



システム管理

ここでは、システムデータベースの更新やシステムのバックアップおよび復元などの、システム管理タスクの実行方法について説明します。

- [ソフトウェアアップデートのインストール \(1 ページ\)](#)
- [システムのバックアップと復元 \(8 ページ\)](#)
- [監査と変更管理 \(14 ページ\)](#)
- [デバイス設定のエクスポート \(21 ページ\)](#)
- [FDM および FTD ユーザ アクセスの管理 \(22 ページ\)](#)
- [システムの再起動またはシャットダウン \(29 ページ\)](#)
- [システムのトラブルシューティング \(30 ページ\)](#)
- [一般的でない管理タスク \(43 ページ\)](#)

ソフトウェアアップデートのインストール

システム データベースとシステム ソフトウェアの更新プログラムをインストールできます。ここでは、これらの更新プログラムのインストール方法について説明します。

システム データベースおよびフィードの更新

システムは、複数のデータベースおよびセキュリティ インテリジェンス フィードを使用して高度なサービスを提供します。シスコでは、セキュリティ ポリシーで最新の情報が使用されるよう、これらのデータベースおよびフィードに対する更新を提供しています。

システム データベースおよびフィードの更新の概要

Firepower Threat Defense は次のデータベースおよびフィードを使用して高度なサービスを提供します。

侵入ルール

新たな脆弱性が発見されると、Cisco Talos Intelligence Group (Talos) から侵入ルールのアップデートがリリースされ、インポートできます。それらの更新は、侵入ルール、プリプロセッサ ルール、およびルールを使用するポリシーに影響を及ぼします。

侵入ルールの更新には、新規および更新された侵入ルールとプリプロセッサルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が含まれています。ルールの更新では、ルールが削除されたり、新しいルールカテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。

侵入ルールの更新によって行われた変更を有効にするには、設定を再展開する必要があります。

侵入ルールの更新は量が多くなることがあるため、ルールのインポートはネットワークの使用量が少ないときに実行してください。低速ネットワークでは更新試行が失敗する可能性があります。再試行する必要があります。

位置情報データベース (GeoDB)

シスコの地理位置情報データベース (GeoDB) は、ルート可能な IP アドレスに関連する位置情報データ (国、都市、緯度と経度の座標など)、および接続関係のデータ (インターネットサービスプロバイダー、ドメイン名、接続タイプなど) のデータベースです。

GeoDB の更新には、物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスにシステムが関連付けることができるものに関する更新情報が含まれています。位置情報データは、アクセス コントロール ルールとして使用できます。

GeoDB の更新にかかる時間はアプライアンスによって異なります。インストールには通常、30～40 分かかります。GeoDB の更新は他のシステムの機能 (実行中の地理情報の収集など) を中断することはありませんが、更新が完了するまでシステムのリソースを消費します。更新を計画する場合には、この点について考慮してください。

脆弱性データベース (VDB)

シスコの脆弱性データベース (VDB) は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。Firepower システムはフィンガープリントと脆弱性を関連付けて、特定のホストがネットワークの侵害のリスクを増大させているかどうかを判断するのをサポートします。Cisco Talos Intelligence Group (Talos) では、VDB の定期的な更新を配布しています。

脆弱性のマッピングを更新するのにかかる時間は、ネットワーク マップ内のホストの数によって異なります。システムのダウンタイムの影響を最小にするために、システムの使用率が低い時間帯に更新をスケジュールすることをお勧めします。一般的に、更新の実行にかかるおおよその時間 (分) を判断するには、ネットワーク上のホストの数を 1000 で割ります。

VDB を更新した後、更新されたアプリケーションディテクタとオペレーティング システム フィンガープリントを有効にするために、設定を再展開する必要があります。

Cisco Talos Intelligence Group (Talos) セキュリティ インテリジェンスのフィード

Talos は、セキュリティ インテリジェンス ポリシーで使用するため定期的に更新されるインテリジェンス フィードへのアクセスを提供します。マルウェア、スパム、ボット ネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。これらのフィードには、既知の脅威のアドレスや URL が含まれています。システムによって

フィードが更新される場合、再展開する必要はありません。後続の接続の評価には新しい一覧が使用されます。

URL カテゴリ/レピュテーション データベース

システムは、Cisco Collective Security Intelligence (CSI) から URL カテゴリとレピュテーションデータベースを取得します。カテゴリとレピュテーションに関してフィルタリングする URL フィルタリング アクセス制御ルールを設定すると、要求された URL がデータベースと照合されます。[システム設定 (System Settings)] > [URL フィルタリングの設定 (URL Filtering Preferences)] でデータベースの更新といくつかのその他の URL フィルタリング設定を設定できます。URL カテゴリ/レピュテーション データベースの更新は、他のシステム データベースの更新を管理する方法では管理できません。

システム データベースの更新

必要に応じて、手動でシステムデータベースの更新を取得して適用できます。更新はシスコサポートサイトから取得されます。したがって、システムの管理アドレスからインターネットへのパスが存在する必要があります。

またデータベースの更新を取得して適用するよう、定期的なスケジュールを設定することもできます。これらの更新はサイズが大きい場合があるため、ネットワークアクティビティが少ない時間帯にスケジュールしてください。



(注) データベース更新が進行中の場合、ユーザインターフェイスのアクションへの応答が遅くなる場合があります。

始める前に

保留中の変更に対して潜在的な影響を与えることを避けるため、これらのデータベースを手動で更新する前に、デバイスに設定を展開します。

VDB と URL カテゴリの更新によって、アプリケーションまたはカテゴリが削除される可能性があることに注意してください。変更を展開する前に、これらの廃止された項目を使用しているアクセス制御ルールまたは SSL 復号ルールを更新する必要があります。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[更新 (Updates)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

これによって、[更新 (Updates)] ページが開きます。このページの情報には、各データベースの現在のバージョン、および各データベースの最終更新日時が表示されます。

ステップ 2 手動でデータベースを更新するには、そのデータベースのセクションで [今すぐ更新 (Update Now)] をクリックします。

ルールおよび VDB の更新では、アクティブにするための設定の展開が必要です。今すぐ展開するかどうかを尋ねられます。[はい (Yes)] をクリックします。[いいえ (No)] をクリックする場合は、都合の良いときにできるだけ早く展開ジョブを開始してください。

ステップ 3 (オプション) 定期的なデータベース更新スケジュールを設定するには、次の手順に従います。

- a) 目的のデータベースのセクションで [設定 (Configure)] リンクをクリックします。すでにスケジュールが設定されている場合、[編集 (Edit)] をクリックします。

データベースの更新スケジュールは独立しています。スケジュールは別途定義する必要があります。

- b) 更新開始時刻を設定します。

- 更新の頻度 (日次、週次、または月次) 。
- 週次または月次の場合、更新が必要な曜日または日付。
- 更新を開始する時刻。指定された時刻はサマータイムのため調整され、当該地域で時刻が調整されるたびに 1 時間、前または後に移動します。年間を通して正確な時刻を保持するには、時刻の変更の際にスケジュールを編集する必要があります。

- c) ルールまたは VDB の更新では、データベースが更新されるたびにシステムが設定を展開するようにする場合は、[更新の自動展開 (Automatically Deploy the Update)] チェックボックスをオンにします。

更新は、展開されるまでは有効になりません。自動展開では、まだ展開されていないその他の設定変更も展開されます。

- d) [保存 (Save)] をクリックします。

(注) 定期的なスケジュールを削除する場合、[編集 (Edit)] リンクをクリックしてスケジュールリング ダイアログボックスを開き、[削除 (Remove)] ボタンをクリックします。

Cisco Security Intelligence フィードの更新

Cisco Talos Intelligence Group (Talos) は、定期的に更新されるセキュリティインテリジェンスフィードへのアクセスを提供します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。システムによってフィードが更新される場合、再展開する必要はありません。後続の接続の評価には新しい一覧が使用されます。

システムがフィードをインターネットから更新するタイミングを厳密に制御したい場合は、そのフィードの自動更新を無効にできます。ただし、自動更新を行えば、最新の関連するデータであることが確実にあります。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[更新 (Updates)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

これによって、[更新 (Updates)] ページが開きます。ページには、[セキュリティインテリジェンスフィード (Security Intelligence Feeds)] の現在のバージョン、およびフィードの最終更新日時が表示されます。

ステップ 2 フィードを手動で更新するには、[セキュリティインテリジェンスフィード (Security Intelligence Feeds)] グループで [今すぐ更新 (Update Now)] をクリックします。

ハイ アベイラビリティ グループ内の 1 台の装置のフィードを手動で更新する場合は、その他の装置のフィードも手動で更新して一貫性を確保する必要があります。

ステップ 3 (オプション) 定期的な更新の頻度を設定するには：

- a) [シスコのフィード (Cisco Feeds)] セクションにある [設定 (Configure)] リンクをクリックします。すでにスケジュールが設定されている場合、[編集 (Edit)] をクリックします。
- b) 希望する頻度を選択します。

デフォルトは [毎時 (Hourly)] です。[毎日 (Daily)] 更新 (時刻を指定) または [毎週 (Weekly)] 更新 (曜日と時刻を指定) を設定することもできます。指定された時刻はサマータイムのため調整され、当該地域で時刻が調整されるたびに 1 時間、前または後に移動します。年間を通して正確な時刻を保持するには、時刻の変更の際にスケジュールを編集する必要があります。

[削除 (Delete)] をクリックして、自動更新されないようにします。

- c) [OK] をクリックします。

Firepower Threat Defense ソフトウェアのアップグレード

Firepower Threat Defense ソフトウェアアップグレードが使用可能になると、インストールできます。次の手順は、システム上ですでに Firepower Threat Defense バージョン 6.2.0 以降が稼働していて、正常に動作していることを前提としています。

アップグレードには、ホットフィックス、マイナーアップグレード、メジャーアップグレードの 3 種類があります。ホットフィックスアップグレードは再起動を必要としない場合がありますが、マイナーバージョンおよびメジャーバージョンのアップグレードには再起動が必要です。再起動が必要な場合、インストール後に自動的に再起動します。更新のインストールによりトラフィックが中断される可能性があるため、インストールは時間外に行ってください。

高可用性グループ内の装置をアップグレードする場合は、スタンバイデバイスをアップグレードし、モードを切り替えてアクティブ/スタンバイ装置を交換して、新しいスタンバイデバイスにアップグレードをインストールします。詳細については、[HA デバイスでのソフトウェアアップグレードのインストール](#)を参照してください。

この手順では、デバイスのイメージ再作成も、ASA ソフトウェアから Firepower Threat Defense ソフトウェアへの移行もできません。



- (注) 更新をインストールする前に、保留中の変更がすべて展開されていることを確認します。またバックアップを実行し、バックアップ コピーをダウンロードする必要があります。

始める前に

タスクリストを確認し、実行中のタスクがないことを確認します。アップグレードをインストールする前に、データベースの更新などのすべてのタスクが完了するまでお待ちください。また、スケジュールされたタスクがないかどうかを確認します。アップグレードタスクにスケジュールタスクが重複しないようにしてください。

更新を実行する前に、アプリケーションフィルタ、アクセスルール、またはSSL復号ルールに非推奨のアプリケーションが存在しないことを確認してください。これらのアプリケーションには、アプリケーション名の後に「(廃止) (Deprecated)」が付加されています。これらのオブジェクトに廃止されたアプリケーションを追加することはできませんが、後続の VDB 更新により、以前に有効になっていたアプリケーションが廃止される可能性があります。この場合、アップグレードは失敗し、デバイスは使用不能状態のままになります。

Cisco.com にログインし、アップグレードイメージをダウンロードします。

- 適切なアップグレードファイル（ファイルタイプが REL.tar）を入手していることを確認します。システム ソフトウェア パッケージまたはブートイメージをダウンロードしないでください。
- アップグレードファイルの名前を変更しないでください。名前が変更されたファイルは無効だと見なされます。
- パッチをダウングレードまたはアンインストールすることはできません。
- アップグレードに必要なベースラインイメージを実行していることを確認します。互換性の情報については、『Cisco Firepower Compatibility Guide』 (<http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html>) を参照してください。
- 新しいバージョンの場合は、リリース ノートをお読みください。リリース ノートは <http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html> をご覧ください。

手順

- ステップ 1** [デバイス (Device)] をクリックし、[更新サマリー (Updates summary)] の [設定の表示 (View Configuration)] をクリックします。

[システムアップグレード (System Upgrade)] セクションには、現在実行中のソフトウェアバージョン、およびすでにアップロードされた更新が表示されます。

