

Cisco Secure Network Analytics

フェールオーバー コンフィギュレーションガイド 7.5.0



目次

はじめに	5
はじめる前に	5
Data Store の展開	5
セキュリティ分析とロギング(オンプレミス)	5
アプライアンス ステータス	5
設定要件	5
管理者ユーザー	5
設定ファイルとデータベースのバックアップ	6
証明書	6
フェールオーバーロール	6
設定の順序	6
設定の変更	6
ソフトウェア バージョン	6
フェールオーバー設定の保存	6
プライマリマネージャ	6
セカンダリ Manager(読み取り専用)	7
パスワード	7
ドメインの変更	7
Flow Collector	7
外部認証サービス	7
外部サービス	7
ロールの変更	7
証明書	7
プライマリマネージャの復元	8
プライマリマネージャの再起動	8
ネットワーク インターフェイスの変更	8
フェールオーバー設定の概要	9
1. フェールオーバーロールの計画	10
2. Manager の設定とデータベースのバックアップ	11
1. バックアップ設定ファイルの作成	11
2. Manager データベースのバックアップ	11
1. データベースのバックアップ	11
2. データベースのバックアップの確認	14


3. 信頼ストアへの証明書の追加	15
信頼ストアの要件	15
信頼ストアへの証明書のアップロード	15
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	15
2. Manager 信頼ストアへの証明書の追加	15
データストア初期化後のフェールオーバーの設定	17
フェールオーバーペアの設定	17
Data Store 初期化後の Manager の追加	17
4. フェールオーバーペアの設定	18
はじめる前に	18
1. Manager アプライアンスステータスの確認	18
2. セカンダリマネージャの設定	19
3. プライマリマネージャの設定	19
5. フェールオーバー設定の確認	21
1. 設定の変更の確認	21
2. フローコレクションの確認	22
フェールオーバーロールの変更	24
時刻	24
1. プライマリマネージャのバックアップ	24
2. アプライアンスステータスの確認	24
3. フェールオーバー設定の変更	25
1. プライマリ Manager をセカンダリに変更する	25
2. セカンダリ Manager をプライマリに変更する	26
4. 設定の変更の確認	26
ネットワーク インターフェイスの変更	27
1. フェールオーバー設定の削除	27
2. Manager ネットワーク インターフェイスの変更	27
3. Manager フェールオーバーの設定	27
フェールオーバー設定の削除	28
1. アプライアンス ステータスの確認	28
2. フェールオーバーロールの確認	29
3. フェールオーバー設定の削除	29
4. [集中管理 (Central Management)] からのセカンダリ Manager の削除	30
5. セカンダリ Manager 証明書の削除	30
6. セカンダリ Manager を工場出荷時の初期状態にリセットする	31

障害対応	32
Manager がオフラインまたは障害状態になっている	32
信頼エラー	33
セカンダリマネージャにフローが表示されない	33
パスワードの有効期限切れ	33
Analytics ジョブが遅延する	33
セカンダリ Manager がプライマリ Manager に昇格	33
劣化によりアプライアンスがダウン	33
サポートへの問い合わせ	34
変更履歴	35

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 管理コンソールまたは SMC) 間にフェールオーバー関係を確立すると、一方のマネージャをもう一方のバックアップとして機能させることができます。

プライマリ Manager で障害が発生した場合は、セカンダリ Manager を手動でプライマリ Manager に設定してシステムのモニタリングを継続できます。

 プライマリ Manager がオフラインになっても、Manager のロールは自動的に交換されないため注意してください。このガイドに示されている順序で Manager ロールを変更してください。

はじめる前に

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て、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](#) [英語] および [Cisco Secure Network Analytics システム コンフィギュレーションガイド](#) [英語] 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。

Data Store の展開

Secure Network Analytics システムで Data Store 展開を使用している場合は、Data Store 初期化の前にフェールオーバーを設定することをお勧めします。すでに初期化済みの Data Store 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 Manager で Cisco Security Analytics and Logging (オンプレミス) が有効になっている場合は、フェールオーバー設定を開始する前に、もう一方の Manager でも有効になっていることを確認します。

