# Cisco Secure Network Analytics

Data Store 仮想エディション導入および構成ガイド 7.4.0

# 目次

# Data Store の設置と構成の概要

## 概要

このマニュアルでは、Cisco Secure Network Analytics データストア を使用した Cisco Secure Network Analytics（旧 Stealthwatch）のインストール方法について説明します。Secure Network Analytics のコンポーネントとそれらのシステム内での配置方法について、特に Data Store との関連で説明します。

この章は、次の項で構成されています。

- **対象読者**
- **展開オプション**
- **このガイドの使用方法**

## 対象読者

このガイドは、Secure Network Analytics システムの仮想アプライアンスの設置を担当する方を対象にしています。仮想アプライアンス、特に Cisco Secure Network Analytics Flow Collector および Cisco Secure Network Analytics Manager（旧 Stealthwatch Management Console）の設置に関する一般的な知識があることを前提にしています。

Secure Network Analytics 製品の設定については、『Cisco Secure Network Analytics System Configuration Guide』を参照してください。

## 展開オプション

Data Store を使用した Secure Network Analytics に対し、排他的なハードウェア導入または仮想の導入に加えて、v7.4.0 では、ハードウェアと仮想の混合導入オプションも提供されます。v7.4.0 以降、Secure Network Analytics では DS6200 ハードウェア Data Store で、仮想 マネージャ と Flow Collector の組み合わせがサポートされるようになりました。

すべてのアプライアンス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、選択した展開のドキュメントを確認してください。開始する前に、すべての要件を理解することが重要です。

- **ハードウェアと Virtual Edition（VE）アプライアンスの組み合わせ**
- **Virtual Edition（VE）アプライアンスのみ**

## ハードウェアと Virtual Edition（VE）アプライアンスの組み合わせ

以下のガイドを使用して、マネージャ VE および Flow Collector VE を使用した Data Store 6200 の導入を行います。

| 手順 | ドキュメント | 説明 |
|---|---|---|
| 準備 | リリース ノート | 最新の Data Store リリースに関する最新情報（直前の情報を含む）を確認してください。 |
| 準備 | Data Store 6200 仕様シート | 物理的なレイアウトと機能を確認します。 |
| 1. | 『x2xx シリーズ ハードウェア（Data Store 付属）アプライアンス設置ガイド』 | 物理ハードウェアアプライアンス（ラック、ケーブルなど）をインストールします。 |
| 2. | 『Data Store 仮想エディション導入および構成ガイド』 | マネージャ VE を導入して構成します。**「Manager Configuration for Use with a Data Store」**セクションを参照してください。<br>• リソース要件、ISO の展開、および初回セットアップの詳細については、『Virtual Edition (with Data Store) Appliance Installation Guide』を参照してください。<br>• アプライアンス設定ツールの詳細については、『System Configuration Guide』を参照してください。 |
| 3. | 『x2xx シリーズ ハードウェア（Data Store 付属）アプライアンス設置ガイド』<br>および『Data Store Hardware Deployment and Configuration Guide』 | 各 Data Node を展開して構成します。<br>**「Data Node の設定」**セクションの指示に従って、Data Node 間通信ポート設定を構成してください。<br>展開の考慮事項と前提条件については、『Data Store Hardware Deployment and Configuration Guide』を参照してください。 |
| 4. | 『Data Store 仮想エディション導入および構成ガイド』 | Flow Collector VE を導入して構成します。**「Flow Collector Configuration for Use with a Data Store」**セクションを参照してください。<br>• リソース要件、ISO の展開、および初回セットアップの詳細については、『Virtual Edition (with Data Store) Appliance Installation Guide』を参照してください。<br>• アプライアンス設定ツールの詳細については、『System Configuration Guide』を参照してくださ |

| | | |
|---|---|---|
| | | い。 |
| 5. | 『Data Store 仮想エディション導入および構成ガイド』 | Data Store を初期化します。「**Data Store の初期化と設定**」セクションを参照します。<br>フローインターフェイス統計の保持と Data Store の圧縮を設定します。 |
| 6. | スマート ライセンシング ガイド | 評価期間（90 日間）が終了する前に、Secure Network Analytics 展開とアプライアンスのライセンスを取得します。 |

### Virtual Edition（VE）アプライアンスのみ

次のガイドを使用して、Data Store Virtual Edition とともに Secure Network Analytics Virtual Edition をデプロイします。

| 手順 | ドキュメント | 説明 |
|---|---|---|
| 準備 | リリース ノート | 最新の Data Store リリースに関する最新情報（直前の情報を含む）を確認してください。 |
| 1. | 『Data Store 仮想エディション導入および構成ガイド』<br>および『Virtual Edition (with Data Store) Appliance Installation Guide』 | 『Data Store Virtual Edition の導入および設定ガイド』に示されている順序でアプライアンスを導入および設定します（「**Data Store の設置**」セクションを参照）。<br>1. マネージャ VE<br>2. Data Node：Data Node 間の通信ポート設定を構成するための指示に従っていることを確認してください。<br>3. Flow Collector VE<br>4. Data Store を初期化します。<br>5. フローインターフェイス統計の保持と Data Store の圧縮を設定します。<br>リソース要件、ISO の展開、および初回セットアップの詳細については、『Virtual Edition (with Data Store) Appliance Installation Guide』を参照してください。<br>アプライアンス設定ツールの詳細については、『System Configuration Guide』を参照してください。 |
| 2. | スマート ライセンシング ガイド | 評価期間（90 日間）が終了する前に、Secure Network Analytics 展開とアプライアンスのライセンスを取得します。 |

## このガイドの使用方法

この概要の他に、このガイドは次の章に分かれています。

| 章 | 説明 |
| --- | --- |
| Data Store の概念とアーキテクチャ | Data Store データベースの基礎となる基本概念、および Data Store の導入に関連する基本アーキテクチャについて、マネージャ や Flow Collector と関連付けて説明します。 |
| Data Store の導入の前提条件と推奨事項 | Data Store と互換性がある Secure Network Analytics アプライアンスについて説明し、開く必要がある通信ポートなど、Data Store の導入に関する要件と推奨事項を示します。 |
| Secure Network Analytics と Data Store の導入の概要 | Data Store で使用する Secure Network Analytics アプライアンスの導入について、大まかな概要を示します。 |
| Data Store の設置 | Data Store で使用する Secure Network Analytics アプライアンスの展開から、Data Store データベースを初期化する設定手順まで、エンドツーエンドの概要を示します。 |
| フローインターフェイス統計の保持設定 | Data Store フローインターフェイス統計データの保持期間の設定に関する情報を提供します。 |
| Data Store のインストールの次のステップ | Data Store の展開と設定が完了した後の次のステップについて説明します。 |
| Data Store のメンテナンス | Data Store のメンテナンスタスクについて説明します。 |
| Data Store の導入のトラブルシューティング | Data Store の設置プロセスで発生する一般的な問題と推奨される解決策について説明します。 |

# Data Store の概念とアーキテクチャ

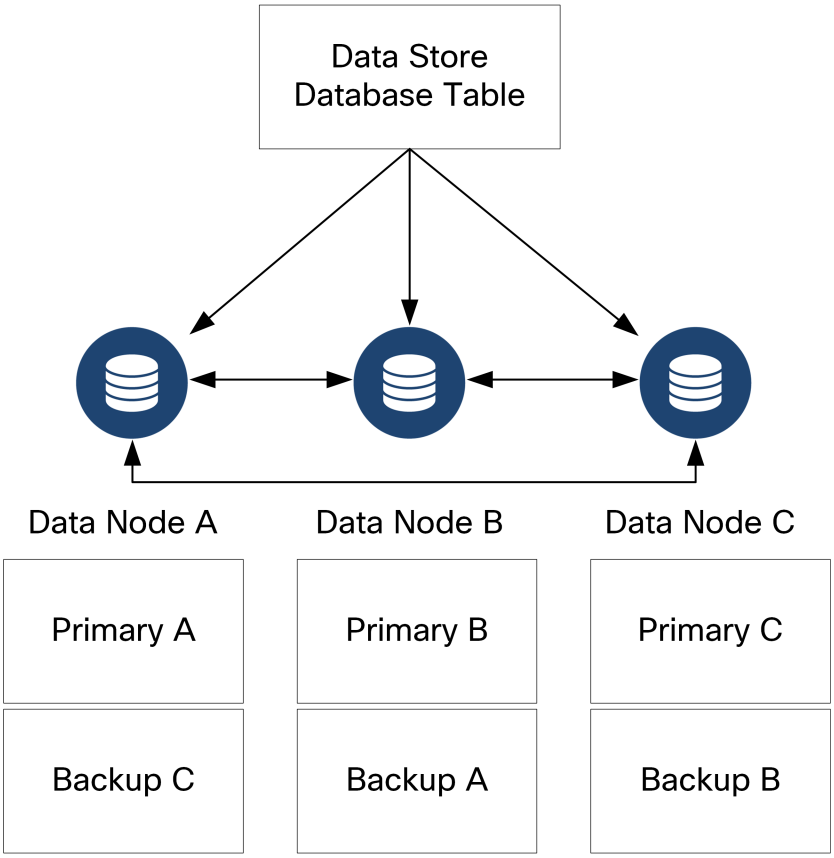
Data Store は、Flow Collector によって収集されたネットワークのテレメトリを保存する中央リポジトリを提供します。Data Store は、Data Store のクラスタで構成されます。各クラスタには、データの一部と個別データノードのデータのバックアップが含まれます。すべてのデータが 1 つの集中型データベースに存在し、複数の Flow Collector に分散されていないため、マネージャはすべての Flow Collector に個別にクエリする場合よりも Data Store から迅速にクエリ結果を取得できます。Data Store クラスタは、耐障害性の向上、クエリ応答の改善、グラフとチャート生成の迅速化を実現します。

### Data Store のストレージと耐障害性

Data Store では、Flow Collector からデータを収集し、クラスタ内の Data Node に均等に分散させます。それぞれの Data Node に、全体のテレメトリの一部が格納され、さらに別の Data Node のテレメトリについてのバックアップも格納されます。この方法でデータを格納することで、次のような利点があります。

