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と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

システム データベースとシステム ソフトウェアにアップデートをインストールできます。ここでは、このようなアップデートをインストールする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

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

新たな脆弱性が既知になると、Cisco Talos Intelligence Group（Talos） はユーザがインポート可能な侵入ルールの更新をリリースします。こ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します。

侵入ルールを更新すると、更新された新しい侵入ルールおよびプリプロッセサ ルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。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。

侵入ルール更新による変更を有効にするには、設定を再導入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、更新の試行が失敗し、再試行が必要になることがあります。

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、ルーティング可能な IP アドレスに関連する地理情報データ（国、都市、緯度と経度など）のデータベースです。

GeoDB の更新には、検出されたルーティング可能な IP アドレスにシステムが関連付けることが可能な物理的な場所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、これらを考慮してください。

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。ファイアウォール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） は、VDB の定期的な更新を発行します。

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 を更新した後で、更新されたアプリケーション検出器およびオペレーティング システム フィンガープリントを有効にするには、設定を再導入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 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に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。セキュリティに対する脅威（マルウェア、スパム、ボットネット、スパム、フィッシングなど）を表すサイトが現れては消えるペースが早すぎて、カスタム設定を更新して導入するのが間に合わないことがあります。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 カテゴリおよび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

システム データベースのアップデートは、必要に応じて、手動で取得して適用することができます。更新はシスコサポートサイトから取得されます。そのため、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必要です。

または、インターネットから更新パッケージを取得して、ワークステーションからアップロードできます。この方法は、主に、シスコから更新を取得するためのインターネットへのパスがないエアギャップネットワークを対象としています。software.cisco.com のシステム ソフトウェア アップグレードをダウンロードするのと同じフォルダから更新をダウンロードします。

（注） 2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。Device Manager は IP パッケージの情報を使用しません。また、これまでに使用したこともありません。この分割により、ローカルで管理された Threat Defense 展開においてディスク容量が大幅に節約されます。シスコからご自身で GeoDB を入手する場合は、古いオールインワンパッケージと同じファイル名を持つ国コードパッケージ（Cisco_GEODB_Update-*date-build*）を入手してください。

また、データベースアップデートを定期的に取得して適用するようにスケジュールすることもできます。ただし、アップデートは大きくなる可能性があるため、ネットワーク アクティビティが少ない時間にスケジュールしてください。

（注） データベースの更新中、ユーザ インターフェイスの反応が鈍くなることがあります。

始める前に

保留中の変更に影響が及ばないようにするため、データベースを手動で更新する前に、まず設定をデバイスに展開します。

VDBおよびURLカテゴリを更新すると、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]のサマリーで[設定の表示]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。各データベースの現行バージョンと各データベースが最後に更新された日時が表示されます。

ステップ 2 データベースを手動で更新するには、そのデータベースのセクションで次のいずれかのオプションをクリックします。

- [クラウドから更新（Update From Cloud）]：Device Manager が更新パッケージをシスコから取得するようにします。これは最も簡単で信頼性の高い方法ですが、使用するにはインターネットへのパスが必要です。
- **（下矢印）** > ***[オプション（option）]***：ワークステーションまたはワークステーションに接続されているドライブから更新パッケージを選択します。オプションは次のいずれかです。
  - [ファイルの選択（Select File）]：VDB または地理位置情報パッケージを選択します。
  - [新しいバージョンに更新（Update to Newer Version）]：現在インストールされている侵入ルールパッケージよりも新しいパッケージを選択します。
  - [古いバージョンにダウングレード（Downgrade to Older Version）]：現在インストールされている侵入ルールパッケージよりも古いパッケージを選択します。

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。クラウドから更新する場合、今すぐ展開するかどうかを尋ねられるので、[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。

独自のファイルをアップロードする場合は、必ず手動で変更を展開する必要があります。

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存在する場合、[編集（Edit）] をクリックします。

更新スケジュールは、データベースごとに違います。スケジュールはそれぞれに定義する必要があります。

b) 更新の開始時刻を次のように設定します。

- 更新の頻度（毎日、毎週、毎月）。

- 毎週または毎月の場合、更新を実行する曜日または日付。
- 更新を開始する時刻。 指定した時間はサマータイムに合わせて調整されるため、地域で時間が調整されるたびに 1 時間前または後に進みます。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）
定期スケジュールを削除する場合は、[編集（Edit）] リンクをクリックしてスケジュー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） 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。セキュリティに対する脅威（マルウェア、スパム、ボットネット、スパム、フィッシングなど）を表すサイトが現れては消えるペースが早すぎて、カスタム設定を更新して導入するのが間に合わないことがあります。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。

システムがインターネットからフィードを更新するタイミングを厳密に制御する場合は、そのフィードの自動更新を無効にすることができます。ただし、自動更新を使用すると、最新の関連データであることが確認されます。

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。

[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** 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。

高可用性グループ内の 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存在する場合、[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。指定した時間はサマータイムに合わせて調整されるため、地域で時間が調整されるたびに 1 時間前または後に進みます。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。

のアップグレードThreat Defense

この手順を使用して、スタンドアロンの Threat Defense デバイスをアップグレードします。FXOS を更新する必要がある場合は、それを最初に実行します。高可用性脅威防御をアップグレードするには、ハイアベイラビリティ Threat Defense のアップグレードを参照してください。

⚠

注意 アップグレード中にトラフィックがドロップされます。システムが非アクティブまたは無反応に見えても、アップグレード中は手動で再起動またはシャットダウンしないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。失敗した（または進行中）のアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。問題が解消されない場合は、Cisco TAC にお問い合わせください。

アップグレード中に発生する可能性のあるこれらの問題およびその他の問題の詳細については、Threat Defense のアップグレードのトラブルシューティング （11 ページ）を参照してください。

始める前に

アップグレードの計画を完了します。正常に展開され、通信が確立されていることを確認します。

ヒント アップグレードの計画は、『Cisco Secure Firewall Threat Defense リリースノート』を読むことから始まります。次に、バックアップの作成、アップグレードパッケージの取得、および関連するアップグレード（Firepower 4100/9300 の FXOS など）の実行が含まれます。また、必要な構成変更のチェック、準備状況のチェック、ディスク容量のチェック、実行中のタスクとスケジュールされたタスクの両方のチェックも含まれます。詳細については、お使いのバージョンの『Device Manager 用 Cisco Secure Firewall Threat Defense アップグレードガイド』を参照してください。