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](#) [英語] を参照してください。

アプライアンス ステータス

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。

管理者ユーザー

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 Manager 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で、Manager を完全に復元するためには両方のバックアップが必要です。手順については、「[2. Manager 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 Manager 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 Manager が読み取り専用になります。プライマリまたはセカンダリフェールオーバーロールで設定する Manager 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 Manager が [集中管理 (Central Management)] でアプライアンスを管理している場合は、フェールオーバー設定を開始する前にプライマリ Manager (または別の Manager) にアプライアンスを移動します。手順については、[Cisco Secure Network Analytics システム コンフィギュレーション ガイド \[英語\]](#) を参照してください。

設定の順序

プライマリ Manager を設定する前にセカンダリ Manager を設定してください。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 Manager を設定する前に、セカンダリ Manager をフェールオーバー用に設定してください。フェールオーバー設定を保存すると、セカンダリ Manager ドメインの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

このガイド記載の手順を進める前に、Secure Network Analytics v7.5.0 が Manager 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、プライマリおよびセカンダリ Manager 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 Manager は自身のドメイン設定、ユーザー設定、およびポリシーをセカンダリ Manager にプッシュします。

セカンダリ Manager (読み取り専用)

セカンダリ Manager ドメイン設定が削除されます。セカンダリ Manager は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 Manager と同期します。

パスワード

プライマリ Manager からローカルユーザーとパスワードログイン情報がセカンダリ Manager にプッシュされるため、両方が同期されます。つまり、プライマリ Manager とセカンダリ Manager へのログインには同じパスワードを使用します。セカンダリ Manager のパスワードを変更するには、プライマリ Manager にログインします。

ドメインの変更

プライマリ Manager は、ホストグループ、ユーザー、ポリシーなどのドメイン設定の変更を自動的にセカンダリ Manager と共有します。

セカンダリ Manager への通信チャンネルがダウン ([構成チャンネルがダウン (Config Channel Down)]) している間に、プライマリ Manager 上のドメイン設定を変更した場合、セカンダリ Manager の通信チャンネルが復旧するとすぐに、プライマリ Manager から完全な設定プッシュが送信されます。

Flow Collector

フローコレクタは、データを自動的に両方のマネージャに送信します。

外部認証サービス

外部認証サービス (LDAP、TACACS+、RADIUS など) は、プライマリ Manager でのみ使用できます。セカンダリ Manager で設定された外部認証サービスを使用するには、セカンダリ Manager をプライマリ Manager に昇格させる必要があります。

外部サービス

外部サービスがプライマリ Manager で設定されている場合は、セカンダリ Manager でも外部サービスを設定してください。たとえば、プライマリ Manager で脅威 フィードを有効にする場合は、セカンダリ Manager でも有効にします。

ロールの変更

セカンダリ Manager 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 Manager がオフラインになっている場合、詳細については「[障害対応](#)」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 Manager アイデンティティ証明書とルート証明書 (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ルート証明書 (該当する場合) は、プライマリ Manager の [集中管理 (Central Management)] に追加されると、セカンダリ

Manager 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 Manager を復元する場合、復元完了後に、セカンダリ Manager がプライマリ Manager と同期されます。

プライマリマネージャの再起動

再起動したためにプライマリ Manager 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 Manager が検出されると、プライマリはフェールオーバーロールを再開します。

- プライマリ Manager のロールがセカンダリに変更され、自動的に解決しない場合は、「[障害対応](#)」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

Manager がフェールオーバー用に設定されている場合は、Manager 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。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. Manager 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、プライマリまたはセカンダリフェールオーバーロールで設定する Manager を計画します。

- **IP アドレス:** 各 Manager の IP アドレスを確認します。
- **セカンダリ Manager:** セカンダリ Manager が [集中管理 (Central Management)] でアプライアンスを管理している場合は、フェールオーバー設定を開始する前にプライマリ Manager (または別の Manager) にアプライアンスを移動します。手順については、[Cisco Secure Network Analytics システム コンフィギュレーション ガイド \[英語\]](#) を参照してください。

 フェールオーバー構成を開始する前に、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) が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 \[英語\]](#) 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 Manager 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 Manager が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。

計画済み フェールオーバー ロール	要約	IP アドレス (IP Address)
プライマリ Manager	Secure Network Analytics をアクティブに監視 および管理する	
セカンダリ Manager	読み取り専用	

