPort=$dport|proto=$proto|usrName=$srcuser| SerialNumber=
$serial|Type=$type|subtype=$subtype|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=
$rule|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app| VirtualSystem=
$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if
|EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=$flags
|totalBytes=$bytes|totalPackets=$packets|ElapsedTime=$elapsed|URLCategory=$category
|dstBytes=$bytes_received|srcBytes=$bytes_sent|action=$action
```

PAN-OS v7.1

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender
_sw_version|$action|cat=$type|ReceiveTime=$receive_time|SerialNumber=$serial|Type=
$type|subtype=$subtype|devTime=$cef-formatted-receive_time|src=$src|dst=$dst|
srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|usrName=$srcuser|SourceUser=
$srcuser|DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|SourceZone
=$from|DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound
_if|LogForwardingProfile=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|
srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|
Flags=$flags|proto=$proto|action=$action|totalBytes=$bytes|dstBytes=$bytes_received
|srcBytes=$bytes_sent|totalPackets=$packets|StartTime=$start|ElapsedTime=$elapsed|
URLCategory=$category|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=
$srcloc|DestinationLocation=$dstloc|dstPackets=$pkts_received|srcPackets=$pkts_
sent|SessionEndReason=$session_end_reason|DeviceGroupHierarchyL1=$dg_hier_level_1
|DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|
ActionSource=$action_source
```

f. 以下のテキストをコピーして、「**HIP Match**」ログ・タイプの「カスタム・フォーマット **(Custom Format)**」列に貼り付けます。PAN-OS v3.0 から v6.1 を使用している場合は、この手順を省略します。

PAN-OS v7.1

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender
_sw_version|$matchname|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type
|subtype=$subtype|devTime=$cef-formatted-receive_time|usrName=$srcuser|
VirtualSystem=$vsys|identHostName=$machinename|OS=$os|identSrc=$src|HIP=$matchname
|RepeatCount=$repeatcnt|HIPType=$matchtype|sequence=$seqno|ActionFlags=$actionflags
|DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name
```

注**:** 「**DeviceGroupHierarchy**」フィールドと「**URLIndex**」フィールドは完全性と一貫性のために含まれています。ただし、これらは実験的なフィールドであり、アーカイブ目的にのみ使用する必要があります。

7. 「**OK**」をクリックします。
8. Syslog メッセージに含めるイベントの重大度を指定します。
   a. 「ログ設定」>「システム」をクリックしてから、「編集」をクリックします。
   b. Syslog メッセージに含める各イベント重大度レベルのチェック・ボックスを選択します。
   c. syslog 宛先の名前を入力します。
   d. 「**OK**」をクリックします。
9. 「デバイス」タブをクリックしてから、「コミット」をクリックします。

次のタスク

Palo Alto Networks デバイスと QRadar の間の通信を許可するには、転送ポリシーを作成します。『Palo Alto PA シリーズ・デバイスに対する転送ポリシーの作成』を参照してください。

関連概念:

885 ページの『第 101 章 Palo Alto Networks PA シリーズ』

Palo Alto PA シリーズのデバイスからイベントを収集するには、Palo Alto PAシリーズ用の IBM Security QRadar DSM を使用します。

Palo Alto PA シリーズ・デバイスに対する転送ポリシーの作成

IBM Security QRadar コンソールまたはイベント・コレクター (Event Collector) が、Palo Alto PA シリーズ・デバイスとは異なるセキュリティー・ゾーンに含まれる場合、転送ポリシー・ルールを作成します。

手順

1. Palo Alto Networks にログインします。
2. ダッシュボードで、「ポリシー」タブをクリックします。
3. 「ポリシー」>「ポリシー・ベースの転送 **(Policy Based Forwarding)**」をクリックします。
4. 「新規」をクリックします。
5. パラメーターを構成します。ポリシー・ベースの転送の値についての説明は、「パロアルトネットワークス管理者ガイド」を参照してください。

関連概念:

885 ページの『第 101 章 Palo Alto Networks PA シリーズ』
Palo Alto PA シリーズのデバイスからイベントを収集するには、Palo Alto PAシリーズ用の IBM Security QRadar DSM を使用します。

Palo Alto PA シリーズ Networks のファイアウォール・デバイスでの ArcSight CEF 形式の Syslog イベントの作成

ArcSight CEF 形式の Syslog イベントを IBM Security QRadar に送信するように Palo Alto Networks のファイアウォールを構成できます。

手順

1. Palo Alto Networks インターフェースにログインします。
2. 「**Panorama/Device**」 > 「**Setup**」 > 「**Management**」を選択して、Syslog メッセージのヘッダーにその IP アドレスを含めるようにデバイスを構成します。
3. 「**Logging and Reporting Settings**」セクションで、「**Edit**」をクリックします。
4. 「**Syslog HOSTNAME Format**」リストで、「**ipv4-address**」または「**ipv6-address**」を選択し、「**OK**」をクリックします。
5. 「**Device**」 > 「**Server Profiles**」 > 「**Syslog**」を選択し、「**Add**」をクリックします。
6. 「**Name**」および「**Location**」を指定します。デバイスで仮想システムが有効になっている場合、「Location」は仮想システムを指します。
7. 「サーバー」タブで「追加」をクリックします。
8. Syslog サーバーとして使用する QRadar システムの名前、サーバー IP アドレス、ポート、およびファシリティーを指定します。
   a. 「**Name**」は Syslog サーバー名です。
   b. 「**Syslog Server**」は Syslog サーバーの IP アドレスです。
   c. 「**Transport/Port**」のデフォルトは **514** です。
   d. 「**Faculty**」のデフォルトは **LOG_USER** です。
9. ログ・タイプに対する ArcSight CEF に基づいてカスタムの形式を定義するために、リストされるログ・タイプのいずれかを選択するには、次の手順を実行します。
   a. 「**Custom Log Format**」タブをクリックし、リストされるログ・タイプのいずれかを選択して、そのログ・タイプに対する ArcSight CEF に基づい

てカスタムの形式を定義します。リストされるログ・タイプは、「**Config**」、「**System**」、「**Threat**」、「**Traffic**」、および「**HIP Match**」です。

b. 「**OK**」を 2 回クリックして項目を保存し、「**Commit**」をクリックします。

10. ArcSight の資料「*Implementing ArcSight CEF*」に用意されているイベント・マッピング・テーブルを使用する独自の CEF スタイルの形式を定義するには、CEF スタイルの形式の定義方法に関する次の情報を使用できます。

「**Custom Log Format**」タブは、CEF に定義されている任意の文字の特殊文字としてのエスケープをサポートします。例えば、円記号を使用して円記号および等号をエスケープするには、「**Escaping**」チェック・ボックスを有効にし、¥=as を「**Escaped Characters**」に、¥as を「**Escape Character**」に指定します。

各ログ・タイプの認証プロセス中に使用された CEF スタイルの形式を次のリストに示します。これらのカスタムの形式には、Syslog の表示のデフォルトの形式に含まれるすべてのフィールドが、類似の順序で含まれています。

重要: PDF の書式設定により問題が発生することがあるため、このメッセージ形式を直接 PAN-OS の Web インターフェースにコピーして貼り付けないでください。そうではなく、テキスト・エディターに貼り付けて、復帰文字や改行文字を削除してから、Web インターフェースにコピーして貼り付けてください。

Traffic

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$type
|1|rt=$cef-formatted-receive_time deviceExternalId
=$serial src=$src dst=$dst sourceTranslatedAddress
=$natsrc destinationTranslatedAddress=$natdst
 cs1Label=Rule cs1=$rule suser=$srcuser duser
=$dstuser app=$app cs3Label=Virtual System
 cs3=$vsys cs4Label=Source Zone cs4=$from
cs5Label=Destination Zone cs5=$to deviceInboundInterface=
$inbound_if deviceOutboundInterface=$outbound_if
 cs6Label=LogProfile cs6=$logset cn1Label=SessionID
 cn1=$sessionid cnt=$repeatcnt
 spt=$sport dpt=$dport sourceTranslatedPort=$natsport
 destinationTranslatedPort=$natdport flexString1Label=Flags
 flexString1=$flags proto=$proto act=$action
flexNumber1Label=Total bytes flexNumber1=
$bytes in=$bytes_sent out=$bytes_received
 cn2Label=Packets cn2=$packets PanOSPacketsReceived=
$pkts_received PanOSPacketsSent=$pkts_sent
start=$cef-formatted-time_generated cn3Label
=Elapsed time in seconds cn3=$elapsed cs2Label
=URL Category cs2=$category externalId=$seqno
```

Threat

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$type|
$number-of-severity|rt=$cef-formatted-receive_time
deviceExternalId=$serial src=$src dst=$dst
sourceTranslatedAddress=$natsrc
destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule
 suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual
System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=
Destination Zone cs5=$to deviceInboundInterface=$inbound_if
 deviceOutboundInterface=$outbound_if cs6Label=LogProfile
```

```
cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt
 spt=$sport dpt=$dport sourceTranslatedPort=$natsport
destinationTranslatedPort=$natdport flexString1Label=Flags
 flexString1=$flags proto=$proto act=$action request=$misc
 cs2Label=URL Category cs2=$category flexString2Label=Direction
 flexString2=$direction externalId=$seqno requestContext=
$contenttype cat=$threatid filePath=$cloud fileId=$pcap_id
 fileHash=$filedigest
```

Config

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$result|$type|1|rt=$cef-
formatted-receive_time deviceExternalId=$serial dvchost=$host
 cs3Label=Virtual System cs3=$vsys act=$cmd duser=$admin
destinationServiceName=$client msg=$path externalId=$seqno
```

オプション:

```
cs1Label=Before Change Detail cs1=$before-change-detail
 cs2Label=After Change Detail cs2=$after-change-detail
```

System

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$type|
$number-of-severity|rt=$cef-formatted-receive_time
deviceExternalId=$serial cs3Label=Virtual System cs3=$vsys
 fname=$object flexString2Label=Module flexString2=$module
msg=$opaque externalId=$seqno cat=$eventid
```

HIP Match

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$matchtype|$type|1|
rt=$cef-formatted-receive_time deviceExternalId=$serial
suser=$srcuser cs3Label=Virtual System cs3=$vsys shost=$machinename
 src=$src cnt=$repeatcnt externalId=$seqno cat=$matchname
 cs2Label=Operating System cs2=$os
```

次のタスク

Syslog 構成の詳細については、Palo Alto Networks の Web サイト (https://www.paloaltonetworks.com) の「*PAN-OS Administrator's Guide*」を参照してください。

関連概念:

885 ページの『第 101 章 Palo Alto Networks PA シリーズ』
Palo Alto PA シリーズのデバイスからイベントを収集するには、Palo Alto PAシリーズ用の IBM Security QRadar DSM を使用します。

第 102 章 Pirean Access: One

IBM Security QRadar 用の Pirean Access: One DSM は、DB2 監査データベースをポーリングしてアクセス管理および認証イベントを取得することによってイベントを収集します。

QRadar は、DB2 v9.7 データベースを使用してアクセス管理 および認証 イベントを格納する Pirean Access: One ソフトウェアのインストール済み環境をサポートしています。

始める前に

Pirean Access: One と統合するように QRadar を構成する前に、QRadar 用のデータベース・ユーザー・アカウントとパスワードを作成することができます。QRadar アカウントの作成は必須ではありませんが、QRadar ユーザーに対するアクセス管理 および認証 イベント表データのセキュリティーを確保するのに有効です。

QRadar ユーザーには、イベントを格納するデータベース表の読み取り権限が必要です。JDBC プロトコルにより、QRadar がデータベースにログインしてタイム・スタンプに基づいてイベントをポーリングできるため、最新のデータを確実に取得することができます。

注**:** ファイアウォール・ルールが Pirean Access: One インストール済み環境と QRadar コンソールまたは JDBC でイベントをポーリングする役割を担う管理対象ホストの間の通信をブロックしていないことを確認します。

ログ・ソースの構成

イベントを収集するには、JDBC プロトコルを使用して Access: One インストール・データベースをポーリングするように、IBM Security QRadar でログ・ソースを構成する必要があります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「**Pirean Access: One**」を選択します。
8. 「プロトコル構成」リストで「**JDBC**」を選択します。
9. 以下の値を構成します。

表 329. *Pirean Access: One* のログ・ソース・パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で定義する必要があります。 <*database*>@<*hostname*> 各部分について以下で説明します。 <*database*> は、「データベース名」パラメーターで定義されているデータベース名です。データベース名は必須パラメーターです。 <*hostname*> は、「**IP** またはホスト名」パラメーターで定義されている、ログ・ソースのホスト名または IP アドレスです。ホスト名は必須パラメーターです。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
データベース・タイプ	イベント・ソースに使用するデータベースのタイプとして、リストから「DB2」を選択します。
データベース名	接続先データベースの名前を入力します。デフォルトのデータベース名は LOGINAUD です。
IP またはホスト名	データベース・サーバーの IP アドレスまたはホスト名を入力します。
ポート	監査データベース DB2 インスタンスが使用する TCP ポート番号を入力します。 DB2 管理者から、このフィールドに必要な TCP ポートを確認できます。
ユーザー名	DB2 データベース・サーバーと監査テーブルにアクセスできるユーザー名を入力します。 ユーザー名は、英数字で最大 255 文字までです。ユーザー名には下線 (_) も使用できます。
パスワード	データベース・パスワードを入力します。 パスワードの最大長は 255 文字です。
パスワードの確認	データベースにアクセスするためのパスワードを確認します。
テーブル名	イベント・レコードを含むテーブルまたはビューの名前として AUDITDATA と入力します。 テーブル名は、英数字で最大 255 文字までです。テーブル名に使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
選択リスト	テーブルまたはビューのすべてのフィールドを含めるには、* を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。

表 329. *Pirean Access: One* のログ・ソース・パラメーター (続き)

パラメーター	説明
比較フィールド	テーブルに対する照会から次の照会までの間に追加された新しいイベントを特定するため、**TIMESTAMP** を入力します。 比較フィールドは、英数字で最大 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
準備済みステートメントの使用 **(Use Prepared Statements)**	準備済みステートメントを使用する場合はこのチェック・ボックスを選択します。準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度も実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 プリコンパイル・ステートメントを使用しない代替照会手法を使用する場合は、このチェック・ボックスをクリアします。
開始日時	オプション。データベース・ポーリングの開始日時を構成します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。指定子の H および M のない数値の場合は、秒単位のポーリングになります。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
有効	Pirean Access: One のログ・ソースを有効にするには、このチェック・ボックスを選択します。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。Pirean Access: One のアクセス管理イベントと認証イベントが QRadar の「ログ・アクティビティー」タブに表示されます。

第 103 章 PostFix メール転送エージェント

IBM Security QRadar は、ネットワークにインストールされた PostFix メール転送エージェント (MTA) から syslog メール・イベントを収集して分類することができます。

syslog イベントを収集するには、syslog イベントを QRadar に転送するように PostFix MTA インストール済み環境を構成する必要があります。PostFix MTA インストール済み環境から転送される syslog イベントは複数行イベントであるため、QRadar がそれらのイベントを自動的に検出することはありません。QRadar は、PostFix MTA V2.6.6 からの syslog イベントをサポートしています。

PostFix MTA を構成するには、以下の作業を行います。

1. PostFix MTA システムで、メール・イベントを QRadar に転送するように `syslog.conf` を構成します。
2. QRadar システムで、UDP multiline syslog プロトコルを使用するための PostFix MTA のログ・ソースを作成します。
3. QRadar システムで、UDP multiline syslog イベント用に定義したポートにイベントをリダイレクトするように IPtables を構成します。
4. QRadar システムで、PostFix MTA イベントが「ログ・アクティビティー」タブに表示されることを確認します。

複数の PostFix MTA インストール済み環境が存在し、イベントを異なる QRadar システムに転送する場合は、PostFix MTA の複数行 UDP syslog イベントを受け取る QRadar システムごとにログ・ソースおよび IPtables を構成する必要があります。

PostFix Mail Transfer Agent 用の Syslog の構成

イベントを収集するには、メール・イベントを IBM Security QRadar に転送するように PostFix MTA インストール済み環境で Syslog を構成する必要があります。

手順

1. SSH を使用して、root ユーザーとして PostFix MTA インストール済み環境にログインします。
2. 以下のファイルを編集します。

   `/etc/syslog.conf`
3. すべてのメール・イベントを転送するには、以下のコマンドを入力して `-/var/log/maillog/` を IP アドレスに変更します。それ以外の行は変更しないでください。

   `mail.*@<IP address>`

ここで、*<IP address>* は QRadar コンソール、イベント・プロセッサー (Event Processor)、イベント・コレクター (Event Collector)、またはオールインワン・システムの IP アドレスです。

4. ファイルを保存して終了します。
5. 変更内容を保存するため Syslog デーモンを再始動します。

PostFix MTA ログ・ソースの構成

syslog イベントを収集するには、UDP Multiline Syslog プロトコルを使用するように PostFix MTA 用のログ・ソースを構成する必要があります。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで「**PostFix Mail Transfer Agent**」を選択します。
6. 「プロトコル構成」リストで「**UDP** 多重回線 **Syslog (UDP Multiline Syslog)**」を選択します。
7. 以下の値を構成します。

表 *330. PostFix MTA* のログ・ソース・パラメーター

パラメーター	説明
ログ・ソース **ID**	PostFix MTA インストール済み環境を識別するための IP アドレス、ホスト名、または名前を入力します。
Listen ポート	着信 UDP 多重回線 Syslog イベントを受け取るために QRadar が使用するポート番号として **517** と入力します。有効なポート範囲は、1 から 65535 です。 保存済みの構成を編集して新しいポート番号を使用するには、以下のようにします。 1. 「**listen** ポート **(Listen Port)**」フィールドに、UDP 多重回線 Syslog イベント受信用の新しいポート番号を入力します。 2. 「保存」をクリックします。 3. 「管理」タブで、「拡張」 > 「すべての構成のデプロイ」を選択します。 すべてのデプロイが完了したら、QRadar は更新された listen ポートでイベントの受信を開始します。 「すべての構成のデプロイ」をクリックすると、QRadar はすべてのサービスを再始動します。このため、デプロイが完了するまで、イベントとフローのデータ収集に差異が発生します。

表 330. PostFix MTA のログ・ソース・パラメーター (続き)

パラメーター	説明
メッセージ ID のパターン	イベント・ペイロード・メッセージをフィルタリングするために必要な以下の正規表現 (regex) を入力します。 `postfix/.*?[ ¥[]¥d+[ ¥]](?:- - |: )([A-Z0-9]{8,10})`
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。
信頼性	ログ・ソースの「信頼性」を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信ペイロードのエンコード	イベント・ログの解析に必要な文字エンコードを選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
ログ・ソース言語	PostFix MTA により生成されるイベントの言語を選択します。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

多重回線 UDP Syslog イベント用の IPtables の構成

イベントを収集するには、イベントを標準 PostFix MTA ポートから UDP 多重回線プロトコル用のポート 517 にリダイレクトする必要があります。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar にログインします。
2. IPtables ファイルを編集するには、以下のコマンドを入力します。

   ```
   vi /opt/qradar/conf/iptables-nat.post
   ```

3. QRadar に対し、Syslog イベントを UDP ポート 514 から UDP ポート 517 にリダイレクトするように指示するには、以下のコマンドを入力します。

   ```
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port <new-port> -s <IP address>
   ```

   各部分について以下で説明します。

   - *<IP address>* は、PostFix MTA インストール済み環境の IP アドレスです。
   - *<New port>* は、PostFix MTA 用に UDP 多重回線プロトコルで構成されているポート番号です。

   例えば、QRadar と通信する PostFix MTA インストール済み環境が 3 つある場合は、以下のコードを入力できます。

   ```
   -A PREROUTING -p udp --dport 514 -j
   REDIRECT --to-port 517 -s 10.10.10.10 -A PREROUTING -p udp --dport 514 -j
   REDIRECT --to-port 517 -s 10.10.10.11 -A PREROUTING -p udp --dport 514 -j
   REDIRECT --to-port 517 -s 10.10.10.12
   ```

4. IPtables NAT 構成を保存します。

   これで、PostFix MTA インストール済み環境からイベントを受け取るように QRadar コンソールまたはイベント・コレクター (Event Collector)で IPtables を構成することができます。

5. 以下のコマンドを入力して、IPtables ファイルを編集します。

   ```
   vi /opt/qradar/conf/iptables.post
   ```

6. 以下のコマンドを入力して、QRadar に対し、PostFix MTA インストール済み環境からの通信を許可するように指示します。

   ```
   -I QChain 1 -m udp -p udp --src <IP address> --dport <New port> -j
   ACCEPT
   ```

   各部分について以下で説明します。

   - *<IP address>* は、PostFix MTA インストール済み環境の IP アドレスです。
   - *<New port>* は、UDP 多重回線プロトコルで構成されているポート番号です。

   例えば、イベント・コレクター (Event Collector)と通信する PostFix MTA インストール済み環境が 3 つある場合は、以下のコードを入力できます。

   ```
   -I QChain 1 -m udp -p udp --src 10.10.10.10
   --dport 517 -j ACCEPT -I QChain 1 -m udp -p udp
   --src 10.10.10.11 --dport 517 -j ACCEPT -I QChain 1 -m udp -p udp
   --src 10.10.10.12 --dport 517 -j ACCEPT
   ```

7. 変更内容を保存して IPtables を更新するため、以下のコマンドを入力します。

```
./opt/qradar/bin/iptables_update.pl
```

第 104 章 ProFTPd

IBM Security QRadar は、syslog を使用して ProFTP サーバーからイベントを収集できます。

デフォルトでは、ProFTPd は、**auth** (または **authpriv**) 機能を使用して認証関連のメッセージをローカル syslog に記録します。それ以外のロギングは、すべてデーモン機能を使用して実行されます。ProFTPd メッセージを QRadar に記録するには、SyslogFacility ディレクティブを使用してデフォルトの機能を変更してください。

ProFTPd の構成

ProFTPd デバイスで Syslog を構成できます。

手順

1. /etc/proftd.conf ファイルを開きます。
2. LogFormat ディレクティブの下に以下の行を追加します。

   ```
   SyslogFacility <facility>
   ```

   ここで *<facility>* は、**AUTH** (または **AUTHPRIV**)、**CRON**、**DAEMON**、**KERN**、**LPR**、**MAIL**、**NEWS**、**USER**、**UUCP**、**LOCAL0**、**LOCAL1**、**LOCAL2**、**LOCAL3**、**LOCAL4**、**LOCAL5**、**LOCAL6**、**LOCAL7** のいずれかです。
3. ファイルを保存して終了します。
4. /etc/syslog.conf ファイルを開きます。
5. ファイルの終わりに以下の行を追加します。

   ```
   <facility> @<QRadar host>
   ```

   各部分について以下で説明します。

   <facility> は、『ProFTPd の構成』 で選択したファシリティーに一致します。ファシリティーは小文字で入力する必要があります。

   <QRadar host> は、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスです。
6. Syslog と ProFTPd を再始動します。

   ```
   /etc/init.d/syslog restart

   /etc/init.d/proftpd restart
   ```

次のタスク

これで、QRadar でログ・ソースを構成できるようになりました。

ログ・ソースの構成

IBM Security QRadar は、ProFTPd からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

このタスクについて

ProFTPd のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**ProFTPd サーバー (ProFTPd Server)**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   Syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *331. Syslog* パラメーター

パラメーター	説明
ログ・ソース ID	ProFTPd インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

第 105 章 Proofpoint Enterprise Protection and Enterprise Privacy

Proofpoint Enterprise Protection and Enterprise Privacy 用の IBM Security QRadar DSM は、Proofpoint Enterprise Protection and Enterprise Privacy DSM サーバーからイベントを収集することができます。

Proofpoint Enterprise Protection and Enterprise Privacy DSM の仕様を以下の表に示します。

表 332. *Proofpoint Enterprise Protection and Enterprise Privacy DSM* の仕様

仕様	値
製造元	Proofpoint
DSM 名	Proofpoint Enterprise Protection/Enterprise Privacy
RPM ファイル名	`DSM-Proofpoint_Enterprise_Protection/Enterprise_Privacy`*`Qradar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	V7.02 V7.1 V7.2 V7.5 V8.0
プロトコル	Syslog ログ・ファイル
記録されるイベント・タイプ	システム E メール・セキュリティーの脅威の分類 E メールの監査および暗号化
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Proofpoint の Web サイト (https://www.proofpoint.com/us/solutions/products/enterprise-protection)

Proofpoint Enterprise Protection and Enterprise Privacy DSM を QRadar と統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Proofpoint Enterprise Protection and Enterprise Privacy DSM RPM をダウンロードして QRadar コンソールにインストールしてください。

2. Proofpoint Enterprise Protection and Enterprise Privacy のインスタンスごとに、QRadar と通信できるように Proofpoint Enterprise Protection and Enterprise Privacy DSM アプライアンスを構成します。
3. QRadar が Proofpoint Enterprise Protection and Enterprise Privacy ログ・ソースを自動的に検出しない場合は、ネットワーク上の Proofpoint Enterprise and Enterprise Privacy DSM のインスタンスごとにログ・ソースを作成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

IBM Security QRadar との通信のための Proofpoint Enterprise Protection and Enterprise Privacy DSM の構成

Proofpoint Enterprise Protection and Enterprise Privacy DSM からすべての監査ログおよびシステム・イベントを収集するには、IBM Security QRadar を Syslog サーバーとして指定する宛先を追加する必要があります。

手順

1. Proofpoint Enterprise インターフェースにログインします。
2. 「ログとレポート **(Logs and Reports)**」をクリックします。
3. 「ログの設定 **(Log Settings)**」をクリックします。
4. 「リモート・ログ設定 (Remote Log Settings)」ペインで、Syslog 通信を有効にするため以下のオプションを構成します。
   a. 通信プロトコルとして「**Syslog**」を選択します。
5. QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
6. 「ポート **(Port)**」フィールドに、Syslog 通信用のポート番号として 514 と入力します。
7. 「**Syslog** フィルターの有効化 **(Syslog Filter Enable)**」リストで「オン **(On)**」を選択します。
8. 「ファシリティー **(Facility)**」リストで「**local1**」を選択します。
9. 「レベル **(Level)**」リストで「通知 **(Information)**」を選択します。
10. 「**Syslog MTA** の有効化 **(Syslog MTA Enable)**」リストで「オン **(On)**」を選択します。
11. 「保存」をクリックします。

Proofpoint Enterprise Protection and Enterprise Privacy ログ・ソースの構成

IBM Security QRadar は、Proofpoint Enterprise Protection and Enterprise Privacy アプライアンスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Proofpoint Enterprise Protection/Enterprise Privacy**」を選択します。
9. **Syslog** プロトコルを構成する場合は、それを「プロトコル構成」リストから選択し、以下の値を構成します。

表 *333. Syslog* パラメーター

パラメーター	説明
ログ・ソース ID	ログ・ソースの IP アドレスまたはホスト名。Proofpoint Enterprise Protection and Enterprise Privacy インストール済み環境からのイベントの ID として使用されます。 複数のインストール済み環境がある場合には、作成する追加の各ログ・ソースに対して、IP アドレスまたはホスト名などの固有 ID を含めます。

10. **Log File** プロトコルを構成する場合は、それを「プロトコル構成」リストから選択し、以下の値を構成します。

表 *334.* ログ・ファイル・パラメーター

パラメーター	説明
ログ・ソース ID	ログ・ソースの IP アドレスまたはホスト名を入力します。ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。

表 334. ログ・ファイル・パラメーター (続き)

パラメーター	説明
サービス・タイプ	リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを、リストから選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート IP またはホスト名	Proofpoint Enterprise Protection and Enterprise Privacy システムの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。サービス・タイプを FTP として構成する場合、デフォルトは 21 です。サービス・タイプを SFTP または SCP として構成する場合、デフォルトは 22 です。 有効な範囲は、1 から 65535 です。
リモート・ユーザー	Proofpoint Enterprise Protection and Enterprise Privacy システムにログインするのに必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	Proofpoint Enterprise Protection and Enterprise Privacy システムにログインするのに必要なパスワードを入力します。
パスワードの確認	Proofpoint Enterprise Protection and Enterprise Privacy システムにログインするのに必要なリモート・パスワードを確認します。
SSH 鍵ファイル	SCP または SFTP を「サービス・タイプ **(Service Type)**」フィールドから選択する場合、SSH 秘密鍵ファイルへのディレクトリー・パスを定義できます。 SSH 秘密鍵ファイルを使用する場合、「リモート・パスワード **(Remote Password)**」フィールドは無視できます。
リモート・ディレクトリー	ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。

表 334. ログ・ファイル・パラメーター (続き)

パラメーター	説明
再帰的 (Recursive)	サブフォルダーからもファイル・パターンを検索したい場合は、このチェック・ボックスを選択します。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」パラメーターは使用されません。デフォルトでは、このチェック・ボックスはクリアされています。
FTP ファイル・パターン	SFTP または FTP をサービス・タイプとして選択する場合、このオプションによって、リモート・ディレクトリーで指定されたファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 別の例として、ファイル名にキーワード「_filter」が含まれているすべての Syslog ファイルを取得する場合は、`.*_filter.*¥.syslog` と入力します。 このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、FTP をサービス・タイプとして選択した場合にのみ表示されます。「FTP 転送モード」パラメーターにより、FTP を介してログ・ファイルを取得するときのファイル転送モードを定義できます。 リストから、このログ・ソースに適用する転送モードを選択します。 • バイナリー - バイナリー・データ・ファイル、または圧縮された .zip、.gzip、.tar、.tar + .gzip のアーカイブ・ファイルを必要とするログ・ソースには、「バイナリー」を選択します。 • ASCII - ASCII FTP ファイル転送を必要とするログ・ソースには、ASCII を選択します。 ASCII を転送モードとして使用する場合、「プロセッサー」フィールドには「なし」を、「イベント・ジェネレーター **(Event Generator)**」 フィールドには「**LINEBYLINE**」を選択する必要があります。
SCP リモート・ファイル	SCP をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。

表 334. ログ・ファイル・パラメーター (続き)

パラメーター	説明
開始時刻	処理を開始する時刻を入力します。このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し (Recurrence)	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、ディレクトリーを 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リモート・ホストにあるファイルが .zip、.gzip、.tar、または .tar + .gzip のアーカイブ・フォーマットで保管されている場合、アーカイブを展開して内容を処理することができるプロセッサーを選択します。
以前に処理したファイルを無視 (Ignore Previously Processed File(s))	既に処理済みのファイルを追跡し、2 回目のファイルの処理を希望しない場合は、このチェック・ボックスを選択します。これは FTP および SFTP のサービス・タイプにのみ適用されます。

表 *334.* ログ・ファイル・パラメーター *(*続き*)*

パラメーター	説明
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar システム上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。このチェック・ボックスはクリアしたままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。これによりファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター (Event Generator)	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LINEBYLINE)**」を選択します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。 Proofpoint Enterprise Protection and Enterprise Privacy により QRadar に転送されるイベントは、「ログ・アクティビティー」タブに表示されます。

第 106 章 Radware

IBM Security QRadar は Radware デバイスを幅広くサポートしています。

Radware AppWall

Radware AppWall 用の IBM Security QRadar DSM は、Radware AppWall アプライアンスからログを収集します。

以下の表は、Radware AppWall DSM の仕様を示しています。

表 *335. Radware AppWall DSM* の仕様

仕様	値
製造元	Radware
DSM 名	Radware AppWall
RPM ファイル名	DSM-RadwareAppWall-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	V6.5.2
プロトコル	Syslog
イベント・フォーマット	Vision ログ
記録されるイベント・タイプ	管理 監査 学習 セキュリティー システム
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Radware Web サイト (http://www.radware.com)

Radware AppWall を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの Radware AppWall DSM RPM をダウンロードして、QRadar コンソールにインストールします。
2. ログを QRadar に送信するように Radware AppWall デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Radware AppWall ログ・ソースを追加してください。以下の表は、Radware AppWall イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 336. *Radware AppWall* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Radware AppWall
プロトコル構成	Syslog

注**:** RadWare AppWall デバイスには、TCP Syslog ペイロードのデフォルトの最大長である 4096 バイトより長いイベント・ペイロードが存在する可能性があります。この超過分が原因で、QRadar によって、イベント・ペイロードが複数のイベントに分割される可能性があります。この振る舞いを防止するために、TCP Syslog ペイロードの最大長を増やしてください。パフォーマンスを最適化するには、値をまず 8192 バイトに構成してください。RadWare AppWall イベントの最大長は、14019 バイトです。

『QRadar との通信のための Radware AppWall の構成』手順のステップ 6 を実行すると、Radware AppWall デバイスからイベントを受信するように QRadar が構成されていることを確認できます。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

『QRadar との通信のための Radware AppWall の構成』
ログを IBM Security QRadar に送信するように Radware AppWall デバイスを構成します。AppWall ログを QRadar と統合するには、Vision ログ・イベント・フォーマットを使用します。

915 ページの『Radware AppWall の TCP Syslog ペイロードの最大長の増大』
IBM Security QRadar で、Radware AppWall アプライアンスの TCP Syslog ペイロードの最大長を増やします。

QRadar との通信のための Radware AppWall の構成

ログを IBM Security QRadar に送信するように Radware AppWall デバイスを構成します。AppWall ログを QRadar と統合するには、Vision ログ・イベント・フォーマットを使用します。

手順

1. Radware AppWall コンソールにログインします。
2. メニュー・バーから「構成ビュー **(Configuration View)**」を選択します。
3. ウィンドウの左側のツリー・ビュー・ペインで、「**appwall Gateway**」 > 「**Services**」 > 「**Vision Support**」をクリックします。
4. ウィンドウの右側の「**Server List**」タブで、「Server List」ペイン内の追加アイコン **(+)** をクリックします。
5. 「Add Vision Server」ウィンドウで、次のパラメーターを構成します。

パラメーター	値
Address	QRadar コンソールの IP アドレス。
ポート	514
バージョン	リストから最新バージョンを選択します。リストの最後の項目です。

6. 「**Check**」をクリックして、AppWall が QRadar に正常に接続できることを確認します。
7. 「**Submit**」と「**Save**」をクリックします。
8. 「適用 **(Apply)**」 > 「**OK**」をクリックします。

Radware AppWall の TCP Syslog ペイロードの最大長の増大

IBM Security QRadar で、Radware AppWall アプライアンスの TCP Syslog ペイロードの最大長を増やします。

始める前に

注**:** RadWare AppWall デバイスには、TCP Syslog ペイロードのデフォルトの最大長である 4096 バイトより長いイベント・ペイロードが存在する可能性があります。この超過分が原因で、QRadar によって、イベント・ペイロードが複数のイベントに分割される可能性があります。この振る舞いを防止するために、TCP Syslog ペイロードの最大長を増やしてください。パフォーマンスを最適化するには、値をまず 8192 バイトに構成してください。RadWare AppWall イベントの最大長は、14019 バイトです。

手順

1. QRadar V7.2.6 に対して TCP Syslog ペイロードの最大長を増やす場合、次の手順に従います。
   a. QRadar コンソールに管理者としてログインします。
   b. 「管理」タブから「システム設定」をクリックします。
   c. 「詳細 **(Advanced)**」をクリックします。
   d. 「**TCP Syslog** ペイロードの最大長」フィールドに、8192 を入力します。
   e. 「保存」をクリックします。
   f. 「管理」タブから「変更のデプロイ」をクリックします。
2. QRadar V7.2.5 以前に対して TCP Syslog ペイロードの最大長を増やす場合、次の手順に従います。
   a. SSH を使用して、QRadar コンソールにログインします。
   b. `/opt/qradar/conf/templates/configservice/pluggablesources/` ディレクトリーに移動し、`TCPSyslog.vm` ファイルを編集します。
   c. **`MaxPayload`** パラメーターの値として 8192 と入力します。

      例: `<parameter type=MaxPayload>8192</parameter>`。
   d. `TCPSyslog.vm` ファイルを保存します。
   e. QRadar コンソールに管理者としてログインします。

f. 「管理」タブで「拡張」 > 「すべての構成のデプロイ」をクリックします。

Radware DefensePro

IBM Security QRadar 用の Radware DefensePro DSM は syslog を使用してイベントを受け取ります。イベント・トラップを syslog サーバーにミラーリングすることもできます。

Radware DefensePro デバイスと統合するように QRadar を構成する前に、syslog イベントを QRadar に転送するように Radware DefensePro デバイスを構成する必要があります。「デバイス **(Device)**」**>**「トラップおよび **SMTP** のオプション **(Trap and SMTP option)**」を使用して、適切な情報を構成する必要があります。

Radware デバイスで生成されたトラップは、すべて指定の syslog サーバーにミラーリングされます。最新の Radware Syslog サーバーでは、状況およびイベント・ログ・サーバーのアドレスを定義することができます。

通知基準 (ファシリティーや重大度など) を追加で定義することもできます。基準は、以下のように数値によって表します。

- 「ファシリティー **(Facility)**」 は、送信側が使用するデバイスのタイプを示すユーザー定義の値です。この基準は、デバイスが syslog メッセージを送信するときに適用されます。デフォルト値は 21 であり、Local Use 6 を意味します。
- 重大度は、報告されたイベントの重要度や影響を示します。重大度は、送信されるメッセージごとに、デバイスによって動的に決定されます。

「Security Settings」ウィンドウでは、接続および保護/セキュリティー設定を使用して、セキュリティー・レポート機能を有効化する必要があります。syslog へのセキュリティー報告を有効にして、重大度 (syslog リスク) を構成する必要があります。

これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Radware DefensePro からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

このタスクについて

Radware DefensePro のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。

4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Radware DefensePro**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   Syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *337. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Radware DefensePro インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

第 107 章 Raz-Lee iSecurity

IBM Security QRadar は、IBM iSeries® 上の Raz-Lee iSecurity インストール済み環境から転送されるログ・イベント拡張フォーマット (LEEF) イベントを収集して解析します。イベントは IBM AS/400 iSeries DSM で解析されて分類されます。

QRadar は、iSecurity Firewall V15.7 および iSecurity Audit V11.7 に対する Raz-Lee iSecurity インストール済み環境からのイベントをサポートしています。

以下の表は、Raz-Lee iSecurity インストール済み環境用の IBM iSeries® DSM の仕様を示しています。

表 *338. Raz-Lee iSecurity* 用の *IBM AS/400 iSeries DSM* の仕様

仕様	値
製造元	IBM
DSM 名	IBM AS/400 iSeries
RPM ファイル名	`DSM-IBMiSeries-`*`QRadar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	iSecurity Firewall V15.7 iSecurity Audit V11.7
プロトコル	Syslog
イベント・フォーマット	LEEF
記録されるイベント・タイプ	セキュリティー、コンプライアンス、および監査のすべてのイベント。
自動的に検出?	はい
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	IBM Web サイト (http://www.ibm.com)

QRadar と通信するための Raz-Lee iSecurity の構成

セキュリティー・イベント、コンプライアンス・イベント、および監査イベントを収集するには、ログ・イベント拡張フォーマット (LEEF) Syslog イベントを IBM Security QRadar に転送するように Raz-Lee iSecurity インストール済み環境を構成します。

手順

1. IBM System i のコマンド・ライン・インターフェースにログインします。
2. コマンド・ラインで、`STRAUD` と入力して「監査 **(Audit)**」メニュー・オプションにアクセスします。
3. 「監査 **(Audit)**」メニューから「**81.** システム構成 **(81. System Configuration)**」を選択します。

4. 「**iSecurity/**基本システム構成 **(iSecurity/Base System Configuration)**」メニューで「**32. SIEM 1**」を選択します。
5. **32.SIEM 1** のパラメーター値を構成します。

32. SIEM 1 のパラメーター値の詳細**:**

表 *339. 32.SIEM 1* のパラメーター値

パラメーター	値
SIEM 1 名	QRadar と入力します。
ポート	Syslog メッセージの送信に使用するポートを入力します。デフォルトのポートは 514 (Syslog 標準) です。
SYSLOG タイプ	UDP の場合、1 と入力します。
宛先アドレス	QRadar のIP アドレスを入力します。
自動送信の重大度範囲 (Severity range to auto send)	メッセージの重大度レベルを 0 から 7 までの範囲で入力します。例えば、すべての Syslog メッセージを送信する場合、**7** と入力します。
使用するファシリティー (Facility to use)	Syslog のファシリティー・レベルを 0 から 23 までの範囲で入力します。
メッセージ構造 (Message structure)	*LEEF と入力します。
データを CCSID に変換 (Convert data to CCSID)	「データを **CCSID** に変換 **(Convert data to CCSID)**」フィールドに 0 と入力します。これは、デフォルトの文字変換です。
最大長 (Maximum Length)	1024 と入力します。

6. 「**iSecurity/**基本システム構成 **(iSecurity/Base System Configuration)**」メニューで「**31.** メイン・コントロール **(31. Main Control)**」を選択します。
7. 「**31.** メイン・コントロール **(31. Main Control)**」パラメーター値を構成します。

「**31.** メイン・コントロール **(31. Main Control)**」パラメーター値の詳細**:**

表 *340.* 「**31.** メイン・コントロール **(31. Main Control)**」パラメーター値

パラメーター	値
送信前にルールを実行 (Run rules before sending)	送信するイベントを処理するには、Y と入力します。 すべてのイベントを送信するには、N と入力します。
SIEM 1: QRadar	Y と入力します。
JSON メッセージの送信 (DAM の場合) (Send JSON messages (for DAM))	N と入力します。
操作のみとして (As only operation)	N と入力します。

8. 「ファイアウォール」オプションを構成するために、コマンド・ラインで、STRFW と入力してメニュー・オプションにアクセスします。

9. 「ファイアウォール」メニューで「**81.** システム構成 **(81. System Configuration)**」を選択します。
10. 「**iSecurity (**パート **1)** グローバル・パラメーター**: (iSecurity (part 1) Global Parameters:)**」メニューで「**72. SIEM 1**」を選択します。
11. 「**72.SIEM 1**」パラメーター値を構成します。

「**72. SIEM 1**」パラメーター値の詳細**:**

表 *341.* 「**72.SIEM 1**」パラメーター値

パラメーター	値
SIEM 1 名	`QRadar` と入力します。
ポート	Syslog メッセージの送信に使用するポートを入力します。デフォルトのポートは 514 (Syslog 標準) です。
SYSLOG タイプ	UDP Syslog タイプの場合、1 と入力します。
FYI モードで送信 (Send in FYI mode)	`N` と入力します。
宛先アドレス	QRadar コンソールの IP アドレスを入力します。
自動送信の重大度範囲 (Severity range to auto send)	重大度レベルを 0 から 7 までの範囲で入力します。
使用するファシリティー (Facility to use)	ファシリティー・レベルを入力します。
メッセージ構造 (Message structure)	`*LEEF` と入力します。
データを CCSID に変換 (Convert data to CCSID)	`0` と入力します。
最大長 (Maximum Length)	`1024` と入力します。

12. 「**iSecurity (**パート **1)** グローバル・パラメーター**: (iSecurity (part 1) Global Parameters:)**」メニューで「**71.** メイン・コントロール **(71. Main Control)**」を選択します。
13. 「**71.** メイン・コントロール **(71. Main Control)**」パラメーター値を構成します。

「**71.** メイン・コントロール **(71. Main Control)**」パラメーター値の詳細**:**

表 *342.* 「**71.** メイン・コントロール **(71. Main Control)**」パラメーター値

パラメーター	値
SIEM 1: QRadar	`2` と入力します。
JSON メッセージの送信 (DAM の場合) (Send JSON messages (for DAM))	`0` と入力します。

タスクの結果

Raz-Lee iSecurity によって転送される Syslog LEEF イベントは、QRadar DSM for IBM AS/400 iSeries により自動的に検出されます。ほとんどの場合、いくつかのイベントが検出されると、ログ・ソースが QRadar で自動的に作成されます。

イベント速度が低い場合は、QRadar で Raz-Lee iSecurity のログ・ソースを手動で構成できます。ログ・ソースが自動的に検出されて識別されるまで、「ログ・アクティビティー」タブでイベント・タイプは「不明」と表示されます。自動的に検出されたログ・ソースは、「ログ・ソース」アイコンをクリックすることで、「管理」タブに表示されます。

Raz-Lee iSecurity のログ・ソースの構成

IBM Security QRadar は、Raz-Lee iSecurity から転送される Syslog LEEF イベントに対して、ログ・ソースの検出と作成を自動的に実行します。ログ・ソースが自動的に検出されない場合は、手動でログ・ソースを作成できます。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「**IBM AS/400 iSeries**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。
8. Syslog プロトコル値を構成します。

Syslog プロトコル・パラメーターの詳細**:**

表 *343. Syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Raz-Lee iSecurity デバイスからイベントを送信するログ・ソースの IP アドレスまたはホスト名。
有効	このチェック・ボックスはデフォルトで選択されます。
信頼性	ログ・ソースの「信頼性」。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
イベントの統合	デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信ペイロードのエンコード	ログの解析と保管を行うための「受信ペイロード・エンコーダー」を選択します。

表 *343. Syslog* プロトコルのパラメーター *(*続き*)*

パラメーター	説明
イベント・ペイロードの保管	デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

第 108 章 Redback ASE

IBM Security QRadar 用の Redback ASE DSM は syslog を使用してイベントを受け取ります。

Redback ASE デバイスは、Redback デバイス・コンソールまたは QRadar と統合されたログ・サーバーにログ・メッセージを送信し、デプロイメント固有のレポートを生成することができます。QRadar で Redback ASE デバイスを構成する前に、syslog イベントを転送するようにデバイスを構成する必要があります。

Redback ASE の構成

Syslog イベントを IBM Security QRadar に送信するようにデバイスを構成できます。

手順

1. Redback ASE デバイスのユーザー・インターフェースにログインします。
2. CLI 構成モードを開始します。
3. グローバル構成モードで、セキュリティー・サービスのデフォルト設定を構成します。

   ```
   asp security default
   ```

4. ASP セキュリティーのデフォルト構成モードでは、ログ・サーバーの IP アドレスとオプションのトランスポート・プロトコルを構成します。

   ```
   log server <IP address> transport udp port 9345
   ```

   ここで、*<IP address>* は QRadar の IP アドレスです。
5. ログ・メッセージで送信元 IP アドレスとして使用する IP アドレスを構成します。

   ```
   log source <source IP address>
   ```

   ここで、*<source IP address>* はコンテキスト・ローカルのループバック・インターフェースの IP アドレスです。
6. トランザクションをコミットします。

   Redback ASE デバイスの構成について詳しくは、ベンダーの資料を参照してください。

   例えば、次のように構成するとします。
   - ログ・ソース・サーバーの IP アドレス: 10.172.55.55
   - デフォルトのトランスポート・プロトコル: UDP
   - デフォルトのサーバー・ポート: 514

ログ・メッセージに使用される送信元 IP アドレスは 10.192.22.24 です。このアドレスは、コンテキスト・ローカルのループバック・インターフェースの IP アドレスでなければなりません。

```
asp security default log server 10.172.55.55 log source 10.192.22.24
```

次のタスク

これで、QRadar でログ・ソースを構成できるようになりました。

ログ・ソースの構成

IBM Security QRadar は、Redback ASE からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

このタスクについて

Redback ASE のログ・ソースを手動で構成するには、以下のようにします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Redback ASE**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   Syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *344. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Redback ASE アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

第 109 章 Resolution1 CyberSecurity

Resolution1 CyberSecurity は、以前は AccessData InSight と呼ばれていました。Resolution1 CyberSecurity DSM for IBM Security QRadar は、Resolution1 CyberSecurity デバイスからイベント・ログを収集します。

以下の表は、Resolution1 CyberSecurity DSM の仕様を示しています。

表 345. *Resolution1 CyberSecurity DSM* の仕様

仕様	値
製造元	Resolution1
DSM 名	Resolution1 CyberSecurity
RPM ファイル名	DSM-Resolution1CyberSecurity-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	V2
イベント・フォーマット	ログ・ファイル
QRadar で記録されるイベント・タイプ	揮発性データ メモリー分析データ メモリー獲得データ 収集データ ソフトウェア・インベントリー プロセス・ダンプ・データ 脅威スキャン・データ エージェント修復データ
自動的に検出?	いいえ
ID を含む?	いいえ

