Cisco Secure Network Analytics

v7.4.2 フェールオーバー コンフィギュレーション ガイド

目次

はじめに

フェールオーバー設定を使用して、2 つの Cisco Secure Network Analytics Manager（旧 Stealthwatch Management Console または SMC）間のフェールオーバー関係を確立し、一方が他方のバックアップとして機能するようにします。

プライマリ マネージャが失敗した場合、セカンダリ マネージャがプライマリ マネージャになってシステムのモニタリングを継続するように手動で設定できます。

> ⚠ プライマリ マネージャがオフラインになった場合、マネージャは自動的にロールをスワップしないことにご注意ください。必ずこのガイドに示されている順序でマネージャのロールを変更してください。

始める前に

フェールオーバー設定を開始する前に、Cisco Secure Network Analytics（旧 Stealthwatch）アプライアンスをインストールし、システム設定を完了します。手順については、『Cisco Secure Network Analytics 設置ガイド』および『Cisco Secure Network Analytics システム設定ガイド』を参照してください。

また、フェールオーバー設定の要件と実装に備えて、このガイドで詳細および手順を確認してください。

データストアの展開

Secure Network Analytics システムでデータストア展開を使用している場合は、データストアを初期化する前にフェールオーバーを設定することをお勧めします。初期化済みのデータストアがある場合は、「**データストア初期化後のフェールオーバーの設定**」を参照してください。

セキュリティ分析とロギング（オンプレミス）

一方のマネージャで Cisco Security Analytics and Logging（オンプレミス）が有効になっている場合、フェールオーバー設定を開始する前に、もう一方のマネージャでも有効になっていることを確認してください。

両方のマネージャで セキュリティ分析とロギング（オンプレミス）を有効にするには、『Cisco Security Analytics and Logging（オンプレミス）：Firepower イベント統合ガイド』を参照してください。

アプライアンス ステータス（Appliance Status）

Secure Network Analytics で設定の変更を開始する前に、アプライアンスのステータスが [接続済み（Connected）] と表示されていることを確認します。このガイドには、ステータスを確認する手順が含まれています。

> ⚠ フェールオーバー設定が完了するまで、他の設定を変更したり、[集中管理（Central Management）] からアプライアンスを追加または削除したりしないでください。

設定要件

このガイドには、正常に設定するために重要な、次を含む詳細事項が記載されています。

管理者ユーザ（Admin User）

フェールオーバーを設定するには、管理者ユーザーとしてマネージャにログインします。

設定ファイルとデータベースのバックアップ

各マネージャの設定とデータベースをバックアップする時間を計画します。フェールオーバー設定に問題がある場合はバックアップファイルが必要となり、マネージャを完全に復元するには両方のバックアップが必要です。手順については、「**2. マネージャの設定とデータベースのバックアップ**」を参照してください。

証明書

フェールオーバーを設定する前に、必要なアプライアンスの信頼ストアに正しい証明書を保存してください。この手順では、アプライアンス間の信頼を確立して、互いに通信できるようにします。手順については、「**3. 信頼ストアへの証明書の追加**」を参照してください。

フェールオーバーロール

フェールオーバー設定を保存すると、プライマリ マネージャがアプライアンスをアクティブに監視および管理し、セカンダリ マネージャは読み取り専用になります。プライマリまたはセカンダリのフェールオーバーロールをどちらのマネージャに設定するかを計画するには、「**フェールオーバー設定の保存**」および「**1. フェールオーバーロールの計画**」を参照してください。

セカンダリ マネージャが [集中管理(Central Management)] でアプライアンスを管理している場合、フェールオーバー設定を開始する前に、それらをプライマリ マネージャ(または別のマネージャ)に移動させます。手順については、『Cisco Secure Network Analytics システム設定ガイド』を参照してください。

> ⚠ アプライアンスにカスタム証明書がある場合、アプライアンスを [集中管理(Central Management)] に追加する前に、アイデンティティ証明書と証明書チェーン(ルートおよび中間)をマネージャ信頼ストアに保存してください。

設定の順序

プライマリ マネージャの前にセカンダリ マネージャを設定します。手順については、「**4. フェールオーバーペアの設定**」を参照してください。

> ⚠ プライマリ マネージャを設定する前に、必ずセカンダリ マネージャのフェールオーバーを設定してください。フェールオーバー設定を保存すると、セカンダリ マネージャのドメイン設定が削除されるため、手順を順番に実行してください。

設定の変更

フェールオーバー設定が完了するまで、他の設定を変更したり、[集中管理(Central Management)] からアプライアンスを追加または削除したりしないでください。

ソフトウェア バージョン

このガイドの手順に進む前に、Secure Network Analytics v7.4.2 がマネージャにインストールされていることを確認してください。

フェールオーバー設定の保存

フェールオーバー設定を保存すると、プライマリ マネージャとセカンダリ マネージャの間に信頼関係と構成チャネルが確立されます。また、次のシステム変更が発生します。

プライマリ マネージャ

プライマリ マネージャは、ドメイン設定、ユーザー設定、およびポリシーをセカンダリ マネージャにプッシュします。

セカンダリ マネージャ（読み取り専用）

セカンダリ マネージャのドメイン設定は削除されます。そしてすべてのユーザーに対して読み取り専用になり、プライマリ マネージャと同期します。

パスワード

プライマリ マネージャは、ローカルユーザーとパスワードのログイン情報をセカンダリ マネージャにプッシュするため、それらは同期されます。これは、同じパスワードを使用してプライマリ マネージャとセカンダリ マネージャにログインすることを意味します。セカンダリ マネージャのパスワードを変更するには、プライマリ マネージャにログインします。

ドメインの変更

プライマリ マネージャは、ホストグループ、ユーザー、ポリシーなど、あらゆるドメイン設定の変更をセカンダリ マネージャと自動的に共有します。

セカンダリ マネージャへの通信チャネルがダウンしている（構成チャネルのダウン（Config Channel Down））ときにプライマリ マネージャのドメイン設定を変更した場合、プライマリ マネージャは、セカンダリ マネージャの通信チャネルが復旧され次第、完全な設定プッシュを送信します。

Flow Collector

Flow Collector は、両方のマネージャにデータを自動的にこの「両方に」は必要か送信します。

外部サービス（External Services）

プライマリ マネージャで外部サービスが設定されている場合は、それをセカンダリ マネージャでも必ず設定してください。たとえば、プライマリ マネージャで 脅威フィード を有効にしている場合、それをセカンダリ マネージャでも有効にします。

ロールの変更

セカンダリ マネージャをプライマリ フェールオーバー ロールに昇格させる必要がある場合は、ロールを順番に変更してください。順序は重要で、ロールは自動的に交換されません。

- プライマリ マネージャがオフラインの場合は、詳細について「**トラブルシューティング**」を参照してください。
- フェールオーバーロールを変更するには、「**フェールオーバーロールの変更**」を参照してください。

証明書

マネージャがフェールオーバー用に設定されている場合、次のように信頼ストアが自動的に更新されます。

- すべての管理対象アプライアンスの信頼ストアにセカンダリ マネージャのアイデンティティ証明書とチェーン（該当する場合）が追加されます。
- すべての管理対象アプライアンスのアイデンティティ証明書とチェーン（該当する場合）は、プライマリ マネージャの［集中管理（Central Management）］に追加されると、セカンダリ マネージャの信頼ストアに追加されます。

プライマリ マネージャの復元

フェールオーバー用に設定されているプライマリ マネージャを復元する場合、復元が完了すると、セカンダリ マネージャがプライマリ マネージャと同期します。

プライマリ マネージャの再起動

再起動によってプライマリ マネージャがオフラインになった場合、アプライアンスのステータスが [接続済み(Connected)] に戻り、セカンダリ マネージャが検出されると、プライマリのフェールオーバー ロールが再開されます。

- プライマリ マネージャのロールがセカンダリに変更され、それ自体が解決されない場合は、「**トラブルシューティング**」を参照してください。
- フェールオーバーロールを変更するには、「**フェールオーバーロールの変更**」を参照してください。

ネットワーク インターフェイスの変更

マネージャがフェールオーバー用に設定されている場合は、マネージャのネットワーク インターフェイス、ホスト名、またはネットワークドメイン名を変更する前に、フェールオーバー関係を削除してください。詳細については、「**ネットワーク インターフェイスの変更**」を参照してください。