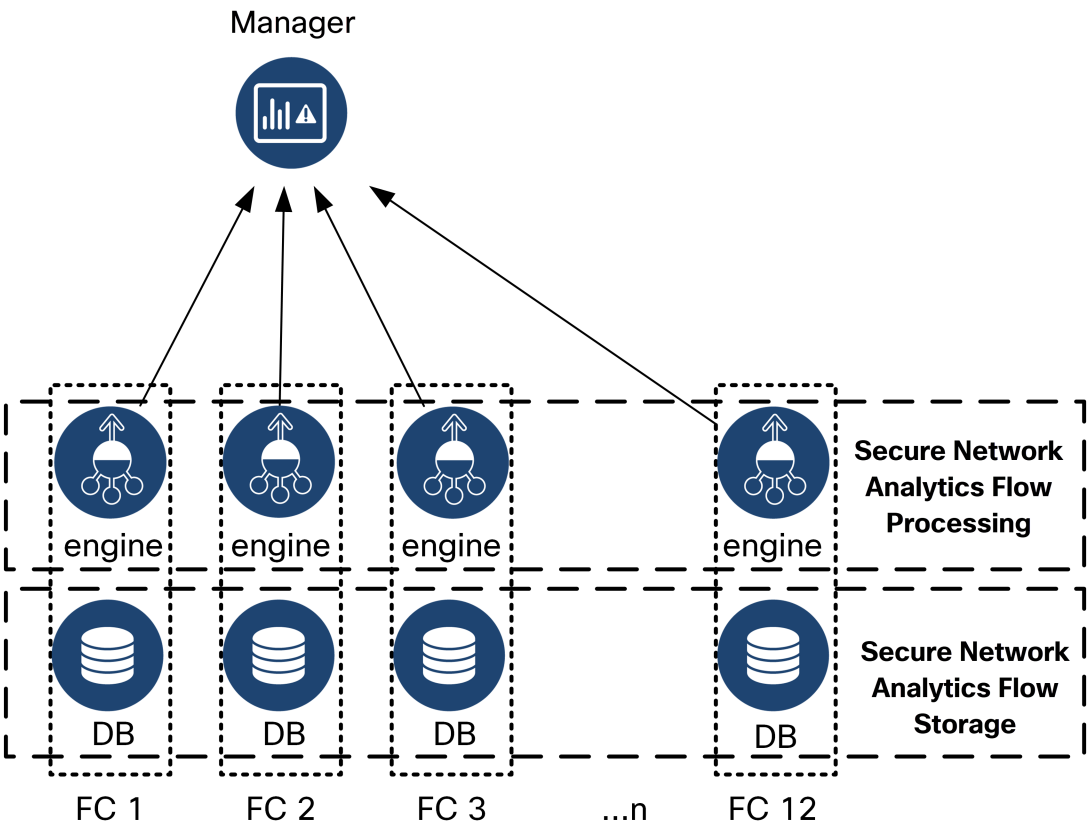
- ロードバランシングに役立ちます。
- 各ノードに処理が分散されます。
- Data Store に取り込まれたすべてのデータのバックアップが保持され、耐障害性が確保されます。
- Data Node の数を増やすことで、全体的なストレージとクエリのパフォーマンスを向上させることができます。

いずれかのノードが停止しても、そのバックアップを格納しているノードがまだ使用可能であり、Data Node の総数の少なくとも半分が稼働していれば、Data Store 全体は稼働状態を維持します。この間に、停止した接続や不具合のあるハードウェアを修復できます。問題がある Data Node を交換すると、そのノードのデータが Data Store の隣接する Data Node に格納されている既存のバックアップから復元され、その Data Node にデータのバックアップが作成されます。Data Node におけるテレメトリの格納方法の例については、次の図を参照してください。

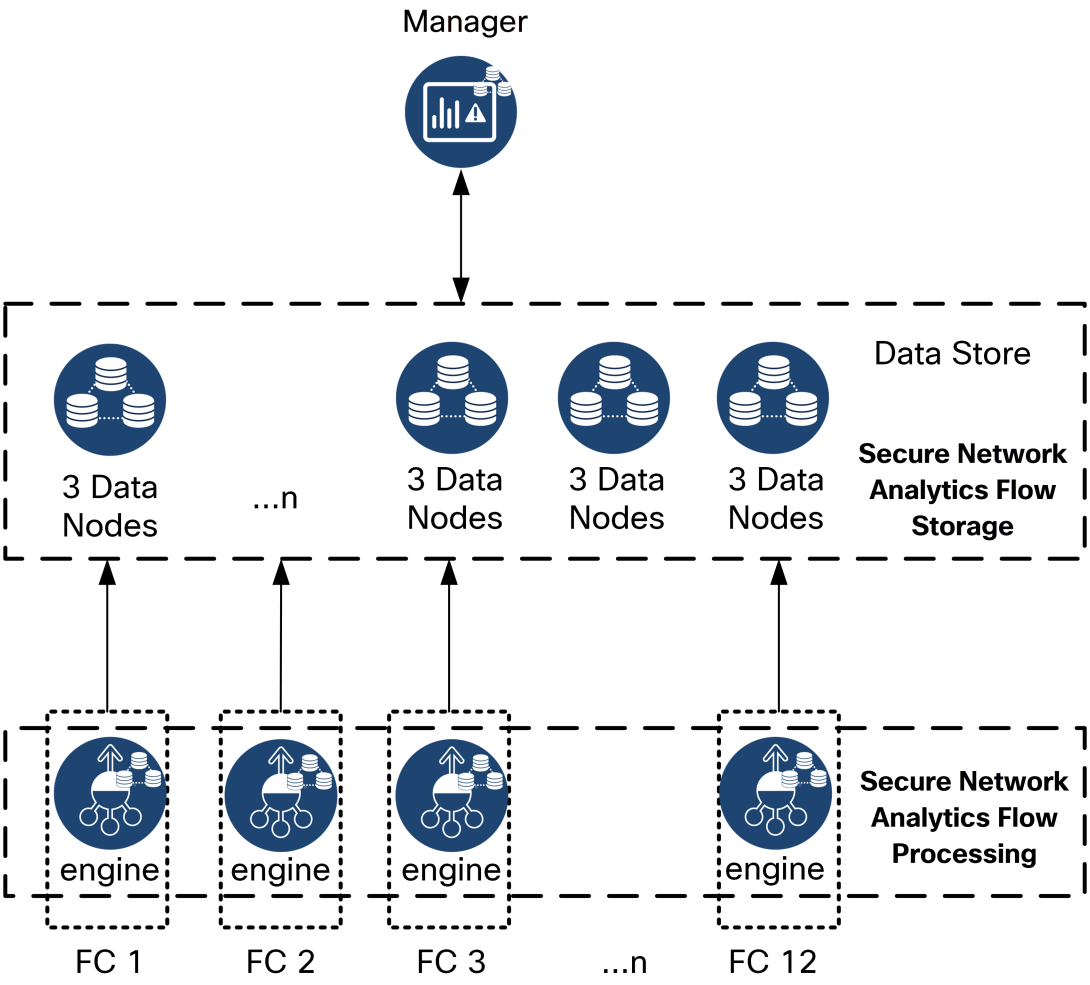


### Data Store の導入アーキテクチャ

Data Store なしの Secure Network Analytics の展開では、1 つ以上の Flow Collector がデータを取り込んで複製し、分析を実行し、データと結果を マネージャ に直接レポートします。グラフやチャートを含むユーザーが送信したクエリを解決するために、マネージャ は管理対象のすべての Flow Collector にクエリします。各 Flow Collector は、一致する結果を マネージャ に返します。マネージャ はさまざまな結果セットからの情報を照合し、結果を表示するグラフまたはチャートを生成します。この展開では、各 Flow Collector はローカルデータベースにデータを格納します。例として次の図を参照してください。



Data Store を使用した Secure Network Analytics の導入では、Data Store クラスタは マネージャ と Flow Collector の間に配置されます。1 つ以上の Data Store がフローを取り込み、重複排除し、分析を実行して、データと結果を Data Store に直接報告し、すべてのデータノードにほぼ均一に分散させます。Data Store は、データストレージを促進し、すべてのトラフィックを複数の Flow Collector に分散させずに一元化された場所に保持し、複数の Flow Collector よりも大きなストレージ容量を提供します。例として次の図を参照してください。




グラフやチャートを含むユーザーが送信したクエリを解決するために、マネージャ は Data Store にクエリします。Data Store は、クエリに関連する列で一致する結果を検索し、一致する行を取得してクエリ結果を マネージャ に返します。マネージャ は、複数の Flow Collector からの複数の結果セットの照合を必要とせずに、グラフまたはチャートを生成します。したがって、複数の Flow Collector にクエリする場合と比較して、クエリのコストが軽減され、クエリのパフォーマンスが向上します。

### Secure Network Analytics 導入の考慮事項

次の点に注意してください。

- Data Store で使用するように 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）で特定の機能が非表示になります。Flow Collector の設定やその他の関連タスクを実行するには、Central Management を使用します。ストレージの統計を監視するには、マネージャ（[ダッシュボード（Dashboard）] > レポートビルダー）でレポートビルダーを使用します。
- Data Store を展開する場合は、Secure Network Analytics 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。Secure Network Analytics 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。
- Data Store で使用するように マネージャ を設定した場合は、ETA 暗号化監査またはホスト分類子アプリケーションを使用できません。
- Data Store データベースアーキテクチャでは、マネージャ およびすべての Flow Collector は Data Store と通信する必要があり、展開時に Data Store と連携するように設定する必要があります。一部の Flow Collector を Data Store なしで動作するように設定し、他の Flow Collector を Data Store と連携するように設定することはできません。
- 仮想 Data Store は、3 つの仮想 Data Node、仮想 マネージャ、および仮想 Flow Collector とともに展開できます。

### Data Store アーキテクチャ

各 Data Store は、3 つ以上の Data Node で構成されます。

仮想 Data Store をダウンロードすると、3 つの Data Node Virtual Edition を導入できます。

Data Store を導入するには、Data Node ごとに以下を割り当てる必要があります。

- Secure Network Analytics アプライアンスとの管理、取り込み、クエリの通信に使用するルーティング可能な IP アドレス
- Data Store クラスタの一部として Data Node 間の通信に使用する独立した LAN または VLAN のルーティング不可の IP アドレス（`169.254.42.0/24` CIDR ブロック）
- 管理、取り込み、クエリの通信用と Data Node 間の通信用の 2 つのネットワーク接続