2. Manager 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。次の項に進みます。「[3. 信頼ストアへの証明書の追加](#)」。

! 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

各 Manager のバックアップ設定ファイルを作成するには、次の手順を実行します。Manager が Central Manager としてアプライアンスも管理している場合、Manager バックアップ設定ファイルと Central Management バックアップ設定ファイルが作成されます。

1. セカンダリ Manager 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. Manager の **...** (省略符号) 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. **[バックアップアクション (Backup Actions)]** ドロップダウンメニューをクリックします。
7. **[バックアップを作成 (Create Backup)]** を選択します。
8. **[ダウンロード (Downloads)]** 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 Manager にログインします。手順 2 ~ 8 を繰り返して、プライマリ Manager のバックアップ設定ファイルを保存します。

2. Manager データベースのバックアップ

Manager 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. データベースのバックアップ
2. データベースのバックアップの確認

! プライマリ Manager とセカンダリ Manager でデータベースのバックアップ手順を完了していることを確認します。

1. データベースのバックアップ

次の手順を使用して、Manager 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. Manager 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 (Central Management)] で、[Manager] の [... (省略符号) アイコン] > [アプライアンス統計情報の表示 (View Appliance Statistics)] の順にクリックします。

The screenshot shows the 'Inventory' section of the Central Management interface. It displays a table with 4 appliances found. The table has columns for Appliance Status, Host Name, Type, and IP Address. A context menu is open over the first row, with 'View Appliance Statistics' highlighted in blue.

Appliance Status	Host Name	Type	IP Address
Connected	[Redacted]	Manager	[Redacted]
Connected	nfl- [Redacted]	Flow Collector	[Redacted]
Connected	fs- [Redacted]	Flow Sensor	[Redacted]
Connected	fr- [Redacted]	UDP Director	[Redacted]

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 [使用量 (バイト) (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。

Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	45%	19.1G	8.09G	10.04G
/lancope/var	43%	33.32G	14G	18.62G

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。

Remote File System	
IP Address:	<input type="text"/>
Port Number:	<input type="text" value="445"/>
Share Name:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
Security Protocol:	<input type="radio"/> ntlm <input checked="" type="radio"/> ntlmv2

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) というプロトコルが使用されます。

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。

2. データベースのバックアップの確認

「[2. Manager データベースのバックアップ](#)」をバックアップし、各 Manager 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ルート証明書(該当する場合)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 Manager 証明書のプライマリ Manager 信頼ストアへの追加。
- プライマリ Manager 証明書のセカンダリ Manager 信頼ストアへの追加。

信頼ストアへの証明書のアップロード

各アプライアンス アイデンティティ証明書(リーフ)およびルート証明書(該当する場合)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. Manager 信頼ストアへの証明書の追加](#)」に進みます。



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 アドレスまたはホスト名の後のパスを `/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、または別のブラウザを試します。

3. 各 Manager で手順 1 と 2 を繰り返します。

2. Manager 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 Manager アプライアンス アイデンティティ証明書(リーフ)とルート証明書(該当する場合)をプライマリ Manager 信頼ストアに保存します。

1. Manager 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. Manager の **[アクション (Action)]** 列にある **[… (省略符号) 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 (リーフ) およびルート証明書 (該当する場合) 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 Manager にログインしている場合は、プライマリ Manager アプライアンス アイデンティティ証明書 (リーフ) とルート証明書 (該当する場合) を追加します。
 - プライマリ Manager にログインしている場合は、セカンダリ Manager アプライアンス アイデンティティ証明書 (リーフ) とルート証明書 (該当する場合) 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)]**: Central Management のインベントリページで、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. 他の Manager 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 Manager 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従って、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 Manager の [集中管理 (Central Management)] インベントリに「Data Store が設定されていません (Data Store Not Configured)」というメッセージが表示されます。「[Data Store 初期化後の Manager の追加](#)」の手順に従って、セカンダリ Manager を設定します。


Data Store 初期化後の Manager 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。

1. RFD:『[Secure Network Analytics System Configuration Guide](#)』の「Resetting Factory Defaults」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. プライマリ Manager アプライアンスコンソールに sysadmin としてログインします。
4. [データストア (Data Store)] を選択します。
5. [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。
6. [データストア (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。
7. 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。