Resolution1 CyberSecurity から QRadar にイベントを送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードしてください。
   - LogFileProtocol
   - DSMCommon
   - Resolution1 CyberSecurity DSM
2. QRadar と通信するように Resolution1 CyberSecurity デバイスを構成します。
3. QRadar コンソールで、Resolution1 CyberSecurity ログ・ソースを作成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『QRadar との通信のための Resolution1 CyberSecurity デバイスの構成』
Resolution1 CyberSecurity イベントを収集するには、LEEF 形式でイベント・ログを生成するようにサード・パーティー・デバイスを構成する必要があります。
Resolution1 CyberSecurity で LEEF ファイルを転送するために FTP サイトを作成する必要もあります。そうすれば、QRadar で FTP サーバーからログをプルすることができます。

929 ページの『QRadar コンソールへの Resolution1 CyberSecurity のログ・ソースの追加』
QRadar は、Resolution1 CyberSecurity のログ・ソースを自動的に検出することはありません。手動でログ・ソースを追加する必要があります。

QRadar との通信のための Resolution1 CyberSecurity デバイスの構成

Resolution1 CyberSecurity イベントを収集するには、LEEF 形式でイベント・ログを生成するようにサード・パーティー・デバイスを構成する必要があります。
Resolution1 CyberSecurity で LEEF ファイルを転送するために FTP サイトを作成する必要もあります。そうすれば、QRadar で FTP サーバーからログをプルすることができます。

手順

1. Resolution1 CyberSecurity デバイスにログインします。
2. `ADGIntegrationServiceHost.exe.config` ファイルを開きます。このファイルは、`C:¥Program Files¥AccessData¥eDiscovery¥Integration Services` ディレクトリーにあります。
3. ファイル内のテキストを以下の行に一致するように変更します。

```
<Option Name="Version" Value="2.0" />
<Option Name="Version" Value="2.0" />
<Option Name="OutputFormat" Value="LEEF" />
<Option Name="LogOnly" Value="1" />
<Option Name="OutputPath" Value="C:¥CIRT¥logs" />
```

4. Resolution1 サード・パーティー統合サービスを再始動します。
5. 以下のようにして、`C:¥CIRT¥logs` 出力フォルダー用の FTP サイトを作成します。
   a. Internet Information Services Manager (IIS) を開きます。
   b. 「サイト」タブを右クリックし、「**FTP** サイトの追加 **(Add FTP Site)**」をクリックします。
   c. FTP サイトの名前を指定し、生成済みの LEEF ファイルのロケーションとして、`C:¥CIRT¥logs` と入力します。
   d. Web サービスを再始動します。

QRadar コンソールへの Resolution1 CyberSecurity のログ・ソースの追加

QRadar は、Resolution1 CyberSecurity のログ・ソースを自動的に検出することはありません。手動でログ・ソースを追加する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース **ID**」フィールドに、Resolution1 CyberSecurity デバイスの IP アドレスまたはホスト名を入力します。
7. 「ログ・ソース・タイプ」リストで「**Resolution1 CyberSecurity**」を選択します。
8. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
9. 残りのパラメーターを構成します。
10. 「保存」をクリックします。

第 110 章 Riverbed

IBM Security QRadar は複数の Riverbed DSM をサポートしています。

Riverbed SteelCentral NetProfiler (Cascade Profiler) Audit

Riverbed SteelCentral NetProfiler Audit 用の IBM Security QRadar DSM は、Riverbed SteelCentral NetProfiler システムから監査ログを収集します。この製品は、*Cascade Profiler* とも呼ばれています。

以下の表は、Riverbed SteelCentral NetProfiler DSM の仕様を示しています。

表 *346. Riverbed SteelCentral NetProfiler* の仕様

仕様	値
製造元	Riverbed
DSM 名	SteelCentral NetProfiler Audit
RPM ファイル名	DSM-RiverbedSteelCentralNetProfilerAudit-*Qradar_version-build_number*.noarch.rpm
イベント・フォーマット	ログ・ファイル・プロトコル
記録されるイベント・タイプ	監査イベント
自動的に検出?	いいえ
ID を含む?	はい
カスタム・プロパティーを含む?	いいえ
その他の情報	Riverbed Web サイト (http://www.riverbed.com/)

Riverbed SteelCentral NetProfiler Audit を QRadar と統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Protocol-LogFile RPM
   - Riverbed SteelCentral NetProfiler Audit RPM
2. Riverbed ホストに監査レポート・テンプレートを作成してサード・パーティー製ホストを構成し、そのテンプレートを使用して監査ファイルを生成します。932 ページの『Riverbed SteelCentral NetProfiler レポート・テンプレートの作成と監査ファイルの生成』を参照してください。
3. QRadar コンソール上でログ・ソースを作成します。このログ・ソースにより、QRadar がサード・パーティー製ホストにアクセスして監査ファイルを取得することができます。Riverbed 固有のパラメーターを定義するには以下の表の内容を使用します。

表 *347. Riverbed SteelCentral NetProfiler* ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース・タイプ	Riverbed SteelCentral NetProfiler Audit
プロトコル構成	ログ・ファイル

表 347. *Riverbed SteelCentral NetProfiler* ログ・ソース・パラメーター (続き)

パラメーター	説明
リモート IP またはホスト名	生成された監査ファイルを格納するサード・パーティー製ホストの IP アドレスまたはホスト名。
リモート・ユーザー	ホストにアクセス可能なアカウントのユーザー名。
リモート・パスワード	ユーザー・アカウントのパスワード。
リモート・ディレクトリー	生成された監査ファイルを格納するサード・パーティー製ホスト上の絶対ファイル・パス。
FTP ファイル・パターン	監査ファイルの名前に一致する正規表現パターン。
繰り返し (Recurrence)	繰り返しは、リモート・ホストで `SteelScript for Python` SDK スクリプトを実行する頻度に一致していなければなりません。
イベント・ジェネレーター (Event Generator)	行比較機能
行比較機能の正規表現 (Line Matcher RegEx)	`^¥d+/¥d+/¥d+ ¥d+:¥d+,`

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Riverbed SteelCentral NetProfiler レポート・テンプレートの作成と監査ファイルの生成

Riverbed SteelCentral NetProfiler と QRadar の統合に向けて準備するため、Riverbed SteelCentral NetProfiler でレポート・テンプレートを作成し、サード・パーティー・ホストを使用して監査ファイルを生成します。サード・パーティー・ホストは、Riverbed SteelCentral NetProfiler または QRadar に使用するホスト以外のシステムでなければなりません。

始める前に

監査レポートの実行に使用するサード・パーティー・ホストに、以下のアイテムがインストールされていることを確認します。

Python

Python Web サイト (https://www.python.org/download/) から Python をダウンロードしてインストールします。

SteelScript for Python

Riverbed SteelScript for Python Web サイト (https://support.riverbed.com/apis/steelscript/index.html) から `SteelScript for Python` SDK をダウンロードしてインストールします。このスクリプトにより、監査ファイルが CSV フォーマットで生成され、ダウンロードされます。定期的にこのスクリプトを実行する必要があります。

手順

1. 監査ファイル・レポート・テンプレートを定義します。
   a. Riverbed SteelCentral NetProfiler ホスト・ユーザー・インターフェースにログインします。
   b. 「システム **(System)**」 > 「監査証跡 **(Audit Trail)**」を選択します。
   c. 監査ファイルに含める条件を選択します。
   d. 時間フレームを選択します。
   e. ウィンドウの右側で「テンプレート **(Template)**」をクリックします。
   f. 「名前を付けて保存/スケジュール **(Save As/Schedule)**」を選択します。
   g. レポート・テンプレートの名前を入力します。
2. レポート・テンプレートを実行して監査ファイルを生成するには、以下の手順を実行します。
   a. Python をインストールしたサード・パーティー・ホストにログインします。
   b. 以下のコマンドを入力します。

```
$ python ./get_template_as_csv.py  <riverbed_host_name>
  -u admin -p admin -t "<report_template_name>"  -o
<absolute_path_to_target file>
```

   ヒント: レポート・テンプレートの名前とファイル・パスを記録します。この名前は、レポート・テンプレートを実行する際、および QRadar インターフェースでログ・ソースを構成する際に必要です。

Riverbed SteelCentral NetProfiler (Cascade Profiler) アラート

Riverbed SteelCentral NetProfiler 用の IBM Security QRadar DSM は、Riverbed SteelCentral NetProfiler システムからアラート・ログを収集します。この製品は、*Cascade Profiler* とも呼ばれています。

以下の表は、Riverbed SteelCentral NetProfiler DSM の仕様を示しています。

表 *348. Riverbed SteelCentral NetProfiler* の仕様

仕様	値
製造元	Riverbed
DSM 名	SteelCentral NetProfiler
RPM ファイル名	DSM-RiverbedSteelCentralNetProfiler-*Qradar_version-build_number*.noarch.rpm
イベント・フォーマット	JDBC
記録されるイベント・タイプ	アラート・イベント
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Riverbed Web サイト (http://www.riverbed.com/)

Riverbed SteelCentral NetProfiler を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Protocol-JDBC RPM
   - Riverbed SteelCentral NetProfiler RPM
2. QRadar と通信するように Riverbed SteelCentral NetProfiler システムを構成します。
3. QRadar コンソール上でログ・ソースを作成します。Riverbed 固有のパラメーターを定義するには以下の表の内容を使用します。

表 *349. Riverbed SteelCentral NetProfiler* ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース・タイプ	**Riverbed SteelCentral NetProfiler**
プロトコル構成	**JDBC**
データベース名	Riverbed データベースの実際の名前を入力する必要があります。ほとんどの構成では、データベース名は `mazu` です。 **ヒント:** Riverbed データベースの実際の名前を確認してください。
テーブル名	`events.export_csv_view`
ユーザー名	Riverbed SteelCentral NetProfiler システムの PostgreSQL データベースにアクセスするように構成されたアカウントのユーザー名。
比較可能フィールド (Comparable Field)	`start_time`
ポーリング間隔 (Polling Interval)	**5M**

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信できるように Riverbed SteelCentral NetProfiler システムを構成する

Riverbed SteelCentral NetProfiler アラート・イベントを収集するには、Riverbed SteelCentral NetProfiler システムを構成して、QRadar が PostgreSQL データベースからイベントを取得できるようにする必要があります。

手順

1. Riverbed SteelCentral NetProfiler ホスト・ユーザー・インターフェースにログインします。
2. 「構成 **(Configuration)**」>「アプライアンス・セキュリティー **(Appliance Security)**」>「セキュリティー・コンプライアンス **(Security Compliance)**」を選択します。
3. 「**ODBC** アクセスを有効にする **(Enable ODBC Access)**」チェック・ボックスにチェック・マークを付けます。

4. 「構成 **(Configuration)**」>「アカウント管理 **(Account Management)**」>「ユーザー・アカウント **(User Accounts)**」を選択します。
5. QRadar が PostgreSQL データベースにアクセスするために使用できるアカウントを追加します。

第 111 章 RSA Authentication Manager

RSA Authentication Manager DSM を使用すると、Syslog またはログ・ファイル・プロトコルを使用して、IBM Security QRadar と RSA Authentication Manager 6.x または 7.x を統合できます。RSA Authentication Manager 8.x は Syslog のみを使用します。

RSA Authentication Manager と統合するように QRadar を構成する前に、次の構成設定を選択します。

- 『RSA Authentication Manager 6.x、7.x および 8.x の Syslog の構成』
- 939 ページの『RSA Authentication Manager 6.x および 7.x のログ・ファイル・プロトコルの構成』

注: syslog を構成する前に、最新のホット・フィックスを、RSA Authentication Manager 7.1 のプライマリー、レプリカ、ノード、データベース、および Radius の各インストールに適用する必要があります。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

RSA Authentication Manager 6.x、7.x および 8.x の Syslog の構成

syslog を使用して RSA Authentication Manager 6.x、7.x および 8.x を構成する手順は、ご使用の RSA Authentication Manager または SecureID 3.0 アプライアンスでのオペレーティング・システムのバージョンにより異なります。

RSA Authentication Manager on Linux を使用している場合は、『Linux の構成』を参照してください。

RSA Authentication Manager on Windows を使用している場合は、938 ページの『Windows の構成』を参照してください。

Linux の構成

Linux ベースのオペレーティング・システム上で Syslog 用に RSA Authentication Manager を構成するには、以下のようにします。

手順

1. RSA Security Console コマンド・ライン・インターフェース (CLI) にログインします。

2. ご使用のオペレーティング・システムに基づいて、編集する以下のファイルを開きます。

   ```
   /usr/local/RSASecurity/RSAAuthenticationManager/utils/resources/
   ims.properties
   ```

3. 以下の項目を ims.properties ファイルに追加します。

   ```
   ims.logging.audit.admin.syslog_host = <IP address>
   ims.logging.audit.admin.use_os_logger = true
   ims.logging.audit.runtime.syslog_host = <IP address>
   ims.logging.audit.runtime.use_os_logger = true
   ims.logging.system.syslog_host = <IP address>
   ims.logging.system.use_os_logger = true
   ```

   ここで *<IP address>* は、IBM Security QRadar の IP アドレスまたはホスト名です。

4. ims.properties ファイルを保存します。
5. 編集する以下のファイルを開きます。

   ```
   /etc/syslog.conf
   ```

6. 以下のコマンドを入力して、QRadar を Syslog 項目として追加します。

   ```
   *.* @<IP address>
   ```

   ここで *<IP address>* は、QRadar の IP アドレスまたはホスト名です。

7. 以下のコマンドを入力して、Linux の Syslog サービスを再始動します。

   ```
   service syslog restart
   ```

8. QRadar でログ・ソースとプロトコルを構成できます。RSA Authentication Manager からイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**RSA Authentication Manager**」オプションを選択します。

   Syslog 転送の構成について詳しくは、*RSA Authentication Manager* の資料 を参照してください。

Windows の構成

Microsoft Windows を使用して Syslog 用に RSA Authentication Manager を構成するには、以下のようにします。

手順

1. RSA Security Console をホストするシステムにログインします。
2. ご使用のオペレーティング・システムに基づいて、編集する以下のファイルを開きます。

   ```
   /Program Files/RSASecurity/RSAAuthenticationManager/utils/resources/
   ims.properties
   ```

3. 以下の項目を ims.properties ファイルに追加します。

```
ims.logging.audit.admin.syslog_host = <IP address>
ims.logging.audit.admin.use_os_logger = true
ims.logging.audit.runtime.syslog_host = <IP address>
ims.logging.audit.runtime.use_os_logger = true
ims.logging.system.syslog_host = <IP address>
ims.logging.system.use_os_logger = true
```

ここで *<IP address>* は、QRadar の IP アドレスまたはホスト名です。

4. `ims.properties` ファイルを保存します。
5. RSA サービスを再始動します。

これで、QRadar でログ・ソースを構成する準備ができました。

6. RSA Authentication Manager デバイスからイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**RSA Authentication Manager**」オプションを選択します。

Syslog 転送の構成について詳しくは、*RSA Authentication Manager* の資料 を参照してください。

RSA Authentication Manager 6.x および 7.x のログ・ファイル・プロトコルの構成

ログ・ファイル・プロトコルにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取り出すことができます。RSA Authentication Manager DSM は、ログ・ファイル・プロトコル・ソースを使用して、ログ・ファイルの一括ロードをサポートします。

ログ・ファイル・プロトコルを使用して RSA Authentication Manager を構成する手順は、RSA Authentication Manager のバージョンによって異なります。

- RSA Authentication Manager V6.x を使用している場合は、『RSA Authentication Manager 6.x の構成』を参照してください。
- RSA Authentication Manager V7.x を使用している場合は、 940 ページの『RSA Authentication Manager 7.x の構成』を参照してください。

RSA Authentication Manager 6.x の構成

RSA Authentication Manager 6.x デバイスを構成できます。

手順

1. RSA Security Console にログインします。
2. RSA データベース管理ツールにログインします。
3. 「拡張」ツールをクリックします。

システムにより再度ログインするように要求されます。

4. 「データベース管理 **(Database Administration)**」をクリックします。

SecurID の使用に関する詳細情報については、ご使用のベンダーの資料を参照してください。

5. 「ログ **(Log)**」リストで「自動ログ保守 **(Automate Log Maintenance)**」を選択します。

   「自動ログ保守 (Automatic Log Maintenance)」ウィンドウが表示されます。
6. 「自動監査ログ保守を有効にする **(Enable Automatic Audit Log Maintenance)**」チェック・ボックスを選択します。
7. 「削除して保管 **(Delete and Archive)**」を選択します。
8. 置換ファイルを選択します。
9. アーカイブ・ファイル名を入力します。
10. 「バージョンのサイクル回数 **(Cycle Through Version(s))**」フィールドに、値を入力します。
11. 例えば、「すべてのログを選択する **(Select all Logs)**」を選択します。
12. 頻度を選択します。
13. 「**OK**」をクリックします。
14. これで、IBM Security QRadar でログ・ソースとプロトコルを構成する準備ができました。
    a. RSA デバイスからイベントを受け取るように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**RSA Authentication Manager**」オプションを選択する必要があります。
    b. ログ・ファイル・プロトコルを構成するには、「プロトコル構成」リストから「ログ・ファイル」オプションを選択する必要があります。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

RSA Authentication Manager 7.x の構成

RSA Authentication Manager 7.x デバイスを構成できます。

手順

1. RSA Security Console にログインします。
2. 「管理」 > 「ログ管理 **(Log Management)**」 > 「反復ログ・アーカイブ・ジョブ **(Recurring Log Archive Jobs)**」をクリックします。
3. 「スケジュール」セクションで、**Job Starts**、**Frequency**、**Run Time**、および **Job Expires** の各パラメーターの値を構成します。
4. 「操作 **(Operations)**」フィールドで、「管理ログ設定 **(Administration Log Settings)**」、「ランタイム・ログ設定 **(Runtime Log Settings)**」、および「システム・ログ設定 **(System Log Settings)**」の各設定に対して、「エクスポートのみ **(Export Only)**」または「エクスポートして消去 **(Export and Purge)**」を選択します。

   注**:** 「エクスポートして消去 **(Export and Purge)**」操作は、ログ・レコードをデータベースからアーカイブにエクスポートして、次にログをデータベースから

消去します。「エクスポートのみ **(Export Only)**」操作では、ログ・レコードをデータベースからアーカイブにエクスポートしますが、レコードはデータベースに残ります。

5. 「管理」、「ランタイム **(Runtime)**」、および「システム **(System)**」に対して、アーカイブ・ファイルのエクスポート先とする**エクスポート**・ディレクトリーを構成します。

   続行する前に、FTP を使用して、管理ログ、ランタイム・ログ、およびシステム・ログにアクセスできることを確認します。

6. Administration、Runtime、および System の各パラメーターに対して、Days Kept Online パラメーターを 1 に設定します。こうすると、1 日を経過したログがエクスポートされます。「エクスポートして消去 **(Export and Purge)**」を選択すると、ログもデータベースから消去されます。
7. 「保存」をクリックします。
8. これで、QRadar でログ・ソースとプロトコルを構成する準備ができました。
   a. RSA デバイスからイベントを受け取るように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**RSA Authentication Manager**」オプションを選択する必要があります。
   b. ログ・ファイル・プロトコルを構成するには、「プロトコル構成」リストから「ログ・ファイル」オプションを選択する必要があります。

関連概念:

22 ページの『ログ・ファイル・プロトコルの構成オプション』
リモート・ホストからイベントを受信するには、ログ・ファイル・プロトコルを使用するようにログ・ソースを構成します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 112 章 SafeNet DataSecure

SafeNet DataSecure 用の IBM Security QRadar DSM は、SafeNet DataSecure デバイスから Syslog イベントを収集します。

DataSecure は、レコード管理アクション、ネットワーク・アクティビティー、暗号化要求などのアクティビティーを保守します。QRadar は SafeNet DataSecure V6.3.0 をサポートしています。

SafeNet DataSecure は、以下のイベント・ログを作成します。

アクティビティー・ログ
: 鍵サーバーによって受信された各要求のレコードが含まれます。

監査ログ
: 管理コンソールまたはコマンド・ライン・インターフェースのいずれかを使用して、SafeNet KeySecure に対して行われたすべての構成変更およびユーザー入力エラーのレコードが含まれます。

クライアント・イベント・ログ
: <RecordEventRequest> エレメントを持つすべてのクライアント要求のレコードが含まれます。

システム・ログ
: すべてのシステム・イベントのレコードが含まれます。例えば、以下のイベントです。
  - サービスの開始、停止、および再始動
  - SNMP トラップ
  - ハードウェア障害
  - クラスター複製および同期の成功または失敗
  - ログ転送の失敗

SafeNet DataSecure を QRadar に統合するには、以下の手順を実行します。

1. SafeNet DataSecure デバイスで Syslog を有効にします。
2. システムが 25 件のイベントを受信し、ログ・ソースを構成した後で、QRadar は SafeNet DataSecure を自動的に検出します。QRadar が SafeNet DataSecure を自動的に検出しない場合は、ログ・ソースを追加します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するための SafeNet DataSecure の構成

SafeNet DataSecure 用の DSM を追加する前に、SafeNet DataSecure デバイスで Syslog を有効にします。

手順

1. ロギング・アクセス制御を持つ管理者として SafeNet DataSecure 管理コンソールにログインします。
2. 「デバイス **(Device)**」 > 「ログ構成 **(Log Configuration)**」を選択します。
3. 「ローテーションと **Syslog (Rotation & Syslog)**」タブを選択します。
4. 「**Syslog** 設定 **(Syslog Settings)**」セクションでログを選択し、「編集 **(Edit)**」をクリックします。
5. 「**Syslog** を有効にする **(Enable Syslog)**」を選択します。
6. 以下のパラメーターを構成します。

パラメーター	説明
Syslog サーバー #1 IP (Syslog Server #1 IP)	ターゲット QRadar の IP アドレスまたはホスト名。イベント・コレクター (Event Collector).
Syslog サーバー #1 ポート (Syslog Server #1 Port)	QRadar の listen ポート。ポート 514 を使用します。
Syslog サーバー #1 プロトコル (Syslog Server #1 Proto)	QRadar は、UDP または TCP のいずれかを使用して Syslog メッセージを受信できます。

7. オプション。Syslog サーバー #2 の IP アドレス、ポート、およびプロトコルを入力します。2 つのサーバーが構成されている場合、SafeNet DataSecure は、両方のサーバーにメッセージを送信します。
8. Syslog ファシリティーを入力するか、デフォルト値の local1 を受け入れます。
9. 「保存」をクリックします。

第 113 章 Salesforce

IBM Security QRadar は Salesforce DSM を幅広くサポートしています。

Salesforce Security Auditing

Salesforce Security Auditing 用の IBM Security QRadar DSM は、QRadar がアクセスできる場所にクラウドからコピーされた Salesforce Security Auditing 監査証跡ログを収集することができます。

以下の表は、Salesforce Security Auditing DSM の仕様を示しています。

表 *350. Salesforce Security Auditing DSM* の仕様

仕様	値
製造元	Salesforce
DSM	Salesforce Security Auditing
RPM ファイル名	DSM-SalesforceSecurityAuditing->*QRadar-version-Build_number*.noarch.rpm
プロトコル	ログ・ファイル
QRadar で記録されるイベント	セットアップ監査レコード
自動的に検出?	いいえ
ID を含む?	いいえ
その他の情報	Salesforce Web サイト (http://www.salesforce.com/)

Salesforce Security Auditing DSM 統合プロセス

Salesforce Security Auditing DSM を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - ログ・ファイル・プロトコル RPM
   - Salesforce Security Auditing RPM
2. Salesforce 監査証跡ファイルを、QRadar がアクセスできるリモート・ホストにダウンロードします。
3. Salesforce Security Auditing のインスタンスごとに、QRadar コンソール上でログ・ソースを作成します。

Salesforce 監査証跡ファイルのダウンロード

Salesforce Security Auditing イベントを収集するには、QRadar がアクセスできるリモート・ホストに Salesforce 監査証跡ファイルをダウンロードする必要があります。

このタスクについて

更新された一連の監査データを QRadar にインポートする場合は、必ず以下の手順を実行する必要があります。監査証跡ファイルをダウンロードする際に、以前の監査証跡ファイル (CSV 形式のファイル) を上書きすることができます。QRadar は、監査証跡ファイルのデータを受信すると、以前にインポートされなかった監査レコードだけを処理します。

手順

1. Salesforce Security Auditing サーバーにログインします。
2. 「セットアップ **(Setup)**」セクションに移動します。
3. 「セキュリティー管理 **(Security Controls)**」をクリックします。
4. 「セットアップ監査証跡の表示 **(View Setup Audit Trail)**」をクリックします。
5. 「過去 **6** カ月間のセットアップ監査証跡をダウンロード **(Excel.csv** ファイル**) (Download setup audit trail for last six months (Excel.csv file))**」をクリックします。
6. ダウンロードしたファイルを、QRadar がログ・ファイル・プロトコルを使用してアクセスできる場所にコピーします。

QRadar で Salesforce Security Auditing のログ・ソースを構成する

Salesforce Security Auditing イベントを収集するには、QRadar でログ・ソースを構成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**Salesforce Security Auditing**」を選択します。
7. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
8. 以下に示す Salesforce Security Auditing のパラメーターを構成します。

パラメーター	説明
イベント・ジェネレーター **(Event Generator)**	正規表現ベースの複数行
開始パターン **(Start Pattern)**	(¥d{1,2}/¥d{1,2}/¥d{4} ¥d{1,2}:¥d{2}:¥d{2} ¥w+)
終了パターン **(End Pattern)**	このパラメーターは空のままにしてください。
日時の正規表現 **(Date Time RegEx)**	(¥d{1,2}/¥d{1,2}/¥d{4} ¥d{1,2}:¥d{2}:¥d{2} ¥w+)
日時形式 **(Date Time Format)**	dd/MM/yyyy hh:mm:ss z

重要: これらの値は、Salesforce Security Auditing の Winter '15 バージョンに基づいています。これより前のバージョンの場合は、以下の regex ステートメントを使用してください。

- 「開始パターン **(Start Pattern)**」パラメーターには、以下のステートメントを使用します。

  ```
  (¥d{1,2}/¥d{1,2}/¥d{4} ¥d{1,2}:¥d{2}:¥d{2} [APM]{2} ¥w+)
  ```

- 「日時の正規表現 **(Date Time RegEx)**」パラメーターには、以下のステートメントを使用します。

  ```
  (¥d{1,2}/¥d{1,2}/¥d{4} ¥d{1,2}:¥d{2}:¥d{2} ¥w{2} ¥w+)
  ```

- 「日時形式 **(Date Time Format)**」パラメーターには、`MM/dd/yyyy hh:mm:ss aa z` を使用します。

9. 残りのパラメーターを構成します。
10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

Salesforce Security Monitoring

Salesforce Security Monitoring 用の IBM Security QRadar DSM は、クラウド内で RESTful API を使用して、Salesforce コンソールからイベント・ログを収集することができます。

以下の表は、Salesforce Security Monitoring DSM の仕様を示しています。

表 *351. Salesforce Security Monitoring DSM* の仕様

仕様	値
製造元	Salesforce
DSM	Salesforce Security Monitoring
RPM ファイル名	DSM-SalesforceSecurityMonitoring->*QRadar-version-Build_number*.noarch.rpm
プロトコル	Salesforce REST API プロトコル
QRadar で記録されるイベント	ログイン履歴、アカウント履歴、ケース履歴、ライセンス履歴、サービス契約履歴、契約明細履歴、契約履歴、問い合わせ履歴、リード履歴、オポチュニティー履歴、ソリューション履歴
自動的に検出?	いいえ
ID を含む?	はい
その他の情報	Salesforce Web サイト (http://www.salesforce.com/)

Salesforce Security Monitoring DSM 統合プロセス

Salesforce Security Monitoring DSM を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。

- DSMCommon RPM
- SalesforceRESTAPI Protocol RPM
- Salesforce Security Monitoring RPM

2. QRadar と通信するように Salesforce Security Monitoring サーバーを構成します。
3. Salesforce Security Monitoring と QRadar との通信を有効にするための証明書を取得してインストールします。この証明書は、/opt/QRadar/conf/trusted_certificates/ フォルダーに .DER 形式で格納する必要があります。
4. Salesforce Security Monitoring のインスタンスごとに、QRadar コンソール上でログ・ソースを作成します。

QRadar との通信用に Salesforce Security Monitoring サーバーを構成する

QRadar と通信できるようにするには、Salesforce コンソール上で Connected App を構成し、Connected App が生成する情報を収集する必要があります。この情報は、QRadar のログ・ソースを構成する際に必要になります。

始める前に

Salesforce サーバー上で RESTful API が使用可能になっていない場合は、Salesforce サポートに連絡してください。

手順

1. Salesforce Security Monitoring サーバーにログインします。
2. 「セットアップ **(Setup)**」メニューで、「作成 **(Create)**」>「アプリケーション **(Apps)**」>「新規 **(New)**」をクリックします。
3. アプリケーションの名前を入力します。
4. 連絡先の E メールの情報を入力します。
5. 「**OAuth** 設定を有効にする **(Enable OAuth Settings)**」を選択します。
6. 「選択した **OAuth** 範囲 **(Selected OAuth Scopes)**」リストで「フルアクセス **(Full Access)**」を選択します。
7. 「情報 **URL (Info URL)**」フィールドで、アプリケーションの詳細情報を参照できる場所の URL を入力します。
8. 残りのオプション・パラメーターを構成します。
9. 「保存」をクリックします。

次のタスク

Connected App により、QRadar 上でログ・ソースを構成する際に必要な情報が生成されます。以下の情報をメモしてください。

コンシューマ鍵 **(Consumer Key)**
: 「コンシューマ鍵 **(Consumer Key)**」の値を使用して、QRadar ログ・ソースの「クライアント **ID (Client ID)**」パラメーターを構成します。

コンシューマの秘密 **(Consumer Secret)**
: このリンクをクリックすると、コンシューマーの秘密を表示することができ

ます。「コンシューマの秘密 **(Consumer Secret)**」の値を使用して、QRadar ログ・ソースの「シークレット **ID (Secret ID)**」パラメーターを構成します。

重要**:** 「コンシューマの秘密 **(Consumer Secret)**」の値は機密情報です。この値をプレーン・テキストで保存しないでください。

セキュリティトークン **(Security token)**
セキュリティー・トークンは、連絡先の E メールとして構成した E メール・アドレスに E メールで送信されます。

QRadar で Salesforce Security Monitoring のログ・ソースを構成する

Salesforce Security Monitoring イベントを収集するには、QRadar でログ・ソースを構成します。

始める前に

Salesforce Security Monitoring サーバーで Connected App を構成すると、以下の情報が生成されます。

- コンシューマ鍵 (Consumer Key)
- コンシューマの秘密 (Consumer Secret)
- セキュリティトークン (Security token)

これらの情報は、QRadar で Salesforce Security Monitoring のログ・ソースを構成する際に必要になります。

Salesforce Security Monitoring インスタンスの信頼された証明書が、QRadar システムの `/opt/qradar/conf/trusted_certificates/` フォルダーに .DER 形式でコピーされていることを確認してください。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**Salesforce Security Monitoring**」を選択します。
7. 「プロトコル構成」リストで「**Salesforce Rest API**」を選択します。
8. 以下の値を構成します。

パラメーター	説明
ログイン **URL (Login URL)**	Salesforce セキュリティー・コンソールの URL。
ユーザー名	Salesforce セキュリティー・コンソールのユーザー名。

パラメーター	説明
セキュリティトークン **(Security Token)**	Salesforce セキュリティー・コンソールで Connected App の連絡先 E メールとして構成された E メール・アドレスに送信されたセキュリティー・トークン。
クライアント **ID (Client ID)**	Salesforce セキュリティー・コンソールで Connected App を構成したときに生成されたコンシューマー鍵。
シークレット **ID (Secret ID)**	Salesforce セキュリティー・コンソールで Connected App を構成したときに生成されたコンシューマーの秘密。
プロキシーの使用 (Use Proxy)	プロキシーが構成されている場合は、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Salesforce Security バケットにアクセスします。 「プロキシー・サーバー」、「プロキシー・ポート」、「プロキシー・ユーザー名」、「プロキシー・パスワード」の各フィールドを構成します。プロキシーが認証を必要としない場合、「プロキシー・ユーザー名」フィールドと「プロキシー・パスワード」フィールドはブランクのままでかまいません。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

第 114 章 Samhain Labs

Samhain Labs の Host-Based Intrusion Detection System (HIDS) は、システム上のファイルに対する変更をモニターします。

IBM Security QRadar 用の Samhain HIDS DSM は、ファイル保全性モニター (FIM) に使用する場合に Samhain バージョン 2.4 をサポートしています。

Syslog または JDBC を使用してイベントを収集するように、Samhain HIDS DSM を構成できます。

関連概念:

17 ページの『JDBC プロトコルの構成オプション』
QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Samhain イベントの収集のための Syslog 構成

Syslog を使用して Samhain HIDS と統合するように IBM Security QRadar を構成する前に、QRadar システムにログを転送するように Samhain HIDS システムを構成する必要があります。

このタスクについて

以下の手順は、デフォルトの samhainrc ファイルに基づいています。samhainrc ファイルが変更されている場合、Syslog ファシリティーなどの一部の値が異なることがあります。

手順

1. コマンド・ライン・インターフェースから Samhain HIDS にログインします。
2. 以下のファイルを開きます。

   ```
   /etc/samhainrc
   ```
3. 以下の行からコメント・マーカー (#) を削除します。

   ```
   SetLogServer=info
   ```
4. ファイルを保存して終了します。

   Syslog を使用してローカル・システムにアラートが送信されます。

5. 以下のファイルを開きます。

   ```
   /etc/syslog.conf
   ```

6. 以下の行を追加します。

   ```
   local2.* @<IP Address>
   ```

   ここで *<IP address>* は、QRadar の IP アドレスです。

7. ファイルを保存して終了します。
8. Syslog を再始動します。

   ```
   /etc/init.d/syslog restart
   ```

   Samhain が Syslog を使用してログを QRadar に送信します。

   これで、QRadar で Samhain HIDS DSM を構成できるようになりました。Samhain からイベントを受信するように QRadar を構成するには、以下のようにします。

9. 「ログ・ソース・タイプ」リストで「**Samhain HIDS**」オプションを選択します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Samhain イベントの収集のための JDBC の構成

ログ・アラートをデータベースに送信するように Samhain HIDS を構成できます。 Samhain でネイティブ・レベルでサポートされるのは Oracle、PostgreSQL、および MySQL です。

このタスクについて

JDBC プロトコルを使用してこれらのデータベースからイベントを収集するように IBM Security QRadar を構成することもできます。

注**:** IBM Security QRadar には、JDBC 向けの MySQL ドライバーは含まれていません。MySQL JDBC ドライバーを必要とする DSM またはプロトコルを使用する場合は、プラットフォーム に依存しない `MySQL Connector/J` を http://dev.mysql.com/downloads/connector/j/ からダウンロードしてインストールする必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。

6. 「ログ・ソース・タイプ」リストで「**Samhain HIDS**」オプションを選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. JDBC 構成を更新して以下の値を追加します。
   a. データベース・タイプ **(Database Type)**: <*Samhain Database Type*>
   b. データベース名: <*Samhain SetDBName*>
   c. テーブル名 **(Table Name)**: <*Samhain SetDBTable*>
   d. 選択リスト **(Select List)**: *
   e. 比較フィールド **(Compare Field)**: log_index
   f. **IP** またはホスト名 **(IP or Hostname)**: <*Samhain SetDBHost*>
   g. ポート: <デフォルト・ポート>
   h. ユーザー名: <*Samhain SetDBUser*>
   i. パスワード: <*Samhain SetDBPassword*>
   j. ポーリング間隔 **(Polling Interval)**: <デフォルトの間隔>

   各部分について以下で説明します。

   - <*Samhain Database Type*> は、Samhain が使用するデータベースのタイプです (Samhain システム管理者にお問い合わせください)。
   - <*Samhain SetDBName*> は、samhainrc ファイルに指定されているデータベース名です。
   - <*Samhain SetDBTable*> は、samhainrc ファイルに指定されているデータベース表です。
   - <*Samhain SetDBHost*> は、samhainrc ファイルに指定されているデータベース・ホストです。
   - <*Samhain SetDBUser*> は、samhainrc ファイルに指定されているデータベース・ユーザーです。
   - <*Samhain SetDBPassword*> は、samhainrc ファイルに指定されているデータベース・パスワードです。
9. これで、QRadar でログ・ソースを構成できるようになりました。Samhain からイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Samhain HIDS**」オプションを選択します。

   Samhain について詳しくは、http://www.la-samhna.de/samhain/manual を参照してください。

関連概念:

17 ページの『JDBC プロトコルの構成オプション』
QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 115 章 Seculert

Seculert 用の IBM Security QRadar DSM は、Seculert クラウド・サービスからイベントを収集します。

以下の表は、Seculert DSM の仕様を示しています。

表 *352. Seculert DSM* の仕様

仕様	値
製造元	Seculert
DSM 名	Seculert
RPM ファイル名	`DSM-SeculertSeculert-`*`Qradar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	v1
プロトコル	Seculert Protection REST API プロトコル
記録されるイベント・タイプ	すべてのマルウェア通信イベント
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Seculert の Web サイト (https://www.seculert.com)

Seculert を QRadar に統合するには、以下の手順を実行します。

1. 以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - プロトコル共通
   - DSM-DSMCommon
   - Seculert DSM RPM
   - SeculertProtectionRESTAPI PROTOCOL RPM
2. QRadar コンソールで、Seculert ログ・ソースを追加します。以下の表は、Seculert イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *353. Seculert* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Seculert
プロトコル構成	Seculert Protection REST API
API 鍵	32 文字の UUID API 鍵の取得について詳しくは、API 鍵の取得を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

API 鍵の取得

Seculert からイベントを収集するには、その前に Seculert クラウド・サービスのユーザー・インターフェースから QRadar に API 鍵をコピーする必要があります。

手順

1. Seculert Web ポータルにログインします。
2. ダッシュボードで、「**API**」タブをクリックします。
3. 「**Your API Key**」の値をコピーします。

次のタスク

QRadar で Seculert のログ・ソースを構成する際に、コピーした API 鍵が必要となります。

第 116 章 Sentrigo Hedgehog

Sentrigo Hedgehog デバイスを IBM Security QRadar と統合できます。

このタスクについて

Sentrigo Hedgehog デバイスは、syslog を使用して LEEF イベントを受け入れます。Sentrigo Hedgehog デバイスと統合するように QRadar を構成する前に、以下の手順を実行します。

手順

1. Sentrigo Hedgehog のコマンド・ライン・インターフェース (CLI) にログインします。
2. 編集する以下のファイルを開きます。

   `<Installation directory>/conf/sentrigo-custom.properties`

   ここで、*<Installation directory>* は、Sentrigo Hedgehog のインストールが含まれるディレクトリーです。
3. カスタム・プロパティー・ファイルに以下の *log.format* 項目を追加します。

   注: Sentrigo Hedgehog の構成またはインストール済み環境によっては、既存の *log.format* 項目の置換または上書きが必要な場合があります。

```
sentrigo.comm.ListenAddress=1996
log.format.body.custom=usrName=$osUser:20$|duser=$execUser:20$|
severity=$severity$|identHostName=$sourceHost$|src=$sourceIP$|
dst=$agent.ip$|devTime=$logonTime$|
devTimeFormat=EEE MMM dd HH:mm:ss z yyyy|
cmdType=$cmdType$|externalId=$id$|
execTime=$executionTime.time$|
dstServiceName=$database.name:20$|
srcHost=$sourceHost:30$|execProgram=$execProgram:20$|
cmdType=$cmdType:15$|oper=$operation:225$|
accessedObj=$accessedObjects.name:200$

log.format.header.custom=LEEF:1.0|
Sentrigo|Hedgehog|$serverVersion$|$rules.name:150$|
log.format.header.escaping.custom=¥¥|
log.format.header.seperator.custom=,
log.format.header.escape.char.custom=¥¥
log.format.body.escaping.custom=¥=
log.format.body.escape.char.custom=¥¥
log.format.body.seperator.custom=|
log.format.empty.value.custom=NULL
log.format.length.value.custom=10000
log.format.convert.newline.custom=true
```

4. カスタム・プロパティー・ファイルを保存します。
5. `log.format` の変更内容を実装するために、Sentrigo Hedgehog サービスを停止してから、再始動します。

   これで、QRadar でログ・ソースを構成できるようになりました。

6. Sentrigo Hedgehog デバイスからのイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストから、「**Sentrigo Hedgehog**」オプションを選択します。

Sentrigo Hedgehog について詳しくは、ベンダーの資料を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 117 章 Skyhigh Networks Cloud Security Platform

Skyhigh Networks Cloud Security Platform DSM 用の IBM Security QRadar DSM は Skyhigh Networks Cloud Security Platform からログを収集します。

Skyhigh Networks Cloud Security Platform DSM の仕様を以下の表に示します。

表 *354. Skyhigh Networks Cloud Security Platform DSM* の仕様

仕様	値
製造元	Skyhigh Networks
DSM 名	Skyhigh Networks Cloud Security Platform
RPM ファイル名	DSM-SkyhighNetworksCloudSecurityPlatform-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	2.4
イベント・フォーマット	LEEF
記録されるイベント・タイプ	アノマリ・イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Skyhigh Networks の Web サイト (www.skyhighnetworks.com/)

Skyhigh Networks Cloud Security Platform を QRadar と統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Skyhigh Networks Cloud Security Platform DSM RPM
   - DSMCommmon RPM
2. syslog イベントを QRadar に送信するように Skyhigh Networks Cloud Security Platform デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Skyhigh Networks Cloud Security Platform ログ・ソースを追加してください。以下の表は、Skyhigh Networks Cloud Security Platform イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *355. Skyhigh Networks Cloud Security Platform* ログ・ソースのパラメーター

パラメーター	値
ログ・ソース・タイプ	Skyhigh Networks Cloud Security Platform
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインスト

ールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と通信するための Skyhigh Networks Cloud Security Platform の構成

手順

1. Skyhigh Enterprise Connector の管理インターフェースにログインします。
2. 「**Enterprise** 統合 **(Enterprise Integration)**」 > 「**SIEM** 統合 **(SIEM Integration)**」を選択します。
3. 以下の **SIEM SYSLOG SERVICE** の各パラメーターを構成します。

パラメーター	値
SIEM サーバー **(SIEM server)**	ON
フォーマット	ログ・イベント拡張フォーマット (LEEF)
Syslog プロトコル **(Syslog Protocol)**	TCP
Syslog サーバー	<*QRadar* の *IP* またはホスト名>
Syslog ポート **(Syslog Port)**	514
SIEM に送信 **(Send to SIEM)**	新規アノマリのみ

4. 「保存」をクリックします。

第 118 章 SolarWinds Orion

IBM Security QRadar 用の SolarWinds Orion DSM は、SolarWinds Alert Manager からの SNMPv2 および SNMPv3 構成のアラートをサポートします。

このタスクについて

イベントは syslog を使用して QRadar に送信されます。QRadar を統合するには、SNMP トラップを作成し、syslog イベントを転送するように **SolarWinds Alert Manager** を構成する必要があります。

SolarWinds Orion Alert Manager で SNMP トラップを構成するには、以下の手順を実行します。

手順

1. 「スタート」 > 「すべてのプログラム」 > 「**SolarWinds Orion**」 > 「アラート、レポート、マッピング **(Alerting, Reporting, and Mapping)**」 > 「拡張アラート・マネージャー **(Advanced Alert Manager)**」を選択します。

   「Alert Manager クイック・スタート (Alert Manager Quick Start)」が表示されます。
2. 「アラートの構成 **(Configure Alerts)**」をクリックします。

   「アラートの管理 (Manage Alerts)」ウィンドウが表示されます。
3. 既存のアラートを選択して、「編集 **(Edit)**」をクリックします。
4. 「トリガー・アクション **(Triggered Actions)**」タブを選択します。
5. 「新規アクションの追加 **(Add New Action)**」をクリックします。

   「アクションの選択 (Select an Action)」ウィンドウが表示されます。
6. 「**SNMP** トラップの送信 **(Send an SNMP Trap)**」を選択して、「**OK**」をクリックします。
7. 「**SNMP** トラップの定義 **(SNMP Trap Definitions)**」の構成 - QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
8. 「トラップ・テンプレート **(Trap Template)**」の構成 - 「**ForwardSyslog**」を選択します。
9. 「**SNMP** バージョン **(SNMP Version)**」の構成 - イベントの転送に使用する SNMP バージョンを選択します。QRadar では、SNMPv2c または SNMPv3 がサポートされます。

   「**SNMPv2c**」 - SNMPv2c 認証で使用する SNMP コミュニティー・ストリングを入力します。デフォルトのコミュニティー・ストリング値は public です。

   「**SNMPv3**」 - ユーザー名を入力し、SNMPv3 で使用する「認証方式 **(Authentication Method)**」を選択します。

QRadar では、MD5 または SH1 の認証方式、および DES56 または AES128 ビットの暗号化がサポートされます。

10. 「**OK**」をクリックして、SNMP トリガー・アクションを保存します。

    「アラートの管理 (Manage Alerts)」ウィンドウが表示されます。

    注**:** SNMP トラップが正しく構成されていることを確認するには、編集したアラートを選択して「テスト **(Test)**」をクリックします。このアクションで syslog イベントがトリガーされ、QRadar に転送されます。
    QRadar でモニターするすべての SNMP トラップ・アラートに関して Alert Manager を構成するには、この手順を繰り返します。

    これで、QRadar でログ・ソースを構成できるようになりました。

11. QRadar では、正しく構成された SNMP トラップ・アラート・トリガーからの syslog イベントの検出が自動的に行われます。ただし、SolarWinds Orion からのイベントを受信するように QRadar を手動で構成する場合、「ログ・ソース・タイプ」リストから「**SolarWinds Orion**」を選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 119 章 SonicWALL

SonicWALL SonicOS DSM は syslog を使用してイベントを受け取ります。

IBM Security QRadar は、SonicOS のファームウェアを使用して、SonicWALL アプライアンスから転送された関連する syslog イベントをすべて記録します。SonicWALL SonicOS デバイスと統合するには、SonicWALL SonicOS アプライアンスで syslog 転送を構成する必要があります。

syslog イベントを転送するための SonicWALL の構成

SonicWALL は、すべての SonicOS イベント・アクティビティーを取り込みます。このイベントは、SonicWALL のデフォルトのイベント・フォーマットを使用して IBM Security QRadar に転送できます。

手順

1. SonicWALL Web インターフェースにログインします。
2. ナビゲーション・メニューから、「ログ **(Log)**」 > 「**Syslog**」を選択します。
3. 「Syslog サーバー (Syslog Servers)」ペインから、「追加 **(Add)**」をクリックします。
4. 「名前 **(Name)**」または「**IP** アドレス **(IP Address)**」のフィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
5. 「ポート **(Port)**」フィールドに 514 を入力します。

   SonicWALL syslog 転送機能により、UDP ポート 514 を使用してイベントが QRadar に送信されます。
6. 「**OK**」をクリックします。
7. 「**Syslog** 形式 **(Syslog Format)**」リストから、「デフォルト **(Default)**」を選択します。
8. 「適用」をクリックします。

   syslog イベントが QRadar に転送されます。QRadar に転送された SonicWALL イベントは自動的に検出され、ログ・ソースが自動的に作成されます。SonicWALL アプライアンスの構成、または特定のイベントの情報について詳しくは、ベンダーの資料を参照してください。

ログ・ソースの構成

QRadar は、SonicWALL アプライアンスからの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

このタスクについて

SonicWALL syslog イベントのログ・ソースを手動で構成するには以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「**SonicWALL SonicOS**」を選択します。
8. 「プロトコル構成」リストで「**Syslog**」を選択します。
9. 以下の値を構成します。