ステップ2 アップグレードファイルをアップロードします。

- アップグレードファイルをまだアップロードしていない場合、[検索 (Browse)] をクリックしてファイルを選択します。
- すでにアップロードされたファイルがあるか、別のファイルをアップロードする場合、[別のファイルをアップロード (Upload Another File)] をクリックします。1つのファイルのみアップロードできます。新規ファイルをアップロードすると、古いファイルが置き換えられます。
- ファイルを削除するには、[削除 (Delete)] アイコン () をクリックします。

ステップ3 [インストール (Install)] をクリックして、インストールプロセスを開始します。

アイコンの隣の情報は、インストール中にデバイスが再起動するかどうかを示します。システムから自動的にログアウトされます。インストールには30分以上かかることがあります。

待機してからシステムに再度ログインしてください。[デバイスサマリー (Device Summary)] または[システム監視ダッシュボード (System monitoring dashboard)] には、新しいバージョンが表示されます。

(注) 単にブラウザ ウィンドウを更新するだけではありません。代わりに、URL からパスを削除してホームページに再接続します。これにより、最新のコードではキャッシュされている情報が更新されます。

ステップ4 (オプション) システム データベースを更新します。

地理位置情報、ルール、脆弱性 (VDB) データベースに設定された自動更新ジョブがない場合、この機会に更新してください。

デバイスの再イメージ化

デバイスを再イメージ化すると、デバイス設定が消去され、新しいソフトウェアイメージがインストールされます。再イメージ化の目的は、工場出荷時のデフォルト設定でクリーンインストールすることです。

次の場合に、デバイスを再イメージ化します。

- ASA ソフトウェアから Firepower Threat Defense ソフトウェアにシステムを変換する場合。ASA イメージを実行しているデバイスを Firepower Threat Defense イメージを実行しているデバイスにアップグレードすることはできません。
- デバイスが 6.1.0 以前のイメージを実行していて、6.1 以降のイメージにアップグレードし、Firepower Device Manager を使用してデバイスを設定したい場合。Firepower Management

Center を使用して、6.1 以前のデバイスをアップグレードしてからローカル管理を切り替えることはできません。

- デバイスが正しく機能せず、設定の修正ですべての試行が失敗した場合。

デバイスの再イメージ化の詳細については、ご使用のデバイス モデルの『*Reimage the Cisco ASA or Firepower Threat Defense Device*』または *Firepower Threat Defense* のクイック スタート ガイドを参照してください。これらのガイドは、<http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html> で入手できます。

システムのバックアップと復元

後の設定ミスまたは物理的な事故が原因で設定が損なわれた場合にデバイスを復元できるように、システム設定をバックアップできます。

代替のデバイスにバックアップを復元できるのは、どちらのデバイスも同じモデルで、（同時リリースだけでなく、ビルド番号を含む）同じバージョンのソフトウェアを実行している場合のみです。アプライアンス間で設定をコピーするためにバックアップおよび復元プロセスを使用しないでください。バックアップファイルには、この方法で共有することができないようにアプライアンスを一意に特定する情報が含まれます。



- (注) バックアップには管理 IP アドレス設定は含まれません。したがって、バックアップ ファイルを復元しても、管理アドレスがバックアップコピーにより置き換えられることはありません。これにより、アドレスに行きたいかなる変更も保持され、別のネットワークセグメント上のさまざまなデバイスの設定を復元することも可能になります。

バックアップには設定だけが含まれ、システムソフトウェアは含まれません。デバイスを完全に再イメージ化する必要がある場合、ソフトウェアを再インストールしてからバックアップをアップロードして、設定を回復する必要があります。

バックアップ中は設定データベースがロックされます。バックアップの間はポリシー、ダッシュボードなどを表示できますが、設定を変更することはできません。復元を行っている間、システムは完全に使用できません。

「バックアップと復元」ページの表は、バックアップのファイル名、作成日時、ファイルサイズを含む、システムで使用できる既存のすべてのバックアップコピーを示します。バックアップのタイプ（手動、スケジュール、繰り返し）は、システムに指示したバックアップコピーの作成方法に基づいています。



- ヒント バックアップコピーはシステム自体に作成されます。ディザスタリカバリのために必要なバックアップコピーを確保するため、バックアップコピーは手動でダウンロードし、安全なサーバに保存する必要があります。

次に、バックアップの管理と復元操作について説明します。

システムの即時バックアップ

希望する場合はいつでもバックアップを開始できます。

手順

-
- ステップ 1** [デバイス (Device)] をクリックしてから、[バックアップと復元 (Backup and Restore)] のサマリーで [設定の表示 (View Configuration)] をクリックします。
- これにより、[バックアップおよび復元 (Backup and Restore)] ページが開きます。使用可能なすべての既存のバックアップ コピーが表にリストされています。
- ステップ 2** [手動バックアップ (Manual Backup)] > [今すぐバックアップ (Back Up Now)] をクリックします。
- ステップ 3** バックアップの名前を入力し、任意で説明を入力します。
- 今すぐではなく、将来のある時刻にバックアップする場合は、代わりに [スケジュール (Schedule)] をクリックできます。
- ステップ 4** (ISA 3000 のみ) [バックアップファイルの場所 (Location of Backup Files)] を選択します。
- [ローカルハードディスク (Local Hard Disk)] または [SDカード (SD Card)] にバックアップを作成できます。SD カードを使用する利点は、カードを使用して設定を交換デバイスに回復できることです。
- ステップ 5** [今すぐバックアップ (Back Up Now)] をクリックします。
- システムがバックアップ プロセスを開始します。バックアップが完了すると、バックアップ ファイルが表に表示されます。必要に応じて、バックアップ コピーをシステムにダウンロードして、他の場所に保存できます。
- バックアップが開始されたら、[バックアップと復元 (Backup and Restore)] ページを閉じててもかまいません。ただし、システムの動作が遅くなる可能性があるため、バックアップが完了するまで作業を一時停止することを検討する必要があります。
- また、一部または全部のバックアップ中に、システムによってコンフィギュレーションデータベースのロックが取得され、それが原因でバックアッププロセス中に変更を加えることができなくなる場合があります。

スケジュールされた時間でのシステムのバックアップ

システムを将来の特定の日にバックアップするために、スケジュールバックアップを設定できます。スケジュールバックアップは、1回だけ実行されます。定期的にバックアップを作成

するようにバックアップスケジュールを作成するには、スケジュールバックアップではなく、繰り返しバックアップを設定します。



- (注) 将来のバックアップのスケジュールを削除するには、スケジュールを編集して、[削除 (Remove)] をクリックします。

手順

- ステップ 1** [デバイス (Device)] をクリックしてから、[バックアップと復元 (Backup and Restore)] のサマリーで [設定の表示 (View Configuration)] をクリックします。
- ステップ 2** [スケジュールバックアップ (Scheduled Backup)] > [バックアップをスケジュール (Schedule a Backup)] をクリックします。
- すでにスケジュールバックアップがある場合は、[スケジュールバックアップ (Scheduled Backup)] > [編集 (Edit)] をクリックします。
- ステップ 3** バックアップの名前を入力し、任意で説明を入力します。
- ステップ 4** バックアップの日時を入力します。
- ステップ 5** (ISA 3000 のみ) [バックアップファイルの場所 (Location of Backup Files)] を選択します。
- [ローカルハードディスク (Local Hard Disk)] または [SDカード (SD Card)] にバックアップを作成できます。SD カードを使用する利点は、カードを使用して設定を交換デバイスに回復できることです。
- ステップ 6** [スケジュール (Schedule)] をクリックします。
- 選択した日時に達すると、システムがバックアップされます。完了すると、バックアップコピーがバックアップの表に一覧されます。

定期的なバックアップスケジュールの設定

定期的なバックアップを設定し、システムを定期的にバックアップできます。たとえば、毎週金曜日の真夜中にバックアップをとることもできます。定期的なバックアップスケジュールにより、常に最新のバックアップセットを保持できます。



- (注) 定期的なスケジュールを削除する場合、スケジュールを編集し、[削除 (Delete)] をクリックします。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[バックアップと復元 (Backup and Restore)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

ステップ 2 [定期バックアップ (Recurring Backup)] > [設定 (Configure)] をクリックします。

すでに定期バックアップを設定している場合は、[定期バックアップ (Recurring Backup)] > [編集 (Edit)] をクリックします。

ステップ 3 バックアップの名前を入力し、任意で説明を入力します。

ステップ 4 [頻度 (Frequency)] と関連スケジュールを選択します。

- [日次 (Daily)] : 時刻を選択します。バックアップは毎日、スケジュールされた時刻に取得されます。
- [週次 (Weekly)] : 曜日と時刻を選択します。バックアップは選択した日付のスケジュールされた時刻に取得されます。たとえば、毎週月曜日、水曜日、金曜日の 23 時 (午後 11 時) にバックアップをスケジュールすることもできます。
- [月次 (Monthly)] : 日付と時刻を選択します。バックアップは選択した日付のスケジュールされた時刻に取得されます。たとえば、1 日、15 日、28 日の 23 時 (午後 11 時) にバックアップをスケジュールすることもできます。

指定された時刻はサマータイムのため調整され、当該地域で時刻が調整されるたびに 1 時間、前または後に移動します。年間を通して正確な時刻を保持するには、時刻の変更の際にスケジュールを編集する必要があります。

ステップ 5 (ISA 3000 のみ) [バックアップファイルの場所 (Location of Backup Files)] を選択します。

[ローカルハードディスク (Local Hard Disk)] または [SD カード (SD Card)] にバックアップを作成できます。SD カードを使用する利点は、カードを使用して設定を交換デバイスに回復できることです。

ステップ 6 [保存 (Save)] をクリックします。

選択した日付と時刻になると、バックアップが取得されます。完了すると、バックアップ コピーがバックアップテーブルにリストされます。

定期的なスケジュールを変更または削除するまで、バックアップを取得し続けます。

バックアップの復元

デバイスでバックアップを取得したときに実行されていたものと同じソフトウェアバージョン (ビルド番号を含む) が実行されている限り、バックアップを復元できます。代替のデバイスにバックアップを復元できるのは、どちらのデバイスも同じモデルで、同じバージョンのソフトウェア (ビルド番号を含む) を実行している場合のみです。

ただし、このデバイスがハイアベイラビリティペアの一部である場合、バックアップは復元できません。まず、[デバイス (Device)] > [ハイアベイラビリティ (High Availability)] ページから HA を無効化することで、バックアップを復元できます。バックアップに HA の設定が含まれている場合、デバイスは HA グループに再度参加します。両方のユニットで同じバックアップを復元しないでください (両方のユニットがアクティブになってしまうため)。代わりに、まず、アクティブにする装置でバックアップを復元し、その後、別のユニットで同等のバックアップを復元してください。

復元するバックアップコピーがまだデバイスに存在しない場合、復元する前にまずバックアップをアップロードする必要があります。

復元している間、システムはまったく使用できません。



- (注) バックアップには管理 IP アドレスの設定は含まれません。したがって、バックアップ ファイルを復元しても、管理アドレスがバックアップ コピーにより置き換えられることはありません。これにより、アドレスに対する変更はすべて保持され、また異なるネットワークセグメント上の別のデバイスに設定を復元することもできます。

手順

- ステップ 1** [デバイス (Device)] をクリックしてから、[バックアップと復元 (Backup and Restore)] のサマリーで [設定の表示 (View Configuration)] をクリックします。

これにより、[バックアップおよび復元 (Backup and Restore)] ページが開きます。使用可能なすべての既存のバックアップ コピーが表にリストされています。

- ステップ 2** 復元しようとするバックアップコピーが、使用可能なバックアップのリストにない場合、[アップロード (Upload)] > [検索 (Browse)] をクリックし、バックアップ コピーをアップロードします。

- ステップ 3** ファイルの [復元 (restore)] アイコン (🔄) をクリックします。

復元するかどうかの確認が求められます。デフォルトでは、復元後にバックアップコピーは削除されますが、これを保持するには、復元を続行する前に、[復元後にバックアップを削除しない (Do not remove the backup after restoring)] を選択します。

復元が完了すると、システムは再起動します。

- (注) システムが再起動後、脆弱性データベース (VDB)、地理位置情報、およびルールデータベースの更新が自動的にチェックされ、必要に応じてダウンロードされます。これらの更新は大規模な場合があるため、初回の試行が失敗する可能性があります。タスクリストを確認し、ダウンロードが失敗した場合は [システムデータベースの更新 \(3 ページ\)](#) の説明に従って手動で更新をダウンロードしてください。またポリシーも再展開されます。更新が成功しないと、それ以降の展開はすべて失敗します。

ステップ 4 必要に応じて、[デバイス (Device)] > [スマートライセンス (Smart License)] > [設定の表示 (View Configuration)] をクリックし、デバイスを再登録し、必要なオプションライセンスを再度有効にします。

元のデバイスと同じデバイスにバックアップを復元する場合、ライセンスの状態はバックアップ時に存在していたものに戻ります。ライセンスの有効化または無効化など、その後に変更を加えた場合は、これらの変更をやり直す必要があります。

