



Firepower Management Center ハイアベイラビリティ

以下のトピックでは、Cisco Firepower Management Center のアクティブ/スタンバイ ハイアベイラビリティを設定する方法を示します。

- [Firepower Management Center のハイアベイラビリティについて \(1 ページ\)](#)
- [Firepower Management Center の高可用性の設定 \(8 ページ\)](#)
- [Firepower Management Center ハイアベイラビリティ ステータスの表示 \(10 ページ\)](#)
- [Firepower Management Center ハイアベイラビリティ ペアで同期される設定 \(11 ページ\)](#)
- [Firepower Management Center のハイアベイラビリティにおけるデバイス登録を解決するための CLI の使用 \(12 ページ\)](#)
- [Firepower Management Center ハイアベイラビリティ ペアにおけるピアの切り替え \(12 ページ\)](#)
- [Firepower Management Center ペア間の通信の一時停止 \(13 ページ\)](#)
- [Firepower Management Center ペア間の通信の再開 \(14 ページ\)](#)
- [高可用性ペアの Firepower Management Center の IP アドレスの変更 \(14 ページ\)](#)
- [ハイアベイラビリティ ペアでの Firepower Management Center のアップグレード \(15 ページ\)](#)
- [Firepower Management Center ハイアベイラビリティの無効化 \(16 ページ\)](#)

Firepower Management Center のハイアベイラビリティについて

運用の継続性を確保するために、ハイアベイラビリティ機能を使用して、冗長 Firepower Management Center でデバイスを管理するように指定することができます。Firepower Management Center では、1つのアプライアンスがアクティブユニットであり、デバイスを管理する、アクティブ/スタンバイハイアベイラビリティがサポートされます。スタンバイユニットは、アクティブにデバイスを管理しません。アクティブユニットは、データストアに設定データを書き込み、両方のユニットのデータを複製し、必要な場合は同期を使用してスタンバイユニットと一部の情報を共有します。

アクティブ/スタンバイ ハイ アベイラビリティでは、プライマリ Firepower Management Center に障害が発生した場合、セカンダリ Firepower Management Center を設定して、プライマリの機能を引き継ぐことができます。プライマリ Firepower Management Center に障害が発生した場合は、セカンダリ Firepower Management Center をプロモートしてアクティブユニットにする必要があります。

イベント データは、管理対象デバイスからハイ アベイラビリティ ペアの両方の Firepower Management Center に配信されます。一方の Firepower Management Center で障害が発生した場合、他方の Firepower Management Center の使用を中断せずにネットワークをモニタすることができます。

ハイ アベイラビリティ ペアとして設定する 2 つの Firepower Management Center は、信頼された同じ管理ネットワーク上に存在する必要も、同じ地理的ロケーションに存在する必要もありません。



注意 システムでは一部の機能をアクティブ Firepower Management Center に制限しているため、そのアプライアンスで障害が発生した場合は、スタンバイ Firepower Management Center をアクティブにプロモートする必要があります。

Firepower Management Center のシステム要件

この項では、ハイアベイラビリティ設定にある Firepower Management Center のハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

- 2 つの Firepower Management Center の間にハイ アベイラビリティ構成を設定するには、それらの間に少なくとも 5 MBPS のネットワーク帯域幅が必要です。
- ハイアベイラビリティ設定の 2 台の Firepower Management Center は、モデルが同じである必要があります。
- プライマリ Firepower Management Center バックアップをセカンダリ Firepower Management Center に復元することはできません。

ソフトウェア要件

ハイアベイラビリティ設定の 2 台の Firepower Management Center には、同じメジャー（最初の番号）、マイナー（2 番めの番号）、メンテナンス（3 番めの番号）バージョンのソフトウェアがインストールされている必要があります。

ライセンス要件

ハイアベイラビリティ構成の Firepower Management Center で管理されるデバイスには、単一の Firepower Management Center で管理されるデバイスと同じ数の機能ライセンスと関連するサブスクリプションが必要です。