フェールオーバーの設定の概要

フェールオーバーを設定するには、次の手順を完了してください。

1. フェールオーバーロールの計画
2. マネージャの設定とデータベースのバックアップ
3. 信頼ストアへの証明書の追加
4. フェールオーバーペアの設定
5. フェールオーバー設定の確認

1. フェールオーバーロールの計画

フェールオーバー設定を開始する前に、どちらのマネージャをプライマリまたはセカンダリのフェールオーバーロールに設定するかを計画します。

- **IP アドレス**：各マネージャに IP アドレスがあることを確認します。
- **セカンダリ マネージャ**：セカンダリ マネージャが［集中管理（Central Management）］でアプライアンスを管理している場合、フェールオーバー設定を開始する前に、それらをプライマリ マネージャ（または別のマネージャ）に移動させます。手順については、『Cisco Secure Network Analyticsシステム構成ガイド』を参照してください。

> ⚠ アプライアンスにカスタム証明書がある場合、アプライアンスを［集中管理（Central Management）］に追加する前に、アイデンティティ証明書と証明書チェーン（ルートおよび中間）をマネージャ信頼ストアに保存してください。

> ⚠ フェールオーバー設定を開始する前に、セキュリティ分析とロギング（オンプレミス） が両方のマネージャで有効になっていることを確認してください。両方のマネージャで セキュリティ分析とロギング（オンプレミス） を有効にするには、『Cisco Security Analytics and Logging（オンプレミス）：Firepower イベント統合ガイド』を参照してください。

- **フェールオーバー設定の保存**：フェールオーバー設定を保存すると、プライマリ マネージャがアプライアンスをアクティブに監視および管理し、セカンダリ マネージャは読み取り専用になります。詳細については、「**フェールオーバー設定の保存**」を参照してください。

計画した フェールオーバー	要約	IP アドレス（IP Address）
プライマリ マネージャ	Secure Network Analytics をアクティブに監視および管理	
セカンダリ マネージャ	読み取り専用	

2. マネージャの設定とデータベースのバックアップ

フェールオーバー用にマネージャを設定する前に、各アプライアンスの設定とデータベースをバックアップします。マネージャを完全に復元するには、両方のバックアップが必要です。

新規インストール：マネージャ が新規インストールで、今後設定を復元する必要がない場合は、この手順をスキップできます。「**3. 信頼ストアへの証明書の追加**」に進んでください。

> ⚠ バックアップがないと、フェールオーバー設定中に問題が発生した場合にファイルを回復できません。サポートが必要な場合は、シスコサポートまでお問い合わせください。

1. バックアップ設定ファイルの作成

次の手順を実行し、各マネージャのバックアップ設定ファイルを作成します。マネージャが Central Manager としてアプライアンスの管理もしている場合、マネージャ バックアップ設定ファイルと集中管理バックアップ設定ファイルを作成します。

1. **セカンダリ** マネージャにログインします。
2. メインメニューから **[構成（Configure）]** > **[グローバル集中管理（GLOBAL Central Management）]** を選択します。
3. マネージャの ••• （[省略記号（Ellipsis）]）アイコンをクリックします。
4. [サポート（Support）] を選択します。
5. [設定ファイル（Configuration Files）] タブを選択します。
6. [Backup Actions] ドロップダウンメニューをクリックします。
7. [Create Backup] を選択します。
8. [Download] をクリックします。安全な場所にファイルを保存します。
9. プライマリ マネージャにログインします。手順 2 ～ 8 を繰り返して、プライマリ マネージャのバックアップ設定ファイルを保存します。

2. マネージャ データベースのバックアップ

マネージャ データベースをリモートファイルシステムにバックアップするには、集中管理およびアプライアンス管理インターフェイスを使用します。

1. データベースのスナップショットの削除
2. データベースのバックアップ
3. データベースのスナップショットの削除
4. データベースのバックアップの確認

> ⚠ プライマリ マネージャおよびセカンダリ マネージャで、データベースをバックアップする手順が完了していることを確認してください。

1. データベースのスナップショットの削除

バックアップファイルを作成する前に、次の手順を使用して、マネージャ データベースに保存されているスナップショットをすべて削除します。

> ⚠ マネージャ データベースのスナップショットは必ず削除してください。これは、バックアップを成功させるために不可欠な手順です。

1. **管理者**としてマネージャ アプライアンスコンソールにログインします。
2. **スナップショットの確認**：次のように入力します。

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from database_snapshots;"
   ```

3. **スナップショット（存在する場合）の削除**：次のように入力します。

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_database_snapshot('StealthWatchSnap1');"
   ```

4. **スナップショットフォルダが削除されるまで待機**：次を確認します。

   ```
   ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
   ```

   結果が空でない場合は、そのまま待機します。データベースのサイズによっては、フォルダが削除されるまで数分かかる場合があります。

5. 手順 1 ～ 4 を繰り返し、保存されているマネージャ データベースのスナップショットをすべて削除します。

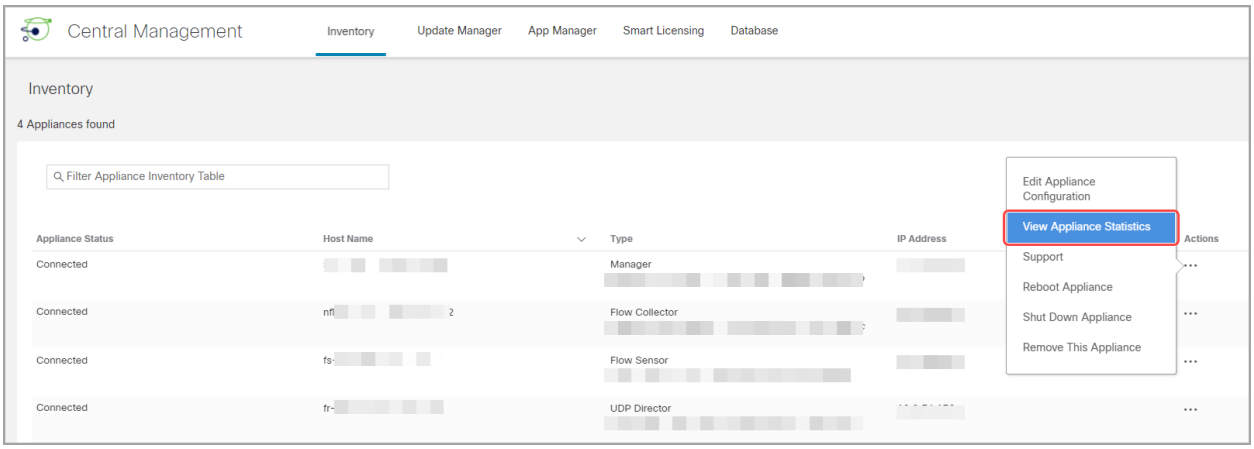
2. データベースのバックアップ

次の手順を使用して、マネージャ データベースをバックアップします。また、次の情報を確認してください。

- 領域：リモート ファイル システムに、データベースのバックアップを保存するための十分な空き領域があることを確認します。
- **時間**：データベースを 1 回バックアップすると、以後は前回のバックアップからの変更点だけがバックアップされるため、バックアップにかかる時間は短くなります。このプロセスでは、1 分あたり約 0.5 GB ～ 2 GB のデータがバックアップされます。

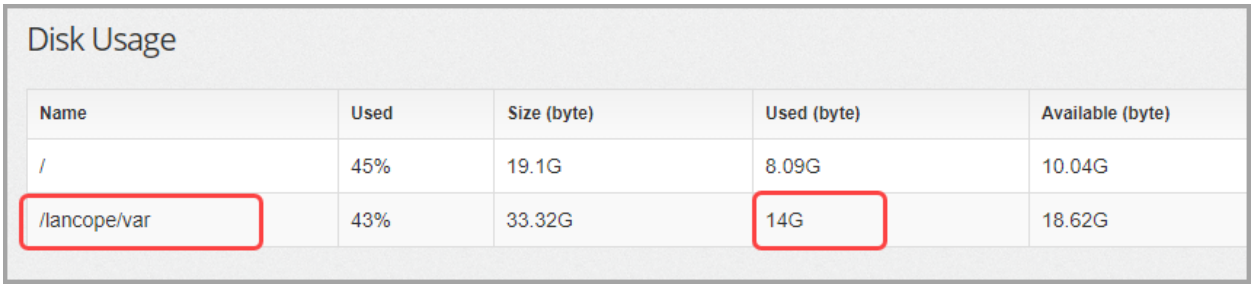
1. マネージャ アプライアンス管理インターフェイスにログインします。

   集中管理で、[マネージャ ••• ([省略記号（Ellipsis）]) アイコン] > **[アプライアンス統計の表示（View Appliance Statistics）]** をクリックします。

