Firepower Management Center のハイ 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

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 はアクティブ/スタンバイ ハイ アベイラビリティをサポートしています。つまり 1 台のアプライアンスがアクティブなユニットとなってデバイスを管理します。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。

リモート アクセス VPN のハイ アベイラビリティについて

プライマリ デバイスに、CertEnrollment オブジェクトを使用して登録された ID 証明書を使用したリモート アクセス VPN 設定がある場合、セカンダリ デバイスには、同じ CertEnrollment オブジェクトを使用して登録された ID 証明書が必要です。CertEnrollment オブジェクトは、デバイス固有のオーバーライドにより、プライマリ デバイスとセカンダリ デバイスに異なる値を持つことができます。この制限は、ハイ アベイラビリティの形成前に 2 つのデバイスに同じ CertEnrollment オブジェクトを登録することだけです。

Firepower Management Center 高可用性のシステム要件

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

- 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。
- 帯域幅要件：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。

ソフトウェア要件

[アプライアンス情報（Appliance Information）] ウィジェットにアクセスして、ソフトウェア バージョン、侵入ルールの更新バージョン、および脆弱性データベースの更新バージョンを確認します。デフォルトでは、[詳細ダッシュボード（Detailed Dashboard）] と [サマリー ダッシュボード（Summary Dashboard）] の [ステータス（Status）] タブにウィジェットが表示されます。詳細については、[アプライアンス情報（Appliance Information）] ウィジェットを参照してください。

- 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。
- ハイ アベイラビリティ構成内の 2 つの Firepower Management Center には、同じバージョンの侵入ルールの更新をインストールする必要があります。
- ハイ アベイラビリティ構成内の 2 つの Firepower Management Center には、同じバージョンの脆弱性データベースの更新をインストールする必要があります。

警告 両方の Firepower Management Center でソフトウェア バージョン、侵入ルールの更新バージョン、および脆弱性データベースの更新バージョンが同一でない場合は、ハイ アベイラビリティを確立できません。

ライセンス要件

すべてのライセンスタイプ

高可用性ペア内の Firepower Management Center アプライアンスに特別なライセンスは必要ありません。

高可用性設定の Firepower Management Center アプライアンスで管理されているデバイスには、1 つの Firepower Management Center で管理されているデバイスと同じ数の機能ライセンスとサブスクリプションが必要です。

特定ライセンス予約の展開では、プライマリ FMC のみが特定ライセンス予約を必要とします。

システムは、高可用性ペアが形成された時点でアクティブからスタンバイ Firepower Management Center にすべての機能ライセンスを複製し、実行中のデータ同期の間にライセンスの変更を更新します。そのため、ライセンスはフェールオーバー時に使用できます。

スマート ライセンス

例：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。

アクティブな Firepower Management Center のみが Cisco Smart Software Manager に登録されます。フェールオーバーが実行されると、システムは Cisco Smart Software Manager と通信して、スマート ライセンスの付与資格を最初にアクティブだった Firepower Management Center から解放し、新たにアクティブになる Firepower Management Center に割り当てます。

従来のライセンス

例：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。

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 ユニットに同期されます。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 のハイ アベイラビリティを確立するための前提条件

Firepower Management Center ハイ アベイラビリティ ペアを確立する前に、次の操作を行います。

- 必要なポリシーを、対象のセカンダリ Firepower Management Center から対象のプライマリ Firepower Management Center にエクスポートします。詳細については、設定のエクスポートを参照してください。
- 対象のセカンダリ Firepower Management Center にデバイスが追加されていないことを確認します。対象のセカンダリ Firepower Management Center からデバイスを削除し、そのデバイスを対象のプライマリ Firepower Management Center に登録します。詳細については、Firepower Management Center からのデバイスの削除 と Firepower Management Center へのデバイスの追加 を参照してください。

