Cisco Secure Network Analytics

システム コンフィギュレーション ガイド 7.4.2

目次

はじめに

概要

次の Cisco Secure Network Analytics（旧 Stealthwatch）ハードウェアおよび Virtual Edition アプライアンスを v7.4.2 の 1 つの管理対象システムに設定するには、このガイドを使用します。

- Cisco Secure Network Analytics Manager（旧 Stealthwatch Management Console）
- Cisco Secure Network Analytics データノード
- Cisco Secure Network Analytics Flow Collector
- Cisco Secure Network Analytics Flow Sensor
- Cisco Secure Network Analytics UDP Director

Secure Network Analytics の詳細については、次のオンラインリソースを参照してください。

- **概要**：https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html [英語]
- **アプライアンス**：https://www.cisco.com/c/en/us/products/security/stealthwatch/datasheet-listing.html [英語]
- **リリースノート**：詳細については、リリースノートを参照してください。

対象読者

このガイドは、Secure Network Analytics製品のインストールおよび設定を担当するネットワーク管理者とその他の担当者を対象としています。

専門家によるインストールを希望する場合は、最寄りのシスコパートナーまたはシスコサポートに連絡してください。

インストール要件

このガイドを使用して Secure Network Analytics を管理対象システムに構成する前に、次のガイドを使用してハードウェアと仮想アプライアンスをインストールしてください。

ハードウェア

- **ハードウェアのインストール**：この設定を開始する前に、『Secure Network Analytics x2xx Series Hardware Installation Guide』または『Secure Network Analytics x3xx Series Hardware Installation Guide』を使用してアプライアンスハードウェア（物理アプライアンス）をインストールします。
- **仕様**：ハードウェア仕様 は Cisco.com で入手できます。
- **サポートされているプラットフォーム**：各システムバージョンでサポートされているハードウェアプラットフォームについては、Cisco.com の Hardware and Software Version Support Matrix を参照してください。

バーチャルエディション（VE）アプライアンス

- **Virtual Edition のインストール**：この設定を開始する前に、『Secure Network Analytics Virtual Edition Installation Guide』を使用して仮想アプライアンスをインストールします。

クイックリファレンスの概要

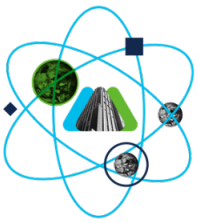
インストールを成功させるには、次の手順を順番に実行してください。詳細な手順については、手順のリンクをクリックしてください。

「**はじめる前に**」および「**システム設定のプランニング**」

アプライアンスの設定と Data Store ありまたは Data Store なしの Secure Network Analytics の展開に必要な情報がすべて揃っていることを確認します。

1. 初回セットアップを使用した環境の設定

- **ログイン**:コンソールから sysadmin(パスワード:lan1cope)として各アプライアンスにログインします。コマンドプロンプトで、`SystemConfig` と入力します。
- **Data Store ありの Flow Collector**:root(パスワード:lan1cope)としてログインします。
- **必要なアプライアンス**:どの展開にも Manager と Flow Collector が必要です。Data Store ありの展開の場合は、(Data Node 間通信を使用して)Data Node を設定する必要もあります。



2. 管理対象システムの設定

アプライアンス設定ツールを使用して、各アプライアンスを Manager で管理されるように順番に設定します。アプライアンスの Data Store ドメインか非 Data Store ドメインも作成します。

- **アプライアンス設定ツール**:ブラウザのアドレス フィールドに、**https://** に続けてアプライアンスの IP アドレスを入力します。
- **ログイン**:admin
- **パスワード**:lan411cope
- **sysadmin と root のデフォルトパスワード**:lan1cope

アプライアンスを順番に設定します。クラスタ内の次のアプライアンスの設定を開始する前に、中央管理インベントリを確認し、各アプライアンスのステータスが [接続済み(Connected)](または[データストアが初期化されていません(Data Store Not Initialized)])になっていることを確認します。

1. プライマリ Manager(Central Management)
2. Data Node
3. Flow Collector 5000 シリーズ データベース
4. Flow Collector 5000 シリーズ エンジン
5. その他のすべての Flow Collector

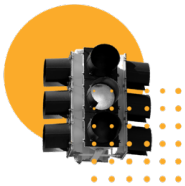
6. UDP Director
7. Flow Sensor
8. セカンダリ Manager

3. Manager フェールオーバー関係の定義

- この手順は、プライマリ Manager とセカンダリ Manager を設定した場合に必要です。
- フェールオーバーを使用すると、2 つの Manager 間にフェールオーバーペアを確立し、一方をもう一方のバックアップコンソールとして機能させることができます。
- 『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』の手順に従います。

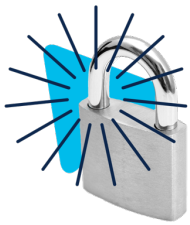
4. サイト冗長性の設定

- この手順はオプションであり、Data Store が必要です。
- サイトの冗長性を使用すると、類似のアプライアンスを使用した個別の展開を含む 2 つの Cisco Secure Network Analytics サイトのクラスタ間でほぼ冗長性を確立できます。



5. v7.4.2 パッチのインストール

- Cisco Software Central（https://software.cisco.com）の Cisco スマートアカウントから最新の **v7.4.2 パッチ**をダウンロードします。
- パッチの readme ファイルの手順に従って、各パッチをインストールします。



6. Data Store の初期化

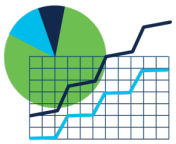
Data Store 展開のみに必要です。

1. Manager アプライアンスコンソール（SystemConfig）にroot としてログインします。
2. [Data Store] > [SSH] の順に選択します。
3. [Data Store] > [初期化（Initialization）] の順に選択します。

7. デスクトップクライアントのインストール

非 Data Store 展開のみに必要です。

- デスクトップクライアントには、64 ビットのオペレーティングシステムが必要です。32 ビットのオペレーティング システムまたは Linux では実行できません。
- Manager にログインします。（[ダウンロード（Download）]）アイコンをクリックします。



8. 通信の確認

- Manager にログインします。[フロー収集のトレンド（Flow Collection Trend）] を確認します。
- Data Store データベースのステータスを参照し、[アップ（Up）] になっていることを確認します（[構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] > [Data Store] タブ）。
- レポートビルダーでレポートを実行して、Flow Collector と Data Store でフローが受信されていることを確認します（[レポート（Report）] > [レポートビルダー（Report Builder）] > Flow Collector によるフロー収集のトレンドレポート、フローデータベース取り込みトレンドレポート）。

9. アプライアンス設定の完了

- Flow Sensor アプリケーション ID およびペイロード（すべての Flow Sensor に必要）
- UDP Director 高可用性
- その他のオプションのアプライアンス設定

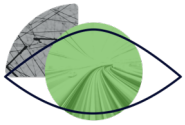
10. テレメトリの設定

追加のテレメトリタイプが有効になっている Data Store 展開に必要です。

- **NVM フロー**：『エンドポイントライセンスおよび Network Visibility Module（NVM）コンフィギュレーション ガイド』の手順に従います。
- **ファイアウォールログ**：『Cisco Security Analytics and Logging：ファイアウォールイベント統合ガイド』の手順に従って、Manager にアプリケーションをインストールします。

11. Secure Network Analytics ライセンシング

- 90 日間の評価期間が終了する前に Cisco スマートアカウント（https://software.cisco.com）に製品インスタンスを登録します。
- 『Secure Network Analytics スマート ソフトウェア ライセンシング ガイド』の手順に従います。



12. Secure Network Analyticsの管理

Manager にログインして以下を選択します。

- **ホストグループ**：[設定（Configure）] > [検出ホストグループ管理（DETECTION Host Group Management）]
- **ポリシー**：[設定（Configure）] > [検出ポリシー管理（DETECTION Policy Management）]
- **フロー検索**：[調査（Investigate）] > [フロー検索（Flow Search）]
- **レポート**：[ダッシュボード（Dashboards）] > [レポートビルダー（Report Builder）]
- **ユーザー管理**：[設定（Configure）] > [グローバルユーザー管理（GLOBAL User Management）]
- **手順**：任意のページから [?（[ヘルプ（Help）]）アイコン] > [ヘルプ（Help）] の順に選択します。また、「環境の管理」、「動作の調査」、「脅威への対応」も参照してください。

追加の設定、メンテナンス、およびトラブルシューティングについては、次のガイドを確認してください。

- Analytics
- アプリケーション
- 認証/許可
- ドメイン
- パスワード
- SSL/TLS アプライアンス アイデンティティと 追加の SSL/TLS クライアント アイデンティティ
- 脅威フィード
- Central Management（アプライアンスの管理）
- Data Store データベース
- Data Store のメンテナンス
- 非 Data Store Flow Collector の Data Store Flow Collector への移行
- トラブルシューティング

はじめる前に

設定プロセスを開始する前に、このガイドを確認して、プロセスについて、および設定のために計画する必要がある準備、時間、リソースについて理解してください。

用語

このガイドでは、Flow Sensor Virtual Edition（VE）などの仮想製品を含むすべての Secure Network Analytics 製品に「**アプライアンス**」という用語を使用しています。

「**クラスタ**」は、Manager によって管理される Secure Network Analytics アプライアンスのグループです。

略語

このガイドでは、次の略語が使用される場合があります。

略語	定義
DNS	ドメイン ネーム システム（サービスまたはサーバー）
dvPort	分散仮想ポート
ESX	Enterprise Server X
GB	ギガバイト
IDS	侵入検知システム
IPS	侵入防御システム
ISO	International Standards Organization; 国際標準化機構
IT	情報技術
KVM	カーネルベース仮想マシン
MTU	最大伝送ユニット
NTP	ネットワーク タイム プロトコル
TB	テラバイト
UUID	汎用一意識別子
VDS	vNetwork 分散型スイッチ
VE	バーチャル エディション

略語	定義
VLAN	仮想ローカル エリア ネットワーク
VM	仮想マシン

設定の詳細

Secure Network Analytics システムの設定には、次のようなものがあります。

- **要件**：Secure Network Analytics は、Data Store ありか Data Store なしで、または（Data Store ドメインと非 Data Store ドメイン両方の）ハイブリッド展開として設定できます。アプライアンス設定とドメイン要件を確認するには、「**システム設定のプランニング**」を参照してください。
- **設定の順序**：このガイドの手順に従い、アプライアンス設定ツールの指定された順序でアプライアンスの設定を行ってください。
- **証明書**：アプライアンスは、一意の自己署名アプライアンス アイデンティティ証明書とともにインストールされます。
- **Central Management**：プライマリ Manager/Central Manager からアプライアンスを管理できます。

ソフトウェアのダウンロード

Cisco Software Central を使用して、仮想アプライアンス（VE）のインストールファイル、パッチ、およびソフトウェア更新ファイルをダウンロードします。https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

パスワード要件

システムの設定中にデフォルトのパスワードを置き換え、次の新しいパスワードを作成します。

ユーザー	デフォルト パスワード
admin	lan411cope
root	lan1cope
sysadmin	lan1cope
dbadmin	Data Store を初期化するときにパスワードを割り当てます。
readonlyuser	Data Store を初期化するときにパスワードを割り当てます。

CIMC admin	ハードウェアアプライアンスにリモートアクセスするには、CIMC にログインします。まだ CIMC を設定していない場合は、『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide』の手順に従います。 デフォルト パスワードは **password** です。このパスワードは初回ログイン時に変更してください。

ライセンス

Secure Network Analytics のライセンスを取得するには、スマートアカウントを使用して製品インスタンスを登録し、ライセンスを管理し、レポートを実行し、通知を設定します。https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

Secure Network Analytics を評価モードで使用すると、選択された機能を 90 日間使用できます。Secure Network Analytics のデフォルト機能を最大限に活用してライセンスと機能をアカウントに追加するには、スマート ソフトウェア ライセンシングの製品インスタンスを登録します。詳細については、「**11. Secure Network Analytics ライセンシング**」を参照してください。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、フロー収集が停止します。フロー収集を再度開始するには、製品インスタンスを登録します。

TLS

Secure Network Analytics v1.2 が必要です。

サード パーティ製アプリケーション

Secure Network Analytics アプライアンスへのサードパーティ製アプリケーションのインストールをサポートしていません。

ブラウザ

Secure Network Analytics は、Chrome、Firefox、および Microsoft Edge の最新バージョンをサポートしています。

ホスト名

アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。

ドメイン名

各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスはインストールできません。

NTP サーバー

- **設定**：各アプライアンスに少なくとも 1 台の NTP サーバーが必要です。
- **問題のある NTP**：130.126.24.53 NTP サーバーがサーバーのリストに含まれている場合は削除します。このサーバーには問題があることが判明しており、シスコのデフォルトの NTP サーバー リストからはすでに除外されています。

タイム ゾーン

すべての Secure Network Analytics アプライアンスは協定世界時（UTC）を使用します。

- **仮想ホスト サーバー**：仮想ホスト サーバーが正しい時刻に設定されていることを確認します。

> ⚠ 仮想アプライアンスをインストールする仮想ホスト サーバーに設定された時刻が正しい時刻に設定されていることを確認します。正しくない場合、アプライアンスを起動できないことがあります。

システム設定のプランニング

設定を開始する前に手順を確認し、初回セットアップでアプライアンスを設定して、アプライアンス設定ツールで 1 つの管理対象システムにそれらのアプライアンスを構成する場合のプランニング、時間、および要件について理解しておいてください。

システム設定要件

ネットワークアーキテクトおよび管理者と話し合って、Secure Network Analytics v7.4.2 の展開の詳細を確認してください。設定要件については、各セクションを参照してください。

- **Secure Network Analytics（Data Store あり）**
- **Secure Network Analytics（Data Store なし）**
- **Secure Network Analytics ハイブリッド展開**
- **システム設定のプランニング**

Secure Network Analytics（Data Store あり）

Data Store ありの Secure Network Analytics では、Flow Collector が Data Store Data Node にテレメトリを送信して保存します。

- **Data Node の数**：Data Store には、1 つの Data Node（単一 Data Node 展開）か、3 つ以上の Data Node（複数 Data Node 展開）を含めることができます。Data Node が 2 つしかない Data Store はサポートされません。
- **ハードウェアまたは仮想**：Data Node が同じタイプ（すべてハードウェアかすべて Virtual Edition）であることを確認します。
- **サイズ**：Data Nodes Virtual Edition で同じプロファイルサイズが使用されており、RAM、CPU、およびディスク容量が同じであることを確認します。詳細については、『Virtual Edition アプライアンス設置ガイド』を参照してください。
- **テレメトリ取り込み**：NetFlow に加えて、NVM（Network Visibility Module）フローとファイアウォールログのテレメトリ取り込みを設定できます。

設定が正しく行われるよう、次の点に注意してください。

1. 初回セットアップで、Data Store 設定用のアプライアンスを設定します。次のアプライアンスを設定します。
    - **Manager**：「**次の設定：Manager**」を参照してください。
    - **Flow Collector**：「**Data Store ありの Flow Collector の設定**」を参照してください。
    - **Data Node**：「**Data Node の設定**」を参照してください。
2. Manager アプライアンス設定ツールで Secure Network Analytics アプライアンスの Data Store ドメインを作成します。
3. NVM フローとファイアウォールログのテレメトリ取り込みを有効にするには、「**10. テレメトリの設定**」に記載されている追加の設定手順を完了してください。

Secure Network Analytics（Data Store なし）

Data Store なしの Secure Network Analytics では、Flow Collector が Flow Collector または Flow Collector データベースでテレメトリをローカルに保存します（5000 シリーズのみ）。

設定が正しく行われるよう、次の点に注意してください。

1. 初回セットアップで次のアプライアンスを設定します。

    - **Manager**：「**次の設定：Manager**」を参照してください。
    - **Flow Collector**：「**Data Store なしの Flow Collector の設定**」を参照してください。

2. Manager アプライアンス設定ツールで Secure Network Analytics アプライアンスの 非 Data Store ドメインを作成します。

管理対象システムの設定が完了したら、後で展開に Data Store を追加できます（手順については、「**非 Data Store 展開への Data Store の追加**」を参照してください）。

移行前のデータや可視性を失うことなく、既存の Flow Collector を移行して Data Store データベースを使用することもできます。これにより、Data Store でのみ使用可能な機能を利用できます。詳細については、「**非 Data Store Flow Collector の Data Store Flow Collector への移行**」を参照してください。

Secure Network Analytics ハイブリッド展開

ハイブリッド設定の Secure Network Analytics では、Data Store データノードにテレメトリを送信して保存するように特定の Flow Collector を設定できます。また、テレメトリを Flow Collector か Flow Collector データベース にローカルに保存するように他の Flow Collector を設定することが可能です（5000 シリーズのみ）。

設定が正しく行われるよう、次の順序でアプライアンスとドメインを設定します。

1. 初回セットアップで Data Store なしのアプライアンスを設定します。次のアプライアンスを設定します。

    - **Manager**：「**次の設定：Manager**」を参照してください。
    - **Flow Collector**：「**Data Store なしの Flow Collector の設定**」を参照してください。

2. Manager アプライアンス設定ツールで Secure Network Analytics アプライアンスの 非 Data Store ドメインを作成します。
3. 「**9. アプライアンス設定の完了**」までのすべての手順を実行し、非 Data Store ドメインを使用して初期システム設定を完了します。
4. 「**非 Data Store 展開への Data Store の追加**」の手順に従います。Data Store ドメインを作成し、そのドメインに Flow Collector とデータノードを追加します。

アプライアンス設定要件

初回セットアップで各アプライアンスを設定するには、次の情報が必要です。またこの情報を使用して、アプライアンス設定ツールで管理対象システムにアプライアンスを構成します。

設定要件	詳細	アプライアンス
IPアドレス	`eth0` 管理ポートにルーティング可能な IP アドレスを割り当てます。	
ネットマスク		
ゲートウェイ		
ホスト名	アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。	
ドメイン名	各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスはインストールできません。	
DNS サーバ	名前解決のための内部 DNS サーバー	
NTP サーバ	サーバー間同期のための内部タイムサーバー。各アプライアンスに少なくとも 1 台の NTP サーバーが必要です。 130.126.24.53 NTP サーバーがサーバーのリストに含まれている場合は削除します。このサーバーには問題があることが判明しており、シスコのデフォルトの NTP サーバー リストからはすでに除外されています。	
メールリレーサーバー	アラートと通知を送信する SMTP メールサーバー	
Flow Collector エクスポートポート	Flow Collector のみに必要です。 NetFlow のデフォルト：2055	
プライベート LAN または VLAN 内のルーティング不可能な IP アドレス（Data Node 間通信用）	Data Node のみに必要です。 • ハードウェア eth2、または eth2 と eth3 のボンディング。最大 20G のスループットを実現するボンディングされた LACP `eth2/eth3` ポートチャネルを作成すると、Data Node 間の高速な通信が可能になり、Data Store への Data Node の追加や交換が迅速になります。LACP ポートボンディングは、ハードウェア Data Node で使用できる唯一のボンディング	

	オプションであることに注意してください。 • 仮想 eth1 **IP アドレス**：提供された IP アドレスを使用するか、Data Node 間通信の次の要件を満たす値を入力できます。 • **169.254.42.0/24 CIDR ブロック**（169.254.42.2 ～ 169.254.42.254）の **ルーティング不可能な IP アドレス** • **最初の 3 オクテット**：169.254.42 • **サブネット**：/24 • **シーケンシャル**：メンテナンスを容易にするために、連続した IP アドレス（169.254.42.10、169.254.42.11、169.254.42.12 など）を選択します。 **ネットマスク**： ネットマスクは 255.255.255.0 にハードコードされており、変更できません。	
eth0 ハードウェア接続ポート	データ ストア ハードウェア アプライアンスを使用する Secure Network Analytics でのみ必要です。 • Manager 2210 • Flow Collector 4210 • Data Node eth0 ハードウェア接続ポートオプション： • **SFP+**：SFP+：eth0 用の 10G SFP+/DAC 光ファイバポート。 • **BASE-T**：100Mbs/1GbE/10GbE eth0 用の BASE-T 銅線ポート。BASE-T がデフォルトです。	

ハードウェア（物理）アプライアンスへの接続

Cisco Integrated Management Controller（CIMC）、キーボードとモニター、またはシリアルケーブルかシリアルコンソールを使用してアプライアンスに接続します。手順については、「x2xx Series Hardware Installation Guide」または「Secure Network Analytics x3xx Series Hardware Installation Guide」を参照してください。

CIMC アクセス

リモートアクセスするには、CIMC にログインします。まだ CIMC を設定していない場合は、『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide』の手順に従います。

デフォルト パスワードは **password** です。このパスワードは初回ログイン時に変更してください。

Virtual Edition アプライアンスへの接続

1. ハイパーバイザ ホスト(仮想マシン ホスト)に接続します。
2. ハイパーバイザ ホストで仮想マシンを見つけます。
3. 仮想マシンの電源が入っていることを確認します。

   仮想マシンの電源が入っていない場合や、使用可能なメモリの不足に関するエラー メッセージを受信した場合、次のいずれかを実行します。

   - **リソース**:アプライアンスがインストールされているシステムの使用可能リソースを増やします。詳細については、『Virtual Edition アプライアンス設置ガイド』の「**リソース要件**」を参照してください。
   - **VMware 環境**:アプライアンスのメモリ予約制限とリソース プールを増やします。

> 「リソース要件」を確認して、十分なリソースを割り当てます。この手順は、システムパフォーマンスにとって重要です。
>
> 必要なリソースがない状態で Cisco Secure Network Analytics アプライアンスを展開する場合は、アプライアンスのリソース使用率を注意深く監視し、必要に応じてリソースを増やし、展開の正常性および機能を適切に維持する必要があります。

4. 仮想マシン コンソールにアクセスします。仮想アプライアンスの起動が完了します。

> お使いの VM ホストの速度によっては、すべてのサービスが起動するまでに 30 分程度かかることがあります。

1. 初回セットアップを使用した環境の設定

次の手順に従って、各アプライアンスの基本的な環境を設定します。ハードウェア（物理）アプライアンスでも Virtual Edition（VE）アプライアンスでも、初回セットアップで任意の順序でアプライアンスを設定できます。

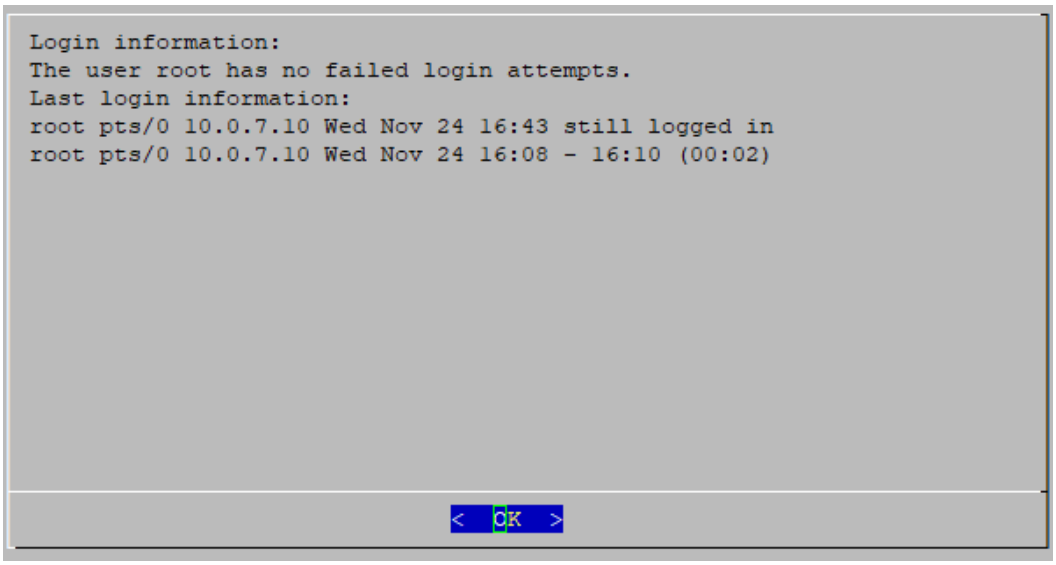
これらの設定手順を開始する前に、「**システム設定のプランニング**」を確認してください。

アプライアンスの設定の概要

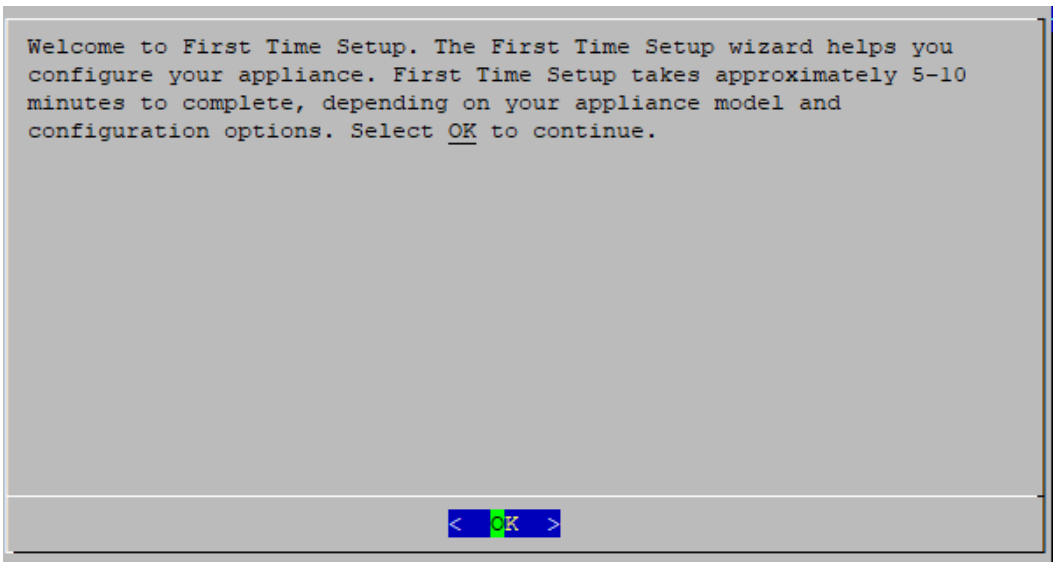
アプライアンスの説明	Data Store での要否	注記
次の設定：Manager	Yes	Manager は、Data Store ありと Data Store なしの展開に必要です。
Data Node の設定	Yes	1 つの Data Node を展開するか（単一 Data Node 展開）、3 つ以上の Data Node を展開できます（複数 Data Node 展開）。 Data Node 2 つだけを展開することはできません。 Data Node がすべてハードウェアであるか、すべて Virtual Edition であることを確認します。また、Data Nodes Virtual Edition で同じプロファイルサイズが使用されており、RAM、CPU、およびディスク容量が同じであることを確認します。詳細については、『Virtual Edition アプライアンス設置ガイド』を参照してください。
Data Store ありの Flow Collector の設定	Yes	Flow Collector は、Data Store Data Node にテレメトリを送信して保存します。取り込むテレメトリタイプも確認します。
Data Store なしの Flow Collector の設定		Flow Collector は、Flow Collector または Flow Collector データベース でテレメトリをローカルに保存します（5000 シリーズのみ）。
次の設定：Flow Sensor または UDP Director		Flow Sensor と UDP Director はオプションです。 UDP Director の代わりに Cisco Telemetry Broker をインストールするには、このガイドの手順に従ってシステム設定を完了します。その後、『Cisco Telemetry Broker 仮想アプライアンス導入および設定ガイド』の手順に従います。

次の設定：Manager

1. コンソールから Manager にログインします。
   - **ログイン**：sysadmin
   - **デフォルト パスワード**：lan1cope
   - システムを設定するときに、デフォルトのパスワードを変更します。
2. システム設定（`SystemConfig`）が開きます。
3. 失敗したログイン試行の情報を確認します。[OK] を選択して続行します。

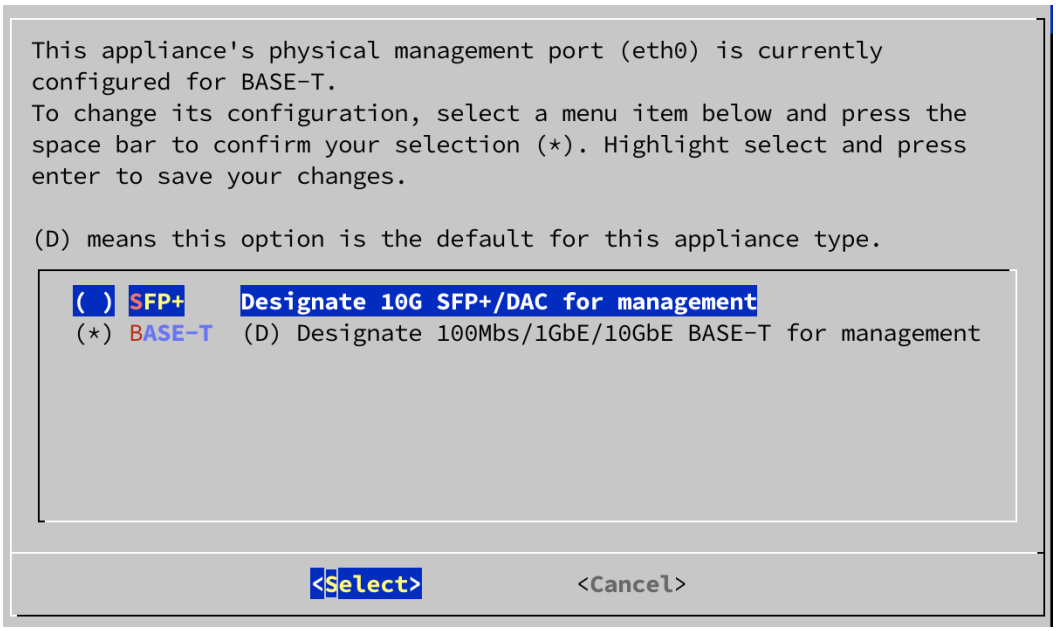


4. 初回セットアップの概要を確認します。[OK] を選択して続行します。



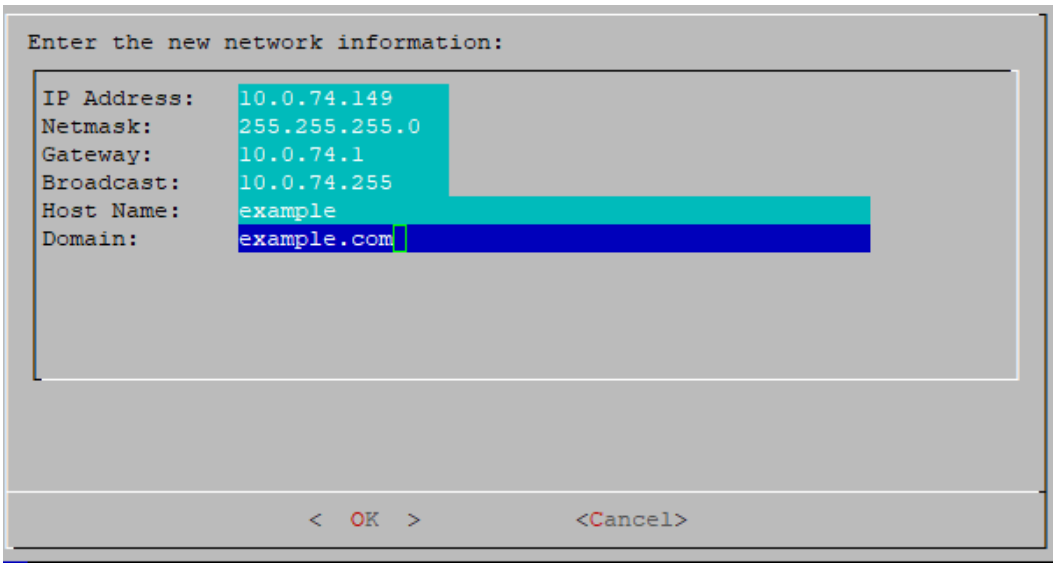
5. **eth0 のポート順序設定（Manager 2210 ハードウェアのみ）**：次のいずれかを選択します。

- **SFP+**：eth0 に 10G SFP+/DAC 光ファイバポートを使用するようにアプライアンスを設定する場合。
- **BASE-T**：100Mbs/1GbE/10GbE を使用するようにアプライアンスを設定する場合。eth0 用の BASE-T 銅線ポート。BASE-T がデフォルトです。

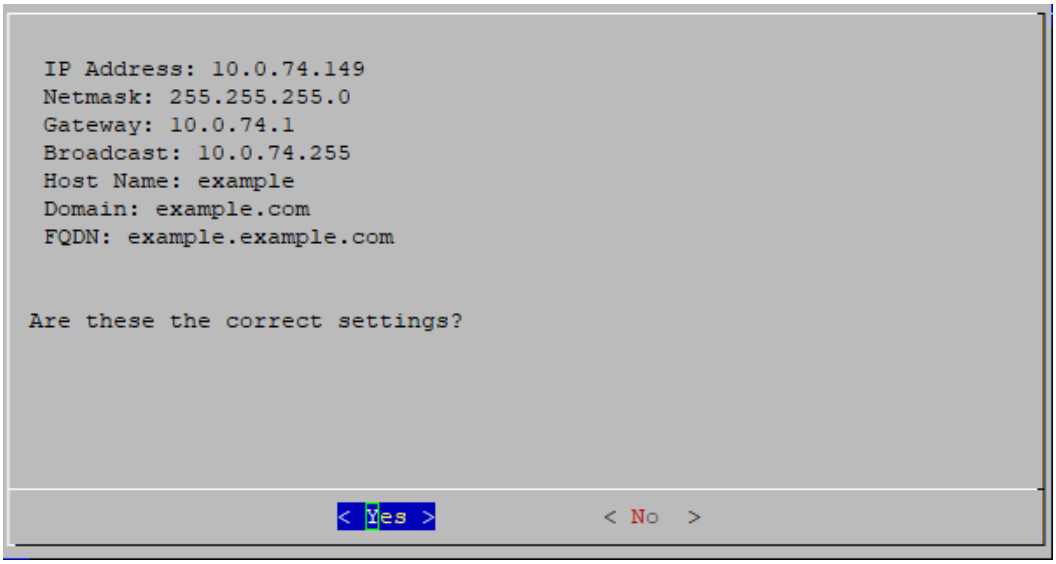


6. 管理インターフェイスの [IPアドレス（IP Address）]（eth0）、[ネットマスク（Netmask）]、[ゲートウェイ（Gateway）]、[ブロードキャスト（Broadcast）]、[ホスト名（Host Name）]、[ドメイン（Domain）] を入力し、[OK] を選択して続行します。

> ⚠ アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。



7. 設定を確認します。[Yes] を選択して続行します。



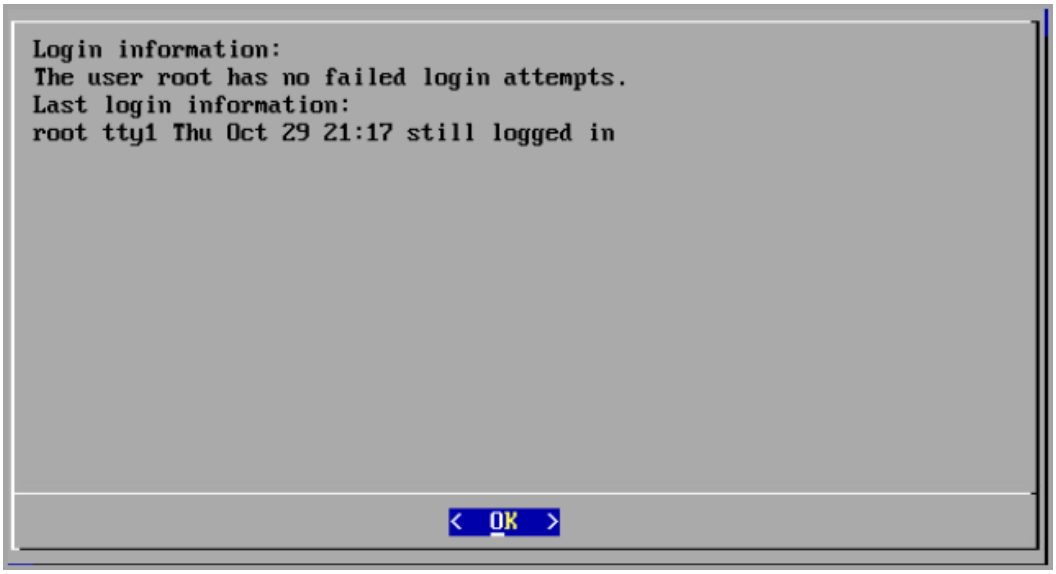
8. [OK] を選択して選択を確定します。画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。
9. Ctrl + Alt を押して、コンソールを終了します。
10. システムの次の Manager について、「**次の設定：Manager**」に記載されているすべての手順を繰り返します。

    初回セットアップですべての Manager を設定した場合は、「**アプライアンスの設定の概要**」に戻って Flow Collector とその他のアプライアンスを設定します。

Data Node の設定

1 つの Data Node を展開するか（単一 Data Node 展開）、3 つ以上の Data Node を展開できます（複数 Data Node 展開）。Data Node 2 つだけを展開することはできません。

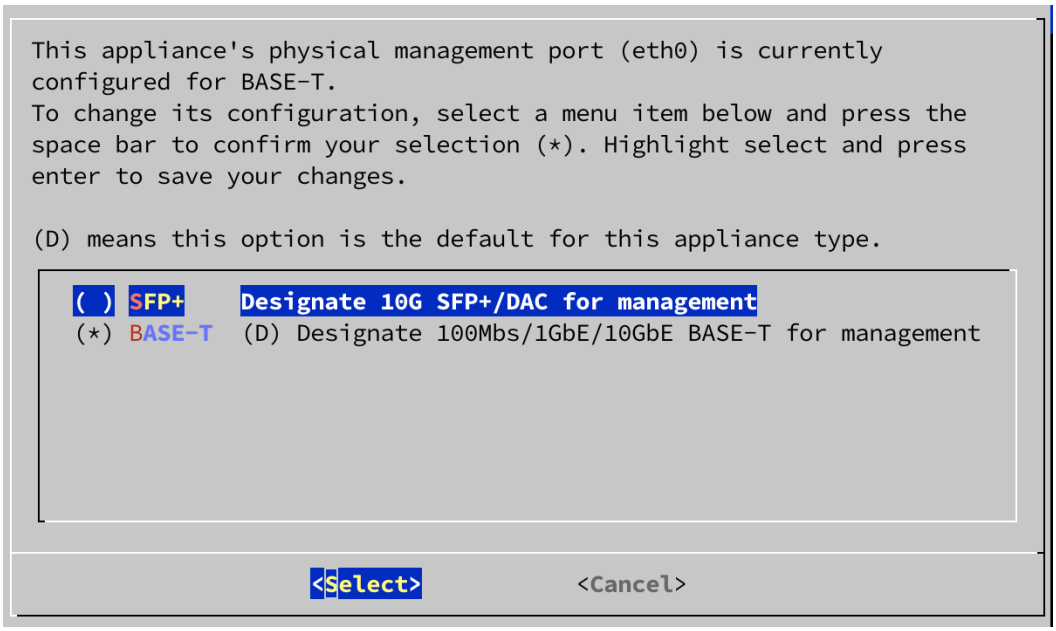
1. コンソールから Data Node にログインします。
   - **ログイン**：sysadmin
   - **デフォルト パスワード**：lan1cope
   - システムを設定するときに、デフォルトのパスワードを変更します。
2. システム設定（`SystemConfig`）が開きます。
3. 失敗したログイン試行の情報を確認します。[OK] を選択して続行します。



4. 初回セットアップの概要を確認します。[OK] を選択して続行します。

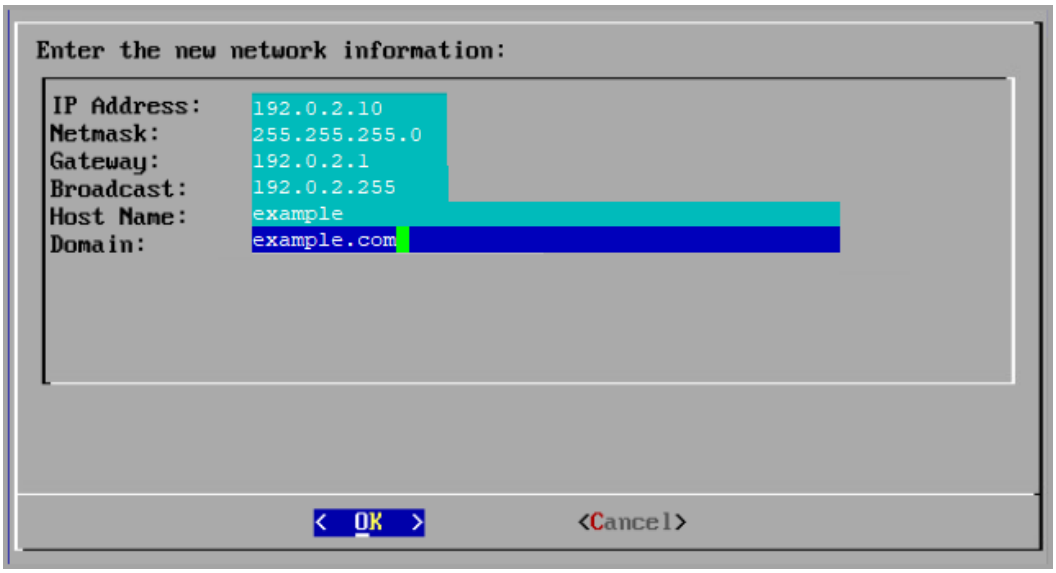
5. **eth0 のポート順序設定（Data Store 6200 ハードウェアのみ）**：次のいずれかを選択します。

- **SFP+**：eth0 に 10G SFP+/DAC 光ファイバポートを使用するようにアプライアンスを設定する場合。
- **BASE-T**：100Mbs/1GbE/10GbE を使用するようにアプライアンスを設定する場合。eth0 用の BASE-T 銅線ポート。BASE-T がデフォルトです。

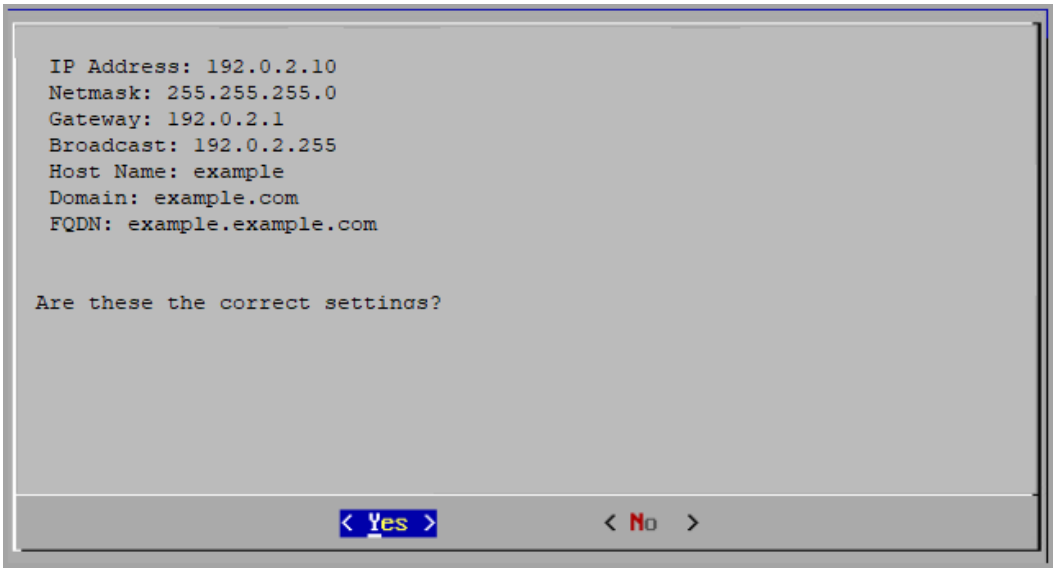


6. 管理インターフェイスの [IPアドレス（IP Address）]、[ネットマスク（Netmask）]、[ゲートウェイ（Gateway）]、[ブロードキャスト（Broadcast）]、[ホスト名（Host Name）]、[ドメイン（Domain）] を入力し、[OK] を選択して続行します。