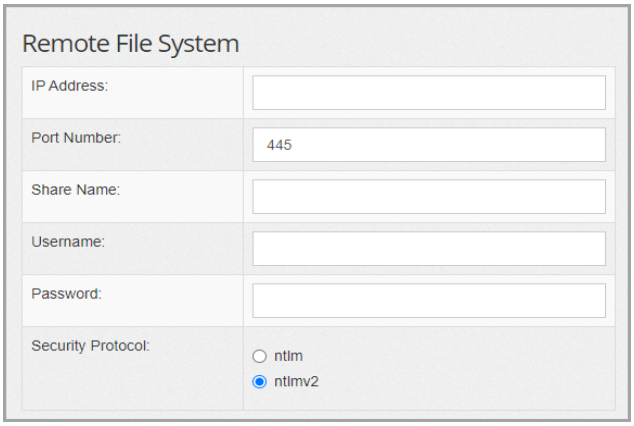


2. 次の手順を実行して、リモート ファイル システム上に必要となるデータベース バックアップ保存容量を確認します。

   - [ホーム(Home)] をクリックします。
   - [ディスク使用量(Disk Usage)] セクションを見つけます。
   - **/lancope/var** ファイルシステムの [Used (byte)] 列を確認します。データベースのバックアップを保存するためには、リモート ファイル システム上に少なくともこの数値にその 15% を足した分の空き容量が必要です。



3. [設定(Configuration)] > [リモートファイルシステム(Remote File System)] の順にクリックします。



4. バックアップ ファイルを保存するリモート ファイル システムの設定を使用して、フィールドに入力します。

   Secure Network Analytics ファイル共有では、CIFS（Common Internet File System）、別名 SMB（Server Message Block）というプロトコルを使用します。

5. [適用（Apply）] をクリックして、設定ファイルに設定を適用します。

   パスワードを入力しても [適用（Apply）] ボタンが有効にならない場合、[リモートファイルシステム（Remote File System）] ページの空白部分を 1 回クリックすると有効になります。

6. **[テスト（Test）]** をクリックして、Secure Network Analytics アプライアンスとリモートファイルシステムが相互に通信できることを確認します。

   テストが完了したら、[リモートファイルシステム（Remote File System）] ページの下部に次のメッセージが表示されていることを確認します。

   File sharing appears to be properly configured.

7. [サポート（Support）] > [データベースのバックアップおよび復元（Backup/Restore Database）] の順にクリックします。
8. [バックアップの作成（Create Backup）] をクリックします。このプロセスは長時間かかる場合があります。

   - バックアップ プロセスの開始後は、マウスをページから離してもプロセスは中断されません。ただし、バックアップの実行中に、[キャンセル（Cancel）] をクリックすると、アプライアンスを再起動しないとバックアップを再開できなくなる場合があります。
   - バックアップが完了するまで、画面に表示される指示に従います。
   - バックアッププロセスの詳細を確認するには、[ログの表示（View Log）] をクリックします。

9. [閉じる（Close）] をクリックして進捗状況ウィンドウを閉じます。

> 終了する前にバックアップをキャンセルする場合は、必ずデータベースのスナップショットを削除してください。手順については、「**3. データベースのスナップショットの削除**」を参照してください。

3. データベースのスナップショットの削除

バックアップファイルを保存した後、次の手順を使用して、マネージャ データベースのスナップショットを削除します。

> マネージャ データベースのスナップショットは必ず削除してください。

1. **管理者**としてマネージャ アプライアンスコンソールにログインします。
2. **スナップショットの確認**：次のように入力します。

```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from
database_snapshots;"
```

3. **スナップショット（存在する場合）の削除**：次のように入力します。

```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_
database_snapshot('StealthWatchSnap1');"
```

4. **スナップショットフォルダが削除されるまで待機**：次を確認します。

```
ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
```

結果が空でない場合は、そのまま待機します。データベースのサイズによっては、フォルダが削除されるまで数分かかる場合があります。

5. 手順 1 ～ 4 を繰り返し、保存されているマネージャ データベースのスナップショットをすべて削除します。

4. データベースのバックアップの確認

「2. マネージャ データベースのバックアップ」の手順を繰り返し、各マネージャのデータベースのバックアップを保存したことを確認します。

3. 信頼ストアへの証明書の追加

次の手順を使用して、必要なアプライアンス アイデンティティ証明書とチェーンを信頼ストアに保存します。

信頼ストアの要件

この手順では、次の要件について説明します。

- セカンダリ マネージャ証明書の、プライマリ マネージャ信頼ストアへの追加。
- プライマリ マネージャ証明書の、セカンダリ マネージャ信頼ストアへの追加。

証明書チェーン（Certificate Chain）

アプライアンス アイデンティティ証明書に証明書チェーンが含まれている場合、信頼ストアに証明書チェーン（ルートおよび中間）を必ず追加してください。

信頼ストアへの証明書のアップロード

各ファイルを個別にアップロードします。

1. アプライアンス アイデンティティ証明書のダウンロード

次の手順を使用して、アプライアンス アイデンティティ証明書をダウンロードして保存します。手順は、使用しているブラウザによって異なります。

証明書がすでに保存されている場合は、この手順をスキップできます。「**2. マネージャ信頼ストアへの証明書の追加**」に進んでください。

> ブラウザのロックまたはセキュリティアイコンをクリックすることもできます。画面に表示される指示に従って証明書をダウンロードします。手順は、使用しているブラウザによって異なります。

1. ブラウザのアドレスバーで、IP アドレスの後のパスを **/secrets/v1/server-identity** に置き換えます。

   例：https://<IPaddress>/secrets/v1/server-identity

2. 画面に表示される指示に従って証明書を保存します。

   オープン：ファイルを表示するには、テキストファイル形式を選択します。

   トラブルシューティング：証明書をダウンロードするためのプロンプトが表示されない場合は、自動的にダウンロードされている場合があるため、[ダウンロード（Downloads）] フォルダを確認するか、別のブラウザを試します。

3. 各マネージャで、手順 1 と 2 を繰り返します。

2. マネージャ信頼ストアへの証明書の追加

次の手順を使用して、セカンダリ マネージャ アプライアンスのアイデンティティ証明書とチェーン（該当する場合）を、プライマリ マネージャ信頼ストアに保存します。

1. マネージャにログインします。
2. メインメニューから **[構成（Configure）]** > **[グローバル集中管理（GLOBAL Central Management）]** を選択します。
3. [アプライアンスステータス（Appliance Status）] が [接続済み（Connected）] と表示されていることを確認します。
4. マネージャの **[アクション（Action）]** 列にある ••• （[省略記号（Ellipsis）]）アイコンをクリックします。
5. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
6. **[全般（General）]** タブをクリックし、**[信頼ストア（Trust Store）]** セクションを見つけます。
7. [新規追加（Add New）] をクリックします。

> ⚠ 各アプライアンス アイデンティティ証明書とチェーン（ルートおよび中間）証明書を個別にアップロードしていることを確認します。

8. [フレンドリ名（Friendly Name）] フィールドに、証明書の名前を入力します。
9. [ファイルの選択（Choose File）] をクリックします。証明書を選択します。
10. [証明書の追加（Add Certificate）] をクリックします。[信頼ストア（Trust Store）] リストに証明書が表示されていることを確認します。
11. 手順 6 ～ 9 を繰り返して、他の必要な証明書を信頼ストアに追加します。

    - セカンダリ マネージャにログインしている場合は、プライマリ マネージャ証明書を追加します。
    - プライマリ マネージャにログインしている場合は、セカンダリ マネージャ証明書を追加します。

12. [設定の適用（Apply settings）] をクリックします。画面に表示される指示に従って操作します。
13. **[接続済み（Connected）]**：[集中管理インベントリ（Central Management Inventory）] ページで、アプライアンスのステータスが [接続済み（Connected）] に戻っていることを確認します。
14. もう一方のマネージャで手順 1 ～ 13 を繰り返します。

データストア初期化後のフェールオーバーの設定

Data Store を使用して Cisco Secure Network Analytics を展開した場合は、Data Store を初期化する前にフェールオーバーを設定してください。Data Store を初期化した後にフェールオーバーを設定する場合は、以下のセクションの手順に従って、Data Store とのセキュア通信のためにセカンダリ Manager を設定します。