導入および導入の前提条件の詳細については、「Data Store の導入の要件と考慮事項」を参照してください。

# Data Store の導入の前提条件と推奨事項

次に、Data Store の導入の前提条件に関する情報と推奨事項を示します。

## Secure Network Analytics バージョン サポート

Data Store を使用して Secure Network Analytics を導入する場合、すべての Secure Network Analytics アプライアンスが同じバージョン（7.4.x）である必要があります。7.4.x の利用可能な最新バージョンは 7.4.0 です。

## Secure Network Analytics ライセンス

Secure Network Analytics の導入には、フローレート（FPS）スマートライセンスが必要です。Data Store 自体に追加のライセンスは必要ありません。

マネージャ Virtual Edition または Flow Collector を導入する場合は、software.cisco.com でアカウントを登録すると、マネージャ Virtual Edition および Flow Collector VE のライセンスが付与されます。

## Secure Network Analytics 仮想アプライアンスの互換性とネットワーキングの要件

次の表に、Data Store VE への Secure Network Analytics の展開に必要な仮想アプライアンスの概要を示します。

| 仮想アプライアンスコンポーネント | サポートされているキャパシティ |
|---|---|
| データストア | • 3 つの Data Node VE のみまたは Data Store 6200（詳細については、「展開オプション」を参照） |
| マネージャ | • 1 つ以上の マネージャ VE |
| Flow Collector | • 1 つ以上の Flow Collector VE |

Data Store は、v7.3.1 以降の Flow Sensor と UDP Director をサポートします。Data Store を使用して展開する必要もありません。アプライアンスをクラスタに追加する場合は、すべてのアプライアンスに同じバージョンがインストールされていることを確認してください。

### マネージャ VE

マネージャ VE への最小リソース割り当てを決定するには、1 秒あたりのフロー数（FPS）を想定する必要があります。

リソース割り当てを決定するには、次の仕様を参照してください。

| 同時使用ユーザー | 必須予約済みメモリ | 必須予約済み CPU | 最小ストレージ容量 |
|---|---|---|---|
| 9 まで | 32 GB | 4 | 125 GB |
| 10 以上 | 64 GB | 8 | 200 GB |

## Flow Collector VE

Flow Collector VE のリソース要件を決定するには、ネットワークで予想される 1 秒あたりのフロー数と、モニターする見込みのホストとエクスポータの数を決める必要があります。Flow Collector ではなく Data Store がフローを保存するため、リソース要件は Data Store を導入するかどうかによって異なります。リソース要件を決定するには、次の仕様を参照してください。

| 1 秒あたりのフロー数 | インターフェイス | エクスポータ | 必須予約済みメモリ | 必須予約済み CPU | 必須最小データストレージ |
|---|---|---|---|---|---|
| 最大 50,000 | 最大 65,535 | 最大 2,048 | 32 GB | 6 | 200 GB |
| 最大 120,000 | 最大 65,535 | 最大 4,096 | 70 GB | 8 | 200 GB |

## Data Node VE

Data Node VE のリソース要件を決定するには、ネットワークで予想される 1 秒あたりのフロー（FPS）を決定する必要があります。これは Flow Collector VE のリソース要件にも影響します。リソース要件の詳細については、「Flow Collector VE」を参照してください。

ネットワークに導入可能な Data Node VE は 3 つまでです。追加の Data Node VE を導入することはできません。

3 つの Data Node VE に Data Store VE を展開する場合は、Data Node ごとに、ストレージ割り当てを次の方法で計算することを推奨します。

[(日時平均 FPS/1,000) X 1.6 X 日数] / Data Node 数

- 日時平均 (FPS)を決定します。
- この数値を 1,000 FPS で割ります。
- この数値にストレージの 1.6 GB を掛けると、1 日分のストレージに相当する値が得られます。
- この数値に、Data Store の全ストレージのフローを保存する日数を掛けます。
- この数値を Data Store 内の データノード 数で割って、Data Node あたりのストレージを算出します

たとえば、次のシステムの場合：

- 日時平均 50,000(FPS)
- 90 日間フローを保存
- 3 つの Data Node を装備

Data Node あたりの数値を次のように算出できます。

[(50,000/1,000) X 1.6 X 90] / 3 = Data Node あたり 2,400 GB(2.4 TB) データノード

- 日時平均 FPS = 50,000
- 日時平均 50,000 FPS / 1,000= 50
- 50 X 1.6 GB = 1 日あたりのストレージ相当量 80 GB
- Data Store あたり 80 GB X 90 日 = Data Store あたり 7,200 GB
- 7,200 GB / 3 データノード = データノード あたり 2,400 GB（2.4 TB）

リソース要件を決定するには、次の仕様を参照してください。

| 1 秒あたりの<br>フロー数 | 必須予約済みメモリ | 必須予約済み CPU | 30 日間に必要な最小データストレージ |
|---|---|---|---|
| 最大<br>50,000 | Data Node VE あたり 32 GB | Data Node VE あたり 6 | • Data Node あたり 800 GB<br>• 3 つの Data Node で合計 2.4 TB |
| 最大<br>120,000 | Data Node VE あたり 32 GB | Data Node VE あたり 12 | • Data Node あたり 1.92 TB<br>• 3 つの Data Node で合計 5.76 TB |
| 最大<br>220,000 | Data Node VE あたり 64 GB | Data Node VE あたり 16 | • Data Node あたり 3.52 TB<br>• 3 つの Data Node で合計 10.56 TB |

## Data Store の導入に必要なログイン情報

次のユーザーアカウントのパスワードを準備します。

- それぞれの マネージャ、Data Node、および Flow Collector の root と sysadmin。これらは、システムの初期設定時に割り当てます。
- それぞれの マネージャ、Data Node、および Flow Collector の admin。これらは、アプライアンス セットアップ ツールを使用して割り当てます。
- Data Store の dbadmin と readonlyuser。これらは、Data Store の初期化時に割り当てます。

## Data Store のネットワーキングとスイッチングに関する考慮事項

次の表に、Secure Network Analytics を Data Store とともに導入する場合のネットワーキングとスイッチングに関する考慮事項の概要を示します。

| ネットワークに関する考慮事項 | 説明 |
|---|---|
| 必要なログイン情報 | 各 Data Node、マネージャ および Flow Collector について：<br>• 初期システム設定時に設定：`root`、`sysadmin`<br>• アプライアンス設定ツールを使用して設定：`admin`<br>Data Store の初期化時に設定：`dbadmin`、`readonlyuser` |
| Data Node 間通信 | • Data Node が相互に通信できるように、仮想スイッチを使用して独立した LAN を設定します。<br>• すべての Data Node VE を同じ ESXi ホストに導入することをお勧めします。別々の ESXi ホストに Data Node を導入する場合は、Cisco Professional Services に連絡して、独立した LAN の設定に関する支援を受けてください。 |
| Secure Network Analytics アプライアンス通信 | • マネージャ、Data Node、Flow Collector に必要で、マネージャ から設定される SSH および SSH ルートアクセス<br>• マネージャ および Flow Collector は、すべての Data Node に到達できる必要があります<br>• Data Node は、マネージャ、すべての Flow Collector、および各 Data Node に到達できる必要があります |

全 Secure Network Analytics 環境用のフローレート（FPS）スマートライセンスを取得する必要があることに注意してください。

> 現在、Data Store では、プライマリ Data Node が停止した場合のスペア Data Node との自動交換はサポートされていません。詳細については、シスコ サポート にお問い合わせください。

各 Data Node に次の IP アドレスを割り当てる必要があります。

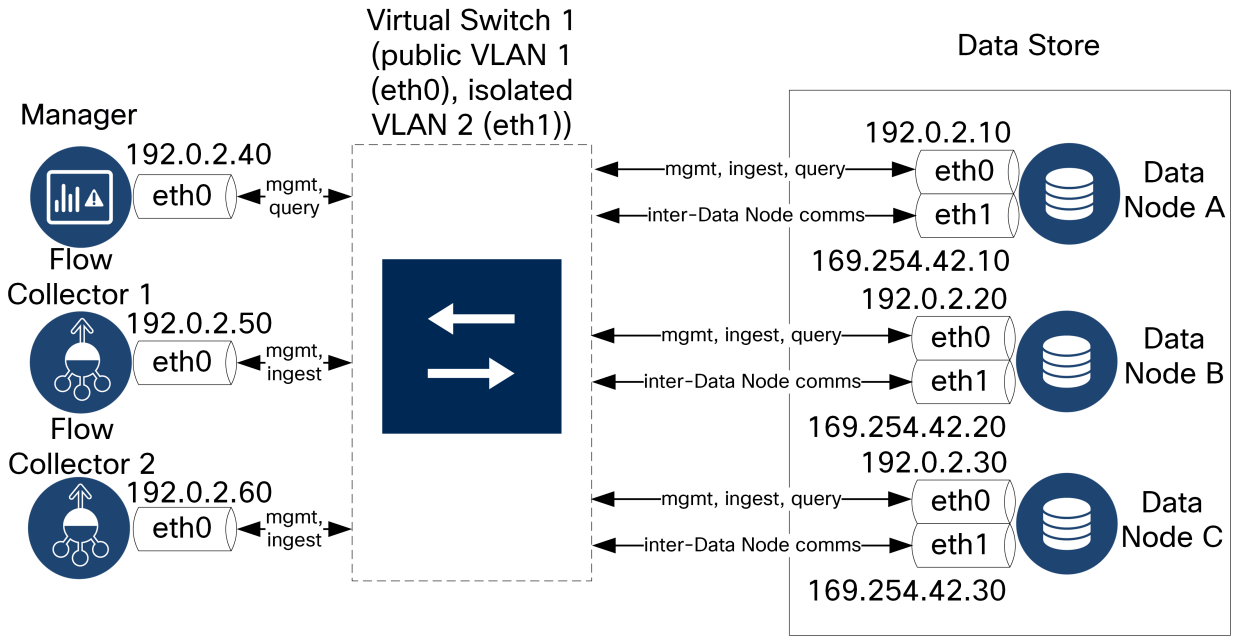
- Secure Network Analytics アプライアンスとの通信に使用するルーティング可能な IP アドレス（`eth0`）。

