アップグレードを復元するまたはアンインストールする

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、復元またはアンインストールが可能な場合があります。

- メジャーおよびメンテナンスアップグレードを Threat Defense に復元することができます。
- アンインストールは、Management Center を搭載した Threat Defense へのパッチが対象です。Management Center パッチをアンインストールすることもできます。

これらの方法のいずれも機能しない場合、以前のバージョンに戻すには、イメージを再作成する必要があります。ホットフィックスでは、復元もアンインストールもサポートされていないことに注意してください。

- Threat Defense アップグレードの復元 （1 ページ）
- パッチのアンインストール （6 ページ）

Threat Defense アップグレードの復元

Management Center を使用して、メジャーおよびメンテナンスアップグレードを Threat Defense に復元することができます。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（スナップショットとも呼ばれます）の直前の状態に戻ります。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。

元に戻る設定

次の設定が元に戻ります。

- Snort バージョン。
- デバイス固有の設定。

一般的なデバイス設定、ルーティング、インターフェース、インラインセット、DHCP、SNMPなど、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**ページで設定するものすべて。

- デバイス固有の設定で使用されるオブジェクト。

  アクセスリスト、AS パス、キーチェーン、インターフェイス、ネットワーク、ポート、ルートマップ、SLA モニターオブジェクトなどが含まれます。デバイスのアップグレード後にこれらのオブジェクトを編集した場合、システムは新しいオブジェクトを作成するか、元に戻されたデバイスが使用するオブジェクトのオーバーライドを設定します。これにより、他のデバイスは現在の設定に従ってトラフィックを処理し続けることができます。

  復元に成功したら、復元したデバイスで使用されているオブジェクトを調べ、必要な調整を行うことをお勧めします。

元に戻されない設定

次の設定は元に戻りません。

- 複数のデバイスで使用できる共有ポリシー。たとえば、プラットフォーム設定やアクセスコントロール ポリシーなどです。

  正常に元に戻されたデバイスは期限切れとしてマークされているため、設定を再展開する必要があります。

- Firepower 4100/9300 で、Secure Firewall Chassis Manager または FXOS CLI を使用して Threat Defense 論理デバイスに加えたインターフェイスの変更。

  Firepower 4100/9300 では、復元に成功した後にインターフェイスの変更を同期します。

復元ガイドライン

システム要件

復元を行うには、Threat Defense および Management Center 両方でバージョン 7.1.0 以降が必要です。

たとえば、バージョン 7.1.0 の Management Center はデバイスをバージョン 6.5.0 までさかのぼって管理でき、そのバージョン 7.1.0 の Management Center を使用してデバイスを中間バージョン（6.6.x、6.7.x、7.0.x）までアップグレードできる場合であっても、デバイスをバージョン 7.1.0 にアップグレードするまで、復元はサポートされません。

復元は、Firepower 4100/9300 のコンテナインスタンスではサポートされません。

高可用性/スケーラビリティデバイスの復元

Management Center Web インターフェイスを使用してデバイスを復元する場合、個々の高可用性またはクラスタ化されたユニットを選択することはできません。

すべてのユニットを同時に復元させたほうが、復元が成功する可能性が高くなります。Management Center から復元を開始すると、システムは自動的にすべてのユニットを同時に復元させます。デバイス CLI を使用する必要がある場合は、手動で行います。すべて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、プロセスを同時に開始します。同時復元とは、すべてのデバイスがスタンドアロンであるかのように、トラフィックフローと検査の中断がインターフェイスの設定のみに依存することを意味します。

完全または部分的にアップグレードされたグループで復元がサポートされていることに注意してください。部分的にアップグレードされたグループの場合、システムはアップグレードされたユニットからのみアップグレードを削除します。元に戻しても高可用性やクラスタが壊れることはありませんが、グループを分解してその新しいスタンドアロンユニットを復元することができます。

復元しても FXOS はダウングレードされない

Firepower 4100/9300 の場合、Threat Defense 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 FXOS バージョンがあります。Threat Defense の以前のバージョンに戻った後、推奨されていないバージョンの FXOS（新しすぎる）を実行している可能性があります。