Data Store 初期化後にフェールオーバーを設定するプロセスの概要を以下に示します。

1. フェールオーバーペアを設定します。
2. セカンダリマネージャを追加します。

フェールオーバーペアの設定

このガイドの「**4. フェールオーバーペアの設定**」セクションの指示にしたがって、フェールオーバーペアを設定します。このプロセスが完了すると、セカンダリ マネージャの集中管理インベントリに「データストアが設定されていません」というメッセージが表示されます。セカンダリ マネージャを設定するには、「**データストアの初期化後のマネージャの追加**」にしたがってください。

データストアの初期化後のマネージャの追加

Data Store をすでに初期化している場合は、次の手順に従って Data Store に Manager を追加します。

データストアなしで使用するように設定した既存の マネージャ または Flow Collector がある場合は、各アプライアンスを工場出荷時のデフォルトにリセット（RFD）してから、データストアありで使用するように設定して展開に追加する必要があります。

1. **RFD**：『Cisco Secure Network Analytics システム設定ガイド』の「工場出荷時のデフォルトへのリセット」セクションの指示に従ってください。

> 現在のネットワーク設定を保持するか破棄するかを選択できます。破棄する場合は、それらのネットワーク設定を再設定する必要があります。

2. 「1. Configuring Your Environment using First Time Setup」と「2. Configuring the Managed System」（『Secure Network Analytics System Configuration Guide』に記載）の手順に従って、アプライアンスを設定し Central Management に追加します。初回セットアップでアプライアンスを設定します。
3. ルートとしてプライマリ マネージャ アプライアンスコンソールにログインします。
4. `SystemConfig` と入力して、Enter キーを押します。
5. [データストア（Data Store）] を選択します。
6. [SSH] を選択します。アプライアンス間で SSH が有効になるまで待ちます。
7. [Data Store] メニューから [新しいアプライアンス（New Appliances）] を選択します。画面に表示される指示に従って操作します。
8. SystemConfig を終了します。

> [データストア（Data Store）] メニューを終了すると、システムで以前の SSH 設定が復元されます。

9. Central Management をチェックして、アプライアンスのステータスが［接続済み（Connected）］になっていることを確認します。

4. フェールオーバーペアの設定

次の手順を使用して、マネージャのフェールオーバーを設定します。フェールオーバー設定を保存すると、セカンダリ マネージャのドメイン設定が削除されます。そして読み取り専用になり、プライマリ マネージャと同期します。詳細については、「**フェールオーバー設定の保存**」を参照してください。

始める前に

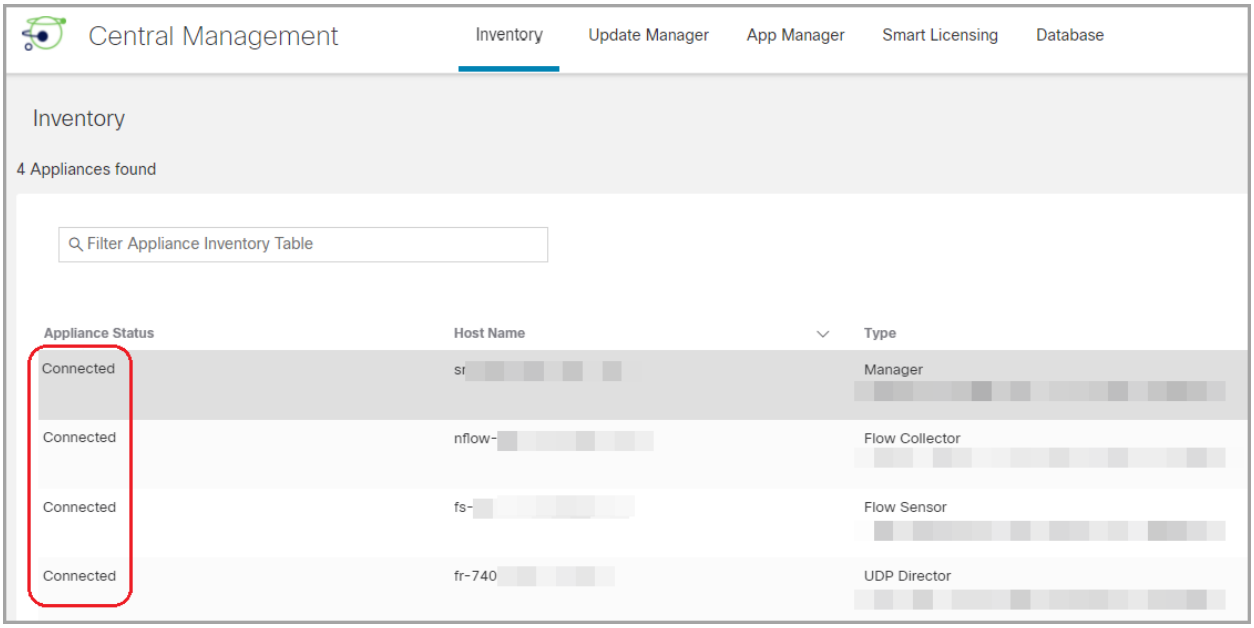
これらの手順を開始する前に、次の手順を完了してください。

1. **フェールオーバーロールの計画**
2. **マネージャの設定とデータベースのバックアップ**
3. **信頼ストアへの証明書の追加**

> ⚠ プライマリ マネージャを設定する前に、必ずセカンダリ マネージャのフェールオーバーを設定してください。フェールオーバー設定を保存すると、セカンダリ マネージャのドメイン設定が削除されるため、手順を順番に実行してください。

1. マネージャ アプライアンスのステータスの確認

1. **プライマリ** マネージャにログインします。
2. メインメニューから **[構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)]** を選択します。
3. 各アプライアンスの [アプライアンスステータス(Appliance Status)] が [接続済み(connected)] と表示されていることを確認します。

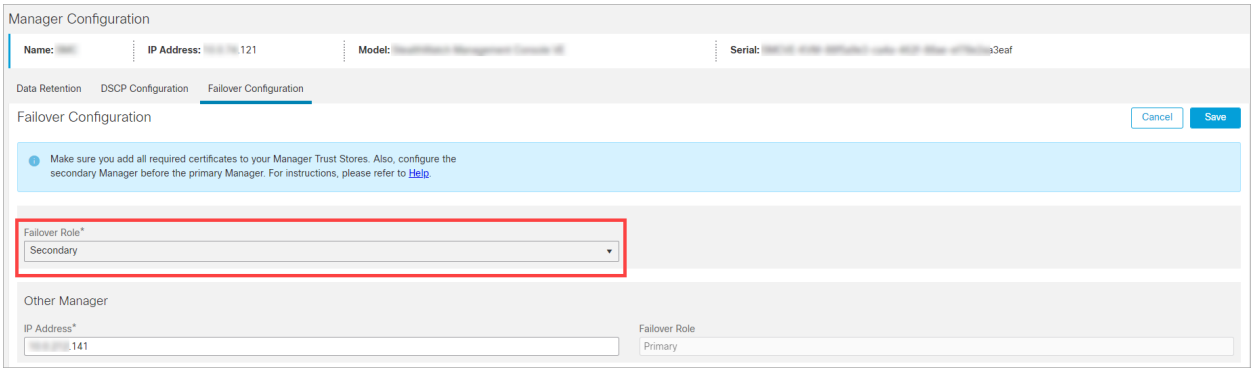


4. **セカンダリ** マネージャにログインします。
5. メインメニューから **[構成(Configure)]** > **[グローバル集中管理(GLOBAL Central Management)]** を選択します。
6. [アプライアンスステータス(Appliance Status)] が [接続済み(Connected)] と表示されていることを確認します。
7. 両方のマネージャにログインしたまま、次の手順に進みます。

2. セカンダリ マネージャの設定

フェールオーバー設定を保存すると、セカンダリ マネージャのドメイン設定が削除されます。そして読み取り専用になり、プライマリ マネージャと同期します。詳細については、「**フェールオーバー設定の保存**」を参照してください。