- 対象のプライマリ Firepower Management Center にポリシーをインポートします。詳細については、設定のインポートを参照してください。
- 対象のプライマリ Firepower Management Center で、インポートされたポリシーを確認して、必要に応じて編集し、適切なデバイスに展開します。詳細については、設定変更の展開を参照してください。
- 対象のプライマリ Firepower Management Center で、適切なライセンスを新しく追加したデバイスに関連付けます。詳細については、[デバイス管理（Device Management）]ページで管理対象デバイスにライセンスを割り当てるを参照してください。
- なお、Cisco Security Packet Analyzer と統合のための対象のセカンダリ Firepower Management Center の既存設定は、同期が発生した場合は上書きされます。必要に応じて、対象のプライマリ Firepower Management Center でこのような設定を再作成します。

これで、ハイ アベイラビリティの確立に進むことができます。詳細については、Firepower Management Center ハイ アベイラビリティの確立 （10 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/ISE-PIC、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。

Cisco Threat Intelligence Director (TID) およびハイ アベイラビリティ構成

ハイ アベイラビリティ構成のアクティブな Firepower Management Center で TID をホスティングする場合、システムは TID 構成と TID データをスタンバイ Firepower Management Center に同期しません。フェールオーバー後にデータを復元できるように、アクティブ Firepower Management Center で TID データの定期的なバックアップを実行することを推奨します。

詳細は、TID データのバックアップおよび復元についてを参照してください。

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 （16 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 をスタンバイとして使用するかを決定します。同期を一時停止した後にスタンバイに追加された追加のデバイスまたはポリシーは、アクティブ Firepower Management Center に同期されません。その追加のデバイスのみを登録解除し、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した Firepower Management Center は、同期されていないデバイス登録と展開されたポリシー設定を失います。

ステップ 5 最新のポリシーとデバイスに必要なすべての設定を含む新しいアクティブ 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と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
システム プロセスが起動しています、お待ちください（System processes are starting, please wait） 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.）	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。	**1.** Firepower Management Center シェルにアクセスし、`manage_hadc.pl` 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） `sudo` 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 ハイ アベイラビリティの確立

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）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	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 がハイ アベイラビリティ システム要件を満足していることを確認します。詳細については、Firepower Management Center 高可用性のシステム要件 （2 ページ）を参照してください。
- ハイ アベイラビリティを確立するための前提条件を満足していることを確認します。詳細については、Firepower Management Center のハイ アベイラビリティを確立するための前提条件 （4 ページ）を参照してください。

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 **[System]** > **[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 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。この登録キーはセカンダリおよびプライマリ Firepower Management Center の登録に使用されます。

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 **[System]** > **[Integration]**を選択します。

ステップ 11 [ハイ アベイラビリティ（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。

次のタスク

Firepower Management Center ハイ アベイラビリティ ペアを確立すると、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。

（注） 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 （14 ページ） を参照してください。

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）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	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 **[System]** > **[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

2 つの Firepower Management Center の間でハイ アベイラビリティを確立すると、次の設定データが同期されます。

- ライセンスの付与資格
- 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
- 相関ポリシー ルール

- アラート（Alerts）
- スキャナ（Scanners）
- 応答グループ
- イベントを調査するための外部リソースのコンテキスト クロス起動
- Cisco Security Packet Analyzer との統合
- 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）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	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。
このコマンドは、現在の Firepower Management Center を無効にして削除します。

ステップ 4 CLI コマンド `configure manager add` を実行します。
このコマンドは、デバイスを設定して Firepower Management Center への接続を開始します。

ヒント　デバイスのリモート管理を、アクティブな Firepower Management Center の場合のみ設定します。ハイ アベイラビリティを確立すると、デバイスは自動的に追加され、スタンバイ Firepower Management Center によって管理されます。

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）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	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　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　**[System]** > **[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）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	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 **[System]** > **[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 [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）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	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 **[System]** > **[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 [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）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	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 **[System]** > **[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 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。

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）	MC1000、MC1500、MC1600、MC2000、MC2500、MC2600、MC3500、MC4000、MC4500、MC4600	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 **[System]** > **[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。

