バックアップ/復元

バックアップと復元について

災害から回復する能力は、システム保守計画の重要な部分を占めます。災害復旧計画の一環として、セキュアなリモートの場所への定期的なバックアップを実行することをお勧めします。

バックアップの内容

デバイスバックアップは常に設定のみです。Management Center のバックアップは次のとおりです。

表 *1 : Management Center* のバックアップ

バックアップタイプ	バックアップされる	バックアップされない
設定	ほとんどの設定がバックアップされます。 マルチドメイン展開では、設定をバックアップする必要があります。イベントまたはTIDデータのみをバックアップすることはできません。	次の設定はバックアップされないため、復元後に再設定する必要があります。 • リモートストレージの設定。 • 監査ログサーバーの証明書の設定。 • パブリックおよびプライベート AMP クラウド接続）。

バックアップタイプ	バックアップされる	バックアップされない
イベント	Firewall Management Center データベース内のすべてのイベント。	侵入イベントのレビューステータスはバックアップされません。復元された侵入イベントは、[確認済みイベント（Reviewed Events）] ページには表示されません。
Threat Intelligence Director（TID）データ。	詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Backing Up and Restoring Threat Intelligence Director Data*」を参照してください。	
レポート	—	Firewall Management Center に保存されているレポートは、 バックアップの一部としてバックアップされません。レポートは、安全なリモートロケーションに保存する必要があります。

復元の内容

設定を復元すると、ごくわずかの例外を除いて、バックアップされたすべての設定が上書きされます。Firewall Management Center では、イベントおよび TID データを復元すると、侵入イベントを除くすべての既存のイベントおよび TID データが上書きされます。

次のことを理解して計画してください。

- 上記のように、バックアップされていないものは復元できません。
- VPN 証明書の復元は失敗します。

  Firewall Threat Defense 復元プロセスでは、VPN 証明書およびすべての VPN 設定が Firewall Threat Defense デバイスから削除されます。これには、バックアップの作成後に追加された証明書も含まれます。Firewall Threat Defense デバイスを復元した後に、すべての VPN 証明書を再追加/再登録し、デバイスを再展開する必要があります。
- 設定済みの Firewall Management Center への復元：工場出荷時または再イメージ化された状態に復元されるのではなく、侵入イベントおよびファイル リストがマージされます。

  Firewall Management Center のイベント復元プロセスでは、侵入イベントは上書きされません。代わりに、バックアップ内の侵入イベントがデータベースに追加されます。重複を避けるには、復元する前に既存の侵入イベントを削除してください。

  Firewall Management Center の設定復元プロセスでは、マルウェア防御 で使用されるクリーンおよびカスタム検出ファイルリストは上書きされません。代わりに、既存のファイルリストとバックアップ内のファイルリストがマージされます。ファイルリストを置き換えるには、復元する前に既存のファイルリストを削除してください。

オンデマンドバックアップ

Firewall Management Center から、Firewall Management Center および多数の Firewall Threat Defense デバイスでオンデマンド バックアップを実行できます。

詳細については、「Firewall Management Center または管理対象デバイスのバックアップ （13 ページ）」を参照してください。

スケジュール バックアップ

Firewall Management Center でスケジューラを使用して、バックアップを自動化することができます。Firewall Management Center からデバイスのリモートバックアップをスケジュールすることもできます。

Firewall Management Center のセットアッププロセスでは、設定のみのバックアップを毎週ローカルに保存するようにスケジュールされます。これは、オフサイトのフルバックアップの代わりにはなりません。初期設定が完了したら、スケジュールされたタスクを確認し、組織のニーズに合わせて調整する必要があります。

詳細については、「スケジュール バックアップ」を参照してください。

バックアップファイルの保存

バックアップはローカルに保存することができます。ただし、NFS、SMB、またはSSHFS ネットワークボリュームをリモートストレージとしてマウントして、Firewall Management Center および管理対象デバイスを安全なリモートロケーションにバックアップすることをお勧めします。これを実行すると、その後のすべてのバックアップがそのボリュームにコピーされますが、引き続き Firewall Management Center を使用してそれらを管理することができます。

詳細については、「リモート ストレージデバイス」および「バックアップとリモートストレージの管理 （38 ページ）」を参照してください。

バックアップからの復元

[バックアップ管理（Backup Management）] ページから Firewall Management Center を復元できます。Firewall Threat Defense デバイスを復元するには、Firewall Threat Defense CLI を使用する必要があります。ただし、SD カードと [Reset] ボタンを使用する ISA 3000 ゼロタッチ復元は除きます。

詳細については、「Firewall Management Center および管理対象デバイスの復元 （19 ページ）」を参照してください。

バックアップと復元の要件

バックアップと復元には次の要件があります。

プラットフォーム要件：バックアップ

次の表に、プラットフォームごとのバックアップのサポートを示します。デバイスのバックアップは、アプリケーションとコンテナの両方のインスタンスでサポートされています。

表 *2:* プラットフォーム別のバックアップのサポート

プラットフォーム	バックアップがサポートされているか		
	スタンドアロン	ハイ アベイラビリティ	クラスタ（**Clusters**）
Management Center、ハードウェアおよび仮想	**YES**	**YES**	—
Threat Defense ハードウェア	**YES**	**YES**	**YES**
Threat Defense Virtual、オンプレミス/プライベートクラウド	VMware [HyperFlex] Nutanix OpenStack	VMware	VMware
Threat Defense Virtual、パブリッククラウド	—	—	—

プラットフォーム要件：復元

交換用の管理対象デバイスは、交換するものと同じモデルで、同じ数のネットワークモジュールと同じタイプおよび数の物理インターフェイスを備えている必要があります。

Firewall Management Center の場合、RMA シナリオでバックアップと復元を使用できるだけでなく、Firewall Management Center 間で設定とイベントを移行するためにバックアップと復元を使用できます。サポート対象の移行先モデルなどの詳細については、Cisco Secure Firewall Management Center モデル移行ガイド を参照してください。

バージョン要件

バックアップの最初のステップとして、パッチレベルを書き留めておきます。バックアップを復元するには、新旧のアプライアンスで、同じソフトウェアバージョン（パッチも含む）が実行されている必要があります。Firepower 4100/9300 シャーシを復元するには、互換性のある FXOS バージョンが実行されている必要があります。

Firewall Management Center バックアップの場合、同じ VDB または SRU が必要ではありません。ただし、バックアップを復元すると、既存の VDB がバックアップファイル内の VDB に置き換えられることに注意してください。これが発生した場合は、メッセージセンターで報告されます。復元された SRU または VDB バージョンが シスコ サポートおよびダウンロード サイトで利用可能なものより古い場合は、新しいバージョンをインストールすることをお勧めします。

ライセンス要件

ベストプラクティスと手順の説明に従って、ライセンスまたは孤立した権限付与の問題に対処してください。ライセンスの競合に気付いた場合は、Cisco TAC にお問い合わせください。

ドメインの要件

方法：

- Firewall Management Center のバックアップまたは復元：グローバルのみ。
- Firewall Management Center からデバイスをバックアップ：グローバルのみ。
- デバイスの復元：なし。CLI でデバイスをローカルに復元してください。

マルチドメイン展開では、イベント/TIDデータのみをバックアップすることはできません。設定もバックアップする必要があります。

バックアップと復元の注意事項と制限事項

バックアップと復元には次の注意事項と制限事項があります。

バックアップと復元はディザスタリカバリ/RMA 用です

バックアップと復元は、主に RMA シナリオを対象としています。問題または障害がある物理アプライアンスの復元プロセスを開始する前に、交換用のハードウェアについて Cisco TAC にお問い合わせください。

Firewall Management Center 間で設定とイベントを移行するためにバックアップと復元を使用することもできます。これにより、組織の拡大、物理実装から仮想実装への移行、ハードウェアの更新など、技術面またはビジネス面の理由による Firewall Management Center の交換が容易になります。

再イメージ化された Management Center での復元

常に、新しく再イメージ化された Firewall Management Center に Firewall Management Center を復元します。再イメージ化せずに復元し、バックアップ後に Firewall Threat Defense をFirewall Management Center に登録した場合、復元された Firewall Management Center にデバイスを再度登録すると、認定エラーによってデバイスの登録が失敗します。このエラーは、復元された証明書データベースと、復元された再イメージ化されていない Firewall Management Center バックアップの不一致が原因で発生します。

バックアップと復元は、コンフィギュレーションのインポート/エクスポートではありません

バックアップファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。アプライアンスまたはデバイス間で設定をコピーする目的で、または新しい設定をテストする際に設定を保存する方法として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。代わりに、インポート/エクスポート機能を使用してください。

たとえば、Firewall Threat Defense デバイスのバックアップには、デバイスの管理 IP アドレスと、デバイスが管理 Firewall Management Center に接続するために必要なすべての情報が含まれます。別の Firewall Management Center によって管理されているデバイスに Firewall Threat Defense バックアップを復元しないでください（復元されたデバイスがバックアップで指定された Firewall Management Center への接続を試みるため）。

復元は個別かつローカルです

Firewall Management Center および管理対象デバイスは、個別かつローカルに復元します。これは、以下を意味します。

- 高可用性またはクラスタ化 Firewall Management Center またはデバイスに一括で復元することはできません。
- Firewall Management Center を使用してデバイスを復元することはできません。Firewall Management Center の場合は、Web インターフェイスを使用して復元することができます。Firewall Threat Defense デバイスの場合は、SD カードとリセットボタンを使用する ISA 3000 ゼロタッチ復元を除き、Firewall Threat Defense CLI を使用する必要があります。
- Firewall Management Center をバックアップから復元すると、正常性性ポリシーも復元されます。ただし、正常性モニタリング設定の更新はデバイスに展開されません。正常な復元後、正常性モニタリングの不一致を避けるために、すべての正常性ポリシーを再展開する必要があります。
- Firewall Management Center のユーザーアカウントを使用して、いずれかの管理対象デバイスにログインし、復元することはできません。Firewall Management Center とデバイスでは、独自のユーザーアカウントが維持されます。

Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポートに関するガイドライン

Firepower 4100/9300 シャーシの論理デバイスとプラットフォームのコンフィギュレーション設定を含む XML ファイルをリモート サーバまたはローカル コンピュータにエクスポートするコンフィギュレーションのエクスポート機能を使用できます。そのコンフィギュレーション ファイルを後でインポートして Firepower 4100/9300 シャーシに迅速にコンフィギュレーション設定を適用し、よくわかっている構成に戻したり、システム障害から回復させたりすることができます。