> ⚠ アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。



7. 設定を確認します。[Yes] を選択して続行します。

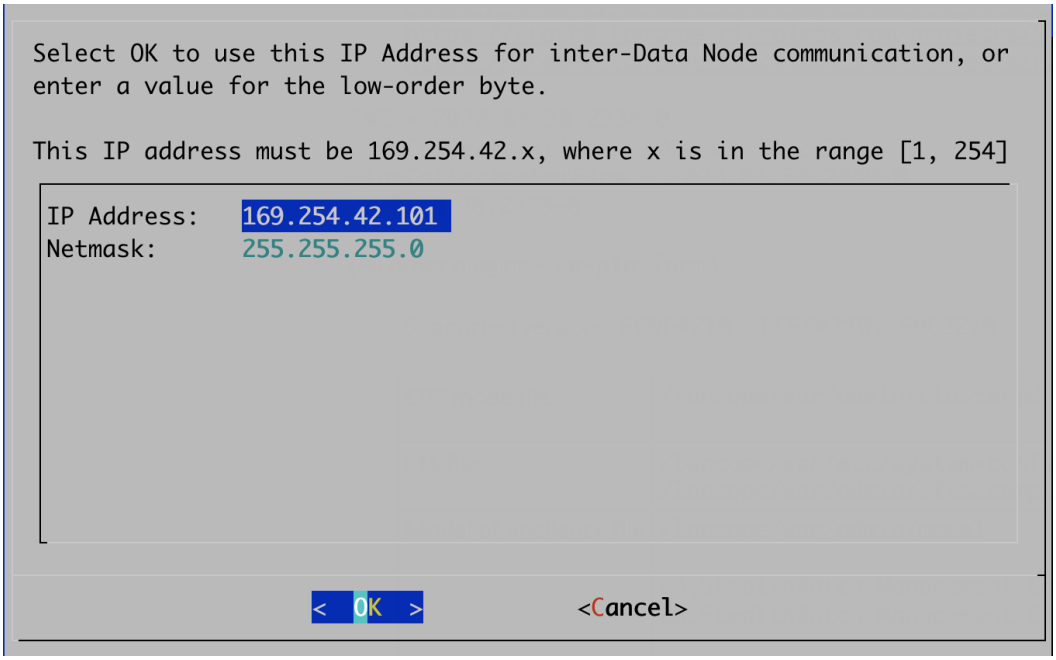


8. [OK] を選択して選択を確定します。画面に表示される指示に従って操作します。
9. **Data Node 間通信用に物理ポート（eth2）とポートチャネル（eth2 および eth3）を設定します。**

> ハードウェア Data Node の場合、通常の Data Node 間の通信には、`eth2` ポートで 10G のスループットを設定すれば十分です。最大 20G のスループットを実現するボンディングされた LACP `eth2/eth3` ポートチャネルを作成すると、Data Node 間の高速な通信が可能になり、新しい各 Data Node が隣接する Data Node からトラフィックを受信してデータを取り込むため、Data Store への Data Node の追加や交換が迅速になります。LACP ポートボンディングは、ハードウェア Data Node で使用できる唯一のボンディングオプションであることに注意してください。

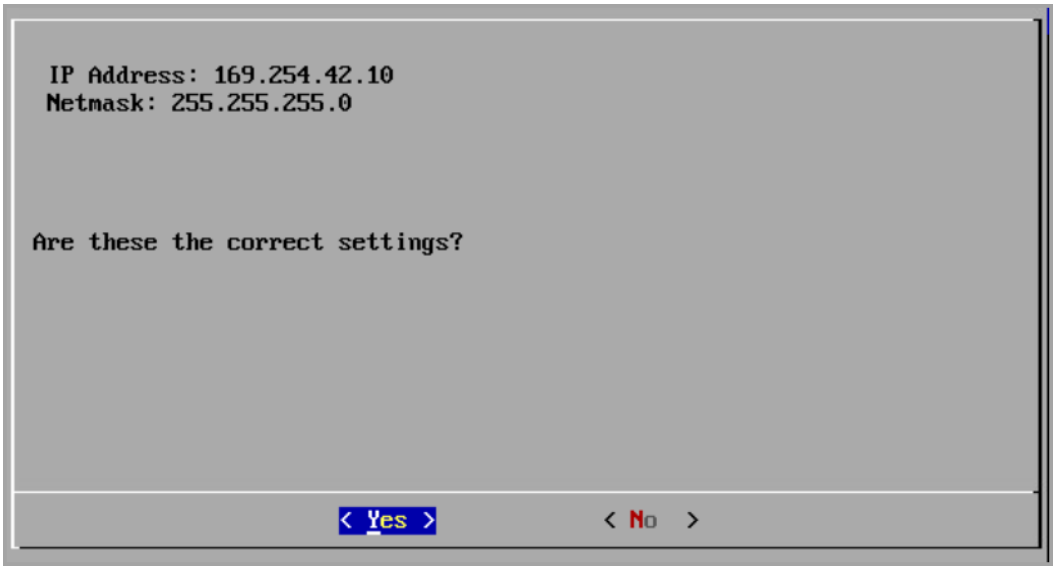
次を入力します。

フィールド	要件
IPアドレス	**提供された IP アドレス**を使用するか、Data Node 間通信用の eth2 および eth3 インターフェイスに関する次の要件を満たす**値を入力**します。 • **169.254.42.0/24 CIDR ブロック**(169.254.42.2 ～ 169.254.42.254)の **ルーティング不可能な IP アドレス** • **最初の 3 オクテット**:169.254.42 • **サブネット**:/24 • **シーケンシャル**:メンテナンスを容易にするために、連続した IP アドレス(169.254.42.10、169.254.42.11、169.254.42.12 など)を選択します。
ネットマスク	255.255.255.0



10. [OK] を選択して続行します。

11. 設定を確認します。[Yes] を選択して続行します。



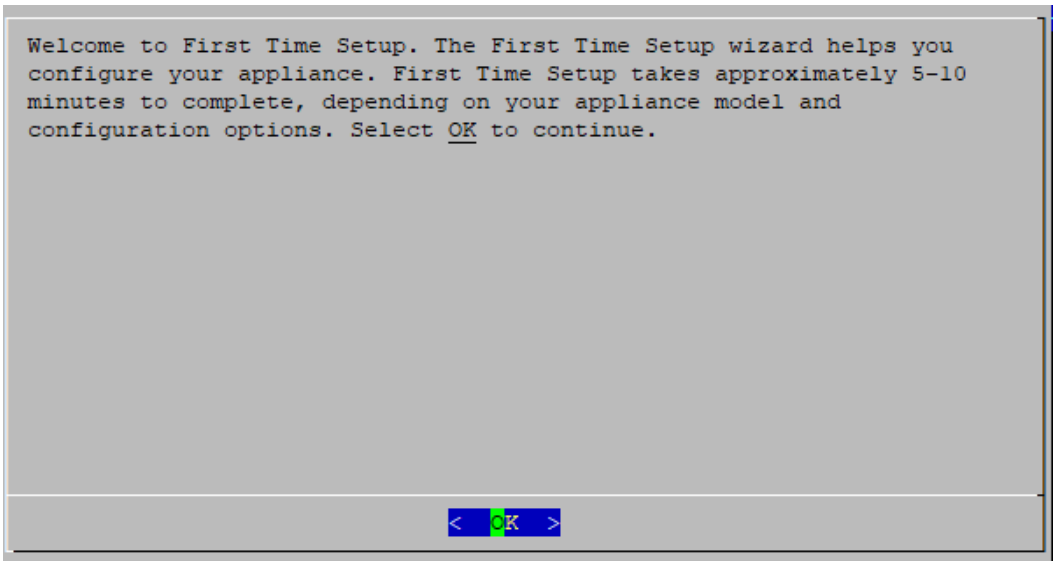
12. 画面に表示されるプロンプトに従って環境を終了し、アプライアンスを再起動します。
13. Ctrl + Alt を押して、コンソールを終了します。
14. システム内の次の Data Node について、「**Data Node の設定**」のすべての手順を繰り返します。
    - 初回セットアップですべての Data Node を設定した場合は、次のセクションに進んで Data Store ありの Flow Collector を設定するか、「**アプライアンスの設定の概要**」に戻ってその他のアプライアンスを設定します。
    - 初回セットアップですべてのアプライアンスを設定した場合は、「**2. 管理対象システムの設定**」に進みます。

Data Store ありの Flow Collector の設定

Data Store を使用するように Flow Collector を設定した場合、Flow Collector は Data Store Data Node にテレメトリを送信して保存します。取り込むテレメトリタイプも確認します。

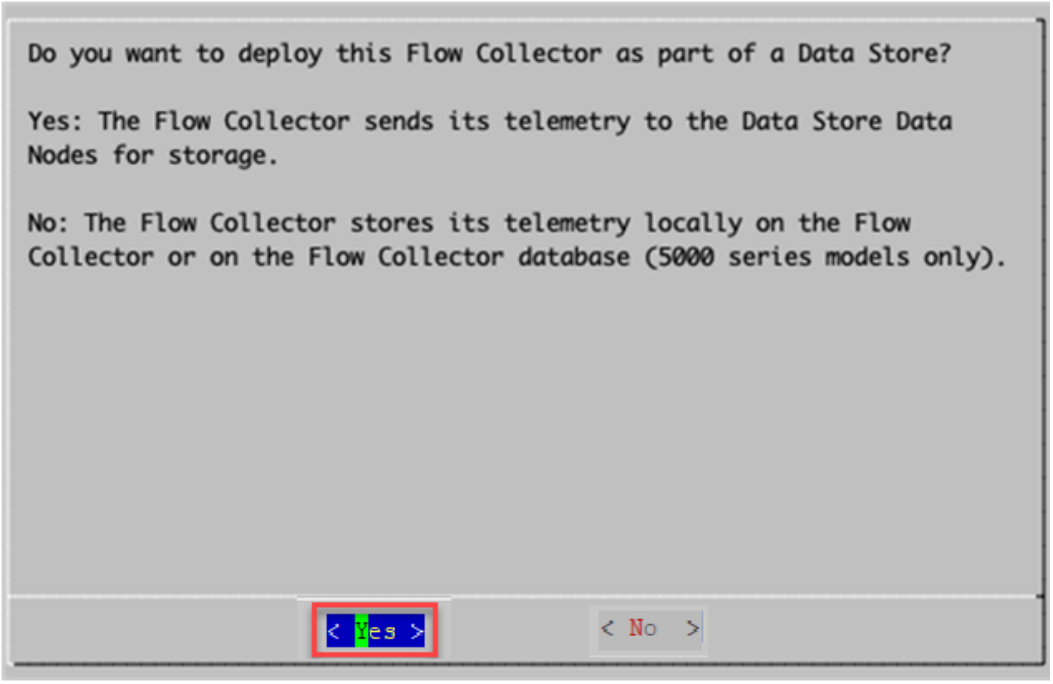
> v7.4.2 以降では、非 Data Store Flow Collector を Data Store Flow Collector に移行できます。詳細については、「**非 Data Store Flow Collector の Data Store Flow Collector への移行**」を参照してください。

1. コンソールから Flow Collector にログインします。
    - **ログイン**：root
    - **デフォルト パスワード**：lan1cope
    - システムを設定するときに、デフォルトのパスワードを変更します。
2. コマンドプロンプトで、`SystemConfig` と入力します。Enter キーを押します。
3. 失敗したログイン試行の情報を確認します。[OK] を選択して続行します。
4. 初回セットアップの概要を確認します。[OK] を選択して続行します。

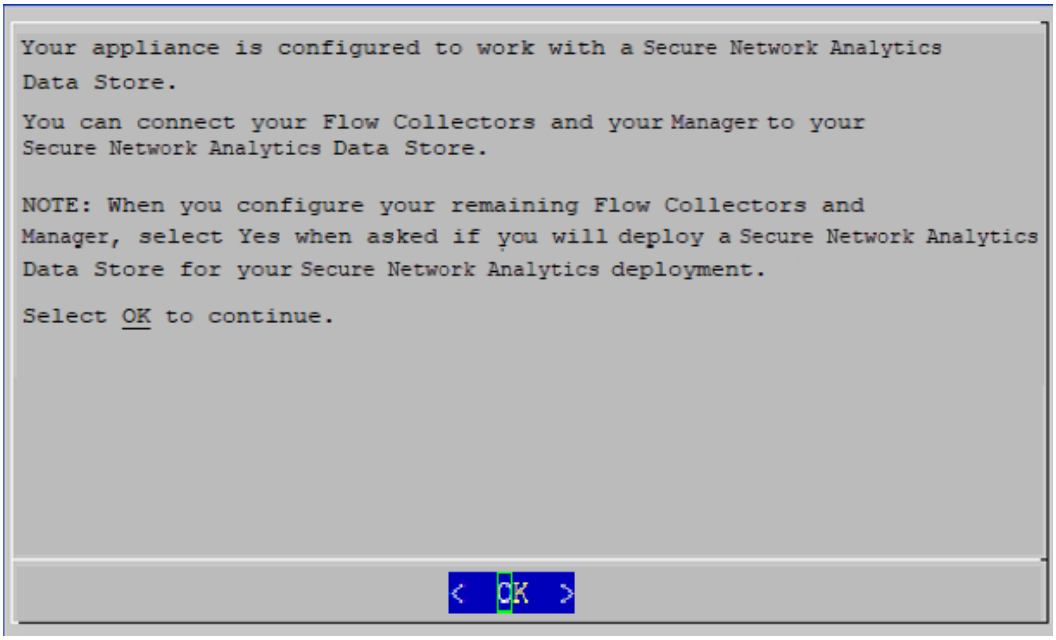


5. [Data Storeの一部としてこのFlow Collectorを展開しますか？（Do you want to deploy this Flow Collector as part of a Data Store?）] と表示されたら、[Yes] を選択します。

> Data Store を使用するように Flow Collector を設定した後に、この設定を変更することはできません。ネットワークに Data Store を展開する場合にのみ、[はい（Yes）] を選択してください。
>
> ⚠ Data Store なしで Secure Network Analytics を展開する必要がある場合は、このセクションの手順ではなく、「**Data Store なしの Flow Collector の設定**」の手順に従ってください。
>
> 選択を誤った場合は、新しい仮想アプライアンスを展開するか、お使いのアプライアンスを RFD してください。



6. [OK] を選択して続行します。



7. 取り込むテレメトリタイプを選択します。

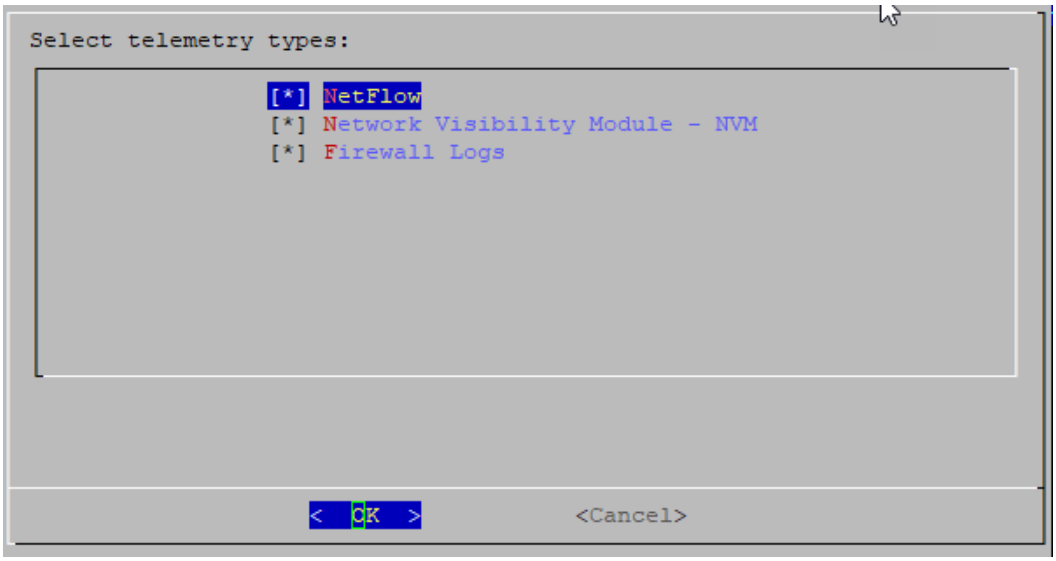
- **デフォルト**：デフォルトでは、すべてのテレメトリタイプが選択されています。アスタリスク(*)は、選択されたテレメトリを示します。

- **選択解除**：テレメトリの選択を解除するには、テレメトリタイプを選択してクリックします（またはキーボードのスペースキーを押します）。

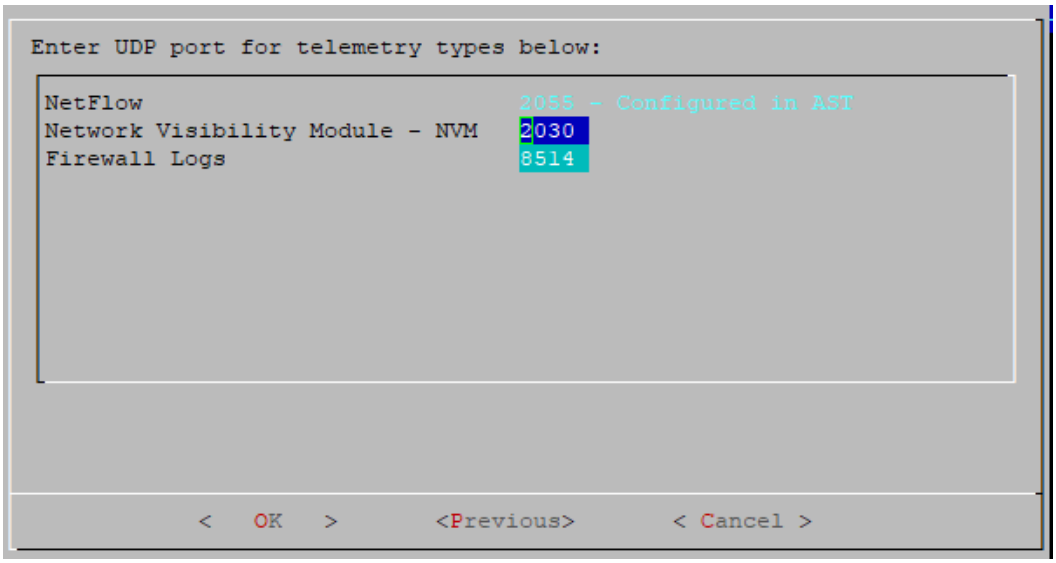
詳細情報：

- [Network Visibility Module – NVM]：[Network Visibility Module – NVM] を選択すると、Flow Collector は NVM フローを取り込んで保存します。詳細については、『Cisco Secure Network Analytics Endpoint License and Network Visibility Module (NVM) Configuration Guide』を参照してください。
- [ファイアウォールログ（Firewall Logs）]：[ファイアウォールログ（Firewall Logs）] を選択すると、Flow Collector は Cisco Security Analytics and Logging（オンプレミス）のファイアウォール イベント ログを取り込んで保存します。詳細については、『Security Analytics and Logging：ファイアウォールイベント統合ガイド』を参照してください。

> NetFlow を無効にするように Flow Collector を設定した場合、エクスポータ、ホストグループ、セキュリティイベント、ホストレポートの変更などの設定オプションを更新しても効果はありません。

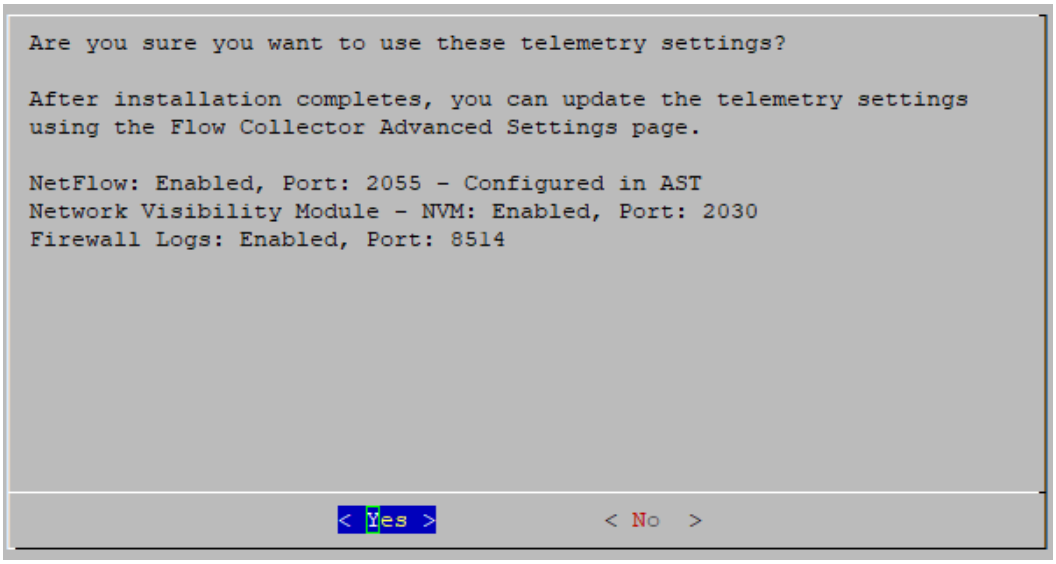


8. 選択したテレメトリタイプの UDP ポートを入力します。[OK] を選択します。



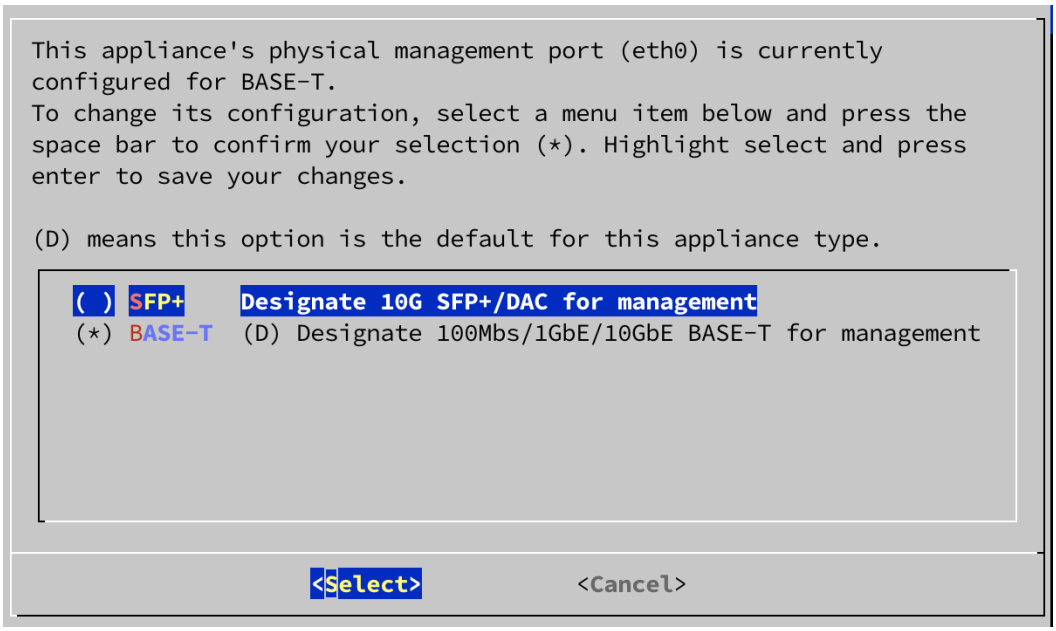
> テレメトリポートが一意であることを確認します。テレメトリポートを重複して設定すると、フローデータの消失を回避するためにポートが内部のデフォルト値にリセットされます。たとえば、NetFlow と NVM が同じテレメトリポートにエクスポートされると、NVM データをエクスポートする各デバイスがFlow Collectorにエクスポータを作成し、Flow Collectorエンジンのエクスポータリソースを使い切ってしまうため、フローデータが消失します。

9. 設定を確認します。[Yes] を選択して続行します。



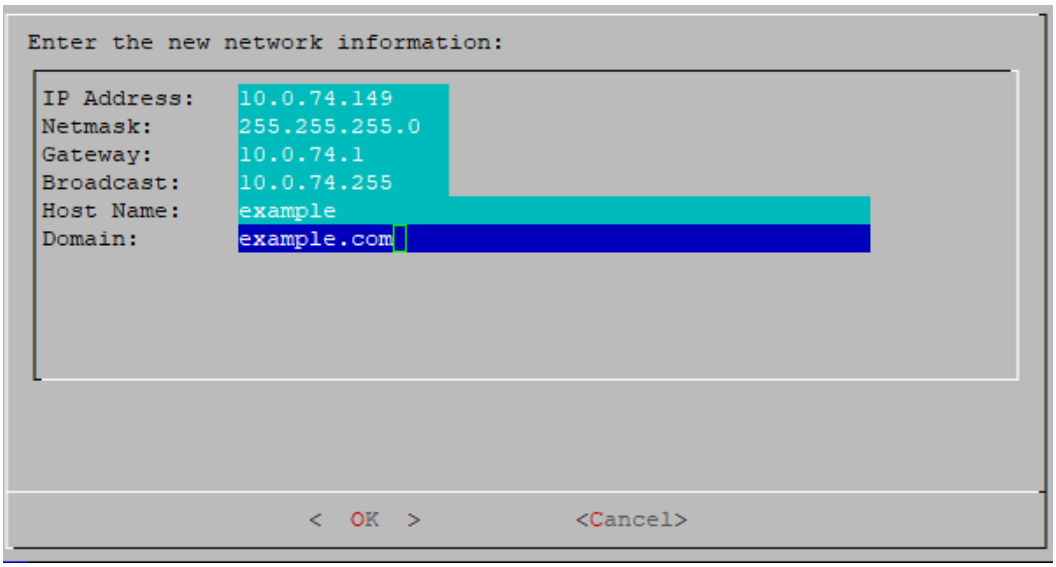
10. **eth0 のポート順序設定（Flow Collector4210 ハードウェアのみ）**：次のいずれかを選択します。

- **SFP+**：eth0 に 10G SFP+/DAC 光ファイバポートを使用するようにアプライアンスを設定する場合。
- **BASE-T**：100Mbs/1GbE/10GbE を使用するようにアプライアンスを設定する場合。eth0 用の BASE-T 銅線ポート。BASE-T がデフォルトです。

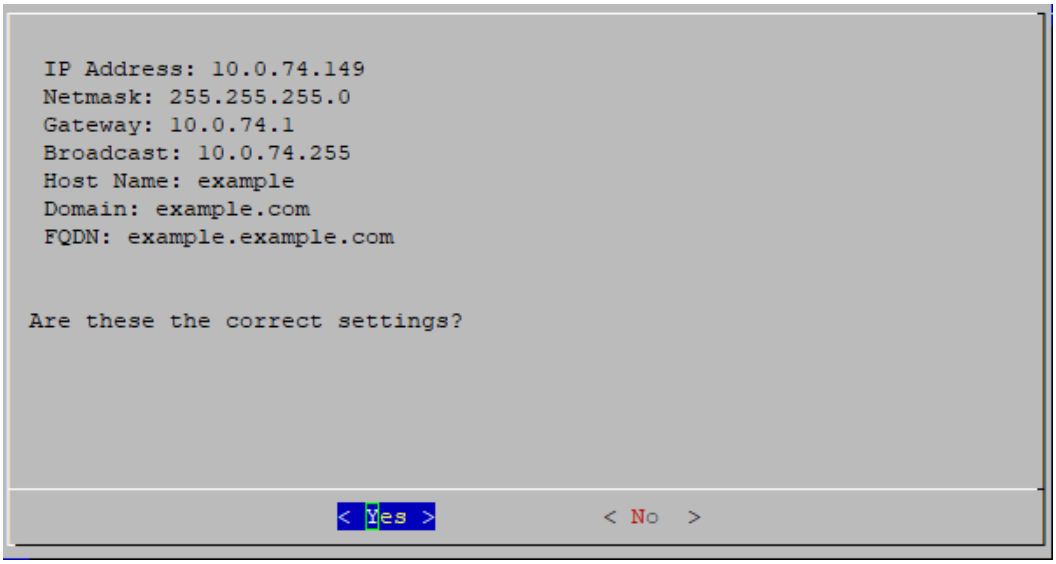


11. 管理インターフェイスの [IPアドレス（IP Address）]、[ネットマスク（Netmask）]、[ゲートウェイ（Gateway）]、[ブロードキャスト（Broadcast）]、[ホスト名（Host Name）]、[ドメイン（Domain）] を入力し、[OK] を選択して続行します。

> ⚠ アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。



12. 設定を確認します。[Yes] を選択して続行します。



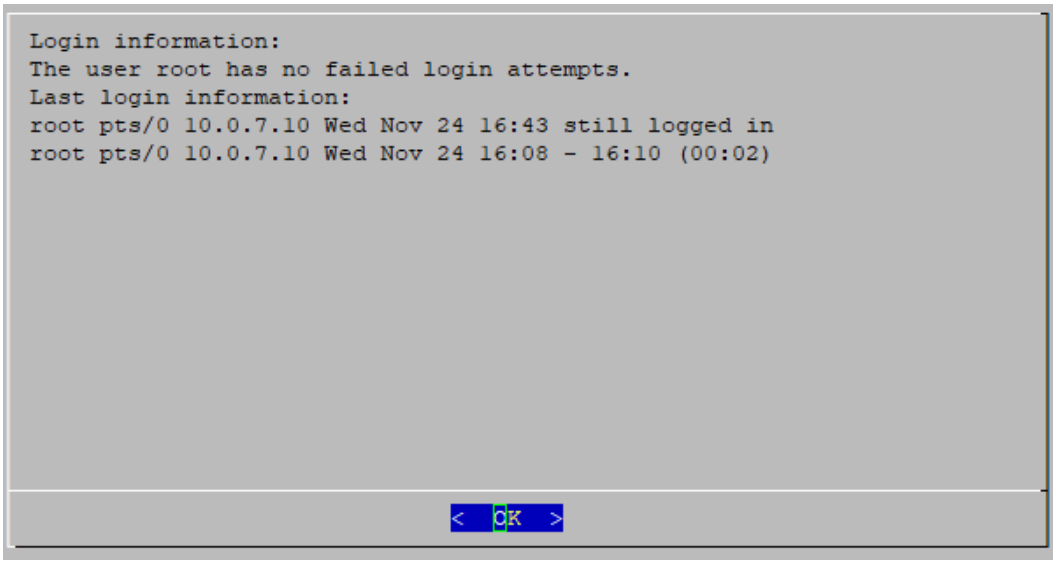
13. [OK] を選択して選択を確定します。画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。
14. Ctrl + Alt を押して、コンソールを終了します。
15. システムの次の Flow Collector について、「**Data Store ありの Flow Collector の設定**」に記載されているすべての手順を繰り返します。

    初回セットアップで Data Store のすべての Flow Collector を設定した場合は、「**アプライアンスの設定の概要**」に戻ってその他のアプライアンスを設定します。

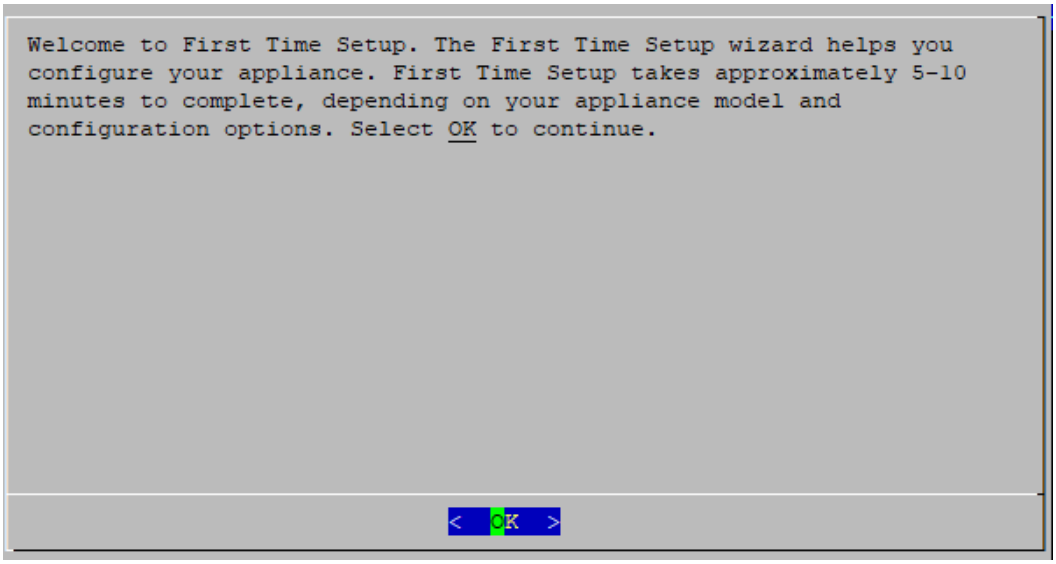
Data Store なしの Flow Collector の設定

Data Store を使用しないように Flow Collector を設定すると、Flow Collector は、テレメトリを Flow Collector か Flow Collector データベースにローカルに保存します（5000 シリーズのみ）。

1. コンソールから Flow Collector にログインします。
   - **ログイン**：sysadmin
   - **デフォルト パスワード**：lan1cope
   - システムを設定するときに、デフォルトのパスワードを変更します。
2. システム設定（`SystemConfig`）が開きます。
3. 失敗したログイン試行の情報を確認します。[OK] を選択して続行します。

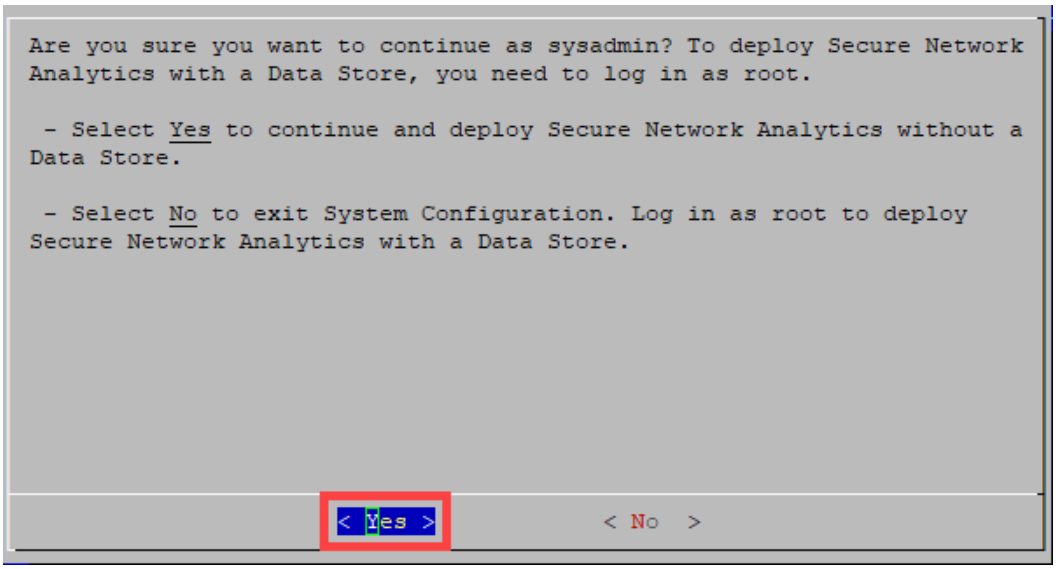


4. 初回セットアップの概要を確認します。[OK] を選択して続行します。

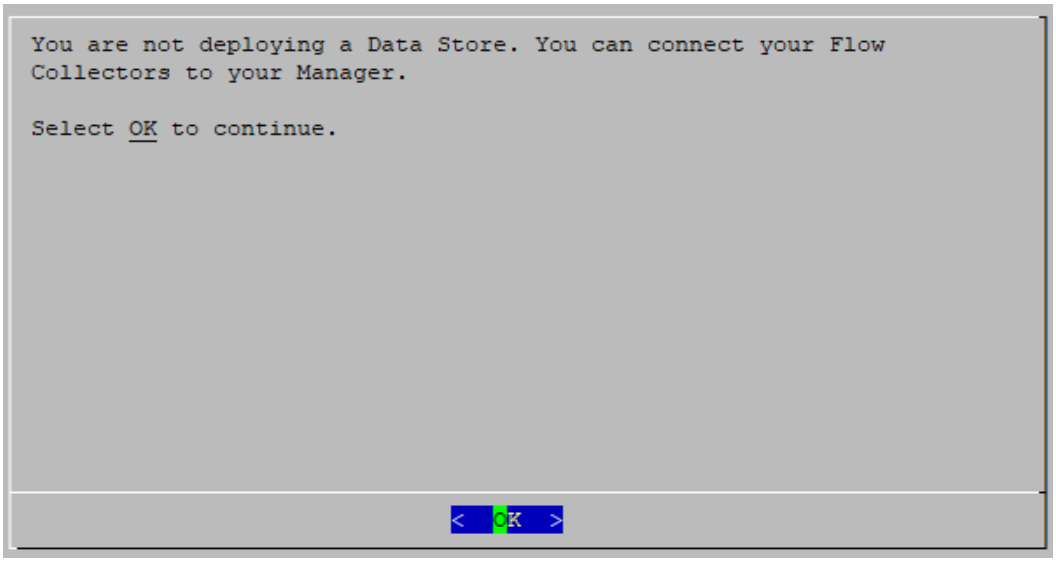


5. 「sysadminとして続行しますか？（Are you sure you want to continue as sysadmin?）」と表示されたら、[はい（Yes）] を選択して、Data Store なしでの設定を続行します。

> ⚠ 必ず [はい（Yes）] を選択してください。Data Store ありで Secure Network Analytics を展開する必要がある場合は、このセクションの手順ではなく、「**Data Store ありの Flow Collector の設定**」の手順に従います。
> 選択を誤った場合は、新しい仮想アプライアンスを展開するか、仮想アプライアンスを RFD してください。

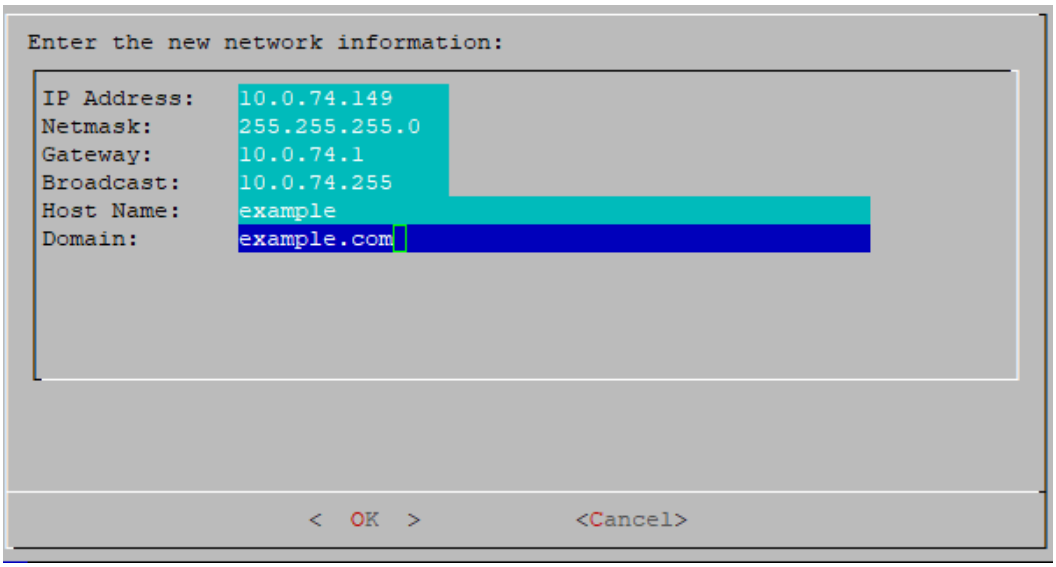


6. Data Store なしで Secure Network Analytics を展開していることを確認します。[OK] を選択して続行します。

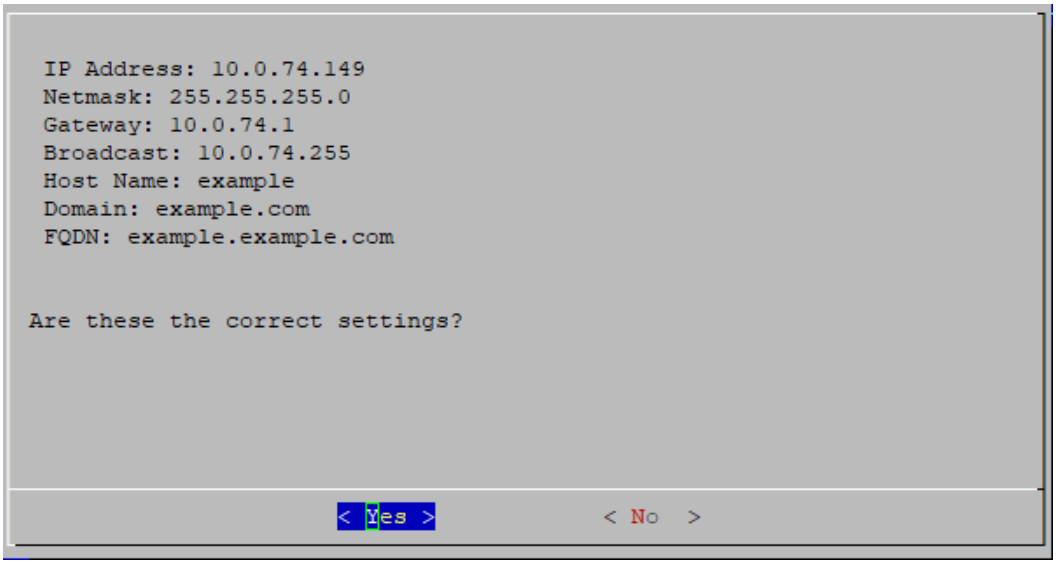


7. 管理インターフェイスの [IPアドレス(IP Address)]、[ネットマスク(Netmask)]、[ゲートウェイ(Gateway)]、[ブロードキャスト(Broadcast)]、[ホスト名(Host Name)]、[ドメイン(Domain)] を入力します。[OK] を選択して続行します。