表 *356. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	SonicWALL アプライアンスからのイベントの ID としてログ・ソースの IP アドレスまたはホスト名を入力します。 SonicWALL SonicOS アプライアンスに対して作成する各ログ・ソースに、IP アドレス、ホスト名などの固有の ID を含めることをお勧めします。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。 SonicWALL SonicOS アプライアンスにより QRadar に転送されたイベントは「ログ・アクティビティー」タブに表示されます。詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

第 120 章 Sophos

IBM Security QRadar は複数の Sophos DSM をサポートしています。

Sophos Enterprise Console

IBM Security QRadar には、JDBC を使用して Sophos Enterprise Console からイベントを収集するための 2 つのオプションが用意されています。

ご使用の Sophos Enterprise Console インストール済み環境に最も適した方法を選択してください。

- 『Sophos Enterprise Console プロトコルを使用する QRadar の構成』
- 969 ページの『JDBC プロトコルを使用した IBM Security QRadar の構成』

注**:** Sophos Enterprise Console プロトコルを使用するには、Sophos Enterprise Console とともに Sophos Reporting Interface がインストールされている必要があります。Sophos Reporting Interface がない場合は、JDBC プロトコルを使用して QRadar を構成する必要があります。Sophos Reporting Interface のインストールについて詳しくは、Sophos Enterprise Console の資料を参照してください。

関連概念:

17 ページの『JDBC プロトコルの構成オプション』
QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Sophos Enterprise Console プロトコルを使用する QRadar の構成

IBM Security QRadar 用の Sophos Enterprise Console DSM は、Java Database Connectivity (JDBC) を使用してイベントを受け入れます。

このタスクについて

Sophos Enterprise Console DSM は、Sophos Enterprise Console プロトコルと連携して動作し、アンチウィルス、アプリケーション制御、デバイス制御、改ざんからの保護、およびファイアウォールの各ログからのペイロード情報を `vEventsCommonData` テーブルに結合し、それらのイベントを QRadar に提供します。QRadar を構成する前に Sophos Enterprise Console プロトコルをインストールしておく必要があります。

JDBC プロトコルを使用して Sophos データベースにアクセスするように QRadar を構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース・タイプ」リストで、「**Sophos Enterprise Console**」を選択します。
7. 「プロトコル構成」リストで「**Sophos Enterprise Console JDBC**」を選択します。

   注**:** QRadar での Sophos Enterprise Console JDBC プロトコルの構成に必要なパラメーターを定義するには、Sophos Enterprise Console で「データベース設定の構成 **(Configure Database Settings)**」を参照する必要があります。
8. 以下の値を構成します。

表 *357. Sophos Enterprise Console* の *JDBC* パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<Sophos Database>@<Sophos Database Server IP or Host Name>* 各部分について以下で説明します。 • *<Sophos Database>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<Sophos Database Server IP or Host Name>* は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。 ログ・ソース ID の名前の定義時は、Management Enterprise Console での Sophos データベースの値、およびデータベース・サーバーの IP アドレスまたはホスト名の値を使用する必要があります。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	Sophos データベースの正確な名前を入力します。
IP またはホスト名	Sophos SQL Server の IP アドレスまたはホスト名を入力します。

表 357. *Sophos Enterprise Console* の *JDBC* パラメーター (続き)

パラメーター	説明
ポート	データベース・サーバーが使用するポート番号を入力します。Sophos Enterprise Console の **MSDE** のデフォルト・ポートは 1168 です。 JDBC 構成ポートは、Sophos データベースのリスナー・ポートと一致している必要があります。Sophos データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして **MSDE** を使用する際に「データベース・インスタンス」を定義する場合は、構成の「ポート」パラメーターをブランクのままにする必要があります。
ユーザー名	データベースへのアクセスに必要なユーザー名を入力します。
パスワード	データベースへのアクセスに必要なパスワードを入力します。パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」パラメーターに入力したパスワードと同じでなければなりません。
認証ドメイン	「データベース・タイプ」として **MSDE** を選択し、データベースが Windows 用に構成されている場合は、Window 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックする場合は、構成内の「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを格納するテーブルまたはビューの名前として `vEventsCommonData` と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに `*` を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	比較フィールドとして `InsertedAt` と入力します。比較フィールドを使用して、テーブルに対する照会から次の照会までの間に追加されたい新しいイベントを特定できます。

表 357. *Sophos Enterprise Console* の *JDBC* パラメーター (続き)

パラメーター	説明
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。
NTLMv2 の使用	MSDE を「データベース・タイプ」として選択した場合、「**NTLMv2** の使用」チェック・ボックスが表示されます。 NTLMv2 認証を必要とする SQL サーバーとの通信時に、MSDE 接続で NTLMv2 プロトコルを使用するように強制する場合は、「**NTLMv2** の使用」チェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。 「**NTLMv2** の使用」チェック・ボックスを選択した場合でも、NTLMv2 認証を必要としない SQL サーバーへの MSDE 接続には影響しません。

注**:** 「信頼性」パラメーターに 5 より大きい値を選択すると、Sophos ログ・ソースに対し、QRadar 内の他のログ・ソースよりも高い重要度が設定されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

JDBC プロトコルを使用した IBM Security QRadar の構成

IBM Security QRadar 用の Sophos Enterprise Console DSM は、Java Database Connectivity (JDBC) を使用してイベントを受け入れます。

QRadar は、関連するアンチウィルス・イベントをすべて記録します。本書では、JDBC プロトコルを使用して Sophos Enterprise Console データベースにアクセスするための QRadar の構成について説明します。

データベース・ビューの構成

IBM Security QRadar を Sophos Enterprise Console と統合するには、以下の手順を実行します。

手順

1. Sophos Enterprise Console デバイスのコマンド・ライン・インターフェース (CLI) にログインします。
2. 以下のコマンドを入力して、QRadar をサポートするための Sophos データベースのカスタム・ビューを作成します。

```
CREATE VIEW threats_view AS SELECT t.ThreatInstanceID,
t.ThreatType, t.FirstDetectedAt, c.Name, c.LastLoggedOnUser,
c.IPAddress, c.DomainName, c.OperatingSystem, c.ServicePack,
t.ThreatSubType, t.Priority, t.ThreatLocalID,
t.ThreatLocalIDSource, t.ThreatName, t.FullFilePathCheckSum,
t.FullFilePath, t.FileNameOffset, t.FileVersion, t.CheckSum,
t.ActionSubmittedAt, t.DealtWithAt, t.CleanUpable, t.IsFragment,
t.IsRebootRequired, t.Outstanding, t.Status, InsertedAt
FROM <Database Name>.dbo.ThreatInstancesAll
t, <Database Name>.dbo.Computers c
WHERE t.ComputerID = c.ID;
```

ここで、*<Database Name>* は、Sophos データベースの名前です。

注: データベース名にスペースを使用することはできません。

次のタスク

カスタム・ビューを作成したら、JDBC プロトコルを使用するイベント情報を受信するように、QRadar を構成する必要があります。QRadar での Sophos Enterprise Console DSM の構成については、『QRadar での JDBC ログ・ソースの構成』を参照してください。

QRadar での JDBC ログ・ソースの構成

IBM Security QRadar は、JDBC プロトコルを使用して Sophos データベースにアクセスするように構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

「ログ・ソース」ウィンドウが表示されます。

5. 「追加」をクリックします。

「ログ・ソースの追加」ウィンドウが表示されます。

6. 「ログ・ソース・タイプ」リストで、「**Sophos Enterprise Console**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。

注**:** QRadar での Sophos Enterprise Console DSM の構成に必要なパラメーターを定義するには、Sophos Enterprise Console で「データベース設定の構成 **(Configure Database Settings)**」を参照する必要があります。

8. 以下の値を構成します。

表 *358. Sophos Enterprise Console* の *JDBC* パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<Sophos Database>@<Sophos Database Server IP or Host Name>* 各部分について以下で説明します。 • *<Sophos Database>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<Sophos Database Server IP or Host Name>* は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。 ログ・ソース ID の名前の定義時は、Management Enterprise Console での Sophos データベースの値、およびデータベース・サーバーの IP アドレスまたはホスト名の値を使用する必要があります。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	Sophos データベースの正確な名前を入力します。
IP またはホスト名	Sophos SQL Server の IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。MSDE のデフォルト・ポートは 1433 です。 JDBC 構成ポートは、Sophos データベースのリスナー・ポートと一致している必要があります。Sophos データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして MSDE を使用する際に「データベース・インスタンス」を定義する場合は、構成の「ポート」パラメーターをブランクのままにする必要があります。
ユーザー名	データベースへのアクセスに必要なユーザー名を入力します。
パスワード	データベースへのアクセスに必要なパスワードを入力します。パスワードの最大長は 255 文字です。

表 *358. Sophos Enterprise Console* の *JDBC* パラメーター *(*続き*)*

パラメーター	説明
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」パラメーターに入力したパスワードと同じでなければなりません。
認証ドメイン	「データベース・タイプ」として **MSDE** を選択し、データベースが Windows 用に構成されている場合は、Window 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックする場合は、構成内の「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを格納するテーブルまたはビューの名前として `threats_view` と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに `*` を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	比較フィールドとして `ThreatInstanceID` を入力します。比較フィールドを使用して、テーブルに対する照会から次の照会までの間に追加されたい新しいイベントを特定できます。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
準備済みステートメントの使用 **(Use Prepared Statements)**	準備済みステートメントを使用する場合は、このチェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行するオプションを利用できます。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。

表 358. Sophos Enterprise Console の JDBC パラメーター (続き)

パラメーター	説明
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

注**:** 「信頼性」パラメーターに 5 より大きい値を選択すると、Sophos ログ・ソースに対し、QRadar 内の他のログ・ソースよりも高い重要度が設定されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

Sophos PureMessage

IBM Security QRadar 用の Sophos PureMessage DSM は、Java Database Connectivity (JDBC) を使用してイベントを受け取ります。

QRadar は、関連する E メール検疫イベントをすべて記録します。本書では、JDBC プロトコルを使用して Sophos PureMessage データベースにアクセスするための QRadar の構成について説明します。

QRadar は、以下の Sophos PureMessage バージョンをサポートしています。

- Sophos PureMessage for Microsoft Exchange - `savexquar` として指定された Microsoft SQL Server データベースにイベントを格納します。
- Sophos PureMessage for Linux - `pmx_quarantine` として指定された PostgreSQL データベースにイベントを格納します。

ここでは、QRadar と Sophos の統合について説明します。

- 『QRadar と Sophos PureMessage for Microsoft Exchange との統合』
- 977 ページの『QRadar と Sophos PureMessage for Linux との統合』

関連概念:

17 ページの『JDBC プロトコルの構成オプション』
QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar と Sophos PureMessage for Microsoft Exchange との統合

QRadar は、Sophos PureMessage for Microsoft Exchange と統合することができます。

手順

1. Microsoft SQL Server コマンド・ライン・インターフェース (CLI)にログインします。

   ```
   osql -E -S localhost¥sophos
   ```

2. QRadar と統合するデータベースを入力します。

   ```
   use savexquar; go
   ```

3. 以下のコマンドを入力して、Sophos データベースに QRadar をサポートする SIEM ビューを作成します。

   ```
   create view siem_view as select
   'Windows PureMessage' as application, id, reason,
   timecreated, emailonly as sender, filesize, subject,
   messageid, filename from dbo.quaritems,
   dbo.quaraddresses where ItemID = ID and Field = 76;
   ```

次のタスク

SIEM ビューを作成したら、JDBC プロトコルを使用してイベント情報を受信するように、QRadar を構成する必要があります。QRadar での Sophos PureMessage DSM の構成については、「『Sophos PureMessage の JDBC ログ・ソースの構成』」を参照してください。

Sophos PureMessage の JDBC ログ・ソースの構成

QRadar を、JDBCプロトコルを使用して Sophos PureMessage for Microsoft Exchange データベースにアクセスするように構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース・タイプ」リストで、「**Sophos PureMessage**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。

   注**:** QRadar での Sophos PureMessage DSM の構成に必要なパラメーターを定義するには、Sophos PureMessage デバイスでデータベース構成の設定を参照する必要があります。
8. 以下の値を構成します。

表 *359. Sophos PureMessage JDBC* のパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<Sophos PureMessage* データベース*>@<Sophos PureMessage* データベース・サーバー *IP* またはホスト名*>* 各部分について以下で説明します。 • *<Sophos PureMessage* データベース*>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<Sophos PureMessage* データベース・サーバー *IP* またはホスト名*>* は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。 ログ・ソース ID の定義時に、Sophos PureMessage デバイスのデータベースの値、およびデータベース・サーバー IP アドレスまたはホスト名の値を使用する必要があります。
データベース・タイプ	リストから「**MSDE**」を選択します。
データベース名	`savexquar` と入力します。
IP またはホスト名	Sophos PureMessage サーバーの IP アドレスまたはホスト名を入力します。

表 359. Sophos PureMessage JDBC のパラメーター (続き)

パラメーター	説明
ポート	データベース・サーバーが使用するポート番号を入力します。MSDE のデフォルト・ポートは 1433 です。Sophos インストール環境では、通常 24033 を使用します。ポート使用状況は、SQL Server の構成マネージャー・ユーティリティーを使用して確認できます。詳しくは、ベンダーの資料を参照してください。 JDBC 構成ポートは、Sophos データベースのリスナー・ポートと一致している必要があります。Sophos データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 「データベース・インスタンス」パラメーターでデータベース・インスタンスを定義する場合は、「ポート」パラメーターをブランクのままにしておく必要があります。データベース・サーバーがデフォルトのポート 1433 を使用している場合にのみ、データベース・インスタンスを定義できます。これは標準の Sophos 構成ではありません。
ユーザー名	データベースへのアクセスに必要なユーザー名を入力します。
パスワード	データベースへのアクセスに必要なパスワードを入力します。パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」パラメーターに入力したパスワードと同じでなければなりません。
認証ドメイン	「データベース・タイプ」として **MSDE** を選択し、データベースが Windows 用に構成されている場合は、Window 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 「ポート」パラメーターでデフォルト以外のポート番号を定義した場合、または、SQL データベース解決用のポート 1434 へのアクセスをブロックする場合は、「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを格納するテーブルまたはビューの名前として `siem_view` と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに `*` を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。

表 359. Sophos PureMessage JDBC のパラメーター (続き)

パラメーター	説明
比較フィールド	ID を入力します。「比較フィールド」パラメーターは、テーブルに対する照会から次の照会までの間に追加された新規イベントの識別に使用されます。
準備済みステートメントの使用 **(Use Prepared Statements)**	準備済みステートメントを使用する場合は、このチェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH:mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。「開始日時」パラメーターをクリアすると、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力した数値の場合は、秒単位のポーリングになります。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

注**:** 「信頼性」パラメーターに 5 より大きい値を選択すると、Sophos PureMessage ログ・ソースに対し、QRadar 内の他のログ・ソースよりも高い重要度が設定されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

QRadar と Sophos PureMessage for Linux との統合

IBM Security QRadar は、Sophos PureMessage for Linux と統合することができます。

手順

1. Sophos PureMessage PostgreSQL データベース・ディレクトリーに移動します。

   ```
   cd /opt/pmx/postgres-8.3.3/bin
   ```

2. pmx_quarantine データベース SQL プロンプトにアクセスします。

   ```
   ./psql -d pmx_quarantine
   ```

3. 以下のコマンドを入力して、Sophos データベースに QRadar をサポートする SIEM ビューを作成します。

   ```
   create view siem_view as select
   'Linux PureMessage' as application, id,
   b.name, m_date, h_from_local, h_from_domain,
   m_global_id, m_message_size, outbound,
   h_to, c_subject_utf8 from message a,
   m_reason b where a.reason_id = b.reason_id;
   ```

次のタスク

データベース・ビューを作成したら、JDBC プロトコルを使用してイベント情報を受信するように、QRadar を構成する必要があります。

Sophos PureMessage for Microsoft Exchange のログ・ソースの構成

IBM Security QRadar を、JDBC プロトコルを使用して Sophos PureMessage データベースにアクセスするように構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース・タイプ」リストで、「**Sophos PureMessage**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。

注**:** QRadar で Sophos PureMessage DSM の構成に必要なパラメーターを定義するには、Sophos PureMessage の「データベース設定の構成 **(Configure Database Settings)**」を参照する必要があります。

8. 以下の値を構成します。

Sophos PureMessage JDBC のパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<Sophos PureMessage* データベース*>@<Sophos PureMessage* データベース・サーバー *IP* またはホスト名*>* 各部分について以下で説明します。 • *<Sophos PureMessage* データベース*>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<Sophos PureMessage* データベース・サーバー *IP* またはホスト名*>* は、「IP またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。 ログ・ソース ID の定義時に、Sophos PureMessage デバイスのデータベースの値、およびデータベース・サーバー IP アドレスまたはホスト名の値を使用する必要があります。
データベース・タイプ	リストから「**Postgres**」を選択します。
データベース名	`pmx_quarantine` と入力します。
IP またはホスト名	Sophos PureMessage サーバーの IP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。デフォルトのポートは 1532 です。 JDBC 構成ポートは、Sophos データベースのリスナー・ポートと一致している必要があります。Sophos データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。
ユーザー名	データベースへのアクセスに必要なユーザー名を入力します。
パスワード	データベースへのアクセスに必要なパスワードを入力します。パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」パラメーターに入力したパスワードと同じでなければなりません。
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスをブロックしている場合は、構成内の「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。

Sophos PureMessage JDBC のパラメーター

パラメーター	説明
テーブル名	イベント・レコードを格納するテーブルまたはビューの名前として siem_view と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに * を入力します。 ご使用の構成に必要な場合は、コンマ区切りリストを使用して、テーブルまたはビューの特定のフィールドを定義することができます。このリストには、比較フィールド・パラメーターで定義したフィールドを含める必要があります。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	ID を入力します。 「比較フィールド」パラメーターは、テーブルに対する照会から次の照会までの間に追加された新規イベントの識別に使用されます。
準備済みステートメントの使用 **(Use Prepared Statements)**	準備済みステートメントを使用する場合は、このチェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。「開始日時」パラメーターをクリアすると、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力した数値の場合は、秒単位のポーリングになります。

注**:** 「信頼性」パラメーターに 5 より大きい値を選択すると、Sophos PureMessage ログ・ソースに対し、QRadar 内の他のログ・ソースよりも高い重要度が設定されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

Sophos Astaro Security Gateway

IBM Security QRadar 用の Sophos Astaro Security Gateway DSM は、syslog を使用してイベントを受け入れ、QRadar は関連するすべてのイベントを記録できます。

このタスクについて

Sophos Astaro Security Gateway の syslog を構成するには、以下の手順を実行します。

手順

1. Sophos Astaro Security Gateway コンソールにログインします。
2. ナビゲーション・メニューから、「ロギング **(Logging)**」 > 「設定 **(Settings)**」を選択します。
3. 「リモート **Syslog** サーバー **(Remote Syslog Server)**」タブをクリックします。

   「リモート Syslog ステータス (Remote Syslog Status)」ウィンドウが表示されます。
4. 「**Syslog** サーバー **(Syslog Servers)**」パネルで、「**+**」アイコンをクリックします。

   Syslog サーバーの追加 (Add Syslog Server)」ウィンドウが表示されます。
5. 以下のパラメーターを構成します。
   a. 名前 **(Name)** - syslog サーバーの名前を入力します。
   b. サーバー **(Server)** - フォルダー・アイコンをクリックして、事前定義のホストを追加するか、「**+**」をクリックして、新規のネットワーク定義を入力します。
   c. ポート **(Port)** - フォルダー・アイコンをクリックして事前定義のポートを追加するか、「**+**」をクリックして新規のサービス定義を入力します。 デフォルトでは、QRadar は、UDP/TCP ポート 514 で syslog プロトコルを使用して通信します。
   d. 「保存」をクリックします。
6. 「リモート **syslog** ログの選択 **(Remote syslog log selection)**」フィールドでは、以下のログのチェック・ボックスを選択する必要があります。
   a. **POP3** プロキシー **(POP3 Proxy)** - このチェック・ボックスを選択します。
   b. パケット・フィルター **(Packet Filter)** - このチェック・ボックスを選択します。
   c. パケット・フィルター **(Packet Filter)** - このチェック・ボックスを選択します。
   d. 侵入防止システム **(Intrusion Prevention System)** - このチェック・ボックスを選択します。
   e. コンテンツ・フィルター **(HTTPS) (Content Filter(HTTPS))** - このチェック・ボックスを選択します。
   f. 高可用性 **(High availability)** - このチェック・ボックスを選択します。

g. **FTP** プロキシー **(FTP Proxy)** - このチェック・ボックスを選択します。

h. **SSL VPN** - このチェック・ボックスを選択します。

i. **PPTP** デーモン **(PPTP daemon)** - このチェック・ボックスを選択します。

j. **IPSEC VPN** - このチェック・ボックスを選択します。

k. **HTTP** デーモン **(HTTP daemon)** - このチェック・ボックスを選択します。

l. ユーザー認証デーモン **(User authentication daemon)** - このチェック・ボックスを選択します。

m. **SMTP** プロキシー **(SMTP proxy)** - このチェック・ボックスを選択します。

n. 「適用」をクリックします。

o. 「リモート **syslog** ステータス **(Remote syslog status)**」セクションで「有効 **(Enable)**」をクリックします。

これで、QRadar でログ・ソースを構成できるようになりました。

7. Sophos Astaro Security Gateway デバイスからのイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**Sophos Astaro Security Gateway**」を選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Sophos Web セキュリティー・アプライアンス

IBM Security QRadar 用の Sophos Web Security Appliance (WSA) DSM は、syslog を使用してイベントを受け入れます。

このタスクについて

QRadar は、Sophos Web Security Appliance のトランザクション・ログから転送される、関連するすべてのイベントを記録します。QRadar を構成する前に、syslog イベントを転送するように Sophos WSA Appliance を構成しておく必要があります。

syslog イベントを転送するように Sophos Web Security Appliance を構成するには、以下の手順を実行します。

手順

1. Sophos Web Security Appliance にログインします。
2. メニューから、「構成 **(Configuration)**」 > 「システム **(System)**」 > 「アラートと監視 **(Alerts & Monitoring)**」を選択します。
3. 「**Syslog**」タブを選択します。

4. 「**Web** トラフィックの **syslog** 転送を有効にする **(Enable syslog transfer of web traffic)**」チェック・ボックスを選択します。
5. 「ホスト名**/IP (Hostname/IP)**」テキスト・ボックスに、QRadar の IP アドレスまたはホスト名を入力します。
6. 「ポート **(Port)**」テキスト・ボックスに 514 と入力します。
7. 「プロトコル **(Protocol)**」リストから、プロトコルを選択します。オプションは以下のとおりです。
   - 「**TCP**」 - QRadar ではポート 514 で TCP プロトコルがサポートされます。
   - 「**UDP**」 - QRadar ではポート 514 で UDP プロトコルがサポートされます。
   - 「**TCP - Encrypted**」 - TCP 暗号化は、QRadar でサポートされないプロトコルです。
8. 「適用」をクリックします。 これで、QRadar での Sophos Web Security Appliance DSM の構成が可能になりました。
9. QRadar は、Sophos Web Security Appliance からの syslog データを自動的に検出します。Sophos Web Security Appliance からのイベントを受信するように QRadar を手動で構成するには、「ログ・ソース・タイプ」リストから「**Sophos Web Security Appliance**」を選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 121 章 Splunk

IBM Security QRadar は、Splunk アプライアンスから転送された複数のイベント・タイプを受け取って解析します。

Splunk から転送される Check Point イベントについては、 225 ページの『第 29 章 Check Point』を参照してください。

Splunk アプライアンスから転送された Windows イベントの収集

イベントを収集するために、Windows エンドポイントを構成して、イベントを QRadar コンソールおよび Splunk インデクサーに転送することができます。

Splunk デプロイメントで集約ノードから Windows イベントを転送することは推奨されません。複数の Windows エンドポイントから QRadar にイベントを転送する Splunk インデクサーの場合は、Splunk インデクサーの IP アドレスによってイベント本来のソースが分からなくなることがあります。ログ・ソースで誤った IP アドレスが関連付けられる事態を防ぐために、Windows エンドポイント・システムを更新し、インデクサーと QRadar コンソールの両方に転送することができます。

Splunk イベントは、TCP multiline syslog プロトコルによって Microsoft Windows セキュリティー・イベント・ログ DSM を使用して解析されます。プロトコルで構成された正規表現によって、イベント・ペイロードでの Splunk イベントの開始位置および終了位置が定義されます。イベント・パターンにより、QRadar が、Windows ロー・イベントのペイロードを QRadar による読み取りが可能な単一行イベントに構成することができます。Windows イベントの収集に必要な正規表現については、ログ・ソースの構成で説明します。

Splunk syslog イベントのイベント収集を構成するには、以下の作業を行う必要があります。

1. QRadar アプライアンスで、Microsoft Windows セキュリティー・イベント・ログ DSM を使用するようにログ・ソースを構成します。

   注: Splunk イベントに対して構成する必要があるログ・ソースは 1 つです。QRadar は、最初のログ・ソースを使用して他の Windows エンドポイントを自動検出することができます。
2. Splunk アプライアンスで、Windows イベント・データを QRadar コンソールまたはイベント・コレクター (Event Collector)に送信するように Windows インスタンスの各 Splunk Forwarder を構成します。

   Splunk Forwarder を構成するには、`props.conf`、`transforms.conf`、および `output.conf` の各構成ファイルを編集する必要があります。イベントの転送について詳しくは、Splunk の資料を参照してください。
3. ファイアウォール・ルールが Splunk アプライアンスと QRadar コンソールまたはイベント取得の役割を担う管理対象ホストの間の通信をブロックしていないことを確認します。

4. QRadar アプライアンスで「ログ・アクティビティー」タブを確認し、Splunk イベントが QRadar に転送されることを確認します。

Splunk 転送イベントのログ・ソースの構成

Splunkから転送される Raw Event を収集するには、IBM Security QRadar でログ・ソースを構成する必要があります。

始める前に

Splunk 転送機能で、転送機能が生データを QRadar に送信するように、「**sendCookedData**」を **false** に設定する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. オプション: 「ログ・ソースの説明」フィールドに、ログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「Microsoft Windows セキュリティー・イベント・ログ」を選択します
9. 「プロトコル構成」リストで、「**TCP 複数行 syslog (TCP Multiline Syslog)**」を選択します。
10. 以下の値を構成します。

表 *360. TCP 複数行 syslog* のプロトコル・パラメーター

パラメーター	説明
ログ・ソース **ID**	Splunk アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。 ログ・ソース ID は、固有値でなければなりません。

表 *360. TCP* 複数行 *syslog* のプロトコル・パラメーター *(*続き*)*

パラメーター	説明
Listen ポート	QRadar が、Splunk から着信 TCP の複数行 Syslog イベントを受け入れる際に使用するポート番号を入力します。 デフォルトの Listen ポートは 12468 です。 **重要:** Listen ポート 514 は使用しないでください。 QRadar で構成するポート番号は、Splunk Forwarder で構成されているポート番号と一致する必要があります。QRadar 内の各 Listen ポートは、Forwarder のインバウンド接続を最大で 50 件まで受け入れます。 Forwarder 接続がさらに必要な場合は、複数の Splunk Forwarder ログ・ソースを別のポート上に作成します。接続制限は、各 Forwarder 接続から入ってくるログ・ソース数ではなく、Forwarder 接続数を参照します。
イベント・フォーマッター **(Event Formatter)**	リストから、Windows 「複数行」を選択します。 イベント・フォーマッターにより、選択したイベント・タイプのイベント・パターンと TCP 複数行イベントのフォーマットが一致することが保証されます。
イベント開始パターン **(Event Start Pattern)**	Splunk Windows イベントの開始を識別するための以下の正規表現 (regex) を入力します。 `(?:<(¥d+)>¥s?(¥w{3} ¥d{2} ¥d{2}:¥d{2}:¥d{2}) (¥S+) )?(¥d{2}/¥d{2}/¥d{4} ¥d{2}:¥d{2}:¥d{2} [AP]M)` TCP 複数行 syslog プロトコルは、定義された正規表現パターンの各オカレンス間のすべての情報をキャプチャーして、単一行の syslog イベントを作成します。
イベント終了パターン **(Event End Pattern)**	このフィールドのすべての正規表現パターンを消去することができます。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
信頼性	リストから、ログ・ソースの信頼性を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。

表 *360. TCP* 複数行 *syslog* のプロトコル・パラメーター *(*続き*)*

パラメーター	説明
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	リストから、ログの解析と保管を行うための受信ペイロード・エンコーダーを選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。
13. オプション: Windows のソースが 50 個以上ある場合は、このプロセスを繰り返して、別のログ・ソースを作成する必要があります。

    Splunk Forwarder により QRadar に提供されるイベントは、「ログ・アクティビティー」タブに表示されます。

第 122 章 Squid Web プロキシー

IBM Security QRadar 用の Squid Web プロキシー DSM は、syslog を使用してキャッシュおよびアクセス・ログ・イベントをすべて記録します。

QRadar を Squid Web プロキシーと統合するには、syslog を使用してキャッシュおよびアクセス・ログを転送するように Squid Web プロキシーを構成する必要があります。

Syslog の転送の構成

Syslog を使用してアクセス・イベントとキャッシュ・イベントを転送するように Squid を構成できます。

手順

1. SSH を使用して Squid デバイスのコマンド・ライン・インターフェースにログインします。
2. 以下のファイルを開きます。

   ```
   /etc/rc3.d/S99local
   ```

3. 以下の行を追加します。

   ```
   tail -f /var/log/squid/access.log | logger -p <facility>.<priority> &
   ```

   - <facility> は、小文字で記述された任意の有効な Syslog ファシリティー (authpriv、daemon、local0 から local7、user など) です。
   - *<priority>* は、小文字で記述された任意の有効な優先順位 (err、warning、notice、info、debug) です。

4. ファイルを保存して閉じます。

   ロギングは、システムの次回再始動時に開始されます。

5. ロギングをすぐに開始するには、以下のコマンドを入力します。

   ```
   nohup tail -f /var/log/squid/access.log | logger -p
   <facility>.<priority> &
   ```

   <facility> オプションと *<priority>* オプションは、入力したのと同じ値です。

6. 以下のファイルを開きます。

   ```
   /etc/syslog.conf
   ```

7. 以下の行を追加して、ログを QRadar に送信します。

   ```
   <priority>.<facility> @<QRadar_IP_address>
   ```

   Squid メッセージに対する優先順位とファシリティー、および QRadar の IP アドレスを次の例に示します。

```
info.local4 @172.16.210.50
```

8. 次の行を squid.conf ファイルに追加して、httpd ログ・ファイル・エミュレーションをオフにします。

```
emulate_httpd_log_off
```

9. 次のオプションのいずれかを選択してください。
   - Squid サービスを再開するために、次のコマンドを入力します。

     ```
     service squid restart
     ```

   - サービスを再開せずに構成を再ロードするために、次のコマンドを入力します。

     ```
     /usr/sbin/squid -k reconfigure
     ```

10. ファイルを保存して閉じます。
11. 以下のコマンドを入力して、syslog デーモンを再始動します。

```
/etc/init.d/syslog restart
```

Squid の構成方法について詳しくは、ベンダーの資料を参照してください。

タスクの結果

キャッシュとアクセス・ログの Syslog 転送を構成したら、構成は完了します。QRadar は、Squid から転送された syslog イベントを自動的に検出することができます。

ログ・ソースの作成

IBM Security QRadar は Squid Web プロキシー・アプライアンスから転送される syslog イベントのログ・ソースの検出と作成を自動的に実行します。ログ・ソースを作成するための構成手順はオプションです。

このタスクについて

Squid Web プロキシーのログ・ソースを手動で構成するには以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。

7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Squid Web** プロキシー」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコル構成が表示されます。
10. 以下の値を構成します。

表 *361. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Squid Web プロキシーからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    構成は完了です。

第 123 章 SSH CryptoAuditor

SSH CryptoAuditor 用の IBM Security QRadar DSM は、SSH CryptoAuditor からログを収集します。

以下の表は、SSH CryptoAuditor DSM の仕様を示しています。

表 *362. SSH CryptoAuditor DSM* の仕様

仕様	値
製造元	SSH Communications Security
製品	CryptoAuditor
DSM 名	SSH CryptoAuditor
RPM ファイル名	`DSM-SSHCryptoAuditor-QRadar_release-Build_number.noarch.rpm`
サポートされるバージョン	1.4.0 以降
イベント・フォーマット	Syslog
QRadar で記録されるイベント・タイプ	監査、Forensics
QRadar UI でのログ・ソース・タイプ	SSH CryptoAuditor
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	SSH Communications Security Web サイト (http://www.ssh.com/)

SSH CryptoAuditor から QRadar にイベントを送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - SSH CryptoAuditor RPM
2. SSH CryptoAuditor の各インスタンスについて、QRadar と通信するように SSH CryptoAuditor システムを構成します。
3. QRadar が SSH CryptoAuditor を自動的に検出しない場合は、SSH CryptoAuditor のインスタンスごとに、QRadar コンソール上でログ・ソースを作成します。以下の SSH CryptoAuditor 固有のパラメーターを使用します。

パラメーター	値
ログ・ソース・タイプ	SSH CryptoAuditor
プロトコル構成	Syslog

関連タスク:

『QRadar との通信のための SSH CryptoAuditor アプライアンスの構成』
SSH CryptoAuditor イベントを収集するには、イベントを IBM Security QRadar に送信するようにサード・パーティー・アプライアンスを構成する必要があります。

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

QRadar との通信のための SSH CryptoAuditor アプライアンスの構成

SSH CryptoAuditor イベントを収集するには、イベントを IBM Security QRadar に送信するようにサード・パーティー・アプライアンスを構成する必要があります。

手順

1. SSH CryptoAuditor にログインします。
2. 「設定」 > 「外部サービス」 > 「外部 **Syslog** サーバー **(External Syslog Servers)**」の順に、Syslog 設定に移動します。
3. QRadar のサーバー設定を作成するには、「**Syslog** サーバーの追加 **(Add Syslog Server)**」をクリックします。
4. QRadar のサーバー設定、つまりアドレス (IP アドレスまたは FQDN) と QRadar がログ・メッセージを収集するポートを入力します。
5. Syslog 形式をユニバーサル LEEF に設定するには、「**LEEF** 形式 **(Leef format)**」チェック・ボックスを選択します。
6. 構成を保存するには、「保存」をクリックします。
7. 「設定」 > 「アラート」で SSH CryptoAuditor のアラートを構成します。SSH CryptoAuditor のアラート構成により、外部システム (E メールまたは SIEM/Syslog) に送信するイベントを定義します。
   a. 既存のアラート・グループを選択するか、「アラート・グループの追加」をクリックして新規アラート・グループを作成します。
   b. 「外部 **Syslog** サーバー **(External Syslog Server)**」ドロップ・ボックスで前に定義した QRadar サーバーを選択します。
   c. 新規アラート・グループを作成した場合は、「保存」をクリックします。アラートをグループにバインドする前に、グループを保存してください。
   d. アラートをアラート・グループにバインドすることによって、QRadar に送信するアラートを定義します。QRadar で収集するアラートの横の **[+]** をクリックし、QRadar を外部 Syslog サーバーとして持っているアラート・グループを選択します。QRadar で収集するアラートごとに、このステップを繰り返します。
   e. 「保存」をクリックします。
8. 保留中の構成変更を適用します。保存済みの構成変更は、保留状態から適用するまでは有効にはなりません。

第 124 章 Starent Networks

IBM Security QRadar 用の Starent Networks DSM は、イベント、トレース、アクティブ、およびモニターの各イベントを受け入れます。

このタスクについて

QRadar で Starent Networks デバイスを構成する前に、syslog イベントを QRadar に転送するように Starent Networks デバイスを構成しておく必要があります。

syslog イベントを QRadar に送信するようにデバイスを構成するには、以下のようにします。

手順

1. Starent Networks デバイスにログインします。
2. syslog サーバーを構成します。

   ```
   logging syslog <IP address> [facility <facilities>] [<rate value>]
   [pdu-verbosity <pdu_level>] [pdu-data <format>] [event-verbosity
   <event_level>]
   ```

   以下の表は必要なパラメーターを記載しています。

表 363. *Syslog* サーバーのパラメーター

パラメーター	説明
syslog *<IP address>*	QRadar の IP アドレスを入力します。
facility *<facilities>*	ロギング・オプションが適用されるローカル・ファシリティーを入力します。オプションは、以下のとおりです。 • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 デフォルトは local7 です。
rate value	ログ項目をシステムのログ・サーバーに送信する速度を入力します。この値は 0 から 100000 までの整数値にする必要があります。デフォルトは 1 秒あたり 1000 個のイベントです。

表 363. *Syslog* サーバーのパラメーター (続き)

パラメーター	説明
pdu-verbosity <*pdu_level*>	プロトコル・データ単位 (PDU) のロギングで使用する詳細レベルを入力します。範囲は、1 から 5 までです。5 が最も詳細度が高くなります。このパラメーターはプロトコル・ログのみに影響します。
pdu-data <*format*>	ロギング時の PDU の出力フォーマットを、以下のいずれかで入力します。 • none - 未加工または未フォーマットのテキストとして結果を表示します。 • hex - 16 進数形式で結果を表示します。 • hex-ascii - メインフレーム・ダンプと類似した 16 進数および ASCII フォーマットで結果を表示します。
event-verbosity <*event_level*>	イベントのロギングで使用する詳細レベルを入力します。以下のレベルがあります。 • min - イベント名、ファシリティー、イベント ID、重大度レベル、データ、時刻など、イベントに関する最小限の情報を提供します。 • concise - イベントに関する詳細な情報を提供しますが、イベント・ソースは提供しません。 • full - イベントに関する詳細情報を提供し、イベントが生成されたタスクまたはサブシステムを識別するソース情報が含まれます。

3. Exec モードのルート・プロンプトから、トレース・ログが生成されるセッションを識別します。

   ```
   logging trace {callid <call_id> | ipaddr <IP address> | msid <ms_id> |
   name <username>}
   ```

   以下の表は必要なパラメーターを記載しています。

表 364. トレース・ログのパラメーター

パラメーター	説明
callid <*call_id*>	セッションにトレース・ログが生成されたことを示し、このセッションは呼び出し ID 番号で識別されます。この値は 4 バイトの 16 進数です。
ipaddr <*IP address*>	セッションにトレース・ログが生成されたことを示し、このセッションは指定された IP アドレスで識別されます。
msid <*ms_id*>	セッションにトレース・ログが生成されたことを示し、このセッションはモバイル・ステーション ID (MSID) 番号で識別されます。この値は 7 桁から 16 桁で、IMSI、MIN、または RMI として指定されます。

表 *364.* トレース・ログのパラメーター *(*続き*)*

パラメーター	説明
name <*username*>	セッションにトレース・ログが生成されたことを示し、このセッションはユーザー名によって識別されます。この値は、あらかじめ構成されている加入者の名前です。

4. config モードでアクティブ・メモリー・バッファーにアクティブ・ログを書き込むには、以下を実行します。

   ```
   logging runtime buffer store all-events
   ```

5. アクティブ・ログのフィルターを構成します。

   ```
   logging filter active facility <facility> level <report_level>
   [critical-info | no-critical-info]
   ```

   以下の表は必要なパラメーターを記載しています。

表 *365.* アクティブ・ログのパラメーター

パラメーター	説明
facility <facility>	ファシリティーのメッセージ・レベルを入力します。ファシリティーはシステムで使用中のプロトコルまたはタスクです。ローカル・ファシリティーによって、ローカルで実行されるプロセスに適用されるロギング・オプションが定義されます。オプションは、以下のとおりです。 • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 デフォルトは local7 です。

表 *365.* アクティブ・ログのパラメーター *(*続き*)*

パラメーター	説明
level *<report_level>*	以下のログ重大度レベルのいずれかを入力します。 • critical - 重大なエラーの発生を示すイベント、およびシステムまたはシステム・コンポーネントの機能停止の原因になるイベントのみをログに記録します。「critical」が最も高いレベルの重大度です。 • error - システムまたはシステム・コンポーネントの動作が低下状態になるエラーが発生していることを示すイベントをログに記録します。このレベルでは、重大度がこのレベルより高いイベントも記録されます。 • warning - 問題が発生する可能性があることを示すイベントをログに記録します。このレベルでは、重大度がこのレベルより高いイベントも記録されます。 • unusual - 異常であり、調査が必要になる可能性があるイベントをログに記録します。このレベルでは、重大度がこのレベルより高いイベントも記録されます。 • info - 情報イベント、および重大度がこのレベルより高いイベントがログに記録されます。 • debug - 重大度に関係なく、すべてのイベントがログに記録されます。 ログに記録される情報の価値を最大化し、生成されるログの量を少なく抑えるように error または critical のレベルを構成できることが示されています。
critical-info	critical-info パラメーターは、重大な情報のカテゴリー属性があるイベントを識別して表示します。このイベント・タイプの例は、システム・プロセスまたはタスクの開始時に見ることができます。
no-critical-info	no-critical-info パラメーターは、重大な情報のカテゴリー属性のあるイベントが表示されないようにすることを指定します。

6. モニター・ログのターゲットを構成します。

```
logging monitor {msid <ms_id>|username <username>}
```

以下の表は必要なパラメーターを記載しています。

表 *366.* モニター・ログ・パラメーター

パラメーター	説明
msid *<md_id>*	msid を入力して、モバイル・ステーション ID (MSID) 番号を使用して識別されるセッションにモニター・ログが生成されることを定義します。この値は 7 桁から 16 桁で、IMSI、MIN、または RMI として指定されます。

表 *366.* モニター・ログ・パラメーター *(*続き*)*

パラメーター	説明
username *<username>*	ユーザー名を入力して、セッションに生成されたモニター・ログをユーザー名によって識別します。このユーザー名は、あらかじめ構成されている加入者の名前です。

7. これで、QRadar でログ・ソースを構成する準備ができました。

   Starent デバイスからのイベントを受信するように QRadar を構成するには、以下の手順を実行します。

   a. 「ログ・ソース・タイプ」リストから、「**Starent Networks Home Agent (HA)**」オプションを選択します。

      デバイスについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 125 章 STEALTHbits

IBM Security QRadar は STEALTHbits DSM を幅広くサポートしています。

STEALTHbits StealthINTERCEPT

STEALTHbits StealthINTERCEPT 用の IBM Security QRadar DSM は、STEALTHbits StealthINTERCEPT サービスおよび STEALTHbits File Activity Monitor サービスからイベント・ログを収集できます。

以下の表は、STEALTHbits StealthINTERCEPT DSM の仕様を示しています。

表 *367. STEALTHbits StealthINTERCEPT DSM* の仕様

仕様	値
製造元	STEALTHbits Technologies
DSM	STEALTHbits StealthINTERCEPT
RPM ファイル名	`DSM-STEALTHbitsStealthINTERCEPT-`*`QRadar_Version-build_number`*`.noarch.rpm`
サポートされるバージョン	3.3
プロトコル	Syslog
イベント・フォーマット	LEEF
QRadar で記録されるイベント	Active Directory 監査イベント、ファイル・アクティビティー・モニター・イベント
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	http://www.stealthbits.com/resources

IBM Security QRadar での STEALTHbits StealthINTERCEPT のログ・ソースの構成

STEALTHbits StealthINTERCEPT イベントを収集するには、QRadar でログ・ソースを構成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・ペインで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**STEALTHbits StealthINTERCEPT**」を選択します。

7. 「プロトコル構成」リストで「**Syslog**」を選択します。
8. 残りのパラメーターを構成します。
9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

QRadar との通信のための STEALTHbits StealthINTERCEPT の構成

STEALTHbits StealthINTERCEPT からすべての監査ログとシステム・イベントを収集するには、IBM Security QRadar を Syslog サーバーとして指定して、メッセージ・フォーマットを構成する必要があります。

手順

1. STEALTHbits StealthINTERCEPT サーバーにログインします。
2. 管理コンソールを始動します。
3. 「構成」 > 「**Syslog** サーバー」をクリックします。
4. 以下のパラメーターを構成します。

表 *368. Syslog* パラメーター

パラメーター	説明
ホスト・アドレス	QRadar コンソールの IP アドレス
ポート	514

5. 「マッピング・ファイルのインポート **(Import mapping file)**」をクリックします。
6. `SyslogLeefTemplate.txt` ファイルを選択し、Enter キーを押します。
7. 「保存」をクリックします。
8. 管理コンソールで、「アクション」をクリックします。
9. インポートしたマッピング・ファイルを選択し、「**Syslog** に送信 **(Send to Syslog)**」チェック・ボックスを選択します。

   「イベント **DB** に送信 **(Send to Events DB)**」チェック・ボックスは、選択したままにしておきます。 StealthINTERCEPT は、イベント・データベースを使用してレポートを生成します。
10. 「追加」をクリックします。

QRadar との通信のための STEALTHbits File Activity Monitor の構成

STEALTHbits File Activity Monitor からイベント収集するには、IBM Security QRadar を Syslog サーバーとして指定し、メッセージ・フォーマットを構成する必要があります。

手順

1. STEALTHbits File Activity Monitor を実行するサーバーにログインします。
2. 「モニター対象ホスト **(Monitored Hosts)**」タブを選択します。

3. モニター対象ホスト選択し、「編集」をクリックしてホストのプロパティー・ウィンドウを開きます。
4. 「Syslog」タブを選択し、以下のパラメーターを構成します。

パラメーター	説明
サーバー[:ポート] 形式でのバルク Syslog サーバー (Bulk Syslog server in SERVER[:PORT] format)	<*QRadar Event Collector IP* アドレス>:514 例: 1.1.1.1:514 <*qradarhostname*>:514
Syslog メッセージ・テンプレート・ファイル・パス (Syslog message template file path)	`SyslogLeefTemplate.txt` テンプレートは、STEALTHbits File Activity Monitor のインストール・ディレクトリーに格納されています。

5. 「**OK**」をクリックします。

QRadar での STEALTHbits File Activity Monitor のログ・ソースの構成

STEALTHbits File Activity Monitor イベントを収集するには、QRadar で STEALTHbits StealthINTERCEPT ログ・ソースを構成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・ペインで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**STEALTHbits StealthINTERCEPT**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。
8. 残りのパラメーターを構成します。
9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

STEALHbits StealthINTERCEPT DSM のサンプル・イベント・メッセージを次の表に示します。

表 *369. STEALTHbits StealthINTERCEPT DSM* でサポートされる *STEALTHbits StealthINTERCEPT* および *STEALTHbits File Activity Monitor* のサンプル・イベント・メッセージ

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
Active Directory グループの作成	追加されたグループ	LEEF:1.0|STEALTHbits |StealthINTERCEPT| 2.6.297.1| Active Directorygroup Object AddedTrueFalse| cat=Object Added devTimeFormat=yyyy-MM-dd HH:mm:ss.SSS devTime=2013- 10-24 15:41:38.387 SettingName=All AD Changes domain=2008R264 BITDOM usrName=CN=Administrator, CN=Users, DC=2008R264BitDomain, DC=com src=LDAP:[fe80::741e:5e04: e643:28b5%10]:60843 DistinguishedName= cn=asdfasdfasdf, OU=American Fork, OU=Utah, DC=2008R264BitDomain, DC=com ClassName=group OrigServer=2008R264BITDOM ¥2008R264BITSRVR Success=True Blocked=False AttNames= AttNewValues= AttOldValues=

表 *369. STEALTHbits StealthINTERCEPT DSM* でサポートされる *STEALTHbits StealthINTERCEPT* および *STEALTHbits File Activity Monitor* のサンプル・イベント・メッセージ *(*続き*)*

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
Windows ファイル・システムのフォルダーまたはファイルの削除	削除されたファイル	LEEF:1.0|STEALTHbits |STEALTHbits Technologies File Monitoring| 2,3,0,402|Windows File SystemDeleteTrueFalse| cat=Delete devTimeFormat=yyyy-MM-dd HH:mm:ss.SSS devTime=2016-04-19 13:15:12.000 SettingName=FileMonitor domain=SBPMLAB usrName=SBPMLAB¥ajnish src=192.168.30.1 DistinguishedName=C:¥ Share1_CIFS_volume¥1 (2) - Copy ClassName= OrigServer=SBPMLABNA832 Success=True Blocked=False AttrName= AttrNewValue= AttrOldValue= Operation=