デバイスを交換するなどの理由で別のデバイスでバックアップを復元する場合、新しいデバイスは未登録です。デバイスを再登録し、必要なオプションライセンスを有効にする必要があります。復元に HA の設定が含まれている場合、デバイスは HA グループへの参加を試みません。最初にデバイスを登録し、設定を手動で展開する必要があります。

ISA 3000 デバイスの交換

ISA 3000 の SD カードは、別の ISA 3000 デバイスとの間でやり取りできます。SD カード上にシステムバックアップを作成すれば、この機能を使用してデバイスを簡単に交換できます。その方法は、障害が発生したデバイスから SD カードを取り出して新しいデバイスに挿入するだけです。その後、バックアップを使用して復元できます。

必要なバックアップを確実に用意するには、SD カードにバックアップを作成するバックアップジョブを設定します。

バックアップ ファイルの管理

新しいバックアップを作成すると、バックアップファイルがバックアップと復元ページに表示されます。バックアップコピーは無期限に保たれません。デバイスのディスク領域の利用量が最大しきい値に達すると、新しいバックアップ コピー用の場所を空けるために、古いバックアップ コピーが削除されます。したがって、定期的にバックアップ ファイルを管理し、最も保持したい特定のバックアップ コピーが削除されていないことを確認してください。

バックアップ コピーを管理するには、次の操作を行うことができます。

- ファイルを安全なストレージにダウンロード：バックアップファイルをワークステーションにダウンロードするには、ファイルの[ダウンロード (download)] アイコン (📄) をクリックします。その後、安全なファイル ストレージにファイルを移動できます。
- システムにバックアップ ファイルをアップロードする：デバイスで使用できなくなったバックアップ コピーを復元する場合は、[アップロード (Upload)] > [ファイルの参照 (Browse File)] をクリックして、バックアップ コピーをワークステーションからアップロードします。その後、復元できます。



(注) アップロードされたファイルは、元のファイル名と一致するように名前が変更される場合があります。また、システムに 10 以上のバックアップコピーがすでに存在する場合、アップロードされたファイル用の場所を空けるために最も古いものは削除されます。古いソフトウェアバージョンによって作成されたファイルをアップロードすることはできません。

- バックアップを復元する：バックアップ コピーを復元するには、ファイルの [復元 (restore)] アイコン (🔄) をクリックします。復元の間システムは使用できなくなり、復元が完了するとリブートします。システムが稼働していて、動作中になってから設定を展開してください。
- バックアップファイルを削除する：特定のバックアップが必要でなくなったら、ファイルの削除アイコン (🗑️) をクリックします。削除の確認が求められます。削除すると、バックアップ ファイルを回復することはできません。

監査と変更管理

システムイベントやユーザが実行したアクションに関するステータス情報を表示できます。この情報は、システムを監査し、システムが適切に管理されていることを確認するために役立ちます。

監査ログを表示するには、[デバイス (Device)] > [デバイス管理 (Device Administration)] > [監査ログ (Audit Log)] をクリックします。さらに、右上隅にある [タスクリスト (Task List)] アイコン ボタンまたは [展開 (Deployment)] アイコン ボタンをクリックすると、システム管理情報を確認できます。

ここでは、システム監査および変更管理のいくつかの主要な概念とタスクについて説明します。

監査イベント

監査ログには、次のタイプのイベントを含めることができます。

[カスタムフィードの更新イベント (Custom Feed Update Event)]、[カスタムフィードの更新に失敗 (Custom Feed Update Failed)]

これらのイベントは、カスタムのセキュリティ インテリジェンス フィードの更新が正常に完了したか失敗したことを示します。詳細には、更新を開始したユーザと、更新されたフィードに関する情報が含まれます。

Deployment Completed (展開完了)、Deployment Failed (展開失敗) : ジョブ名またはエンティティ名

これらのイベントは、正常に完了した展開ジョブまたは失敗した展開ジョブを示します。詳細には、ジョブを開始したユーザと、そのジョブエンティティに関する情報が含まれます。失敗したジョブには、その失敗に関連するエラーメッセージが含まれます。

詳細には[差異ビュー (Differences View)]タブもあります。このタブには、ジョブでデバイスに展開された変更が表示されます。これは、展開されたエンティティのすべてのエンティティ変更イベントの組み合わせです。

これらのイベントをフィルタリングするには、事前定義フィルタの[展開履歴 (Deployment History)]をクリックします。これらのイベントのイベントタイプは Deployment Event (展開イベント) であり、完了したイベントまたは失敗したイベントのみをフィルタリングすることはできないことに注意してください。

イベント名には、ユーザ定義のジョブ名 (定義している場合) または「User (*username*) Triggered Deployment (ユーザ (ユーザ名) トリガー イベント) 」が含まれます。また、デバイスセットアップウィザードの実行時に発生する「Device Setup Automatic Deployment (デバイスセットアップ自動展開) 」ジョブと「Device Setup Automatic Deployment (Final Step) (デバイスセットアップ自動展開 (最終手順)) 」ジョブもあります。

Entity Created (エンティティ作成)、Entity Updated (エンティティ更新)、Entity Deleted (エンティティ削除) : エンティティ名 (エンティティ型)

これらのイベントは、識別されたエンティティまたはオブジェクトに変更が加えられたことを示します。エンティティの詳細には、エンティティ名、タイプ、およびIDに加えて、変更を加えたユーザが含まれます。これらの項目に関してフィルタリングできます。詳細には[差異ビュー (Differences View)]タブもあります。このタブには、オブジェクトに加えられた変更が表示されます。

HA Action Event (HA アクション イベント)

これらのイベントは、高可用性設定でのアクション (ユーザが開始したアクションまたはシステムが開始したアクション) に関連したものです。HA Action Event はイベントタイプですが、イベント名は次のいずれかです。

- **HA Suspended** (HA 一時停止) : ユーザがシステムで HA を意図的に一時停止しました。
- **HA Resumed** (HA 再開) : ユーザがシステムで HA を意図的に再開しました。
- **HA Reset** (HA リセット) : ユーザがシステムで HA を意図的にリセットしました。
- **HA Failover: Unit Switched Modes** (HA フェールオーバー: ユニットモード切り替え) : ユーザがモードを意図的に切り替えたか、ヘルスメトリック違反のためにシステムがフェールオーバーしました。このメッセージは、アクティブピアがスタンバイになったか、スタンバイピアがアクティブになったことを示します。

Interface List Scanned (スキャンされたインターフェイス リスト)

このイベントは、インターフェイスインベントリの変更をスキャンしたことを示します。

Pending Changes Discarded（保留中の変更の破棄）

このイベントは、保留中のすべての変更をユーザが削除したことを示します。このイベントと以前の Deployment Completed イベントの間の Entity Created、Entity Updated、および Entity Deleted イベントで示されたすべての変更が削除され、影響を受けたオブジェクトの状態が、最後に展開されたバージョンに戻されています。

Task Started（タスク開始）、Task Completed（タスク完了）、Task Failed（タスク失敗）

タスクイベントは、システムまたはユーザによって開始されたジョブの開始および終了を示します。これらの2つのイベントは、タスクリストで1つのタスクに統合されます。このタスクリストは、右上隅にある [タスクリスト (Task List)] ボタンをクリックすると表示されます。



タスクには、展開ジョブや手動（またはスケジュールされた）データベース更新などのアクションが含まれます。タスクリスト内の任意の項目は、監査ログの2つのタスクイベント、タスクの開始の表示、正常な完了または失敗のいずれかに対応します。

User Logged In（ユーザ ログイン）、User Logged Out（ユーザ ログアウト）：ユーザ名

これらのイベントは、Firepower Device Manager のユーザ ログインおよびユーザ ログアウトの時間と送信元 IP アドレスを示します。User Logged Out イベントは、アクティブ ログアウトと、アイドル時間を超過したための自動ログアウトの両方で発生します。

これらのイベントは、デバイスとの接続を確立している RA VPN ユーザに関するものではありません。また、デバイス CLI のログイン/ログアウトも含まれません。

監査ログの表示および分析

監査ログには、展開ジョブ、データベースの更新、Firepower Device Manager のログインとログアウトなど、システムが開始したイベントやユーザが開始したイベントに関する情報が含まれています。

ログで確認できるイベントの種類の説明については、[監査イベント（14 ページ）](#) を参照してください。

手順

ステップ 1 [デバイス (Device)] をクリックし、[デバイス管理 (Device Administration)] > [設定の表示 (View Configuration)] リンクをクリックします。

ステップ 2 目次の [監査ログ (Audit Log)] をクリックします (未選択の場合)。

イベントは日付別にグループ分けされ、1日の中では時間別にグループ分けされます。最新の日時がリストの一番上に表示されます。初めは、各イベントは折りたたまれているため、時間、イベント名、そのイベントを開始したユーザ、ユーザの送信元 IP アドレスのみ確認できます。ユーザと IP アドレスの「システム」は、デバイス自体がイベントを開始したことを意味しています。

次を実行できます。

- イベント名の横にある[>]をクリックしてイベントを開き、イベントの詳細を確認します。もう一度アイコンをクリックするとイベントが閉じます。多くのイベントには、イベント属性（イベントタイプ、ユーザ名、送信元IPアドレスなど）の簡単なリストがあります。ただし、エンティティイベントと展開イベントには次の2つのタブがあります。
 - [概要 (Summary)] : 基本的なイベント属性が示されます。
 - [差異ビュー (Differences View)] : 既存の「展開済み」設定とイベントの一部として行われた変更との比較が示されます。展開ジョブの場合、このビューは長く、スクロールする必要がある場合があります。このタブには、展開ジョブの一部だったエンティティイベントの変更のすべての差異が要約されます。
- [フィルタ (Filter)] フィールドの右にあるドロップダウンリストから別の時間範囲を選択します。デフォルトでは、過去2週間のイベントが表示されますが、過去24時間、7日間、月、または6ヵ月に変更できます。[カスタム (Custom)]をクリックし、開始および終了日時を入力して、正確な範囲を指定します。
- ログ内で任意のリンクをクリックして、該当項目の検索フィルタを追加します。リストが更新されて、該当項目を含むイベントだけが表示されます。単純に[フィルタ (Filter)] ボックスをクリックして、フィルタを直接作成することもできます。フィルタボックスの下には事前定義済みのフィルタがいくつかあり、クリックして関連するフィルタ条件をロードできます。イベントのフィルタリングの詳細については、[監査ログのフィルタリング \(17 ページ\)](#) を参照してください。
- ブラウザ ページをリロードして、ログを最新のイベントで更新します。

監査ログのフィルタリング

監査ログにフィルタを適用して、特定のタイプのメッセージだけが表示されるように絞り込むことができます。フィルタの各要素は、正確な完全一致です。たとえば、「User = admin」では **admin** という名前のユーザが開始したイベントだけが表示されます。

次の手法を単独または組み合わせて使用して、フィルタを作成できます。このリストは、フィルタ要素を追加するたびに自動的に更新されます。

事前定義のフィルタをクリック

[フィルタ (Filter)] フィールドの下には事前定義のフィルタがあります。リンクをクリックするだけでフィルタがロードされます。確認を求められます。すでにフィルタが適用されている場合は、追加されず、置き換えられます。

強調表示された項目をクリック

フィルタを作成する最も簡単な方法は、フィルタリングの基準となる値を含むログテーブルまたはイベント詳細情報内の項目をクリックすることです。項目をクリックすると、その値と要素の組み合わせに正しく定式化されている要素を使用して、[フィルタ (Filter)]

フィールドが更新されます。ただし、この手法を使用するには、イベントの既存のリストに目的の値が含まれている必要があります。

項目に関するフィルタ要素を追加できる場合は、その項目にマウスカーソルを合わせると下線が引かれ、[クリックしてフィルタに追加 (Click to Add to Filter)] コマンドが表示されます。

アトミック要素を選択

[フィルタ (Filter)] フィールドをクリックして、ドロップダウンリストから必要なアトミック要素を選択し、等号の後に照合値を入力してから Enter キーを押すことでフィルタを作成することもできます。次の要素に関するフィルタリングを実行できます。すべての要素がすべてのイベントタイプに関連するわけではないことに注意してください。