ガイドラインと制限

- コンフィギュレーション ファイルの内容は、修正しないでください。コンフィギュレーション ファイルが変更されると、そのファイルを使用するコンフィギュレーション インポートが失敗する可能性があります。
- 用途別のコンフィギュレーション設定は、コンフィギュレーション ファイルに含まれていません。用途別の設定やコンフィギュレーションを管理するには、アプリケーションが提供するコンフィギュレーション バックアップ ツールを使用する必要があります。

- Firepower 4100/9300 シャーシへのコンフィギュレーションのインポート時、Firepower 4100/9300 シャーシのすべての既存のコンフィギュレーション（論理デバイスを含む）は削除され、インポートファイルに含まれるコンフィギュレーションに完全に置き換えられます。
- RMA シナリオを除き、コンフィギュレーションファイルのエクスポート元と同じFirepower 4100/9300 シャーシだけにコンフィギュレーション ファイルをインポートすることをお勧めします。
- インポート先の Firepower 4100/9300 シャーシのプラットフォーム ソフトウェア バージョンは、エクスポートしたときと同じバージョンになるはずです。異なる場合は、インポート操作の成功は保証されません。シスコは、Firepower 4100/9300 シャーシをアップグレードしたりダウングレードしたりするたびにバックアップ設定をエクスポートすることを推奨します。
- インポート先のFirepower 4100/9300 シャーシでは、エクスポートしたときと同じスロットに同じネットワークモジュールがインストールされている必要があります。
- インポート先のFirepower 4100/9300 シャーシでは、インポートするエクスポートファイルに定義されているすべての論理デバイスに、正しいソフトウェアアプリケーションイメージがインストールされている必要があります。
- 既存のバックアップファイルが上書きされるのを回避するには、バックアップ操作内のファイル名を変更するか、既存のファイルを別の場所にコピーします。

（注） FXOS のインポート/エクスポートはFXOS の設定のみをバックアップするため、ロジックアプリを個別にバックアップする必要があります。FXOS の設定をインポートすると、論理デバイスが再起動され、工場出荷時のデフォルト設定でデバイスが再構築されます。

バックアップと復元のベストプラクティス

バックアップと復元には、次のベストプラクティスがあります。

バックアップのタイミング

メンテナンスの時間帯やその他の使用率の低い時間帯にバックアップすることをお勧めします。

バックアップデータの収集中に、データの相関付けが一時的に停止して（Firewall Management Center のみ）、バックアップ関連の設定を変更できなくなることがあります。イベントデータを含める場合、eStreamer などのイベント関連機能は使用できません。

次の状況でバックアップする必要があります。

- 定期的なスケジュールバックアップまたはオンデマンドバックアップ。

災害復旧計画の一環として、定期的なバックアップを実行することをお勧めします。

Firewall Management Center のセットアッププロセスでは、設定のみのバックアップを毎週ローカルに保存するようにスケジュールされます。これは、オフサイトのフルバックアップの代わりにはなりません。初期設定が完了したら、スケジュールされたタスクを確認し、組織のニーズに合わせて調整する必要があります。詳細については、スケジュールバックアップを参照してください。

- SLR が変更された後。

  特定ライセンス予約（SLR）に変更を加えた後に、Firewall Management Center をバックアップします。変更を加えてから古いバックアップを復元すると、特定ライセンスの戻りコードに問題が発生し、孤立した権限付与が発生する可能性があります。

- アップグレードまたは再イメージ化の前。

  アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。

（注） バックアップから復元しても、再イメージ化または RMA 後に設定したパスワードはリセットされません。

- アップグレードの後。

  アップグレード後にバックアップします。これにより、新しくアップグレードした展開のスナップショットが得られます。新しい Firewall Management Center バックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後に Firewall Management Center をバックアップすることをお勧めします。

バックアップファイルのセキュリティの維持

バックアップは、暗号化されていないアーカイブ（.tar）ファイルとして保存されます。

PKI オブジェクトの秘密キー（展開をサポートするために必要な公開キー証明書とペアになった秘密キーを表す）は、バックアップされる前に復号されます。バックアップを復元すると、このキーはランダムに生成されるキーで再暗号化されます。

（注） Firewall Management Center とデバイスを安全なリモートロケーションにバックアップし、転送が成功することを確認することをお勧めします。ローカルに残っているバックアップは、手動または（ローカルに保存されたバックアップが消去される）アップグレードプロセスによって削除される可能性があります。

特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。Admin/Maint ロールを持つユーザーは [バックアップ管理（Backup Management）] ページにアクセスでき、そこでリモートストレージからファイルを移動および削除できることに注意してください。

Firewall Management Center のシステム設定では、NFS、SMB、または SSHFS ネットワークボリュームをリモートストレージとしてマウントできます。これを実行すると、その後のすべてのバックアップがそのボリュームにコピーされますが、引き続き Firewall Management Center を使用してそれらを管理することができます。詳細については、リモート ストレージ デバイスおよびバックアップとリモートストレージの管理 （38 ページ）を参照してください。

Firewall Management Center だけがネットワークボリュームをマウントすることに注意してください。管理対象デバイスのバックアップファイルは、Firewall Management Center を介してルーティングされます。Firewall Management Center とそのデバイスの間に大容量のデータを転送するための帯域幅があることを確認します。詳細については、『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

Firewall Management Center ハイアベイラビリティ展開でのバックアップと復元

Firewall Management Center ハイアベイラビリティ展開では、一方の Firewall Management Center をバックアップしても他方はバックアップされません。定期的に両方のピアをバックアップする必要があります。一方の HA ピアを他方のバックアップファイルで復元しないでください。バックアップ ファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。

正常なバックアップがなくても HA Firewall Management Center を交換できることに注意してください。正常なバックアップの有無にかかわらず、HA Firewall Management Center の交換の詳細については、高可用性ペアでの Firewall Management Center の交換を参照してください。

Firewall Threat Defense 高可用性展開でのバックアップと復元

Firewall Threat Defense高可用性展開では、次のことを行う必要があります。

- Firewall Management Center からデバイスペアをバックアップしますが、復元は Firewall Threat Defense CLI から個別かつローカルに行います。

  バックアッププロセスにより、ペアごとの一意のバックアップファイルが生成されます。一方のピアを他方のバックアップファイルで復元しないでください。バックアップファイルは、アプライアンスを一意に識別する情報を含んでおり、共有することはできません。

デバイスの役割は、バックアップファイル名に示されます。復元する際は、必ず、適切なバックアップファイル（プライマリまたはセカンダリ）を選択してください。

- 復元する前に高可用性を一時停止または解除しないでください。

  高可用性設定を維持することで、交換用デバイスを復元後に簡単に再接続できます。

- 両方のピアで **restore** CLI コマンドを同時に実行しないでください。

  バックアップが正常に完了したら、ピアの一方または両方のピアを交換できます。任意の物理的な交換タスク（ラックからの取り外し、ラックへの再設置など）を同時に実行できます。ただし、再起動を含め、最初のデバイスの復元プロセスが完了するまで、2 つ目のデバイスで **restore** コマンドを実行しないでください。

- 両方のピアに障害が発生した場合は、デバイスが廃止される前に、Firewall Management Center から両方のピアを登録解除します。

正常なバックアップがなくても高可用性デバイスを交換できます。

Firewall Threat Defense クラスタリング展開でのバックアップと復元

Firewall Threat Defense クラスタリング展開では、次の操作を行う必要があります。

- Firewall Management Center からクラスタ全体をバックアップし、Firewall Threat Defense CLI から個別かつローカルにノードを復元します。

  バックアッププロセスにより、クラスタノードごとに一意のバックアップファイルを含むバンドルされた tar ファイルが生成されます。あるノードを別のノードのバックアップファイルで復元しないでください。バックアップファイルには、デバイスを一意に識別する情報が含まれており、共有できません。

  ノードの役割は、そのバックアップファイル名に示されます。復元する際は、適切なバックアップファイル（制御またはデータ）を選択してください。

  個々のノードはバックアップできません。データノードがバックアップに失敗した場合でも、Firewall Management Center は他のすべてのノードを引き続きバックアップします。制御ノードのバックアップに失敗した場合、バックアップはキャンセルされます。

- 復元する前にクラスタリングを一時停止または解除しないでください。

  クラスタ設定を維持することで、復元後に交換用デバイスを簡単に再接続できます。

- 複数のノードで **restore** CLI コマンドを同時に実行しないでください。最初に制御ノードを復元し、クラスタに再参加するまで待ってから、データノードを復元することを推奨します。

  バックアップが正常に実行されている場合、クラスタ内の複数のノードを交換できます。任意の物理的な交換タスク（ラックからの取り外し、ラックへの再設置など）を同時に実行できます。ただし、再起動を含め、前のノードの復元プロセスが完了するまで、追加のノードで **restore** コマンドを実行しないでください。

Firepower 4100/9300 シャーシのバックアップと復元

Firepower 4100/9300 シャーシで Firewall Threat Defense ソフトウェアを復元するには、シャーシで互換性のある FXOS バージョンが実行されている必要があります。Firepower 4100/9300 シャーシをバックアップする場合は、FXOS 設定もバックアップすることを強くお勧めします。追加のベストプラクティスについては、Firepower 4100/9300 のコンフィギュレーションのインポート/エクスポートに関するガイドライン （6 ページ）を参照してください。

バックアップ前

バックアップの前に、次のことを行う必要があります。

- Firewall Management Center で VDB と SRU を更新します。

  常に最新の脆弱性データベース（VDB）と侵入ルール（SRU）を使用することをお勧めします。Firewall Management Center をバックアップする前に、シスコ サポートおよびダウンロード サイト の新しいバージョンがないか確認してください。

- ディスク容量を確認します。

  バックアップを開始する前に、アプライアンスまたはリモートストレージサーバーに十分なディスク容量があることを確認します。使用可能な容量は、[バックアップ管理（Backup Management）] ページに表示されます。

  十分な容量がない場合、バックアップが失敗する可能性があります。 特にバックアップをスケジュールする場合は、必ず、バックアップ ファイルを定期的にプルーニングするか、リモートの保存場所により多くのディスク容量を割り当ててください。

復元前

復元の前に、次のことを行う必要があります。

- ライセンスの変更を元に戻します。

  バックアップを実行した後に行われたライセンス変更を元に戻します。

  そうしないと、復元後にライセンスの競合や孤立した権限付与が発生する可能性があります。ただし、Cisco Smart Software Manager（CSSM）の登録を解除しないでください。CSSM の登録を解除すると、復元後に再度登録を解除してから再登録する必要があります。