手順

ステップ 1 [デバイス（Device）] を選択し、[更新（Updates）] パネルの [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）] パネルには、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アップグレードパッケージが表示されます。

ステップ 2 アップグレードパッケージをアップロードします。

アップロードできるパッケージは 1 つだけです。新しいパッケージをアップロードすると、古いパッケージが置き換えられます。ターゲットバージョンとデバイスモデルに適したパッケージがあることを確認してください。[参照（Browse）] または [別のファイルをアップロード（Upload Another File）][ファイルの置き換え（Replace File）] をクリックしてアップロードを開始します。

アップロードが完了すると、確認ダイアログボックスが表示されます。[OK] をクリックする前に、必要に応じて [すぐにアップグレードを実行（Run Upgrade Immediately）] を選択して、ロールバックオプションを選択し、今すぐアップグレードします。今すぐアップグレードする場合は、アップグレード前のチェックリストをできるだけ多く完了することが特に重要です（次のステップを参照）。

ステップ 3 準備状況チェックを含む、アップグレード前の最終チェックを実行します。

アップグレード前のチェックリストを再確認します。関連するすべてのタスク、特に最終チェックを完了していることを確認してください。準備状況チェックを手動で実行しない場合、アップグレードの開始時に実行されます。準備状況チェックに失敗すると、アップグレードはキャンセルされます。詳細については、アップグレード準備状況チェックの実行 （8 ページ）を参照してください。

ステップ 4 [インストール（Install）][今すぐアップグレード（Upgrade Now）] をクリックしてアップグレードを開始します。

a) ロールバックオプションを選択します。

[アップグレードに失敗すると自動的にキャンセルされ、前のバージョンにロールバックする（Automatically cancel on upgrade failure and roll back to the previous version）] を選択できます。オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的に

アップグレード前の状態に戻ります。失敗したアップグレードを手動でキャンセルまたは再試行できるようにする場合は、このオプションを無効にします。

b) [続行（Continue）] をクリックして、アップグレードしてデバイスを再起動します。

自動的にログオフされ、デバイスが再起動するまでアップグレードを監視できるステータスページに移動します。また、このページには、進行中のインストールをキャンセルするオプションが含まれています。自動ロールバックを無効にしてアップグレードが失敗した場合は、アップグレードを手動でキャンセルするか、再試行できます。

アップグレード中にトラフィックがドロップされます。

ステップ 5 可能なときに再度ログインし、アップグレードが成功したことを確認します。

[デバイスの概要（Device Summary）] ページには、現在実行中のソフトウェアのバージョンが表示されます。

ステップ 6 アップグレード後のタスクを完了します。

a) システムデータベースを更新します。侵入ルール、VDB、GeoDBの自動更新が設定されていない場合は、ここで更新します。
b) アップグレード後に必要な構成変更が他にもあれば、実行します。
c) 展開します。

アップグレード準備状況チェックの実行

アップグレードパッケージがインストールされる前に、準備状況チェックが実行されて、システムに有効なアップグレードであるか確認されます。また、他にもアップグレードの成功を妨げる可能性のある項目がないかチェックされます。準備状況チェックに失敗した場合は、インストールを再試行する前に問題を修正する必要があります。チェックに失敗した場合、次回インストールを試みると、チェック失敗についてのプロンプトが表示され、強制的にインストールを実行するオプションが与えられます。

次の手順の説明に従って、アップグレードを開始する前に手動で準備状況チェックを実行することもできます。

始める前に

チェックするアップグレードパッケージをアップロードします。

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 [Readiness Check] セクションを確認します。

- アップグレードチェックがまだ実行されていない場合は、[Run Upgrade Readiness Check] リンクをクリックします。チェックの進行状況がこの領域に表示されます。プロセスの完了には、20 秒程度かかります。
- アップグレードチェックがすでに実行されている場合、このセクションにはチェックが成功か失敗かが示されます。チェックに失敗した場合は、[See Details] をクリックして、準備状況チェックの詳細を表示します。問題を修正した後、チェックを再度実行します。

ステップ 3 準備状況チェックに失敗した場合は、アップグレードパッケージをインストールする前に問題を解決する必要があります。詳細情報には、指摘された問題の修正方法に関するヘルプが含まれています。失敗したスクリプトについては、[Show Recovery Message] リンクをクリックすると情報が表示されます。

一般的な問題のいくつかを以下に示します。

- FXOS バージョンに互換性がない：FXOS アップグレードを個別にインストールする Firepower 4100/9300 などのシステムでは、現行の Threat Defense ソフトウェアバージョンとは異なる FXOS の最小バージョンが必要になる場合があります。この場合、Threat Defense ソフトウェアをアップグレードする前に、まず FXOS をアップグレードする必要があります。
- デバイスモデルがサポートされていない：アップグレードパッケージは、サポートされていないデバイスにはインストールできません。誤ったパッケージをアップロードしたか、デバイスが旧モデルのため、新しい Threat Defense ソフトウェアバージョンではサポートされていない可能性があります。デバイスの互換性を確認し、サポートされているパッケージがあればアップロードしてください。
- ディスク容量が不十分：十分な空き容量がない場合は、システムバックアップなどの不要なファイルを削除してください。作成したファイルのみを削除します。

アップグレードのモニタリング Threat Defense

Threat Defense のアップグレードを開始すると、自動的にログオフされ、アップグレードの進捗を監視できるステータスページに移動します。また、このページには、進行中のインストールをキャンセルするオプションが含まれています。自動ロールバックを無効にしてアップグレードが失敗した場合は、このページから、アップグレードを手動でキャンセルするか、再試行できます。

デバイスに SSH で接続し、CLI（**show upgrade status**）を使用することもできます。ログエントリが生成されたときにそれらを表示するには **continuous** キーワードを追加します。また、詳細情報を表示するには **detail** キーワードを追加します。両方のキーワードを追加して、継続的な詳細情報を取得します

アップグレードが完了した後は、デバイスがリブートすると、ステータスページと CLI にアクセスできなくなります。

Threat Defense のアップグレードのキャンセルまたは再試行

アップグレードステータスのページまたは CLI を使用して、失敗した（または進行中）のメジャーおよびメンテナンスアップグレードを手動でキャンセルし、失敗したアップグレードを再試行することができます。