  Data Store の展開と設定においては、Data Node `eth0` IP アドレスを Data Store の名前にマッピングして、テレメトリの保存やクエリの要求と応答がより均等に分散されるようにします。詳細については、「Data Store の初期化と設定」を参照してください。
- Data Node 間の通信に使用するプライベート LAN または VLAN 内のルーティング不可の IP アドレス（`eth1`）。各 Data Node から仮想スイッチまたは隔離ネットワークを介して他のすべての Data Node に到達できることを確認します。Data Store の一部として、Data Node は相互

に通信します。

> 169.254.42.0/24 CIDR ブロックからルーティングできない IP アドレスを割り当てる必要があります。

eth1 を介した Data Node 間の通信を有効にするには、仮想スイッチで Data Node 間の通信用に独立した LAN または VLAN を設定します。この仮想スイッチは Data Node 間の通信専用にします。また、Data Node の マネージャ および Flow Collector との eth0 通信用にパブリック LAN または VLAN を設定します。例として次の図を参照してください。




Data Store クラスタでは、独立 VLAN 内のノード間で継続的なハートビートが必要です。このハートビートがないと、Data Node がオフラインになる可能性があり、Data Store が停止するリスクが高まります。

> 導入の計画については、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 の導入の要件と考慮事項

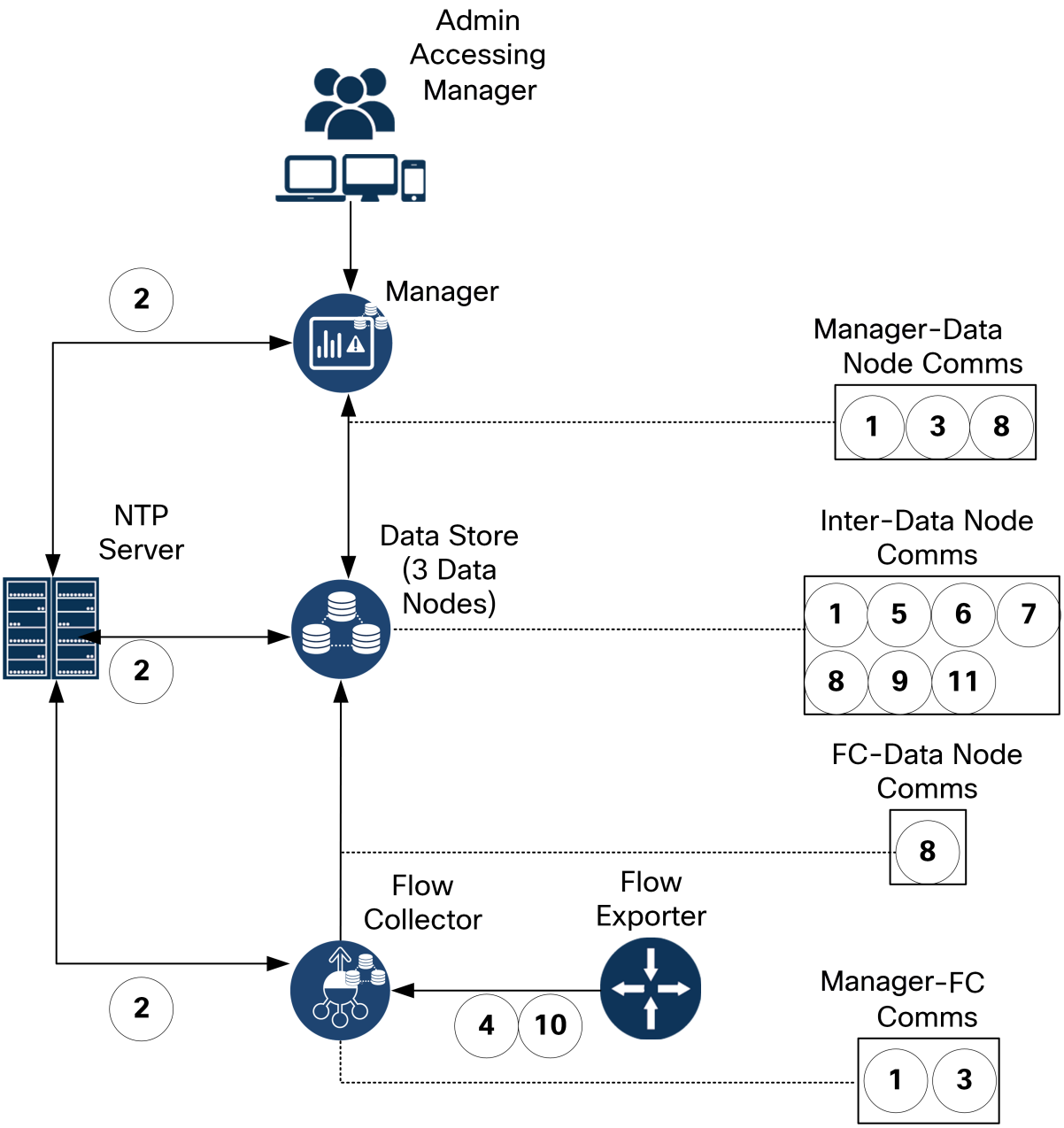
Data Node は、それぞれがすべての Flow Collector、マネージャ、および他の Data Node と通信できるように配置します。最適なパフォーマンスを得るには、Data Node と Flow Collector を同じ場所に配置して通信の遅延を最小限に抑え、Data Node と マネージャ を同じ場所に配置してクエリのパフォーマンスを最適化します。シスコでは、Data Node をファイアウォール内（NOC 内など）に配置することを強く推奨しています。設定を容易にするために、すべての Data Nodes Virtual Edition を同じ物理ホストまたはハイパーバイザに展開します。これにより、独立した LAN で Data Node 間の設定を簡単に設定できます。

電力の喪失やハードウェアの障害が原因で Data Store が停止すると、データ破損やデータ損失のリスクが高くなります。Data Node の導入においては、常に稼働時間が維持されるように考慮することをお勧めします。

> 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、その Data Node のデータベースインスタンスが自動的に再起動しないことがあります。データベースインスタンスを手動で再起動する方法については、「Data Store のトラブルシューティング」を参照してください。

## Data Store 通信ポート

次の図に、Secure Network Analytics のアーキテクチャの例と開く必要がある通信ポートを示します。各引き出し線で示されたポートの表を確認してください。



Data Store を展開するためにファイアウォールで開く通信ポートを次に示します。これ以外に Secure Network Analytics の展開全体で開く通信ポートについては、『Cisco Secure Network Analytics Virtual Edition (with Data Store) Appliance Installation Guide』を参照してください。

| # | 送信元(クライアント) | 宛先(サーバー) | ポート | プロトコルまたは目的 |
|---|---|---|---|---|
| 1 | マネージャ | Flow Collector と Data Node | 22/TCP | SSH(Data Store データベースの初期化に必要) |
| 1 | データノード | 他のすべての Data Node | 22/TCP | SSH(Data Store データベースの初期化およびデータベース管理タスクに必要) |
| 2 | マネージャ、Flow Collector と Data Node | NTP サーバー | 123/UDP | NTP(時刻同期に必要) |
| 2 | NTP サーバー | マネージャ、Flow Collector と Data Node | 123/UDP | NTP(時刻同期に必要) |
| 3 | マネージャ | Flow Collector と Data Node | 443/TCP | HTTPS(アプライアンス間のセキュア通信に必要) |
| 3 | Flow Collector | マネージャ | 443/TCP | HTTPS(アプライアンス間のセキュア通信に必要) |
| 3 | データノード | マネージャ | 443/TCP | HTTPS(アプライアンス間のセキュア通信に必要) |
| 4 | NetFlow エクスポータ | Flow Collector:NetFlow | 2055/UDP | NetFlow の取り込み |
| 5 | データノード | 他のすべての Data Node | 4803/TCP | Data Node 間メッセージングサービス |
| 6 | データノード | 他のすべての Data Node | 4803/UDP | Data Node 間メッセージングサービス |
| 7 | データノード | 他のすべての Data Node | 4804/UDP | Data Node 間メッセージングサービス |
| 8 | マネージャ、Flow Collector と Data Node | データノード | 5433/TCP | Vertica クライアント接続 |

| | | | | |
|---|---|---|---|---|
| 9 | データノード | 他のすべての Data Node | 5433/UDP | Vertica メッセージングサービスのモニターリング |
| 10 | sFlow エクスポータ | Flow Collector：sFlow | 6343/UDP | sFlow の取り込み |
| 11 | データノード | 他のすべての Data Node | 6543/UDP | Data Node 間メッセージングサービス |

# Secure Network Analytics と Data Store の導入の概要

次に、Secure Network Analytics を Data Store とともに導入する場合の大まかな手順を説明します。

1. Data Store で使用する マネージャ の設定：マネージャ を展開して設定し、次に進む前に最新バージョンとロールアップパッチをインストールします。
2. Data Store の初期導入と設定：Data Node を展開して設定し、次に進む前にそれぞれで最新バージョンとロールアップパッチをインストールします。
3. Data Store で使用する Flow Collector の設定：Flow Collector を展開して設定し、次に進む前にそれぞれで最新バージョンとロールアップパッチをインストールします。
4. Data Store の初期化と設定：Data Store を初期化し、Data Store ユーザーのパスワードを割り当てます。
5. フローインターフェイス統計の保持設定：Data Store の保持設定を構成します。
6. Data Store の次のステップ

さらに、オプションの Secure Network Analytics コンポーネントについては次のセクションを参照してください。

- UDP Director（オプション）の導入
- Flow Sensor（オプション）の導入
- フェールオーバーマネージャ（オプション）の導入

# Data Store の設置

## Secure Network Analytics 仮想アプライアンスの導入と考慮事項

マネージャ、Data Node、および Flow Collector の各 Secure Network Analytics アプライアンスを以下の手順に従って展開および設定します。Data Node を展開してネットワークに接続するときは、「Data Store の導入の要件と考慮事項」を参照してください。マネージャ、Data Node、および Flow Collector は同じバージョン(7.4.0)で、最新のロールアップパッチが適用されている必要があります。

個々のアプライアンスのインストールと設定の詳細については、『Cisco Secure Network Analytics Virtual Edition (with Data Store) Installation Guide v7.4.0』を参照してください。個々のアプライアンスでのアプライアンス セットアップ ツールの実行については、『Cisco Secure Network Analytics System Configuration Guide v7.4.0』を参照してください。