8. [集中管理 (Central Management)] で、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、フェールオーバー用のマネージャを設定します。フェールオーバー設定を保存すると、セカンダリ Manager ドメイン設定が削除されます。セカンダリは読み取り専用になり、プライマリ Manager 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。

はじめる前に

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. Manager 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 Manager を設定する前に、セカンダリ Manager をフェールオーバー用に設定してください。フェールオーバー設定を保存すると、セカンダリ Manager ドメインの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. Manager アプライアンスステータスの確認

1. プライマリ Manager 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。

The screenshot shows the 'Inventory' page in the Central Management interface. It displays a table with 4 appliances found. The 'Appliance Status' column for all entries is 'Connected', which is highlighted with a red box. The table columns are Appliance Status, Host Name, and Type.

Appliance Status	Host Name	Type
Connected	sr-...	Manager
Connected	nflow-...	Flow Collector
Connected	fs-...	Flow Sensor
Connected	fr-740	UDP Director

4. **セカンダリ Manager** 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 Manager ドメイン設定が削除されます。セカンダリは読み取り専用になり、プライマリ Manager 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 Manager** で、**[セキュリティ分析ダッシュボード (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。

The screenshot shows the 'Manager Configuration' page with the 'Failover Configuration' tab selected. A blue informational banner at the top states: 'Make sure you add all required certificates to your Manager Trust Stores. Also, configure the secondary Manager before the primary Manager. For instructions, please refer to [Help](#).' Below this, the 'Failover Role' dropdown menu is highlighted with a red box and set to 'Secondary'. At the bottom, the 'Other Manager' section shows 'IP Address*' as '141' and 'Failover Role' as 'Primary'.

5. **[IPアドレス (IP Address)]** フィールドに、他の Manager の IP アドレスを入力します。これがプライマリ Manager 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 Manager** で、**[セキュリティ分析ダッシュボード (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。

Manager Configuration

Name: [redacted] IP Address: [redacted] 121 Model: [redacted] Serial: [redacted] Seal

Data Retention DSCP Configuration Failover Configuration

Failover Configuration Cancel Save

● Make sure you add all required certificates to your Manager Trust Stores. Also, configure the secondary Manager before the primary Manager. For instructions, please refer to [Help](#).

Failover Role*
Primary

Other Manager

IP Address* [redacted].103 Failover Role
Secondary

5. [IPアドレス (IP Address)] フィールドに、セカンダリ Manager 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、マネージャがフェールオーバーおよび通信用に設定され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 Manager にフェールオーバー設定の変更が表示され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 Manager 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 Manager がインベントリに表示されていること。
- 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 Manager の表示の確認

Inventory

4 Appliances found

Q Filter Appliance Inventory Table

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Changes Pending	fs- [redacted] -1	Flow Sensor FSVE-KVM-[redacted]	[redacted] 134	⋮
Config Changes Pending	nflow- [redacted] [5-2]	Flow Collector FCNFVE-KVM-[redacted]	[redacted] 135	⋮
Config Changes Pending	[redacted] -103-4	Manager [redacted]	[redacted] 103	⋮
Connected	[redacted] -141-4	Manager [redacted]	[redacted] 141	⋮

i [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

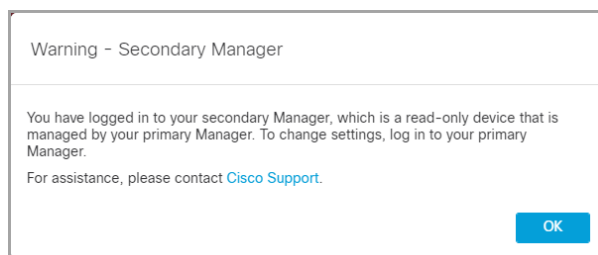
The screenshot shows the 'Central Management' interface with the 'Inventory' tab selected. It displays '4 Appliances found' and a table with the following data:

Appliance Status	Host Name	Type
Connected	sr-...	Manager
Connected	nflow-...	Flow Collector
Connected	fs-...	Flow Sensor
Connected	fr-740	UDP Director