STEALTHbits StealthINTERCEPT Alerts

IBM Security QRadar は、STEALTHbits StealthINTERCEPT Alerts DSM を使用して、STEALTHbits StealthINTERCEPT サーバーからアラート・ログを収集します。

以下の表は、STEALTHbits StealthINTERCEPT Alerts DSM の仕様を示しています。

表 *370. STEALTHbits StealthINTERCEPT Alerts DSM* の仕様

仕様	値
製造元	STEALTHbits Technologies
DSM 名	STEALTHbits StealthINTERCEPT Alerts
RPM ファイル名	DSM-STEALTHbitsStealthINTERCEPTAlerts-*Qradar_version-build_number*.noarch.rpm
サポートされるバージョン	3.3
プロトコル	Syslog LEEF
記録されるイベント・タイプ	Active Directory アラート・イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ

表 370. STEALTHbits StealthINTERCEPT Alerts DSM の仕様 (続き)

仕様	値
その他の情報	StealthINTERCEPT (http://www.stealthbits.com/products/stealthintercept)

STEALTHbits StealthINTERCEPT を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - `DSMCommon` RPM
   - `STEALTHbitsStealthINTERCEPT` RPM
   - `STEALTHbitsStealthINTERCEPTAlerts` RPM
2. Syslog イベントを QRadar に送信するように STEALTHbits StealthINTERCEPT デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで STEALTHbits StealthINTERCEPT Alerts ログ・ソースを追加してください。以下の表は、STEALTHbits StealthINTERCEPT Alerts イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 371. STEALTHbits StealthINTERCEPT Alerts ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	STEALTHbits StealthINTERCEPT Alerts
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

STEALTHbits StealthINTERCEPT からのアラート・ログの収集

STEALTHbits StealthINTERCEPT からすべてのアラート・ログを収集するには、IBM Security QRadar を Syslog サーバーとして指定し、メッセージ・フォーマットを構成する必要があります。

手順

1. STEALTHbits StealthINTERCEPT サーバーにログインします。
2. 管理コンソールを始動します。
3. 「構成」 > 「**Syslog** サーバー」をクリックします。
4. 以下のパラメーターを構成します。

パラメーター	説明
ホスト・アドレス	QRadar コンソールの IP アドレス
ポート	514

5. 「マッピング・ファイルのインポート **(Import mapping file)**」をクリックします。
6. **SyslogLeefTemplate.txt** ファイルを選択し、Enter キーを押します。
7. 「保存」をクリックします。
8. 管理コンソールで、「アクション」をクリックします。
9. インポートしたマッピング・ファイルを選択し、「**Syslog** に送信 **(Send to Syslog)**」チェック・ボックスを選択します。

   ヒント**:** 「イベント **DB** に送信 **(Send to Events DB)**」チェック・ボックスは、選択したままにしておきます。 StealthINTERCEPT は、イベント・データベースを使用してレポートを生成します。
10. 「追加」をクリックします。

STEALTHbits StealthINTERCEPT Analytics

IBM Security QRadar は、STEALTHbits StealthINTERCEPT Analytics DSM を使用して、STEALTHbits StealthINTERCEPT サーバーから分析ログを収集します。

以下の表は、STEALTHbits StealthINTERCEPT Analytics DSM の仕様を示しています。

表 372. STEALTHbits StealthINTERCEPT Analytics DSM の仕様

仕様	値
製造元	STEALTHbits Technologies
DSM 名	STEALTHbits StealthINTERCEPT Analytics
RPM ファイル名	`DSM-STEALTHbitsStealthINTERCEPTAnalytics-`*`Qradar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	3.3
プロトコル	Syslog LEEF
記録されるイベント・タイプ	Active Directory 分析イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	StealthINTERCEPT (http://www.stealthbits.com/products/stealthintercept)

次の手順を実行することで、STEALTHbits StealthINTERCEPT を QRadar と統合します。

1. 自動更新が有効になっていない場合は、次の RPM の最新バージョンをリストされている順序でダウンロードして QRadar コンソールにインストールしてください。

- DSMCommon RPM
- STEALTHbitsStealthINTERCEPT RPM
- STEALTHbitsStealthINTERCEPTAnalytics RPM

2. Syslog イベントを QRadar に送信するように STEALTHbits StealthINTERCEPT デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで STEALTHbits StealthINTERCEPT Analytics ログ・ソースを追加してください。以下の表は、STEALTHbits StealthINTERCEPT Analytics イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 373. *STEALTHbits StealthINTERCEPT Analytics* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	STEALTHbits StealthINTERCEPT Analytics
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『STEALTHbits StealthINTERCEPT からの分析ログの収集』
STEALTHbits StealthINTERCEPT からすべての分析ログを収集するには、IBM Security QRadar を Syslog サーバーとして指定し、メッセージ・フォーマットを構成する必要があります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

STEALTHbits StealthINTERCEPT からの分析ログの収集

STEALTHbits StealthINTERCEPT からすべての分析ログを収集するには、IBM Security QRadar を Syslog サーバーとして指定し、メッセージ・フォーマットを構成する必要があります。

手順

1. STEALTHbits StealthINTERCEPT サーバーにログインします。
2. 管理コンソールを始動します。
3. 「構成」 > 「**Syslog** サーバー」をクリックします。
4. 以下のパラメーターを構成します。

パラメーター	説明
ホスト・アドレス	QRadar コンソールの IP アドレス
ポート	514

5. 「マッピング・ファイルのインポート **(Import mapping file)**」をクリックします。
6. **SyslogLeefTemplate.txt** ファイルを選択し、Enter キーを押します。

7. 「保存」をクリックします。
8. 管理コンソールで、「アクション」をクリックします。
9. インポートしたマッピング・ファイルを選択し、「**Syslog** に送信 **(Send to Syslog)**」チェック・ボックスを選択します。

   ヒント**:** 「イベント **DB** に送信 **(Send to Events DB)**」チェック・ボックスは、選択したままにしておきます。 StealthINTERCEPT は、イベント・データベースを使用してレポートを生成します。
10. 「追加」をクリックします。

第 126 章 Stonesoft Management Center

IBM Security QRadar 用の Stonesoft Management Center DSM は syslog を使用してイベントを受け取ります。

QRadar は、LEEF 形式の関連する syslog イベントをすべて記録します。QRadar を構成する前に、LEEF 形式の syslog イベントをエクスポートするように Stonesoft Management Center を構成する必要があります。

本書では、LogServerConfiguration.txt ファイルの編集に必要な手順についても説明しています。テキスト・ファイルを構成することで、Stonesoft Management Center が syslog を使用して LEEF 形式のイベント・データを QRadar にエクスポートすることができます。構成に関する詳細については、「StoneGate Management Center Administrator's Guide」を参照してください。

Stonesoft Management Center の構成

Stonesoft Management Center は構成できます。

手順

1. Stonesoft Management Center をホストするアプライアンスにログインします。
2. Stonesoft Management Center の Log Server を停止します。
3. Windows の場合 - 以下の方法のいずれかを選択して、Log Server を停止します。
   - Windows の「サービス」一覧で Log Server を停止します。
   - バッチ・ファイル <installation path>/bin/sgStopLogSrv.bat を実行します。

   Linux の場合 - Linux で Log Server を停止するには、スクリプト <installation path>/bin/sgStopLogSrv.sh を実行します。
4. LogServerConfiguration.txt ファイルを編集します。構成ファイルは以下のディレクトリーにあります。

   <installation path>/data/LogServerConfiguration.txt
5. LogServerConfiguration.txt ファイルで以下のパラメーターを構成します。

表 374. *Log Server* の構成オプション

パラメーター	値	説明
SYSLOG_EXPORT_FORMAT	LEEF	syslog に使用するエクスポート形式として LEEF と入力します。
SYSLOG_EXPORT_ALERT	YES | NO	以下の値のいずれかを入力します。 • tableBullets

表 374. *Log Server* の構成オプション (続き)

パラメーター	値	説明
SYSLOG_EXPORT_FW	YES | NO	以下の値のいずれかを入力します。 • Yes - syslog を使用してアラート項目を QRadar にエクスポートします。 • No - syslog を使用した、アラート項目のエクスポートは行われません。
SYSLOG_EXPORT_IPS	YES | NO	以下の値のいずれかを入力します。 • Yes - syslog を使用してファイアウォール項目と VPN 項目を QRadar にエクスポートします。 • No - syslog を使用した、ファイアウォール項目と VPN 項目のエクスポートは行われません。
SYSLOG_PORT	514	syslog イベントを QRadar に転送する UDP ポートとして 514 と入力します。
SYSLOG_SERVER_ADDRESS	QRadar IPv4 アドレス	QRadar コンソールまたはイベント・コレクター (Event Collector)の IPv4 アドレスを入力します。

6. LogServerConfiguration.txt ファイルを保存します。
7. Log Server を始動します。
   - Windows - <インストール・パス>/bin/sgStartLogSrv.bat と入力します。
   - Linux - <インストール・パス>/bin/sgStartLogSrv.sh と入力します。

次のタスク

これで、syslog のトラフィック・ルールを構成することができます。

注: ファイアウォール・ルールは、使用する QRadar コンソールまたはイベント・コレクター (Event Collector)がファイアウォールによって Stonesoft Management Server と隔てられている場合にのみ必要になります。Stonesoft Management Server と QRadar の間にファイアウォールが存在しない場合は、QRadar でログ・ソースを構成する必要があります。

syslog トラフィック・ルールの構成

ネットワーク内で Stonesoft Management Center と QRadar がファイアウォールによって隔てられている場合は、ファイアウォールまたは IPS ポリシーを変更して Stonesoft Management Center と QRadar 間のトラフィックを許可する必要があります。

手順

1. Stonesoft Management Center で、以下のいずれかのトラフィック・ルール変更方法を選択します。

- ファイアウォール ポリシー **(Firewall policies)** - 「構成 **(Configuration)**」 > 「構成 **(Configuration)**」 > 「ファイアウォール **(Firewall)**」を選択します。
- **IPS** ポリシー **(IPS policies)** - 「構成 **(Configuration)**」 > 「構成 **(Configuration)**」 > 「**IPS**」を選択します。

2. 変更するポリシーのタイプを選択します。
   - ファイアウォール **(Firewall)** - 「ファイアウォール・ポリシー **(Firewall Policies)**」 > 「ファイアウォール・ポリシーの編集 **(Edit Firewall Policy)**」を選択します。
   - **IPS** - 「**IPS** ポリシー **(IPS Policies)**」 > 「ファイアウォール・ポリシーの編集 **(Edit Firewall Policy)**」を選択します。
3. 以下の値を使用して、IPv4 アクセス・ルールをファイアウォール・ポリシーに追加します。

   ソース **(Source)** - Stonesoft Management Center Log Server の IPv4 アドレスを入力します。
4. 宛先 **(Destination)** - QRadar コンソールまたはイベント・コレクター (Event Collector)の IPv4 アドレスを入力します。
5. サービス **(Service)** - 「**Syslog (UDP)**」を選択します。
6. アクション **(Action)** - 「許可 **(Allow)**」を選択します。
7. ロギング **(Logging)** - 「なし **(None)**」を選択します。

   注**:** ほとんどのケースでロギング値を「なし **(None)**」に設定することをお勧めします。syslog 接続のロギングで syslog フィルターが構成されていないと、ループが発生する場合があります。詳しくは、「*StoneGate Management Center Administrator's Guide*」を参照してください。
8. 変更内容を保存して、ファイアウォールまたは IPS のポリシーを更新します。

   これで、QRadar でログ・ソースを構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar は、Stonesoft Management Center の syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。

7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Stonesoft Management Center**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *375. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Stonesoft Management Center アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 127 章 Sun

IBM Security QRadar は Sun DSM を幅広くサポートしています。

Sun ONE LDAP

QRadar 用の Sun ONE LDAP DSM は、Sun ONE Directory Server からの複数行の UDP アクセス・イベントおよび LDAP イベントを受け入れます。

Sun ONE LDLAP は、Oracle Directory Server として知られています。

QRadar は、イベント・ログのダウンロード対象の各サーバーに接続することで、Sun ONE Directory Server からアクセスおよび LDAP イベントを取得します。イベント・ファイルは、QRadar のログ・ファイル・プロトコル (FTP、SFTP、または SCP) によってアクセス可能な場所に書き込まれる必要があります。イベント・ログは、複数行のイベント形式が書き込まれます。この形式で、適切にイベントを解析するには、ログ・ファイル・プロトコルに特殊なイベント・ジェネレーターが必要です。ID-Linked Multiline イベント・ジェネレーターは、複数行のイベントの各行が共通の開始値を共有するときに QRadar に対する複数行のイベントを組み立てるのに正規表現を使用できます。

Sun ONE LDAP DSM は、UDP Multiline Syslog プロトコルを使用してストリーミングされたイベントも受け入れます。ただし、ほとんどの状況で、イベント・ログを QRadar に転送するには、サード・パーティー製の Syslog 転送機能がシステムに必要です。この場合、QRadar コンソール上のトラフィックを、UDP Multiline プロトコルによって定義されているポートを使用するように転送することが必要になる可能性があります。

関連概念:

41 ページの『UDP 複数行 Syslog プロトコルの構成オプション』
単一行 Syslog イベントを複数行イベントから作成するには、UDP 複数行プロトコルを使用するようにログ・ソースを構成します。UDP 複数行 Syslog プロトコルは、正規表現を使用して複数行 Syslog メッセージを識別し、単一のイベント・ペイロードに再組み立てします。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Sun ONE Directory Server 用のイベント・ログの有効化

Sun ONE Directory Server からイベントを収集するには、イベント・ログがファイルにイベントを書き込むのを有効にする必要があります。

手順

1. Sun ONE Directory Server コンソールにログインします。
2. 「構成 **(Configuration)**」タブをクリックします。
3. ナビゲーション・メニューで、「**Logs**」を選択します。
4. 「**Access Log**」タブをクリックします。
5. 「ロギングの有効化 **(Enable Logging)**」チェック・ボックスを選択します。
6. Sun ONE Directory Server のアクセス・ログへのディレクトリー・パスを入力するか、「**Browse**」をクリックして指定します。
7. 「保存」をクリックします。

次のタスク

これで、ログ・ソースを QRadar で構成することができます。

Sun ONE LDAP のログ・ソースの構成

イベントを受信するには、Sun ONE Directory サーバー用のログ・ソースを手動で作成する必要があります。QRadar は、ログ・ファイル・プロトコル・イベントを自動的に検出することはありません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リスト・ボックスで、「**Sun ONE LDAP**」を選択します。
9. 「プロトコル構成」リスト・ボックスで「ログ・ファイル」を選択します。
10. 「**Event Generator**」リスト・ボックスで、「**ID-Linked Multiline**」を選択します。
11. 「**Message ID Pattern**」フィールドに、複数行のイベントを定義する正規表現として `conn=(¥d+)` と入力します。
12. 以下のログ・ファイル・プロトコル・パラメーターを構成します。

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。IP アドレスまたはホスト名によって、QRadar が固有のイベント・ソースに対するログ・ファイルを識別できるようになります。 例えば、ネットワークに複数のデバイス (管理コンソール、ファイル・リポジトリーなど) が含まれている場合、イベントを作成したデバイスの IP アドレスまたはホスト名を指定します。これにより、管理コンソールまたはファイル・リポジトリーに対するイベントを識別する代わりに、ネットワーク内のデバイス・レベルでイベントを識別できるようになります。
サービス・タイプ	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。有効な範囲は、1 から 65535 です。オプションは、以下のとおりです。 **FTP** TCP Port 21。 **SFTP** TCP Port 22。 **SCP** TCP Port 22。 **重要:** イベント・ファイルのホストが FTP、SFTP、または SCP に非標準のポート番号を使用する場合は、ポート値を調整する必要があります。
リモート・ユーザー	イベント・ファイルが含まれているホストにログインするために必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
パスワードの確認	ホストにログインするために必要なパスワードを確認します。
SSH 鍵ファイル	「**Service Type**」として SCP または SFTP を選択すると、このパラメーターにより SSH 秘密鍵ファイルを定義できます。 SSH 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。

パラメーター	説明
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 **重要:** FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。これは、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートするためです。
再帰的 **(Recursive)**	FTP 接続または SFTP 接続で、リモート・ディレクトリーのサブフォルダー内のイベント・データを再帰的に検索できるようにするには、このチェック・ボックスを有効にします。サブフォルダーから収集されるデータは、FTP ファイル・パターン内の正規表現に一致するかどうかに依存します。 「**Recursive**」オプションは、SCP 接続では使用できません。
FTP ファイル・パターン	サービス・タイプとして SFTP または FTP を選択すると、このオプションにより、リモート・ディレクトリーで指定されているファイルのリストをフィルターに掛けるために必要な正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 例えば、log という単語で始まり 1 つ以上の数字が続き、tar.gz で終わるファイルをすべてリストするには、log[0-9]+¥.tar¥.gz を使用します。このパラメーターの使用には、正規表現 (regex) の知識が必要です。正規表現について詳しくは、Oracle の Web サイト (http://docs.oracle.com/javase/tutorial/essential/regex/) を参照してください。

パラメーター	説明
FTP 転送モード	このオプションは、FTP をサービス・タイプとして選択した場合にのみ表示されます。「FTP Transfer Mode」パラメーターにより、FTP 経由でログ・ファイルを取得するときのファイル転送モードを定義できます。 リスト・ボックスから、このログ・ソースに適用する転送モードを選択します。 バイナリー バイナリー・データ・ファイル、または圧縮された zip、gzip、tar、tar + gzip のアーカイブ・ファイルを必要とするログ・ソースには、「バイナリー」を選択します。 **ASCII** ASCII FTP ファイル転送を必要とするログ・ソースには、「**ASCII**」を選択します。 **重要:** FTP 転送モードとして ASCII を使用するときは、「**Processor**」パラメーターに「**NONE**」を、「**Event Generator**」に「**LINEBYLINE**」を選択する必要があります。
SCP リモート・ファイル	「サービス・タイプ」として SCP を選択した場合は、リモート・ファイルのファイル名を入力する必要があります。
開始時刻	処理を開始する時刻を入力します。このパラメーターは、「繰り返し (Recurrence)」の値と連携して、リモート・ディレクトリーのファイルをスキャンするタイミングと頻度を設定します。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。例えば、ディレクトリーを 2 時間おきにスキャンする場合は、2H です。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 (Ignore Previously Processed File)」パラメーターの、以前に処理したファイルのリストはクリアされます。

パラメーター	説明
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
Processor	リモート・ホストにあるファイルが zip、gzip、tar、または tar+gzip のアーカイブ形式で格納されている場合は、アーカイブを展開して内容を処理することができるプロセッサーを選択します。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	処理済みのファイルを追跡し、ファイルの再度の処理を希望しない場合は、このチェック・ボックスを選択します。 これは FTP および SFTP のサービス・タイプに適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar 上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 ほとんどの構成では、このチェック・ボックスをクリアしたままにしてかまいません。このチェック・ボックスを選択すると、「**Local Directory**」フィールドが表示されます。これにより、ファイルを一時的に格納するために使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	取得したイベント・ログを複数行のイベントとして処理するには、「**ID-Linked Multiline**」を選択します。 「ID-Linked Multiline」形式では、複数行のイベント・メッセージの各行の先頭に共通の値を含む複数行のイベント・ログを処理します。このオプションにより、正規表現を使用して、単一のイベント・ペイロード内の複数行のイベントの識別および再組み立てを実行する「**Message ID Pattern**」フィールドが表示されます。
フォルダー分離文字 **(Folder Separator)**	オペレーティング・システムのフォルダーを分離するために使用される文字を入力します。デフォルト値は / です。 ほとんどの構成では、「フォルダー分離文字 **(Folder Separator)**」フィールドのデフォルト値を使用できます。このフィールドを使用するのは、分離フォルダーの定義に代替文字を使用するオペレーティング・システムのみです。例えば、メインフレーム・システムでフォルダーを分離するピリオドがあります。

13. 「保存」をクリックします。
14. 「管理」タブで「変更のデプロイ」をクリックします。

UDP 多重回線 Syslog ログ・ソースの構成

Syslog イベントを収集するには、UDP 多重回線 Syslog プロトコルを使用するように Sun ONE LDAP のログ・ソースを構成する必要があります。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストから「**Sun ONE LDAP**」を選択します。
6. 「プロトコル構成」リストで「**UDP** 多重回線 **Syslog (UDP Multiline Syslog)**」を選択します。
7. 以下の値を構成します。

表 *376. Sun ONE LDAP UDP* 多重回線 *Syslog* ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース **ID**	Sun ONE LDAP インストール済み環境を識別するための IP アドレス、ホスト名、または名前を入力します。
Listen ポート	着信 UDP 多重回線 Syslog イベントを受け取るために QRadar が使用するポート番号として **517** と入力します。有効なポート範囲は、1 から 65535 です。 保存済みの構成を編集して新しいポート番号を使用するには、以下のステップを実行します。 1. 「**listen** ポート **(Listen Port)**」フィールドに、UDP 多重回線 Syslog イベント受信用の新しいポート番号を入力します。 2. 「保存」をクリックします。 3. 「管理」タブで、「拡張」 > 「すべての構成のデプロイ」を選択します。 すべてのデプロイが完了したら、QRadar は更新された listen ポートでイベントの受信を開始します。 「すべての構成のデプロイ」をクリックすると、QRadar はすべてのサービスを再始動します。このため、デプロイが完了するまで、イベントとフローのデータ収集に差異が発生します。
メッセージ **ID** のパターン	イベント・ペイロード・メッセージをフィルタリングするために必要な以下の正規表現 (regex) を入力します。 `conn=(¥d+)`
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。

表 376. Sun ONE LDAP UDP 多重回線 Syslog ログ・ソース・パラメーター (続き)

パラメーター	説明
信頼性	ログ・ソースの「信頼性」を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信ペイロードのエンコード	イベント・ログの解析に必要な文字エンコードを選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
ログ・ソース言語	Sun ONE LDAP により生成されるイベントの言語を選択します。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

Sun Solaris DHCP

IBM Security QRadar は、Sun Solaris DHCP インストール済み環境からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。

7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Solaris** オペレーティング・システム認証メッセージ」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *377. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Sun Solaris インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。 複数のインストール済み環境が存在する場合は、作成した追加ログ・ソースのそれぞれに IP アドレス、ホスト名などの固有 ID を含めることをお勧めします。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが IBM Security QRadar に追加されます。 Solaris Sendmail により QRadar に転送されるイベントは、「ログ・アクティビティー」タブに表示されます。

Sun Solaris DHCP の構成

for IBM Security QRadar 用の Sun Solaris DHCP DSM は、syslog を使用して関連するすべての DHCP イベントを記録します。

このタスクについて

Sun Solaris DHCP からイベントを収集するには、イベントを QRadar に転送するように syslog を構成する必要があります。

手順

1. Sun Solaris コマンド・ライン・インターフェースにログインします。
2. `/etc/default/dhcp` ファイルを編集します。
3. 以下の行を追加して、syslog への DHCP トランザクションのロギングを有効にします。

```
LOGGING_FACILITY=X
```

`X` は、0 から 7 の番号など、ローカル syslog ファシリティーに対応する番号です。

4. ファイルを保存して終了します。
5. `/etc/syslog.conf` ファイルを編集します。
6. システム認証ログを QRadar に転送するために、以下の行をファイルに追加します。

```
localX.notice @<IP address>
```

各部分について以下で説明します。

X は、 1021 ページの『Sun Solaris DHCP の構成』 で指定したロギング・ファシリティー番号です。

<*IP address*> は、QRadar の IP アドレスです。行をフォーマットするには、スペースではなくタブを使用します。

7. ファイルを保存して終了します。
8. 以下のコマンドを入力します。

```
kill -HUP `cat /etc/syslog.pid`
```

次のタスク

これで、QRadar でログ・ソースを構成する準備ができました。

Sun Solaris の構成

IBM Security QRadar 用の Sun Solaris DSM は、syslog を使用して関連するすべての Solaris 認証イベントを記録します。

このタスクについて

Sun Solaris から認証イベントを収集するには、イベントを IBM Security QRadar に転送するように syslog を構成する必要があります。

手順

1. Sun Solaris コマンド・ライン・インターフェースにログインします。
2. `/etc/syslog.conf` ファイルを開きます。
3. システム認証ログを QRadar に転送するために、以下の行をファイルに追加します。

```
*.err;auth.notice;auth.info@<IP address>
```

ここで <*IP address*> は、QRadar の IP アドレスです。行をフォーマットするには、スペースではなくタブを使用します。

注: 実行中の Solaris のバージョンによっては、ログ・タイプをファイルにさらに追加することが必要な場合があります。詳細については、システム管理者にお問い合わせください。

4. ファイルを保存して終了します。
5. 以下のコマンドを入力します。

```
kill -HUP `cat /etc/syslog.pid`
```

次のタスク

これで、QRadar でログ・ソースを構成する準備ができました。

注: イベントを送信する Solaris システムの Linux ログ・ソースを作成した場合は、Linux ログ・ソースを無効にしてから、構文解析順序を調整します。必ず Solaris DSM が最初にリストされているようにしてください。

.

Sun Solaris Sendmail

IBM Security QRadar 用の Sun Solaris Sendmail DSM は、syslogを使用して認証イベントを受け入れ、関連するすべての sendmail イベントを記録します。

このタスクについて

Sun Solaris Sendmail からイベントを収集するには、イベントを QRadar に転送するように Syslog を構成する必要があります。

手順

1. Sun Solaris コマンド・ライン・インターフェースにログインします。
2. `/etc/syslog.conf` ファイルを開きます。
3. システム認証ログを QRadar に転送するために、以下の行をファイルに追加します。

   ```
   mail.*; @<IP address>
   ```

   ここで *<IP address>* は、QRadar の IP アドレスです。行をフォーマットするには、スペースではなくタブを使用します。

   注: 実行中の Solaris のバージョンによっては、ログ・タイプをファイルにさらに追加することが必要な場合があります。詳細については、システム管理者にお問い合わせください。
4. ファイルを保存して終了します。
5. 以下のコマンドを入力します。

   ```
   kill -HUP 'cat /etc/syslog.pid'
   ```

   これで、QRadar でログ・ソースを構成する準備ができました。

Sun Solaris Sendmail のログ・ソースの構成

IBM Security QRadar は、Sun Solaris Sendmail アプライアンスの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**Solaris** オペレーティング・システムの **Sendmail** ログ **(Solaris Operating System Sendmail Logs)**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *378. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Sun Solaris Sendmail インストール済み環境からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。 複数のインストール済み環境が存在する場合は、作成した追加ログ・ソースのそれぞれに IP アドレス、ホスト名などの固有 ID を含めることをお勧めします。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。 Solaris Sendmail により QRadar に転送されるイベントは、「ログ・アクティビティー」タブに表示されます。

Sun Solaris 基本セキュリティー・モジュール (BSM)

Sun Solaris 基本セキュリティー・モジュール (BSM) は、システム管理者が Sun Solaris システムから詳細な監査イベントを取得するための監査トラッキング・ツールです。

IBM Security QRadar は、ログ・ファイル・プロトコルを使用して Sun Solaris BSM イベントを取得します。Solaris 基本セキュリティー・モジュールと統合するように QRadar を構成するには、以下のステップを実行します。

1. Solaris 基本セキュリティー・モジュールを有効にします。
2. 監査ログをバイナリー形式から人間が読める形式に変換します。
3. スケジュールに従って変換スクリプトを実行するようにクーロン・ジョブをスケジュールします。
4. ログ・ファイル・プロトコルを使用して QRadar で Sun Solaris イベントを収集します。

Solaris 10 での基本セキュリティー・モジュールの有効化

Solaris 10 で Sun Solaris BSM を構成するには、Solaris 基本セキュリティー・モジュールを有効にして、システムが監査ログ・ファイルに記録するイベントのクラスを構成する必要があります。

このタスクについて

基本セキュリティー・モジュールを構成し、Sun Solaris 10 での監査を有効にします。

手順

1. superuser または root ユーザーとして Solaris コンソールにログインします。
2. Solaris コンソールでシングルユーザー・モードを有効にします。
3. 以下のコマンドを入力して、bsmconv スクリプトを実行し、監査を有効にします。

   ```
   /etc/security/bsmconv
   ```

   bsmconv スクリプトは Solaris 基本セキュリティー・モジュールを有効にして、監査サービス auditd を開始します。
4. 以下のコマンドを入力して、監査制御ログを開いて編集します。

   ```
   vi /etc/security/audit_control
   ```
5. 以下の情報が含まれるように、監査制御ファイルを編集します。

   ```
   dir:/var/audit flags:lo,ad,ex,-fw,-fc,-fd,-fr naflags:lo,ad
   ```
6. audit_control ファイルの変更内容を保存してから、Solaris コンソールをリブートして auditd を開始します。
7. 以下のコマンドを入力して、auditd が開始したことを確認します。

   ```
   /usr/sbin/auditconfig -getcond
   ```

   auditd プロセスが開始していれば、以下のストリングが返されます。

   ```
   audit condition = auditing
   ```

次のタスク

これで、バイナリーの Solaris 基本セキュリティー・モジュール・ログを、人が認識できるログ形式に変換できるようになりました。

Solaris 11 での基本セキュリティー・モジュールの有効化

Solaris 11 で Sun Solaris BSM を構成するには、Solaris 基本セキュリティー・モジュールを有効にして、システムが監査ログ・ファイルに記録するイベントのクラスを構成する必要があります。

手順

1. superuser または root として Solaris 11 コンソールにログインします。
2. 以下のコマンドを入力して、監査サービスを開始します。

   ```
   audit -s
   ```
3. 以下のコマンドを入力して、帰属クラスをセットアップします。

   ```
   auditconfig -setflags lo,ps,fw
   ```

4. 以下のコマンドを入力して、非帰属クラスをセットアップします。

   ```
   auditconfig -setnaflags lo,na
   ```

5. 監査サービスの開始を確認するには、以下のコマンドを入力します。

   ```
   /usr/sbin/auditconfig -getcond
   ```

   auditd プロセスが開始していれば、以下のストリングが返されます。

   ```
   audit condition = auditing
   ```

Sun Solaris BSM 監査ログの変換

IBM Security QRadar では Sun Solaris BSM からのバイナリー・ファイルを直接処理することができません。QRadar が監査ログ・データを取得できるようにするには、praudit を使用して、監査ログを既存のバイナリー形式から人が認識できるログ形式に変換しておく必要があります。

手順

1. 以下のコマンドを入力して、Sun Solaris コンソールでスクリプトを新規作成します。

   ```
   vi /etc/security/newauditlog.sh
   ```

2. newauditlog.sh スクリプトに、以下の情報を追加します。

   ```
   #!/bin/bash # # newauditlog.sh - Start a new audit file and expire the
   old logs #

   AUDIT_EXPIRE=30 AUDIT_DIR="/var/audit" LOG_DIR="/var/log/"
   /usr/sbin/audit -n cd $AUDIT_DIR # in case it is a link #
   Get a listing of the files based on creation date that are not current in use
   FILES=$(ls -lrt | tr -s " " | cut -d" " -f9 | grep -v "not_terminated")
    # We just created a new audit log by doing 'audit -n',
   so we can # be sure that the last file in the list will be the
   latest # archived binary log file.

   lastFile="" for file in $FILES; do

    lastFile=$file

   done
   # Extract a human-readable file from the binary log file
   echo "Beginning praudit of $lastFile"
   praudit -l $lastFile > "$LOG_DIR$lastFile.log" echo "Done praudit,
   creating log file at: $LOG_DIR$lastFile.log"

    /usr/bin/find . $AUDIT_DIR -type f -mtime +$AUDIT_EXPIRE ¥ -exec rm {}
   > /dev/null 2>&1 ¥;

   # End script
   ```

   このスクリプトは、*<starttime>*.*<endtime>*.*<hostname>*.log 形式でログ・ファイルを出力します。

例えば、/var/log のログ・ディレクトリーには、以下の名前のファイルが格納されます。

```
20111026030000.20111027030000.qasparc10.log
```

3. オプション: ログ・ファイルのデフォルトのディレクトリーを変更するには、スクリプトを編集します。
   a. AUDIT_DIR="/var/audit" - Audit ディレクトリーは、 1024 ページの『Solaris 10 での基本セキュリティー・モジュールの有効化』で構成した監査制御ファイルで指定されたロケーションと一致している必要があります。
4. LOG_DIR="/var/log/" - このログ・ディレクトリーは、人が認識できる Sun Solaris システムのログ・ファイルのロケーションで、QRadar が取得できる状態になっています。
5. newauditlog.sh スクリプトに対する変更内容を保存します。

次のタスク

これで、CRON を使用してこのスクリプトを自動化し、Sun Solaris 基本セキュリティー・モジュール・ログを人が認識できる形式に変換できます。

cron ジョブの作成

cron とは Solaris デーモン・ユーティリティーで、システム全体を対象とするスクリプトとコマンドの実行をスケジュールに基づいて自動化します。

このタスクについて

以下の手順は、newauditlog.sh が毎日午前 0 時に実行されるように自動化する例を示しています。1 日に複数回、Solaris システムからログ・ファイルを取得する必要がある場合は、cron スケジュールを変更する必要があります。

手順

1. 以下のコマンドを入力して、cron ファイルのコピーを作成します。

   ```
   crontab -l > cronfile
   ```

2. 以下のコマンドを入力して、cronfile を編集します。

   ```
   vi cronfile
   ```

3. cronfile に以下の情報を追加します。

   ```
   0 0 * * * /etc/security/newauditlog.sh
   ```

4. cronfile に対する変更内容を保存します。
5. 以下のコマンドを入力して、cronfile を crontab に追加します。

   ```
   crontab cronfile
   ```

6. これで、Sun Solaris BSM 監査ログ・ファイルを取得するための IBM Security QRadar でログ・ソースを構成できるようになりました。

次のタスク

これで、ログ・ソースを QRadar で構成することができます。

Sun Solaris BSM のログ・ソースの構成

ログ・ファイル・プロトコルのソースにより、IBM Security QRadar はリモート・ホストからアーカイブ・ログ・ファイルを取得することができます。Sun Solaris BSM は、ログ・ファイル・プロトコルを使用することによって監査ログ・ファイルの一括ロードをサポートします。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「ログ・ソース・タイプ」リストで「**Solaris BSM**」を選択します。
6. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
7. 以下のパラメーターを構成します。

表 *379.* ログ・ファイル・パラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
サービス・タイプ	リモート・サーバーからログ・ファイルを取得するときに使用するプロトコルを、リストから選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	Sun Solaris BSM システムの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。サービス・タイプを FTP として構成する場合、デフォルトは 21 です。サービス・タイプを SFTP または SCP として構成する場合、デフォルトは 22 です。 有効な範囲は、1 から 65535 です。
リモート・ユーザー	Sun Solaris システムにログインするのに必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	Sun Solaris システムにログインするのに必要なパスワードを入力します。
パスワードの確認	Sun Solaris システムにログインするためのリモート・パスワードを確認します。

表 379. ログ・ファイル・パラメーター (続き)

パラメーター	説明
SSH 鍵ファイル	**SCP** または **SFTP** を「サービス・タイプ **(Service Type)**」フィールドから選択する場合、SSH 秘密鍵ファイルへのディレクトリー・パスを定義できます。SSH 秘密鍵ファイルを使用する場合、「リモート・パスワード」フィールドは無視できます。
リモート・ディレクトリー	ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。デフォルトでは、newauditlog.sh スクリプトは、人間が理解できるログ・ファイルを `/var/log/` ディレクトリーに書き込みます。
再帰的 **(Recursive)**	サブフォルダーからもファイル・パターンを検索したい場合は、このチェック・ボックスを選択します。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」パラメーターは使用されません。デフォルトでは、このチェック・ボックスはクリアされています。
FTP ファイル・パターン	「サービス・タイプ」として「**SFTP**」または「**FTP**」を選択すると、「リモート・ディレクトリー」で指定されたファイルのリストのフィルタリングに必要な正規表現 (regex) を構成するオプションを使用できます。一致するすべてのファイルは処理に組み込まれます。 例えば、`<starttime>.<endtime>.<hostname>.log`形式のすべてのファイルを取得する場合は、入力として `¥d+¥.¥d+¥.¥w+¥.log` を使用します。 このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として「FTP」を選択した場合にのみ表示されます。「**FTP** 転送モード」パラメーターには、FTP を介してログを取得する際のファイル転送モードを定義するオプションがあります。 リストから、このログ・ソースに適用する転送モードを選択します。 • **バイナリー** - バイナリー・データ・ファイル、または圧縮された `.zip`、`.gzip`、`.tar`、`.tar+gzip` のアーカイブ・ファイルを必要とするログ・ソースには、「バイナリー」を選択します。 • **ASCII** - ASCII FTP ファイル転送を必要とするログ・ソースには、ASCII を選択します。転送モードとして ASCII を使用する場合は、「プロセッサー」フィールドで「**NONE**」を、「イベント・ジェネレーター **(Event Generator)**」フィールドで「**1** 行ずつ **(LINEBYLINE)**」を選択する必要があります。
SCP リモート・ファイル	**SCP** をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。
開始時刻	処理を開始する時刻を入力します。このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。

表 379. ログ・ファイル・パラメーター (続き)

パラメーター	説明
繰り返し **(Recurrence)**	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、ディレクトリーを 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リモート・ホストにあるファイルが .zip、.gzip、.tar、または tar+gzip のアーカイブ・フォーマットで保管されている場合、アーカイブを展開して内容を処理することができるプロセッサーを選択します。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	既に処理済みのファイルを追跡し、処理済みのファイルの再処理が必要ない場合は、このチェック・ボックスを選択します。これは FTP および SFTP のサービス・タイプにのみ適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar システム上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。チェック・ボックスは選択されていない状態のままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示され、ファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LINEBYLINE)**」を選択します。

8. 「保存」をクリックします。

構成は完了です。ログ・ファイル・プロトコルを使用して取得されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。.

第 128 章 Sybase ASE

Sybase Adaptive Server Enterprise (ASE) デバイスを IBM Security QRadar SIEM と統合すると、JDBC を使用して関連するすべてのイベントを記録することができます。

このタスクについて

Sybase ASE デバイスを構成するには、以下の手順を実行します。

手順

1. Sybase の監査を構成します。

   Sybase の監査の構成について詳しくは、お手持ちの *Sybase* の資料を参照してください。
2. sa ユーザーとして Sybase データベースにログインします。

   ```
   isql -Usa -P<password>
   ```

   <password> は、データベースへのアクセスに必要なパスワードです。
3. セキュリティー・データベースに移動します。
   - `use sybsecurity`
   - `go`
4. IBM Security QRadar SIEM 用のビューを作成します。
   - `create view audit_view`
   - `as`
   - `select audit_event_name(event) as event_name, * from <audit_table_1>`
   - `union`
   - `select audit_event_name(event) as event_name, * from <audit_table_2>`
   - `go`
5. 監査構成の追加の監査テーブルのそれぞれで、**union select** パラメーターが繰り返されていることを確認します。

   例えば、4 つの監査テーブル (sysaudits_01、sysaudits_02、sysaudits_03、sysaudits_04) で監査を構成する場合は、以下のコマンドを入力します。
   - `create view audit_view as select audit_event_name(event) as event_name, * from sysaudits_01`
   - `union select audit_event_name(event) as event_name, * from sysaudits_02,`
   - `union select audit_event_name(event) as event_name, * from sysaudits_03,`
   - `union select audit_event_name(event) as event_name, * from sysaudits_04`

次のタスク

これで、IBM Security QRadar SIEM でログ・ソースを構成できるようになりました。

関連概念:

17 ページの『JDBC プロトコルの構成オプション』
QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Sybase ASE デバイスからのイベントを受信するための IBM Security QRadar SIEM の構成

QRadar SIEM は、Sybase ASE デバイスからのイベントを受信するように構成することができます。

手順

1. QRadar SIEM にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
4. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
5. 「追加」をクリックします。

   「ログ・ソースの追加」ウィンドウが表示されます。
6. 「ログ・ソース・タイプ」リストで「**Sybase ASE**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。

   JDBC プロトコル構成が表示されます。
8. JDBC 構成を更新して、以下の値を追加します。
   - データベース名: **sybsecurity**
   - ポート: **5000 (デフォルト)**
   - ユーザー名: **sa**
   - テーブル名: **audit_view**
   - 比較フィールド: **eventtime**

パラメーター「データベース名」と「テーブル名」では、大/小文字が区別されます。

Sybase ASE デバイスについて詳しくは、ベンダーの資料を参照してください。

第 129 章 Symantec

IBM Security QRadar は複数の Symantec DSM をサポートしています。

Symantec Critical System Protection

Symantec Critical System Protection 用の IBM Security QRadar DSMでは、Symantec Critical System Protection システムからイベント・ログを収集できます。

以下の表は、Symantec Critical System Protection DSM の仕様を示しています。

表 *380. Symantec Critical System Protection DSM* の仕様

仕様	値
製造元	Symantec
DSM 名	Critical System Protection
RPM ファイル名	DSM-SymantecCriticalSystemProtection-*Qradar_version_build number*.noarch.rpm
サポートされるバージョン	5.1.1
イベント・フォーマット	DB 項目
QRadar で記録されるイベント・タイプ	「CSPEVENT_VW」ビューからのすべてのイベント
QRadar UI でのログ・ソース・タイプ	Symantec Critical System Protection
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む	いいえ
詳細情報	Symantec Web ページ (http://www.symantec.com/)

Symantec Critical System Protection を QRadar に統合するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソール にインストールしてください。
   - Protocol-JDBC RPM
   - Symantec Critical System Protection RPM
2. Symantec Critical System Protection インスタンスごとに、Symantec Critical System Protection を構成して QRadar と通信できるようにします。

   QRadar が TCP ポート 1433 またはログ・ソースに構成されているポートを使用して、イベントを対象にデータベースをポーリングできることを確認します。プロトコル接続がデータベースで無効になっていることがよくあります。したがって、特定の状況では、イベント・ポーリング用の接続を許可するために、追加

の構成ステップが必要になります。Symantec Critical System Protection と QRadar の間にあるファイアウォールを構成して、イベント・ポーリング用のトラフィックを許可します。

3. QRadar が Symantec Critical System Protection を自動的に検出しない場合、Symantec Critical System Protection インスタンスごとに、QRadar コンソール上でログ・ソースを作成します。ログ・ソースの必須パラメーターには、以下の値を使用します。

パラメーター	説明
ログ・ソース・タイプ	Symantec Critical System Protection
プロトコル構成	JDBC
データベース・タイプ	MSDE
インスタンス	SCSP
データベース名	SCSPDB
テーブル名	CSPEVENT_VW
比較フィールド	EVENT_ID

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Symantec Data Loss Prevention (DLP)

IBM Security QRadar 用の Symantec Data Loss Protection (DLP) DSM は syslog を使用して Symantec DLP アプライアンスからのイベントを受け取ります。

QRadar を構成する前に、Symantec DLP で応答ルールを構成する必要があります。応答ルールにより、データ損失ポリシー違反が発生したときに Symantec DLP アプライアンスが syslog イベントを QRadar に転送することができます。Symantec DLP を統合するには、QRadar 用の 2 つのプロトコル応答ルール (SMTP および None of SMTP) を作成する必要があります。これらのプロトコル応答ルールは、インシデントがトリガーされたときに syslog を使用してイベント情報を転送するためのアクションを作成します。

QRadar で Symantec DLP を構成するには、以下の手順を実行します。

1. SMTP 応答ルールを作成します。
2. None of SMTP 応答ルールを作成します。
3. QRadar でログ・ソースを構成します。
4. QRadar で Symantec DLP イベントをマップします。

SMTP 応答ルールの作成

Symantec DLP で SMTP 応答ルールを構成できます。

手順

1. Symantec DLP ユーザー・インターフェースにログインします。
2. メニューから、「管理 **(Manage)**」 > 「ポリシー **(Policies)**」 > 「応答ルール **(Response Rules)**」を選択します。
3. 「応答ルールの追加 **(Add Response Rule)**」をクリックします。
4. 以下の応答ルール・タイプのいずれかを選択します。
   - 「自動応答 **(Automated Response)**」 - 自動応答ルールは、インシデントの発生時に自動的にトリガーされます。これはデフォルト値です。
   - 「スマート応答 **(Smart Response)**」 - スマート応答ルールは「インシデント・コマンド (Incident Command)」画面に追加され、権限のある Symantec DLP ユーザーによって処理されます。
5. 「次へ」をクリックします。

   以下の値を構成します。
6. 「ルール名 **(Rule Name)**」 - 作成するルールの名前を入力します。この名前はポリシー作成者がルールを識別できる記述的な名前にすることをお勧めします。例えば、`QRadar Syslog SMTP` のようにします。
7. 「説明」 - オプション。作成するルールについての説明を入力します。
8. 「条件の追加 **(Add Condition)**」をクリックします。
9. 「条件 **(Conditions)**」パネルで、以下の条件を選択します。
   - 最初のリストでは「プロトコルまたはエンドポイント・モニタリング **(Protocol or Endpoint Monitoring)**」を選択します。
   - 2 番目のリストで、「次のいずれか **(Is Any Of)**」を選択します。
   - 3 番目のリストで、「**SMTP**」を選択します。
10. 「アクション (Actions)」ペインで、「アクションの追加 (Add Action)」をクリックします。
11. 「アクション **(Actions)**」リストから、「すべて**: Syslog** サーバーにログを記録 **(All: Log to a Syslog Server)**」を選択します。
12. 以下のオプションを構成します。
    a. 「ホスト **(Host)**」 - IBM Security QRadar の IP アドレスを入力します。
13. 「ポート **(Port)**」 - syslog ポートとして `514` と入力します。
14. 「メッセージ **(Message)**」 - 以下のストリングを入力して、SMTP イベントのメッセージを追加します。

```
LEEF:1.0|Symantec|DLP|2:medium|$POLICY$
|usrName=$SENDER$|duser=$RECIPIENTS$|rules=$RULES$
|matchCount=$MATCH_COUNT$|blocked=$BLOCKED$
|incidentID=$INCIDENT_ID$|incidentSnapshot=$INCIDENT_SNAPSHOT$
|subject=$SUBJECT$|fileName=$FILE_NAME$|parentPath=$PARENT_PATH$
|path=$PATH$|quarantineParentPath=$QUARANTINE_PARENT_PATH$
|scan=$SCAN$|target=$TARGET$
```

15. 「レベル **(Level)**」 - このリストから **6 -** 通知 **(6 - Informational)**」を選択します。
16. 「保存」をクリックします。

次のタスク

これで、None Of SMTP 応答ルールの構成が可能になりました。

None Of SMTP 応答ルールの作成

Symantec DLP で None Of SMTP 応答ルールを構成できます。

手順

1. メニューから、「管理 **(Manage)**」 > 「ポリシー **(Policies)**」 > 「応答ルール **(Response Rules)**」を選択します。
2. 「応答ルールの追加 **(Add Response Rule)**」をクリックします。
3. 以下の応答ルール・タイプのいずれかを選択します。
   - 「自動応答 **(Automated Response)**」 - 自動応答ルールは、インシデントの発生時に自動的にトリガーされます。これはデフォルト値です。
   - 「スマート応答 **(Smart Response)**」 - スマート応答ルールは「インシデント・コマンド (Incident Command)」画面に追加され、権限のある Symantec DLP ユーザーによって処理されます。
4. 「次へ」をクリックします。

