IBM Security Access Manager for Web
バージョン 7.0

IBM Security Web Gateway Appliance 管理ガイド

SA88-5103-01
(英文原典：SC22-5432-01)

IBM Security Access Manager for Web
バージョン 7.0

IBM Security Web Gateway Appliance 管理ガイド

SA88-5103-01
(英文原典：SC22-5432-01)

お願い

本書および本書で紹介する製品をご使用になる前に、 143 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、IBM Security Access Manager (製品番号 5724-C87) バージョン 7 リリース 0 モディフィケーション 0、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

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。

原典： SC22-5432-01
IBM Security Access Manager for Web
Version 7.0
IBM Security Web Gateway Appliance
Administration Guide

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

第1刷 2013.4

目次

図

表

本書について

*IBM Security Web Gateway Appliance 管理ガイド*へようこそ。

IBM Security Access Manager for Web (旧称: IBM Tivoli Access Manager for e-business) は、ユーザー認証、許可、および Web シングル・サインオンに対応したソリューションであり、さまざまな Web リソースとアプリケーション・リソースにセキュリティー・ポリシーを適用することが可能です。

IBM Security Access Manager for Web WebSEAL は、Security Access Manager セキュア・ドメイン内の Web ベースのリソースのためのリソース・マネージャーです。WebSEAL は、ハイパフォーマンスでかつマルチスレッド化された Web サーバーであり、保護 Web オブジェクト・スペースに対してきめの細かいセキュリティー・ポリシーを適用します。WebSEAL は、シングル・サインオン・ソリューションを提供でき、バックエンド Web アプリケーション・サーバー・リソースをそのセキュリティー・ポリシーの中に取り込むことができます。

IBM Security Web Gateway Appliance は、WebSEAL の強みを活かして、アクセス制御および Web ベースの脅威からの保護を行います。

対象読者

本書は、Security Access Manager WebSEAL 環境の構成および保守を担当するシステム・アドミニストレーターを対象としています。

本書の読者には、以下の知識が必要です。

- PC および UNIX または Linux の オペレーティング・システム
- データベースのアーキテクチャーと概念
- セキュリティー管理
- HTTP、TCP/IP、ファイル転送プロトコル (FTP)、Telnet などのインターネット・プロトコル
- Lightweight Directory Access Protocol (LDAP) とディレクトリー・サービス
- サポートされるユーザー・レジストリー
- WebSphere® Application Server の管理
- 認証と許可

SSL (Secure Sockets Layer) 通信を使用可能にしようとしている場合は、SSL プロトコル、鍵交換 (公開鍵と秘密鍵)、デジタル署名、暗号アルゴリズム、および認証局 (CA) についての知識も必要です。

資料および用語集へのアクセス

このセクションには、以下が含まれています。

- 『IBM Security Access Manager for Web ライブラリー』の資料のリスト。
- xiv ページの『オンライン資料』へのリンク。
- xv ページの『IBM Terminology Web サイト』 へのリンク。

IBM Security Access Manager for Web ライブラリー

以下の資料はIBM Security Access Manager for Web ライブラリーにあります。

- *IBM Security Access Manager for WebQuick Start Guide*、GI11-9333-01

  主なインストールおよび構成タスクを要約した手順を説明します。

- *IBM Security Web Gateway Appliance - ハードウェア・オファリング・クイック・スタート・ガイド*、SC22-5434-00

  WebSEAL Hardware Appliance に接続し、初期構成を実行するプロセスの手順を示しています。

- *IBM Security Web Gateway Appliance - 仮想オファリング・クイック・スタート・ガイド*

  WebSEAL Virtual Appliance に接続し、初期構成を実行するプロセスの手順を示しています。

- *IBM Security Access Manager for Web インストール・ガイド*、 GC88-8428-01

  Security Access Manager のインストールおよび構成方法の説明があります。

- *IBM Security Access Manager for Web アップグレード・ガイド*、SA88-5102-00

  ユーザーがバージョン 6.0 または 6.1.x からバージョン 7.0 にアップグレードするための情報が記載されています。

- *IBM Security Access Manager for Web 管理ガイド*、SC23-6504-03

  Security Access Manager の概念および使用手順を説明しています。 Web Portal Manager インターフェースから、および **pdadmin** ユーティリティーを使用したタスクの実行方法が記載されています。

- *IBM Security Access Manager for Web WebSEAL 管理ガイド*、SC23-6505-03

  WebSEAL を使用してユーザーのセキュア Web ドメインのリソースを管理する場合の背景資料、管理手順、および参照情報が記載されています。

- *IBM Security Access Manager for Web Plug-in for Web Servers 管理ガイド*、SC88-8429-01

  Web サーバー・プラグインを使用して Web ドメインを保護するための手順および参照情報が記載されています。

- *IBM Security Access Manager for Web 共用セッション管理 管理ガイド*、SC88-4659-02

  Session Management Server の管理時の考慮事項および操作手順について説明しています。

- *IBM Security Access Manager for Web 共用セッション管理 デプロイメント・ガイド*、SA88-5105-00

Session Management Server のデプロイメントの考慮事項について説明しています。

- *IBM Security Web Gateway Appliance 管理ガイド*、SC22-5432-01

  WebSEAL Appliance の管理手順およびテクニカル・リファレンス情報が記載されています。

- *IBM Security Web Gateway Appliance Web リバース・プロキシーの構成ガイド*、SC22-5433-01

  WebSEAL Appliance の構成手順およびテクニカル・リファレンス情報が記載されています。

- *IBM Security Web Gateway Appliance Web リバース・プロキシー・スタンザ・リファレンス*、SC27-4442-01

  IBM® Security Web Gateway Appliance Web リバース・プロキシーの完全なスタンザ・リファレンスが示されています。

- *IBM Security Access Manager for Web WebSEAL 構成スタンザ・リファレンス*、SC27-4443-01

  WebSEAL の完全なスタンザ・リファレンスが示されています。

- *IBM Global Security Kit: CapiCmd Users Guide*、SC22-5459-00

  鍵データベース、公開鍵と秘密鍵のペア、および認証要求の作成に関して説明されています。

- *IBM Security Access Manager for Web Auditing Guide*、SC23-6511-03

  ネイティブ Security Access Manager アプローチおよび Common Auditing and Reporting Service (共通監査報告サービス) を使用した監査イベントの構成および管理に関する情報があります。 また、Common Auditing and Reporting Service (共通監査報告サービス) のインストールおよび構成についての情報もあります。このサービスは、運用レポートの生成および表示に使用します。

- *IBM Security Access Manager for Web Command Reference*、SC23-6512-03

  Security Access Manager で提供されるコマンド、ユーティリティー、およびスクリプトに関する参照情報が記載されています。

- *IBM Security Access Manager for Web Administration C API Developer Reference*、SC23-6513-02

  管理 API の C 言語インプリメンテーションを使用して、アプリケーションが Security Access Manager の管理タスクを実行できるようにするための参照情報が記載されています。

- *IBM Security Access Manager for Web Administration Java Classes Developer Reference*、SC23-6514-02

  管理 API の Java™ 言語インプリメンテーションを使用して、アプリケーションが Security Access Manager の管理タスクを実行できるようにするための参照情報が記載されています。

- *IBM Security Access Manager for Web Authorization C API Developer Reference*、SC23-6515-02

  許可 API の C 言語インプリメンテーションを使用して、アプリケーションが Security Access Manager セキュリティーを使用できるようにするための参照情報が記載されています。

- *IBM Security Access Manager for Web Authorization Java Classes Developer Reference*、SC23-6516-02

  許可 API の Java 言語インプリメンテーションを使用して、アプリケーションが Security Access Manager セキュリティーを使用できるようにするための参照情報が記載されています。

- *IBM Security Access Manager for Web Web Security Developer Reference*, SC23-6517-02

  認証モジュールを開発するためのプログラミングおよび参照の情報が記載されています。

- *IBM Security Access Manager for Web Error Message Reference*、GI11-8157-02

  メッセージおよび戻りコードについての説明および修正アクションが記載されています。

- *IBM Security Access Manager for Web Troubleshooting Guide*、GC27-2717-01

  問題判別についての説明が記載されています。

- *IBM Security Access Manager for Web Performance Tuning Guide*、SC23-6518-02

  ユーザー・レジストリーとして IBM Tivoli Directory Server を使用する、Security Access Manager からなる環境の、パフォーマンス・チューニングについての説明があります。

オンライン資料

IBM では、製品のリリース時および資料の更新時に、以下の場所に製品資料を掲載しています。

IBM Security Access Manager for Web のインフォメーション・センター
http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.isam.doc_70/welcome.html サイトでは、この製品のインフォメーション・センターのウェルカム・ページが表示されます。

IBM Security Systems Documentation Central およびウェルカム・ページ
IBM Security Systems Documentation Central では、すべての IBM Security Systems 製品資料のアルファベット順リストと、各製品の特定のバージョンの製品インフォメーション・センターへのリンクが提供されています。

Welcome to IBM Security Systems Information Centers では、IBM Security Systems のインフォメーション・センターの概要、インフォメーション・センターへのリンク、およびインフォメーション・センターの一般情報が提供されています。

IBM Publications Center

このサイト (http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) には、必要なすべての IBM 資料を見つけるのに役立つカスタマイズ検索機能が用意されています。

IBM Terminology Web サイト

IBM Terminology Web サイトは、製品ライブラリーの用語を 1 つのロケーションに統合したものです。Terminology Web サイトには、http://www.ibm.com/software/globalization/terminology からアクセスできます。

関連資料

このセクションには、Security Access Manager ソリューションに組み込まれている関連した IBM 製品がリストされています。

注: 以下のミドルウェア製品は、IBM Security Web Gateway Appliance には同梱されていません。

IBM Global Security Kit

Security Access Manager では、 Global Security Kit (GSKit) バージョン 8.0.x を使用したデータ暗号化が提供されます。 GSKit は、特定のプラットフォーム用の *IBM Security Access Manager for Web バージョン 7.0* 製品イメージまたは DVD に含まれています。

GSKit バージョン 8 には、鍵管理用のコマンド行ツール GSKCapiCmd (**gsk8capicmd_64**) が含まれています。

GSKit バージョン 8 では、鍵管理ユーティリティー iKeyman (**gskikm.jar**) は含まれなくなりました。 iKeyman は、IBM Java バージョン 6 以降とともにパッケージされており、ネイティブ GSKit ランタイムに依存しないピュア Java アプリケーションになりました。バンドルされている *java*/jre/lib/gskikm.jar ライブラリーを移動したり、削除したりしないでください。

Security Access Manager インフォメーション・センターで、「*IBM Developer Kit and Runtime Environment, Java Technology Edition, Version 6 and 7, iKeyman User's Guide for version 8.0*」を入手できます。また、この資料は、以下の場所から直接ご利用いただけます。

http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/60/iKeyman.8.User.Guide.pdf

注:

GSKit バージョン 8 には、セキュリティー問題を修正するために必要な、トランスポート層セキュリティーの実装に対する重要な変更が含まれています。

GSKit バージョン 8 の変更は、Internet Engineering Task Force (IETF) の Request For Comments (RFC) の要件に準拠しています。ただし、古いバージョンの GSKit との互換性はありません。GSKit を使用する、 Security Access Manager と通信する

すべてのコンポーネントは、 GSKit バージョン 7.0.4.42、または 8.0.14.26 以降を使用するようにアップグレードする必要があります。 そうしないと、通信の問題が発生することがあります。

IBM Tivoli Directory Server

IBM Tivoli Directory Server バージョン 6.3 FP17 (6.3.0.17-ISS-ITDS-FP0017) は、特定のプラットフォーム用の *IBM Security Access Manager for Web バージョン 7.0* 製品イメージまたは DVD に含まれています。

Tivoli Directory Server について詳しくは、以下にあります。

http://www.ibm.com/software/tivoli/products/directory-server/

IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator バージョン 7.1.1 は、特定のプラットフォーム用の *IBM Tivoli Directory Integrator Identity Edition V 7.1.1 for Multiplatform* 製品イメージまたは DVD に含まれています。

IBM Tivoli Directory Integrator について詳しくは、以下にあります。

http://www.ibm.com/software/tivoli/products/directory-integrator/

IBM DB2 Universal Database™

IBM DB2 Universal Database Enterprise Server Edition バージョン 9.7 FP4 は、特定のプラットフォーム用の *IBM Security Access Manager for Web Version 7.0* 製品イメージまたは DVD で提供されます。DB2® は、Tivoli Directory Server ソフトウェアとともにインストールするか、スタンドアロン製品としてインストールできます。Security Access Manager のユーザー・レジストリーとして Tivoli Directory Server または z/OS® LDAP サーバーを使用する場合は、DB2 は必須です。 z/OS LDAP サーバーでは、DB2 を別途ご購入いただく必要があります。

DB2 について詳しくは、以下にあります。

http://www.ibm.com/software/data/db2

IBM WebSphere 製品

WebSphere Application Server Network Deployment バージョン 8.0 および WebSphere eXtreme Scale バージョン 8.5.0.1 のインストール・パッケージは、Security Access Manager バージョン 7.0 に同梱されています。WebSphere eXtreme Scale が必要になるのは、 Session Management Server (SMS) コンポーネントを使用する場合のみです。

WebSphere Application Server は、以下のアプリケーションのサポートを可能にします。

- Web Portal Manager インターフェース (Security Access Manager を管理します)。
- Web Administration Tool (Tivoli Directory Server を管理します)。
- Common Auditing and Reporting Service (共通監査報告サービス) (監査イベントの処理およびレポート作成を行います)。

- Session Management Server (Web セキュリティー・サーバー環境で共有セッションを管理します)。
- 属性検索サービス

WebSphere Application Server について詳しくは、以下にあります。

http://www.ibm.com/software/webservers/appserv/was/library/

アクセシビリティー

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーがソフトウェア・プロダクトを快適に使用できるようにサポートします。これらの製品を使用することにより、インターフェースを耳で聴いて確認したり、ナビゲートしたりするための支援テクノロジーをご利用いただけます。また、グラフィカル・ユーザー・インターフェースのすべての機能は、マウスを使用しなくてもキーボードから操作できるようになっています。

IBM のアクセシビリティーの取り組みに関する詳細は、IBM Accessibility Center をご覧ください。

技術研修

以下は英語のみの対応となります。技術研修の情報については、IBM Education Web サイト (http://www.ibm.com/software/tivoli/education) を参照してください。

サポート情報

IBM サポートは、コード関連の問題、およびインストールまたは使用方法に関する短時間の定型質問に対する支援を提供します。IBM ソフトウェア・サポート・サイトには、http://www.ibm.com/software/support/probsub.html から直接アクセスできます。

「*IBM Security Access Manager for Web Troubleshooting Guide*」では、以下の詳細について説明されています。

- IBM サポートへの連絡前に収集する情報。
- IBM サポートに連絡するための各種方法。
- IBM Support Assistant の利用方法。
- ユーザー自身で問題を切り分けて修正するための説明と問題判別リソース。

注: 製品のインフォメーション・センターの「**コミュニティーおよびサポート**」タブに、追加のサポート・リソースが示されています。

第 1 章 概要

IBM Security Web Gateway Appliance は、アクセス制御および Web ベースの脅威からの保護の両方が可能なネットワーク・アプライアンス・ベースのセキュリティー・ソリューションです。

本アプライアンスの主な機能は、次のとおりです。

- フロントエンドのロード・バランシング機能。
- Web アプリケーション・ファイアウォール機能。
- システム通知、リバース・プロキシーの正常性の状況、ディスク使用量などのシステム状況を表示するダッシュボード。
- イベント・ログ、メモリー統計、CPU 使用率などの分析および診断ツール。
- ランタイム・コンポーネント、動的 URL 構成ファイル、SSL 証明書などのリバース・プロキシー設定の集中管理。
- 更新、ライセンス、ネットワーク設定などのシステム設定の制御。

機能の大半は、ローカル管理インターフェースまたは Web サービス・インターフェースを使用して構成できます。

アプライアンスの形式

IBM Security Web Gateway Appliance には、ハードウェア・アプライアンスと仮想アプライアンスの 2 つの形式があります。

ハードウェア・アプライアンスは、アプライアンス・ハードウェア、およびプリインストール済みの Web Gateway Appliance ファームウェアから構成されます。ハードウェア・アプライアンスのマシン仕様を以下に示します。

- Intel i7 2600 プロセッサー
- 32 GB メモリー
- 100 GB ソリッド・ステート・ドライブ
- 6 ネットワーク・ポート

  注: これらのポートのうちの 2 つは、アプライアンスの管理専用で使用されます。

仮想アプライアンスは、Security Access Manager コンポーネントです。これは、以下の仮想ハイパーバイザーでホストできます。

- VMware ESX 4.1 および今後のフィックスパック
- VMware ESXi 4.1 および今後のフィックスパック
- VMware ESXi 5.0 および今後のフィックスパック

Web リバース・プロキシー機能のサポート

IBM Security Web Gateway Appliance の Web リバース・プロキシー機能は、IBM Security Access Manager WebSEAL 製品に組み込まれているテクノロジーをベースにしています。アプライアンスは、WebSEAL で提供される機能の大部分をサポートしていますが、以下の表に含まれる項目は除きます。

表 1. アプライアンスがサポートしていない WebSEAL 機能

機能	説明
カスタム・ライブラリー、CDAS および EAS のインクルード	アプライアンスはカスタム CDAS モジュールをサポートしていません。したがって、アプライアンスは以下の認証メカニズムをサポートしていません。 • IP アドレス • HTTP ヘッダー • Post パスワード変更 WebSEAL は、これらのメカニズム用の CDAS モジュールを提供していません。 **注:** アプライアンスは、IBM Security Identity Manager のパスワード同期化プラグインをサポートしています。詳しくは、「*IBM Security Web Gateway Appliance: Web リバース・プロキシー・スタンザ・リファレンス*」の **[itim]** スタンザを参照してください。
RSA トークン	デフォルトでは、アプライアンスは RSA トークン認証をサポートしていません。ただし、トークン認証用の EAI を実装することは可能です。
Kerberos (Windows デスクトップ・シングル・サインオン)	アプライアンスは、Kerberos 認証を内部的にサポートしていません。ただし、Kerberos 認証を処理するように EAI を構成することは可能です。
ローカル junction	アプライアンスのローカル junction サポートには、以下の制限が適用されます。 • アプライアンスは、WebSEAL インスタンスのローカル junction に対して、固定された単一のファイル・システム・パスをサポートします。 • アプライアンスのローカル junction では、どの CGI スクリプトも実行できません。
ハードウェア・ベースの暗号化	アプライアンスは、どのハードウェア・ベースの暗号化もサポートしていません。ただし、ハードウェア・アプライアンスには、i7-2600 プロセッサーの AES-NI サポートが組み込まれているため、暗号化操作の処理が可能です。

表 1. アプライアンスがサポートしていない WebSEAL 機能 (続き)

機能	説明
アプリケーション応答測定 (ARM)	WebSEAL ソフトウェアには、ARM のサポートが組み込まれているため、要求および応答処理ストリーム全体でトランザクションをモニターできます。アプライアンスは ARM サポートを含みません。
Tivoli® Common Directory ロギング	Tivoli Common Directory ロギング機能は、IBM Security ソフトウェア・アプリケーションのすべてのログ・ファイルを共通のファイル・システム・ディレクトリーに保管します。アプライアンスはこの共通ロギングをサポートしていません。アプライアンスのロギングは、LMI を通じて管理されます。
パイプまたは CARS の監査	アプライアンスは、監査レコードを直接パイプまたは CARS サーバーに送信することはできません。ただし、中間 ISAM 許可サーバーを使用して、監査レコードを間接的に宛先に送信することは可能です。
ARS (Web サービス)	IBM Security Access Manager for Web ARS Web サービスは、許可のために要求情報を外部の ARS サーバーに送信できます。アプライアンスでは ARS を使用できません。

アプライアンスの使用に関するヒント

アプライアンスを管理する際に役立つヒントを以下に示します。

バックアップ

アプライアンスは頻繁にバックアップすることが重要です。アプライアンスをバックアップするには、アプライアンスで提供されるスナップショット機能を使用します。

スナップショット とは、特定時刻におけるアプライアンスの状態のコピーのことです。スナップショット・ファイルを使用することにより、アプライアンスをバックアップして、後でリストアすることができます。スナップショットを定期的に作成し、アプライアンスからダウンロードして、バックアップとして利用することをお勧めします。ただし、スナップショットはディスク・スペースを大量に消費するので、古いスナップショットは定期的にクリーンアップするのが最善です。

スナップショットの使用について詳しくは、 126 ページの『スナップショットの管理』を参照してください。

ディスク・スペース使用量

ハードウェア・アプライアンスのディスク・スペースは、取り付けられているハード・ディスクの容量によって制限されます。ファイルによっては、時間と共に大量のディスク・スペースを消費するものがあります。通常、このようなファイルには、以下のものがあります。

サポート・ファイル

サポート・ファイル は、アプライアンスに関する問題をトラブルシューティングするために IBM サポート担当員が使用するものです。サポート・ファイルには、すべてのログ・ファイル、一時ファイル、中間ファイル、および顧客サポートの問題を診断するために必要なコマンド出力が含まれます。これらのファイルのサイズは、時間と共に増加する場合があります。これらのファイルが使用するディスク・スペースを削減するには、未使用のサポート・ファイルを外部のドライブにダウンロードします。次に、これらのサポート・ファイルをアプライアンスから削除します。詳細については、 127 ページの『サポート・ファイルの管理』 を参照してください。

スナップショット・ファイル

スナップショット・ファイル は、特定時刻におけるアプライアンスの状態を記録したものです。このファイルを使用すると、アプライアンスを以前の状態にリストアできます。デフォルトでは、スナップショット・ファイルは、アプライアンスに保管されます。使用されるディスク・スペースを削減するには、スナップショット・ファイルを外部のドライブにダウンロードして、アプライアンスから削除します。詳細については、 126 ページの『スナップショットの管理』 を参照してください。

Web リバース・プロキシー・ログ・ファイル

このログ・ファイルには、アプライアンスの日常操作での Web リバース・プロキシーのイベントとアクティビティーが記録されます。このファイルで消費されるディスク・スペースを削減するには、2 つの方法があります。

- ログ情報をリモート・サーバーに送信するように Web リバース・プロキシーを構成します。
- 未使用のログ・ファイルを定期的に消去します。詳しくは、 23 ページの『リバース・プロキシー・ログ・ファイルの管理』を参照してください。あるいは、コマンド行インターフェースを使用して、ログ・ファイルを USB デバイスにバックアップし、ロールオーバーされたログ・ファイルをすべて消去します。詳しくは、 28 ページの『コマンド行インターフェースを使用した Web リバース・プロキシーのログ・ファイルのアーカイブおよび削除』を参照してください。

  注: アプライアンスは、ディスク使用率が特定のしきい値 (デフォルト構成は 95%) に達すると、古いログ・ファイルを自動的に消去するように構成されています。ディスク使用率がしきい値を超えると、ログ・ファイルが個々に削除されます。最も古いファイルから削除が開始され、ディスク使用率がしきい値を下回るまで削除が繰り返されます。

管理者は、残りの空きディスク・スペースをモニターし、十分なディスク・スペースを確保するために必要なアクションを実行する必要があります。アプライアンスは、管理者が現在のディスク使用量をモニターするための「ディスク使用量」ダッ

シュボード・ウィジェットを用意しています。ディスク・スペースの管理について詳しくは、 18 ページの『ディスク使用量の表示』 を参照してください。

第 2 章 始めに

以下のタスクのうち、ご使用のアプライアンスの形式に該当するものを実行します。

ハードウェア・アプライアンス・タスク

ハードウェア・アプライアンスの場合は、IBM Security Web Gateway Appliance をネットワークのどこに配置するのかを決定した後、以下のタスクを実行します。

- ネットワーク・ケーブルを取り付けます。
- ローカル管理インターフェース (LMI) またはシリアル・コンソールと接続します。
- アプライアンスの初期設定を構成します。

ケーブルの接続およびアプライアンスの始動

ネットワーク上で配置する場所を決定した後に、IBM Security Web Gateway Applianceをネットワークに接続します。

手順

1. IBM Security Web Gateway Appliance に電源ケーブルを接続します。
2. アプライアンスの管理に使用するネットワークに管理インターフェース 1 を接続します。
3. ネットワーク・ケーブルをアプリケーション・インターフェースに接続します。
4. アプライアンスの電源をオンにします。

ハードウェア・アプライアンスの構成オプション

アプライアンスに接続されているシリアル・コンソール・デバイス、または LMI を使用して、ハードウェア・アプライアンスを構成できます。

LMI は、より高度な構成オプションを備えているため、推奨されるオプションです。

シリアル・コンソール・デバイスを使用するには、コンソール・デバイスをシリアル・ケーブルでハードウェア・アプライアンスに接続する必要があります。手順については、『シリアル・コンソールのアプライアンスへの接続』を参照してください。

アプライアンスを構成するために LMI を使用するには、アプライアンスの IP アドレスを参照する必要があります。 アプライアンスの IP アドレスがわからない場合は、8 ページの『システム IP アドレスの判別』の指示に従ってください。

シリアル・コンソールのアプライアンスへの接続

コマンド行インターフェース (CLI) を通じて構成タスクを開始する前に、シリアル・コンソールをハードウェア・アプライアンスに接続する必要があります。

手順

1. シリアル・ケーブルを使用して、コンソール・デバイスをハードウェア・アプライアンスに接続します。
2. コンピューターをコンソール・デバイスとして使用する場合は、Microsoft ハイパーターミナルまたは別の端末エミュレーション・プログラムで、以下の設定を使用してアプライアンスに接続します。

オプション	説明
通信ポート	通常は COM1
エミュレーション	VT100
ビット/秒	9600
データ・ビット	8
パリティー	なし
ストップ・ビット	1
フロー制御	なし

3. アプライアンスの初期設定を構成するには、10 ページの『共通タスク』 の手順にしたがってください。

システム IP アドレスの判別

LMI を使用してアプライアンスを構成する場合は、以下のいずれかの方法を使用して、アプライアンスに割り当てられた IP アドレスを判別し、LMI にアクセスできるようにします。

- **方法 1:** LCD パネルを使用して、アプライアンスの IP アドレスを判別します。
  1. LCD パネルで 「**OK**」を押して、メインメニューを表示します。

     注: 「**OK**」ボタンには、矢印のラベルが付いています。
  2. 矢印を使用して「**IP アドレス**」を選択します。
  3. 「**OK**」を押します。

     LCD パネルに IBM Security Web Gateway Appliance の IP アドレスが表示されます。アドレスをメモします。
- **方法 2:** ゼロ構成ネットワーキングを使用して、ご使用のネットワーク上でアプライアンスをディスカバーします。

  アプライアンスは、業界標準の一連の IP プロトコルを使用するため、ネットワークに物理的に接続すると、自動的にディスカバーできます。

仮想アプライアンス・タスク

仮想アプライアンスの場合は、ローカル管理インターフェースまたは仮想コンソールに接続して、アプライアンスの初期設定を構成します。

仮想ネットワークのセットアップ

アプライアンスのインストールを試みる前に、VMWare 環境を正しく構成する必要があります。アプライアンスをインストールする管理者は、VMWare ネットワーキングの概念を十分に理解する必要があります。

仮想アプライアンスのインストールでは、スクリプトまたはサイレント・モードのインストールはサポートされません。複数の仮想アプライアンスをインストールするには、最初のアプライアンスを手動でインストールし、次に VMware ESX または vSphere を使用して仮想マシンのコピーを作成します。

VMware を使用した仮想アプライアンスのインストール

付属の .iso イメージを使用して、仮想アプライアンスをインストールします。

手順

1. VMware ESX または vSphere を使用して新規仮想マシンを作成します。

   注:

   - 仮想マシンを作成する手順は、ご使用の VMware ESX または vSphere のバージョンによって異なる場合があります。具体的な手順については、ご使用のバージョンに該当する VMware 資料を参照してください。
   - 仮想マシンで、アプライアンスの構成およびログ・ファイル・データを保管するために、十分な量のディスク・スペースが割り振られていることを確認してください。アプライアンス用に少なくとも 100 GB のディスク・スペースを割り振ってください。
   - 仮想マシン・バージョンとして「**Virtual Machine Version: 7**」を指定します。
   - ゲスト・オペレーティング・システムとして「**Linux**」を指定し、ゲスト・オペレーティング・システム・バージョンとして「**Other 2.6x Linux (64-bit)**」を指定します。
   - メモリー・サイズは、作成可能な WebSEAL インスタンスの数および同時にアクティブにできるセッション数に影響します。推奨最小メモリー・サイズは 4096 MB です。
   - アプライアンスでは、4 つから 6 つの仮想ネットワーク・アダプターが必要です。最初の 2 つのネットワーク・アダプターは、管理インターフェースとして機能します。残りのネットワーク・アダプターは、アプリケーション・インターフェースとして機能します。ウィザードを使用して、4 つのネットワーク・アダプターを構成できます。追加のネットワーク・アダプターは、ウィザードの完了後に追加可能です。各ネットワーク・アダプターのタイプは「**E1000**」でなければなりません。
   - SCSI コントローラーとして、「**LSI Logic Parallel**」を選択します。
   - 仮想デバイス・ノードとして「**SCSI (0:0)**」を選択します。
2. 付属の .iso ファイルからブートするように仮想マシンを構成してから、仮想マシンを開始します。 インストーラーが自動的に実行されます。
3. インストール時に使用する言語を選択します。目的の言語に対応する数字を入力してください。

4. 「YES」と入力して、インストールを進めます。 あるいは、インストールを進めない場合は、「NO」と入力してリブート・プロンプトに移動します。
5. インストール・メッセージを調べて、正常にインストールされたことを確認します。インストール・プロセスが完了したら、インストール・メディアをアンマウントしてから、**Enter** キーを押してアプライアンスをリブートします。
6. リブート操作が終了したら、パスワード admin を使用して admin ユーザーとしてログオンすることで、コンソール・ベースのアプライアンス・セットアップ・ウィザードを開始できます。あるいは、LMI からアプライアンスのセットアップ・ウィザードにアクセスできます。

共通タスク

このタスクは、ハードウェア・アプライアンスと仮想アプライアンスの両方で共通のものです。

以下のいずれかの方法を選択して、アプライアンスの初期設定を構成できます。

- コマンド行インターフェース (CLI)
- ローカル管理インターフェース (LMI)

LMI の方法には、より詳細な構成オプションが用意されています。

コマンド行インターフェースの初期アプライアンス設定ウィザード

初期アプライアンス設定ウィザードは、未構成のアプライアンスのコマンド行インターフェース (CLI) に管理者が初めてログインしたときに実行されます。

ナビゲーション

以下のオプションを使用して、ウィザード内で画面間を移動できます。

- p: 前の画面
- n: 次の画面

任意の時点でセットアップ・プロセスをキャンセルするには、exit コマンドを使用します。

モジュール

以下のモジュールを構成して、アプライアンスをセットアップする必要があります。

モジュール	説明
ようこそ	ウィザードを使用して構成できるアプライアンス設定について説明します。
ソフトウェアのご使用条件	アプライアンスの使用許諾契約書、IBM の条件、IBM 以外の条件について説明します。
パスワード構成	パスワードを変更します。
ホスト構成	ホスト名を変更してください。

モジュール	説明
管理インターフェース設定	管理ネットワーク・インターフェースを構成します。プライマリー・インターフェースおよびセカンダリー・インターフェースのデバイス設定および現行作業セット・ポリシーが表示されます。
DNS 構成	アプライアンスで使用される DNS サーバーを構成します。
時刻構成	アプライアンスの時刻、日付、およびタイム・ゾーンを構成できます。

ローカル管理インターフェース・アプライアンスのセットアップ・ウィザード

アプライアンスのセットアップ・ウィザードは、未構成のアプライアンスのローカル管理インターフェース (LMI) に管理者が初めてログインしたときに実行されます。

LMI に初めてログインしたら、アプライアンスのセットアップ・ウィザードに従って、アプライアンスの初期構成を実行します。初期構成で実行する必要のあるタスクを以下に示します。

- ご使用条件を読み、受け入れます。
- ライセンス・ファイルをダウンロードし、インストールします。ハードウェア・アプライアンスのファームウェアおよび IBM X-Force の最新情報をダウンロードするには、ライセンスをインストールする必要があります。
- アプライアンスのパスワードを設定します。
- ホスト名、管理インターフェース設定、DNS 構成などのネットワークの構成を行います。
- アプリケーション・インターフェース設定を構成します。
- 日時の設定を構成します。

基本的な構成が完了すると、要約画面が表示されます。「完了」ページで詳細を確認し、「**セットアップの完了**」をクリックします。

第 3 章 アプライアンスの管理

アプライアンスは、その管理手段として、ローカル管理インターフェース (LMI)、コマンド行インターフェース (CLI)、および Web サービス・インターフェースという 3 つのメカニズムを備えています。