> ⚠ アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。



8. 設定を確認します。[Yes] を選択して続行します。



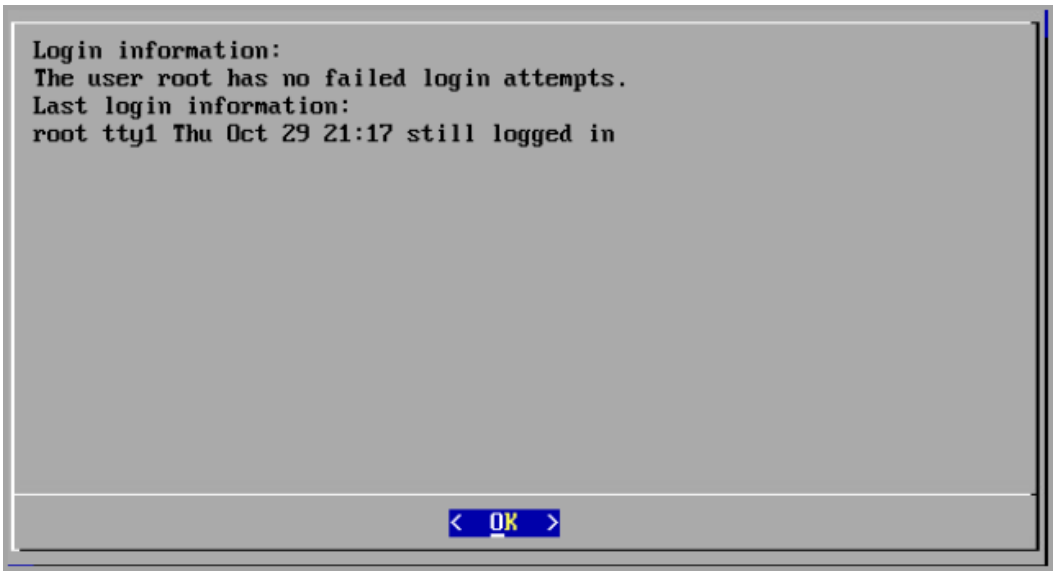
9. [OK] を選択して選択を確定します。画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。
10. Ctrl + Alt を押して、コンソールを終了します。

11. システムの次の Flow Collector について、「**Data Store なしの Flow Collector の設定**」に記載されているすべての手順を繰り返します。

    - 初回セットアップで Data Store なしですべての Flow Collector を設定した場合は、次のセクション(「**次の設定:Flow Sensor または UDP Director**」)に進むか、「**アプライアンスの設定の概要**」に戻ってその他のアプライアンスを設定します。
    - 初回セットアップですべてのアプライアンスを設定した場合は、「**2. 管理対象システムの設定**」に進みます。

次の設定:Flow Sensor または UDP Director

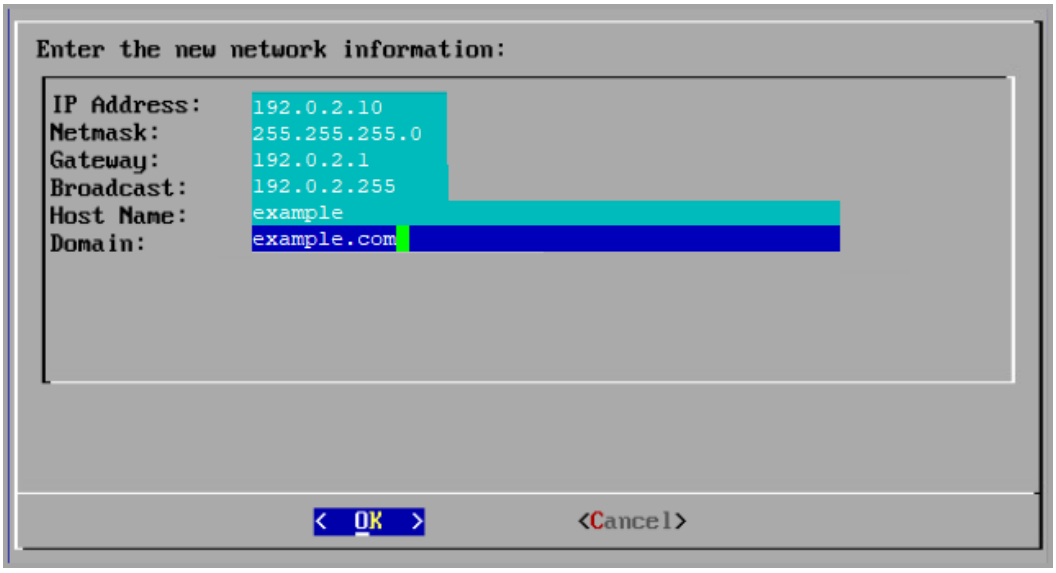
1. コンソールから Flow Sensor か UDP Director にログインします。
    - **ログイン**:sysadmin
    - **デフォルト パスワード**:lan1cope
    - システムを設定するときに、デフォルトのパスワードを変更します。
2. システム設定(`SystemConfig`)が開きます。
3. 失敗したログイン試行の情報を確認します。[OK] を選択して続行します。



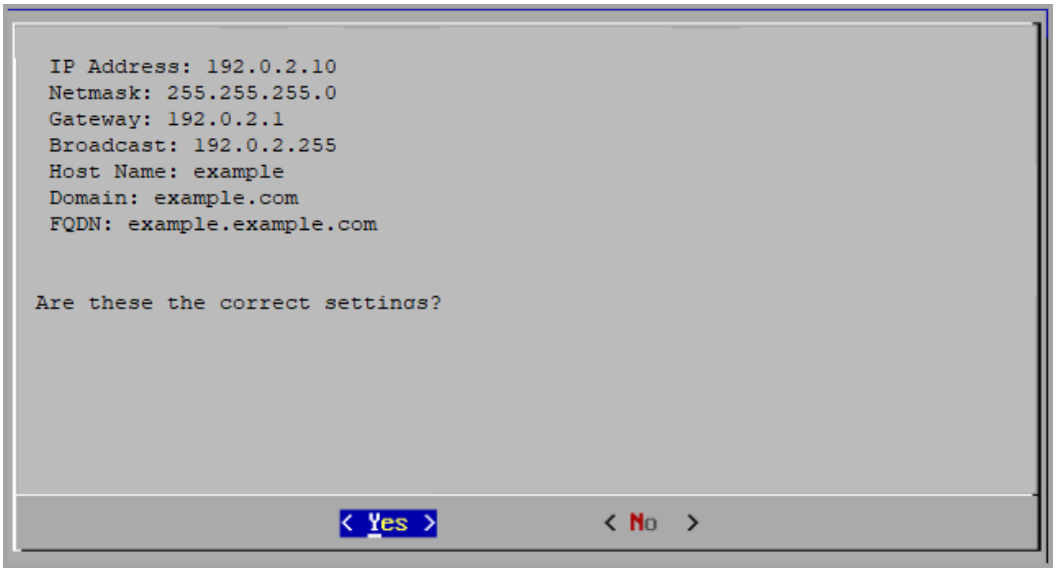
4. 初回セットアップの概要を確認します。[OK] を選択して続行します。

5. 管理インターフェイスの [IPアドレス(IP Address)]、[ネットマスク(Netmask)]、[ゲートウェイ(Gateway)]、[ブロードキャスト(Broadcast)]、[ホスト名(Host Name)]、[ドメイン(Domain)] を入力し、[OK] を選択して続行します。

> ⚠ アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。



6. 設定を確認します。[Yes] を選択して続行します。



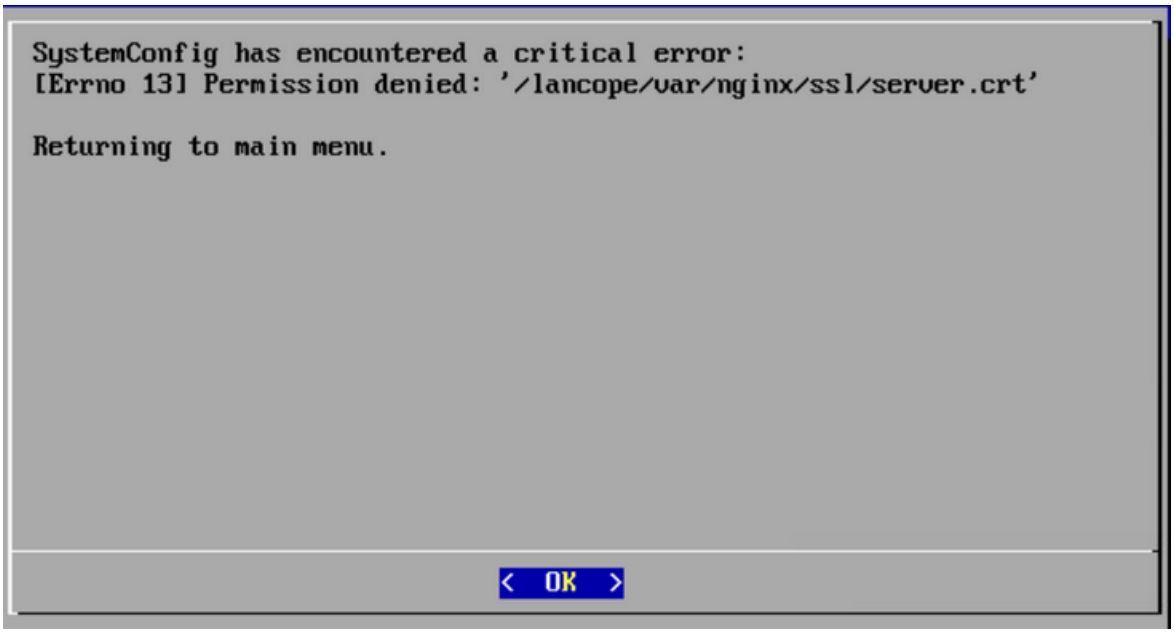
7. [OK] を選択して選択を確定します。画面に表示される指示に従って仮想環境を終了し、アプライアンスを再起動します。
8. Ctrl + Alt を押して、コンソールを終了します。
9. 「**次の設定：Flow Sensor または UDP Director**」の手順を繰り返し、システムで次の Flow Sensor か UDP Director を設定します。

   初回セットアップですべてのアプライアンスを設定した場合は、「**2. 管理対象システムの設定**」に進みます。

トラブルシューティング

証明書エラー

VM 環境の使用率が高い場合は、タイミングエラーが発生し、一部のイベントが順不同で発生する可能性があります。証明書エラー（.crt）が原因で権限が拒否されるという次のようなエラーが表示される場合は、次の手順を実行します。



1. アプライアンスコンソールに sysadmin としてログインします。デフォルトのパスワードは、lan1cope です。
2. [詳細(Advanced)] > [ルートシェル(Root Shell)] の順に選択します。
3. 次のコマンドを実行します。

   ```
   /lancope/admin/plugins/update/.98-FIX-SECRET-PERMS.sh
   ```

4. SystemConfig を実行します。
5. システム設定を終了します。
6. 「**アプライアンスの設定の概要**」に戻り、セクションのすべての手順を完了します。アプライアンスにアクセスできない場合は、シスコサポートにお問い合わせください。

アプライアンスへのアクセス

再起動後にアプライアンスにアクセスできない場合は、次の手順を実行します。

1. root としてログインします。
2. 次のコマンドを実行して、Docker コンテナおよびサービスが稼働していることを確認します。

   - `docker ps`
   - `systemctl list-units --failed`
   - `systemd-analyze critical-chain`

3. すべての Docker コンテナおよびサービスが稼働状態になったら、ログインを再試行します。アプライアンスにアクセスできない場合は、シスコサポートにお問い合わせください。

2. 管理対象システムの設定

初めてアプライアンスにログインする場合、アプライアンス設定ツールを使用して各アプライアンスを設定し、Manager で管理できるようにします。

準備

設定を開始する前に、手順を確認して、アプライアンスの設定順序、ベストプラクティス、および追加要件を理解してください。

アプライアンス設定ツールの要件

- ファイアウォールと ACL（アクセス制御リスト）でアクセスが許可されていることを確認します。
- アプライアンスのホスト名と次の IP アドレスを収集します。
    - アプライアンス
    - サブネット マスク
    - デフォルト ゲートウェイとブロードキャスト ゲートウェイ
    - NTP サーバーと DNS サーバー
    - Manager Central Management の IP アドレス

詳細については、「**アプライアンス設定要件**」を参照してください。

管理対象アプライアンス

アプライアンス設定ツールの実行の一環として、プライマリ Manager によって管理されるようにアプライアンスを設定します。

アプライアンスが Manager によって管理されている場合、Central Management を使用してアプライアンス設定の編集、ソフトウェアの更新、再起動、シャットダウンなどができます。

Manager フェールオーバー

複数の Manager がある場合、Manager フェールオーバーペアを設定して、それらの 1 つを他方のバックアップコンソールとして動作させることができます。

- 各 Manager を設定するには、アプライアンス設定ツールを使用します。
- プライマリとセカンダリにする Manager を計画します。
- アプライアンス設定ツールを使用して Manager とその他のすべてのアプライアンスを設定した後に Manager のフェールオーバー関係を定義します。詳細については、「**3. Manager フェールオーバー関係の定義**」を参照してください。

Cisco Secure Network Analytics ドメイン

Manager を設定するときに、Secure Network Analytics アプライアンスの Data Store ドメインか非 Data Store ドメインを作成します。アプライアンス設定ツールで他のアプライアンスを設定するときに、作成したドメインにそれらを追加します。詳細については、「**システム設定のプランニング**」を参照してください。

最初のドメインでシステム設定を完了したら、設定にドメインを追加できます（「**ドメイン**」を参照）。非 Data Store ドメインを使用して Secure Network Analytics を設定する場合、システム設定の完了後

に展開に Data Store を追加できます。「**非 Data Store 展開への Data Store の追加**」に記載されている手順に従います。

ベスト プラクティス

システムを正常に設定するには、このガイドの手順に従っていることを確認します。次のことを確認してください。

- **一度に1 つ**:一度に 1 つのアプライアンスを設定します。クラスタ内で次のアプライアンスの設定を開始する前に、アプライアンスが [接続済み(Connected)](または [Data Storeが初期化されていません(Data Store Not Initialized)])になっていることを確認します。
- **順序**:「アプライアンスの設定順序」に従います。
- **複数の Central Manager**:システムには複数の Central Manager を設定できます。ただし、各アプライアンスは 1 つのプライマリ Manager/Central Manager でのみ管理できます。
- **アクセス**:Central Management にアクセスするための管理者権限が必要です。

アプライアンスの設定順序

次の順序でアプライアンスを設定し、各アプライアンスの詳細を書き留めます。

順序	アプライアンス	詳細
1.	プライマリ Manager	プライマリ Manager は、Central Manager です。 システム内で次のアプライアンスの設定を開始する前に、Manager が [接続済み(Connected)] と表示されていることを確認します。 Manager を設定するときに、Data Store あり(Data Store ドメイン)か Data Store なし(非 Data Store ドメイン)で Secure Network Analytics ドメインを作成します。
2.	すべてのデータノード	Data Store 展開に必要です。 クラスタ内で次のアプライアンスを設定する前に、Data Node のアプライアンスステータスが [Data Storeが初期化されていません(Data Store Not Initialized)] になっていることを確認します。
3.	Flow Collector 5000 シリーズ データベース	エンジン設定を開始する前に、データベース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。 **データベースとエンジンのペア**:データベースとエンジンのペアが複数ある場合は、各ペアを一度に 1 つずつ設定します。たとえば、ペア 2(database2 と engine2)を設定する前に、ペア 1(database1 と engine1)を設定します。エンジンの設定を開始する前に、各ペアでデータベースが [接続済み(Connected)] と表示されていることを確認します。 また、一意のホスト名を設定するときは、データベースと

		エンジンの各ペアに名前を付けて、中央管理で識別できるようにします。 システム設定を完了すると、各ペアの信頼ストアにあるアプライアンス ID 証明書を確認できます。詳細については、「**信頼ストア証明書の確認**」を参照してください。
4.	Flow Collector 5000 シリーズ エンジン	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [接続済み(Connected)] と表示されていることを確認します。
5.	その他のすべての Flow Collector	**Data Store ありの Flow Collector**:クラスタ内で次のアプライアンスを設定する前に、アプライアンスステータスが [データストアが初期化されていません(Data Store Not Initialized)] になっていることを確認します。 **Data Store なしの Flow Collector**:クラスタ内で次のアプライアンスを設定する前に、アプライアンスステータスが [接続済み(Connected)] になっていることを確認します。
6.	UDP Director (別名 FlowReplicators)	クラスタ内で次のアプライアンスを設定する前に、UDP Director のアプライアンスステータスが [接続済み(Connected)] になっていることを確認します。 UDP Director の代わりに Cisco Telemetry Broker をインストールする場合は、Secure Network Analytics のシステム設定を完了します。その後、『Cisco Telemetry Broker 仮想アプライアンス導入および設定ガイド』の手順に従います。
7.	Flow Sensor	Flow Sensor の設定を開始する前に、Flow Sensor のアプライアンスステータスが [接続済み(Connected)] になっていることを確認します。
8.	セカンダリ Manager (使用する場合)	セカンダリ Manager の設定を開始する前に、プライマリ Manager のアプライアンスステータスが [接続済み(Connected)] と表示されていることを確認します。 セカンダリ Manager は、自身を Central Manager として選択します。アプライアンス設定ツールですべてのアプライアンスを設定した後にフェールオーバーを設定します。詳細については、「**3. Manager フェールオーバー関係の定義**」を参照してください。

システムによっては、ここに示されているアプライアンスの一部が存在しない場合があります。

1. アプライアンス設定ツールへのログイン

アプライアンス設定ツールを使用して各アプライアンスを設定するには、次の手順を使用します。

1. ブラウザのアドレス フィールドに、**https://** およびアプライアンスの IP アドレスを入力します。

   - **プライマリ Manager**：最初にプライマリ Manager を設定します。
   - **接続済み**：クラスタ内で次のアプライアンスの設定を開始する前に、各アプライアンスが [接続済み（Connected）] か [Data Storeが初期化されていません（Data Store Not Initialized）] になっていることを確認します。
   - **順番**：アプライアンスが正常に通信するように、必ずそれらを順番どおり設定します。

> アプライアンスにアクセスできない場合は、「1. 初回セットアップを使用した環境の設定」の「トラブルシューティング」を参照してください。

2. 次のクレデンシャルを入力して、ログインします。

   - **ユーザー名**：admin
   - **パスワード**：lan411cope

> これが初回インストールでない場合は、（このガイドの最後の）「トラブルシューティング」に移動して、ホスト名、ネットワークドメイン名、IP アドレスなどのアプライアンスネットワーク設定を変更します。

2. アプライアンスの設定

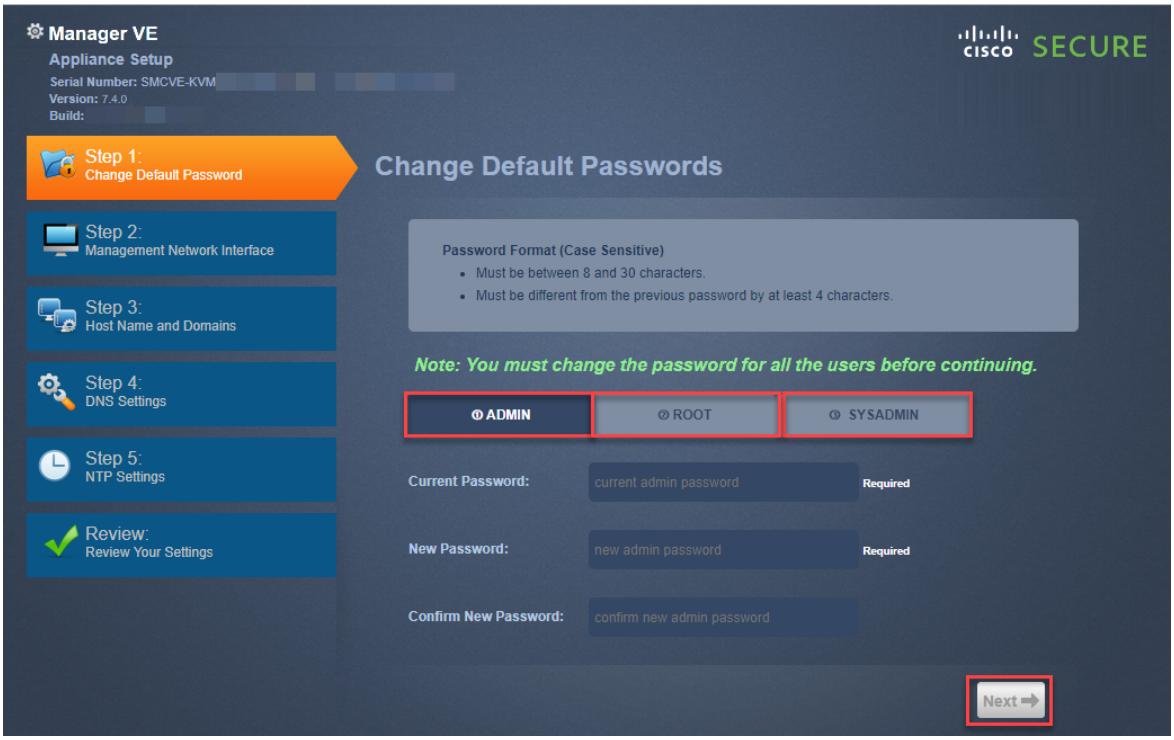
初めてアプライアンスにログインする場合、アプライアンス設定ツールによって各設定手順が示されます。

1. **デフォルト パスワードの変更**:admin、root、および sysadmin の新しいパスワードを入力します。[次へ(Next)] をクリックして各ユーザーにスクロールします。

   次の基準を使用します。

   - 長さ:8 ～ 256 文字
   - **変更**:新しいパスワードがデフォルト パスワードと最低 4 文字異なっていることを確認します。

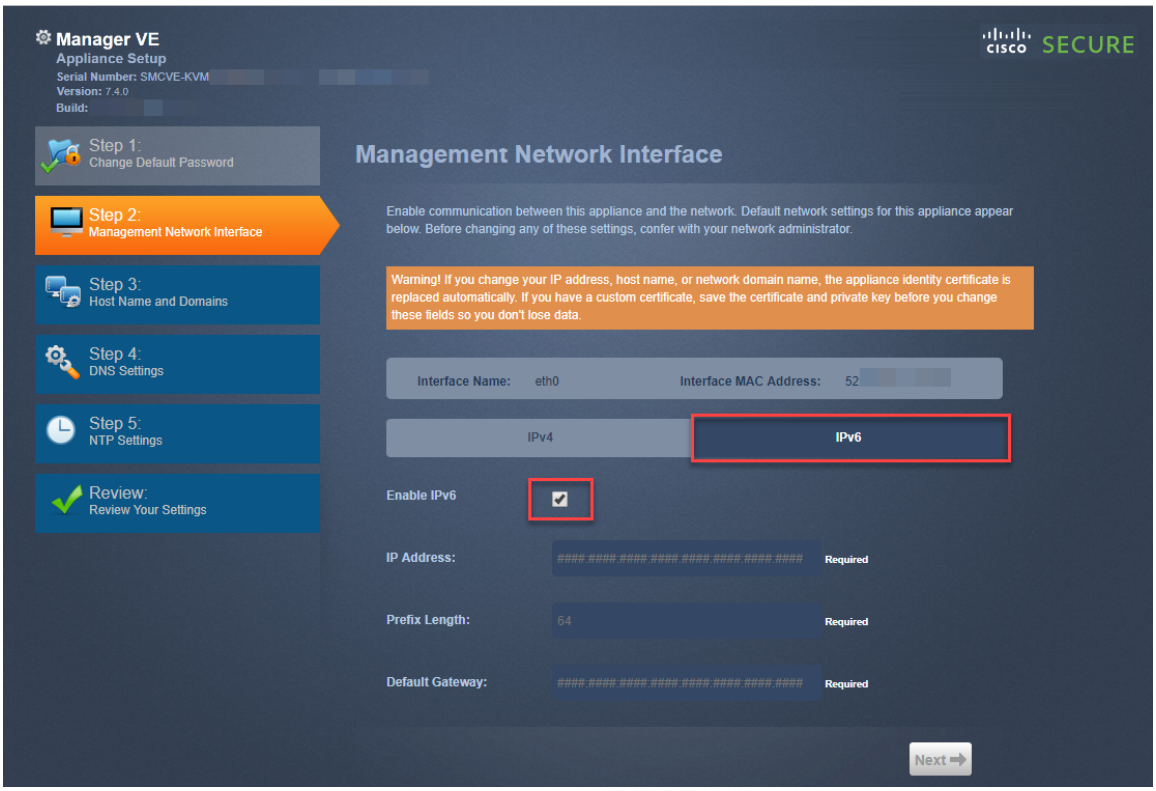
ユーザー	デフォルト パスワード
admin	lan411cope
root	lan1cope
sysadmin	lan1cope



> すでにハードウェア設置時にデフォルト パスワードを変更している場合は、[sysadmin] メニューと [root] メニューは使用できません。

2. **管理ネットワーク インターフェイス**：IP アドレスおよびネットワーク インターフェイス フィールドを確認します。デフォルト設定が正しいことを確認します。[次へ（Next）] をクリックします。

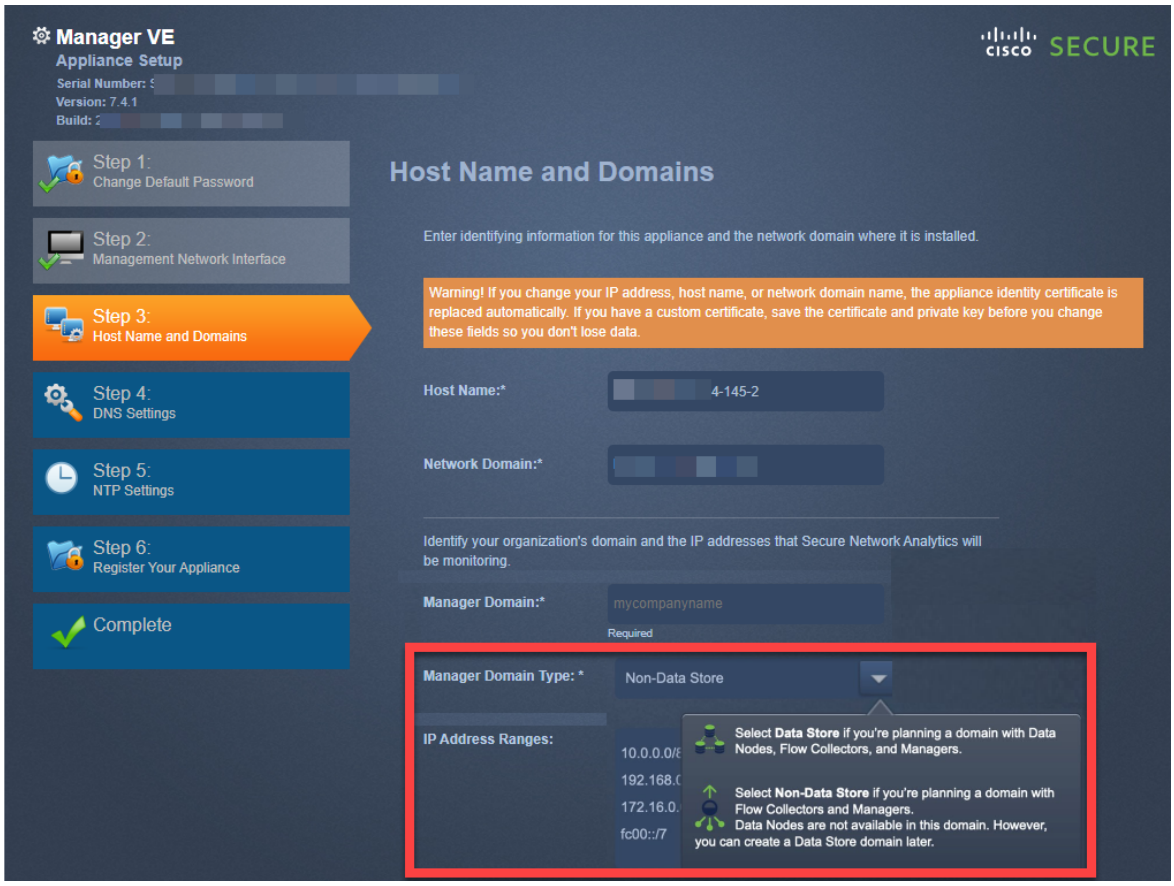
   - **変更**：この情報を変更するには、ネットワーク管理者と協議するとともに、「トラブルシューティング」を参照してください。
   - **IPv6（オプション）**：IPv6 を有効にするには、[IPv6] をクリックします。[IPv6 の有効化（Enable IPv6）] チェックボックスをオンにして、フィールドに入力します。



3. **ホスト名とドメイン**：次の情報を入力します。[次へ（Next）] をクリックします。

フィールド名	注記
ホスト名	アプライアンスには一意のホスト名が必要です。複数のアプライアンスに同じホスト名を割り当てた場合、それらは正常にインストールされません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。 **Flow Collector 5000 シリーズのデータベースとエンジンのペア**：各データベースとエンジンのペアに、中央管理でペアを識別しやすいように一意のホスト名を付けます。たとえば、database1 と engine1、database2 と engine2 などです。

ネットワークドメイン（Network Domain）	各アプライアンスには完全修飾ドメイン名が必要です。
Manager ドメイン（Manager Domain）（Manager のみ）	Secure Network Analytics 展開のドメイン名を入力します。
Manager ドメインタイプ（Domain Type） Manager（のみ）	**Data Store ドメイン**：初回セットアップで Data Store ありのアプライアンスを設定した場合は、[Data Storeドメイン（Data Store Domain）] を選択します。 **非Data Storeドメイン**：初回セットアップで Data Store なしのアプライアンスを設定した場合は、[非Data Storeドメイン（Non-Data Store Domain）] を選択します。 このガイドのシステム設定を完了したら、展開にドメインを追加できます。「**ドメイン**」を参照してください。
IP アドレス範囲（IP Address Ranges）（Manager のみ）	Secure Network Analytics ネットワークの IP アドレス範囲を選択します。



4. **DNS 設定**：デフォルトが正しいことを確認するか、ドメイン サーバー IP アドレスを入力します。[次へ（Next）] をクリックします。

   DNS サーバーの追加または削除（オプション）

   - **追加**：[+] アイコンをクリックします。
   - **削除**：チェックボックスをクリックして DNS サーバーを選択します。[–] アイコンをクリックします。

5. **NTP の設定**：デフォルトが正しいことを確認するか、[メニュー（Menu）] アイコンをクリックして Network Time Protocol（NTP）サーバーを選択します。[次へ（Next）] をクリックします。

   - **複数の NTPサーバー**：冗長性と精度を確保するために複数の NTP サーバーを設定することをお勧めします。
   - **パブリック ソース**：NTP の適切なパブリック ソースとして pool.ntp.org が適しています。

   NTP サーバーの追加または削除（オプション）

   - **追加**：[+] アイコンをクリックします。
   - **削除**：チェックボックスをクリックして NTP サーバーを選択します。[–] アイコンをクリックします。

6. プライマリ Manager は、Central Manager です。次のように Central Management にアプライアンスを追加します。

   - **Manager**：アプライアンスが Manager の場合は 3. 次の登録：Managerの登録」に進みます。
   - **その他すべてのアプライアンス**：アプライアンスが Manager でない場合は、「4. Central Management へのアプライアンスの追加」に進みます。

3. 次の登録：Manager

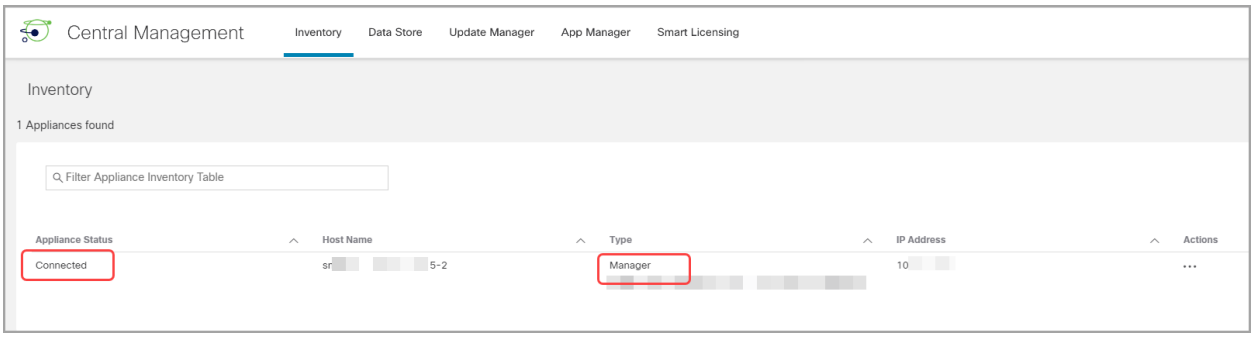
1. **設定を確認**：アプライアンスの情報が正確であることを確認します。
2. [適用（Apply）] または [再起動して続行（Restart and Proceed）] をクリックします。

   - アプライアンスの再起動中は、画面に表示される指示に従います。
   - 新しいシステム設定が有効になるまで数分待ちます。ページの更新が必要な場合があります。

3. Manager にログインします。
4. アプライアンス設定ツールが再び開きます。**[続行(Continue)]** をクリックします。
5. [アプライアンスの登録(Register Your Appliance)] タブで IP アドレスを確認し、[保存(Save)] をクリックします。

    - Manager IP アドレスは自動的に検出されるため、変更できません。
    - この手順で Manager に Central Management がインストールされます。

6. アプライアンスの設定が完了したら、**[ダッシュボードに移動(Go to Dashboard)]** をクリックします。
7. [構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
8. インベントリを確認します。Manager のアプライアンスステータスが [接続済み(Connected)] と表示されていることを確認します。



> クラスタ内で次のアプライアンスの設定を開始する前に、プライマリ Manager のアプライアンスステータスが [接続済み(Connected)] と表示されていることを確認します(設定の順序と詳細を使用)。

9. システム内で次のアプライアンスを設定するには、「**1. アプライアンス設定ツールへのログイン**」に戻り、クラスタ内で次のアプライアンスを設定します。

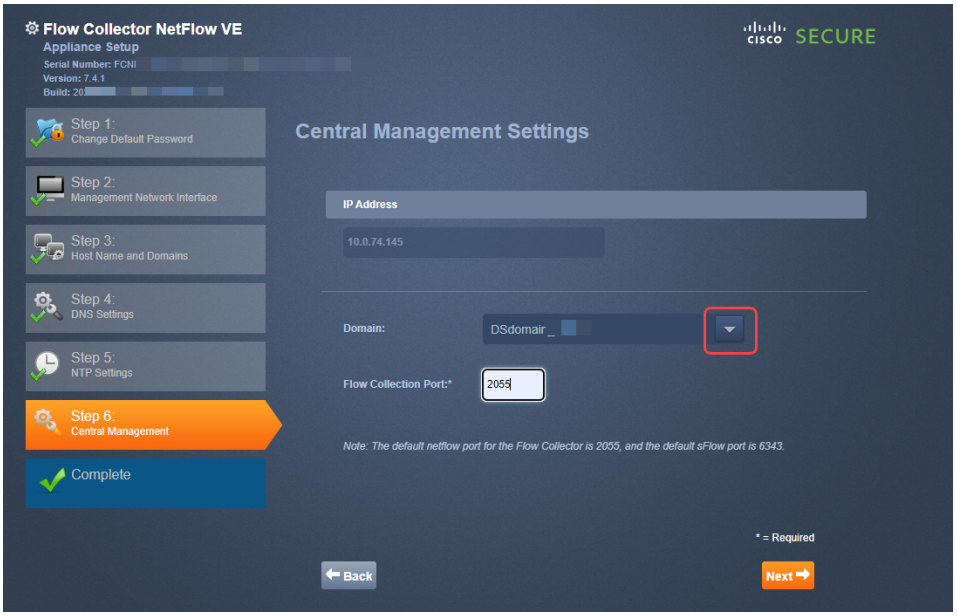
4. Central Management へのアプライアンスの追加

アプライアンス設定ツールを使用して、Central Management でのアプライアンスの設定を続けます。一部の手順は、アプライアンスによって異なる場合があります。画面に表示される指示に従って操作します。

1. [集中管理(Central Management)] タブで、プライマリ Manager の IP アドレスを入力します。
2. [保存(Save)] をクリックします。
3. 画面に表示される指示に従って、プライマリ Manager アプライアンスのアイデンティティ証明書を信頼します。[はい(Yes)] をクリックして証明書を信頼し、アプライアンスと Manager の通信を許可します。
4. プライマリ Manager のログインクレデンシャルを入力します。
5. [ドメイン(Domain)]:Secure Network Analytics ドメインを選択します。これは、Manager の登録時に Data Store ドメインか非 Data Store ドメインとして設定したドメインです。

- **Flow Collector**：フローコレクションのポート番号を入力します。NetFlow のデフォルト：2055
- **Flow Sensor**：Flow Collector を選択します。

Secure Network Analytics ドメインの選択



6. ［Central Managementに移動（Go to Central Management）］をクリックします。「5. アプライアンス ステータスの確認」までの手順を完了します。

5. アプライアンス ステータスの確認

アプライアンス設定ツールでアプライアンスを設定したら、Central Management でアプライアンスのステータスを確認します。

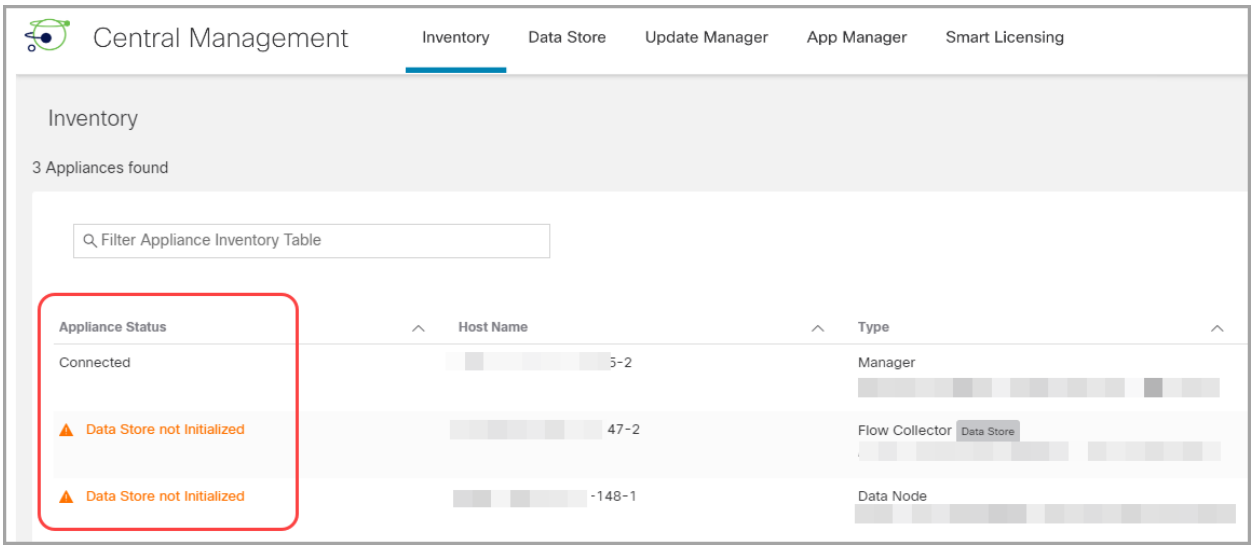
1. アプライアンス設定ツールが Central Management インベントリで開きます。あるいは、次の手順で開くことができます。

   - プライマリ Manager にログインします。
   - ［構成（Configure）］>［グローバル集中管理（GLOBAL Central Management）］を選択します。

2. ［インベントリ（Inventory）］タブでアプライアンスを確認します。

   - アプライアンスがインベントリに表示されていることを確認します。
   - **［アプライアンスステータス（Appliance Status）］**：クラスタ内で次のアプライアンスの設定を開始する前に、プライマリ Manager と各アプライアンスが［接続済み（Connected）］と表示されていることを確認します。

- **[Data Storeが初期化されていません(Data Store Not Initialized)]**:Data Store ドメイン内の Flow Collector と Data Node に関しては、アプライアンスステータスが [Data Store が初期化されていません(Data Store Not Initialized)] になっていることを確認します。後の手順で初期化を完了すると、それらのアプリケーションステータスは [接続済み(Connected)] と表示されます。
- **[タイプ(Type)]**:Flow Collector に Data Store タグがある場合、フローを Data Store データベースに送信するように設定されています。



> クラスタ内で次のアプライアンスの設定を開始する前に、プライマリ Manager と各アプライアンスが [接続済み(Connected)](または [Data Storeが初期化されていません(Data Store Not Initialized)])と表示されていることを確認してください(設定の順序と詳細を使用)。

3. システム内の次のアプライアンスを設定するには、「**1. アプライアンス設定ツールへのログイン**」に進み、「**5. アプライアンス ステータスの確認**」までの手順を完了します。

3. Manager フェールオーバー関係の定義

フェールオーバー設定を使用すると、2 つの Manager 間にフェールオーバーペアを確立し、一方をもう一方のバックアップコンソールとして機能させることができます。Data Store ありの Secure Network Analytics を展開している場合は、Data Store を初期化する前にフェールオーバーを設定することが重要です。

セカンダリ Manager がない場合は、「**5. v7.4.2 パッチのインストール**」に進みます。

フェールオーバーを正しく設定して運用するには、『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』で要件を確認し、その手順に従ってください。

> ⚠ 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ので注意してください。『Secure Network Analytics Failover Configuration Guide』に記載されている順序で Manager のロールを変更してください。

Data Store

Data Store ありの Secure Network Analytics を展開している場合は、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、『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』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。

フェールオーバーの設定

Manager をフェールオーバーペアとして設定するには、『Secure Network Analytics Failover Configuration Guide』の手順に従います。

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。

- **証明書**：アプライアンス間に信頼を設定してアプライアンス同士が通信できるようにするために、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いることを確認します。
- **バックアップファイル**：フェールオーバー設定を開始する前に、アプライアンスをバックアップします。
- **設定の順序**：セカンダリ Manager をフェールオーバー用に設定してからプライマリ Manager を設定します。
- **ロールの変更**：プライマリ Manager がオフラインになった場合は、このガイドに示されている順序で Manager のロールを変更してください。順序は重要で、ロールは自動的に交換されません。
- **トラブルシューティング**：解決策については、『Secure Network Analytics Failover Configuration Guide』を参照してください。

> ⚠ 正しく設定して運用するには、『Secure Network Analytics Failover Configuration Guide』の手順に従ってください。

プライマリおよびセカンダリのロール

設定の一部として、プライマリ Manager とセカンダリ Manager を割り当てます。設定を保存すると、次の処理が行われます。

- **プライマリ Manager**：プライマリ Manager はそのドメイン設定、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。プライマリ Manager では、アプライアンスの管理、アプライアンス設定の変更、パスワードの変更、アラームの定義、ポリシーの適用などを行います。
- **セカンダリManager**：セカンダリ Manager は自身の設定を削除します。したがってプライマリ Manager の構成および設定と同期できます。また、セカンダリ Manager がすべてのユーザーに対して読み取り専用に変更されます。したがって、セカンダリ Manager のセクションにアクセスすることもセカンダリ Manager からファイルを取得することもできなくなります。

4. サイト冗長性の設定

> Data Store が設定されていない場合または冗長サイトを作成したくない場合は、「**6. Data Store の初期化**」に進みます。

サイトの冗長性を使用すると、類似のアプライアンスを使用した個別の展開を含む 2 つの Cisco Secure Network Analytics サイトのクラスタ間でほぼ冗長性を確立できます。サイトの冗長性により、プライマリサイトでドメインと Analytics 構成を維持し、冗長サイトと手動で同期することができます。また、データセンターが停電した場合に高可用性保護を提供します。サイトの冗長性を使用すると、冗長クラスタのいずれかにログインして、ほぼ同じデータを表示できます。