  復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。

- 障害のあるアプライアンスを切断します。

  管理インターフェイスを切断し、デバイスの場合はデータインターフェイスも切断します。

  Firewall Threat Defense デバイスを復元すると、交換用デバイスの管理 IP アドレスが古いデバイスの管理 IP アドレスに設定されます。IP の競合を回避するには、バックアップを交換用デバイスに復元する前に、古いデバイスを管理ネットワークから切断します。

Firewall Management Center を復元しても管理 IP アドレスが変更されないことに注意してください。交換時に手動で設定する必要があります。必ず、設定する前に、古いアプライアンスをネットワークから切断してください。

- 管理対象デバイスの登録を解除しないでください。

  Firewall Management Center または管理対象デバイスのいずれを復元する場合でも、アプライアンスをネットワークから物理的に切断しても、デバイスの Firewall Management Center 登録を解除しないでください。

  登録を解除した場合は、一部のデバイス設定（セキュリティゾーンとインターフェイスのマッピングなど）をやり直す必要があります。復元後、Firewall Management Center とデバイスは正常に通信を開始します。

- 再イメージ化します。

  RMA シナリオでは、交換用アプライアンスは、工場出荷時のデフォルト設定で納品されます。ただし、交換用アプライアンスがすでに設定されている場合は、再イメージ化することをお勧めします。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。メジャーバージョンにのみ再イメージ化できるため、再イメージ化後にパッチの適用が必要な場合があります。

  再イメージ化しない場合は、Firewall Management Center の侵入イベントおよびファイルリストが上書きされるのではなくマージされることに注意してください。

復元後

復元の後に、次のことを行う必要があります。

- 復元されなかったものをすべて再設定します。

  これには、ライセンス、リモートストレージ、および監査ログサーバー証明書設定の再設定が含まれる場合があります。 また、失敗した Firewall Threat Defense VPN 証明書を再追加/再登録する必要があります。

- Firewall Management Center で VDB と SRU を更新します。

  常に最新の脆弱性データベース（VDB）と侵入ルール（SRU）を使用することをお勧めします。 バックアップ内の VDB によって交換用 Firewall Management Center 上の VDB が上書きされるため、これは VDB にとって特に重要です。

- 展開します。

  Firewall Management Center を復元するかデバイスを復元するかを問わず、必ず展開する必要があります。復元されたデバイスの場合は、強制的に展開する必要がある場合があります。Cisco Secure Firewall Management Center デバイス構成ガイドのデバイスへの既存の設定の再展開を参照してください。

Firewall Management Center または管理対象デバイスのバックアップ

サポートされるアプライアンスのオンデマンドバックアップまたはスケジュールバックアップを実行できます。

Firewall Management Center からデバイスをバックアップする場合、バックアッププロファイルは必要ありません。ただし、Firewall Management Center のバックアップにはバックアッププロファイルが必要です。。オンデマンド バックアップ プロセスでは、新しいバックアッププロファイルを作成できます。

のバックアップ Firewall Management Center

Firewall Management Center のオンデマンドバックアップを実行するには、次の手順を実行します。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （3 ページ）
- バックアップと復元の注意事項と制限事項 （5 ページ）
- バックアップと復元のベストプラクティス （7 ページ）

手順

ステップ 1 [システム（System）]（⚙）>**[ツール（Tools）]**>**[バックアップ/復元（Backup/Restore）]** を選択します。

[バックアップ管理（Backup Management）] ページには、ローカルとリモートで保存されたすべてのバックアップが一覧表示されます。また、バックアップの保存に使用できるディスク容量も一覧表示されます。十分な容量がない場合、バックアップが失敗する可能性があります。

ステップ 2 既存のバックアッププロファイルを使用するか、新しく開始するかを選択します。

Firewall Management Center のバックアップでは、バックアッププロファイルを使用または作成する必要があります。

- 既存のバックアッププロファイルを使用するには、[バックアッププロファイル（Backup Profiles）] をクリックします。

使用するプロファイルの横にある編集アイコンをクリックします。[バックアップの開始（Start Backup）] をクリックして、今すぐバックアップを開始することができます。プロファイルを編集する場合は、次の手順に進みます。

- [Firepower 管理バックアップ（Firepower Management Backup）] をクリックして新しく開始し、新しいバックアッププロファイルを作成します。

  [名前（Name）] にバックアップファイルの名前を入力します。

ステップ 3 バックアップするものを選択します。

- **設定のバックアップ**。Firewall Management Center の高可用性で、アクティブ Firewall Management Center 上の設定のみのバックアップを選択する場合、デフォルトでは、アクティブとスタンバイの Firewall Management Center の両方が単一の統合バックアップファイルにバックアップされます。高可用性での Firewall Management Center の統合バックアップについては、高可用性の Management Center の統合バックアップを参照してください。
- **イベントのバックアップ**
- **Threat Intelligence Director のバックアップ**

マルチドメイン展開では、設定をバックアップする必要があります。イベントまたは TID データのみをバックアップすることはできません。これらの各選択肢のバックアップ対象および対象外の詳細については、バックアップと復元について （1 ページ）を参照してください。

ステップ 4 Firewall Management Center バックアップファイルの**保存場所**に注意してください。

これは、ローカルストレージ（`/var/sf/backup/`）またはリモート ネットワーク ボリュームのいずれかにすることができます。詳細については、「バックアップとリモートストレージの管理 （38 ページ）」を参照してください。

ステップ 5 （任意）[完了時にコピー（Copy when complete）] を有効にして、完了した Firewall Management Center バックアップをリモートサーバーにコピーします。

ホスト名または IP アドレス、リモートディレクトリへのパス、およびユーザー名とパスワードを入力します。パスワードの代わりに SSH 公開キーを使用するには、[SSH 公開キー（SSH Public Key）] フィールドの内容を、リモートサーバー上の指定ユーザーの `authorized_keys` ファイルにコピーします。

（注）
このオプションは、バックアップをローカルに保存し、リモートの場所にも SCP で保存する場合に便利です。SSH リモートストレージを設定した場合は、[完了時にコピー（Copy when complete）] を使用してバックアップファイルを同じディレクトリにコピーしないでください。

ステップ 6 （任意）[電子メール（Email）] を有効にして、バックアップの完了時に通知する電子メールアドレスを入力します。

電子メール通知を受信するには、メールサーバーに接続するように Firewall Management Center を設定する必要があります（メール リレー ホストおよび通知アドレスの設定）。

ステップ 7 [バックアップの開始（Start Backup）] をクリックしてオンデマンドバックアップを開始します。

既存のバックアッププロファイルを使用しない場合、システムが自動的に作成し、それを使用します。今すぐバックアップを実行しない場合は、[保存（Save）] または [新規として保存（Save As New）] をクリックしてプロファイルを保存することができます。どちらの場合も、新しく作成されたプロファイルを使用して、スケジュールされたバックアップを設定できます。

（注）
リモート ストレージを設定している場合、接続の問題により、リモート ストレージへのバックアップが失敗することがあります。このような場合、ローカル Management Center の空き領域が 30% 以上あれば、生成されたバックアップファイルはローカルに保存され、最も古いローカル Management Center バックアップと置き換えられます。

ステップ 8 デバイスが再起動するまで、Message Center で進行状況をモニターします。

メッセージセンターに、Management Center とそのデバイスの詳細なバックアップステータスが表示されるようになりました。進行中のデバイスバックアップをキャンセルすることもできます。

バックアップデータの収集中に、データの相関付けが一時的に停止してバックアップ関連の設定を変更できなくなることがあります。リモートストレージが設定されている場合または [完了時にコピー（Copy when complete）] が有効になっている場合は、Firewall Management Center が一時ファイルをリモートサーバーに書き込むことがあります。これらのファイルは、バックアッププロセスの最後にクリーンアップされます。

次のタスク

リモートストレージが設定されている場合または [完了時にコピー（Copy when complete）] が有効になっている場合は、バックアップファイルの転送が成功したことを確認します。

Firewall Management Center からのデバイスのバックアップ

オンデマンド バックアップを実行するには、次の手順を実行します。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。 手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （3 ページ）
- バックアップと復元の注意事項と制限事項 （5 ページ）
- バックアップと復元のベストプラクティス （7 ページ）

Firepower 4100/9300 シャーシをバックアップする場合は、FXOS 設定もバックアップすることが特に重要です（FXOS コンフィギュレーション ファイルのエクスポート （17 ページ））。

手順

ステップ 1 [システム（System）]（⚙）>**[ツール（Tools）]**>**[バックアップ/復元（Backup/Restore）]** を選択し、[管理対象デバイスのバックアップ（Managed Device Backup）] をクリックします。

ステップ 2 1 つ以上の**管理対象デバイス**を選択します。

クラスタリングの場合は、クラスタを選択します。個々のノードでバックアップを実行することはできません。

ステップ 3 デバイスバックアップファイルの**保存場所**に注意してください。

これは、ローカルストレージ（`/var/sf/remote-backup/`）またはリモート ネットワーク ボリュームのいずれかにすることができます。ISA 3000 では、SD カードが取り付けられている場合、バックアップのコピーも SD カード（`/mnt/disk3/backup`）に作成されます。詳細については、「バックアップとリモートストレージの管理 （38 ページ）」を参照してください。

ステップ 4 リモートストレージを設定しなかった場合は、Firewall Management Center のローカル ストレージに保存するか、**[管理センターで取得する（Retrieve to Management Center）]** チェックボックスを使用してデバイスに保存するかを選択します。

- 有効（デフォルト）：バックアップが Firewall Management Center の `/var/sf/remote-backup/` に保存されます。

  クラスタの場合は、このオプションが常にオンになります。個別のノードのバックアップファイルは、Firewall Management Center にコピーされ、単一の圧縮 tar ファイルにバンドルされてから、リモートストレージにコピーされます。

- 無効：バックアップがデバイスの `/var/sf/backup` に保存されます。

ステップ 5 [バックアップの開始（Start Backup）] をクリックしてオンデマンドバックアップを開始します。

ステップ 6 デバイスが再起動するまで、Message Center で進行状況をモニターします。

バージョン 7.7.0 以降のデバイスの場合、**[キャンセル（Cancel）]** をクリックして進行中のバックアップをキャンセルできます。

次のタスク

リモートストレージを設定した場合は、バックアップファイルの転送が成功したことを確認します。

FXOS コンフィギュレーション ファイルのエクスポート

エクスポート設定機能を使用して、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含むXMLファイルをリモート サーバまたはローカル コンピュータにエクスポートします。