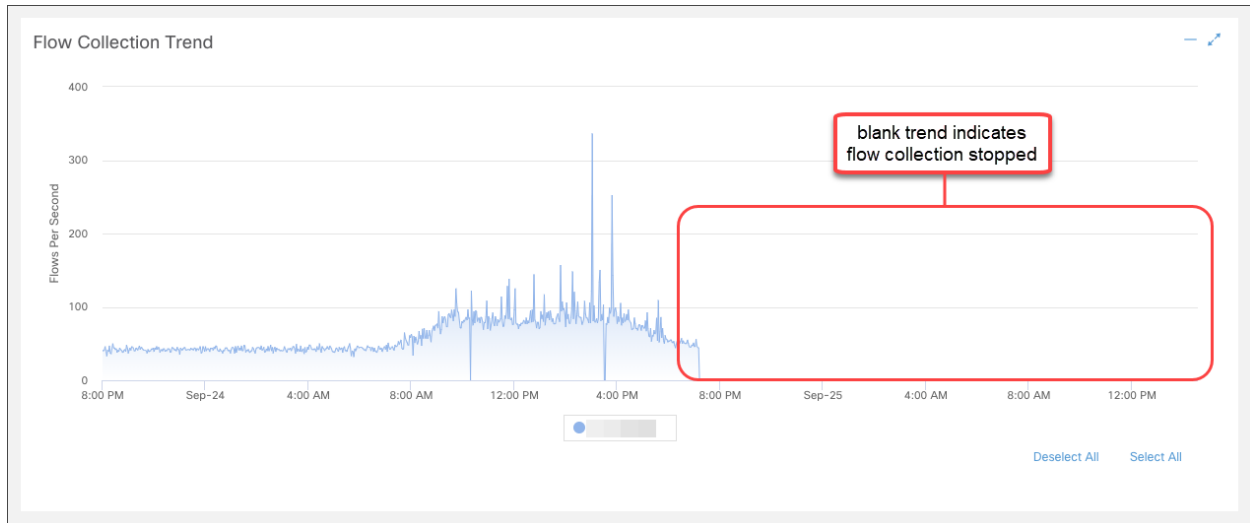
2. フローコレクションの確認

次の手順を使用して、セカンダリ Manager が読み取り専用として動作し、フローを受信していることを確認します。

1. セカンダリ Manager にログインします。
2. Manager が読み取り専用であることを示す通知が表示されます。セカンダリ Manager 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ます。



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。

フローコレクションが停止している場合は、[集中管理 (Central Management)] を使用して、次の順番で Flow Collector およびセカンダリ Manager を再起動します (または「[障害対応](#)」を参照)。


- プライマリ Manager 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 [... (省略符号) 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:** 手順を繰り返して、[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 Manager:** 手順を繰り返して、セカンダリ Manager を再起動します。



再起動したためにプライマリ Manager 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 Manager が検出されると、プライマリはフェールオーバーロールを再開します。プライマリ Manager のロールがセカンダリに変更され、自動的に解決しない場合は、「[障害対応](#)」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 Manager のロールを変更します。ロールは自動的に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 Manager ドメインの設定が削除されるため、手順を順番に実行してください。

時刻

セカンダリ Manager 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 [構成チャネルがダウン (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。手順については、「[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 Manager をバックアップします。手順については、「[2. Manager 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 Manager 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。
 - **Manager:** プライマリまたはセカンダリ Manager のアプライアンスステータスが [構成チャネルがダウン (Config Channel Down)] と表示されている場合は、通信設定を確認し、「[障害対応](#)」を参照してください。
 - **その他のアプライアンス:** Flow Collector、Data Node、Flow Sensor、UDP Director のアプライアンスステータスが [構成チャネルがダウン (Config Channel Down)] と表示されている場合は、設定を確認し、[集中管理 (Central Management)] を使用してアプライアンスを再起動します ([...] (省略符号) 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 コンフィギュレーション ガイド \[英語\]](#) を参照してください。

Central Management

Inventory Update Manager App Manager Smart Licensing Database

Inventory

4 Appliances found

Q Filter Appliance Inventory Table

Appliance Status	Host Name	Type
Connected	sr-██████████	Manager
Connected	nflow-██████████	Flow Collector
Connected	fs-██████████	Flow Sensor
Connected	fr-740-██████████	UDP Director