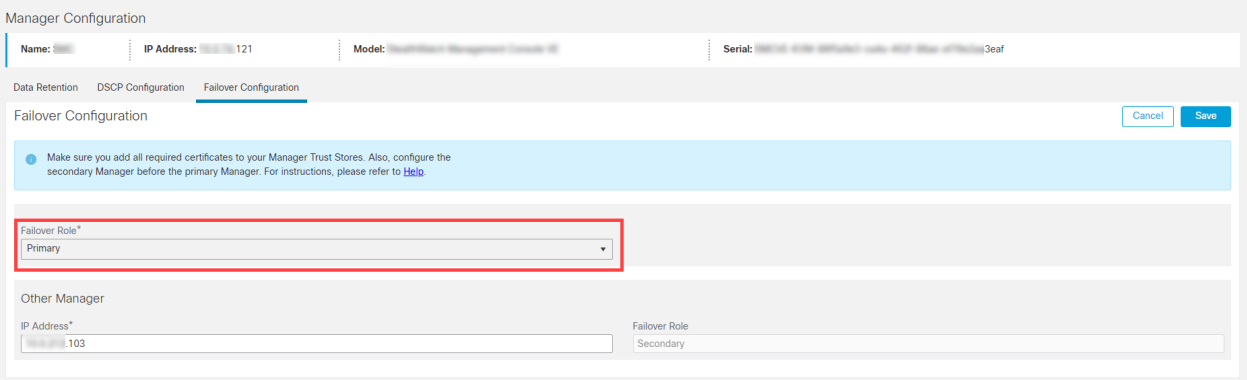
1. **セカンダリ** マネージャで、**[セキュリティ インサイト ダッシュボード(Security Insight dashboard)]** タブをクリックします。
2. メインメニューから **[構成(Configure)]** > **[グローバルマネージャ(GLOBAL Manager)]** を選択します。
3. [フェールオーバー設定(Failover Configuration)] タブをクリックします。
4. [フェールオーバーロール(Failover Role)] ドロップダウンメニューをクリックします。[セカンダリ(Secondary)] を選択します。



5. **[IPアドレス(IP Address)]** フィールドに、その他のマネージャの IP アドレスを入力します。これがプライマリ マネージャになります。
6. [保存(Save)] をクリックします。
7. 画面に表示される指示に従って、変更を保存します。

3. プライマリ マネージャの設定

1. **プライマリ** マネージャで、**[セキュリティ インサイト ダッシュボード(Security Insight dashboard)]** タブをクリックします。
2. メインメニューから **[構成(Configure)]** > **[グローバルマネージャ(GLOBAL Manager)]** を選択します。
3. [フェールオーバー(Failover)] タブをクリックします。
4. [フェールオーバーロール(Failover Role)] ドロップダウンメニューをクリックします。[プライマリ(Primary)] を選択します。



5. **[IPアドレス(IP Address)]** フィールドに、セカンダリ マネージャの IP アドレスを入力します。
6. [保存(Save)] をクリックします。
7. 画面に表示される指示に従って、変更を保存します。

5. フェールオーバー設定の確認

次の手順を使用して、マネージャのフェールオーバーが設定され通信していることを確認します。

1. 設定の変更の確認

プライマリ マネージャにフェールオーバーの設定変更が表示されていることを確認します。各アプライアンスの [アプライアンスステータス(Appliance Status)] に [接続済み(connected)] と表示されていることも確認します。

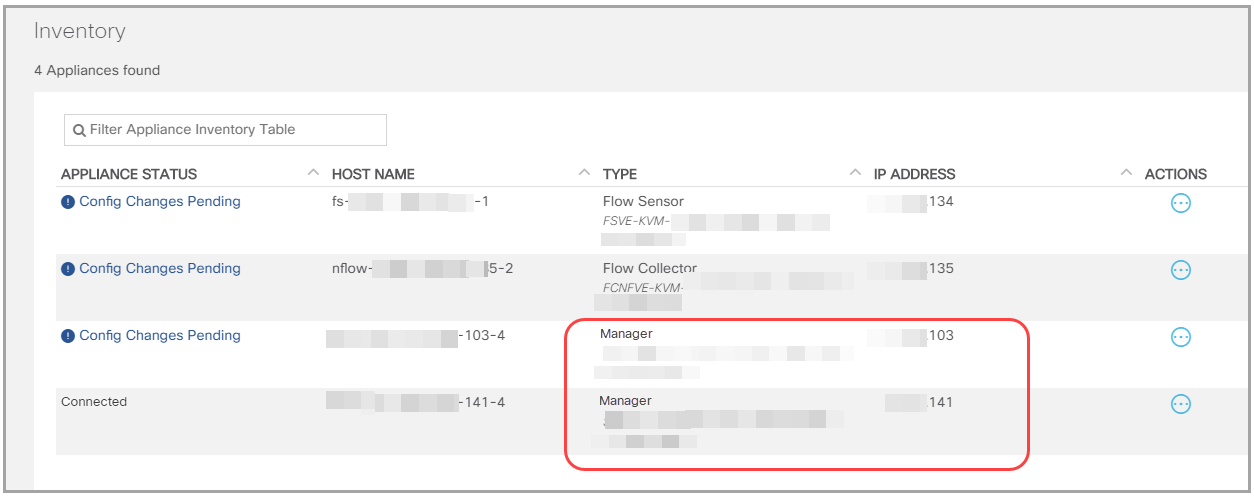
1. プライマリ マネージャで、[集中管理(Central Management)] を開きます。

   [構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。

2. 次を確認します。

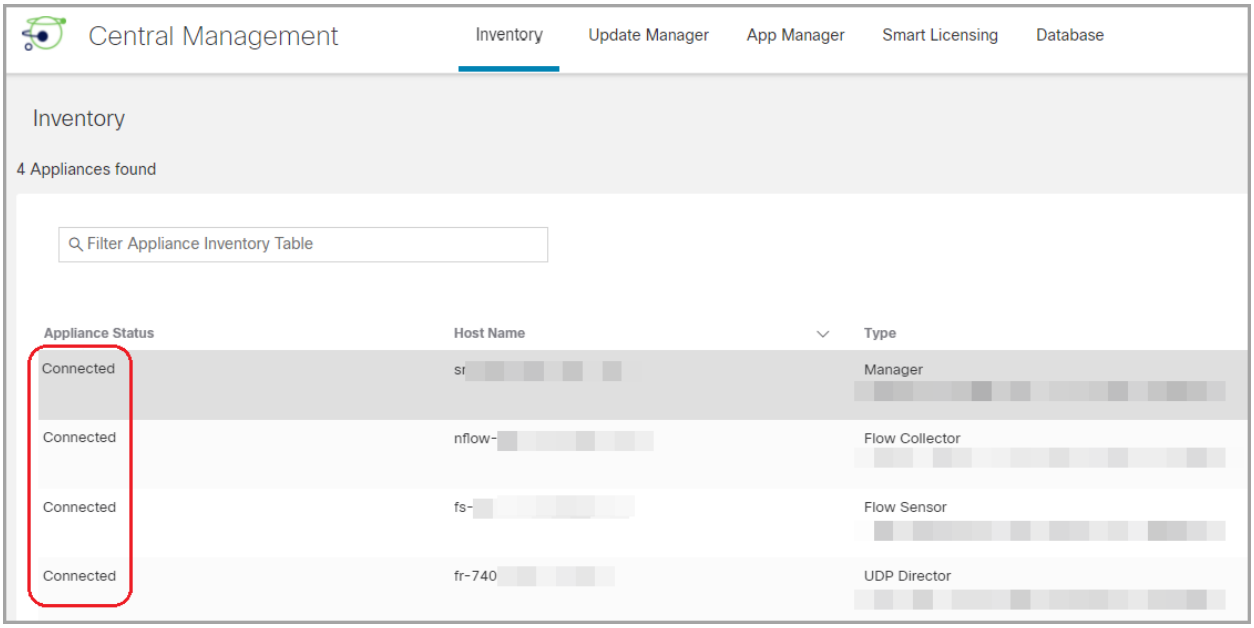
   - セカンダリ マネージャがインベントリに表示されます。
   - 各アプライアンスの [アプライアンスステータス(Appliance Status)] に [接続済み(connected)] と表示されていること。

プライマリおよびセカンダリ マネージャの表示の確認



[集中管理(Central Management)] が更新されるまで待ちます。アプライアンスの [アプライアンスステータス(Appliance Status)] に [設定の変更が保留中(Config Changes Pending)] と表示されます。

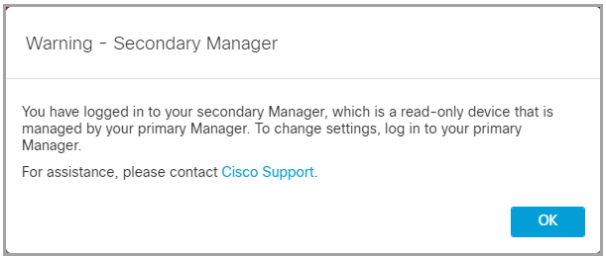
すべてのアプライアンスが [接続済み（connected）] になっていることの確認