- [イベントタイプ (Event Type)] : これは、通常、イベント名と同じですが、異なる場合もあります (エンティティ名やユーザのような可変修飾子はありません)。展開イベントの場合、イベントタイプは **Deployment Event** (展開イベント) です。イベントタイプの説明については、[監査イベント \(14 ページ\)](#) を参照してください。
- [ユーザ (User)] : イベントを開始したユーザの名前。システムユーザは **SYSTEM** (すべて大文字) です。
- [送信元IP (Source IP)] : ユーザがイベントを開始した IP アドレス。システムが開始したイベントの送信元 IP アドレスは **SYSTEM** です。
- [エンティティID (Entity ID)] : エンティティまたはオブジェクトの UUID。これは、理解できない長い文字列 (8e7021b4-2e1e-11e8-9e5d-0fc002c5f931 など) です。通常、このフィルタを使用するには、イベント詳細情報内のエンティティ ID をクリックするか、REST API を使用し、関連する GET コールによって必要な ID を取得する必要があります。
- [エンティティ名 (Entity Name)] : エンティティまたはオブジェクトの名前。ユーザが作成したエンティティの場合は、通常、ユーザがオブジェクトに付けた名前 (ネットワークオブジェクトの **InsideNetwork** など) です。システムが生成したエンティティの場合は (一部のユーザ定義のエンティティについても)、事前定義されていて理解できる名前です。たとえば、明示的に名前を付けない展開ジョブの場合は「**User(admin) Triggered Deployment**」です。
- [エンティティタイプ (Entity Type)] : エンティティまたはオブジェクトの種類。これらは、事前定義されていて理解できる名前 (**Network Object** など) です。API エクスプローラで「**type**」値の関連オブジェクトモデルを調べることによってエンティティタイプを確認できます。通常、API タイプはすべて小文字であり、スペースは含まれません。それらをモデルに表示されているとおりに正確に入力し、Enter キーを押すと、文字列が理解しやすい形式に変更されます。どちらの形式で入力しても機能します。API エクスプローラを開くには、[詳細オプション (More options)] ボタン (☰) をクリックし、[API エクスプローラ (API Explorer)] を選択します。

複雑な監査ログフィルタのルール

複数のアトミック要素を含む複雑なフィルタを作成する場合、次のルールに注意してください。

- 同じタイプの要素には、そのタイプのすべての値の間に OR 関係があります。たとえば、「User = admin」と「User = SYSTEM」が含まれている場合、いずれかのユーザによって開始されたイベントと一致します。
- 異なるタイプの要素には、AND 関係があります。たとえば、「Event Type = Entity Updated」と「User = SYSTEM」が含まれている場合、アクティブ ユーザではなくシステムがエンティティを更新したイベントだけが表示されます。
- ワイルドカード、正規表現、部分一致、または単純なテキスト文字列の一致は使用できません。

展開およびエンティティ変更履歴の確認

展開およびエンティティイベントの詳細には、[差異ビュー (Differences View)] タブが含まれています。このタブには、古い設定と変更の色分けされた比較が表示されます。

- 展開ジョブの場合は、展開前にデバイスで実行されていた設定と、実際に展開された変更との比較です。
- エンティティイベントの場合は、オブジェクトの以前のバージョンに行われた設定の変更です。エンティティイベントの場合は、オブジェクトの以前のバージョンに行われた設定の変更です。

手順

ステップ 1 [デバイス (Device)] をクリックし、[デバイス管理 (Device Administration)] > [設定の表示 (View Configuration)] リンクをクリックします。

ステップ 2 目次の [監査ログ (Audit Log)] をクリックします (未選択の場合)。

ステップ 3 (オプション) メッセージのフィルタ処理：

- 展開イベント：フィルタ ボックスの下にある [展開履歴 (Deployment History)] 事前定義フィルタをクリックします。
- エンティティ変更イベント：関心のある変更の種類に対して、[イベントの種類 (Event Type)] 要素を使用してフィルタを手動で作成します。すべてのエンティティの変更を確認するには、[作成済みエンティティ (Entity Created)]、[更新済みエンティティ (Entity Updated)]、および [削除済みエンティティ (Entity Deleted)] の 3 つの仕様を含めます。フィルタは次のようになります。



ステップ4 イベントを開き、[差異ビュー (Differences View)] タブをクリックします。

Deployment Completed: User (admin) Triggered Deployment

Summary Differences View

DEPLOYED VERSION

PENDING VERSION

Legend: Removed Added Edited

Syslog Server Removed

Entity ID: 4a1605df-311d-11e8-893d-c15d8f450fd9

syslogServerIpAddress: 192.168.1.25

portNumber: 514

deviceInterface:

inside

-

-

-

Network Object Added

Entity ID: b64f4101-311d-11e8-893d-a302db0bc31e

-

-

-

-

subType: Network

value: 10.1.10.0/24

isSystemDefined: false

name: RemoteNetwork

Network Object Edited

Entity ID: ddb608e9-311c-11e8-893d-5588b92854ca

value: 192.168.2.0/24

192.168.1.0/24

変更は色分けされていて、見出しにはオブジェクトの種類と、Added（作成）、Removed（削除）、または Edited（更新）が表示されます。Edited オブジェクトには、変更された属性またはオブジェクトから削除された属性のみ表示されます。展開ジョブの場合、変更されたエンティティごとに個別の見出しがあります。見出しには、オブジェクトのエンティティタイプが表示されます。

保留中の全変更の廃棄

まだ展開されていない一連の設定の変更に納得していない場合は、すべての保留中の変更を破棄できます。破棄すると、すべての機能がデバイスに存在する状態に戻ります。その後、設定の変更をもう一度を開始できます。

手順

ステップ1 Web ページの右上にある [変更の展開 (Deploy Changes)] アイコンをクリックします。

保留中の変更がある場合、アイコンがドット付きで強調表示されます。



ステップ2 [詳細オプション (More Options)] > [すべて破棄 (Discard All)] をクリックします。

ステップ3 確認ダイアログで [OK] をクリックします。

変更が破棄され、プロセスが完了すると、保留中の変更がないことを示すメッセージが表示されます。監査ログに [保留中の変更の破棄 (Pending Changes Discarded)] イベントが追加されます。

デバイス設定のエクスポート

現在展開されている設定のコピーを JSON 形式でエクスポートできます。このファイルは、アーカイブまたはレコードの保存目的で使用できます。パスワードや秘密キーなどのセンシティブデータはすべてマスク処理されます。

ファイルを当該デバイスや別のデバイスにインポートすることはできません。この機能は、システムバックアップの代替機能ではありません。

設定をダウンロードする前に、少なくとも1つの展開ジョブが正常に完了している必要があります。

手順

ステップ1 [デバイス (Device)] を選択し、[デバイス管理 (Device Administration)] グループで [設定の表示 (View Configuration)] をクリックします。

ステップ2 目次で [設定のダウンロード (Download Configuration)] をクリックします。

ステップ3 [デバイス設定の取得 (Get Device Configuration)] をクリックして、ファイルを作成するジョブを開始します。

ファイルを事前に作成している場合、ファイルの作成日とともに、[ダウンロード (Download)] ボタンと「File is ready to download」メッセージが表示されます。

設定のサイズによっては、ファイルの生成に数分かかることがあります。タスクリストや監査ログを確認したり、定期的にこのページに戻ったりして、Export Config ジョブが完了してファイルが生成されるのを待ちます。

ステップ4 ファイルが生成されたらこのページに戻り、[設定ファイルのダウンロード (Download the Configuration File)] ボタン (📄) をクリックして、ファイルをワークステーションに保存します。

FDM および FTD ユーザ アクセスの管理

ユーザが Firepower Device Manager にログインするための外部認証および認可ソースを設定できます (HTTPS アクセス)。ローカルユーザデータベースとシステム定義の**管理者**ユーザに加えて (またはその代わりに) 外部サーバを使用できます。FDM アクセスでは追加のローカルユーザアカウントは作成できないことに注意してください。

設定を変更できる複数の外部 FDM ユーザアカウントを用意できますが、それらの変更がユーザごとに追跡されることはありません。1 人のユーザが変更を展開すると、すべてのユーザが行った変更が展開されます。ロック機能はありません。つまり、複数のユーザが同じオブジェクトの更新を同時に試みることができます。その結果、1 人のユーザだけが変更を正常に保存できます。また、ユーザに基づいて変更を破棄することもできません。

Firepower Device Manager では、5 つの同時ユーザセッションが可能です。6 人目のユーザがログインすると、最も古いユーザセッションが自動的にログオフされます。また、アイドルタイムアウトがあり、非アクティブユーザは 20 分後にログアウトされます。

FTD CLI への SSH アクセスでは、外部認証および認可を設定することもできます。ローカルデータベースは外部ソースを使用する前に常にチェックされるため、フェールセーフアクセスでは追加のローカルユーザを作成することができます。ローカルソースと外部ソースの両方で重複するユーザを作成しないでください。**管理者**ユーザを除き、CLI ユーザと Firepower Device Manager ユーザが入れ替わることはありません。ユーザアカウントは完全に個別です。



- (注) 外部サーバを使用する場合、別の RADIUS サーバグループをセットアップするか、または特定の FTD デバイスの IP アドレスのみへのユーザアクセスを許可する RADIUS サーバ内で認証/認可ポリシーを作成することにより、デバイスのサブセットへのユーザアクセスを制御することができます。

ここでは、Firepower Device Manager のユーザアクセスの設定および管理方法と CLI ユーザアクセスについて説明します。

FDM (HTTPS) ユーザ用の外部認証 (AAA) 設定

Firepower Device Manager への HTTPS アクセスを外部 RADIUS サーバから提供できます。RADIUS 認証および認可を有効にすることにより、さまざまなレベルのアクセス権を付与でき、すべてのユーザがローカル**管理者**アカウントを使用してログインする必要がなくなります。

これらの外部ユーザは、Firepower Threat Defense API および API エクスプローラについても認証されます。

ロールベース アクセス コントロール (RBAC) を提供するには、RADIUS サーバ上のユーザアカウントを更新して、**cisco-av-pair** 属性を定義します (ISE の場合。ただし、FreeRADIUS での属性の綴りは **Cisco-AVPair** となります。システムで正しいスペルを確認してください)。ユーザアカウントでこの属性を正しく定義する必要があります。そうしなければ、ユーザは

Firepower Device Manager へのアクセスを拒否されます。 **cisco-av-pair** 属性のサポートされる値は、次のとおりです。

- **fdm.userrole.authority.admin** はフル管理者アクセスを提供します。これらのユーザは、ローカル管理者ユーザが実行できるすべてのアクションを実行できます。
- **fdm.userrole.authority.rw** は読み取り/書き込みアクセスを提供します。これらのユーザは、読み取り専用ユーザが実行できるすべてのアクションを実行でき、設定を編集および展開することもできます。アップグレードのインストール、バックアップの作成と復元、監査ログの表示、Firepower Device Manager ユーザのセッションの終了など、システムクリティカルなアクションに対してのみ制限があります。
- **fdm.userrole.authority.ro** は読み取り専用アクセスを提供します。これらのユーザは、ダッシュボードと設定を表示できますが、変更できません。ユーザが変更しようとする、権限が不足していることを示すエラーメッセージが表示されます。

ユーザが Firepower Device Manager にログインすると、ページの右上隅にユーザ名とロール ([管理者 (Administrator)]、[読み取り/書き込みユーザ (Read-Write User)]、または[読み取り専用ユーザ (Read-Only User)]) が表示されます。

RADIUS サーバで正しくアカウントを設定すると、次の手順で管理アクセス用にそのアカウントを有効にできます。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[システム設定 (System Settings)] > [管理アクセス (Management Access)] リンクの順にクリックします。

[システム設定 (System Settings)] ページがすでに表示されている場合は、目次で [管理アクセス (Management Access)] をクリックします。

ステップ 2 まだ選択されていない場合は、[AAA設定 (AAA Configuration)] タブをクリックします。

ステップ 3 [HTTPS接続 (HTTPS Connection)] のオプションを設定します。

- [管理/REST API用のサーバグループ (Server Group for Management/REST API)] : プライマリ認証ソースとして使用する RADIUS サーバグループまたはローカルユーザデータベース (LocalIdentitySource) を選択します。外部認証を使用する RADIUS サーバグループを選択する必要があります。

サーバグループがまだ存在しない場合は、[新しいRADIUSサーバグループの作成 (Create New RADIUS Server Group)] リンクをクリックしてすぐに作成します。サーバごとに RADIUS サーバ オブジェクトを作成してグループに追加する必要がありますが、サーバグループを定義するときにこれを実行できます。RADIUS の詳細については、[RADIUS サーバおよびグループ](#)を参照してください。

- [ローカルによる認証 (Authentication with LOCAL)] : 外部サーバグループを選択する場合、ローカル[管理 (admin)] アカウントを含むローカルアイデンティティソースを使用する方法を指定できます。次のいずれかを選択します。

- [外部サーバの前 (Before External Server)]: システムは、まずローカルソースに対してユーザ名とパスワードを確認します。
- [外部サーバの後 (After External Server)]: 外部ソースが使用できない場合またはユーザアカウントが外部ソースで見つからなかった場合にのみ、ローカルソースが確認されます。
- [使用しない (Never)]: (非推奨) ローカルソースがまったく使用されないため、管理者ユーザとしてログインできません。