- アップグレードステータスのページ：進行中のアップグレードをキャンセルするには、[アップグレードのキャンセル（Cancel Upgrade）] をクリックします。アップグレードが失敗した場合は、[アップグレードのキャンセル（Cancel Upgrade）] をクリックしてジョブを停止し、アップグレード前のデバイスの状態に戻すことができます。また、[続行（Continue）] をクリックしてアップグレードを再試行することができます。
- CLI：進行中のアップグレードをキャンセルするには、**upgrade cancel** を使用します。アップグレードが失敗した場合は、**upgrade cancel** を使用してジョブを停止し、アップグレード前のデバイスの状態に戻すことができます。また、**upgrade retry** を使用してアップグレードを再試行することができます。

（注） デフォルトでは、Threat Defense はアップグレードが失敗すると自動的にアップグレード前の状態に復元されます（「自動キャンセル」）。失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、アップグレードを開始するときに自動キャンセルオプションを無効にします。高可用性の展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

パッチでは、キャンセルと再試行はサポートされていません。正常なアップグレードを元に戻す方法については、Threat Defense の復元 （10 ページ）を参照してください。

Threat Defense の復元

メジャーアップグレードまたはメンテナンスアップグレードに成功したにもかかわらず、システムが期待どおりに機能しない場合は、復元が可能です。Threat Defense を復元すると、ソフトウェアは、最後のメジャーアップグレードまたはメンテナンスアップグレードの直前の状態に戻ります。アップグレード後の設定変更は保持されません。パッチ適用後に復元すると、パッチも必然的に削除されます。またはホットフィックスを元に戻すことはできないので注意してください。

次の手順では、Device Manager から復元する方法について説明します。Device Manager にアクセスできない場合は、 **upgrade revert** コマンドを使用して SSH セッションの Threat Defense コマンドラインから復元できます。**show upgrade revert-info** コマンドを使用すると、システムがどのバージョンに戻るのかを確認できます。

始める前に

ユニットがハイアベイラビリティペアの一部である場合は、両方のユニットを元に戻す必要があります。理想的には、フェールオーバーの問題なしに設定を復元できるように、両方のユ

ニットで復元を同時に開始します。両方のユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを開始します。復元時にトラフィックが中断されることに注意してください。そのため、可能であれば、これを業務時間外に実行してください。

Firepower 4100/9300 シャーシの場合、Firepower のメジャーバージョンには特別に認定および推奨されている付随の Threat Defense バージョンがあります。これは、Threat Defense ソフトウェアを復元した後に、推奨されていない（新しすぎる）バージョンの FXOS を実行している可能性があることを意味します。新しいバージョンの FXOS は旧バージョンの Threat Defense と下位互換性がありますが、シスコでは推奨の組み合わせについて拡張テストを実施しています。FXOS をダウングレードすることはできないため、このような状況下で推奨の組み合わせを稼働するには、デバイスの再イメージ化が必要になります。

手順

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

ステップ 2 [システムのアップグレード（System Upgrade）] セクションで、[アップグレードの復元（Revert Upgrade）] リンクをクリックします。

現在のバージョンと復元されるバージョンを示す確認ダイアログボックスが表示されます。復元できるバージョンがない場合、[アップグレードの復元（Revert Upgrade）] リンクは表示されません。

ステップ 3 ターゲットバージョンが許容できるバージョンである場合（かつ使用可能な場合）、[復元（Revert）] をクリックします。

復元後、デバイスを Smart Software Manager に再登録する必要があります。

Threat Defense のアップグレードのトラブルシューティング

以下の問題は、スタンドアロンまたはハイアベイラビリティペアのデバイスをアップグレードするときに発生する可能性があります。ハイアベイラビリティのアップグレードに固有の問題をトラブルシューティングするには、ハイアベイラビリティ Threat Defense のアップグレードのトラブルシューティングを参照してください。

アップグレードパッケージのエラー。

適切なアップグレードパッケージを見つけるには、使用しているモデルを シスコ サポートおよびダウンロード サイト で選択または検索し、適切なバージョンのソフトウェアのダウンロードページを参照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、ソフトウェアバージョン、およびビルドが反映されています。

バージョン 6.2.1 以降のアップグレードパッケージは署名されており、ファイル名の最後は .sh.REL.tar です。署名付きのアップグレードパッケージは解凍しないでください。アップグレードパッケージの名前を変更したり、電子メールで転送したりしないでください。

アップグレード中にデバイスにまったく到達できない。

デバイスは、アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止します。アップグレードする前に、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。

アップグレード中にデバイスが非アクティブまたは無反応に見える。

進行中のメジャーおよびメンテナンスアップグレードは手動でキャンセルできます。Threat Defense のアップグレードのキャンセルまたは再試行 （10 ページ）を参照してください。デバイスが応答しない場合、またはアップグレードをキャンセルできない場合は、Cisco TAC にお問い合わせください。

注意 システムが非アクティブに見えても、アップグレード中は手動で再起動またはシャットダウン「しない」でください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。

アップグレードは成功したが、システムが予期どおりに機能しない。

まず、キャッシュされた情報が更新されていることを確認します。単にブラウザウィンドウを更新して再度ログインするのではなく、URL から「余分な」パスを削除し、ホームページに再接続します（たとえば、http://threat-defense.example.com/）。

引き続き問題が発生し、以前のメジャーリリースまたはメンテナンスリリースに戻す必要がある場合は、復元できる場合があります。Threat Defense の復元 （10 ページ）を参照してください。復元できない場合は、イメージを再作成する必要があります。

アップグレードが失敗する。

メジャーアップグレードまたはメンテナンスアップグレードを開始する場合は、[アップグレードに失敗すると自動的にキャンセルされる...（Automatically cancel on upgrade failure...）]（自動キャンセル）オプションを使用して、次のように、アップグレードが失敗した場合の動作を選択します。

- [自動キャンセルが有効（Auto-cancel enabled）]（デフォルト）：アップグレードが失敗すると、アップグレードがキャンセルされ、デバイスは自動的にアップグレード前の状態に復元されます。問題を修正し、後で再試行してください。
- [自動キャンセルが無効（Auto-cancel disabled）]：アップグレードが失敗した場合、デバイスはそのままになります。問題を修正してすぐに再試行するか、手動でアップグレードをキャンセルして後で再試行してください。

詳細については、Threat Defense のアップグレードのキャンセルまたは再試行 （10 ページ）を参照してください。再試行またはキャンセルできない場合、または問題が解消されない場合は、Cisco TAC にお問い合わせください。

デバイスのイメージ再作成

デバイスのイメージを再作成するには、デバイス設定を除去し、新しいソフトウェアイメージをインストールする必要があります。イメージの再作成の目的は、工場出荷時のデフォルト設定を使用してクリーン インストールを行うことです。