3. フェールオーバー設定の変更

次の手順を使用して、プライマリ Manager をセカンダリに変更し、セカンダリ Manager をプライマリに昇格させます。

この設定では、プライマリ Manager がセカンダリ Manager になり、そのドメイン設定が削除されます。セカンダリは読み取り専用になり、新しく昇格したプライマリ Manager 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)] でアプリケーションを追加または削除しないでください。

1. プライマリ Manager をセカンダリに変更する

1. 現在のプライマリ Manager で、[セキュリティ分析ダッシュボード (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 Manager が [セカンダリ (Secondary)] と表示されている場合は、「[障害対応](#)」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 Manager をプライマリに変更する


1. セカンダリ Manager 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、すべてのドメイン設定データがセカンダリ Manager から削除されます。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、「[フェールオーバー設定の削除](#)」を参照してください。

2. Manager 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。また、画面に表示される指示に従って、証明書の再生成が必要かどうか、または証明書を保持することを選択できるかどうかを確認してください。

 カスタム証明書を使用している場合は、誤って証明書を上書きした場合に備えて、ネットワーク設定 (ホスト名、ネットワークドメイン名、または IP アドレス) を変更する前に、証明書を保存します。『[SSL/TLS Certificates for Managed Appliances Guide](#)』[英語] の手順に従うか、[シスコサポート](#)に問い合わせてください。

3. Manager 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。Manager をバックアップし、新しい証明書を Manager 信頼ストアに追加します。

フェールオーバー設定の削除

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、すべてのドメイン設定データがセカンダリ Manager から削除されます。

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 Manager にセカンダリ Manager が管理対象アプライアンスとして表示されていること、および両方の Manager が [接続済み (Connected)] と表示されていることを確認します。

1. プライマリ Manager 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。
 - **Manager:** プライマリまたはセカンダリ Manager のアプライアンスステータスが [構成チャネルがダウン (Config Channel Down)] と表示されている場合は、通信設定を確認し、「[障害対応](#)」を参照してください。
 - **その他のアプライアンス:** Flow Collector、Flow Sensor、または UDP Director の [アプライアンスステータス (Appliance Status)] が [構成チャネルがダウン (Config Channel Down)] と表示されている場合は、設定を確認し、[集中管理 (Central Management)] を使用してアプライアンスを再起動します。
([...] (省略符号) 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 コンフィギュレーション ガイド \[英語\]](#) を参照してください。

Central Management | Inventory | Update Manager | App Manager | Smart Licensing | Database

Inventory

4 Appliances found

Q Filter Appliance Inventory Table

Appliance Status	Host Name	Type
Connected	sr-...	Manager
Connected	nflow-...	Flow Collector
Connected	fs-...	Flow Sensor
Connected	fr-740	UDP Director

2. フェールオーバーロールの確認

1. プライマリ Manager で、[セキュリティ分析ダッシュボード (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。

The screenshot shows the 'Manager Configuration' interface. At the top, there are fields for Name, IP Address (121), Model, and Serial. Below this, there are tabs for Data Retention, DSCP Configuration, and Failover Configuration. The Failover Configuration tab is active. A blue banner contains a note: 'Make sure you add all required certificates to your Manager Trust Stores. Also, configure the secondary Manager before the primary Manager. For instructions, please refer to [Help](#).' Below the banner, there is a dropdown menu for 'Failover Role*' which is currently set to 'Primary'. At the bottom, there is a section for 'Other Manager' with fields for IP Address* (103) and Failover Role (Secondary).

5. セカンダリ Manager 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 Manager のフェールオーバーロールが正しい場合は、両方のマネージャで [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。
 - 両方の Manager がセカンダリとして表示されている場合は、フェールオーバー設定を更新して、1 つのプライマリ Manager と 1 つのセカンダリ Manager が存在する状態にしてから、削除を進めます。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](#)」の設定の順序と手順に従ってください。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、すべてのドメイン設定データがセカンダリ Manager から削除されます。

1. プライマリ Manager 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、すべてのドメイン設定データがセカンダリ Manager から削除されます。

4. **セカンダリ Manager** 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. [集中管理 (Central Management)] からのセカンダリ Manager の削除

1. **プライマリ Manager** 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 Manager** を見つけます。

