高可用性

以下のトピックでは、Cisco Secure Firewall 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。

Firewall 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 Firewall 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。Firewall 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/スタンバイ高可用性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 Firewall Management Center に障害が発生した場合、セカンダリ Firewall 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 Firewall Management Center に障害が発生した場合は、セカンダリ Firewall 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 Firewall Management Center に配信されます。一方の Firewall Management Center で障害が発生した場合、他方の Firewall 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 Firewall 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 Firewall 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 Firewall Management Center をアクティブにプロモートする必要があります。

（注） 変更の展開が成功した直後に Firewall Management Center でスイッチオーバーがトリガーされると、新しいアクティブ Firewall Management Center でプレビュー設定が機能しなくなる可能性があります。これは、ポリシー展開機能に影響を与えません。必要な同期が完了した後に Firewall Management Center でスイッチオーバーをトリガーすることをお勧めします。

同様に、Firewall Management Center HA 同期が劣化状態の場合、スイッチオーバーをトリガーしたり、ロールを変更したりすると、Firewall Management Center HA によってデータベースが破損し、致命的な状態になる可能性があります。この問題を解決するための支援が必要な場合は、Cisco Technical Assistance Center（TAC）にただちに連絡することをお勧めします。

この HA 同期は、さまざまな理由で劣化状態になる可能性があります。この章にある「高可用性ペアでの Firewall Management Center の交換 （25 ページ）」の項では、いくつかの障害シナリオと、問題を修正するための後続の手順について説明しています。劣化状態の理由またはシナリオが説明されているシナリオと一致する場合は、手順に従って問題を修正します。それら以外の理由の場合は、TAC に連絡することをお勧めします。

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。

Firewall Management Center High Availability での SNMP の動作

SNMP が設定された HA ペアでは、アラートポリシーを展開すると、アクティブ Firewall Management Center が SNMP トラップを送信します。プライマリ Firewall Management Center に障害が発生すると、セカンダリ Firewall Management Center がアクティブユニットになり、追加の設定を必要とせずに SNMP トラップの送信を開始します。

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

Secure Firewall 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 Secure Firewall 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 Secure Firewall Management Center がアクティブ ピアになり、セカンダリ Secure Firewall 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 Secure Firewall 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 Secure Firewall 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 Secure Firewall 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。

Firewall Management Center 高可用性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 Firewall 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、いずれかの Firewall 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 Firewall 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 Firewall 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 Firewall 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 Secure Firewall Management Center の間で同期されます。ただし、プライマリ Secure Firewall 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 Secure Firewall Management Center に障害が発生した場合は、セカンダリ Secure Firewall 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 Secure Firewall 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。

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

プライマリ Firewall Management Center に障害が発生した場合、セカンダリ Firewall Management Center は、TS エージェント アイデンティティ ソースからのユーザーから IP へのマッピングと、ISE/ISE-PIC アイデンティティソースからの SGT マッピングを、管理対象デバイスに伝播します。アイデンティティソースでまだ認識されていないユーザーは、[不明（Unknown）] として識別されます。

ダウンタイム後、[不明（Unknown）]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び識別され、処理されます。

Firewall Management Center 高可用性ペアの設定管理

ハイ アベイラビリティ展開では、アクティブな Firewall 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 Firewall Management Center は継続的な同期状態を保ちます。

アクティブ状態の Firewall 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。

Firewall Management Center 高可用性ディザスタリカバリ

ディザスタリカバリの状況では、手動スイッチオーバーを実行する必要があります。プライマリ Firewall Management Center（FMC1）で障害が発生した場合は、セカンダリ Firewall 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。これは、逆に、セカンダリ（FMC2）に障害が発生した場合にも当てはまります。詳細については、Firewall Management Center のハイアベイラビリティペアにおけるピアの切り替え （22 ページ）を参照してください。

障害が発生した Firewall Management Center の復旧については、高可用性ペアでの Firewall Management Center の交換 （25 ページ）を参照してください。

シングルサインオンと高可用性ペア

高可用性設定の Firewall Management Center ではシングルサインオンをサポートできますが、次の考慮事項に留意する必要があります。

- SSO 設定は、高可用性ペアのメンバー間で同期されません。ペアの各メンバーで個別に SSO を設定する必要があります。
- 高可用性ペアの両方の Firewall Management Center は、SSO に同じアイデンティティ プロバイダー（IdP）を使用する必要があります。SSO 用に設定された各 Firewall Management Center の IdP で、サービス プロバイダー アプリケーションを設定する必要があります。
- 両方が SSO をサポートするように設定されている Firewall Management Center の高可用性ペアでは、ユーザーは SSO を使用してセカンダリ Firewall Management Center に初めてアクセスする前に、最初に SSO を使用してプライマリ Firewall Management Center に少なくとも 1 回ログインする必要があります。
- 高可用性ペアで Firewall Management Center の SSO を設定する場合：
  - プライマリ Firewall Management Center で SSO を設定する場合、セカンダリ Firewall Management Center で SSO を設定する必要はありません。
  - セカンダリ Firewall Management Center で SSO を設定する場合は、プライマリ Firewall Management Center でも SSO を設定する必要があります。（これは、SSO ユーザーがセカンダリ Firewall Management Center にログインする前に、プライマリ Firewall Management Center に少なくとも 1 回ログインする必要があるためです）。

関連トピック

SAML シングルサインオンの設定

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

Firewall 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 Firewall 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。

Firewall Management Center 高可用性スプリットブレイン

高可用性ペアのアクティブな Firewall 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 Firewall Management Center をアクティブ状態に昇格させることができます。HA はスプリットブレイン状態になります。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Firewall 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 Firewall Management Center は縮退状態になります。

（注） スタンバイとしての使用意図のあ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、スタンバイとして意図されていたアプライアンスに存在し、アクティブとして意図されていたアプライアンスには存在しなかったポリシーへの変更は失われます。Firewall 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 Firewall 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 Firewall Management Center にポリシーをインポートすることができます。