ローカル管理インターフェース

IBM Security Web Gateway Appliance は、ローカルの単一アプライアンスを管理するためのブラウザー・ベースのグラフィカル・ユーザー・インターフェースを備えています。

以下の段落は、ローカル管理インターフェース (LMI) の使用法に関する一般注意です。 LMI を使用した特定のコマンドの例については、本書の以降の部分で説明します。

LMI にログインするには、ご使用のアプライアンスの IP アドレスまたはホスト名を Web ブラウザーに入力します。以下の Web ブラウザーがサポートされています。

- Windows
  - Google Chrome バージョン 19.0 以降
  - Microsoft Internet Explorer、バージョン 9 以降
  - Mozilla Firefox バージョン 12.0 以降
- Linux/AIX®/Solaris
  - Mozilla Firefox バージョン 12 以降

初めてログインするときは、以下のデフォルトの資格情報を使用して、ローカル管理インターフェースにログインします。

- **ユーザー名:** admin
- **パスワード:** admin

初めてログインした後は、初回の構成ページを使用して、パスワードを変更してください。

ローカル管理インターフェースからログアウトするには、「**ログアウト**」をクリックします。

同時にアプライアンスにログインしたままでいることができるのは、1 人のユーザーのみです。既存のユーザー・セッションがある場合は、ログインしようとするとエラーが発生します。自分自身のユーザー・セッションでログインするためには、既存のユーザー・セッションを強制終了しておく必要があります。

注: LMI にアクセスした後にブラウザー・ウィンドウを閉じても、セッションはシステム上でアクティブのままとなります。次回 LMI にログインするときには、「**すべての既存のセッションを強制終了します**」チェック・ボックスを選択する必

要があります。既存のユーザー・セッションの強制終了について詳しくは、 135 ページの『既存のユーザー・セッションがあることによるログインの失敗』を参照してください。

コマンド行インターフェース

ssh セッションまたはコンソールを使用して、アプライアンスのコマンド行インターフェース (CLI) にアクセスします。

以下の段落は、CLI の使用法に関する一般注意です。 CLI を使用した特定のコマンドの例については、本書の以降の部分で説明します。

以下の例は、ssh セッションを使用してアプライアンスにアクセスするトランスクリプトを示しています。

```
usernameA@example.ibm.com>ssh -l admin webapp.vwasp.gc.au.ibm.com
admin@webapp.vmasp.gc.au.ibm.com's password:
Welcome to the IBM Security Web Gateway
Enter "help" for a list of available commands
webapp.vwasp.gc.au.ibm.com>
```

コンソールにアクセスする方法は、ハードウェア・アプライアンスと仮想アプライアンスとで異なります。

- ハードウェア・アプライアンスの場合は、シリアル・コンソール・デバイスを使用する必要があります。シリアル・コンソール・デバイスをハードウェアに接続する方法について詳しくは、 7 ページの『シリアル・コンソールのアプライアンスへの接続』を参照してください。
- 仮想アプライアンスの場合は、適切な VMWare ソフトウェアを使用してコンソールにアクセスできます。

  例えば、VMWare vSphere クライアント。

注: CLI には、ローカル管理インターフェースから使用できる機能のサブセットのみが組み込まれています。以下のリストは、コマンド行インターフェースから使用できる機能の概要を示しています。

- ファームウェア・イメージを処理します。
- フィックスパックを処理します。
- ハードウェア設定を処理します。
- ライセンスを処理します。
- ローカル管理インターフェースを処理します。
- 管理設定を処理します。
- ポリシー・スナップショット・ファイルを処理します。
- サポート情報ファイルを処理します。
- ネットワーク診断ツールを処理します。
- ファームウェアおよびセキュリティー・アップデートを処理します。
- Web Gateway 設定を処理します。

Web サービス

アプライアンスを管理するには、アプライアンスに RESTful Web サービス要求を送信するという方法もあります。

同時にアプライアンスにログインしたままでいることができるのは、1 人のユーザーのみです。Web サービス要求が出されるごとに、既存のセッションはすべて自動的に強制終了されます。

以下の段落は、Web サービス・インターフェースの使用法に関する一般注意です。これらの Web サービス要求の内容および形式については、本書の以降の部分で説明します。

Web サービスの呼び出しに必要なヘッダー

すべての Web サービス要求には、以下の 2 つのヘッダーを含める必要があります。

Accept:application/json
: accept ヘッダーが存在しており、その値に application/json が設定されている必要があります。ヘッダーがない場合、またはヘッダーに別の値が設定されている場合は、Web サービス要求が失敗します。

BA ヘッダー
: 各要求には、BA ヘッダーと有効なユーザー名およびパスワードが含まれている必要があります。このヘッダーがない場合は、要求が失敗します。

以下の例は、curl を使用してリバース・プロキシー・インスタンスのリストを取得するための有効な要求形式です。

```
curl -k -H "Accept:application/json" --user username:password
https://{appliance_hostname}/reverseproxy
```

注: 上記のリストでは、すべての Web サービス要求に必要な 2 つのヘッダーのみを示しました。これは、すべての要求アクションに必要なヘッダーの詳細なリストではありません。上記の例は、リソース URI に対する curl GET 要求を示しています。この要求では、リストされた 2 つの必須ヘッダーのみが必要です。他の HTTP メソッド (POST や PUT など) では、さらに多くのヘッダーが必要です。。以下の例は、curl を使用して inst1 という名前のリバース・プロキシー・インスタンスを始動するための有効な要求です。

```
curl -k -H "Accept:application/json" -H "Content-type:application/json"
--user username:password --data-binary '{ 'operation':'start' }'
-X PUT https://{appliance_hostname}/reverseproxy/inst1
```

PUT 操作に必要なヘッダー **Content-type** が追加されていることに注意してください。

他の HTTP クライアント (Java など) では、さらに多くのヘッダーが必要な場合があります。 RESTful Web サービスに必要なヘッダーについては、HTTP クライアントの資料を確認してください。

Web サービス応答

Web サービス呼び出しの応答は、HTTP 応答コードおよび JSON メッセージという 2 つのコンポーネントから構成されます。

成功した Web サービス要求の応答には、状況コード 200 と、要求処理に関するコンテキスト固有の情報を含む JSON データが入っています。失敗した Web サービス要求の応答には、HTTP エラー応答コードと、エラー・メッセージを含む JSON データが入っています。

HTTP 応答コード

表 2. HTTP エラー応答コード

コード	説明
200	成功。
400	要求に問題があります。 JSON メッセージに問題の説明があります。
404	要求で指定されたリソースは存在しません。 JSON メッセージには、どのリソースであるかが示されます。
500	要求が処理されている間に内部エラーが起きました。JSON メッセージに問題を示します。

JSON エラー応答フォーマット

```
{"message":"The error message"}
```

第 4 章 ホーム: アプライアンス・ダッシュボード

アプライアンスのローカル管理インターフェースには、一連のダッシュボード・ウィジェットが用意されています。これらのウィジェットを使用して、よく使用されるシステム情報を表示できます。

これらのウィジェットは、ログイン直後に表示されます。これらのウィジェットは、メニューバーの「**ホーム: アプライアンス・ダッシュボード**」をクリックしてアクセスすることもできます。

システム通知の表示

「通知」ダッシュボード・ウィジェットを使用して、潜在的な問題に関する警告情報を表示できます。

手順

1. ダッシュボードから「通知」ウィジェットを見つけます。 以下の潜在的な問題に関する警告メッセージが表示されます。
   - まもなく有効期限切れになる証明書。
   - 現在実行されていないリバース・プロキシー・インスタンス。
   - ディスク・スペース使用率が警告しきい値を超えている。
   - CPU 使用率が警告しきい値を超えている。
2. 必要に応じて、適切なアクションを実行します。

リバース・プロキシーの正常性状況の表示

リバース・プロキシーの正常性状況は、インスタンス、Junction、および Junction サーバーの状態によって決定されます。「リバース・プロキシーの正常性」ダッシュボード・ウィジェットを使用して、正常性状況情報を表示できます。

手順

1. ダッシュボードから「リバース・プロキシーの正常性」ウィジェットを見つけます。

   各インスタンス、その Junction、および Junction サーバーの正常性状況が階層構造で表示されます。正常性状況は、階層内の現在のエレメントよりも低いエレメントすべての正常性によって決定されます。
   - インスタンスが正常ではないのは、そのインスタンスが停止している場合、または pdadmin がそのインスタンスに接続できない場合です。
   - Junction が正常ではないのは、Junction が使用不可になっている場合、または pdadmin がその情報を返すことができない場合です。
   - Junction サーバーが正常でないのは、そのサーバーが使用不可になっているかオフラインになっている場合です。

   各エレメントは、以下の 3 つのいずれかの正常性状況になります。

アイコン	状態	説明
	正常	すべての子エレメントが正常です。
	警告	エレメントに、少なくとも 1 つの正常ではない子エレメント、および少なくとも 1 つの正常な子エレメントが含まれています。
	正常でない	どの子エレメントも正常ではありません。

2. *オプション:*「**最新表示**」をクリックして、正常性データを最新表示します。

ディスク使用量の表示

「ディスク使用量」ダッシュボード・ウィジェットを使用して、ディスク・スペース状況および残りのディスク存続情報を表示できます。

手順

1. ダッシュボードから「ディスク使用量」ウィジェットを見つけます。

   ディスク・スペースの円グラフ
   使用されているディスク・スペースおよび空きディスク・スペースに関する情報が、円グラフで視覚化されます。

   消費ディスク・スペース
   既に使用されているスペース量 (GB)。

   注: 通常、ほとんどのディスク・スペースは、ログ・ファイルおよびトレース・ファイルによって使用されます。ディスク・フットプリントを最小化するには、ログ・ファイルおよびトレース・ファイルをリモート・サーバーに保管するよう、アプライアンスを設定してください。使用されていないログ・ファイルおよびトレース・ファイルを定期的にクリアするのもよい方法です。

   空きディスク・スペース
   空きスペース量 (GB)。

   合計ディスク・スペース
   アプライアンスで使用可能な合計スペース量 (GB)。

   注: ハードウェア・アプライアンスのディスク・スペースは、搭載されているハード・ディスクの容量によって制限されます。

2. *オプション:*「**最新表示**」をクリックして、データを最新表示にします。

IP アドレスの表示

「インターフェース」ダッシュボード・ウィジェットを使用して、アプライアンスが listen している IP アドレスの、カテゴリー化されたリストを表示できます。

手順

1. ダッシュボードから「インターフェース」ウィジェットを見つけます。 すべての使用可能になっているインターフェースおよび構成されているインターフェースの IP アドレスが、フロントエンド・ロード・バランサーで管理されている仮想 IP アドレスとともに表示されます。

   管理 IP
   使用可能になっている/構成されている管理インターフェース (M.1、M.2) の IP アドレスのリスト。

   アプリケーション IP
   使用可能になっている/構成されているアプリケーション・インターフェース (P.1、P.2、P.3、P.4) の IP アドレスのリスト。

   ロード・バランサー IP
   ロード・バランサー・サービスの IP アドレスのリスト。

2. オプション:「**最新表示**」をクリックして、データを最新表示にします。

フロントエンド・ロード・バランサーの正常性状況の表示

フロントエンド・ロード・バランサーの正常性状況は、ロード・バランス・サーバーの状態によって決定されます。「ロード・バランサーの正常性」ダッシュボード・ウィジェットを使用して、正常性状況情報を表示できます。

手順

1. ダッシュボードから「ロード・バランサーの正常性」ウィジェットを見つけます。
   - 「**高可用性**」は以下のようになっています (高可用性が構成されている場合)。
     - 最初の行に、セルフ・フロントエンド・ロード・バランサーの正常性状況、およびそのバランサーがアクティブかパッシブかが表示されます。
     - 2 番目の行に、ピア・フロントエンド・ロード・バランサーの正常性状況、およびそのバランサーがアクティブかパッシブかが表示されます。
   - 「**サービス**」は以下のようになっています (少なくとも 1 つのサービスが構成されている場合)。
     - 構成されているサービスおよびロード・バランス・サーバーの正常性状況が、階層構造で表示されます。サービスを展開して、そのサービスに関連付けられているサーバーの正常性状況を表示できます。

   各エレメントは、以下のいずれかの正常性状況になります。

アイコン	状態	説明
	正常	すべての子エレメントが正常です。
	警告	エレメントに、少なくとも 1 つの正常ではない子エレメント、および少なくとも 1 つの正常な子エレメントが含まれています。
	正常でない	どの子エレメントも正常ではありません。

2. *オプション:*「**最新表示**」をクリックして、正常性データを最新表示します。

平均応答時間の統計の表示

トランザクション・ログを記録するよう Web リバース・プロキシーを構成できます。記録される属性の 1 つは、平均要求応答時間です。この情報は、Junction レベルごとに記録されます。記録された平均応答時間の要約を表示するには、「平均応答時間」ウィジェットを使用します。

手順

1. ダッシュボードから「平均応答時間」ウィジェットを見つけます。 要求への平均応答時間がグラフに表示されます。

   注: このウィジェットが表示されるのは、1 つ以上のリバース・プロキシー・インスタンスでフロー・データ機能が使用可能になっている場合のみです。
2. 「**リバース・プロキシー・インスタンス**」で、平均応答時間統計を表示するインスタンスを選択します。
3. 「**Junction**」で、グラフに表示する Junction を選択します。各 Junction は、グラフ上の個別の行で表されます。
4. 「**日付範囲**」で、応答時間が記録されている期間を選択します。

セキュリティー・アクションの統計の表示

Web リバース・プロキシーは、Web コンテンツに対して検査を実行して、潜在的な悪意を持つ要求 (問題として既知) を検索するよう構成できます。これにより、ディスカバーされた問題に対し、特定の防御アクションを実行できます。「セキュリティー・アクション」ウィジェットを使用して、実行された防御アクションの要約を表示できます。

手順

1. ダッシュボードから「セキュリティー・アクション」ウィジェットを見つけます。各防御アクションについて実行された回数が、グラフに表示されます。

   注: このウィジェットが表示されるのは、1 つ以上のインスタンスでセキュリティー統計機能が使用可能になっている場合のみです。
2. 「**リバース・プロキシー・インスタンス**」で、アクション統計を表示するインスタンスを選択します。

   注: セキュリティー統計機能が使用可能になっているインスタンスのみが、選択用にリストされます。
3. 「**アクション**」で、統計に含めるアクションを選択します。表示されるアクションの数は、選択したすべてのアクションの合計です。
4. 「**日付範囲**」で、アクションが実行された期間を選択します。

証明書の有効期限の表示

証明書の詳細は、「証明書の有効期限」ウィジェットで表示できます。

手順

1. ダッシュボードから「証明書の有効期限」ウィジェットを探します。 証明書に関する詳細が表示されています。

   証明書ラベル
   証明書のラベル

   有効期限
   証明書の有効期限が切れる日付

   タイプ 証明書のタイプ。

   鍵データベース
   証明書が属する鍵データベースの名前。
2. *オプション:* 「**最新表示**」をクリックして、データを最新表示します。

区画情報の表示

「区画情報」ウィジェットを使用して、アクティブ区画およびバックアップ区画に関する情報を表示できます。

手順

1. ダッシュボードから「区画情報」ウィジェットを見つけます。 アクティブ区画およびバックアップ区画に関する詳細が表示されます。

   ファームウェア・バージョン
   アプライアンス・ファームウェアのバージョン情報

   インストール日
   アプライアンス・ファームウェアがインストールされた日付

   インストール・タイプ
   アプライアンス・ファームウェア・インストールのタイプ

   最終ブート
   アプライアンスが最後にブートされた時刻
2. *オプション:* 「**ファームウェア設定**」をクリックして、ファームウェアの設定を変更するためのページに移動します。

リバース・プロキシーのスループットの表示

「リバース・プロキシーのスループット」ウィジェットを使用して、アプライアンス全体レベルでフロー・データを表示できます。

手順

1. ダッシュボードから「リバース・プロキシーのスループット」ウィジェットを見つけます。
2. 「**データ範囲**」リストを使用して、データを収集して表示する期間を選択します。

   デフォルトでは、このアプライアンス上に構成されているすべての WebSEAL インスタンスの過去 24 時間のデータが表示されます。
3. *オプション:*「**最新表示**」をクリックして、データを最新表示にします。

ネットワーク・トラフィックの表示

「ネットワーク・トラフィック」ウィジェットを使用して、過去 1 時間のネットワーク・トラフィックを表示できます。

手順

1. ダッシュボードから「ネットワーク・トラフィック」ウィジェットを見つけます。 過去 1 時間の「**入力 (In)**」および「**出力 (Out)**」トラフィック詳細が表示されます。
2. *オプション:* 「**P.1**」、「**P.2**」、「**P.3**」、または「**P.4**」をクリックすると、特定のインターフェースの詳細が表示されます。

第 5 章 モニター: 分析および診断

Security Web Gateway Appliance では、正常性および統計をモニターすることが可能です。

イベント・ログの表示

システム設定が変更された場合、および問題がシステムで発生した場合に、システム・イベントがログに記録されます。システム・イベントを表示するには、「イベント・ログ」管理ページを使用します。

手順

1. 「**モニター: 分析および診断**」 > 「**ログ**」 > 「**イベント・ログ**」をクリックします。 システム・イベントが表示されます。
2. イベント・ログのライブ更新を停止するには、「**ライブ・ストリーミングの一時停止**」をクリックします。
3. イベント・ログのライブ更新を再開するには、「**ライブ・ストリーミングの開始**」をクリックします。

リバース・プロキシー・ログ・ファイルの管理

「リバース・プロキシー・ログ・ファイルの管理」管理ページを使用して、リバース・プロキシー・ログ・ファイルを処理します。

手順

1. 上部のメニューから、「**モニター: 分析および診断**」 > 「**ログ**」 > 「**リバース・プロキシー・ログ・ファイルの管理**」を選択します。 「**選択したインスタンスのログ・ファイル**」に、すべての共通ログ・ファイルの詳細が表示されます。

   「**名前**」の下にあるフィルター・バーを使用して、特定の条件を満たすエントリーをフィルタリングすることができます。「**フィルターのクリア**」をクリックすると、完全なリストに戻ります。
2. オプション: インスタンス固有のログ・ファイルを対象にする場合は、「**リバース・プロキシー・インスタンス**」の下のリストから、そのインスタンスを選択します。 「**選択したインスタンスのログ・ファイル**」に、すべての共通ログ・ファイルおよびインスタンス固有のログ・ファイルの詳細が表示されます。
3. リバース・プロキシー・ログ・ファイルを処理します。
   - **リバース・プロキシー・ログ・ファイルの内容の表示**
     a. 表示するログ・ファイルを選択します。
     b. 「**表示**」をクリックします。ログ・ファイルの内容が表示されます。ファイルが 100 行よりも長い場合、デフォルトでは、ログ・ファイルの最後の 100 行が表示されます。表示する行数を定義するには、「**表示行数**」フィールドに数値を入力してから、「**再ロード**」をクリックします。オプションとして、「**開始行**」フィールドに値を指定して、行の開始を定義できま

す。「**開始行**」フィールドが設定されている場合、「**表示行数**」フィールドは開始行からの順方向の表示行数を決定します。「**開始行**」フィールドが設定されていない場合、「**表示行数**」フィールドはログ・ファイルの末尾からの表示行数を決定します。

注: 返すことができる最大サイズは、214800000 行です。これよりも大きいサイズを指定した場合は、この最大サイズ (214800000 行) が返されます。

c. *オプション:* 「**エクスポート**」をクリックして、ログ・ファイルをダウンロードします。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

- **リバース・プロキシー・ログ・ファイルのエクスポート**
  a. エクスポートするログ・ファイルを選択します。
  b. 「**管理**」 > 「**エクスポート**」をクリックします。

  注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
  c. ブラウザー・ウィンドウで保存操作を確定して、ファイルをローカル・ロケーションにエクスポートします。
- **リバース・プロキシー・ログ・ファイルのクリア**
  a. クリアするログ・ファイルを選択します。
  b. 「**クリア**」をクリックします。
  c. 「アクションの確認」確認ページで、「**はい**」をクリックします。

メモリーの統計情報の表示

メモリー・グラフを表示して、Security Web Gateway Appliance のメモリー使用率を確認します。

手順

1. 「**モニター: 分析および診断**」 > 「**システム・グラフ**」 > 「**メモリー**」をクリックします。
2. 以下の中から「**表示範囲**」を選択します。

オプション	説明
1 日	過去 24 時間の 1 分ごとのデータ・ポイントを表示します。
3 日	過去 3 日の 5 分ごとのデータ・ポイントを表示します。各データ・ポイントは、その 1 時間に発生したアクティビティーの平均です。

オプション	説明
7 日	過去 7 日の 20 分ごとのデータ・ポイントを表示します。各データ・ポイントは、その 1 時間に発生したアクティビティーの平均です。
30 日	過去 30 日の 1 時間ごとのデータ・ポイントを表示します。各データ・ポイントは、その 1 時間に発生したアクティビティーの平均です。

3. 「凡例」ボックスの「**使用メモリー**」を選択して、全体のメモリー使用状況を確認します。

CPU 使用率の表示

CPU グラフを表示して、Security Web Gateway Appliance の CPU 使用率を確認します。

手順

1. 「**モニター: 分析および診断**」 > 「**システム・グラフ**」 > 「**CPU**」をクリックします。
2. 以下の中から「**表示範囲**」を選択します。

オプション	説明
1 日	過去 24 時間の 1 分ごとのデータ・ポイントを表示します。
3 日	過去 3 日の 5 分ごとのデータ・ポイントを表示します。各データ・ポイントは、その 1 時間に発生したアクティビティーの平均です。
7 日	過去 7 日の 20 分ごとのデータ・ポイントを表示します。各データ・ポイントは、その 1 時間に発生したアクティビティーの平均です。
30 日	過去 30 日の 1 時間ごとのデータ・ポイントを表示します。各データ・ポイントは、その 1 時間に発生したアクティビティーの平均です。

3. 「凡例」ボックスで、以下の中から確認する CPU 使用率データを選択します。
   - ユーザー
   - システム
   - アイドル

ストレージ使用率の表示

ストレージ・グラフを表示して、Security Web Gateway Appliance のブート・パーティションおよびルート・パーティションで使用されているディスク・スペースのパーセンテージを確認します。

手順

1. **「モニター: 分析および診断」** > **「システム・グラフ」** > **「ストレージ」**をクリックします。
2. 以下の中から**「表示範囲」**を選択します。

オプション	説明
1 日	過去 24 時間の 1 分ごとのデータ・ポイントを表示します。
3 日	過去 3 日の 5 分ごとのデータ・ポイントを表示します。各データ・ポイントは、その 1 時間に発生したアクティビティーの平均です。
7 日	過去 7 日の 20 分ごとのデータ・ポイントを表示します。各データ・ポイントは、その 1 時間に発生したアクティビティーの平均です。
30 日	過去 30 日の 1 時間ごとのデータ・ポイントを表示します。各データ・ポイントは、その 1 時間に発生したアクティビティーの平均です。

3. 「凡例」ボックスで、確認するパーティションを選択します。

   ブート ブート・パーティション。

   ルート システム・ユーザーが root である基本ファイル・システム。

アプリケーション・インターフェース統計の表示

アプリケーション・インターフェースで使用されている帯域幅およびフレームを表示するには、「アプリケーション・インターフェース統計」管理ページを使用します。

手順

1. 上部のメニューから、**「モニター: 分析および診断」** > **「ネットワーク・グラフ」** > **「アプリケーション・インターフェース統計」**を選択します。
2. **「日付範囲」**フィールドで、統計を表示する期間を選択します。

オプション	説明
1 日	1 日の 20 分間隔ごとのデータが表示されます。
3 日	過去 3 日の 20 分間隔ごとのデータが表示されます。

オプション	説明
7 日	過去 7 日の 20 分間隔ごとのデータが表示されます。
30 日	過去 30 日の毎日のデータが表示されます。

リバース・プロキシーのトラフィックの表示

ローカル管理インターフェースを使用してインスタンス固有レベルでフロー・データを表示するには、「リバース・プロキシーのトラフィック」管理ページを使用します。

手順

1. 上部のメニューから、**「モニター: 分析および診断」 > 「リバース・プロキシーのグラフ」 > 「リバース・プロキシーのトラフィック」**を選択します。
2. 「リバース・プロキシーのトラフィック」ページで、表示されるグラフの設定を指定します。

   インスタンス
   表示されるデータが属するインスタンス。

   アスペクト・タイプ (Aspect Type)
   データを表示するために使用するグラフのタイプ。**「列と行 (Column and Lines)」**、**「列 (Column)」**、および**「行 (Lines)」**のいずれかから選択します。

   開始日 開始する日。

   開始時刻
   開始する時刻。

   日付範囲
   データを収集して表示する対象期間。**「1 時間」**から**「30 日」**までの間から選択します。

   例えば、選択された日時が `04.12.2012 10.00` で、期間が **「12 時間」**の場合、2012 年 4 月 12 日の午前 10:00 から午後 10:00 までに収集されたデータが表示されます。

   デフォルトでは、過去 24 時間における、インスタンス・リスト内の最初のインスタンスのデータが、Junction でグループ化されて表示されます。

リバース・プロキシーのスループットの表示

ローカル管理インターフェースを使用してアプライアンス全体レベルでフロー・データを表示するには、「リバース・プロキシーのスループット」管理ページを使用します。

手順

1. 上部のメニューから、**「モニター: 分析および診断」 > 「リバース・プロキシーのグラフ」 > 「リバース・プロキシーのスループット」**を選択します。

2. 「リバース・プロキシーのスループット」ページで、表示されるグラフの設定を指定します。

   グラフ・タイプ (Chart Type)
   データを表示するために使用するグラフのタイプ。「**列と行 (Column and Lines)**」、「**列 (Column)**」、および「**行 (Lines)**」のいずれかから選択します。

   日付範囲
   データを収集して表示する対象期間。「**1 時間**」から「**30 日**」までの間から選択します。

   開始日 開始する日。

   開始時刻
   開始する時刻。

   例えば、選択された日時が `04.12.2012 10.00` で、期間が 「`12 時間`」の場合、2012 年 4 月 12 日の午前 10:00 から午後 10:00 までに収集されたデータが表示されます。

   デフォルトでは、このアプライアンス上に構成されているすべての WebSEAL インスタンスの過去 24 時間のデータが表示されます。

コマンド行インターフェースを使用した Web リバース・プロキシーのログ・ファイルのアーカイブおよび削除

Web リバース・プロキシーのログ・ファイルを USB デバイスにアーカイブしたり、古いログ・ファイルを削除してディスク・スペースを解放したりするには、コマンド行インターフェースで `logs` オプションを使用します。

手順

1. コマンド行インターフェースで、**wga > logs** に移動します。
2. *オプション:* すべての使用可能なコマンドを表示するには、`help` を入力します。

```
Current mode commands:
archive         Archive the log files to a USB device.
delete          Delete the log files which have been rolled over by the system.
Global commands:
back            Return to the previous command mode.
exit            Log off from the appliance.
help            Display information for using the specified command.
reboot          Reboot the appliance.
shutdown        End system operation and turn off the power.
top             Return to the top level.
```

3. ログ・ファイルをアーカイブまたは削除します。
   - **USB デバイスにログ・ファイルをアーカイブします。**
     a. USB デバイスにログ・ファイルを保存するために`archive` と入力します。
     b. USB デバイスをアプライアンスの USB ポートに挿入します。
     c. `YES` と入力して、アーカイブ操作を開始します。アーカイブされたファイルのリストが表示され、アーカイブ操作が完了したことを示すメッセージが表示されます。出力例を以下に示します。

```
updating: var/PolicyDirector/log/ (stored 0%)
updating: var/PolicyDirector/log/msg__pdmgrd_utf8.log (deflated 85%)
updating: var/PolicyDirector/log/PDMgr_config_start.log (deflated 37%)
updating: var/PolicyDirector/log/ivmgrd.pid (stored 0%)
updating: var/pdweb/default/log/ (stored 0%)
updating: var/pdweb/default/log/iss-pam1.so (deflated 59%)
updating: var/pdweb/default/log/webseald-default.pid (stored 0%)
updating: var/pdweb/default/log/config_data__default
-webseald-felbb.wga.gc.au.ibm.com.log (deflated 92%)
updating: var/pdweb/default/log/referer.log (stored 0%)
updating: var/pdweb/default/log/msg__webseald-default.log (deflated 89%)
updating: var/pdweb/default/log/pam.log (deflated 98%)
updating: var/pdweb/default/log/agent.log (stored 0%)
updating: var/pdweb/default/log/request.log (stored 0%)
The log files have been successfully archived to the USB drive:
iswga_logs.zip. It is now safe to remove the USB drive.
```

d. USB ポートから USB デバイスを取り外します。

- **ログ・ファイルを削除します。**

  a. ロールオーバーされたログ・ファイルをすべて消去するために `delete` と入力します。

  b. `YES` と入力して、削除操作を確定します。

第 6 章 セキュア: リバース・プロキシー設定

リバース・プロキシー設定を管理するには、アプライアンスを使用します。

設定のいくつかは、すべてのリバース・プロキシー・インスタンスにグローバルに適用されます。その他の設定は、特定のインスタンスに固有のものです。以下のトピックで詳細を参照してください。

マイグレーション

ソフトウェアとして実行中の WebSEAL インスタンスをアプライアンスにマイグレーションすることが可能です。

注: 各環境は異なります。 WebSEAL インスタンスのマイグレーションを支援するツールが提供されていますが、管理者はマイグレーション・プロセスを理解し、ツールを適切に構成する責任があります。

マイグレーション・ステップの概要を以下に示します。

準備

1. カスタム・ライブラリーの CDAS または EAS は、サポートされていません。システムのマイグレーションを開始する前に、カスタム・ライブラリーの CDAS または EAS への依存関係がないことを確認してください。例えば、カスタム CDAS 処理がある場合は、EAI に変換する必要があります。
2. ローカル junction がサポートされますが、固定ロケーションが文書ルートとして使用されます。また、ローカル junction は、CGI スクリプトの実行が許可されていません。静的ページ・コンテンツのみ提供できます。すべての CGI スクリプトをリモート・サーバーにマイグレーションする必要があります。アプライアンスは、単一のローカル junction のみをサポートします。その他のすべてのローカル junction (ある場合) のコンテンツもリモート・サーバーにマイグレーションする必要があります。
3. ソース WebSEAL サーバー上で、以下の表に示す構成ファイルのディレクトリー構造を作成します。ファイルをマイグレーションするディレクトリーのみを作成する必要があります。これらのディレクトリーは、単一のソース・ディレクトリーの下のサブディレクトリーとして作成します。

表 3. ディレクトリー構造

ディレクトリー	ディレクトリー
dynurl	動的 URL 構成ファイル。
fsso	フォーム・ベースのシングル・サインオン構成ファイル。
jmt	Junction マッピング・テーブル構成ファイル。
keytab	WebSEAL インスタンスで使用される鍵データベース (kdb/sth) ファイル。ポリシー・サーバーと通信するために使用される鍵ファイルは含まれません。
ltpa-keys	LTPA 鍵ファイル

表 3. ディレクトリー構造 (続き)

ディレクトリー	ディレクトリー
tam-keys	**cdsso-key-gen** ユーティリティーで生成される鍵ファイル。フェイルオーバー Cookie の暗号化などに使用されます。
xslt/user-map-cdas	クライアント証明書のユーザー・マッピング CDAS で使用される XSLT 構成ファイル。
xslt/http-transformation	HTTP 変換ルール機能で使用される XSLT 構成ファイル。
doc-root/docs	WebSEAL ローカル junction によって提供されるファイル。通常、このファイルは、/opt/pdweb/www-<instance>/lib/docs ディレクトリーの下に配置されます。
doc-root/errors	WebSEAL インスタンスによって提供されるエラー・ページ。通常、これらのファイルは、/opt/pdweb/www-*<instance>*/lib/errors ディレクトリーの下に配置されます。
doc-root/html	WebSEAL インスタンスによって提供される管理 HTML ページ (login.html など)。通常、このファイルは、/opt/pdweb/www-*<instance>*/lib/html ディレクトリーの下に配置されます。
doc-root/oauth	WebSEAL 構成ファイルの [oauth-eas] スタンザ内で定義される OAuth 応答ファイル。
junctions	WebSEAL インスタンスの junction 定義を含む XML ファイル。通常、これらのファイルは、/opt/pdweb/www-*<instance>*/jct ディレクトリーの下に配置されます。
etc	WebSEAL インスタンスで使用される構成ファイル。具体的には、ルーティング・ファイル、webseald-<instance>.conf ファイル、および webseald-<instance>.conf.obf ファイルです。