! 削除する前に、セカンダリ Manager の IP アドレスを確認します。

3. [... (省略符号) 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. 画面上の指示に従い、[集中管理 (Central Management)] からセカンダリ Manager を削除します。

5. セカンダリ Manager 証明書の削除

次の手順を使用して、その他のアプライアンスの信頼ストアからセカンダリ Manager 証明書を削除します。

! 無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

1. **プライマリ Manager** の [集中管理 (Central Management)] に戻ります。次を確認します。
 - セカンダリ Manager がインベントリに表示されていないこと。
 - 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 [... (省略符号) 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てます。
5. セカンダリ Manager 証明書を見つけてます。
6. [削除 (Delete)] をクリックして、各セカンダリ Manager 証明書を信頼ストアから削除します。
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 Manager を工場出荷時の初期状態にリセットする

セカンダリ Manager を使用するには、工場出荷時の初期状態にリセットします。[Cisco Secure Network Analytics システム コンフィギュレーション ガイド \[英語\]](#) の手順に従います。

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。
- 初回セットアップ (SystemConfig) を使用して Manager を設定する。

障害対応

Manager がオフラインまたは障害状態になっている

ネットワークがダウンした場合、Manager をシャットダウンして再起動した場合やその他のさまざまな理由で、プライマリ Manager がオフラインになることがあります。

再起動したためにプライマリ Manager 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 Manager が検出されると、プライマリはフェールオーバーロールを再開します。

プライマリ Manager ロールがセカンダリに変更され、自動的に解決しない場合は、次のシナリオを確認して、必要な作業を決定します。

 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 Manager で障害が発生したか、またはシャットダウンして再起動しました。	既存のセカンダリ Manager をプライマリに手動で昇格しました。プライマリがオンラインです。	新しいプライマリ Manager がプライマリとしてのロールを維持します。再起動すると、元のプライマリ Manager 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 Manager で障害が発生したか、またはシャットダウンして再起動しました。	既存のセカンダリ Manager をプライマリに手動で昇格していないため、オンラインのプライマリ Manager がありません。	元のプライマリ Manager を再起動すると、プライマリと元のセカンダリ Manager の両方がセカンダリのロールを担います。いずれかの Manager をプライマリ Manager に昇格させます。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。
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 Manager をプライマリに手動で昇格しました。プライマリがオンラインです。	新しいプライマリ Manager がプライマリとしてのロールを維持します。再起動すると、元のプライマリ Manager 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 Manager をプライマリに手動で昇格していないため、オンラインのプライマリ Manager がありません。	元のプライマリ Manager は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 Manager はセカンダリ Manager としてのロールを自動的に再開します。

信頼エラー

Manager 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。詳細については、「[3. 信頼ストアへの証明書の追加](#)」を参照し、手順を確認します。

セカンダリマネージャにフローが表示されない

セカンダリ Manager にフローが表示されない場合は、セカンダリ Manager 証明書が Flow Collector の信頼ストアに保存されていることを確認します。詳細については、「[3. 信頼ストアへの証明書の追加](#)」を参照し、手順を確認します。

パスワードの有効期限切れ

フェールオーバー設定が保存されると、プライマリ Manager からローカルユーザーとパスワードログイン情報がセカンダリ Manager にプッシュされるため、両方が同期されます。つまり、プライマリ Manager とセカンダリ Manager へのログインには同じパスワードを使用します。セカンダリ Manager のパスワードを変更するには、プライマリ Manager にログインします。

プライマリ Manager がダウンし、パスワードの有効期限が切れた場合、セカンダリ Manager 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 Manager アプライアンスのステータスが [接続済み (Connected)] に戻るまで待ちます。その後、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 コンフィギュレーション ガイド \[英語\]](#) を参照してください。
- プライマリ Manager を工場出荷時の初期状態にリセットする、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 Manager も工場出荷時の初期状態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。工場出荷時の初期状態にリセットするには、[Cisco Secure Network Analytics システム コンフィギュレーション ガイド \[英語\]](#) 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。

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が、この障害の原因と考えられます。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、以下にお問い合わせください: [シスコサポート](#)。

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12月13日	最初のバージョン。

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、以下の URL でご確認いただけます。

https://www.cisco.com/c/ja_jp/about/legal/trademarks.html。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)