> この機能は、管理者ロールと設定マネージャロールでのみ使用できます。

サイト冗長性設定同期には、次のものが含まれます。

Data Store ドメイン固有の設定とアラート設定（有効な場合）。ドメイン設定には、次のものが含まれます。

- ホストグループ管理
- ポリシー管理
- アプリケーション
- エクスポータ SNMP プロファイル（パスワードを除く）
- アラームの重大度（Alarm Severity）
- サービス
- ドメイン AS 番号

分析設定には、次のものが含まれます。

- Priorities
- 国のウォッチリスト
- アラートの有効期限

冗長サイトの要件

冗長サイト設定を開始する前に、次の要件を確認してください。

- 同じ名前を使用して、プライマリサイトと冗長サイトの両方に冗長 Data Store ドメインを作成します。両方のサイトに同じ数の Data Store ドメインがあり、Data Store ドメイン名が両方のサイトで同じであることを確認します。ドメインの詳細については、「**ドメイン**」を参照してください。

> サイトの冗長性のために同期されるのは Data Store ドメインのみです。非 Data Store ドメインは同期されません。

- Secure Network Analytics ソフトウェアバージョンが両方のサイトで同じであることを確認します。
- 冗長 Manager 証明書をプライマリ Manager 信頼ストアに追加します。詳細については、「信頼ストアへの証明書の追加」を参照してください。
- プライマリ Manager 証明書を冗長 Manager 信頼ストアに追加します。詳細については、「信頼ストアへの証明書の追加」を参照してください。

要件を満たしたら、「冗長サイトの構成」の手順に進むことができます。

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。

- 冗長 Manager 証明書をプライマリ Manager 信頼ストアに追加します。
- プライマリ Manager 証明書を冗長 Manager 信頼ストアに追加します。

証明書チェーン

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. Manager 信頼ストアへの証明書の追加**」に移動してください。

> 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、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、冗長 Manager アプライアンス 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 Manager 信頼ストアに保存します。

1. 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. [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(Actions)] メニューをクリックします。
5. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
6. Central Management のインベントリ > [全般(General)] タブで、[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。
    - 冗長 Manager にログインしている場合は、プライマリ Manager 証明書を追加します。
    - プライマリ Manager にログインしている場合は、冗長 Manager 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)]**: 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。

サイトの冗長構成を開く

サイトの冗長構成を開くには、次の手順を使用します。

1. 管理者または設定管理者として 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Manager(GLOBAL Manager)] を選択します。
3. [サイトの冗長構成(Site Redundancy Configuration)] タブをクリックします。

冗長サイトの構成

冗長サイトを構成するには、次の手順を実行します。

1. [構成を有効にする(Enable Configuration)] チェックボックスをオンにします。
2. [冗長サイトの Manager名(Name of Manager at Redundant Site)] フィールドに、冗長サイトの Manager の完全修飾ドメイン名(FQDN)または IP アドレスを入力します。Manager 名は、Manager アイデンティティ証明書の共通名またはサブジェクトの別名と一致する必要があることに注意してください。
3. [Save] ボタンをクリックして変更を保存します。

4. [同期(Synchronize)] ボタンをクリックして、プライマリサイトとリモートサイトを同期します。これにより、2 つのサイト間でドメイン設定と分析設定が同期されます。
5. 画面の指示に従って、変更の同期を確認します。続行するには、[同期(Synchronize)] をクリックします。

   同期が進行中であることを示す、「進行中」の省略記号のアイコンが表示されます。完了すると、成功または失敗のバナーが表示されます。

   > 同期を実行すると、このプロセスで冗長サイト フロー コレクタ エンジンの設定が上書きされます。1 時間に複数回同期することは推奨しません。

冗長サイトの無効化

冗長サイトを無効にするには、次の手順を実行します。

1. 冗長サイトを無効にするには、[構成を有効にする(Enable Configuration)] チェックボックスをオフにします。
2. [Save] ボタンをクリックして変更を保存します。これにより、冗長サイトと [同期(Synchronize)] ボタンが無効になります。
3. (オプション)無効化された冗長サイトのサイト証明書を削除すると、Secure Network Analytics システムに保護レイヤを追加できます。「冗長サイトの構成」の手順で追加したサイト証明書を削除する場合は、次の手順を実行します。
   1. 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. [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(Actions)] メニューをクリックします。
   5. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
   6. Central Management のインベントリ > [全般(General)] タブで、[信頼ストア(Trust Store)] セクションを見つけます。
   7. [アクション(Actions)] 列で、削除する証明書ごとに [削除(Delete)] をクリックします。

トラブルシューティング

サイトの冗長構成で問題が発生した場合は、次のことを確認してください。

- 証明書が正しい信頼ストアにあることを確認します。詳細については、「信頼ストアへの証明書の追加」を参照してください。
- Secure Network Analytics ソフトウェアバージョンが両方のサイトで同じである必要があります。
- 両方のサイトの Data Store ドメインの数と名前が一致している必要があります。

エラーのログファイルを確認するには、/lancope/var/smc/log/smc-configuration.log に移動します

5. v7.4.2 パッチのインストール

アプライアンスに最新の v7.4.2 パッチをインストールします。

1. Cisco Software Central（https://software.cisco.com）の Cisco スマートアカウントから最新の **v7.4.2 パッチ**をダウンロードします。
2. パッチの readme ファイルの手順に従って、各パッチをインストールします。
3. 最新のパッチでアプライアンスを更新したら、このガイドの次の手順に進みます。

    - **Data Store ドメイン**：「**6. Data Store の初期化**」の手順に従います。
    - **非 Data Store ドメイン**：「**7. デスクトップクライアントのインストール**」の手順に従います。

6. Data Store の初期化

システム設定を使用して Data Store を初期化します。この手順の一環として SSH を一時的に有効にします。

> この手順を開始する前に、すべてのアプライアンスを Central Management のインベントリに追加してください。Flow Collector では、Data Store を初期化する必要はありませんが、初期化プロセスを開始する前に、少なくとも 1 つの Data Node と 1 つの Manager が Central Management のインベントリにある必要があります。

1. Manager アプライアンスコンソール（SystemConfig）に root としてログインします。
2. メニューから [Data Store] を選択します。
3. [SSH] を選択します。画面に表示されるプロンプトに従って SSH を有効にします。
4. [Data Store] メニューから [初期化（Initialization）] を選択します。
5. 画面に表示されるプロンプトに従って Data Store を初期化します。

   [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。

6. 次の「**8. 通信の確認**」の手順に進みます。

7. デスクトップクライアントのインストール

v7.4.0 以降、SMC の名称は Manager に変更されています。このセクション内では、SMC を Manager と記載しています。

Data Store Flow Collector を使用して Secure Network Analytics を展開した場合、デスクトップ クライアント は使用しません。ハイブリッド Data Store/非 Data Store システムの場合、デスクトップ クライアントは 非 Data Store ドメインのみと連携します。

次の情報は、デスクトップクライアントのインストールと使用に適用されます。

- デスクトップクライアントのさまざまなバージョンをローカルにインストールできます。
- デスクトップクライアントには、Stealthwatch Management Console や SMC（Manager）などの Stealthwatch 用語が含まれています。
- デスクトップクライアントの複数のバージョンにアクセスするには、各 Manager において異なる実行ファイルが必要になります。
- プライマリおよびセカンダリ Manager の両方を使用している場合は、一方の Manager をログオフしてからもう一方の Manager にログインする必要があります。
- デスクトップクライアントの複数のバージョンを同時に開くことができます。
- Secure Network Analytics の最新バージョンに更新する場合は、デスクトップクライアントの新しいバージョンをインストールする必要があります。
- Data Store を展開する場合は、Web アプリケーションを使用して Secure Network Analytics インストールをモニターおよび設定します。デスクトップクライアントは Data Store と互換性がありません。

デスクトップクライアントのインストール手順は、Windows と macOS のどちらを使用しているかによって異なります。

- **Windows を使用したデスクトップクライアントのインストール**
- **macOS を使用したデスクトップクライアントのインストール**

また、Windows と macOS のどちらを使用しているかに応じて、メモリサイズを異なる方法で変更します。

- **Windows Explorer からメモリサイズを変更する**
- **Finder からメモリサイズを変更する**

Windows を使用したデスクトップクライアントのインストール

- デスクトップクライアントをインストールするための十分な権限が必要です。
- デスクトップクライアントには、64 ビットのオペレーティングシステムが必要です。32 ビットのオペレーティング システムまたは Linux では実行できません。

以下の手順で、Windows を使用してデスクトップクライアントをインストールします。

1. Manager にログインします。
2. （[ダウンロード（Download）]）アイコンをクリックします。

3. .exe ファイルをクリックして、インストール プロセスを開始します。
4. ウィザードの手順を実行してデスクトップクライアントをインストールします。
5. デスクトップ上のデスクトップ クライアント アイコン をクリックします。
6. [SMCサーバー名(SMC Server Name)] フィールドに、Manager サーバー名または IP アドレス(IPv4 または IPv6)を入力します。
7. Manager ユーザ名とパスワードを入力します。
8. 画面に表示される指示に従ってデスクトップ クライアントを開き、アプライアンスのアイデンティティ証明書を信頼します。

Windows Explorer からメモリサイズを変更する

> デスクトップ クライアント インターフェイスを実行するために、クライアントコンピュータで割り当てるランダムアクセスメモリ(RAM)の量を変更できます。

開いている多数のドキュメントや大量のデータ セット(100,000 個を超えるレコードが含まれたフロークエリなど)を扱う場合は、割り当てるメモリを増やすことを検討してください。

1. Windows Explorer で、ホームディレクトリに移動します。
2. フォルダを次の順に開きます。[AppData] > [ローミング(Roaming)] > [Stealthwatch]。

   フォルダが非表示の場合は、「Stealthwatch」を検索する必要がある場合があります。

3. Stealthwatch ディレクトリで、目的の Stealthwatch バージョンが含まれているフォルダを開きます。
4. 適切な編集アプリケーションを使用して **application.vmoptions** ファイルを開き、編集を開始します(このファイルは、デスクトップクライアントを最初に開いた後に作成されます)。

   最小メモリサイズ(Xms):512 MB 以上を割り当てることをお勧めします。この番号は、ファイルの 3 番目の行に表示されます。

   コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、どの数字が最小メモリ サイズを表しているかを確認してください。

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   最大メモリサイズ(Xmx):最大メモリサイズには、最大でコンピュータの RAM の半分のサイズを割り当てることができます。この番号は、ファイルの 4 番目の行に表示されます。

   コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、最大メモリサイズを表している数字を確認してください。

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   すべての番号を使用します。たとえば、Xmx0.5m ではなく、-xmx512m を入力します。

> - デスクトップクライアントが頻繁に「ハング」する場合は、メモリサイズを大きくします。
> - Java に関連するエラー メッセージが表示される場合は、これよりも小さなメモリ割り当て量を選択してください。

macOS を使用したデスクトップクライアントのインストール

- デスクトップクライアントをインストールするための十分な権限が必要です。
- デスクトップクライアントには、64 ビットのオペレーティングシステムが必要です。32 ビットのオペレーティング システムまたは Linux では実行できません。

以下の手順で、macOS を使用してデスクトップクライアントをインストールします。

1. Manager にログインします。
2. ([ダウンロード(Download)])アイコンをクリックします。
3. .dmg ファイルをクリックして、インストール プロセスを開始します。

   アイコンとフォルダは、以下に示すようにモニターに表示されます。

4. [デスクトップクライアント(Desktop Client)] アイコン( )をアプリケーションフォルダにドラッグします。

   アイコンは、スタート パッドに追加されます。

5. デスクトップ上の [デスクトップクライアント(Desktop Client)] アイコン( )をクリックします。
6. [SMCサーバー名(SMC Server Name)] フィールドに、Manager サーバー名または IP アドレス(IPv4 または IPv6)を入力します。
7. Manager ユーザ名とパスワードを入力します。
8. 画面に表示される指示に従ってデスクトップ クライアントを開き、アプライアンスのアイデンティティ証明書を信頼します。

Finder からメモリサイズを変更する

> デスクトップ クライアント インターフェイスを実行するために、クライアントコンピュータで割り当てるランダムアクセスメモリ(RAM)の量を変更できます。

開いている多数のドキュメントや大量のデータ セット(100,000 個を超えるレコードが含まれたフロークエリなど)を扱う場合は、割り当てるメモリを増やすことを検討してください。

1. 検索で、ホーム ディレクトリに移動します。
2. Stealthwatch フォルダを開きます。
3. Stealthwatch ディレクトリで、目的の Stealthwatch バージョンが含まれているフォルダを開きます。
4. 適切な編集アプリケーションを使用して application.vmoptions ファイルを開き、編集を開始します(このファイルは、デスクトップクライアントを最初に開いた後に作成されます)。

最小メモリサイズ（Xms）：512 MB 以上を割り当てることをお勧めします。この番号は、ファイルの 3 番目の行に表示されます。

コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、どの数字が最小メモリ サイズを表しているかを確認してください。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

最大メモリサイズ（Xmx）：最大メモリサイズには、最大でコンピュータの RAM の半分のサイズを割り当てることができます。この番号は、ファイルの 4 番目の行に表示されます。

コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、最大メモリサイズを表している数字を確認してください。

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

すべての番号を使用します。たとえば、Xmx0.5m ではなく、−xmx512m を入力します。

- デスクトップクライアントが頻繁に「ハング」する場合は、メモリサイズを大きくします。
- Java に関連するエラー メッセージが表示される場合は、これよりも小さなメモリ割り当て量を選択してください。

8. 通信の確認

1. [フロー収集のトレンド(Flow Collection Trend)] の確認

1. プライマリ Manager にログインします。

   フェールオーバー設定:プライマリ Manager とセカンダリ Manager にログインします。

2. [フロー収集のトレンド(Flow Collection Trend)] を確認します。

2. Data Store データベースのステータスの確認

> Data Store ありの Secure Network Analytics を展開しなかった場合は、「**3. 次でのレポートの実行:レポートビルダー**」に進みます。

1. プライマリ Manager ダッシュボードで、[構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
2. [Data Store] タブをクリックします。
3. Data Store データベースのステータスが [アップ(Up)] と表示されていることを確認します。

   データベースのステータスが [ダウン(Down)] の場合は、そのデータベースの [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。[スタート(Start)] を選択します。

4. すべての Data Node のステータスが [アップ(Up)] になっていることを確認します。

   Data Node のステータスが [ダウン(Down)] の場合は、その Data Node の [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。[スタート(Start)] を選択します。

> [Data Store] タブの詳細については、「**Data Store データベース**」を参照してください。

3. 次でのレポートの実行：レポートビルダー

1. ［セキュリティ分析（Security Insight）］ダッシュボードに戻ります。
2. ［レポート（Report）］メニューを選択します。
3. ［レポートビルダー（Report Builder）］を選択します。
4. ［新しいレポートの作成（Create New Report）］をクリックします。
5. ［Flow Collectorによるフロー収集のトレンド（Flow Collection Trend by Flow Collector）］テンプレートをクリックします。
6. 必要に応じてパラメータを選択します。［実行（Run）］をクリックします。
7. レポートを参照して、Flow Collector がフローを受信していることを確認します。
8. Flow Collector データベース（5000 シリーズのみ）か Data Store がある場合は、レポートビルダーのダッシュボードに戻って手順 4 ～ 7 を繰り返し、**フローデータベース取り込みトレンドレポート**を実行します。データベースまたは Data Store がフローを受信していることを確認します。

レポートビルダーの詳細については、ヘルプの情報を参照してください。

9. アプライアンス設定の完了

アプライアンスに必要な設定がすべて完了していることを確認します。

アプライアンス	必須設定	オプション設定
データノード	なし	データ圧縮 フローインターフェイス統計
Flow Collector	なし	NetFlow を sFlow に変更
UDP Director	なし	高可用性 （ハードウェアでのみ使用可能）
Flow Sensor	アプリケーション ID およびペイロード	アプリケーションの識別

次のフロー設定の変更：Flow Collector

1. Flow Collector にログインします。
2. [サポート（Support）] > [詳細設定（Advanced Settings）] の順にクリックします。
3. **engine_startup_mode フィールド**に、次のいずれかの値を入力します。

    - モデルファイルのデフォルト値：0
    - NetFlow：1
    - sFlow：2

> engine_startup_mode フィールドが [詳細設定（Advanced Settings）] リストに表示されない場合は、ページ下部の [新しいオプションの追加（Add New Option）] フィールドおよび [オプション値（Option Value）] フィールドを使用して追加できます。

4. [Apply] をクリックし、[OK] をクリックします。
5. Manager にログインします。
6. [設定（Configure）] > [システムフローコレクタ（SYSTEM Flow Collectors）] を選択します。
7. [モニターポート（Monitor Port）] フィールドに次のいずれかの数値を入力します（これらは NetFlow および sFlow の業界標準であるデフォルトのポート番号です。エクスポータが非標準ポートを使用するように設定されている場合は、代わりにそのポート番号を使用する必要があります）。

    - 2055：NetFlow
    - 6343：sFlow

8. [保存（Save）] をクリックして変更内容を保存します。

モードの切り替え（NetFlow から sFlow、または sFlow から NetFlow）が完了すると、前のモードのフローに基づく次の項目がクリアされます。

- キャッシュ：ホストキャッシュ、フローキャッシュ、セキュリティ イベント キャッシュ
- 保存済みのベースラインファイル

フローが新しいモードで処理されているかどうかをダッシュボードのフロートレンドグラフでチェックすることで、モードの切り替えを確認できます。

UDP Director の高可用性の設定

次の手順に従って、UDP Director を高可用性ペアとして設定します。

> 高可用性は、UDP Director ハードウェアアプライアンスでのみ使用できます。高可用性は、仮想アプライアンスでは使用できません。

- **転送ルール**：高可用性を設定する場合、少なくとも 1 つの転送ルールを設定します。「**転送ルールの設定**」を参照してください。
- **高可用性**：複数の UDP Director がある場合、高可用性ペアを設定できます。高可用性を設定する場合、少なくとも 1 つの転送ルールを設定します（「**ハイ アベイラビリティの設定**」を参照）。

転送ルールの設定

UDP Director から Manager へのメッセージ送信には SSL が使用されます。

1. Manager にログインします。
2. [構成（Configure）] > [グローバル（GLOBAL）] **UDP Director**を選択します。
3. アプライアンスの [アクション（Actions）] メニューをクリックします。[転送ルールの設定（Configure Forwarding Rules）] を選択します。
4. [Add New Rule] をクリックします。
5. **説明（Description）**：ルールを識別するための短い説明を入力します。
6. **送信元IPアドレス：ポート（Source IP Address:Port）**：UDP Director にデータを送信するデバイスの IP アドレスを入力し、データ送信用のポート番号を入力します。

   - **形式**：[IP アドレス]:[ポート番号] の構文を使用します。
   - **範囲**：Classless Inter-Domain Routing（CIDR）表記法を使用して IPアドレスの範囲を入力することができます。
   - **すべて**：「All」と入力すれば、このポートで任意の送信元 IP アドレスからデータを受け入れられます。
   - **組み合わせ**：「送信元 IP アドレス:ポート」の組み合わせをルールに追加するには、それらを新しい行に追加します。

   例：

- 10.11.16.38:5322
- 192.168.0.0/16:9000
- All:2055

7. **宛先IPアドレス（Destination IPAddress）**：UDP Director からデータを受け取るデバイスの IP アドレスを入力します。
8. **宛先ポート番号（Destination Port Number）**：受信するデバイスのポート番号を入力します。
9. ［保存（Save）］をクリックします。
10. **オプション**：変更を同期するには、［同期（Sync）］をクリックします。
11. 必要に応じて、転送ルールを追加する手順を繰り返します。
12. 高可用性ペアを設定するには、「**ハイ アベイラビリティの設定**」に進みます。

> 高可用性は、UDP Director ハードウェアアプライアンスでのみ使用できます。高可用性は、仮想アプライアンスでは使用できません。

ハイ アベイラビリティの設定

複数の UDP Director がある場合は、アプライアンス管理インターフェイスを使用して高可用性を設定します。

> 高可用性は、UDP Director ハードウェアアプライアンスでのみ使用できます。高可用性は、仮想アプライアンスでは使用できません。

UDP Director 高可用性（HA）を使用すると、ユーザーは冗長 UDP Director の設定を行えます。両方のノードには完全な冗長性がありますが、一度にオンラインにできるのは 1 つのノードのみです。

> UDP Director で高可用性が設定されていて、Secure Network Analytics をバージョン 7.4.0 以降に更新する場合は、更新後に以下の手順を使用して高可用性を再設定します。
> Secure Network Analytics の更新の詳細については、更新ガイドを参照してください。

プライマリ ノードおよびセカンダリ ノード

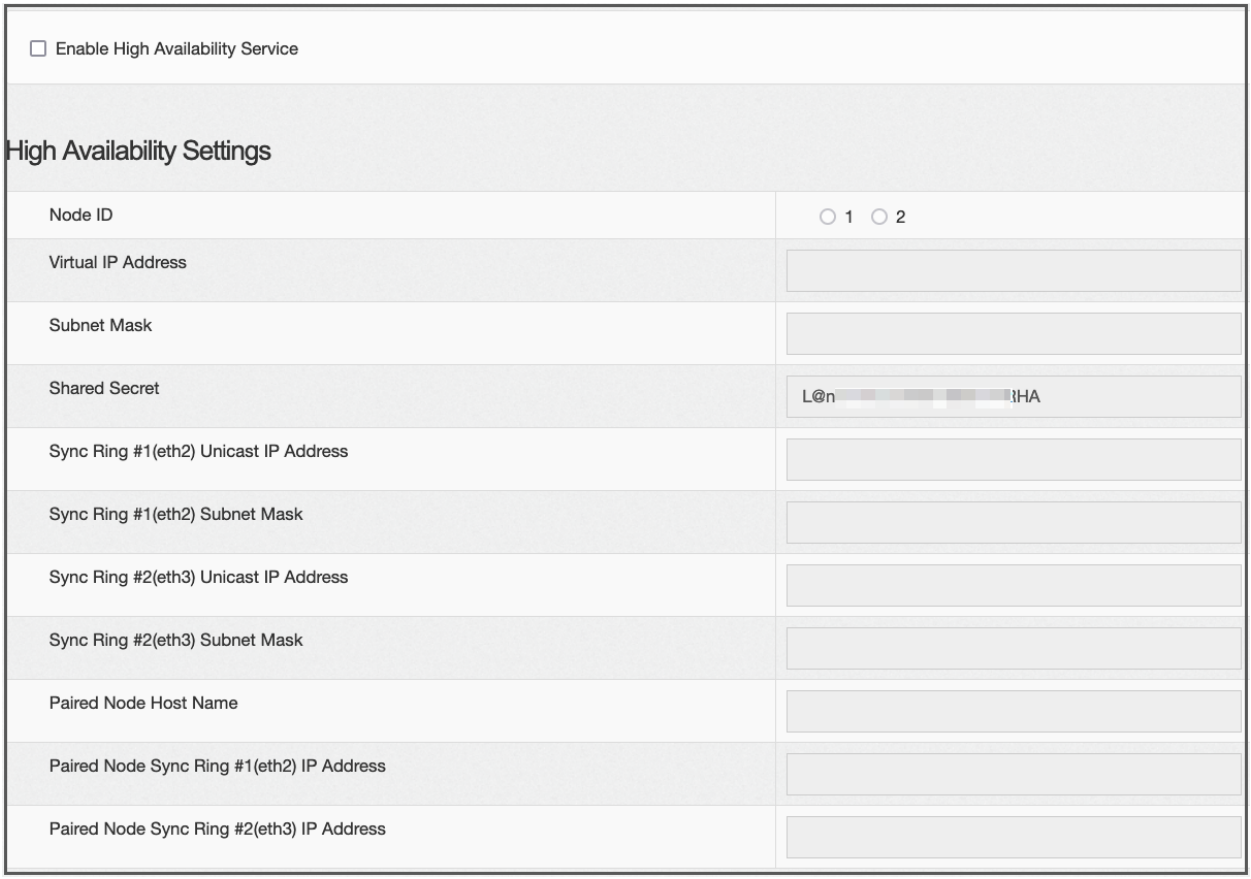
ペアの中でオンライン ノードをプライマリ、オフライン ノードをセカンダリといいます。ペアのプライマリ ノードで障害が発生した場合、セカンダリ ノードがそれを引き継いでプライマリになります。

要件

- 転送ルール：高可用性システムの UDP Director 用の転送ルールを 1 つ以上設定します。
- ルール設定ファイルを保存：UDP Director のルールがすでに設定されている場合、UDP Director ルールをエクスポート（ルール設定ファイルを保存）します。次に、このファイルを 2 番目の UDP Director にインポートして、それぞれのルールが一致するようにします。
- 順序：最初にプライマリ UDP Director を設定した後、セカンダリで設定を繰り返します。
- **新規または設定済み**：どちらも新しい UDP Director である場合、それぞれについてこのガイドの手順に従います。ただし、セカンダリがすでに Secure Network Analytics システム上のアプライアンスとして設定済みの場合は、セカンダリ UDP Director にログインし、このセクションの説明に従って高可用性コンポーネントを設定します。

1. プライマリ UDP Director 高可用性の設定

1. プライマリ UDP Director にログインします。
2. [設定(Configuration)] > [高可用性(High Availability)] をクリックします。
3. 高可用性設定の [高可用性サービスの有効化(Enable High Availability Service)] チェックボックスをオンにします。



4. **[ノードID(Node ID)]** を選択します。プライマリ UDP Director の場合は、1 を選択します。セカンダリ UDP Director の場合は、2 を選択します。
5. **[仮想IPアドレス(Virtual IP Address)]** フィールドに、eth0 インターフェイスと同じサブネット上にある未使用の IP アドレスを入力します。[サブネットマスク(Subnet Mask)] 値を、eth0 インターフェイスで使用されるサブネットマスクの値に設定します。

> i 仮想 IP アドレスが両方のノードで同じであることを確認します。

6. [共有シークレット(Shared Secret)] フィールドに、両方の UDP Director の文字列を入力します(これは暗号化されるため、安全に転送できます)。
7. **同期リング 1(Eth2)ユニキャスト IP アドレス**用のフィールドに、IP アドレスとサブネットマスクを入力します。(ユニキャスト IP アドレスは単一のネットワーク宛先を識別します。)
8. **同期リング 2(Eth3)ユニキャスト IP アドレス**用のフィールドに、IP アドレスとサブネットマスクを入力します。

各 IP アドレス（eth0、eth02、eth03）は、それぞれ別個のユニキャスト サブネット上である必要があります。

9. ［ペアリングされたノードのホスト名（Paired Node Host Name）］フィールドに、セカンダリ UDP Director のホスト名を入力します。
10. ［ペアリングされたノード同期リング 1（eth2）のIPアドレス（Paired Node Sync Ring #1(eth2) IP Address）］フィールドに、セカンダリ UDP Director の Eth2 IP アドレスを入力します。
11. ［ペアリングされたノード同期リング 1（eth3）のIPアドレス（Paired Node Sync Ring #1(eth3) IP Address）］フィールドに、セカンダリ UDP Director の Eth3 IP アドレスを入力します。
12. 設定を確認したら、［適用（Apply）］をクリックして、設定を適用します。
13. クラスタの 2 番目の UDP Director を設定するには、次のセクションに進みます。

2. セカンダリ UDP Director 高可用性の設定

> 前述の手順 4 でノード ID 2 を選択した場合は、プライマリ UDP Director に対して以下の手順を実行します。

セカンダリ UDP Director を設定するには次の手順を実行します。

1. セカンダリ UDP Director にログインします。
2. ［設定（Configuration）］>［高可用性（High Availability）］をクリックします。
3. ［ペアリングされたノードのホスト名（Paired Node Host Name）］フィールドに、セカンダリ UDP Director のホスト名を入力します。
4. この画面ですべてのパラメータを設定します（最初のアプライアンスで詳細パラメータを変更した場合にはそれも含みます）。その際、次の項目を除くすべてのフィールドで、最初のアプライアンスとまったく同じ値を設定してください。

   - **［同期リング#1（eth2）ユニキャストIPアドレス（Sync Ring #1(eth2) Unicast IP Address）］**：プライマリ上のこのフィールドで設定したものとは異なる IP アドレスを入力しますが、プライマリで指定した同期リング 1 ユニキャストアドレスと同じサブネットにある必要があります。
   - **［同期リング#2（eth3）ユニキャストIPアドレス（Sync Ring #2(eth3) Unicast IP Address）］**：プライマリ上のこのフィールドで設定したものとは異なる IP アドレスを入力しますが、プライマリで指定した同期リング 2 ユニキャストアドレスと同じサブネットにある必要があります。
   - **［ペアリングされたノードのホスト名（Paired Node Host Name）］**：このフィールドに、プライマリ UDP Director のホスト名を入力します。
   - **［ペアリングされたノード同期リング1（eth2）のIPアドレス（Paired Node Sync Ring #1 (eth2) IP Address）］**：このフィールドに、プライマリ UDP Director の Eth2 IP アドレスを入力します。
   - **［ペアリングされたノード同期リング1（eth3）のIPアドレス（Paired Node Sync Ring #1 (eth3) IP Address）］**：このフィールドに、プライマリ UDP Director の Eth3 IP アドレスを入力します。

5. [適用(Apply)] をクリックして変更内容を保存し、このアプライアンスのクラスタリング サービスを開始します。
6. プライマリ アプライアンスを指定するには、[昇格(Promote)] ボタンをクリックします。

次の設定 : Flow Sensor

1. アプリケーション ID およびペイロードの設定

Flow Sensor を設定するには、アプリケーション ID とペイロードを設定する追加の手順が必要です。

1. Flow Sensor 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。
2. [設定(Configuration)] > [詳細設定(Advanced Settings)] をクリックします。

[詳細設定(Advanced Settings)] ページが開きます。

3. ネットワークに関する適切な設定を次のように選択します。

項目	説明
パケット ペイロードのエクスポート(Export Packet Payload)	Flow Sensor が Collector に送るデータの中に、最初の 26 バイトのバイナリペイロードデータを含めるかどうかを指定できます。
アプリケーション識別情報のエクスポート(Export Applications Identification)	Collector にデータを送る前に、Flow Sensor がアプリケーションの識別を試みるかどうかを指定できます。さらに、次の設定が効果を及ぼすには、この設定を有効にする必要があります。 IPv6を含める(Include IPv6) : Flow Sensor で IPv4 と IPv6 両方のパケットを分析するかどうかを指定できます。この設定を無効にすると、Flow Sensor は IPv4 パケットのみを分析します。 HTTPSヘッダーデータのエクスポート(Export HTTPS Header Data) : Flow Sensor から Collector に送るデータの中に、HTTPS フローのヘッダーデータを含めるかどうかを指定できます。データには SSL 共通名と SSL 組織名が含まれます。この設定を使用するには、フロー タイプが IPFIX に設定されている必要があります。最大 256 バイトが可能です。 HTTPヘッダーデータのエクスポート(Export HTTP Header Data) : Flow Sensor から Collector に送るデータの中に、HTTP フローのヘッダーデータを含めるかどうかを指定できます。この設定を選択すると、Flow Sensor がフローデータの一部として含める HTTP パスの最大長(バイト単位)をセカンダリフィールドで指定できます。この設定を使用するには、フロー タイプが IPFIX に設定されている必要があります。

項目	説明
VXLAN カプセル化解除の有効化（Enable VXLAN Decapsulation）	Flow Sensor が Virtual Extensible Local Area Network（VXLAN）カプセル化解除機能を使用するかどうかを指定できます。VXLAN カプセル化解除を使用しない場合、Flow Sensor は単純に 2 つの仮想トンネルエンドポイント（VTEP）間のフローとして VXLAN カプセル化トラフィックを検出します。カプセル化解除を使用すると、トンネル化されたトラフィックを分析して、ネットワーク内のトラフィックパターンをより詳細に把握できるため、より豊富なコンテンツを取得できます。 Flow Sensor は、標準の VXLAN ポート（4789）に元々送信された VXLAN トラフィックだけをカプセル化解除します。
GENEVEカプセル化解除の有効化（Enable GENEVE Decapsulation）	Flow Sensor がモニタリングポートで受信したトラフィックに対して Generic Network Virtualization Encapsulation（GENEVE）カプセル化解除を使用するかどうかを指定できます。
ERSPANカプセル化解除の有効化（Enable ERSPAN Decapsulation）	Flow Sensor で Encapsulated Remote Switching Port Analyzer（ERSPAN）のカプセル化解除機能を使用してパケット内の ERSPAN ヘッダーを検出し、ヘッダーのカプセル化を解除してカプセル化されていたパケットの中身を処理するかどうかを指定できます。 Flow Sensor の ERSPAN トンネルを終了できるようにするには、モニタリング インターフェイスに IP アドレスを割り当てる必要があります。 FS 4210 の ERSPAN のカプセル化解除はサポートされていません。
X-Forwarded-For 処理の有効化（Enable X-Forwarded-For Processing）	Flow Sensor が X-Forwarded-For（XFF）処理を使用して、HTTP プロキシまたはロードバランサを介して Web サーバーに接続しているクライアントの発信元 IP アドレスを識別するかどうかを指定できます。 ETA と X-Forwarded-For 処理を一緒に設定することはできません。

項目	説明
ETA 処理の有効化（Enable ETA Processing）	Flow Sensor が ETA 処理を使用して IDP および SPLT フィールドを生成し、Manager に送信するかどうかを指定できます。 ETA を有効にすると、特に v9 使用時の NetFlow 帯域幅の使用量が増加します。フローエクスポート形式には IPFIX を使用することをお勧めします。 ETA と X-Forwarded-For 処理を一緒に設定することはできません。 ETA を Dell または PowerEdge Flow Sensor モデルで有効にすることはできません。
ロード バランシングの有効化（Enable Load Balancing）	Flow Sensor 4000 シリーズが複数の Flow Collector にフローデータを配信できるかどうかを指定できます。 Flow Sensor からのフローデータが 1 つの Flow Collector のキャパシティを超える場合には、このオプションを使用します。
インターフェイス選択のモニターリング	以下の項目を指定できます。 • Flow Sensor 4240：2 x 40G または 4 x 10G（SFP）インターフェイス • Flow Sensor 4300：2 x 40G/100G または 4 x 10G（SFP）インターフェイス この設定が正常に機能するには、複数の Flow Collector を使用し、ロードバランシングを有効にしておく必要があります。詳細については、『Flow Sensor とロードバランサの統合ガイド』を参照してください。 このオプションは、Flow Sensor 4240 および Flow Sensor 4300 でのみ使用できます。 Flow Sensor 4240 のデフォルト設定は 2 x 40G ですが、Flow Sensor 4300 のデフォルト設定は 2 x 40G/100G です。

項目	説明
キャッシュ モード（Cache Mode）	次のいずれかの設定を選択できます。 すべての監視ポートに単一の共有キャッシュを使用（Use single, shared, cache for all monitoring ports）： • 非対称ルーティングが存在する場合に使用します。 • アプリケーションと遅延計算に 1 つの状態テーブル。 • より少ないメモリを使用。 • 全体的により低い pps 処理率。 • 結果として複数のインターフェイス全体で 1 つの NetFlow イベントが作成されます。 • Flow Sensor にポートが 2 つだけ存在し、TAP で接続されている場合にのみ使用します。 監視ポートごとに独立したキャッシュを使用（Use independent caches for each monitoring port）： • 各 Flow Sensor インターフェイスでパケットの重複排除を許可する。 • より多くのメモリを使用。 • 全体的により高い pps 処理率。 • 各インターフェイスは独自の遅延とアプリケーション データベースを維持します。 • 結果として、特定のパケットを認識するインターフェイスごとに固有の NetFlow レコードが生成されます。

4. ［適用（Apply）］をクリックして設定を保存します。

2. アプリケーションを識別するための Flow Sensor の設定（オプション）

Flow Sensor でアプリケーションを識別する場合は、次のように設定します。

1. Flow Sensor 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。
2. [設定（Configuration）] > [詳細設定（Advanced Settings）] をクリックします。
3. [アプリケーションIDのエクスポート（Export Application Identification）] チェックボックスをオンにします。デフォルトでは、このオプションは選択されていません。
4. 複数の監視 NIC がある場合、[キャッシュ モード（Cache Mode）] セクションで次のいずれかのオプションを選択します。

   - **すべてのモニターリング ポートに単一の共有キャッシュを使用する（Use single, shared, cache for all monitoring ports）**：通常、TAP 方式でフローをモニターリングするシステムに対して使用します。

   - **モニターリング ポートごとに個別のキャッシュを使用する（Use independent caches for each monitoring port）**：通常、SPAN 方式でフローをモニターリングするシステムの場合、およびパフォーマンスを強化する必要がある場合に使用します。

3. アプライアンスの再起動

1. [操作（Operations）] > [アプライアンスの再起動（Restart Appliance）] を選択します。
2. Central Management でアプライアンスステータスが [接続済み（Connected）] になっていることを確認します。

10. テレメトリの設定

Data Store を使用してデプロイした場合、は複数のタイプのテレメトリを同時に取り込むことができます。Secure Network AnalyticsFlow Collector初回セットアップ時にフローコレクタを構成できます。既存のフローコレクタの場合は、フローコレクタの詳細設定を使用してテレメトリ取得設定を更新できます。

> ⚠ テレメトリポートが一意であることを確認します。テレメトリポートを重複して設定すると、フローデータの消失を回避するためにポートが内部のデフォルト値にリセットされます。たとえば、NetFlow と NVM が同じテレメトリポートにエクスポートされると、NVM データをエクスポートする各デバイスがFlow Collectorにエクスポータを作成し、Flow Collectorエンジンのエクスポータリソースを使い切ってしまうため、フローデータが消失します。

ネットワーク可視性モジュール（Network Visibility Module）

[ネットワーク可視性モジュール（NVM）] を選択して設定すると、フローコレクタは NVM フローを取り込んで保存します。『Cisco Secure Network Analytics Endpoint License and Network Visibility Module (NVM) Configuration Guide』の手順に従って、設定のすべての要件を満たします。

ファイアウォールログ（Firewall Logs）

[ファイアウォールログ（Firewall Logs）] を選択して設定すると、フローコレクタは Cisco Security Analytics and Logging（オンプレミス） のファイアウォール イベント ログを取り込んで保存します。『Security Analytics and Logging: Firewall Event Integration Guide』の手順に従って、設定のすべての要件を満たします。

アプリケーション要件：[ファイアウォールログ（Firewall Logs）] を選択して設定する場合は、Manager に セキュリティ分析とロギング（オンプレミス） アプリケーションをインストールします。

テレメトリ設定の更新

NetFlow またはその他のテレメトリを取り込む既存のフローコレクタがある場合は、フローコレクタの詳細設定を使用してテレメトリの取り込み設定を更新できます。[詳細設定（Advanced Settings）] には、次の手順でアクセスします。

1. フローコレクタ（旧アプライアンス管理（Admin）インターフェイス）にログインします。
2. [サポート（Support）] > [詳細設定（Advanced Settings）] を選択します。

> ℹ 各テレメトリタイプの設定は 2 つあります。[詳細設定（Advanced Settings）] を使用したテレメトリ設定の詳細については、[ヘルプ（Help）] の手順に従ってください。❓（**[ヘルプ（Help）]）アイコン** > **[ヘルプ（Help）]** を選択します。

Cisco Telemetry Broker

UDP Director を使用して NetFlow を Flow Collector に送信する代わりに、Cisco Telemetry Broker を使用して多くの入力からネットワークテレメトリを取り込み、テレメトリ形式を変換してそのテレメトリを 1 つ以上の宛先に送信できるようになりました。Cisco Telemetry Broker をインストールするには、『Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide』の手順に従います。

11. Secure Network Analytics ライセンシング

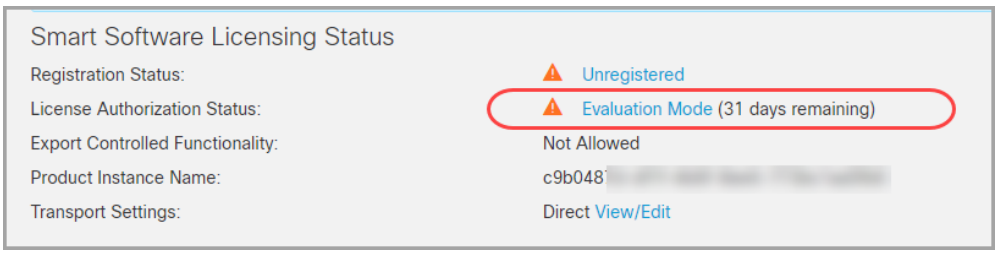
シスコ スマート ソフトウェア ライセンシングを使用して、Secure Network Analytics のアプライアンスおよび機能をライセンシングします。詳細については、cisco.com のスマートライセンシングを参照してください。

- **オンライン**:スマートライセンシングおよび Secure Network Analytics をオンラインで使用するには、『Secure Network Analytics Smart Software Licensing Guide』を参照してください。この設定にはインターネットアクセスが必要です。
- **オフライン**:クローズド/エアギャップネットワークのライセンスオプションの説明については、シスコサポートに連絡してください。
- **Cisco スマートアカウント**:Cisco スマートアカウントを設定するには、https://software.cisco.com で登録するか、管理者にお問い合わせください。

評価モード

Secure Network Analytics を評価モードで使用すると、選択された機能を 90 日間使用できます。Secure Network Analytics のデフォルト機能を最大限に活用してライセンスと機能をアカウントに追加するには、スマート ソフトウェア ライセンシングの製品インスタンスを登録します。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、フロー収集が停止します。フロー収集を再度開始するには、製品インスタンスを登録します。



- **管理者ユーザー**:Manager でスマートライセンシングのステータスと使用状況の詳細を確認するには、管理者ユーザーとしてログインします。
- **残り日数**:評価モードの残り日数を確認するには、管理者ユーザーとして Manager にログインします。[Central Management] > [スマートライセンシング(Smart Licensing)] の順に移動します。[ライセンス承認ステータス(License Authorization Status)] を確認します。
- **製品インスタンス**:製品インスタンス名は、お客様の Secure Network Analytics の製品インスタンスに使用する識別子であり、Manager と管理対象アプライアンスが含まれます。

12. Secure Network Analyticsの管理

アプライアンスの設定が完了したら、ヘルプで環境の管理、動作の調査、脅威への対応などに関する手順を確認できます。

> 手順については、任意のページから [?([ヘルプ(Help)])アイコン] > [ヘルプ(Help)] の順に選択して確認してください。

ホストグループの設定

1. Manager にログインします。
2. [設定(Configure)] > [検出ホストグループ管理(DETECTION Host Group Management)] を選択します。

ポリシーの作成と管理

1. Manager にログインします。
2. [設定(Configure)] > [検出ポリシー管理(DETECTION Policy Management)] を選択します。

フロー検索の作成

1. Manager にログインします。
2. [調査(Investigate)] > [フロー検索(Flow Search)] を選択します。

レポートビルダーでのレポートの実行

1. Manager にログインします。
2. [レポート(Report)] > [レポートビルダー(Report Builder)] を選択します。

ユーザー権限の管理

1. Manager にログインします。
2. [構成(Configure)] > [グローバルユーザー管理(GLOBAL User Management)] を選択します。

動作の調査(アラーム、セキュリティイベントなど)