2. フローコレクションの確認

次の手順を使用して、セカンダリ マネージャが読み取り専用で稼働しており、フローを受信していることを確認します。

1. **セカンダリ マネージャ** にログインします。
2. マネージャは読み取り専用ですという通知が表示されます。セカンダリ マネージャが読み取り専用に変更されていない場合は、フェールオーバー設定を確認してください。



3. [セキュリティ分析ダッシュボード（Security Insight Dashboard）] で、フロー コレクション トレンドを確認します。

4. フロー コレクションが進行中の場合、アクションは不要です。フェールオーバー設定が完了しました。

   フロー収集が停止した場合は、集中管理を使用して Flow Collector とセカンダリ マネージャを次の順序で再起動します（または**トラブルシューティング**を参照してください）。

   - プライマリマネージャにログインします。
   - メインメニューから **[構成（Configure）]** > **[グローバル集中管理（GLOBAL Central Management）]** を選択します。
   - Flow Collector を見つけます。
   - **[アクション（Actions）]** 列の ••• （[省略記号（Ellipsis）]）アイコンをクリックします。
   - [アプライアンスの再起動（Reboot Appliance）] を選択します。画面に表示される指示に従って操作します。
   - **Flow Collector**：これらの手順を繰り返し、[集中管理（Central Management）] ですべての Flow Collector を再起動します。
   - **セカンダリ マネージャ**：これらの手順を繰り返し、セカンダリ マネージャを再起動します。

⚠ 再起動によってプライマリ マネージャがオフラインになった場合、アプライアンスのステータスが [接続済み（Connected）] に戻り、セカンダリ マネージャが検出されると、プライマリのフェールオーバーロールが再開されます。プライマリ マネージャのロールがセカンダリに変更され、それ自体が解決されない場合は、「**トラブルシューティング**」を参照してください。

フェールオーバーロールの変更

次の手順を使用して、プライマリおよびセカンダリ マネージャのロールを変更します。ロールは自動的には交換されないことに注意してください。

> ⚠ フェールオーバー設定を変更すると、セカンダリ マネージャのドメイン設定が削除されるため、手順を順番に実行してください。

[Time]

セカンダリ マネージャをプライマリに昇格させると、すべてのアプライアンスのステータスが **[構成チャネルのダウン(Config Channel Down)]** から **[接続済み(Connected)]** に変わるまでに少なくとも 1 時間かかることがあります。[集中管理(Central Management)] でステータスをモニターします。詳細については、「**5. フェールオーバー設定の確認**」を参照してください。

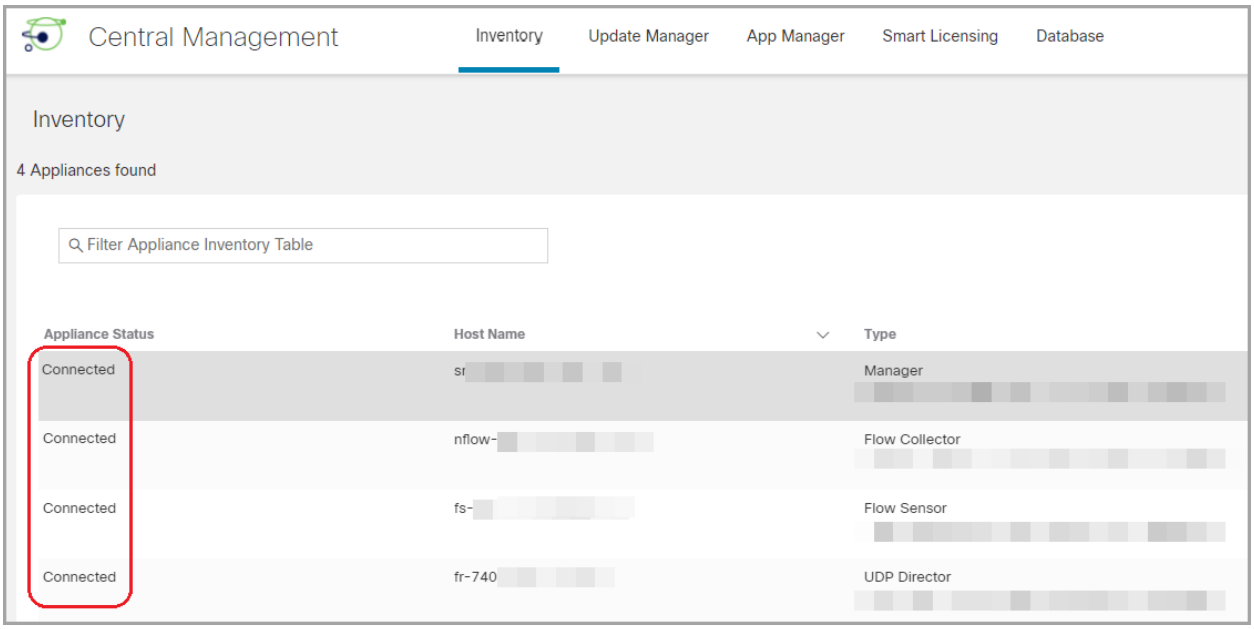
1. プライマリ マネージャのバックアップ

フェールオーバーロールを変更する前に、今後設定を復元する必要がある場合に備えてプライマリ マネージャをバックアップします。詳細については、「**2. マネージャの設定とデータベースのバックアップ**」を参照してください。

2. アプライアンスステータスの確認

1. プライマリマネージャにログインします。
2. メインメニューから **[構成(Configure)]** > **[グローバル集中管理(GLOBAL Central Management)]** を選択します。
3. 各アプライアンスの [アプライアンスステータス(Appliance Status)] が [接続済み(connected)] と表示されていることを確認します。

   - **マネージャ**:プライマリまたはセカンダリ マネージャのアプライアンスステータスが [構成チャネルのダウン(Config Channel Down)] になっている場合は、通信設定を確認し、「**トラブルシューティング**」を参照してください。
   - **その他のアプライアンス**:Flow Collector 、データノード、フローセンサー、または UDP Director のアプライアンスのステータスが [構成チャネルのダウン(Config Channel Down)] になっている場合は、構成設定を確認し、集中管理を使用してアプライアンスを再起動します(••• ([省略記号(Ellipsis)]) アイコン > **[アプライアンスの再起動(Reboot Appliance)]**)。その他のトラブルシューティングについては、『Cisco Secure Network Analytics システム設定ガイド』を参照してください。



3. フェールオーバー設定の変更

プライマリ マネージャをセカンダリに変更し、セカンダリ マネージャをプライマリに昇格させるには、次の手順を使用します。

この構成では、プライマリ マネージャがセカンダリ マネージャになり、そのドメイン設定は削除されます。そして読み取り専用になり、新しく昇格したプライマリ マネージャと同期します。詳細については、「**フェールオーバー設定の保存**」を参照してください。

> ⚠ フェールオーバー設定の変更が完了するまで、[集中管理(Central Management)] でアプライアンスを追加または削除しないでください。

1. プライマリ マネージャのセカンダリへの変更

1. 現在の**プライマリ** マネージャで、**[セキュリティ インサイト ダッシュボード(Security Insight dashboard)]** タブをクリックします。
2. メインメニューから **[構成(Configure)]** > **[グローバルマネージャ(GLOBAL Manager)]** を選択します。
3. [フェールオーバー設定(Failover Configuration)] タブをクリックします。
4. [フェールオーバーロール(Failover Role)] が [プライマリ(Primary)] と表示されていることを確認します。

   プライマリ マネージャがセカンダリとして表示される場合は、「トラブルシューティング」を参照してください。

5. [フェールオーバーロール(Failover Role)] ドロップダウンメニューをクリックします。[セカンダリ(Secondary)] を選択します。
6. [保存(Save)] をクリックします。
7. 画面に表示される指示に従って、変更を保存します。

2. セカンダリ マネージャのプライマリへの変更

1. **セカンダリ** マネージャにログインします。
2. メインメニューから **[構成(Configure)]** > **[グローバルマネージャ(GLOBAL Manager)]** を選択します。
3. [フェールオーバー設定(Failover Configuration)] タブをクリックします。
4. フェールオーバーロールがセカンダリとして表示されていることを確認します。
5. [フェールオーバーロール(Failover Role)] ドロップダウンメニューをクリックします。[プライマリ(Primary)] を選択します。
6. [保存(Save)] をクリックします。
7. 画面に表示される指示に従って、変更を保存します。