注意 [使用しない (Never)]を選択すると、[管理 (admin)]アカウントを使用して Firepower Device Manager にログインできなくなります。RADIUS サーバが使用できなくなった場合または RADIUS サーバのアカウント設定が間違っている場合は、システムがロックされます。

ステップ 4 [保存 (Save)]をクリックします。

FTD CLI (SSH) ユーザ用の外部認証 (AAA) 設定

外部 RADIUS サーバから FTD CLI への SSH アクセスを提供できます。RADIUS 認証および許可を有効にすることで、デバイスごとに個別のローカルユーザアカウントを定義するのではなく、単独の認証ソースからさまざまなレベルのアクセス権を提供することができます。

これらの SSH 外部ユーザは、Firepower Threat Defense API および API エクスプローラには認証されません。SSH の認証を定義するために使用するメカニズムは、HTTPS アクセスに必要なものとは異なります。ただし、SSH と HTTPS の両方の許可条件で同じ RADIUS ユーザを設定し、どちらのプロトコルでも特定のユーザがシステムにアクセスできるようにすることは可能です。

SSH アクセスにロールベースのアクセス制御 (RBAC) を提供するには、RADIUS サーバ上のユーザアカウントを更新して **Service-Type** 属性を定義します。この属性はユーザアカウントで定義されている必要があります。定義されていないと、ユーザの SSH へのアクセスが拒否されます。次に、**Service-Type** 属性でサポートされている値を示します。

- **Administrator (6)**: CLI への **config** アクセス認証を提供します。これらのユーザは、CLI ですべてのコマンドを使用できます。
- **NAS Prompt (7)** または 6 以外のレベル: CLI への **basic** アクセス認証を提供します。これらのユーザは **show** コマンドなど、モニタリングやトラブルシューティングのための読み取り専用コマンドを使用できます。

RADIUS サーバで正しくアカウントを設定すると、次の手順で SSH 管理アクセス用にそのアカウントを有効にすることができます。



- (注) ローカルソースと外部ソースの両方で重複するユーザを作成しないでください。重複するユーザ名を作成した場合は、同じ許可権限があることを確認します。許可権限がローカルユーザアカウントで異なる場合、外部バージョンのユーザアカウントのパスワードを使用してログインすることはできません。ログインできるのはローカルのパスワードを使用した場合のみです。権限が同じ場合、パスワードが異なっていれば、使用するパスワードによって外部ユーザまたはローカルユーザのどちらでログインしているかが判断されます。最初にローカルデータベースが確認されますが、ユーザ名がローカルデータベースに存在するがパスワードが正しくない場合、外部サーバが確認され、外部ソースのパスワードが正しい場合、ログインが成功します。

始める前に

外部定義ユーザに次の動作を通知し、希望通りに設定できるようにしてください。

- 外部ユーザが初めてログインすると、FTD は必要な構造体を作成しますが、ユーザセッションを同時に作成することはできません。ユーザがセッションを開始するには、再度認証する必要があります。ユーザには次のようなメッセージが表示されます。「新しい外部ユーザ名が特定されました。(New external username identified.) セッションを開始するにはもう一度ログインしてください。(Please log in again to start a session.)」
- 同様に、最後のログイン以降に Service-Type で定義したユーザの認証が変更された場合は、ユーザは再認証する必要があります。ユーザには次のようなメッセージが表示されません。「認証権限が変更されています。(Your authorization privilege has changed.) セッションを開始するにはもう一度ログインしてください。(Please log in again to start a session.)」

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[システム設定 (System Settings)] > [管理アクセス (Management Access)] リンクの順にクリックします。

[システム設定 (System Settings)] ページがすでに表示されている場合は、目次で [管理アクセス (Management Access)] をクリックします。

ステップ 2 まだ選択されていない場合は、[AAA設定 (AAA Configuration)] タブをクリックします。

ステップ 3 [SSH接続 (SSH Connection)] のオプションを設定します。

- [サーバグループ (Server Group)]: プライマリ認証ソースとして使用する RADIUS サーバグループまたはローカルユーザデータベース (LocalIdentitySource) を選択します。外部認証を使用する RADIUS サーバグループを選択する必要があります。

サーバグループがまだ存在しない場合は、[新しいRADIUSサーバグループの作成 (Create New RADIUS Server Group)] リンクをクリックしてすぐに作成します。サーバごとに RADIUS サーバ オブジェクトを作成してグループに追加する必要もありますが、サーバグループを定義するときこれを実行できます。RADIUS の詳細については、[RADIUS サーバおよびグループ](#)を参照してください。

SSH 接続はグループ内の最初の 2 つのサーバのみ使用することに注意してください。3 つ以上のサーバがあるグループを使用する場合、追加のサーバが試行されることはありません。さらに、[デッドタイム (Dead Time)] と [最大失敗試行数 (Maximum Failed Attempts)] グループ属性は使用されません。

- [ローカルによる認証 (Authentication with LOCAL)] : 外部サーバグループを選択する場合、ローカルアイデンティティソースを使用する方法を指定できます。SSH アクセスでは、ローカルデータベースが常に外部サーバの前に確認されます。

ステップ 4 [保存 (Save)] をクリックします。

Firepower Device Manager ユーザセッションの管理

[モニタリング (Monitoring)] > [セッション (Sessions)] を選択すると、現在 Firepower Device Manager にログインしているユーザのリストが表示されます。このリストには、各ユーザが現在のセッションにログインしている時間が示されます。

同じユーザ名が複数回表示される場合は、ユーザが異なる送信元アドレスからセッションを開いたことを意味します。セッションは、ユーザ名と送信元アドレスに基づいて個別に追跡され、各セッションは固有のタイムスタンプを持ちます。

このシステムでは、5 つの同時ユーザセッションが可能です。6 人目のユーザがログインすると、最も古い現在のセッションが自動的にログアウトされます。また、アイドル状態のユーザは、アクティビティが 20 分間ないと自動的にログアウトされます。

FDM ユーザが、誤ったパスワードを入力し、3 回連続してログインに失敗した場合、ユーザのアカウントは 5 分間ロックされます。ユーザは再度ログインを試みる前に待つ必要があります。FDM ユーザアカウントをロック解除する方法はありません。また、再試行回数やロックタイムアウトを調整することもできません (SSH ユーザの場合は、これらの設定を調整し、アカウントをロック解除することができます)。

必要に応じて、セッションの [削除 (delete)] アイコン (🗑️) をクリックすることにより、ユーザセッションを終了させることができます。自分自身のセッションを削除すると、自分もログアウトされます。セッションを終了させた場合、ロックアウト期間はなく、ユーザはすぐにログインしなおすことができます。

外部ユーザ用のスタンバイ HA ユニットでの FDM アクセスの有効化

FDM ユーザ用に外部認証を設定すると、これらのユーザはハイアベイラビリティペアのアクティブおよびスタンバイ装置の両方にログインできます。ただし、スタンバイ装置への最初のログインを正常に行うには、アクティブな装置にログインする場合と比較して、いくつかの追加手順が必要です。

外部ユーザがアクティブな装置に最初にログインした後、システムはユーザおよびユーザのアクセス権を定義するオブジェクトを作成します。管理者または読み取り/書き込みユーザはそ

の後、アクティブな装置からユーザオブジェクトの設定を展開し、スタンバイ装置で表示されるようにする必要があります。

展開および後続の設定同期が正常に終了した後にのみ、外部ユーザがスタンバイ装置にログインすることができます。

管理者および読み取り/書き込みユーザは、アクティブな装置にログインした後に変更を展開できます。ただし、読み取り専用ユーザは設定を展開できないため、適切な権限を持つユーザに設定を展開を依頼する必要があります。

FTD CLI のローカル ユーザ アカウントの作成

FTD デバイスで CLI にアクセスするユーザを作成できます。これらのアカウントは管理アプリケーションへのアクセスは許可されず、CLI へのアクセスのみが有効になります。CLI はトラブルシューティングやモニタリング用に役立ちます。

複数のデバイス上にローカルユーザアカウントを一度に作成することはできません。デバイスごとに固有のローカルユーザ CLI アカウントのセットがあります。

手順

ステップ 1 config 権限を持つアカウントを使用してデバイスの CLI にログインします。

管理者ユーザアカウントには必要な権限がありますが、config 権限を持っていればどのアカウントでも問題ありません。SSH セッションまたはコンソールポートを使用できます。

特定のデバイスモデルでは、コンソールポートから FXOS CLI に移動します。connect ftd を使用して FTD の CLI にアクセスします。

ステップ 2 ユーザアカウントを作成します。

configure user add username {basic | config}

次の権限レベルを持つユーザを定義できます。

- **config** : ユーザに設定アクセス権を付与します。すべてのコマンドの管理者権限がユーザに与えられます。
- **basic** : ユーザに基本的なアクセス権を付与します。ユーザはコンフィギュレーションコマンドを入力することはできません。

例 :

次の例では、config アクセス権を使用して、joecool という名前のユーザアカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login          UID   Auth Access  Enabled Reset   Exp Warn  Str Lock Max
admin          1000  Local Config Enabled  No   Never  N/A  Dis  No N/A
```