アラーム、イベント、ホストなどの調査については、ヘルプの情報を参照してください。

1. Manager にログインします。
2. ?([ヘルプ(Help)])アイコンをクリックします。
3. **[ヘルプ(Help)]** を選択します。
4. ページの上部にある **[ヘルプ(Help)]** メニューを選択します。
5. **[動作の調査(Investigating Behavior)]** を選択します。

脅威への対応

ポリシー情報については、ヘルプの情報を参照してください。

1. Manager にログインします。
2. ?([ヘルプ(Help)])アイコンをクリックします。
3. **[ヘルプ(Help)]** を選択します。
4. ページの上部にある [ヘルプ(Help)] メニューを選択します。
5. [脅威への対応(Responding to Threats)] を選択します。

Analytics

Secure Network Analytics は、ダイナミック エンティティ モデリングを使用してネットワークの状態を追跡します。Secure Network Analytics のコンテキストにおけるエンティティとは、ネットワーク上のホストやエンドポイントといった、何らかの経時的に追跡できるものです。ダイナミック エンティティ モデリングは、ネットワークで送信されるトラフィックと実行されるアクティビティに基づいて、エンティティに関する情報を収集します。詳細については、『 Analytics: Detections, Alerts, and Observations Guide』を参照してください。

アプライアンスをインストールするには、『Virtual Edition Appliance Installation Guide』、『x2xx Series Hardware Appliance Installation Guide』、または『x3xx Series Hardware Appliance Installation Guide』[英語] の手順に従います。

アプリケーション

Secure Network Analytics アプリケーションは、Secure Network Analytics の機能を強化および拡張する、独自にリリース可能なオプションの機能です。

Secure Network Analytics アプリケーションのリリーススケジュールは、通常の Secure Network Analytics のアップグレードプロセスとは無関係です。そのため、Secure Network Analytics のコアリリースとリンクさせなくても、必要に応じて Secure Network Analytics アプリケーションを更新できます。Secure Network Analytics の新しいリリースに対応するように設計されたアプリが、すぐにインストールできない場合があります。アプリケーションの最新バージョンが提供されるまでに数週間かかる場合もあります。

最新の Secure Network Analytics アプリケーションの情報、提供状況、および互換性については、次を参照してください。

- Secure Network Analytics アプリケーションのバージョン互換性マトリクス
- Secure Network Analytics アプリケーションのリリースノート

認証/許可

Secure Network Analytics による各認証または許可の設定の詳細については、次の手順を参照してください。

[名前(Name)]	手順
LDAP	ヘルプの手順に従います。 1. Manager にログインします。 2. [構成(Configure)] > [グローバルユーザー管理(GLOBAL User Management)] を選択します。 3. **[認証と許可(Authentication and Authorization)]** タブをクリックします。 4. ?([ヘルプ(Help)])アイコン > [ヘルプ(Help)] を選択します。
セキュリティ アサーション マークアップ言語 シングルサインオン(SAML SSO)	このガイドの「**SAML SSO の設定**」セクションを参照してください。
TACACS+ 構成ガイド	『TACACS+ コンフィギュレーション ガイド』を参照してください。

SAML SSO の設定

以下の手順に従って、セキュリティ アサーション マークアップ言語シングル サインオン(SAML SSO)を設定します。SSO は、ユーザーが 1 組のクレデンシャルで複数のアプリケーションにアクセスすることを可能にする認証プロセスです。

サポートの詳細

次の設定がサポートされているかどうかに注意してください。

サポート対象	サポート対象外
SAML/SSO 対応 Microsoft Active Directory Federation Services(ADFS)	Microsoft ADFS のクラウドサービス
Microsoft ADFS のオンプレミスソリューション	統合 Windows 認証(IWA)
追加のプロキシ	外部サービス(External Services)
	SAML リクエストの署名

デスクトップクライアントは、Data Store 展開ではサポートされません。

1. 設定の準備

SSO を設定するには次の情報が必要です。

要件	詳細
アイデンティティ プロバイダの URL	この URL には完全修飾ドメイン名または IPv4 アドレスを使用する必要があります。
アイデンティティ プロバイダの証明書	IDP の URL が「HTTPS」で始まる場合は、CA 証明書をダウンロードしてください。

2. 信頼ストアへの証明書のアップロード

アイデンティティ サービス プロバイダ（IDP）の URL が「HTTPS」で始まる場合は、**ルート CA 証明書**を Manager 信頼ストアに追加します。

> IDP の URL が「HTTPS」で始まらない場合は、この手順をスキップして次の項「**3. サービス プロバイダの設定**」に進むことができます。

以下の手順に従って、ルート CA 証明書を Manager 信頼ストアに追加します。

1. Central Management の［インベントリ（Inventory）］ページで、Manager の［アクション（Actions）］メニューをクリックします。
2. ［アプライアンス構成の編集（Edit Appliance Configuration）］を選択します。
3. ［Appliance Manager］>［全般（General）］タブで、［信頼ストア（Trust Store）］セクションを見つけます。
4. ［新規追加（Add New）］をクリックします。
5. ［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。
6. ［ファイルの選択（Choose File）］をクリックします。新しい証明書を選択します。
7. ［証明書の追加（Add Certificate）］をクリックします。［信頼ストア（Trust Store）］リストに新しい証明書が表示されることを確認します。
8. ［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。
9. **［接続済み（Connected）］**：［インベントリ（Inventory）］ページで、Manager が設定変更を完了し、アプライアンスステータスが［接続済み（Connected）］に戻ることを確認します。

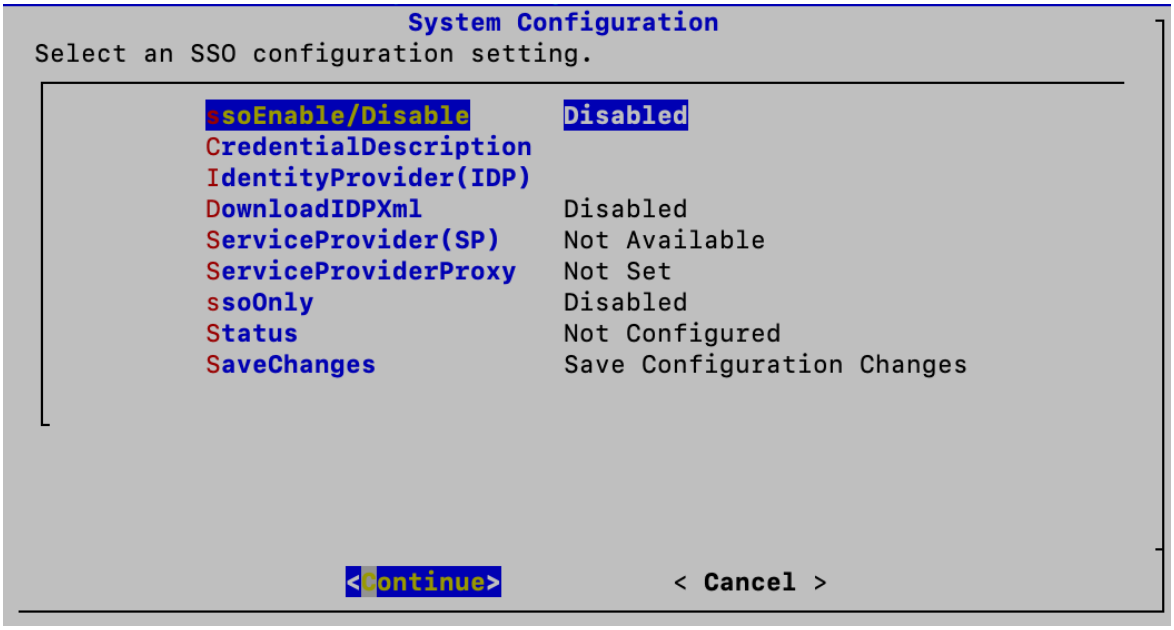
> ⚠ 設定の変更が保留中の間は、アプライアンスを再起動させないでください。

10. セカンダリ Manager がある場合は、この手順を繰り返して、ルート CA 証明書をセカンダリ Manager 信頼ストアに追加します。
11. ルート CA 証明書を Manager 信頼ストアに追加した場合は、次の項に進みます。

> LDP のメタデータを更新すると、SSO が接続されないことがあります。メタデータを更新する必要があります。これを行う最も簡単な方法は、システム構成ツールで新しい SSO 情報を更新した後に再起動することです。

3. サービス プロバイダの設定

1. Manager コンソールに root としてログインします。
2. `SystemConfig` と入力します。Enter を押します。
3. [詳細設定(Advanced)] を選択します。
4. [SSO] を選択します。
5. [SSO 有効/無効(ssoEnable/Disable)] が [無効(Disabled)] と表示されていることを確認します。



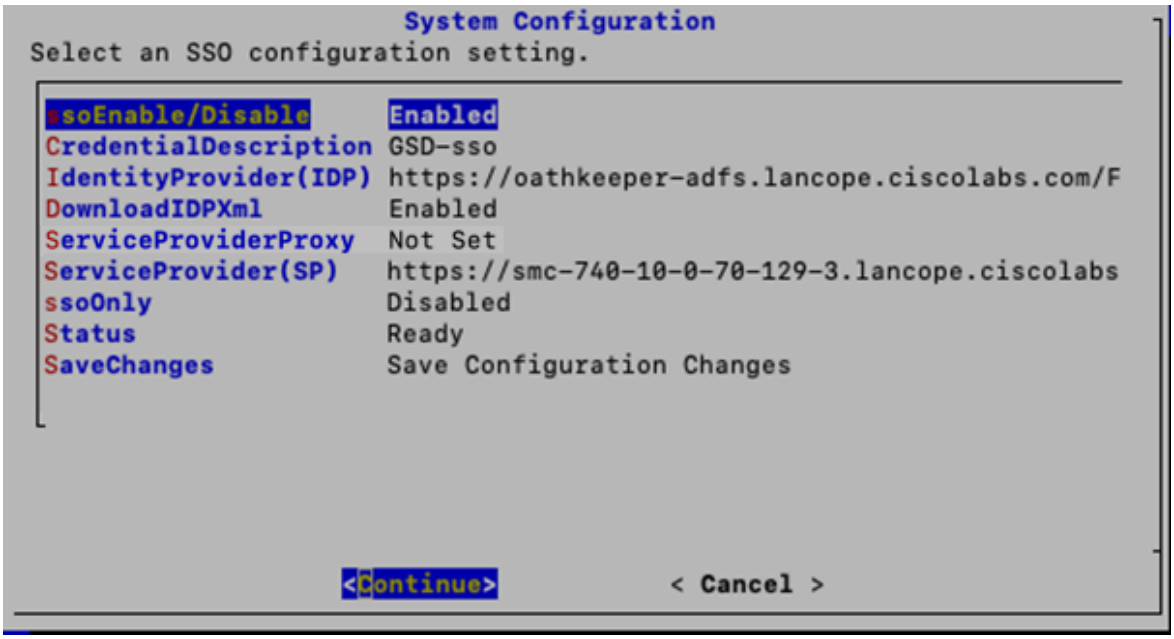
6. [アイデンティティ プロバイダ(IDP)(IdentityProvider(IDP))] を選択します。[続行(Continue)] をクリックします。
7. アイデンティティ プロバイダの設定ファイルをダウンロードできる URL を入力します。

   Requirements(要件):完全修飾ドメイン名または IPv4 アドレスを入力します。

8. [IDP のダウンロード(DownloadIDP)] を選択します。画面に表示される指示に従って、有効にします。
9. [変更の保存(SaveChanges)] を選択します。[続行(Continue)] をクリックします。

   画面の指示に従って、IDP 設定ファイルをダウンロードします。

10. [SSO] を選択します。
11. [サービス プロバイダ(SP)(ServiceProvider(SP))] を確認します。URL をコピーしてください。これは、アイデンティティ プロバイダの設定に使用します。
12. [ステータス(Status)] を確認します。これが [準備(Ready)] と表示されていることを確認してください。



4. SSO の有効化

1. [SSO 有効/無効(ssoEnable/Disable)] を選択します。
2. 画面に表示される指示に従って、SSO を有効にします。
3. [クレデンシャルの説明(CredentialDescription)] を選択します。[続行(Continue)] をクリックします。
4. ユーザーがログインするために必要な SSO サービス クレデンシャルの説明を入力します。
5. [OK] をクリックします。
6. [IDP のダウンロード(DownloadIDP)] を選択します。新しい SSO 設定を保存する必要があるまで [IDP のダウンロード(DownloadIDP)] を無効にします。

   - [続行(Continue)] をクリックします。
   - 画面に表示される指示に従って、[IDP のダウンロード(DownloadIDP)] を無効にします。

7. [変更の保存(SaveChanges)] を選択します。[続行(Continue)] をクリックします。
8. システム設定を終了します。

5. サービス プロバイダー プロキシの設定(オプション)

1. [SSO有効/無効(ssoEnable/Disable)] が [有効(Enabled)] と表示されていることを確認します。
2. [ServiceProviderProxy] を選択します。
3. 使用するサービス プロバイダー プロキシの完全修飾ドメイン名(FQDN)を入力します。
4. [OK] をクリックします。
5. Manager をリブートして、プロキシ設定プロセスを完了します。

6. アイデンティティ プロバイダの設定

1. ブラウザのアドレス フィールドにサービス プロバイダの URL を入力します。
2. サービス プロバイダのメタ データファイル **sp.xml** をダウンロードします。
3. **sp.xml** を使用してアイデンティティ プロバイダを設定します。
4. 発信クレーム タイプにユーザーの電子メール アドレスが含まれていることを確認します。

   - **例**：属性ストアが Active Directory の場合、発信クレーム タイプを LDAP 属性タイプのユーザー ID の電子メール アドレスに設定します。
   - **Microsoft Active Directory フェデレーション サービス（ADFS）**：IDP タイプが ADFS の場合は、次のカスタム ルールが表示されていることを確認します。

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue
(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, Value = c.Value, ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://<IDP FQDN>/adfs/com/adfs/service/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<SMC FQDN>/fedlet");
```

7. SSO ユーザーの追加

SSO ユーザーを追加するには、次の手順を使用します。ユーザーはアイデンティティ プロバイダを介して（アイデンティティ プロバイダによって）認証されます。

1. Manager（Web アプリケーション）にログインします。
2. [構成（Configure）] > [グローバルユーザー管理（GLOBAL User Management）] を選択します。
3. [作成（Create）] > [ユーザー（User）] の順に選択します。

   手順については、?（[ヘルプ（Help）]）アイコンをクリックします。**[ヘルプ（Help）]** を選択します。ユーザーの追加の詳細については、「ユーザーの設定」を参照してください。

4. フィールドに入力して、新しいユーザーを作成します。次のようにユーザーを設定してください。
   - **認証サービス（Authentication Service）**：[SSO] を選択します。
   - **ユーザー名（User Name）**：IDP アカウントの電子メール アドレスの最初の部分を入力します。ID がログイン時に SSO に使用されるものと同じであることを確認してください。たとえば、name @ cisco.com の場合、このフィールドに「 name 」と入力します。
5. [保存（Save）] をクリックします。
6. [ユーザー管理（User Management）] に [SSO ユーザー（SSO User）] が表示されていることを確認します。

8. SAML ログインのテスト

1. Web UI ログインページで、[SSOでログイン(Log in with SSO)] を選択します。
2. クレデンシャル ボタンをクリックします。
3. ログイン クレデンシャルを入力します。Manager で [セキュリティ分析ダッシュボード(Security Insight Dashboard)] が開きます。

トラブルシューティング

シナリオ	注記
アカウントのロックアウト	緊急アカウント アクセスを使用してシステム設定で [SSO のみ(SSO Only)] を無効にします。
IDP XML をダウンロードできない	IDP 証明書が Manager 信頼ストアにアップロードされていることを確認します。
IDP 設定を保存できない	IDP 設定を調べて、入力したデータが正確で、余分なスペースが含まれていないことを確認します。また、IDP イベント ログを調べます。
その他の問題	使用しているブラウザ用の SAML トレーサーをダウンロードします。SSO ログインを繰り返して、IDP と SP の間の交換を確認します。

ドメイン

ドメインは、モニタおよび管理するホストおよびその他のデバイスのグループです。Flow Collector はドメイン内に存在し、1 つの Secure Network Analytics システム内に複数のドメインを持つことができます。ドメインは他のドメインから完全に独立しており、すべてのドメインに [ホストグループ(Host Group)] ツリーが含まれます。[ホストグループ(Host Group)] ツリーに存在するホストグループについては、ヘルプの「ホストグループの管理と設定」を参照してください。

このセクションは、次のトピックで構成されています。

- **Data Store ドメインと非 Data Store ドメイン**
- **ドメインの追加と設定**
- **Data Store ドメインと非 Data Store ドメインの同期**
- **ドメインの削除**

Data Store ドメインと非 Data Store ドメイン

アプライアンス設定ツール で Manager を設定してシステムをセットアップするときに、Data Store あり(Data Store ドメイン)か Data Store なし(非 Data Store ドメイン)で Secure Network Analytics ドメインを作成します。

- **Data Store ドメイン**:Flow Collector は、Data Store Data Node にテレメトリを送信して保存します。
- **非 Data Store ドメイン**:Flow Collector は、Flow Collector または Flow Collector データベースでテレメトリをローカルに保存します(5000 シリーズのみ)。
- **ハイブリッド設定**:ハイブリッド設定の Secure Network Analytics では、Data Store ドメインと非 Data Store ドメインを設定できます。Flow Collector を設定するときに、使用するドメインを選択してデータの送信先を決定すること可能です。

> 非 Data Store 展開に Data Store ドメインを追加する場合は、「**非 Data Store 展開への Data Store の追加**」に記載されている手順を確認してください。

ドメインの追加と設定

次の手順に従ってドメインを追加し、ドメイン設定を定義します。新しい Data Store ドメインに非 Data Store 設定をインポートすることもできます。

- **ロール権限**:ドメインを設定するには、管理者または設定マネージャロールが必要です。パワーアナリストが行えるのはドメインの表示のみです。
- **Data Store ドメイン**:非 Data Store 展開に Data Store ドメインを追加する場合は、この手順を開始する前に「**非 Data Store 展開への Data Store の追加**」に記載されている手順を確認してください。

1. ドメインの追加

1. メニューバーから、[現在のドメイン名(Current domain name)] > [ドメインの追加(Add Domain)] の順に選択します。

2. 次のフィールドを設定します。

   - **[ドメイン名(Domain Name)]**:ドメインに割り当てる名前。この名前は[ホストグループ(Host Group)]ツリーに表示されます。
   - **[方法の選択(Select Method)]**:追加するドメインに使用するホストグループ構造を指定するために、次の表で説明されている方法のいずれかを選択します。

この方式を選択すると...	次の操作
デフォルト	Secure Network Analytics では、デフォルトのホストグループ構造を使用し、Flow Collector を使用せずにドメインを作成します。
Import from File	Secure Network Analytics により、エクスポートした特定のドメインコンテンツ(ホストグループ、ドメイン、またはその両方)に基づいてドメインが作成され、適切な設定が使用されます。ドメイン設定を含む XML ファイルのエクスポートについては、「設定のエクスポート」セクションを参照してください。 • ドメイン設定を含む XML ファイルには、下位互換性がありません。これらのファイルは、同じシステムバージョン番号内でのみ互換性があります(たとえば、Flow Collector v7.0 と Manager v7.0)。 • また、[ホストグループ管理(Host Group Management)]ページを使用して、ホストグループ設定全体をインポートすることもできます。 • 別のドメインから[ホストグループ(Host Group)]ツリーの[ネットワークデバイス(Network Devices)]ブランチにインターフェイスグループをインポートする必要がある場合は、このオプションを使用します。最初に、グループ設定を XML ファイルとしてローカルドライブにエクスポートする必要があります。 • XML ファイルに含まれる Flow Collector はインポートされません。

既存のドメインに Flow Collector を追加すると、そのドメイン固有の設定(ポリシー、アラーム重大度、サービス、エクスポータ SNMP など)がその Flow Collector に適用されます。

3. [ドメインの追加(Add a Domain)]を選択して、ドメインタイプを選択します。Data Store ドメインは Data Store を使用している Secure Network Analytics システム用であり、非 Data Store ドメインは Data Store を使用していない Secure Network Analytics システム用です。詳細については、「**Data Store ドメインと非 Data Store ドメイン**」を参照してください。

   Data Store ドメインを追加する場合は、[Data Storeドメインとして設定(Configure as a Data Store Domain)]チェックボックスをオンにします。

複数の Data Store ドメインを作成している場合は、Analytics のパフォーマンスが最適化されないため、Analytics を有効にしないでください。

4. 設定を保存するには、[追加(Add)]をクリックします。

既存の Data Store 以外のドメイン設定のインポートによる Data Store ドメインの作成（オプション）

現在非 Data Store ドメイン上にあり、将来 Data Store に拡張するために Secure Network Analytics システムに Data Store ドメインを追加する場合は、非 Data Store 設定を新しい Data Store ドメインにインポートすることでドメインを追加できます。

既存のドメインをインポートする場合、アラームやホストグループなどの項目を再設定する必要はありません。既存のドメインからのインポートは、新しいドメインの作成に似ていますが、既存の設定を使用します。

ドメインを新しく作成した場合は、Secure Network Analytics を設定し直す必要があります。

以下の手順に従って新しい Data Store ドメインを追加し、その設定のすべてを非 Data Store ドメインからインポートします。

1. [ドメインの追加（Add a Domain）] ドロップダウンメニューを使用して、非 Data Store ドメインを選択します。
2. トップメニューから、[構成（Configuration）] > [システムドメインのプロパティ（SYSTEM Domain Properties）] を選択します。
3. [すべての設定のエクスポート（Export All configuration）] ラジオボタンがオンになっていることを確認します。エクスポートされるデータのリストを表示するには、以下の「ドメイン設定の指定」セクションを参照してください。
4. [エクスポート（Export）] ボタンをクリックして、XML ファイルをダウンロードします。
5. ページの左上隅にあるメインメニューの左端で、[現在のドメイン名（Current domain name）] > [ドメインの追加（Add Domain）] の順に選択します。
6. [ドメイン名（Domain Name）] フィールドに新しいドメインの名前を入力します。
7. [方法の選択（Select Method）] ドロップダウンメニューをクリックし、[ファイルからのインポート（Import from File）] オプションを選択します。
8. 手順 4 でダウンロードした XML ファイルを選択します。
9. [Data Storeドメインとして設定（Configure as a Data Store Domain）] チェックボックスをクリックしてオンにします。
10. [追加（Add）] ボタンをクリックして、新しいドメインを追加します。

2. ドメイン設定の指定

1. 追加するドメインに関する次の設定を完了します。

設定	説明
Domain Name	現在のドメインの名前。
アーカイブ時間	ドメイン内の各 Flow Collector がすべてのカウントをクリアする時間を設定できます。0 ～ 23 の整数を入力できます（0 はローカルタイムゾーンの午前 0 時です）。ローカルタイムゾーンは、[アーカイブ時間（Archive hour）] フィールドの右側に表示されます。 Flow Collector は、定義した時間にすべてのインデックスカウントを 0 にリセットします。さらに、Flow Collector は過去 24 時間に収集したログファイルと Web ファイルを保存し、新しいデータ収集日を開始します。

内部自律システム（AS）番号（Internal autonomous system（AS）number）	[内部AS番号（Internal AS Numbers）] フィールド内をクリックし、AS 番号を入力します。複数のエントリをカンマで区切るか、各エントリの後で **Enter** キーを押して各エントリを別々の行に配置します。 内部自律システム（AS）番号は、Flow Collector を含むドメインにのみ割り当てることができます。Secure Network Analytics は、フローデータでこれらの番号を含むトラフィックを検出すると、自律システム トラフィックドキュメントでそのトラフィックを「起点」トラフィックとして分類します。起点トラフィックとは、ネットワークからのトラフィックかネットワーク内部のトラフィックです。これに対し、外部ネットワークから発信されてネットワークを通過するトラフィックを中継トラフィックといいます。 自律システム トラフィックドキュメントについては、デスクトップクライアントのヘルプにある「自律システムトラフィック」トピックを参照してください。

2. エクスポート設定を指定します。

   [ドメインプロパティ（Domain Properties）] ダイアログの [エクスポート（Export）] ページで、特定のドメインコンテンツをエクスポートできます。今後追加するドメインのテンプレートとしてそのコンテンツを使用できます。

   使用可能な設定については、次の表を参照してください。

次のチェックボックスをオンにした場合...	**Secure Network Analytics がエクスポートするデータ...**
すべての設定をエクスポート（Export All configurations）*	以下の「ドメイン設定のエクスポート（Export the Domain configuration）」に記載されているすべてのデータ。さらに、Flow Collector、およびエクスポータとそのインターフェイスのリストもエクスポートされます。
ホスト グループ設定のエクスポート（Export the Host Group configuration）*	ホスト グループの名前と IP アドレス範囲を含む、ホスト グループ定義構造全体。この出力にはポリシーは含まれません。
ドメイン設定のエクスポート（Export the Domain configuration）*	• [ドメインプロパティ（Domain Properties）] ダイアログからのアーカイブ時間設定。 • すべてのサービス定義。サービスについては、デスクトップクライアントのヘルプにある「サービス」トピックを参照してください。 • すべてのアラーム設定。アラームの設定については、デスクトップクライアントのヘルプにある「アラームの重大度について」トピックを参照してください。 • ホストグループの名前と IP アドレス範囲を含む、ホストグループ構造全体。詳細については、Secure Network Analytics のヘルプにある「ホストグループの管理と設定」トピックを参照してください。 • すべてのポリシー。詳細については、Secure Network Analytics のヘルプにある「コアポリシーの管理」トピックを参照してください。 緩和アラームアクションは、手動でデフォルトから変更された場合（つまり*非継承*に設定された場合）にのみエクスポートされます。

次のチェックボックスをオンにした場合...	Secure Network Analytics がエクスポートするデータ...
*これらのコマンドによって生成される XML ファイルを使用して、ホストグループ設定を置換できます。詳細については、デスクトップクライアントのヘルプにある「ホストグループ設定を置き換える方法」トピックを参照してください。	

3. [エクスポート(Export)] をクリックします。

   Secure Network Analytics により、ダウンロードされた XML ファイル内の対応する設定がダウンロードフォルダに保存されます。

> ドメインのエクスポートは、設定のバックアップとは異なります。アプライアンス設定をバックアップするには、「**アプライアンス設定のバックアップの作成**」を参照してください。

Data Store ドメインと非 Data Store ドメインの同期

非 Data Store Flow Collector を Data Store Flow Collector に移行するプロセスの実行中、非 Data Store ドメインと Data Store ドメインの間で設定と調整の同期を維持したい場合があります。ここでは、非 Data Store ドメインを、関連する Data Store ドメインと同期するプロセスについて説明します。

はじめる前に

非 Data Store ドメインと同期する Data Store ドメインがすでに作成されていることを確認します。「**非 Data Store Flow Collector の Data Store Flow Collector への移行**」で概説されているプロセスをすでに完了している場合は、Data Store ドメインがすでに作成されています。ドメインの追加手順については、「**ドメインの追加と設定**」を参照してください。

> この手順には管理者アクセスが必要です。

同期されるプロパティ

次のプロパティはドメイン間で同期されます。

- Data Store ドメイン固有の設定とアラート設定(有効な場合)。ドメイン設定には、次のものが含まれます。
  - ホストグループ管理
  - アラーム重大度
  - ポリシー管理
  - サービス、アプリケーション
  - エクスポータ SNMP プロファイル(パスワードを除く)
  - ドメイン AS 番号

推奨同期頻度

ドメインは何度でも同期できますが、同期は、一連の変更を実行した後か 1 日または 1 週間に 1 回のみに制限することをお勧めします。これは、同期プロセスでリソースが使用され、日常的な処理の能力が奪われるためです。

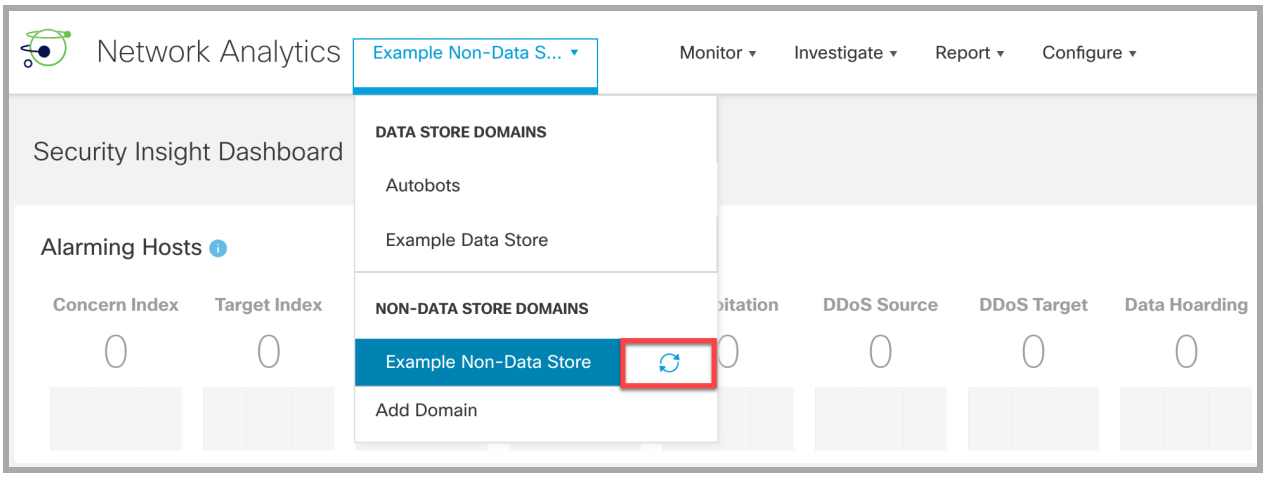
ドメイン同期化の手順

以下の手順に従って、非 Data Store ドメイン（ソース）と Data Store ドメイン（対象）を同期します。

1. メニューバーから、Data Store ドメインと同期する非 Data Store ドメインを選択します。
2. メインメニューから、[設定（Configure）] > [システムドメインのプロパティ（SYSTEM Domain Properties）] を選択します。
3. [編集（Edit）] ボタンを選択します。
4. [同期する対象ドメイン（Target Domain to Synchronize）] ドロップダウンメニューで、このドメインを同期する Data Store ドメインを選択します。

> 対象の Data Store ドメインは、1 つのソースの非 Data Store ドメインとのみ同期できます。対象の Data Store ドメインを複数のソースの非 Data Store ドメインと同期しようとすると、エラーが表示されます。

5. [Save] ボタンをクリックして変更を保存します。Data Store ドメインとの同期を選択した非 Data Store ドメインの横に、同期ボタンが表示されます。



ドメイン同期の対象ドメインの削除

対象ドメインを削除するには、次の手順に従います。

1. メニューバーから、Data Store ドメインと同期する非 Data Store ドメインを選択します。
2. メインメニューから、[設定（Configure）] > [ドメインのプロパティ（Domain Properties）] の順に選択します。
3. [編集（Edit）] ボタンを選択します。
4. [対象ドメインをクリア（Clear Target Domain）] ボタンをクリックします。
5. [Save] ボタンをクリックして変更を保存します。

ドメインの削除

ドメインを削除する前に、これらの手順を確認して要件を把握しておいてください。

> ⚠ ドメインを削除すると、そのドメインについて収集されたすべてのデータにアクセスできなくなります。ドメインは、ドメイン内の収集されたデータにアクセスする必要がなくなった場合にのみ削除してください。

1. Central Management から Flow Collector を削除する

ドメインに Flow Collector が含まれている場合は、ドメインを削除する前に、それらを Central Management から削除します。Flow Collector を別のドメインに追加できますが、手順には工場出荷時のデフォルトへのリセット（RFD）が含まれます。手順については、以下を参照してください。

1. **Central Management からのアプライアンスの削除**
2. **工場出荷時のデフォルトへのリセット**
3. **Central Management へのアプライアンスの追加**

> ⚠ Flow Collector を Central Management から削除してドメインを削除すると、関連する Flow Collector のデータが失われます。

2. ドメインを削除する

1. 最初にドメインにアクセスする必要がある場合は、ドロップダウンメニューから［現在のドメイン名（Current domain name）］を選択します。

2. メインメニューから、［設定（Configure）］>［システムドメインのプロパティ（SYSTEM Domain Properties）］を選択します。
3. ［ドメインの削除（Delete Domain）］をクリックします。

> ⚠ ドメインを削除すると、そのドメインについて収集されたすべてのデータにアクセスできなくなります。ドメインは、ドメイン内の収集されたデータにアクセスする必要がなくなった場合にのみ削除してください。

デスクトップ クライアントドメインの削除

Data Store なしの Secure Network Analytics でデスクトップ クライアントを使用している場合は、デスクトップ クライアントからドメインを削除することもできます。

> ⚠ 削除するドメインについて収集されたすべてのデータにアクセスできなくなるため、削除するデスクトップ クライアントドメインを決定するときは注意が必要です。
> **回避策**：デスクトップクライアントのドメインを誤ってすべて削除してしまい、Manager Web アプリケーションからロックアウトされた場合は、デスクトップクライアントで新しい非 Data Store ドメインを作成します。これにより、Manager Web アプリケーションへのアクセスを回復できます。ドメインの作成については、デスクトップ クライアント ヘルプの「ドメインの追加」トピックを参照してください。

統合と追加の設定

次の追加の統合と設定が用意されています。

https://www.cisco.com/c/ja_jp/support/security/stealthwatch/products-installation-and-configuration-guides-list.html 統合に関しては、このリストより多い場合があります。

- Stealthwatch に NSEL をエクスポートするための Cisco ASA の設定
- Customer Success Metrics 構成ガイド
- 複数の NetFlow エクスポータの有効化
- エンドポイントライセンスおよび Network Visibility Module（NVM）コンフィギュレーション ガイド
- Flow Sensor およびロード バランサ コンフィギュレーション ガイド
- グローバル脅威アラート構成ガイド
- ISE および ISE-PIC 構成ガイド
- Secure Network Analytics SecureX 統合ガイド
- 管理対象アプライアンスの SSL/TLS 証明書ガイド
- TACACS+ 構成ガイド
- Cisco Security Analytics and Logging（オンプレミス）

パスワード

パスワードは次の方法で変更できます。

- **パスワードのリセットの有効化または無効化**
- **パスワードのデフォルト設定へのリセット**
- **パスワードの変更**
- **Data Store データベースのパスワードの変更**
- **Flow Collector データベースのパスワードの変更（非 Data Store ドメイン）**

パスワードのリセットの有効化または無効化

パスワードのリセット機能を有効化または無効化するには、次の手順を使用します。[有効化（Enable）] を選択すると、GRUB コマンドライン インターフェイスを使用してパスワードをデフォルト設定にリセットできます。

> ⚠ パスワードのリセットを無効化し、パスワードを失った場合は、アプライアンスに保存されているデータへのアクセスが失われます。再度アプライアンスにアクセスするには、工場出荷時のデフォルトにリセットして再設定してください。

1. アプライアンスコンソールに root としてログインします。
2. **SystemConfig** と入力します。Enter を押します。
3. [セキュリティ（Security）] を選択します。
4. [パスワードのリセット（Password Reset）] を選択します。
5. 画面に表示される指示に従い、パスワードのリセットを有効または無効にします。

パスワードのデフォルト設定へのリセット

パスワードをデフォルト設定にリセットする方法は 2 つあります。

- **管理者パスワード**：**次での管理パスワードのリセット：Manager**を使用します。
- **admin、root、sysadmin パスワード**：「**admin、root、sysadmin パスワードをデフォルトにリセット**」を使用します。

> ⚠ アプライアンスのパスワードをデフォルトにリセットしたら、必ずパスワードを変更してください。この手順は、セキュリティにとって重要です。手順については、「**パスワードの変更**」を参照してください。

次での管理パスワードのリセット：Manager

次の手順を使用して、**admin** パスワードを Manager のデフォルト設定にリセットします。次に、セキュリティを最大限に高めるためにアプライアンスのパスワードを変更します。

- **要件**：次の手順を完了するには、アプライアンスのルート パスワードが必要です。
- **その他のユーザー**：次の手順により、admin ユーザーがデフォルト パスワードにリセットされます。個人ユーザーのパスワードは変更されません。

- **その他のアプライアンス**：これらの手順では、他の Secure Network Analytics アプライアンス（Flow Collector、Flow Sensor、または UDP Director）の admin パスワードはリセットされません。

1. アプライアンスコンソールに root としてログインします。
2. `rm /lancope/var/smc/config/users/admin/user.xml` と入力します。Enter を押します。
3. `docker restart smc` と入力します。Enter を押します。
4. `docker restart nginx` と入力します。Enter を押します。

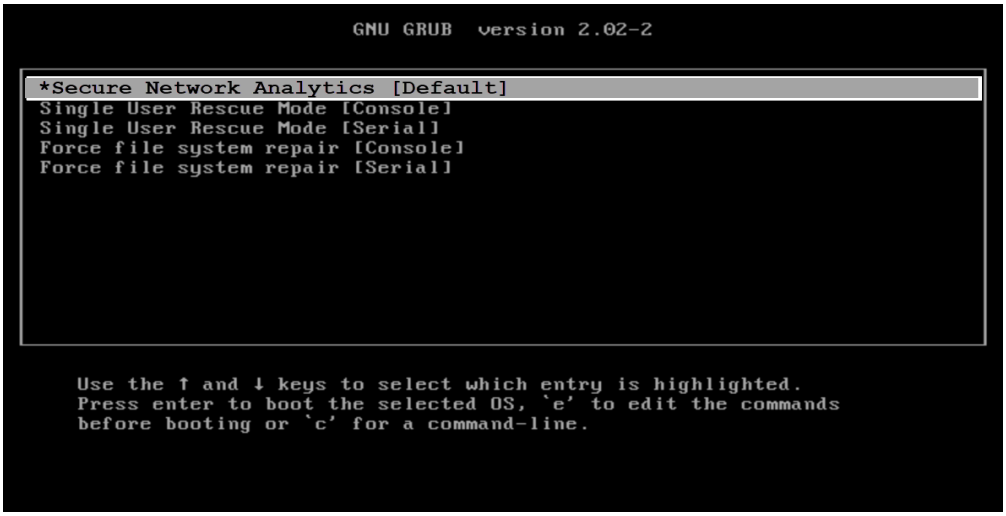
   これにより、admin パスワードがデフォルト値にリセットされます。

5. アプライアンスコンソールを終了します。
6. admin パスワードをデフォルトから変更するには、「**パスワードの変更**」に進みます。この手順は、セキュリティにとって重要です。

admin、root、sysadmin パスワードをデフォルトにリセット

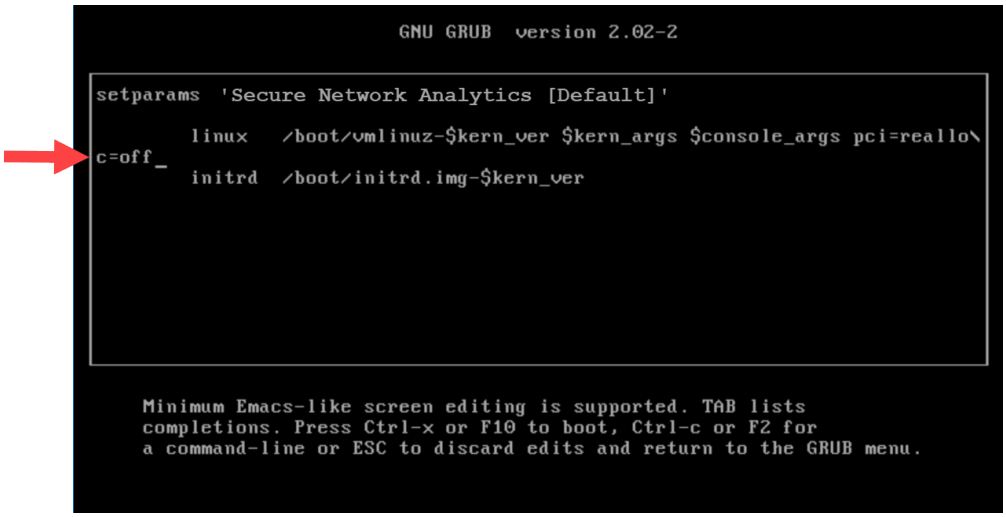
コンソールアクセスを使用して、アプライアンスの admin、root、および sysadmin パスワードをデフォルト設定にリセットします。次に、セキュリティを最大限に高めるためにアプライアンスのパスワードを変更します。

1. アプライアンスコンソール（CIMC またはハイパーバイザ）にログインします。
2. アプライアンスを再起動します。
3. コンソール画面に GRUB メニューが表示されたら、「e」と入力して編集モードに切り替えます。



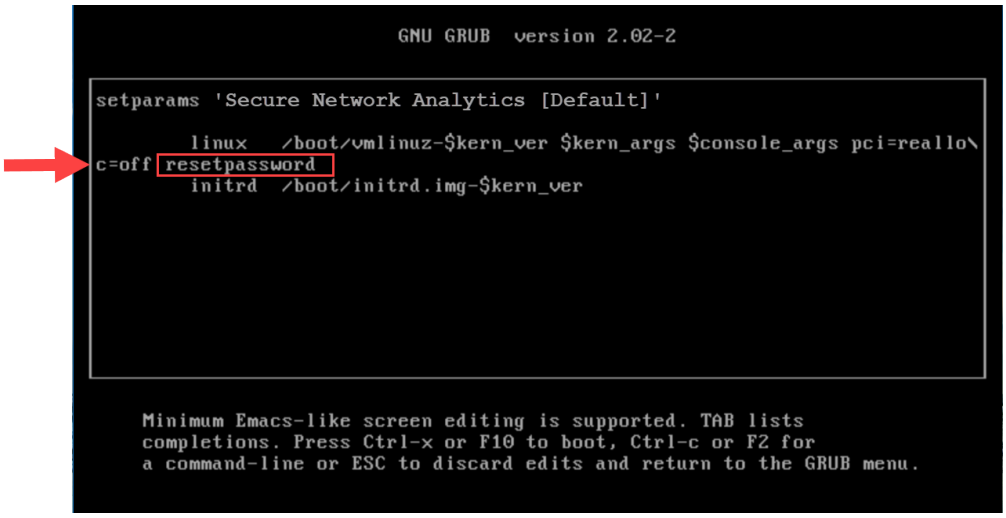
4. 2 番目の行にカーソルを移動します。

   コマンド ラインは、アプライアンスのバージョンによってわずかに異なる場合があります。



5. `c=off` の後に `resetpassword` と入力して、コマンド ラインを次の例のようにします。