4. 設定の変更の確認

フェールオーバー設定の変更を確認するには、「**5. フェールオーバー設定の確認**」に進み、手順に従います。

ネットワーク インターフェイスの変更

マネージャがフェールオーバー用に設定されている場合は、アプライアンスのネットワーク インターフェイス、ホスト名、またはネットワークドメイン名を変更する前に、フェールオーバー関係を削除します。全体的な手順は次のとおりです。

> ⚠ フェールオーバー設定を削除すると、セカンダリ マネージャからすべてのドメイン設定データが削除されます。すべての手順を順番に実行してください。

1. フェールオーバー設定の削除

手順については、「**フェールオーバーの設定の削除**」を参照してください。

2. マネージャのネットワーク インターフェイスの変更

管理対象アプライアンスの SSL/TLS 証明書ガイド [英語] の手順に従います。

手順の一環として、アプライアンスを Central Management から一時的に削除します。アプライアンス アイデンティティ証明書が自動的に置き換えられます。

> アプライアンス アイデンティティ証明書は、この手順の一環として自動的に置き換えられます。
>
> ⚠ **アプライアンスがカスタム証明書を使用している場合は、**これらの設定の変更についてシスコサポートにお問い合わせください。次に示す手順を使用しないでください。カスタム証明書と秘密キーのコピーがあることを確認してください。

3. マネージャ フェールオーバーの設定

このガイドの手順に従い、フェールオーバーを設定します。マネージャをバックアップし、新しい証明書をマネージャ信頼ストアに追加してください。

フェールオーバーの設定の削除

フェールオーバー設定を削除する前に、両方のマネージャのステータスを確認し、手順を順番に実行してください。

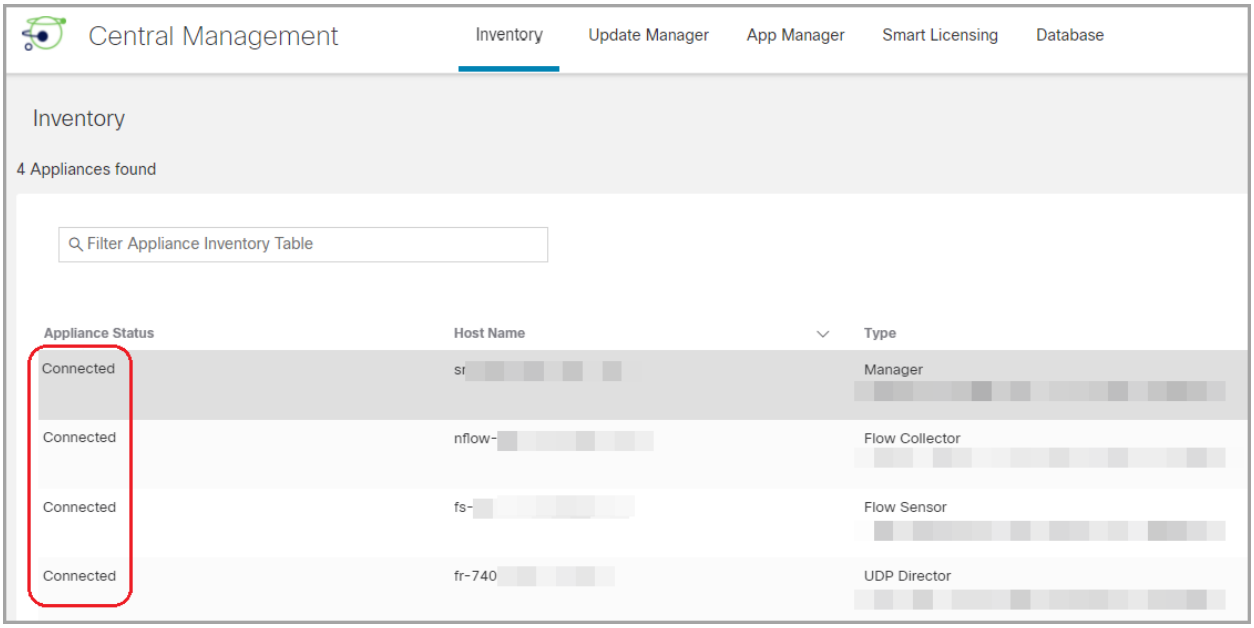
> ⚠ フェールオーバー設定を削除すると、セカンダリ マネージャからすべてのドメイン設定データが削除されます。

1. アプライアンス ステータスの確認

開始する前に、プライマリ マネージャがセカンダリ マネージャを管理対象アプライアンスとして表示していることを確認し、両方のマネージャが [接続済み(Connected)] になっていることを確認します。

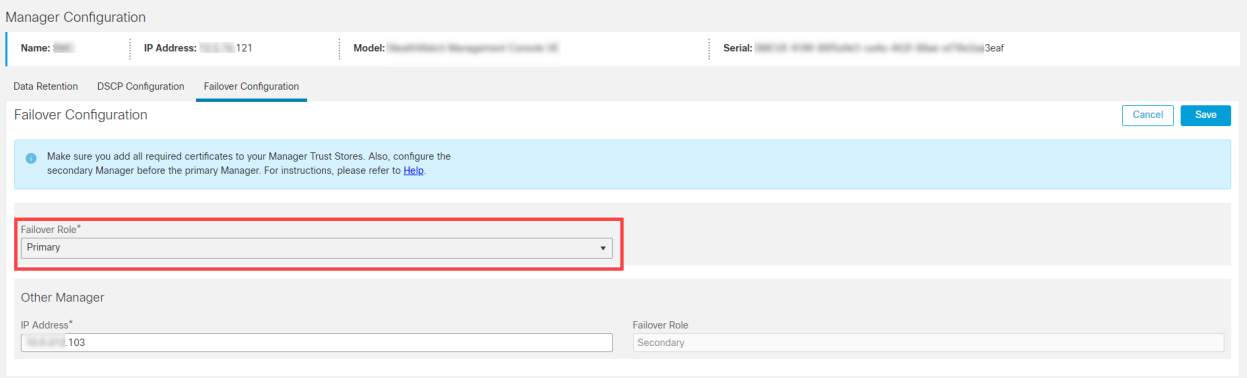
1. **プライマリ** マネージャにログインします。
2. **[構成(Configure)]** > **[グローバル集中管理(GLOBAL Central Management)]** を選択します。
3. 各アプライアンスの [アプライアンスステータス(Appliance Status)] が [接続済み(connected)] と表示されていることを確認します。

   - **マネージャ**:プライマリまたはセカンダリ マネージャのアプライアンスステータスが [構成チャネルのダウン(Config Channel Down)] になっている場合は、通信設定を確認し、「トラブルシューティング」を参照してください。
   - **その他のアプライアンス**:Flow Collector 、フローセンサー、または UDP Director のアプライアンスのステータスが [構成チャネルのダウン(Config Channel Down)] になっている場合は、構成設定を確認し、集中管理を使用してアプライアンスを再起動します(**[省略記号(Ellipsis)]アイコン** > **[アプライアンスの再起動(Reboot Appliance)]**)。その他のトラブルシューティングについては、『Cisco Secure Network Analytics システム設定ガイド』を参照してください。



2. フェールオーバーロールの確認

1. **プライマリ** マネージャで、**[セキュリティ インサイト ダッシュボード(Security Insight dashboard)]** タブをクリックします。
2. メインメニューから **[構成(Configure)]** > **[グローバルマネージャ(GLOBAL Manager)]** を選択します。
3. [フェールオーバー設定(Failover Configuration)] タブをクリックします。
4. [フェールオーバーロール(Failover Role)] が [プライマリ(Primary)] と表示されていることを確認します。



5. **セカンダリ** マネージャにログインします。手順 1 ～ 4 に従って、[フェールオーバーロール(Failover Role)] が [セカンダリ(Secondary)] として表示されていることを確認します。

   - 各マネージャのフェールオーバーロールが正しい場合は、両方のマネージャの [フェールオーバー設定(Failover Configuration)] タブを開いたままにし、「**3. フェールオーバー設定の削除**」に進みます。
   - マネージャが両方ともセカンダリと表示される場合、削除を進める前にフェールオーバー設定を更新し、1 つがプライマリ マネージャ 、1 つがセカンダリ マネージャになるようにします。手順については、「**フェールオーバーロールの変更**」を参照してください。