注: ディレクトリー構造を作成する場合、ディレクトリーへのサブディレクトリーの追加はサポートされませんが、doc-root のサブディレクトリー (doc-root/docs、doc-root/errors、doc-root/html、doc-root/oauth) はサポートされます。例えば、/doc-root/error/<folder>/<file> のようなディレクトリー構造は作成できますが、xslt/http-transformation/<folder>/<file> のような構造は無効です。 doc-root 以外のディレクトリーでは、 31 ページの表 3 に示すデフォルトのルート・ディレクトリーにのみファイルを配置できます。例えば、xslt/http-transformation/<file> です。

注: コピーするすべてのファイルには、固有のファイル名が必要です。 2 つのファイルの名前が同じ場合、マイグレーション・ツールは、名前が一致した最初のファイルのみをコピーします。例えば、以下のような構造があるとします。

```
[http-transformation]
request_pop1 = <path1>/pop1.xsl
response_pop1 = <path2>/pop1.xsl
```

ディレクトリー構造には、<path1>/pop1.xsl のみが作成されます。構成ファイル内の <path1>/pop1.xsl と <path2>/pop1.xsl に対するすべての参照は pop1.xsl に変更され、これが同じファイルを指すようになります。

ファイル収集用の Perl ユーティリティー

WebSEAL インスタンスで必要なファイルを容易に収集できる Perl ユーティリティーが提供されています。このユーティリティーでは、指定された WebSEAL

インスタンスの構成を処理できます。また、Web Gateway Appliance のインポート機能で要求されたディレクトリー構造に、必要なファイルをコピーすることもできます。

このユーティリティーを設定および実行するには、以下のステップを実行します。

a. Perl スクリプトを取得するために、以下の URL にあるアプライアンスから Perl スクリプトをダウンロードします。

```
https://<appliance>/reverseproxy/wga_migrate.pl
```

b. スクリプトを WebSEAL サーバーにコピーします。

c. Perl が WebSEAL サーバーにインストールされ、使用可能であることを確認します。

d. マイグレーションする WebSEAL インスタンスの構成ファイルの名前を探します。

e. WebSEAL 構成ファイル名と宛先ディレクトリーを指定して wga_migrate.pl スクリプトを実行します。スクリプトを使用する際の形式を以下に示します。

```
perl wga_migrate.pl [-c config-file] [-d dst-dir] {-v}
```

-c *config-file*	WebSEAL構成ファイルの名前。
-d *dst-dir*	宛先ディレクトリーの名前。このディレクトリーは、ファイル・システム上に存在してはなりません。
-v	スクリプトの実行中により多くの状況メッセージを表示します。

例えば、以下のとおりです。

```
perl wga_migrate.pl -c /var/pdweb/etc/webseald-default.conf
-d /tmp/migrate_out
```

f. 宛先ディレクトリーに含まれているファイルを調べて、必要なファイルがすべて配置されていることを確認します。

4. マイグレーションする一連の構成ファイルに WebSEAL 構成ファイルが含まれている必要があります。また、[configuration-database] スタンザと **file** 構成エントリーで定義済みの難読化された構成ファイルも含まれている必要があります。難読化されたデータベースの名前 (webseald-<instance>.conf.obf) は変更しないでください。難読化されたデータベースのファイル名が異なる場合は、デフォルトの名前に戻し、構成エントリーをそれに応じて更新します。

5. コピーされた WebSEAL 構成ファイルを変更して、新しい WebSEAL インスタンスに適用されない構成エントリーをすべて削除します。マイグレーションしない可能性のあるエントリーの例としては、ネットワーク設定などがあります。構成ファイルをアプライアンスにインポートする場合、以下の構成エントリーは無視されます。

   - [authentication-levels] スタンザからの **token-card** 構成エントリー
   - [server] スタンザからの **server-name** 構成エントリー
   - [server] スタンザからの **network-interface** 構成エントリー
   - [interfaces] 構成スタンザ

6. コピー対象ファイルの格納場所を基準にして各コンテンツが配置された圧縮ファイルを作成します。例えば、ディレクトリー構造を /tmp/migrate に作成した場合、コマンドは以下のようになります。

   ```
   cd /tmp/migrate; zip -r /tmp/migrate.zip *
   ```

マイグレーション

マイグレーション圧縮ファイルが使用可能になると、マイグレーションを開始できます。

1. ローカル管理インターフェースを使用して、新しい WebSEAL インスタンスをアプライアンス上に作成します。このインスタンスの名前は、マイグレーションするインスタンスの名前と同じにする必要があります。
2. マイグレーション圧縮ファイルをインポートします。

   注: インポート操作の一環としてファイルが上書きされる可能性があると警告された場合は、上書き操作について検証してから続行する必要があります。アプライアンス上で実行中の他の WebSEAL インスタンスに上書き操作の影響が及ばないことを確認してください。ローカル管理インターフェースを使用してインポートを行う場合の詳しいステップについては、『管理ページ・ルートへの .zip ファイルの内容のインポート』を参照してください。
3. 変更内容をデプロイします。
4. WebSEAL インスタンスを再始動します。
5. WebSEAL ログ・ファイルにマイグレーションに関する潜在的な問題がないかどうかを検査します。

構成変更のコミット・プロセス

LMI では、アプライアンスを変更したときに 2 ステージ・コミット・プロセスが使用されます。

ステージ 1
: 変更が LMI を使用して行われ、ステージング・エリアに保存されます。

ステージ 2
: ユーザーが明示的に変更を実稼働環境にデプロイします。

同時に複数の変更が保留状態で存在できます。これらの変更は、ユーザーがデプロイまたはロールバックしたときに一度にコミットまたはロールバックされます。

変更によって、実行中のリバース・プロキシー・インスタンスに影響が及ぶ場合は、変更を有効にする前に、影響を受けるインスタンスを再始動する必要があります。

特定のアプライアンスの更新では、変更を有効にする前に、アプライアンスまたは Web サーバーを再始動する必要があります。これらの更新の 1 つ以上を他のリバース・プロキシーの更新と一緒に行う場合は、リバース・プロキシーの更新をデプロイするために追加のステップが必要です。必ず以下を行ってください。

1. すべての更新をデプロイします。
2. アプライアンスまたはWeb サーバーを再始動します。

3. 残りの更新をデプロイします。

保留中の変更および実動ファイルの間に矛盾がある場合、保留中のすべての変更は自動的にロールバックされ、実動ファイルは未変更のままとなります。

Web サービス

保留中の構成変更のデプロイ

URL

```
https://{appliance_hostname}/pending_changes/deploy
```

メソッド

```
GET
```

パラメーター

N/A

応答

HTTP 応答コードおよび JSON エラー応答 (該当する場合)

注: Web サービス呼び出しから返される可能性があるエラー応答については、16 ページの『Web サービス応答』を参照してください。

例

要求:

```
GET https://{appliance_hostname}/pending_changes/deploy
```

応答:

```
200 ok
```

保留中の構成変更のロールバック

URL

```
https://{appliance_hostname}/pending_changes/forget
```

メソッド

```
GET
```

パラメーター

N/A

応答

HTTP 応答コードおよび JSON エラー応答 (該当する場合)

注: Web サービス呼び出しから返される可能性があるエラー応答については、16 ページの『Web サービス応答』を参照してください。

例

要求:

```
GET https://{appliance_hostname}/pending_changes/forget
```

応答:

```
200 ok
```

未処理の変更の数の取得

URL

```
https://{appliance_hostname}/pending_changes/count
```

メソッド

```
GET
```

パラメーター

N/A

応答

HTTP 応答コード、および保留中の変更の数を表す JSON データ。

注: Web サービス呼び出しから返される可能性があるエラー応答については、16 ページの『Web サービス応答』を参照してください。

例

要求:

```
GET https://{appliance_hostname}/pending_changes/count
```

応答:

```
{"count": 3}
```

未処理の変更のリストの取得

URL

```
https://{appliance_hostname}/pending_changes
```

メソッド

```
GET
```

パラメーター

N/A

応答

HTTP 応答コード、および保留中の変更のリストを表す JSON データ。

注: Web サービス呼び出しから返される可能性があるエラー応答については、16 ページの『Web サービス応答』を参照してください。

例

要求:

```
GET https://{appliance_hostname}/pending_changes
```

応答:

```
200 ok

[{
"id": 0,
"policy": "SSL Certificates",
"user": "admin",
"date": "2012-11-05T11:22:20+10:00"
}]
```

注: Web サービス要求では、 15 ページの『Web サービスの呼び出しに必要なヘッダー』で説明されている形式を使用する必要があります。

ローカル管理インターフェース

保留中の変更がある場合は、メイン・ペインの上部に警告メッセージが表示されます。保留中の変更をデプロイまたはロールバックするには、以下のステップを実行します。

1. 警告メッセージ内の「**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**」リンクをクリックします。
2. 「保留中の変更の適用」ページでは、以下のことを行います。
   - 特定のモジュールに対する変更の詳細を表示するには、そのモジュールのリンクをクリックします。
   - 変更をデプロイするには、「**デプロイ**」をクリックしてください。
   - 変更を中止するには、「**ロールバック**」をクリックします。
   - 変更に対するアクションを実行せずにポップアップ・ページを閉じるには、「**キャンセル**」をクリックします。

ランタイム・コンポーネントの管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」「**管理**」「**ランタイム・コンポーネント**」を選択します。

ランタイム環境構成状況の表示

ローカル管理インターフェースを使用してランタイム環境構成状況を表示するには、「ランタイム・コンポーネント」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**ランタイム・コンポーネント**」を選択します。
2. ランタイム環境の構成状況が表示されます。

ランタイム構成ファイルの管理

ローカル管理インターフェースを使用して構成ファイルを管理するには、「ランタイム・コンポーネント」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**ランタイム・コンポーネント**」を選択します。
2. 「**編集**」をクリックします。
3. 対象のランタイム構成ファイルを選択します。
4. 構成ファイルを編集し、「**保存**」をクリックして変更を保存します。変更を保存しない場合は、「**キャンセル**」をクリックします。前のバージョンの構成ファイルに戻す場合は、「**元に戻す**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

ランタイム環境の構成

ローカル管理インターフェースを使用してランタイム環境を構成するには、「ランタイム・コンポーネント」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「管理」** > **「ランタイム・コンポーネント」**を選択します。
2. **「構成」**をクリックします。 ポリシー・サーバーはローカルまたはリモートとして構成できます。
   - **リモート LDAP ユーザー・レジストリーを使用したローカル・ポリシー・サーバー**
     a. **「ポリシー・サーバー」**で**「ローカル」**を選択します。
     b. **「ユーザー・レジストリー」**で**「LDAP リモート」**を選択します。
     c. **「次へ」**をクリックします。
     d. 「ポリシー・サーバー」タブで、表示されたフィールドに設定を指定します。アスタリスクが付いているフィールドは必須なので、入力する必要があります。
        – **管理サフィックス**: IBM Security Access Manager secAuthority データを保持するために使用する LDAP サフィックス。
        – **管理ドメイン**: IBM Security Access Manager のドメイン名。
        – **アドミニストレーター・パスワード**: セキュリティー・アドミニストレーターのパスワード。
        – **アドミニストレーター・パスワードの確認**: セキュリティー・アドミニストレーターのパスワード。
        – **SSL サーバー証明書の存続期間 (日)**: SSL サーバー証明書の存続期間 (日数)。
        – **SSL 準拠性**: 任意の追加 SSL 準拠性を指定します。
     e. **「次へ」**をクリックします。
     f. 「LDAP」タブで、表示されたフィールドに設定を指定します。
        – **ホスト名**: LDAP サーバーの名前。
        – **ポート**: システムが LDAP サーバーと通信する際に使用するポート。
        – **DN**: システムがユーザー・レジストリーに接続する際に使用する識別名。
        – **パスワード**: DN のパスワード。
        – **SSL を使用可能にする**: SSL を使用可能にするかどうか。
        – **証明書データベース**: ユーザー・レジストリーとの通信に使用される証明書が含まれている KDB ファイル。「SSL を使用可能にする」が選択されている場合は、このフィールドは必須です。
        – **証明書ラベル**: 要求時にユーザー・レジストリーに提示される SSL 証明書のラベル。このフィールドはオプションです。SSL が使用可能になっ

ていて、かつユーザー・レジストリーがクライアント証明書を要求するように構成されている場合にのみ必須です。

g. 「**終了**」をクリックして、設定を保存します。

- **ローカル・ユーザー・レジストリーを使用したローカル・ポリシー・サーバー**

  注: ローカル・ユーザー・レジストリー内のユーザーおよびグループは、Security Access Manager 管理フレームワーク (例えば、pdadmin) を使用して管理します。これらのすべてのユーザーおよびグループは、サフィックス「dc=iswga」の下に格納されます。

  a. 「**ポリシー・サーバー**」で「**ローカル**」を選択します。

  b. 「**ユーザー・レジストリー**」で、「**LDAP ローカル**」を選択します。

  c. 「**次へ**」をクリックします。

  d. 「ポリシー・サーバー」タブで、表示されたフィールドに設定を指定します。アスタリスクが付いているフィールドは必須なので、入力する必要があります。

     – **アドミニストレーター・パスワード**: セキュリティー・アドミニストレーターのパスワード。

     – **アドミニストレーター・パスワードの確認**: セキュリティー・アドミニストレーターのパスワード。

     – **SSL サーバー証明書の存続期間 (日)**: SSL サーバー証明書の存続期間 (日数)。

     – **SSL 準拠性**: 任意の追加 SSL 準拠性を指定します。

  e. 「**終了**」をクリックして、設定を保存します。

- **リモート・ポリシー・サーバー**

  a. 「**ポリシー・サーバー**」で、「**リモート**」を選択します。

  b. 「**ユーザー・レジストリー**」で、「**LDAP**」を使用するのか、「**Active Directory**」を使用するのかを選択します。

  c. 「**次へ**」をクリックします。

  d. 「ポリシー・サーバー」タブで、表示されたフィールドに設定を指定します。

     – **ホスト名**: IBM Security Access Manager Policy Server をホストするホストの名前。

     – **ポート**:IBM Security Access Manager Policy Server との通信が行われるポート。

     – **管理ドメイン**: IBM Security Access Manager のドメイン名。

  e. 「**次へ**」をクリックします。

     – 上記ステップでユーザー・レジストリーとして「**LDAP**」を選択した場合は、「**LDAP**」タブで設定を行います。

       - **ホスト名**: LDAP サーバーの名前。

       - **ポート**: システムが LDAP サーバーと通信する際に使用するポート。

     – 上記ステップでユーザー・レジストリーとして「**Active Directory**」を選択した場合は、「**Active Directory**」タブおよび「**Active Directory SSL**」タブで設定を行います。

1) 「**Active Directory**」タブで、以下の項目の設定を指定します。
   - **ホスト名**:Active Directory サーバーの名前。
   - **ドメイン**: Active Directory ドメインの名前。
   - **Active Directory マルチ・ドメイン環境で IBM Security Access Manager を構成します**: 環境をマルチ・ドメイン Active Directory に対して構成するかどうか。
   - **IBM Security Access Manager データを保管するための識別名 (DN)**: Security Access Manager データを保管するために使用される、Active Directory 内の DN。
   - **E メール・アドレスをユーザー ID として使用する**: Security Access Manager ユーザー ID として E メール・アドレスを使用するかどうか。
   - **Global Catalog サーバー・ホスト名**: Active Directory グローバル・カタログ・サーバーの名前。
2) 「**次へ**」をクリックします。
3) 「**Active Directory SSL**」タブで、以下の項目の設定を指定します。
   - **SSL を使用可能にする**: Active Directory サーバーに SSL を介して通信するかどうか。
   - **SSL 鍵ファイル**: ユーザー・レジストリーとの通信に使用される証明書が含まれている KDB ファイル。「SSL を使用可能にする」が選択されている場合は、このフィールドは必須です。
   - **証明書ラベル**: システムがユーザー・レジストリーと通信する際に使用する SSL 証明書のラベル。このフィールドはオプションであり、有効になるのは、SSL 鍵ファイルを入力した場合のみです。

f. 「**終了**」をクリックして、設定を保存します。

ランタイム環境の構成解除

ローカル管理インターフェースを使用してアプライアンスのランタイム環境コンポーネントを構成解除するには、「ランタイム・コンポーネント」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**ランタイム・コンポーネント**」を選択します。
2. 「**構成解除**」をクリックします。
3. 以下の一連のアクションのいずれかを実行します。
   - **リモート LDAP ユーザー・レジストリーを使用したローカル・ポリシー・サーバーの構成解除**
     a. LDAP DN および LDAP パスワードを入力します。
     b. 構成解除操作で Security Access Manager のドメイン、ユーザー、およびグループの情報をすべて削除する場合は、「**ユーザー・レジストリー項目のクリア**」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・ボックスは選択されていません。

c. 構成解除操作ですべての構成データを強制的に削除する場合は、「**強制的に実行**」チェック・ボックスをクリックします。デフォルトではこのチェック・ボックスは選択されていません。

注: 「**強制的に実行**」チェック・ボックスを選択するのは、何度構成解除を行っても失敗する場合のみにしてください。このオプションを使用するのは、最後の手段としてのみです。

d. 「**送信**」をクリックして、操作を確定します。

- **ローカル・ユーザー・レジストリーを使用したローカル・ポリシー・サーバーの構成解除**

a. 構成解除操作で Security Access Manager のドメイン、ユーザー、およびグループの情報をすべて削除する場合は、「**ユーザー・レジストリー項目のクリア**」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・ボックスは選択されていません。

b. 構成解除操作ですべての構成データを強制的に削除する場合は、「**強制的に実行**」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・ボックスは選択されていません。

注: 「**強制的に実行**」チェック・ボックスを選択するのは、何度構成解除を行っても失敗する場合のみにしてください。このオプションを使用するのは、最後の手段としてのみです。

c. 「**送信**」をクリックして、操作を確定します。

- **リモート・ポリシー・サーバーの構成解除**

a. 構成解除操作ですべての構成データを強制的に削除する場合は、「**強制的に実行**」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・ボックスは選択されていません。

注: 「**強制的に実行**」チェック・ボックスを選択するのは、何度構成解除を行っても失敗する場合のみにしてください。このオプションを使用するのは、最後の手段としてのみです。

b. 「**送信**」をクリックして、操作を確定します。

リバース・プロキシーの管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。

インスタンスの管理

Web リバース・プロキシー・インスタンスを制御および構成するには、IBM Web Security Gateway Appliance のローカル管理インターフェースを使用します。

リバース・プロキシーの概念について詳しくは、「*IBM Security Access Manager for Web WebSEAL 管理ガイド*」(SC23-6505-03) を参照してください。

すべてのインスタンスの現在の状態の表示

ローカル管理インターフェースを使用してすべてのインスタンスの現在の状態を表示するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. すべてのインスタンスの現在の状態およびバージョン情報を表示できます。

インスタンスの停止、開始、または再始動

ローカル管理インターフェースを使用してインスタンスを停止、開始、または再始動するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 対象のインスタンスを選択します。

   インスタンスの停止

   a. 「**停止**」をクリックします。
   b. インスタンスが正常に停止されたことを示すメッセージが表示されます。

   インスタンスの開始

   a. 「**開始**」をクリックします。
   b. インスタンスが正常に開始されたことを示すメッセージが表示されます。

   インスタンスの再始動

   a. 「**再始動**」をクリックします。
   b. インスタンスが正常に再始動されたことを示すメッセージが表示されます。

インスタンスの構成

ローカル管理インターフェースを使用してインスタンスを構成するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 「**新規**」をクリックします。
3. 「**インスタンス**」、「**IBM Security Access Manager**」、「**トランスポート**」、および「**ユーザー・レジストリー**」の各タブに表示されたフィールドの設定を指定します。
   - 「**インスタンス**」タブでは、以下を指定します。

フィールド	説明
インスタンス名	これは、インスタンスを識別する固有の名前である新規インスタンス名です。複数のインスタンスを同じコンピューター・システムにインストールできます。それぞれのインスタンスに固有の名前がなければなりません。

フィールド	説明
ホスト名	IBM Security Access Manager Policy Server がアプライアンスとの接続に使用するホスト名。このホスト名に対応するアドレスは、アプライアンスの管理インターフェースのアドレスに一致している必要があります。アプライアンスのアプリケーション・インターフェースに関連付けられているアドレスは、IBM Security Access Manager Policy Server との通信には使用できません。 有効な値には、有効なホスト名または IP アドレスが含まれます。例: libra.dallas.ibm.com
listen ポート	これは、インスタンスが Security Access Manager Policy Server と通信する際に使用する listen ポートです。
プライマリー・インターフェースの IP アドレス	論理インターフェースの IP アドレス。

- 「**IBM Security Access Manager**」 タブでは、以下を指定します。

フィールド	説明
アドミニストレーター名	Security Access Manager アドミニストレーター名。
アドミニストレーター・パスワード	Security Access Manager アドミニストレーター・パスワード。
ドメイン	Security Access Manager ドメイン。

- 「**トランスポート**」タブでは、以下を指定します。

フィールド	説明
HTTP を使用可能にする	HTTP プロトコルを使用してユーザー要求を受け入れるかどうかを指定します。
HTTP ポート	HTTP 要求を listen するポート。このフィールドが有効なのは、「**HTTP を使用可能にする**」チェック・ボックスが選択されている場合のみです。
HTTPS を使用可能にする	HTTPS プロトコルを使用してユーザー要求を受け入れるかどうかを指定します。
HTTPS ポート	HTTPS 要求を listen するポート。このフィールドが有効なのは、「**HTTPS を使用可能にする**」チェック・ボックスが選択されている場合のみです。

- 「**ユーザー・レジストリー**」タブでは、以下を指定します。

フィールド	説明
SSL を使用可能にする	インスタンスと LDAP サーバーとの間の SSL 通信を使用可能にするかどうかを指定します。
鍵ファイル名	LDAP SSL 証明書が入るファイルです。このフィールドが有効なのは、「**SSL を使用可能にする**」チェック・ボックスが選択されている場合のみです。

フィールド	説明
証明書ラベル	LDAP クライアントの証明書ラベルです。このフィールドが有効なのは、「**SSL を使用可能にする**」チェック・ボックスが選択されている場合のみです。
ポート	LDAP サーバーとの通信に使用されるポート番号。このフィールドが有効なのは、「**SSL を使用可能にする**」チェック・ボックスが選択されている場合のみです。

4. 「**終了**」をクリックしてください。 インスタンスが正常に構成されたことを示すメッセージが表示されます。

インスタンスの構成解除

ローカル管理インターフェースを使用してインスタンスを構成解除するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 構成解除するインスタンスを選択します。
3. 「**削除**」をクリックします。
4. アドミニストレーター名とパスワードを入力します。
5. 「**削除**」をクリックします。

注: 何度構成解除を行っても失敗する場合は、「**強制的に実行**」チェック・ボックスを選択してください。このオプションを使用するのは、最後の手段としてのみです。

構成エントリーおよびファイル管理

構成エントリーおよび構成ファイルの設定を管理するには、IBM Web Security Gateway Appliance のローカル管理インターフェース (LMI) を使用します。

Web リバース・プロキシー構成エントリーの管理

Web リバース・プロキシーの基本構成を管理するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 対象のインスタンスを選択します。
3. 「**編集**」を選択します。
4. 「**サーバー**」、「**SSL**」、「**Junction**」、「**認証**」、「**SSO**」、「**セッション**」、「**応答**」、「**ロギング**」、「**インターフェース**」の各タブで設定を変更します。

   サーバー

   「サーバー」タブには、一般的なサーバー構成に関する項目が含まれています。

フィールド	説明
HTTPS	リバース・プロキシー内で HTTPS ポートを使用可能にする場合は、このチェック・ボックスを選択します。
HTTPS ポート	リバース・プロキシーが HTTPS 要求を listen するポート。
HTTP	リバース・プロキシー内で HTTP ポートを使用可能にする場合は、このチェック・ボックスを選択します。
HTTP ポート	リバース・プロキシーが HTTP 要求を listen するポート。
インターフェース・アドレス	リバース・プロキシー・サーバーが要求を listen するネットワーク・インターフェース。
持続接続のタイムアウト	クライアントとの持続接続が非アクティブであることを許容する最大秒数。これを過ぎると、持続接続はサーバーによって閉じられます。
ワーカー・スレッド	サービス要求に割り当てられるスレッドの数。
クラスターはマスターです	リバース・プロキシーのクラスタリング機能を使用する場合、このチェック・ボックスにより、このリバース・プロキシー・サーバーがクラスター・マスターとして機能するかどうかを制御します。
マスター・インスタンス名	クラスター内でマスターとして機能するリバース・プロキシー・インスタンスのサーバー名。このオプションは、「**クラスターはマスターです**」チェック・ボックスを選択していない場合にのみ使用可能です。
メッセージのロケール	リバース・プロキシーが実行されるロケール。

SSL　「SSL」タブには、サーバーの一般的な SSL 構成に関する項目が含まれています。

フィールド	説明
SSL 証明書鍵ファイル	リバース・プロキシーによってクライアントに提示される証明書を保管するために使用する鍵データベース。
SSL サーバー証明書	クライアントに提示される SSL 証明書の、鍵データベースでの名前。
JCT 証明書鍵ファイル	リバース・プロキシーによって Junction Web サーバーに提示される証明書を保管するために使用する鍵データベース。

Junction

「Junction」タブには、一般的な Junction 構成に関する項目が含まれています。

フィールド	説明
HTTP タイムアウト	TCP Junction との間で送信および読み取りを行うときのタイムアウト (秒)。
HTTPS タイムアウト	SSL Junction との間で送信および読み取りを行うときのタイムアウト (秒)。
ping 間隔	Junction Web サーバーの状態を判別するためにリバース・プロキシーによって Junction Web サーバーに要求が送信される間隔(秒)。

フィールド	説明
ping の方式	正常性検査要求を Junction Web サーバーに送信するときにリバース・プロキシーが使用する HTTP メソッド。
ping URI	正常性検査要求を Junction Web サーバーに送信するときにリバース・プロキシーが使用する URI。
キャッシュに入れる持続接続の最大数	後で使用するためにキャッシュに入れる、リバース・プロキシーと Junction Web サーバーの間の接続の最大数。
持続接続のタイムアウト	キャッシュに入れられた、Junction Web サーバーとの接続がアイドル状態であることを許容する最大時間 (秒)。これを過ぎると、接続はリバース・プロキシーによって閉じられます。
管理 Cookie list	リバース・プロキシー Cookie JAR に格納される Cookie の、パターン・マッチング用の Cookie 名をコンマで区切ったリスト。その他の Cookie は、リバース・プロキシーによってクライアントに返されます。

認証 「認証」タブには、サーバーによって使用される認証メカニズムの構成に関する項目が含まれています。

基本認証

フィールド	説明
トランスポート	基本認証をサポートするトランスポート。
レルム名	基本認証のレルム名。

フォーム認証

フィールド	説明
フォーム認証	フォーム認証をサポートするトランスポート。

クライアント証明書認証

フィールド	説明
クライアント証明書の受け入れ	リバース・プロキシーがクライアント証明書を要求する条件を定義します。
証明書 EAI URI	外部クライアント証明書認証を実行するために呼び出すアプリケーションのリソース ID。
証明書データ	EAI アプリケーションに渡されるクライアント証明書データ。

Kerberos 認証

フィールド	説明
トランスポート	Kerberos 認証をサポートするトランスポート。
キータブ・ファイル	Kerberos キータブ・ファイルの名前。キータブ・ファイルには、SPNEGO 認証に使用される各サービス・プリンシパル名が含まれていなければなりません。

フィールド	説明
Kerberos サービス名	サーバー用に使用される Kerberos サービス・プリンシパル名のリスト。 リスト内の最初のサービス名が、デフォルトのサービス名です。あるサービス名をデフォルトにするには、そのサービス名を選択してから「**デフォルト**」をクリックします。

EAI 認証

フィールド	説明
トランスポート	EAI 認証をサポートするトランスポート。
トリガー URL	応答の EAI 認証ヘッダーを調べるかどうかを決定するためにリバース・プロキシーで使用される URL パターン。
認証レベル	それぞれの構成認証メカニズムに指定された認証レベル。

セッション

「セッション」タブには、一般的なセッション構成に関する項目が含まれています。

フィールド	説明
非アクティブの場合の再認証	非アクティブ状態が原因でサーバー資格情報キャッシュ内のユーザーのエントリーがタイムアウトになった場合に、再認証するようにユーザーにプロンプトを出すかどうか。
最大キャッシュ・エントリー数	セッション・キャッシュ内の並行エントリーの最大数。
存続期間タイムアウト	セッション・キャッシュ内のエントリーの最大存続期間 (秒)。
非アクティブ・タイムアウト	セッション・キャッシュから削除するまでの、セッションがアイドル状態であることを許容する最大時間 (秒)。
TCP セッション Cookie 名	HTTP セッション ID を保持するために使用する Cookie の名前。
SSL セッション Cookie 名	HTTPS セッション ID を保持するために使用する Cookie の名前。
同じセッションを使用	HTTP 要求と HTTPS 要求の両方に同じセッションを使用するには、このチェック・ボックスを選択します。

応答　「応答」タブには、応答生成に関する項目が含まれています。

フィールド	説明
HTML リダイレクトを使用可能にする	HTML リダイレクト機能を使用可能にする場合は、このチェック・ボックスを選択します。
ローカル応答リダイレクトを使用可能にする	ローカル応答リダイレクト機能を使用可能にする場合は、このチェック・ボックスを選択します。

フィールド	説明
ローカル応答リダイレクト URI	ローカル応答リダイレクトが使用可能である場合は、このフィールドに、リバース・プロキシー応答でクライアントがリダイレクトされる URI が含まれます。
ローカル応答リダイレクト・マクロ	ローカル応答リダイレクトに含めるマクロ情報。

SSO 「SSO」タブには、サーバーによって使用される各種シングル・サインオン・メカニズムの構成に関する項目が含まれています。

フェイルオーバー

フィールド	説明
トランスポート	フェイルオーバー認証をサポートするトランスポート。
Cookie の存続期間	フェイルオーバー Cookie の最大存続期間 (秒)。
Cookie 鍵ファイル	フェイルオーバー Cookie の暗号化に使用する鍵ファイル。

LTPA

フィールド	説明
トランスポート	LTPA 認証をサポートするトランスポート。
Cookie 名	LTPA トークンのトランスポートに使用する Cookie の名前。
鍵ファイル	LTPA Cookie にアクセスするときに使用する鍵ファイル。
鍵ファイル - パスワード	LTPA 鍵ファイルにアクセスするために使用するパスワード。

CDSSO

フィールド	説明
トランスポート	CDSSO 認証をサポートするトランスポート。
トランスポート (生成)	CDSSO トークンの作成をサポートするトランスポート。
ピア	CDSSO ドメインに参加している他のリバース・プロキシー・サーバーの名前。リバース・プロキシー・サーバーで使用される鍵ファイルの名前とともに表示されます。

ECSSO

フィールド	説明
トランスポート	e-community SSO 認証をサポートするトランスポート。
名前	e-community の名前。
マスター認証サーバーかどうか	このリバース・プロキシー・サーバーが e-community のマスターである場合は、このチェック・ボックスを選択します。
マスター認証サーバー	e-community のマスターとして機能するリバース・プロキシー・サーバーの名前。このリバース・プロキシー・サーバーをマスターとして指定した場合、このフィールドは必須ではありません。

フィールド	説明
ドメイン・キー	e-community に参加している他のリバース・プロキシー・サーバーの名前。各種リバース・プロキシー・サーバーで使用される鍵ファイルの名前とともに表示されます。

ロギング

「ロギング」タブには、ロギングおよび監査の構成に関する項目が含まれています。

フィールド	説明
エージェントのロギングを使用可能にする	エージェント・ログを使用可能にするには、このチェック・ボックスを選択します。
リファラーのロギングを使用可能にする	リファラー・ログを使用可能にするには、このチェック・ボックスを選択します。
要求のロギングを使用可能にする	要求ログを使用可能にするには、このチェック・ボックスを選択します。
要求のログ形式	要求ログ内に含まれているエントリーの形式。
最大ログ・サイズ	ログ・ファイルの最大サイズ。このサイズに達すると、ファイルがロールオーバーされます。
フラッシュ時刻	リバース・プロキシーがログ・エントリーをキャッシュに入れる期間 (秒)。この期間が過ぎると、システムはエントリーをログ・ファイルに書き込みます。
監査ログを使用可能にする	監査イベントの生成を使用可能にするには、このチェック・ボックスを選択します。
監査ログ・タイプ	監査するイベントを選択します。
監査ログ・サイズ	監査ログ・ファイルの最大サイズ。このサイズに達すると、ファイルがロールオーバーされます。
監査ログのフラッシュ	リバース・プロキシーが監査ログ・エントリーをキャッシュに入れる期間 (秒)。この期間が過ぎると、システムはエントリーをログ・ファイルに書き込みます。