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 を手動ではダウングレードできないため、このような状況下で推奨の組み合わせを稼働するには、完全な再イメージ化が必要になります。

復元を妨げるシナリオ

次のいずれかの状況で復元を試みると、システムはエラーを表示します。

表 *1:* 復元を妨げるシナリオ

シナリオ	解決方法
次の理由により、スナップショットを復元することはできません。 • デバイスをアップグレードしたときに、復元を有効にしていませんでした。 • Management Center またはデバイスからスナップショットを削除したか、スナップショットの期限が切れました。 • 別の Management Center でデバイスをアップグレードしました。	なし。 アップグレード完了後に元に戻す必要が生じる可能性がある場合は、**システム**（⚙）>**[更新（Updates）]**ページを使用し、Management Center で Threat Defense をアップグレードします。これは、「**アップグレード成功後の復元を可能にする**」オプションを設定する唯一の方法です。 **重要** これは、**[デバイス（Devices）]**>**[デバイスのアップグレード（Device Upgrade）]**ページでウィザードを使用する通常の推奨とは対照的です。 復元スナップショットは、Management Center とデバイスに 30 日間保存され、その後自動的に削除され、復元できなくなります。ディスク容量を節約するためにどのアプライアンスからでもスナップショットを手動で削除できますが、復元の機能が失われます。
最後のアップグレードに失敗しました。	アップグレードをキャンセルして、デバイスをアップグレード前の状態に戻します。または、問題を修正して再試行してください。 復元は、アップグレードは成功したものの、アップグレードされたシステムが期待どおりに機能しない場合に使用します。復元は、失敗または進行中のアップグレードをキャンセルすることとは異なります。元に戻すこともキャンセルすることもできない場合は、イメージを再作成する必要があります。
アップグレード以降に、管理アクセスインターフェイスが変更されています。	元に戻して、もう一度お試しください。
クラスタのユニットが異なるバージョンからアップグレードされました。	すべて一致するまでユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。
クラスタでのアップグレード後に 1 つ以上のユニットがクラスタに追加されました。	新しいユニットを削除し、クラスタメンバーを調整してから、小さなクラスタを復元します。新しくスタンドアロンユニットを復元することもできます。

シナリオ	解決方法
クラスタで Management Center と FXOS が異なる数のクラスタユニットを識別しています。	クラスタメンバーを調整して再試行しますが、すべてのユニットを復元することはできない場合があります。

Management Center を使用して Threat Defense を復元する

Management Center とデバイス間の通信が中断されない限り、Management Center を使用してデバイスを復元する必要があります。通信が中断された場合は、デバイスで **upgrade revert** CLI コマンドを使用できます。システムがどのバージョンに戻るのかを確認するには、**show upgrade revert-info** コマンドを使用します。

⚠

注意 CLI から復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。

始める前に

- 復元がサポートされていることを確認してください。ガイドラインを読んで理解してください。
- 安全な外部の場所にバックアップします。復元に失敗した場合、再イメージ化が必要になることがあります。再イメージ化を行うと、ほとんどの設定が工場出荷時の状態に戻ります。

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 復元するデバイスの横にある **その他**（⋮） をクリックして、[アップグレードの復元（Revert Upgrade）] を選択します。

ハイ アベイラビリティペアとクラスタを除き、複数のデバイスを選択して復元することはできません。

ステップ 3 復元して再起動することを確認します。

復元中のトラフィックフローとインスペクションの中断は、すべてのデバイスがスタンドアロンであるかのように、インターフェイス設定に依存します。 これは、高可用性/スケーラビリティ展開であっても、システムがすべてのユニットを同時に復元するためです。

ステップ 4 復元の進行状況を監視します。

高可用性/スケーラビリティ展開では、最初のユニットがオンラインに戻ると、トラフィックフローとインスペクションが再開されます。数分間にわたり進展がない場合、または復元が失敗したことを示している場合は、Cisco TAC にお問い合わせください。