たとえば、Firepower Management Center ペアで管理されている 2 つの デバイスに対して高度なマルウェア防御を有効にしたい場合は、2 つのマルウェア ライセンスと 2 つの TAM サブスクリプションを購入し、それらのライセンスを Firepower Management Center に追加してから、ライセンスをアクティブ Firepower Management Center 上の 2 つの デバイスに割り当てます。システムは、すべての機能ライセンスをアクティブからスタンバイ Firepower Management Center に自動的に複製するため、ライセンスをフェールオーバー時に使用できます。

また、Firepower Management Center ペアで管理されている 2 つの Firepower Threat Defense デバイスに対して高度なマルウェア防御を有効にしたい場合は、2 つのマルウェア ライセンスと 2 つの TM サブスクリプションを購入し、アクティブ Firepower Management Center を Cisco Smart Software Manager に登録してから、ライセンスをアクティブ Firepower Management Center 上の 2 つの Firepower Threat Defense デバイスに割り当てます。フェールオーバーが行われると、システムは Smart Software Manager と通信して、スマートライセンスの権利をアクティブ Firepower Management Center から解放し、スタンバイ Firepower Management Center に割り当てます。

高可用性 Firepower Management Center での役割とステータス

プライマリ/セカンダリの役割

Firepower Management Center を高可用性ペアの形でセットアップする際は、一方の Firepower Management Center をプライマリとして設定し、もう一方をセカンダリとして設定します。設定中に、プライマリ ユニットのポリシーは、セカンダリ ユニットの同期されます。この同期が完了すると、プライマリ Firepower Management Center がアクティブピアになり、セカンダリ Firepower Management Center がスタンバイピアになって、2 つのユニットが管理対象デバイスおよびポリシー設定に対して単一のアプライアンスとして機能します。

アクティブ/スタンバイ ステータス

高可用性ペアを構成する 2 つの Firepower Management Center の間の主な違いは、どちらがアクティブピアで、どちらがスタンバイピアであるかという点です。アクティブ Firepower Management Center は、完全に機能する状態に維持され、デバイスとポリシーを管理するために使用できます。スタンバイ Firepower Management Center では機能が非表示になるため、設定の変更を行うことはできません。

Firepower Management Center ハイ アベイラビリティ ペアのデバイス登録

高可用性を確立する前に、すべての管理対象デバイスを目的のアクティブ Firepower Management Center に登録する必要があります。これには、目的のセカンダリからデバイスを削除し、それらを目的のプライマリに登録することが含まれます。

また、高可用性を確立する前に、目的のセカンダリでポリシーをエクスポートする必要があります。セカンダリとして使用するアプライアンスがどれであっても、デバイス登録とポリシー設定のすべてが失われます。

高可用性が確立されると、アクティブ Firepower Management Center に登録されたデバイスが自動的にスタンバイ Firepower Management Center に登録されます。

登録済みのデバイスに NAT IP アドレスが割り当てられている場合、デバイスの自動登録は失敗し、セカンダリ Firepower Management Center の [ハイ アベイラビリティ (High Availability)] ページには、そのデバイスがローカルで保留中であると表示されます。次に、スタンバイ Firepower Management Center の [ハイ アベイラビリティ (High Availability)] ページで、異なる NAT IP アドレスをデバイスに割り当てることができます。

自動登録がスタンバイ Firepower Management Center で失敗しても、デバイスがアクティブな Firepower Management Center に登録されているように見える場合は、[Firepower Management Center のハイ アベイラビリティにおけるデバイス登録を解決するための CLI の使用 \(12 ページ\)](#) を参照してください。

Firepower Management Center のハイ アベイラビリティ ペアでのイベント処理

ハイ アベイラビリティ ペアの両方の Firepower Management Center が管理対象デバイスからイベントを受信するため、アプライアンスの管理 IP アドレスは共有されません。これは Firepower Management Center で障害が発生した場合に、継続的な処理を確保するために介入する必要がないことを意味します。

AMP クラウド接続とマルウェア情報

ハイ アベイラビリティ ペアを構成する Firepower Management Center は、ファイル ポリシーおよび関連する設定は共有しますが、シスコ AMP クラウド接続およびマルウェア処理は共有しません。運用の継続性を確保し、検出されたファイルのマルウェア処理が両方の Firepower Management Center で同じであるようにするためには、プライマリとセカンダリ両方の Firepower Management Center が AMP クラウドにアクセスできる必要があります。