```
linux /boot/vmlinuz-$kern_ver $kern_args $console_args
pci=reallo\
c=off resetpassword
```



6. Ctrl+X を押して起動を再開します。

   admin、root、および sysadmin パスワードがデフォルト値にリセットされます。

7. パスワードをデフォルトから変更するには、「**パスワードの変更**」に進みます。この手順は、セキュリティにとって重要です。

パスワードの変更

デフォルトのパスワードまたは以前のパスワードからパスワードを変更するには、次の手順を使用します。次の基準を使用していることを確認します。

- 長さ:8 ～ 256 文字
- 変更:新しいパスワードが以前のパスワードと最低 4 文字異なっていることを確認します。

ユーザー	デフォルト パスワード
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

sysadmin パスワードの変更

1. アプライアンスコンソールに sysadmin としてログインします。
2. [セキュリティ(Security)] を選択します。
3. [パスワード(Password)] を選択します。
4. 画面に表示される指示に従って、sysadmin パスワードを変更します。
5. システム設定を終了します。

ルート パスワードの変更

1. アプライアンスコンソールに root としてログインします。
2. **SystemConfig** と入力します。Enter を押します。
3. [セキュリティ(Security)] を選択します。
4. [パスワード(Password)] を選択します。
5. 画面に表示される指示に従って、ルート パスワードを変更します。
6. システム設定を終了します。

次での管理者パスワードの変更:Manager

1. 管理者として Manager にログインします。

   - URL:https://<IPAddress>
   - ログイン:admin
   - デフォルトパスワード:lan411cope

2. [構成(Configure)] > [グローバルユーザー管理(GLOBAL User Management)] を選択します。
3. リスト内で admin ユーザーを見つけます。

4. [アクション(Actions)] メニューをクリックします。[パスワードの変更] を選択します。
5. 画面に表示される指示に従って、admin パスワードを変更します。次の基準を使用します。

    - 長さ:8 ～ 256 文字
    - **変更**:新しいパスワードがデフォルト パスワードと最低 4 文字異なっていることを確認します。

他のすべてのアプライアンスの admin パスワードの変更

Data Node、Flow Collector、Flow Sensor、または UDP Director の admin ユーザーパスワードを変更するには、次の手順に従います。

1. admin として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。

    - URL:https://<IPAddress>
    - ログイン:admin
    - デフォルトパスワード:lan411cope

2. [ユーザーの管理(Manage Users)] > [パスワードの変更(Change Password)] を選択します。
3. 現在のパスワードと新しいパスワードを入力します。
4. [適用(Apply)] をクリックします。画面に表示される指示に従って、パスワードを変更します。
5. 別のアプライアンスの admin パスワードを変更するには、ステップ 1 ～ 4 を繰り返します。

Data Store データベースのパスワードの変更

システム構成を使用して、Data Store データベースのパスワード（dbadmin および readonlyuser）を変更します。この手順の一環として SSH を一時的に有効にする必要があります。

1. Manager アプライアンスコンソール（SystemConfig）に root としてログインします。
2. メニューから [Data Store] を選択します。
3. [SSH] を選択します。画面に表示されるプロンプトに従って SSH を有効にします。
4. [Data Store] メニューから [パスワード（Passwords）] を選択します。
5. 画面に表示される指示に従って、パスワードを変更します。

   [Data Store] メニューを終了すると、以前の SSH 設定が復元されます。

Flow Collector データベースのパスワードの変更（非 Data Store ドメイン）

[Central Management] ページの [データベース（Database）] タブを使用して、非 Data Store ドメインのすべての Flow Collector データベースについて、Flow Collector データベースのパスワードを更新します。

> 必ずデフォルトのパスワードを変更してください。新しいフローコレクタが Central Management に追加されると、データベースのパスワードは現在のパスワードと一致するように自動的に更新されます。

1. [集中管理（Central Management）] を開きます。
2. [データベース（Database）] タブをクリックします。
3. ランダムパスワードを生成するには、[パスワードの生成（Generate Password）] ボタンをクリックします。それ以外の場合は、[パスワード（Password）] フィールドおよび [パスワードの確認（Confirm Password）] フィールドにパスワードを入力します。
4. [パスワードの表示（Show Password）] チェックボックスをオンにして、選択したパスワードを表示します。
5. [設定の適用（Apply Settings）] ボタンをクリックして、変更を保存します。

> データベースのパスワードを変更すると、非 Data Store Flow Collector と移行中の Flow Collector のみが新しいパスワードを受け取ります。

SSL/TLS アプライアンス アイデンティティと 追加の SSL/TLS クライアント アイデンティティ

SSL/TLS アプライアンス アイデンティティと追加の SSL/TLS クライアント アイデンティティを使用して、選択したアプライアンスのセキュア ソケット レイヤ（SSL）と Transport Layer Security（TLS）証明書を管理します。証明書に関連したすべての変更では、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。

> ⚠ 証明書はシステムのセキュリティにとって重要です。証明書を不適切に変更すると、Secure Network Analytics アプライアンスの通信が停止し、データ損失の原因となります。証明書に関連したすべての変更では、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。

アプライアンス アイデンティティ

Secure Network Analytics バージョン 7.x アプライアンスはそれぞれ、固有の自己署名アプライアンス アイデンティティ証明書と一緒にインストールされます。アプライアンス アイデンティティ証明書を置き換えるには、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。

アプライアンスは、SSL 証明書を使用してそのアイデンティティの信頼性を他のアプライアンスに対して証明します。たとえば、Manager がフロークエリを生成して Flow Collector と通信する場合、Manager は自身のサーバー ID 証明書を提供することで認証されます。Flow Collector は、提供されたサーバー ID 証明書が信頼できる証明書かどうかを確認します。

クライアント アイデンティティ

クライアント アイデンティティは外部サービス間の通信に使用されます。詳細については、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。

証明書の確認

次の手順に従って、選択したアプライアンスのアプライアンス アイデンティティ証明書またはクライアント証明書を確認します。

1. Central Management を開きます。
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. ［アプライアンス（Appliance）］タブを選択します。
5. **アプライアンス アイデンティティ証明書を確認するには、**［SSL/TLS アプライアンス アイデンティティ（SSL/TLS Appliance Identity）］セクションに移動します。

   クライアント アイデンティティ証明書を確認するには、追加の SSL/TLS クライアント アイデンティティ（Additional SSL/TLS Client Identities）］セクションに移動します。

> ⚠ 証明書はシステムのセキュリティにとって重要です。証明書を不適切に変更すると、Secure Network Analytics アプライアンスの通信が停止し、データ損失の原因となります。証明書に関連したすべての変更では、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。

カスタム証明書を使用した Central Management へのアプライアンスの追加

詳細については、「**Central Management へのアプライアンスの追加**」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 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 Manager 信頼ストアに保存してください。手順については、『SSL/TLS Certificates for Managed Appliances Guide』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 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 Manager 信頼ストアに保存してください。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

ホスト名、ネットワークドメイン名、または IP アドレスの変更

アプライアンスの設置および設定後に、アプライアンスのホスト名、ネットワークドメイン名、または IP アドレスを変更するには、『SSL/TLS Certificates for Managed Appliances Guide』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。

信頼ストア証明書の確認

アプライアンスの信頼ストアに証明書を追加すると、別の Secure Network Analytics アプライアンスであるか外部サービスであるかにかかわらず、そのアイデンティティとの通信が可能になります。

- **手順**：信頼ストアに関するすべての変更では、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。
- **個別のファイルのアップロード**：ファイルに複数の証明書が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。

> ⚠ アプライアンスの信頼ストアに証明書を追加すると、アプライアンスはそのアイデンティティを信頼し、通信できるようになります。信頼ストアに関するすべての変更では、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。

次の手順に従って、選択したアプライアンスの信頼ストアに保存した証明書を確認します。

1. Central Management を開きます。
2. アプライアンスの［アクション（Actions）］メニューをクリックします。
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）］タブを選択します。
5. ［信頼ストア（Trust Store）］リストを確認します。

脅威フィード

Cisco Secure Network Analytics 脅威フィード（旧 Stealthwatch 脅威インテリジェンスフィード）は、ネットワークに対する脅威に関するグローバル脅威フィードからのデータを提供します。フィードは頻繁に更新され、悪意のあるアクティビティに使用されたことがわかっている IP アドレス、ポート番号、プロトコル、ホスト名、および URL が含まれています。フィードには、コマンドアンド コントロールサーバー、bogon、および Tor の各ホストグループが含まれています。

ライセンス

脅威フィードのライセンスを Cisco スマートアカウントに追加します。手順については、『Secure Network Analytics Smart Software Licensing Guide』を参照してください。

有効化

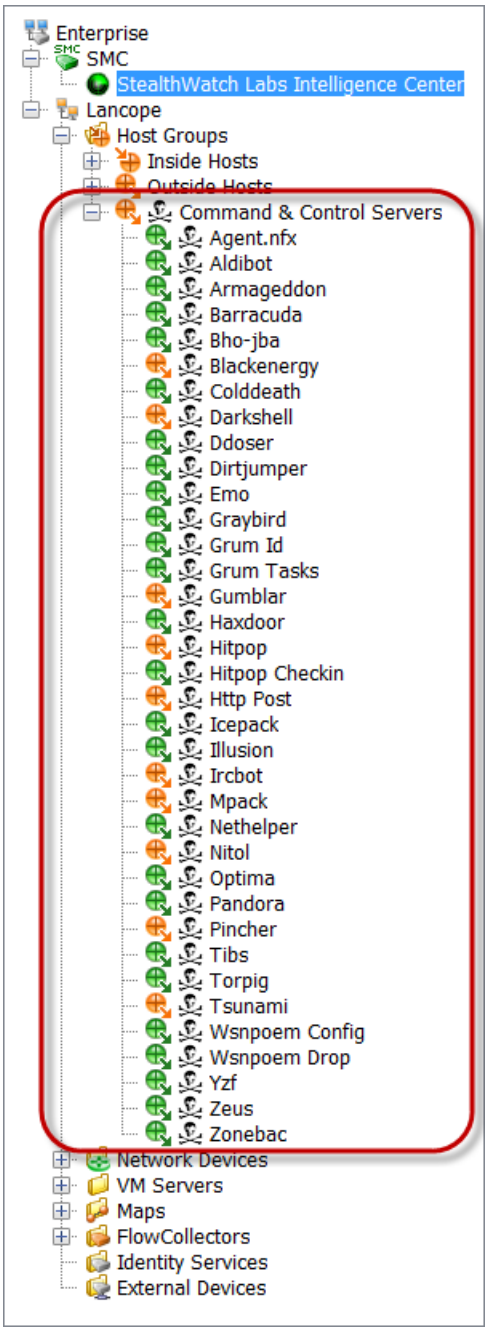
Central Management でフィードを有効にするには、ヘルプの手順に従います。手順の一部として DNS サーバーとファイアウォールを設定することに注意してください。また、フェールオーバー設定がある場合は、プライマリ Manager とセカンダリ Manager で脅威フィードを有効にする必要もあります。

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. ?（**[ヘルプ（Help）]）アイコン**をクリックします。**[ヘルプ（Help）]** を選択します。
4. **[アプライアンス構成（Appliance Configuration）]** > [**脅威フィード**] を選択します。

アラームとセキュリティイベントの確認

脅威フィード が有効になっている場合、Stealthwatch Labs Intelligence Center のアイコンがデスクトップクライアントのエンタープライズツリーにアラームステータスとともに表示され、脅威は各ホストグループのブランチに表示されます。詳細については、『 Desktop Client User Guide』またはヘルプを参照してください。

> **[ヘルプ（Help）]**：ヘルプにアクセスするには、Stealthwatch **[ラボインテリジェンスセンター（Labs Intelligence Center）]** ブランチを右クリックし、**[設定（Configuration）]** > **[SLIC脅威フィード設定（SLIC Threat Feed Configuration）]** の順に選択します。[ヘルプ（Help）] をクリックします。



Central Management（アプライアンスの管理）

Central Management を使用して、プライマリ Manager からアプライアンスを管理します。ここでは、Central Management の概要について説明します。各セクションの詳細については、ヘルプを参照してください。

- **Central Management について**：アプライアンスが Central Management によって管理されている場合、それらのステータスを確認できるのに加えて、アプライアンス設定の編集、ソフトウェアの更新、再起動、シャットダウンなどを管理できます。
- **ヘルプ**：[ヘルプ（Help）] を開くには、?（[ヘルプ（Help）]）アイコンをクリックします。**[ヘルプ（Help）]** を選択します。

この項では、次の項目について説明します。

- Central Management および アプライアンス管理インターフェイス
- Central Management を開く
- アプライアンス管理を開く
- アプライアンス設定の編集
- アプライアンス統計の表示
- Central Management からのアプライアンスの削除
- Central Management へのアプライアンスの追加
- アプライアンス設定のバックアップの作成
- SSH の有効化/無効化

Central Management および アプライアンス管理インターフェイス

アプライアンスが Central Management で管理されている場合、アプライアンスの機能には、Central Management およびアプライアンス管理インターフェイス（アプライアンス管理）からアクセスします（次の表を参照）。

Central Management	アプライアンス管理インターフェイス
アプライアンス構成の編集	システム統計情報の表示
ライセンス ステータスの確認（概要）	
構成ファイルのバックアップ	データベースファイルのバックアップ
監査ログの表示	診断パックの作成
再起動	ネットワークホストと IP の検索
シャットダウン	パケット キャプチャ

ソフトウェアの更新	DNS キャッシュのクリア
	アプライアンス固有の設定

Data Store との互換性のために Flow Collector を設定すると、アプライアンス管理インターフェイス（アプライアンス管理）によって特定の機能が非表示になります。Flow Collector やその他の関連タスクを設定するには、Central Management を使用します。

Central Management を開く

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。

アプライアンス管理を開く

アプライアンス管理インターフェイスには、Central Management を通じて、またはアプライアンスに直接ログインすることでアクセスできます。

Central Management を通じてアプライアンス管理を開く

1. Central Management の［インベントリ（Inventory）］ページで、アプライアンスの［アクション（Actions）］メニューをクリックします。
2. ［アプライアンス統計情報の表示（View Appliance Statistics）］を選択します。
3. 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。

直接ログインを介してアプライアンス管理を開く

1. ブラウザのアドレス フィールドに、次のようにアプライアンスの IP アドレスを入力します。

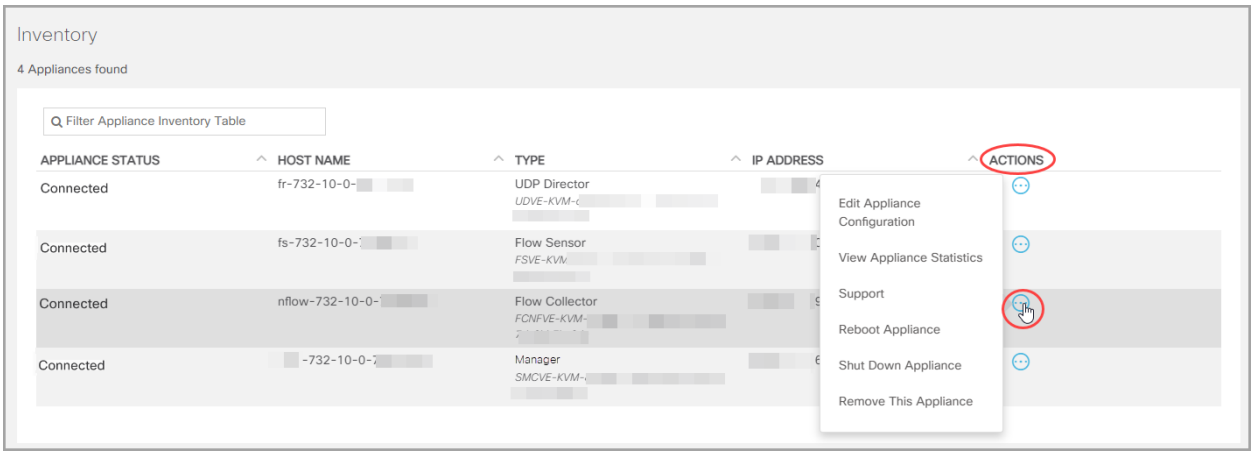
   https://<IPAddress>

   - **Manager**：IP アドレスの後に **/Manager/index.html** を追加します。
   - **例**：https://1.1.1.1/Manager/index.html

2. Enter を押します。

アプライアンス設定の編集

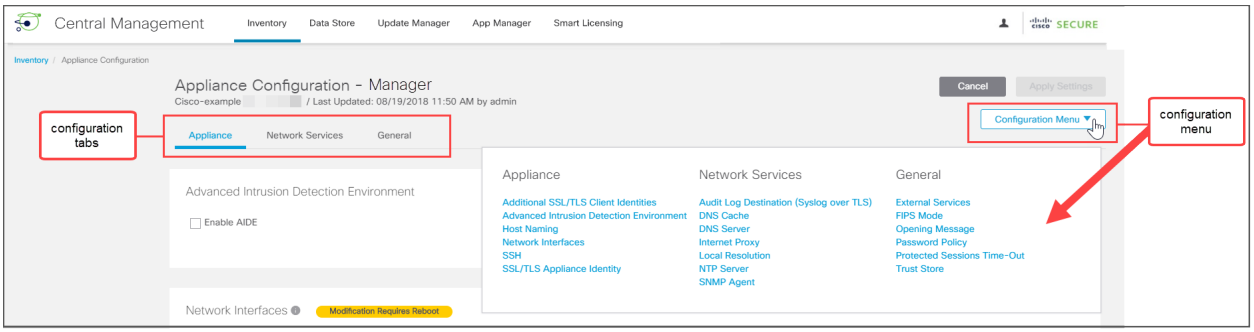
1. Central Management の［インベントリ（Inventory）］ページで、アプライアンスの［アクション（Actions）］メニューをクリックします。
2. ［アプライアンス構成の編集（Edit Appliance Configuration）］を選択します。



3. ［設定（Configuration）］メニューをクリックします。リストから項目を選択します。

   または

   各タブをクリックして、各設定カテゴリを確認します。



4. 必要に応じて、各設定セクションに変更を加えます。各設定タブでは、複数の設定カテゴリを編集することができます。

> 手順については、［ユーザー（User）］ アイコンをクリックします。

5. ［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、設定変更を保存します。

   一部の変更には、システムの再起動が必要です。待機する場合は、変更を元に戻して、後で設定を編集して再起動します。

> アプライアンスが自動的に再起動します。設定の変更が保留中の間は、アプライアンスを再起動させないでください。アプライアンスのステータスが［接続済み（Connected）］であることを確認するには、［Central Management］>［インベントリ（Inventory）］を参照します。

6. ［接続済み（Connected）］:［インベントリ（Inventory）］ ページで、アプライアンスが設定変更を完了し、アプライアンスステータスが［接続済み（Connected）］に戻ることを確認します。

アプライアンス統計の表示

ホバー：各アプライアンス ステータスの詳細を確認する場合は、ステータスの上にマウス ポインタを置きます。

システムの統計情報、サービス、ディスク使用率、および Docker サービスを確認するには、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。

1. Central Management の［インベントリ（Inventory）］ページで、アプライアンスの［アクション（Actions）］メニューをクリックします。
2. ［アプライアンス統計情報の表示（View Appliance Statistics）］を選択します。
3. 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。

Central Management からのアプライアンスの削除

次の手順に従って、Central Manager からアプライアンスを削除します。

1. Central Management の［インベントリ（Inventory）］ページで、アプライアンスの［アクション（Actions）］メニューをクリックします。
2. ［このアプライアンスを削除（Remove This Appliance）］を選択します。

- **Data Store アプライアンス**：追加の要件については、「**Central Manager からの Data Store アプライアンスの削除**」を参照してください。
- **Flow Collector**：フローコレクタを Central Management から削除すると、ドメインからも削除されます。別のドメインに追加する予定の場合は、工場出荷時のデフォルトにリセット（RFD）する必要があります。手順については、「**Central Management へのアプライアンスの追加**」と「**Central Management からのアプライアンスの削除**」を参照してください。
- **構成チャネルのダウン**：構成チャネルがダウンしているためアプライアンスを削除する場合、「トラブルシューティング」の「構成チャネルのダウン」に移動して追加の手順を参照してください。
- トラブルシューティング：アプライアンス管理インターフェイスにログインしても、アプライアンスが Central Management から削除されない場合は、「トラブルシューティング」の「構成チャネルのダウン」の手順に進み、システム設定を使用して削除します。
- **Central Management**：異なる Central Manager にアプライアンスを追加するには、アプライアンス設定ツールを使用します。

> ⚠ 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 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 Manager 信頼ストアに保存してください。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

Central Manager からの Data Store アプライアンスの削除

Central Manager から Data Store アプライアンス（Manager、Flow Collector、Data Node）を削除しても、Data Store 自体からは削除されません。Data Store 自体から削除するには、手動でのクリーンアップが必要です。

- **Manager と Flow Collector**：Manager と Flow Collector については、**/lancope/var/services/data-store/config-datastore-inventory-snapshot** ディレクトリから削除できます。
- **Data Node**：Data Node の削除はプロセスがより複雑であるため、シスコサポートに連絡してサポートを依頼してください。

Central Management へのアプライアンスの追加

Central Management にアプライアンスを追加するには、アプライアンス設定ツールを使用します。次を確認することが重要です。

- **カスタム証明書**：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 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）をその独自の信頼ストアおよび Manager 信頼ストアに保存してください。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。
- **Manager 管理クレデンシャル**：Central Management にアプライアンスを追加するには、Manager のユーザー ID とパスワードが必要です。
- **RFD**：アプライアンスで工場出荷時のデフォルトにリセットした場合、アプライアンスを Central Management に追加する前にその IP アドレス、ホスト名、およびドメインを設定します（RFD 時にネットワーク設定を保持している場合でも設定します）。

  アプライアンスコンソールに **sysadmin** としてログインし、画面に表示される指示に従って IP アドレス、ホスト名、およびドメインを設定します。手順については、Secure Network Analytics ハードウェアまたは Virtual Edition の設置ガイドを参照してください。

- **新規インストール**：新規インストールの場合は、インストールを完了し、Central Management に追加する前に IP アドレス、ホスト名、およびドメインを設定します。手順については、「**1. 初回セットアップを使用した環境の設定**」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 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 Manager 信頼ストアに保存してください。『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

1. アプライアンスにログインします。

   ブラウザのアドレスバーに、次のようにアプライアンスの IP アドレスを入力します。
   https://<IPAddress>

2. 次のように URL の末尾を /lc-ast に置き換えます。

   https://<IPaddress>/lc-ast

3. Enter を押します。
4. [次へ（Next）] をクリックして [Central Management] タブにスクロールします。
5. [IPアドレス（IP Address）]：Manager/Central 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 Manager 管理ログイン情報を入力し、設定を終了します。アプライアンスの種類によっては、追加情報を入力する必要があります。
8. アプライアンス設定ツールの詳細については、「**2. 管理対象システムの設定**」を参照してください。

アプライアンス設定のバックアップの作成

Central Management を使用して、アプライアンス設定をバックアップします。

> アプライアンスをバックアップする前に、ヘルプの手順に従っていることを確認してください。Data Store をバックアップするには、「**Data Store のバックアップの作成**」を参照してください。Flow Collector データベースをバックアップするには、「**データベースのバックアップの作成（非 Data Store ドメイン）**」を参照してください。

1. [集中管理（Central Management）] を開きます。
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. [サポート（Support）] を選択します。
4. [設定ファイル（Configuration Files）] タブを選択します。
5. ?（[ヘルプ（Help）]）アイコンを選択します。ヘルプの手順に従います。

   アプライアンス設定のバックアップを復元するには、ヘルプの指示に従ってください。

SSH の有効化/無効化

このセクションは、SSH（セキュア シェル）を使用してアプライアンスにアクセスできるかどうかを制御する場合に使用します。

デフォルト：無効

> SSH を有効にすると、システムの侵害リスクが増加します。SSH は必要な場合のみ有効にすることが重要です。SSH は、使用終了後に無効にします。

SSH を開く

次の手順に従って、選択したアプライアンスの SSH を開きます。

1. Central Management を開きます。
2. アプライアンスの [アクション（Actions）] メニューをクリックします。
3. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
4. [アプライアンス（Appliance）] タブを選択します。

SSH の有効化

1. [SSH] セクションを見つけます。
2. アプライアンスへの SSH アクセスを許可するには、[SSH の有効化（Enable SSH）] チェックボックスをオンにします。
3. アプライアンスへのルート アクセスの有効化を許可するには、[ルート SSH アクセスの有効化（Enable Root SSH Access）]チェックボックスをオンにします。

4. ［設定の適用（Apply settings）］をクリックします。
5. 画面に表示される指示に従って操作します。

SSH の無効化

1. アプライアンスへの SSH アクセスを削除するには、［SSH の有効化（Enable SSH）］チェックボックスをオフにします。
2. アプライアンスへのルート アクセスを削除するには、［ルート SSH アクセスの有効化（Enable Root SSH Access）］チェックボックスをオフにします。
3. ［設定の適用（Apply settings）］をクリックします。
4. 画面に表示される指示に従って操作します。

データベースのバックアップの作成（非 Data Store ドメイン）

Manager と Flow Collector のデータベースをバックアップするには、次の手順に従います。Data Store をバックアップするには、「**Data Store のバックアップの作成**」を参照してください。

> ⚠ バックアップしていないと、更新プロセス中に問題が発生した場合にファイルを回復できません。手順に従って、データベースのバックアップのすべての手順を実行してください。また、この手順はデータストア以外の Flow Collector にのみ適用されることに注意してください。サポートが必要な場合は、シスコサポートにお問い合わせください。

このプロセスには、次の手順が含まれます。

1. **Flow Collector データベースのトリミング**
2. **データベースのスナップショットの削除**
3. **リモートファイルシステムへのバックアップ**
4. **データベースのスナップショットの削除**

1. Flow Collector データベースのトリミング

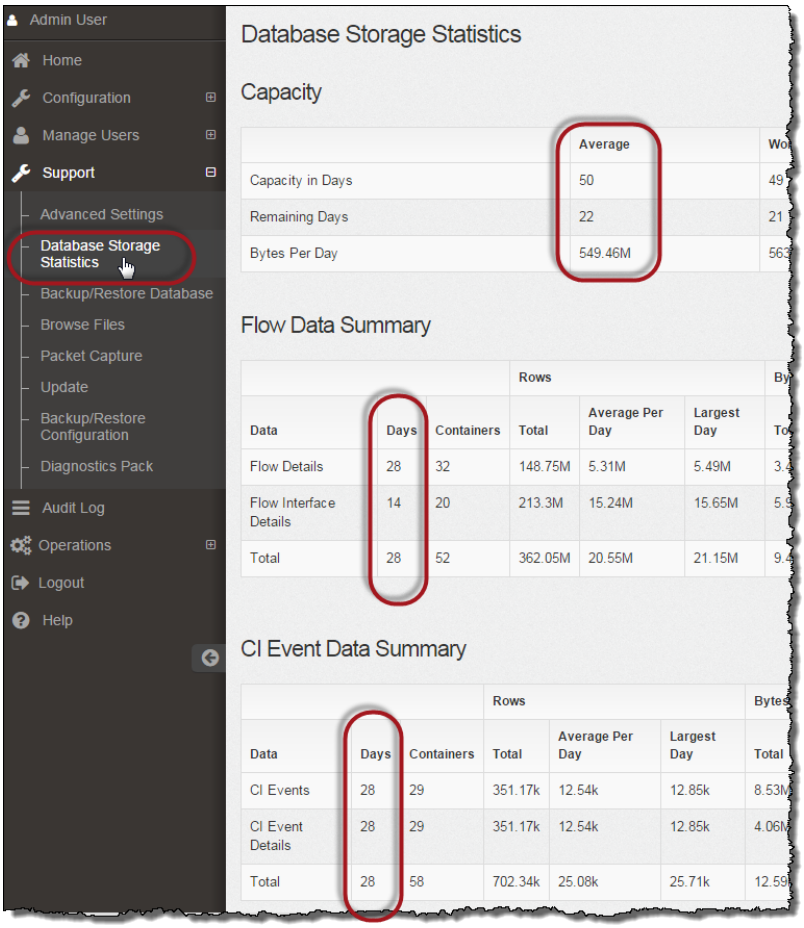
Flow Collector データベースのバックアップは、完了するまでに数日かかる場合があります。また、データベースが大きい場合はネットワークの速度が低下します。データベースをバックアップする前に、Flow Collector データベースをトリミングすることを推奨します。これにより、フローの保存に使用できるディスク容量が解放され、データベースのバックアップにかかる時間が短縮されます。

Flow Collector には、ディスク領域と、1 日あたりに収集されたデータ量に基づいて最大日数が保存されます。最大（/lancope/var パーティションの 75%）に達すると、データベースは最初に最も古いデータを削除して新しいデータを保存できるようにします。

1. データベースストレージの統計情報の確認

次の手順に従って、データベースストレージを確認します。

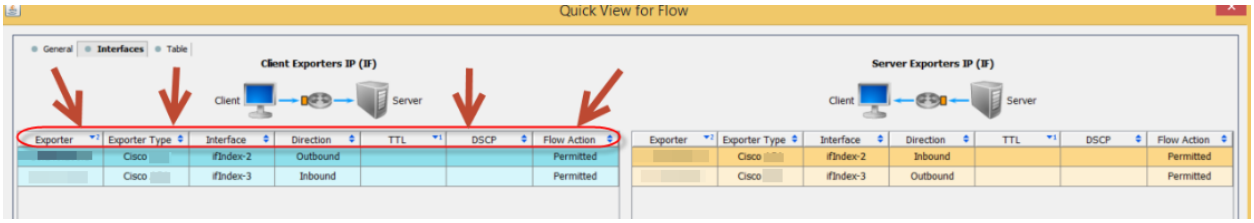
1. Flow Collector アプライアンス管理インターフェイスにログインします。
2. ［サポート（Support）］>［データベースストレージの統計情報（Database Storage Statistics）］を選択します。
3. ［キャパシティ（Capacity）］、［フローデータの概要（Flow Data Summary）］、および［CIイベントデータの概要（CI Event Data Summary）］（または［セキュリティイベントデータの概要（Security Event Data Summary）］）に保存されている日数を確認します。



2. インターフェイスの詳細のトリミング

フロー インターフェイス データは、エクスポータのインターフェイスに関連するデータです。Secure Network Analytics でフロー インターフェイス データおよびフローデータを保存します。

フローインターフェイスのデフォルト設定では、システムによってフローデータがプッシュされるため、可能な限り、すべてのインターフェイスの統計情報を保持できます。この機能は、Data Store システムには適用されないメインツールとしてデスクトップ クライアントを使用します。トリミング手順が Data Store システム以外にのみ適用されることを示すために、ノードが必要になる場合があります。



このデータのバックアップ処理には時間がかかります。すべてのデータが必要なわけではない場合は、保存期間を短くします（例：7日）。この期間よりも古いデータは失われます。

指定した保存期間よりも古いインターフェイス統計データのデータベースを消去し、フローを保存するために使用可能なディスク領域を解放するには、次の手順を実行します。

1. admin ユーザーとして デスクトップ クライアント にログインします。
2. [企業（Enterprise）] ツリーで Flow Collector を見つけます。プラス（+）記号をクリックしてコンテナを展開します。
3. [Flow Collector] を右クリックします。[設定（Configuration）] > [プロパティ（Properties）] を選択します。
4. [Flow Collector のプロパティ（Flow Collector Properties）] ダイアログボックスで、[詳細設定（Advanced）] をクリックします。
5. [フロー インターフェイス データの保存（Store flow interface data）] を選択します。
6. 保存期間を短く設定します。たとえば、期間を**最大 7 日**に設定すると、7 日前より古いデータは失われます。
7. [OK] をクリックします。
8. 5 分待ってから次の手順に進みます。

3. フローの詳細と CI イベントデータのトリミング

Flow Collector データベースのフローの詳細と CI イベント/詳細のサイズを縮小するには、シスコサポートにお問い合わせください。この手順は任意であり、トリミングプロセスは完了までに数分しかかかりませんが、プロセスにはガイダンスが必要です。

NetFlow をトリミングするときは、Flow Collector データベースのフローの詳細と CI イベント/詳細を保持する日数を指定します。この設定では、次の 2 つが発生します。

- データベースは、入力した日数まで切り捨てられます。
- データベースは、最も古い日付に基づいて古いデータからロールアウトを開始しますが、できるだけ多くを保存しようとはしません。

2. 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、次の手順に従って、Manager および Flow Collector 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てください。

> ⚠ Manager および Flow Collector 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. Manager および Flow Collector アプライアンス データベース コンソールに **admin** としてログインします。
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 を繰り返して、保存されているすべての Manager および Flow Collector データベースのスナップショットを削除します。

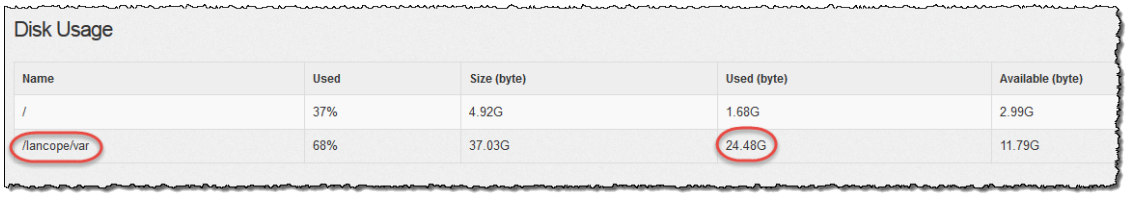
3. リモートファイルシステムへのバックアップ

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、次の手順を実行します。

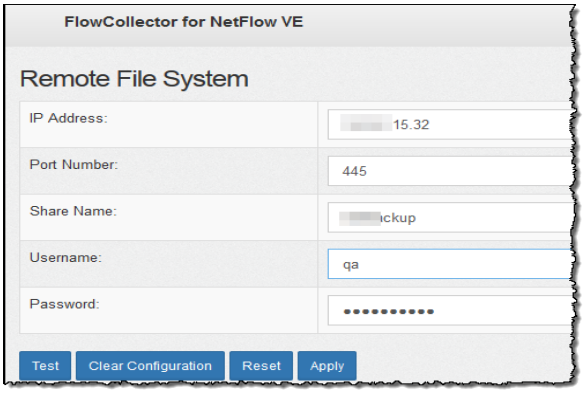
- **領域**：リモート ファイル システムに、データベースのバックアップを保存するための十分な空き領域があることを確認します。
- **時間**：データベースを 1 回バックアップすると、以後は前回のバックアップからの変更点だけがバックアップされるため、バックアップにかかる時間は短くなります。このプロセスでは、1 分あたり約 0.5 GB ～ 2 GB のデータがバックアップされます。

1. アプライアンス管理インターフェイスに戻ります（ただし、デスクトップクライアントは閉じないでください）。
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。

   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。

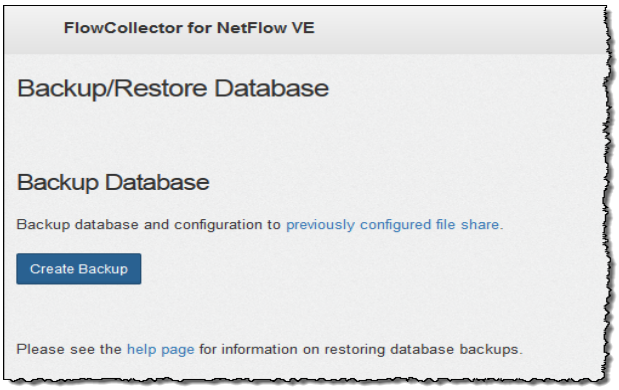
   パスワードを入力しても [適用（Apply）] ボタンが有効にならない場合、[リモートファイルシステム（Remote File System）] ページの空白部分を 1 回クリックすると有効になります。

6. [テスト（Test）] をクリックして、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。

   テストが完了すると、リモート ファイル システムのページの下部に次のメッセージが表示されます。

   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。[データベースのバックアップ（Backup Database）] ページが開きます（次の例を参照）。



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再度削除してください。詳細な手順については、「4. 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。

4. 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、次の手順に従って Manager および Flow Collector データベースのスナップショットを削除します。

> Manager および Flow Collector 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、更新を成功させるために不可欠な手順です。

1. Manager または Flow Collector アプライアンス データベース コンソールに **admin** としてログインします。
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 を繰り返して、保存されているすべての Manager および Flow Collector データベースのスナップショットを削除します。

データベースのバックアップの復元（非 Data Store ドメイン）

Manager と Flow Collector のデータベースを復元するには、次の手順に従います。Data Store を復元するには、「**Data Store バックアップの復元**」を参照してください。

概要

> ⚠ データベースを復元する前に、シスコサポートに連絡することをお勧めします。

データベース復元操作を実行すると、現在のデータベースと設定が以前のバックアップの内容で上書きされます。既存のネットワーク設定は上書きされません。

- **同じバージョン**：以前のバージョンの Secure Network Analytics アプライアンスのバックアップファイルを使用してアプライアンスデータベースを復元することはできません。バックアップファイルのバージョンがアプライアンスのバージョンと一致していることを確認します。
- **以前のバックアップの復元**：コマンド ライン インターフェイスを使用して、データベースの以前のバックアップを復元できます。バックアップされるデータベースは、過去に設定されたリモートファイルシステム（ファイル共有）内に存在するデータベースです。
- **デフォルト**：復元するデータベースの名前を指定しないと、デフォルト名（システムのシリアル番号）が使用されます。

データベースの復元

> ⚠ データベース復元操作を実行すると、現在のデータベースと設定が以前のバックアップの内容で上書きされます。既存のネットワーク設定は上書きされません。
>
> 復元プロセスの開始後は、このプロセスを中断しないでください。

操作の開始後に、このページから離れる（マウスカーソルをページ外部へ移動する）ことができます。プロセスは中断せずに続行されます。戻るとステータスが更新されます。

1. sysadmin としてアプライアンスコンソールにログインし、ルートシェルにアクセスします。
2. **sysadmin** と入力して、Enter を押します。
3. パスワードプロンプトが表示されたら、**lan1cope** と入力して Enter を押します。
4. [システム設定（System Configuration）] メニューで、[詳細設定（Advanced）] を選択し、Enter を押します。
5. [ルートシェル（Root Shell）] を選択して、Enter を押します。
6. ルートシェルパスワードを入力して、Enter を押します。
7. 次のコマンドを実行します。

   ```
   cd /var/tmp
   nohup doDbRestore -c -q &
   ```

   このツールで使用可能なスイッチを確認するには、`doDbRestore -h` コマンドを入力します。

> ⚠ 復元するデータベースの名前を指定しないと、デフォルト名（システムのシリアル番号）が使用されます。

8. 進行中の復元操作のステータスを確認するには、次の 2 つのファイルを表示します。

   /lancope/var/logs/VerticaRestore.log

   /lancope/var/logs/DatabaseRestore.log

   システムは、復元操作を完了すると、再起動してデータ収集を開始します。

Data Store データベース

Data Store を使用して Secure Network Analytics を設定した場合は、Central Management の [Data Store] タブにアクセスできます。

> Data Store を設定に追加するには、「**非 Data Store Flow Collector の Data Store Flow Collector への移行**」および「**非 Data Store 展開への Data Store の追加**」を参照してください。

[Data Store] タブ

Central Management の [Data Store] タブを使用して、次の操作を行います。

- **[ステータス(Status)]**: データベースまたは任意の Data Node のステータスを表示します。詳細については、「**Data Store データベースのステータスの表示**」を参照してください。
- **[起動(Start)] または [停止(Stop)]**: データベースまたは任意の Data Node を起動するか停止できます。詳細については、「**Data Store データベースのステータスの表示**」を参照してください。
- **[ストレージ使用量(Storage Usage)]**: データベースの現在のストレージ使用量に関する統計を表示します。フロー インターフェイス データの保持ステータスを変更することもできます。詳細については、「**[データベース保持(Database Retention)] の表示**」を参照してください。
- **[更新ステータス(Update Status)]**: 更新中のデータノードすべてのステータスを表示します。詳細については、「**Data Node の更新ステータスの監視**」を参照してください。

> すべての Data Node で SSH が有効になっていることを確認します。すべての Data Node で SSH が有効になっていない場合、一部のデータベースアクションを正常に完了できません。

[Data Store] タブを開く

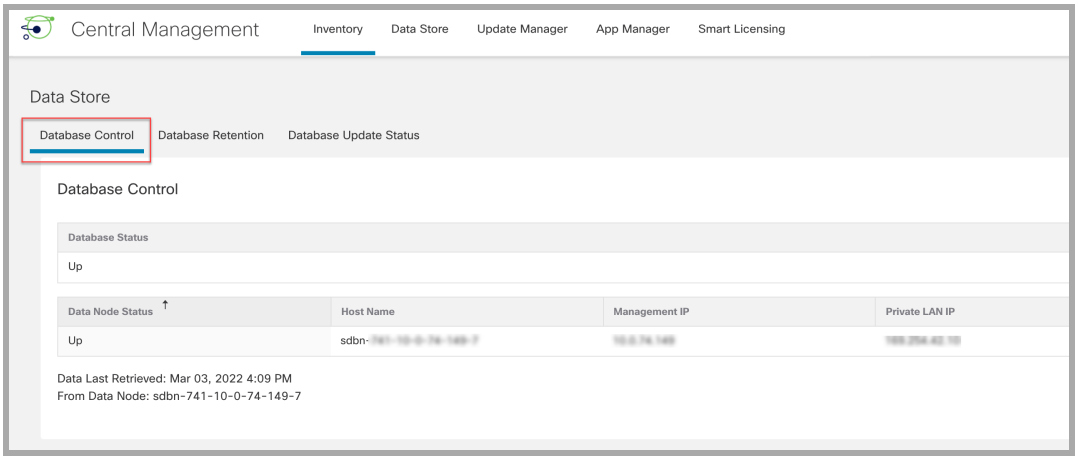
1. Manager にログインします。
2. [構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
3. [Data Store] タブをクリックします。

Data Store データベースのステータスの表示

Central Management の [Data Store] タブをクリックすると、[データベースコントロール(Database Control)] ページが開きます。このタブには、データベースと各データノードのステータスが表示されます。

- **[ソート(Sorting)]**: このタブの Data Node は、デフォルトではプライベート LAN IP でソートされます。ソートに使用する列ヘッダーをクリックして、データノードのノードを再ソートできます。
- **[ステータス(Status)]**: 通常の状態では、データベースとすべての Data Node のステータスは [アップ(Up)] と表示されます。データベースが [アップ(Up)] になっていても、いずれかの Data Node のステータスが [ダウン(Down)] になっていることがあります。障害が発生した Data Node が回復すると、データベースが [アップ(Up)] と表示されていても、新たに回復した Data Node は「回復中」の状態になります。

- **[アクション(Actions)] メニュー**:データベース(または Data Node)を起動または停止するときは、必ず [アクション(Actions)] メニューを使用します。



データベース(または Data Node)を起動または停止するときは、必ず [アクション(Actions)] メニューを使用してください。

データベースの起動

1. [データベースコントロール(Database Control)] タブが選択されていることを確認します。
2. データベースの [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。
3. [スタート(Start)] を選択します。
4. データベースのステータスが [アップ(Up)] と表示されていることを確認します。

データベースの停止

1. [データベースコントロール(Database Control)] タブが選択されていることを確認します。
2. データベースの [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。
3. [停止(Stop)] を選択します。
4. データベースのステータスが [ダウン(Down)] と表示されていることを確認します。

データノードの起動

次の手順に従って、データノードを起動します。

1. [データベースコントロール(Database Control)] タブが選択されていることを確認します。
2. 起動する Data Node 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。
3. [起動(Start)] を選択して Data Node を起動します。
4. Data Node のステータスが [アップ(Up)] と表示されていることを確認します。

Data Node の停止

次の手順に従って、Data Node を停止します。

1. [データベースコントロール(Database Control)] タブが選択されていることを確認します。
2. 停止する Data Node 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。
3. [停止(Stop)] を選択して Data Node を停止します。
4. Data Node のステータスが [ダウン(Down)] と表示されていることを確認します。

最後のアクション結果の確認

ユーザー数に関係なく、一度に実行できるアクションは 1 つだけです。アクションが進行中の場合、他のアクションは実行できません。アクションが完了すると、画面上部のバナーにすべてのユーザーの完了ステータスが表示されます。最後のアクション結果を確認するには、以下の手順に従います。

1. [データベースコントロール(Database Control)] タブが選択されていることを確認します。
2. 画面の下部にある [最後のアクション結果(Last Action Results)] リンクをクリックします。[アクション結果(Action Results)] バナーは、閉じるまで画面に表示されたままになります。

[データベース保持(Database Retention)] の表示

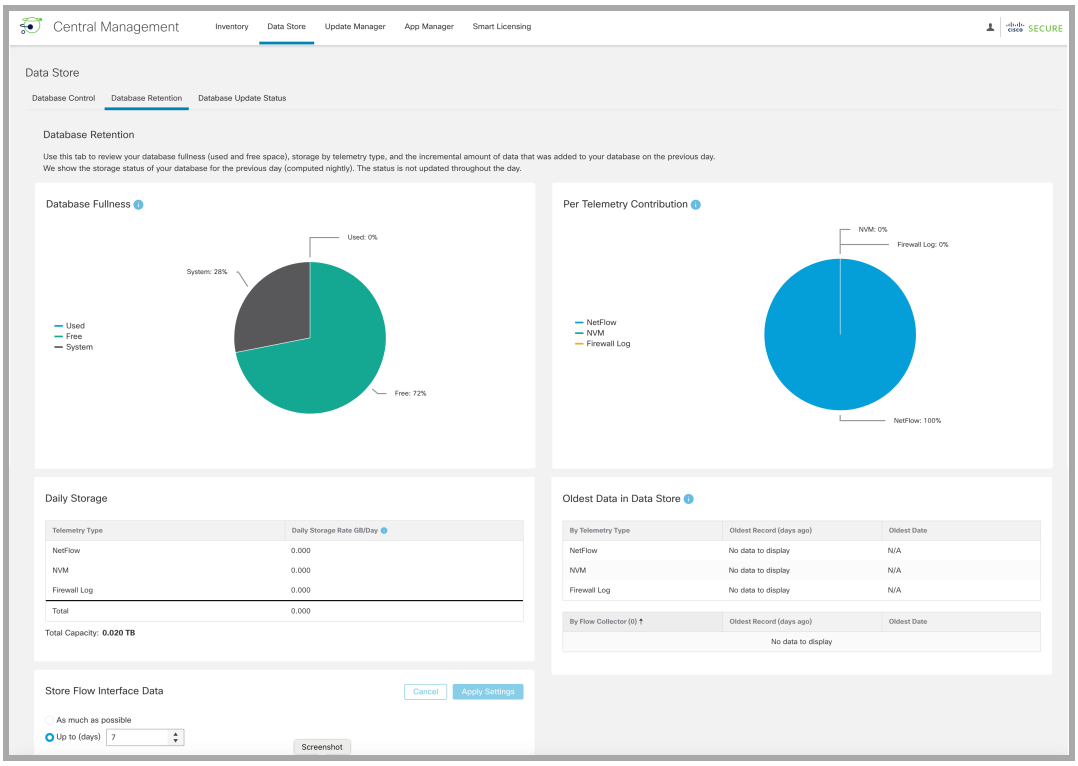
[データベースの保持(Database Retention)] タブには、次のような質問に対する回答があります。

- データベースの空き容量はどの程度ですか。
- 各テレメトリタイプ(NetFlow、NVM、ファイアウォールログ)によってどの程度使用されていますか。
- 昨日、データベースに新たに保存されたデータ量はどの程度ですか。
- データベースの総容量はどの程度ですか。

> このページのすべてのチャートと [データストレージ統計(Data Storage Statistics)] セクションの内容は、1 日に 1 回更新されます。

[Data Store] – [データベースの保持(Database Retention)] タブを開く

1. [構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
2. [Data Store] タブをクリックします。
3. [データベースの保持(Database Retention)] タブをクリックします。



[データベースの充満度（Database Fullness）] チャート

[データベースの充満度（Database Fullness）] チャートには、Data Store データベースの使用済み容量と空き容量が表示されます。

[テレメトリごとの使用量（Per Telemetry Contribution）] チャート

[テレメトリごとの使用量（Per Telemetry Contribution）] チャートには、Data Store データベース内のデータの内訳が表示されます。

[日次ストレージ（Daily Storage）]

[日次ストレージ（Daily Storage）] セクションには、前日にデータベースに追加されたデータの増分量が表示されます。日次ストレージレートを監視することで、データベースがいっぱいになる速度と、各テレメトリタイプが日次ストレージの蓄積に寄与する程度を評価できます。

データストア内の最も古いデータ

この表は、最も古いレコードが Data Store に書き込まれてからの日付と日数を示しています。このデータは 1 日に 1 回更新されます。

Flow Collector（または Flow Collector データベース）にローカルに保存されたデータは、このテーブルには含まれません。非 Data Store Flow Collector を Data Store Flow Collector に移行していて、データ保持ポリシーがある場合は、この表を使用すると、Data Store 内に新しいデータがどれだけあるかを理解し、移行を完了するのに最適な時期を知ることができます。

フロー インターフェイス データの保存の変更

フローインターフェイス統計では、より詳細なフロー統計情報を確認できます。特定のフローに対してネットワーク内に複数の監視ポイントがあり、最近のフローデータのトラブルシューティングや調

査に役立ちます。たとえば、複数のエクスポータや同じエクスポータの複数のインターフェイスでフローが観察された場合、フローインターフェイス統計に詳細が保存されます。

Data Store ではデータが可能な限り保持され、保持期間はシステムの取り込みレートによって決まります。Data Store が最大容量に達すると、最も古いデータの自動削除が開始されます。

フローインターフェイス統計はストレージ消費率が高く、それによって他の重要なデータ（フロー統計など）を保持できる期間が短くなる可能性があります。

> ここでフロー インターフェイス データの保存期間を変更しても、影響を受けるのはシステム内のスペースを占有しているデータの NetFlow 部分のみです。デフォルトは 7 日です。必要に応じて、保持日数を延ばすことも短くすることもできます。

1. [フローインターフェイスデータの保存（Store Flow Interface Data）] セクションで、[可能な限り（As much as possible）] か [最大日数（Up to days）]（上下矢印をクリックして日数を変更）を選択します。
2. [設定の適用（Apply Settings）] をクリックします。

   - 保持期間を長い期間に変更する場合、保存されるデータが保持設定に正確に一致するようになるまで、変更前と変更後の期間の差が経過するのを待ちます。その時点まで、データは使用可能な最も減らされた（最も粗い）分解能を使用して表示されます。たとえば、保持期間を 3 日から 10 日に変更した場合、保存されるデータが保持設定に正確に一致するまでに 7 日かかります。
   - ディスクの使用状況に応じたデータのトリミングにより、選択した保持期間が経過する前にデータが削除されることがあります。データを可能な限り保存するように選択した場合、Data Store が最大容量に達すると最も古いデータの削除が開始されます。

Data Node の更新ステータスの監視

Central Management の Update Manager から Data Node の更新を開始した後、[データベース更新ステータス（Database Update Status）] タブを使用して、各 Data Node におけるデータベースサービスの更新の進行状況を監視します。

[Data Store] – [データベース更新ステータス（Database Update Status）] タブを開く

1. [構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] を選択します。
2. [Data Store] タブをクリックします。
3. [データベース更新ステータス（Database Update Status）] タブをクリックします。

データベースの更新ステータスの監視

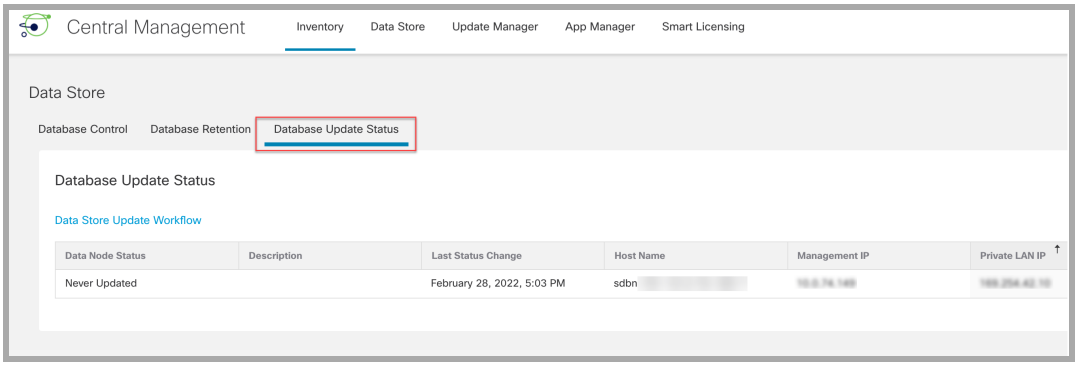
各データノードの更新は一連の状態を経て進行します。[Data Store更新ワークフロー（Data Store Update Workflow）] リンクをクリックして、更新プロセスを視覚的に確認できます（以下に表示）。

> 正常に更新するには、Cisco Secure Network Analytics システム更新ガイド [英語] の更新順序および手順に従ってください。

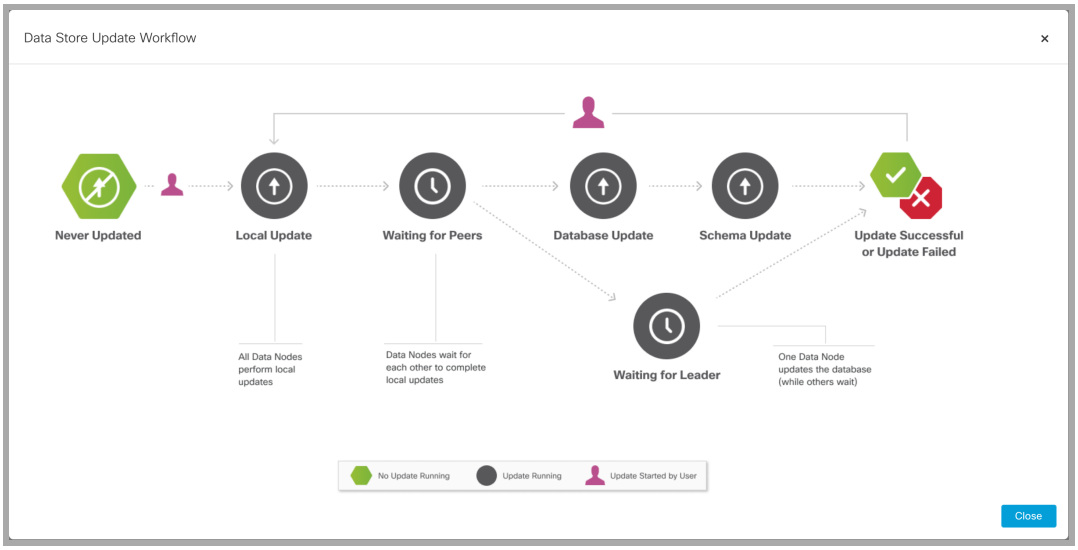
> 以下の画像に表示されている状態遷移の一部は、更新プロセス中に瞬時に発生するため、画面の更新中は遷移を確認できない場合があります。

[データベース更新ステータス（Database Update Status）] タブには、Data Node の現在の更新ステータスが表示されます。Update Manager でソフトウェア更新（アップグレードまたはパッチ適用）を開始したら、このタブで各 Data Node のステータスを監視して更新が完了したことを確認します。更新のワークフローを視覚的に表示するには、[図の表示（View Diagram）] をクリックします。

更新が完了したら、**Data Store データベース**に移動して、データベースのステータスが [アップ（Up）] になっていることを確認します。詳細については、『更新ガイド』を参照してください。



次の図に Data Store の更新のワークフローを示します。



Data Store のバックアップの作成

> これらのタスクの計画と実装については、Cisco プロフェッショナルサービスにお問い合わせください。

Data Store をバックアップするには、次の手順を実行します。

1. バックアップホストのストレージ要件を見積もる

2. バックアップホストを準備する（ストレージ容量がバックアップサイズの 2 倍のバックアップホスト）。バックアップホストに Python v3.7 と rsync 3.0.5 をインストールします。

> Secure Network Analytics アプライアンスとは別の Linux ベースのホストを使用します。

3. dbadmin のパスワードレス SSH アクセスを有効にする。すべての Data Node がパスワードレス SSH アクセスを使用してバックアップホストに到達できることを確認します。

4. バックアップホストのバックアップディレクトリを初期化する

5. データストアデータベースのバックアップ

1. バックアップホストのストレージ要件を見積もる

1. Data Node のコンソールに `root` としてログインします。
2. 次のコマンドをコピーし、コマンドラインに貼り付けて Enter を押して、vsql を使用してデータベースに接続してクエリを実行します。プロンプトが表示されたら、パスワードを入力します。結果をメモします。