デバイスのイメージの再作成は、次のような状況で行います。

- ASA ソフトウェアから 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 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 Threat Defense Device*』または *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、次の URL から入手可能です。
http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html

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 ファイルにはアプライアンスを一意に識別する情報が含まれているので、この要領で情報を共有することはできません。

（注） バックアップには管理 IP アドレスの設定は含められません。このため、バックアップ ファイルを回復しても、管理アドレスはバックアップ コピーから置換されません。これにより、アドレスに行った変更は維持され、異なるネットワーク セグメントの異なるデバイスの設定を復元することもできるようになります。バックアップにはライセンス情報やクラウド登録情報も含まれていないため、復元時に存在するライセンスやクラウド登録の状態はすべて保持されます。

バックアップには設定のみが含まれ、システム ソフトウェアは含まれません。デバイスのイメージを完全に再作成する必要がある場合は、ソフトウェアを再インストールする必要があり、その後バックアップをアップロードして設定を回復できます。

バックアップ中は設定データベースがロックされます。バックアップ中にポリシーやダッシュボードなどの表示はできますが、設定の変更はできません。復元中は、システムは完全に使用できなくなります。

[バックアップと復元（Backup and Restore）] ページのテーブルには、システムで利用可能な既存のバックアップのコピーが、バックアップのファイル名、作成された日時、ファイルサイズとともにリストされます。バックアップの種類（手動、スケジュール、反復）は、バックアップ コピーを作成する際にシステムで指定します。

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 リカバリ用にバックアップ コピーを確保するため、バックアップ コピーを手動でダウンロードして安全なサーバに保存しておく必要があります。システムは、デバイス上に最大3つのバックアップコピーを保持します。新しいバックアップによって、最も古いバックアップが置き換えられます。

以下のトピックでは、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）]** の順にクリックします。

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　（任意）[Encrypt File] オプションを選択して、バックアップファイルを暗号化します。

このオプションを選択した場合は、バックアップ ファイルの復元に必要な [パスワード（Password）]（および [パスワードの確認（Confirm Password）]）を入力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）] で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、カードを使用して代替デバイスに設定を回復できることです。

ステップ 6 [今すぐバックアップ（Back Up Now）] をクリックします。

システムによってバックアップ プロセスが開始されます。バックアップが完了すると、バックアップ ファイルがテーブルに表示されます。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、別の場所に保存できます。

バックアップを開始した後は、[バックアップと復元（Backup and Restore）] ページから移動しても構いません。ただし、システムの動作が遅くなる可能性があるため、バックアップを完了するために作業を一時停止することを検討してください。

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。

システムのスケジュール バックアップ

スケジュール バックアップを設定して、将来の特定の日時にシステムをバックアップできます。スケジュールバックアップは、一度だけ行われます。定期的にバックアップを作成するようバックアップ スケジュールを作成する必要がある場合は、スケジュール バックアップではなく定期的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 （任意）[Encrypt File] オプションを選択して、バックアップファイルを暗号化します。

このオプションを選択した場合は、バックアップ ファイルの復元に必要な [パスワード（Password）]（および [パスワードの確認（Confirm Password）]）を入力する必要があります。

ステップ 6 （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）] で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、カードを使用して代替デバイスに設定を回復できることです。

ステップ 7 [スケジュール（Schedule）] をクリックします。

選択した日時になると、システムによってバックアップが作成されます。バックアップが完了すると、作成されたバックアップ コピーがバックアップ テーブルに表示されます。

反復バックアップ スケジュールの設定

反復バックアップをセットアップして、定期的なスケジュールでシステムをバックアップすることができます。たとえば、毎週金曜日の午前0時にバックアップを実行するなどです。反復バックアップ スケジュールにより、バックアップ セットを常に最新の状態に保つことができます。

（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）] および関連する項目を選択します。

- [毎日（Daily）]：時刻を選択します。毎日スケジュールした時刻にバックアップが行われます。
- [毎週（Weekly）]：曜日と時刻を選択します。指定した曜日の指定した時刻にバックアップが行われます。たとえば、毎週月曜日/水曜日/金曜日の23:00（午後11時）にバックアップをスケジュールするというぐあいです。
- [毎月（Monthly）]：日付と時刻を選択します。指定した日の指定した時刻にバックアップが行われます。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。

指定した時間はサマータイムに合わせて調整されるため、地域で時間が調整されるたびに1時間前または後に進みます。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 （任意）[Encrypt File] オプションを選択して、バックアップファイルを暗号化します。

このオプションを選択した場合は、バックアップ ファイルの復元に必要な [パスワード（Password）] （および [パスワードの確認（Confirm Password）] ）を入力する必要があります。

ステップ6 （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）] で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、カードを使用して代替デバイスに設定を回復できることです。

ステップ7 [保存（Save）] をクリックします。

指定した日時にシステムはバックアップを行います。バックアップが完了すると、作成されたバックアップ コピーがバックアップ テーブルに表示されます。

バックアップは、反復スケジュールを変更または削除するまで続行されます。

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することができます。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）]** > **[高可用性（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、アクティブする装置でバックアップを復元し、その後に、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。

復元中、システムは完全に使用できなくなります。

（注） バックアップには管理 IP アドレスの設定は含められません。このため、バックアップ ファイルを回復しても、管理アドレスはバックアップ コピーから置換されません。これにより、アドレスに行った変更は維持され、異なるネットワーク セグメントの異なるデバイスの設定を復元することもできるようになります。バックアップにはライセンス情報やクラウド登録情報も含まれていないため、復元時に存在するライセンスやクラウド登録の状態はすべて保持されます。

始める前に

別のシステムでバックアップを復元する場合（デバイスを交換するときなど）、ベストプラクティスは、最初にデバイスを登録し、バックアップファイルで設定された機能に必要なオプションのライセンスを有効にすることです。バックアップファイルにはライセンス情報やクラウドサービス情報が含まれていないため、復元前に行ったライセンスの変更やクラウドの登録は保持されます。

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存在しない場合は、**[アップロード（Upload）]** > **[参照（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。

復元の確認が求められます。デフォルトで、バックアップ コピーは復元後に削除されますが、[復元後にバックアップを削除しない（Do not remove the backup after restoring）] を選択してバックアップを保存することが可能です。

バックアップファイルが暗号化されている場合は、ファイルを開いて復号するために必要な [パスワード（Password）] を入力する必要があります。

復元が完了すると、システムが再起動します。

（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。さらに、システムはポリシーを再展開します。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。