URL フィルタリングとセキュリティ インテリジェンス

URL フィルタリングとセキュリティ インテリジェンスの設定および情報は、ハイ アベイラビリティ展開の Firepower Management Center の間で同期されます。ただし、プライマリ Firepower Management Center だけが、セキュリティ インテリジェンス フィードの更新用の URL カテゴリおよびレピュテーションデータをダウンロードします。

プライマリ Firepower Management Center に障害が発生した場合は、セカンダリ Firepower Management Center がインターネットにアクセスして脅威インテリジェンスを更新できることを確認する必要があるだけでなく、セカンダリ Firepower Management Center の Web インターフェイスを使用してセカンダリをアクティブにプロモートする必要もあります。

Firepower Management Center のフェールオーバー中のユーザ データの処理

プライマリ Firepower Management Center で障害が発生した場合、ユーザ エージェント、ISE、TS エージェント、またはキャプティブ ポータル デバイスから報告されるすべてのログインは、それらのユーザが前に確認されて Firepower Management Center にダウンロードされていた場合でも、フェールオーバーのダウンタイム中に識別することはできません。識別されていないユーザは、Firepower Management Center で [不明 (Unknown)] のユーザとして記録されます。

ダウンタイム後、不明のユーザはアイデンティティ ポリシーのルールに従って再確認され、処理されます。

Firepower Management Center ハイ アベイラビリティ ペアの構成管理

ハイ アベイラビリティ 展開では、アクティブな Firepower Management Center のみがデバイスを管理し、ポリシーを適用できます。両方の Firepower Management Center は継続的な同期状態を保ちます。

アクティブ状態の Firepower Management Center に障害が発生すると、ハイ アベイラビリティ ペアは縮退状態となります。縮退状態は、スタンバイ状態のアプライアンスを手動でアクティブ状態に上げるまで続きます。スタンバイ状態のアプライアンスをアクティブ状態に上げると、両アプライアンスのメンテナンス モードが終了します。

バックアップ中の Firepower Management Center の高可用性動作

Firepower Management Center 高可用性ペアでバックアップを実行する場合、バックアップ動作によってピア間の同期が一時停止します。この動作中は、引き続きアクティブな Firepower Management Center を使用できますが、スタンバイ ピアを使用することはできません。

バックアップが完了すると、同期が再開され、少しの間、アクティブピアでのプロセスが無効になります。この一時停止中、[高可用性 (High Availability)] ページには、すべてのプロセスが再開されるまでは一時的に保留ページが表示されます。

Firepower Management Center ハイ アベイラビリティのスプリットブレイン

高可用性ペアのアクティブな Firepower Management Center が（電源の問題、ネットワークや接続の問題で）ダウンした場合は、スタンバイ Firepower Management Center をアクティブ状態に昇格させることができます。元のアクティブなピアが起動すると、両方のピアがアクティブであるとみなされる場合があります。この状態は「スプリットブレイン」と定義されます。このような状況が発生すると、システムによってアクティブなアプライアンスを選択するように要求されます。それによって、もう一方のアプライアンスはスタンバイ状態に降格します。

アクティブな Firepower Management Center がダウンした（またはネットワーク障害により切断された）場合は、高可用性を中断するか、またはロールを切り替えることができます。スタンバイ Firepower Management Center は縮退状態になります。



- (注) セカンダリとして使用するアプライアンスがどれであっても、スプリットブレインの解決時にデバイス登録とポリシー設定のすべてが失われます。たとえば、セカンダリに存在し、プライマリには存在しなかったポリシーへの変更は失われます。Firepower Management Center が両方のアプライアンスがアクティブな高可用スプリットブレインシナリオである場合に、スプリットブレインを解決する前に管理対象デバイスを登録してポリシーを展開する場合は、ハイアベイラビリティを再確立する前に、ポリシーをエクスポートして、管理対象デバイスを対象のスタンバイ Firepower Management Center から登録解除する必要があります。その後、管理対象デバイスを登録し、目的のアクティブ Firepower Management Center にポリシーをインポートすることができます。