インターフェース

「インターフェース」タブには、WebSEAL セカンダリー・インターフェースに関する設定が含まれています。

- 新規セカンダリー・インターフェースを追加するには、「**新規**」をクリックします。次に、以下のフィールドが含まれているポップアップ・ウィンドウで設定を定義します。

フィールド	説明
アプリケーション・インターフェースの IP アドレス	WebSEAL インスタンスが要求を listen する IP アドレス。
HTTP ポート	このフィールドには、WebSEAL インスタンスが HTTP 要求を listen するポートが含まれます。

フィールド	説明
HTTPS ポート	このフィールドには、WebSEAL インスタンスが HTTPS 要求を listen するポートが含まれます。
Web HTTP ポート	これは、WebSEAL によって使用されるとクライアントが見なすポートです。
Web HTTP プロトコル	これは、WebSEAL によって使用されるとクライアントが見なすプロトコルです。
証明書ラベル	WebSEAL インスタンスによってクライアントに提示される SSL サーバー証明書のラベル。
クライアント証明書の受け入れ	WebSEAL がクライアント証明書を要求する条件を定義します。
ワーカー・スレッド	サービス要求に割り当てるスレッドの数。

「**保存**」をクリックして、設定を保存します。

- セカンダリー・インターフェースを削除するには、インターフェースを選択してから、「**削除**」をクリックします。
- セカンダリー・インターフェースを編集するには、インターフェースを選択してから、「**編集**」をクリックします。次に、前述したフィールドが含まれているポップアップ・ウィンドウで設定を更新します。

5. 「**保存**」をクリックして、変更を適用します。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

Web リバース・プロキシー構成ファイルの管理

ローカル管理インターフェースを使用してリバース・プロキシー構成を管理するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 対象のインスタンスを選択します。
3. 「**管理**」 > 「**構成**」 > 「**構成ファイルの編集**」を選択します。
4. 表示された構成ファイルを編集してから、「**保存**」をクリックして変更を保存します。変更を保存しない場合は、「**キャンセル**」をクリックします。前のバージョンの構成ファイルに戻す場合は、「**元に戻す**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

管理ページ・ルートの処理

ローカル管理インターフェースを使用して、管理ページ・ルートのファイルおよびディレクトリーを管理するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 対象のインスタンスを選択します。
3. 「**管理**」 > 「**管理ルート**」を選択します。 現在のすべての管理ファイルおよび管理ディレクトリーが表示されます。デフォルト・ディレクトリーには、以下のものが含まれています。

   管理 Web リバース・プロキシー管理ページ。例えば、`login.html` です。

   エラー Web リバース・プロキシーで返されることがあるエラー・ページ。

   oauth oauth モジュールで返されることがある HTML ファイル。

   Junction ルート
   Web リバース・プロキシーのローカル Junction によって提供される静的 HTML ファイル。

   注: 固定ロケーションが、文書ルートとして使用されます。ローカル Junction は CGI スクリプトを実行できません。静的ページ・コンテンツのみ提供できます。
4. すべての管理ファイルおよび管理ディレクトリーを処理します。
   - **管理ページ・ルートでの新規ファイルの作成**
     a. ファイルの作成先のディレクトリーを選択します。
     b. 「**ファイル**」 > 「**新規**」 > 「**ファイル**」を選択します。
     c. ファイル名を入力します。
     d. オプションとして、「**新しいファイル内容**」フィールドにファイル内容を追加できます。
     e. 「**保存**」をクリックします。

     注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。
   - **管理ページ・ルートでの新規ディレクトリーの作成**
     a. ディレクトリーの作成先のディレクトリーを選択します。
     b. 「**ファイル**」 > 「**新規**」 > 「**ディレクトリー**」を選択します。
     c. ディレクトリー名を入力します。
     d. 「**保存**」をクリックします。

     注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。
   - **管理ページ・ルート内のファイルの内容の表示または更新**
     a. 対象のファイルを選択します。
     b. 「**ファイル**」 > 「**開く**」を選択します。ファイルの内容を表示できます。
     c. オプションとして、ファイルの内容を編集します。次に「**保存**」をクリックします。

     注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

- **管理ページ・ルートからのファイルのエクスポート**
  a. 対象のファイルを選択します。
  b. 「**管理**」 > 「**エクスポート**」を選択します。

     注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
  c. ブラウザーで確認ウィンドウが表示されたら、保存操作を確定します。
- **管理ページ・ルート内のファイルまたはディレクトリーの名前変更**
  a. 対象のファイルまたはディレクトリーを選択します。
  b. 「**管理**」 > 「**名前変更**」を選択します。
  c. 「**新規リソース名**」フィールドにファイルまたはディレクトリーの新規名を入力します。
  d. 「**保存**」をクリックします。

     注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。
- **管理ページ・ルート内のファイルまたはディレクトリーの削除**
  a. 対象のファイルまたはディレクトリーを選択します。
  b. 「**管理**」 > 「**削除**」を選択します。
  c. 「**はい**」をクリックして削除操作を確定します。

     注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。
- **管理ページ・ルートへのファイルのインポート**
  a. ファイルのインポート先のディレクトリーを選択します。
  b. 「**管理**」 > 「**インポート**」を選択します。
  c. 「**参照**」をクリックします。
  d. インポートするファイルを参照してから、「**開く**」をクリックします。
  e. 「**インポート**」をクリックします。
- **管理ページ・ルートへの .zip ファイルの内容のインポート**
  a. 「**管理**」 > 「**Zip のインポート**」を選択します。
  b. 「**参照**」をクリックします。
  c. インポートする .zip ファイルを参照してから、「**開く**」をクリックします。
  d. 「**インポート**」をクリックします。
- **.zip ファイルとしての管理ページ・ルートの内容のエクスポート**
  a. 「**管理**」 > 「**Zip のエクスポート**」を選択します。

     注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
  b. ブラウザーで確認ウィンドウが表示されたら、保存操作を確定します。

トレース制御

トレースを制御するには、IBM Web Security Gateway Appliance のローカル管理インターフェース (LMI) を使用します。

トレース・データは主に、IBM Software Support が使用することを意図して作成されています。トレース・データは、報告された問題の診断処理の一環として要求される場合もあります。しかし、経験のある製品アドミニストレーターなら、トレース・データを使用して IBM Security Access Manager 環境における問題の診断および修正を行うことができます。トレース・イベント・ロギングについて詳しくは、「*IBM Security Access Manager Troubleshooting Guide*」を参照してください。

注: 十分注意してトレースを使用してください。これは、IBM ソフトウェア・サポートの指示のもとで使用する手段として提供されています。トレースからのメッセージは、ときに分かりにくく、未翻訳であり、システム・パフォーマンスを大幅に低下させる場合があります。

すべてのトレース・コンポーネントおよび状況のリスト

ローカル管理インターフェースを使用してすべてのトレース・コンポーネント、その現行レベル、およびトレース・ファイル・サイズをリストするには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「管理」** > **「リバース・プロキシー」**を選択します。
2. 対象のインスタンスを選択します。
3. **「管理」** > **「トラブルシューティング」** > **「トレース」**を選択します。 すべてのトレース・コンポーネント、その現行レベル、およびトレース・ファイル・サイズが表示されます。

コンポーネントのトレース・レベル、フラッシュ間隔、およびロールオーバー・サイズの変更

コンポーネントのトレース・レベル、フラッシュ間隔、およびロールオーバー・サイズを変更するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「管理」** > **「リバース・プロキシー」**を選択します。
2. 対象のインスタンスを選択します。
3. **「管理」** > **「トラブルシューティング」** > **「トレース」**を選択します。 すべてのトレース・コンポーネント、その現行レベル、およびトレース・ファイル・サイズが表示されます。
4. 変更するコンポーネントを選択してから、**「編集」**をクリックします。
5. トレース・レベル、フラッシュ間隔、およびロールオーバー・サイズを変更します。
6. **「保存」**をクリックします。

コンポーネントのトレース・ファイルの管理

コンポーネントのトレース・ファイルおよびロールオーバー・ファイルを管理するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 対象のインスタンスを選択します。
3. 「**管理**」 > 「**トラブルシューティング**」 > 「**トレース**」を選択します。
4. トレース・ファイルおよびロールオーバー・ファイルをリストする対象のコンポーネントを選択します。次に、「**ファイル**」をクリックします。 このコンポーネントのすべてのトレース・ファイルおよびロールオーバー・ファイルのファイル名、ファイル・サイズ、および最終変更時刻情報が表示されます。

   トレース・ファイルまたはロールオーバー・ファイルの表示またはエクスポート

   a. 対象のファイルを選択します。
   b. 「**表示**」をクリックします。トレース・ファイルの内容が表示されます。特定の行数のトレースを表示するには、「**表示行数**」フィールドに値を指定してから、「**再ロード**」をクリックします。オプションとして、「**開始行**」フィールドに値を指定して、行の開始を定義できます。「**開始行**」フィールドが設定されている場合は、「**表示行数**」フィールドは、開始行からの順方向の表示行数を決定します。「**開始行**」フィールドが設定されていない場合は、「**表示行数**」フィールドは、ログ・ファイルの末尾からの表示行数を決定します。

      注: 返すことができる最大サイズは、214800000 行です。これよりも大きいサイズを指定した場合は、この最大サイズ (214800000 行) が返されます。
   c. ファイルをエクスポートする場合は、「**エクスポート**」をクリックします。

      注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
   d. ブラウザーでファイルを保存するように求めるプロンプトが出されたら、保存操作を確定します。

   トレース・ファイルまたはロールオーバー・ファイルの削除

   a. 対象のファイルを選択します。

      注: 削除できるのは、使用されていないファイルのみです。
   b. 「**削除**」をクリックします。
   c. 「**はい**」をクリックして、操作を確定します。

   トレース・ファイルまたはロールオーバー・ファイルのエクスポート

   a. 対象のファイルを選択します。
   b. 「**管理**」 > 「**エクスポート**」をクリックします。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

c. ブラウザーでファイルを保存するように求めるプロンプトが出されたら、保存操作を確定します。

使用されていないすべてのトレース・ファイルおよびロールオーバー・ファイルの削除

a. 「**管理**」 > 「**すべて削除**」をクリックします。

b. 「**はい**」をクリックして、操作を確定します。

ロギング

リバース・プロキシーのログ・ファイルを管理するには、IBM Web Security Gateway Appliance のローカル管理インターフェース (LMI) を使用します。

すべてのログ・ファイルの名前およびファイル・サイズのリスト表示

ローカル管理インターフェースを使用して、すべてのログ・ファイルの名前およびファイル・サイズをリストするには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. *オプション:* インスタンス固有のログ・ファイルが対象である場合は、そのインスタンスを選択します。
3. 「**管理**」 > 「**ロギング**」を選択します。 インスタンスが選択されている場合は、すべての共通ログ・ファイルおよびインスタンス固有のログ・ファイルの詳細が表示されます。インスタンスが選択されていない場合は、共通ログ・ファイルの詳細のみが表示されます。

   「**名前**」の下にあるフィルター・バーを使用して、特定の条件を満たすエントリーをフィルタリングすることができます。「**フィルターのクリア**」をクリックすると、完全なリストに戻ります。

ログ・ファイルの断片の表示またはログ・ファイルのエクスポート

ローカル管理インターフェースを使用してログ・ファイルの断片を表示するか、ログ・ファイルをエクスポートするには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. *オプション:* インスタンス固有のログ・ファイルが対象である場合は、そのインスタンスを選択します。
3. 「**管理**」 > 「**ロギング**」を選択します。
4. 表示するログ・ファイルを選択します。

5. 「**表示**」をクリックします。 ログ・ファイルの内容が表示されます。ログ・ファイルが 100 行よりも長い場合、デフォルトでは、ログ・ファイルの最後の 100 行が表示されます。表示する行数を定義するには、「**表示行数**」フィールドに数値を入力してから、「**再ロード**」をクリックします。オプションとして、「**開始行**」フィールドに値を指定して、行の開始を定義できます。「**開始行**」フィールドが設定されている場合、「**表示行数**」フィールドは、開始行からの順方向の表示行数を決定します。「**開始行**」フィールドが設定されていない場合、「**表示行数**」フィールドは、ログ・ファイルの末尾からの表示行数を決定します。

   注: 返すことができる最大サイズは、214800000 行です。これよりも大きいサイズを指定した場合は、この最大サイズ (214800000 行) が返されます。
6. 「**エクスポート**」をクリックして、ログ・ファイルをダウンロードします。

   注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

   ファイルを選択してから「**管理**」 > 「**エクスポート**」をクリックすることで、ファイルをエクスポートすることもできます。

ログ・ファイルのクリア

ローカル管理インターフェースを使用して、ログ・ファイルをクリアし、そのサイズを 0 にするには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. *オプション:* インスタンス固有のログ・ファイルが対象である場合は、そのインスタンスを選択します。
3. 「**管理**」 > 「**ロギング**」を選択します。
4. クリアするログ・ファイルを選択します。
5. 「**クリア**」をクリックします。
6. 「アクションの確認」確認ページで、「**はい**」をクリックします。

統計制御

統計を管理するには、IBM Web Security Gateway Appliance のローカル管理インターフェース (LMI) を使用します。

すべての統計コンポーネントおよびその詳細の取得

ローカル管理インターフェースを使用してすべての統計コンポーネントの詳細を取得するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 対象のインスタンスを選択します。

3. 「**管理**」 > 「**トラブルシューティング**」 > 「**統計**」を選択します。 すべての統計コンポーネント、およびその状況、間隔、カウント、合計累積統計ログ・ファイル・サイズ、フラッシュ間隔、ロールオーバー・サイズが表示されます。

コンポーネントの統計設定の変更

ローカル管理インターフェースを使用して特定のコンポーネントの統計設定を変更するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 対象のインスタンスを選択します。
3. 「**管理**」 > 「**トラブルシューティング**」 > 「**統計**」を選択します。
4. 変更する統計コンポーネントを選択します。
5. 「**編集**」をクリックします。
6. 「**使用可能**」の横のチェック・ボックスにまだチェック・マークが付いていない場合は、そのチェック・ボックスを選択します。
7. 必要に応じて、「**間隔**」、「**カウント**」、「**フラッシュ間隔**」、および「**ロールオーバー・サイズ**」の各フィールドを変更します。
8. 「**保存**」をクリックして、変更内容を保存します。

統計ログ・ファイルの管理

ローカル管理インターフェースを使用して統計ログ・ファイルを管理するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 対象のインスタンスを選択します。
3. 「**管理**」 > 「**トラブルシューティング**」 > 「**統計**」を選択します。
4. 対象の統計コンポーネントを選択します。
5. 「**ファイル**」をクリックします。 すべての統計ログ・ファイルのファイル名、ファイル・サイズ、および最終変更時刻情報が表示されます。
   - **統計ログ・ファイルまたは統計ログ・ファイルの断片の表示**
     a. 表示する統計ログ・ファイルを選択してから、「**表示**」をクリックします。統計ログ・ファイルの内容が表示されます。
     b. 「**表示行数**」フィールドに値を入力してから、「**再ロード**」をクリックすることで、ログ・ファイルのカスタマイズされた断片を表示できます。オプションとして、「**開始行**」フィールドに値を指定して、行の開始を定義できます。「**開始行**」フィールドが設定されている場合は、「**表示行数**」フィールドは、開始行からの順方向の表示行数を決定します。「**開始行**」フィールドが設定されていない場合は、「**表示行数**」フィールドは、ログ・ファイルの末尾からの表示行数を決定します。

注: 返すことができる最大サイズは、214800000 行です。これよりも大きいサイズを指定した場合は、この最大サイズ (214800000 行) が返されます。

- **統計ログ・ファイルのエクスポート**
  a. エクスポートする統計ログ・ファイルを選択します。
  b. 「**管理**」 > 「**エクスポート**」をクリックします。

     注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
  c. 表示されたブラウザー・ウィンドウで保存操作を確定します。
- **統計ログ・ファイルの削除**
  a. 削除する統計ログ・ファイルを選択し、「**削除**」をクリックします。

     注: 削除できるのは、使用されていないログ・ファイルのみです。ログ・ファイルを使用不可にするには、ログ・ファイルを選択し、「**編集**」をクリックし、「**使用可能**」チェック・ボックスをクリアしてから、「**保存**」をクリックします。
  b. 「**はい**」をクリックして、操作を確定します。
- **使用されていないすべての統計ログ・ファイルの削除**
  a. 「**管理**」 > 「**すべて削除**」をクリックします。
  b. 「**はい**」をクリックして、操作を確定します。

ルーティング・コントロール・ファイルの更新

ローカル管理インターフェースを使用してルーティング・コントロール・ファイルを更新するには、「リバース・プロキシー・インスタンス」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. 対象のインスタンスを選択します。
3. 「**管理**」 > 「**構成**」 > 「**ルーティング・ファイルの編集**」を選択します。 ルーティング・ファイルの内容が表示されます。
4. ルーティング・ファイルを変更します。
5. 「**保存**」をクリックして、変更を保存します。あるいは、変更を保存しない場合は、「**クローズ**」をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

トランザクション・ロギング・コンポーネントおよびデータ・ファイルの管理

ローカル管理インターフェースを使用してトランザクション・ロギング・コンポーネントおよびデータ・ファイルを管理するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「管理」** > **「リバース・プロキシー」**を選択します。
2. 対象のインスタンスを選択します。
3. **「管理」** > **「トラブルシューティング」** > **「トランザクション・ロギング」**を選択します。 すべてのトランザクション・ロギング・コンポーネント、およびその状況、合計ファイル・サイズ、ロールオーバー・サイズが表示されます。
   - **トランザクション・ロギング・コンポーネントの使用可能化または使用不可化**
     a. 対象のトランザクション・ロギング・コンポーネントを選択します。
     b. **「編集」**をクリックします。
     c. **「使用可能」**チェック・ボックスを選択またはクリアして、トランザクション・ロギング・コンポーネントを使用可能または使用不可にします。
     d. オプションとして、**「ロールオーバー・サイズ」**フィールドに値を指定して、ロールオーバー・サイズを定義します。値を指定しない場合、デフォルトのロールオーバー・サイズが使用されます。
     e. **「保存」**をクリックして、変更内容を保存します。
   - **トランザクション・ロギング・コンポーネントのデータ・ファイルのロールオーバー**
     a. 対象のトランザクション・ロギング・コンポーネントを選択します。
     b. **「管理」** > **「ロールオーバー」**をクリックします。
     c. **「はい」**をクリックして、操作を確定します。
   - **トランザクション・ロギング・データ・ファイルの管理**
     a. 対象のトランザクション・ロギング・コンポーネントを選択します。
     b. **「ファイル」**をクリックします。
        – **トランザクション・ロギング・データ・ファイルのエクスポート**
          1) 対象のトランザクション・ロギング・データ・ファイルを選択します。
          2) **「管理」** > **「エクスポート」**をクリックします。

             注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
          3) ブラウザー・ウィンドウでエクスポートしたファイルを開くのか、保存するのかを確認します。
        – **トランザクション・ロギング・データ・ファイルの削除**

          注: 削除できるのは、使用されていないトランザクション・ロギング・データ・ファイルのみです。

1) 対象のトランザクション・ロギング・データ・ファイルを選択します。
2) 「**削除**」をクリックします。
3) 「**はい**」をクリックして、操作を確定します。

– **使用されていないすべてのトランザクション・ロギング・データ・ファイルの削除**
1) 「**管理**」 > 「**すべて削除**」をクリックします。
2) 「**はい**」をクリックして、操作を確定します。

標準 Junction および仮想 Junction の管理

ローカル管理インターフェースを使用して標準 Junction および仮想 Junction を管理するには、「Junction 管理」ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. Junction を管理するリバース・プロキシーを選択します。
3. 「**管理**」 > 「**Junction 管理**」を選択します。
4. 必要に応じて、Junction 関連のタスクを実行します。
   - **標準 Junction の作成**
     a. 「**新規**」 > 「**標準 Junction**」をクリックします。
     b. 「Junction」タブ・ページで以下を行います。
        1) Junction ポイント名を入力します。

           注: 標準 Junction の名前は、スラッシュ (/) 文字で開始する必要があります。
        2) Junction 名がバックエンド・サーバー文書スペースのルートの下のサブディレクトリーの名前と一致する必要がある場合は、「**透過パス Junction の作成**」チェック・ボックスを選択します。
        3) Junction をステートフルにする場合は、「**ステートフル Junction**」チェック・ボックスを選択します。
        4) リストされるオプションから Junction タイプを選択します。
     c. 「サーバー」タブ・ページで以下を行います。
        1) 「**新規**」をクリックして、ターゲット・バックエンド・サーバーを追加します。

           注: Junction を作成するには、少なくとも 1 つのターゲット・バックエンド・サーバーを追加する必要があります。サーバーの追加時に使用可能なオプションは、選択した Junction タイプによって異なります。
        2) 表示されているフィールドに入力します。
        3) 「**保存**」をクリックします。
     d. 「基本認証」タブ・ページで以下を行います。
        1) バックエンド・サーバーとの認証に BA ヘッダー情報を使用する場合は、「**基本認証を使用可能にする**」チェック・ボックスを選択します。

2) WebSEAL ユーザー名を「**ユーザー名**」フィールドに入力します。
3) 「**パスワード**」フィールドに WebSEAL パスワードを入力します。
4) フロントエンド WebSEAL サーバーとバックエンド WebSEAL サーバーとの間で相互認証を使用する場合は、「**Junction WebSEAL サーバーに対する相互認証を使用可能にします**」チェック・ボックスを選択します。
5) 相互認証に使用する鍵ファイルをリストから選択します。
6) 相互認証に使用する鍵ラベルをリストから選択します。

e. 「ID」タブ・ページで以下を行います。
1) 「**HTTP 基本認証ヘッダー**」の下のリストから該当するアクションを選択することにより、WebSEAL サーバーが BA ヘッダーのクライアント識別情報をバックエンド・サーバーに渡す方法を定義します。
2) 前のステップで「**GSO**」を選択した場合は、「**GSO リソースまたはグループ**」フィールドに GSO リソース名またはリソース・グループ名を入力します。前のステップで「**GSO**」以外の値を選択した場合は、このステップはスキップします。
3) 「**HTTP ヘッダー ID 情報**」フィールドで、バックエンド・サーバーに渡す HTTP ヘッダー ID 情報を選択します。
4) 「**HTTP ヘッダーのエンコード**」の下のリストから、エンコードを選択します。
5) 「**Junction Cookie JavaScript ブロック**」の下のリストからオプションを選択します。
6) 必要に応じて、右にあるチェック・ボックスを選択します。

f. SSO および LTPA タブ・ページで以下を行います。
1) Junction で LTPA Cookie をサポートする場合は、「**LTPA Cookie のサポートを使用可能にする**」チェック・ボックスを選択します。
2) LTPA バージョン 2 Cookie (LtpaToken2) を使用する場合は、「**バージョン 2 Cookie を使用**」チェック・ボックスを選択します。
3) 「**LTPA 鍵ファイル**」の下のリストから LTPA 鍵ファイルを選択します。
4) 「**LTPA 鍵ファイルのパスワード**」フィールドに鍵ファイルのパスワードを入力します。

g. 「一般」タブ・ページで以下を行います。
1) 「**FSSO 構成ファイル**」フィールドに、フォーム・ベースのシングル・サインオン構成ファイルの名前を指定します。
2) 「**ワーカー・スレッドのハード制限のパーセント値**」フィールドに、ワーカー・スレッドの消費量のハード制限を定義します。
3) 「**ワーカー・スレッドのソフト制限のパーセント値**」フィールドに、ワーカー・スレッドの消費量のソフト制限を定義します。
4) 許可ルールにより拒否された要求およびその失敗理由の情報を Boolean Rule ヘッダーで送信する場合は、「**許可ルールの決定情報を含めます**」チェック・ボックスを選択します。

h. 「**保存**」をクリックします。

- **仮想 Junction を作成します。**
  a. 「**新規**」 > 「**仮想 Junction**」をクリックします。
  b. 「Junction」タブ・ページで以下を行います。
     1) 「**Junction ラベル**」フィールドに対応するJunction ラベルを入力します。
     2) Junction をステートフルにする場合は、「**ステートフル Junction**」チェック・ボックスを選択します。
     3) 右側にリストされるオプションから Junction タイプを選択します。
  c. 「サーバー」タブ・ページで以下を行います。
     1) 「**新規**」をクリックして、ターゲット・バックエンド・サーバーを追加します。

        注: Junction を作成するには、少なくとも 1 つのターゲット・バックエンド・サーバーを追加する必要があります。
     2) 表示されているフィールドに入力します。
     3) 「**保存**」をクリックします。
  d. 「基本認証」タブ・ページで以下を行います。
     1) バックエンド・サーバーとの認証に BA ヘッダー情報を使用する場合は、「**基本認証を使用可能にする**」チェック・ボックスを選択します。
     2) WebSEAL ユーザー名を「**ユーザー名**」フィールドに入力します。
     3) 「**パスワード**」フィールドに WebSEAL パスワードを入力します。
     4) フロントエンド WebSEAL サーバーとバックエンド WebSEAL サーバーとの間で相互認証を使用する場合は、「**Junction WebSEAL サーバーに対する相互認証を使用可能にします**」チェック・ボックスを選択します。
     5) 相互認証に使用する鍵ファイルをリストから選択します。
     6) 相互認証に使用する鍵ラベルをリストから選択します。
  e. 「ID」タブ・ページで以下を行います。
     1) 「**HTTP 基本認証ヘッダー**」の下のリストから該当するアクションを選択することにより、WebSEAL サーバーが BA ヘッダーのクライアント識別情報をバックエンド・サーバーに渡す方法を定義します。
     2) 前のステップで「**GSO**」を選択した場合は、「**GSO リソースまたはグループ**」フィールドに GSO リソース名またはリソース・グループ名を入力します。前のステップで「**GSO**」以外の値を選択した場合は、このステップはスキップします。
     3) 「**HTTP ヘッダー ID 情報**」フィールドで、バックエンド・サーバーに渡す HTTP ヘッダー ID 情報を選択します。
     4) 「**HTTP ヘッダーのエンコード**」の下のリストから、エンコードを選択します。
     5) 必要に応じて、右にあるチェック・ボックスを選択します。
  f. SSO および LTPA タブ・ページで以下を行います。
     1) Junction で LTPA Cookie をサポートする場合は、「**LTPA Cookie のサポートを使用可能にする**」チェック・ボックスを選択します。

2) LTPA バージョン 2 Cookie (LtpaToken2) を使用する場合は、「**バージョン 2 Cookie を使用**」チェック・ボックスを選択します。

3) 「**LTPA 鍵ファイル**」の下のリストから LTPA 鍵ファイルを選択します。

4) 「**LTPA 鍵ファイルのパスワード**」フィールドに鍵ファイルのパスワードを入力します。

g. 「一般」タブ・ページで以下を行います。

1) 「**FSSO 構成ファイル**」フィールドに、フォーム・ベースのシングル・サインオン構成ファイルの名前を指定します。

2) 「**ワーカー・スレッドのハード制限のパーセント値**」フィールドに、ワーカー・スレッドの消費量のハード制限を定義します。

3) 「**ワーカー・スレッドのソフト制限のパーセント値**」フィールドに、ワーカー・スレッドの消費量のソフト制限を定義します。

4) 許可ルールにより拒否された要求およびその失敗理由の情報を Boolean Rule ヘッダーで送信する場合は、「**許可ルールの決定情報を含めます**」チェック・ボックスを選択します。

h. 「**保存**」をクリックします。

- **標準 Junction または仮想 Junction を編集**
  a. 編集する Junction をリストから選択します。
  b. 「**編集**」をクリックします。
  c. 必要に応じて設定を変更します。
  d. 「**保存**」をクリックします。
- **標準 Junction または仮想 Junction を削除**
  a. 削除する Junction をリストから選択します。
  b. 「**削除**」をクリックします。
  c. ポップアップ表示される確認ウィンドウで、「**はい**」 をクリックします。

注: 一部の Junction 管理タスクは、Web サービスでのみ実行でき、ローカル管理インターフェースでは実行できません。例えば、以下の Web サービス・コマンドを使用して実行される機能は、ローカル管理インターフェースを使用して実行することはできません。

- jmt load
- jmt clear
- offline
- online
- throttle

Web アプリケーション・ファイアウォールの構成

ローカル管理インターフェースを使用して Web アプリケーション・ファイアウォールを構成するには、「リバース・プロキシー」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**管理**」 > 「**リバース・プロキシー**」を選択します。
2. Web アプリケーション・ファイアウォールを構成するリバース・プロキシー・インスタンスを選択します。
3. 「**管理**」 > 「**構成**」 > 「**Web コンテンツ保護**」をクリックします。
4. 「動作の構成」タブで、Web コンテンツ保護の一般設定を構成します。
   a. 「**Web コンテンツ保護の有効化**」チェック・ボックスを選択して、Web アプリケーション・ファイアウォールを有効にします。
   b. **必要に応じて、「プロキシー HTTP ヘッダーの使用」**チェック・ボックスを選択します。 これは、ネットワーク接続から取得したクライアントの IP アドレスと X-Forwarded-For HTTP ヘッダーから取得した IP アドレスのどちらを監査ログに含めるのかを制御するために使用されます。この設定は、ネットワークを終端するファイアウォールがリバース・プロキシーとクライアントとの間に配置されている場合に有用です。
   c. 「**最大メモリー・サイズ**」フィールドに値 (バイト) を指定します。これにより、PAM エンジンが使用できる最大メモリーが定義されます。

      注: PAM には、最小メモリー・サイズが事前定義されています。設定した構成値が最小値よりも小さい場合は、割り振られるメモリーがこの最小サイズまで自動的に増加されます。
   d. 「**リソース・アクション**」の下で、以下の作業を行います。

      注: このテーブルは、特定リソースで問題が検出されたときに実行するアクションをカスタマイズする場合に使用します。これは、パターン・マッチ・リストであり、順番に検索されます。リソース名には、パターン・マッチング文字として「*」と「?」を含めることができます。一致するリソースが見つからない場合は、X-force チームが推奨するデフォルト・アクションが実行されます。

      - リソースを追加するには、以下のようにします。
        1) 「**新規**」をクリックします。
        2) 「カスタム・リソースの追加」ページでリソース名を指定します。当該リソースで選択可能な問題は、すべて事前に設定されています。

           注: リソース名には、パターン・マッチング文字として「*」と「?」を含めることができます。例えば、*.html と入力します。
        3) 変更する問題を選択して、「**編集**」をクリックします。
        4) 「カスタム・リソースの問題の編集」ページの「**応答**」フィールドで、この問題に対して実行するアクションを選択します。
        5) *オプション:* 前のステップでイベント応答として「**検疫**」を選択した場合は、「**検疫期間**」フィールドに検疫時間を指定します。
        6) 「カスタム・リソースの問題の編集」ページで「**保存**」をクリックします。
        7) 「カスタム・リソースの追加」ページで「**保存**」をクリックします。
      - リソースを編集するには、以下のようにします。

1) 編集するリソース名を選択します。
2) 「**編集**」をクリックします。
3) 「カスタム・リソースの編集」ページで、変更する問題を選択してから「**編集**」をクリックします。
4) 「カスタム・リソースの問題の編集」ページで、必要に応じて、イベント応答および検疫時間を変更します。
5) 「カスタム・リソースの問題の編集」ページで「**保存**」をクリックします。
6) 「カスタム・リソースの編集」ページで「**保存**」をクリックします。

- リソースを削除するには、以下のようにします。
  1) 削除するリソース名を選択します。
  2) 「**削除**」をクリックします。

     注: この削除操作では、確認ウィンドウは表示されません。選択したリソースが削除対象のリソースであることを確認してから、「**削除**」をクリックしてください。

e. 「**登録済みリソース**」の下で、以下の作業を行います。

注: 登録済みリソースは、検査エンジンに渡される要求を指定するために使用されます。 Web リバース・プロキシーが要求を受信すると、一致が見つかるまで、リスト内のエントリーが順次検索されます。一致するリソースに割り振られたアクションによって、検査が使用可能になるか使用不可になるかが制御されます。リソースには、パターン・マッチングのためのワイルドカード文字を含めることができます。