ステップ 5 復元が成功したことを確認します。

復元が完了したら、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、復元したデバイスのソフトウェアバージョンが正しいことを確認します。

ステップ 6 （Firepower 4100/9300）Chassis Manager または FXOS CLI を使用して、Threat Defense 論理デバイスに加えたインターフェイスの変更を同期します。

Management Center で [デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、 デバイスを編集して [同期（Sync）] をクリックします。

ステップ 7 その他に必要となる復元後の構成変更を完了します。

たとえば、デバイスのアップグレード後にデバイス固有の設定で使用されるオブジェクトを編集した場合、システムは新しいオブジェクトを作成するか、復元されたデバイスが使用するオブジェクトのオーバーライドを設定します。復元したデバイスで使用されるオブジェクトを調べ、必要な調整を行うことをお勧めします。

ステップ 8 復元したデバイスに構成を再度展開します。

正常に復元されたデバイスは期限切れとしてマークされます。デバイスは古いバージョンを実行することになるため、展開が成功した後でも、新しい構成がサポートされない場合があります。

パッチのアンインストール

パッチをアンインストールするとアップグレード前のバージョンに戻り、設定は変更されません。Management Center では、管理対象デバイスと同じかより新しいバージョンを実行する必要があるため、最初にデバイスからパッチをアンインストールします。

アンインストールに対応するパッチ

特定のパッチをアンインストールすると、アンインストールが成功した場合でも、問題が発生する可能性があります。次のような問題があります。

- アンインストール後に設定変更を展開できない
- オペレーティングシステムと ソフトウェアの間に互換性がなくなる
- セキュリティ認定コンプライアンスが有効な状態（CC/UCAPL モード）でそのパッチが適用されていた場合、アプライアンスの再起動時に FSIC（ファイル システム整合性チェック）が失敗する

⚠

注意 セキュリティ認定の遵守が有効な場合に FSIC が失敗すると、ソフトウェアは起動せず、リモート SSH アクセスが無効になるため、ローカルコンソールを介してのみアプライアンスにアクセスできます。この問題が発生した場合は、Cisco TACにお問い合わせください。

アンインストールに対応したバージョン 7.2 のパッチ

現在、すべてのバージョン 7.2 パッチがアンインストールに対応しています。

高可用性/拡張性のアンインストール順序

高可用性/拡張性の展開では、一度に 1 つのアプライアンスからアンインストールすることで中断を最小限に抑えます。アップグレードとは異なり、システムはこの操作を行いません。次に移る前に、パッチが 1 つのユニットから完全にアンインストールされるまで待ちます。

表 *2 : Management Center* 高可用性のアンインストール順序

設定	アンインストール順序
Management Center ハイ アベイラビリティ	同期を一時停止した状態（「スプリットブレイン」と呼びます）で、ピアから一度に 1 つずつアンインストールします。ペアが split-brain の状況で、構成の変更または展開を行わないでください。 **1.** 同期を一時停止します（スプリットブレインに移行します）。 **2.** スタンバイからアンインストールします。 **3.** アクティブからアンインストールします。 **4.** 同期を再開します（スプリットブレインから抜けます）。

表 *3 : Threat Defense* 高可用性およびクラスタのアンインストール順序

設定	アンインストール順序
Threat Defense ハイ アベイラビリティ	ハイ アベイラビリティ用に設定されたデバイスからパッチをアンインストールすることはできません。先にハイ アベイラビリティを解除する必要があります。 **1.** ハイ アベイラビリティを解除します。 **2.** 以前のスタンバイからアンインストールします。 **3.** 以前のアクティブからアンインストールします。 **4.** ハイ アベイラビリティを再確立します。
Threat Defense クラスタ	一度に1つのユニットからアンインストールし、制御ユニットを最後に残します。クラスタ化されたユニットは、パッチのアンインストール中はメンテナンス モードで動作します。 **1.** データモジュールから一度に 1 つずつアンインストールします。 **2.** データモジュールの 1 つを新しい制御モジュールに設定します。 **3.** 以前のコントロールからアンインストールします。