バックアップにはライセンス情報やクラウド登録情報は含まれません。そのため、新しいシステムにバックアップを復元する場合（デバイスを交換するときなど）、システムが評価モードのときは、それを登録し、必要なすべてのライセンスを有効にする必要があります。復元前にデバイスを登録し、ライセンスを有効にした場合、追加の変更は必要ありません。

以前のバックアップを同じシステムに単に復元するだけの場合は、ライセンスやクラウド登録を変更する必要はありません。ただし、バックアップにはバックアップの作成後に無効にしたライセンスを必要とする機能が含まれている可能性があるため、必要なすべてのオプションライセンスが有効になっていることを確認してください。

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（Backup and Restore）] 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持されません。デバイスのディスク容量の使用状況が最大しきい値に達すると、古いバックアップが削除され、新しいバックアップ用に容量が解放されます。さらに、ホットフィックス以外のアップグレードをインストールすると、すべてのバックアップファイルが削除されます。このため、維持が必須である特定のバックアップ コピーを確保するために、定期的にバックアップ ファイルを管理する必要があります。

バックアップ コピーを管理するには、次を実行します。

- 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。
- システムへのバックアップ ファイルのアップロード：デバイスで使用不可能になったバックアップ コピーを復元する場合、**[アップロード（Upload）] > [ファイルの参照（Browse File）]** をクリックし、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の名前を、元のファイル名に一致させるために、変更する必要がある場合があります。また、システムに既存するバックアップコピーの数が 3 を超えると、容量確保のために、最も古いコピーが削除されます。古いソフトウェア バージョンで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。システムは復元中、使用できず、復元が

完了するとリブートされます。システムが動作するようになったら、設定を展開する必要があります。

- 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。一旦削除したバックアップ ファイルは回復できません。

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 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または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。

カスタムルールファイルのインポートの概要イベント

これらのイベントは、1つ以上のカスタム侵入ルールを含むファイルをインポートしたことを示します。イベントには、追加、更新、および削除されたルールの数の概要と、インポートされたルールの詳細を示す差異ビューが含まれます。

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。

High Availability Sync Completed（高可用性同期完了）

アクティブユニットがスタンバイユニットと設定を同期しました。イベントには、同期バージョンと比較した前のバージョンの変更情報が含まれています。

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。

ルール更新イベント

Snort 3 を実行している場合、LSPUpdateServer エンティティからのこのイベントは、新しい侵入ルールパッケージがダウンロードされてインストールされたときに追加、削除、または変更された侵入ルールに関する詳細情報を示します。イベントは100のルールに制限されているため、100 を超えるルールが追加、削除、または変更された場合、イベントには完全な情報が含まれなくなります。

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、Device Manager のユーザーログインおよびユーザー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、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ー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 （20 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]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 ヵ月に変更することができます。[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することができます。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 （23 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 （20 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）、事前定義されているものの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、事前定義されているものの理解できる名前（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 タイプを確認することができます。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

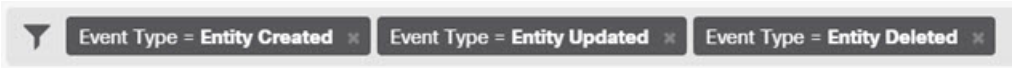
ステップ 1 [デバイス（Device）] をクリックし、**[デバイス管理（Device Administration）]** > **[設定の表示（View Configuration）]** リンクをクリックします。

ステップ 2 目次の[監査]をクリックします(未選択の場合)。

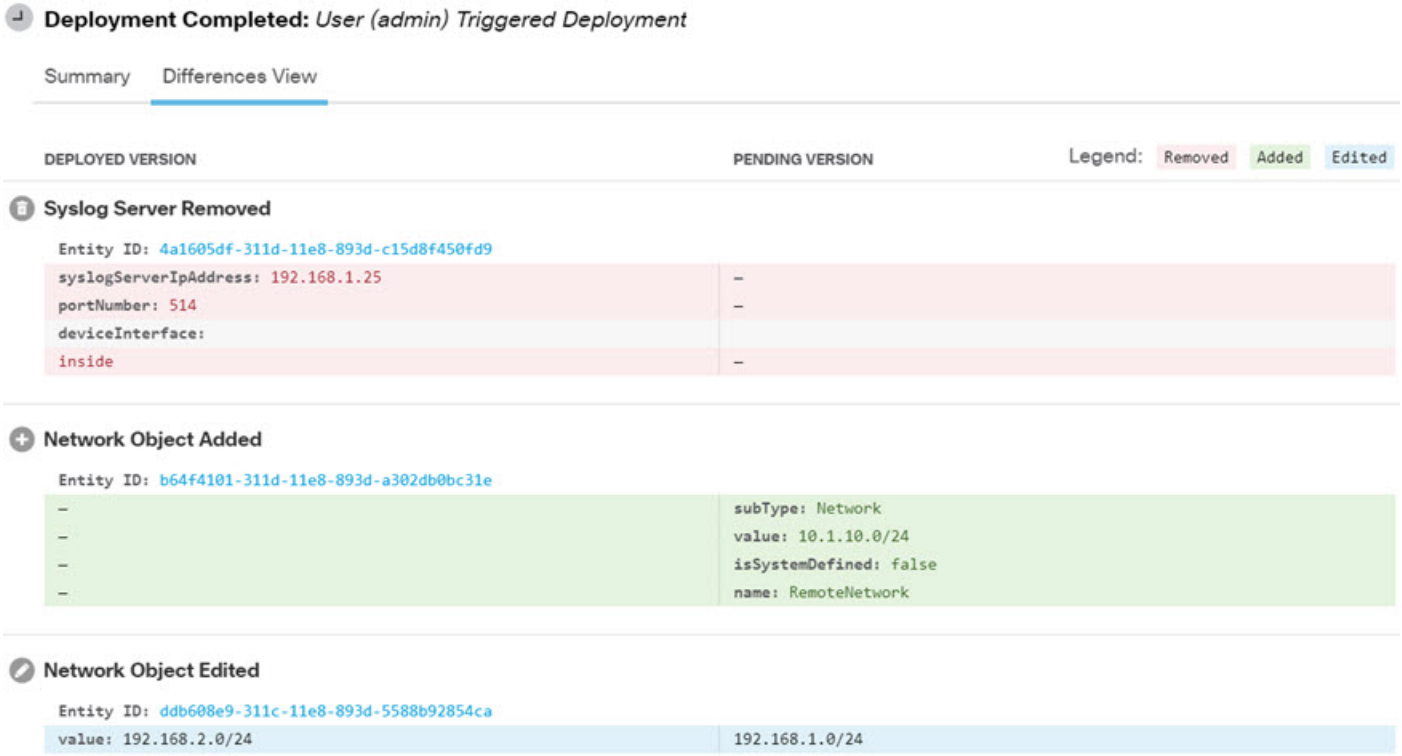
ステップ 3 （オプション）メッセージのフィルタ処理：

- 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。



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示されす。

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。パスワードや秘密鍵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。