マネージャ および Flow Collector の初回セットアップでの設定時は、セキュリティ分析とロギング(オンプレミス)を有効にするオプションもあります。セキュリティ分析とロギング(オンプレミス)を有効にする場合は、Secure Network Analytics の展開を使用して Firepower イベント情報を保存します。また、マネージャ と Flow Collector の両方で有効にする必要があります。これによって Flow Collector で NetFlow 収集が無効になることに注意してください。詳細については、『Security Analytics and Logging: Firepower Event Integration Guide』を参照してください。

> Data Store を導入する場合は、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。

## マネージャ Data Store で使用する設定

Data Store で使用する マネージャ を導入して設定し、Data Node および Flow Collector を管理します。

> Data Store と連携するセカンダリ マネージャ の展開と設定の詳細なコンテキストについては、「**フェールオーバーマネージャ(オプション)の導入**」を参照してください。

次の手順を実行します。

1. 最初に、マネージャ をネットワークに展開します。その後、アプライアンスのコンソールに `root` として接続して `SystemConfig` を実行し、初回セットアップウィザードを使用して、Data Store と セキュリティ分析とロギング(オンプレミス)(オプション)で使用するための、管理ポートの設定を更新します。仮想アプライアンスの導入と初回セットアップの実行の詳細については、『Cisco Secure Network Analytics Virtual Edition (with Data Store) Installation Guide v7.4.0』を参照してください。

   セキュリティ分析とロギング(オンプレミス)を有効にする場合は、Secure Network Analytics の展開を使用して Firepower イベント情報を保存します。また、マネージャ と Flow Collector の両方で有効にする必要があります。これによって Flow Collector で NetFlow 収集が無効になることに注意してください。詳細については、『Security Analytics and Logging: Firepower Event Integration Guide』を参照してください。

> システム構成に初めてアクセスした場合のみ、初回セットアップが自動的に開始され、アプライアンスの初期設定プロセスを実行できます。

> マネージャ または Flow Collector を Data Store および セキュリティ分析とロギング（オンプレミス）で使用するように設定した後に、アプライアンスの設定を更新してこの設定を変更することはできません。選択を間違えた場合は、アプライアンスを RFD する必要があります。これは、ネットワークに Data Store を導入する場合にのみ有効にします。

2. 次に、Web ブラウザで、管理ポートに割り当てた IP アドレスに移動します。アプライアンス セットアップ ツールを使用して、`admin` ユーザーのパスワード（およびシステム構成で割り当てなかった場合は `root` ユーザーと `sysadmin` ユーザーのパスワード）の割り当て、Secure Network Analytics ドメインの設定、その他のネットワークの設定、DNS および NTP の設定、マネージャ への Central Management のインストールなど、追加の設定を実行します。アプライアンス セットアップ ツールの使用方法の詳細については、『Cisco Secure Network Analytics System Configuration Guide』を参照してください。
3. 最後に、マネージャ を最新のバージョンとパッチに更新します。現在のバージョンへ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。パッチの更新の詳細については、パッチの readme を参照してください。

   マネージャ を更新したら、次のセクションの説明に従って Data Node を展開して設定します。

## Data Store の初期導入と設定

マネージャ を展開したら、Data Node アプライアンスを展開して設定します。Data Node を展開してネットワークに接続するときは、「Data Store の導入の要件と考慮事項」を参照してください。

Data Nodes Virtual Edition を展開する場合は、Data Node 間の通信用の仮想スイッチを作成します。独立 LAN の確立の詳細については、『Cisco Secure Network AnalyticsVirtual Edition (with Data Store) Installation Guide v7.4.0』または仮想スイッチのドキュメントを参照してください。

各 Data Node について、以下を実行します。

1. まず、Data Node をネットワークに展開します。Data Node Virtual Edition を展開する場合は、必ず 2 つのネットワークアダプタを割り当て、ネットワークアダプタの 1 つを仮想スイッチに割り当てます。その後、アプライアンスのコンソールに `root` として接続して `SystemConfig` を実行し、初回セットアップウィザードを使用して、管理ポートの設定、Data Node 間の通信ポートの設定、および `root` ユーザーと `sysadmin` ユーザーのパスワードを更新します。仮想アプライアンスの導入と初回セットアップの実行の詳細については、『Cisco Secure Network Analytics Virtual Edition (with Data Store) Installation Guide v7.4.0』を参照してください。

   > システム構成に初めてアクセスした場合のみ、初回セットアップが自動的に開始され、アプライアンスの初期設定プロセスを実行できます。

2. 次に、Web ブラウザで、管理ポートに割り当てた IP アドレスに移動します。アプライアンス セットアップ ツールを使用して、`admin` ユーザーのパスワード（およびシステム構成で割り当てなかった場合は `root` ユーザーと `sysadmin` ユーザーのパスワード）の割り当て、Secure Network Analytics ドメインの設定、その他のネットワークの設定、DNS および NTP の設定、

Central Management による Data Node 管理の有効化など、追加の設定を実行します。アプライアンス セットアップ ツールの使用方法の詳細については、『Cisco Secure Network Analytics System Configuration Guide』を参照してください。

3. 最後に、Data Node を最新のバージョンとパッチに更新します。現在のバージョンへ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。パッチの更新の詳細については、パッチの readme を参照してください。

> 続行する前に、該当する更新ガイドとパッチの readme ドキュメントを確認します。データノードの更新プロセスでは、Secure Network Analytics の他のアプライアンスよりも多くの手順が必要になります。

Data Node を更新したら、「**Data Store の初期導入と設定**」の先頭に戻り、残りの Data Node に対してこの手順を繰り返して、Data Node のインストールと初期設定、アプライアンス セットアップ ツールの設定、および Central Management の設定を行います。

4. すべての Data Node を展開して設定したら、「**Data Store で使用する Flow Collector の設定**」の説明に従って Flow Collector を設定します。

## Data Store で使用する Flow Collector の設定

マネージャ、Data Node、および Flow Collector を展開して設定したら、Data Store を初期化して設定します。次に進む前に、すべての Manager、Data Node、および Flow Collector が最新のバージョンとパッチに更新されていることを確認してください。

各 Flow Collector について、次の手順を実行します。

1. 最初に、Flow Collector をネットワークに展開します。その後、アプライアンスのコンソールに `root` として接続して `SystemConfig` を実行し、初回セットアップウィザードを使用して、管理ポートの設定、Data Store とセキュリティ分析とロギング（オンプレミス）（オプション）で使用するための設定、および `root` ユーザーと `sysadmin` ユーザーのパスワードを更新します。仮想アプライアンスの導入と初回セットアップの実行の詳細については、『Cisco Secure Network Analytics Virtual Edition (with Data Store) Installation Guide v7.4.0』を参照してください。

   セキュリティ分析とロギング（オンプレミス）を有効にする場合は、Secure Network Analytics の展開を使用して Firepower イベント情報を保存します。また、マネージャと Flow Collector の両方で有効にする必要があります。これによって Flow Collector で NetFlow 収集が無効になることに注意してください。詳細については、『Security Analytics and Logging: Firepower Event Integration Guide』を参照してください。

   > システム構成に初めてアクセスした場合のみ、初回セットアップが自動的に開始され、アプライアンスの初期設定プロセスを実行できます。

   > マネージャまたは Flow Collector を Data Store および セキュリティ分析とロギング（オンプレミス）で使用するように設定した後に、アプライアンスの設定を更新してこの設定を変更することはできません。選択を間違えた場合は、アプライアンスを RFD する必要があります。これは、ネットワークに Data Store を導入する場合にのみ有効にします。

2. 次に、Web ブラウザで、管理ポートに割り当てた IP アドレスに移動します。アプライアンス セットアップ ツールを使用して、`admin` ユーザーのパスワード（およびシステム構成で割り当てなかった場合は `root` ユーザーと `sysadmin` ユーザーのパスワード）の割り当て、Secure Network Analytics ドメインの選択、その他のネットワークの設定、DNS および NTP の設定、フロー収集ポート番号（NetFlow の場合は `2055`、sFlow の場合は `6343`）、Flow Collector の Central Management による管理の有効化など、追加の設定を実行します。アプライアンス セットアップ ツールの使用方法の詳細については、『Cisco Secure Network Analytics System Configuration Guide』を参照してください。

   > Data Store で使用するように 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）で特定の機能が非表示になります。Flow Collector の設定やその他の関連タスクを実行するには、Central Management を使用します。ストレージの統計を監視するには、マネージャ（[ダッシュボード（Dashboard）] > レポートビルダー）でレポートビルダーを使用します。

3. 最後に、Flow Collector を最新のバージョンとパッチに更新します。現在のバージョンへ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。パッチの更新の詳細については、パッチの readme を参照してください。

   Flow Collector を更新したら、残りの Flow Collector のそれぞれに対して「**Data Store で使用する Flow Collector の設定**」の手順を繰り返して、Flow Collector のインストールと初期設定、アプライアンス セットアップ ツールによる設定、および Central Management の設定を行います。

4. すべての Flow Collector を展開して設定したら、「**Data Store の初期化と設定**」の説明に従って Data Store を初期化して設定します。

## Data Store の初期化と設定

Manager を展開して設定したら、次に進む前に、すべての Manager、Data Node および Flow Collector が最新のバージョンとパッチに更新されていることを確認してください。

次の手順を実行します。

1. 最初に、Central Management で、必要なアプライアンスが マネージャ で管理されていることを確認します。
   - すべての Data Node
   - すべての Flow Collector
   - セカンダリ マネージャ（展開した場合）

### Data Node と Flow Collector が Central Management で管理されていることを確認する

**はじめる前に**

- Central Management で管理する必要があるすべての Data Node と Flow Collector の IP アドレスとホスト名のリストを作成します。
- システム管理者として マネージャ Web アプリケーションにログインし、Central Management に移動します。

**手順**

- アプライアンスインベントリで、Data Node と Flow Collector のリスト、および展開した場合はセカンダリ マネージャ について、それぞれをインベントリのリストと比較し、[**アプライアンスのステータス（Appliance Status）**] が [**アップ（Up）**] であることを確認します。目的のすべてのアプライアンスが管理対象になり、[**アプライアンスのステータス（Appliance Status）**] が [**アップ（Up）**] になるまで、Data Store の初期化を開始**しない**でください。