Firewall 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、Firewall 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（Description）	ソリューション
スタンバイにログインする前に、アクティブな Firewall Management Center でパスワードをリセットする必要があります。	アカウントの強制的なパスワードリセットが有効になっているときに、スタンバイ Firewall Management Center にログインしようとしました。	データベースはスタンバイ Firewall Management Center に対して読み取り専用であるため、アクティブな Firewall Management Center のログインページでパスワードをリセットします。
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 Firewall 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（Description）	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 Firewall 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.** Firewall Management Center シェルにアクセスし、`manage_hadc.pl` コマンドを使用して Firewall 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。 Firewall 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。**[統合（Integration）]** > **[その他の統合（Other Integrations）]** を選択し、[高可用性（High Availability）] タブをクリックして、[同期の再開（Resume Synchronization）] を選択します。

エラー（Error）	説明（Description）	ソリューション
デバイス登録ステータス：ホスト <string> が到達不能（Device Registration Status:Host <*string*> is not reachable）	Firewall Threat Defense の初期設定時に、Firewall Management Center の IP アドレスと NAT ID が指定されている場合は、[ホスト（Host）] フィールドを空白のままにできます。ただし、両方の Firewall Management Center が NAT の背後にある HA 環境では、Firewall Threat Defense をセカンダリ Firewall Management Center に追加すると、このエラーが発生します。	1. プライマリ Firewall Management Center から Firewall Threat Defense を削除します。『Cisco Secure Firewall Management Center Device Configuration Guide』の「*Delete a Device from the* Firewall Management Center」を参照してください。 2. **configure manager delete** コマンドを使用して Firewall Threat Defense からマネージャを削除します。Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。 3. [ホスト（Host）] フィールドで、Firewall Threat Defense デバイスの IP アドレスまたは名前を使用して Firewall Threat Defense を Firewall Management Center に追加します。『Cisco Secure Firewall Management Center Device Configuration Guide』の「*Add a Device to the* Firewall Management Center」を参照してください。

エラー（Error）	説明（Description）	ソリューション
デバイス登録ステータス：ホスト <string> が到達不能（Device Registration Status:Host <*string*> is not reachable）	セカンダリ Firewall Management Center と Firewall Threat Defense デバイスの両方が NAT の背後にある高可用性展開で、Firewall Threat Defense デバイスをセカンダリ Firewall Management Center センターに追加すると、エラーが発生します。	スタンバイ Firewall Management Center Web インターフェイスで、**[統合（Integration）] > [その他の統合（Other Integrations）] > [高可用性（High Availability）]** をクリックします。保留中のデバイス登録のテーブルで、保留中のデバイスの IP アドレスをクリックし、IP アドレスを Firewall Threat Defense のパブリック IP アドレスに変更します。 または **1.** Firewall Threat Defense シェルにアクセスし、`show manager` コマンドを使用して、スタンバイ Firewall Management Center のエントリ識別子の値を取得します。 **2.** Firewall Threat Defense シェルで、スタンバイ Firewall Management Center のホスト名をパブリック IP アドレスに編集します。エントリ識別子とホスト IP アドレスを使用して `configure manager edit <standby_uuid> hostname <standby_ip>` コマンドを実行します。 詳細については、「Firewall Management Center 高可用性で CLI を使用してデバイス登録を解決する （21 ページ）」を参照してください。

エラー（Error）	説明（Description）	ソリューション
高可用性 Management Center 間のデバイス設定の同期が停止しています。（Device configuration synchronization has been stopped between high availability Firewall Management Centers.）	Firewall Management Center HA 同期中にデバイス設定履歴ファイルが他の設定データと並行して同期されるようになりました。Firewall Management Center は、設定履歴ファイルの同期タスクをモニターし、過去 6 時間以内に同期が行われていない場合は通知します。この正常アラートは、アクティブとスタンバイの両方の Firewall Management Center に表示されます。	アクティブとスタンバイの両方の Firewall Management Center が劣化状態に移行します。問題のトラブルシューティングについては、Cisco TAC にお問い合わせください。

Firewall Management Center高可用性の要件

モデルのサポート

「ハードウェア要件 （10 ページ）」を参照してください。

仮想モデルのサポート

「仮想プラットフォームの要件 （11 ページ）」を参照してください。

サポートされるドメイン

Global

ユーザの役割

管理者

ハードウェア要件

- すべての Firewall Management Center ハードウェアが高可用性をサポートしている。ピアは同じモデルである必要がある。
- ピアは異なるデータセンターにあり、互いに物理的および地理的に分離可能である。
- 高可用性設定の帯域幅要件は、ネットワークのサイズ、管理対象デバイスの数、イベントとログの量、設定更新のサイズと頻度など、さまざまな要因によって異なります。

  一般的な Firewall Management Center 高可用性展開では、100 ミリ秒に近い高遅延のネットワークの場合、ピア間に 5 Mbps 以上のネットワーク帯域幅が推奨されます。

Firewall Management Center に保存される設定のバージョンの数を減らすことで、高可用性の同期速度を向上させることができます。詳細については、『Cisco Secure Firewall Management Center デバイス設定ガイド』の「設定バージョン番号の設定」を参照してください。このオプションは、Secure Firewall Management Center バージョン 7.3.0 および 7.4.0 ではサポートされていないことに注意してください。

- 両方の Firewall Management Centerに一意の UUID があることを確認します。UUID を確認するには、`/etc/sf/ims.conf`ファイルを確認します。
- プライマリピアのバックアップをセカンダリに復元しないでください。
- Firewall Management Center ハイアベイラビリティ構成のライセンス要件 （12 ページ） も参照してください。

仮想プラットフォームの要件

高可用性は、次のパブリッククラウド プラットフォームでサポートされています。

- Amazon Web Services（AWS）
- Oracle Cloud Infrastrucure（OCI）
- Microsoft Azure

また、次のオンプレミス/プライベートクラウド プラットフォームでサポートされています。

- Cisco HyperFlex
- カーネルベース仮想マシン（KVM）
- Microsoft Hyper-V
- VMware vSphere/VMware ESXi