ハイ アベイラビリティ ペアでの Firepower Management Center のアップグレード

Cisco は、各種の更新プログラムを電子形式で定期的に配信します。更新プログラムには、システムソフトウェアのメジャーおよびマイナーアップグレードが含まれます。ハイアベイラビリティセットアップでは、これらの更新を両方の Firepower Management Center にインストールする必要が生じることがあります。



- 警告** アップグレード中には、少なくとも 1 つの Firepower Management Center を動作状態に維持してください。

始める前に

アップグレードに付属しているリリースノートまたはアドバイザリテキストを読んでください。リリースノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

手順

- ステップ 1** アクティブ Firepower Management Center の Web インターフェイスにアクセスし、データ同期を一時停止します（[Firepower Management Center ペア間の通信の一時停止（13 ページ）](#)を参照）。
- ステップ 2** スタンバイ Firepower Management Center をアップグレードします（[Firepower Management Center でのソフトウェアの更新](#)を参照）。
- アップグレードが完了すると、スタンバイユニットがアクティブになります。両方のピアがアクティブになると、ハイアベイラビリティペアが劣化状態（スプリットブレイン）になります。

ステップ 3 もう一方の Firepower Management Center をアップグレードします。

ステップ 4 どちらの Firepower Management Center をセカンダリとして使用するかを決定します。そのデバイスを登録解除し、維持する必要がある設定をエクスポートします。

新しいアクティブ Firepower Management Center を選択すると、セカンダリとして指定される Firepower Management Center のデバイス登録と展開済みポリシー設定がすべて失われます。たとえば、同期を一時停止した後に行ったポリシーの変更内容はすべて失われます。

ステップ 5 新しいアクティブ Firepower Management Center を選択してスプリットブレインを解決します。

Firepower Management Center のハイアベイラビリティのトラブルシューティング

この項では、Firepower Management Center のハイアベイラビリティ操作のいくつかの一般的なエラーに関するトラブルシューティング情報を示します。

エラー (Error)	説明	ソリューション
500 内部 (500 Internal)	ピア ロールの切り替えや同期の一時停止と再開などのクリティカルな Firepower Management Center のハイアベイラビリティ操作を実行しているときに Web インターフェイスにアクセスしようとする则表示されることがあります。	Web インターフェイスを使用する前に、操作が完了するまでお待ちください。

エラー (Error)	説明	ソリューション
<p>システム プロセスが起動していません、お待ちください (System processes are starting, please wait)</p> <p>また、Web インターフェイスは応答しません。 (Also, the web interface does not respond.)</p>	<p>ハイアベイラビリティまたはデータ同期操作中に Firepower Management Center が再起動 (手動でまたは電源切断からの回復中に) する場合に表示されることがあります。</p>	<ol style="list-style-type: none"> 1. Firepower Management Center シェルにアクセスし、<code>manage_hadc.pl</code> コマンドを使用して Firepower Management Center のハイアベイラビリティ構成ユーティリティにアクセスします。 (注) <code>sudo</code> を使用して、ルート ユーザとしてユーティリティを実行します。 2. オプション 5 を使用してミラーリング操作を一時停止します。 Firepower Management Center Web インターフェイスをリロードします。 3. Web インターフェイスを使用して同期を再開します。[システム (System)] > [統合 (Integration)] の順に選択し、[ハイアベイラビリティ (High Availability)] タブをクリックして、[同期の再開 (Resume Synchronization)] を選択します。

Firepower Management Center の高可用性の設定

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

高可用性を確立するには、ピア間の帯域幅とポリシーの数に応じてかなりの時間がかかり、数時間かかることもあります。また、スタンバイ状態の Firepower Management Center と同期される必要のある、アクティブ Firepower Management Center に登録されたデバイスの数によっても