  アプライアンスのステータスが [**ダウン（Down）**] の場合は、アプライアンスの設定および マネージャ とそのアプライアンスの接続を確認します。

  アプライアンスがインベントリに表示されない場合は、アプライアンスを追加します。

2. 次に、マネージャ から `SystemConfig` を使用して、マネージャ、Data Node、および Flow Collector でパスワードレス SSH を有効にします。

> SystemConfig で Data Store を設定するときは、最初の手順としてパスワードレス SSH を毎回有効にする必要があります。Data Store の設定を終了した時点で、すべてのアプライアンスのパスワードレス SSH が無効になります。

## Secure Network Analytics アプライアンスでパスワードレス SSH を有効にする

**はじめる前に**

- マネージャ のコンソールに `root` としてログインします。

**手順**

1. コマンドプロンプトで `SystemConfig` と入力して Enter を押し、システム構成ユーティリティにアクセスします。
2. [**データストア（Data Store）**] を選択します。
3. [**パスワードレスSSH（Passwordless SSH）**] を選択します。パスワードレス SSH が有効になるまで数分待ちます。

   次に進む前に、Central Management ですべてのアプライアンスが稼働していることを確認します。

3. 最後に、`SystemConfig` を使用して Data Store を初期化します。

Data Store を初期化すると、ウィザードでいくつかのタスクが実行されます。

- 前提条件として、Central Management のインベントリに少なくとも 1 つの マネージャ、1 つの Flow Collector、3 つの Data Node が含まれていることが確認されます
- Data Store に関連するパスワードの入力を求められます
- Data Store 内のすべてのアプライアンスと Data Node にパスワードと証明書が配布されます
- Data Node 間通信を設定します。
- Data Store が初期化されます。
- Data Store のセットアップが確定されます。

これらのステップのいくつかでは、ウィザードで設定が更新されてプロセスの次のステップに進むまでに数分かかります。ウィザードでの Data Store のセットアップが完了したら、Central Management のインベントリですべてのアプライアンスが稼働していることを確認します。Data Store を使用した Secure Network Analytics の展開が完了しました。

ウィザードのプロンプトに従って、`dbadmin` と `readonlyuser` のパスワードを割り当てます。各パスワードは、次の要件を満たしている必要があります。

- 少なくとも 1 つの数字
- 少なくとも 1 つの小文字
- 少なくとも 1 つの大文字
- 次のうちの少なくとも 1 つの特殊文字： `<>.,?/'"|:;` ` ~!@#$%^&*()-_+={}[]`
- 8 文字以上（上限はなし）
- ASCII エンコード文字のみ

## Data Store を初期化する

### はじめる前に

- `SystemConfig` でパスワードレス SSH を有効にします。
- 次に進む前に、Central Management ですべてのアプライアンスが稼働していることを確認します。

### 手順

- `SystemConfig` の [データストア（Data Store）] メニューから、**[データストアの初期化（Initialize Data Store）]** を選択します。ウィザードの手順に従います。プロセスの各ステップが完了するまでに数分かかる場合があることに注意してください。

  Data Store が初期化され、ウィザードでの Data Store のセットアップを完了したら、Central Management ですべてのアプライアンスが稼働していることを確認します。Data Store を使用した Secure Network Analytics の展開が完了しました。

### 次の作業

- UDP Director、Flow Sensor、またはセカンダリ マネージャ がない場合は、「**フローインターフェイス統計の保持設定**」の説明に従ってフローインターフェイス統計データの保持方法を設定します。
- UDP Director、Flow Sensor、またはセカンダリ マネージャ がある場合は、次のセクションの説明に従って、それらを展開します。

# UDP Director（オプション）の導入

UDP Director を展開する場合は、『Cisco Secure Network Analytics Virtual Edition (with Data Store) Appliance Installation Guide』および『Cisco Secure Network Analytics System Configuration Guide』の手順に従います。UDP Director のインストールプロセスは、Data Store を展開するかどうかに関係なく同じになります。Data Store で使用するために UDP Director を構成する必要はありません。

UDP Director を展開したら、以降のセクションの説明に従って Flow Sensor またはセカンダリ マネージャ を展開するか、「**フローインターフェイス統計の保持設定**」の説明に従って Data Store のデータの保持方法を設定します。

## Flow Sensor（オプション）の導入

Flow Sensor を展開する場合は、『Cisco Secure Network Analytics Virtual Edition (with Data Store) Appliance Installation Guide』および『Cisco Secure Network Analytics System Configuration Guide』の手順に従います。Flow Sensor のインストールプロセスは、Data Store を導入するかどうかに関係なく同じになります。Data Store で使用するために Flow Sensor を構成する必要はありません。

Flow Sensor を展開して設定したら、次のセクションの説明に従ってセカンダリ マネージャ をフェールオーバー マネージャ として設定するか、「**フローインターフェイス統計の保持設定**」の説明に従ってフローインターフェイス統計データの保持方法を設定します。

## フェールオーバーマネージャ（オプション）の導入

フェールオーバー マネージャ として設定するセカンダリ マネージャ がある場合は、『Cisco Secure Network Analytics Virtual Edition (with Data Store) Appliance Installation Guide』、『Cisco Secure Network Analytics System Configuration Guide』、および『Cisco Secure Network AnalyticsFailover Configuration Guide』の手順に従います。

セカンダリ マネージャ の設定が完了し、Central Management でプライマリ マネージャ によって管理されていることを確認したら、「**フローインターフェイス統計の保持設定**」の説明に従ってフローインターフェイス統計データの保持方法を設定します。

# フローインターフェイス統計の保持設定

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るため、フローインターフェイス統計の保持期間はデフォルトでは最大 7 日間に制限されています。

フローインターフェイス統計の保持期間は、Secure Network Analytics REST APIを使用して次のように変更できます。

- 別の日数(最大 3000 日)に変更する。
- Data Store が最大容量に達するまで、データを可能な限り保存する。

Data Store フローインターフェイス統計の保持について、次の点に注意してください。

- データ保持設定を更新した後に Secure Network Analytics のアプライアンスや Data Store を再起動する必要はありません。設定は数分で有効になります。
- 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つ必要があります。その時点まで、データは使用可能な最も減らされた(つまり、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。
- フローインターフェイス統計を保存しない場合は、各 Flow Collector の管理ユーザーインターフェイスにアクセスし、**[サポート(Support)] > [詳細設定(Advanced Settings)]** の順にクリックします。各 Flow Collector について、[オプションのラベル(Option Label)] 列の「interface_retention_days」エントリを 0(ゼロ)に変更し、Flow Collector(可能な場合は Flow Collector エンジン)を再起動します。

これらの設定を更新するには、REST API を使用して以下を実行します。

**マネージャ の REST API に対して認証を行う**

要求リソースの情報

| リソース | 説明 |
|---|---|
| URI | `https://[smc-eth0-ip]/token/v2/authenticate` |
| 説明 | マネージャ の REST API に対して認証を行います。 |
| URI パラメータ | • *[smc-eth0-ip]*:マネージャ eth0 管理 IP アドレス |

| リソース | 説明 |
|---|---|
| HTTP メソッド | POST |
| 要求本文 MIME タイプ | application/x-www-form-urlencoded |
| 要求本文 | `username=[username]&password=[password]` |
| 要求本文パラメータ | • *[username]*:(必須)マネージャ admin ユーザー<br>• *[password]*:(必須)マネージャ admin ユーザーアカウントのパスワード |

成功応答コードと定義

| 応答 | 説明 |
|---|---|
| 応答コード | 200:成功 |
| 応答本文 | 応答本文には、このセッションの後続の REST API コールで渡す必要がある Cookie 情報が含まれています。セッションの有効期間は 20 分です。 |

### Data Store の現在のデータ保持設定を取得する

要求リソースの情報

| リソース | 説明 |
|---|---|
| URI | `https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings` |
| 説明 | Data Store の現在のデータ保持設定を取得します。 |
| URI パラメータ | • *[smc-eth0-ip]*:マネージャ eth0 管理 IP アドレス |
| HTTP メソッド | GET |
| 要求本文 MIME タイプ | 適用対象外 |
| 要求本文 | 適用対象外 |
| 要求本文パラメータ | 適用対象外 |

成功応答コードと情報

| リソース | 説明 |
|---|---|
| 応答コード | 200：成功 |
| 応答本文 | 応答本文には、現在の Data Store フローインターフェイス統計の保持設定が含まれます。以前に変更していない場合、デフォルト値は 7 日です。 |

### Data Store フローインターフェイス統計データの保持設定を更新する

要求リソースの情報

| リソース | 説明 |
|---|---|
| URI | `https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings` |
| 説明 | Data Store フローインターフェイス統計データの保持設定を更新します。 |
| URI パラメータ | • *[smc-eth0-ip]*：マネージャ eth0 管理 IP アドレス |
| HTTP メソッド | PUT |
| 要求本文 MIME タイプ | application/json |
| 要求本文 | `{`<br>`"interfaceRetentionType":"[type]",`<br>`"interfaceRetentionAmount":"[#]"`<br>`}` |
| 要求本文パラメータ | • *[type]*：（必須）データ保持のタイプ。次のいずれかの文字列値に設定します。<br>  • `AMOUNT`：interfaceRetentionAmount で定義された日数が経過するまで、データを削除せずに保存します。<br>  • `FOREVER`：Data Store フローインターフェイス統計の最大容量に達するまで、可能な限りデータを削除せずに保存します<br>• *[#]*：（必須）Data Store でデータを削除せずに保存する最大日数。`1-3000` の範囲の整数に設定します。<br>  ℹ `interfaceRetentionType` を `FOREVER` に設定する場合も、`interfaceRetentionAmount` を渡す必要があります。この値は無視されます。この場合、`interfaceRetentionAmount` で渡す値に関係なく、内部的にデフォルト値の `7` として保存されます。 |

成功応答コードと情報

| リソース | 説明 |
|---|---|
| 応答コード | 204：成功（コンテンツなし） |
| 応答本文 | 応答本文のコンテンツはありません。 |

REST API の詳細については、Secure Network Analytics REST API のドキュメントを参照してください。

次の手順では、フローインターフェイス統計データの保持期間を更新する curl 構文を示します。

# フローインターフェイス統計の保持期間を更新する

**はじめる前に**

- curl がインストールされている Linux ベースのアプライアンスのコンソールにログインします。

**手順**

1. 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。

   ```
   curl -c cookies.txt -d "username=[username]&password=[password]"
   https://[smc-eth0-ip]/token/v2/authenticate
   ```