（注） この手順では、Firewall Threat Defense をバックアップするときに FXOS 設定をエクスポートするための Secure Firewall シャーシマネージャ の使用方法について説明します。CLI の手順については、該当するバージョンの『 Cisco Firepower 4100/9300 FXOS CLI Configuration Guide 』を参照してください。

始める前に

「ガイドラインと制限事項」を確認してください。

手順

ステップ 1 Secure Firewall シャーシマネージャ で **[システム（System）]** > **[設定（Configuration）]** > **[エクスポート（Export）]** の順に選択します。

ステップ 2 コンフィギュレーション ファイルをローカル コンピュータにエクスポートするには、次の手順を実行します。

a) [ローカル（Local）] をクリックします。

b) [エクスポート（Export）] をクリックします。
コンフィギュレーションファイルが作成され、ブラウザによって、ファイルがデフォルトのダウンロード場所に自動的にダウンロードされるか、またはファイルを保存するようプロンプトが表示されます。

ステップ 3 コンフィギュレーション ファイルをリモート サーバにエクスポートするには、次の操作を行います。

a) [リモート（Remote）] をクリックします。

b) リモートサーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。

c) バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。サーバ、ストレージ アレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

IPアドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。

d) デフォルト以外のポートを使用する場合は、[ポート（Port）] フィールドにポート番号を入力します。

e) リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

（注）
パスワードは 64 文字以下にする必要があります。64 文字を超えるパスワードを入力すると、Firewall シャーシ マネージャ にorg-root/cfg-exp-policy-default のプロパティパスワードが範囲外であることを示すエラーが表示されます。

g) [場所（Location）] フィールドに、ファイル名を含む設定ファイルをエクスポートする場所のフル パスを入力します。
h) [エクスポート（Export）] をクリックします。
コンフィギュレーション ファイルが作成され、指定の場所にエクスポートされます。

バックアッププロファイルの作成

バックアッププロファイルとは、保存済みの一連の設定（何をバックアップするか、どこにバックアップファイルを保存するかなど）です。

Firewall Management Center のバックアップにはバックアップ プロファイルが必要です。Firewall Management Center からデバイスをバックアップする場合、バックアップ プロファイルは必要ありません。

Firewall Management Center のオンデマンドバックアップを実行する際に、既存のバックアッププロファイルを選択しなかった場合、システムが自動的に作成し、それを使用します。その後、新しく作成されたプロファイルを使用して、スケジュールされたバックアップを設定できます。

次の手順では、オンデマンドバックアップを実行せずにバックアッププロ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 [システム（System）]（⚙） > **[ツール（Tools）]** > **[バックアップ/復元（Backup/Restore）]** を選択し、[バックアッププロファイル（Backup Profiles）] をクリックします。

ステップ 2 [プロファイルの作成（Create Profile）] をクリックし、[名前（Name）] に名前を入力します。

ステップ 3 バックアップの対象を選択します。

- **バックアップ構成**
- **イベントのバックアップ**
- **Threat Intelligence Director のバックアップ**

マルチドメイン展開では、設定をバックアップする必要があります。イベントまたはTIDデータのみをバックアップすることはできません。これらの各選択肢のバックアップ対象および対象外の詳細については、バックアップと復元について （1 ページ）を参照してください。

ステップ 4 バックアップファイルの**保存場所**に注意してください。

これは、ローカルストレージ（`/var/sf/backup/`）またはリモート ネットワーク ボリュームのいずれかにすることができます。ISA 3000 では、SD カードが取り付けられている場合、バックアップのコピーも SD カード（/mnt/disk3/backup）に作成されます。詳細については、「バックアップとリモートストレージの管理 （38 ページ）」を参照してください。

ステップ 5 （任意）[完了時にコピー（Copy when complete）] を有効にして、完了した Firewall Management Center バックアップをリモートサーバーにコピーします。

ホスト名または IP アドレス、リモートディレクトリへのパス、およびユーザー名とパスワードを入力します。パスワードの代わりに SSH 公開キーを使用するには、[SSH 公開キー（SSH Public Key）] フィールドの内容を、リモートサーバー上の指定ユーザーの `authorized_keys` ファイルにコピーします。

（注）
このオプションは、バックアップをローカルに保存し、リモートの場所にも SCP で保存する場合に便利です。SSHFS リモートストレージを設定した場合は、[完了時にコピー（Copy when complete）] を使用してバックアップファイルを同じディレクトリにコピーしないでください。

ステップ 6 （任意）[電子メール（Email）] を有効にして、バックアップの完了時に通知する電子メールアドレスを入力します。

電子メール通知を受信するには、メールサーバーに接続するように Firewall Management Center を設定する必要があります（メール リレー ホストおよび通知アドレスの設定）。

ステップ 7 [保存（Save）] をクリックします。

Firewall Management Center および管理対象デバイスの復元

Firewall Management Center の場合は、Web インターフェイスを使用してバックアップから復元します。Firewall Threat Defense デバイスの場合、Firewall Threat Defense CLI を使用する必要があります。Firewall Management Center を使用してデバイスを復元することはできません。

ここでは、Firewall Management Center と管理対象デバイスを復元する方法について説明します。

バックアップからの Firewall Management Center の復元

Firewall Management Center のバックアップを復元する場合、バックアップファイルに含まれるコンポーネント（イベント、設定、TIDデータ）の一部またはすべての復元を選択できます。

（注） 設定を復元すると、ごくわずかの例外を除いて、すべての設定が上書きされます。また、Firewall Management Center が再起動されます。イベントおよび TID データを復元すると、侵入イベントを除くすべての既存のイベントおよびTIDデータが上書きされます。準備が整っていることを確認してください。

バックアップから Firewall Management Center を復元するには、次の手順を実行します。Firewall Management Center の HA 展開でのバックアップと復元の詳細については、高可用性ペアでの Firewall Management Center の交換を参照してください。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （3 ページ）
- バックアップと復元の注意事項と制限事項 （5 ページ）
- バックアップと復元のベストプラクティス （7 ページ）

手順

ステップ 1 復元する Firewall Management Center にログインします。

ステップ 2 [システム（System）]（⚙） > **[ツール（Tools）]** > **[バックアップ/復元（Backup/Restore）]** を選択します。

[バックアップ管理（Backup Management）] ページには、ローカルとリモートで保存されたすべてのバックアップファイルが一覧表示されます。バックアップファイルをクリックすると、そのコンテンツが表示されます。

バックアップファイルが一覧になく、ローカルコンピュータに保存している場合は、[バックアップのアップロード（Upload Backup）] をクリックします。バックアップとリモートストレージの管理 （38 ページ）を参照してください。

ステップ 3 復元するバックアップファイルを選択し、[復元（Restore）] をクリックします。

ステップ 4 利用可能コンポーネントから復元するコンポーネントを選択し、もう一度 [復元（Restore）] をクリックして開始します。

ステップ 5 デバイスが再起動するまで、Message Center で進行状況をモニターします。

設定を復元する場合は、Firewall Management Center の再起動後に再度ログインできます。

次のタスク

- 必要に応じて、復元前に元に戻したライセンス設定を再指定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。
- 必要に応じて、リモートストレージと監査ログサーバー証明書の設定を再指定します。これらの設定は、バックアップには含まれていません。
- SRU と VDB を更新します。復元された VDB がシステム VDB と異なる場合、Message Center は復元された VDB のバージョンを示します。復元された SRU または VDB のバージョンが、シスコ サポートおよびダウンロード サイト で利用可能なバージョンよりも古い場合は、デバイスに変更を展開する前に、必ず VDB を最新バージョンに更新してください。
- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

バックアップからの Firewall Threat Defense の復元：Firepower 1000、Cisco Secure Firewall 1200/3100/4200、ISA 3000（非ゼロタッチ）

デバイスのバックアップと復元は、RMA を対象としています。設定を復元すると、管理 IP アドレスを含む、デバイス上のすべての設定が上書きされます。また、デバイスが再起動されます。

この手順では、ハードウェア障害が発生した場合にスタンドアロンまたは高可用性ペアの（またはクラスタとして）Firepower 1000、Cisco Secure Firewall 1200/3100/4200、または ISA 3000 Firewall Threat Defense デバイスを交換する方法の概要を示します。交換するデバイスの正常なバックアップにアクセスできることを前提としています。Firewall Management Center からのデバイスのバックアップ （15 ページ）を参照してください。SD カードを使用した ISA 3000 でのゼロタッチ復元については、バックアップからの Firewall Threat Defense のゼロタッチ復元：ISA 3000 （25 ページ）を参照してください。

高可用性デバイスおよびクラスタ化デバイスの場合は、この手順を使用してすべてのピアを交換できます。すべて交換するには、**restore** CLI コマンド自体を除き、すべてのデバイスですべての手順を同時に実行します。

（注） ネットワークからデバイスを切断する場合でも、Firewall Management Center の登録を解除しないでください。Firewall Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （3 ページ）
- バックアップと復元の注意事項と制限事項 （5 ページ）
- バックアップと復元のベストプラクティス （7 ページ）

手順

ステップ 1 交換用ハードウェアについては、Cisco TAC にお問い合わせください。

同じ数のネットワークモジュールと同じタイプおよび数の物理インターフェイスを備えた同じモデルを入手してください。シスコ返品ポータル から RMA プロセスを開始できます。

ステップ 2 障害のあるデバイスの正常なバックアップを見つけます。

バックアップ設定に応じて、デバイスのバックアップは次の場所に保存されています。

- 障害のあるデバイス自体の `/var/sf/backup`。
- Firewall Management Center の `/var/sf/remote-backup`。
- リモートの保存場所。

Firewall Threat Defense の高可用性デバイスおよびクラスタ化デバイスの場合は、グループを 1 つのユニットとしてバックアップします。高可用性デバイスの場合は、バックアッププロセスによって一意のバックアップファイルが作成され、各デバイスのロールがバックアップファイル名に示されます。クラスタの場合は、制御ノードとデータノードのバックアップファイルが、単一の圧縮ファイルにバンドルされます。ファイルを抽出する必要があります。このファイルにもデバイスのロールが示されます。

バックアップの唯一のコピーが、障害のあるデバイス上にある場合は、ここで別の場所にコピーします。デバイスを再イメージ化すると、バックアップが消去されます。他に問題が発生した場合、バックアップを回復できなくなる可能性があります。詳細については、「バックアップとリモートストレージの管理 （38 ページ）」を参照してください。

交換用デバイスにはバックアップが必要ですが、復元プロセス中に SCP によってバックアップを取得できます。交換用デバイスに SCP でアクセス可能な場所にバックアップを配置しておくことをお勧めします。または、バックアップを交換用デバイス自体にコピーすることができます。