- 登録済みリソースを追加するには、以下のようにします。
  1) 「**新規**」をクリックします。
  2) ポップアップ表示される「保護リソースの追加」ページで、「**リソース名**」を指定します。例えば、 index.html、*.html、または *.gif などを入力します。
  3) 必要に応じて、「**使用可能**」または「**使用不可**」を選択します。
  4) 「**保存**」をクリックします。
- 登録済みリソースを編集するには、以下のようにします。
  1) 編集するリソースをリストから選択します。
  2) 「**編集**」をクリックします。
  3) ポップアップ表示される「保護リソースの編集」ページで、必要に応じて、リソース名と、リソース名を使用可能にするかどうかを変更します。
  4) 「**保存**」をクリックします。
- 登録済みリソースを削除するには、以下のようにします。
  1) 削除するリソースをリストから選択します。
  2) 「**削除**」をクリックします。

注: この削除操作では、確認ウィンドウは表示されません。選択したリソースが削除対象のリソースであることを確認してから、「**削除**」をクリックしてください。

f. 「**インジェクション・チューニング・パラメーター**」の下で、必要に応じて、「**ユニット (Units)**」列の値をダブルクリックしてインラインで編集を行い、リストされたパラメーターを変更します。各パラメーターの説明を参照するには、マウス・カーソルをパラメーターの上に移動して、説明を含むポップアップ・メッセージを表示します。

5. 「問題」タブで、特定の問題を使用可能または使用不可にします。

注: 検査エンジンがモニターするイベントは、問題のリストによって制御されます。問題が使用不可の場合、検査エンジンは、その問題を検査しなくなります。

- 方法 1:
  a. 編集するイベントを選択します。
  b. 「**編集**」をクリックします。
  c. 「問題の編集」ページで、必要に応じて、「**使用可能**」または「**使用不可**」を選択します。
  d. 「**保存**」をクリックします。
- 方法 2:
  – 「**使用可能**」チェック・ボックスを選択またはクリアして、特定の問題を使用可能または使用不可にします。
- 方法 3:
  – 「**X-Force を信頼**」をクリックして、デフォルト応答がないすべての問題を自動的に使用不可にします。

6. 「監査」タブで、ロギングおよび監査の設定を構成します。
   a. 「**詳細な監査イベントをログに記録**」の下で、詳細な監査イベントのロギングを使用可能にする場合に、そのチェック・ボックスを選択します。
   b. 「**監査イベントをログに記録**」の下で、監査イベントの送信先を示すオプションのいずれかを選択します。
   c. 「**監査構成をログに記録**」の下で、前のステップの選択内容に基づいて、以下のパラメーターを定義します。
      - 「**ファイルに記録**」 を選択した場合:

パラメーター	説明
ファイル名	このエントリーは、ログ・ファイルの名前を指定します。
ロールオーバー・サイズ	ログ・ファイルは、この最大サイズに達するとロールオーバーされます。デフォルト値は 2000000 バイトです。
バッファー・サイズ	より小さなイベントを結合するときに使用されるメッセージの最大サイズ。
キュー・サイズ	イベントがキューに格納されてからファイル・ログ・エージェントがそのイベントを削除するまでには、遅延があります。このパラメーターは、キューの上限となる最大サイズを指定します。

パラメーター	説明
上限基準点	イベント・キューの処理は、構成されたフラッシュ間隔で定期的にスケジュールされます。また、キューのサイズがイベント・キューの上限基準点に達した場合も、非同期的に起動されます。デフォルト値は、構成された最大キュー・サイズの 3 分の 2 です。最大キュー・サイズがゼロの場合、上限基準点にはデフォルトの 100 が設定されます。イベント・キューの上限基準点に 1 が設定された場合、キューに入れられたすべてのイベントは、可能な限り早期にログ・エージェントに中継されます。
フラッシュ間隔	このエントリーは、サーバーがファイル・ストリームをディスクに非同期的かつ強制的にフラッシュする頻度を制御します。このパラメーターに定義する値は 0、< 0、または秒単位のフラッシュ間隔のいずれかです。

- 「**リモート Authorization Server に記録**」 を選択した場合:

パラメーター	説明
圧縮	ネットワーク・トラフィックを削減するには、このパラメーターを使用して、バッファーを圧縮してから送信し、受信時に展開します。デフォルト値は no です。
バッファー・サイズ	ネットワーク・トラフィックを削減するため、イベントは、指定されたサイズのブロックでバッファーに入れられてからリモート・サーバーに中継されます。このパラメーターは、ローカル・プログラムが複数の小さいイベントを結合してバッファーに格納することによって構成しようとする最大メッセージ・サイズを指定します。デフォルト値は 1024 バイトです。
フラッシュ間隔	このパラメーターは、統合バッファーがいっぱいになるのをプロセスが待機する時間を制限します。デフォルト値は 20 秒です。フラッシュ間隔 0 は許可されていません。値 0 を指定すると、バッファーが 600 秒ごとにフラッシュされます。
キュー・サイズ	イベントがキューに格納されてからファイル・ログ・エージェントがそのイベントを削除するまでには、遅延があります。このパラメーターは、キューの上限となる最大サイズを指定します。
上限基準点	イベント・キューの処理は、構成されたフラッシュ間隔で定期的にスケジュールされます。また、キューのサイズがイベント・キューの上限基準点に達した場合も、非同期的に起動されます。デフォルト値は、構成された最大キュー・サイズの 3 分の 2 です。最大キュー・サイズがゼロの場合、上限基準点にはデフォルトの 100 が設定されます。イベント・キューの上限基準点に 1 が設定された場合、キューに入れられたすべてのイベントは、可能な限り早期にログ・エージェントに中継されます。
エラー再試行のタイムアウト	リモート・サービスへの送信操作に失敗した場合、システムが再試行します。システムは、エラー再試行のタイムアウト (秒) だけ待機してから、再試行を行います。デフォルト値は 2 秒です。
ロギング・ポート	リモート Authorization Server がリモート・ロギング要求を listen するポートを指定するには、port パラメーターを構成します。デフォルト値はポート 7136 です。
再バインドの再試行	リモート Authorization Server が使用不可の場合、ログ・エージェントは、この頻度 (秒) でこのサーバーへの再バインドを試行します。デフォルトの再バインドの再試行タイムアウト値は、300 秒です。
ホスト名	リモート・ロギング・サービスは、許可サービスによって提供されます。server パラメーターは、イベント記録のために Authorization Server プロセスをバインドするホストを指定します。

パラメーター	説明
DN	リモート・サーバーの相互認証を設定するには、識別名 (DN) を構成する必要があります。識別名は、二重引用符で囲んだストリングとして指定する必要があります。

- 「**リモート syslog サーバーに記録**」を選択した場合:

パラメーター	説明
リモート syslog サーバー	イベント記録のために syslog サーバー・プロセスをバインドするホスト。
ポート	リモート syslog サーバーがリモート・ロギング要求を listen するポート。
アプリケーション ID	リモート syslog サーバーに送信するメッセージに出力されるアプリケーション名。
エラー再試行のタイムアウト	リモート・サービスへの送信操作に失敗した場合、システムが再試行します。システムは、エラー再試行のタイムアウト (秒) だけ待機してから、再試行を行います。デフォルト値は 2 秒です。
フラッシュ間隔	このパラメーターは、統合バッファーがいっぱいになるのをプロセスが待機する時間を制限します。デフォルト値は 20 秒です。フラッシュ間隔 0 は許可されていません。値 0 を指定すると、バッファーが 600 秒ごとにフラッシュされます。
上限基準点	イベント・キューの処理は、構成されたフラッシュ間隔で定期的にスケジュールされます。また、キューのサイズがイベント・キューの上限基準点に達した場合も、非同期的に起動されます。デフォルト値は、構成された最大キュー・サイズの 3 分の 2 です。最大キュー・サイズがゼロの場合、上限基準点にはデフォルトの 100 が設定されます。イベント・キューの上限基準点に 1 が設定された場合、キューに入れられたすべてのイベントは、可能な限り早期にログ・エージェントに中継されます。
キュー・サイズ	イベントがキューに格納されてからファイル・ログ・エージェントがそのイベントを削除するまでには、遅延があります。このパラメーターは、キューの上限となる最大サイズを指定します。
再バインドの再試行	リモート・システム・ログ・サーバーが使用不可の場合、ログ・エージェントは、この頻度 (秒) でこのサーバーへの再バインドを試行します。デフォルトの再バインドの再試行タイムアウト値は、300 秒です。
イベントの最大長	リモート syslog サーバーに送信するイベントの最大長。イベント・テキストが構成された長さより長い場合は、イベントの最大長に切り捨てられます。イベントの最大長がゼロの場合、イベント・テキストが切り捨てられることはありません。イベントを平文でリモート syslog サーバーに送信する場合は、イベントの最大長に設定する値を、サーバーへのネットワーク・パスの最大伝送単位 (MTU) より小さくします。これにより、イベントのフラグメント化が回避されます。
SSL 通信の有効化	SSL を通信に使用するかどうかを設定します。
SSL 鍵ファイル	CA 証明書を含む GSKit 鍵データベース・ファイルの名前。これは、システムが TLS を介してリモート syslog サーバーとのセキュア接続を確立するときに使用されます。「**SSL 通信の有効化**」チェック・ボックスがオンの場合、このフィールドは必須です。

パラメーター	説明
SSL 証明書ラベル	システムがセキュア接続を確立するときに、要求に応じてリモート syslog サーバーに提示される証明書の名前。このフィールドに値を設定しない場合は、鍵データベースからのデフォルトの証明書が使用されます。

7. 「拡張構成」タブで、コアレッサー、検査エンジン、問題、およびカスタム・アクションを構成します。
   a. 「**コアレッサー構成**」の下で、以下の作業を行います。

      注: コアレッサーは、監査イベントを相関させる場合に使用されます。管理者は、これらの構成設定を使用して、コアレッサーの処理を微調整することにより、監査ログに送信されるメッセージの数を削減できます。

      - コアレッサー・パラメーターを追加するには、以下のようにします。
        1) 「**新規**」をクリックします。
        2) ポップアップ表示される「コアレッサー・パラメーターの追加」ページで、パラメーターの名前および値を指定します。
        3) 「**保存**」をクリックします。
      - コアレッサー・パラメーターを編集するには、以下のようにします。
        1) 編集するパラメーターをリストから選択します。
        2) 「**編集**」をクリックします。
        3) ポップアップ表示される「コアレッサー・パラメーターの編集」ページで、必要に応じて、パラメーターの名前および値を変更します。
        4) 「**保存**」をクリックします。
      - コアレッサー・パラメーターを削除するには、以下のようにします。
        1) 削除するパラメーターをリストから選択します。
        2) 「**削除**」をクリックします。

           注: この削除操作では、確認ウィンドウは表示されません。選択したパラメーターが削除対象のパラメーターであることを確認してから、「**削除**」をクリックしてください。

   b. 「**検査エンジン構成**」の下で、以下の作業を行います。
      - 検査エンジン構成パラメーターを追加するには、以下のようにします。
        1) 「**新規**」をクリックします。
        2) ポップアップ表示される「検査パラメーターの追加」ページで、パラメーターの名前および値を指定します。
        3) 「**保存**」をクリックします。
      - 検査エンジン構成パラメーターを編集するには、以下のようにします。
        1) 編集するパラメーターをリストから選択します。
        2) 「**編集**」をクリックします。
        3) ポップアップ表示される「検査パラメーターの編集」ページで、必要に応じて、パラメーターの名前および値を変更します。
        4) 「**保存**」をクリックします。

- 検査エンジン構成パラメーターを削除するには、以下のようにします。
  1) 削除するパラメーターをリストから選択します。
  2) 「**削除**」をクリックします。

     注: この削除操作では、確認ウィンドウは表示されません。選択したリソースが削除対象のリソースであることを確認してから、「**削除**」をクリックしてください。

8. 「**保存**」をクリックします。

DynURL 構成ファイルの管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**URL マッピング**」を選択します。

すべての DynURL 構成ファイルのリストの取得

ローカル管理インターフェースを使用してすべての DynURL 構成ファイルのリストを取得するには、「URL マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**URL マッピング**」を選択します。
2. すべての DynURL 構成ファイルのファイル名、ファイル・サイズ、および最終変更時刻の情報が表示されます。

DynURL 構成ファイルの表示

ローカル管理インターフェースを使用して DynURL 構成ファイルの内容を表示するには、「URL マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**URL マッピング**」を選択します。
2. 表示するファイルを選択します。
3. 「**編集**」をクリックします。 ファイルの内容がポップアップ・ウィンドウに表示されます。

DynURL 構成ファイルの作成

ローカル管理インターフェースを使用して DynURL 構成ファイルを作成するには、「URL マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**URL マッピング**」を選択します。
2. 「**新規**」をクリックします。
3. ポップアップ表示されるウィンドウで、以下を実行します。
   a. ファイルの内容を変更します。

b. 「**DynURL 構成ファイル名**」フィールドに、作成するファイルの名前を入力します。

c. 「**保存**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

新規 DynURL 構成ファイルのインポート

ローカル管理インターフェースを使用して新規 DynURL 構成ファイルをインポートするには、「URL マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**URL マッピング**」を選択します。
2. 「**管理**」 > 「**インポート**」をクリックします。
3. ポップアップ表示されるウィンドウで、「**参照**」をクリックします。
4. ローカル・ワークステーションからインポートするファイルを選択します。
5. 「**インポート**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

DynURL 構成ファイルのエクスポート

ローカル管理インターフェースを使用して DynURL 構成ファイルをエクスポートするには、「URL マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**URL マッピング**」を選択します。
2. エクスポートする DynURL 構成ファイルを選択します。
3. 「**管理**」 > 「**エクスポート**」をクリックします。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

4. ポップアップ表示されるウィンドウで、ローカル・ワークステーションへのファイルの保存を確認します。

既存の DynURL 構成ファイルの更新

ローカル管理インターフェースを使用して既存の DynURL 構成ファイルを更新するには、「URL マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**URL マッピング**」を選択します。
2. 編集するDynURL 構成ファイルを選択します。

3. 「**編集**」をクリックします。
4. ポップアップ表示されるウィンドウで、以下を実行します。
   a. ファイル内容を変更します。
   b. 「**保存**」をクリックします。

   注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

DynURL 構成ファイルの名前変更

ローカル管理インターフェースを使用して DynURL 構成ファイルを名前変更するには、「URL マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**URL マッピング**」を選択します。
2. 名前変更する DynURL 構成ファイルを選択します。
3. 「**管理**」 > 「**名前変更**」をクリックします。
4. ポップアップ表示されるウィンドウの「**新規リソース名**」フィールドに、ファイルの新規名を入力します。
5. 「**保存**」をクリックします。

   注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

DynURL 構成ファイルの削除

ローカル管理インターフェースを使用して DynURL 構成ファイルを削除するには、「URL マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**URL マッピング**」を選択します。
2. 削除する DynURL 構成ファイルを選択します。
3. 「**削除**」をクリックします。
4. ポップアップ表示されるウィンドウで、「**はい**」をクリックします。

   注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

JMT 構成ファイルの管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**Junction マッピング**」を選択します。

すべての JMT 構成ファイルのリストの取得

ローカル管理インターフェースを使用してすべての JMT 構成ファイルのリストを取得するには、「Junction マッピング」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「Junction マッピング」**を選択します。
2. すべての JMT 構成ファイルのファイル名、ファイル・サイズ、および最終変更時刻の情報が表示されます。

JMT 構成ファイルの表示

ローカル管理インターフェースを使用して JMT 構成ファイルの内容を表示するには、「Junction マッピング」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「Junction マッピング」**を選択します。
2. 表示するファイルを選択します。
3. **「編集」**をクリックします。 ファイルの内容がポップアップ・ウィンドウに表示されます。

JMT 構成ファイルの作成

ローカル管理インターフェースを使用して JMT 構成ファイルを作成するには、「Junction マッピング」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「Junction マッピング」**を選択します。
2. **「新規」**をクリックします。
3. ポップアップ表示されるウィンドウで、以下を実行します。
   a. ファイルの内容を変更します。
   b. **「JMT 構成ファイル名」**フィールドに、作成するファイルの名前を入力します。
   c. **「保存」**をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

新規 JMT 構成ファイルのインポート

ローカル管理インターフェースを使用して新規 JMT 構成ファイルをインポートするには、「Junction マッピング」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「Junction マッピング」**を選択します。
2. **「管理」** > **「インポート」**をクリックします。
3. ポップアップ表示されるウィンドウで、**「参照」** をクリックします。
4. ローカル・ワークステーションからインポートするファイルを選択します。
5. **「インポート」**をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

JMT 構成ファイルのエクスポート

ローカル管理インターフェースを使用して JMT 構成ファイルをエクスポートするには、「Junction マッピング」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「Junction マッピング」**を選択します。
2. エクスポートするJMT 構成ファイルを選択します。
3. **「管理」** > **「エクスポート」**をクリックします。

   注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
4. ポップアップ表示されるウィンドウで、ローカル・ワークステーションへのファイルの保存を確認します。

既存の JMT 構成ファイルの更新

ローカル管理インターフェースを使用して既存の JMT 構成ファイルを更新するには、「Junction マッピング」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「Junction マッピング」**を選択します。
2. 編集するJMT 構成ファイルを選択します。
3. **「編集」**をクリックします。
4. ポップアップ表示されるウィンドウで、以下を実行します。
   a. ファイル内容を変更します。
   b. **「保存」**をクリックします。

   注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

JMT 構成ファイルの名前変更

ローカル管理インターフェースを使用して JMT 構成ファイルを名前変更するには、「Junction マッピング」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「Junction マッピング」**を選択します。
2. 名前変更するJMT 構成ファイルを選択します。
3. **「管理」** > **「名前変更」**をクリックします。

4. ポップアップ表示されるウィンドウの「**新規リソース名**」フィールドに、ファイルの新規名を入力します。
5. 「**保存**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

JMT 構成ファイルの削除

ローカル管理インターフェースを使用して JMT 構成ファイルを削除するには、「Junction マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**Junction マッピング**」を選択します。
2. 削除するJMT 構成ファイルを選択します。
3. 「**削除**」をクリックします。
4. ポップアップ表示されるウィンドウで、「**はい**」 をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

クライアント認証 CDAS ファイルの管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**クライアント証明書マッピング**」を選択します。

すべてのクライアント認証 CDAS ファイルのリストの取得

ローカル管理インターフェースを使用してすべてのクライアント認証 CDAS ファイルのリストを取得するには、「クライアント証明書マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**クライアント証明書マッピング**」を選択します。
2. すべてのクライアント認証 CDAS ファイルのファイル名、ファイル・サイズ、および最終変更時刻の情報が表示されます。

クライアント認証 CDAS ファイルの作成

ローカル管理インターフェースを使用してクライアント認証 CDAS ファイルを作成するには、「クライアント証明書マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**クライアント証明書マッピング**」を選択します。
2. 「**新規**」をクリックします。

3. ポップアップ表示されるウィンドウの「**新規リソース名**」フィールドに、作成するファイルの名前を入力します。
4. 「**保存**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

クライアント認証 CDAS ファイルのインポート

ローカル管理インターフェースを使用して既存のクライアント認証 CDAS ファイルをインポートするには、「クライアント証明書マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**クライアント証明書マッピング**」を選択します。
2. 「**管理**」 > 「**インポート**」をクリックします。
3. ポップアップ表示されるウィンドウで、「**参照**」をクリックします。
4. ローカル・ワークステーションからインポートするファイルを選択します。
5. 「**インポート**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

クライアント認証 CDAS ファイルのエクスポート

ローカル管理インターフェースを使用してクライアント認証 CDAS ファイルをエクスポートするには、「クライアント証明書マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**クライアント証明書マッピング**」を選択します。
2. エクスポートするクライアント認証 CDAS ファイルを選択します。
3. 「**管理**」 > 「**エクスポート**」をクリックします。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

4. ポップアップ表示されるウィンドウで、ローカル・ワークステーションへのファイルの保存を確認します。

クライアント認証 CDAS ファイルの編集

ローカル管理インターフェースを使用してクライアント認証 CDAS ファイルを編集するには、「クライアント証明書マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**クライアント証明書マッピング**」を選択します。

2. 編集するクライアント認証 CDAS ファイルを選択します。
3. 「**編集**」をクリックします。
4. ポップアップ表示されるウィンドウで、以下を実行します。
   a. ファイル内容を変更します。
   b. 「**保存**」をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

クライアント認証 CDAS ファイルの名前変更

ローカル管理インターフェースを使用してクライアント認証 CDAS ファイルを名前変更するには、「クライアント証明書マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**クライアント証明書マッピング**」を選択します。
2. 名前変更するクライアント認証 CDAS ファイルを選択します。
3. 「**管理**」 > 「**名前変更**」をクリックします。
4. ポップアップ表示されるウィンドウの「**新規リソース名**」フィールドに、ファイルの新規名を入力します。
5. 「**保存**」をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

クライアント認証 CDAS ファイルの削除

ローカル管理インターフェースを使用してクライアント認証 CDAS ファイルを削除するには、「クライアント証明書マッピング」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**クライアント証明書マッピング**」を選択します。
2. 削除するクライアント認証 CDAS ファイルを選択します。
3. 「**削除**」をクリックします。
4. ポップアップ表示されるウィンドウで、「**はい**」 をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

FSSO 構成ファイルの管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**フォーム・ベースのシングル・サインオン**」を選択します。

すべての FSSO 構成ファイルのリストの取得

ローカル管理インターフェースを使用してすべての FSSO 構成ファイルのリストを取得するには、「フォーム・ベースのシングル・サインオン」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「フォーム・ベースのシングル・サインオン」**を選択します。
2. すべての FSSO 構成ファイルのファイル名、ファイル・サイズ、および最終変更時刻の情報が表示されます。

FSSO 構成ファイルの表示

ローカル管理インターフェースを使用して FSSO 構成ファイルの内容を表示するには、「フォーム・ベースのシングル・サインオン」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「フォーム・ベースのシングル・サインオン」**を選択します。
2. 表示するファイルを選択します。
3. **「編集」**をクリックします。 ファイルの内容がポップアップ・ウィンドウに表示されます。

FSSO 構成ファイルの作成

ローカル管理インターフェースを使用して FSSO 構成ファイルを作成するには、「フォーム・ベースのシングル・サインオン」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「フォーム・ベースのシングル・サインオン」**を選択します。
2. **「新規」**をクリックします。
3. ポップアップ表示されるウィンドウで、以下を実行します。
   a. ファイルの内容を変更します。
   b. **「FSSO 構成ファイル名」**フィールドに、作成するファイルの名前を入力します。
   c. **「保存」**をクリックします。

   注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

新規 FSSO 構成ファイルのインポート

ローカル管理インターフェースを使用して新規 FSSO 構成ファイルをインポートするには、「フォーム・ベースのシングル・サインオン」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**フォーム・ベースのシングル・サインオン**」を選択します。
2. 「**管理**」 > 「**インポート**」をクリックします。
3. ポップアップ表示されるウィンドウで、「**参照**」 をクリックします。
4. ローカル・ワークステーションからインポートするファイルを選択します。
5. 「**保存**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

FSSO 構成ファイルのエクスポート

ローカル管理インターフェースを使用して FSSO 構成ファイルをエクスポートするには、「フォーム・ベースのシングル・サインオン」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**フォーム・ベースのシングル・サインオン**」を選択します。
2. エクスポートするFSSO 構成ファイルを選択します。
3. 「**管理**」 > 「**エクスポート**」をクリックします。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

4. ポップアップ表示されるウィンドウで、ローカル・ワークステーションへのファイルの保存を確認します。

既存の FSSO 構成ファイルの更新

ローカル管理インターフェースを使用して既存の FSSO 構成ファイルを更新するには、「フォーム・ベースのシングル・サインオン」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**フォーム・ベースのシングル・サインオン**」を選択します。
2. 編集するFSSO 構成ファイルを選択します。
3. 「**編集**」をクリックします。
4. ポップアップ表示されるウィンドウで、以下を実行します。
   a. ファイル内容を変更します。
   b. 「**保存**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

FSSO 構成ファイルの名前変更

ローカル管理インターフェースを使用して FSSO 構成ファイルの名前を変更するには、「フォーム・ベースのシングル・サインオン」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**フォーム・ベースのシングル・サインオン**」を選択します。
2. 名前を変更する FSSO 構成ファイルを選択します。
3. 「**管理**」 > 「**名前変更**」をクリックします。
4. ポップアップ表示されるウィンドウの「**新規リソース名**」フィールドに、ファイルの新規名を入力します。
5. 「**保存**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

FSSO 構成ファイルの削除

ローカル管理インターフェースを使用して FSSO 構成ファイルを削除するには、「フォーム・ベースのシングル・サインオン」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**フォーム・ベースのシングル・サインオン**」を選択します。
2. 削除するFSSO 構成ファイルを選択します。
3. 「**削除**」をクリックします。
4. ポップアップ表示されるウィンドウで、「**はい**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

HTTP 変換ルール・ファイルの管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**HTTP 変換**」を選択します。

すべての HTTP 変換ルール・ファイルのリストの取得

ローカル管理インターフェースを使用してすべての HTTP 変換ルール・ファイルのリストを取得するには、「HTTP 変換」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**HTTP 変換**」を選択します。
2. すべての HTTP 変換ルール・ファイルのファイル名、ファイル・サイズ、および最終変更時刻の情報が表示されます。

HTTP 変換ルール・ファイルの作成

ローカル管理インターフェースを使用して HTTP 変換ルール・ファイルを作成するには、「HTTP 変換」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**HTTP 変換**」を選択します。
2. 「**新規**」をクリックします。
3. ポップアップ表示されるウィンドウの「**新規リソース名**」フィールドに、作成するファイルの名前を入力します。
4. テンプレートとして「**要求**」または「**応答**」のいずれかを使用することを選択します。
5. 「**保存**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

HTTP 変換ルール・ファイルのインポート

ローカル管理インターフェースを使用して既存の HTTP 変換ルール・ファイルをインポートするには、「HTTP 変換」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**HTTP 変換**」を選択します。
2. 「**管理**」 > 「**インポート**」をクリックします。
3. ポップアップ表示されるウィンドウで、「**参照**」 をクリックします。
4. ローカル・ワークステーションからインポートするファイルを選択します。
5. 「**インポート**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

HTTP 変換ルール・ファイルのエクスポート

ローカル管理インターフェースを使用して HTTP 変換ルール・ファイルをエクスポートするには、「HTTP 変換」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**HTTP 変換**」を選択します。
2. エクスポートする HTTP 変換ルール・ファイルを選択します。
3. 「**管理**」 > 「**エクスポート**」をクリックします。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

4. ポップアップ表示されるウィンドウで、ローカル・ワークステーションへのファイルの保存を確認します。

HTTP 変換ルール・ファイルの編集

ローカル管理インターフェースを使用して HTTP 変換ルール・ファイルを編集するには、「HTTP 変換」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「HTTP 変換」**を選択します。
2. 編集する HTTP 変換ルール・ファイルを選択します。
3. **「編集」**をクリックします。
4. ポップアップ表示されるウィンドウで、以下を実行します。
   a. ファイル内容を変更します。
   b. **「保存」**をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

HTTP 変換ルール・ファイルの名前変更

ローカル管理インターフェースを使用して HTTP 変換ルール・ファイルを名前変更するには、「HTTP 変換」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「HTTP 変換」**を選択します。
2. 名前変更する HTTP 変換ルール・ファイルを選択します。
3. **「管理」** > **「名前変更」**をクリックします。
4. ポップアップ表示されるウィンドウの**「新規リソース名」**フィールドに、ファイルの新規名を入力します。
5. **「保存」**をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

HTTP 変換ルール・ファイルの削除

ローカル管理インターフェースを使用して HTTP 変換ルール・ファイルを削除するには、「HTTP 変換」管理ページを使用します。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「HTTP 変換」**を選択します。
2. 削除する HTTP 変換ルール・ファイルを選択します。
3. **「削除」**をクリックします。
4. ポップアップ表示されるウィンドウで、**「はい」** をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

SSL 証明書の管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。

現在の証明書データベース名のリスト

ローカル管理インターフェースを使用して現在のすべての証明書データベース名をリストするには、「SSL 証明書」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。
2. 現在のすべての証明書データベース名およびその最終変更時刻情報を表示できます。

証明書データベースへの説明の追加

ローカル管理インターフェースを使用して説明を証明書データベースに追加するには、「SSL 証明書」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。
2. 説明の対象の証明書データベースを選択します。
3. 「**管理**」 > 「**説明**」を選択します。
4. 「SSL 証明書データベースの説明」ウィンドウで、証明書データベースの説明を入力します。
5. 「**保存**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

証明書データベースの作成

ローカル管理インターフェースを使用して証明書データベースを作成するには、「SSL 証明書」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。
2. メニュー・バーから、「**新規**」をクリックします。
3. 「SSL 証明書データベースの作成」ページで、作成する証明書データベースの名前を入力します。証明書データベース名の名前は、固有でなければなりません。
4. 「**保存**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

証明書データベースのインポート

ローカル管理インターフェースを使用して証明書データベースをインポートするには、「SSL 証明書」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。
2. 「**管理**」 > 「**インポート**」を選択します。
3. 「**証明書データベース・ファイル**」の下の「**参照**」をクリックします。
4. インポートするファイルが含まれているディレクトリーを参照して、ファイルを選択します。「**開く**」をクリックします。
5. 「**stash ファイル**」の下の「**参照**」をクリックします。
6. インポートするファイルが含まれているディレクトリーを参照して、ファイルを選択します。「**開く**」をクリックします。
7. 「**インポート**」をクリックします。 インポートが正常に行われたことを示すメッセージが表示されます。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

証明書データベースのエクスポート

ローカル管理インターフェースを使用して証明書データベースをエクスポートするには、「SSL 証明書」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。
2. エクスポートする証明書データベースを選択します。
3. 「**管理**」 > 「**エクスポート**」を選択します。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

4. ブラウザーで .zip ファイルを保存するように求めるプロンプトが出されたら、保存操作を確定します。

証明書データベースの名前変更

ローカル管理インターフェースを使用して証明書データベースを名前変更するには、「SSL 証明書」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。

2. 名前変更する証明書データベースを選択します。
3. 「**管理**」 > 「**名前変更**」を選択します。
4. 「SSL 証明書データベースの名前変更」ウィンドウで、証明書データベースの新規名を入力します。証明書データベース名の新規名は、固有でなければなりません。
5. 「**保存**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

証明書データベースの削除

ローカル管理インターフェースを使用して証明書データベースを削除するには、「SSL 証明書」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。
2. 削除する証明書データベースを選択します。
3. 「**削除**」を選択します。
4. ポップアップ表示されるウィンドウで、「**はい**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

証明書データベース内の署名者証明書の管理

証明書データベース内の署名者証明書を管理するには、「SSL 証明書」管理ページを使用します。具体的には、署名者証明書のインポート、エクスポート、または削除、およびすべての署名者証明書名のリスト表示を行うことができます。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。
2. 対象の証明書データベースを選択します。
3. 「**管理**」 > 「**SSL 証明書データベースの編集**」を選択します。
4. 「**署名者証明書**」タブに、すべての署名者証明書名が表示されます。

署名者証明書のインポート

a. 「**管理**」 > 「**インポート**」をクリックします。
b. 「**参照**」をクリックします。次に、インポートする署名者証明書を選択します。
c. 「**証明書ラベル**」フィールドに、署名者証明書のラベルを入力します。
d. 署名者証明書を信頼できる証明書として設定する場合は、「**信頼できる**」を選択します。
e. 「**インポート**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

署名者証明書の表示およびエクスポート

a. 表示する署名者証明書を選択します。
b. 「**管理**」 > 「**表示**」をクリックします。ブラウザーに署名者証明書の内容が表示されます。
c. *オプション:* 「**エクスポート**」をクリックします。次に、ポップアップ表示されるウィンドウで保存操作を確定します。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

署名者証明書のエクスポート

a. エクスポートする署名者証明書を選択します。
b. 「**管理**」 > 「**エクスポート**」をクリックします。
c. ポップアップ表示されるブラウザー・ウィンドウで保存操作を確定します。

署名者証明書の削除

a. 削除する署名者証明書を選択します。
b. 「**削除**」をクリックします。
c. ポップアップ表示されるウィンドウで、「**はい**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

信頼できる証明書または信頼できない証明書としての署名者証明書の設定

a. 編集する署名者証明書を選択します。
b. 「**編集**」をクリックします。
c. 「**信頼できる**」チェック・ボックスを選択またはクリアして、署名者証明書を信頼できる証明書または信頼できない証明書として設定します。
d. 「**保存**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

証明書データベース内の個人証明書の管理

ローカル管理インターフェースを使用して証明書データベース内の個人証明書を管理するには、「SSL 証明書」管理ページを使用します。具体的には、個人証明書のインポート、表示、エクスポート、または削除、すべての個人証明書名のリスト表示、および自己署名個人証明書の作成を行うことができます。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。