2. *[username]* を マネージャ の admin ユーザーのユーザー名に置き換えます。
3. *[password]* を マネージャ の admin ユーザーのパスワードに置き換えます。
4. *[smc-eth0-ip]* を マネージャ の `eth0` IP アドレスに置き換えます。
5. 更新した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、マネージャ で REST API を使用するための認証を行います。

   セッションの有効期間は 20 分です。
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。

   ```
   curl -X GET -b cookies.txt https://[smc-eth0-ip]/smc-
   configuration/rest/v1/cds/retentionsettings
   ```

7. *[smc-eth0-ip]* を マネージャ の `eth0` IP アドレスに置き換えます。
8. 更新した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、現在の保持設定を取得します。

   初めて確認した場合は、フローインターフェイス統計の保持期間がデフォルトの 7 日に設定されています。
9. 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。

   ```
   curl -X PUT -b cookies.txt -H "X-XSRF-TOKEN:TOKEN" -H "Content-
   Type:application/json" -d '
   {"interfaceRetentionType":"AMOUNT","interfaceRetentionAmount":"
   ```

```
[#]"}' https://[smc-eth0-ip]/smc-
configuration/rest/v1/cds/retentionsettings
```

10. *[type]* を次のいずれかに置き換えます。
    - 保持日数を設定する場合は AMOUNT。
    - データを可能な限り保存する場合は FOREVER。
11. *TOKEN* を、手順 1 で作成した cookies.txt ファイルの XSRF-TOKEN 値に置き換えます。これは、cookies.txt ファイルの XSRF-TOKEN 名の後に表示される値で、次の例のような形式が含まれています：fd1fedc9-4686-4ce6-a0ba-9dc6dbdc242a
12. *[#]* を 1-3000 の範囲の保持日数を示す整数に置き換えます。
13. これは、*[type]*=FOREVER と設定した場合も定義する必要があります。この場合、この値は無視され、内部的に 7 に設定されます。
14. *[smc-eth0-ip]* を マネージャ の eth0 IP アドレスに置き換えます。
15. 更新した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、保持設定を更新します。

> 保持設定を更新した後に Secure Network Analytics のアプライアンスや Data Store を再起動する必要はありません。設定は数分で有効になります。ただし、フローインターフェイス統計の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つ必要があります。

### 次の作業

- 次のセクションの説明に従って、次のステップを確認します。

# Data Store のインストールの次のステップ

Data Store で使用するために Secure Network Analytics の導入環境を展開して設定した後、次の手順を実行します。

- **レポートビルダー**：レポートビルダーを使用して Secure Network Analytics 導入環境でレポートを実行し、Data Store のストレージ統計情報を表示します。詳細については、リリースノートを参照してください。
- **ヘルプ**：Secure Network Analytics の使用方法の詳細については、Web アプリケーション ヘルプを確認してください。

# Data Store のメンテナンス

次に、Data Store と Data Store に関連するメンテナンスタスクについて説明します。

- Data Node と Data Store の再起動
- Data Store のバックアップと復元
- Data Node の追加、削除、交換
- Data Store の初期化後の Manager および Flow Collector 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。

## Data Node の再起動

> 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 Node を再起動する必要がある場合は、停止するコマンドを発行してから、再起動するコマンドを発行します。

### Data Node を停止して再起動する

**はじめる前に**

- Data Node のコンソールに `root` としてログインします。

**手順**

1. `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。
2. 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。

   ```
   /opt/vertica/bin/admintools -t stop_node -s [data-node-hostname]
   ```

3. `[data-node-hostname]` を再起動前に停止する Data Node のホスト名に置き換えます。
4. 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、Data Node を停止します。
5. 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。

   ```
   /opt/vertica/bin/admintools -t restart_node -d sw [data-node-hostname]
   ```

6. `[data-node-hostname]` を再起動する Data Node のホスト名に置き換えます。これは、ノードのプライベート LAN IP アドレス（通常、関連付けられたホスト名はありません）またはノード名のいずれかです。次に例を示します。「v_sw_node0001」。
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、Data Node を再起動します。

# Data Store の再起動

> 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 を再起動するには、停止するコマンドを発行してから、再起動するコマンドを発行します。

## Data Store を停止して再起動する

### はじめる前に

- Data Node のコンソールに `root` としてログインします。
- CIMC またはハイパーバイザコンソールを使用して、Data Node のコンソールにアクセスできます。詳細については、更新ガイドの「Alternative Access」を参照してください。
- SSH を使用して Data Node にアクセスする場合は、最初に Central Manager で SSH を有効にする必要がある場合があります。詳細については、更新ガイドの「**Additional Option**」セクションを参照してください。

> この手順を開始する前に、停電後、データベースをアップグレードまたは起動する前に、[SSHの有効化（Enable SSH）] オプションを選択して、すべての DNODE で SSH が有効になっていることを確認します。
>
> DNODE で SSH を無効にする場合は、アップグレードプロセスが完了したら、戻って各 DNODE の SSH を無効にすることができます。このガイドの「**Data Store のメンテナンス**」セクションの手順に従って、すべての DNODE で SSH を有効にし、[ルートSSHアクセスの有効化（Enable Root SSH Access）] オプションではなく、必ず **[SSHの有効化（Enable SSH）]** チェックボックスを選択してください。

### 手順

1. `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。
2. 次の選択肢があります。
   - コマンドプロンプトで `/opt/vertica/bin/admintools -t stop_db -p <password>` と入力して Enter を押し、Data Store を停止します。
   - コマンドプロンプトで `/opt/vertica/bin/admintools -t stop_db -p <password> -F` と入力して Enter を押し、Flow Collector や マネージャ の接続を無効にして Data Store を停止します。
3. コマンドプロンプトで `/opt/vertica/bin/admintools -t start_db -d sw` と入力して Enter を押し、Data Store を再起動します。

# 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、以下を実行する必要があります。

- バックアップのサイズを見積もる
- バックアップサイズの 2 倍のストレージ容量を持つバックアップホストを準備する

  > 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。

- バックアップホストに Python 3.7 と rsync 3.0.5 をインストールする
- すべての Data Node からバックアップホストにパスワードレス SSH アクセスを使用して到達できることを確認する
- 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
- Data Store をバックアップする

## バックアップホストのストレージ要件を見積もる

### はじめる前に

- Data Node のコンソールに `root` としてログインします。

### 手順

1. 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;"
   ```

2. 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。

## バックアップホストを準備する

### はじめる前に

- 前のタスク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の Linux ホストを特定するか、必要なストレージ要件を満たす Linux 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。

- 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。

### 手順

1. 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 がインストールされている場合は、手順 4 に進みます。
   - それ以外の場合は、Python 3.7 をインストールします。手順 2 に進みます。
2. `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。
3. `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。
4. 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 がインストールされている場合は、手順 7 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 5 に進みます。
5. `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。
6. `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。
7. 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。「**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 5 に進みます。
8. コマンドプロンプトで `useradd 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。
9. `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。
10. 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。

### 次の作業

- 次のセクションの説明に従って、`dbadmin` ユーザーアカウントのパスワードレス SSH アクセスを有効にします。

## dbadmin のパスワードレス SSH アクセスを有効にする

### はじめる前に

- SSH 用にバックアップホストと各 Data Node 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 Data Node の間でポート 50000/TCP を開きます。
- OpenSSH の `ssh-copy-id` に関するドキュメントで詳細を確認します。
- 最初の Data Node に `root` としてログインします。

### 手順

1. 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 -i dbadmin@[hostname]`

2. `[hostname]` をバックアップホストのホスト名に置き換えます。
3. 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。
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 'dbadmin@[hostname]'`

5. `[hostname]` をバックアップホストのホスト名に置き換えます。
6. 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。

## 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

### はじめる前に

- 最初の Data Node 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。「Data Store データベースをバックアップする」の説明に従って、この Data Node からバックアップも実行します。

### 手順

1. `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。
2. 次のコマンドをテキストエディタにコピーします。`ssh [backup-host-ip]`
3. `[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。
4. 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、バックアップホストのインターフェイスに `dbadmin` と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。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。
5. `cd /home/dbadmin` と入力して Enter を押し、ディレクトリを変更します。
6. `mkdir backups` と入力して Enter を押し、`backups` ディレクトリを作成します。
7. `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。
8. `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する場合は、`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。詳細については、「Data Store の dbadmin および readonlyuser のパスワードを初期化後に更新する」を参照してください。

9. 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]
```