ステップ 3 障害のあるデバイスを取り外します（ラックから取り外します）。

すべてのインターフェイスの接続を切断します。Firewall Threat Defense の高可用性展開では、フェールオーバーリンクが対象に含まれます。クラスタリングの場合、クラスタ制御リンクが対象に含まれます。

ご使用のモデル用のハードウェア設置ガイドとスタートアップガイドを参照してください：http://www.cisco.com/go/ftd-quick。

（注）
ネットワークからデバイスを切断する場合でも、Firewall Management Center の登録を解除しないでください。Firewall Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

ステップ 4 交換用デバイスを取り付け、管理ネットワークに接続します。

デバイスを電源に接続し、管理インターフェイスを管理ネットワークに接続します。Firewall Threat Defense の高可用性展開では、フェールオーバーリンクを接続します。 クラスタリングの場合は、クラスタ制御リンクを接続します。ただし、データインターフェイスは接続しないでください。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

ステップ 5 （任意）交換用の デバイスを再イメージ化します。

RMA シナリオでは、交換用デバイスは、工場出荷時のデフォルト設定で納品されます。交換用デバイスが障害のあるデバイスと同じメジャーバージョンを実行していない場合は、再イメージ化することをお勧めします。

Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。

ステップ 6 交換用デバイスで初期設定を行います。

Firewall Threat Defense CLI に `admin` ユーザーとしてアクセスします。セットアップウィザードでは、管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定を指定するように求められます。

障害のあるデバイスと同じ管理 IP アドレスを設定しないでください。それにより、パッチを適用するためにデバイスを登録する必要がある場合に問題が発生する可能性があります。復元プロセスにより、管理 IP アドレスが正しくリセットされます。

ご使用のモデル用のスタートアップガイドで、初期設定に関するトピックを参照してください：http://www.cisco.com/go/ftd-quick。

（注）
交換用デバイスにパッチを適用する必要がある場合は、スタートアップガイドの説明に従って Firewall Management Center 登録プロセスを開始します。パッチを適用する必要がない場合は、登録しないでください。

ステップ 7 交換用デバイスで、障害のあるデバイスと同じソフトウェアバージョン（パッチを含む）が実行されていることを確認します。

既存のデバイスが Firewall Management Center から削除されていないことを確認します。交換用デバイスは物理ネットワークからは管理できない必要があり、新しいハードウェアおよび交換

する Firewall Threat Defense パッチは同じバージョンである必要があります。Firewall Threat Defense CLI には、upgrade コマンドはありません。パッチを適用するには、次の手順を実行します。

a) Firewall Management Center Web インターフェイスから、デバイス登録プロセスを完了します。

新しい AC ポリシーを作成し、デフォルトアクション「Network Discovery」を使用します。このポリシーはそのままにします。機能や変更を追加しないでください。これは、デバイスを登録して、機能が含まれないポリシーを展開するために使用されています。これにより、ライセンスを要求されなくなり、その後、デバイスにパッチを適用できます。バックアップが復元されると、ライセンスとポリシーが予想どおりの状態に復元されます。

b) デバイスにパッチを適用します：https://www.cisco.com/go/ftd-upgrade。

c) Firewall Management Center から、パッチを適用したばかりのデバイスの登録を解除します。

登録を解除しないと、復元プロセスによって「古い」デバイスが再起動された後で、非実体デバイスが Firewall Management Center に登録されます。

ステップ 8 交換用デバイスがバックアップファイルにアクセスできることを確認します。

復元プロセスでは SCP によってバックアップを取得できるため、バックアップをアクセス可能な場所に配置することをお勧めします。または、交換用デバイス自体（`/var/sf/backup`）にバックアップを手動でコピーすることもできます。クラスタ化されたデバイスの場合は、バックアップバンドルから適切なバックアップファイルを抽出します。

ステップ 9 Firewall Threat Defense CLI から、バックアップを復元します。

Firewall Threat Defense CLI に `admin` ユーザーとしてアクセスします。コンソールを使用するか、新しく設定された管理インターフェイス（IP アドレスまたはホスト名）に SSH で接続することができます。復元プロセスによってこの IP アドレスが変更されることに注意してください。

復元するには、次の手順を実行します。

- SCP を使用：**restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- ローカルデバイスから：**restore remote-manager-backup** *backup tar-file*

Firewall Threat Defense の高可用性とクラスタリングの展開では、適切なバックアップファイル（プライマリとセカンダリ、または制御とデータ）を選択してください。役割は、バックアップファイル名に示されます。すべてのデバイスを復元する場合は、この手順を順番に実行します。再起動を含め、最初のデバイスの復元プロセスが完了するまで、次のデバイスで **restore** コマンドを実行しないでください。

ステップ 10 Firewall Management Center にログインし、交換用デバイスが接続されるまで待ちます。

復元が完了すると、デバイスは、ユーザーを CLI からログアウトさせ、再起動して、自動的に Firewall Management Center に接続します。この時点では、デバイスが期限切れと表示されます。

ステップ 11 展開する前に、復元後のタスクを実行し、復元後の問題を解決します。

- ライセンスの競合や孤立した権限付与を解決します。Cisco TAC にお問い合わせください。
- ハイ アベイラビリティ同期を再開します。Firewall Threat Defense CLI から、`configure high-availability resume` と入力します。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Suspend and Resume High Availability*」を参照してください。

  （注）
  Firewall Threat Defense バージョン 7.2.10 7.6.0 のコマンドを手動で実行する必要はありません。Firewall Threat Defense 高可用性は、バックアップからの復元後に、自動的に回復するからです。

- すべての VPN 証明書を再追加/再登録します。復元プロセスでは、VPN 証明書（バックアップの実行後に追加された証明書を含む）が Firewall Threat Defense デバイスから削除されます。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Managing VPN Certificates*」を参照してください。

ステップ 12 設定を展開します。

この展開は必須です。デバイスを復元したら、[デバイス管理（Device Management）]ページから強制的に展開する必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Redeploy Existing Configurations to a Device*」を参照してください。

ステップ 13 デバイスのデータインターフェイスを接続します。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

次のタスク

復元が成功し、交換用デバイスが予期どおりにトラフィックを通過させていることを確認します。

バックアップからの Firewall Threat Defense のゼロタッチ復元：ISA 3000

デバイスのバックアップと復元は、RMA を対象としています。設定を復元すると、管理 IP アドレスを含む、デバイス上のすべての設定が上書きされます。また、デバイスが再起動されます。

ハードウェア障害が発生した場合のために、この手順で、スタンドアロンまたは HA ペアの ISA 3000 Firewall Threat Defense デバイスを交換する方法の概要を示します。SD カードに障害が発生したユニットのバックアップがあることを前提としています。Firewall Management Center からのデバイスのバックアップ （15 ページ）を参照してください。

高可用性デバイスおよびクラスタ化デバイスの場合は、この手順を使用してすべてのピアを交換できます。すべて交換するには、**restore** CLI コマンド自体を除き、すべてのデバイスですべての手順を同時に実行します。

（注） ネットワークからデバイスを切断する場合でも、Firewall Management Center の登録を解除しないでください。Firewall Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （3 ページ）
- バックアップと復元の注意事項と制限事項 （5 ページ）
- バックアップと復元のベストプラクティス （7 ページ）

手順

ステップ 1 交換用ハードウェアについては、Cisco TAC にお問い合わせください。

同じ数のネットワークモジュールと同じタイプおよび数の物理インターフェイスを備えた同じモデルを入手してください。シスコ返品ポータル から RMA プロセスを開始できます。

ステップ 2 障害のあるデバイスから SD カードを取り外し、デバイスをラックから外します。

すべてのインターフェイスの接続を切断します。Firewall Threat Defense の HA 展開では、フェールオーバーリンクが対象に含まれます。

（注）
ネットワークからデバイスを切断する場合でも、Firewall Management Center の登録を解除しないでください。Firewall Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

ステップ 3 交換用デバイスをラックに再度取り付け、管理ネットワークに接続します。Firewall Threat Defense の HA 展開では、フェールオーバーリンクを接続します。ただし、データインターフェイスは接続しないでください。

デバイスのイメージを再作成するか、ソフトウェアパッチを適用する必要がある場合は、電源コネクタを接続します。

ステップ 4 （任意）交換用のデバイスを再イメージ化します。

RMA シナリオでは、交換用デバイスは、工場出荷時のデフォルト設定で納品されます。交換用デバイスが障害のあるデバイスと同じメジャーバージョンを実行していない場合は、再イ

メージ化する必要があります。https://www.cisco.com/go/isa3000-software からインストーラを取得します。

再イメージ化するには、Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。

ステップ 5 （必要な場合あり）交換用デバイスが、障害のあるデバイスと同じ Cisco Secure Firewall ソフトウェアバージョン（同じパッチバージョンを含む）を実行していることを確認します。デバイスにパッチを適用する必要がある場合は、Secure Firewall Device Manager （Firewall Device Manager）に接続してパッチをインストールできます。

次の手順は、工場出荷時のデフォルト設定を前提としています。デバイスをすでに設定している場合は、Firewall Device Manager にログインし、**[デバイス（Device）]** > **[アップグレード（Upgrades）]** ページに直接移動してパッチをインストールできます。

いずれの場合も、https://www.cisco.com/go/isa3000-software からパッチパッケージを取得します。

a) コンピュータを内部（イーサネット 1/2）インターフェイスに直接接続し、デフォルトの IP アドレス（https://192.168.95.1）で Firewall Device Manager にアクセスします。
b) ユーザー名（admin）とデフォルトのパスワード（Admin123）を入力して、[Login] をクリックします。
c) セットアップ ウィザードを完了します。Firewall Device Manager で設定した内容は保持されないことに注意してください。パッチを適用できるように、初期設定を行うだけなので、セットアップウィザードで入力した内容は関係ありません。
d) **[Device]** > **[Upgrades]** ページに移動します。

   [System Upgrade] セクションに、現在実行中のソフトウェアバージョンが表示されます。

e) [Browse] をクリックして、パッチファイルをアップロードします。
f) [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。

   アイコンの横にある情報は、インストール時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。

   システムに再度ログインできるまで待機します。[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。URL からパスを削除してホームページに再接続してください。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 6 交換用デバイスに SD カードを挿入します。

ステップ 7 デバイスの電源をオンにするか、デバイスを再起動し、ブートアップの開始直後に、[Reset] ボタンを 3 ～ 15 秒間押し続けます。

パッチのインストールに Firewall Device Manager を使用した場合は、**[Device]** > **[System Settings]** > **[Reboot/Shutdown]** ページからリブートできます。Firewall Threat Defense CLI から、**reboot** コマンドを使用します。まだ電源を接続していない場合は、ここで接続します。