Firewall Management Center は、同じデバイス管理機能（FMCv2 ではサポートされていません）と同じライセンスを持っている必要があります。また、管理対象デバイスあたり 1 つの Firewall Threat Defense 権限が必要です。詳細については、「Firewall Management Center ハイアベイラビリティ構成のライセンス要件 （12 ページ）」を参照してください。

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 Firewall 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 Firewall 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 Firewall 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。
- ハイアベイラビリティ構成内の 2 つの Firewall Management Center には、同じバージョンの LSP（Lightweight Security Package）をインストールする必要があります。
- 高可用性構成の 2 つの管理センターには、通信のためにポート 8305 がそれらの間でアクセス可能である必要があります。

警告 両方の Firewall 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。

Firewall Management Center ハイアベイラビリティ構成のライセンス要件

各デバイスには、単一の Firewall Management Center によって管理されているか、ハイアベイラビリティペア（ハードウェアまたは仮想）の Firewall Management Center によって管理されているかにかかわらず、同じライセンスが必要です。

例：Firewall 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する場合は、2 つの マルウェア防御 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 Firewall Management Center を Smart Software Manager に登録してから、ライセンスをアクティブ Firewall Management Center 上の 2 つのデバイスに割り当てます。

アクティブな Firewall Management Center のみが 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 Smart Software Manager と通信して、ライセンスの付与資格を最初にアクティブだった Firewall Management Center から解放し、新たにアクティブになる Firewall Management Center に割り当てます。

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

ハードウェア（Hardware） Firewall Management Center

ハイアベイラビリティペア内のハードウェア Firewall Management Center に特別なライセンスは必要ありません。

Firewall Management Center Virtual

同じライセンスの Firewall Management Center Virtual が 2 つ必要です。

例：10 台のデバイスを管理する Firewall Management Center Virtual ハイアベイラビリティペアの場合は、以下を使用できます。

- 2 個の Firewall Management Center Virtual 10 エンタイトルメント
- 10 個のデバイスライセンス

ハイアベイラビリティペアを解除すると、セカンダリ Firewall Management Center Virtual に関連付けられた Firewall Management Center Virtual エンタイトルメントが解放されます。（この例では、2 個のスタンドアロン Firewall Management Center Virtual 10 があります。）

Firewall Management Center 高可用性の前提条件

Firewall Management Center 高可用性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 Firewall Management Center から対象のプライマリ Firewall 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 Firewall 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 Firewall 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 Firewall Management Center に登録します。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「Delete a Device from Firewall Management Center」および「Add a Device to Firewall Management Center」を参照してください。
- 対象のプライマリ Firewall 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 Firewall 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、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Deploy Configuration Changes*」を参照してください。
- 対象のプライマリ Firewall 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、単一のデバイスへのライセンスの割り当てを参照してください。

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、「Firewall Management Centerのハイアベイラビリティの確立 （14 ページ）」を参照してください。

Firewall Management Centerのハイアベイラビリティの確立

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Firewall Management Centerと同期される必要のある、アクティブFirewall 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 Firewall 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、Firewall Management Center高可用性の要件 （10 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、Firewall Management Center 高可用性の前提条件 （13 ページ）を参照してください。
- マルチドメイン展開でこのタスクを実行するには、グローバルドメインに属している必要があります。

手順

ステップ 1 セカンダリとして指定する Firewall Management Center にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）]** 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 Firewall Management Center の権限で、[セカンダリ（Secondary）] を選択します。

ステップ 5 **[プライマリファイアウォール Management Center ホスト（Primary Firewall Management Center Host）]** テキストボックスに、プライマリ Firewall Management Center のホスト名または IP アドレスを入力します。

ピア Firewall Management Center から到達可能な IP アドレス（パブリックまたはプライベート IP アドレス）がプライマリ Firewall Management Center にない場合は、これを空のままにできます。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。HA接続を有効にするには、少なくとも1つのFirewall Management Center 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 Firewall 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 Firewall 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 [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 Firewall Management Center にログインします。

ステップ 10 **[統合（Integration）] > [その他の統合（Other Integrations）]** 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 Firewall Management Center の権限で、[プライマリ（Primary）] を選択します。

ステップ 13 **[セカンダリファイアウォール Management Center ホスト（Secondary Firewall Management Center Host）]** テキストボックスに、セカンダリ Firewall Management Center のホスト名または IP アドレスを入力します。

ピア Firewall Management Center から到達可能な IP アドレス（パブリックまたはプライベート IP アドレス）がセカンダリ Firewall Management Center にない場合は、これを空のままにできます。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。HA 接続を有効にするには、少なくとも 1 つの Firewall Management Center 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 [Register] をクリックします。

次のタスク

Firewall Management Center 高可用性ペアを確立すると、アクティブ Firewall Management Center に登録されたデバイスが自動的にスタンバイ Firewall Management Center に登録されます。