   以下の値を構成します。
5. 「ルール名 **(Rule Name)**」 - 作成するルールの名前を入力します。この名前はポリシー作成者がルールを識別できる記述的な名前にすることをお勧めします。例えば、`QRadar Syslog None Of SMTP` のようにします。
6. 「説明」 - オプション。作成するルールについての説明を入力します。
7. 「条件の追加 **(Add Condition)**」をクリックします。
8. 「条件 (Conditions)」ペインで、以下の条件を選択します。
   - 最初のリストでは「プロトコルまたはエンドポイント・モニタリング **(Protocol or Endpoint Monitoring)**」を選択します。
   - 2 番目のリストで、「次のいずれか **(Is Any Of)**」を選択します。
   - 3 番目のリストで、「**None Of SMTP**」を選択します。
9. 「アクション (Actions)」ペインで、「アクションの追加 **(Add Action)**」をクリックします。
10. 「アクション **(Actions)**」リストから、「すべて**: Syslog** サーバーにログを記録 **(All: Log to a Syslog Server)**」を選択します。
11. 以下のオプションを構成します。

    a. 「ホスト **(Host)**」 - QRadar の IP アドレスを入力します。
12. 「ポート (Port)」 - syslog ポートとして `514` と入力します。
13. 「メッセージ **(Message)**」 -以下のストリングを入力して、*None Of SMTP* イベントのメッセージを追加します。

```
LEEF:1.0|Symantec|DLP|2:medium|$POLICY$|
src=$SENDER$|dst=$RECIPIENTS$|rules=$RULES$|matchCount=$MATCH_COUNT$|
blocked=$BLOCKED$|incidentID=$INCIDENT_ID$|
incidentSnapshot=$INCIDENT_SNAPSHOT$|subject=$SUBJECT$|
fileName=$FILE_NAME$|parentPath=$PARENT_PATH$|path=$PATH$|
quarantineParentPath=$QUARANTINE_PARENT_PATH$|scan=$SCAN$|target=$TARGET$
```

14. 「レベル **(Level)**」 - このリストから **6 -** 通知 **(6 - Informational)**」を選択します。
15. 「保存」をクリックします。

次のタスク

これで、IBM Security QRadar を構成する準備ができました。

ログ・ソースの構成

IBM Security QRadar では、Symantec DLP アプライアンスからのイベントを受信するようにログ・ソースを構成することができます。

このタスクについて

QRadar は、作成した SMTP 応答ルールおよび None of SMTP 応答ルールで syslog イベントを自動的に検出します。ただし、Symantec DLP アプライアンスからイベントを受信するように QRadar を手動で構成する場合は、以下のようにします。

手順

「ログ・ソース・タイプ」リストで「**Symantec DLP**」オプションを選択します。
Symantec DLP について詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Symantec DLP イベントに対するイベント・マップの作成

さまざまな Symantec DLP イベントに対するイベント・マッピングが必要です。ポリシー・ルールはカスタマイズ可能であるため、デフォルト・ポリシー・イベントを除くほとんどのイベントには、セキュリティー・イベントをカテゴリー化するための事前定義の QRadar ID (QID) マップが含まれていません。 QRadar ID (QID) マップが含まれません。

デバイスの各イベントは、個別に QRadar のイベント・カテゴリーにマップすることができます。イベントをマップすることで、QRadar は、ネットワーク・デバイスからの繰り返しイベントを識別、統合、および追跡できます。イベントをマップしない限り、Symantec DLP の「ログ・アクティビティー」タブに表示されるイベントは、すべて「不明」に分類されます。不明 なイベントは「イベント名」列に示され、「下位カテゴリー」列に「不明」と表示されるため、簡単に分かります。

不明イベントの検出

デバイスから IBM Security QRadar にイベントを転送すると、イベント・ソース・アプライアンスまたはソフトウェアが一部のイベントを即時に生成しないことがあるため、デバイスのすべてのイベントの分類に時間がかかる場合があります。

このタスクについて

不明イベントを迅速に検索する方法を把握しておくと有益です。不明イベントの検索方法が分かっている場合は、ほぼすべてのイベントを識別できたと判断できるまで、この検索を繰り返すことをお勧めします。

手順

1. QRadar にログインします。
2. 「ログ・アクティビティー」タブをクリックします。
3. 「フィルターの追加」をクリックします。
4. 最初のリストから「ログ・ソース」を選択します。
5. 「ログ・ソース・グループ」リストから、ログ・ソース・グループまたは「その他」を選択します。

   グループに割り当てられていないログ・ソースは「その他」に分類されます。
6. 「ログ・ソース」リストから、「Symantec DLP」ログ・ソースを選択します。
7. 「フィルターの追加」をクリックします。

   「ログ・アクティビティー」タブに、ログ・ソース用のフィルターが表示されます。
8. 「表示」リストから「過去 **1** 時間」を選択します。

   Symantec DLP DSM によって過去 1 時間に生成されたイベントがすべて表示されます。「イベント名」列、または「下位カテゴリー」列に「不明」として表示されているイベントについては、QRadar でのイベント・マッピングが必要です。

   注**:** 「条件の保存」をクリックすると、既存の検索フィルターを保存することができます。

次のタスク

これで、イベント・マップの変更を行うことができるようになりました。

イベント・マップの変更

イベント・マップを変更する際に、イベントを手動で QRadar ID (QID) マップに分類できます。

このタスクについて

ログ・ソースに分類されたイベントはすべて、新しい QRadar ID (QID) に再マップできます。

注**:** ログ・ソースが定義されていないイベントは、イベントにマップできません。ログ・ソースのないイベントの場合、「ログ・ソース」列に「SIM 汎用ログ (SIM Generic Log)」と表示されます。

手順

1. 「イベント名」列で、Symantec DLP の不明 イベントをダブルクリックします。

   詳細なイベント情報が表示されます。
2. 「イベントのマップ」をクリックします。
3. 「QID の参照 (Browse for QID)」ペインから、以下のいずれかの検索オプションを選択して、IBM Security QRadar ID (QID) のイベント・カテゴリーを絞り込みます。
   a. 「上位カテゴリー」リストから、上位イベント・カテゴリーを選択します。

      上位イベント・カテゴリーと下位イベント・カテゴリーの全リストおよびカテゴリーの定義については、「*IBM Security QRadar* 管理ガイド」の『イベント・カテゴリー』セクションを参照してください。
4. 「下位カテゴリー」リストから、下位イベント・カテゴリーを選択します。
5. 「ログ・ソース・タイプ」リストから、ログ・ソース・タイプを選択します。

   「ログ・ソース・タイプ」リストでは、他のログ・ソースからの QID を検索できます。イベントが既存の別のネットワーク・デバイスからのイベントに類似している場合、ログ・ソースで QID を検索すると便利です。例えば、Symantec はポリシー・イベントおよびデータ損失防止イベントを提供しており、類似するイベントをキャプチャーする可能性のある別の製品を選択することができます。
6. 名前で QID を検索するには、「**QID/**名前」フィールドに名前を入力します。

   「**QID/**名前」フィールドでは、特定の単語 (例:「ポリシー」) で QID の完全なリストをフィルタリングできます。
7. 「検索」をクリックします。

   QID のリストが表示されます。
8. 不明イベントに関連付ける QID を選択します。
9. 「**OK**」をクリックします。

   イベント・ペイロードと一致する同じ QID を持つデバイスから転送されるすべての追加イベントがマップされます。QRadar によってイベントが識別されるたびに、イベントの数が増加します。

   新しい QRadar ID (QID) マップでイベントを更新する場合、QRadar に保管されている過去のイベントは更新されません。新しいイベントだけが新しい QID によって分類されます。

Symantec Endpoint Protection

IBM Security QRadar 用の Symantec Endpoint Protection DSM は、syslog を使用してイベントを受け入れます。

このタスクについて

QRadar は、監査ログおよびセキュリティー・ログのすべてのイベントを記録します。QRadar で Symantec Endpoint Protection デバイスを構成する前に、syslog イベントを転送するようにデバイスを構成しておく必要があります。

手順

1. Symantec Endpoint Protection Manager にログインします。
2. 左のペインで、「管理 **(Admin)**」アイコンをクリックします。

   「サーバーの表示 (View Servers)」オプションが表示されます。
3. 「サーバーの表示 (View Servers)」ペインの下部で「サーバー **(Servers)**」をクリックします。
4. 「サーバーの表示 (View Servers)」ペインから「ローカル・サイト **(Local Site)**」をクリックします。
5. 「タスク (Tasks)」ペインから「外部ロギングの構成 **(Configure External Logging)**」をクリックします。
6. 「一般 **(Generals)**」タブで「**Syslog** サーバーへのログ送信を有効にする **(Enable Transmission of Logs to a Syslog Server)**」チェック・ボックスを選択します。
7. **Syslog** サーバー **(Syslog Server)**」フィールドに、ログを解析する QRadar の IP アドレスを入力します。
8. 「**UDP** 宛先ポート **(UDP Destination Port)**」フィールドに 514 と入力します。
9. 「ログ・ファシリティー **(Log Facility)**」フィールドに 6 と入力します。
10. 「ログ・フィルター **(Log Filter)**」タブで以下のようにします。
    a. 「管理サーバー・ログ **(Management Server Logs)**」で「監査ログ **(Audit Logs)**」チェック・ボックスを選択します。
11. 「クライアント・ログ (Client Log)」ペインで「セキュリティー・ログ **(Security Logs)**」チェック・ボックスを選択します。
12. 「クライアント・ログ (Client Log)」ペインで「リスク **(Risks)**」チェック・ボックスを選択します。
13. 「**OK**」をクリックします。
14. これで、QRadar でログ・ソースを構成できるようになりました。

    Symantec Encpoint Protection デバイスからのイベントを受信するように QRadar を構成するには、以下のようにします。
    a. 「ログ・ソース・タイプ」リストで「**Symantec Endpoint Protection**」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプラ

イアンスからイベントを受信するログ・ソースを手動で追加できます。

Symantec PGP Universal Server

IBM Security QRadar 用の PGP Universal Server DSM は PGP Universal Server から syslog イベントを受け取ります。

QRadar は、以下のカテゴリーの関連イベントをすべて受け取ります。

- 管理
- ソフトウェア更新
- クラスター化
- バックアップ
- Web メッセンジャー
- 検証対象ディレクトリー
- Postfix
- クライアント・ログ
- メール (Mail)
- ディスク全体暗号化ログ

PGP Universal Server イベントを QRadar と統合するには、PGP Universal Server を有効にして、syslog イベントを QRadar に転送するように構成する必要があります。

PGP Universal Server の syslog の構成

外部ロギングを有効にすると、syslog イベントを IBM Security QRadar に転送できるようになります。

手順

1. Web ブラウザーで、PGP サーバーの管理インターフェースにログインします。

   `https://<PGP Server IP address>:9000`
2. 「設定」をクリックします。
3. 「外部 **Syslog** を有効にする **(Enable External Syslog)**」チェック・ボックスを選択します。
4. 「プロトコル **(Protocol)**」リストから、「**UDP**」または「**TCP**」のいずれかを選択します。

   デフォルトでは、QRadar はポート 514 を使用して UDP Syslog または TCP Syslog のイベントのメッセージを受信します。
5. 「ホスト名 **(Hostname)**」フィールドに QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
6. 「ポート (Port)」フィールドに 514 を入力します。
7. 「保存」をクリックします。

構成は完了です。PGP Universal Server イベントが自動的に検出されると、ログ・ソースが QRadar に追加されます。PGP Universal Server によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。.

ログ・ソースの構成

IBM Security QRadar は、PGP Universal Server からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**PGP Universal Server**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *381. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	PGP Universal Server からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

Symantec SGS

IBM Security QRadar 用の Symantec Gateway Security (SGS) Appliance DSM は、syslog を使用して SGS イベントを受け入れます。

このタスクについて

QRadar は、SGS からの関連するすべてのイベントを記録します。SGS と統合するように QRadar を構成する前に、SGS アプライアンス内で syslog を構成しておく必要があります。Symantec SGS について詳しくは、ベンダーの資料を参照してください。

QRadar にイベントを転送するように syslog を構成すると、構成は完了です。syslog を使用して Symantec SGS から QRadar に転送されるイベントは自動的に検出されます。ただし、Symantec SGS のログ・ソースを手動で作成する場合は、以下のようにします。

手順

「ログ・ソース・タイプ」リストから「**Symantec Gateway Security (SGS) Appliance**」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Symantec System Center

IBM Security QRadar 用の Symantec System Center (SSC) DSM は、QRadar 用に作成されたカスタム・ビューを使用して SSC データベースからイベントを取得します。

QRadar は SSC イベントをすべて記録します。ビューをポーリングして情報を取得できるようにするには、カスタム QRadar ビューに対する読み取り特権および書き込み特権を持つユーザーを使用して SSC データベースを構成する必要があります。Symantec System Center (SSC) は JDBC プロトコルのみをサポートしています。

Symantec System Center 用のデータベース・ビューの構成

JDBC プロトコルで SSC イベントのポーリングを行うにはデータベース・ビューが必要です。

手順

SSC デバイスが使用する Microsoft SQL Server データベースで、IBM Security QRadar をサポートするカスタムのデフォルト・ビューを構成します。

注: データベース名にスペースを使用することはできません。

- `CREATE VIEW dbo.vw_qradar AS SELECT`
- `dbo.alerts.Idx AS idx,`
- `dbo.inventory.IP_Address AS ip,`
- `dbo.inventory.Computer AS computer_name,`
- `dbo.virus.Virusname AS virus_name,`
- `dbo.alerts.Filepath AS filepath,`
- `dbo.alerts.NoOfViruses AS no_of_virus,`
- `dbo.actualaction.Actualaction AS [action],`
- `dbo.alerts.Alertdatetime AS [date],`

- dbo.clientuser.Clientuser AS user_name FROM
- dbo.alerts INNER JOIN
- dbo.virus ON dbo.alerts.Virusname_Idx = dbo.virus.Virusname_Idx INNER JOIN
- dbo.inventory ON dbo.alerts.Computer_Idx = dbo.inventory.Computer_Idx INNER JOIN
- dbo.actualaction ON dbo.alerts.Actualaction_Idx =
- dbo.actualaction.Actualaction_Idx INNER JOIN
- dbo.clientuser ON dbo.alerts.Clientuser_Idx = dbo.clientuser.Clientuser_Idx

次のタスク

カスタム・ビューを作成したら、JDBC プロトコルを使用してイベント情報を受信するように、QRadar を構成する必要があります。

ログ・ソースの構成

IBM Security QRadar を、JDBC プロトコルを使用して SSC データベースにアクセスするように構成できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**Symantec System Center**」を選択します。
7. 「プロトコル構成」リストで「**JDBC**」を選択します。
8. 以下のパラメーターを構成します。

表 382. Symantec System Center の JDBC のパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの ID を入力します。ログ・ソース ID は以下の形式で入力します。 *<SSC Database>@<SSC Database Server IP or Host Name>* 各部分について以下で説明します。 • *<SSC Database>* は、「データベース名」パラメーターに入力するデータベース名です。 • *<SSC Database Server IP or Host Name>* は、「**IP** またはホスト名」パラメーターに入力するこのログ・ソースのホスト名または IP アドレスです。
データベース・タイプ	リストから「**MSDE**」を選択します。

表 382. *Symantec System Center* の *JDBC* のパラメーター (続き)

パラメーター	説明
データベース名	Symantec System Center データベースの名前として `Reporting` と入力します。
IP またはホスト名	Symantec System Center SQL Server のIP アドレスまたはホスト名を入力します。
ポート	データベース・サーバーが使用するポート番号を入力します。MSDE のデフォルト・ポートは 1433 です。 JDBC 構成ポートは、Symantec System Center データベースのリスナー・ポートと一致している必要があります。 Symantec System Center データベースでは、QRadar と通信できるように着信 TCP 接続を有効にしておく必要があります。 データベース・タイプとして MSDE を使用する際の「データベース・インスタンス」を定義する場合は、構成内の「ポート」パラメーターをブランクのままにしておく必要があります。
ユーザー名	データベースへのアクセスに必要なユーザー名を入力します。
パスワード	データベースへのアクセスに必要なパスワードを入力します。パスワードの最大長は 255 文字です。
パスワードの確認	データベースへのアクセスに必要なパスワードを確認します。確認パスワードは、「パスワード」パラメーターに入力したパスワードと同じでなければなりません。
認証ドメイン	「データベース・タイプ」として**MSDE**を選択し、データベースが Windows 用に構成されている場合は、Windows 認証ドメインを定義する必要があります。それ以外の場合は、このフィールドをブランクのままにします。
データベース・インスタンス	オプション。データベース・サーバーに複数の SQL サーバー・インスタンスがある場合に、データベース・インスタンスを入力します。 データベース構成で標準外ポートを使用する場合、または SQL データベース解決用のポート 1434へのアクセスをブロックする場合は、構成内で「データベース・インスタンス」パラメーターをブランクのままにしておく必要があります。
テーブル名	イベント・レコードを格納するテーブルまたはビューの名前として `vw_qradar` と入力します。
選択リスト	テーブルまたはビューのすべてのフィールドに `*` を入力します。 ご使用の構成での必要に応じて、コンマ区切りリストを使用して特定のテーブルまたはビューを定義することができます。コンマ区切りリストの長さは、英数字で 255 文字までです。リストに使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、en ダッシュ (-)、ピリオド (.) です。
比較フィールド	比較フィールドとして `idx` と入力します。比較フィールドを使用して、テーブルに対する照会から次の照会までの間に追加されたい新しいイベントを特定できます。

表 382. *Symantec System Center の JDBC のパラメーター (続き)*

パラメーター	説明
開始日時	オプション。データベース・ポーリングの開始日時を入力します。 「開始日時」パラメーターは、yyyy-MM-dd HH: mm 形式で入力する必要があります (HH は 24 時間形式で指定します)。開始日または開始時間をクリアした場合は、すぐにポーリングが開始され、指定のポーリング間隔で繰り返されます。
準備済みステートメントの使用 **(Use Prepared Statements)**	準備済みステートメントを使用する場合は、このチェック・ボックスを選択します。 準備済みステートメントを使用すると、JDBC プロトコル・ソースで一度 SQL ステートメントをセットアップすれば、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由から、準備済みステートメントを使用することをお勧めします。 このチェック・ボックスをクリアする場合は、プリコンパイル・ステートメントを使用しない代替照会メソッドを使用する必要があります。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。デフォルトのポーリング間隔は 10 秒です。 より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。H または M を使用せずに入力された数値は、秒数のポーリング間隔です。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。デフォルトは 20000 EPS です。
名前付きパイプ通信の使用 **(Use Named Pipe Communication)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスをクリアします。 名前付きパイプ接続を使用する場合は、データベースのユーザー名およびパスワードではなく、Windows 認証の適切なユーザー名とパスワードを使用する必要があります。また、デフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 **(Database Cluster Name)**	「名前付きパイプ通信の使用 **(Use Named Pipe Communication)**」チェック・ボックスを選択すると、「データベース・クラスター名 **(Database Cluster Name)**」パラメーターが表示されます。SQL サーバーをクラスター環境で実行している場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにしてください。

注**:** 「信頼性」パラメーターに 5 より大きい値を選択すると、Symantec System Center ログ・ソースに対し、QRadar 内の他のログ・ソースよりも高い重要度が設定されます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

第 130 章 Symark

Symark PowerBroker は、すべてのイベントを複数行形式で単一イベントのログ・ファイルに記録します。このファイルを表示するには、Symark の *pblog* ユーティリティーを使用します。

PowerBroker の *pblogs* は、スクリプトを使用して形式を変換してから IBM Security QRadar に転送する必要があります。イベントを QRadar に転送するには、この構成を行うために、Symark PowerBroker アプライアンスのスクリプトをダウンロードして構成する必要があります。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

ログ・ソースの構成

IBM Security QRadar は、外部ソースからのほぼすべての受信 syslog イベントを自動的に検出して識別します。

このタスクについて

以下の構成手順はオプションです。

ログ・ソースを作成するには、以下の手順を実行します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。

   「データ・ソース」ペインが表示されます。
3. 「ログ・ソース」アイコンをクリックします。

   「ログ・ソース」ウィンドウが表示されます。
4. 「ログ・ソース名」フィールドに、Symark PowerBroker ログ・ソースの名前を入力します
5. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
6. 「ログ・ソース・タイプ」リストで「**Symark PowerBroker**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。

   syslog プロトコルのパラメーターが表示されます。
8. 以下の値を構成します。

表 383. *syslog* ログ・ソースの追加

パラメーター	説明
ログ・ソース **ID**	Symark PowerBroker アプライアンスの IP アドレスまたはホスト名を入力します。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されています。
信頼性	リストから、ログ・ソースの信頼性を選択します。範囲は 0 から 10 です。送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 自動的に検出されたログ・ソースは、「システム設定」ウィンドウの「イベントの統合」リストで構成されたデフォルト値を使用します。このウィンドウには「管理」タブからアクセスできます。ただし、ログ・ソースの新規作成時、または自動的に検出されたログ・ソースの構成の更新時に、ログ・ソースのそれぞれでこのチェック・ボックスを構成することによってデフォルト値をオーバーライドできます。
イベント・ペイロードの保管	QRadar によるイベント・ペイロードの保管を有効または無効にするには、このチェック・ボックスを選択します。 自動的に検出されたログ・ソースは、「システム設定」ウィンドウの「イベント・ペイロードの保管」リストのデフォルト値を使用します。このウィンドウには「管理」タブからアクセスできます。ただし、ログ・ソースの新規作成時、または自動的に検出されたログ・ソースの構成の更新時に、ログ・ソースのそれぞれでこのチェック・ボックスを構成することによってデフォルト値をオーバーライドできます。

9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

Symark PowerBroker の構成

Symark PowerBroker デバイスを、syslog を IBM Security QRadar に転送するように構成できます。

手順

1. IBM サポート Web サイトで、以下のファイルをダウンロードします。

   `pbforwarder.pl.gz`

   スクリプトは、以下の Web サイトからダウンロードすることができます。

   http://www.ibm.com/support
2. このファイルを Symark PowerBroker をホストするデバイスにコピーします。

注: Symark PowerBroker をホストするデバイスには Perl 5.8 がインストールされている必要があります。

3. 以下のコマンドを入力して、ファイルを解凍します。

```
gzip -d pbforwarder.pl.gz
```

4. 以下のコマンドを入力して、スクリプト・ファイルの権限を設定します。

```
chmod +x pbforwarder.pl
```

5. SSH を使用して、Symark PowerBroker をホストするデバイスにログインします。

使用する資格情報には、ログ・ファイルに対する読み取り、書き込みおよび実行の権限が必要です。

6. 適切なパラメーターを入力します。

表 *384.* コマンド・パラメーター

パラメーター	説明
-h	**-h** パラメーターは、Symark PowerBroker からイベントを受信する syslog ホストを定義します。これは、使用する QRadar またはイベント・コレクター (Event Collector)の IP アドレスです。
-t	**-t** パラメーターは、ログ・ファイルの追跡およびリスナーからの新規出力のモニターにコマンド・ラインが使用されることを定義します。 PowerBroker では、このコマンドを "pblog -l -t" と指定する必要があります。
-p	**-p** パラメーターは、イベント転送時に使用される TCP ポートを定義します。 何も指定しない場合、デフォルトはポート 514 です。
-H	**-H** パラメーターは、すべての送信イベントの syslog ヘッダー用のホスト名または IP アドレスを定義します。これは、Symark PowerBroker の IP アドレスにすることをお勧めします。
-r	**-r** パラメーターは、プロセス ID (.pid) ファイルを作成するディレクトリーの名前を定義します。デフォルトは /var/run です。 **-D** が指定されている場合、このパラメーターは無視されます。
-l	**-I** パラメーターは、ロック・ファイルの作成先ディレクトリーの名前を定義します。デフォルトは /var/lock です。 **-D** が指定されている場合、このパラメーターは無視されます。

表 *384.* コマンド・パラメーター *(*続き*)*

パラメーター	説明
-D	**-D** パラメーターは、スクリプトがフォアグラウンドで実行されることを定義します。 デフォルトの設定では、デーモンとして実行され、ローカルの Syslog サーバーに対するすべての内部メッセージがログに記録されます。
-f	**-f** パラメーターは、イベント・コレクター (Event Collector)に送信されるメッセージの syslog ファシリティーを定義し、またオプションで重大度も定義します。 値が指定されていない場合は、`user.info` が使用されます。
-a	**-a** パラメーターは、AIX 互換 *ps* メソッドを有効にします。 このコマンドが必要になるのは、AIX システム上で Symark PowerBroker を実行する場合のみです。
-d	**-d** パラメーターは、デバッグ・ロギングを有効にします。
-v	**-v** パラメーターは、スクリプトのバージョン情報を表示します。

7. 以下のコマンドを入力して、`pbforwarder.pl` スクリプトを開始します。

   ```
   pbforwarder.pl -h <IP address> -t "pblog -l -t"
   ```

   <IP address> は、QRadar またはイベント・コレクター (Event Collector)の IP アドレスです。
8. 以下のコマンドを入力して、`pbforwarder.pl` スクリプトを停止します。

   ```
   kill -QUIT `cat /var/run/pbforwarder.pl.pid`
   ```
9. 以下のコマンドを入力して、`pbforwarder.pl` スクリプトを再接続します。

   ```
   kill -HUP `cat /var/run/pbforwarder.pl.pid`
   ```

   QRadar は、Symark PowerBroker から転送される syslog イベントのログ・ソースの検出と作成を自動的に実行します。

第 131 章 Sourcefire Intrusion Sensor

IBM Security QRadar 用の Sourcefire Intrusion Sensor DSM は、Sourcefire デバイスから Snort ベースの侵入および防止の syslog イベントを受け入れます。

Sourcefire Intrusion Sensor の構成

Sourcefire Intrusion Sensor を構成するには、ポリシー・アラートを有効にして、QRadar にイベントを転送するようにアプライアンスを構成する必要があります。

手順

1. Sourcefire ユーザー・インターフェースにログインします。
2. ナビゲーション・メニューで、「侵入センサー **(Intrusion Sensor)**」>「検出ポリシー **(Detection Policy)**」>「編集」を選択します。
3. アクティブ・ポリシーを選択して「編集」をクリックします。
4. 「アラート設定 **(Alerting)**」をクリックします。
5. ポリシーの Syslog アラートを有効にする場合は、「状態」フィールドでオンを選択します。
6. ファシリティー・リストから「アラート」を選択します。
7. 優先順位リストから「アラート」を選択します。
8. 「ロギング・ホスト **(Logging Host)**」フィールドに、QRadar コンソールまたはイベント・コレクターの IP アドレスを入力します。
9. 「保存」をクリックします。
10. ナビゲーション・メニューで、「侵入センサー **(Intrusion Sensor)**」>「検出ポリシー **(Detection Policy)**」>「適用」を選択します。
11. 「適用」をクリックします。

次のタスク

これで、QRadar でログ・ソースを構成する準備ができました。

Cisco FireSIGHT Management Center イベントのログ・ソースの構成

QRadar では Cisco FireSIGHT Management Center イベントを自動的に検出しないため、ログ・ソースを構成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。

6. 「ログ・ソース・タイプ」リストで、「**Cisco FireSIGHT Management Center**」を選択します。
7. 「プロトコル構成」リストで「**Cisco Firepower eStreamer**」を選択します。
8. 以下のパラメーターを構成します。

パラメーター	説明
サーバー・アドレス	FireSIGHT Management Center デバイスの IP アドレスまたはホスト名。
サーバー・ポート	QRadar が FireSIGHT Management Center eStreamer イベントの受信に使用するポート番号。
鍵ストア・ファイル名	鍵ストアの秘密鍵と関連証明書のディレクトリー・パスおよびファイル名。
トラストストア・ファイル名	トラストストア・ファイルのディレクトリー・パスおよびファイル名。クライアントから信頼されている証明書を含むトラストストア・ファイルです。
追加データの要求 **(Request Extra Data)**	FireSIGHT Management Center eStreamer からの追加データを要求するには、このオプションを選択します。例えば、追加データには、イベントの元の IP アドレスなどがあります。
拡張要求の使用 **(Use Extended Requests)**	eStreamer ソースからイベントを取得する代替メソッドを使用するには、このオプションを選択します。 拡張要求は、FireSIGHT Management Center eStreamer バージョン 5.0 以降でサポートされます。

第 132 章 ThreatGRID Malware Threat Intelligence Platform

IBM Security QRadar 用の ThreatGRID Malware Threat Intelligence Platform DSM は、ログ・ファイル・プロトコルまたは syslog を使用してマルウェア・イベントを収集します。

QRadar は、QRadar ログ・イベント拡張フォーマット (LEEF) 作成スクリプトを使用する、v2.0 ソフトウェアを備えた ThreatGRID Malware Threat Intelligence Platform アプライアンスをサポートしています。

ThreatGRID Malware Threat Intelligence の場合にサポートされるイベント収集プロトコル

ThreatGRID Malware Threat Intelligence Platform は、IBM Security QRadar による読み取りが可能なマルウェア・イベントを書き込みます。

LEEF 作成スクリプトは ThreatGRID アプライアンスで構成され、ThreatGRID API を照会して、QRadar による読み取りが可能な LEEF イベントを書き込みます。ログ・ソースがマルウェア・イベントの収集に使用するイベント収集プロトコルは、ThreatGRID アプライアンスにインストールされたスクリプトによって決定されます。

LEEF 形式のイベントを収集するために、以下の 2 つのスクリプト・オプションを使用できます。

- `syslog` - syslog 版の LEEF 作成スクリプトでは、ThreatGRID アプライアンスがイベントを直接 QRadar に転送することができます。syslog スクリプトによって転送されたイベントは、QRadar によって自動的に検出されます。
- **ログ・ファイル** - ログ・ファイル・プロトコル版の LEEF 作成スクリプトでは、ThreatGRID アプライアンスがマルウェア・イベントをファイルに書き込むことができます。QRadar は、ログ・ファイル・プロトコルを使用してイベント・ログ・ホストと通信し、マルウェア・イベントを取得して解析します。

LEEF 作成スクリプトは ThreatGRID のカスタマー・サポートから入手できます。詳しくは、ThreatGRID の Web サイト http://www.threatgrid.com にアクセスするか、ThreatGRID のサポート (support@threatgrid.com) に E メールで問い合わせてください。

ThreatGRID Malware Threat Intelligence の構成の概要

ThreatGRID Malware Threat Intelligence イベントを IBM Security QRadar と統合することができます。

以下の作業を行う必要があります。

1. 収集のタイプに応じた QRadar ログ・イベント拡張フォーマット作成スクリプトを ThreatGRID のサポート Web サイトからアプライアンスにダウンロードします。

2. ThreatGRID アプライアンスにスクリプトをインストールし、ThreatGRID API をポーリングしてイベントを取得するように構成します。
3. QRadar アプライアンスで、ThreatGRID アプライアンスにインストールしたスクリプトに基づいてイベントを収集するためのログ・ソースを構成します。
4. ファイアウォール・ルールが ThreatGRID インストール済み環境と QRadar コンソールまたはイベント取得の役割を担う管理対象ホストの間の通信をブロックしていないことを確認します。

ThreatGRID の syslog ログ・ソースの構成

IBM Security QRadar は、ThreatGRID Malware Threat Intelligence Platform から転送されるマルウェア・イベントのログ・ソースの検出と作成を自動的に実行します。

このタスクについて

この手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「**ThreatGRID Malware Intelligence Platform**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *385. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	ThreatGRID Malware Intelligence Platform からのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
信頼性	リストから、ログ・ソースの信頼性を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。

表 385. *syslog* プロトコルのパラメーター (続き)

パラメーター	説明
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	リストから、ログの解析と保管を行うための受信ペイロード・エンコーダーを選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

QRadar に転送されたマルウェア・イベントは、QRadar の 「ログ・アクティビティー」タブに表示されます。

ThreatGRID ログ・ファイル・プロトコルのログ・ソースの構成

ログ・ファイル・プロトコルを使用してイベントを収集するには、マルウェア・イベントを含むイベント・ログをポーリングするように、IBM Security QRadar でログ・ソースを構成する必要があります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで、「**ThreatGRID Malware Intelligence Platform**」を選択します。
8. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
9. 以下の値を構成します。

表 *386.* ログ・ファイル・プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	イベント・ソースを識別するための IP アドレス、ホスト名、または名前を入力します。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
サービス・タイプ	リモート・サーバーからのログ・ファイルの取得に使用するプロトコルをリストから選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー・プロトコル SCP と SFTP のサービス・タイプは、「リモート **IP** またはホスト名」フィールドのホスト・サーバーで SFTP サブシステムが有効になっている必要があります。
リモート **IP** またはホスト名	イベント・ログ・ファイルが格納されている ThreatGRID サーバーの IP アドレスまたはホスト名を入力します。
リモート・ポート	ThreatGRID サーバーからのイベント・ログの取得に選択したプロトコルのポート番号を入力します。有効な範囲は、1 から 65535 です。 サービス・タイプのデフォルト・ポート番号のリスト • **FTP** - TCP ポート 21 • **SFTP** - TCP ポート 22 • **SCP** - TCP ポート 22
リモート・ユーザー	監査イベント・ログが格納される ThreatGRID Web サーバーへのログインに必要なユーザー名を入力します。 ユーザー名の長さは最大で 255 文字までです。
リモート・パスワード	ThreatGRID サーバーにログインするためのパスワードを入力します。
パスワードの確認	ThreatGRID サーバーにログインするためのパスワードを確認します。
SSH 鍵ファイル	サービス・タイプとして **SCP** または **SFTP** を選択する場合、このパラメーターを使用して SSH 秘密鍵ファイルを定義します。**SSH** 鍵ファイルを指定すると、「リモート・パスワード」フィールドは無視されます。
リモート・ディレクトリー	ログインに使用しているユーザー・アカウントに関連した、ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。「リモート・ディレクトリー」フィールドのブランク値は、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムが存在するシステムをサポートします。

表 386. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
再帰的 **(Recursive)**	ファイル・パターンでリモート・ディレクトリーのサブフォルダーを検索するようにしたい場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 「サービス・タイプ」として SCP を構成している場合は、「再帰的 **(Recursive)**」パラメーターが無視されます。
FTP ファイル・パターン	「リモート・ディレクトリー」で指定されたファイルのリストのフィルタリングに必要な正規表現 (regex) を入力します。この正規表現と一致するすべてのファイルが取得および処理されます。 FTP ファイル・パターンは、ThreatGRID イベント・ログに割り当てた名前と一致する必要があります。例えば、先頭が `leef` または `LEEF` で、末尾がテキスト・ファイル拡張子のファイルを収集するには、以下の値を入力します。 `(leef|LEEF)+.*¥.txt` このパラメーターの使用には、正規表現 (regex) の知識が必要です。このパラメーターは、FTP または SFTP の使用が構成されているログ・ソースに適用されます。
FTP 転送モード	「サービス・タイプ」として「**FTP**」を選択した場合は、リストから「ASCII」を選択します。 テキスト・ベースのイベント・ログには ASCII が必須です。
SCP リモート・ファイル	「サービス・タイプ」として「**SCP**」を選択した場合は、リモート・ファイルのファイル名を入力します。
開始時刻	ログ・ファイル・プロトコルを開始する時刻を表す時刻値を入力します。開始時刻は 24 時間クロックに基づき、HH:MM の形式を使用します。 例えば、午前 0 時にイベント・ファイルを収集するようにログ・ファイル・プロトコルをスケジュールするには、`00:00` と入力します。 このパラメーターは、新規イベント・ログ・ファイルがないかどうか ThreatGRID サーバーをポーリングするタイミングを設定するための「繰り返し **(Recurrence)**」フィールド値とともに機能します。
繰り返し **(Recurrence)**	新規イベント・ログ・ファイルがないかどうか ThreatGRID サーバーのリモート・ディレクトリーをスキャンする頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、開始時刻から 2 時間ごとにリモート・ディレクトリーをスキャンするには、`2H` と入力します。デフォルトの繰り返し値は 1H です。最短の時間間隔は 15M です。

表 386. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。 保存アクションが完了すると、ログ・ファイル・プロトコルは構成した開始時刻および繰り返しのスケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 **(Ignore Previously Processed File)**」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リストから「なし」を選択します。 プロセッサーによってイベント・ファイル・アーカイブの展開およびそれらのイベントの処理が可能になります。ファイルはダウンロード後に処理されます。QRadar は、`zip`、`gzip`、`tar`、または `tar+gzip` の各アーカイブ・フォーマットのファイルを処理できます。
以前に処理したファイルを無視 **(Ignore Previously Processed File(s))**	このチェック・ボックスを選択すると、既に処理済みのファイル追跡し、無視します。 QRadar は、リモート・ディレクトリー内のログ・ファイルを調べて、イベント・ログがログ・ソースによって処理されたかどうかを判別します。既に処理済みのファイルが検出された場合、ログ・ソースはそのファイルをダウンロードしません。新規、または未処理のイベント・ログ・ファイルのみが QRadar によってダウンロードされます。 このオプションは、**FTP** と **SFTP** のサービス・タイプに適用されます。
ローカル・ディレクトリーの変更	処理時のイベント・ログ・ファイルを格納するための QRadar アプライアンスのローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 大半のシナリオでは、このチェック・ボックスを選択しなくてもかまいません。このチェック・ボックスを選択すると、「ローカル・ディレクトリー **(Local Directory)**」フィールドが表示されます。イベント・ログ・ファイルを一時的に格納するローカル・ディレクトリーを構成できます。イベント・ログが処理されると、イベントは QRadar に追加され、ローカル・ディレクトリー内のイベント・ログが削除されます。
イベント・ジェネレーター **(Event Generator)**	「イベント・ジェネレーター **(Event Generator)**」リストで、「**1** 行ずつ **(LINEBYLINE)**」を選択します。 「イベント・ジェネレーター **(Event Generator)**」は、取得したイベント・ファイルに追加処理を適用します。ファイルの各行が、単一イベントです。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

10. 「保存」をクリックします。

11. 「管理」タブで「変更のデプロイ」をクリックします。

    ログ・ソースによって取得されたマルウェア・イベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

第 133 章 TippingPoint

IBM Security QRadar は、さまざまな Tipping Point DSM をサポートしています。

Tipping Point Intrusion Prevention System

IBM Security QRadar 用の Tipping Point Intrusion Prevention System (IPS) DSM は、syslog を使用して Tipping Point イベントを受け取ります。

QRadar は、Local Security Management (LMS) デバイスまたは Security Management System (SMS) を備えた複数のデバイスからの関連イベントをすべて記録します。

Tipping Point と統合するように QRadar を構成する前に、以下のようにタイプに応じてデバイスを構成する必要があります。

- SMS を使用する場合は、『SMS のリモート syslog の構成』を参照してください。
- LSM を使用する場合は、 1066 ページの『LSM の通知連絡先の構成』を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

SMS のリモート syslog の構成

Tipping Point を SMS 用に構成するには、アプライアンスによる syslog を使用したリモート・ホストへのイベントの転送を有効化して構成する必要があります。

このタスクについて

Tipping Point SMS を構成するには、以下の手順を実行します。

手順

1. Tipping Point システムにログインします。
2. 「管理 **(Admin)**」ナビゲーション・メニューで、「サーバー・プロパティー **(Server Properties)**」を選択します。
3. 「管理 **(Management)**」タブを選択します。
4. 「追加」をクリックします。

   「Syslog 通知の編集 (Edit Syslog Notification)」ウィンドウが表示されます。

5. 「有効にする **(Enable)**」チェック・ボックスを選択します。
6. 以下の値を構成します。
   a. **Syslog** サーバー **(Syslog Server)** - syslog イベント・メッセージを受信する QRadar の IP アドレスを入力します。
   b. ポート **(Port)** - ポート・アドレスとして 514 と入力します。
   c. ログ・タイプ **(Log Type)** - リストから「**SMS 2.0 / 2.1 Syslog** 形式 **(SMS 2.0 / 2.1 Syslog format)**」を選択します。
   d. ファシリティー **(Facility)** - リストから「ログ監査 **(Log Audit)**」を選択します。
   e. 重大度 **(Severity)** - リストから「イベントの重大度 **(Severity in Event)**」を選択します。
   f. 区切り文字 **(Delimiter)** - 生成されたログの区切り文字として「**TAB (**タブ**)**」を選択します。
   g. タイム・スタンプをヘッダーに含める **(Include Timestamp in Header)** - 「元のイベントのタイムスタンプを使用 **(Use original event timestamp)**」を選択します。
   h. 「**SMS** ホスト名をヘッダーに含める **(Include SMS Hostname in Header)**」チェック・ボックスを選択します。
   i. 「**OK**」をクリックします。
   j. これで、QRadar でログ・ソースを構成する準備ができました。
7. Tipping Point デバイスからのイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**Tipping Point** 侵入防止システム **(IPS) (Tipping Point Intrusion Prevention System (IPS))**」オプションを選択します。

   Tipping Point デバイスについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

LSM の通知連絡先の構成

LSM の通知連絡先を構成することができます。

手順

1. Tipping Point システムにログインします。
2. 「**LSM**」メニューで、「**IPS**」 > 「アクション・セット **(Action Sets)**」を選択します。

   「IPS プロファイル - アクション・セット (IPS Profile - Action Sets)」ウィンドウが表示されます。
3. 「通知連絡先 **(Notification Contacts)**」タブをクリックします。
4. 「連絡先リスト (Contacts List)」で「リモート・システム・ログ (Remote System Log)」をクリックします。

「通知連絡先の編集 (Edit Notification Contact)」ページが表示されます。

5. 以下の値を構成します。
   a. **Syslog** サーバー **(Syslog Server)** - syslog イベント・メッセージを受信する QRadar の IP アドレスを入力します。
   b. ポート **(Port)** - ポート・アドレスとして 514 と入力します。
   c. アラート・ファシリティー **(Alert Facility)** - 何も選択しないか、リストから数値 (0 から 31 まで) を選択します。syslog は、これらの数値を使用して、メッセージ・ソースを識別します。
   d. ブロック・ファシリティー **(Block Facility)** - 何も選択しないか、リストから数値 (0 から 31 まで) を選択します。 syslog は、これらの数値を使用して、メッセージ・ソースを識別します。
   e. デリミッター **(Delimiter)** - リストから「**TAB**」を選択します。
   f. 「テーブルの下に追加 **(Add to table below)**」をクリックします
   g. リモート・システム・ログの集計期間 (分) を構成します。
6. 「保存」をクリックします。

注**:** QRadar が Tipping Point デバイスとは別のサブネット内にある場合は、静的ルートの追加が必要になることがあります。詳しくは、ベンダーの資料を参照してください。

次のタスク

これで、LSM のアクション・セットを構成する準備ができました。詳しくは「『LSM のアクション・セットの構成』」を参照してください。

LSM のアクション・セットの構成

LSM のアクション・セットを構成することができます。

手順

1. Tipping Point システムにログインします。
2. 「**LSM**」メニューで、「**IPS** アクション・セット **(IPS Action Sets)**」を選択します。

   「IPS プロファイル - アクション・セット (IPS Profile - Action Sets)」ウィンドウが表示されます。
3. 「アクション・セットの作成 **(Create Action Set)**」をクリックします。

   「アクション・セットの作成/編集 (Create/Edit Action Set)」ウィンドウが表示されます。
4. アクション・セット名を入力します。
5. アクションに対してフロー制御アクション設定を選択します。
   - 許可 **(Permit)** - トラフィックを許可します。
   - 速度制限 **(Rate Limit)** - トラフィックの速度を制限します。「速度制限 (Rate Limit)」を選択した場合は、目的の速度を選択することもできます。
   - ブロック **(Block)** - トラフィックを許可しません。

- **TCP** リセット **(TCP Reset)** - ブロック・アクション とともに使用すると、特定の攻撃について送信元、宛先またはこの両方の IP アドレスがリセットされます。このオプションはブロックされた TCP フローをリセットします。
- 検疫 **(Quarantine)** - ブロック・アクション とともに使用すると、フィルターをトリガーした IP アドレス (ソースまたは宛先) がブロックされます。

6. 選択したアクションごとに「リモート・システム・ログ **(Remote System Log)**」チェック・ボックスを選択します。
7. 「作成」をクリックします。

   これで、QRadar でログ・ソースを構成する準備ができました。
8. Tipping Point デバイスからのイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストから「**Tipping Point** 侵入防止システム **(IPS) (Tipping Point Intrusion Prevention System (IPS))**」オプションを選択します。

   Tipping Point デバイスについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Tipping Point X505/X506 デバイス

IBM Security QRadar 用の Tipping Point X505/X506 DSM は syslog を使用してイベントを受け取ります。

QRadar は、関連するシステム・イベント、監査イベント、VPN イベント、およびファイアウォール・セッション・イベントをすべて記録します。

syslog の構成

イベントを IBM Security QRadar に転送するようにデバイスを構成することができます。

手順

1. Tipping Point X505/X506 デバイスにログインします。
2. 「**LSM**」メニューで「システム **(System)**」 > 「構成 **(Configuration)**」 > 「**Syslog** サーバー **(Syslog Servers)**」を選択します。

   「Syslog サーバー (Syslog Servers)」ウィンドウが表示されます。
3. 転送するログ・タイプごとに、チェック・ボックスを選択し、QRadar の IP アドレスを入力します。

   注**:** QRadar が Tipping Point デバイスとは別のサブネット内にある場合は、静的ルートの追加が必要になることがあります。詳しくは、ベンダーの資料を参照してください。

これで、QRadar でログ・ソースを構成する準備ができました。

4. Tipping Point X505/X506 デバイスからのイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで、「**Tipping Point X シリーズ・アプライアンス (Tipping Point X Series Appliances)**」オプションを選択します。

   注**:** 以前に構成した Tipping Point X505/X506 DSM が QRadar 上にインストールされ、構成されている場合は、「ログ・ソース・タイプ」リストに「Tipping Point X シリーズ・アプライアンス (Tipping Point X Series Appliances)」オプションが引き続き表示されます。ただし、構成対象のすべての新規 Tipping Point X505/X506 DSM に対して、「**Tipping Point Intrusion Prevention System (IPS)**」オプションを選択する必要があります。

関連タスク:

5 ページの『ログ・ソースの追加』

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 134 章 Top Layer IPS

IBM Security QRadar 用の Top Layer IPS DSM は syslog を使用して Top Layer IPS イベントを受け取ります。

QRadar は Top Layer イベントを記録して処理します。Top Layer デバイスと統合するように QRadar を構成する前に、Top Layer IPS デバイス内で syslog を構成する必要があります。Top Layer の構成について詳しくは、Top Layer の資料を参照してください。

構成は完了です。Top Layer IPS イベントが自動的に検出されるため、ログ・ソースが QRadar に追加されます。Top Layer IPS によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

Top Layer IPS デバイスからイベントを受信するように QRadar を構成するには、以下のようにします。

「ログ・ソース・タイプ」リストから「**Top Layer** 侵入防止システム **(IPS) (Top Layer Intrusion Prevention System (IPS))**」 オプションを選択します。

Top Layer デバイスについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 135 章 Townsend Security LogAgent

IBM iSeries® インフラストラクチャー上の Townsend Security LogAgent インストール済み環境から CEF 形式のイベントを収集できる IBM Security QRadar。

QRadar は、IBM iSeries V5.1 以上にインストールされた Townsend Security ソフトウェアからの CEF イベントをサポートしています。

サポートされるイベント・タイプ

IBM iSeries 上の Townsend Security LogAgent インストール済み環境は、セキュリティー、コンプライアンス、および監査のために Syslog イベントを QRadar に転送できます。

Raz-Lee iSecurity によって転送された syslog イベントはすべて自動的に検出されます。イベントは IBM AS/400 iSeries DSM で解析されて分類されます。

Raz-Lee iSecurity の構成

セキュリティー・イベントおよび監査イベントを収集するには、syslog イベントを IBM Security QRadar に転送するように Raz-Lee iSecurity インストール済み環境を構成する必要があります。

手順

1. IBM System i のコマンド・ライン・インターフェースにログインします。
2. 以下のコマンドを入力して、監査メニュー・オプションにアクセスします。

   ```
   STRAUD
   ```

3. 「監査 **(Audit)**」メニューから「**81.** システム構成 **(81. System Configuration)**」を選択します。
4. 「**iSecurity/**基本システム構成 **(iSecurity/Base System Configuration)**」メニューから、「**31. Syslog** 定義 **(31. SYSLOG Definitions)**」を選択します。
5. 以下のパラメーターを構成します。
   a. **SYSLOG** メッセージの送信 **(Send SYSLOG message)** - 「はい **(Yes)**」を選択します。
   b. 宛先アドレス **(Destination address)** - QRadar の IP アドレスを入力します。
   c. 使用する「ファシリティー」**("Facility" to use)** - ファシリティー・レベルを入力します。
   d. 自動送信する「重大度」の範囲 **("Severity" range to auto send)** - 重大度レベルを入力します。
   e. メッセージ構造 **(Message structure)** - syslog メッセージに必要な追加のメッセージ構造パラメーターがあれば、それを入力します。