ワイヤゲージ 0.033 インチ以下の標準サイズの #1 ペーパークリップを使用して [Reset] ボタンを押します。復元プロセスは、ブートアップ時にトリガーされます。デバイスの設定が復元され、再起動します。その後、デバイスは自動的に Firewall Management Center に登録されます。

HA ペアの両方のデバイスを復元する場合は、この手順を順番に実行します。再起動を含め、最初のデバイスの復元プロセスが完了するまで、2 つ目のデバイス復元しないでください。

ステップ 8 Firewall Management Center にログインし、交換用デバイスが接続されるまで待ちます。

この時点では、デバイスが期限切れと表示されます。

ステップ 9 展開する前に、復元後のタスクを実行し、復元後の問題を解決します。

- ライセンスの競合や孤立した権限付与を解決します。Cisco TAC にお問い合わせください。
- ハイ アベイラビリティ同期を再開します。Firewall Threat Defense CLI から、`configure high-availability resume` と入力します。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Suspend and Resume High Availability*」を参照してください。

  （注）
  Firewall Threat Defense バージョン 7.2.10 7.6.0 のコマンドを手動で実行する必要はありません。Firewall Threat Defense 高可用性は、バックアップからの復元後に、自動的に回復するからです。

- すべての VPN 証明書を再追加/再登録します。復元プロセスでは、VPN 証明書（バックアップの実行後に追加された証明書を含む）が Firewall Threat Defense デバイスから削除されます。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Managing VPN Certificates*」を参照してください。

ステップ 10 設定を展開します。

この展開は必須です。デバイスを復元したら、[デバイス管理（Device Management）]ページから強制的に展開する必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Redeploy Existing Configurations to a Device*」を参照してください。

ステップ 11 デバイスのデータインターフェイスを接続します。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

次のタスク

復元が成功し、交換用デバイスが予期どおりにトラフィックを通過させていることを確認します。

バックアップからの Firewall Threat Defense の復元：Firepower 4100/9300 シャーシ

デバイスのバックアップと復元は、RMA を対象としています。設定を復元すると、管理 IP アドレスを含む、デバイス上のすべての設定が上書きされます。また、デバイスが再起動されます。

この手順では、ハードウェア障害が発生した場合にスタンドアロンまたは高可用性ペアの（またはクラスタとして）Firepower 4100/9300 を交換する方法の概要を示します。次の正常なバックアップにアクセスできることを前提としています。

- 交換する論理デバイス。Firewall Management Center からのデバイスのバックアップ （15 ページ）を参照してください。
- FXOS の設定。FXOS コンフィギュレーション ファイルのエクスポート （17 ページ）を参照してください。

高可用性デバイスおよびクラスタ化デバイスの場合は、この手順を使用してすべてのピアを交換できます。すべて交換するには、**restore** CLI コマンド自体を除き、すべてのデバイスですべての手順を同時に実行します。

（注） ネットワークからデバイスを切断する場合でも、Firewall Management Center の登録を解除しないでください。Firewall Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。 手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （3 ページ）
- バックアップと復元の注意事項と制限事項 （5 ページ）
- バックアップと復元のベストプラクティス （7 ページ）

手順

ステップ 1 交換用ハードウェアについては、Cisco TAC にお問い合わせください。

同じ数のネットワークモジュールと同じタイプおよび数の物理インターフェイスを備えた同じモデルを入手してください。シスコ返品ポータル から RMA プロセスを開始できます。

ステップ 2 障害のあるデバイスの正常なバックアップを見つけます。

バックアップ設定に応じて、デバイスのバックアップは次の場所に保存されています。

- 障害のあるデバイス自体の `/var/sf/backup`。
- Firewall Management Center の `/var/sf/remote-backup`。
- リモートの保存場所。

Firewall Threat Defense の高可用性デバイスおよびクラスタ化デバイスの場合は、グループを 1 つのユニットとしてバックアップします。高可用性デバイスの場合は、バックアッププロセスによって一意のバックアップファイルが作成され、各デバイスのロールがバックアップファイル名に示されます。クラスタの場合は、制御ノードとデータノードのバックアップファイルが、単一の圧縮ファイルにバンドルされます。ファイルを抽出する必要があります。このファイルにもデバイスのロールが示されます。

バックアップの唯一のコピーが、障害のあるデバイス上にある場合は、ここで別の場所にコピーします。デバイスを再イメージ化すると、バックアップが消去されます。他に問題が発生した場合、バックアップを回復できなくなる可能性があります。詳細については、「バックアップとリモートストレージの管理 （38 ページ）」を参照してください。

交換用デバイスにはバックアップが必要ですが、復元プロセス中に SCP によってバックアップを取得できます。交換用デバイスに SCP でアクセス可能な場所にバックアップを配置しておくことをお勧めします。または、バックアップを交換用デバイス自体にコピーすることができます。

ステップ 3 FXOS 設定の正常なバックアップを見つけます。

ステップ 4 障害のあるデバイスを取り外します（ラックから取り外します）。

すべてのインターフェイスの接続を切断します。Firewall Threat Defense の高可用性展開では、フェールオーバーリンクが対象に含まれます。クラスタリングの場合、クラスタ制御リンクが対象に含まれます。

ご使用のモデル用のハードウェア設置ガイドとスタートアップガイドを参照してください：http://www.cisco.com/go/ftd-quick。

（注）
ネットワークからデバイスを切断する場合でも、Firewall Management Center の登録を解除しないでください。Firewall Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

ステップ 5 交換用デバイスを取り付け、管理ネットワークに接続します。

デバイスを電源に接続し、管理インターフェイスを管理ネットワークに接続します。Firewall Threat Defense の高可用性展開では、フェールオーバーリンクを接続します。 クラスタリングの場合は、クラスタ制御リンクを接続します。ただし、データインターフェイスは接続しないでください。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

ステップ 6 （任意）交換用の デバイスを再イメージ化します。

RMA シナリオでは、交換用デバイスは、工場出荷時のデフォルト設定で納品されます。交換用デバイスが障害のあるデバイスと同じメジャーバージョンを実行していない場合は、再イメージ化することをお勧めします。

該当するバージョンの Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager のコンフィギュレーションガイドに記載されている工場出荷時のデフォルト設定の復元に関する説明を参照してください。

ステップ 7 FXOS が互換性のあるバージョンを実行していることを確認します。

論理デバイスを再追加する前に、互換性のある FXOS バージョンを実行している必要があります。Firewall Chassis Manager を使用して、バックアップされた FXOS 設定をインポートできます（コンフィギュレーション ファイルのインポート （33 ページ）を参照）。

ステップ 8 Firewall Chassis Manager を使用して、論理デバイスを追加し、初期設定を行います。

障害のあるシャーシ上の 1 つまたは複数の論理デバイスと同じ管理 IP アドレスを設定しないでください。それにより、パッチを適用するために論理デバイスを登録する必要がある場合に問題が発生する可能性があります。復元プロセスにより、管理 IP アドレスが正しくリセットされます。

お使いのモデルのスタートアップガイドで、Firewall Management Center の展開に関する章を参照してください。http://www.cisco.com/go/ftd-quick

（注）
論理デバイスにパッチを適用する必要がある場合は、スタートアップガイドの説明に従って Firewall Management Center に登録します。パッチを適用する必要がない場合は、登録しないでください。

ステップ 9 交換用デバイスで、障害のあるデバイスと同じソフトウェアバージョン（パッチを含む）が実行されていることを確認します。

既存のデバイスが Firewall Management Center から削除されていないことを確認します。交換用デバイスは物理ネットワークからは管理できない必要があり、新しいハードウェアおよび交換する Firewall Threat Defense パッチは同じバージョンである必要があります。Firewall Threat Defense CLI には、upgrade コマンドはありません。パッチを適用するには、次の手順を実行します。

a) Firewall Management Center Web インターフェイスから、デバイス登録プロセスを完了します。

新しい AC ポリシーを作成し、デフォルトアクション「Network Discovery」を使用します。このポリシーはそのままにします。機能や変更を追加しないでください。これは、デバイスを登録して、機能が含まれないポリシーを展開するために使用されています。これにより、ライセンスを要求されなくなり、その後、デバイスにパッチを適用できます。バックアップが復元されると、ライセンスとポリシーが予想どおりの状態に復元されます。

b) デバイスにパッチを適用します：https://www.cisco.com/go/ftd-upgrade。
c) Firewall Management Center から、パッチを適用したばかりのデバイスの登録を解除します。

登録を解除しないと、復元プロセスによって「古い」デバイスが再起動された後で、非実体デバイスが Firewall Management Center に登録されます。

ステップ 10 交換用デバイスがバックアップファイルにアクセスできることを確認します。

復元プロセスでは SCP によってバックアップを取得できるため、バックアップをアクセス可能な場所に配置することをお勧めします。または、交換用デバイス自体（`/var/sf/backup`）にバックアップを手動でコピーすることもできます。クラスタ化されたデバイスの場合は、バックアップバンドルから適切なバックアップファイルを抽出します。

ステップ 11 Firewall Threat Defense CLI から、バックアップを復元します。

Firewall Threat Defense CLI に `admin` ユーザーとしてアクセスします。コンソールを使用するか、新しく設定された管理インターフェイス（IP アドレスまたはホスト名）に SSH で接続することができます。復元プロセスによってこの IP アドレスが変更されることに注意してください。

復元するには、次の手順を実行します。

- SCP を使用：**restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- ローカルデバイスから：**restore remote-manager-backup** *backup tar-file*

Firewall Threat Defense の高可用性とクラスタリングの展開では、適切なバックアップファイル（プライマリとセカンダリ、または制御とデータ）を選択してください。役割は、バックアップファイル名に示されます。すべてのデバイスを復元する場合は、この手順を順番に実行します。再起動を含め、最初のデバイスの復元プロセスが完了するまで、次のデバイスで **restore** コマンドを実行しないでください。

ステップ 12 Firewall Management Center にログインし、交換用デバイスが接続されるまで待ちます。

復元が完了すると、デバイスは、ユーザーを CLI からログアウトさせ、再起動して、自動的に Firewall Management Center に接続します。この時点では、デバイスが期限切れと表示されます。