2. 対象の証明書データベースを選択します。
3. 「**管理**」 > 「**SSL 証明書データベースの編集**」を選択します。
4. 「**個人証明書**」タブをクリックします。このタブに、すべての個人証明書名が表示されます。

個人証明書のインポート

a. 「**管理**」 > 「**インポート**」をクリックします。
b. 「**参照**」をクリックします。次に、インポートする個人証明書が含まれているファイルを選択します。
c. *オプション:* インポートする個人証明書が含まれているファイルのパスワードを指定します。
d. 「**インポート**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

個人証明書の受信

注: 個人証明書を受信できるのは、対応する認証要求が存在する場合のみです。

a. 「**管理**」 > 「**受信**」をクリックします。
b. 「**参照**」をクリックします。次に、受信する個人証明書を選択します。
c. その個人証明書をデフォルトとして設定する場合は、「**デフォルト**」チェック・ボックスを選択します。
d. 「**受信 (Receive)**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

個人証明書の表示

a. 表示する個人証明書を選択します。
b. 「**管理**」 > 「**表示**」をクリックします。ブラウザーに個人証明書の内容が表示されます。
c. *オプション:* 「**エクスポート**」をクリックします。次に、ポップアップ表示されるウィンドウで保存操作を確定します。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

個人証明書のエクスポート

a. エクスポートする個人証明書を選択します。
b. 「**管理**」 > 「**エクスポート**」をクリックします。

注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。

c. ポップアップ表示されるブラウザー・ウィンドウで保存操作を確定します。

個人証明書の削除

a. 削除する個人証明書を選択します。
b. 「**削除**」をクリックします。
c. ポップアップ表示されるウィンドウで、「**はい**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

個人証明書 (自己署名) の作成

a. 「**新規**」をクリックします。
b. 「**証明書ラベル**」、「**証明書の識別名**」、「**鍵サイズ**」、および「**有効期限**」を入力します。「**有効期限**」のデフォルト値は 365 日です。
c. この個人証明書をデフォルト証明書として設定する場合は、「**デフォルト**」チェック・ボックスを選択します。
d. 「**保存**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

デフォルトとしての個人証明書の設定

a. 編集する個人証明書を選択します。
b. 「**編集**」をクリックします。
c. 「**デフォルトの証明書として設定してください**」チェック・ボックスを選択して、個人証明書をデフォルト証明書として設定します。
d. 「**保存**」をクリックします。

注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

証明書データベース内の認証要求の管理

ローカル管理インターフェースを使用して証明書データベース内の認証要求を管理するには、「SSL 証明書」管理ページを使用します。具体的には、認証要求の作成、表示、エクスポート、または削除、およびすべての認証要求名のリスト表示を行うことができます。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSL 証明書**」を選択します。
2. 対象の証明書データベースを選択します。
3. 「**管理**」 > 「**SSL 証明書データベースの編集**」を選択します。
4. 「**認証要求**」タブをクリックします。このタブに、すべての認証要求名が表示されます。

認証要求の作成

a. 「**新規**」をクリックします。
b. 「**認証要求ラベル**」、「**認証要求の識別名**」、および「**鍵サイズ**」を入力します。
c. 「**保存**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

認証要求の表示およびエクスポート

a. 表示したい認証要求を選択します。
b. 「**管理**」 > 「**表示**」をクリックします。ブラウザーに認証要求の内容が表示されます。
c. *オプション:* 「**エクスポート**」をクリックします。次に、ポップアップ表示されるウィンドウで保存操作を確定します。

認証要求のエクスポート

a. エクスポートしたい認証要求を選択します。
b. 「**管理**」 > 「**エクスポート**」をクリックします。ブラウザーに認証要求の内容が表示されます。
c. ポップアップ表示されるウィンドウで保存操作を確定します。

認証要求の削除

a. 削除したい認証要求を選択します。
b. 「**削除**」をクリックします。
c. ポップアップ表示されるウィンドウで、「**はい**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

SSO 鍵の管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSO 鍵**」を選択します。

現在の SSO 鍵ファイルのリスト

ローカル管理インターフェースを使用して現在のすべての SSO 鍵ファイルをリストするには、「SSO 鍵」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSO 鍵**」を選択します。
2. 現在のすべての SSO 鍵ファイルおよびその最終変更時刻情報を確認できます。

SSO 鍵ファイルの作成

ローカル管理インターフェースを使用して SSO 鍵ファイルを作成するには、「SSO 鍵」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSO 鍵**」を選択します。
2. 「**新規**」をクリックします。
3. 作成する鍵データベースの名前を入力してから、「**保存**」をクリックします。鍵データベース名の名前は、固有でなければなりません。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

SSO 鍵ファイルのインポート

既存の SSO 鍵ファイルをインポートするには、「SSO 鍵」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSO 鍵**」を選択します。
2. 「**管理**」 > 「**インポート**」を選択します。
3. 「**参照**」をクリックします。
4. インポートするファイルが含まれているディレクトリーを参照して、ファイルを選択します。
5. 「**インポート**」をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

SSO 鍵ファイルのエクスポート

ローカル管理インターフェースを使用して SSO 鍵ファイルをエクスポートするには、「SSO 鍵」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSO 鍵**」を選択します。
2. エクスポートする SSO 鍵ファイルを選択します。
3. 「**管理**」 > 「**エクスポート**」を選択します。 ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
4. ブラウザーで確認ウィンドウが表示された場合は、保存操作を確定します。

SSO 鍵ファイルの削除

ローカル管理インターフェースを使用して既存の SSO 鍵ファイルを削除するには、「SSO 鍵」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**SSO 鍵**」を選択します。
2. 削除するファイルを選択します。
3. 「**削除**」をクリックします。
4. ポップアップ表示されるウィンドウで、「**はい**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

LTPA 鍵の管理

ローカル管理インターフェースで「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**LTPA 鍵**」を選択します。

現在のすべての LTPA 鍵ファイルの取得

ローカル管理インターフェースを使用して現在のすべての LTPA 鍵ファイルを取得するには、「LTPA 鍵」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**LTPA 鍵**」を選択します。
2. 現在のすべての LTPA 鍵ファイルおよびその最終変更時刻情報が表示されます。

LTPA 鍵ファイルのインポート

ローカル管理インターフェースを使用して LTPA 鍵ファイルをインポートするには、「LTPA 鍵」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**LTPA 鍵**」を選択します。
2. 「**管理**」 > 「**インポート**」をクリックします。
3. ポップアップ表示されるウィンドウで、「**参照**」 をクリックします。
4. インポートするファイルを選択してから、「**インポート**」をクリックします。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

LTPA 鍵ファイルのエクスポート

ローカル管理インターフェースを使用して LTPA 鍵ファイルをエクスポートするには、「LTPA 鍵」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**LTPA 鍵**」を選択します。

2. エクスポートする LTPA 鍵ファイルを選択します。
3. 「**管理**」 > 「**エクスポート**」をクリックします。

   注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
4. ブラウザーでファイルを保存するように求めるプロンプトが出されたら、保存操作を確定します。

LTPA 鍵ファイルの名前変更

ローカル管理インターフェースを使用して LTPA 鍵ファイルを名前変更するには、「LTPA 鍵」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**LTPA 鍵**」を選択します。
2. 名前変更する LTPA 鍵ファイルを選択します。
3. 「**管理**」 > 「**名前変更**」をクリックします。
4. ポップアップ表示されるウィンドウで、「**新規リソース名**」フィールドに新規名を入力します。
5. 「**保存**」をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

LTPA 鍵ファイルの削除

ローカル管理インターフェースを使用して LTPA 鍵ファイルを削除するには、「LTPA 鍵ファイル」管理ページを使用します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル・キー**」 > 「**LTPA 鍵**」を選択します。
2. 削除する LTPA 鍵ファイルを選択します。
3. 「**削除**」をクリックします。
4. ポップアップ表示されるウィンドウで、「**はい**」をクリックします。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

Kerberos 構成の管理

ローカル管理インターフェースから、以下の Kerberos 設定を作成、編集、削除、およびテストすることができます。

表 4. Kerberos 構成設定の管理

設定	説明
libdefault	Kerberos ライブラリーが使用するデフォルト値が含まれています。
realms	Kerberos レルム名によってキーが付けられたサブセクションが含まれています。各サブセクションには、そのレルム用の Kerberos サーバーがある場所などの、レルム固有の情報が記述されています。
domain realms	ドメイン名およびサブドメインを Kerberos レルム名にマップする関係が含まれています。ホストの完全修飾ドメイン名が分かっていれば、これらの関係をプログラムが使用して、ホストが存在するレルムを判別します。
CA paths	直接的な (非階層的な) クロスレルム認証で使用される認証パスが含まれています。このセクション内のエントリーは、クロスレルム認証で使用できる中間レルムを判別するためにクライアントが使用します。末端のサービスが、信頼できる中間レルム用の transited フィールドをチェックするときにも使用します。
keytab files	Kerberos 認証に使用されるキータブ・ファイルが含まれています。それらのファイルには、Kerberos プリンシパルと暗号化鍵のペアが含まれています。

Kerberos が使用するデフォルト値の管理

LMI 内の「Kerberos 構成」管理ページにある「デフォルト」タブを使用して、以下の設定を管理します。これらの設定は、Kerberos ライブラリーによってデフォルト値として使用されます。

このタスクについて

「デフォルト」タブには、対応する Kerberos 構成ファイルの **libdefault** セクションの設定が含まれています。このセクション内のプロパティーを作成、編集、および削除することができます。自分の Web サーバーのプリンシパル名およびパスワードを使用して、認証をテストすることもできます。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「Kerberos 構成」**を選択します。 現在の Kerberos 構成が表示されます。
2. 「デフォルト」タブで、必要に応じてアクションを実行します。

- プロパティーの作成
  a. 「**新規**」をクリックします。
  b. 「新規プロパティーの作成」ウィンドウで、「**事前定義名**」リストから名前を選択するか、新規プロパティーの名前として「**名前**」フィールドに名前を入力します。
  c. 「**値**」フィールドに新規プロパティーの値を入力します。
  d. 「**保存**」をクリックします。
- プロパティーの編集
  a. テーブルから、編集するプロパティーを選択します。
  b. 「**編集**」をクリックします。
  c. 「プロパティーの編集」ウィンドウで、必要に応じてプロパティーの値を変更します。
  d. 「**保存**」をクリックします。
- プロパティーの削除
  a. テーブルから、削除するプロパティーを選択します。
  b. 「**削除**」をクリックします。
  c. 「アクションの確認」ウィンドウで、「**はい**」をクリックします。
- プリンシパルおよびパスワードを使用した認証のテスト
  a. 「**テスト**」をクリックします。
  b. 「Kerberos 認証のテスト」ウィンドウで、Web サーバー・プリンシパルとして作成されたユーザーの名前を「**ユーザー名**」フィールドに入力します。
  c. 「**パスワード**」フィールドにパスワードを入力します。
  d. 「**テスト**」をクリックします。

レルムの管理

LMI 内の「Kerberos 構成」管理ページにある「レルム」タブを使用して、以下の設定を管理します。これらの設定は、レルム固有の情報を記述します。

このタスクについて

「レルム」タブには、対応する Kerberos 構成ファイルの **realms** セクションの設定が含まれています。このセクション内のレルム、構成サブセクション、およびプロパティーを作成、編集、および削除することができます。自分の Web サーバーのプリンシパル名およびパスワードを使用して、認証をテストすることもできます。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**Kerberos 構成**」を選択します。 現在の Kerberos 構成が表示されます。
2. 「レルム」タブで、必要に応じてアクションを実行します。
   - レルムの作成
     a. 「**新規**」 > 「**レルム**」をクリックします。

b. 「新規レルムの作成」ウィンドウで、「**レルム**」フィールドに新規レルムの名前を入力します。
c. 「**保存**」をクリックします。

- 構成サブセクションの作成
  a. サブセクションを作成するレルムを選択します。
  b. 「**新規**」 > 「**サブセクション**」をクリックします。
  c. 「新規サブセクションの作成」ウィンドウで、「**事前定義名**」リストから名前を選択するか、「**サブセクション**」フィールドに名前を入力します。
  d. 「**保存**」をクリックします。
- プロパティーの作成
  a. プロパティーを作成するレルムまたはサブセクションを選択します。
  b. 「**新規**」 > 「**プロパティー**」をクリックします。
  c. 「新規プロパティーの作成」ウィンドウで、「**事前定義名**」リストから名前を選択するか、「**名前**」フィールドに名前を入力します。
  d. 「**値**」フィールドにプロパティーの値を入力します。
  e. 「**保存**」をクリックします。
- プロパティーの編集
  a. 編集するプロパティーを選択します。
  b. 「**編集**」をクリックします。
  c. 「プロパティーの編集」ウィンドウで、必要に応じて値を変更します。
  d. 「**保存**」をクリックします。
- レルムの削除
  a. テーブルから、削除するレルムを選択します。
  b. 「**削除**」をクリックします。
  c. 「アクションの確認」ウィンドウで、「**はい**」をクリックします。
- プリンシパルおよびパスワードを使用した認証のテスト
  a. 「**テスト**」をクリックします。
  b. 「Kerberos 認証のテスト」ウィンドウで、Web サーバー・プリンシパルとして作成されたユーザーの名前を「**ユーザー名**」フィールドに入力します。
  c. 「**パスワード**」フィールドにパスワードを入力します。
  d. 「**テスト**」をクリックします。

ドメイン・レルム・プロパティーの管理

LMI 内の「Kerberos 構成」管理ページにある「ドメイン」タブを使用して、以下の設定を管理します。これらの設定は、ドメイン名およびサブドメインを Kerberos レルム名にマップする関係を記述するものです。

このタスクについて

「ドメイン」タブには、対応する Kerberos 構成ファイルの **domain_realm** セクションの設定が含まれています。このセクション内のプロパティーを作成、編集、および削除することができます。自分の Web サーバーのプリンシパル名およびパスワ

ードを使用して、認証をテストすることもできます。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**Kerberos 構成**」を選択します。 現在の Kerberos 構成が表示されます。
2. 「ドメイン」タブで、必要に応じてアクションを実行します。
   - ドメイン・レルム・プロパティーの作成
     a. 「**新規**」をクリックします。
     b. 「新規変換の作成」ウィンドウで、「**ローカル DNS 値**」フィールドにローカル DNS アドレスを入力します。
     c. 「**レルム**」リストからレルムを選択します。
     d. 「**保存**」をクリックします。
   - ドメイン・レルム・プロパティーの編集
     a. テーブルから、編集するドメイン・レルム・プロパティーを選択します。
     b. 「**編集**」をクリックします。
     c. 「プロパティーの編集」ウィンドウで、必要に応じてレルムを変更します。
     d. 「**保存**」をクリックします。
   - ドメイン・レルム・プロパティーの削除
     a. テーブルから、削除するドメイン・レルム・プロパティーを選択します。
     b. 「**削除**」をクリックします。
     c. 「アクションの確認」ウィンドウで、「**はい**」をクリックします。
   - プリンシパルおよびパスワードを使用した認証のテスト
     a. 「**テスト**」をクリックします。
     b. 「Kerberos 認証のテスト」ウィンドウで、Web サーバー・プリンシパルとして作成されたユーザーの名前を「**ユーザー名**」フィールドに入力します。
     c. 「**パスワード**」フィールドにパスワードを入力します。
     d. 「**テスト**」をクリックします。

CA パスの管理

LMI 内の「Kerberos 構成」管理ページにある「CA パス」タブを使用して、以下の設定を管理します。これらの設定には、直接的な (非階層的な) クロスレルム認証で使用される認証パスが含まれています。

このタスクについて

「CA パス」タブには、対応する Kerberos 構成ファイルの **capaths** セクションの設定が含まれています。このセクションで、プロパティーおよび CA パスを作成、編集、および削除することができます。自分の Web サーバーのプリンシパル名およびパスワードを使用して、認証をテストすることもできます。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**グローバル設定**」 > 「**Kerberos 構成**」を選択します。 現在の Kerberos 構成が表示されます。
2. 「CA パス」タブで、必要に応じてアクションを実行します。
   - CA パスの作成
     a. 「**新規**」 > 「**クライアント・レルム**」をクリックします。
     b. 「クライアント・レルムの作成」ウィンドウで、「**クライアント・レルム**」フィールドにレルム名を入力します。
     c. 「**保存**」をクリックします。
   - プロパティーの作成
     a. プロパティーを作成するクライアント・レルムを選択します。
     b. 「**新規**」 > 「**プロパティー**」をクリックします。
     c. 「新規プロパティーの作成」ウィンドウで、「**サーバー・レルム**」および「**中間レルム**」の値を指定します。
     d. 「**保存**」をクリックします。
   - プロパティーの編集
     a. テーブルから、編集するプロパティーを選択します。
     b. 「**編集**」をクリックします。
     c. 「プロパティーの編集」ウィンドウで、必要に応じて値を変更します。
     d. 「**保存**」をクリックします。
   - CA パスの削除
     a. テーブルから、削除する CA パスを選択します。
     b. 「**削除**」をクリックします。
     c. 「アクションの確認」ウィンドウで、「**はい**」をクリックします。
   - プロパティーの削除
     a. テーブルから、削除するプロパティーを選択します。
     b. 「**削除**」をクリックします。
     c. 「アクションの確認」ウィンドウで、「**はい**」をクリックします。
   - プリンシパルおよびパスワードを使用した認証のテスト
     a. 「**テスト**」をクリックします。
     b. 「Kerberos 認証のテスト」ウィンドウで、Web サーバー・プリンシパルとして作成されたユーザーの名前を「**ユーザー名**」フィールドに入力します。
     c. 「**パスワード**」フィールドにパスワードを入力します。
     d. 「**テスト**」をクリックします。

キータブ・ファイルの管理

LMI 内の「Kerberos 構成」管理ページにある「鍵ファイル」タブを使用して、以下の設定を管理します。

このタスクについて

「鍵ファイル」タブには、Kerberos 認証に使用されるキータブ・ファイル用の設定が含まれています。キータブ・ファイルをインポート、結合、および削除することができます。Kerberos プリンシパル名およびキータブ・ファイルを使用して、認証をテストすることもできます。

手順

1. 上部のメニューから、**「セキュア: リバース・プロキシー設定」** > **「グローバル設定」** > **「Kerberos 構成」**を選択します。 現在の Kerberos 構成が表示されます。
2. 「鍵ファイル」タブで、必要に応じてアクションを実行します。
   - キータブ・ファイルのインポート
     a. **「インポート」**をクリックします。
     b. 「キータブ・ファイルのインポート」ウィンドウで**「参照」**をクリックします。
     c. インポートするキータブ・ファイルを選択して、**「開く」**をクリックします。
     d. **「インポート」**をクリックします。
   - キータブ・ファイルの削除
     a. テーブルから、削除するファイルを選択します。
     b. **「削除」**をクリックします。
     c. 「アクションの確認」ウィンドウで、**「はい」**をクリックします。
   - キータブ・ファイルの結合
     a. テーブルから、結合するキータブ・ファイルを選択します。
     b. **「結合」**をクリックします。
     c. 「キータブ・ファイルの結合」ウィンドウで、**「新規リソース名」**フィールドに結合されるファイルの名前を入力します。
     d. **「保存」**をクリックします。
   - キータブ・ファイルを使用した認証の検証
     a. テーブルから、テストするキータブ・ファイルを選択します。
     b. **「テスト」**をクリックします。
     c. 「キータブ認証のテスト」ウィンドウで、**「ユーザー名」**フィールドに Kerberos プリンシパルの値を入力します。
     d. **「テスト」**をクリックします。

照会サイトのコンテンツ・ファイルの管理

LMI 内の「照会サイトのコンテンツ」管理ページを使用して、照会サイトのコンテンツ・ファイルを管理します。

手順

1. 上部のメニューから、「**セキュア: リバース・プロキシー設定**」 > 「**ツール**」 > 「**照会サイトのコンテンツ**」を選択します。 すべての照会コンテンツ・ファイルおよびそのバージョン情報が表示されます。
2. 対象のファイルを選択します。
3. ファイルをローカル・ドライブにエクスポートする場合は、「**エクスポート**」をクリックします。

   注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
4. ポップアップ表示されるブラウザー・ウィンドウで保存操作を確定します。

第 7 章 管理: システムの設定

アプライアンスのセキュリティー、ネットワーク、およびシステム設定の構成に関する情報。

更新およびライセンス登録

Security Web Gateway Appliance での更新の管理とライセンス登録に関する情報。

更新およびライセンス登録の概要の表示

「概要」ページには、Security Web Gateway Appliance のファームウェア、不正侵入防御のコンテンツ、更新サーバー、およびライセンスに関する現在の情報が表示されます。

このタスクについて

「概要」ページで、使用可能な更新をインストールできます。ただし、更新を手動で追加したり、更新の有無を確認したり、更新をスケジュールしたりするには、「使用可能な更新」ページにアクセスする必要があります。

手順

1. **「管理: システムの設定」** > **「更新およびライセンス登録」** > **「概要」**をクリックします。
2. 以下の 1 つ以上のアクションを実行します。
   - 使用可能な更新をインストールするには、**「インストール」**をクリックします。
   - ライセンスを登録するには、**「ライセンスの登録」**をクリックします。

     注: 「ライセンスの登録」リンクが表示されるのは、登録されたライセンスがない場合のみです。

     a. 「ライセンス登録」ページで、**「ライセンスの選択」**をクリックして、インストールするライセンス・ファイルを見つけます。

     b. インストールするライセンス・ファイルを選択してから、**「開く」**をクリックします。

     c. **「構成の保存」**をクリックします。

更新のインストール

ファームウェアおよび不正侵入防御の更新をインストールして、Security Web Gateway Appliance およびアプライアンスによって提供されるネットワーク・プロテクションを向上させます。

このタスクについて

重要: ファームウェアの更新をインストールした後に、アプライアンスを再起動する必要があります。

ファームウェアの更新には、新規プログラム・ファイル、フィックスまたはパッチ、機能拡張、およびオンライン・ヘルプが含まれます。

不正侵入防御の更新には、IBM X-Force 研究開発チームが提供する最新のセキュリティー・コンテンツが含まれています。

手順

1. **「管理: システムの設定」 > 「更新およびライセンス登録」 > 「使用可能な更新」**をクリックします。
2. 「使用可能な更新」ページで、以下のコマンドを 1 つ以上使用します。

オプション	説明
アップロード	更新を手動で追加するには、**「アップロード」**をクリックします。「新しい更新」ウィンドウで、**「更新の選択」**をクリックし、更新ファイルを参照し、**「開く」**をクリックしてから、**「送信」**をクリックします。 **注:** 更新を手動で追加した後に、その更新をインストールできます。
最新表示	更新がないかを確認するには、**「最新表示」**をクリックします。
インストール	更新をインストールするには、更新を選択してから、**「インストール」**をクリックします。
スケジュール	更新スケジュールを作成または編集するには、更新を選択してから、**「スケジュール」**をクリックします。「スケジュールの編集」ウィンドウで、以下の 1 つ以上のアクションを実行します。 • 更新スケジュールを削除するには、**「スケジュールの削除」**を選択します。 • 更新スケジュールを作成するには、更新をインストールする日時を選択します。 **「送信」**をクリックして、変更を保存します。

更新スケジュールの構成

更新スケジュールを構成して、X-Force コンテンツの更新を毎日、毎週、または指定した時間間隔に従って受け取ります。

このタスクについて

更新サーバーが過負荷状態にならないように、15 分のバッファーが更新時刻に適用されます。更新は、指定した時刻の最大で 15 分前または 15 分後にダウンロードされます。

手順

1. 「**管理: システムの設定**」 > 「**更新およびライセンス登録**」 > 「**更新スケジュール**」をクリックします。
2. 「更新スケジュール」ペインで、「**自動更新**」を選択して、X-Force コンテンツの更新を受け取ります。
3. 以下のいずれかの方法を使用して、更新をスケジュールします。
   - 更新を毎日受け取るには、「**日次または週次**」を選択し、最初のリストから「**毎日**」を選択してから、2 番目のリストから時刻を選択します。
   - 更新を毎週受け取るには、「**日次または週次**」を選択し、更新を受け取る曜日を選択してから、2 番目のリストから時刻を選択します。
   - 1 時間から 24 時間の範囲のスケジュール間隔で更新を受け取るには、「**指定された間隔**」を選択してから、更新間隔 (分数) を選択します。

     範囲: 60 から 1440 分
4. 「**保存**」をクリックします。

更新サーバー設定の構成

更新ファイルを更新サーバーからダウンロードするようにアプライアンスを構成します。

このタスクについて

順序付けられた複数のサーバーをフェイルオーバー用に構成できます。

注: デフォルトの IBM ISS ライセンスおよび更新サーバーは削除できません。無効にすることはできます。

手順

1. 「**管理: システムの設定**」 > 「**更新およびライセンス登録**」 > 「**更新サーバー**」をクリックします。
2. 「更新サーバー」ペインで、以下のいずれかのアクションを実行します。
   - 更新サーバーを追加するには、「**新規**」をクリックします。「サーバーの追加」ウィンドウが表示されます。
   - 更新サーバーを編集するには、サーバーを選択してから、「**編集**」をクリックします。「サーバーの編集」ウィンドウが表示されます。
   - 更新サーバーを削除するには、サーバーを選択してから、「**削除**」をクリックします。
3. 更新サーバーを追加または編集する際には、「一般」タブで以下のオプションを構成します。

オプション	説明
順序	アプライアンス・ソフトウェアの更新について更新サーバーに照会する順位を定義します。 アプライアンスは、サーバーからの応答が 24 時間より長くかかる場合は、リストの次のサーバーを使用します。

オプション	説明
使用可能	更新サーバーを有効にして、アプライアンスで使用できるようにします。
名前	更新サーバーを記述する名前。
サーバー・アドレス	更新サーバーの IP アドレスまたは DNS 名。
ポート	更新サーバーとの通信にアプライアンスが使用するポート番号。 **ヒント:** IBM ISS Download Center のポート番号は 443 です。内部更新サーバーのデフォルト・ポートは 3994 です。

オプション	説明
信頼レベル	アプライアンスが更新サーバーを認証する方法を定義します。 **明示的 (ユーザー定義)** アプライアンスは、「証明書」ボックスに貼り付けられたローカル証明書を使用して、更新サーバーへの接続を認証します。証明書は、Base64 PEM エンコード・データでなければなりません。 明示的信頼は、最もセキュアな信頼レベルです。明示的信頼証明書は、Base64 PEM エンコード・データでなければなりません。 **明示的 (xpu.iss.net)** アプライアンスは、IBM ISS 更新サーバーのローカル証明書を使用して、更新サーバーへの接続を認証します。IBM ISS 更新サーバーの証明書は、デフォルトで、アプライアンスにインストールされます。証明書は、Base64 PEM エンコード・データです。 明示的信頼は、最もセキュアな信頼レベルです。明示的信頼証明書は、Base64 PEM エンコード・データでなければなりません。 **初回のみ信頼** 証明書がアプライアンス上にない場合は、アプライアンスは、サーバーへの初回接続時にサーバーから証明書をダウンロードします。 「初回のみ信頼」は、「すべて信頼する」よりもセキュアであり、明示的信頼よりセキュアではありません。 **注:** アプライアンスは、証明書をダウンロードした後に、明示的信頼機能に戻ります。 **すべて信頼する** アプライアンスは更新サーバーを信頼し、認証に SSL 証明書を使用しません。 「すべて信頼する」信頼は、最もセキュアではない信頼レベルです。 **重要:** 「すべて信頼する」信頼レベルは、セキュリティー・リスクになります。これは、内部更新サーバーになりすまして、偽のサーバーにリダイレクトできるからです。

4. オプション: プロキシー・サーバーを使用する場合は、「プロキシー設定」タブで以下の設定を構成します。

オプション	説明
プロキシーの使用	アプライアンスが更新サーバー用にプロキシー・サーバーを使用できるようにします。
サーバー・アドレス	プロキシー・サーバーの IP アドレスまたは DNS 名。 **注:** 「**サーバー・アドレス**」フィールドは、「プロキシーの使用」チェック・ボックスを選択した場合に表示されます。
ポート	更新サーバーとの通信にプロキシー・サーバーが使用するポート番号。 **注:** 「**ポート**」フィールドは、「プロキシーの使用」チェック・ボックスを選択した場合に表示されます。
認証の使用	アプライアンスがプロキシー・サーバーを認証できるようにします。
ユーザー名	プロキシー・サーバーに対する認証に必要なユーザー名。 **注:** 「**ユーザー名**」フィールドは、「認証の使用」チェック・ボックスを選択した場合に表示されます。
パスワード	プロキシー・サーバーに対する認証に必要なパスワード。 **注:** 「**パスワード**」フィールドは、「認証の使用」チェック・ボックスを選択した場合に表示されます。

5. 「**送信**」をクリックします。

更新履歴の表示

更新履歴を表示して、アプライアンスでダウンロード、インストール、およびロールバックされたファームウェアおよびセキュリティー・コンテンツの更新を確認します。

このタスクについて

更新をインストールした後に、更新パッケージは、アプライアンスから削除されます。

手順

1. 「**管理: システムの設定**」 > 「**更新およびライセンス登録**」 > 「**更新履歴**」をクリックします。
2. ページを最新表示するには、「**最新表示**」をクリックします。

フィックスパックのインストール

IBM カスタマー・サポートの指示があった場合は、フィックスパックをインストールします。

始める前に

フィックスパックを適用したとき、アプライアンスは、パーティションのバックアップ・コピーを自動的に作成しません。フィックスパックの適用前にパーティションをバックアップする場合は、手動でバックアップを行う必要があります。

制約事項: フィックスパックをアンインストールすることはできません。

このタスクについて

フィックスパックは、現在のパーティションに適用されます。フィックスパックがアプライアンスにインストールされている場合は、フィックスパックをインストールしたユーザー、コメント、パッチ・サイズ、およびインストール日付に関する情報を表示できます。

手順

1. 「**管理**」をクリックしてから、「**フィックスパック**」をクリックします。
2. 「フィックスパック」ペインで、「**新規**」をクリックします。
3. 「フィックスパックの追加」ウィンドウで、「**参照**」をクリックしてフィックスパック・ファイルを見つけてから、「**開く**」をクリックします。
4. 「**送信**」をクリックして、フィックスパックをインストールします。

ライセンスのインストール

アプライアンスの更新を受信するには、現行のライセンス・ファイルをインストールする必要があります。

このタスクについて

IBM 担当員に連絡して、ライセンス登録番号を入手してください。IBM Security Systems License Key Center (https://ibmss.flexnetoperations.com) からライセンスをダウンロードし、登録できます。

手順

1. オプション: アプライアンスを初めて構成しているのではない場合は、「**管理**」 > 「**ライセンス登録**」をクリックします。
2. 「ライセンス登録」ページで、「**ライセンスの選択**」をクリックして、インストールするライセンス・ファイルを見つけます。
3. インストールするライセンス・ファイルを選択してから、「**開く**」をクリックします。
4. 「**構成の保存**」をクリックします。

   注: OCNID は、Order Confirmation Number and ID (注文確認番号および ID) の略語です。

ファームウェア設定の管理

IBM Security Web Gateway Appliance は 2 つのパーティションがあり、それぞれのパーティションに別個のファームウェアが含まれています。ファームウェアの更新をロールバックできるように、パーティションはファームウェアの更新時にスワップされます。

このタスクについて

アプライアンスでどちらかのパーティションをアクティブにすることができます。工場出荷時の状態では、パーティション 1 がアクティブになっていて、現在のリリースの製品のファームウェア・バージョンが含まれています。ファームウェアの更新を適用すると、更新はパーティション 2 にインストールされ、ポリシーおよび設定がパーティション 1 からパーティション 2 にコピーされます。アプライアンスは、パーティション 2 (現在のアクティブ・パーティション) を使用してシステムを再起動します。

注: 工場出荷時には、アプライアンスの両方のパーティションに同じファームウェア・バージョンがインストールされているため、初期ファームウェア構成のバックアップが用意されていることになります。

ヒント: 構成およびポリシー設定をリストアする目的でパーティションをスワップすることは避けてください。構成およびポリシー設定のバックアップおよびリストアには、スナップショットを使用してください。

手順

1. **「管理: システムの設定」 > 「更新およびライセンス登録」 > 「ファームウェア設定」**をクリックします。
2. 「ファームウェア設定」ページで、以下の 1 つ以上のアクションを実行します。

オプション	説明
編集	パーティションに関連付けられたコメントを編集するには、パーティションを選択し、**「編集」**をクリックします。
バックアップの作成	**重要:** ファームウェアのバックアップを作成するのは、IBM カスタマー・サポートによって提供されるフィックスパックをインストールする場合のみにしてください。フィックスパックはアクティブ・パーティションにインストールされ、フィックスパックをアンインストールできないことがあります。 **注:** バックアップ・プロセスが完了するには、数分かかることがあります。