Threat Defense パッチのアンインストール

Linux シェル（エキスパートモード）を使用して Threat Defense パッチをアンインストールします。デバイスの admin ユーザーとして、または CLI 設定アクセス権を持つ別のローカル ユーザーとして、デバイス シェルにアクセスできる必要があります。Management Center ユーザー アカウントは使用できません。 シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

注意 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、シャットダウン、または再起動しないでください。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。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストールで問題が発生した場合には、Cisco TAC にお問い合わせください。

始める前に

- 高可用性ペアを解除します。「高可用性/拡張性のアンインストール順序 （7 ページ）」を参照してください。
- 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。

ステップ 1 デバイスの設定が古い場合は、この時点で Management Center から展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。展開とその他の必須のタスクが完了していることを確認してください。アンインストールの開始時に実行中だったタスクは停止され、失敗したタスクとなって再開できなくなります。後で失敗ステータス メッセージを手動で削除できます。

ステップ 2 デバイスの Threat Defense CLI にアクセスします。admin として、または設定アクセス権を持つ別の CLI ユーザーとしてログインします。

デバイスの管理インターフェイスに SSH 接続するか（ホスト名または IP アドレス）、コンソールを使用できます。コンソールを使用する場合、一部のデバイスではデフォルトでオペレーティング システムの CLI に設定されており、Threat Defense CLI にアクセスする場合は追加の手順が必要になります。

Firepower 1000 シリーズ	`connect ftd`
Firepower 2100 シリーズ	`connect ftd`
Firepower 3100 シリーズ	`connect ftd`
Firepower 4100/9300	`connect module` *slot_number* `console`、次に `connect ftd`（最初のログインのみ）

ステップ 3 `expert` コマンドを使用して Linux シェルにアクセスします。

ステップ 4 アップグレードディレクトリにアンインストールパッケージがあることを確認します。

```
ls /var/sf/updates
```

パッチのアンインストーラには、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には Patch ではなく Patch_Uninstaller が含まれています。デバイスにパッチを適用すると、そのパッチ用のアンインストーラがアップグレードディレクトリに自動的に作成されます。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

ステップ 5 uninstall コマンドを実行し、プロンプトが表示されたらパスワードを入力します。

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

注意 確認を求められることはありません。このコマンドを入力すると、デバイスの再起動を含むアンインストールが開始されます。アンインストール時のトラフィック フローとインスペクションの中断は、アップグレード時に発生する中断と同じです。準備が整っていることを確認してください。--detach オプションを使用すると、SSH セッションがタイムアウトした場合にアンインストールプロセスが強制終了されなくなり、デバイスが不安定な状態になる可能性があることに注意してください。

ステップ 6 ログアウトするまでアンインストールを監視します。

個別のアンインストールの場合は、tail か tailf を使用してログを表示します。

```
tail /ngfw/var/log/sf/update.status
```

それ以外の場合は、コンソールか端末で進行状況を監視します。

ステップ 7 アンインストールが成功したことを確認します。

アンインストールが完了したら、デバイスのソフトウェアバージョンが正しいことを確認します。Management Center で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

ステップ 8 高可用性/スケーラビリティの展開では、ユニットごとに手順 2 から 6 を繰り返します。

クラスタの場合、制御ユニットからアンインストールしないでください。すべてのデータユニットからアンインストールしたら、そのうちの 1 つを新しい制御ユニットに設定し、以前の制御ユニットからアンインストールします。

ステップ 9 構成を再展開します。

例外：複数のバージョンが構成されている高可用性ペアまたはデバイスクラスタには展開しないでください。展開は最初のデバイスからアンインストールする前に行いますが、すべてのグループメンバからパッチのアンインストールを終えるまでは再度展開しないでください。

次のタスク

- 高可用性については、高可用性を再確立します。
- クラスタについては、特定のデバイスに優先するロールがある場合は、それらの変更をすぐに行います。

スタンドアロン Management Center パッチのアンインストール

Management Center パッチのアンインストールには Web インターフェイスを使用することをお勧めします。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの `admin` ユーザーまたはシェル アクセス権を持つ外部ユーザーのどちらかとして 使用できます。シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