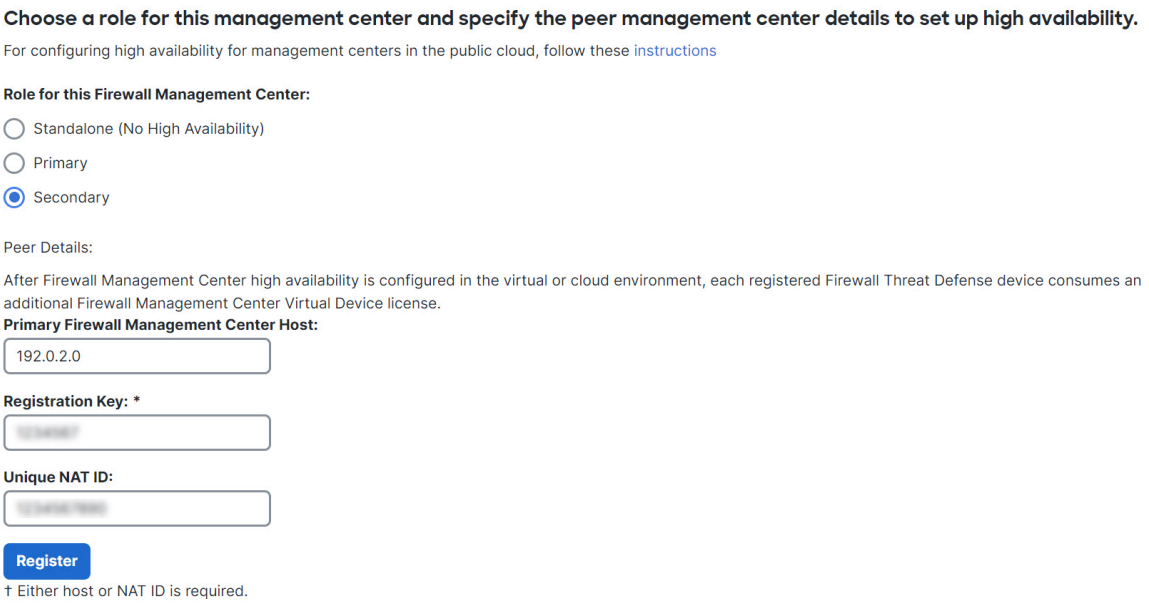
（注） 登録済みのデバイスに NAT IP アドレスが割り当てられている場合、デバイスの自動登録は失敗し、セカンダリ Firewall Management Center の [高可用性（High Availability）] ページには、そのデバイスがローカルで保留中であると表示されます。次に、スタンバイ Firewall Management Center の [ハイ アベイラビリティ（High Availability）] ページで、異なる NAT IP アドレスをデバイスに割り当てることができます。自動登録がスタンバイ Firewall Management Center で失敗しても、デバイスがアクティブな Cisco Secure Firewall Management Center に登録されているように見える場合は、「Firewall Management Center 高可用性で CLI を使用してデバイス登録を解決する （21 ページ）」を参照してください。

パブリッククラウドでホストされる Firewall Management Center の高可用性

パブリッククラウドでホストされている Firewall Management Center 間で高可用性を確立する際、以下で説明するプライマリとセカンダリの Firewall Management Center の IP アドレスまたはホスト名の組み合わせにより、高可用性を正常に形成し、両方のピアにデバイスを登録できます。**[高可用性（High Availability）]** ページ（**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[高可用性（High Availability）]**）で、次のいずれかの設定を実行して、パブリッククラウドでホストされている Firewall Management Center 間の高可用性を正常に形成します。

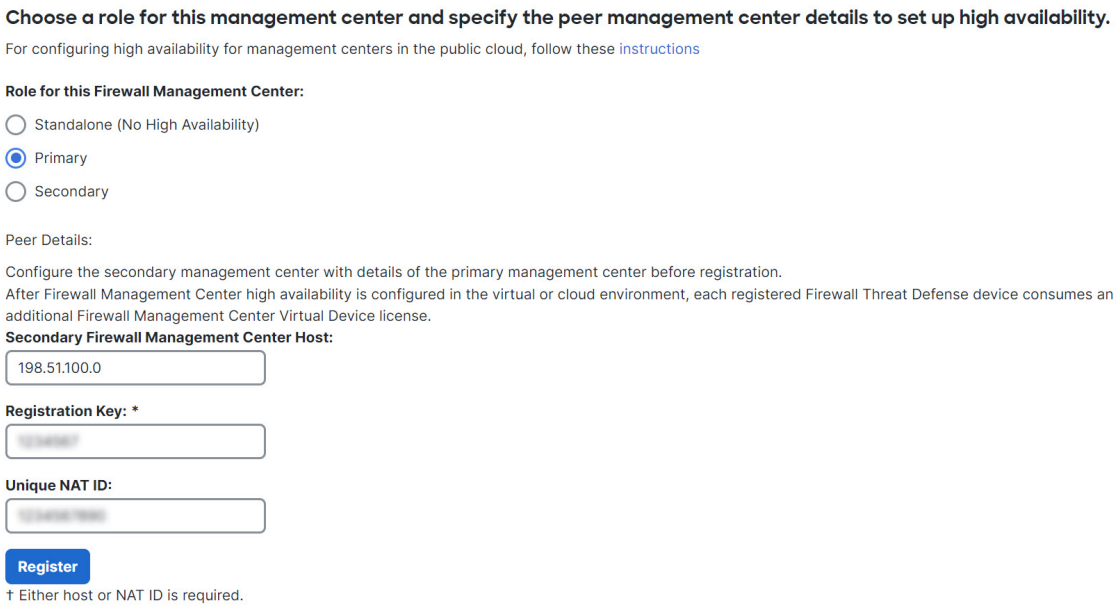
プライマリとセカンダリの Firewall Management Center の両方にパブリック IP アドレスまたはホスト名を使用する

1. セカンダリ Firewall Management Centerで、次の手順を実行します。
    1. **セカンダリ**をこの **Firewall Management Center のロール**として選択します。
    2. **[プライマリ Firepower Management Center ホスト（Primary Firepower Management Center Host）]** フィールドに、セカンダリ Firewall Management Center のホスト名または IP アドレスを入力します。
    3. 登録キーを入力します。
    4. プライマリ Firewall Management Centerで使用したのと同じ NAT ID を入力します。