オプション	説明
アクティブに設定	パーティションにインストールされたファームウェアを使用する場合は、そのパーティションをアクティブに設定します。例えば、最近適用された更新およびフィックスパックが含まれていないファームウェアを使用するために、パーティションをアクティブに設定することができます。

3. 「**はい**」をクリックします。 パーティションをアクティブに設定した場合は、アプライアンスは、新たにアクティブ化されたパーティションを使用して、システムを再起動します。

ネットワーク設定

ネットワーク・インターフェースの構成に関する情報と Security Web Gateway Appliance に関する情報です。

アプリケーション・インターフェースの管理

ローカル管理インターフェースを使用してアプリケーション・インターフェースを管理するには、「アプリケーション・インターフェース」管理ページを使用します。

手順

1. 上部のメニューから、「**管理: システムの設定**」 > 「**ネットワーク設定**」 > 「**アプリケーション・インターフェース**」を選択します。 現行のすべてのアプリケーション・インターフェースがタブに表示されます。各タブには、特定のインターフェースの現行のアドレスおよび設定が含まれます。
2. 作業したいインターフェースのタブを選択します。これにより、対応するインターフェース・タブでアドレスを追加、編集、または削除できます。
   - **アドレスの追加**
     a. 「**新規**」をクリックします。
     b. 「アドレスの追加」ページでは、追加するアドレスの詳細を指定します。
        – このアドレスを作成した後に使用可能にする場合は、「**使用可能**」チェック・ボックスを選択します。
        – 「**IPv4**」または「**IPv6**」を選択して、追加するアドレスのタイプを指定します。
          - **IPv4** を選択した場合:
            1) 「**IPv4 設定**」の下で「**静的**」または「**自動**」を選択して、IPv4 アドレスが静的であるのか、それとも DHCP で割り当てられるのかを指定します。

               注: インターフェースあたり 1 つのアドレスのみを自動に設定できます。既存のアドレスが既に自動に設定されている場合、「**自動**」チェック・ボックスは使用不可です。

2) オプション: 前のステップで「**静的**」を選択した場合は、IPv4 アドレスとサブネット・マスクを入力する必要があります。前のステップで「**自動**」を選択した場合は、「**アドレス**」フィールドと「**サブネット・マスク**」フィールドを無視できます。

- 「**IPv6**」を選択した場合は、IPv6 の「**アドレス**」と「**プレフィックス**」を入力します。

– 「**保存**」をクリックします。

- **アドレスの変更**
  – *方法 1:*
    a. テーブルから変更するアドレスを選択します。
    b. 「**編集**」をクリックします。
    c. 「アドレスの編集」ページで、必要に応じて変更を行います。各フィールドの説明については、『アドレスの追加』セクションを参照してください。
    d. 「**保存**」をクリックして、変更内容を保存します。
  – *方法 2:*
    a. テーブルで、編集するフィールドをダブルクリックします。
    b. インラインで変更を行います。

    注: インラインで編集できるのは、一部のフィールドに限られます。
    c. 編集フィールドの外側をクリックして、変更を保存します。
- **アドレスの削除**
  a. テーブルから削除するアドレスを選択します。
  b. 「**削除**」をクリックします。
  c. 「アドレスの削除」ページで「**はい**」をクリックして、削除を確定します。
- **サーバーへのテスト接続**
  a. 「**テスト**」をクリックします。
  b. 「サーバーの ping」ページで、接続をテストするサーバーの IP アドレスまたは名前を入力します。
  c. 「**テスト**」をクリックします。 ping 操作が成功したかどうかを示すメッセージが表示されます。

管理インターフェースの構成

「管理インターフェース」ページを使用して、アプライアンスのネットワーク・セキュリティー・インターフェースを表示および管理できます。

このタスクについて

注: 管理インターフェースの IP アドレスを変更した場合は、今後のセッションでは、Web ブラウザーを新規 IP アドレスに接続してください。

手順

1. **「管理: システムの設定」** > **「ネットワーク設定」** > **「管理インターフェース」**をクリックします。
2. 「管理インターフェース」ページで、**「ホスト名」**を入力します。
3. ネットワーク・ユーザーがゼロ構成ネットワーキングを使用してアプライアンスを見つけることができるようにするには、**「マルチキャスト DNS を使用した管理インターフェースの名前解決を有効にする」**を選択します。
4. **「デフォルト・インターフェース」**を選択します。
5. 他の管理インターフェースを有効にするには、**「インターフェース名 を有効にする」**を選択します。
6. プライマリー・インターフェースのタブをクリックしてから、**「IPV4」**または**「IPV6」**をクリックします。
7. 以下のオプションを構成してください。

オプション	説明
Auto/Manual	IP アドレスを DHCP サーバーから取得する場合は、**「自動」**を選択します。固定 IP アドレス、ネットマスク、およびゲートウェイ (IPv4) またはプレフィックス長 (IPv6) を指定する場合は、**「手動」**を選択します。
アドレス	**「手動」**モードを選択した場合は、インターフェースに使用する IP アドレスを入力します。
ゲートウェイ	**「手動」**モードを選択した場合は、インターフェースのゲートウェイを入力します。
ネットマスク (IPv4)	IPv4 で**「手動」**モードを選択した場合は、インターフェースのサブネット・マスクを入力します。
プレフィックス長 (IPv6)	IPv6 で**「手動」**モードを選択した場合は、インターフェースのプレフィックス長を入力します。

8. 「DNS」タブをクリックしてから、以下のオプションを構成します。

オプション	説明
Auto/Manual	DNS サーバー・アドレスを DHCP サーバーから取得する場合は、**「自動」**を選択します。DNS サーバーを指定する場合は、**「手動」**を選択します。
プライマリー DNS	プライマリー DNS サーバーの IP アドレスを指定します。
セカンダリー DNS	セカンダリー DNS サーバーの IP アドレスを指定します。
ターシャリ DNS	オプションの 3 番目の DNS サーバーの IP アドレスを指定します。

オプション	説明
DNS 検索パス	1 つ以上の DNS 検索パスを指定します。指定するパスは、それぞれコンマで区切ります。

9. セカンダリー・インターフェースのタブをクリックしてから、「**IPV4**」または「**IPV6**」をクリックします。
10. 以下のオプションを構成してください。
    - Auto/Manual
    - アドレス
    - ゲートウェイ
    - ネットマスク (IPv4)
    - プレフィックス長 (IPv6)
11. 「**保存**」をクリックします。

静的ルートの構成

アプライアンス上のペアのプロテクション・インターフェースへの静的ルートを構成して、ネットワーク・ルーターがユーザーをブロック・ページまたは認証ページにリダイレクトできるようにします。

このタスクについて

このタスクは、ユーザー・セグメントとアプライアンスとの間に追加のネットワーク・セグメントが含まれているネットワークでのみ必要になります。

手順

1. 「**管理: システムの設定**」 > 「**ネットワーク設定**」 > 「**静的ルート**」をクリックします。
2. 「静的ルート」ページで、以下のいずれかのアクションを実行します。
    - 「**新規**」をクリックして、ルートを作成します。
    - 既存のルートを選択してから、「**編集**」をクリックします。
3. 各フィールドに次の情報を定義します。
    - 宛先
    - ゲートウェイ
    - メトリック
    - インターフェースまたはセグメント
4. 「**保存**」をクリックします。

フロントエンド・ロード・バランサー

アプライアンスは、指定されたスケジューリング・アルゴリズムに基づいてクライアント要求を適切なリバース・プロキシー・サーバーに自動的に割り当てるフロントエンド・ロード・バランシング機能を備えています。

標準的なセットアップでは、2 つのフロントエンド・ロード・バランサー・サーバーと複数のリバース・プロキシー・サーバーが配置されます。フロントエンド・ロ

ード・バランサーとは、仮想 IP アドレスを使用してクライアントからの要求を受け入れ、指定されたスケジューリング・アルゴリズムに基づいて最適なリバース・プロキシー・サーバーを判別し、そのサーバーに要求を転送するサーバーです。 2 つのフロントエンド・ロード・バランサー間では、各フロントエンド・ロード・バランサーの状態を認識するためにハートビートが送信されています。プライマリー・フロントエンド・ロード・バランサーが使用不可でハートビートを検出できない場合、バックアップ側のロード・バランサーは、プライマリー・ロード・バランサーの仮想 IP アドレスを引き継いで、クライアント要求の受け入れを開始します。

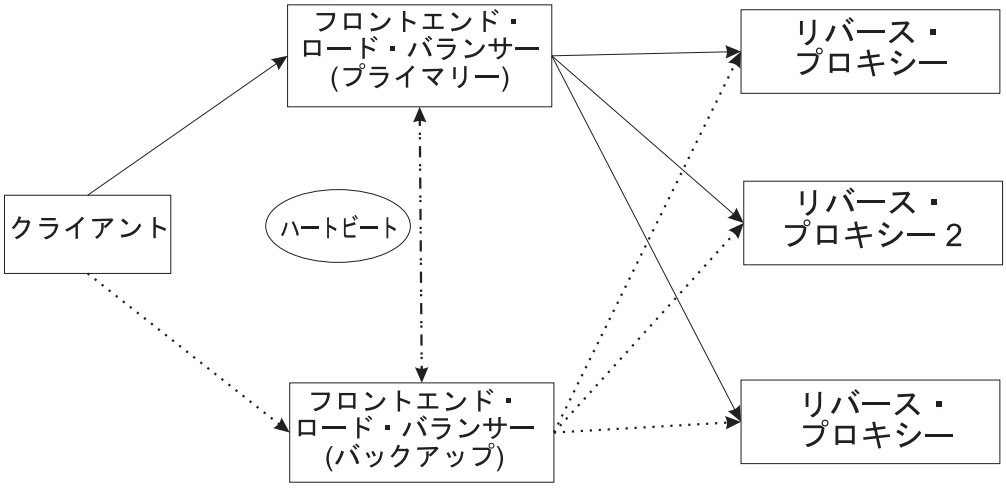

図 1. フロントエンド・ロード・バランサー

注: ご使用の環境で使用できるフロントエンド・ロード・バランサーは、2 つに限られます。

フロントエンド・ロード・バランサーとして機能しているマシン上でリバース・プロキシーの機能を構成することも可能です。ただし、その場合、フロントエンド・ロード・バランサーのパフォーマンスが低下することがあります。このような設定を使用することを決定した場合は、リバース・プロキシーが使用するリソースを考慮する必要があります。

ルーティングを効率的に実行するための十分なリソースが依然としてフロントエンド・ロード・バランサーにあることを確認してください。この構成では、リバース・プロキシーが、構成済みアプリケーション・インターフェースを listen し、また、ロード・バランシング環境用の仮想 IP アドレスを listen するように構成されていなければなりません。

注: ロード・バランシング・サーバーのデフォルト・ゲートウェイとして、バックエンド IP アドレスを設定する必要があります。フロントエンド・ロード・バランサーを使用可能にしたら、各バックエンド・サーバーで設定されているデフォルト・ゲートウェイが、バックエンドの「**アドレス**」フィールドに設定されている値と同じであることを確認してください。

スケジューリング

アプライアンスのフロントエンド・ロード・バランシング機能は、いくつかのタイプのスケジューリングをサポートします。

サポートされるスケジューリング・タイプは以下のとおりです。

lc 最小接続数

rr ラウンドロビン

wlc 重み付き最小接続数

wrr 重み付けラウンドロビン

lblc 局所性ベースの最小接続数

dh 宛先のハッシュ

sh ソースのハッシュ

持続性

持続性とは、クライアントがセッション中に同じリバース・プロキシー・サーバーに確実に接続できるようにするメカニズムです。

持続性の機能は、TCP 層 (第 4 層) で機能します。この機能は、構成を通じて使用可能にしたり、使用不可にしたりできます。

持続性は、クライアント IP アドレスおよび宛先ポート番号で制御されます。

フロントエンド・ロード・バランサーの構成

ローカル管理インターフェースを使用してフロントエンド・ロード・バランサーを構成するには、「フロントエンド・ロード・バランサー」管理ページを使用します。

手順

1. 上部のメニューから、「**管理: システムの設定**」 > 「**ネットワーク設定**」 > 「**フロントエンド・ロード・バランサー**」を選択します。
2. *オプション:* 「**ダイアグラムの表示**」を展開して、ネットワーク図を表示します。ネットワーク図を見ると、構成パネル内で使用されている各種の用語をネットワーク内の対応する場所に関係付けることができます。
3. 「**一般**」タブ・ページで以下を実行します。
   a. このフロントエンド・ロード・バランサーを使用可能にする場合は、「**使用可能**」を選択します。
   b. より多くのデバッグ・メッセージをセキュリティー・ログに送信する場合は、「**デバッグ**」を選択します。
   c. 「**ゲートウェイ**」の下では、

      注: これは、ロード・バランサーと、ロード・バランスの取られたサーバーが通信するネットワークです。

      1) 「**ゲートウェイ・アドレス**」フィールドには、このフロントエンド・ロード・バランサーをプライベート・ネットワークに接続する IP アドレスを指定します。

注: バックエンド・アドレスは、ロード・バランスの取られたサーバーのデフォルト・ゲートウェイとして設定する必要があります。フロントエンド・ロード・バランサーを使用可能にしたら、各バックエンド・サーバーで設定されているデフォルト・ゲートウェイが、前述したバックエンドの「**アドレス**」フィールドに設定されている値と同じであることを確認してください。

2) 「**マスク**」フィールドには、このフロントエンド・ロード・バランサーをプライベート・ネットワークに接続するサブネットのネットワーク・マスクを指定します。

3) 「**インターフェース**」の下のリストからバックエンド・インターフェースを選択します。

d. *オプション:* 「**イベント・ログ**」をクリックし、システム・イベントを表示します。

4. 「**サーバー**」タブ・ページで仮想サーバーと実サーバーを処理します。各仮想サーバーは、ロード・バランスの取られたインターフェース (仮想 IP アドレスおよびポート) に対応しています。各実サーバーは、ロード・バランスの取られたサーバーに対応しています。

- **仮想サーバーを追加**

  a. 「**新規**」をクリックします。

  b. 「仮想サーバーの追加」ページで、追加する仮想サーバーの設定を定義します。

  「**一般**」タブ・ページで以下を実行します。

フィールド	**説明**
使用可能	新規仮想サーバーがアクティブであるかどうかを指定します。
名前	仮想サーバーの名前。
仮想アドレス	この仮想サーバーをパブリック・ネットワークに接続する IP アドレスを指定します。
ポート	この仮想サーバーが listen するポートを指定します。
マスク	仮想サーバーの IP アドレスに適用されるネットワーク・マスクを指定します。
インターフェース	新規仮想サーバーがパブリック・ネットワークに接続するアプライアンス・インターフェースを指定します。

「**スケジューラー**」タブ・ページで以下を実行します。

フィールド	説明
スケジューラー	ジョブを実サーバーに配布するスケジューリング・アルゴリズムを指定します。利用可能な選択項目は以下のとおりです。 • ラウンドロビン • 重み付けラウンドロビン • 最小接続数 • 重み付け最小接続数 • 局所性ベースの最小接続数 • 宛先のハッシュ • ソースのハッシュ
タイムアウト	このパラメーターに指定した時間 (秒) の間、仮想サーバーが非アクティブであると、その仮想サーバーはルーティング・テーブルから削除されます。
再入力	これより前に障害が原因でルーティング・テーブルから削除された仮想サーバーが、このパラメーターに指定した時間 (秒) の間アクティブであると、ルーティング・テーブルに再度追加されます。
持続性	持続的な仮想サーバーの接続をアクティブのままにする時間 (秒) を指定します。この値を指定しない場合、または 0 に設定した場合は、持続性がオフになります。

c. 「**保存**」をクリックします。

- **仮想サーバーの削除**
  a. リストから削除する仮想サーバーを選択します。
  b. 「**削除**」をクリックします。
  c. 確認ページで「**はい**」をクリックします。
- **仮想サーバーの編集**
  – 方法 1:
    a. リストから編集する仮想サーバーを選択します。
    b. 「**編集**」をクリックします。
    c. 「仮想サーバーの編集」ページで、必要に応じて設定を変更します。
    d. 「**保存**」をクリックします。
  – 方法 2:
    a. フィールドをダブルクリックして編集します。

    注: 「**名前**」を除くすべてのフィールドをインラインで編集できます。
    b. インラインで変更を行います。
    c. 編集フィールドの外側をクリックして、変更を保存します。
- **実サーバーの管理**
  a. 仮想サーバーのリストから、実サーバーを関連付ける仮想サーバーを選択します。
  b. 「**実サーバー**」をクリックします。「実サーバー」ページが表示されます。
    – 実サーバーを追加するには、以下を実行します。

1) 「**新規**」をクリックします。
2) ポップアップ表示される「実サーバーの追加」ページで、追加するリバース・プロキシー・サーバーの設定を定義します。

フィールド	説明
使用可能	新規実サーバーがアクティブであるかどうかを指定します。
アドレス	実サーバーの IP アドレスを指定します。
重みづけ	このサーバーの処理能力を他の実サーバーの処理能力の相対値として表す整数を指定します。例えば、2000 を割り当てられたサーバーは、1000 を割り当てられたサーバーの 2 倍の能力を持ちます。重み付きスケジューリング・アルゴリズムは、作業負荷に基づいてこの数値を動的に調整します。

3) 「**保存**」をクリックします。

– 実サーバーを削除するには、以下を実行します。
1) リストから削除する実サーバーを選択します。
2) 「**削除**」をクリックします。
3) 確認ページで「**はい**」をクリックします。

– 実サーバーを編集するには、以下を実行します。
- 方法 1:
1) リストから編集する実サーバーを選択します。
2) 「**編集**」をクリックします。
3) 「実サーバーの編集」ページで、必要に応じて設定を変更します。
4) 「**保存**」をクリックします。
- 方法 2:
1) フィールドをダブルクリックして編集します。

注: 「**アドレス**」を除くすべてのフィールドをインラインで編集できます。

2) インラインで変更を行います。
3) 編集フィールドの外側をクリックして、変更を保存します。

c. 「**クローズ**」をクリックして、フロントエンド・ロード・バランサーのメイン・ページに戻ります。

5. 「**高可用性**」タブ・ページで、フロントエンド・ロード・バランサー機能の高可用性を使用可能にする設定を定義します。例えば、2 番目のフロントエンド・ロード・バランサーを、ご使用の環境の プライマリー・ロード・バランサーまたはバックアップ・ロード・バランサーとして構成します。
a. 「**高可用性を使用可能にする**」チェック・ボックスを選択して、この機能を使用可能にします。
b. 「**プライマリー**」または「**バックアップ**」を選択して、このシステムを プライマリーまたはバックアップのフロントエンド・ロード・バランサーとして指定します。

c. 「**ローカル・アドレス - プライマリー (Local Address - Primary)**」フィールドで、フロントエンド・ロード・バランサーのローカル IP アドレスを選択します。

d. 「**リモート・アドレス - バックアップ (Remote Address - Backup)**」フィールドで、このシステムが他のフロントエンド・ロード・バランサーと通信するために使用する IP アドレスを指定します。このフィールドは、バックアップ・ロード・バランサーが使用されている場合に必要です。

e. 「**正常性検査の間隔**」フィールドで、プライマリーおよびバックアップのフロントエンド・ロード・バランサー間で送信されるハートビート・メッセージの間隔 (秒) を指定します。

f. 「**正常性検査のタイムアウト**」フィールドで、システムが未応答のルーターを使用不可であると宣言してフェイルオーバーを開始するまでに待機する時間 (秒) を指定します。

6. 「**保存**」をクリックして、「フロントエンド・ロード・バランサー」管理ページで行った変更をすべて保存します。

注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

フロントエンド・ロード・バランサーと Web リバース・プロキシーの両方としてのアプライアンスのマルチタスキング

同じアプライアンスにある Web リバース・プロキシーへのロード・バランシングを行うことができるように、アプライアンスを構成することができます。この機能を使用すると、わずか 2 つのアプライアンスで、可用性の高い Web リバース・プロキシー環境を構成できます。この機能は、特に、アプライアンスをフロントエンド・ロード・バランサーとして専用に使用することができない小規模な環境で役立ちます。

このタスクについて

以下の環境の例を使用して、最小限の HA 環境をセットアップするための手順を示します。

注: この手順は、この環境の例のみに固有です。ご使用の環境に合うように変更する必要があります。

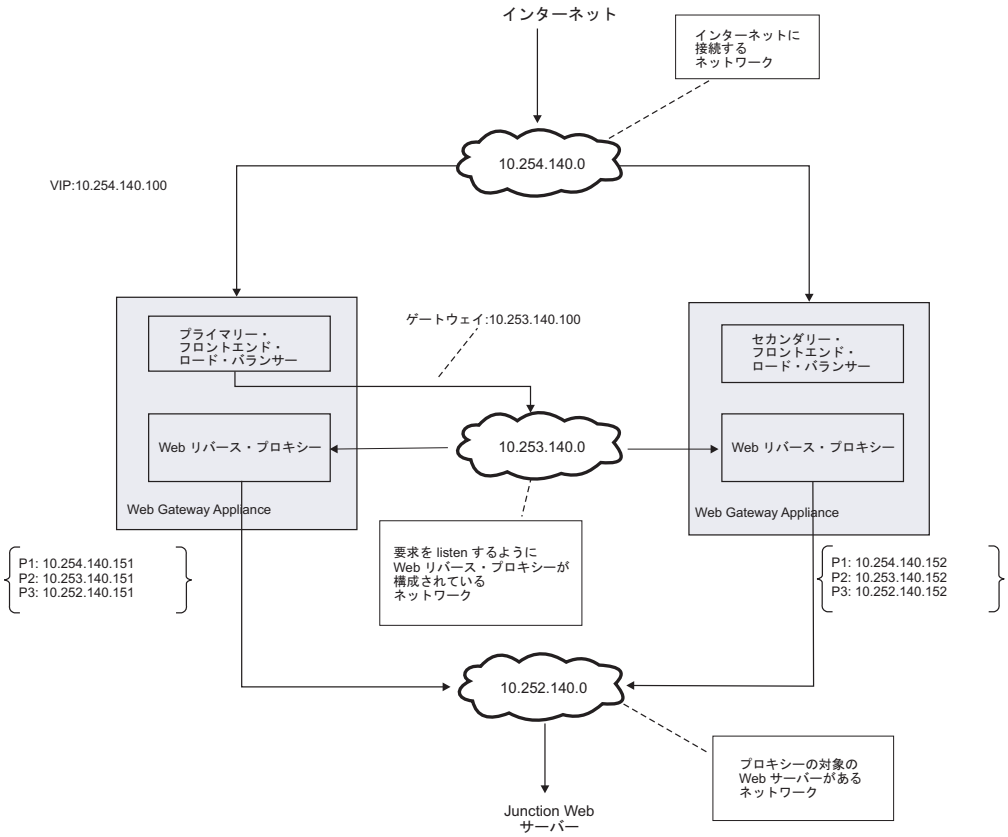

図 2. HA 環境の例

手順

1. それぞれのアプライアンスで、Web リバース・プロキシー・インスタンスを構成します。システムへのアクセス (フロントエンド・ロード・バランサーを介する) に使用されるインターフェースとは異なるインターフェースを listen するように、これらのインスタンスを構成します。この環境の例では、Web リバース・プロキシーは 10.253.140.0 ネットワークを listen するように構成されています。
2. 以下の情報に基づいて、プライマリー・フロントエンド・ロード・バランサーおよびセカンダリー・フロントエンド・ロード・バランサーを構成します。以下の設定は、プライマリー・フロントエンド・ロード・バランサー用のものですが、セカンダリーの構成も類似しています。
   a. 上部のメニューから、「**管理: システムの設定**」 > 「**ネットワーク設定**」 > 「**フロントエンド・ロード・バランサー**」を選択します。
   b. 「一般」タブで、この環境のゲートウェイの詳細を指定します。
      1) 「**ロード・バランサー**」で「**有効**」を選択します。
      2) 「**ゲートウェイ・アドレス**」に `10.253.140.100` と入力します。
      3) 「**マスク**」に `255.255.255.0` と入力します。
      4) 「**インターフェース**」に「**P.2**」を選択します。
   c. 「サーバー」タブで、以下のようにしてこの環境の仮想サーバーの詳細を指定します。
      1) 「**新規**」をクリックします。

2) 「仮想サーバーの追加」ウィンドウで、以下の設定を指定し、「**保存**」をクリックします。
   - **有効**: チェック・マークを付ける
   - **名前**: example-service
   - **仮想アドレス**: 10.254.140.100
   - **ポート**: 80
   - **マスク**: 255.255.255.0
   - **インターフェース**: P.1
3) 「**仮想サーバー**」テーブルで、「**example-service**」エントリーを選択します。
4) 「**実サーバー**」をクリックします。
5) 「**実サーバー - example-service**」ウィンドウで、環境内の Web リバース・プロキシー・インスタンスごとにエントリーを作成します。
   - エントリー 1:
     - **有効**: チェック・マークを付ける
     - **アドレス**: 10.253.140.51
     - **重み**: 1
   - エントリー 2:
     - **有効**: チェック・マークを付ける
     - **アドレス**: 10.253.140.52
     - **重み**: 1

d. 「高可用性」タブで、ピア・フロントエンド・ロード・バランサーの詳細を指定します (サーバーがプライマリー・フロントエンド・ロード・バランサーであるかセカンダリー・フロントエンド・ロード・バランサーであるかによって、このタブ内の詳細は異なります)。
   1) 「**高可用性を使用可能にする**」を選択します。
   2) 「**プライマリー**」を選択します。
   3) 「**ローカル・アドレス - プライマリー**」に、`10.253.140.51` と入力します。
   4) 「**リモート・アドレス - バックアップ**」に、`10.253.140.52` と入力します。

e. 「**保存**」をクリックします。

f. 変更内容が有効になるように、それらをデプロイします。

3. 環境の仮想 IP アドレス (この環境の例では `10.254.140.100`) も listen するように、Web リバース・プロキシー・インスタンスを更新します。

   注: 変更内容を有効にするには、この更新を行った後に必ず Web リバース・プロキシーを再始動してください。

タスクの結果

この構成の制限の 1 つとして、ルーティングが自動的に使用可能になるため、WebSEAL listen インターフェース (この環境の例では 10.253.140.0 ネットワーク) から受信された着信要求は自動的に構成済みゲートウェイ・アドレス (この環境の

例では 10.253.140.100 ネットワーク) を介してルーティングされることが挙げられます。すなわち、WebSEAL listen インターフェースが処理できるのは、フロントエンド・ロード・バランサーの仮想 IP アドレスから発信された要求のみとなります。

ホスト・ファイルの管理

ローカル管理インターフェースでホスト・ファイルを管理するには、「ホスト・ファイル」管理ページを使用します。

手順

1. 上部のメニューから、**「管理: システムの設定」 > 「ネットワーク設定 (Network Settings)」 > 「ホスト・ファイル」**を選択します。 すべての現在のホスト・レコードが IP アドレスおよびホスト名とともに表示されます。
2. これで、ホスト・レコードおよびホスト名を処理できます。
   - **ホスト・レコードの追加**
     a. ルート・レベルの**「ホスト・レコード」**エントリーを選択するか、エントリーを選択しないでください。
     b. **「新規」**をクリックします。
     c. 「ホスト・レコードの作成」ページで、追加するホスト・レコードの IP アドレスおよびホスト名を指定します。
     d. **「保存」**をクリックします。
   - **ホスト・レコードへのホスト名の追加**
     a. ホスト名の追加先のホスト・レコード・エントリーを選択します。
     b. **「新規」**をクリックします。
     c. 「ホスト名をホスト・レコードに追加」ページで、追加するホスト名を入力します。
     d. **「保存」**をクリックします。
   - **ホスト・レコードの削除**
     a. 削除するホスト・レコード・エントリーを選択します。
     b. **「削除」**をクリックします。
     c. 確認ページで、**「はい」**をクリックして削除を確認します。
   - **ホスト・レコードからのホスト名の削除**
     a. 削除するホスト名エントリーを選択します。
     b. **「削除」**をクリックします。
     c. 確認ページで、**「はい」**をクリックして削除を確認します。

     注: 削除されるホスト名が IP アドレスに関連付けられた唯一のホスト名である場合は、ホスト・レコード全体 (IP アドレスとホスト名) が削除されます。

パケット・トレースの管理

ローカル管理インターフェースでパケット・トレースを管理するには、「パケット・トレース」管理ページを使用します。

手順

1. 上部のメニューから、「**管理: システムの設定**」 > 「**ネットワーク設定**」 > 「**パケット・トレース**」を選択します。 パケット・トレースの状況が表示されます。
2. パケット・トレース設定を管理します。
   - **パケット・トレースの開始**
     a. 「**開始**」をクリックします。
     b. 「パケット・トレースの開始」ページで、以下の手順を実行します。
        1) 「**インターフェース**」フィールドで、インターフェースの名前を選択します。

           注: 「**インターフェース**」フィールドで値を選択しなかった場合は、すべてのインターフェースでパケット・トレースが使用可能になります。
        2) 「**フィルター**」フィールドをクリックします。
        3) 「フィルターの設定」ページの「**フィルターの表示**」フィールドで事前定義フィルターを選択するか、「**フィルター・ストリング**」フィールドに手動でフィルターを入力します。
        4) 「**保存**」をクリックします。
        5) 「**最大ファイル・サイズ**」フィールドに、パケット・トレース・ファイル (PCAP ファイル) の最大サイズを定義します。この値はパケット・トレース・ファイルの最大サイズであり、このサイズに達すると、パケット・トレースは使用不可になります。

           注: 「**最大ファイル・サイズ**」フィールドで値を選択しなかった場合、最大ファイル・サイズは、残存ディスク・サイズの半分に設定されます。
     c. 「**開始**」をクリックします。

        注: 同時に実行できるパケット・トレース操作は 1 つのみです。前のトレースの PCAP ファイルが削除されるまで、新規パケット・トレースは開始できません。
   - **パケット・トレースの停止**
     a. 「**停止**」をクリックします。
     b. アクションを確認するには、「**はい**」をクリックします。
   - **パケット・トレース PCAP ファイルのエクスポート**
     a. 「**エクスポート**」をクリックします。

        注: ファイルをエクスポートする前に、アプライアンスのポップアップ・ウィンドウを許可するよう、ブラウザーでポップアップ・ウィンドウをブロックするソフトウェアを構成する必要があります。
     b. ブラウザー・ポップアップ・ウィンドウで保存アクションを確認します。
   - **パケット・トレース PCAP ファイルの削除**
     a. 「**削除**」をクリックします。
     b. アクションを確認するには、「**はい**」をクリックします。

注: パケット・トレースの実行中は、PCAP ファイルを削除することはできません。PCAP ファイルを削除する前に、関連するパケット・トレースを停止する必要があります。

システム設定

Security Web Gateway Appliance でのシステム設定の管理に関する情報。

日時設定の構成

「日時」構成ページを使用して、日付、時刻、タイム・ゾーン、および NTP サーバー情報を構成します。

手順

1. 「**管理: システムの設定**」 > 「**システム設定**」 > 「**日時**」をクリックします。
2. 以下のオプションを構成してください。

オプション	説明
時間帯	アプライアンスのタイム・ゾーンを指定します。
日時	アプライアンスの日、月、年、および時刻を指定します。
NTP サーバー・アドレス	アプライアンスが使用する NTP (NIST Internet Time Service) サーバーをリストします。コンマで区切って複数の NTP サーバーを入力できます。

3. 「**保存**」をクリックします。

管理者設定の構成

アプライアンスへのアクセスに使用するパスワード、およびセッションがタイムアウトになるまでのアイドル時間の長さを変更するには、管理者設定を使用します。

手順

1. 「**管理: システムの設定**」 > 「**システム設定**」 > 「**管理者設定**」をクリックします。
2. 「管理者設定」ページで、「**現在のパスワード**」フィールドに現在のパスワードを入力します。
3. 「**新規パスワード**」フィールドに新規パスワードを入力します。
4. 「**新規パスワードの確認**」フィールドに新規パスワードを入力します。
5. 「**セッション・タイムアウト**」フィールドで、矢印をクリックして、自動的にログアウトするまでにアイドルでいられる期間を選択します。
6. 「**保存**」をクリックします。