10. `[dbadmin-password]` を Data Store の `dbadmin` パスワードに更新します。
11. 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。
12. 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。
13. `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。
14. `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。
15. 各ノードについて、`-o AllowUsers=dbadmin` および `-o AllowTcpForwarding=yes` を含む行を `/etc/default/ssh` ファイルに追加します。次に、`systemctl restart ssh` を実行します。
16. 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
```

17. *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。
18. `[Mapping]` の下のホスト名が Data Node と一致しない場合は、それらのホスト名を更新します。
19. 3 つより多くの Data Node 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。
20. 更新した行をコピーし、`config.ini` ファイルに貼り付けます。
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。

## Data Store データベースをバックアップする

### はじめる前に

- 「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」の説明に従って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 `root` としてログインします。

### 手順

1. `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。
2. `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。次の選択肢があります。
   - バックアップテストに成功した場合は、Data Store をバックアップします。手順 2 に進みます。
   - 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。問題を解決できない場合は、シスコサポートにお問い合わせください。
3. `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。

# Data Store の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。

バックアップから Data Store を復元するには、次のことを確認する必要があります。

- Data Store が停止している。Flow Collector や マネージャ が接続されておらず、変更を行っていない場合のみ、Data Store を停止できます。
- ノード名およびノード数がバックアップと Data Store で同じである。

> シスコは、バックアップの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。

## Data Store を停止する

### はじめる前に

- Flow Collector が Data Store に接続されておらず、データを渡していないことを確認します。これを行うには、UDP Director からのトラフィックを停止します。
- マネージャ が Data Store に接続しておらず、Data Store をクエリまたは更新していないことを確認します。
- Data Node のコンソールに `root` としてログインします。

### 手順

1. `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。
2. - コマンドプロンプトで `/opt/vertica/bin/admintools -t stop_db -d sw -<password>` と入力して Enter を押し、Data Store を停止します。

## 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次のコマンドを実行することをお勧めします。
> `/opt/vertica/bin/vsql -U dbadmin -w <password> -c "select* from partitions;" >/lancope/var/tcpdump/partitions-full-DBbackup`

### はじめる前に

- `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。詳細については、「Data Store の dbadmin および readonlyuser のパスワードを初期化後に更新する」を参照してください。
- `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。

### 手順

1. `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。
2. 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。

## Data Store を起動する

### はじめる前に

- Data Node のコンソールに `root` としてログインします。

### 手順

1. `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。
2. コマンドプロンプトで `/opt/vertica/bin/admintools -t start_db -d sw -p <password>` と入力して Enter を押し、Data Store を起動します。

### 次の作業

- 次のセクションの説明に従って、catalog スナップショットを削除します。

## 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。

### はじめる前に

- Data Node のコンソールに `root` としてログインします。

### 手順

1. `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。
2. 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。

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

3. `[password]` を `dbadmin` のパスワードに置き換えます。
4. 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、`catalog` スナップショットを削除します。

### 次の作業

- Flow Collector を Data Store に再接続し、データを渡していることを確認します。
- マネージャを Data Store に再接続します。

# Data Store からの Data Node の削除

> 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 から Data Node を削除する場合は、次の点に注意してください。

- Data Store が実行されている必要があります。
- 先にバックアップを実行します。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。
- 耐障害性の設定のため、Data Store には少なくとも 3 つのノードが必要です。ノードを交換する場合の詳細については、「**別の IP アドレスを持つスペア Data Node への Data Node の交換**」を参照してください。

## Data Store からノードを削除する

### はじめる前に

- `root` として Data Node にログインします。

**手順**

1. `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。
2. 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。

   ```
   /opt/vertica/bin/admintools -t db_remove_node -d sw -s [data-node-hostname]
   ```

3. `[data-node-hostname]` を Data Store から削除する Data Node のホスト名に置き換えます。
4. 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、Data Node を削除します。これには時間がかかることがあります。

# 別の IP アドレスを持つスペア Data Node への Data Node の交換

> 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。

## 障害が発生した Data Node を交換するための Data Store の準備

- Data Store をバックアップします。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。
- スペア Data Node を Data Store に追加します。詳細については、「**Data Store のメンテナンス**」を参照してください。

## Data Node の交換

交換する Data Node で Vertica がまだ実行されている場合は、Vertica を停止します。その後、前の Data Node を新しい Data Node に交換し、必要な設定を新しい Data Node に配布します。前の Data Node を削除し、新しい Data Node を再起動します。

# Data Node での Vertica の停止

削除する Data Node で Vertica がまだ実行されている場合は、その Data Node で Vertica を停止します。その Data Node が停止しているか Vertica が実行されていない場合は、次の手順に進みます。

**はじめる前に**

- Data Node のコンソールに `root` としてログインします。

**手順**

1. `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。
2. 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。

   ```
   /opt/vertica/bin/admintools -t stop_host -s [node-ip-addresses]
   ```

3. `[node-ip-addresses]` を Data Store から削除する Data Node の `eth0` ルーティング可能 IP アドレスのカンマ区切りリストに置き換えます。

4. 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、その Data Node で Vertica を停止します。

## Data Node の交換

### はじめる前に

- Data Node のコンソールに `root` としてログインします。

### 手順

1. `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。
2. 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。

   `/opt/vertica/bin/admintools -t db_replace_node -d sw -o [old-data-node-hostname] -n [new-data-node-hostname]`

3. `[old-data-node-hostname]` を Data Store から削除する Data Node のホスト名に置き換えます。
4. `[new-data-node-hostname]` を代わりに Data Store に追加する Data Node のホスト名に置き換えます。
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、前の Data Node を新しい Data Node に交換します。
6. `/opt/vertica/bin/admintools -t distribute_config_files` 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、設定ファイルを新しい Data Node に配布します。
7. 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。

   `/opt/vertica/sbin/update_vertica --remove-hosts [old-data-node-hostname]`

8. `[old-data-node-hostname]` を Data Store から削除する Data Node のホスト名に置き換えます。
9. 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、前の Data Node を Data Store から削除します。
10. 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。

    `/opt/vertica/bin/admintools -t restart_node -s [new-data-node-hostname]`

11. `[new-data-node-hostname]` を代わりに Data Store に追加する Data Node のホスト名に置き換えます
12. 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、新しい Data Node を再起動します。

## 応答しない Data Node の交換

これらのタスクの計画と実装については、シスコサポートにお問い合わせください。

## Data Store の初期化後の マネージャ および Flow Collector の追加

Data Store を初期化した後に Manager または Flow Collector を展開に追加する場合は、それらを Data Store で使用するように設定し、Data Store とのセキュアな通信を設定する必要があります。その後、SystemConfig で、マネージャ または Flow Collector と Data Store の間のセキュアな通信を設定します。

## 既存のアプライアンスを Data Store で使用するために RFD を実行する

Data Store なしで使用するように設定された既存の Manager または Flow Collector があり、それらを Secure Network Analytics の展開に追加する場合は、最初にアプライアンスの RFD を実行してから、アプライアンスを Data Store 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。

**手順**

1. 『System Configuration Guide』の手順に従って、アプライアンスの RFD を実行します。

   > 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再設定する必要があります。

2. 「マネージャData Store で使用する設定」および「Data Store で使用する Flow Collector の設定」の手順に従って、マネージャ または Flow Collector を展開して Data Store で使用するように設定し、アプライアンス セットアップ ツールを使用します。
3. コマンドプロンプトで `SystemConfig` と入力して Enter を押し、システム構成ユーティリティにアクセスします。
4. **[データストア(Data Store)]** を選択します。
5. **[パスワードレスSSH(Passwordless SSH)]** を選択します。アプライアンスにおけるパスワードレス SSH が SystemConfig で有効になるまで数分待ちます。

   次に進む前に、Central Management ですべてのアプライアンスが稼働していることを確認します。

6. **[データストア(Data Store)]** メニューから、**[新しいマネージャとFlow Collectorの設定(Config new, Flow Collectors)]** を選択します。マネージャ または Flow Collector がシステムで認識されて追加されるまで数分待ちます。

   Central Management で、新しく追加したアプライアンスが稼働していることを確認します。

## Data Store とのセキュアな通信のために、新しい マネージャ または Flow Collector を設定します

展開していない新しい Manager または Flow Collector がある場合は、Data Store で使用するようにアプライアンスを設定し、展開に追加します。

**手順**

1. 「マネージャData Store で使用する設定」および「Data Store で使用する Flow Collector の設定」の手順に従って、マネージャ または Flow Collector を展開して Data Store で使用するように設定し、アプライアンス セットアップ ツールを使用します。
2. プライマリ マネージャ 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 `SystemConfig` と入力して Enter を押し、システム構成ユーティリティにアクセスします。
4. **[データストア(Data Store)]** を選択します。
5. **[パスワードレスSSH(Passwordless SSH)]** を選択します。アプライアンスにおけるパスワードレス SSH が SystemConfig で有効になるまで数分待ちます。

   次に進む前に、Central Management ですべてのアプライアンスが稼働していることを確認します。
6. **[データストア(Data Store)]** メニューから、**[新しいマネージャとFlow Collectorの設定(Config new, Flow Collectors)]** を選択します。マネージャ または Flow Collector がシステムで認識されて追加されるまで数分待ちます。

   Central Management で、新しく追加したアプライアンスが稼働していることを確認します。

フェールオーバー マネージャ への データストア 信頼情報のコピー

## Data Store でのデータ圧縮の有効化

1. データ圧縮は、Flow Collector と Data Store の間の帯域幅使用量を削減するために使用できるオプションです。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。データ圧縮はデフォルトで無効になっています。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。
2. Flow Collector インターフェイスにログインします。
3. **[サポート(Support)]** > **[詳細設定(Advanced Settings)]** の順にクリックします。
4. 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します。
   - 0:データ圧縮を無効にします。
4. **[適用(Apply)]** をクリックし、表示される情報ウィンドウで **[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 の導入のトラブルシューティング

## 仮想アプライアンスの導入のトラブルシューティング

マネージャ Virtual Edition または Flow Collector Virtual Edition の導入と設定に関する問題の詳細については、『Cisco Secure Network AnalyticsVirtual Edition (with Data Store) Appliance Installation Guide』を参照してください。

Data Node Virtual Edition の 2 つのネットワークアダプタを割り当てないと、初回セットアップの開始時に、初回セットアップで 2 番目のネットワークアダプタを検出できないために解決に失敗します。この場合、Data Node 間の通信に使用するルーティング不可の IP アドレスを割り当てることができなくなります。

## 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。少なくとも、合計容量の 60% はフロー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 Data Node 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 Data Node 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 Data Node から取得し、残りの Data Node と同じ状態にする必要があります。

この場合、Data Node にログインし、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。

**はじめる前に**

- Data Node の CLI に root としてログインします。

**手順**

1. 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
   ```

2. *[node_name]* を Data Node の名前（`node0001` など）に置き換えます。
3. 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、`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。
4. 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
   ```

5. *[data-node-ip-address]* を該当する Data Node の IP アドレスに置き換えます。

6. *[dbadmin-password]* を Data Store の `dbadmin` のパスワードに置き換えます。
7. 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。
8. 「`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。

**次の作業**

- 「Data Store の導入の要件と考慮事項」で、Data Node への電力の供給に関するシスコの推奨事項を確認します。

## Data Store が電源障害後に起動しない

複数の Data Node の電源が予期せずに失われ、Data Store データベースが停止した場合、該当する Data Node の電源が回復した後にデータベースが自動的に再起動しないことがあります。

この場合、すべての Data Node で SSH が有効になっていることを Central Management で確認します。その後、Data Node にログインし、Data Store データベースを強制的に再起動します。

**はじめる前に**

- Data Node のコンソールに `root` としてログインします。

**手順**

1. `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。
2. コマンドプロンプトで `/opt/vertica/bin/admintools -t start_db -d sw` と入力して Enter を押し、Data Store を起動します。

   > Data Store データベースの再起動を試行したときに、SSH で到達できなかった Data Node がコンソールで報告される場合は、それらの Data Node の SSH を有効にしてから、この手順をもう一度試してください。

# 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

# 著作権情報



このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。