```
joecool          1001 Local Config Enabled No Never N/A Dis No 5
```

(注) 自分のパスワードを **configure password** コマンドを使用して変更できることをユーザに伝えます。

ステップ3 (オプション) セキュリティ要件を満たすようにアカウントの性質を調整します。

アカウントのデフォルト動作を変更するには、次のコマンドを使用できます。

- **configure user aging** *username max_days warn_days*

ユーザパスワードの有効期限を設定します。パスワードの最大有効日数と、有効期限が近づいたことをユーザに通知する警告を期限切れとなる何日前に発行するかを指定します。どちらの値も 1~9999 ですが、警告までの日数は最大日数以内にする必要があります。アカウントを作成した場合、パスワードの有効期限はありません。

- **configure user forcereset** *username*

次回ログイン時にユーザにパスワードを強制的に変更するよう要求します。

- **configure user maxfailedlogins** *username number*

アカウントがロックされる前の連続したログイン失敗の最大回数を 1~9999 までで設定します。**configure user unlock** コマンドを使用してアカウントのロックを解除します。新しいアカウントのデフォルトは、5 回連続でのログインの失敗です。

- **configure user minpasswdlen** *username number*

パスワードの最小長を 1~127 までで設定します。

- **configure user strengthcheck** *username {enable | disable}*

パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

ステップ4 必要に応じてユーザアカウントを管理します。

ユーザをアカウントからロックアウトしたり、アカウントを削除するか、またはその他の問題を修正したりしなければならない可能性があります。システムのユーザアカウントを管理するには、次のコマンドを使用します。

- **configure user access** *username {basic | config}*

ユーザアカウントの権限を変更します。

- **configure user delete** *username*

指定したアカウントを削除します。

- **configure user disable** *username*

指定したアカウントを削除せずに無効にします。ユーザは、アカウントを有効にするまでログインできません。

- **configure user enable** *username*

指定したアカウントを有効にします。

- **configure user password** *username*

指定したユーザのパスワードを変更します。ユーザは通常、**configure password** コマンドを使用して自分のパスワードを変更する必要があります。

- **configure user unlock** *username*

ログイン試行の最大連続失敗回数の超過が原因でロックされたユーザアカウントをロック解除します。

システムの再起動またはシャットダウン

必要に応じて、システムを再起動またはシャットダウンすることができます。

下記の手順以外に、**reboot** または **shutdown** コマンドを使用して、SSH セッションまたは FDM CLI コンソールからこれらのタスクを実行することもできます。

手順

ステップ 1 [デバイス (Device)] をクリックし、[システム設定 (System Settings)] > [再起動/シャットダウン (Reboot/Shutdown)] リンクをクリックします。

すでに [システム設定 (System Settings)] ページを表示している場合は、目次の [再起動/シャットダウン (Reboot/Shutdown)] をクリックします。

ステップ 2 必要な機能を実行するボタンをクリックします。

- [再起動 (Reboot)] : システムが正常に動作しておらず、どうしても問題が解決できないと判断した場合に、デバイスを再起動できます。また、システムソフトウェアをリロードするためにデバイスを再起動するよう求める手順がいくつかあります。
- [シャットダウン (Shut Down)] : システムをシャットダウンし、制御された方法で電源をオフにします。ネットワークからデバイスを削除する場合 (デバイスの交換などの場合) は、シャットダウンを使用します。デバイスをシャットダウンした後は、ハードウェアのオン/オフ スイッチからのみ電源をオンにすることができます。

ステップ 3 操作が完了するまで待ちます。

システムの再起動またはシャットダウン中は、FDM または CLI で他の操作を実行することはできません。

再起動中、FDM のページが更新され、再起動が完了するとログイン ページに移動します。再起動が完了する前に Web ブラウザでページを更新しようとすると、その時点での FDM Web サーバの動作状態に基づいて、503 または 404 エラーを返すことがあります。

シャットダウンの場合、システムは最終的には応答できず、404 エラーが表示されます。システムを完全にオフにしようとしているため、これは想定される結果です。

システムのトラブルシューティング

ここでは、いくつかのシステムレベルのトラブルシューティングのタスクおよび機能について説明します。特定の機能（アクセスコントロールなど）のトラブルシューティングの詳細については、その機能に関する章を参照してください。

接続をテストするための ping アドレス

ping は、特定のアドレスが使用可能で、応答するかどうかを確認するための単純なコマンドです。これは基本接続が機能していることを意味します。ただし、デバイスで実行されている他のポリシーにより、特定のタイプのトラフィックは正常にデバイスを通過できないことがあります。コマンドは、**ping CLI** コンソールを開くかデバイスの CLI にログインすることにより使用できます。



- (注) システムには複数のインターフェイスがあるため、アドレスの ping に使用されるインターフェイスを制御できます。接続をテストすることが重要であるため、確実に正しいコマンドを使用する必要があります。たとえば、システムは仮想管理インターフェイスを介してシスコライセンスサーバに到達できる必要があるため、**ping system** コマンドを使用して接続をテストする必要があります。**ping** を使用すると、複数のデータ インターフェイスを通じて到達できるかをテストするため、同じ結果が得られない可能性があります。

通常の ping は、ICMP パケットを使用して接続をテストします。ネットワークで ICMP が禁止されている場合は、代わりに TCP ping を使用できます（データ インターフェイスの ping のみ）。

次に、ネットワーク アドレスを ping するための主なオプションを示します。

仮想管理インターフェイスを介したアドレスの ping

ping system コマンドを使用します。

ping system ホスト

ホストは IP アドレスまたは完全修飾ドメイン名 (FQDN) (www.example.com など) にできます。データ インターフェイスを介した ping とは違い、システム ping のデフォルト数はありません。ping は Ctrl+c を使用して停止するまで続けられます。次に例を示します。

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

ルーティングテーブルを使用するデータ インターフェイスを介したアドレスの ping

ping コマンドを使用します。インターフェイスを指定せずに、システムが一般的にホストへのルートを検索できるかどうかをテストします。システムは通常このようにしてトラフィックをルーティングするため、一般的に実行する必要があるのはこのテストです。

ping ホスト

ホストの IP アドレスを指定します。FQDN のみ判明している場合は、**nslookup fqdn-name** コマンドを使用して、IP アドレスを判別します。次に例を示します。

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```



- (注) タイムアウト、繰り返し回数、パケットサイズ、さらには送信するデータパターンを指定できます。使用可能なオプションを表示するには、CLI でヘルプインジケータの「?」を使用します。

特定のデータ インターフェイスを介したアドレスの ping

特定のデータインターフェイスを経由した接続をテストする場合、**ping interface if_name** コマンドを使用します。このコマンドを使用して診断インターフェイスを指定することもできますが、仮想管理インターフェイスは指定できません。

ping interface if_name host

ホストの IP アドレスを指定します。FQDN のみ判明している場合は、**nslookup fqdn-name** コマンドを使用して、IP アドレスを判別します。次に例を示します。

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

TCP ping を使用するデータ インターフェイスを介したアドレスの ping

ping tcp コマンドを使用します。TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。

ping tcp [interface *if_name*] *host port*

ホストと TCP ポートを指定する必要があります。FQDN のみ判明している場合は、**nslookup fqdn-name** コマンドを使用して、IP アドレスを判別します。

オプションで、ping を送信するインターフェイスではなく、ping の送信元インターフェイスであるインターフェイスを指定できます。このタイプの ping では、必ずルーティングテーブルを使用します。

TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。次に例を示します。

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```



(注) タイムアウト、繰り返し回数、および TCP ping の送信元アドレスも指定できます。使用可能なオプションを表示するには、CLI でヘルプインジケータの「?」を使用します。

ホストまでのルートの追跡

IP アドレスへのトラフィックの送信で問題が発生している場合は、ホストまでのルートを追跡することによってネットワークパスに問題がないかどうかを確認できます。トレースルートでは、宛先に対して、無効なポートで UDP パケットを送信したり、ICMPv6 エコーを送信したりします。宛先までの途中にあるルータから ICMP Time Exceeded メッセージが返され、トレースルートにそのエラーが報告されます。各ノードは 3 つのパケットを受信するため、有益な結果を得る機会が 1 台のノードにつき 3 回あります。**traceroute** CLI コンソールを開く、またはデバイス CLI へのログインによって、を使用することができます。



(注) データインターフェイス (**traceroute**) または仮想管理インターフェイス (**traceroute system**) を経由するルートをトレースするための個別のコマンドがあります。適切なコマンドを使用するようにしてください。

次の表に、パケットによって出力に表示される可能性のある結果を示します。

| 出力記号 | 説明 |
|----------------|---------------------------------------|
| * | タイムアウトの期間内にプローブへの応答を受信しませんでした。 |
| <i>nn msec</i> | 各ノードに対する、指定した数のプローブのラウンドトリップ時間 (ミリ秒)。 |
| !N. | ICMP ネットワークに到達できません。 |
| !H | ICMP ホストに到達できません。 |
| !P | ICMP プロトコルに到達できません。 |
| !A | ICMP が管理者によって禁止されています。 |
| ? | 原因不明の ICMP エラーが発生しました。 |

仮想管理インターフェイスを介したルートの追跡

traceroute system コマンドを使用します。

traceroute system [接続先 (*Destination*)]

ホストには、IPv4/IPv6 アドレスまたは完全修飾ドメイン名 (FQDN) (www.example.com など) を使用できます。次に例を示します。

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1 192.168.0.254 (192.168.0.254) 0.213 ms 0.310 ms 0.328 ms
 2 10.88.127.1 (10.88.127.1) 0.677 ms 0.739 ms 0.899 ms
 3 lab-gw1.example.com (10.89.128.25) 0.638 ms 0.856 ms 0.864 ms
 4 04-bb-gw1.example.com (10.152.240.65) 1.169 ms 1.355 ms 1.409 ms
 5 wan-gw1.example.com (10.152.240.33) 0.712 ms 0.722 ms 0.790 ms
 6 wag-gw1.example.com (10.152.240.73) 13.868 ms 10.760 ms 11.187 ms
 7 rbb-gw2.example.com (172.30.4.85) 7.202 ms 7.301 ms 7.101 ms
 8 rbb-gw1.example.com (172.30.4.77) 8.162 ms 8.225 ms 8.373 ms
 9 sbb-gw1.example.com (172.16.16.210) 7.396 ms 7.548 ms 7.653 ms
10 corp-gw2.example.com (172.16.16.58) 7.413 ms 7.310 ms 7.431 ms
11 dmzbb-gw2.example.com (172.16.0.78) 7.835 ms 7.705 ms 7.702 ms
12 dmzdcc-gw2.example.com (172.16.0.190) 8.126 ms 8.193 ms 11.559 ms
13 dcz05n-gw1.example.com (172.16.2.106) 11.729 ms 11.728 ms 11.939 ms
14 ww1.example.com (172.16.4.161) 11.645 ms 7.958 ms 7.936 ms
```

データ インターフェイスを介したルートの追跡

traceroute コマンドを使用します。

traceroute [接続先 (*Destination*)]

ホストの IP アドレスを指定します。FQDN のみ判明している場合は、**nslookup fqdn-name** コマンドを使用して、IP アドレスを判別します。次に例を示します。

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1 10.83.194.1 0 msec 10 msec 0 msec
 2 10.83.193.65 0 msec 0 msec 0 msec
```

```

3 10.88.193.101 0 msec 10 msec 0 msec
4 10.88.193.97 0 msec 0 msec 10 msec
5 10.88.239.9 0 msec 10 msec 0 msec
6 10.88.238.65 10 msec 10 msec 0 msec
7 172.16.7.221 70 msec 70 msec 80 msec
8 209.165.200.225 70 msec 70 msec 70 msec

```



(注) タイムアウト、パケット存続時間、1 ノードあたりのパケット数、およびトレースルートへの送信元として使用する IP アドレスまたはインターフェイスを指定できます。使用可能なオプションを表示するには、CLI でヘルプ インジケータの「?」を使用します。

Firepower Threat Defense デバイスのトレースルートへの表示

デフォルトでは、Firepower Threat Defense デバイスは、トレースルートにホップとして表示されません。表示されるようにするには、デバイスを通過するパケットの存続可能時間を減らし、ICMP 到達不能メッセージのレート制限を増やす必要があります。そのためには、必要なサービス ポリシー ルールとその他のオプションを設定する FlexConfig オブジェクトを作成する必要があります。

サービス ポリシー とトラフィック クラスの詳細については、<https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html> で入手可能な『Cisco ASA Series Firewall Configuration Guide』を参照してください。



(注) パケット存続時間 (TTL) をデクリメントすると、TTL が 1 のパケットはドロップされますが、接続に TTL がより大きいパケットを含むと想定されるセッションでは、接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL = 1 で送信されるため、パケット存続時間 (TTL) をデクリメントすると、予期しない結果が発生する可能性があります。トラフィック クラスを定義する際には、これらの考慮事項に注意してください。

手順

- ステップ 1 [デバイス (Device)] > [詳細設定 (Advanced Configuration)] で [設定の表示 (View Configuration)] をクリックします。
- ステップ 2 詳細設定の目次で [FlexConfig] > [FlexConfig オブジェクト (FlexConfig Objects)] をクリックします。
- ステップ 3 TTL を減らすためのオブジェクトを作成します。
 - a) 新しいオブジェクトを作成するには、[+] ボタンをクリックします。
 - b) オブジェクトの名前を入力します。例、**Decrement_TTL**。
 - c) [テンプレート (Template)] エディタで、インデントを含む次の行を入力します。

```
icmp unreachable rate-limit 50 burst-size 1
```

```
policy-map global_policy
  class class-default
    set connection decrement-ttl
```

- d) [ネゲートテンプレート (Negate Template)]エディタで、この設定を元に戻すために必要な行を入力します。

適切なサブモードでコマンドを有効にするために、ネゲートテンプレートに、親コマンドと同様にこれらのコマンドも含める必要があります。

FlexConfig ポリシーからこのオブジェクトを削除した場合（正常に導入された後）、および導入が失敗した場合でも（設定を前の状態にリセットするため）、ネゲートテンプレートが適用されます。

したがって、この例では、ネゲートテンプレートは次のようになります。

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
  class class-default
    no set connection decrement-ttl
```

- e) [OK] をクリックしてオブジェクトを保存します。

ステップ 4 オブジェクトを FlexConfig ポリシーに追加します。

FlexConfig ポリシー内の選択したオブジェクトのみ展開されます。

- a) 目次で [FlexConfig ポリシー (FlexConfig Policy)] をクリックします。
b) [グループリスト (Group List)] で [+] をクリックします。
c) Decrement_TTL オブジェクトを選択し、[OK] をクリックします。

プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。

- d) [保存 (Save)] をクリックします。

これでポリシーを展開できます。

NTP のトラブルシューティング

システムは、正確で一貫性のある時間に基づいて正しく動作し、イベントやその他のデータポイントを正確に処理します。少なくとも1つ、理想的には3つの Network Time Protocol (NTP) サーバで、システムが常に信頼できる時間情報を取得できるようにする必要があります。

デバイスの接続概要図（メインメニューで [デバイス (Device)] をクリック）に、NTP サーバへの接続ステータスが示されます。ステータスが黄色またはオレンジ色の場合、設定したサーバへの接続に問題があります。接続の問題が解消されない（一時的な問題ではない）場合は、次の操作を試します。

- まず、[デバイス (Device)] > [システム設定 (System Settings)] > [NTP (NTP)] で3つ以上のNTPサーバが設定されていることを確認します。これは要件になっていませんが、NTPサーバが3つ以上あると信頼性が大幅に向上します。
- 管理インターフェイス IP アドレス ([デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] で定義される) と NTPサーバの間にネットワークパスがあることを確認します。
 - 管理インターフェイス ゲートウェイがデータ インターフェイスであり、デフォルトルートが不適切な場合、[デバイス (Device)] > [ルーティング (Routing)] で NTPサーバに対するスタティック ルートを設定できます。
 - 明示的な管理インターフェイス ゲートウェイを設定する場合は、デバイス CLI にログインし、**ping system** コマンドを使用して各 NTPサーバへのネットワークパスがあるかどうかテストします。
- デバイス CLI にログインし、次のコマンドを使用して NTPサーバのステータスを確認します。
 - **show ntp** : このコマンドは、NTPサーバとその可用性に関する基本的な情報を示します。ただし、Firepower Device Manager の接続ステータスではその他の情報を使用してステータスを示すため、このコマンドが示す内容や接続ステータス図が示す内容と一致しないことがあります。このコマンドはCLIコンソールから発行することもできます。
 - **system support ntp** : このコマンドには、**show ntp** の出力と、NTP プロトコルで記載される標準NTPコマンド **ntpq** の出力が含まれています。NTP同期を確認する必要がある場合は、このコマンドを使用します。