```
/opt/vertica/bin/vsql -U dbadmin -c "SELECT SUM(used_bytes)
FROM storage_containers;"
```

3. 合計に 2 を掛けて、バックアップホストに必要なストレージ容量を見積もります。

2. バックアップホストを準備する

1. 「**1. バックアップホストのストレージ要件を見積もる**」で見積もったストレージ要件に基づいて、バックアップを格納するネットワーク上で Linux を実行しているホストを特定するか、必要なストレージ要件を満たす Linux を実行しているホストを展開します。

> Secure Network Analytics アプライアンスとは別の Linux ベースのホストを使用します。

2. バックアップホストのコンソールに `root` としてログインします。
3. コマンドプロンプトで `python3 --version` と入力して Enter を押し、インストールされている Python のバージョンを確認します。次の選択肢があります。
   - Python 3.7 以降がインストールされている場合は、手順 6 に進みます。
   - それ以外の場合は、手順 4 から Python 3.7 をインストールします。

4. `sudo apt-get update` と入力して Enter を押し、Python を含むパッケージの更新バージョンをダウンロードします。プロンプトが表示されたら、パスワードを入力します。
5. `sudo apt-get install python3.7` と入力して Enter を押し、Python 3.7 をインストールします（違うバージョンをインストールするにはコマンドを修正してください）。
6. コマンドプロンプトで `rsync -version` と入力して Enter を押し、インストールされている rsync のバージョンを確認します。次の選択肢があります。
   - rsync 3.0.5 以降がインストールされている場合は、手順 9 に進みます。
   - それ以外の場合は、rsync 3.0.5 をインストールします。手順 7 に進みます。
7. `sudo apt-get update` と入力して Enter を押し、rsync を含むパッケージの更新バージョンをダウンロードします。プロンプトが表示されたら、パスワードを入力します。
8. `sudo apt-get install rsync` と入力して Enter を押し、rsync をインストールします。
9. コマンドプロンプトで `getent passwd | grep dbadmin` と入力して Enter を押し、このホストに `dbadmin` ユーザーアカウントが存在するかどうかを確認します。次の選択肢があります。
   - `dbadmin` ユーザーアカウントが存在していれば、バックアップホストの準備は完了です。「**3. dbadmin のパスワードレス SSH アクセスを有効にする**」に進みます。
   - それ以外の場合は、このホストに `dbadmin` ユーザーアカウントを作成します。手順 10 に進みます。
10. コマンドプロンプトで `adduser dbadmin` と入力して Enter を押し、`dbadmin` ユーザーアカウントを作成します。
11. `passwd dbadmin` と入力して Enter を押し、`dbadmin` にパスワードを割り当てます。
12. 新しいパスワードを入力して Enter を押し、`dbadmin` のパスワードを設定します。プロンプトが表示されたら、確認のためにパスワードを再入力します。

3. dbadmin のパスワードレス SSH アクセスを有効にする

1. SSH 用にバックアップホストと各データノードの間でポート 22/TCP を開き、rsync 用にバックアップホストと各データノードの間でポート 50000/TCP を開きます。
2. OpenSSH の `ssh-copy-id dbadmin@<hostname>` に関するドキュメントで詳細を確認します。
3. 次のように入力して、最初のデータノードに `dbadmin` としてログインします。

   ```
   su dbadmin
   ```

4. 次のコマンドをコピーし、プレーンテキストエディタに貼り付けます。

   `ssh-copy-id dbadmin@[hostname]` ここで、`[hostname]` はバックアップホストのホスト名か IP アドレスです。
5. 更新したコマンドをコピーし、コマンドプロンプトに貼り付けて Enter を押して、`dbadmin` の SSH 認証キーをバックアップホストにコピーします。
6. 次のコマンドをコピーし、プレーンテキストエディタに貼り付けます。

`ssh 'dbadmin@[hostname]'` ここで、`[hostname]` はバックアップホストのホスト名か IP アドレスです。

7. 更新したコマンドをコピーし、コマンドプロンプトに貼り付けて Enter を押して、この Data Node からリモートホストのコンソールに SSH を介してパスワードなしでログインできることを確認します。

4. バックアップホストのバックアップディレクトリを初期化する

1. 最初のデータノードのコンソールに `root` としてログインします。

> バックアップディレクトリの初期化に使用する Data Node をメモします。同じデータノードを使用して、後の手順（「**5. データストアデータベースのバックアップ**」）で Data Store データベースをバックアップします。

2. `su - dbadmin` と入力して Enter を押し、以降のコマンドを `dbadmin` ユーザーとして実行します。
3. `ssh [backup-host]` と入力します。ここで、[backup host] はバックアップサーバーのホスト名または IP アドレスです。パスワードの入力を求められることなく、`dbadmin` としてバックアップホストのインターフェイスにログインできます。バックアップホストからパスワードの入力を求められる場合は、設定を確認します。
4. `cd /home/dbadmin` と入力して Enter を押し、ディレクトリを変更します。
5. `mkdir backups` と入力して Enter を押し、`backups` ディレクトリを作成します。
6. `exit` と入力して Enter を押し、Data Node のコマンドラインプロンプトに戻ります。
7. `vi pw.ini` と入力して Enter を押し、`pw.ini` バックアップ パスワード ファイルを作成して編集します。

> setup-sw-datastore-secure-connectivity スクリプトを使用して dbadmin のパスワードを更新した場合は、pw.ini バックアップ パスワード ファイルに保存されているパスワードも更新する必要があります。これを行わないとバックアップが失敗します。

8. 次の行をプレーンテキストエディタにコピーします。

```
[Passwords]
dbPassword = [dbadmin-password]
```

9. `[dbadmin-password]` を Data Store の `dbadmin` パスワードに更新します。
10. 更新した行をコピーし、`pw.ini` バックアップ パスワード ファイルに貼り付けます。
11. Esc を押してから、`:wq` と入力して Enter を押し、変更を保存して終了します。
12. `chmod 640 pw.ini` と入力して Enter を押し、`pw.ini` ファイルの権限を変更して、`dbadmin` ユーザーにファイルの読み取りと編集を許可します。
13. 各ノードについて、次に示すように `/etc/default/ssh` ファイルの `SSHD_OPTS` を編集/変更します。このプロセスを完了するには、`root` としてログインする必要があります。

    作業前：

```
SSHD_OPTS="-o AllowUsers=root -o AllowUsers=sysadmin -o
Banner=/etc/issue.net -o PermitRootLogin=yes -o
AllowTcpForwarding=no"
```

作業後:

```
SSHD_OPTS="-o AllowUsers=root -o AllowUsers=sysadmin -o
AllowUsers=dbadmin -o Banner=/etc/issue.net -o
PermitRootLogin=yes -o AllowTcpForwarding=yes"
```

14. 次のように ssh サービスを再起動します。

```
systemctl restart ssh
```

15. 次の行をコピーし、プレーンテキストエディタに貼り付けます。

```
[Mapping]
v_sw_node0001 = backup-host-ip:/home/dbadmin/backups
v_sw_node0002 = backup-host-ip:/home/dbadmin/backups
v_sw_node0003 = backup-host-ip:/home/dbadmin/backups

[Misc]
snapshotName = data_store_backup
passwordFile = /home/dbadmin/pw.ini
enableFreeSpaceCheck = True
retryCount = 2
retryDelay = 1

[Transmission]
encrypt = true
checksum = true
concurrency_backup = 2
concurrency_restore = 2
```

16. `vi config.ini` と入力して Enter を押し、`config.ini` バックアップ設定ファイルを作成して編集します。
17. 手順 15 でプレーンテキストエディタに貼り付けたテキストをコピーし、`config.ini` ファイルに貼り付けます。
18. *backup-host-ip* をバックアップホストの IP アドレスに置き換えます。
19. `[Mapping]` の下のホスト名がデータノードと一致しない場合は、それらのホスト名を更新します。データノードのノード名を決定するには、次の手順を実行します。

    - データノードコンソールに `root` として接続します。
        - `su dbadmin` と入力します。
        - `admintools -t node_map` と入力します。
    - `[Mapping]` エントリの「NODENAME」列にはノード名を使用します。

例:

```
dbadmin@sdbn-742-10-0-56-133-5:/root$ admintools -t node_map
データベース     | ノード名                  | ホスト名
-------------------------------------------------------
sw          | v_sw_node0001          | 169.254.42.10
sw          | v_sw_node0002          | 169.254.42.12
sw          | v_sw_node0003          | 169.254.42.15
```

20. 4 つ以上のデータノードを環境に展開した場合は、それぞれのエントリがあることを確認します。データノードが 1 つしかない場合は、余分な [Mapping] 行を削除して、単一のデータノードに 1 行だけを残します。
21. Esc を押してから、:wq と入力して Enter を押し、変更を保存して終了します。
22. vbr -t init -c config.ini と入力して Enter を押し、Data Store のバックアップを受信するバックアップホストの /home/dbadmin/backups ディレクトリを初期化します。

5. データストアデータベースのバックアップ

> マルチノードデータベース全体をバックアップするには、1 つのデータノードでバックアップコマンドを発行します。

1. root として、「**4. バックアップホストのバックアップディレクトリを初期化する**」でバックアップホストのディレクトリを初期化した Data Node のコンソールにログインします。
2. su - dbadmin と入力して Enter を押し、以降のコマンドを dbadmin ユーザーとして実行します。
3. vbr -t backup -c config.ini --debug 3 --dry-run と入力して Enter を押し、バックアップを作成せずにバックアップのテストを実行します。次のオプションがあります。
   - バックアップのテストに成功した場合は、Data Store をバックアップし、手順 4 に進みます。
   - バックアップテストが失敗した場合は、スナップショットファイルが作成されている可能性があるため、削除する必要があります。削除手順については、「Data Store のバックアップの失敗」を参照してください。バックアップテストに失敗した場合は、/tmp/vbr ディレクトリのデバッグログファイルを確認し、根本原因を解決してから、バックアップのテストを再度実行します。さらに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。
4. vbr -t backup -c config.ini と入力して Enter を押し、Data Store をバックアップホストの /home/dbadmin/backups ディレクトリにバックアップします。

データストアのバックアップの失敗

Data Store のバックアップが失敗した場合、別のバックアップを試みる前に、データベースのスナップショットを削除してください。次の手順に従って、Data Store データベースのスナップショットを削除します。

1. **vsql** を使用してテータストアデータベースのクラスタに接続します。
2. 次のコマンドを実行して、スナップショットのリストを取得します。

   ```
   select * from database_snapshots;
   ```

3. 「snapshot_name」を削除するスナップショットの名前に置き換えてから、次のコマンドを実行します。

   ```
   select remove_database_snapshot('snapshot_name');
   ```

4. 次のコマンドを実行して終了します。

   ```
   \q
   ```

Data Store バックアップの復元

> これらのタスクの計画と実装については、Cisco プロフェッショナルサービスにお問い合わせください。

Data Store をバックアップするには、次の手順を実行します。

1. バックアップ名とソフトウェアバージョンを確認する
2. Data Store データベースを停止する
3. バックアップから Data Store を復元する
4. Data Store を起動する
5. catalog スナップショットを削除する
6. 復元したデータベースを確認する

> Data Store のバックアップは、そのバックアップを取った Data Store にのみ復元できます。ある Data Store から取得したバックアップを別の Data Store に復元することはできません。Data Store のバックアップを作成するときは、任意の Data Node を使用してバックアップコマンドを発行します。Data Store のバックアップを復元するときは、任意の Data Node を使用して復元コマンドを発行します（バックアップの作成に使用した Data Node である必要はありません）。

1. バックアップ名とソフトウェアバージョンを確認する

1. Data Store データベースのバックアップと Data Store の Data Node 名と Data Node 数が同じであることを確認します。
2. Data Store データベースのバックアップと Data Store に同じバージョンの Secure Network Analytics がインストールされていることを確認します。

> シスコは、バックアップバージョンと異なるバージョンへのデータベースの復元をサポートしていません。

2. Data Store データベースを停止する

1. 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. [Data Store] タブをクリックします。
4. データベースを見つけます。
5. [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。
6. [停止（Stop）] を選択します。
7. [Data Storeデータベースコントロール（Data Store Database Control）] タブを開いたままにしておきます。このタブは後の手順で使用します。

3. バックアップから Data Store を復元する

> 比較のために、データベースの復元の前後に必ず次のコマンドを実行します。
> `/opt/vertica/bin/vsql -U dbadmin -w <'password'> -c "select* from partitions;" >/lancope/var/tcpdump/partitions-full-DBbackup`

1. `setup-sw-datastore-secure-connectivity` スクリプトを使用して `dbadmin` のパスワードを更新した場合は、`pw.ini` バックアップ パスワード ファイルに保存されているパスワードも更新する必要があります。これを行わないと復元が失敗します。
2. `config.ini` バックアップ設定ファイルを保存した Data Node を特定し、そのコンソールに `root` としてログインします。詳細については、「**4. バックアップホストのバックアップディレクトリを初期化する**」を参照してください。
3. `su - dbadmin` と入力して Enter を押し、以降のコマンドを `dbadmin` ユーザーとして実行します。
4. コマンドプロンプトで `vbr --task restore --config-file config.ini` と入力して Enter を押し、バックアップホストから Data Store を復元します。

> マルチノードデータベース全体を復元するには、1 つのデータノードで復元コマンドを発行します。

4. Data Store を起動する

1. Central Management の [Data Storeデータベースコントロール（Data Store Database Control）] タブに戻ります。
2. データベースを見つけます。
3. [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。
4. [スタート（Start）] を選択します。

5. catalog スナップショットを削除する

Data Store を再起動したら、`catalog` という名前のスナップショットを削除します。このスナップショットは復元に成功した後は不要であり、削除しないと Vertica による保持管理が実行されません。

1. Data Node のコンソールに `root` としてログインします。
2. `su - dbadmin` と入力して Enter を押し、以降のコマンドを `dbadmin` ユーザーとして実行します。
3. 次のコマンドを入力して `[password]` を `dbadmin` パスワードに置き換えてから Enter を押します。これにより、`catalog` スナップショットが削除されます。

   ```
   /opt/vertica/bin/vsql -U dbadmin -w [password] -c "select remove_database_snapshot('catalog');"
   ```

6. 復元したデータベースを確認する

比較のために、データベースの復元の前後に必ず次のコマンドを実行します。