Device Manager および Threat Defense ユーザーアクセスの管理

ユーザーが Threat Defense にログイン（HTTPS アクセス）するための外部認証および認可ソースを設定できますローカル 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。Device Manager アクセス用の追加のローカルユーザー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 Device Manager ユーザーアカウントを用意できますが、それらの変更がユーザー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。

5 つのユーザーセッションを同時に処理できます。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。

脅威に対する防御 CLI への SSH アクセスの外部認証および認可も設定できます。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**ユーザーを除き、CLI ユーザーと Device Manager ユーザーが入れ替わることはありません。ユーザーアカウントは完全に個別です。

（注） 外部サーバーを使用する場合、個別の AAA サーバーグループを設定するか、 AAA サーバー内に認証/認可ポリシーを作成して、ユーザーが特定の 脅威に対する防御 デバイスの IP アドレスだけにアクセスできるようにすることで、ユーザーによるデバイスのサブセットへのアクセスを制御できます。

ここでは、Device Manager および CLI ユーザーアクセスの設定方法と管理方法について説明します。

Device Manager （HTTPS）ユーザー用の外部認証（AAA）設定

外部 AAA サーバーからの Device Manager への HTTPS アクセスを提供できます。AAA 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、すべてのユーザー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、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。

AAA サーバーで管理ユーザーの認可を設定することで、ロールベース アクセス コントロール（RBAC）を提供できます。使用できる値はサーバータイプによって異なります。ユーザーが Device Manager にログインすると、ページの右上隅にユーザー名とロールが表示されます。AAA サーバー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。

SAML ユーザー認証

SAML サーバー アイデンティティ ソースを設定するときに、承認レベルを含むフィールドを指定します。外部ユーザーには、管理者、監査管理者、暗号管理者、読み取り/書き込みユーザー、読み取り専用ユーザーの認証アクセスタイプを設定できます。SAML サーバの設定 を参照してください。

RADIUS ユーザー認証

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 サーバー上のユーザーアカウントを更新して、**cisco-av-pair** 属性を定義します（これはISEの場合で、FreeRADIUSではこの属性のスペルはCisco-AVPairです。使用しているシステムで正しいスペルを確認してください）。この属性はユーザーアカウントで正しく定義されている必要があります。正しく定義されていないと、ユーザーの Device Manager へのアクセスが拒否されます。**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、Device Manager ユーザー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と、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。

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。

[System Settings] ページがすでに表示されている場合は、目次で [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）] オプションの設定。

- [管理/REST API用のサーバーグループ（Server Group for Management/REST API）]：プライマリ認証ソースとして使用する RADIUS または SAML サーバーグループ（外部認証/認可用）またはローカル ユーザー データベース（LocalIdentitySource）を選択します。

  サーバーグループがまだ存在しない場合は、リンクをクリックしてすぐに作成します。RADIUS の場合、サーバーごとに RADIUS サーバー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、サーバー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。 SAML の詳細については、SAML サーバの設定を参照してください。

- [ローカルによる認証（Authentication with LOCAL）]（RADIUS のみ）：外部 RADIUS サーバー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 Device Manager にログインできなくなります。AAA サーバーが使用できなくなった場合または AAA サーバー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。

（注）
[ローカルによる認証（Authentication with LOCAL）] は、SAML を使用する場合は適用されません。SAML では、SAML ログイン情報を入力するために [シングルサインオン（SSO）（Single-Sign On (SSO)）] リンクを明示的にクリックする必要があるため、ローカルのユーザー名とパスワードを入力することで、いつでもローカルデータベースを使用してログインできます。

ステップ 4 **[保存（Save）]** をクリックします。

Threat Defense CLI（SSH）ユーザー用の外部認証（AAA）設定

外部 RADIUS サーバーからの Threat Defense 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、Threat Defense API および API エクスプローラについては認証**されません**。SSH の許可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する場合は、同じ認証権限を持ってい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、パスワードが異なると仮定して、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。

- 外部ユーザーが初めてログインすると、Threat Defense は必要な構造を作成しますが、ユーザー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るだけです。ユーザには次のようなメッセージが表示されます。「New external username identified. 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.）」

外部ユーザが GUI に正常にログインできても CLI に正常にログインできない場合は、AAA サーバーの秘密鍵に問題がある可能性があります。キーに & または \ の文字が含まれていないことを確認してください。これらは GUI ログインでは機能する可能性がありますが、SSH ログインでは機能しません。

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。

[System Settings] ページがすでに表示されている場合は、目次で [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。

  SSH 接続では、グループ内の最初の 2 台のサーバのみが使用され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。

Device Manager ユーザーセッションの管理

[モニタリング（Monitoring）] > **[セッション（Sessions）]** を選択すると、現在 Device Manager にログインしているユーザー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。

Device Manager ユーザー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、アカウントは5分間ロックされます。ユーザーが再度ログインを試みるには、待機する必要があります。Device Manager ユーザー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、アカウントのロックを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。

外部ユーザー用のスタンバイ HA ユニットでの Device Manager アクセスの有効化

Device Manager ユーザー用に外部認証を設定すると、これらのユーザー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、スタンバイユニットへの初回ログインを成功させるには、アクティブユニットへのログインと比較して、いくつかの追加手順を実行する必要があります。

外部ユーザがアクティブユニットに初めてログインすると、そのユーザとユーザのアクセス権を定義するオブジェクトが作成されます。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の同期が正常に完了して初めて、外部ユーザはスタンバイユニットにログインできます。

管理者ユーザと読み取り/書き込みユーザは、アクティブユニットにログイン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。

Threat Defense CLI のローカル ユーザ アカウントの作成

脅威に対する防御 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ませんが、CLI のみアクセスできます。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、設定権限を持つ任意のアカウントで作業できます。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 脅威に対する防御 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。使用できるコマンドは、dig、ping、traceroute です。