⚠

注意 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、シャットダウン、または再起動しないでください。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。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストールで問題が発生した場合には、Cisco TAC にお問い合わせください。

始める前に

- アンインストールによって Management Center のパッチレベルが管理対象デバイスより低くなる場合は、最初にデバイスからパッチをアンインストールします。
- 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。

ステップ 1 構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 [利用可能なアップデート（Available Updates）] で該当するアンインストールパッケージの横にある [インストール（Install）] アイコンをクリックして、Management Center を選択します。

パッチのアンインストーラには、アップグレードパッケージと同様に名前が付けられていますが、ファイル名には `Patch` ではなく `Patch_Uninstaller` が含まれています。Management Center にパッチを適用すると、そのパッチ用のアンインストーラが自動的に作成されます。アンインストーラがない場合は、Cisco TAC までお問い合わせください。

ステップ 3 [インストール（Install）] をクリックしてから、アンインストールすることを確認して再起動します。

ログアウトするまで、メッセージセンターでアンインストールの進行状況を確認します。

ステップ 4 可能なときに再度ログインし、アンインストールが成功したことを確認します。

ログイン時にアンインストールの成功メッセージが表示されない場合は、[ヘルプ（Help）] > [バージョン情報（About）] の順に選択して、現在のソフトウェアのバージョン情報を表示します。

ステップ 5 管理対象デバイスに構成を再展開します。

高可用性 Management Center パッチのアンインストール

Management Center パッチのアンインストールには Web インターフェイスを使用することをお勧めします。Web インターフェイスを使用できない場合は、Linux シェルを、シェルの `admin` ユーザーまたはシェル アクセス権を持つ外部ユーザーのどちらかとして 使用できます。シェルアクセスを無効にした場合は、 ロックダウンを元に戻すために Cisco TAC にご連絡ください。

高可用性ピアから一度に 1 つずつアンインストールします。同期を一時停止した状態で、先にスタンバイからアンインストールし、次にアクティブからアンインストールします。スタンバイでアンインストールが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態のことを「スプリットブレイン」と呼び、アップグレード中とアンインストール中を除き、サポートされていません。

注意 ペアが split-brain の状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。 アンインストール中に設定の変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、進行中のアンインストールを手動で再起動、シャットダウン、または再起動しないでください。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。アンインストールに失敗する、アプライアンスが応答しないなど、アンインストールで問題が発生した場合には、Cisco TAC にお問い合わせください。

始める前に

- アンインストールによって Management Center のパッチレベルが管理対象デバイスより低くなる場合は、最初にデバイスからパッチをアンインストールします。
- 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。

ステップ 1 アクティブな Management Center で、構成が古い管理対象デバイスに展開します。

アンインストールする前に展開すると、失敗する可能性が減少します。

ステップ 2 アクティブ状態の Management Center で、同期を一時停止します。

a) **[システム（System）] > [統合（Integration）]** の順に選択します。

b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 3 ピアからパッチを一度に 1 つずつアンインストールします。先にスタンバイで行い、次はアクティブで行います。

「スタンドアロン Management Center パッチのアンインストール （10 ページ）」の手順に従います。ただし、初期の展開は省略し、各ピアでアンインストールが成功したことを確認したら停止します。要約すると、各ピアで次の手順を実行します。

a) [システム（System）] > [更新（Updates）] ページで、パッチをアンインストールします。

b) ログアウトするまで進行状況を確認し、ログインできる状態になったら再びログインします。
c) アンインストールが成功したことを確認します。

ステップ 4 アクティブ ピアにする Management Center で、同期を再開します。

a) **[システム（System）]** > **[統合（Integration）]** の順に選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[アクティブにする（Make-Me-Active）] をクリックします。
c) 同期が再開し、その他の Management Center がスタンバイ モードに切り替わるまで待ちます。

ステップ 5 管理対象デバイスに構成を再展開します。

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。