```
/opt/vertica/bin/vsql -U dbadmin -w <password> -c "select*
from partitions;" >/lancope/var/tcpdump/partitions-full-
DBbackup
```

Data Store のメンテナンス

このセクションは、次の Data Store のトピックで構成されています。

- **Data Store でのデータ圧縮の有効化**
- **Data Store ドメインの追加**
- **Data Store 初期化後のセカンダリ Manager または Flow Collector の追加**
- **Data Store への Data Node の追加**
- **Data Node の交換（ハードウェアのみ）**

> 開始する前に手順を確認してください。一部の手順には、シスコサポートへのサポートの依頼が含まれています。

Data Store でのデータ圧縮の有効化

Data Store で設定された Flow Collector の新規インストールでは、データ圧縮がデフォルトで有効になっています。データ圧縮を使用すれば、Flow Collector と Data Store 間の帯域幅使用量を削減できます。これは、Flow Collector から Data Store へのネットワーク帯域幅が制限されているシナリオで特に便利です。

圧縮を有効にすると、この帯域幅を最大 90% 削減できます。データ圧縮が無効になっている場合は、Flow Collector 単位で有効にできます。Data Store に送信されるデータの圧縮を有効にするには、Flow Collector インターフェイスで次の設定変更を実行します。

1. Flow Collector 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。
2. [サポート（Support）] > [詳細設定（Advanced Settings）] の順にクリックします。
3. ingest_enable_compression フィールドに次のいずれかを入力します。
   - 1：データ圧縮を有効にする。
   - 0：データ圧縮を無効にする。
4. [適用（Apply）] をクリックしてから、情報ウィンドウで [OK] をクリックします。

このページの設定の多くは、誤って設定するとパフォーマンスに悪影響を与える可能性がありますが、データ圧縮の有効化に関しては、Flow Collector と Data Store の間のデータ転送に関するシステムパフォーマンスが向上する以外の影響はありません。

Data Store ドメインの追加

このセクションに示すように、既存の Data Store に Manager、Flow Collector、およびデータノードを追加できます。展開内に Data Store ドメインがない場合は、「**非 Data Store 展開への Data Store の追加**」の手順に従ってください。

Data Store 初期化後のセカンダリ Manager または Flow Collector 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 にセカンダリ Manager または Flow Collector を追加します。

セカンダリ Manager およびフェールオーバー設定の詳細については、「3. Manager フェールオーバー関係の定義」を参照してください。

Data Store なしで使用するように設定した既存の 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、Data Store 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. **Data Store なしの既存の Flow Collector**：「工場出荷時のデフォルトへのリセット」の手順に従います。

> 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やり直す必要があります。

2. 「1. 初回セットアップを使用した環境の設定」と「2. 管理対象システムの設定」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。
3. Manager アプライアンスコンソールに root としてログインします。
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。画面の指示に従います。
   - プロセスが完了したら、Central Management をチェックして、アプライアンスステータスが [接続済み（Connected）] になっていることを確認します。
   - [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。

Data Store への Data Node の追加

> これらのタスクの計画と実装については、Cisco プロフェッショナルサービスにお問い合わせください。

要件

Data Store に Data Node を追加する前に、次の要件を確認してください。

- Data Store は、1 つまたは 3 つ以上の Data Node をサポートします。Data Node は 3 つ 1 セットで追加できます。
- 単一 Data Node（1）展開がある場合は、2 つの Data Node を追加して、展開を 3 つの Data Node のセット（および追加の 3 つ 1 セット）に拡張できます。
- Data Node が 2 つしかない Data Store はサポートされません。

はじめる前に

Data Store を拡張するときは、メンテナンスウィンドウの使用を検討することをお勧めします。

Data Store を拡張する前に、すべてのデータがデータノード全体に均等に分散されます。たとえば、3 ノードの Data Store では、データの 3 分の 1 が各データノードに存在します。Data Store を拡張すると、すべてのデータが新しく追加されたノードに均等に再分散されます。たとえば、3 ノードの Data Store が合計 6 ノードに拡張された場合、各データノードにデータの 6 分の 1 が再分散されます。単

一ノードの Data Store を 3 つのノードに拡張すると、各ノードにデータの 3 分の 1 が再分散されます。

データの再分散の操作中は、Data Store のクエリフォーマンスが一時的に低下する場合があります。影響の規模と期間は、移動する必要があるデータの量と、データノード間のプライベート LAN の帯域幅に関連します。たとえば、ポートボンディングを備えたハードウェア Data Store は、20GB のプライベート LAN 帯域幅を使用してデータを移動できます。データの再分散中もデータベースは動作し続けますが、ユーザーへの影響を最小限に抑えるには、メンテナンスウィンドウを使用することをお勧めします。

手順

展開に Data Node を追加するには、次の手順を実行します。

1. Data Store のバックアップを作成する

Data Node を追加する前に、Data Store をバックアップします。手順の詳細については、「**Data Store のバックアップの作成**」を参照してください。

2. Data Node を設定して Central Management に追加する

1. ネットワークに Data Node を展開します。手順については、『x2xx シリーズ ハードウェア アプライアンス設置ガイド』、『Secure Network Analyticsx3xx シリーズ ハードウェア アプライアンス設置ガイド』、または『Virtual Edition アプライアンス設置ガイド』を参照してください。

> インストール中に Data Node Virtual Edition に 2 つのネットワークアダプタを割り当ててください。初回セットアップの開始時に 2 番目のネットワークアダプタを検出できなければ解決に失敗し、Data Node 間通信に使用するルーティング不可能な IP アドレスを割り当てることができなくなります。

2. 初回セットアップで Data Node を設定します。この手順では、ルーティング可能な（eth0）管理 IP アドレスを割り当てて Data Node 間通信を設定します。
3. アプライアンス設定ツールを使用して Central Management に Data Node を追加します。

3. Data Store に Data Node を追加する

1. Manager アプライアンスコンソールに root としてログインします。
2. `SystemConfig` と入力して、Enter キーを押します。
3. [データストア（Data Store）] を選択します。
4. [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。
5. [Data Store] メニューから [新しいData Node（New Data Nodes）] 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。

    - プロセスが完了したら、Central Management をチェックして、アプライアンスステータスが [接続済み（Connected）] になっていることを確認します。
    - [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。

4. Data Store のデータを再調整する

> ⚠ 追加の Data Node を Data Store に追加した後は、再調整が必要です。このプロセスで支援が必要な場合は、シスコ サポート までお問い合わせください。

Data Node の交換（ハードウェアのみ）

次の手順に従って、次のシナリオ用に新しい（スペア）Data Node を準備します。

- 別の IP アドレスを持つスペア Data Node による Data Node の交換
- 応答しない Data Node の交換
- 既存の Data Node が停止した後のスペア Data Node の追加

どのシナリオでも、新しい（スペア）Data Node を準備し、シスコサポートと連携して交換を完了します。

> ℹ これらのタスクの計画と実装については、Cisco プロフェッショナルサービスにお問い合わせください。

1. 新しい（スペア）Data Node を準備する

1. 既存の Data Node アプライアンスと同じラックセットアップ内に新しい（スペア）Data Node アプライアンスを設置します。設置手順については、『x2xx シリーズ ハードウェア アプライアンス設置ガイド』または『Secure Network Analytics x3xx シリーズ ハードウェア アプライアンス設置ガイド』を参照してください。

   次の点をチェックします。

   - 新しい Data Node が同じスイッチ/ポートに接続されていることを確認します。
   - 新しい Data Node が、既存の Data Node のプライベートおよびパブリックインターフェイスと同じ VLAN 内にあることを確認します。

2. Data Node を電源に接続して電源を入れます。
3. 既存の Data Node ですでに実行されているイメージと一致するように、新しい Data Node のイメージをアップグレードします。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。
4. 初回セットアップで Data Node を設定します。Data Node に適切な eth0 管理 IP およびプライベート IP アドレスを割り当て、その Data Node が既存の Data Node の eth0 およびプライベート IP と同じ VLAN 内にあることを確認します。
5. 次の手順を実行して、接続が完全であることを確認します。

   - Manager とすべての Flow Collector から新しいデータノードの eth0 IP アドレスに ping を実行します。
   - 既存のすべての Data Node から新しい Data Node のプライベート IP に ping を実行します。

- 新しいデータノードから Manager とすべての Flow Collector の eth0 管理 IP に ping を実行します。
- 新しい Data Node から既存の Data Node すべてのプライベート IP に ping を実行します。

2. Data Store のバックアップを作成する

手順の詳細については、「**Data Store のバックアップの作成**」を参照してください。

3. シスコサポートの連絡先

シスコサポートに連絡して交換を完了します。

非 Data Store Flow Collector の Data Store Flow Collector への移行

非 Data Store Flow Collector を Data Store Flow Collector に移行するには、次の手順を使用します。このプロセスにより、移行前のデータや可視性を失うことなく、既存の Flow Collector を、Data Store データベースを使用するように移行できます。以下の手順を完了すると、必要がなくなるまで既存のデータを保持できます。非 Data Store Flow Collector を Data Store Flow Collector に移行すると、Data Store でのみ使用可能な次のような機能も利用できます。

- **取り込み容量の増加**：Data Store の展開は、1 秒あたり最大 300 万フローまで拡張可能であり、現在の取り込み容量の制限の一部を緩和できる可能性があります。Data Store モードの Flow Collector は、パフォーマンスが最大 200% 向上する可能性があります。
- **マルチテレメトリのサポート**：Data Store の展開は、NetFlow、リモートワーカー/エンドポイント（NVM）、ファイアウォール接続、およびセキュリティ イベント テレメトリを処理できます。
- **長期データ保持**：Data Store の展開はスケーラブルなストレージを提供し、Flow Collector を追加することなく長期データ保持（最大 2 年間）を可能にします。
- **エンタープライズクラスのデータ回復力**：テレメトリデータはデータノード全体に冗長的に保存されます。これにより、単一ノードの障害時にサービスが中断されることはありません。
- **クエリとレポートの応答時間の大幅な改善**：Data Store は、クエリのパフォーマンスとレポートの応答時間を大幅に改善します。これは、非 Data Store 展開モデルと比較して、場合によっては 10 倍以上高速です。
- **Analytics**：Analytics は、追加の検出機能やモデリング機能に加えて、セキュリティ上の懸念事項を確認して優先順位付けし、対処できる新しいインターフェイス機能を提供します。Analytics は以下を提供します。
  - 自動ロール検出
  - 追加アラート機能
  - 実験的なアラートダッシュボード
  - サポートデバイスレポート
- **SAL テレメトリ**：Security Analytics and Logging（SAL）は、ファイアウォール（FTD および ASA）からのログを集約し、ネットワークアクティビティの直感的なビューを提供することにより、意思決定を合理化します。SAL は自由に拡張できるため、長期間の保持と分析が可能になり、ファイアウォールで見つかった潜在的な脅威に関するアラートも可能になります。

準備

移行を開始する前に、作業内容を確認して、Flow Collector の移行に必要な準備と手順を把握してください。

次の点に注意してください。

- **1 つずつ**：一度に 1 つの Flow Collector のみ、移行を開始できます。ただし、多数の Flow Collector を同時に移行状態にすることができます。
- **クエリオプション**：Flow Collector が移行状態になると、非 Data Store ドメインを介した移行を開始する前に収集された非 Data Store 履歴データと、非 Data Store ドメインを介した移行の後に Data Store で収集された新しいデータの両方をクエリできます。

構成ファイルのバックアップ

> ⚠ Flow Collector の状態（非 Data Store、移行中、または Data Store）を変更したら、必ず Central Management の構成ファイルをバックアップしてください。Flow Collector がバックアップを取ったときと同じ状態である場合にのみ、システムに復元できます。

Flow Collector 移行要件

Flow Collector を移行する前に、少なくとも 1 つの Data Node が展開されていることと、「**6. Data Store の初期化**」で説明されている Data Store 初期化プロセスが完了していることを確認してください。まだ Data Node を 1 つも展開していない場合、その手順については、『x2xx シリーズ ハードウェア アプライアンス設置ガイド』、『x3xx シリーズ ハードウェア アプライアンス設置ガイド』、または『Virtual Edition アプライアンス設置ガイド』を参照してください。Data Node を展開したら、「**Flow Collector の Data Store への移行の開始**」の手順を実行できます。

Flow Collector の Data Store への移行の開始

非 Data Store Flow Collector を Data Store Flow Collector に移行するには、次の手順に従います。

> ⚠ このプロセスを開始したら、Flow Collector を以前の状態に戻すことはできません。以下の手順に従って移行を完了する必要があります。

1. Data Store ドメインの確認

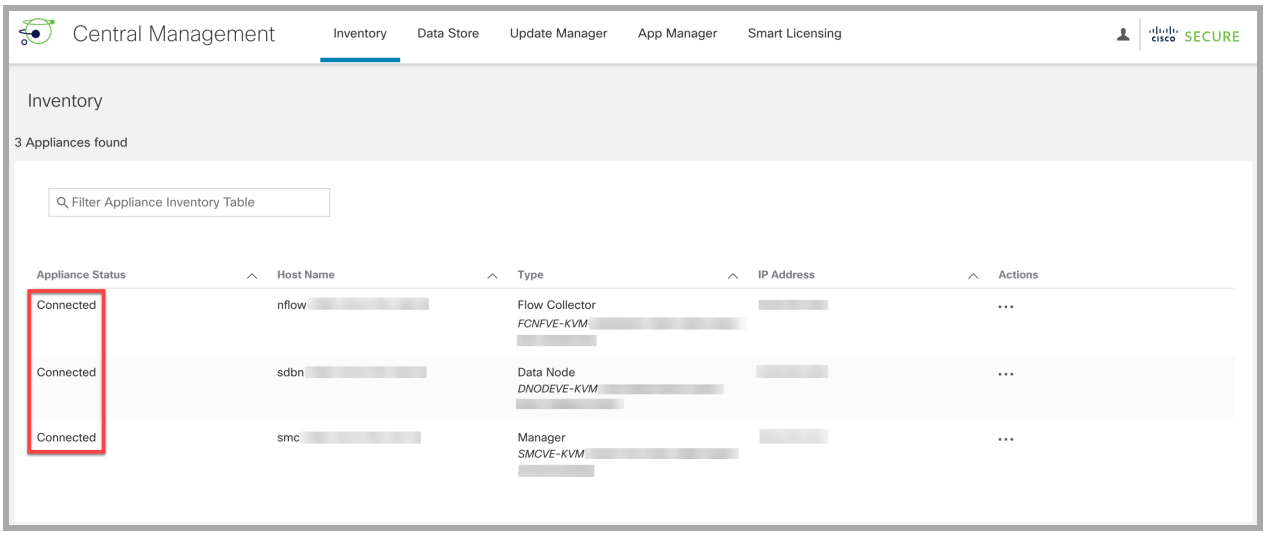
移行する Flow Collector に対応する Data Store ドメインを特定します。Flow Collector は、このドメインに移行します。

- **Data Store ドメインの追加**：Data Store ドメインを追加する必要がある場合は、このガイドの「**ドメインの追加と設定**」セクションの手順に従ってドメインを作成できます。
- **既存のドメインのインポート**：既存の非 Data Store ドメインから設定をインポートする場合は、このガイドの「**既存の Data Store 以外のドメイン設定のインポートによる Data Store ドメインの作成（オプション）**」セクションの指示に従います。
- **ドメインの同期**：Flow Collector の移行中、移行前の非 Data Store ドメインと Data Store ドメインの間で設定と調整の同期を維持できます。詳細については、「**Data Store ドメインと非 Data Store ドメインの同期**」を参照してください。

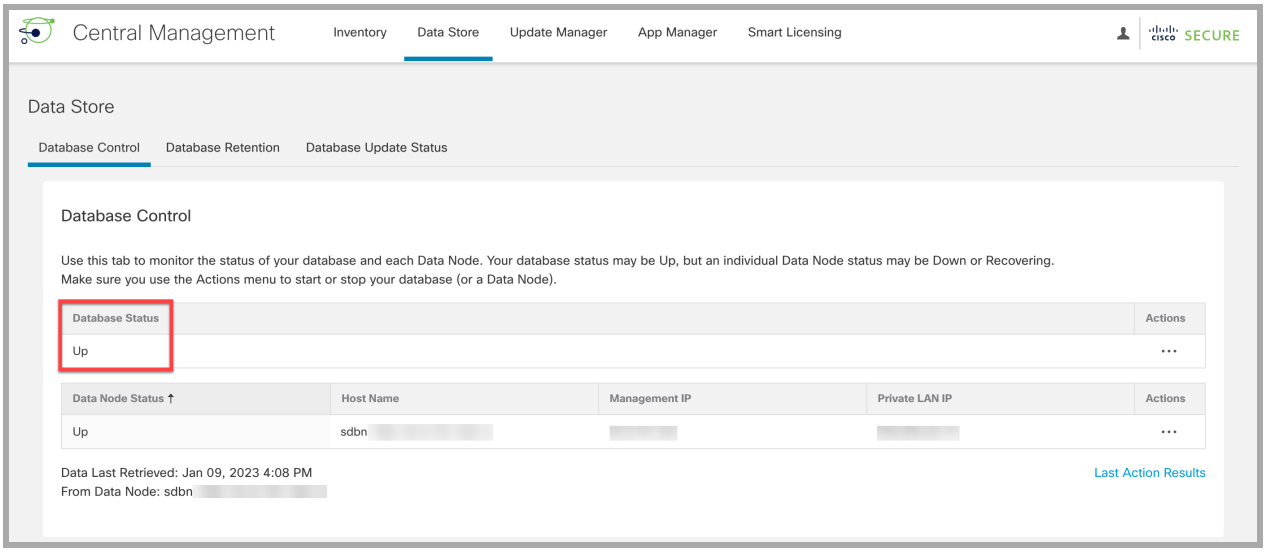
2. アプライアンスのステータスのチェック

Central Management のインベントリを確認します。

1. ［構成（Configure）］>［グローバル集中管理（GLOBAL Central Management）］を選択します。
2. すべてのアプライアンスが［接続済み（Connected）］と表示されていることを確認します。アプライアンスがこれらの状態でない場合は、次の手順に進む前に、これらの状態にすることを試みてください。アプライアンスをこれらの状態にできない場合は、シスコ サポート にお問い合わせください。



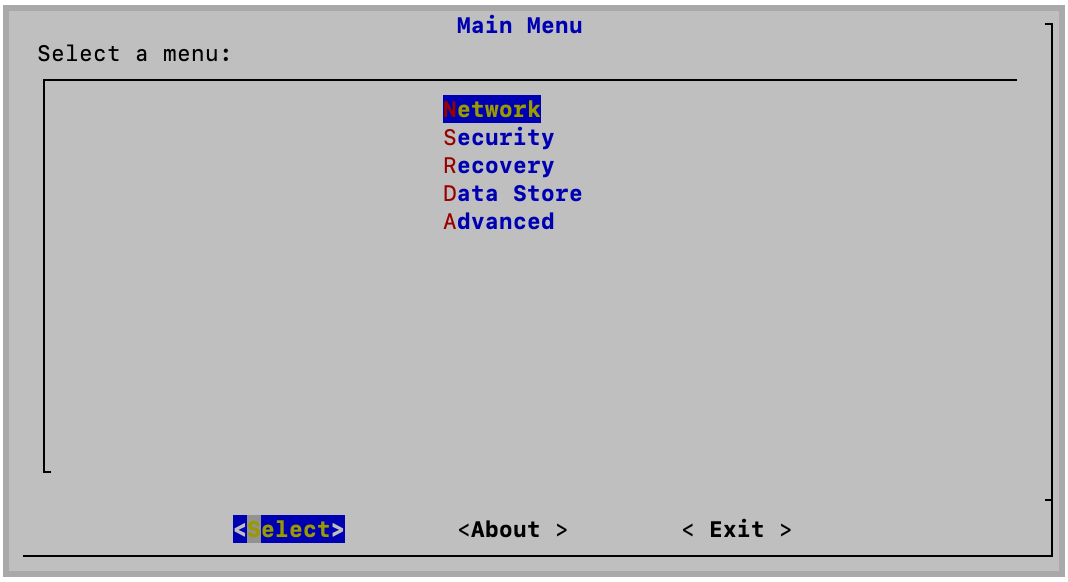
3. [Data Storeデータベースコントロール（Data Store Database Control）] タブを選択します。[データベースのステータス（Database Status）] に [アップ（Up）] と表示されていることを確認します。



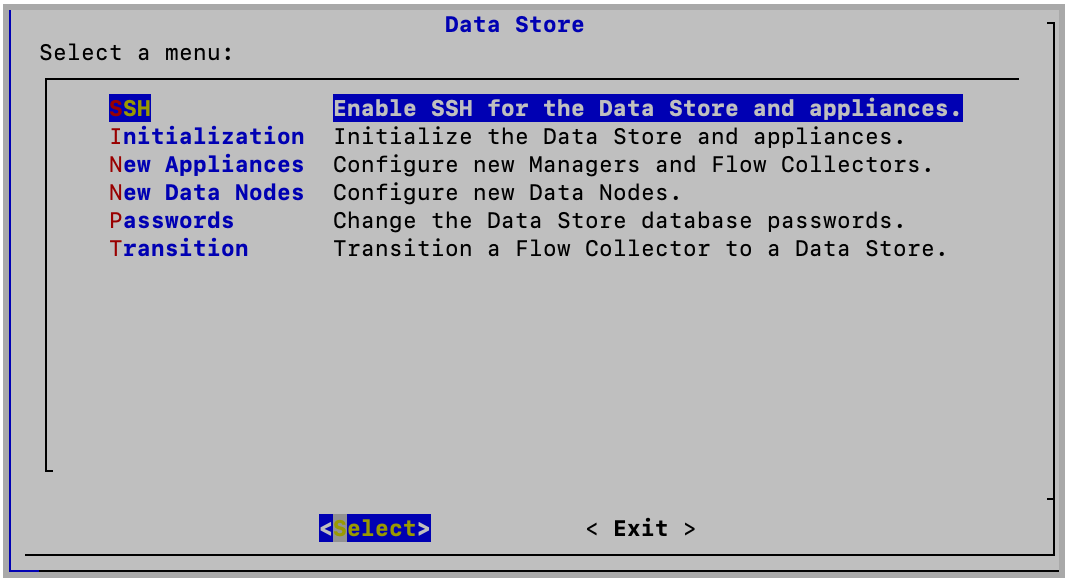
3. Flow Collector の移行

> 移行操作中に Flow Collector が再起動します。再起動が完了すると、Flow Collector は、Flow Collector のローカル Vertica データベースではなく、Data Store データベースに新しいデータを保存しはじめます。

1. Manager アプライアンスコンソール（SystemConfig）に root としてログインします。



2. [Data Store] > [SSH] を選択します。これで SSH が有効になります。



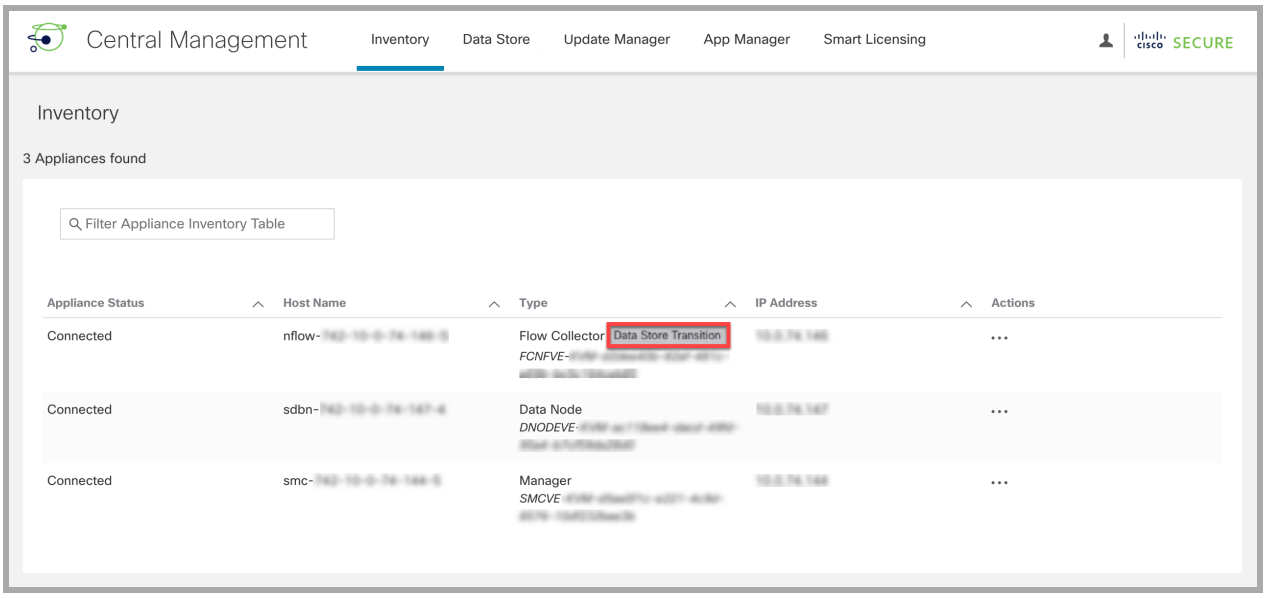
> [Data Store] メニューが表示されない場合は、Data Store ドメインがあることを確認してください。詳細については、「1. Data Store ドメインの確認」を参照してください。

3. [Data Store] メニューから、[移行(Transition)] > [移行の開始(Initiate Transition)] を選択します。
4. 移行する Flow Collector を選択します。
5. [Data Storeドメイン(Data Store Domains)] 画面で、「1. Data Store ドメインの確認」で特定(または作成)した Data Store ドメインを選択します。移行した Data Store Flow Collector のデータは、Data Store データベースにルーティングされ、以前の非 Data Store ドメインではなく、この新しいドメインを介してアクセスできるようになります。
6. 画面の指示に従って、移行を確認します。

> ⚠ 移行開始手順を完了したら、Flow Collector にローカル保存されている履歴データが不要であることを確認するまで、Flow Collector の移行を完了しないでください。完了すると、そのプロセス中に履歴データが削除されます。詳細については、「**Data Store Flow Collector の移行の完了**」を参照してください。

7. Central Management のインベントリを確認します（[構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）]）。

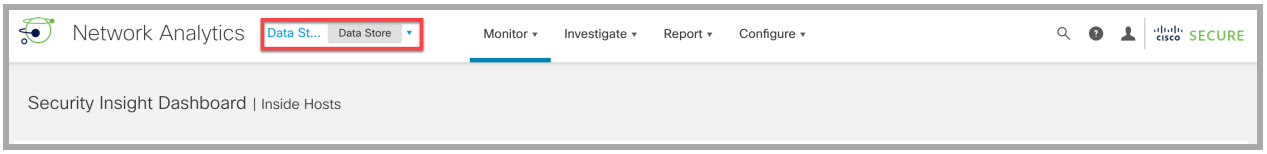
   移行した Flow Collector に [Data Storeの移行（Data Store Transition）] タグが表示されていることを確認してください。



4. 通信の確認

Data Store がフローを受信していることを確認します。

1. [セキュリティ分析（Security Insight）] ダッシュボードに戻ります。
2. 画面上部の [ドメイン（Domains）] メニューから Data Store ドメインが選択されていることを確認します。



3. [レポート（Report）] メニューを選択します。
4. [レポートビルダー（Report Builder）] を選択します。
5. [新しいレポートの作成（Create New Report）] をクリックします。
6. [フローデータベース取り込みトレンドレポート（Flow Database Ingest Trend Report）] テンプレートをクリックします。
7. 必要に応じてパラメータを選択します。[実行（Run）] をクリックします。

8. レポートを調べて、データベースまたは Data Store がフローを受信していることを確認します。

フローデータベース取り込みトレンドレポートの実行に加えて、次の手順を実行して、Data Store がフローを受信していることを確認することもできます。

- **Flow Collector トレンドテーブル**:[セキュリティ分析ダッシュボード(Security Insight Dashboard)] に移動して、[Flow Collectorトレンド(Flow Collector Trend)] テーブルを確認します。Data Store がフローを受信している場合は、それらがここに表示されます。
- **データベースの保持**:Central Management を開き([構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)])、[Data Store] > [データベースの保持(Database Retention)] タブの情報を確認します。このページの [Data Store 内の最も古いデータ(Oldest Data in Data Store)] テーブルは、最も古いレコードが Data Store に書き込まれてからの日付と日数を追跡するために役立ちます。このテーブルのデータは 1 日に 1 回しか更新されないため、移行日にはこのテーブルにデータが表示されないことに注意してください。詳細については、このガイドの「**[データベース保持(Database Retention)] の表示**」セクションを参照してください。

フロー検索の実行

ドメインごとにフロークエリを実行するには、[調査(Investigate)] > [フロー検索(Flow Search)] を選択します。カスタムの日付範囲を使用して、結果をカスタマイズします。

- **移行前のクエリ**:非 Data Store ドメインの移行前の履歴データをクエリするには、Flow Collector 移行日より前の終了日を選択してください。
- **移行後のクエリ**:移行後のすべての Data Store データをクエリするには、Flow Collector 移行日以降に開始される開始日を選択してください。

移行中の Flow Collector の Central Manager インベントリからの削除

> ⚠ 移行中の Flow Collector を Central Manager インベントリから削除しないでください。削除すると、シスコサポートの支援を受けて移行プロセスを完了することが必要になります。

移行中の Flow Collector の動作

移行中の Flow Collector では、次のような動作が発生します。

- **新しいデータ**:「**Flow Collector の Data Store への移行の開始**」の手順を完了すると、移行中の Flow Collector は、すべての新しいテレメトリを Data Node の Data Store データベースに送信します。新しいデータは、「**1. Data Store ドメインの確認**」で特定(または作成)した Data Store ドメインにおいてアクセスできるようになり、移行前のローカルデータは引き続き非 Data Store ドメインに存在します。
- **移行前のデータ**:Flow Collector は、そのデータへのアクセスを維持したいだけ、移行前のデータをローカルに保存しつづけることができます。不要になった移行前のデータを削除する方法については、「**Data Store Flow Collector の移行の完了**」を参照してください。
- **システムパフォーマンス**:Flow Collector 移行中のシステムパフォーマンスは、移行前のパフォーマンスと同様です。移行が完了すると、Data Store Flow Collector に合わせてパフォーマンスが向上します。

Data Store ドメインと非 Data Store ドメインの同期

Flow Collector の移行中、移行前の非 Data Store ドメインと Data Store ドメインの間で設定と調整の同期を維持したい場合があります。ここでは、非 Data Store ドメインを、関連する Data Store ドメインと同期するプロセスについて説明します。

> この手順には管理者アクセスが必要です。

同期されるプロパティ

次のプロパティはドメイン間で同期されます。

- Data Store ドメイン固有の設定とアラート設定（有効な場合）。ドメイン設定には、次のものが含まれます。
  - ホストグループ管理
  - アラーム重大度
  - ポリシー管理
  - サービス、アプリケーション
  - エクスポータ SNMP プロファイル（パスワードを除く）
  - ドメイン AS 番号

推奨同期頻度

ドメインは何度でも同期できますが、同期は、一連の変更を実行した後か 1 日または 1 週間に 1 回のみに制限することをお勧めします。これは、同期プロセスでリソースが使用され、日常的な処理の能力が奪われるためです。

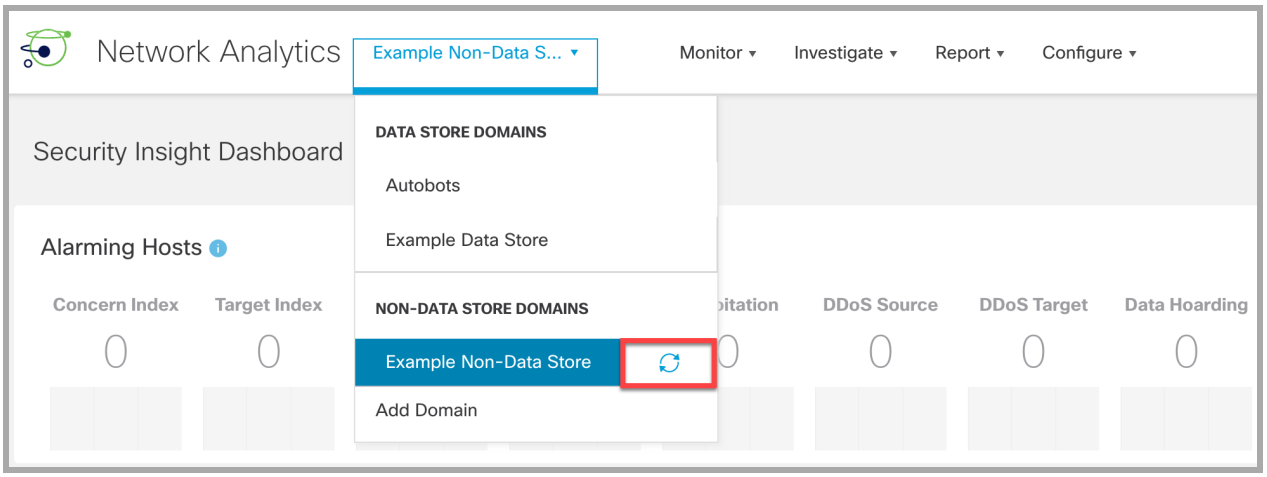
ドメイン同期化の手順

以下の手順に従って、非 Data Store ドメイン（ソース）と Data Store ドメイン（対象）を同期します。

1. メニューバーから、Data Store ドメインと同期する非 Data Store ドメインを選択します。
2. メインメニューから、[設定（Configure）] > [システムドメインのプロパティ（SYSTEM Domain Properties）] を選択します。
3. [編集（Edit）] ボタンを選択します。
4. [同期する対象ドメイン（Target Domain to Synchronize）] ドロップダウンメニューで、このドメインを同期する Data Store ドメインを選択します。

> 対象の Data Store ドメインは、1 つのソースの非 Data Store ドメインとのみ同期できます。対象の Data Store ドメインを複数のソースの非 Data Store ドメインと同期しようとすると、エラーが表示されます。

5. [Save] ボタンをクリックして変更を保存します。Data Store ドメインとの同期を選択した非 Data Store ドメインの横に、同期ボタンが表示されます。



Flow Collector の移行の完了

移行前のデータが不要になったら、「**Data Store Flow Collector の移行の完了**」の手順に従って Flow Collector の移行を完了できます。

> ⚠ Flow Collector にローカル保存されている履歴データが不要であることを確認するまで、Flow Collector の移行を完了しないでください。完了すると、そのプロセス中に履歴データが削除されます。

Data Store Flow Collector の移行の完了

非 Data Store Flow Collector を Data Store Flow Collector に移行するプロセスを実行し、ローカルに保存された非 Data Store データを保持する必要がなくなった場合は、Data Store Flow Collector の移行を完了することができます。

非 Data Store Flow Collector を Data Store Flow Collector に移行するには、主に次の 2 つの手順を実行します。

1. 「**Flow Collector の Data Store への移行の開始**」の手順に従って、移行プロセスを開始します。これにより、Flow Collector は、「**移行中の Flow Collector の動作**」で説明されている Data Store 移行状態に移行します。
2. 移行プロセスを完了します。これにより、Flow Collector は Data Store Flow Collector のみになります。この Flow Collector が保存している既存の非 Data Store データはすべて削除され、リソースが回復されるため、Flow Collector のパフォーマンスが向上します。

要件

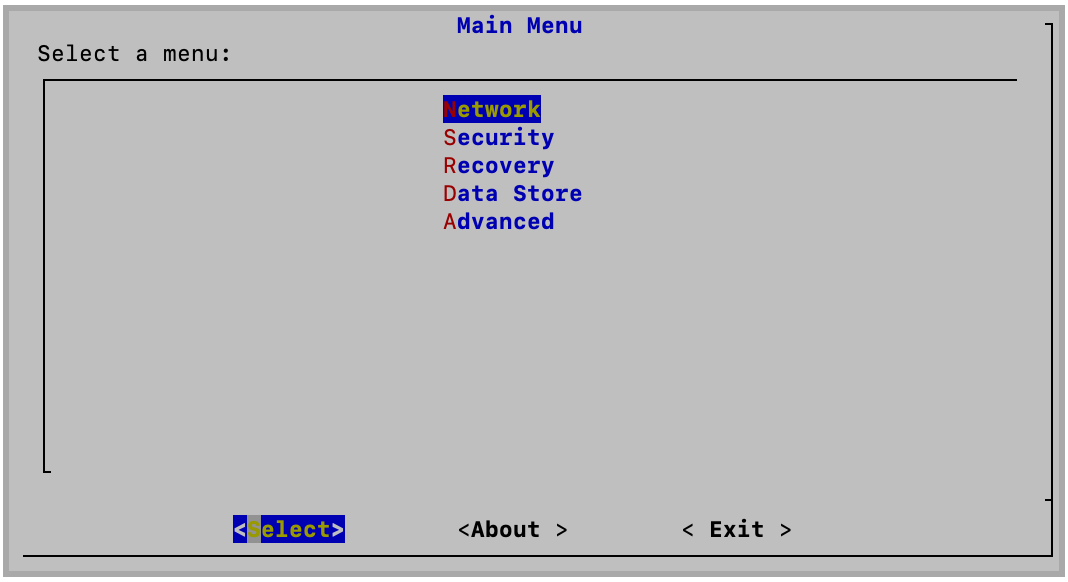
Data Store Flow Collector の移行を完了する前に、次のことを確認してください。

- **移行の開始**:「**Flow Collector の Data Store への移行の開始**」の手順を完了したことを確認します。
- **履歴データ**:このプロセス中に履歴データが削除されるため、Flow Collector にローカルに保存されている履歴データが不要であることを確認します。非 Data Store データのデータ保持ポリシーがあり、Data Store の移行を完了する前に Data Store 内に新しいデータがどれだけあるのかを把握したい場合は、[Data Store内の最も古いデータ(Oldest Data in Data Store)] テーブルを確認してください。詳細については、「**[データベース保持(Database Retention)] の表示**」を参照してください。

Flow Collector の Data Store への移行の完了

Data Store Flow Collector の移行を完了するには、次の手順に従います。

1. Manager アプライアンスコンソール(SystemConfig)に root としてログインします。



2. [Data Store] > [移行(Transition)] > [移行の完了(Complete Transition)] を選択します。
3. Data Store への移行を完了する Flow Collector を選択します。
4. 画面の指示に従って、移行を完了します。
5. Central Management のインベントリを確認します([構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)])。

   移行した Flow Collector に [Data Store] タグが表示されていることを確認してください。

完了後の注意事項

「Flow Collector の Data Store への移行の完了」の手順が完了したら、次の点に注意してください。

- 非 Data Store ドメインでは、この Flow Collector に関してフロークエリに NetFlow レコードが表示されなくなります。
- 古い非 Data Store ドメインに Flow Collector がない場合は、そのドメインを削除できます。詳細については、「ドメインの削除」を参照してください。
- この Flow Collector が保存していた既存の非 Data Store データがすべて削除され、リソースが回復されたため、Flow Collector のパフォーマンスが向上します。
- 移行された Flow Collector では、ディスク容量の使用率が大幅に削減されます。システムの統計情報、サービス、ディスク使用率、および Docker サービスを確認するには、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。

1. Central Management の [インベントリ(Inventory)] ページで、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。
2. [アプライアンス統計情報の表示(View Appliance Statistics)] を選択します。
3. [ホーム(Home)] を選択して統計を確認します。

非 Data Store 展開への Data Store の追加

これらの手順を進める前に、非 Data Store ドメインを含む Secure Network Analytics がすでにインストールされていることを確認してください。手順については、「**システム設定のプランニング**」を参照してください。

非 Data Store 展開をインストールして設定したら、該当する手順に従って非 Data Store 展開に Data Store を追加します。

- **次による Data Store の追加：既存の Flow Collector**
- **次による Data Store の追加：新しい Flow Collector**

> Data Store の互換性情報については、『Secure Network Analytics ハードウェアおよびソフトウェアバージョンのサポートマトリックス』を参照してください。

次による Data Store の追加：既存の Flow Collector

次の手順は、既存の Flow Collector を再利用するシナリオです。

1. アプライアンスを v7.4.2 以降に更新します。『Cisco Secure Network Analytics 更新ガイド』の手順に従います。
2. Secure Network Analytics に Data Store ドメインを追加します。詳細については、このガイドの「Data Store ドメインの作成」セクションを参照してください。
3. Central Manager から Flow Collector を削除します。Flow Collector 52xx を使用している場合は、Central Manager から Flow Collector データベースを削除する必要もあります。詳細については、「Central Management からのアプライアンスの削除」を参照してください。
4. Flow Collector エンジンおよびデータベースで、「工場出荷時のデフォルトへのリセット」に記載されているプロセスを実行します。
5. Flow Collector での初回セットアップを実行し、必ず [Data Store] を選択します。
6. Central Manager に Flow Collector を再度追加します。Flow Collector 52xx を使用している場合は、Central Manager に Flow Collector データベースと Flow Collector エンジンを（この順序で）再度追加します。
7. 手順に従って初回セットアップで各データノードを設定し、アプライアンス設定ツールを使用してそれらを Central Management に追加します。
8. Data Store にアプライアンスを追加します。詳細については、「Data Store 初期化後の Manager または Flow Collector の追加」を参照してください。

次による Data Store の追加：新しい Flow Collector

1. アプライアンスを v7.4.2 に更新します。『Cisco Secure Network Analytics 更新ガイド』の手順に従います。
2. Secure Network Analytics に Data Store ドメインを追加します。詳細については、このガイドの「Data Store ドメインの作成」セクションを参照してください。
3. ハードウェアまたは仮想 Flow Collector と Data Node を展開してインストールします。詳細については、『x2xx シリーズ ハードウェア アプライアンス設置ガイド』、『Secure Network Analytics x3xx シリーズ ハードウェア アプライアンス設置ガイド』、または『Virtual Edition アプ

ライアンス設置ガイド』を参照してください。

4. Flow Collector での初回セットアップを実行し、必ず [Data Store] を選択します。
5. Central Manager に Flow Collector を追加します。Flow Collector 52xx を使用している場合は、Central Manager に Flow Collector データベースと Flow Collector エンジンを（この順序で）再度追加します。この手順では、まったく新しい Flow Collector を使用して Data Store を追加していると想定しています。
6. 手順に従って初回セットアップで各データノードを設定し、アプライアンス設定ツールを使用してそれらを Central Management に追加します。
7. Data Store にアプライアンスを追加します。詳細については、「Data Store 初期化後の Manager または Flow Collector の追加」を参照してください。

トラブルシューティング

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、カスタマーサポートにお問い合わせください。

アプライアンスステータス：構成チャネルのダウン（Config Channel Down）

［インベントリ（Inventory）］ページで、アプライアンスステータスとして［構成チャネルのダウン（Config Channel Down）］が表示されている場合は、次を確認します。

- **通信の設定**：ネットワーク通信の設定を確認します。
- **信頼ストア**：アプライアンス アイデンティティ証明書が正しい信頼ストアに保存されていることを確認します。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。
- **証明書**：アプライアンス アイデンティティ証明書を変更した場合は、その手順を確認し、証明書が正しい信頼ストアに保存されていることを確認します。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。
- **アプライアンスの削除**：構成チャネルのダウン中にアプライアンスを削除する場合は、システム設定からもアプライアンスを削除してください。
    - アプライアンスコンソールに sysadmin としてログインします。
    - **SystemConfig** と入力します。Enter を押します。
    - ［リカバリ（Recovery）］>［アプライアンスの削除（RemoveAppliance）］を選択します。

アプライアンスステータス：データストアが初期化されていません（Data Store Not Initialized）

Secure Network Analytics のシステム設定を完了する必要があります。

すべての Manager、Flow Collector、および Data Node を Central Management のインベントリに追加してから Data Store を初期化する必要があります。手順については、「**6. Data Store の初期化**」を参照してください。

アプライアンスステータス：データストアが設定されていません（Data Store Not Configured）

Data Store に新しい Manager、Flow Collector、または Data Node を追加した場合は、システム設定を完了する必要があります。手順については、「**Data Store のメンテナンス**」を参照してください。

アプライアンス管理インターフェイスを開く

アプライアンス管理インターフェイスには、Central Management を通じて、またはアプライアンスに直接ログインすることでアクセスできます。

トラブルシューティングのために Central Manager から Manager を削除した場合は、アプライアンス管理にログインする必要があります。

1. ブラウザのアドレスバーに、次のようにアプライアンスの IP アドレスを入力します。

   https://<IPAddress>

   - **Manager**：IP アドレスの後に **/Manager/Index.html** を追加します。
   - **例**：https://xx.xxx.xx.xxx/Manager/index.html

アプライアンス アイデンティティの交換

Secure Network Analytics バージョン 7.x アプライアンスはそれぞれ、固有の自己署名アプライアンス アイデンティティ証明書と一緒にインストールされます。アプライアンス アイデンティティ証明書を認証局からの証明書に置き換える場合の手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

> ⚠ 証明書はシステムのセキュリティにとって重要です。証明書を不適切に変更すると、Secure Network Analytics アプライアンスの通信が停止し、データ損失の原因となります。

Central Manager からの Data Store アプライアンスの削除

Central Manager から Data Store アプライアンス（Manager、Flow Collector、Data Node）を削除しても、Data Store 自体からは削除されません。Data Store 自体から削除するには、手動でのクリーンアップが必要です。

- **Manager と Flow Collector**：Manager と Flow Collector については、**/lancope/var/services/data-store/config-datastore-inventory-snapshot** ディレクトリから削除できます。
- **Data Node**：Data Node の削除はプロセスがより複雑であるため、シスコサポートに連絡してサポートを依頼してください。

ホスト名、ネットワークドメイン名、または IP アドレスの変更

アプライアンスの設置および設定後に、アプライアンスのホスト名、ネットワークドメイン名、または IP アドレスを変更するには、『SSL/TLS Certificates for Managed Appliances Guide』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。

[ドメインのプロパティ(Domain Properties)] を開く

メインメニューから、[設定(Configure)] > [システムドメインのプロパティ(SYSTEM Domain Properties)] を選択します。

詳細については、「**ドメイン**」を参照してください。

デスクトップ クライアントドメインの削除

> 削除するドメインについて収集されたすべてのデータにアクセスできなくなるため、削除するデスクトップ クライアントドメインを決定するときは注意が必要です。
> **回避策**:デスクトップクライアントのドメインを誤ってすべて削除してしまい、Manager Web アプリケーションからロックアウトされた場合は、デスクトップクライアントで新しい非 Data Store ドメインを作成します。これにより、Manager Web アプリケーションへのアクセスを回復できます。ドメインの作成については、デスクトップ クライアント ヘルプの「ドメインの追加」トピックを参照してください。

アプライアンス設定ツールを開く

アプライアンスの設定後にアプライアンス設定ツールを開くには、次の手順を使用します。

> アプライアンス設定ツールを使用してホスト名、ネットワークドメイン名、または IP アドレスを変更する場合、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。

1. アプライアンスのブラウザ アドレス バーで、IP アドレスの後ろの URL の終わりを /lc-ast に置き換えます。

   https://<IPaddress>/lc-ast

2. Enter を押します。
3. 詳細については、「**1. 初回セットアップを使用した環境の設定**」を参照してください。

システム設定の概要

新しいメニュー構造でシステム設定が更新されました。多くの場合、システム設定にはトラブルシューティングを伴います。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。

- [ユーザー(Users)]:使用可能なメニューは、ログイン ID(root、sysadmin、または admin)によって決まります。
- SSH:メニューにアクセスするには、SSH を有効にする必要があります。

1. アプライアンスコンソールにログインします。
2. **SystemConfig** と入力します。Enter を押します。
3. メインメニューから次のメニューを選択します。

- **ネットワーク**:アプライアンス管理ポートネットワーク、信頼できるホスト、およびネットワーク インターフェイス(eth0 の設定、MTU など)を変更するには、[ネットワーク(Network)] を選択します。
- **セキュリティ**:パスワードの変更またはリセット(「**パスワード**」を参照)、syslog コンプライアンスの管理を実行するには、[セキュリティ(Security)] を選択します。
- **リカバリ**:Central Management からのアプライアンスの削除、工場出荷時のデフォルトへのリセット、診断パックの作成、またはイメージの更新を実行するには、[リカバリ(Recovery)] を選択します。
- **詳細**:ルートシェルのオープン、管理ユーザーアカウントの管理、シングルサインオンの設定、リブート、またはシャットダウンを実行するには、[詳細(Advanced)] を選択します。
- **Data Store**:このメニューは、Data Store を使用するように設定した Manager で使用できます。このメニューは、SSH の有効化、初期化、Data Store への新しい Manager と Flow Collector の追加、Data Store への Data Node の追加、Data Store データベースのパスワードの変更、および Flow Collector の Data Store への移行で使用します。

信頼できるホストの変更

システム設定を使用すると、信頼できるホストのリストをアプライアンスのデフォルトから変更できます。ただし、信頼できるホストを変更する前に、シスコサポートにお問い合わせください。

> ⚠ 信頼できるホストを変更する前に、シスコサポートにお問い合わせください。

信頼できるホストのリストをデフォルトから変更する場合、各 Secure Network Analytics アプライアンスが展開内の他のすべての Secure Network Analytics アプライアンスの信頼できるホストのリストに含まれていることを確認してください。そうしない場合、アプライアンス間で通信できません。

1. アプライアンスコンソールに sysadmin としてログインします。
2. [ネットワーク(Network)] > [信頼できるホスト(Trusted Hosts)] を選択します。
3. 画面に表示される指示に従って、[信頼できるホスト(Trusted Hosts)] を変更します。

最大伝送単位(MTU)の設定

アプライアンス eth0 ネットワーク インターフェイスの最大伝送単位(MTU)を設定するには、次の手順を使用します。数値により、eth0 インターフェイスがトランザクションごとに送信できる最大パケッ

トサイズを設定します。

> ⚠ MTU はネットワーク処理に影響します。この番号を変更する場合は、ネットワーク内で一貫して構成されていることを確認してください。

1. アプライアンスコンソールに sysadmin としてログインします。
2. [ネットワーク(Network)] > [インターフェイス(Interface)] を選択します。
3. [eth0] を選択します。
4. **1500**(デフォルト)、**9000**、またはネットワーク構成要件を満たす数値を入力します。

> ℹ ファイアウォールログでは 8,192 バイト、NetFlow、sFlow、および NVM フローでは 9,216 バイトの最大 MTU 設定をサポートしています。セキュリティを使用してファイアウォールログを取り込んでいる場合、セキュリティ分析とロギング(オンプレミス) および別のテレメトリタイプでは、8,192 バイトを超える MTU 設定を指定しないでください。

5. [確認(Confirm)] を選択します。
6. 画面に表示される指示に従って、変更を確認します。

診断パックの作成

診断パックがあると、Cisco サポートによる問題のトラブルシューティングが必要な場合に役立ちます。個々のアプライアンスの診断パックを作成するには、次の手順を使用します。

1. アプライアンスコンソールに root としてログインします。
2. [リカバリ(Recovery)] を選択します。
3. [診断パック(Diagnostics Pack)] を選択します。
4. 診断パックをカスタマイズするには、メニューを選択して [編集(Edit)] をクリックします。

メニュー	説明
ファイル名のプレフィックス	診断パックのファイル名にプレフィックスを追加します(最大 127 文字)。
パスワード(Password)	診断パックのファイルパスワードを作成します。ファイルパスワードを作成しない場合、診断パックはデフォルトの方法(Cisco キー)で暗号化されます。
構成のバックアップ	このオプションを選択し、画面の指示に従って診断パックに構成のバックアップを含めます。バックアップの詳細については、ヘルプの「Backup Configuration Files」を参照してください。
モジュール	含める特定のモジュールを選択して、診断パックの内容を編集します。

5. [**終了**(Finish)] をクリックします。画面の指示に従って、診断パックを作成します。

工場出荷時のデフォルトへのリセット

アプライアンスを工場出荷時のデフォルト(RFD)にリセットするには、次の手順を使用します。データを完全に消去するには、工場出荷時のデフォルトを 2 回リセットしてください。

- RFD を 2 回:データを完全に消去するには、工場出荷時のデフォルトを 2 回リセットしてください。
- 設定のバックアップ:アプライアンスの設定を復元する場合は、バックアップ設定とデータベースのバックアップファイルを保存してください。詳細については、ヘルプの「**Backup Configuration Files**」(Central Management)および「**Backup/Restore Database (Appliance Admin interface)**」の各トピックを参照してください。RFD 後にバックアップを復元するには、シスコサポートにお問い合わせください。

> ⚠ アプライアンスを工場出荷時のデフォルト設定にリセット(RFD)すると、すべての既存データと設定情報が削除され、バックアップを作成した場合にのみ復元できます。

> ⚠ アプライアンスを工場出荷時のデフォルトにリセットすると、Central Management を使用して設定を復元できません。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. アプライアンスコンソールに sysadmin としてログインします。
2. [リカバリ(Recovery)] > [工場出荷時のデフォルト(Factory Defaults)] を選択します。
3. 画面に表示される指示に従って工場出荷時のデフォルトにリセットし、アプライアンスを再起動します。

> ⚠ データを完全に消去するには、各アプライアンスで RFD を2 回 実行してください。

4. アプライアンスコンソールに **sysadmin** としてログインし、画面に表示される指示に従ってアプライアンスの IP アドレス、ホスト名、およびドメインを設定します。手順については、このガイドの「初回セットアップを使用した環境の設定」セクションを参照してください。この手順は、RFD 時にネットワーク設定を保持している場合でも必要です。
5. アプライアンス設定ツールにログインし、Central Management にアプライアンスを追加します。詳細については、「**Central Management(アプライアンスの管理)**」を参照してください。

管理者ユーザーの有効化/無効化

デフォルトの管理者アカウントを有効または無効にするには、次の手順を使用します。

1. アプライアンスコンソールに sysadmin としてログインします。
2. [詳細設定(Advanced)] を選択します。
3. [Adminユーザー(Admin User)] を選択します。
4. 画面に表示される指示に従い、管理者ユーザー アカウントを有効または無効にします。
5. 上記の手順を繰り返して、Secure Network Analytics クラスタ内のすべてのアプライアンスで管理ユーザーアカウントを有効または無効にします。

Data Store の導入のトラブルシューティング

ハードウェアの導入のトラブルシューティング

アプライアンスの展開または設定に関する問題の詳細については、『x2xx シリーズ ハードウェア アプライアンス設置ガイド』または『Secure Network Analytics x3xx シリーズ ハードウェア アプライアンス設置ガイド』を参照してください。

仮想アプライアンスの展開のトラブルシューティング

Virtual Edition アプライアンスの展開または設定に関する問題の詳細については、『Virtual Edition アプライアンス設置ガイド』を参照してください。

初回セットアップと Data Node Virtual Edition

インストール中に 2 つのネットワークアダプタを Data Node Virtual Edition に割り当てないと、2 番目のネットワークアダプタを検出できないため、初回セットアップで解決に失敗します。これにより、Data Node 間通信にルーティング不可能な IP アドレスを割り当てることができなくなります。詳細については、『Virtual Edition アプライアンス設置ガイド』を参照してください。

Data Store のトラブルシューティング

Data Store の管理用に Data Store で予約されるストレージ容量は、最大で使用可能なストレージ容量の 40% です。最大で合計容量の 60% をテレメトリの保存に使用できます。

Data Node の電源が失われてリブートした後に Vertica Analytics Platform が自動的に再起動しない

Data Node の電源が予期せずに失われ、アプライアンスをリブートした場合、データが破損する可能性があり、その Data Node の Vertica Analytics Platform（Vertica）インスタンスが自動的に再起動しないことがあります。Data Store の実行を継続できる十分な数のデータノードがまだ実行されていれば、Data Store は Flow Collector からデータの取り込みを続けます。ただし、できるだけ速やかにデータノードを再起動することで、Data Store に再度参加させ、欠落したデータを隣接するデータノードから取得し、残りのデータノードと同じ状態にする必要があります。

Data Node を再起動するには、次の各方法を試してください。

- [Central Management] > [Data Store] タブで Data Node を起動します。詳細については、「**データノードの起動**」を参照してください。
- [Data Store] タブから Data Node が起動しない場合は、Data Node にログインして手動で Vertica を再起動します。これにより、破損したデータが削除され、Vertica が適切に再起動されます。

Data Node ハードウェア アプライアンスに関しては、再起動する前に Data Node の電源復元ポリシーの更新が必要になる場合があります。電源復元ポリシーが [電源オフ（Power Off）] に設定されている場合は、電源喪失後に Data Node を手動で再起動する必要があります。CIMC での電源復元ポリシーの設定の詳細については、『UCS C-Series GUI Configuration Guide』を参照してください。

1. Data Node アプライアンスコンソールに root としてログインします。
2. 次のコマンドをコピーし、テキストエディタに貼り付けます。

```
tail /lancope/var/database/dbs/sw/v_sw_[node_name]_
catalog/ErrorReport.txt
```

3. *[node_name]* をデータノードの名前（`node0001` など）に置き換えます。
4. 更新したコマンドをコピーしてコマンド ライン インターフェイスに貼り付け、Enter を押して `ErrorReport.txt` エラーファイルの最新のエントリを確認します。データ整合性やデータ破損の問題の可能性がエラーメッセージに示されている場合は、次の手順に進んで Vertica を強制的に再起動します。
5. 次のコマンドをコピーし、テキストエディタに貼り付けます。

```
admintools -t restart_node --hosts=[data-node-ip-address] --
database='sw-datastore' --password="[dbadmin-password]" --force
```

6. *[data-node-ip-address]* を該当する Data Node の IP アドレスに置き換えます。必ず **[Data Store] タブ**に表示されているプライベート IP アドレスを使用します。eth0 管理 IP アドレスは使用しないでください。
7. *[dbadmin-password]* を Data Store の `dbadmin` のパスワードに置き換えます。
8. 更新したコマンドをコピーし、CLI に貼り付けて Enter を押して、該当する Data Node で Vertica を強制的に再起動します。破損したデータが削除され、そのデータが隣接する Data Node から復元されます。
9. 「`Do you want to continue waiting? (yes/no) [yes]`」というプロンプトが表示される場合は、`yes` と入力して Enter を押し、待機を続けます。

   Vertica は該当する Data Node の情報を隣接する Data Node から復元するため、問題の Data Node が停止している間にそれらの Data Node が大量のフロートラフィックを取り込んでいた場合、問題の Data Node が回復するまでに時間がかかることがあります。
10. Data Node への電力供給に関するシスコの推奨事項を確認します。詳細については、『x2xx シリーズ ハードウェア アプライアンス設置ガイド』、『Secure Network Analytics x3xx シリーズ ハードウェア アプライアンス設置ガイド』、または『Virtual Edition アプライアンス設置ガイド』を参照してください。

Data Store が電源障害後に起動しない

[Central Management] の [Data Store] タブでデータベースのステータスを確認します。そこからデータベースまたは Data Node を起動できます。詳細については、「**Data Store データベースのステータスの表示**」を参照してください。

パッチのインストールとソフトウェアのアップデート

お使いのソフトウェアバージョンに対する最新のパッチをインストールすることで、Secure Network Analytics を最新の状態に保つようにしてください。詳細および手順については、Cisco Software Central にアクセスして確認してください。

ソフトウェアアップデートは、Cisco Software Central の Cisco スマートアカウントにも送信されます。正常に更新するには、『Secure Network Analytics 更新ガイド』の手順に従ってください。

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 2 月 27 日	最初のバージョン
1_1	2023 年 3 月 29 日	LACP ポートボンディング情報を追加しました。
1_2	2023 年 4 月 6 日	「Data Node の設定」セクションを更新して、ポートの順序付け手順が M5 世代の Data Node にのみ適用されることを示しました。

著作権情報