（注） セカンダリ Firepower Management Center から登録済みデバイスを管理する場合、そのデバイスはプライマリ Firepower Management Center から登録解除されます。そのデバイスは、セカンダリ Firepower Management Center によって管理されるように登録されます。ただし、そのデバイスに適用されていたライセンスは、ハイ アベイラビリティの中断操作のために登録解除されます。次に、セカンダリ Firepower Management Center からデバイス上でライセンスを再登録（有効化）する必要があります。詳細については、管理対象デバイスからのスマート ライセンスの移動または削除を参照してください。

ステップ 6 [OK] をクリックします。

ハイ アベイラビリティ ペアでの Firepower Management Center の交換

Firepower Management Center ハイ アベイラビリティ ペアで障害が発生したユニットを交換する必要がある場合は、次に示すいずれかの手順に従う必要があります。次の表に、4 つの障害シナリオとそれに対応する交換手順を示します。

障害ステータス	データ バックアップ ステータス	交換手順
プライマリ Firepower Management Center の障害	データ バックアップが成功	障害が発生したプライマリ Firepower Management Center の交換（バックアップが成功）（21 ページ）
	データ バックアップが失敗	障害が発生したプライマリ Firepower Management Center の交換（バックアップが失敗）（22 ページ）
セカンダリ Firepower Management Center の障害	データ バックアップが成功	障害が発生したセカンダリ Firepower Management Center の交換（バックアップが成功）（23 ページ）
	データ バックアップが失敗	障害が発生したセカンダリ Firepower Management Center の交換（バックアップが失敗）（24 ページ）

障害が発生したプライマリ Firepower Management Center の交換（バックアップが成功）

2 つの Firepower Management Center（FMC1 と FMC2）がハイ アベイラビリティ ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、プライマリからのデータ バックアップが成功した場合に、障害が発生したプライマリ Firepower Management Center（FMC1）を交換する手順を説明します。

始める前に

障害が発生したプライマリ Firepower Management Center からのデータ バックアップが成功したことを確認します。

手順

ステップ 1 サポートに連絡して、障害が発生した Firepower Management Center（FMC1）の交換を要請します。

ステップ 2 プライマリ Firepower Management Center（FMC1）で障害が発生した場合は、セカンダリ Firepower Management Center（FMC2）の Web インターフェイスにアクセスしてピアを切り替えます。詳細については、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 （15 ページ）を参照してください。

これにより、セカンダリ Firepower Management Center（FMC2）がアクティブに昇格します。

プライマリ Firepower Management Center（FMC1）の交換が完了するまで、FMC2 をアクティブ Firepower Management Center として使用できます。

警告 Firepower Management Center ハイ アベイラビリティを FMC2 から分断しないでください。分断すると、（障害前に）FMC1 から FMC2 に同期されていた従来のライセンスとスマート ライセンスが FMC2 から削除されるため、FMC2 から展開アクションを実行できなくなります。

ステップ 3 FMC1 と同じソフトウェア バージョンを使用して交換用 Firepower Management Center を再イメージ化します。

ステップ 4 FMC1 から取得したデータ バックアップを新しい Firepower Management Center に復元します。

ステップ 5 FMC2 と適合するのに必要な Firepower Management Center パッチ、地理位置情報データベース（GeoDB）更新、脆弱性データベース（VDB）更新、システム ソフトウェア更新をインストールします。

これで、新しい Firepower Management Center と FMC2 の両方がアクティブ ピアとなるため、ハイ アベイラビリティがスプリットブレイン状態になります。

ステップ 6 Firepower Management Center Web インターフェイスからアクティブ アプライアンスを選択するよう求めるプロンプトが出されたら、FMC2 をアクティブとして選択します。

これにより、FMC2 の最新の設定が新しい Firepower Management Center（FMC1）に同期されます。

ステップ 7 設定が正常に同期されたら、セカンダリ Firepower Management Center（FMC2）の Web インターフェイスにアクセスし、役割を切り替えてプライマリ Firepower Management Center（FMC1）をアクティブにします。詳細については、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 （15 ページ）を参照してください。