ステップ 13 展開する前に、復元後のタスクを実行し、復元後の問題を解決します。

- ライセンスの競合や孤立した権限付与を解決します。サポートの詳細については、Cisco TAC までお問い合わせください。
- すべての VPN 証明書を再追加/再登録します。復元プロセスでは、VPN 証明書（バックアップの実行後に追加された証明書を含む）が Firewall Threat Defense デバイスから削除されます。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Managing VPN Certificates*」を参照してください。

ステップ 14 設定を展開します。

この展開は必須です。デバイスを復元したら、[デバイス管理（Device Management）]ページから強制的に展開する必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Redeploy Existing Configurations to a Device*」を参照してください。

ステップ 15 デバイスのデータインターフェイスを接続します。

ご使用のモデル用のハードウェア設置ガイドを参照してください：http://www.cisco.com/go/ftd-quick。

次のタスク

復元が成功し、交換用デバイスが予期どおりにトラフィックを通過させていることを確認します。

コンフィギュレーション ファイルのインポート

設定のインポート機能を使用して、Firepower 4100/9300 シャーシからエクスポートした構成設定を適用できます。この機能を使用して、既知の良好な構成に戻したり、システム障害を解決したりできます。

（注） この手順では、ソフトウェアを復元する前に、Firewall シャーシ マネージャ を使用して FXOS の設定をインポートする方法について説明します。CLI の手順については、該当するバージョンの『 Cisco Firepower 4100/9300 FXOS CLI Configuration Guide 』を参照してください。

始める前に

「ガイドラインと制限事項」を確認してください。

手順

ステップ 1 で、Firewall シャーシ マネージャ**[システム（System）]** > **[ツール（Tools）]** > **[インポート/エクスポート（Import/Export）]** を選択します。

ステップ 2 ローカルのコンフィギュレーション ファイルからインポートする場合は、次の操作を行います。

a) [ローカル（Local）] をクリックします。

b) [ファイルの選択（Choose File）] をクリックし、インポートするコンフィギュレーション ファイルを選択します。

c) [インポート（Import）] をクリックします。
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。

d) [はい（Yes）] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

ステップ 3 リモート サーバからコンフィギュレーション ファイルをインポートする場合は、次の操作を行います。

a) [リモート（Remote）] をクリックします。
b) リモート サーバとの通信で使用するプロトコルを選択します。選択できるプロトコルは、FTP、TFTP、SCP、または SFTP のいずれかです。
c) デフォルト以外のポートを使用する場合は、[ポート（Port）] フィールドにポート番号を入力します。
d) バックアップ ファイルが格納されている場所のホスト名または IP アドレスを入力します。サーバ、ストレージ アレイ、ローカル ドライブ、または Firepower 4100/9300 シャーシがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。

IP アドレスではなくホスト名を使用する場合は、DNS サーバを設定する必要があります。

e) リモート サーバにログインするためのユーザ名を入力します。プロトコルが TFTP の場合、このフィールドは適用されません。
f) リモート サーバのユーザ名のパスワードを入力します。プロトコルが TFTP の場合、このフィールドは適用されません。

（注）
パスワードは 64 文字以下にする必要があります。64 文字を超えるパスワードを入力すると、Firewall シャーシ マネージャ に`org-root/cfg-exp-policy-default` のプロパティパスワードが範囲外であることを示すエラーが表示されます。

g) [ファイルパス（File Path）] フィールドに、コンフィギュレーション ファイルのフルパスをファイル名を含めて入力します。
h) [インポート（Import）] をクリックします。
操作の続行を確認するダイアログボックスが開き、シャーシの再起動についての警告が表示されます。
i) [はい（Yes）] をクリックして、指定したコンフィギュレーション ファイルをインポートします。
既存の設定が削除され、インポートしたファイルの設定が Firepower 4100/9300 シャーシに適用されます。インポート中にブレークアウト ポートの設定が変更された場合は、Firepower 4100/9300 シャーシの再起動が必要になります。

バックアップからの Firewall Threat Defense Virtual の復元

問題または障害がある Firewall Threat Defense Virtual デバイスを交換するには、この手順を使用します。

高可用性デバイスおよびクラスタ化デバイスの場合は、この手順を使用してすべてのピアを交換できます。すべて交換するには、**restore** CLI コマンド自体を除き、すべてのデバイスですべての手順を同時に実行します。

（注） ネットワークからデバイスを切断する場合でも、Firewall Management Center の登録を解除しないでください。Firewall Threat Defense の高可用性デバイスまたはクラスタ化デバイスの場合は、高可用性またはクラスタリングを中断または解除しないでください。これらのリンクを維持することで、交換用デバイスを、復元後に自動的に再接続できます。

始める前に

要件、ガイドライン、制限事項、およびベストプラクティスを確認し、理解する必要があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。

- バックアップと復元の要件 （3 ページ）
- バックアップと復元の注意事項と制限事項 （5 ページ）
- バックアップと復元のベストプラクティス （7 ページ）

手順

ステップ 1 障害のあるデバイスの正常なバックアップを見つけます。

バックアップ設定に応じて、デバイスのバックアップは次の場所に保存されています。

- 障害のあるデバイス自体の `/var/sf/backup`。
- Firewall Management Center の `/var/sf/remote-backup`。
- リモートの保存場所。

Firewall Threat Defense の高可用性デバイスおよびクラスタ化デバイスの場合は、グループを 1 つのユニットとしてバックアップします。高可用性デバイスの場合は、バックアッププロセスによって一意のバックアップファイルが作成され、各デバイスのロールがバックアップファイル名に示されます。クラスタの場合は、制御ノードとデータノードのバックアップファイルが、単一の圧縮ファイルにバンドルされます。ファイルを抽出する必要があります。このファイルにもデバイスのロールが示されます。

バックアップの唯一のコピーが、障害のあるデバイス上にある場合は、ここで別の場所にコピーします。デバイスを再イメージ化すると、バックアップが消去されます。他に問題が発生した場合、バックアップを回復できなくなる可能性があります。詳細については、「バックアップとリモートストレージの管理 （38 ページ）」を参照してください。

交換用デバイスにはバックアップが必要ですが、復元プロセス中に SCP によってバックアップを取得できます。交換用デバイスに SCP でアクセス可能な場所にバックアップを配置しておくことをお勧めします。または、バックアップを交換用デバイス自体にコピーすることができます。

ステップ 2 障害のあるデバイスを取り外します。

仮想マシンをシャットダウンして電源を切り、削除します。手順については、ご使用の仮想環境のマニュアルを参照してください。

ステップ 3 交換用デバイスを展開します。

https://www.cisco.com/go/ftdv-quickを参照してください。

ステップ 4 交換用デバイスで初期設定を行います。

コンソールを使用して、Firewall Threat Defense CLI に `admin` ユーザーとしてアクセスします。セットアップウィザードでは、管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定を指定するように求められます。

障害のあるデバイスと同じ管理 IP アドレスを設定しないでください。それにより、パッチを適用するためにデバイスを登録する必要がある場合に問題が発生する可能性があります。復元プロセスにより、管理 IP アドレスが正しくリセットされます。

スタートアップガイドで、CLI のセットアップに関するトピックを参照してください：https://www.cisco.com/go/ftdv-quick。

（注）
交換用デバイスにパッチを適用する必要がある場合は、スタートアップガイドの説明に従って Firewall Management Center 登録プロセスを開始します。パッチを適用する必要がない場合は、登録しないでください。

ステップ 5 交換用デバイスで、障害のあるデバイスと同じソフトウェアバージョン（パッチを含む）が実行されていることを確認します。

既存のデバイスが Firewall Management Center から削除されていないことを確認します。交換用デバイスは物理ネットワークからは管理できない必要があり、新しいハードウェアおよび交換する Firewall Threat Defense パッチは同じバージョンである必要があります。Firewall Threat Defense CLI には、upgrade コマンドはありません。パッチを適用するには、次の手順を実行します。

a) Firewall Management Center Web インターフェイスから、デバイス登録プロセスを完了します。

新しい AC ポリシーを作成し、デフォルトアクション「Network Discovery」を使用します。このポリシーはそのままにします。機能や変更を追加しないでください。これは、デバイスを登録して、機能が含まれないポリシーを展開するために使用されています。これによ

り、ライセンスを要求されなくなり、その後、デバイスにパッチを適用できます。バックアップが復元されると、ライセンスとポリシーが予想どおりの状態に復元されます。

b) デバイスにパッチを適用します：https://www.cisco.com/go/ftd-upgrade。

c) Firewall Management Centerから、パッチを適用したばかりのデバイスの登録を解除します。

登録を解除しないと、復元プロセスによって「古い」デバイスが再起動された後で、非実体デバイスが Firewall Management Center に登録されます。

ステップ 6 交換用デバイスがバックアップファイルにアクセスできることを確認します。

復元プロセスでは SCP によってバックアップを取得できるため、バックアップをアクセス可能な場所に配置することをお勧めします。または、交換用デバイス自体（`/var/sf/backup`）にバックアップを手動でコピーすることもできます。クラスタ化されたデバイスの場合は、バックアップバンドルから適切なバックアップファイルを抽出します。

ステップ 7 Firewall Threat Defense CLI から、バックアップを復元します。

Firewall Threat Defense CLI に `admin` ユーザーとしてアクセスします。コンソールを使用するか、新しく設定された管理インターフェイス（IP アドレスまたはホスト名）に SSH で接続することができます。復元プロセスによってこのIPアドレスが変更されることに注意してください。

復元するには、次の手順を実行します。

- SCP を使用：**restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- ローカルデバイスから：**restore remote-manager-backup** *backup tar-file*

Firewall Threat Defense の高可用性とクラスタリングの展開では、適切なバックアップファイル（プライマリとセカンダリ、または制御とデータ）を選択してください。役割は、バックアップファイル名に示されます。すべてのデバイスを復元する場合は、この手順を順番に実行します。再起動を含め、最初のデバイスの復元プロセスが完了するまで、次のデバイスで **restore** コマンドを実行しないでください。

ステップ 8 Firewall Management Center にログインし、交換用デバイスが接続されるまで待ちます。

復元が完了すると、デバイスは、ユーザーをCLIからログアウトさせ、再起動して、自動的に Firewall Management Center に接続します。この時点では、デバイスが期限切れと表示されます。

ステップ 9 展開する前に、復元後のタスクを実行し、復元後の問題を解決します。

- ライセンスの競合や孤立した権限付与を解決します。サポートの詳細については、Cisco TAC までお問い合わせください。
- すべての VPN 証明書を再追加/再登録します。復元プロセスでは、VPN 証明書（バックアップの実行後に追加された証明書を含む）がFirewall Threat Defenseデバイスから削除されます。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Managing VPN Certificates*」を参照してください。