次のタスク

Raz-Lee iSecurity によって転送される syslog イベントは、QRadar 用の IBM AS/400 iSeries DSM により自動的に検出されます。ほとんどの場合、いくつかのイベントが検出されると、ログ・ソースが QRadar で自動的に作成されます。イベント速度が低い場合、QRadar で Raz-Lee iSecurity のログ・ソースを手動で作成する必要があります。

ログ・ソースが自動的に検出されて識別されるまで、QRadar の「ログ・アクティビティー」タブでイベント・タイプは「不明」と表示されます。自動的に検出されたログ・ソースは、「ログ・ソース」アイコンをクリックすることで、QRadar の「管理」タブに表示できます。

ログ・ソースの構成

IBM Security QRadar は、Raz-Lee iSecurity から転送される syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。この手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リスト・ボックスで、「IBM AS/400 **iSeries**」を選択します。
9. 「プロトコル構成」リスト・ボックスで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *387. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Raz-Lee iSecurity がインストールされた IBM AS/400 iSeries デバイスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

第 136 章 Trend Micro

IBM Security QRadar は複数の Trend Micro DSM をサポートしています。

Trend Micro Control Manager

Trend Micro Control Manager デバイスを IBM Security QRadar と統合することができます。

Trend Micro Control Manager は、SNMPv1 または SNMPv2 を使用してイベントを受け入れます。Trend Micro Control Manager デバイスと統合するように QRadar を構成する前に、ログ・ソースを構成してから、ご使用の Trend Micro Control Manager の SNMP トラップ設定を構成する必要があります。

ログ・ソースの構成

IBM Security QRadar は、Trend Micro Control Manager からの SNMP イベントを自動的に検出することはありません。

このタスクについて

SNMPv1 または SNMPv2 プロトコルを使用するように、Trend Micro Control Manager 用の SNMP ログ・ソースを構成する必要があります。Trend Micro Control Manager は SNMPv3 をサポートしていません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**Trend Micro Control Manager**」を選択します。
9. 「プロトコル構成」リストで、「**SNMPv2**」を選択します。
10. Trend Micro Control Manager は SNMPv3 をサポートしていません。

    以下の値を構成します。

表 *388. SNMPv2* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Trend Micro Control Manager アプライアンスからのイベントの ID としてログ・ソースの IP アドレスまたはホスト名を入力します。

表 388. SNMPv2 プロトコルのパラメーター (続き)

パラメーター	説明
コミュニティー **(Community)**	SNMP イベントが含まれているシステムにアクセスするために必要な SNMP コミュニティー名を入力します。デフォルトは Public です。
イベント・ペイロードに **OID** を含める **(Include OIDs in Event Payload)**	「イベント・ペイロードに **OID** を含める **(Include OIDs in Event Payload)**」チェック・ボックスが選択されている場合はクリアします。 このオプションを使用すると、標準のイベント・ペイロード形式ではなく、名前と値のペア を使用して SNMP イベント・ペイロードを構成できます。特定の DSM からの SNMPv2 または SNMPv3 のイベントを処理する際に、「イベント・ペイロードに OID を含める (Include OIDs in Event Payload)」が必要になります。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。

SNMP トラップの構成

Trend Micro Control Manager の SNMP トラップを構成することができます。

このタスクについて

Trend Micro Control Manager v5.5 は、正しくフォーマットされた SNMPv2c イベントを提供するために、Hotfix 1697 または Hotfix 1713 を適用した Service Pack 1 Patch 1 以降が必要です。詳しくは、ベンダーの資料を参照してください。

手順

1. Trend Micro Control Manager デバイスにログインします。
2. 「管理 **(Administration)**」 > 「設定 **(Settings)**」 > 「イベントセンターの設定 **(Event Center Settings)**」を選択します。
3. SNMP トラップ通知を設定します。「**SNMP** トラップの設定 **(SNMP Trap Settings)**」フィールドにコミュニティー名を入力します。
4. IBM Security QRadar サーバーの IP アドレスを入力します。
5. 「保存」をクリックします。

これで、イベントセンターでイベントを構成する準備ができました。

6. 「管理 **(Administration)**」 > 「イベントセンター **(Event Center)**」を選択します。
7. 「イベントカテゴリー **(Event Category)**」リストで、「アラート **(Alert)**」を展開します。
8. アラートの「受信者 **(Recipients)**」をクリックします。
9. 「通知方法 **(Notification methods)**」で、「**SNMP** トラップの通知 **(SNMP Trap Notification)**」チェック・ボックスを選択します。
10. 「保存」をクリックします。

「受信者の編集結果 (Edit Recipients Result)」ウィンドウが表示されます。

11. 「**OK**」をクリックします。
12. SNMP トラップ通知を必要とするすべてのアラートに対して、 1076 ページの『SNMP トラップの構成』を繰り返します。

構成は完了です。Trend Micro Control Manager からのイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。Trend Micro Control Manager について詳しくは、ベンダーの資料を参照してください。

Trend Micro Deep Discovery Analyzer

Trend Micro Deep Discovery Analyzer 用の IBM Security QRadar DSM は、Trend Micro Deep Discovery Analyzer コンソールからイベント・ログを収集することができます。

以下の表は、Trend Micro Deep Discovery Analyzer DSM の仕様を示しています。

表 *389. Trend Micro Deep Discovery Analyzer DSM* の仕様

仕様	値
製造元	Trend Micro
DSM 名	Deep Discovery Analyzer
RPM ファイル名	DSM-TrendMicroDeepDiscoveryAnalyzer-*build_number*.noarch.rpm
サポートされるバージョン	1.0
イベント・フォーマット	LEEF
QRadar で記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Trend Micro Web サイト (www.trendmicro.com/DeepDiscovery■)

Trend Micro Deep Discovery イベントを QRadar に送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードしてください。
   - DSMCommon
   - Trend Micro Deep Discovery DSM
2. QRadar と通信するように Trend Micro Deep Discovery デバイスを構成します。
3. QRadar が Trend Micro Deep Discovery をログ・ソースとして自動的に検出しない場合は、QRadar コンソール上で Trend Micro Deep Discovery のログ・ソースを作成します。すべての必須パラメーターを構成します。以下の表を使用して、Trend Micro Deep Discovery Inspector イベントの収集に必要な固有の値を判別してください。

表 390. *Trend Micro Deep Discovery Analyzer* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Trend Micro Deep Discovery Analyzer
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

『QRadar との通信用に Trend Micro Deep Discovery Analyzer インスタンスを構成する』
Trend Micro Deep Discovery Analyzer イベントを収集するには、サード・パーティー・インスタンスを構成してロギングを有効にします。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に Trend Micro Deep Discovery Analyzer インスタンスを構成する

Trend Micro Deep Discovery Analyzer イベントを収集するには、サード・パーティー・インスタンスを構成してロギングを有効にします。

手順

1. Deep Discovery Analyzer Web コンソールにログインします。
2. 「管理者 **(Administrator)**」>「ログ設定 **(Log Settings)**」をクリックします。
3. 「ログを **Syslog** サーバーに転送する **(Forward logs to a syslog server)**」を選択します。
4. ログの形式として「**LEEF**」を選択します。
5. 「**Syslog** サーバー **(Syslog server)**」フィールドに、QRadar コンソールまたはイベント・コレクターの IP アドレスを入力します。
6. 「ポート **(Port)**」フィールドに 514 を入力します。

Trend Micro Deep Discovery Email Inspector

Trend Micro Deep Discovery Email Inspector 用の IBM Security QRadar DSM は、Trend Micro Deep Discovery Email Inspector デバイスからイベントを収集します。

以下の表は、Trend Micro Deep Discovery Email Inspector DSM の仕様を示しています。

表 391. *Trend Micro Deep Discovery Email Inspector DSM* の仕様

仕様	値
製造元	Trend Micro

表 391. *Trend Micro Deep Discovery Email Inspector DSM* の仕様 (続き)

仕様	値
DSM 名	Trend Micro Deep Discovery Email Inspector
RPM ファイル名	`DSM-TrendMicroDeepDiscoveryEmailInspector-`*`Qradar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	V2.1
イベント・フォーマット	ログ・イベント拡張フォーマット (LEEF)
記録されるイベント・タイプ	検出、Virtual Analyzer Analysis ログ、システム・イベント
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Trend Micro Web サイト (http://www.trendmicro.ca)

Trend Micro Deep Discovery Email Inspector を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Trend Micro Deep Discovery Email Inspector DSM RPM
   - DSM 共通 RPM
2. syslog イベントを QRadar に送信するように Trend Micro Deep Discovery Email Inspector デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Trend Micro Deep Discovery Email Inspector ログ・ソースを追加してください。以下の表は、Trend Micro Deep Discovery Email Inspector イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 392. *Trend Micro Deep Discovery Email Inspector* ログ・ソース・パラメーター

パラメーター	説明
ログ・ソース・タイプ	Trend Micro Deep Discovery Email Inspector
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に Trend Micro Deep Discovery Email Inspector を構成する

Trend Micro Deep Discovery Email Inspector からイベントを収集するには、IBM Security QRadar ホストの Syslog サーバー・プロファイルを構成します。

手順

1. Trend Micro Deep Discovery Email Inspector のユーザー・インターフェースにログインします。
2. 「管理 **(Administration)**」 > 「ログ設定 **(Log Settings)**」をクリックします。
3. 「追加」をクリックします。
4. 「状況 **(Status)**」に対して、「有効 **(Enabled)**」が選択されていることを確認します。デフォルトは、「有効」です。
5. 以下のパラメーターを構成します。

パラメーター	説明
プロファイル名	プロファイルの名前を指定します。
Syslog サーバー	QRadar サーバーのホスト名または IP。
ポート	514
ログ・フォーマット	LEEF

6. QRadar に送信するイベントのタイプとして、「検出 **(Detections)**」、「**Virtual Analyzer Analysis** ログ **(Virtual Analyzer Analysis logs)**」、および「システム・イベント **(System events)**」を選択します。

Trend Micro Deep Security

Trend Micro Deep Security 用の IBM Security QRadar DSM は、Trend Micro Deep Security サーバーからログを収集することができます。

以下の表は、Trend Micro Deep Security DSM の仕様を示しています。

表 *393. Trend Micro Deep Security DSM* の仕様

仕様	値
製造元	Trend Micro
DSM 名	Trend Micro Deep Security
RPM ファイル名	`DSM-TrendMicroDeepSecurity-`*`Qradar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	V9.6.1532 V10.0.1962
イベント・フォーマット	ログ・イベント拡張フォーマット

表 393. *Trend Micro Deep Security DSM* の仕様 (続き)

仕様	値
記録されるイベント・タイプ	アンチマルウェア Deep Security ファイアウォール Integrity Monitor 侵入防止 ログ検査 システム Web 評価
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Trend Micro Web サイト (https://www.trendmicro.com/us/)

Trend Micro Deep Security を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - Trend Micro Deep Security DSM RPM
   - DSMCommon RPM
2. syslog イベントを QRadar に送信するように Trend Micro Deep Security デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Trend Micro Deep Security DSM ログ・ソースを追加してください。以下の表は、Trend Micro Deep Security DSM イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 394. *Trend Micro Deep Security DSM* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Trend Micro Deep Security
プロトコル構成	Syslog

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用に Trend Micro Deep Security を構成する

Trend Micro Deep Security からすべてのイベントを収集するには、Syslog サーバーとして IBM Security QRadar を指定し、Syslog フォーマットを構成する必要があります。

始める前に

Deep Security Manager がインストールおよび構成されていることを確認します。

手順

1. 「管理」 > 「システム設定」 > 「**SIEM**」タブをクリックします。
2. Manager の「**System Event Notification**」領域で、「**Forward System Events to remote computer (via Syslog)**オプションを設定します。
3. QRadar システムのホスト名または IP アドレスを入力します。
4. UDP ポートに対して **514** と入力します。
5. 使用する「**Syslog Facility**」を選択します。
6. 「**Syslog Format**」について「**LEEF**」を選択します。

   注**:** Deep Security が LEEF 形式でイベントを送信できるのは、「**Manager**」からのみです。「**SIEM**」タブで「**Direct forward**」オプションを選択すると、「**Syslog Format**」について「**Log Event Extended Format 2.0**」を選択できません。

Trend Micro InterScan VirusWall

IBM Security QRadar 用の Trend Micro InterScan VirusWall DSM は syslog を使用してイベントを受け取ります。

Adaptive Log Exporter を使用することで、InterScan VirusWall ログを QRadar と統合することができます。Adaptive Log Exporter について詳しくは、IBM Security QRadar の「*Adaptive Log Exporter Users Guide*」を参照してください。

Adaptive Log Exporter を構成すると構成が完了します。Trend Micro InterScan VirusWall イベントは自動的に検出されるため、ログ・ソースが QRadar に追加されます。Trend Micro InterScan VirusWall によって QRadar に転送されたイベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

InterScan VirusWall デバイスからイベントを受け取るように手動で QRadar を構成するには、以下のようにします。

「ログ・ソース・タイプ」リストで「**Trend InterScan VirusWall**」オプションを選択します。

Trend Micro InterScan VirusWall デバイスについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Trend Micro Office Scan

IBM Security QRadar 用の Trend Micro Office Scan DSM は SNMPv2 を使用してイベントを受け取ります。

QRadar は、ウィルスおよびスパイウェアのイベントに関連するイベントを記録します。QRadar で Trend Micro デバイスを構成する前に、SNMPv2 イベントを転送するようにご使用のデバイスを構成する必要があります。

QRadar には、Trend Micro デバイスと統合するための 2 つのオプションが用意されています。選択する統合オプションはデバイスのバージョンによって異なり、以下のとおりです。

- 『Trend Micro Office Scan 8.x との統合』
- 1085 ページの『Trend Micro Office Scan 10.x との統合』

関連概念:

34 ページの『SNMPv2 プロトコルの構成オプション』
SNMPv2 プロトコルを使用して SNMPv2 イベントを受信するようにログ・ソースを構成することができます。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Trend Micro Office Scan 8.x との統合

Trend Micro Office Scan 8.x デバイスを IBM Security QRadar と統合することができます。

手順

1. Office Scan 管理インターフェースにログインします。
2. 「通知 **(Notifications)**」を選択します。
3. SNMP トラップの一般設定を構成します。「サーバー **IP** アドレス **(Server IP Address)**」フィールドに QRadar の IP アドレスを入力します。

   注**:** コミュニティー・トラップの情報は変更しないでください。
4. 「保存」をクリックします。
5. 標準アラート通知を構成します。「標準通知 **(Standard Notifications)**」を選択します。
6. 「**SNMP** トラップ **(SNMP Trap)**」タブをクリックします。

7. 「ウィルス/マルウェア検出時の **SNMP** トラップによる通知を有効にする **(Enable notification via SNMP Trap for Virus/Malware Detections)**」チェック・ボックスを選択します。
8. フィールドに以下のメッセージを入力します (これをデフォルトにしてください)。

   ```
   Virus/Malware: %v Computer: %s Domain: %m File: %p Date/Time: %y
   Result: %a
   ```

9. 「スパイウェア/グレーウェア検出時の **SNMP** トラップによる通知を有効にする **(Enable notification via SNMP Trap for Spyware/Grayware Detections)**」チェック・ボックスを選択します。
10. フィールドに以下のメッセージを入力します (これをデフォルトにしてください)。

    ```
    Spyware/Grayware: %v Computer: %s Domain: %m Date/Time: %y Result: %a
    ```

11. 「保存」をクリックします。
12. アウトブレーク・アラート通知を構成します。アウト通知 **(Out Notifications)**」を選択します。
13. 「**SNMP** トラップ **(SNMP Trap)**」タブをクリックします。
14. 「ウィルス/マルウェアのアウトブレーク時の **SNMP** トラップによる通知を有効にする **(Enable notification via SNMP Trap for Virus/Malware Outbreaks)**」チェック・ボックスを選択します。
15. フィールドに以下のメッセージを入力します (これをデフォルトにしてください)。

    ```
    Number of viruses/malware: %CV Number of computers: %CC Log Type
    Exceeded: %A Number of firewall violation logs: %C Number of shared
    folder sessions: %S Time Period: %T
    ```

16. 「スパイウェア/グレーウェアのアウトブレーク時の **SNMP** トラップによる通知を有効にする **(Enable notification via SNMP Trap for Spyware/Grayware Outbreaks)**」チェック・ボックスを選択します。
17. フィールドに以下のメッセージを入力します (これをデフォルトにしてください)。

    ```
    Number of spyware/grayware: %CV Number of computers: %CC Log Type
    Exceeded: %A Number of firewall violation logs: %C Number of shared
    folder sessions: %S Time Period: %T
    ```

18. 「保存」をクリックします。 これで、QRadar でログ・ソースを構成する準備ができました。
19. Trend Micro Office Scan デバイスを構成するには、以下を実行します。
    a. 「ログ・ソース・タイプ」リストで「**Trend Micro Office Scan**」オプションを選択します。
    b. 「プロトコル構成」リストで「**SNMPv2**」オプションを選択します。

Trend Micro Office Scan 10.x との統合

Trend Micro Office Scan 10.x デバイスと統合するように IBM Security QRadar を構成するには、いくつかの準備ステップが必要です。

このタスクについて

必要なステップは以下のとおりです。

1. Trend Micro Office Scan 10.x 用の SNMP 設定を構成する。
2. 標準通知を構成する。
3. アウトブレーク基準およびアラート通知を構成する。

一般設定の構成

このタスクについて

Trend Micro Office Scan 10.x デバイスを IBM Security QRadar と統合することができます。

手順

1. Office Scan 管理インターフェースにログインします。
2. 「通知 **(Notifications)**」 > 「管理者通知 **(Administrator Notifications)**」 > 「一般設定 **(General Settings)**」を選択します。
3. SNMP トラップの一般設定を構成します。「サーバー **IP** アドレス **(Server IP Address)**」フィールドに QRadar の IP アドレスを入力します。
4. Trend Micro Office Scan デバイスのコミュニティー名を入力します。
5. 「保存」をクリックします。

次のタスク

次は、Office Scan の標準通知を構成する必要があります。

標準通知の構成

標準通知を構成することができます。

手順

1. 「通知 **(Notifications)**」 > 「管理者通知 **(Administrator Notifications)**」 > 「標準通知 **(Standard Notifications)**」を選択します。
2. 基準設定を定義します。「基準 **(Criteria)**」タブをクリックします。
3. ウィルス/マルウェア、およびスパイウェア/グレーウェアの検出時、またはこれらのセキュリティー・リスクに対するアクションが失敗したときに管理者にアラートを通知するオプションを選択します。
4. 通知を有効にするには、「**SNMP** トラップ **(SNMP Trap)**」タブを構成します。
5. 「**SNMP** トラップによる通知を有効にする **(Enable notification via SNMP Trap)**」チェック・ボックスを選択します。
6. フィールドに以下のメッセージを入力します。

```
Virus/Malware: %v Spyware/Grayware: %T Computer: %s IP address: %i
Domain: %m File: %p Date/Time: %y Result: %a User name: %n
```

7. 「保存」をクリックします。

次のタスク

次は、アウトブレーク通知を構成する必要があります。

アウトブレークの基準とアラート通知の構成

アウトブレークの基準とアラート通知を構成することができます。

手順

1. 「通知 **(Notifications)**」 > 「管理者通知 **(Administrator Notifications)**」 > 「アウトブレーク通知 **(Outbreak Notifications)**」を選択します。
2. 「基準 **(Criteria)**」タブをクリックします。
3. 各セキュリティー・リスクに対し、検出数と検出期間を入力します。

   基準が指定された検出制限を超えると、通知メッセージが管理者に送信されます。

   注**:** Trend Micro では、検出数と検出期間にデフォルト値を使用することを勧めています。
4. 「共有フォルダー・セッション・リンク **(Shared Folder Session Link)**」を選択し、Office Scan でファイアウォール違反および共有フォルダー・セッションをモニターできるようにします。

   注**:** 共有フォルダーのあるネットワーク上のコンピューター、または現在共有フォルダーを参照中のコンピューターを表示するには、インターフェースで番号リンクを選択します。
5. 「**SNMP** トラップ **(SNMP Trap)**」タブをクリックします。
   a. 「**SNMP** トラップによる通知を有効にする **(Enable notification via SNMP Trap)**」チェック・ボックスを選択します。
6. フィールドに以下のメッセージを入力します。

   ```
   Number of viruses/malware: %CV Number of computers: %CC Log Type
   Exceeded: %A Number of firewall violation logs: %C Number of shared
   folder sessions: %S Time Period: %T
   ```
7. 「保存」をクリックします。
8. これで、QRadar でログ・ソースを構成する準備ができました。

   Trend Micro Office Scan デバイスを構成するには、以下を実行します。
   a. 「ログ・ソース・タイプ」リストで「**Trend Micro Office Scan**」オプションを選択します。
   b. 「プロトコル構成」リストで「**SNMPv2**」オプションを選択します。

第 137 章 Tripwire

Tripwire DSM は、syslog を使用してリソースの追加、削除、変更の各イベントを受け入れます。

手順

1. Tripwire インターフェースにログインします。
2. 左側のナビゲーションで、「アクション **(Actions)**」をクリックします。
3. 「新規アクション **(New Action)**」をクリックします。
4. 新規アクションを構成します。
5. 「ルール **(Rules)**」を選択し、モニターするルールをクリックします。
6. 「アクション **(Actions)**」タブを選択します。
7. 新規アクションが選択されていることを確認します。
8. 「**OK**」をクリックします。
9. モニター対象の各ルールについて、『第 137 章 Tripwire』の手順を繰り返します。 これで、QRadar でログ・ソースを構成する準備ができました。
10. Tripwire デバイスからのイベントを受信するように QRadar を構成するには、「ログ・ソース・タイプ」リストで「**Tripwire Enterprise**」オプションを選択します。

    Tripwire デバイスについて詳しくは、ベンダーの資料を参照してください。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 138 章 Tropos Control

IBM Security QRadar 用の Tropos Control DSM は、syslog を使用してイベントを受け入れます。

このタスクについて

QRadar は、障害管理イベント、ログインとログアウトのイベント、プロビジョニング・イベント、およびデバイス・イメージのアップロード・イベントのすべてを記録できます。QRadar を構成する前に、syslog イベントを転送するように Tropos Control を構成しておく必要があります。

Tropos Control を、syslog を使用してログを QRadar に転送するように構成することができます。

手順

1. SSH を使用して、root ユーザーとして Tropos Control デバイスにログインします。
2. 編集する以下のファイルを開きます。

   ```
   /opt/ControlServer/ems/conf/logging.properties
   ```
3. syslog を有効にするには、以下の行からコメント・マーカー (#) を削除します。

   ```
   #log4j.category.syslog = INFO, syslog
   ```
4. syslog 宛先の IP アドレスを構成するには、以下の行を編集します。

   ```
   log4j.appender.syslog.SyslogHost = <IP address>
   ```

   ここで *<IP address>* は、QRadar の IP アドレスまたはホスト名です。

   デフォルトでは、Tropos Control はファシリティー **USER** とデフォルト・ログ・レベル **INFO** を使用します。これらのデフォルト設定は、Tropos Control デバイスからの syslog イベントの収集に適しています。
5. ファイルを保存して終了します。
6. これで、QRadar で Tropos Control DSM を構成する準備ができました。

   Tropos Control からのイベントを受信するように QRadar を構成するには、以下を実行します。

   a. 「ログ・ソース・タイプ」リストで「**Tropos Control**」を選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプラ

イアンスからイベントを受信するログ・ソースを手動で追加できます。

第 139 章 共通

IBM Security QRadar は、ユニバーサル DSM を使用して、任意のネットワーク・インフラストラクチャーやセキュリティー・デバイスからイベントを収集して相関付けることができます。

イベントの収集後、かつ相関の開始前に、デバイスからの個々のイベントを適切に解析して、イベント名、IP アドレス、プロトコル、およびポートを判別する必要があります。一般的なネットワーク・デバイス (Cisco ファイアウォールなど) の場合は、QRadar が各デバイスからのイベント・メッセージを適切に解析して分類するように事前定義 DSM が設計されています。デバイスからのイベントが DSM によって解析されると、QRadar が引き続きイベントをオフェンスに相関付けることができます。

正式にサポートされていないネットワーク・デバイスまたはセキュリティー・デバイスが 1 つ以上エンタープライズ・ネットワークに存在し、そのデバイスに対する固有の DSM が存在しない場合は、ユニバーサル DSM を使用できます。ユニバーサル DSM により、サポートされないデバイスからイベントおよびメッセージを転送することができます。また、ユニバーサル DSM を使用して QRadar 用にイベントを分類することができます。ユニバーサル DSM を使用することで、実質的にすべてのデバイスや一般的なプロトコル・ソースと QRadar を統合することができます。

ユニバーサル DSM を構成するには、デバイス拡張を使用して、ユニバーサル DSM をデバイスに関連付ける必要があります。「管理」タブでログ・ソース・ウィンドウを使用してデバイス拡張情報を定義する前に、ログ・ソース拡張の文書を作成する必要があります。

ユニバーサル DSM の記述およびテストについて詳しくは、https://www.ibm.com/developerworks/community/forums のサポート・フォーラムを参照してください。

関連概念:

45 ページの『第 3 章 ログ・ソース拡張』
拡張文書により、特定のログ・ソースのエレメントを構文解析する方法を拡張したり変更したりすることができます。拡張文書を使用して、構文解析の問題を修正したり、既存の DSM からのイベントに対するデフォルトの構文解析をオーバーライドしたりすることができます。

関連タスク:

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

Universal CEF

IBM Security QRadar DSM for Universal CEF は、共通イベント・フォーマット (CEF) でイベントを生成するデバイスからイベントを受け取ります。

以下の表は、Universal CEF DSM の仕様を示しています。

表 *395. Universal CEF DSM* の仕様

仕様	値
DSM 名	Universal CEF
RPM ファイル名	DSM-UniversalCEF-*Qradar_version-build_number*.noarch.rpm
プロトコル	Syslog ログ・ファイル
記録されるイベント・タイプ	CEF フォーマットのイベント
自動的に検出?	いいえ
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ

CEF フォーマットのイベントを生成するデバイスから QRadar にイベントを送信するには、以下のステップを実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - Universal CEF RPM
2. QRadar コンソールで、Universal CEF ログ・ソースを追加します。Universal CEF 固有の以下の値を使用します。

パラメーター	説明
ログ・ソース・タイプ	Universal CEF
プロトコル構成	Syslog またはログ・ファイル

3. イベントを QRadar に送信するようにサード・パーティー・デバイスを構成します。サード・パーティー・デバイスの構成方法について詳しくは、ベンダーの資料を参照してください。
4. Universal CEF イベントのイベント・マッピングを構成します。

Universal CEF イベントのイベント・マッピングの構成

Universal CEF イベントには、セキュリティー・イベントを分類するための定義済み QRadar ID (QID) マップが含まれていません。Universal CEF ログ・ソースから不明のイベントを検索し、それらを上位カテゴリーおよび下位カテゴリーにマップする必要があります。

始める前に

QRadar で、Universal CEF DSM がインストールされていること、およびそのログ・ソースが追加されていることを確認してください。

このタスクについて

Universal CEF DSM では、デフォルトでは、すべてのイベントが「不明」として分類されます。すべての Universal CEF イベントで、「ログ・アクティビティー」タブの「イベント名」列および「下位カテゴリー」列には、値として「不明」が表示されます。QRadar で、QID マップを変更して、デバイスの各イベントをイベント・カテゴリーに個別にマップする必要があります。イベントをマップすることで、QRadar は、ネットワーク・デバイスからのイベントを識別、統合、および追跡できます。

イベント・マッピングについて詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

手順

1. QRadar にログインします。
2. 「ログ・アクティビティー」タブをクリックします。
3. 「フィルターの追加」をクリックします。
4. 最初のリストから「ログ・ソース」を選択します。
5. 「ログ・ソース・グループ」リストから「その他」を選択します。
6. 「ログ・ソース」リストから、ご使用の Universal CEF ログ・ソースを選択します。
7. 「フィルターの追加」をクリックします。
8. 「表示」リストから「過去 **1** 時間」を選択します。
9. オプション: 「条件の保存」をクリックして、既存の検索フィルターを保存します。
10. 「イベント名」列で、Universal CEF DSM の不明イベントをダブルクリックします。
11. 「イベントのマップ」をクリックします。
12. 「QID の参照 (Browse for QID)」ペインから、以下のいずれかの検索オプションを選択し、QRadar ID (QID) のイベント・カテゴリーを絞り込みます。
    - 「上位カテゴリー」リストから、上位イベント・カテゴリーを選択します。上位イベント・カテゴリーと下位イベント・カテゴリーの全リストおよびカテゴリーの定義については、「*IBM Security QRadar* 管理ガイド」の『イベント・カテゴリー』セクションを参照してください。
    - 「下位カテゴリー」リストから、下位イベント・カテゴリーを選択します。
    - 「ログ・ソース・タイプ」リストから、ログ・ソース・タイプを選択します。

      ヒント: Universal CEF DSM からのイベントが別の既存のネットワーク・デバイスからのイベントに類似している場合、ログ・ソースで QID を検索すると便利です。例えば、Universal CEF がファイアウォール・イベントを

提供する場合、類似するイベントをキャプチャーする可能性のある別のファイアウォール製品として Cisco ASA を選択します。

- 名前で QID を検索するには、「**QID/**名前」フィールドに名前を入力します。

13. 「検索」をクリックします。
14. 不明の Universal CEF DSM イベントに関連付ける QID を選択し、「**OK**」を選択します。

ユニバーサル LEEF

IBM Security QRadar 用のユニバーサル LEEF DSM は、ログ・イベント拡張フォーマット (LEEF) を使用してイベントを生成するデバイスからイベントを受け取ることができます。

LEEF イベント形式はプロプラエタリーなイベント形式であり、この形式を使用することで、ハードウェア・メーカーおよびソフトウェア製品メーカーが、QRadar と統合するために特に設計されたデバイス・イベントを読み取ってマップすることができます。

パートナーシップ・プログラムの外部で QRadar に LEEF 形式のイベントを送信するには、ユニバーサル LEEF DSM をインストールしておき、不明なイベントをマップすることで、QRadar に転送された各イベントを手動で識別する必要があります。ユニバーサル LEEF DSM は、ログ・ファイル・プロトコルを使用してデバイスまたはディレクトリーからポーリングされた LEEF 形式のイベントを含む syslog またはファイルから転送されたイベントを解析できます。

ユニバーサル LEEF を使用して QRadar でイベントを構成するには、以下を実行する必要があります。

1. QRadar でユニバーサル LEEF ログ・ソースを構成します。
2. LEEF 形式のイベントをデバイスから QRadar に送信します。イベントの転送について詳しくは、ベンダーの資料を参照してください。
3. 不明なイベントを QRadar ID (QID) にマップします。

Universal LEEF ログ・ソースの構成

イベントを IBM Security QRadar に送信するようにデバイスを構成する前に、LEEF イベントを提供するデバイス用のログ・ソースを追加しておく必要があります。

このタスクについて

QRadar は、syslog を使用してリアルタイムのソースから、またはログ・ファイル・プロトコルを使用してデバイスやリポジトリーに保管されたファイルから、イベントを受信できます。

syslog を使用して Universal LEEF 用のログ・ソースを構成するには、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「ユニバーサル **LEEF**」を選択します。
9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *396. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース ID	Universal LEEF イベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

    ログ・ソースが QRadar に追加されます。これで、LEEF イベントを QRadar に転送する準備ができました。

Universal LEEF イベントを収集するためのログ・ファイル・プロトコルの構成

ログ・ファイル・プロトコルにより、IBM Security QRadar は、リモート・ホストまたはファイル・リポジトリーからアーカイブ・イベントまたはログ・ファイルを取得することができます。

このタスクについて

ログ・ファイルは、一度に 1 つずつ、処理のために QRadar に転送されます。QRadar はイベント・ファイルを読み取り、ログ・ソースを新しいイベントで更新します。ログ・ファイル・プロトコルによってアーカイブ・ファイルをポーリングするため、イベントはリアルタイムで提供されず、一括で追加されます。ログ・ファイル・プロトコルは、プレーン・テキストの圧縮ファイル、アーカイブを管理できます。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「ログ・ソース名」フィールドにユニバーサル LEEF のログ・ソースの名前を入力します。

6. 「ログ・ソースの説明」フィールドにユニバーサル LEEF のログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「ユニバーサル **LEEF**」を選択します。
8. 「プロトコル構成」リストで「ログ・ファイル」を選択します。
9. 以下のパラメーターを構成します。

表 *397.* ログ・ファイル・プロトコルのパラメーター

パラメーター	説明
ログ・ソース ID	Universal LEEF ログ・ソースの IP アドレスまたはホスト名を入力します。この値は、「リモート・ホスト **IP (Remote Host IP)**」または「ホスト名 **(Hostname)**」のパラメーターで構成した値と一致している必要があります。 ログ・ソース ID は、ログ・ソース・タイプに対して固有でなければなりません。
サービス・タイプ	削除サーバーからログ・ファイルを取得する際に使用するプロトコルをリストから選択します。デフォルトは SFTP です。 • **SFTP** - SSH ファイル転送プロトコル • **FTP** - ファイル転送プロトコル • **SCP** - セキュア・コピー サービス・タイプ SCP および SFTP のログ・ファイルを取得するために使用される基礎のプロトコルでは、「リモート **IP/**ホスト名」フィールドに指定されているサーバーの SFTP サブシステムが有効になっている必要があります。
リモート IP またはホスト名	受信するファイルの送信元ホストの IP アドレスまたはホスト名を入力します。
リモート・ポート	選択されたサービス・タイプを実行するリモート・ホスト上の TCP ポートを入力します。サービス・タイプを FTP として構成する場合、デフォルトは 21 です。サービス・タイプを SFTP または SCP として構成する場合、デフォルトは 22 です。有効な範囲は、1 から 65535 です。
リモート・ユーザー	選択したサービス・タイプを実行しているホストへのログインに必要なユーザー名を入力します。ユーザー名の長さは 255 文字まで可能です。
リモート・パスワード	LEEF イベント・ファイルを格納しているホストへのログインに必要なパスワードを入力します。
パスワードの確認	LEEF イベント・ファイルを格納しているホストへのログインに必要なリモート・パスワードを確認します。
SSH 鍵ファイル	サービス・タイプとして SCP または SFTP を選択する場合、このパラメーターを使用して SSH 秘密鍵ファイルを定義できます。SSH 鍵ファイルを指定すると、「リモート・パスワード」オプションは無視されます。

表 397. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
リモート・ディレクトリー	ファイルを取得するリモート・ホスト上のディレクトリーの場所を入力します。 FTP の場合のみ。ログ・ファイルがリモート・ユーザーのホーム・ディレクトリー内にある場合は、リモート・ディレクトリーをブランクのままにしておくことができます。これは、作業ディレクトリーの変更 (CWD) コマンドが制限されているオペレーティング・システムをサポートするためです。
再帰的 (Recursive)	ファイル・パターンでサブフォルダーを検索する場合は、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 SCP をサービス・タイプとして構成する場合は、「再帰的 (Recursive)」パラメーターは使用されません。
FTP ファイル・パターン	SFTP または FTP をサービス・タイプとして選択する場合、このオプションによって、リモート・ディレクトリーで指定されたファイルのリストをフィルタリングするために必要な正規表現 (regex) を構成できます。一致するすべてのファイルは処理に組み込まれます。 例えば、先頭が「log」という語で、1 桁以上の数字が続き、末尾が `tar.gz` であるすべてのファイルをリストする場合は、「`log[0-9]+¥.tar¥.gz`」と入力します。このパラメーターの使用には、正規表現 (regex) の知識が必要です。詳しくは、Web サイト http://download.oracle.com/javase/tutorial/essential/regex/ を参照してください。
FTP 転送モード	このオプションは、「サービス・タイプ」として「FTP」を選択した場合にのみ表示されます。「FTP 転送モード」パラメーターにより、FTP を介してログ・ファイルを取得するときのファイル転送モードを定義できます。 リストから、このログ・ソースに適用する転送モードを選択します。 • バイナリー - バイナリー・データ・ファイル、または圧縮された zip、gzip、tar、tar + gzip のアーカイブ・ファイルを必要とするログ・ソースには、「バイナリー」を選択します。 • ASCII - ASCII FTP ファイル転送を必要とするログ・ソースには、ASCII を選択します。 ASCII を FTP 転送モードとして使用する場合は、「プロセッサー」には「なし」を、「イベント・ジェネレーター」には「**1** 行ずつ **(LINEBYLINE)**」を選択する必要があります。
SCP リモート・ファイル	SCP をサービス・タイプとして選択する場合は、リモート・ファイルのファイル名を入力する必要があります。
開始時刻	処理を開始する時刻を入力します。このパラメーターと「繰り返し (Recurrence)」の値の組み合わせにより、リモート・ディレクトリーでファイルをスキャンするタイミングと頻度が決定されます。「HH:MM」の形式で、24 時間クロックに基づいて開始時刻を入力します。

表 397. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
繰り返し (Recurrence)	開始時刻に始まる、リモート・ディレクトリーのスキャンの頻度を入力します。この値は、時間数 (H)、分数 (M)、または日数 (D) で入力します。 例えば、ディレクトリーを 2 時間おきにスキャンする場合は、2H と入力します。デフォルトは 1H です。
保存時に実行	「保存」をクリックした後にログ・ファイル・プロトコルを即時に実行するには、このチェック・ボックスを選択します。「保存時に実行」が完了した後には、ログ・ファイル・プロトコルは構成済みの開始時刻と反復スケジュールに従います。 「保存時に実行」を選択すると、「以前に処理したファイルを無視 (Ignore Previously Processed File)」パラメーターの、以前に処理したファイルのリストはクリアされます。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数を入力します。有効な範囲は、100 から 5000 です。
プロセッサー	リモート・ホストにあるファイルが zip、gzip、tar、または tar+gzip のアーカイブ・フォーマットで保管されている場合は、アーカイブを展開して内容を処理することができるプロセッサーを選択します。
以前に処理したファイルを無視 (Ignore Previously Processed File(s))	再処理を必要としない、既に処理済みのファイルを追跡する際に、このチェック・ボックスを選択します。これは FTP および SFTP のサービス・タイプに適用されます。
ローカル・ディレクトリーの変更	処理中にダウンロードしたファイルを保管するために使用する、QRadar システム上のローカル・ディレクトリーを定義するには、このチェック・ボックスを選択します。 このチェック・ボックスはクリアしたままにしておくことをお勧めします。このチェック・ボックスを選択すると、「ローカル・ディレクトリー」フィールドが表示され、ファイルの保管に使用するローカル・ディレクトリーを構成できます。
イベント・ジェネレーター (Event Generator)	「イベント・ジェネレーター **(Event Generator)**」リストで、LineByLine を選択します。 イベント・ジェネレーターは、取得されたイベント・ファイルに追加の処理を適用します。「1 行ずつ (LineByLine)」オプションは、ファイルの各行を単一のイベントとして読み取ります。例えば、ファイルに 10 行のテキストがある場合、10 件の個別のイベントが生成されます。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。これで、ログ・ファイル・プロトコルを使用して取得可能な LEEF イベントを書き込む準備ができました。

IBM Security QRadar へのイベント転送

ログ・ソースを作成すると、QRadar のためのイベント転送または取得が可能になります。syslog を使用してイベントを転送するには、ネットワーク・デバイスの追加構成が必要になる場合があります。

QRadar が syslog を使用するかログ・ファイルをポーリングすることでイベントが検出されると、イベントが「ログ・アクティビティー」タブに表示されます。LEEF イベントを転送するデバイスからのイベントは、「ログ・ソース名」フィールドに入力した名前によって示されます。QRadar のデフォルトではログ・ソースのイベントが分類されないため、それらの分類が必要です。ユニバーサル LEEF イベントの分類について詳しくは、『ユニバーサル LEEF イベント・マップの作成』を参照してください。

ユニバーサル LEEF イベント・マップの作成

ユニバーサル LEEF イベントにはセキュリティー・イベントを分類する事前定義の QRadar ID (QID) マップが含まれないため、ユニバーサル LEEF DSM の場合はイベントのマッピングが必要です。

SIPP Partner Program のメンバーの QID マップはネットワーク・デバイスに応じて設計されており、構成が文書化されているため、QID マップは IBM Corp. によってテストされています。

ユニバーサル LEEF DSM では、デバイスの各イベントを個別に IBM Security QRadar のイベント・カテゴリーにマップする必要があります。イベントをマップすることで、QRadar は、ネットワーク・デバイスからの繰り返しイベントを識別、統合、および追跡できます。イベントをマップしない限り、ユニバーサル LEEF DSM の「ログ・アクティビティー」タブに表示されるイベントは、すべて「不明」に分類されます。不明なイベントは「イベント名」列に示され、「下位カテゴリー」列に「不明」と表示されるため、簡単に分かります。

不明イベントの検出

デバイスが IBM Security QRadar にイベントを送信するときに、イベント・ソースのアプライアンスまたはソフトウェアが一部のイベントをすぐに生成できない場合があるため、デバイスからのすべてのイベントを分類するには時間がかかる可能性があります。

このタスクについて

不明イベントを迅速に検索する方法を把握しておくと有益です。不明イベントの検索方法が分かっている場合は、ほとんどの Universal LEEF イベントが識別されたと判断できるまで、この検索を繰り返すことをお勧めします。

手順

1. QRadar にログインします。
2. 「ログ・アクティビティー」タブをクリックします。
3. 「フィルターの追加」をクリックします。
4. 最初のリストから「ログ・ソース」を選択します。

5. 「ログ・ソース・グループ」リストから、ログ・ソース・グループまたは「その他」を選択します。

   グループに割り当てられていないログ・ソースは「その他」に分類されます。
6. 「ログ・ソース」リストから、Universal LEEF ログ・ソースを選択します。
7. 「フィルターの追加」をクリックします。

   「ログ・アクティビティー」タブに、Universal LEEF DSM 用のフィルターが表示されます。
8. 「表示」リストから「過去 **1** 時間」を選択します。

   Universal LEEF DSM によって過去 1 時間に生成されたイベントがすべて表示されます。「イベント名」列、または「下位カテゴリー」列に「不明」として表示されているイベントについては、QRadar でのイベント・マッピングが必要です。

   注**:** 「条件の保存」をクリックすると、既存の検索フィルターを保存することができます。

   これで、Universal LEEF DSM のイベント・マップを変更する準備ができました。

イベント・マップの変更

イベント・マップを変更する際に、イベントを手動で IBM Security QRadar ID (QID) マップに分類できます。

このタスクについて

ログ・ソースに分類された任意のイベントを、新しい QRadar ID (QID) に再マップできます。デフォルトでは、Universal LEEF DSM はすべてのイベントを「不明」として分類します。

注**:** ログ・ソースが定義されていないイベントは、イベントにマップできません。ログ・ソースのないイベントの場合、「ログ・ソース」列に「SIM 汎用ログ (SIM Generic Log)」と表示されます。

手順

1. 「イベント名」列で、Universal LEEF DSM の不明イベントをダブルクリックします。

   詳細なイベント情報が表示されます。
2. 「イベントのマップ」をクリックします。
3. 「QID の参照 (Browse for QID)」ペインから、以下のいずれかの検索オプションを選択して、QRadar ID (QID) のイベント・カテゴリーを絞り込みます。
   a. 「上位カテゴリー」リストから、上位イベント・カテゴリーを選択します。

      上位イベント・カテゴリーと下位イベント・カテゴリーの全リストおよびカテゴリーの定義については、「*IBM Security QRadar* 管理ガイド」の『イベント・カテゴリー』セクションを参照してください。

4. 「下位カテゴリー」リストから、下位イベント・カテゴリーを選択します。
5. 「ログ・ソース・タイプ」リストから、ログ・ソース・タイプを選択します。

   「ログ・ソース・タイプ」リストでは、他のログ・ソースからの QID を検索することができます。Universal LEEF DSM からのイベントが既存の別のネットワーク・デバイスからのイベントと類似している場合、ログ・ソースで QID を検索すると便利です。例えば、Universal DSM がファイアウォール・イベントを提供している場合、類似するイベントをキャプチャーする可能性のある別のファイアウォール製品として Cisco CA を選択できます。
6. 名前で QID を検索するには、「**QID/**名前」フィールドに名前を入力します。

   「QID/名前」フィールドでは、特定の単語 (例: MySQL) で QID の完全なリストをフィルタリングできます。
7. 「検索」をクリックします。

   QID のリストが表示されます。
8. 不明な Universal LEEF DSM イベントに関連付ける QID を選択します。
9. 「**OK**」をクリックします。

   QRadar は、イベント・ペイロードに一致する 同じ QID を持つデバイスから転送されるすべての追加イベントをマップします。QRadar によってイベントが識別されるたびに、イベントの数が増加します。

   注**:** 新しい QRadar ID (QID) マップでイベントを更新する場合、QRadar に保管されている過去のイベントは更新されません。新しいイベントだけが新しい QID によって分類されます。

第 140 章 Vectra Networks Vectra

Vectra Networks Vectra 用の IBM Security QRadar DSM は、Vectra Networks Vectra X-Series プラットフォームからイベントを収集します。

以下の表は、Vectra Networks Vectra DSM の仕様を示しています。

表 *398. Vectra Networks Vectra DSM* の仕様

仕様	値
製造元	Vectra Networks
DSM 名	Vectra Networks Vectra
RPM ファイル名	`DSM-VectraNetworksVectra-`*`QRadar_version-build_number`*`.noarch.rpm`
サポートされるバージョン	V2.2
プロトコル	Syslog
イベント・フォーマット	共通イベント・フォーマット
記録されるイベント・タイプ	ホスト・スコアリング、コマンドと制御、ボットネット・アクティビティー、スキャン行為、側方移動、引き出し
自動的に検出?	はい
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Vectra Networks Web サイト (http://www.vectranetworks.com)

Vectra Networks Vectra を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、次の RPM の最新バージョンをリストされている順序でダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - Vectra Networks Vectra DSM RPM
2. Syslog イベントを QRadar に送信するように Vectra Networks Vectra デバイスを構成します。
3. QRadar がログ・ソースを自動的に検出しない場合、QRadar コンソールで Vectra Networks Vectra ログ・ソースを追加してください。以下の表は、Vectra Networks Vectra イベントの収集用に固有の値を必要とするパラメーターを示しています。

表 *399. Vectra Networks Vectra* ログ・ソース・パラメーター

パラメーター	値
ログ・ソース・タイプ	Vectra Networks Vectra
プロトコル構成	Syslog
ログ・ソース ID	ログ・ソースの固有 ID。

Vectra Networks Vectra DSM のサンプル・イベント・メッセージを次の表に示します。

表 *400. Vectra Networks Vectra* サンプル・メッセージ。

イベント名	下位カテゴリー	サンプル・ログ・メッセージ
ホスト・スコアリング	検出されたバックドア	<13>Dec 22 16:38:53 S111817149004 81 - -: CEF:0|Vectra Networks| Vectra|2.3|HSC|Host Score Change|3|externalId =283 cat=HOST SCORING shost=IP-20.20.1.2 src= 20.20.1.2 flexNumber1=26 flexNumber1Label=threat flexNumber2=60 flexNumber 2Label=certainty cs4=https: //10.0.4.49/hosts/283 cs4Label=URL start= 1450831133169 end= 1450831133169

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信のための Vectra Networks Vectra の構成

Vectra Networks Vectra イベントを収集するには、QRadar の Syslog デーモン・リスナーを構成します。

手順

1. Vectra の Web コンソールにログインします。
2. 「**settings**」 > 「**Notifications**」をクリックします。
3. 「**Syslog**」セクションで、「**Edit**」をクリックします。
4. 次の QRadar の Syslog デーモン・リスナー・パラメーターを構成します。

オプション	説明
宛先	QRadar イベント・コレクター (Event Collector) の IP アドレス。
ポート	514
プロトコル	UDP
フォーマット	CEF