ステップ 8 新しい Firepower Management Center（FMC1）で受け取った従来のライセンスを適用し、古いライセンスを削除します。詳細については、クラシック ライセンスの生成と Firepower Management Center への追加を参照してください。

スマート ライセンスはシームレスに機能します。

次のタスク

これで、ハイ アベイラビリティが再確立されたため、プライマリおよびセカンダリ Firepower Management Center が正常に動作するようになります。

障害が発生したプライマリ Firepower Management Center の交換（バックアップが失敗）

2 つの Firepower Management Center（FMC1 と FMC2）がハイ アベイラビリティ ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、プライマリからのデータ バックアップが失敗した場合に、障害が発生したプライマリ Firepower Management Center（FMC1）を交換する手順を説明します。

手順

ステップ 1 サポートに連絡して、障害が発生した Firepower Management Center（FMC1）の交換を要請します。

ステップ 2 プライマリ Firepower Management Center（FMC1）で障害が発生した場合は、セカンダリ Firepower Management Center（FMC2）の Web インターフェイスにアクセスしてピアを切り替えます。詳細については、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 （15 ページ）を参照してください。

これにより、セカンダリ Firepower Management Center（FMC2）がアクティブに昇格します。

プライマリ Firepower Management Center（FMC1）の交換が完了するまで、FMC2 をアクティブ Firepower Management Center として使用できます。

警告 Firepower Management Center ハイ アベイラビリティを FMC2 から分断しないでください。分断すると、（障害前に）FMC1 から FMC2 に同期されていた従来のライセンスとスマート ライセンスが FMC2 から削除されるため、FMC2 から展開アクションを実行できなくなります。

ステップ 3 FMC1 と同じソフトウェア バージョンを使用して交換用 Firepower Management Center を再イメージ化します。

ステップ 4 FMC2 と適合するのに必要な Firepower Management Center パッチ、地理位置情報データベース（GeoDB）更新、脆弱性データベース（VDB）更新、システム ソフトウェア更新をインストールします。

ステップ 5 Firepower Management Center（FMC2）を Cisco Smart Software Manager から登録解除します。詳細については、Cisco Smart Software Manager からの Firepower Management Center の登録解除を参照してください。

Cisco Smart Software Manager から Firepower Management Center の登録を解除すると、バーチャル アカウントから Management Center が削除されます。Firepower Management Center リリースに関連付けられているライセンス権限はすべて、ご使用のバーチャルアカウントに戻ります。登録解除後、Firepower Management Center は適用モードになり、ライセンスが適用される機能に対する更新および変更が許可されなくなります。

ステップ 6 セカンダリ Firepower Management Center（FMC2）の Web インターフェイスにアクセスして、Firepower Management Center ハイ アベイラビリティを分断します。詳細については、Firepower Management Center ハイ アベイラビリティの無効化 （19 ページ）を参照してください。管理対象デバイスを処理する方法を選択するよう求められたら、[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。

これにより、セカンダリ Firepower Management Center（FMC2）に同期されていた従来のライセンスとスマート ライセンスが削除されるため、FMC2 から展開アクティビティを実行できなくなります。

ステップ 7 Firepower Management Center ハイ アベイラビリティを再確立するために、Firepower Management Center（FMC2）をプライマリ、Firepower Management Center（FMC1）をセカンダリとして設定します。詳細については、Firepower Management Center ハイ アベイラビリティの確立 （10 ページ）を参照してください。

ステップ 8 新しい Firepower Management Center（FMC1）で受け取った従来のライセンスを適用し、古いライセンスを削除します。詳細については、クラシック ライセンスの生成と Firepower Management Center への追加を参照してください。

ステップ 9 スマート ライセンスをプライマリ Firepower Management Center（FMC2）に登録します。詳細については、スマート ライセンスの登録を参照してください。