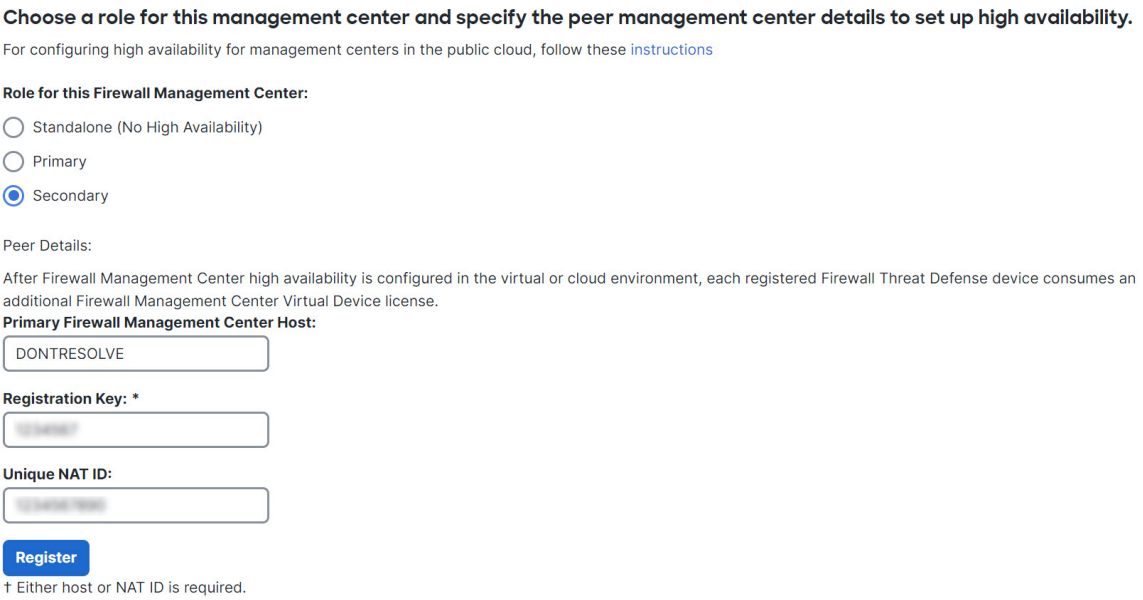
2. プライマリ Firewall Management Centerで、次の手順を実行します。
    1. **プライマリ**をこの **Firewall Management Center のロール**として選択します。

2. **[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 Firewall Management Center のホスト名または IP アドレスを入力します。
3. 登録キーを入力します。
4. 一意の NAT ID を入力します。

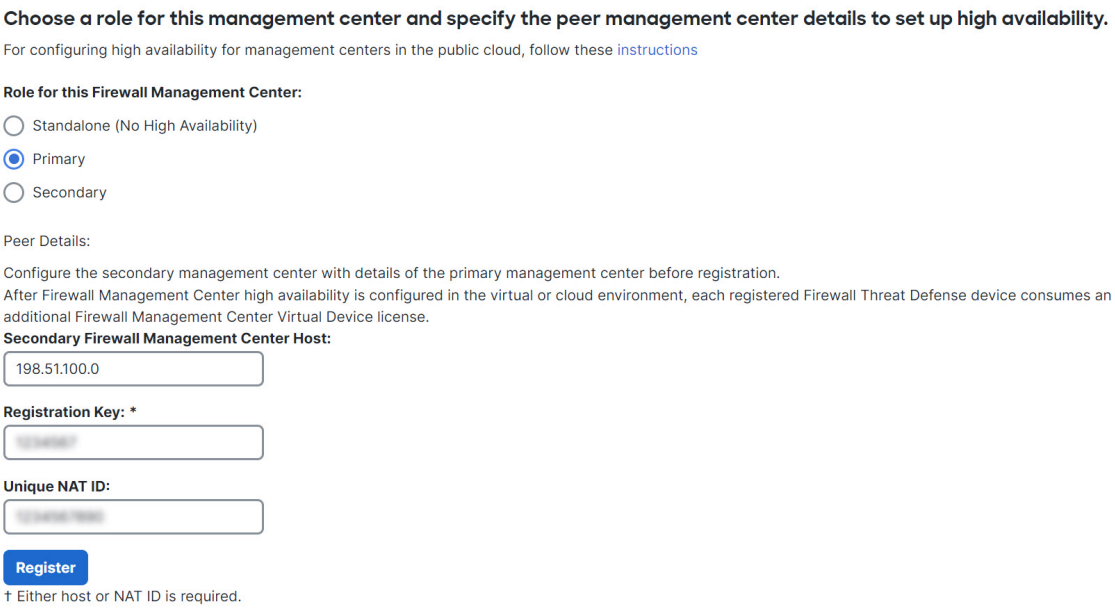


セカンダリ Firewall Management Center に対するパブリック IP アドレスまたはホスト名の使用

1. セカンダリ Firewall Management Centerで、次の手順を実行します。
   1. **セカンダリ**をこの **Firewall Management Center のロール**として選択します。
   2. **[プライマリFirewall Management Centerホスト（Primary Firewall Management Center Host）]** フィールドに **DONTRESOLVE** と入力します。
   3. 登録キーを入力します。
   4. プライマリ Firewall Management Centerで使用したのと同じ NAT ID を入力します。



2. プライマリ Firewall Management Centerで、次の手順を実行します。
   1. **プライマリをこの Firewall Management Center のロール**として選択します。
   2. **[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 Firewall Management Center のホスト名または IP アドレスを入力します。
   3. 登録キーを入力します。
   4. 一意のNAT IDを入力します。



Firewall Management Center 高可用性ステータスの表示

アクティブおよびスタンバイ Firewall Management Center を識別した後、ローカル Firewall 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 ハイ アベイラビリティを使用してペアリングした Firewall Management Center のいずれか一方にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）]** を選択します。

ステップ 3 [高可用性（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

- 高可用性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
- 構成設定で定義されたタイムゾーンで表示される最後の同期時間と、相対的な経過時間。たとえば、 *18* 分前です。

システム ステータス（System Status）

- 両方のピアに設定された IP アドレス
- 両方のピアのソフトウェア バージョン
- 両方のピアの Lightweight Security Package（LSP）バージョン
- 両方のピアの Snort ルール更新（SRU）バージョン
- 両方のピアの脆弱性データベース（VDB）のバージョン

（注）
エクスポート制御およびコンプライアンスステータスは、アクティブ Firewall Management Center でのみ表示できます。

ステップ 4 **[リモートおよびローカルデバイスの登録（Remote and Local Device Registration）]**で、Firewall Management Centerで保留中または登録が失敗したデバイスのリストを表示できます。デバイスに対して次の操作を実行できます。