「Results of 'ntpq -pn」の部分を探します。たとえば、次のように表示されます。

```
Results of 'ntpq -pn'
remote           : +216.229.0.50
refid            : 129.7.1.66
st              : 2
t               : u
when            : 704
poll            : 1024
reach           : 377
delay           : 90.455
offset          : 2.954
jitter          : 2.473
```

この例では、NTPサーバのアドレスの前の「+」は、潜在的な候補であることを示します。アスタリスク*は、現在の時刻源のピアを示します。

NTPデーモン (NTPD) は、各ピアの8つのスライディングウィンドウサンプルを使用して1つのサンプルを選択します。その後、クロックの選択によって正しいチャイマーと不正なチッカーが特定されます。次に、NTPDがラウンドトリップ距離を特定します (候補のオフセットをラウンドトリップ遅延の半分以上にすることはできません)。接続の遅延、パケットの損失、またはサーバの問題が発生して1つまたはすべての候補が拒否されると、同期中に長い遅延が生じます。また、調整にも非常に長い

時間がかかります。クロック規律アルゴリズムによって、クロックオフセットおよびオシレータエラーを解決する必要がありますが、これには数時間かかる可能性があります。



(注) refid が .LOCL. の場合は、ピアが無規律のローカルクロックであることを示します。つまり、時間設定にそのローカルクロックのみを使用します。選択したピアが .LOCL. の場合、Firepower Device Manager は NTP 接続を常に黄色（非同期）にマークします。通常 NTP は、より適切な候補を利用できる場合、.LOCL. 候補を選択しません。そのため、サーバを 3 つ以上設定する必要があります。

管理インターフェイスの DNS のトラブルシューティング

管理インターフェイスで使用する少なくとも 1 つの DNS サーバを設定する必要があります。DNS サーバは、スマートライセンス、データベースの更新（GeoDB、ルール、VDB など）、およびドメイン名を解決する必要があるその他すべてのアクティビティなどのサービスへのクラウド接続のために必要です。

DNS サーバの設定は簡単な作業です。デバイスの初回設定時に、使用する DNS サーバの IP アドレスを入力するだけです。この設定は、**[デバイス (Device)] > [システム設定 (System Settings)] > [DNSサーバ (DNS Server)]** ページで後で変更できます。

ただし、ネットワークの接続性の問題や DNS サーバ自体の問題のために、システムが完全修飾ドメイン名 (FQDN) を解決できないことがあります。システムが DNS サーバを使用できない場合は、問題を特定して解決するために、以下の操作を検討してください。[DNS の一般的な問題のトラブルシューティング](#)も参照してください。

手順

ステップ 1 問題の有無を確認します。

- a) SSH を使用してデバイスの CLI にログインします。
- b) `ping system www.cisco.com` を入力します。次のような「unknown host」メッセージが表示される場合、システムはドメイン名を解決できていません。ping が成功する場合は、これで終了です。DNS は機能しています (ping を停止するには、Ctrl+C キーを押します)。

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

- (注) **system** キーワードを **ping** コマンドに含めることが重要です。 **system** キーワードを指定すると、管理 IP アドレスから ping が送信されます。これは、管理 DNS サーバを使用する唯一のインターフェイスです。スマートライセンスや更新のためにサーバへのルートが必要なため、 **www.cisco.com** の ping 実行も適切なオプションです。

ステップ2 管理インターフェイスの設定を確認します。

- a) [デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] をクリックして、次の点を確認します。変更を加える場合、それらの変更は [保存 (Save)] をクリックするとすぐに適用されます。管理アドレスを変更する場合は、再度接続してログインし直す必要があります。

- 管理ネットワークのゲートウェイ IP アドレスが正しいこと。データ インターフェイスをゲートウェイとして使用している場合は、後続の手順でその設定を確認します。
- データ インターフェイスをゲートウェイとして使用していない場合は、管理 IP アドレスとサブネットマスク、およびゲートウェイ IP アドレスが同じサブネット上にあることを確認します。

- b) [デバイス (Device)] > [システム設定 (System Settings)] > [DNSサーバ (DNS Server)] をクリックして、正しい DNS サーバが設定されていることを確認します。

ネットワーク エッジにデバイスを展開している場合は、使用できる DNS サーバに関するサービス プロバイダー固有の要件が存在する場合があります。

- c) データ インターフェイスをゲートウェイとして使用している場合は、必要なルートがあることを確認します。

0.0.0.0 のデフォルト ルートが必要です。デフォルト ルートのゲートウェイを介して DNS サーバを使用できない場合は、追加のルートが必要になります。次に、2 つの基本的な状況を示します。

- 外部インターフェイスのアドレスを取得するために DHCP を使用していて、 [DHCP を使用してデフォルトルートを取得 (Obtain Default Route using DHCP)] オプションを選択した場合、デフォルト ルートは Firepower Device Manager には表示されません。SSH から **show route** を入力して、0.0.0.0 のルートがあることを確認します。これは外部インターフェイスのデフォルト設定であるため、発生する可能性が高い状況です。
([デバイス (Device)] > [インターフェイス (Interfaces)] に移動して、外部インターフェイスの設定を確認します) 。
- 外部インターフェイスで静的 IP アドレスを使用している場合、または DHCP からデフォルトルートを取得していない場合は、 [デバイス (Device)] > [ルーティング (Routing)] を開きます。デフォルトルートを正しいゲートウェイが使用されていることを確認します。

デフォルトルートから DNS サーバに到達できない場合は、 [ルーティング (Routing)] ページで DNS サーバへのスタティック ルートを定義する必要があります。直接接続ネットワーク (つまり、システムのいずれかのデータ インターフェイスに直接接続されているネット

ワーク) のルートは追加しないでください。システムは、それらのネットワークに自動的にルーティングできるためです。

また、誤ったインターフェイスからサーバにトラフィックをミス誘導するスタティックルートが存在しないことを確認します。

- d) 展開ボタンに未展開の変更の存在が示されている場合は、ここで展開して、展開が完了するまで待ちます。



- e) `ping system www.cisco.com` を再テストします。問題が解消しない場合は、次の手順に進みます。

ステップ 3 SSH セッションで、`nslookup www.cisco.com` を入力します。

- `nslookup` に、DNS サーバから応答を得たことが示されているのに、サーバが名前を検出できない場合、DNS は正しく設定されているものの、使用している DNS サーバに FQDN のアドレスが設定されていないことを意味しています。応答は次のようになります。

```
> nslookup www.cisco.com
Server:         10.163.47.11
Address:        10.163.47.11#53

** server can't find www.cisco.com: NXDOMAIN
```

解決策：この場合、別の DNS サーバを設定するか、更新した DNS サーバを使用して、解決する必要がある FQDN を解決できるようにします。ネットワーク管理者や ISP と協力して、ネットワークで動作する DNS サーバの IP アドレスを取得します。

- 「connection timed out」メッセージが表示される場合、システムが DNS サーバに到達できないか、または現在すべての DNS サーバがダウンしていて応答していません（この可能性は低いです）。次の手順に進みます。

```
> nslookup www.cisco.com
; ; connection timed out; no servers could be reached
```

ステップ 4 `traceroute system DNS_server_ip_address` コマンドを使用して、DNS サーバへのルートをトレースします。

たとえば、DNS サーバが 10.100.10.1 の場合は、次のように入力します。

```
> traceroute system 10.100.10.1
```

可能性がある結果を以下に示します。

- トレースルートが完了し、DNS サーバに到達している。この場合、DNS サーバへのルートが実際にあり、システムが到達できます。したがって、ルーティングの問題はありません。ただし、何らかの理由でこのサーバに対する DNS 要求の応答を得られていません。

解決策：パス沿いのルータやファイアウォールで、DNSに使用されるポートであるUDP/53のトラフィックがドロップされている可能性があります。異なるネットワークパスに沿ってDNSサーバへのアクセスを試すことができます。これは解決が難しい問題です。トラフィックをブロックしているノードを確認し、システム管理者と協力してアクセスルールを変更する必要があります。

- トレースルートから1つのノードにさえ到達できない。これは、次のように表示されます。

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1 * * *
 2 * * *
 3 * * *
 (and so forth)
```

解決策：この場合、システム内にルーティングの問題があります。ゲートウェイIPアドレスに対して **ping system** を試行します。前述の手順に従い、管理インターフェイスの設定を再度確認し、必要なゲートウェイとルートを設定していることを確認します。

- トレースルートは、ルートを解決できなくなる前にいくつかのノードを通過します。これは、次のように表示されます。

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1 192.168.0.254 (192.168.0.254) 0.475 ms 0.532 ms 0.542 ms
 2 10.88.127.1 (10.88.127.1) 0.803 ms 1.434 ms 1.443 ms
 3 site04-lab-gwl.example.com (10.89.128.25) 1.390 ms 1.399 ms 1.435 ms
 4 * * *
 5 * * *
 6 * * *
```

解決策：この場合、最後のノードでルーティングが中断されています。システム管理者と協力して、そのノードに設定されているルートを修正する必要があります。ただし、意図的にそのノードからDNSサーバへのルートを設定していない場合は、ゲートウェイを変更するか、または独自のスタティックルートを作成して、トラフィックをDNSサーバにルーティングできるルータを指すようにする必要があります。

CPU およびメモリ使用率の分析

CPU とメモリ使用率についてのシステムレベルの情報を表示するには、**[モニタリング (Monitoring)] > [システム (System)]** を選択して、CPU およびメモリ使用率を表す棒グラフを確認します。これらのグラフは **show cpu system** および **show memory system** コマンドを使用して CLI で収集した情報を表示します。

CLI コンソールを開くか CLI にログインして、これらのコマンドの別バージョンを使用すると、他の情報を表示できます。通常、この情報を確認するのは使用状況に関する永続的な問題

がある場合や、Cisco Technical Assistance Center (TAC) の指示があった場合に限られます。詳細情報の多くは複雑で、TAC の解釈が必要です。

以下に、調べることができるいくつかのポイントを示します。これらのコマンドの詳細については、『Cisco Firepower Threat Defense Command Reference』 (http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html) を参照してください。

- **show cpu** は、データプレーンの CPU 使用率を表示します。
- **show cpu core** は、各 CPU コアの使用率を別々に表示します。
- **show cpu detailed** は、追加のコアごと、およびデータプレーン全体の CPU の使用率を表示します。
- **show memory** は、データプレーンのメモリ使用量を表示します。



(注) 一部のキーワード（上記に説明されていない）は、最初に **cpu** または **memory** コマンドを使用して、プロファイリングまたは他の機能を設定する必要があります。これらの機能は、TAC の指示があった場合のみ使用します。

ログの表示

システムはさまざまなアクションに関する情報をログに記録します。システムログを開くには **system support view-files** コマンドを使用します。Cisco Technical Assistance Center (TAC) への問い合わせ時にこのコマンドを使用すると、出力を解釈して、適切なログを表示できるようになります。

コマンドは、ログを選択するためのメニューを表示します。ウィザードに移動するには、次のコマンドを使用します。

- サブディレクトリに変更するには、ディレクトリの名前を入力して、**Enter** を押します。
- 表示するファイルを選択するには、プロンプトで **s** と入力します。その後、ファイル名の入力が求められます。完全な名前を入力する必要があります。大文字と小文字は区別されます。ファイルリストにはログのサイズが示されます。非常に大きいログを開く前には検討が必要な場合があります。
- 「--More--」が表示されたら **Space** キーを押してログエントリの次のページを表示します。次のログエントリのみを表示するには **Enter** を押します。ログの最後に到達すると、メインメニューに戻ります。「--More--」の行には、ログのサイズと表示した量が示されます。ログのすべてのページを表示する必要がなく、ログを閉じて、コマンドを終了するには、**Ctrl+C** を使用します。
- メニュー構造のレベルを 1 つ上がるには、**b** を入力します。

ログを開いたままにして、新しいメッセージが追加されたときにそのメッセージを確認できるようにするには、**system support view-files** コマンドの代わりに **tail-logs** コマンドを使用します。