第 141 章 Venustech Venusense

IBM Security QRadar 用の Venustech Venusense DSM は syslog を使用して Venusense アプライアンスからイベントを収集することができます。

QRadar は、syslog を使用してポート 514 で転送された、関連する統合脅威管理イベント、ファイアウォール・イベント、またはネットワーク侵入防止イベントをすべて記録します。

以下の Venustech アプライアンスが QRadar によってサポートされています。

- Venustech Venusense Security Platform
- Venusense Unified Threat Management (UTM)
- Venusense Firewall
- Venusense Network Intrusion Prevention System (NIPS)

Venusense の構成の概要

IBM Security QRadar は、フィルター操作したイベント・ログを syslog 形式で QRadar に転送するように構成された Venustech アプライアンスからイベントを収集することができます。

以下の手順では、Venusense Venustech アプライアンスからイベントを収集するために必要な手順の概要について説明します。

1. Venusense アプライアンスで syslog サーバーを構成します。
2. 特定のイベント・ログを転送するためのログ・フィルターを Venusense アプライアンスで構成します。
3. フィルター処理したログ・イベントに対応するログ・ソースを QRadar で構成します。

Venusense の syslog サーバーの構成

イベントを IBM Security QRadar に転送するには、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを指定して Venusense アプライアンスで syslog サーバーを構成して有効化する必要があります。

手順

1. Venusense アプライアンスの構成インターフェースにログインします。
2. ナビゲーション・メニューで、「ログ **(Logs)**」 > 「ログ構成 **(Log Configuration)**」 > ログ・サーバー **(Log Servers)**」を選択します。
3. 「**IP** アドレス **(IP Address)**」フィールドに QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。.
4. 「ポート **(Port)**」フィールドに 514 を入力します。
5. 「有効にする **(Enable)**」チェック・ボックスを選択します。
6. 「**OK**」をクリックします。

次のタスク

これで、QRadar に転送するイベントをフィルターに掛けるように Venusense アプライアンスを構成する準備ができました。

Venusense イベントのフィルタリングの構成

イベントのフィルタリングによって、Venusense アプライアンスが IBM Security QRadar に送信するイベントを決定します。

手順

1. ナビゲーション・メニューで、「ログ **(Logs)**」 > 「ログ構成 **(Log Configuration)**」 > 「ログ・フィルタリング **(Log Filtering)**」を選択します。
2. 「**Syslog** ログ **(Syslog Log)**」列で、QRadar に転送する各イベント・ログのチェック・ボックスを選択します。
3. リストから、有効化したイベント・ログの syslog ファシリティーを選択します。
4. 追加の syslog イベント・フィルターを構成する場合は、『Venusense イベントのフィルタリングの構成』の手順を繰り返します。
5. 「**OK**」をクリックします。

次のタスク

これで、QRadar で Venusense アプライアンスのログ・ソースを構成できるようになりました。QRadar は、Venusense アプライアンスからの syslog イベントに対して、ログ・ソースの検出や作成を自動的には行うことはありません。

Venusense のログ・ソースの構成

Venusense の syslog イベントを統合する際は、Venusense のイベントを自動的に検出しないため、IBM Security QRadar でログ・ソースを手動で作成しなければなりません。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで、「Venustech Venusense アプライアンス」を選択します。

   選択するログ・ソースのタイプは、Venusense アプライアンスで構成したイベント・フィルターによって決まります。オプションには、以下のタイプがあります。

- **Venustech Venusense Security Platform** - すべてのイベント・フィルター・オプションを有効にした場合は、このオプションを選択します。
- **Venustech Venusense UTM** - 統合フィルタリング・イベント (unified filtering events) を有効にした場合は、このオプションを選択します。
- **Venustech Venusense Firewall** - ファイアウォール・イベントのフィルタリングを有効にした場合は、このオプションを選択します。
- **Venustech Venusense NIPS** - ファイアウォール・イベントのフィルタリングを有効にした場合は、このオプションを選択します。

9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 「ログ・ソース **ID**」フィールドに、Venusense アプライアンスの ID としてログ・ソースの IP アドレスまたはホスト名を入力します。
11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

構成は完了です。Venusense アプライアンスにより QRadar に転送されたイベントは「ログ・アクティビティー」タブに表示されます。

第 142 章 Verdasys Digital Guardian

IBM Security QRadar 用の Verdasys Digital Guardian DSM は、Verdasys Digital Guardian アプライアンスからのアラート・イベントをすべて受け取って分類します。

Verdasys Digital Guardian は包括的なエンタープライズ情報保護 (EIP) プラットフォーム です。Digital Guardian は今日の高度なコラボレーションおよびモバイル・ビジネス環境に存在する情報リスクの課題を組織が解決できるようにすることで、ポリシー駆動のデータ中心型セキュリティーの基盤として機能します。Digital Guardian のエンドポイント・エージェント・アーキテクチャーにより、データ中心型セキュリティー・フレームワークを実装することができます。

Verdasys Digital Guardian により、ビジネス・マネージャーおよび IT マネージャーは以下のことが可能になります。

- 機密データを検出し、コンテキストおよび内容によって分類する。
- ユーザーやプロセスによるデータのアクセスおよび使用状況をモニターする。
- ポリシー駆動の情報保護を自動的に実装する。
- リスクの高い動作に対してアラート、ブロック、および記録を実行することで、コストが高くかかり、損害が大きいデータ損失の問題を未然に防止する。

Digital Guardian を QRadar と統合すると、エンドポイントからコンテキストが提供され、内部の脅威およびサイバー空間での脅威 (高度かつ継続的な脅威 (APT)) を検出して緩和する新しいレベルのセキュリティーを実現できます。

Digital Guardian により、エンドポイントからの豊富な情報を含むデータ・ストリームが QRadar に提供されます。例えば、データなどのコンテキスト変数へのアクセスに使用されるファイル名、ファイル分類、アプリケーションを含むユーザーまたはプロセスによるすべてのデータ・アクセスが可視化されます。

以下の表は、Verdasys Digital Guardian DSM の仕様を示しています。

仕様	値
製造元	Verdasys Digital Guardian
DSM 名	**Verdasys Digital Guardian**
RPM ファイル名	`DSM-VerdasysDigitalGuardian-`*`QRadar_version-Build_number`*`.noarch.rpm`
サポートされるバージョン	V6.1.x および V7.2.1.0248 (QRadar LEEF 形式の場合) V6.0x (Syslog イベント形式の場合)
プロトコル	Syslog、LEEF
イベント・フォーマット	Syslog
記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい

仕様	値
ID を含む?	いいえ
カスタム・プロパティーを含む?	いいえ
その他の情報	Digital Guardian Web サイト (https://digitalguardian.com)

IPtables の構成

Verdasys Digital Guardian でイベントの転送を構成する前に、Verdasys Digital Guardian からの ICMP 要求を許可するように IBM Security QRadar の IPtables を構成しておく必要があります。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。

   ログイン: `root`

   パスワード: *<password>*
2. 以下のコマンドを入力して、IPtables ファイルを編集します。

   ```
   vi /opt/qradar/conf/iptables.post
   ```

   IPtables 構成ファイルが表示されます。
3. 以下のコマンドを入力して、QRadar が Verdasys Digital Guardian からの ICMP 要求を受け入れることができるようにします。

   ```
   -I QChain 1 -m icmp -p icmp --src <IP address> -j ACCEPT
   ```

   ここで、*<IP address>* は、Verdasys Digital Guardian アプライアンスの IP アドレスです。例:

   ```
   -I QChain 1 -m icmp -p icmp --src 10.100.100.101 -j ACCEPT
   ```
4. IPtables の構成を保存します。
5. 以下のコマンドを入力して、QRadar の IPtables を更新します。

   ```
   ./opt/qradar/bin/iptables_update.pl
   ```
6. QRadar が Verdasys Digital Guardian からの ICMP トラフィックを受け入れることを検証するために、以下のコマンドを入力します。 `iptables --list --line-numbers`

   以下の出力が表示されます。

   ```
   [root@Qradar bin]# iptables --list --line-numbers
   Chain QChain (1 references)
   num  target  prot   opt   source           destination
   1    ACCEPT  icmp   --    10.100.100.101   anywhere    icmp any
   2    ACCEPT  tcp    --    anywhere         anywhere    state NEW tcp dpt:https
   3    ACCEPT  tcp    --    anywhere         anywhere    state NEW tcp dpt:http
   ```

これで、QRadar での IPtables の構成は完了です。

データ・エクスポートの構成

データ・エクスポートには、Verdasys Digital Guardian が IBM Security QRadar に転送するイベントを構成するためのオプションがあります。

手順

1. Digital Guardian 管理コンソールにログインします。
2. 「ワークスペース **(Workspace)**」 > 「データ・エクスポート **(Data Export)**」 > 「エクスポートの作成 **(Create Export)**」を選択します。
3. 「データ・ソース **(Data Sources)**」リストから、データ・ソースとして「アラート **(Alerts)**」または「イベント **(Events)**」を選択します。
4. 「エクスポート・タイプ **(Export type)**」リストで、「QRadar **LEEF**」を選択します。

   ご使用の Verdasys Digital Guardian が v6.0.x の場合は、「エクスポート・タイプ **(Export Type)**」として「**Syslog**」を選択できます。「QRadar LEEF」は、V6.1.1.1 以降のすべての Verdasys Digital Guardian アプライアンスに対して推奨されるエクスポート・タイプ・フォーマットです。
5. 「タイプ **(Type)**」リストから、トランスポート・プロトコルとして「**UDP**」または「**TCP**」を選択します。

   QRadar は、どちらのトランスポート・プロトコルからも syslog イベントを受け入れることができます。通常、アラート・イベントの長さが 1024 バイトを超える場合は、「**TCP**」を選択して、イベントが切り捨てられないようにすることができます。
6. 「サーバー **(Server)**」フィールドに、QRadar コンソールまたはイベント・コレクター (Event Collector)の IP アドレスを入力します。
7. 「ポート **(Port)**」フィールドに 514 を入力します。
8. 「重大度レベル **(Severity Level)**」リストで重大度レベルを選択します。
9. 「アクティブである **(Is Active)**」チェック・ボックスを選択します。
10. 「次へ」をクリックします。
11. 選択可能なフィールドのリストから、以下のアラート・フィールドおよびイベント・フィールドをデータ・エクスポートに追加します。
    - エージェント・ローカル時刻 **(Agent Local Time)**
    - アプリケーション
    - コンピューター名 **(Computer Name)**
    - 詳細ファイル・サイズ **(Detail File Size)**
    - **IP** アドレス
    - ローカル・ポート **(Local Port)**
    - 操作 **(Operation)** (必須)
    - ポリシー
    - リモート・ポート

- ルール
- 重大度
- 送信元 **IP** アドレス **(Source IP Address)**
- ユーザー名 **(User Name)**
- ブロック済み **(Was Blocked)**
- 分類済み **(Was Classified)**

12. データ・エクスポート内の各フィールドに対して基準を選択し、「次へ **(Next)**」をクリックします。

    デフォルトでは、基準はブランクになっています。
13. 基準に対してグループを選択し、「次へ **(Next)**」をクリックします。

    デフォルトでは、グループはブランクになっています。
14. 「テスト照会 **(Test Query)**」をクリックします。

    テスト照会により、データベースが正しく稼動していることを確認します。
15. 「次へ」をクリックします。
16. データ・エクスポートを保存します。

    構成は完了です。

次のタスク

Verdasys Digital Guardian からのデータ・エクスポートは 5 分間隔で実行されます。このタイミングは、必要に応じて Verdasys Digital Guardian の ジョブ・スケジューラーで調整できます。Verdasys Digital Guardian により QRadar にエクスポートされたイベントは「ログ・アクティビティー」タブに表示されます。

ログ・ソースの構成

IBM Security QRadar は、Verdasys Digital Guardian アプライアンスからのデータ・エクスポートに対して、ログ・ソースの検出と作成を自動的に実行します。

このタスクについて

以下の手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで、「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. 「ログ・ソースの説明」フィールドにログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「Verdasys Digital Guardian」を選択します。

9. 「プロトコル構成」リストで「**Syslog**」を選択します。
10. 以下の値を構成します。

表 *401. Syslog* パラメーター

パラメーター	説明
ログ・ソース **ID**	Verdasys Digital Guardian アプライアンスからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

ログ・ソースが QRadar に追加されます。

第 143 章 Vericept Content 360 DSM

IBM Security QRadar 用の Vericept Content 360 DSM は、syslog を使用して Vericept イベントを受け入れます。

このタスクについて

QRadar は、イベントからの入手可能な関連情報をすべて記録します。QRadar で Vericept デバイスを構成する前に、syslog を転送するようにデバイスを構成しておく必要があります。Vericept デバイスの構成について詳しくは、ベンダーの資料を参照してください。

QRadar にイベントを転送するように syslog を構成すると、構成は完了です。Vericept Content 360 イベントが自動的に検出されると、QRadar にログ・ソースが追加されます。Vericept Content 360 アプライアンスによって QRadar に転送されたイベントは「ログ・アクティビティー」タブに表示されます。

QRadar が Vericept デバイスからのイベントを受信するようにログ・ソースを手動で構成するには、以下を実行します。

手順

「ログ・ソース・タイプ」リストで「**Vericept Content 360**」オプションを選択します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

第 144 章 VMWare

IBM Security QRadar は、さまざまな VMWare 製品をサポートしています。

VMware ESX および ESXi

IBM Security QRadar 用の EMC VMware DSM は、VMware プロトコルまたは syslog を使用して ESX および ESXi サーバー・イベントを収集します。EMC VMware DSM がサポートするイベントは、VMware ESX または ESXi 3.x、4.x、または 5.x サーバーからのものです。

VMware ESX または ESXi イベントを収集するために、以下のいずれかのイベント収集方式を選択できます。

- 『VMWare ESX サーバーおよび ESXi サーバーでの syslog の構成』
- 1120 ページの『ESX または ESXi サーバーの VMWare プロトコルの構成』

VMWare ESX サーバーおよび ESXi サーバーでの syslog の構成

VMWare の syslog イベントを収集するには、syslog を使用して ESXi サーバーから IBM Security QRadar にイベントを転送するようにサーバーを構成する必要があります。

手順

1. VMWare vSphere Client にログインします。
2. VMWare インベントリーを管理するホストを選択します。
3. 「構成 **(Configuration)**」タブをクリックします。
4. 「ソフトウェア (Software)」ペインで「詳細設定 **(Advanced Settings)**」をクリックします。
5. ナビゲーション・メニューで「**Syslog**」をクリックします。
6. 以下のパラメーターの値を構成します。

表 *402. VMWare syslog* プロトコルのパラメーター

パラメーター	**ESX** バージョン	説明
`Syslog.Local.DatastorePath`	ESX、または ESXi 3.5.x または 4.x	ESXi サーバー上のローカル syslog メッセージのディレクトリー・パスを入力します。 デフォルト・ディレクトリーは、[] `/scratch/log/messages` です。
`Syslog.Remote.Hostname`	ESX、または ESXi 3.5.x または 4.x	QRadar の IP アドレスまたはホスト名を入力します。

表 402. *VMWare syslog* プロトコルのパラメーター (続き)

パラメーター	**ESX** バージョン	説明
Syslog.Remote.Port	ESX、または ESXi 3.5.x または 4.x	ESXi サーバーが syslog データの転送に使用するポート番号を入力します。 デフォルトはポート 514 です。
Syslog.global.logHost	ESXi v5.x	ESXi サーバーが syslog データの転送に使用する URL とポート番号を入力します。 例: udp://<*QRadar IP address*>:514 tcp://<*QRadar IP address*>:514

7. 「**OK**」をクリックして構成を保存します。

VMWare ESXi v5.x サーバーのデフォルトのファイアウォール構成では、発信接続がデフォルトで無効になっています。発信 syslog 接続が無効になっていると、内部の syslog フォワーダーによる、QRadar へのセキュリティー・イベントおよびアクセス・イベントの送信が制限されます。

デフォルトでは、VMWare 製品の syslog ファイアウォール構成は、発信 syslog 通信のみを許可します。セキュリティー上のリスクを防ぐため、受信 syslog 接続を有効にするように、デフォルトの syslog ファイアウォール・ルールを編集しないでください。

vSphere Clients での syslog ファイアウォール設定の有効化

ESXi v5.x サーバーからの syslog イベントを転送するには、セキュリティー・ポリシーを編集して、イベントの発信 syslog 接続を有効化する必要があります。

手順

1. vSphere Client から ESXi v5.x サーバーにログインします。
2. 「インベントリー **(Inventory)**」リストからご使用の ESXi サーバーを選択します。
3. 「管理 **(Manage)**」タブをクリックして、「セキュリティー・プロファイル **(Security Profile)**」を選択します。
4. 「ファイアウォール (Firewall)」セクションで「プロパティー **(Properties)**」をクリックします。
5. 「ファイアウォールのプロパティー (Firewall Properties)」ウィンドウで、「**syslog**」チェック・ボックスを選択します。
6. 「**OK**」をクリックします。

VMware ESX または ESXi の syslog ログ・ソースの構成

IBM Security QRadar は、VMWare からの syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。以下の構成手順はオプションです。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで「**EMC VMWare**」を選択します。
6. 「プロトコル構成」リストで「**Syslog**」を選択します。
7. 以下の値を構成します。

表 *403. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	EMC VMWare サーバーからのイベントの ID として、ログ・ソースの IP アドレスまたはホスト名を入力します。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。
信頼性	リストから、ログ・ソースの信頼性を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	リストから、ログの解析と保管を行うための受信ペイロード・エンコーダーを選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

ESX または ESXi サーバーの VMWare プロトコルの構成

VMWare ESXi サーバーからのイベントを読み取るように VMWare プロトコルを構成することができます。VMware プロトコルは、HTTPS を使用して ESX サーバーおよび ESXi サーバーをポーリングし、イベントを取得します。

このタスクについて

VMWare プロトコルを使用するようにログ・ソースを構成する前に、イベントをポーリングするための固有のユーザーを作成することを推奨します。このユーザーは root または管理グループのメンバーとして作成できますが、 ユーザーには読み取り専用権限の割り当て済みロールを指定する必要があります。これにより、IBM Security QRadar がイベントを最大限に収集でき、 同時に仮想サーバーのセキュリティー・レベルを維持することができます。ユーザー・ロールについて詳しくは、VMWare の資料を参照してください。

EMC VMWare を QRadar と統合するには、以下のタスクを実行する必要があります。

1. QRadar 用の ESX アカウントを作成する。
2. QRadar ユーザーのアカウント権限を構成する。
3. QRadar で VMWare プロトコルを構成する。

root または管理グループに属さないユーザーを作成すると、QRadar が一部のイベントを収集しなくなる可能性があります。管理特権を含む QRadar ユーザーを作成しますが、このカスタム・ユーザーに読み取り専用ロールを割り当てることをお勧めします。

ESX での QRadar 用アカウントの作成

EMC VMWare 用の IBM Security QRadar ユーザー・アカウントを作成することで、プロトコルによってイベントを正しくポーリングできるようになります。

手順

1. vSphere クライアントを使用して ESX ホストにログインします。
2. 「ローカル・ユーザーおよびグループ **(Local Users & Groups)**」タブをクリックします。
3. 「ユーザー **(Users)**」をクリックします。
4. 「追加 **(Add)**」を右クリックして選択します。
5. 以下のパラメーターを構成します。
   a. ログイン **(Login)** - 新規ユーザーのログイン名を入力します。
   b. **UID** - オプション。ユーザー ID を入力します。
   c. ユーザー名 **(User Name)** - アカウントのユーザー名を入力します。
   d. パスワード **(Password)** - アカウントのパスワードを入力します。
   e. パスワードの確認 **(Confirm Password)** - 確認のためパスワードを再度入力します。
   f. グループ **(Group)** - 「グループ **(Group)**」 リストから、「ルート **(root)**」を選択します。

6. 「追加」をクリックします。
7. 「**OK**」をクリックします。

読み取り専用アカウント権限の構成

セキュリティー上の理由により、IBM Security QRadar ユーザー・アカウントを root または管理グループのメンバーとして構成しますが、読み取り専用権限の割り当て済みロールを選択します。

このタスクについて

読み取り専用権限では、QRadar ユーザー・アカウントに対して VMWare プロトコルを使用したイベントの表示および収集が許可されます。

手順

1. 「権限 **(Permissions)**」タブをクリックします。
2. 「権限の追加 **(Add Permissions)**」を右クリックして選択します。
3. 「ユーザーおよびグループ (Users and Groups)」ウィンドウで「追加 **(Add)**」をクリックします。
4. QRadar ユーザーを選択して、「追加 **(Add)**」をクリックします。
5. 「**OK**」をクリックします。
6. 「割り当て済みロール **(Assigned Role)**」リストで「読み取り専用 **(Read-only)**」を選択します。
7. 「**OK**」をクリックします。

VMWare プロトコル用のログ・ソースの構成

EMC VMWare イベントをポーリングするために、VMWare プロトコルを使用してログ・ソースを構成できます。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで「**EMC VMWare**」を選択します。
6. 「プロトコル構成」リストで「**EMCVMWare**」を選択します。
7. 以下の値を構成します。

表 404. VMWare プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。この値は、「**ESX IP**」フィールドに構成された値と一致している必要があります。

表 *404. VMWare* プロトコルのパラメーター *(*続き*)*

パラメーター	説明
ESX IP	VMWare ESX サーバーまたは ESXi サーバーの IP アドレスを入力します。 例: 1.1.1.1。 VMware プロトコルは、イベント・データを要求する前に、HTTPS を VMware ESX サーバーまたは ESXi サーバーの IP アドレスの前に付加 します。
ユーザー名 **(User Name)**	VMWare サーバーへのアクセスに必要なユーザー名を入力します。
パスワード	VMWare サーバーへのアクセスに必要なパスワードを入力します。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

VMware vCenter

IBM Security QRadar 用の VMware vCenter DSM は、VMware プロトコルを使用して vCenter サーバー・イベントを収集します。

VMware プロトコルは、HTTPS を使用して vCenter アプライアンスをポーリングし、イベントを取得します。VMware vCenter イベントを収集するには、QRadar でログ・ソースを構成する必要があります。

VMWare プロトコルを使用するようにログ・ソースを構成する前に、イベントをポーリングするための固有のユーザーを作成することを推奨します。このユーザーは root または管理グループのメンバーとして作成できますが、ユーザーには読み取り専用権限の割り当て済みロールを指定する必要があります。これにより、QRadar がイベントを最大限に収集でき、同時に仮想サーバーのセキュリティー・レベルを維持することができます。ユーザー・ロールについて詳しくは、VMWare の資料を参照してください。

VMWare vCenter のログ・ソースの構成

VMWare プロトコルを使用して vCenter イベントを収集するには、IBM Security QRadar でログ・ソースを構成する必要があります。

手順

1. 「管理」タブをクリックします。
2. 「ログ・ソース」アイコンをクリックします。
3. 「追加」をクリックします。
4. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
5. 「ログ・ソース・タイプ」リストで「**VMWare vCenter**」を選択します。
6. 「プロトコル構成」リストで「**EMCVMWare**」を選択します。
7. 以下の値を構成します。

表 405. VMware プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	ログ・ソースの IP アドレスまたはホスト名を入力します。この値は、「**ESX IP**」フィールドに構成された値と一致している必要があります。
ESX IP	VMWare vCenter サーバーの IP アドレスを入力します。 例: 1.1.1.1。 VMware プロトコルは、イベント・データを要求する前に HTTPS を VMWare vCenter サーバーの IP アドレスの前に付加します。
ユーザー名 **(User Name)**	VMWare vCenter サーバーへのアクセスに必要なユーザー名を入力します。
パスワード	VMWare vCenter サーバーへのアクセスに必要なパスワードを入力します。

8. 「保存」をクリックします。
9. 「管理」タブで「変更のデプロイ」をクリックします。

IBM Security QRadar によって記録されるサポート対象の vCloud イベント・タイプ

QRadar 用の VMware vCloud DSM は、さまざまなカテゴリーのイベントを収集できます。

各イベント・カテゴリーには下位イベントが含まれ、そのイベント・カテゴリー内で実行されるアクションを記述しています。例えば、ユーザー・イベントが下位イベントとしてユーザー作成 やユーザー削除 を持つ場合があります。

QRadar によって vCloud Director から収集されるデフォルトのイベント・カテゴリーを以下のリストに示します。

- ユーザー・イベント
- グループ・イベント
- ユーザー・ロール・イベント
- セッション・イベント
- 組織イベント
- ネットワーク・イベント
- カタログ・イベント
- 仮想データ・センター (VDC) イベント
- 仮想アプリケーション (vApp) イベント
- 仮想マシン (VM) イベント
- メディア・イベント
- タスク操作イベント

VMware vCloud Director

IBM Security QRadar 用の VMware vCloud Director DSM および vCloud プロトコルを使用すると、vCloud REST API をポーリングしてイベントを取得することができます。

QRadar は、vCloud Directory 5.1 アプライアンスからの VMware vCloud Director イベントのポーリングをサポートしています。vCloud REST API を使用して収集されたイベントは、ログ・イベント拡張フォーマット (LEEF) イベントとして構成されます。

vCloud イベントを QRadar と統合するには、以下の作業を実行する必要があります。

1. vCloud アプライアンスで vCloud REST API の公開アドレスを構成します。
2. QRadar アプライアンスで、vCloud イベントをポーリングするためのログ・ソースを構成します。
3. ファイアウォール・ルールが、vCloud アプライアンスと QRadar コンソールまたは vCloud REST API をポーリングする役割を担う管理対象ホストの間の通信をブロックしていないことを確認します。

vCloud REST API の公開アドレスの構成

IBM Security QRadar は、vCloud アプライアンスの REST API をポーリングしてイベントを取得することによって vCloud API からセキュリティー・データを収集します。QRadar がデータを収集するためには、公開 REST API の基本 URL を構成する必要があります。

手順

1. vCloud アプライアンスに管理者としてログインします。
2. 「管理 **(Administration)**」タブをクリックします。
3. 「管理 **(Administration)**」メニューから、「システム設定 **(System Settings)**」 > 「公開アドレス **(Public Addresses)**」を選択します。
4. 「**VCD** 公開 **REST API** 基本 **URL (VCD public REST API base URL)**」フィールドに IP アドレスまたはホスト名を入力します。

   ここで指定するアドレスは、vCloud アプライアンスのファイアウォールまたは NAT の外側で公的に使用可能なアドレスになります。例: `https://1.1.1.1/`。
5. 「適用」をクリックします。

   公開 API URL は、vCloud アプライアンスで作成されます。

次のタスク

これで、QRadar でログ・ソースを構成できるようになりました。

IBM Security QRadar での vCloud ログ・ソースの構成

vCloud イベントを収集するには、QRadar で、vCloud API のポーリングに必要なロケーションと資格情報を指定して、ログ・ソースを構成する必要があります。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
7. オプション: 「ログ・ソースの説明」フィールドに、ログ・ソースの説明を入力します。
8. 「ログ・ソース・タイプ」リストで「**VMware vCloud Director**」を選択します。
9. 「プロトコル構成」リストで「**VMware vCloud Director**」を選択します。
10. 以下の値を構成します。

表 *406. VMware vCloud Director* ログ・ソースのパラメーター

パラメーター	説明
ログ・ソース **ID**	QRadar への vCloud アプライアンス・イベントを識別する IP アドレス、ホスト名、または名前を入力します。
vCloud URL	vCloud アプライアンス上に構成された、REST API にアクセスするための URL を入力します。 入力する URL は、vCloud サーバーの「**VCD 公開 REST API 基本 URL (VCD public REST API base URL)**」フィールドで構成したアドレスと一致している必要があります。 例: `https://10.10.10.1`。
ユーザー名	vCloud サーバーへのリモート・アクセスに必要なユーザー名を入力します。 例: `console/user@organization`。 QRadar で使用するように読み取り専用アカウントを構成する必要がある場合、「コンソール・アクセス専用 **(Console Access Only)**」権限を持つ VCloud ユーザーを組織内に作成できます。
パスワード	vCloud サーバーへのリモート・アクセスに必要なパスワードを入力します。
パスワードの確認	vCloud サーバーへのリモート・アクセスに必要なパスワードを確認します。
ポーリング間隔 **(Polling Interval)**	ポーリング間隔 (イベント・テーブルに対する照会から次の照会までの間の時間) を入力します。 デフォルトのポーリング間隔は 10 秒です。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。

表 406. VMware vCloud Director ログ・ソースのパラメーター (続き)

パラメーター	説明
信頼性	リストから、ログ・ソースの信頼性を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	リストから、ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」による「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	リストから、ログの解析と保管を行うための受信ペイロード・エンコーダーを選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。

11. 「保存」をクリックします。
12. 「管理」タブで「変更のデプロイ」をクリックします。

QRadar に転送された vCloud イベントは、QRadar の「ログ・アクティビティー」タブに表示されます。

VMware vShield

VMware vShield 用の IBM Security QRadar DSM は、VMware vShield サーバーからイベント・ログを収集できます。

VMware vShield Server DSM の仕様を以下の表に示します。

表 407. VMware vShield DSM の仕様

仕様	値
製造元	VMware
DSM	vShield
RPM ファイル名	DSM-VMwarevShield-*build_number*.noarch.rpm
サポートされるバージョン	

表 407. *VMware vShield DSM* の仕様 (続き)

仕様	値
プロトコル	Syslog
QRadar で記録されるイベント	すべてのイベント
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	http://www.vmware.com/

VMware vShield DSM 統合プロセス

VMware vShield DSM を IBM Security QRadar と統合することができます。

以下の手順を実行します。

1. 自動更新が有効になっていない場合は、最新バージョンの VMware vShield RPM をダウンロードして QRadar コンソールにインストールしてください。
2. VMware vShield のインスタンスごとに、QRadar と通信できるように VMware vShield システムを構成します。この手順は、VMware vShield のインスタンスごとに実行する必要があります。
3. QRadar がログ・ソースを自動的に検出しない場合は、統合する VMware vShield サーバーごとに QRadar コンソールでログ・ソースを作成します。

関連タスク

『IBM Security QRadar と通信するための VMWare vShield システムの構成』

1128 ページの『IBM Security QRadar での VMWare vShield のログ・ソースの構成』

IBM Security QRadar と通信するための VMWare vShield システムの構成

VMware vShield からすべての監査ログとシステム・イベントを収集するには、vShield Manager を構成する必要があります。VMware vShield を構成するときに syslog サーバーとして IBM Security QRadar を指定する必要があります。

手順

1. 「vShield Manager インベントリー (vShield Manager inventory)」ペインにアクセスします。
2. 「設定とレポート **(Settings & Reports)**」をクリックします。
3. 「構成 **(Configuration)**」 > 「一般 **(General)**」をクリックします。
4. 「**Syslog** サーバー **(Syslog Server)**」オプションの横にある「編集 **(Edit)**」をクリックします。
5. QRadar コンソールの IP アドレスを入力します。
6. オプション: QRadar コンソールのポートを入力します。ポートを指定しない場合は、QRadar コンソールの IP アドレス/ホスト名にデフォルトの UDP ポートが使用されます。
7. 「**OK**」をクリックします。

IBM Security QRadar での VMWare vShield のログ・ソースの構成

VMware vShield のイベントを収集するには、QRadar でログ・ソースを構成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**VMware vShield**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。
8. 残りのパラメーターを構成します。
9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

第 145 章 Vormetric Data Security

IBM Security QRadar 用の Vormetric Data Security DSM は、Vormetric Data Security サーバーからイベント・ログを収集することができます。

Vormetric Data Security DSM の仕様を以下の表に示します。

Vormetric Data Security DSM の仕様

仕様	値
製造元	Vormetric, Inc.
DSM	Vormetric Data Security
RPM ファイル名	DSM-VormetricDataSecurity-7.1-804377.noarch.rpm DSM-VormetricDataSecurity-7.2-804381.noarch.rpm
サポートされるバージョン	Vormetric Data Security Manager v5.1.3 以降 Vormetric Data Firewall FS Agent v5.2 以降
プロトコル	Syslog (LEEF)
QRadar で記録されるイベント	監査、アラーム、警告、学習モード、システム
自動的に検出	はい
ID を含む?	いいえ
その他の情報	Vormetric の Web サイト (http://www.vormetric.com)

Vormetric Data Security DSM 統合プロセス

Vormetric Data Security DSM を IBM Security QRadar と統合することができます。

以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
2.
   - Syslog プロトコル RPM
   - DSMCommon RPM

   使用できる DSMCommon RPM の最低バージョンは `DSM-DSMCommon-7.1-530016.noarch.rpm` または `DSM-DSMCommon-7.2-572972.noarch.rpm` です。
   - Vormetric Data Security RPM
3. Vormetric Data Security のインスタンスごとに、QRadar と通信できるように Vormetric Data Security システムを構成します。
4. QRadar が DSM を自動的に検出しない場合は、統合する Vormetric Data Security サーバーごとに QRadar コンソールでログ・ソースを作成します。

関連タスク

『IBM Security QRadar と通信するための Vormetric Data Security システムの構成』

1132 ページの『IBM Security QRadar での Vormetric Data Security のログ・ソースの構成』

IBM Security QRadar と通信するための Vormetric Data Security システムの構成

Vormetric Data Security から監査ログとシステム・イベントをすべて収集するには、QRadar と通信できるように Vormetric Data Security Manager を構成する必要があります。

このタスクについて

使用する Vormetric Data Security Manager ユーザー・アカウントにはシステム管理者権限が必要です。

手順

1. システム管理者権限が割り当てられた管理者として Vormetric Data Security Manager にログインします。
2. ナビゲーション・メニューで、「ログ **(Log)**」 > 「**Syslog**」をクリックします。
3. 「追加」をクリックします。
4. 「サーバー名 **(Server Name)**」フィールドに、QRadar システムの IP アドレスまたはホスト名を入力します。
5. 「トランスポート・プロトコル **(Transport Protocol)**」リストで「**TCP**」または QRadar システムでのログ・ソース・プロトコル構成と一致する値を選択します。
6. 「ポート番号 **(Port Number)**」フィールドに、514 または QRadar システムでのログ・ソース・プロトコル構成と一致する値を入力します。
7. 「メッセージ・フォーマット **(Message Format)**」リストで「**LEEF**」を選択します。
8. 「**OK**」をクリックします。
9. 「Syslog サーバー・サマリー (Syslog Server summary)」画面で、QRadar システムに関する入力の詳細を確認します。「**Syslog** へのロギング **(Logging to SysLog)**」値が「オフ **(OFF)**」の場合は、以下の手順を実行します。ナビゲーション・メニューで、「システム **(System)**」 > 「一般設定 **(General Preferences)**」をクリックします。
10. 「システム **(System)**」タブをクリックします。
11. 「**Syslog** 設定 **(Syslog Settings)**」ペインで「**Syslog** の有効化 **(Syslog Enabled)**」チェック・ボックスを選択します。

次のタスク

『Vormetric Data Security Manager をバイパスするための Vormetric Data Firewall FS Agents の構成』

Vormetric Data Security Manager をバイパスするための Vormetric Data Firewall FS Agents の構成

Vormetric Data Security Manager で IBM Security QRadar との通信が有効化されていると、Vormetric Data Firewall FS エージェントからのすべてのイベントが、Vormetric Data Security Manager を介して QRadar システムに転送されます。

このタスクについて

Vormetric Data Security Manager をバイパスするために、LEEF イベントを直接 QRadar システムに送信するように Vormetric Data Firewall FS Agents を構成できます。

使用する Vormetric Data Security Manager ユーザー・アカウントにはシステム管理者権限が必要です。

手順

1. Vormetric Data Security Manager にログインします。
2. ナビゲーション・メニューで、「システム **(System)**」 > 「ログ設定 **(Log Preferences)**」をクリックします。
3. 「**FS Agent** ログ **(FS Agent Log)**」タブをクリックします。
4. 「ポリシー評価 **(Policy Evaluation)**」行で、以下のパラメーターを構成します。
   a. **Syslog/**イベント・ログに記録 **(Log to Syslog/Event Log)**」チェック・ボックスを選択します。
5. 「サーバーにアップロード **(Upload to Server)**」チェック・ボックスをクリアします。
6. 「レベル **(Level)**」リストで、「情報 **(INFO)**」を選択します。

   このセットアップによって、ポリシー評価モジュールからの監査証跡全体を Security Manager ではなく syslog サーバーに直接送信できるようになります。両方の宛先を有効のままにすると、QRadar システムに送信されるイベントの重複が発生することがあります。
7. 「Syslog 設定 (Syslog Settings)」セクションの下で、以下のパラメーターを構成します。「サーバー **(Server)**」フィールドで、以下の構文を使用して QRadar システムの IP アドレスまたはホスト名、およびポート番号を入力します。

   qradar_IP address_or_host:*port*
8. 「プロトコル **(Protocol)**」リストで「**TCP**」または QRadar システムでのログ・ソース構成と一致する値を選択します。

9. 「メッセージ・フォーマット **(Message Format)**」リストで「**LEEF**」を選択します。

次のタスク

この構成は Vormetric Data Security Manager に後から追加されるすべてのホストおよびホスト・グループに適用されます。既存の各ホストまたはホスト・グループについては、「ホスト **(Hosts)**」リストから必要なホストまたはホスト・グループを選択し、この手順を繰り返します。

IBM Security QRadar での Vormetric Data Security のログ・ソースの構成

Vormetric Data Security イベントを収集するには、IBM Security QRadar でログ・ソースを構成します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース・タイプ」リストで「**Vormetric Data Security**」を選択します。
7. 「プロトコル構成」リストで「**Syslog**」を選択します。
8. 残りのパラメーターを構成します。
9. 「保存」をクリックします。
10. 「管理」タブで「変更のデプロイ」をクリックします。

第 146 章 WatchGuard Fireware OS

WatchGuard Fireware OS 用の IBM Security QRadar DSM は、WatchGuard Fireware OS からイベント・ログを収集することができます。

以下の表は、WatchGuard Fireware OS DSM の仕様を示しています。

表 *408. WatchGuard Fireware DSM* の仕様

仕様	値
製造元	WatchGuard
DSM 名	WatchGuard Fireware OS
RPM ファイル名	DSM-WatchGuardFirewareOS->*QRadar-version-Build_number*.noarch.rpm
サポートされるバージョン	Fireware XTM OS v11.9 以降
イベント・フォーマット	syslog
QRadar で記録されるイベント・タイプ	すべてのイベント
自動的に検出?	はい
ID を含む?	いいえ
その他の情報	WatchGuard Web サイト (http://www.watchguard.com/)

WatchGuard Fireware OS を QRadar に統合するには、以下の手順を実行します。

1. 自動更新が有効になっていない場合は、以下に示す RPM の最新バージョンをダウンロードして QRadar コンソールにインストールしてください。
   - DSMCommon RPM
   - WatchGuard Fireware OS RPM
2. WatchGuard Fireware OS のインスタンスごとに、QRadar と通信するように WatchGuard Fireware OS アプライアンスを構成します。以下のいずれかの方法で構成することができます。
   - 1134 ページの『QRadar との通信用にポリシー・マネージャーで WatchGuard Fireware OS アプライアンスを構成する』
   - 1135 ページの『QRadar との通信用に Fireware XTM の WatchGuard Fireware OS アプライアンスを構成する』
3. QRadar が WatchGuard Fireware OS ログ・ソースを自動的に検出しない場合は、ネットワーク上の WatchGuard Fireware OS のインスタンスごとにログ・ソースを作成します。

関連タスク:

4 ページの『DSM の追加』
システムがインターネットから切断されている場合、DSM RPM を手動でインストールしなければならないことがあります。

5 ページの『ログ・ソースの追加』
ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

QRadar との通信用にポリシー・マネージャーで WatchGuard Fireware OS アプライアンスを構成する

WatchGuard Fireware OS イベントを収集するには、ポリシー・マネージャーを使用して、イベントを QRadar に送信するようにサード・パーティー・アプライアンスを構成します。

始める前に

デバイス管理者権限の資格情報が必要です。

手順

1. WatchGuard System Manager を開きます。
2. Firebox デバイスまたは XTM デバイスに接続します。
3. デバイスに対してポリシー・マネージャーを開始します。
4. 「ロギングのセットアップ (Logging Setup)」ウィンドウで、「セットアップ **(Setup)**」>「ロギング **(Logging)**」を選択します。
5. 「この **syslog** サーバーにログ・メッセージを送信 **(Send log messages to this syslog server)**」チェック・ボックスを選択します。
6. 「**IP** アドレス **(IP address)**」テキスト・ボックスに、QRadar コンソールまたはイベント・コレクターの IP アドレスを入力します。
7. 「ポート **(Port)**」テキスト・ボックスに 514 と入力します。
8. 「ログ形式 **(Log Format)**」リストで「IBM **LEEF**」を選択します。
9. オプション: ログ・メッセージに含める詳細を指定します。
   a. 「構成 **(Configure)**」をクリックします。
   b. XTM デバイスのシリアル番号をログ・メッセージの詳細に含めるには、「デバイスのシリアル番号 **(The serial number of the device)**」チェック・ボックスを選択します。
   c. syslog ヘッダーをログ・メッセージの詳細に含めるには、「**syslog** ヘッダー **(The syslog header)**」チェック・ボックスを選択します。
   d. ログ・メッセージのタイプごとに、以下に示すいずれかの syslog 機能を選択します。
      - アラームなど、優先順位の高い syslog メッセージの場合は、「**Local0**」を選択します。
      - 他のタイプのログ・メッセージに優先順位を割り当てるには、「**Local1**」から「**Local7**」までのいずれかのオプションを選択します。数字が小さくなるほど、優先順位が高くなります。
      - ログ・メッセージ・タイプの詳細を送信しない場合は、「なし **(NONE)**」を選択します。
   e. 「**OK**」をクリックします。
10. 「**OK**」をクリックします。

11. 構成ファイルをデバイスに保存します。

QRadar との通信用に Fireware XTM の WatchGuard Fireware OS アプライアンスを構成する

WatchGuard Fireware OS イベントを収集するには、Fireware XTM Web ユーザー・インターフェースを使用して、QRadar にイベントを送信するようにサード・パーティー・アプライアンスを構成します。

始める前に

デバイス管理者権限の資格情報が必要です。

手順

1. Fireware デバイスまたは XTM デバイスの Fireware XTM Web ユーザー・インターフェースにログインします。
2. 「システム **(System)**」>「ロギング **(Logging)]**を選択します。
3. 「Syslog サーバー (Syslog Server)」ペインで、「この **IP** アドレスの **Syslog** サーバーにログ・メッセージを送信 **(Send log messages to the syslog server at this IP address)**」チェック・ボックスを選択します。
4. 「**IP** アドレス **(IP Address)**」テキスト・ボックスに、QRadar コンソールまたはイベント・コレクターの IP アドレスを入力します。
5. 「ポート **(Port)**」テキスト・ボックスに 514 と入力します。
6. 「ログ形式 **(Log Format)**」リストで「IBM**LEEF**」を選択します。
7. オプション: ログ・メッセージに含める詳細を指定します。
   a. XTM デバイスのシリアル番号をログ・メッセージの詳細に含めるには、「デバイスのシリアル番号 **(The serial number of the device)**」チェック・ボックスを選択します。
   b. syslog ヘッダーをログ・メッセージの詳細に含めるには、「**syslog** ヘッダー **(The syslog header)**」チェック・ボックスを選択します。
   c. ログ・メッセージのタイプごとに、以下に示すいずれかの syslog 機能を選択します。
      - アラームなど、優先順位の高い syslog メッセージの場合は、「**Local0**」を選択します。
      - 他のタイプのログ・メッセージに優先順位を割り当てるには、「**Local1**」から「**Local7**」までのいずれかのオプションを選択します。数字が小さくなるほど、優先順位が高くなります。
      - ログ・メッセージ・タイプの詳細を送信しない場合は、「なし **(NONE)**」を選択します。
8. 「保存」をクリックします。

QRadar で WatchGuard Fireware OS のログ・ソースを構成する

QRadar コンソールが WatchGuard Fireware OS のログ・ソースを自動的に検出しなかった場合は、以下の手順を実行します。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. ナビゲーション・メニューで「データ・ソース」をクリックします。
4. 「ログ・ソース」アイコンをクリックします。
5. 「追加」をクリックします。
6. 「ログ・ソース **ID**」フィールドに、WatchGuard Fireware OS デバイスの IP アドレスまたはホスト名を入力します。
7. 「ログ・ソース・タイプ」リストで「**WatchGuard Fireware OS**」を選択します。
8. 「プロトコル構成」リストで「**Syslog**」を選択します。
9. 残りのパラメーターを構成します。
10. 「保存」をクリックします。

第 147 章 Websense

Websense は、今は Forcepoint と呼ばれています。

関連概念:

395 ページの『第 52 章 Forcepoint』

IBM Security QRadar は Forcepoint DSM を幅広くサポートしています。

第 148 章 Zscaler Nanolog Streaming Service

IBM Security QRadar は、syslog イベントを QRadar に転送する Zscaler Nanolog Streaming Service (NSS) ログ・フィードからイベントを収集して分類することができます。

syslog イベントを収集するには、TCP syslog イベントを QRadar に転送するように NSS フィードを使用して Zscaler NSS を構成する必要があります。QRadar は、Zscaler NSS ログ・フィードから転送された syslog イベントに対して、ログ・ソースの検出と作成を自動的に実行します。QRadar は、Zscaler NSS V4.1 からの syslog イベントをサポートしています。

Zscaler NSS を構成するには、以下の作業を行います。

1. Zscaler NSS アプライアンスで QRadar 用のログ・フィードを作成します。
2. QRadar システムで、転送されたイベントが自動的に検出されることを確認します。

Zscaler NSS の場合にサポートされるイベント・タイプ

QRadar 用の ZScaler NSS DSM は、Zscaler NSS インストール済み環境から Web ブラウズ・イベントに関する情報を収集します。

各 Zscaler NSS イベントのイベント・カテゴリー には、Web ブラウズで実行されたアクションに関する情報が入っています。例えば、Web ブラウズ・イベントが、Web サイト・トラフィックの許可や、Web サイト・トラフィックのブロックのカテゴリーに分類される場合があります。各イベントは許可またはブロックされた Web サイトを定義しており、イベント・ペイロード にはイベントの詳細情報がすべて入っています。

Zscaler NSS での syslog フィードの構成

イベントを収集するには、syslog イベントを IBM Security QRadar に転送するように、Zscaler NSS でログ・フィードを構成する必要があります。

手順

1. Zscaler NSS の管理ポータルにログインします。
2. ナビゲーション・メニューで、「ポリシー **(Policy)**」 > 「管理 **(Administration)**」 > 「**Nanolog Streaming Service** の構成 **(Configure Nanolog Streaming Service)**」を選択します。
3. 「フィードの追加 **(Add Feed)**」をクリックします。
4. 「フィード名 **(Feed Name)**」フィールドに NSS フィードの名前を入力します。
5. 「**NSS** 名 **(NSS Name)**」リストで「**ZScaler NSS**」システムを選択します。
6. 「ステータス **(Status)**」リストで「有効 **(Enabled)**」を選択します。
7. 「**SIEM IP**」フィールドに QRadar システムの IP アドレスを入力します。

8. 「**TCP ポート (TCP Port)**」フィールドに 514 と入力します。
9. 「ログ・タイプ **(Log Type)**」リストで「**Web ログ (Web Log)**」を選択します。
10. 「フィード出力タイプ **(Feed Output Type)**」リストで「カスタム **(Custom)**」を選択します。
11. 「フィード出力形式 **(Feed Output Format)**」フィールドに以下のカスタム形式を入力します。