- デバイス上の古いマネージャを削除するには、デバイスのチェックボックスをオンにして、**[マネージャの無効化（Disable Manager）]**をクリックします。マネージャの IP アドレスを入力し、**[無効化（Disable）]**をクリックします。
- デバイスのマネージャを追加するには、デバイスのチェックボックスをオンにして、**[マネージャの追加（Add Manager）]**をクリックします。マネージャのIPアドレスを入力し、**[追加（Add）]**をクリックします。

（注）
デバイス上のマネージャの削除または追加は、一度に 1 つのデバイスでのみ実行できます。

Firewall Management Center 高可用性ペアで同期される設定

2 つの Firewall 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
- 修復設定。ただし、両方の Firewall 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。

高可用性ペアでの Firewall Management Center データベースへの外部アクセスの設定

高可用性設定では、アクティブなピアのみを使用して、データベースへの外部アクセスを設定することを推奨します。外部データベースアクセス用にスタンバイピアを設定すると、頻繁に切断されるようになります。接続を復元するには、スタンバイピアの同期を一時停止してから再開する必要があります。Firewall Management Center への外部データベースアクセスを有効にする方法については、データベースへの外部アクセスの有効化を参照してください。

Firewall Management Center 高可用性で CLI を使用してデバイス登録を解決する

自動デバイス登録がスタンバイ Firewall Management Center で失敗したものの、アクティブ Firewall 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。

警告 セカンダリ Firewall Management Center の RMA を実行するか、セカンダリ Firewall Management Center を追加すると、管理対象デバイスが登録解除されます。その結果、管理対象デバイスの設定が削除されることがあります。

手順

ステップ 1 アクティブな Firewall Management Center からデバイスを削除します。Cisco Secure Firewall Management Center デバイス設定ガイド の「*Firewall Management Center* からのデバイスの登録解除削除（登録解除）」を参照してください。

ステップ 2 スタンバイ Firewall Management Center でデバイスの自動登録をトリガーするには、次の手順を実行します。

1. 影響受けるデバイスの CLI にログインします。
2. CLI コマンドの **configure manager delete** を実行します。

   このコマンドは、現在の Firewall Management Center を無効にして削除します。

3. CLI コマンドの **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 Firewall 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 Firewall Management Center の場合のみ設定します。高可用性を確立すると、デバイスが自動的にスタンバイ Firewall Management Center に登録されます。

4. アクティブ Firewall Management Center にログインし、デバイスを登録します。

ステップ 3 スタンバイ Firewall Management Center が NAT の背後にある場合は、次の手順を実行してスタンバイ Firewall Management Center のホスト名を編集します。

1. Firewall Threat Defense シェルにアクセスし、`show manager` コマンドを使用して、スタンバイ Firewall Management Center のエントリ識別子の値を取得します。
2. Firewall Threat Defense シェルで、スタンバイ Firewall Management Center のホスト名をパブリック IP アドレスに編集します。エントリ識別子とホスト IP アドレスを使用して `configure manager edit <standby_uuid> hostname <standby_ip>` コマンドを実行します。

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

システムでは一部の機能をアクティブ Firewall 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 Firewall 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 Firewall Management Center のいずれか一方にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）]** 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 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。

ペアにされた Firewall Management Center 間での通信の一時停止

一時的に高可用性を無効にする場合は、Firewall Management Center 間の通信チャネルを無効にすることができます。アクティブピアまたはスタンバイピアから同期を再開できます。

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 Firewall Management Center のいずれか一方にログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** 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。

ペアにされた Firewall Management Center 間での通信の再開

一時的に高可用性を無効にしている場合は、Firewall 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。アクティブピアまたはスタンバイピアから同期を再開できます。

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 Firewall Management Center のいずれか一方にログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** 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 Firewall Management Center の IP アドレスの変更

高可用性ピアの一方の IP アドレスを変更した場合、その変更は高可用性同期を実行しても、もう一方のピアに自動的に更新されることはありません。リモートピア Firewall Management Center も更新されるようにするには、IP アドレスを手動で変更する必要があります。

手順

ステップ 1 他のピアマネージャの IP アドレスを手動で変更するピア Firewall Management Center にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）]** 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（Edit）]（） 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、システムのコンテキストでのみ使用されます。名前は、現在の Firewall Management Center の IP アドレス、または特殊文字（アンダースコア（_）とハイフン（-））を含む英数字の文字列である必要があります。

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）] をクリックします。

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

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 Firewall Management Center にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）]** 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 **[HA の解消（Break HA）]** 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 Firewall 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 Firewall 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 Firewall 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 Firewall Management Center から登録解除されます。

（注）
- セカンダリ Firewall 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 Firewall Management Center から登録解除されます。そのデバイスは、セカンダリ Firewall 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 Firewall 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、デバイスへのライセンスの割り当てを参照してください。
- スタンバイ管理センターは、HA の解消が完了した後、アクセス コントロール ポリシーを保持します。

ステップ 6 **[OK]** をクリックします。

高可用性ペアでの Firewall Management Center の交換

Firewall Management Center 高可用性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 Firewall 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 Firewall Management Center の交換（バックアップが成功）（26 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 Firewall Management Center の交換（バックアップが失敗）（27 ページ）

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
セカンダリ Firewall 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 Firewall Management Center の交換（バックアップが成功） （29 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 Firewall Management Center の交換（バックアップが失敗） （30 ページ）

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

2 つの Firewall Management Center（FMC1 と FMC2）が高可用性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 Firewall 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 Firewall 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 Firewall Management Center（FMC1）の交換を依頼します。

ステップ 2 プライマリ Firewall Management Center（FMC1）で障害が発生した場合は、セカンダリ Firewall 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、Firewall Management Center のハイアベイラビリティペアにおけるピアの切り替え （22 ページ）を参照してください。

これで、セカンダリ Firewall Management Center（FMC2）がアクティブに昇格します。

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

注意
Firewall Management Center 高可用性を FMC2 から分断しないでください。分断すると、障害発生前に FMC1 から FMC2 に同期されていたライセンスが 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 Firewall 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 Firewall Management Center に復元します。

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

これで、新しい Firewall Management Center と FMC2 の両方がアクティブピアとなるため、高可用性がスプリットブレイン状態になります。