次の例は、システムへのログイン試行を追跡する **cisco/audit.log** ファイルがどのように表示されるかを示しています。ファイルリストは、最上位のディレクトリで始まり、その後、現在のディレクトリ内のファイル リストが続きます。

```
> system support view-files

===View Logs===

=====
Directory: /ngfw/var/log
-----sub-dirs-----
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----files-----
2016-10-14 18:12:04.514783 | 5371      | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353      | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517   | action_queue.log
2016-10-06 16:00:56.620019 | 1018     | br1.down.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

=====
Directory: /ngfw/var/log/cisco
-----files-----
2017-02-13 22:44:42.394907 | 472      | audit.log
2017-02-13 23:40:30.858198 | 903615   | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0        | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338  | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338  | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218  | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848    | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160  | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login
successful,
2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login
successful,
2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login
```

```
successful,  
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked  
account.,  
  
<remaining log truncated>
```

トラブルシューティング ファイルの作成

問題レポートを提出した際に、Cisco Technical Assistance Center (TAC) の担当者により、システムログ情報の提出を求められることがあります。この情報は、問題の診断に役立ちます。診断ファイルの提出は、求められた場合だけでかまいません。

次の手順では、ログ レベルを設定して診断ファイルを作成する方法について説明します。

手順

ステップ 1 [the name of the device in the menu] をクリックします。[デバイス (Device)]

ステップ 2 [トラブルシューティング (Troubleshooting)] の下で、[ファイルの作成を要求 (Request File to be Created)] または [ファイルの作成を再要求 (Re-Request File to be Created)] (事前に作成していた場合) をクリックします。

システムが診断ファイルの生成を開始します。他のページに移動して、後で戻ってきてステータスを確認できます。ファイルの準備が整うと、ファイル作成日時が [ダウンロード (Download)] ボタンとともに表示されます。

ステップ 3 ファイルの準備が整ったら、[ダウンロード (Download)] ボタンをクリックします。

ファイルは、ブラウザの標準のダウンロード方式を使用してワークステーションにダウンロードされます。

一般的でない管理タスク

次に、ごくまれにしか行われないアクションについて説明します。これらすべてのアクションは、デバイス設定の消去を引き起こします。これらの変更を加える前に、デバイスが現在、実稼働ネットワークに対して重要なサービスを提供していないことを確認します。

ローカル管理とリモート管理の切り替え

デバイスに直接ホストされているローカルの Firepower Device Manager を使用し、またはリモートで Firepower Management Center の複数のデバイス マネージャを使用して、デバイスを設定および管理できます。Firepower Device Manager でサポートされていない機能を設定する場合、または Firepower Management Center で使用可能な電力と分析機能が必要な場合、リモート マネージャを使用できます。

トランスペアレントファイアウォールモードでデバイスを実行する場合、Firepower Management Center も使用する必要があります。

ソフトウェアを再インストールすることなく、ローカル管理とリモートの管理を切り替えることができます。リモート管理からローカル管理に切り替える前に、Firepower Device Manager がすべての設定要件を満たしていることを確認します。



注意 マネージャを切り替えると、デバイス設定は削除され、デフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は保持されます。

始める前に

デバイスを登録した場合、特に機能ライセンスを有効にした場合、リモート管理に切り替える前に、Firepower Device Manager を介してデバイスを登録解除する必要があります。デバイスを登録解除すると、基本ライセンスとすべての機能ライセンスが解放されます。デバイスを登録解除しない場合、これらのライセンスは Cisco Smart Software Manager のデバイスに割り当てられたままになります。[デバイスの登録解除](#)を参照してください。

デバイスがハイアベイラビリティ用に設定されている場合は、まず、デバイスマネージャ（可能な場合）または **configure high-availability disable** コマンドを使用して、ハイアベイラビリティ構成を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします。

手順

ステップ 1 SSH クライアントを使用して [管理IPアドレス (management IP address)] への接続を開き、設定 CLI アクセスを持つユーザ名でデバイス CLI にログインします。たとえば、[管理者 (admin)] ユーザ名など。

管理 IP アドレスに接続している間は、この手順に従うことが重要です。Firepower Device Manager を使用する場合、データインターフェイスの IP アドレスを介してデバイスを管理することもできます。ただしデバイスをリモートで管理するには、管理物理ポートと管理 IP アドレスを使用する必要があります。

管理 IP アドレスに接続できない場合、次のように対処します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理ネットワークに管理 IP アドレスとゲートウェイが設定されていることを確認します。FirePOWER Device Manager から、[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] を選択して、アドレスおよびゲートウェイを設定します (CLI では、**configure network ipv4/ipv6 manual** コマンドを使用します)。

(注) 管理 IP アドレスに外部ゲートウェイを使用していることを確認します。リモート マネージャを使用する場合、データ インターフェイスをゲートウェイとして使用することはできません。

ステップ2 ローカル管理からリモート管理へ切り替えるには、次の手順に従います。

- a) 現在ローカル管理モードになっていることを確認します。

```
> show managers
Managed locally.
```

- b) リモートマネージャを設定します。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey
[nat_id]
```

ここで、

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE} で、このデバイスを管理する Firepower Management Center の DNS ホスト名または IP アドレス (IPv4 あるいは IPv6) を指定します。Firepower Management Center が直接アドレス指定できない場合は、DONTRESOLVE を使用します。DONTRESOLVE を使用する場合は、nat_id が必要です。
- Regkey はデバイスを Firepower Management Center へ登録するのに必要な、英数字の一意の登録キーです。
- nat_id は、Firepower Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。

たとえば、登録キー **secret** で 192.168.0.123 のマネージャを使用するには、以下のコマンドを入力します。

```
> configure manager add 192.168.0.123 secret
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before switching to remote management.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue [yes/no] yes
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status          :
```

(注) 登録が保留中の場合は、**configure manager delete** を使用して登録を取り消してから、**configure manager local** を使用してローカル管理に戻ることができます。

- c) Firepower Management Center にログインし、デバイスを追加します。

詳細については、Firepower Management Center オンラインヘルプを参照してください。

ステップ3 リモート管理からローカル管理へ切り替えるには、次の手順に従います。

- a) 現在リモート管理モードになっていることを確認します。

```
> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status          :
```

- b) リモート マネージャを削除すると、マネージャなしのモードになります。

リモート管理からローカル管理に直接移行することはできません。マネージャを削除するには、**configure manager delete** コマンドを使用します。

```
> configure manager delete
Deleting task list
Manager successfully deleted.
```

```
>
> show managers
No managers configured.
```

- c) ローカル マネージャを設定します。

configure manager local

次に例を示します。

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

これで、Webブラウザで <https://management-IP-address> にアクセスしてローカル マネージャを開くことができるようになりました。

ファイアウォールモードの変更

Firepower Threat Defense ファイアウォールは、ルーテッドモードまたはトランスペアレントモードで実行できます。ルーテッドモードのファイアウォールはルーテッドホップであり、スクリーンサブネットのいずれかに接続するホストのデフォルトゲートウェイとして機能します。一方、トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。

ローカルの Firepower Device Manager はルーテッドモードのみをサポートします。ただし、デバイスをトランスペアレントモードで実行する必要がある場合は、ファイアウォールモードを変更して、Firepower Management Center でデバイスの管理を始めることができます。逆に、トランスペアレントモードのデバイスをルーテッドモードに変換すると、ローカルマネージャ

でそのデバイスを設定することができ、Firepower Management Center を使用してルーテッドモードのデバイスを管理することもできます。

ローカル管理であるか、リモート管理であるかに関係なく、モードを変更するためにはデバイスの CLI を使用する必要があります。

次の手順では、ローカル マネージャを使用している場合、またはローカル マネージャを使用予定の場合のモードの変更方法について説明します。



注意

ファイアウォールモードを変更すると、デバイス設定は削除され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は保持されます。

始める前に

トランスペアレント モードに変換する場合は、ファイアウォール モードを変更する前に Firepower Management Center をインストールします。

いずれかの機能ライセンスを有効にしている場合、ローカルマネージャを削除してリモート管理に切り替える前に、Firepower Device Manager でそれらのライセンスを無効にする必要があります。無効にしないと、それらのライセンスは Cisco Smart Software Manager でデバイスに割り当てられたままになります。 [オプションライセンスの有効化と無効化](#)を参照してください。

デバイスがハイアベイラビリティ用に設定されている場合は、まず、デバイスマネージャ（可能な場合）または **configure high-availability disable** コマンドを使用して、ハイアベイラビリティ構成を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします

手順

ステップ 1 SSH クライアントを使用して [管理IPアドレス (management IP address)] への接続を開き、設定 CLI アクセスを持つユーザ名でデバイス CLI にログインします。たとえば、[管理者 (admin)] ユーザ名など。

管理 IP アドレスに接続している間は、この手順に従うことが重要です。Firepower Device Manager を使用する場合、データインターフェイスの IP アドレスを介してデバイスを管理することもできます。ただしデバイスをリモートで管理するには、管理物理ポートと管理 IP アドレスを使用する必要があります。

管理 IP アドレスに接続できない場合、次のように対処します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理ネットワークに管理 IP アドレスとゲートウェイが設定されていることを確認します。FirePOWER Device Manager から、[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] を選択して、アドレスおよびゲートウェイを設定します (CLI では、**configure network ipv4/ipv6 manual** コマンドを使用します)。

- (注) 管理 IP アドレスに外部ゲートウェイを使用していることを確認します。リモートマネージャを使用している場合、データインターフェイスをゲートウェイとして使用することはできません。

ステップ 2 モードをルーテッドからトランスペアレントに変更して、リモート管理を使用するには、次の手順を実行します。

- a) ローカル管理を無効にし、ノーマネージャモードを開始します。

アクティブなマネージャが存在する間は、ファイアウォールモードを変更できません。マネージャを削除するには、**configure manager delete** コマンドを使用します。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

- b) ファイアウォールモードをトランスペアレントに変更します。

configure firewall transparent

例：

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

- c) リモートマネージャを設定します。

configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]

ここで、

- **{hostname | IPv4_address | IPv6_address | DONTRESOLVE}** で、このデバイスを管理する Firepower Management Center の DNS ホスト名または IP アドレス (IPv4 あるいは IPv6) を指定します。Firepower Management Center が直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。**DONTRESOLVE** を使用する場合は、**nat_id** が必要です。
- **Regkey** はデバイスを Firepower Management Center へ登録するのに必要な、英数字の一意の登録キーです。

- `nat_id` は、Firepower Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。

たとえば、登録キー `secret` で 192.168.0.123 のマネージャを使用するには、以下のコマンドを入力します。

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status         :
```

- d) Firepower Management Center にログインし、デバイスを追加します。

詳細については、Firepower Management Center のオンライン ヘルプを参照してください。

ステップ 3 モードをトランスペアレントからルーテッドに変更して、ローカル管理に変換するには、次の手順を実行します。

- a) FMC からデバイスを登録解除します。
- b) FTD デバイスの CLI にアクセスします。可能ならばコンソールポートからアクセスします。

これは、モードを変更すると設定が削除され、管理 IP アドレスはデフォルトに戻ってしまうため、モード変更後に管理 IP アドレスへの SSH 接続が失われることがあるためです。

- c) ファイアウォール モードをルーテッドに変更します。

configure firewall routed

例 :

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

- d) ローカル マネージャを有効にします。

configure manager local

次に例を示します。

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

これで、Web ブラウザで <https://management-IP-address> にアクセスしてローカル マネージャを開くことができるようになりました。

設定のリセット

最初からやり直す場合は、システム設定を工場出荷時のデフォルトにリセットできます。設定を直接リセットすることはできませんが、マネージャを削除して追加すると設定がクリアされます。

設定を消去してバックアップを復元する場合は、復元するバックアップ コピーを既にダウンロードしていることを確認してください。システムを復元するには、システムのリセット後にバックアップ コピーをアップロードする必要があります。

始める前に

いずれかの機能ライセンスを有効にした場合は、ローカル マネージャを削除する前に Firepower Device Manager でそれらを無効にする必要があります。無効にしないと、それらのライセンスが Cisco Smart Software Manager のデバイスに割り当てられたままになります。[オプション ライセンスの有効化と無効化](#)を参照してください。

デバイスがハイアベイラビリティ用に設定されている場合は、まず、デバイスマネージャ（可能な場合）または **configure high-availability disable** コマンドを使用して、ハイアベイラビリティ構成を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします

手順

ステップ 1 SSH クライアントを使用して、管理 IP アドレスへの接続を開き、設定 CLI アクセス権を持つユーザ名でデバイスの CLI にログインします。たとえば、[管理者 (admin)] ユーザ名を使用します。

ステップ 2 マネージャを削除するには、**configure manager delete** コマンドを使用します。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

ステップ 3 ローカル マネージャを設定します。

configure manager local

次に例を示します。

```
> configure manager local  
Deleting task list  
  
> show managers  
Managed locally.
```

これで、Web ブラウザで <https://management-IP-address> にアクセスしてローカル マネージャを開くことができるようになりました。設定をクリアすると、デバイスセットアップ ウィザードの完了を求めるメッセージが表示されます。