異なります。[ハイ アベイラビリティ (High Availability)] ページを表示すると、ハイ アベイラビリティ ピアのステータスを確認できます。

始める前に

- 両方の Firepower Management Center が同じモデルで、同じソフトウェアバージョンを実行していることを確認します。
- セカンダリの Firepower Management Center に登録されているすべてのデバイスの登録を解除します。

手順

-
- ステップ 1** セカンダリとして指定する Firepower Management Center にログインします。
- ステップ 2** [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 3** [高可用性 (High Availability)] を選択します。
- ステップ 4** この Firepower Management Center の権限で、[セカンダリ (Secondary)] を選択します。
- ステップ 5** [プライマリ Firepower Management Center ホスト (Primary Firepower Management Center Host)] テキストボックスに、プライマリ Firepower Management Center のホスト名または IP アドレスを入力します。
- ルーティング可能なアドレスがプライマリ Firepower Management Center に設定されていない場合は、空白のままにしても構いません。この場合は、[登録キー (Registration Key)] と [一意の NAT ID (Unique NAT ID)] の両方のフィールドを使用します。プライマリ ユニットでセカンダリ IP アドレスを指定する必要もあります。少なくとも 1 つのユニットの IP アドレスを指定する必要があります。
- ステップ 6** [登録キー (Registration Key)] テキストボックスに、1 回限り使用する登録キーを入力します。登録キーは、ユーザ定義の最大 37 文字の英数字値です。
- ステップ 7** プライマリ IP アドレスを指定しなかった場合、またはプライマリ Firepower Management Center でセカンダリ IP アドレスを指定しない場合は、[一意の NAT ID (Unique NAT ID)] フィールドに一意の英数字 ID を入力します。詳細については、[NAT 環境](#) を参照してください。
- ステップ 8** [登録 (Register)] をクリックします。
- ステップ 9** 管理者アクセス権限を持つアカウントを使用して、プライマリとして指定する Firepower Management Center にログインします。
- ステップ 10** [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 11** [高可用性 (High Availability)] を選択します。
- ステップ 12** この Firepower Management Center の権限で、[プライマリ (Primary)] を選択します。
- ステップ 13** [セカンダリ Firepower Management Center ホスト (Secondary Firepower Management Center Host)] テキストボックスに、セカンダリ Firepower Management Center のホスト名または IP アドレスを入力します。

ルーティング可能なアドレスがセカンダリ Firepower Management Center に設定されていない場合は、空白のままにしても構いません。この場合は、[登録キー (Registration Key)] と [一意の NAT ID (Unique NAT ID)] の両方のフィールドを使用します。セカンダリ ユニットでプライマリ IP アドレスを指定する必要もあります。少なくとも 1 つのユニットの IP アドレスを指定する必要があります。

- ステップ 14** [登録キー (Registration Key)] テキストボックスに、ステップ 6 で入力した 1 回限り使用する登録キーと同じものを入力します。
- ステップ 15** 必要に応じて、[一意の NAT ID (Unique NAT ID)] テキストボックスに手順 7 で使用したのと同じ NAT ID を入力します。
- ステップ 16** [登録 (Register)] をクリックします。

Firepower Management Center ハイ アベイラビリティ ステータスの表示

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

アクティブおよびスタンバイ Firepower Management Center を識別した後、ローカル Firepower Management Center とそのピアに関する情報を表示できます。



- (注) このコンテキストでは、ローカル ピアは、システム ステータスを表示するアプライアンスを参照します。リモートピアは、アクティブステータスかスタンバイステータスかに関係なく、その他のアプライアンスを参照します。

手順

- ステップ 1** 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。
- ステップ 2** [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 3** [ハイ アベイラビリティ (High Availability)] を選択します。
- 次の情報を表示できます。

サマリー情報

- ハイ アベイラビリティ ペアのヘルス ステータス
- ハイ アベイラビリティ ペアの現在の同期ステータス
- アクティブ ピアの IP アドレスと最後に同期された時間
- スタンバイ ピアの IP アドレスと最後に同期された時間