> ⚠ 「**フェールオーバーロールの変更**」の設定順序と手順に必ずしたがってください。サポートが必要な場合は、シスコサポートまでお問い合わせください。

3. フェールオーバー設定の削除

次の手順を使用して、フェールオーバー設定を削除します。次の手順を順番に実行してください。

> ⚠ フェールオーバー設定を削除すると、セカンダリ マネージャからすべてのドメイン設定データが削除されます。

1. **プライマリ** マネージャの **[フェールオーバー設定(Failover Configuration)]** タブに移動します。
2. [削除(Delete)] をクリックします。
3. 画面の指示に従って、フェールオーバー設定を削除します。

⚠ フェールオーバー設定を削除すると、セカンダリ マネージャからすべてのドメイン設定データが削除されます。

4. **セカンダリ** マネージャの **[フェールオーバー設定(Failover Configuration)]** タブに移動します。
5. [削除(Delete)] をクリックします。
6. 画面の指示に従って、フェールオーバー設定を削除します。

4. セカンダリ マネージャを [集中管理(Central Management)] から削除します。

1. **プライマリ** マネージャで、[集中管理(Central Management)] を開きます。

   [構成(Configure)] > **[グローバル集中管理(GLOBAL Central Management)]** を選択します。

2. **セカンダリ** マネージャを見つけます。

⚠ 削除する前に、セカンダリ マネージャの IP アドレスを確認します。

3. ••• ([省略記号(Ellipsis)]) アイコンをクリックします。[このアプライアンスを削除(Remove This Appliance)] を選択します。
4. 画面の指示にしたがって、[集中管理(Central Management)] からセカンダリ マネージャを削除します。

5. セカンダリ マネージャ証明書の削除

次の手順を使用して、他方のアプライアンスの信頼ストアからセカンダリ マネージャ証明書を削除します。

⚠ 証明書を削除する前に、セカンダリ マネージャの IP アドレスを確認します。

1. プライマリ マネージャの [集中管理(Central Management)] に戻ります。次を確認します。

   - セカンダリ マネージャがインベントリに表示されなくなります。
   - 各アプライアンスの [アプライアンスステータス(Appliance Status)] に [接続済み(Connected)] と表示されていること。

2. アプライアンスの ••• ([省略記号(Ellipsis)]) アイコンをクリックします。
3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
4. [全般(General)] タブをクリックします。[信頼ストア(Trust Store)] セクションを見つけます。
5. セカンダリ マネージャ証明書を見つけます。
6. **[削除(Delete)]** をクリックして、信頼ストアから各セカンダリ マネージャ証明書を削除します。
7. [集中管理(Central Management)] の各アプライアンスに対して手順 2 ～ 6 を繰り返します。

6. セカンダリ マネージャの工場出荷時のデフォルトへのリセット

セカンダリ マネージャを使用するには、工場出荷時のデフォルトにリセットします。『Cisco Secure Network Analytics システム設定ガイド』の指示にしたがってください。

この手順では、次の手順を実行します。

- アプライアンスを工場出荷時の初期状態にリセットする。
- IP アドレスを設定する。
- アプライアンス セットアップ ツールを使用してマネージャを設定する。

トラブルシューティング

マネージャがオフラインになる、または失敗する

ネットワークがダウンしている場合、マネージャをシャットダウンして再起動した場合、またはその他のさまざまな理由で、プライマリ マネージャがオフラインになる場合があります。

再起動によってプライマリ マネージャがオフラインになった場合、アプライアンスのステータスが [接続済み(Connected)] に戻り、セカンダリ マネージャが検出されると、プライマリのフェールオーバーロールが再開されます。

プライマリ マネージャのロールがセカンダリに変更され、それ自体が解決しない場合は、次のシナリオを確認して必要な作業を判断してください。

> サポートが必要な場合は、シスコサポートまでお問い合わせください。

次の場合...	結合できるフィールド	次の操作
プライマリ マネージャが失敗するか、シャットダウンして再起動する。	既存のセカンダリ マネージャを手動でプライマリに昇格させ、それがオンラインである。	新しいプライマリ マネージャは、プライマリとしてそのロールを維持します。再起動すると、元のプライマリ マネージャが自動的にセカンダリとしての新しいロールを担います。
プライマリ マネージャが失敗するか、シャットダウンして再起動する。	既存のセカンダリ マネージャを手動でプライマリに昇格させていないため、オンラインになっているプライマリ マネージャがない。	元のプライマリ マネージャを再起動すると、それと元のセカンダリ マネージャの両方がセカンダリのロールになります。どちらかをプライマリ マネージャに昇格させてください。手順については、「**フェールオーバーロールの変更**」を参照してください。
ネットワークが停止し、復元されました。	既存のセカンダリ マネージャを手動でプライマリに昇格させ、それがオンラインである。	新しいプライマリ マネージャは、プライマリとしてそのロールを維持します。再起動すると、元のプライマリ マネージャが自動的にセカンダリとしての新しいロールを担います。
ネットワークが停止し、復元されました。	既存のセカンダリ マネージャを手動でプライマリに昇格させていないため、オンラインになっているプライマリ マネージャがない。	元のプライマリ マネージャがプライマリとしてのロールを自動的に再開し、元のセカンダリ マネージャは自動的にセカンダリ マネージャとしてのロールを再開します。

信頼エラー

マネージャが信頼されていないというエラーが表示された場合は、信頼ストアの証明書を確認します。手順については、「**3. 信頼ストアへの証明書の追加**」を参照してください。

フローがセカンダリ マネージャに表示されない

セカンダリ マネージャにフローが表示されない場合、セカンダリ マネージャの証明書が Flow Collector 信頼ストアに保存されていることを確認してください。手順については、「**3. 信頼ストアへの証明書の追加**」を参照してください。

パスワードの有効期限

フェールオーバー設定を保存すると、プライマリ マネージャがローカルユーザーとパスワードのログイン情報をセカンダリ マネージャにプッシュするため、それらは同期されます。これは、同じパスワードを使用してプライマリにログインすることを意味しますマネージャおよび二次。セカンダリ マネージャのパスワードを変更するには、プライマリ マネージャにログインします。

プライマリ マネージャがダウンしていてパスワードの有効期限が切れている場合、セカンダリ マネージャを使用してパスワードを変更することはできません。この場合、プライマリ マネージャのアプライアンスのステータスが [接続済み(Connected)] に戻るまで待つと、パスワードを変更できます。

- パスワードをデフォルトにリセットするには、『Cisco Secure Network Analytics システム設定ガイド』を参照してください。
- プライマリ マネージャを工場出荷時のデフォルトにリセットする、返品許可を処理する、または再導入する必要がある場合は、セカンダリ マネージャも工場出荷時のデフォルトにリセットしてから、フェールオーバー関係を再設定する必要があります。工場出荷時のデフォルトにリセットするには、『Cisco Secure Network Analytics システム設定ガイド』を参照してください。サポートが必要な場合は、シスコサポートまでお問い合わせください。

Analytics ジョブが遅延する

「Analytics のパフォーマンス低下」のシステムアラームがトリガーされる 2 つの例を以下に示します。

セカンダリ Manager がプライマリ Manager に昇格

プライマリ Manager のロールをセカンダリ Manager のロールに変更し、元のプライマリ Manager が回復してプライマリロールに再割り当てされるまで 5 時間以上経過すると、「Analytics のパフォーマンスが低下」のシステムアラームがトリガーされます。Analytics が回復すると、元のプライマリ Manager がダウンしている間の過去 6 時間に発生したジョブを実行します。システムが過去 6 時間のすべてのジョブを処理してリアルタイムでジョブの処理を開始するまで、ジョブのパフォーマンス低下が続きます。

劣化によりアプライアンスがダウン

システムが劣化している場合(通常、CPU やメモリなどのリソース不足が原因)、ジョブの遅延が始まります。この遅延が 5 時間を超えると、「Analytics のパフォーマンス低下」のシステムアラームがトリガーされます。この時点で、ジョブの結果は不完全で信頼できないものになります。

この障害の考えられる原因は、セットアップでサポートされている数を超えて 1 秒あたりのフローを増やしたことです。これを解決するには、1 秒あたりのフローを減らすか、Manager、データストア、またはその両方のリソースを増やします。問題を解決できない場合は、カスタマーサポートにお問い合わせください。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 3 月	最初のバージョン。

著作権情報