ステップ 6 Firewall 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プロンプトが表示されたら、FMC2 をアクティブとして選択します。

FMC2 の最新の設定が新しい Firewall 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 Firewall Management Center（FMC2）の Web インターフェイスにアクセスし、ロールを切り替えてプライマリ Firewall Management Center（FMC1）をアクティブにします。詳細については、Firewall Management Center のハイアベイラビリティペアにおけるピアの切り替え （22 ページ）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 Firewall 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 Firewall Management Center の交換（バックアップが失敗）

2 つの Firewall Management Center（FMC1 と FMC2）が高可用性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 Firewall 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 Firewall Management Center（FMC1）の交換を依頼します。

ステップ 2 プライマリ Firewall Management Center（FMC1）で障害が発生した場合は、セカンダリ Firewall 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、Firewall Management Center のハイアベイラビリティペアにおけるピアの切り替え （22 ページ）を参照してください。

これで、セカンダリ Firewall Management Center（FMC2）がアクティブに昇格します。

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

注意
Firewall 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 Firewall 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 Firewall Management Center パッチ、地理位置情報データベース（GeoDB）の更新、脆弱性データベース（VDB）の更新、システムソフトウェアの更新をインストールします。

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

Cisco Smart Software Manager から Firewall 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。Firewall 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、Firewall 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 Firewall Management Center（*FMC2*）の Web インターフェイスにアクセスして、Firewall 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、Firewall Management Center ハイアベイラビリティの無効化 （24 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 Firewall Management Center（*FMC2*）に同期されていた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 Firewall Management Center 高可用性を再確立するために、Firewall Management Center（*FMC2*）をプライマリ、Firewall Management Center（*FMC1*）をセカンダリとして設定します。詳細については、Firewall Management Centerのハイアベイラビリティの確立 （14 ページ）を参照してください。

ステップ 8 スマートライセンスをプライマリ Firewall Management Center（*FMC2*）に登録します。詳細については、Smart Software Manager での Firewall Management Center 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 Firewall 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 Firewall Management Center の交換（バックアップが成功）

2 つの Firewall Management Center（FMC1 と FMC2）が高可用性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 Firewall 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 Firewall 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 Firewall Management Center（FMC2）の交換を依頼します。

ステップ 2 引き続きプライマリ Firewall Management Center（FMC1）をアクティブ Firewall 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 Firewall 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 Firewall Management Center に復元します。

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

ステップ 6 新しい Firewall 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 Firewall Management Center（FMC1）の最新の設定を同期させます。詳細については、ペアにされた Firewall Management Center 間での通信の再開（23 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 Firewall 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 Firewall Management Center の交換（バックアップが失敗）

2 つの Firewall Management Center（FMC1 と FMC2）が高可用性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 Firewall 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 Firewall Management Center（FMC2）の交換を依頼します。

ステップ 2 引き続きプライマリ Firewall Management Center（FMC1）をアクティブ Firewall 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 Firewall 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 Firewall Management Center パッチ、地理位置情報データベース（GeoDB）の更新、脆弱性データベース（VDB）の更新、システム ソフトウェア アップデートをインストールします。

ステップ 5 プライマリ Firewall Management Center（FMC1）の Web インターフェイスにアクセスして、Firewall Management Center 高可用性を分断します。詳細については、Firewall Management Center ハイアベイラビリティの無効化 （24 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 Firewall Management Center 高可用性を再確立するために、Firewall Management Center（FMC1）をプライマリ、Firewall Management Center（FMC2）をセカンダリとして設定します。詳細については、Firewall Management Centerのハイアベイラビリティの確立 （14 ページ）を参照してください。

- 高可用性が正常に確立されると、プライマリ Firewall Management Center（FMC1）の最新の設定がセカンダリ Firewall 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 Firewall Management Center が正常に動作するようになります。

Firewall Management Center 高可用性ディザスタリカバリ

ディザスタリカバリの状況では、手動スイッチオーバーを実行する必要があります。プライマリ Firewall Management Center（FMC1）で障害が発生した場合は、セカンダリ Firewall 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。これは、逆に、セカンダリ（FMC2）に障害が発生した場合にも当てはまります。詳細については、Firewall Management Center のハイアベイラビリティペアにおけるピアの切り替え （22 ページ）を参照してください。

障害が発生した Firewall Management Center の復旧については、高可用性ペアでの Firewall Management Center の交換 （25 ページ）を参照してください。

（ハードウェアの障害がない）高可用性ペアでの Management Center の復元

ハードウェア障害がないときに Firewall Management Center 高可用性ペアを復元するには、次の手順に従います。

- プライマリ管理センターでのバックアップの復元 （31 ページ）
- セカンダリ管理センターでのバックアップの復元 （32 ページ）

プライマリ管理センターでのバックアップの復元

始める前に

- 管理センターのハードウェアの故障や交換がない。
- バックアップと復元のプロセスに精通している。を参照してくださいバックアップ/復元。

手順

ステップ 1 /var/sf/backup/ のローカルストレージ、またはリモートネットワークボリュームのいずれかで、プライマリ Firewall Management Center のバックアップが使用可能かどうかを確認します。

ステップ 2 プライマリ Firewall Management Center で、同期を一時停止します。**[統合（Integration）] > [その他の統合（Other Integrations）]** を選択し、[高可用性（High Availability）] タブに移動して同期を一時停止します。

ステップ 3 プライマリ Firewall Management Center でバックアップを復元します。復元が完了すると、Firewall Management Center が再起動します。

ステップ 4 プライマリ Firewall Management Center がアクティブになり、そのユーザーインターフェイスに到達できるようになったら、セカンダリ Firewall Management Center で同期を再開します。**[統**

合（**Integration**）] > **[**その他の統合（**Other Integrations**）**]** を選択し、[高可用性（High Availability）] タブに移動して同期を再開します。