システム ステータス

- 両方のピアの IP アドレス
- 両方のピアのオペレーティング システム
- 両方のピアのソフトウェア バージョン
- 両方のピアのアプライアンス モデル

Firepower Management Center ハイ アベイラビリティ ペア で同期される設定

この項では、ハイ アベイラビリティが確立されたときに2つの Firepower Management Center 間で同期される特定の設定データについて説明します。

- アクセス コントロール ポリシー
- 侵入ルール
- マルウェアおよびファイル ポリシー
- DNS ポリシー
- アイデンティティ ポリシー
- SSL ポリシー
- プレフィルタ ポリシー
- ネットワーク検出ルール
- アプリケーション ディテクタ
- 関連ポリシー ルール
- アラート (Alerts)
- スキャナ (Scanners)
- 応答グループ

- 修復設定。ただし、両方の Firepower Management Center にカスタム モジュールをインストールする必要があります。修復設定の詳細については、[修復モジュールの管理](#)を参照してください。

Firepower Management Center のハイ アベイラビリティにおけるデバイス登録を解決するための CLI の使用

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

自動デバイス登録がスタンバイ Firepower Management Center で失敗したものの、アクティブ Firepower Management Center に登録されたと表示される場合、次の手順を実行します。

手順

ステップ 1 アクティブ Firepower Management Center からデバイスの登録を解除します。

ステップ 2 影響を受けるデバイスの CLI にログインします。

ステップ 3 CLI コマンド `configure manager delete` を実行します。

ステップ 4 CLI コマンド `configure manager add` を実行します。

アクティブ Firepower Management Center のリモート管理を設定します。

ステップ 5 アクティブ Firepower Management Center にログインし、デバイスを登録します。

Firepower Management Center ハイ アベイラビリティ ペアにおけるピアの切り替え

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

システムでは一部の機能をアクティブ Firepower Management Center に制限しているため、そのアプライアンスで障害が発生した場合は、スタンバイ Firepower Management Center をアクティブ ステータスにプロモートする必要があります。

手順

-
- ステップ 1** ハイ アベイラビリティを使用してペアリングした Firepower Management Center のいずれか一方にログインします。
- ステップ 2** [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 3** [ハイ アベイラビリティ (High Availability)] を選択します。
- ステップ 4** [ピア ロールの切り替え (Switch Peer Roles)] を選択して、ローカル ロールをアクティブからスタンバイ、またはスタンバイからアクティブに変更します。プライマリまたはセカンダリの指定は変更されずに、2つのピア間でロールが切り替わります。
-

Firepower Management Center ペア間の通信の一時停止

スマート ライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

一時的に高可用性を無効にする場合は、Firepower Management Center 間の通信チャンネルを無効にすることができます。アクティブ ピアの同期を一時停止した場合は、スタンバイ ピアまたはアクティブ ピアのいずれでも同期を再開できます。ただし、スタンバイ ピアで同期を一時停止した場合、同期の再開はスタンバイ ピアでのみ可能になります。

手順

-
- ステップ 1** 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。
- ステップ 2** [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 3** [高可用性 (High Availability)] を選択します。
- ステップ 4** [同期の一時停止 (Pause Synchronization)] を選択します。
-

Firepower Management Center ペア間の通信の再開

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

一時的に高可用性を無効にしている場合は、Firepower Management Center 間の通信チャンネルを有効にすることで、高可用性を再開することができます。アクティブユニットで同期を一時停止した場合、スタンバイ ユニットまたはアクティブ ユニットのいずれでも同期を再開できます。ただし、スタンバイユニットで同期を一時停止した場合、同期の再開はスタンバイユニットでのみ可能になります。

手順

-
- ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。
 - ステップ 2 [システム (System)] > [統合 (Integration)] を選択します。
 - ステップ 3 [高可用性 (High Availability)] を選択します。
 - ステップ 4 [同期の再開 (Resume Synchronization)] を選択します。
-

高可用性ペアの Firepower Management Center の IP アドレスの変更

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin



- (注) 7000 および 8000 シリーズ 管理対象デバイスのリモート管理を編集しているときに、このトピックにたどり着いた場合は、[管理対象デバイスでのリモート管理の編集](#)を参照してください。
-