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss}
zscaler-nss: LEEF:1.0|Zscaler|NSS|4.1|%s{reason}|
cat=%s{action}
¥tdevTime= %s{mon} %02d{dd} %d{yy}
%02d{hh}:%02d{mm}:%02d{ss}%s{tz}
¥tdevTimeFormat=MMM dd yyyy HH:mm:ss z¥tsrc=%s{cip}¥tdst=%s{sip}
¥tsrcPostNAT=%s{cintip}¥trealm=%s{location}¥tusrName=%s{login}
¥tsrcBytes=%d{reqsize}¥tdstBytes=%d{respsize}¥trole=%s{dept}
¥tpolicy=%s{reason}¥turl=%s{url}¥trecordid=%d{recordid}
¥tbwthrottle=%s{bwthrottle}¥tuseragent=%s{ua}¥treferer=%s{referer}
¥thostname=%s{host}¥tappproto=%s{proto}¥turlcategory=%s{urlcat}
¥turlsupercategory=%s{urlsupercat}¥turlclass=%s{urlclass}
¥tappclass=%s{appclass}¥tappname=%s{appname}
¥tmalwaretype=%s{malwarecat}¥tmalwareclass=%s{malwareclass}
¥tthreatname=%s{threatname}¥triskscore=%d{riskscore}
¥tdlpdict=%s{dlpdict}¥tdlpeng=%s{dlpeng}¥tfileclass=%s{fileclass}
¥tfiletype=%s{filetype}¥treqmethod=%s{reqmethod}
¥trespcode=%s{respcode}¥n
```

12. 「完了 **(Done)**」をクリックします。

QRadar は、Zscaler NSS アプライアンスのログ・ソースの検出と作成を自動的に実行します。QRadar に転送されたイベントは、「ログ・アクティビティー」タブで表示できます。

Zscaler NSS ログ・ソースの構成

IBM Security QRadar は、Zscaler NSS から転送される syslog イベントに対して、ログ・ソースの検出および作成を自動的に実行します。

このタスクについて

以下の構成手順はオプションです。

手順

1. QRadar にログインします。
2. 「管理」タブをクリックします。
3. 「ログ・ソース」アイコンをクリックします。
4. 「追加」をクリックします。
5. 「ログ・ソース名」フィールドにログ・ソースの名前を入力します。
6. オプション: 「ログ・ソースの説明」フィールドに、ログ・ソースの説明を入力します。
7. 「ログ・ソース・タイプ」リストで「**Zscaler NSS**」を選択します。
8. 「プロトコル構成」リストで「**Syslog**」を選択します。
9. 以下の値を構成します。

表 *409. syslog* プロトコルのパラメーター

パラメーター	説明
ログ・ソース **ID**	Zscaler NSS インストールからのイベントの ID として IP アドレスを入力します。 ログ・ソース ID は、固有値でなければなりません。
有効	ログ・ソースを有効にするには、このチェック・ボックスを選択します。 このチェック・ボックスはデフォルトで選択されます。
信頼性	ログ・ソースの「信頼性」を選択します。範囲は 0 から 10 です。 送信元デバイスからの信頼性の評価によって判断される、イベントまたはオフェンスの完全性。複数の送信元が同じイベントを報告する場合、信頼性は高くなります。デフォルトは 5 です。
ターゲット・イベント・コレクター	ログ・ソースのターゲットとして使用する「ターゲット・イベント・コレクター」を選択します。
イベントの統合	ログ・ソースがイベントを統合 (バンドル) できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベントの統合」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
受信イベント・ペイロード **(Incoming Event Payload)**	リストから、ログの解析と保管を行うための「受信ペイロード・エンコーダー」を選択します。
イベント・ペイロードの保管	ログ・ソースがイベント・ペイロード情報を保管できるようにするには、このチェック・ボックスを選択します。 デフォルトでは、自動的に検出されたログ・ソースは、QRadar の「システム設定」の「イベント・ペイロードの保管」リストの値を継承します。ログ・ソースを作成するか、既存の構成を編集する際に、各ログ・ソースに対してこのオプションを構成することで、デフォルト値をオーバーライドできます。
ログ・ソース言語	zScaler NSS で生成されるイベントの言語を選択します。

10. 「保存」をクリックします。
11. 「管理」タブで「変更のデプロイ」をクリックします。

第 149 章 QRadar でサポートされる DSM

IBM Security QRadar は、デバイス・サポート・モジュール (DSM) と呼ばれるプラグイン・ファイルを使用することにより、セキュリティー製品からのイベントの収集を行うことができます。

サード・パーティー用および IBM Security QRadar ソリューション用にサポートされている DSM を以下の表に示します。

表 *410. QRadar* でサポートされる *DSM*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
3Com	8800 Series Switch V3.01.30	Syslog	状況イベントおよびネットワーク状況イベント	はい	いいえ	いいえ
AhnLab	AhnLab Policy Center	AhnLabPolicy CenterJdbc	スパイウェア検出 ウィルス検出 監査	いいえ	はい	いいえ
Akamai	Akamai KONA	HTTP レシーバー	警告ルール・イベント 拒否ルール・イベント	いいえ	いいえ	いいえ
Amazon	Amazon AWS CloudTrail	Amazon AWS S3 REST API	すべてのバージョン (1.0、1.02、1.03、1.04) のイベント。	いいえ	いいえ	いいえ
Ambiron	TrustWave ipAngel V4.0	Syslog	Snort ベースのイベント	いいえ	いいえ	いいえ
Apache	HTTP Server V1.3 以降	Syslog	HTTP 状況	はい	いいえ	いいえ
APC	UPS	Syslog	Smart-UPS シリーズ・イベント	いいえ	いいえ	いいえ
Apple	Mac OS X (10)	Syslog	ファイアウォール・イベント、Web サーバー (アクセス/エラー) イベント、特権イベント、および情報イベント	いいえ	はい	いいえ
Application Security, Inc.	DbProtect V6.2、V6.3、V6.3sp1、V6.3.1、および v6.4	Syslog	すべてのイベント	はい	いいえ	いいえ
Arbor Networks	Pravail APS V3.1 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Arpeggio Software	SIFT-IT V3.1 以降	Syslog	SIFT-IT ルール・セットで構成されたすべてのイベント	はい	いいえ	いいえ
Array Networks	SSL VPN ArraySP V7.3	Syslog	すべてのイベント	いいえ	はい	はい
Aruba Networks	ClearPass Policy Manager V6.5.0.71095 以降	Syslog	LEEF	はい	はい	いいえ
Aruba Networks	Mobility Controllers V2.5 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Avaya Inc.	Avaya VPN Gateway V9.0.7.2	Syslog	すべてのイベント	はい	はい	いいえ
BalaBit IT Security	MicrosoftWindows Security Event Log V4.x	Syslog	Microsoft イベント・ログのイベント	はい	はい	いいえ
BalaBit IT Security	Microsoft ISA V4.x	Syslog	Microsoft イベント・ログのイベント	はい	はい	いいえ
Barracuda Networks	Spam & Virus Firewall V5.x 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Barracuda Networks	Web Application Firewall V7.0.x	Syslog	システム・イベント、Web ファイアウォール・イベント、アクセス・イベント、および監査イベント	はい	いいえ	いいえ
Barracuda Networks	Web Filter V6.0.x 以降	Syslog	Web トラフィック・イベントおよび Web インターフェース・イベント	はい	いいえ	いいえ
Bit9	Carbon Black V5.1 以降	Syslog	監視リスト・ヒット	はい	いいえ	いいえ
Bit9	Bit9 Parity	Syslog	LEEF	はい		いいえ
Bit9	Security Platform V6.0.2 以降	Syslog	すべてのイベント	はい	はい	いいえ
BlueCat Networks	Adonis V6.7.1-P2 以降	Syslog	DNS イベントおよび DHCP イベント	はい	いいえ	いいえ
Blue Coat	SG V4.x 以降	Syslog ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	はい
Blue Coat	Web Security Service		Blue Coat ELFF、アクセス・イベント	いいえ	いいえ	いいえ
Box	Box	Box REST API	JSON 管理者イベントとエンタープライズ・イベント	いいえ	はい	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
Bridgewater Systems	AAA V8.2c1	Syslog	すべてのイベント	はい	はい	いいえ
Brocade	Fabric OS V7.x	Syslog	システム・イベントおよび監査イベント	はい	いいえ	いいえ
CA	Access Control Facility V12 から V15	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	はい
CA	SiteMinder	Syslog	すべてのイベント	いいえ	いいえ	いいえ
CA	Top Secret V12 から V15	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	はい
Check Point	Check Point バージョン NG、FP1、FP2、FP3、AI R54、AI R55、R65、R70、R75、R77、R80、および NGX	Syslog または OPSEC LEA	すべてのイベント	はい	はい	はい
Check Point	VPN-1 バージョン NG、FP1、FP2、FP3、AI R54、AI R55、R65、R70、R77、および NGX	Syslog または OPSEC LEA	すべてのイベント	はい	はい	いいえ
Check Point	Check Point Multi-Domain Management (Provider-1) バージョン NG、FP1、FP2、FP3、AI R54、AI R55、R65、R70、R77、および NGX	Syslog または OPSEC LEA	すべてのイベント	はい	はい	いいえ
Cilasoft	Cilasoft QJRN/400 V5.14.K+	Syslog	IBM 監査イベント	はい	はい	いいえ
Cisco	4400 Series Wireless LAN Controller V7.2	Syslog または SNMPv2	すべてのイベント	いいえ	いいえ	いいえ
Cisco	CallManager V8.x	Syslog	アプリケーション・イベント	はい	いいえ	いいえ
Cisco	ACS V4.1 以降 (ACS V3.x 以降から直接アップグレードされ、ALE を使用している場合)	Syslog	失敗したアクセス試行	はい	はい	いいえ
Cisco	Aironet V4.x 以降	Syslog	Cisco Emblem 形式	はい	いいえ	いいえ
Cisco	ACE Firewall V12.2	Syslog	すべてのイベント	はい	はい	いいえ
Cisco	ASA V7.x 以降	Syslog	すべてのイベント	はい	はい	いいえ
Cisco	ASA V7.x 以降	NSEL プロトコル	すべてのイベント	いいえ	いいえ	いいえ
Cisco	CSA V4.x、V5.x、および V6.x	Syslog SNMPv1 SNMPv2	すべてのイベント	はい	はい	いいえ
Cisco	CatOS for catalyst systems V7.3 以降	Syslog	すべてのイベント	はい	はい	いいえ
Cisco	IPS V7.1.10 以降、V7.2.x、V7.3.x	SDEE	すべてのイベント	いいえ	いいえ	いいえ
Cisco	IronPort V5.5、V6.5、V7.1、および V7.5	Syslog、ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	いいえ
Cisco	FireSIGHT Management Center V4.8.0.2 から V6.0.0 (旧称 Sourcefire Defense Center)	FireSIGHT Management Center	侵入イベントおよび追加データ 相関イベント メタデータ・イベント ディスカバリー・イベント ホスト・イベント ユーザー・イベント マルウェア・イベント ファイル・イベント	いいえ	いいえ	いいえ
Cisco	Firewall Service Module (FWSM) v2.1+	Syslog	すべてのイベント	はい	はい	はい
Cisco	Catalyst Switch IOS, 12.2, 12.5+	Syslog	すべてのイベント	はい	はい	いいえ
Cisco	NAC Appliance v4.x +	Syslog	監査イベント、エラー・イベント、失敗イベント、検疫イベント、および感染イベント	いいえ	いいえ	いいえ
Cisco	Nexus v6.x	Syslog	Nexus-OS イベント	はい	いいえ	いいえ
Cisco	PIX Firewall v5.x、v6.3+	Syslog	Cisco PIX イベント	はい	はい	はい
Cisco	IOS 12.2、12.5+	Syslog	すべてのイベント	はい	はい	いいえ
Cisco	VPN 3000 Concentrator バージョン VPN 3005、4.1.7.H	Syslog	すべてのイベント	はい	はい	はい
Cisco	Wireless Services Modules (WiSM) V 5.1 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Cisco	Identity Services Engine V1.1	UDP Multiline Syslog Protocol	デバイス・イベント	いいえ	はい	いいえ
Citrix	NetScaler V9.3 から V10.0	Syslog	すべてのイベント	はい	はい	いいえ
Citrix	Access Gateway V4.5	Syslog	アクセス・イベント、監査イベント、および診断イベント	はい	いいえ	いいえ
Cloudera	Cloudera Navigator	Syslog	HDFS, HBase, Hive, Hue, Cloudera Impala, Sentry に対する監査イベント	はい	いいえ	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
CloudPassage	CloudPassage Halo	Syslog、ログ・ファイル	すべてのイベント	はい	いいえ	いいえ
CrowdStrike	Falcon Host V1.0	Syslog LEEF	Falcon Host 検出サマリー Falcon Host 認証ログ Falcon Host 検出状況更新ログ カスタマー IOC 検出イベント ハッシュ拡散イベント	はい	いいえ	いいえ
CorreLog	CorreLog Agent for IBM z/OS	Syslog LEEF	すべてのイベント	はい	いいえ	いいえ
CRYPTOCard	CRYPTO- Shield V6.3	Syslog	すべてのイベント	いいえ	いいえ	いいえ
CyberArk	CyberArk Privileged Threat Analytics V3.1	Syslog	検出されたセキュリティー・イベント	はい	いいえ	いいえ
CyberArk	CyberArk Vault V6.x	Syslog	すべてのイベント	はい	はい	いいえ
CyberGuard	Firewall/VPN KS1000 V5.1	Syslog	CyberGuard イベント	はい	いいえ	いいえ
Damballa	Failsafe V5.0.2 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Digital China Networks	DCS および DCRS シリーズ・スイッチ V1.8.7	Syslog	DCS および DCRS の IPv4 イベント	いいえ	いいえ	いいえ
DG Technology	DG Technology MEAS	Syslog LEEF	メインフレーム・イベント	はい	いいえ	いいえ
Extreme	Dragon V5.0、V6.x、V7.1、V7.2、V7.3、および V7.4	Syslog SNMPv1 SNMPv3	すべての関連する Extreme Dragon イベント	はい	いいえ	いいえ
Extreme	800-Series Switch	Syslog	すべてのイベント	はい	いいえ	いいえ
Extreme	Matrix Router V3.5	Syslog SNMPv1 SNMPv2 SNMPv3	SNMP および syslog のログイン・イベント、ログアウト・イベント、およびログイン失敗イベント	はい	いいえ	いいえ
Extreme	NetSight Automatic Security Manager V3.1.2	Syslog	すべてのイベント	はい	いいえ	いいえ
Extreme	Matrix N/K/S Series Switch V6.x、V7.x	Syslog	すべての関連する Matrix K-Series、N-Series、および S-Series のデバイス・イベント	はい	いいえ	いいえ
Extreme	Stackable and Standalone Switches	Syslog	すべてのイベント	はい	はい	いいえ
Extreme	XSR Security Router V7.6.14.0002	Syslog	すべてのイベント	はい	いいえ	いいえ
Extreme	HiGuard Wireless IPS V2R2.0.30	Syslog	すべてのイベント	はい	いいえ	いいえ
Extreme	HiPath Wireless Controller V2R2.0.30	Syslog	すべてのイベント	はい	いいえ	いいえ
Extreme	NAC V3.2 および V3.3	Syslog	すべてのイベント	はい	いいえ	いいえ

表 410. QRadar でサポートされる DSM (続き)

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
Enterprise-IT-Security.com	SF-Sherlock V8.1 以降	LEEF	All_Checks, DB2_Security_Configuration, JES_Configuration, Job_Entry_System_Attack, Network_Parameter, Network_Security, No_Policy, Resource_Access_Viol, Resource_Allocation, Resource_Protection, Running_System_Change, Running_System_Security, Running_System_Status, Security_Dbase_Scan, Security_Dbase_Specialty, Security_Dbase_Status, Security_Parm_Change, Security_System_Attack, Security_System_Software, Security_System_Status, SF-Sherlock, Sherlock_Diverse, Sherlock_Diverse, Sherlock_Information, Sherlock_Specialties, Storage_Management, Subsystem_Scan, Sysplex_Security, Sysplex_Status, System_Catalog, System_File_Change, System_File_Security, System_File_Specialty, System_Log_Monitoring, System_Module_Security, System_Process_Security, System_Residence, System_Tampering, System_Volumes, TSO_Status, UNIX_OMVS_Security, UNIX_OMVS_System, User_Defined_Monitoring, xx_Resource_Prot_Templ	はい	いいえ	いいえ
Epic	Epic SIEM バージョン Epic 2014	LEEF	監査、認証	はい	はい	いいえ
Exabeam	Exabeam V1.7 および V2.0	該当なし	重要、異常	はい	いいえ	いいえ
Extreme Networks	Extreme Ware V7.7 および XOS V12.4.1.x	Syslog	すべてのイベント	いいえ	はい	いいえ
F5 Networks	BIG-IP AFM V11.3	Syslog	ネットワーク・イベント、ネットワーク DoS イベント、プロトコル・セキュリティー・イベント、DNS イベント、および DNS DoS イベント	はい	いいえ	いいえ
F5 Networks	BIG-IP LTM V4.5、V9.x から V11.x	Syslog	すべてのイベント	いいえ	はい	いいえ
F5 Networks	BIG-IP ASM V10.1 から V11.6	Syslog	すべてのイベント 共通イベント・フォーマット (CEF) 形式のメッセージ	いいえ	はい	いいえ
F5 Networks	BIG-IP APM V10.x および V11.x	Syslog	すべてのイベント	はい	いいえ	いいえ
F5 Networks	FirePass V7.0	Syslog	すべてのイベント	はい	はい	いいえ
Fair Warning	Fair Warning V2.9.2	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	いいえ
Fidelis Security Systems	Fidelis XPS V7.3.x	Syslog	アラート・イベント	はい	いいえ	いいえ
FireEye	FireEye CMS、MPS、EX、AX、NX、FX、および HX	Syslog	すべての関連イベント 共通イベント・フォーマット (CEF) 形式のメッセージ ログ・イベント拡張フォーマット (LEEF)	いいえ	はい	いいえ
FreeRADIUS	FreeRADIUS V2.x	Syslog	すべてのイベント	はい	はい	いいえ
Forcepoint (旧称 Websense)	TRITON V7.7	Syslog	すべてのイベント	はい	いいえ	いいえ
Forcepoint (旧称 Websense)	V-Series Data Security Suite (DSS) V7.1x	Syslog	すべてのイベント	はい	はい	はい
Forcepoint (旧称 Websense)	V-Series Content Gateway V7.1x	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
ForeScout	CounterACT V7.x 以降	Syslog	サービス妨害イベント、システム・イベント、エクスプロイト・イベント、認証イベント、および疑わしいイベント	いいえ	いいえ	いいえ
Fortinet	FortiGate FortiOS V2.5	Syslog Syslog リダイレクト	すべてのイベント	はい	はい	はい
Foundry	FastIron V3.x.x および V4.x.x	Syslog	すべてのイベント	はい	はい	いいえ
genua	genugate V8.2 以降	Syslog	一般的なエラー・メッセージ 高可用性 汎用リレー・メッセージ リレー固有のメッセージ genua プログラム/デーモン EPSI アカウンティング・デーモン - gg/src/acctd Configfw FWConfig ROFWConfig ユーザー・インターフェース Web サーバー	はい	はい	いいえ
Great Bay	Beacon	Syslog	すべてのイベント	はい	はい	いいえ
H3C Technologies	H3C Comware Platform、H3C スイッチ、H3C ルーター、H3C ワイヤレス LAN デバイス、および H3C IP セキュリティー・デバイス V7 がサポート対象	Syslog	NVP システム	いいえ	いいえ	いいえ
HBGary	Active Defense V1.2 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
HP	Network Automation V10.11	Syslog LEEF	すべての操作可能な構成ネットワーク・イベント。	はい	はい	いいえ
HP	ProCurve K.14.52	Syslog	すべてのイベント	はい	いいえ	いいえ
HP	Tandem	ログ・ファイル・プロトコル	Safe Guard Audit ファイル・イベント	いいえ	いいえ	いいえ
HP	UX V11.x 以降	Syslog	すべてのイベント	いいえ	はい	いいえ
Honeycomb Technologies	Lexicon File Integrity Monitor mesh service V3.1 以降	Syslog	保全性イベント	はい	いいえ	いいえ
Huawei	S Series Switch S5700、S7700、および S9700 (V200R001C00 を使用)	Syslog	S5700、S7700、および S9700 スイッチからの IPv4 イベント	いいえ	いいえ	いいえ
Huawei	AR シリーズ・ルーター (AR150、AR200、 AR1200、 AR2200、および AR3200 ルーター (V200R002C00 を使用))	Syslog	IPv4 イベント	いいえ	いいえ	いいえ
IBM	AIX V6.1 および V7.1	Syslog、ログ・ファイル・プロトコル	構成済みの監査イベント	はい	いいえ	いいえ
IBM	AIX 5.x、6.x、および v7.x	Syslog	認証イベントおよびオペレーティング・システム・イベント	はい	はい	いいえ
IBM	AS/400iSeries DSM V5R4 以降	ログ・ファイル・プロトコル	すべてのイベント	いいえ	はい	いいえ
IBM	AS/400 iSeries - Robert Townsend Security Solutions V5R1 以降	Syslog	CEF 形式のメッセージ	はい	はい	いいえ
IBM	AS/400 iSeries - Powertech Interact V5R1 以降	Syslog	CEF 形式のメッセージ	はい	はい	いいえ
IBM	BigFixV8.2.x から 9.5.2 (旧称 Tivoli EndPoint Manager)	IBM BigFix SOAP プロトコル	サーバー・イベント	いいえ	はい	いいえ
IBM	Bluemix® プラットフォーム	Syslog、TLS Syslog	すべてのシステム (Cloud Foundry) イベント、一部のアプリケーション・イベント	はい	いいえ	いいえ
IBM	Federated Directory Server V7.2.0.2 以降	LEEF	FDS 監査	はい	いいえ	いいえ
IBM	InfoSphere 8.2p45	Syslog	ポリシー・ビルダー・イベント	いいえ	いいえ	いいえ
IBM	ISS Proventia M10 v2.1_2004.1122_15.13.53	SNMP	すべてのイベント	いいえ	いいえ	いいえ
IBM	LotusDomino v8.5	SNMP	すべてのイベント	いいえ	いいえ	いいえ
IBM	Proventia Management SiteProtector v2.0 および v2.9	JDBC	IPS イベントおよび監査イベント	いいえ	いいえ	いいえ
IBM	RACF v1.9 から v1.13	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	はい

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
IBM	CICS v3.1 から v4.2	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	はい
IBM	DB2 v8.1 から v10.1	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	はい
IBM	IBM DataPower FirmwareV6 および V7 (旧称 WebSphere DataPower)	Syslog	すべてのイベント	はい	いいえ	いいえ
IBM	IBM Fiberlink MaaS360	LEEF	コンプライアンス・ルール・イベント デバイス登録イベント アクション履歴イベント	いいえ	はい	いいえ
IBM	z/OS v1.9 から v1.13	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	はい
IBM	Informix v11	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	いいえ
IBM	IMS	ログ・ファイル・プロトコル	すべてのイベント	いいえ	いいえ	いいえ
IBM	Security Access Manager for Mobile (ISAM)	TLS Syslog	IBM_SECURITY_AUTHN IBM_SECURITY_TRUST IBM_SECURITY_RUNTIME IBM_SECURITY_CBA_AUDIT_MGMT IBM_SECURITY_CBA_AUDIT_RTE IBM_SECURITY_RTSS_AUDIT_AUTHZ IBM_SECURITY_SIGNING CloudOE Operations 使用法 IDaaS Appliance Audit IDaaS Platform Audit	はい	いいえ	いいえ
IBM	Security Identity Governance (ISIG)	JDBC	NVP イベント・フォーマット 監査イベント・タイプ	いいえ	いいえ	いいえ
IBM	Security Network Protection (XGS) v5.0 フィックスパック 7	Syslog	システム・イベント、アクセス・イベント、およびセキュリティー・イベント	はい	いいえ	いいえ
IBM	Security Network IPS (GX) v4.6 以降	Syslog	セキュリティー・イベント、正常性イベント、およびシステム・イベント	はい	いいえ	いいえ
IBM	Security Identity Manager 6.0.x 以降	JDBC	監査イベントおよび再認証イベント	いいえ	はい	いいえ
IBM	IBM Security Trusteer Apex Advanced Malware Protection	Syslog/LEEF ログ・ファイル・プロトコル	マルウェア検出 エクスプロイト検出 データ引き出し検出 Java イベントのロックダウン ファイル検査イベント Apex 停止イベント Apex アンインストール・イベント ポリシー変更イベント ASLR 違反イベント ASLR 適用イベント パスワード保護イベント	はい	はい	いいえ
IBM	IBM Sense v1	Syslog	LEEF	はい	いいえ	いいえ
IBM	IBM SmartCloud Orchestrator v2.3 FP1 以降	IBM SmartCloud Orchestrator REST API	監査レコード	いいえ	はい	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
IBM	Tivoli Access Manager IBM Web Security Gateway v7.x	Syslog	監査イベント、アクセス・イベント、および HTTP イベント	はい	はい	いいえ
IBM	Tivoli Endpoint Manager (現在の IBM BigFix)					
IBM	WebSphere Application Server v5.0 から v8.5	ログ・ファイル・プロトコル	すべてのイベント	いいえ	はい	いいえ
IBM	WebSphere DataPower (現称 DataPower)WebSphere DataPower					
IBM	zSecure Alert v1.13.x 以降	UNIX syslog	アラート・イベント	はい	はい	いいえ
IBM	Security Access Manager v8.1 および v8.2	Syslog	監査イベント、システム・イベント、および認証イベント	はい	いいえ	いいえ
IBM	Security Directory v6.3.1 以降	Syslog LEEF	すべてのイベント	はい	はい	いいえ
Imperva	SecureSphere v6.2 および v7.x リリースの Enterprise Edition (Syslog) SecureSphere v9.5 から v11.5 (LEEF)	Syslog LEEF	すべてのイベント	はい	いいえ	いいえ
Internet Systems Consortium (ISC)	BIND v9.9	Syslog	すべてのイベント	はい	いいえ	いいえ
iT-CUBE	agileSI v1.x	SMB Tail	AgileSI SAP イベント	いいえ	はい	いいえ
Itron	Openway Smart Meter	Syslog	すべてのイベント	はい	いいえ	いいえ
Juniper Networks	AVT	JDBC	すべてのイベント	いいえ	いいえ	はい
Juniper Networks	DDoS Secure	Syslog	すべてのイベント	はい	いいえ	いいえ
Juniper Networks	DX	Syslog	状況イベントおよびネットワーク状況イベント	はい	いいえ	はい
Juniper Networks*	Infranet Controller v2.1、v3.1、および v4.0	Syslog	すべてのイベント	いいえ	はい	はい
Juniper Networks	Firewall and VPN v5.5r3 以降	Syslog	NetScreen Firewall イベント	はい	はい	はい
Juniper Networks	Junos WebApp Secure v4.2.x	Syslog	インシデント・イベントおよびアクセス・イベント	はい	いいえ	いいえ
Juniper Networks	IDP v4.0、v4.1、および v5.0	Syslog	NetScreen IDP イベント	はい	いいえ	はい
Juniper Networks	Network and Security Manager (NSM) および Juniper SSG v2007.1r2 から 2007.2r2、2008.r1、 2009r1.1、 2010.x	Syslog	NetScreen NSM イベント	はい	いいえ	はい
Juniper Networks	Junos OS v7.x から v10.x Ex シリーズ Ethernet Switch DSM は v9.0 から v10.x のみをサポート	Syslog または PCAP Syslog***	すべてのイベント	はい**	はい	はい
Juniper Networks	Secure Access RA Juniper SA バージョン 6.1R2 および Juniper IC バージョン 2.1	Syslog	すべてのイベント	はい	はい	はい
Juniper Networks	Juniper Security Binary Log Collector SRX または J Series アプライアンスの v12.1 以降	バイナリー	監査イベント、システム・イベント、ファイアウォール・イベント、および IPS イベント	いいえ	いいえ	はい
Juniper Networks	Steel-Belted Radius v5.x 以降	Syslog	すべてのイベント	はい	はい	はい
Juniper Networks	vGW Virtual Gateway v4.5	Syslog	ファイアウォール・イベント、管理イベント、ポリシー・イベント、および IDS ログ・イベント	はい	いいえ	いいえ
Juniper Networks	Wireless LAN Controller Wireless LAN devices with Mobility System Software (MSS) V7.6 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Kisco	Kisco Information Systems SafeNet/i V10.11	ログ・ファイル	すべてのイベント	いいえ	いいえ	いいえ
Lastline	Lastline Enterprise 6.0	LEEF	アンチマルウェア	はい	いいえ	いいえ
Lieberman	Random Password Manager v4.8x	Syslog	すべてのイベント	はい	いいえ	いいえ
Linux	Open Source Linux OS v2.4 以降	Syslog	オペレーティング・システム・イベント	はい	はい	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
Linux	DHCP Server v2.4 以降	Syslog	DHCP サーバーからのすべてのイベント	はい	はい	いいえ
Linux	IPtables kernel v2.4 以降	Syslog	許可イベント、ドロップ・イベント、または拒否イベント	はい	いいえ	いいえ
McAfee	Application / Change Control v4.5.x	JDBC	変更管理イベント	いいえ	はい	いいえ
McAfee	ePolicy Orchestrator v3.5 から v5.x	JDBC, SNMPv2, SNMPv3	アンチウィルス・イベント	いいえ	いいえ	いいえ
McAfee	Firewall Enterprise v6.1	Syslog	Firewall Enterprise イベント	はい	いいえ	いいえ
McAfee	Intrushield v2.x から v5.x	Syslog	アラート通知イベント	はい	いいえ	いいえ
McAfee	Intrushield v6.x から v7.x	Syslog	アラート通知イベントおよび障害通知イベント	はい	いいえ	いいえ
McAfee	Web v6.0.0 以降	Syslog、ログ・ファイル・プロトコル	すべてのイベント	はい	いいえ	いいえ
MetaInfo	MetaIP v5.7.00-6059 以降	Syslog	すべてのイベント	はい	はい	いいえ
Microsoft	Azure	Syslog	LEEF Authorization, Classic Compute, Classic Storage, Compute, Insights, KeyVault, SQL, Storage	はい	いいえ	いいえ
Microsoft	IIS v6.0、7.0 および 8.x	Syslog	HTTP 状況コード・イベント	はい	いいえ	いいえ
Microsoft	Internet and Acceleration (ISA) Server または Threat Management Gateway 2006	Syslog	ISA イベントまたは TMG イベント	はい	いいえ	いいえ
Microsoft	Exchange Server 2003、2007、2010、2013、および 2016	Windows Exchange プロトコル	Outlook Web Access のイベント (OWA) Simple Mail Transfer Protocol のイベント (SMTP) Message Tracking Protocol のイベント (MSGTRK)	いいえ	いいえ	いいえ
Microsoft	Endpoint Protection 2012	JDBC	マルウェア検出イベント	いいえ	いいえ	いいえ
Microsoft	Hyper V v2008 および v2012	WinCollect	すべてのイベント	いいえ	いいえ	いいえ
Microsoft	IAS Server v2000、2003、および 2008	Syslog	すべてのイベント	はい	いいえ	いいえ
Microsoft	Microsoft Windows Event Security Log v2000、2003、2008、XP、Vista、および Windows 7 (32 ビットまたは 64 ビットのシステムをサポート)	Syslog 非 Syslog MicrosoftWindows イベント・ログ・プロトコル・ソース 共通イベント・フォーマット (CEF) 形式 ログ・イベント拡張フォーマット (LEEF)	すべてのイベント	はい	はい	はい
Microsoft	SQL Server 2008、2012、および 2014	JDBC	SQL 監査イベント	いいえ	いいえ	いいえ
Microsoft	SharePoint 2010 および 2013	JDBC	SharePoint の監査イベント、サイト・イベント、およびファイル・イベント	いいえ	いいえ	いいえ
Microsoft	DHCP Server 2000/2003	Syslog	すべてのイベント	はい	はい	いいえ
Microsoft	Microsoft Office 365	Office 365 REST API	JSON	いいえ	いいえ	いいえ
Microsoft	Operations Manager 2005	JDBC	すべてのイベント	いいえ	いいえ	いいえ
Microsoft	System Center Operations Manager 2007	JDBC	すべてのイベント	いいえ	いいえ	いいえ
Motorola	Symbol AP firmware v1.1 から 2.1	Syslog	すべてのイベント	いいえ	いいえ	いいえ
Niara	Niara V1.6	Syslog	セキュリティー システム 内部アクティビティー 引き出し 感染 コマンドと制御	はい	いいえ	はい
NetApp	Data ONTAP	Syslog	CIFS イベント	はい	はい	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
Netskope	Netskope Active	Netskope Active REST API	アラート、すべてのイベント	いいえ	はい	いいえ
Niksun	NetVCR 2005 v3.x	Syslog	Niksun イベント	いいえ	いいえ	いいえ
Nokia	Firewall NG FP1、FP2、FP3、AI R54、AI R55、NGX on IPSO v3.8 以降	Syslog または OPSEC LEA	すべてのイベント	はい	はい	いいえ
Nokia	VPN-1 NG FP1、FP2、FP3、AI R54、AI R55、NGX on IPSO v3.8 以降	Syslog または OPSEC LEA	すべてのイベント	はい	はい	いいえ
Nominum	Vantio v5.3	Syslog	すべてのイベント	はい	いいえ	いいえ
Nortel	Contivity	Syslog	すべてのイベント	はい	いいえ	いいえ
Nortel	Application Switch v3.2 以降	Syslog	状況イベントおよびネットワーク状況イベント	いいえ	はい	いいえ
Nortel	ARN v15.5	Syslog	すべてのイベント	はい	いいえ	いいえ
Nortel*	Ethernet Routing Switch 2500 v4.1	Syslog	すべてのイベント	いいえ	はい	いいえ
Nortel*	Ethernet Routing Switch 4500 v5.1	Syslog	すべてのイベント	いいえ	はい	いいえ
Nortel*	Ethernet Routing Switch 5500 v5.1	Syslog	すべてのイベント	いいえ	はい	いいえ
Nortel	Ethernet Routing Switch 8300 v4.1	Syslog	すべてのイベント	いいえ	はい	いいえ
Nortel	Ethernet Routing Switch 8600 v5.0	Syslog	すべてのイベント	いいえ	はい	いいえ
Nortel	VPN Gateway v6.0、7.0.1 以降、v8.x	Syslog	すべてのイベント	はい	はい	いいえ
Nortel	Secure Router v9.3、v10.1	Syslog	すべてのイベント	はい	はい	いいえ
Nortel	Secure Network Access Switch v1.6 および v2.0	Syslog	すべてのイベント	はい	はい	いいえ
Nortel	Switched Firewall 5100 v2.4	Syslog or OPSEC	すべてのイベント	はい	はい	いいえ
Nortel	Switched Firewall 6000 v4.2	Syslog or OPSEC	すべてのイベント	はい	はい	いいえ
Nortel	Threat Protection System v4.6 および v4.7	Syslog	すべてのイベント	いいえ	いいえ	いいえ
Novell	eDirectory v2.7	Syslog	すべてのイベント	はい	いいえ	いいえ
ObserveIT	ObserveIT 5.7.x 以降	JDBC	アラート ユーザー・アクティビティー システム・イベント セッション・アクティビティー DBA アクティビティー	いいえ	はい	いいえ
Okta	Okta Identity Management	Okta REST API	JSON	いいえ	はい	いいえ
Onapsis	Onapsis Security Platform v1.5.8 以降	ログ・イベント拡張フォーマット (LEEF)	評価 アタック・シグニチャー 相関 コンプライアンス	はい	いいえ	いいえ
OpenBSD Project	OpenBSD v4.2 以降	Syslog	すべてのイベント	いいえ	はい	いいえ
Open LDAP Foundation	Open LDAP 2.4.x	UDP Multiline Syslog	すべてのイベント	いいえ	いいえ	いいえ
Open Source	SNORT v2.x	Syslog	すべてのイベント	はい	いいえ	いいえ
OpenStack	OpenStack v2015.1	HTTP レシーバー	監査イベント	いいえ	いいえ	いいえ
Oracle	Audit Records v9i、v10g、および v11g	Syslog JDBC	すべての関連する Oracle イベント	はい	はい	いいえ
Oracle	Audit Vault v10.2.3.2 以降	JDBC	Oracle イベント	いいえ	いいえ	いいえ
Oracle	OS Audit v9i、v10g、および v11g	Syslog	Oracle イベント	はい	はい	いいえ
Oracle	BEA WebLogic v10.3.x	ログ・ファイル・プロトコル	Oracle イベント	いいえ	いいえ	いいえ
Oracle	Database Listener v9i、v10g、および v11g	Syslog	Oracle イベント	はい	いいえ	いいえ
Oracle	Directory Server (旧称 Sun ONE LDAP)。					
Oracle	Fine Grained Auditing v9i および v10g	JDBC	ポリシーを指定して構成された表の選択/挿入/削除/更新イベント	いいえ	いいえ	いいえ
OSSEC	OSSEC v2.6 以降	Syslog	関連するすべてのイベント	はい	いいえ	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
Palo Alto Networks	Palo Alto PA シリーズ PanOS v3.0 から v7.1	Syslog LEEF PAN-OS v4.0 から v6.1 の CEF	Traffic Threat Config システム HIP Match	はい	はい	いいえ
Pirean	Access: One v2.2 with DB2 v9.7	JDBC	アクセス管理イベントおよび認証イベント	いいえ	いいえ	いいえ
PostFix	Mail Transfer Agent v2.6.6 以降	UDP Multiline Protocol または Syslog	メール・イベント	いいえ	いいえ	いいえ
ProFTPd	ProFTPd v1.2.x、v1.3.x	Syslog	すべてのイベント	はい	はい	いいえ
Proofpoint	Proofpoint Enterprise Protection and Enterprise Privacy バージョン 7.0.2、7.1、または 7.2	Syslog	システム・イベント、メール監査イベント、メール暗号化イベント、およびメール・セキュリティーの脅威分類イベント	いいえ	いいえ	いいえ
Radware	AppWall v6.5.2	Syslog	イベント・フォーマット: Vision ログ 記録されるイベント・タイプ: 管理 監査 学習 セキュリティー システム	はい	いいえ	いいえ
Radware	DefensePro v4.23、5.01、6.x、および 7.x	Syslog	すべてのイベント	はい	いいえ	いいえ
Raz-Lee iSecurity	AS/400iSeries Firewall 15.7 および Audit 11.7	Syslog	セキュリティー・イベントおよび監査イベント	はい	はい	いいえ
Redback Networks	ASE v6.1.5	Syslog	すべてのイベント	はい	いいえ	いいえ
Resolution1	Resolution1 CyberSecurity 旧称は、AccessData InSightResolution1 CyberSecurity	ログ・ファイル	揮発性データ、メモリー分析データ、メモリー獲得データ、収集データ、ソフトウェア・インベントリー、プロセス・ダンプ・データ、脅威スキャン・データ、エージェント修復データ	いいえ	いいえ	いいえ
Riverbed	SteelCentral NetProfiler	JDBC	アラート・イベント	いいえ	いいえ	いいえ
Riverbed	SteelCentral NetProfiler Audit	ログ・ファイル・プロトコル	監査イベント	いいえ	はい	いいえ
RSA	Authentication Manager v6.x、v7.x、および v8.x	v6.x および v7.x は、Syslog またはログ・ファイル・プロトコルを使用 v8.x は Syslog のみ使用	すべてのイベント	いいえ	いいえ	いいえ
SafeNet	DataSecure v6.3.0 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Salesforce	Security Auditing	ログ・ファイル	セットアップ監査レコード	いいえ	いいえ	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
Salesforce	Security Monitoring	Salesforce REST API プロトコル	ログイン履歴 アカウント履歴 ケース履歴 ライセンス履歴 サービス契約履歴 契約品目履歴 契約履歴 コンタクト履歴 リード履歴 案件履歴 ソリューション履歴	いいえ	はい	いいえ
Samhain Labs	HIDS v2.4	Syslog JDBC	すべてのイベント	はい	いいえ	いいえ
Seculert	Seculert v1	Seculert Protection REST API プロトコル	すべてのマルウェア通信イベント	いいえ	いいえ	いいえ
Seculert	Seculert	Seculert protection REST API プロトコル	すべてのマルウェア通信イベント	いいえ	いいえ	いいえ
Sentrigo	Hedgehog v2.5.3	Syslog	すべてのイベント	はい	いいえ	いいえ
Skyhigh Networks	Skyhigh Networks Cloud Security Platform v2.4	LEEF	アノマリ・イベント	はい	いいえ	いいえ
SolarWinds	Orion v2011.2	Syslog	すべてのイベント	はい	いいえ	いいえ
SonicWALL	UTM/Firewall/VPN Appliance v3.x 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Sophos	Astaro v8.x	Syslog	すべてのイベント	はい	いいえ	いいえ
Sophos	Enterprise Console v4.5.1 および v5.1	Sophos Enterprise Console プロトコル JDBC	すべてのイベント	いいえ	いいえ	いいえ
Sophos	PureMessage v3.1.0.0 以降 (Microsoft Exchange v5.6.0 for Linux 用)	JDBC	検疫された E メール・イベント	いいえ	いいえ	いいえ
Sophos	Web Security Appliance v3.x	Syslog	トランザクション・ログ・イベント	はい	いいえ	いいえ
Sourcefire	Intrusion Sensor IS 500、v2.x、3.x、4.x	Syslog	すべてのイベント	はい	いいえ	いいえ
Sourcefire	Defense Center (現在の Cisco FireSIGHT Management Center)					
Splunk	MicrosoftWindows セキュリティー・イベント・ログ	Splunk Forwarders により提供される Windows ベースのイベント	すべてのイベント	いいえ	はい	いいえ
Squid	Web Proxy v2.5 以降	Syslog	すべてのキャッシュ・イベントおよびアクセス・ログ・イベント	はい	いいえ	いいえ
Startent Networks	Startent Networks	Syslog	すべてのイベント	はい	いいえ	いいえ
STEALTHbits Technologies	STEALTHbits File Activity Monitor	Syslog LEEF	ファイル・アクティビティー・モニター・イベント			
STEALTHbits Technologies	StealthINTERCEPT	Syslog LEEF	Active Directory 監査イベント	はい	いいえ	いいえ
STEALTHbits Technologies	STEALTHbits StealthINTERCEPT Alerts	Syslog LEEF	Active Directory アラート・イベント	はい	いいえ	いいえ
STEALTHbits Technologies	STEALTHbits StealthINTERCEPT Analytics	Syslog LEEF	Active Directory 分析イベント	はい	いいえ	いいえ
Stonesoft	Management Center v5.4	Syslog	Management Center イベント、IPS イベント、ファイアウォール・イベント、および VPN イベント	はい	いいえ	いいえ
Sun	Solaris v5.8、v5.9、Sun OS v5.8、v5.9	Syslog	すべてのイベント	はい	はい	いいえ
Sun	Solaris DHCP v2.8	Syslog	すべてのイベント	はい	はい	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
Sun	Solaris Sendmail v2.x	Syslog ログ・ファイル・プロトコル Proofpoint 7.5 および 8.0 Sendmail のログ	すべてのイベント	はい	いいえ	いいえ
Sun	Solaris 基本セキュリティー・モジュール (BSM) v5.10 および v5.11	ログ・ファイル・プロトコル	すべてのイベント	いいえ	はい	いいえ
Sun	ONE LDAP v11.1 (現在の Oracle Directory Server)	ログ・ファイル・プロトコル UDP Multiline Syslog	すべての関連するアクセス・イベントおよび LDAP イベント	いいえ	いいえ	いいえ
Sybase	ASE v15.0 以降	JDBC	すべてのイベント	いいえ	いいえ	いいえ
Symantec	Endpoint Protection v11 および v12	Syslog	すべての監査ログおよびセキュリティー・ログ	はい	いいえ	はい
Symantec	SGS Appliance v3.x 以降	Syslog	すべてのイベント	はい	いいえ	はい
Symantec	SSC v10.1	JDBC	すべてのイベント	はい	いいえ	いいえ
Symantec	Data Loss Prevention (DLP) v8.x 以降	Syslog	すべてのイベント	いいえ	いいえ	いいえ
Symantec	PGP Universal Server 3.0.x	Syslog	すべてのイベント	はい	いいえ	いいえ
Symark	PowerBroker 4.0	Syslog	すべてのイベント	はい	いいえ	いいえ
ThreatGRID	Malware Threat Intelligence Platform v2.0	ログ・ファイル・プロトコル Syslog	マルウェア・イベント	いいえ	いいえ	いいえ
TippingPoint	Intrusion Prevention System (IPS) v1.4.2 から v3.2.x	Syslog	すべてのイベント	いいえ	いいえ	いいえ
TippingPoint	X505/X506 v2.5 以降	Syslog	すべてのイベント	はい	はい	いいえ
Top Layer	IPS 5500 v4.1 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Trend Micro	Control Manager v5.0 または v5.5 (SP1 Patch 1 の後にホット・フィックス 1697 または 1713 を適用)	SNMPv1 SNMPv2 SNMPv3	すべてのイベント	はい	いいえ	いいえ
Trend Micro	Deep Discovery v3.x	Syslog	すべてのイベント	はい	いいえ	いいえ
Trend Micro	Deep Discovery Email Inspector v2.1	ログ・イベント拡張フォーマット (LEEF)	検出、Virtual Analyzer Analysis ログ、システム・イベント	はい	いいえ	いいえ
Trend Micro	Deep Security V9.6.1532 および V10.0.1962	ログ・イベント拡張フォーマット (LEEF)	アンチマルウェア Deep Security ファイアウォール Integrity Monitor 侵入防止 ログ検査 システム Web 評価	はい	いいえ	いいえ
Trend Micro	InterScan VirusWall v6.0 以降	Syslog	すべてのイベント	はい	いいえ	いいえ
Trend Micro	Office Scan v8.x および v10.x	SNMPv2	すべてのイベント	いいえ	いいえ	いいえ
Tripwire	Enterprise Manager v5.2 以降	Syslog	リソースの追加/削除/変更イベント	はい	いいえ	いいえ
Tropos Networks	Tropos Control v7.7	Syslog	障害管理イベント、ログイン/ログアウト・イベント、プロビジョン・イベント、およびデバイス・イメージのアップロード・イベント	いいえ	いいえ	いいえ
Trusteer	Apex Local Event Aggregator v1304.x 以降	Syslog	マルウェア・イベント、エクスプロイト・イベント、およびデータ引き出し検出イベント	はい	いいえ	いいえ
共通	Syslog および SNMP	Syslog SNMP SDEE	すべてのイベント	いいえ	はい	いいえ

表 *410. QRadar* でサポートされる *DSM (*続き*)*

製造元	デバイス名およびバージョン	プロトコル	記録されるイベントおよびフォーマット	自動的に検出?	ID を含む?	カスタム・プロパティーを含む?
共通	Syslog	Syslog ログ・ファイル・プロトコル	すべてのイベント	いいえ	はい	いいえ
共通	認証サーバー	Syslog	すべてのイベント	いいえ	はい	いいえ
共通	ファイアウォール	Syslog	すべてのイベント	いいえ	いいえ	いいえ
Vectra Networks	Vectra Networks Vectra v2.2	Syslog 共通イベント・フォーマット	ホスト・スコアリング、コマンドと制御、ボットネット・アクティビティー、スキャン行為、側方移動、引き出し	はい	いいえ	いいえ
Verdasys	Digital Guardian V6.0.x (Syslog のみ) Digital Guardian V6.1.1 および V7.2 (LEEF のみ)	Syslog LEEF	すべてのイベント	はい	いいえ	いいえ
Vericept	Content 360 (v8.0 まで)	Syslog	すべてのイベント	はい	いいえ	いいえ
VMware	VMware ESX または ESXi 3.5.x、4.x、および 5.x	Syslog VMWare プロトコル	すべてのイベント	はい (Syslog の場合)	いいえ	いいえ
VMware	vCenter v5.x	VMWare プロトコル	すべてのイベント	いいえ	いいえ	いいえ
VMware	vCloud v5.1	vCloud プロトコル	すべてのイベント	いいえ	はい	いいえ
VMWare	vShield	Syslog	すべてのイベント	はい	いいえ	いいえ
Vormetric, Inc.	Vormetric Data Security	Syslog (LEEF)	監査 アラーム 警告 学習モード システム	はい	いいえ	いいえ
Watchguard	WatchGuard Fireware OS	Syslog	すべてのイベント	はい	いいえ	いいえ
Websense (現称 Forcepoint)						
Zscaler	Zscaler NSS v4.1	Syslog	Web ログ・イベント	はい	いいえ	いいえ

第 4 部 付録

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21