例：

次の例では、joecool という名前の設定アクセス権を持つユーザ 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）
ユーザーは、初回ログイン時にパスワードを変更するように求められます。ユーザーは、**configure password** コマンドを使用して以降のパスワードの変更を開始できます。

ステップ 3 （任意）セキュリティ要件を満たすアカウントの特性を調整します。

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。パスワードが有効である最大日数に続いて、有効期限前にユーザに今後の期限切れを警告する日数を指定します。値は共に 1 から 9999 ですが、警告日数は最大日数よりも小さくなければなりません。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。Use the **configure user unlock** command to unlock accounts. 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*

  パスワードの最小の長さを 1 から 127 に設定します。

- **configure user strengthcheck** ユーザ名 {**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。

ユーザのアカウントをロックアウトできます。そうしないとアカウントの削除やその他の問題の修正が必要な場合があります。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** ユーザ名 {**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。ユーザーは通常 **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*

  連続して失敗したログイン試行が最大数を超えたためにロックされたユーザアカウントのロックを解除します。

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できます。

下記の手順以外に、**reboot** コマンドまたは **shutdown** コマンドを使用して、SSH セッションまたは Device Manager 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]をクリックし、**[システム設定]**>**[再起動/シャットダウン]**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]: システムが正常に動作しておらず、試行錯誤しても問題解決に至らない場合、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]: システムをシャットダウンして、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、たとえばデバイスを交換する場合は、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 アクションが完了するまで待ちます。

コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

ISA 3000 の場合、シャットダウンが完了すると、システム LED が消灯します。電源を切る前に、少なくとも 10 秒待ってください。

システムの再起動またはシャットダウン中は、Device Manager または CLI で他のアクションを実行できません。

再起動中、Device Manager 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ページを更新しようとすると、その時点での Device Manager Web サーバーの動作状態に基づいて、Web ブラウザに 503 または 404 エラーが表示されることがあります。

シャットダウンの場合、システムは最終的にまったく応答しなくなり、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、システム レベルのトラブルシューティング タスクと機能について説明します。アクセス制御など特定の機能のトラブルシューティングについては、その機能に対応する章を参照してください。

接続テストのためのアドレスへの ping

pingは、特定のアドレスが有効であり応答するかどうかを判別できる単純なコマンドです。これは基本的な接続性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。**ping** 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、使用することができます。

（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。目的とする接続性をテストするためには、適切なコマンドを使用してください。たとえば、システムは管理インターフェイスを介してシスコのライセンスサーバに到達する必要があります。この場合、**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、代わりに TCP ping を使用できます（データ インターフェイス ping のみ）。

IP アドレスまたは完全修飾ホスト名（FQDN）のいずれかを ping できます。ping が FQDN で機能するためには、管理インターフェイスまたはデータインターフェイスのいずれかに設定された DNS サーバが IP アドレスを正常に返す必要があります。管理インターフェイスとデータインターフェイスに個別に DNS サーバを設定する必要があります。特定のインターフェイスに DNS サーバが設定されていない場合は、**dig** コマンドを使用して、特定の FQDN の IP アドレスを検索します。

ネットワーク アドレスに ping を実行する場合の主なオプションを次に示します。

管理インターフェイスを経由したアドレスのping

ping systemコマンドを使用します。

ping system *host*

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経由した ping と異なり、システム ping のデフォルト

カウントはありません。Ctrl+C キーを使用して停止させるまで、ping は継続します。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 *host*

例：

```
> 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、繰り返しカウント、パケット サイズのほか、送信するデータ パターンも指定できます。CLI で ? を使用すると、使用可能なオプションが表示されます。

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。

ping interface *if_name host*

例：

```
> 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 のみが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 は常にルーティング 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 ping が成功したとみなします。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、繰り返しカウント、および TCP ping の送信元アドレスを指定することもできます。CLI で ? を使用すると、使用可能なオプションが表示されます。

ホストへのルートのトレース

トラフィックをIPアドレスに送信する際に問題が発生した場合、ホストまでのルートをトレースし、ネットワーク パスに問題があるかどうかを判別できます。トレースルートは、無効なポートまたは ICMPv6 エコーで UDP パケットを宛先に送信することで機能します。宛先までの間にあるルータから 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、パケットごとの出力に表示される結果を示します。

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。
nn msec	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。

出力記号	説明
!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 が管理的に禁止されています。
?	ICMP の原因不明の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  www1.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*）*]*

データインターフェイスに DNS サーバを設定する場合、ホストには IPv4/IPv6 アドレスまたは www.example.com のような完全修飾ドメイン名（FQDN）を指定できます。特定のインターフェイスに DNS サーバが設定されていない場合は、**dig** コマンドを使用して、特定の FQDN の IP アドレスを検索します。例：

```
> 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（TTL）、ノード当たりのパケット数を指定できます。さらに、トレースルート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も指定できます。CLI で ? を使用すると、使用可能なオプションが表示されます。

デバイスのトレースルートへの表示

デフォルトでは、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* シリーズ ファイアウォール コンフィグレーション ガイド [英語] を参照してください。

（注） 存続可能時間を減らすと、TTL が 1 のパケットはドロップされますが、接続に TTL がもっと長いパケットが含まれている可能性があるという仮定の下に、セッションに対して接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL が 1 で送信されるため、存続可能時間を減らすと予期しない結果が生じることがある点に注意してください。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) [+] ボタンをクリックして新しいオブジェクトを作成します。

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。

コマンドを有効にするための正しいサブモードに移行するためには、親コマンドを含める必要があるのと同様に、ネゲートテンプレートにもそれらのコマンドを含める必要があります。

ネゲート テンプレートは、（正常に展開後に）FlexConfig ポリシーからこのオブジェクトを削除した場合に適用されます。また、展開に失敗した場合にも（設定を前の状態にリセットするために）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内のコマンドで更新されます。予想していたコマンドが表示されていることを確認します。

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

システムが正常に機能し、イベントおよびその他のデータ ポイントを正確に処理できることは、正確で一貫性のある時間に依存します。少なくとも 1 つ、理想的には 3 つのネットワーク タイム プロトコル（NTP）サーバ システムが、常に信頼できる時刻情報を持っているように設定する必要があります。

デバイスの接続概要図（メイン メニューの [デバイス（Device）] をクリック）に、NTP サーバへの接続の状態が表示されます。ステータスが黄色またはオレンジ色の場合、設定されている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]**で、少なくとも 3 つの NTP サーバが設定されていることを確認します。必須ではありませんが、少なくとも 3 つの NTP サーバがあると、信頼性が大幅に高くなります。
- 管理インターフェイスの 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）]**で定義されている）と NTP サーバ間のネットワーク 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、デフォルトのルートが十分でない場合、**[デバイス（Device）] > [ルーティング（Routing）]**で、NTP サーバへのスタティック 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、デバイスの 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をテストします。
- デバイスの CLI にログインし、次のコマンドで NTP サーバの状態を確認してください。
  - **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、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。

    セクション「Results of 'ntpq -pn'」を探してください。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、各ピアから取得される 8 つのサンプルのスライディング ウィンドウを使用して、1 つのサンプルをピックアップします。その後、クロック選択によって正しいチャイマーと不正なティ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、Device Manager は NTP 接続を常に黄色（非同期）にマークします。通常、NTP はより適した候補があれば、.LOCL. を選択しません。これが少なくとも 3 台のサーバを設定する必要がある理由です。

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。その後、**[デバイス（Device）]**>**[システム設定（System Settings）]**>**[DNS サーバ（DNS Server）]** ページで設定を変更できます。

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非常に重要です。**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。このインターフェイスは、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）]** > **[インターフェイス（Interfaces）]** をクリックし、[管理インターフェイス（Management Interface）] を編集して、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 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 ルートに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誤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、**dig www.cisco.com** を入力します。

- **dig** 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。このエラーは、NXDOMAIN ステータスによって示されます。応答は次のようになります。