高可用性ピアのいずれかの IP アドレスを変更すると、高可用性が低下した状態になります。高可用性を回復するには、手動で IP アドレスを変更する必要があります。

手順

- ステップ 1 高可用性を使用してペアにした Firepower Management Center のいずれかにログインします。
- ステップ 2 [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 3 [高可用性 (High Availability)] を選択します。
- ステップ 4 [ピア マネージャ (Peer Manager)] を選択します。
- ステップ 5 編集アイコン (✎) を選択します。
- ステップ 6 アプライアンスの表示名を入力します。この表示名は、Firepower システムのコンテキストでのみ使用されます。
別の表示名を入力しても、アプライアンスのホスト名は変更されません。
- ステップ 7 完全修飾ドメイン名を入力するか、ローカル DNS で有効な IP アドレス (ホスト名) に解決される名前、またはホストの IP アドレスを入力します。
- ステップ 8 [保存 (Save)] を選択します。

ハイ アベイラビリティ ペアでの Firepower Management Center のアップグレード

Cisco は、各種の更新プログラムを電子形式で定期的に配信します。更新プログラムには、システム ソフトウェアのメジャーおよびマイナー アップグレードが含まれます。ハイ アベイラビリティセットアップでは、これらの更新を両方の Firepower Management Center にインストールする必要が生じることがあります。



警告 アップグレード中には、少なくとも 1 つの Firepower Management Center を動作状態に維持してください。

始める前に

アップグレードに付属しているリリース ノートまたはアドバイザリ テキストを読んでください。リリースノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

手順

- ステップ 1** アクティブ Firepower Management Center の Web インターフェイスにアクセスし、データ同期を一時停止します（[Firepower Management Center ペア間の通信の一時停止（13 ページ）](#)を参照）。
- ステップ 2** スタンバイ Firepower Management Center をアップグレードします（[Firepower Management Center でのソフトウェアの更新](#)を参照）。
アップグレードが完了すると、スタンバイユニットがアクティブになります。両方のピアがアクティブになると、ハイアベイラビリティペアが劣化状態(スプリットブレイン)になります。
- ステップ 3** もう一方の Firepower Management Center をアップグレードします。
- ステップ 4** どちらの Firepower Management Center をセカンダリとして使用するかを決定します。そのデバイスを登録解除し、維持する必要がある設定をエクスポートします。
新しいアクティブ Firepower Management Center を選択すると、セカンダリとして指定される Firepower Management Center のデバイス登録と展開済みポリシー設定がすべて失われます。たとえば、同期を一時停止した後に行ったポリシーの変更内容はすべて失われます。
- ステップ 5** 新しいアクティブ Firepower Management Center を選択してスプリットブレインを解決します。

Firepower Management Center ハイ アベイラビリティの無効化

スマートライセンス	従来のライセンス	サポートされている Management Center	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	MC1500、 MC2000、 MC3500、MC4000	グローバル	Admin

手順

- ステップ 1** ハイアベイラビリティペアのいずれか一方の Firepower Management Center にログインします。
- ステップ 2** [システム (System)] > [統合 (Integration)] を選択します。
- ステップ 3** [ハイアベイラビリティ (High Availability)] を選択します。
- ステップ 4** [ハイアベイラビリティの解消 (Break High Availability)] を選択します。
- ステップ 5** 管理対象デバイスを処理するための以下のいずれかのオプションを選択します。

- この Firepower Management Center を使用してすべての管理対象デバイスを制御する場合には、[このコンソールから登録済みデバイスを管理 (Manage registered devices from this console)] を選択します。すべてのデバイスがピアから登録解除されます。
- 他の Firepower Management Center を使用してすべての管理対象デバイスを制御する場合には、[ピアコンソールから登録済みデバイスを管理 (Manage registered devices from peer console)] を選択します。すべてのデバイスがこの Firepower Management Center から登録解除されます。
- デバイスの管理をまとめて停止する場合には、[両方のコンソールからの登録済みデバイスの管理を停止 (Stop managing registered devices from both consoles)] を選択します。すべてのデバイスが両方の Firepower Management Center から登録解除されます。

ステップ 6 [OK] をクリックします。