管理認証の構成

ローカル管理インターフェースを使用して管理認証を構成するには、「管理認証」管理ページを使用します。

手順

1. 上部のメニューから、「**管理: システムの設定**」 > 「**システム設定**」 > 「**管理認証**」を選択します。 現行の管理認証設定がすべて表示されます。
2. 「メイン」タブで、以下を実行します。
   - ローカル・ユーザー・データベースを認証に使用する場合は、「**ローカル・ユーザー・データベース**」を選択します。
   - リモート LDAP ユーザー・レジストリーを認証に使用する場合は、「**リモート LDAP ユーザー・レジストリー**」を選択します。
     a. 「LDAP」タブで以下のことを行います。
        1) LDAP サーバーの名前を「**ホスト名**」フィールドに指定します。
        2) LDAP サーバーと通信するときに使用するポートを「**ポート**」フィールドに指定します。
        3) LDAP ユーザー・レジストリーが匿名バインドをサポートしている場合は、「**匿名バインド**」チェック・ボックスを選択します。
        4) レジストリーにバインドするために使用されるユーザーの DN を「**バインド DN**」フィールドに指定します。
        5) バインド DN に関連付けられるパスワードを「**バインド・パスワード**」フィールドに指定します。
     b. 「LDAP 一般」タブで以下のことを行います。
        1) ユーザーに指定された認証ユーザー名を保持する LDAP 属性の名前を「**ユーザー属性**」フィールドに指定します。
        2) グループのメンバーを保持するために使用される LDAP 属性の名前を「**グループ・メンバー属性**」フィールドに指定します。
        3) すべての管理ユーザーを収容するために使用されるベース DN を「**ベース DN**」フィールドに指定します。
        4) すべての管理ユーザーが属するグループの DN を「**管理グループ DN**」フィールドに指定します。
     c. LDAP SSL タブで以下を実行します。
        1) システムが LDAP サーバーと通信するときに SSL を使用するかどうかを定義するには、「**SSL を使用可能にする**」チェック・ボックスを選択します。
        2) 鍵データベース・ファイルの名前を「**鍵ファイル名**」フィールドで選択します。
        3) LDAP サーバーがクライアント認証を要求した場合に使用される証明書の名前を「**証明書ラベル**」フィールドで選択します。
3. 「**保存**」をクリックして設定を保存します。

   注: 変更を有効にするには、34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。
4. *オプション:* 「**テスト**」をクリックして、認証をテストします。

   注: まだデプロイされていない管理認証構成が変更されている場合、このテストは、アンデプロイされた構成を使用して実行されます。

a. 「認証のテスト」ウィンドウの「**ユーザー名**」フィールドにユーザー名を入力します。
b. 「**パスワード**」フィールドにパスワードを入力します。
c. 「**テスト**」をクリックします。

認証が成功すると、成功メッセージが表示されます。認証が正常に行われなかった場合は、エラー・メッセージが表示されます。

SSL 管理証明書の処理

ローカル管理インターフェースで「**管理: システムの設定**」 > 「**システム設定**」 > 「**SSL 管理証明書**」を選択します。

現行の SSL 管理証明書の詳細の表示

ローカル管理インターフェースを使用して現行の SSL 管理証明書の詳細を表示するには、「SSL 管理証明書」ページを使用します。

手順

1. 上部のメニューから、「**管理: システムの設定**」 > 「**システム設定**」 > 「**SSL 管理証明書**」を選択します。
2. 現行の管理証明書の詳細が表示されます。

SSL 管理証明書の更新

ローカル管理インターフェースを使用して SSL 管理証明書を更新するには、「SSL 管理証明書」ページを使用します。

手順

1. 上部のメニューから、「**管理: システムの設定**」 > 「**システム設定**」 > 「**SSL 管理証明書**」を選択します。
2. 「**更新**」を選択します。
3. 「**証明書ファイル**」の下で「**参照**」をクリックします。
4. 証明書コンテナー・ファイルを含むディレクトリーを参照して、そのファイルを選択します。

   注: 証明書コンテナー・ファイルは PKCS12 形式 (.p12 ファイル) である必要があり、含めることができる証明書は 1 つのみです。この証明書は、SSL 管理証明書として使用されます。
5. 「**開く**」をクリックします。
6. 「**更新**」をクリックします。更新が成功したという旨のメッセージが表示されます。

   注: 変更を有効にするには、 34 ページの『構成変更のコミット・プロセス』の説明に従って変更をデプロイする必要があります。

拡張チューニング・パラメーターの管理

拡張チューニング・パラメーターの値は、IBM ソフトウェア・サポートの指示があった場合にのみ変更してください。

スナップショットの管理

スナップショットを使用して、以前の構成およびポリシー設定を Security Web Gateway Appliance にリストアできます。スナップショット・ファイルをダウンロードして、アプライアンスを頻繁にバックアップすることをお勧めします。

このタスクについて

スナップショットは、アプライアンスに保管されます。ただし、システム障害に備えて、スナップショットを外部ドライブにダウンロードできます。

手順

1. **「管理: システムの設定」** > **「システム設定」** > **「スナップショット」**をクリックします。
2. 「スナップショット」ペインで、以下の 1 つ以上のコマンドを使用します。

オプション	説明
新規	スナップショットを作成するには、**「新規」**をクリックし、スナップショットを説明するコメントを入力してから、**「保存」**をクリックします。
編集	スナップショットのコメントを編集するには、スナップショットを選択し、**「編集」**をクリックし、新規コメントを入力してから、**「保存」**をクリックします。
削除	スナップショットを削除するには、1 つ以上のスナップショットを選択してから、**「削除」**をクリックします。
適用	スナップショットを適用するには、スナップショットを選択してから、**「適用」**をクリックします。 **注:** 構成またはポリシーのバージョンがファームウェア・バージョンよりも新しい場合は、設定は拒否されます。構成およびポリシーのバージョンがファームウェア・バージョンよりも古い場合は、設定が、現在のファームウェア・バージョンにマイグレーションされます。
ダウンロード	スナップショットをダウンロードするには、スナップショットを選択し、**「ダウンロード」**をクリックし、スナップショットを保存するドライブを参照してから、**「保存」**をクリックします。 **注:** 複数のスナップショットをダウンロードした場合は、スナップショットは 1 つの .zip ファイルに圧縮されます。

オプション	説明
アップロード	スナップショットをアップロードするには、「**アップロード**」をクリックし、アップロードするスナップショットを参照し、スナップショットを選択してから、「**保存**」をクリックします。 **注:** 一度にアップロードできるスナップショットは 1 つだけです。
最新表示	スナップショットのリストを最新表示するには、「**最新表示**」をクリックします。

サポート・ファイルの管理

IBM カスタマー・サポートは、サポート・ファイルを使用して、ユーザーがアプライアンスに関する問題をトラブルシューティングできるようにします。サポート・ファイルには、カスタマー・サポートの問題を診断するために必要なすべてのログ・ファイル、一時ファイルと中間ファイル、およびコマンド出力が含まれます。

このタスクについて

サポート・ファイルには、IP アドレス、ホスト名、ユーザー名、およびポリシー・ファイルなど、お客様を識別できる情報が含まれる可能性があります。サポート・ファイルには、パスワード、証明書、鍵などの機密情報が含まれる場合もあります。サポート・ファイルの内容は、.zip ファイルとして保管されます。サポート・ファイル内のファイルは、すべてお客様が調べて検閲できます。

ヒント: 経時的に問題を追跡するために、複数のサポート・ファイルを作成できます。

手順

1. 「**管理: システムの設定**」 > 「**システム設定**」 > 「**サポート・ファイル**」をクリックします。
2. 「サポート・ファイル」ペインで、以下の 1 つ以上のコマンドを使用します。

オプション	説明
新規	サポート・ファイルを作成するには、「**新規**」をクリックし、サポート・ファイルを説明するコメントを入力してから、「**保存**」をクリックします。新規サポート・ファイルがアプライアンス上に作成されます。
編集	サポート・ファイルのコメントを編集するには、サポート・ファイルを選択し、「**編集**」をクリックし、新規コメントを入力してから、「**保存**」をクリックします。
削除	サポート・ファイルを削除するには、サポート・ファイルを選択してから、「**削除**」をクリックします。

オプション	説明
ダウンロード	サポート・ファイルをダウンロードするには、サポート・ファイルを選択し、「**ダウンロード**」をクリックし、サポート・ファイルを保存するドライブを参照してから、「**保存**」をクリックします。 **注:** 複数のサポート・ファイルをダウンロードした場合は、ファイルは 1 つの .zip ファイルに圧縮されます。

システム・アラートの構成

システム設定に対する変更およびシステムでの問題について、システムが通知を送信する条件を構成します。

このタスクについて

使用可能なアラートには、システムで事前定義されたシステム・アラートおよびユーザーが作成した任意のアラート・オブジェクトがあります。

手順

1. 「**管理: システムの設定**」 > 「**システム設定**」 > 「**システム・アラート**」をクリックします。
2. 「システム・アラート」ペインで、以下の 1 つ以上のタスクを実行します。
   - システムでの問題の通知を受け取るには、「使用可能なオブジェクト」ペインから 1 つ以上のシステム・アラート・オブジェクトを選択して、追加します。
   - アラート・オブジェクトを作成または編集するには、以下の関連トピックを参照して、以下の 1 つ以上のアラート・オブジェクトを構成します。
     - 129 ページの『メール・アラート・オブジェクトの構成』
     - 130 ページの『リモート Syslog アラート・オブジェクトの構成』
     - 『SNMP アラート・オブジェクトの構成』
   - システム・アラートを削除するには、アラートを選択してから「**削除**」をクリックします。

SNMP アラート・オブジェクトの構成

SNMP アラート・オブジェクトを構成して、システムがシステム・アラートを SNMP マネージャーに送信します。

手順

1. 「**管理: システムの設定**」 > 「**システム設定**」 > 「**システム・アラート**」をクリックします。
2. 「システム・アラート」ページで、以下のいずれかのアクションを実行します。
   - 「**新規**」 > 「**SNMP**」をクリックします。
   - 既存のオブジェクトを選択してから、「**編集**」をクリックします。

3. アラート・オブジェクトの名前を入力します。
4. リストからトラップ・バージョンを選択します。
5. 「SNMP マネージャー・アドレス」ボックスで、SNMP マネージャーの IP アドレス、ホスト名、または完全修飾ドメイン名 (FQDN) を入力します。

   注: SNMP ホストは、SNMP トラップを送信するために、アプライアンスからアクセスできる必要があります。
6. SNMP マネージャーが通知がないかをモニターするポート番号を入力します。

   注: デフォルト・ポート番号は 162 です。
7. SNMP アラート・オブジェクトを説明するコメントを入力します。
8. トラップ・バージョン V1 または V2c の場合は、SNMP エージェントに認証するために使用するコミュニティーの名前を入力します。
9. トラップ・バージョン 3 の場合は、以下のオプションを構成します。

オプション	説明
名前	SNMP データベースで認証するユーザー名を入力します。
通知タイプ	「**通知タイプ**」タブの「**SNMP トラップ・バージョン**」フィールドで、「**通知 (Inform)**」または「**トラップ**」を選択します。
認証	「**認証およびプライバシー**」タブで、「**有効**」を選択して認証を有効にし、認証パスフレーズを入力してから、認証タイプを選択します。
プライバシー	「**有効**」を選択してプライバシーを有効にし、プライバシー・パスフレーズを入力してから、プライバシー・タイプを選択します。

10. 「**保存**」をクリックします。

メール・アラート・オブジェクトの構成

メール・アラート・オブジェクトを作成して、指定イベントがネットワークで発生したときにメール通知を指定ユーザーまたは管理者に送信できます。また、検出されたイベントに関する重要な情報が提供されるように、メッセージに含めるイベント・パラメーターを選択することもできます。

手順

1. 「**管理: システムの設定**」 > 「**システム設定**」 > 「**システム・アラート**」をクリックします。
2. 「システム・アラート」ページで、以下のいずれかのアクションを実行します。
   - 「**新規**」 > 「**E メール**」をクリックします。
   - 既存の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てください。

オプション	説明
名前	応答の、意味のある名前を指定します。 **注:** この名前は、イベントの応答を選択する際に表示されるため、ユーザーが何を選択しているのかを簡単に特定できるような名前を応答に付けてください。
差出人	アラート・メールの「**差出人**」フィールドに表示されるメール・アドレスを指定します。
宛先	アラートを受け取るメール・アドレスまたはメール・アドレスのグループを指定します。 **注:** 各メール・アドレスはコンマまたはセミコロンで区切ってください。
SMTP サーバー	メール・サーバーの完全修飾ドメイン名または IP アドレスを指定します。 **注:** SMTP サーバーは、メール通知を送信するために、アプライアンスからアクセスできる必要があります。
SMTP ポート	SMTP サーバーへの接続に使用するカスタム・ポートを指定します。 デフォルトは 25 です。
コメント	メール・アラート・オブジェクトを識別するコメントを入力します。

4. 「**保存**」をクリックします。

リモート Syslog アラート・オブジェクトの構成

リモート Syslog アラート・オブジェクトを構成して、システムがリモート・ログ・ファイルにシステム・イベントを記録します。

手順

1. 「**管理: システムの設定**」 > 「**システム設定**」 > 「**システム・アラート**」をクリックします。
2. 「システム・アラート」ページで、以下のいずれかのステップを実行します。
   - 「**新規**」 > 「**リモート Syslog**」をクリックします。
   - 既存のリモート Syslog アラート・オブジェクトを選択して、「**編集**」をクリックします。
3. 以下のオプションを構成してください。

オプション	説明
名前	応答の、意味のある名前を指定します。
リモート Syslog コレクター	ログを保存するホストの完全修飾ドメイン名または IP アドレスを指定します。 **注:** このホストは、アプライアンスからアクセス可能でなければなりません。
リモート Syslog コレクター・ポート	Syslog コレクターに接続するために使用するカスタム・ポートを指定します。デフォルトは 514 です。

オプション	説明
コメント	リモート Syslog アラート・オブジェクトを識別するコメントを入力します。

4. 「**保存**」をクリックします。

アプライアンスの再起動またはシャットダウン

「再起動またはシャットダウン」ページを使用して、アプライアンスを再起動またはシャットダウンします。

このタスクについて

重要: アプライアンスの再起動中またはシャットダウン時は、トラフィックがアプライアンスを通過せず、ネットワークが保護されない可能性があります。

手順

1. 「**管理: システムの設定**」 > 「**システム設定**」 > 「**再起動またはシャットダウン**」をクリックします。
2. 以下のタスクのいずれかを実行します。

オプション	説明
「再起動」をクリックして、アプライアンスを再起動します。	アプライアンスを再起動すると、アプライアンスは数分間オフラインになります。
「シャットダウン」をクリックして、アプライアンスをオフにします。	アプライアンスをシャットダウンするとアプライアンスはオフラインになり、再起動するまでネットワークを介してアクセスできなくなります。

3. 「**はい**」をクリックします。

第 8 章 トラブルシューティング

アプライアンスの問題をトラブルシューティングする方法についての情報。

IPMItool

ハードウェア・アプライアンスを使用している場合は、IPMItool を使用して Baseboard Management Controller (BMC) モジュールを管理できます。 IPMItool を仮想アプライアンスと共に使用することはできません。

IPMItool は、Intelligent Platform Management Interface (IPMI) をサポートするデバイスをモニター、構成、および管理するユーティリティーです。 IPMI は、標準化されたメッセージ・ベースのハードウェア管理インターフェースです。 Baseboard Management Controller (BMC) または Management Controller (MC) と呼ばれるハードウェア・チップは、IPMI のコアを実装しています。

BMC は、システム・ハードウェアの健全性をモニターするために必要な主要なインターフェースを提供します。ユーザー・チャネル、モニター要素 (温度、電圧、ファン速度、バス・エラーなど)、手動による復旧 (ローカル・システムまたはリモート・システムのリセット操作と電源オン/オフ操作) 用のインターフェースと、状況が異常または「範囲外」の場合、将来の検査およびアラートのために、オペレーティング・システムの介入なしでロギングを行うためのインターフェースが用意されています。 BMC の電源は常にオンであることに注意することが重要です。 BMC には、たとえメイン・システムがオフであっても、オペレーティング・システムがクラッシュしていても IPMI を実行する小型のプロセッサーが組み込まれています。そのため、ローカル・ハードウェアの状況を別のサーバーから確認するように BMC を構成することができ、安全なリモート・モニターおよび復旧 (システム・リセットなど) が可能です。これは、プラットフォームの状況に関わらず行うことができます。

IPMItool にアクセスするには、以下のステップを実行します。

1. root ユーザーとしてコマンド行インターフェース (CLI) にログオンします。
2. **ハードウェア** メニューを入力します。
3. `ipmitool` を入力します。

   注: IPMItool は、ハードウェア・アプライアンスと共にのみ実行できます。仮想アプライアンスから IPMItool を開始しようとすると、エラーが戻されます。
4. BMC モジュールを管理するための特定のコマンドを必要に応じて入力します。

   IPMItool コマンドのリストを表示するには、`# ipmitool help` と入力します。

   コマンドの後に単語と help を追加すると、多数ある IPMItool コマンドの中から、特定の IPMItool コマンドのヘルプを表示することもできます。例えば、`# ipmitool channel help` です。

自己診断機能のテストの実行 (ハードウェア・アプライアンスのみ)

ハードウェア・アプライアンスは、トラブルシューティングに役立つ自己診断機能プログラムを備えています。この機能は仮想アプライアンスでは使用できません。

手順

1. アプライアンスをリブートします。
2. コンソールの「GNU GRUB」メニューから「**ハードウェア診断**」オプションを選択します。 このオプションを選択すると、診断プログラムが実行を開始します。アプライアンスがブートを完了した後、コンソールから診断プログラムにアクセスできるようになります。
3. 診断テストを実行するには、`phdiag <test_name>` と入力します。ここで `<test_name>` は、以下の値 (太字) のいずれかです。

   すべて すべての標準テストを実行します (ストレージ不良ブロック・テストは除く。これはデフォルトです)。

   lcd LCD テストを実行します。

   システム
   標準システム・テスト (MTM-Serial、Inventory、PSU、FAN、SEL) を実行します。

   ネットワーク
   ネットワーク・ポート・テスト (自己診断テスト、トラフィック) を実行します。

   ストレージ
   ストレージ・テスト (SMART、FSCK) を実行します。

   badblocks
   ストレージ不良ブロック・テストを実行します。

エラー HPDBG1005E: LDAP サーバーに接続できませんでした

このエラーは、アプライアンス上のスタンドアロン・ポリシー・サーバーおよび LDAP を使用してリモート・システム上のランタイム環境を構成するときに発生します。

アプライアンス上のスタンドアロン・ポリシー・サーバーおよび LDAP を使用して Windows 上のランタイム環境を構成するには、独立した LDAP サーバーが必要です。この LDAP サーバーは、ランタイム環境の構成を開始する前にセットアップする必要があります。これには、既存の LDAP サーバーを使用することもできますし、この目的専用にセットアップした一時的な LDAP サーバーを使用することもできます。ランタイム環境の構成時に LDAP は変更されません。

このセットアップが必要であるのは、初期構成プロセス時に LDAP サーバーが実行中であるかどうかが Windows 上のランタイム環境で検査されるからです。実行中の LDAP サーバーが検出されなかった場合、ランタイム環境の構成は失敗します。Windows 上のランタイム環境でこの LDAP サーバーが使用されるのは、最初に LDAP サーバーに接続して実行中であるかどうかを確認するときのみです。

既存のユーザー・セッションがあることによるログインの失敗

別のユーザーがログインしているときにローカル管理インターフェースにログインしようとすると、「ログインに失敗しました。セッションは既に存在します。」というエラーが表示されます。ログインするためには、既存のユーザー・セッションを強制終了するように選択する必要があります。

手順

1. ログイン・ページで、ユーザー名とパスワードを入力します。
2. 「**すべての既存のセッションを強制終了します**」チェック・ボックスを選択します。 このオプションが選択された場合、既存のユーザー・セッションが削除されて、新規ユーザーがログインできるようになります。既存のセッションでのユーザーがさらに操作を試みると、そのユーザーに対し、「セッションは強制終了されました」というエラー・メッセージと共にログイン・ページが表示されます。既存のユーザー・セッションでの変更は、保存されていなければ、すべて失われます。保存されたがデプロイされていない変更は、新規ユーザーのセッションで表示されます。

   注: LMI にアクセスした後にブラウザー・ウィンドウを閉じても、セッションはシステム上でアクティブのままとなります。次回 LMI にログインするときには、「**すべての既存のセッションを強制終了します**」チェック・ボックスを選択する必要があります。
3. 「**ログイン**」をクリックします。

USB ブート・ドライブからのファームウェアのインストール: Windows

Windows OS で USB ブート・ドライブを作成し、それを使用して Security Web Gateway Appliance にファームウェアをインストールします。

このタスクについて

アプライアンスが正常に機能しない原因となっているソフトウェアおよび構成のエラーを解決するために、新規ファームウェアのインストールを選択できます。例えば、この手順を使用して、ソフトウェア・エラーのためにブートしないアプライアンスに新規ファームウェアをインストールできます。

アプライアンスの問題をトラブルシューティングする際のヘルプについては、IBM サポート・ポータルを参照してください。

手順

1. アプライアンスのファームウェアをダウンロードして、ネットワーク内のセキュア・ホストに保存します。
2. USB フラッシュ・ドライブを同じホスト上の USB ポートに挿入し、オペレーティング・システムが USB フラッシュ・ドライブを割り当てた場所をメモします。
3. イメージ書き込みプログラムを使用して、USB フラッシュ・ドライブの内容をファームウェア・イメージで上書きします。

ヒント: Windows 用の一般的な書き込みプログラムには、Win32DiskImager.exe や USB Image Tool があります。

4. アプライアンスをオフにします。
5. USB フラッシュ・ドライブをアプライアンスに接続し、アプライアンスをオンにします。 アプライアンスが、USB ブート・ドライブからブートします。
6. インストーラー・コマンド行インターフェースに管理者としてログオンします。
   - `install login: admin`
   - `password:admin`

   ヒント: `help` と入力することで、現行モードで使用可能なコマンドのリストを表示できます。
7. `restore` と入力します。
8. `YES` と入力して、Enter を押します。

   注: インストールが完了するには、約 30 分かかります。
   ファームウェアがインストールされ、アプライアンスが再起動します。

USB ブート・ドライブからのファームウェアのインストール: Linux

Linux オペレーティング・システムで USB ブート・ドライブを作成し、それを使用してアプライアンスにファームウェアをインストールします。

このタスクについて

アプライアンスが正常に機能しない原因となっているソフトウェアおよび構成のエラーを解決するために、新規ファームウェアのインストールを選択できます。例えば、この手順を使用して、ソフトウェア・エラーのためにブートしないアプライアンスに新規ファームウェアをインストールできます。

アプライアンスの問題をトラブルシューティングする際のヘルプについては、IBM サポート・ポータルを参照してください。

手順

1. アプライアンスのファームウェアをダウンロードして、ネットワーク内のセキュア・ホストに保存します。
2. USB フラッシュ・ドライブを同じホスト上の USB ポートに挿入し、オペレーティング・システムが USB フラッシュ・ドライブを割り当てた場所をメモします。
3. イメージ書き込みプログラムを使用して、USB フラッシュ・ドライブの内容をファームウェア・イメージで上書きします。

   ヒント: ほとんどの Linux ディストリビューションには、USB ImageWriter が含まれています。
4. アプライアンスをオフにします。
5. USB フラッシュ・ドライブをアプライアンスに接続し、アプライアンスをオンにします。 アプライアンスが、USB ブート・ドライブからブートします。
6. インストーラー・コマンド行インターフェースに管理者としてログオンします。

- install login: admin
- password:admin

ヒント: help と入力することで、現行モードで使用可能なコマンドのリストを表示できます。

7. restore と入力します。
8. YES と入力して、Enter を押します。

注: インストールが完了するには、約 30 分かかります。
ファームウェアがインストールされ、アプライアンスが再起動します。

USB ブート・ドライブからのファームウェアのインストール: Mac OS

Mac OS で USB ブート・ドライブを作成し、それを使用してアプライアンスにファームウェアをインストールします。

このタスクについて

アプライアンスが正常に機能しない原因となっているソフトウェアおよび構成のエラーを解決するために、新規ファームウェアのインストールを選択できます。例えば、この手順を使用して、ソフトウェア・エラーのためにブートしないアプライアンスに新規ファームウェアをインストールできます。

アプライアンスの問題をトラブルシューティングする際のヘルプについては、IBM サポート・ポータルを参照してください。

手順

1. アプライアンスのファームウェアをダウンロードして、ネットワーク内のセキュア・ホストに保存します。
2. セキュア・ホスト上で、ターミナル・アプリケーションを開きます。
3. 「ターミナル」アプリケーション・ウィンドウで、diskutil list を実行して、現在のデバイス・リストを取得します。
4. USB フラッシュ・ドライブをセキュア・ホストに接続します。
5. diskutil list を再度実行して、システムが USB ドライブを割り当てたデバイス・ノードを判別します。
6. sudo dd if=/path/to/downloaded.img of=/dev/rdiskN bs=1m を実行します。/path/to/downloaded.img は、ファームウェア・ファイルへのパスで置き換えてください。

   注: 以下のエラーが表示される場合は、bs=1m を bs=1M で置き換えてください。

   ```
   dd: Invalid number `1m', you are using GNU dd
   ```

7. diskutil eject /dev/diskN を実行し、コマンドの完了後にデバイスを取り外します。
8. アプライアンスをオフにします。
9. USB フラッシュ・ドライブをアプライアンスに接続し、アプライアンスをオンにします。 アプライアンスが、USB ブート・ドライブからブートします。

10. インストーラー・コマンド行インターフェースに管理者としてログオンします。
    - `install login: admin`
    - `password:admin`

    ヒント: `help` と入力することで、現行モードで使用可能なコマンドのリストを表示できます。
11. `restore` と入力します。
12. `YES` と入力して、Enter を押します。

    注: インストールが完了するには、約 30 分かかります。
    ファームウェアがインストールされ、アプライアンスが再起動します。

ハードウェア・アプライアンスの消去: Windows

ドライブ上に以前に存在したすべてのデータをリカバリーできないようにする場合は、ハードウェア・アプライアンスに対してセキュア消去を実行します。

このタスクについて

ハードウェア・アプライアンスを IBM に戻して交換ユニットを入手するプロセスの一環として、またはアプライアンスを破棄する前に、アプライアンスを消去する場合があります。ソフトウェアまたは構成のエラーが原因でブートしないアプライアンスを消去できます。また、何らかのハードウェア障害が発生しているアプライアンスも消去できます。ただし、ハード・ディスクの障害などの一部のハードウェア障害では、消去は機能しないことがあります。

アプライアンスを削除しても、機能がアプライアンスにリストアされることはありません。

手順

1. アプライアンスのファームウェアをダウンロードして、ネットワーク内のセキュア・ホストに保存します。
2. USB フラッシュ・ドライブを同じホスト上の USB ポートに挿入し、オペレーティング・システムが USB フラッシュ・ドライブを割り当てた場所をメモします。
3. イメージ書き込みプログラムを使用して、USB フラッシュ・ドライブの内容をファームウェア・イメージで上書きします。

    ヒント: Windows 用の一般的な書き込みプログラムには、Win32DiskImager.exe や USB Image Tool があります。
4. アプライアンスをオフにします。
5. USB フラッシュ・ドライブをアプライアンスに接続し、アプライアンスをオンにします。 アプライアンスが、USB ブート・ドライブからブートします。
6. インストーラー・コマンド行インターフェースに管理者としてログオンします。
    - `install login: admin`
    - `password:admin`

ヒント: `help` と入力することで、現行モードで使用可能なコマンドのリストを表示できます。

7. `wipe` と入力して、Enter を押します。

注: 消去の手順が完了するには、約 30 分かかります。

ハードウェア・アプライアンスの消去: Linux

ドライブ上に以前に存在したすべてのデータをリカバリーできないようにする場合は、ハードウェア・アプライアンスに対してセキュア消去を実行します。

このタスクについて

ハードウェア・アプライアンスを IBM に戻して交換ユニットを入手するプロセスの一環として、またはアプライアンスを破棄する前に、アプライアンスを消去する場合があります。ソフトウェアまたは構成のエラーが原因でブートしないアプライアンスを消去できます。また、何らかのハードウェア障害が発生しているアプライアンスも消去できます。ただし、ハード・ディスクの障害などの一部のハードウェア障害では、消去は機能しないことがあります。

アプライアンスを削除しても、機能がアプライアンスにリストアされることはありません。

手順

1. アプライアンスのファームウェアをダウンロードして、ネットワーク内のセキュア・ホストに保存します。
2. USB フラッシュ・ドライブを同じホスト上の USB ポートに挿入し、オペレーティング・システムが USB フラッシュ・ドライブを割り当てた場所をメモします。
3. イメージ書き込みプログラムを使用して、USB フラッシュ・ドライブの内容をファームウェア・イメージで上書きします。

   ヒント: ほとんどの Linux ディストリビューションには、USB ImageWriter が含まれています。
4. アプライアンスをオフにします。
5. USB フラッシュ・ドライブをアプライアンスに接続し、アプライアンスをオンにします。 アプライアンスが、USB ブート・ドライブからブートします。
6. インストーラー・コマンド行インターフェースに管理者としてログオンします。
   - `install login: admin`
   - `password:admin`

   ヒント: `help` と入力することで、現行モードで使用可能なコマンドのリストを表示できます。
7. `wipe` と入力して、Enter を押します。

   注: 消去の手順が完了するには、約 30 分かかります。

ハードウェア・アプライアンスの消去: Mac OS

ドライブ上に以前に存在したすべてのデータをリカバリーできないようにする場合は、ハードウェア・アプライアンスに対してセキュア消去を実行します。

このタスクについて

ハードウェア・アプライアンスを IBM に戻して交換ユニットを入手するプロセスの一環として、またはアプライアンスを破棄する前に、アプライアンスを消去する場合があります。ソフトウェアまたは構成のエラーが原因でブートしないアプライアンスを消去できます。また、何らかのハードウェア障害が発生しているアプライアンスも消去できます。ただし、ハード・ディスクの障害などの一部のハードウェア障害では、消去は機能しないことがあります。

アプライアンスを削除しても、機能がアプライアンスにリストアされることはありません。

手順

1. アプライアンスのファームウェアをダウンロードして、ネットワーク内のセキュア・ホストに保存します。
2. セキュア・ホスト上で、ターミナル・アプリケーションを開きます。
3. 「ターミナル」アプリケーション・ウィンドウで、`diskutil list` を実行して、現在のデバイス・リストを取得します。
4. USB フラッシュ・ドライブをセキュア・ホストに接続します。
5. `diskutil list` を再度実行して、システムが USB ドライブを割り当てたデバイス・ノードを判別します。
6. `sudo dd if=/path/to/downloaded.img of=/dev/rdiskN bs=1m` を実行します。`/path/to/downloaded.img` は、ファームウェア・ファイルへのパスで置き換えてください。

   注: 以下のエラーが表示される場合は、`bs=1m` を `bs=1M` で置き換えてください。

   ```
   dd: Invalid number `1m', you are using GNU dd
   ```
7. `diskutil eject /dev/diskN` を実行し、コマンドの完了後にデバイスを取り外します。
8. アプライアンスをオフにします。
9. USB フラッシュ・ドライブをアプライアンスに接続し、アプライアンスをオンにします。 アプライアンスが、USB ブート・ドライブからブートします。
10. インストーラー・コマンド行インターフェースに管理者としてログオンします。
    - `install login: admin`
    - `password:admin`

    ヒント: `help` と入力することで、現行モードで使用可能なコマンドのリストを表示できます。
11. `wipe` と入力して、Enter を押します。

注: 消去の手順が完了するには、約 30 分かかります。

技術サポート

IBM Security では、サポートを受ける資格をお持ちのお客様に対して技術サポートを提供しています。

IBM サポート・ポータル

問題について IBM Security Solutions に連絡する前に、IBM サポート・ポータル (http://www.ibm.com/software/support) を参照してください。

IBM ソフトウェア・サポート・ガイド

技術サポートに連絡する必要がある場合は、IBM ソフトウェア・サポート・ガイド (http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html) に記載されている方法に従ってください。

このガイドには、以下の情報が記載されています。

- サポートを受けるための登録および資格要件
- お客様の所在国におけるカスタマー・サポートの電話番号
- 電話する前に収集しておく必要がある情報

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あり、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
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更に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。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラット

フォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年).このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。© Copyright IBM Corp. _年を入れる_. All rights reserved.

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 商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、PostScript は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency の登録商標です。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Centrino、Intel Centrino ロゴ、Celeron、Xeon、Intel SpeedStep、Itanium、Pentium は、Intel Corporation または子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。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

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。

ITIL は英国 The Minister for the Cabinet Office の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

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。

Cell Broadband Engine、Cell/B.E は、米国およびその他の国における Sony Computer Entertainment, Inc. の商標であり、同社の許諾を受けて使用しています。

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。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

C

D

W

X

Z

Printed in Japan

SA88-5103-01

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