ステップ 10 設定を展開します。

この展開は必須です。デバイスを復元したら、[デバイス管理（Device Management）]ページから強制的に展開する必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「*Redeploy Existing Configurations to a Device*」を参照してください。

ステップ 11 データインターフェイスを追加して設定します。

スタートアップガイドを参照してください：https://www.cisco.com/go/ftdv-quick。

次のタスク

復元が成功し、交換用デバイスが予期どおりにトラフィックを通過させていることを確認します。

バックアップとリモートストレージの管理

バックアップは、暗号化されていないアーカイブ（.tar）ファイルとして保存されます。ファイル名には、次のような識別情報が含まれる場合があります。

- バックアップに関連付けられているバックアッププロファイルまたはスケジュールタスクの名前。
- バックアップされたアプライアンスの表示名または IP アドレス。
- アプライアンスのロール（HA ペアのメンバーなど）。

アプライアンスを安全なリモートロケーションにバックアップし、転送が成功することを確認することをお勧めします。アプライアンスに残っているバックアップは、手動またはアップグレードプロセスによって削除できます。アップグレードすると、ローカルに保存されたバックアップは削除されます。オプションの詳細については、バックアップ保存場所 （40 ページ）を参照してください。

注意 特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。Admin/Maint ロールを持つユーザーは [バックアップ管理（Backup Management）] ページにアクセスでき、そこでリモートストレージからファイルを移動および削除できることに注意してください。

次の手順では、バックアップファイルを管理する方法について説明します。

手順

ステップ 1 [システム（System）]（⚙）>**[ツール（Tools）]**>**[バックアップ/復元（Backup/Restore）]**を選択します。

[バックアップ管理（Backup Management）]ページには、使用可能なバックアップが一覧表示されます。また、バックアップの保存に使用できるディスク容量も一覧表示されます。十分な容量がない場合、バックアップが失敗する可能性があります。

ステップ 2 次のいずれかを実行します。

表 *3:* リモートストレージとバックアップファイルの管理

目的	操作手順
Firewall Management Center のシステム設定を編集せずに、バックアップのリモートストレージを有効または無効にします。	[バックアップのリモートストレージを有効にする（Enable Remote Storage for Backups）] をクリックします。 このオプションは、リモートストレージを設定した後にのみ表示されます。ここで切り替えると、システム設定（[システム（System）]>[設定（Configuration）]>[リモートストレージデバイス（Remote Storage Device）]）でも切り替わります。 **ヒント** リモートストレージ設定にすばやくアクセスするには、[バックアップ管理（Backup Management）] ページの右上にある [リモートストレージ（Remote Storage）] をクリックします。 **（注）** バックアップをリモート ストレージ ロケーションに保存するには、[Management Centerに取得（Retrieve to Management Center）] オプションを有効にする必要があります（Firewall Management Center からのデバイスのバックアップ （15 ページ） を参照）。
Firewall Management Center とリモートの保存場所の間でファイルを移動します。	[移動（Move）] をクリックします。 ファイルは、必要に応じて何度でも移動したり戻したりすることができます。これにより、現在の場所では、ファイルがコピーされずに削除されます。 バックアップファイルをリモートストレージから Firewall Management Center に移動する場合、Firewall Management Center での保存場所は、バックアップの種類によって異なります。 • Firewall Management Center のバックアップ：`/var/sf/backup` • デバイスのバックアップ：`/var/sf/remote-backup`

目的	操作手順
バックアップの内容を表示します。	バックアップファイルをクリックします。
バックアップファイルを削除します。	バックアップファイルを選択し、[削除（Delete）] をクリックします。 ローカル保存とリモート保存のどちらのバックアップファイルも削除できます。
ご使用のコンピュータからバックアップファイルをアップロードします。	[バックアップのアップロード（Upload Backup）] をクリックし、バックアップファイルを選択して、もう一度[バックアップのアップロード（Upload Backup）] をクリックします。
ご使用のコンピュータにバックアップをダウンロードします。	バックアップファイルを選択し、[ダウンロードして（Download）] をクリックします。 バックアップファイルの移動とは異なり、バックアップは Firewall Management Center から削除されません。ダウンロードしたバックアップを安全な場所に保存します。

バックアップ保存場所

次の表に、Firewall Management Center および管理対象デバイスのバックアップ ストレージ オプションを示します。

表 *4*:バックアップ保存場所

参照先	詳細
リモート。ネットワークボリューム（NFS、SMB、SSHFS）をマウントします。	（注） リモートストレージを構成し、[Management Centerに取得（Retrieve to Management Center）] オプションを有効にした場合にのみ、バックアップはリモート ストレージ ロケーションに保存されます（Firewall Management Center からのデバイスのバックアップ （15 ページ） を参照）。 Firewall Management Center のシステム設定では、NFS、SMB、または SSHFS ネットワークボリュームを Firewall Management Center およびデバイスバックアップのリモートストレージとしてマウントできます。リモート ストレージ デバイス を参照してください。） これを実行すると、その後のすべての Firewall Management Center バックアップと *Firewall Management Center* が開始するデバイスバックアップがそのボリュームにコピーされますが、引き続き Firewall Management Center を使用してそれらを管理（復元、ダウンロード、アップロード、削除、移動）することができます。 Firewall Management Center だけがネットワークボリュームをマウントすることに注意してください。管理対象デバイスのバックアップファイルは、Firewall Management Center を介してルーティングされます。Firewall Management Center とそのデバイスの間に大容量のデータを転送するための帯域幅があることを確認します。詳細については、『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

参照先	詳細
リモート。コピー（SCP）します。	（注） リモートストレージを構成し、[Management Centerに取得（Retrieve to Management Center）] オプションを有効にした場合にのみ、バックアップはリモート ストレージ ロケーションに保存されます（Firewall Management Center からのデバイスのバックアップ （15 ページ） を参照）。 Firewall Management Center の場合は、[完了時にコピー（Copy when complete）] オプションを使用して、完了したバックアップをリモートサーバーに安全にコピー（SCP）できます。 ネットワークボリュームをマウントすることによるリモートストレージとは異なり、[完了時にコピー（Copy when complete）] では NFS または SMB ボリュームにコピーすることはできません。CLI オプションを指定したり、ディスク容量のしきい値を設定することもできません。また、レポートのリモートストレージに影響を与えることはありません。さらに、コピーされたバックアップファイルを管理できません。 このオプションは、バックアップをローカルに保存するとともに、リモートの場所への SCP を実行する場合に便利です。 （注） Firewall Management Center のシステム設定で SSHFS リモートストレージを設定する場合は、[完了時にコピー（Copy when complete）] を使用してバックアップファイルを同じディレクトリにコピーしないでください。
ローカル、Firewall Management Center	ネットワークボリュームをマウントすることによってリモートストレージを設定しない場合は、Firewall Management Center にバックアップファイルを保存できます。 • Firewall Management Center のバックアップは `/var/sf/backup` に保存されます。 • バックアップの実行時に [管理センターで取得する（Retrieve to Management Center）] オプションを有効にすると、デバイスのバックアップは Firewall Management Center 上の `/var/sf/remote-backup` に保存されます。

参照先	詳細
ローカル（デバイスの内部フラッシュメモリ上）。	次の場合、デバイスのバックアップファイルはデバイス上の /var/sf/backup に保存されます。 • ネットワークボリュームをマウントすることによってリモートストレージを設定しない。 • [管理センターで取得する（Retrieve to Management Center）] を有効にしない。
ローカル（デバイスのSDカード上）。	ISA 3000 の場合、デバイスをローカルの内部フラッシュメモリの場所（/var/sf/backup）にバックアップするときに、SD カードを取り付けていると、バックアップはゼロタッチ復元で使用するために SD カード（/mnt/disk3/backup/）に自動的にコピーされます。

バックアップと復元の履歴

表 *5:* バックアップと復元の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
廃止：Cisco AMP クラウド接続のバックアップ。	7.7.0 7.6.1 7.2.10 7.0.7	任意（Any）	パブリックおよびプライベート AMP クラウド接続はバックアップされなくなりました。それらは、復元後に再設定する必要があります。
廃止：Management Center にローカルに保存されたレポートのバックアップ。	7.6.0	任意（Any）	ローカルに保存されたレポートはバックアップされなくなりました。レポートは、安全なリモートロケーションに保存する必要があります。
高可用性 Firewall Management Center 用の単一のバックアップファイル。	7.4.1 7.2.6	任意（Any）	高可用性ペアのアクティブ Firewall Management Center の設定だけのバックアップを実行すると、いずれかのユニットの復元に使用できる単一のバックアップファイルが作成されるようになりました。 バージョンの制限：Firewall Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
デバイスクラスタのバックアップと復元。	7.3.0	いずれか	Firewall Management Center を使用してデバイス クラスタをバックアップできるようになりました。ただし、パブリック クラウドではバックアップできません。復元するには、デバイス CLI を使用します。 新規/変更された画面：**[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [管理対象デバイスのバックアップ（Managed Device Backup）]** 新規/変更されたコマンド： **restore remote-manager-backup**
SD カードを使用した ISA 3000 でのゼロタッチ復元。	7.0.0	7.0.0	ローカルバックアップを実行すると、バックアップファイルが SD カードにコピーされます（カードがある場合）。交換用デバイスの設定を復元するには、新しいデバイスに SD カードを取り付け、デバイスの起動中に [リセット（Reset）] ボタンを 3 ー 15 秒間押します。
FTD コンテナインスタンスのバックアップと復元。	6.7.0	6.7.0	FMC を使用して、Firepower 4100/9300 で FTD コンテナインスタンスのオンデマンド リモート バックアップを実行できるようになりました。
復元するために VDB を一致させる必要がなくなりました。	6.6.0	任意（Any）	バックアップから FMC を復元すると、既存の VDB がバックアップファイル内の VDB に置き換えられます。復元する前に VDB バージョンを一致させる必要がなくなりました。
自動スケジュール済みバックアップ。	6.5.0	いずれか	新規または再イメージ化された FMC の場合、セットアッププロセスにより、FMC の設定をバックアップしてローカルに保存する、週次のスケジュール済みタスクが作成されます。
管理対象デバイスのオンデマンドでのリモートバックアップ。	6.3.0	6.3.0	FMC を使用して、特定の管理対象デバイスのリモート バックアップをオンデマンドで実行できるようになりました。 サポートされるプラットフォームについては、バックアップと復元の要件 （3 ページ）を参照してください。 新規/変更された画面：**[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）] > [管理対象デバイスのバックアップ（Managed Device Backup）]** 新規/変更された FTD CLI コマンド： **restore**

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。