```
> dig www.cisco.com

; <<>> DiG 9.11.4 <<>> www.cisco.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43246
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 78b1c6b2b3ef5b689fc2f65260db9e9b36a7d9fefb301943 (good)
;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     a.root-servers.net.
nstld.verisign-grs.com. 2021062901 1800 900 604800 86400

;; Query time: 13 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 22:28:43 UTC 2021
;; MSG SIZE  rcvd: 145
```

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。

- コマンドがタイムアウトする場合、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。

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** を試行してください。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-gw1.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 およびメモリ使用量の分析

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。これらのグラフには**show cpu system**コマンドと**show memory system**コマンドを使用してCLIで収集した情報が表示されます。

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。多くの詳細情報は複雑で、TAC による解釈を必要とします。

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、http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.htmlでCisco Firepower Threat Defense コマンド リファレンス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 からの指示のもとでのみ使用してください。

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。

このコマンドは、ログを選択するためのメニューを表示します。ウィザードを操作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 リストにログのサイズが示されます。非常に大きいログを開く場合は、十分に検討してください。
- 「--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 エントリを表示するには Enter キーを押します。ログの最後に到達すると、メイン メニューに移動します。「--More--」の行は、ログのサイズと表示した量を示します。

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。このファイル リストは、最上位のディレクトリから始まり、現在のディレクトリのファイル リストへと続きます。

```
> 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、しばらくしてからこのページに戻って状態を確認することができます。ファイルが生成されると、ダウンロードボタンがファイルの作成日時と一緒に表示されます。

ステップ 3 ファイルの生成が完了したら、ダウンロード ボタンをクリックします。

ブラウザの標準的なダウンロード方法を使用して、ファイルがワークステーションにダウンロードされます。

ハードウェア管理のタスク

ここでは、一部のハードウェア メンテナンス タスクの実行方法について説明します。詳細およびここに記されている以外のハードウェア管理タスクについては、対応するハードウェア ガイドを参照してください。

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。その後に、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。

Cisco Secure Firewall 3100 での SSD のホットスワップ

SSD が 2 つある場合、起動時に RAID が形成されます。ファイアウォールの電源が入っている状態で Threat Defense CLI で次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

⚠

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

手順

ステップ 1 SSD の 1 つを取り外します。

a) SSD を RAID から取り外します。

configure raid remove-secure local-disk {**1** | **2**}

remove-secure キーワードは SSD を RAID から削除し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。SSD を RAID から削除するだけでデータをそのまま維持する場合は、**remove** キーワードを使用できます。

例：

```
> configure raid remove-secure local-disk 2
```

b) SSD がインベントリに表示されなくなるまで、RAID ステータスを監視します。

show raid

SSD が RAID から削除されると、**操作性**と**ドライブの状態**が**劣化**として表示されます。2 つ目のドライブは、メンバーディスクとして表示されなくなります。

例：

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
```

```
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) SSD をシャーシから物理的に取り外します。

ステップ 2 SSD を追加します。

a) SSD を空のスロットに物理的に追加します。

b) SSD を RAID に追加します。

configure raid add local-disk {**1** | **2**}

新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。ステータスを表示するには、**show raid** コマンドを使用します。

以前に別のシステムで使用されており、まだロックされている SSD を取り付ける場合は、次のコマンドを入力します。

configure raid add local-disk {**1** | **2**} *psid*

psid は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。

USB ポートの無効化

デフォルトでは、タイプ A USB ポートは有効になっています。セキュリティ上の理由から、USB ポートへのアクセスを無効にする必要がある場合があります。USB の無効化は、次のモデルでサポートされています。

- Firepower 1000 シリーズ
- Cisco Secure Firewall 3100

ガイドライン

- USB ポートを有効または無効にするには再起動が必要です。
- USB ポートが無効で、この機能をサポートしていないバージョンにダウングレードすると、ポートは無効のままになります。NVRAM を消去（FXOS local-mgmt **erase secure all** コマンド）せずに再度有効にすることはできません。
- ROMMON **factory-reset** または FXOS local-mgmt **erase secure** を実行すると、USB ポートが再度有効になります。
- 高可用性を設定するには、各ユニットでポートを個別に無効にしたり再度有効にしたりする必要があります。

（注） この機能は、USB コンソールポート（存在する場合）には影響しません。

手順

ステップ 1 USB ポートを無効化します。

system support usb configure disable

reboot

USB ポートを再度有効にするには、**system support usb configure enable** と入力します。

例：

```
>system support usb configure disable
USB Port Admin State set to 'disabled'.
Please reboot the system to apply any control state changes.

>reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES
```

ステップ 2 ポートステータスを表示します。

system support usb show

[管理ステータス（Admin State）] には、USB ポートの設定が表示されます。[動作ステータス（Oper State）] には、現在の動作が表示されます。たとえば、USB ポートを無効化してリロードしていない場合、[管理ステータス（Admin State）] には無効と表示され、[動作ステータス（Oper State）] は有効になります。

例：

```
>system support usb show
USB Port Info
---------------
Admin State: disabled
Oper State: disabled
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。