次のタスク

これで、ハイ アベイラビリティが再確立されたため、プライマリおよびセカンダリ Firepower Management Center が正常に動作するようになります。

障害が発生したセカンダリ Firepower Management Center の交換（バックアップが成功）

2 つの Firepower Management Center（FMC1 と FMC2）がハイ アベイラビリティ ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、セカンダリからのデータ バックアップが成功した場合に、障害が発生したセカンダリ Firepower Management Center（FMC2）を交換する手順を説明します。

始める前に

障害が発生したセカンダリ Firepower Management Center からのデータ バックアップが成功したことを確認します。

手順

ステップ 1 サポートに連絡して、障害が発生した Firepower Management Center（FMC2）の交換を要請します。

ステップ 2 引き続きプライマリ Firepower Management Center（FMC1）をアクティブ Firepower Management Center として使用します。

ステップ 3 FMC2 と同じソフトウェア バージョンを使用して交換用 Firepower Management Center を再イメージ化します。

ステップ 4 FMC2 から取得したデータ バックアップを新しい Firepower Management Center に復元します。

ステップ 5 FMC1 と適合するのに必要な Firepower Management Center パッチ、地理位置情報データベース（GeoDB）更新、脆弱性データベース（VDB）更新、システム ソフトウェア更新をインストールします。

ステップ 6 新しい Firepower Management Center（FMC2）の Web インターフェイスからデータ同期を再開して（停止されていた場合）、プライマリ Firepower Management Center（FMC1）の最新の設定を同期させます。詳細については、Firepower Management Center ペア間の通信の再開 （17 ページ）を参照してください。

従来のライセンスとスマート ライセンスはシームレスに機能します。

次のタスク

これで、ハイ アベイラビリティが再確立されたため、プライマリおよびセカンダリ Firepower Management Center が正常に動作するようになります。

障害が発生したセカンダリ Firepower Management Center の交換（バックアップが失敗）

2 つの Firepower Management Center（FMC1 と FMC2）がハイ アベイラビリティ ペアを構成しています。FMC1 がプライマリ、FMC2 がセカンダリです。このタスクでは、セカンダリからのデータ バックアップが失敗した場合に、障害が発生したセカンダリ Firepower Management Center（FMC2）を交換する手順を説明します。

手順

ステップ 1 サポートに連絡して、障害が発生した Firepower Management Center（FMC2）の交換を要請します。

ステップ 2 引き続きプライマリ Firepower Management Center（FMC1）をアクティブ Firepower Management Center として使用します。

ステップ 3 FMC2 と同じソフトウェア バージョンを使用して交換用 Firepower Management Center を再イメージ化します。

ステップ 4 FMC1 と適合するのに必要な Firepower Management Center パッチ、地理位置情報データベース（GeoDB）更新、脆弱性データベース（VDB）更新、システム ソフトウェア更新をインストールします。

ステップ 5 プライマリ Firepower Management Center（FMC1）の Web インターフェイスにアクセスして、Firepower Management Center ハイ アベイラビリティを分断します。詳細については、Firepower Management Center ハイ アベイラビリティの無効化 （19 ページ）を参照してください。管理対象デバイスを処理する方法を選択するよう求められたら、[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。

ステップ 6 Firepower Management Center ハイ アベイラビリティを再確立するために、Firepower Management Center（FMC1）をプライマリ、Firepower Management Center（FMC2）をセカンダリとして設定します。詳細については、Firepower Management Center ハイ アベイラビリティの確立 （10 ページ）を参照してください。

- ハイ アベイラビリティが正常に確立されると、プライマリ Firepower Management Center（FMC1）の最新の設定がセカンダリ Firepower Management Center（FMC2）に同期されます。
- 従来のライセンスとスマート ライセンスはシームレスに機能します。

次のタスク

これで、ハイ アベイラビリティが再確立されたため、プライマリおよびセカンダリ Firepower Management Center が正常に動作するようになります。