セカンダリ管理センターでのバックアップの復元

始める前に

- 管理センターのハードウェアの故障や交換がない。
- バックアップと復元のプロセスに精通している。を参照してくださいバックアップ/復元。

手順

ステップ 1 /var/sf/backup/ のローカルストレージ、またはリモート ネットワーク ボリュームのいずれかで、セカンダリ Firewall Management Center のバックアップが使用可能かどうかを確認します。

ステップ 2 プライマリ Firewall Management Center で、同期を一時停止します。**[**統合（**Integration**）**]** > **[**その他の統合（**Other Integrations**）**]** を選択し、[高可用性（High Availability）] タブに移動して同期を一時停止します。

ステップ 3 セカンダリ Firewall Management Center でバックアップを復元します。復元が完了すると、Firewall Management Center が再起動します。

ステップ 4 セカンダリ Firewall Management Center がアクティブになり、そのユーザーインターフェイスに到達できるようになったら、プライマリ Firewall Management Center で同期を再開します。**[**統合（**Integration**）**]** > **[**その他の統合（**Other Integrations**）**]** を選択し、[高可用性（High Availability）] タブに移動して同期を再開します。

高可用性の Management Center の統合バックアップ

アクティブ Firewall Management Center で統合バックアップを実行できます。この場合、アクティブとスタンバイの両方の Firewall Management Center に対して単一のバックアップファイルが作成されます。統合バックアップは、設定のみのバックアップにのみ適用されます。イベントまたは TID バックアップが必要な場合は、アクティブおよびスタンバイ Firewall Management Center に対して個別のバックアップを取る必要があります。設定のみのバックアップを選択すると、デフォルトで統合バックアップが適用されます。統合バックアップでは、アクティブ Firewall Management Center がスタンバイ Firewall Management Center からバックアップ tar ファイルを取得できない場合、復元に使用できるアクティブユニットの通常のバックアップファイルが生成されます。統合バックアップには、通常のバックアップと比較していくつかの利点があります。

- 統合バックアップでは、アクティブとスタンバイ Firewall Management Center で個別のバックアップを取る必要はありません。

- 統合バックアップでは、バックアップ内の冗長データとストレージの制約が削除されます。
- 通常のバックアップでは、プライマリユニットに障害が発生した場合、セカンダリユニットのバックアップを使用できないと、セカンダリ RMA の高可用性ペアリングを解除する必要がありました。この状況は、統合バックアップでは解消されます。
- 通常、スタンバイユニットのバックアップはスケジュールできません。スケジュールされた統合バックアップでは、アクティブユニットとスタンバイユニットの両方のバックアップが取られます。
- 統合バックアップの実行中は、スタンバイユニットでバックアップを実行するために HA 同期を一時停止する必要はありません。

予期しないインシデントが発生した場合、統合バックアップを使用して新しい RMA デバイスを回復できます。統合バックアップのファイルは名前で識別できます。統合バックアップのファイル名には「Unified」というプレフィックスが追加されます。Firewall Management Center を選択して復元するとともに、その状態（アクティブ/スタンバイ）を選択することもできます。

スプリットブレインの競合を防ぐために、復元された Firewall Management Center の適切な状態を選択していることを確認してください。

統合バックアップからの Management Center の復元

統合バックアップ（設定のみ）から Firewall Management Center を復元するには、次の手順を使用します。

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、統合バックアップファイル（設定のみ）を含め、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。

統合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を参照してください。

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

ステップ 4 [バックアップの復元（Restore Backup）] ページで、復元するユニットを選択します。統合バックアップにはプライマリとセカンダリの両方の Firewall Management Center のバックアップ設定が保存されるため、復元するユニットを選択する必要があります。

ステップ 5 復元される Firewall Management Center の状態を選択するには、[アクティブ（Active）] または [スタンバイ（Standby）] オプションボタンをクリックします。作業中の Management Center のロールと状態を確認して、両方のピアのロールと状態が同じ設定にならないようにする必要があります。復元時に Management Center に誤ったロールと状態を選択すると、HA 障害が発生する可能性があります。

ステップ 6 [復元（Restore）] をクリックし、[復元の確認（Confirm Restore）] をクリックして復元を開始します。

Firewall Management Center 高可用性の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Azure での高可用性のサポート。	7.4.2	任意（Any）	Firewall Management Center Virtual で Azure の高可用性がサポートされるようになりました。
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	いずれか	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。
Management Center の高可用性同期の機能拡張。	7.4.1	任意	Management Center の高可用性（HA）には、次の同期機能拡張が含まれています。 • 設定履歴ファイルが大きいと、遅延の大きいネットワークで同期が失敗する可能性があります。これを防ぐために、デバイス設定履歴ファイルは他の設定データと並行して同期されるようになりました。この機能拡張により、同期時間も短縮されます。 • Firewall Management Center は、設定履歴ファイルの同期プロセスをモニターし、同期がタイムアウトした場合に正常性アラートを表示するようになりました。 新規/変更された画面：次の画面でこれらのアラートを確認できます。 • [通知（Notifications）] > [メッセージセンター（Message Center）] > [正常性（Health）] • [統合（Integration）] > [その他の統合（Other Integrations）] > [高可用性（High Availability）] > [ステータス （Status）]（[概要（Summary）] の下）

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Hyper-V での高可用性のサポート。	7.4.0	任意（Any）	Firewall Management Center Virtual で Hyper-V の高可用性がサポートされるようになりました。
KVM での高可用性のサポート。	7.3.0	いずれか	Firewall Management Center Virtual で KVM の高可用性がサポートされるようになりました。
AWS および OCI での高可用性のサポート。	7.1.0	いずれか	Firewall Management Center Virtual で AWS および OCI の高可用性がサポートされるようになりました。
HyperFlex での高可用性のサポート。	7.0.0	いずれか	Firewall Management Center Virtual で HyperFlex の高可用性がサポートされるようになりました。
VMware での高可用性のサポート。	6.7.0	いずれか	Firewall Management Center Virtual で VMware の高可用性がサポートされるようになりました。
シングルサインオン。	6.7.0	いずれか	シングルサインオン用に高可用性ペアの一方または両方のメンバーを設定するときは、特別な考慮事項を考慮する必要があります。

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