

# Cisco Stealthwatch

Data Store 仮想エディション導入および構成ガイド 7.3.2



---

# 目次

<b>Data Store の設置と構成の概要</b> .....	<b>4</b>
概要 .....	4
対象読者 .....	4
このマニュアルの使い方 .....	4
<b>Data Store の概念とアーキテクチャ</b> .....	<b>6</b>
<b>Data Store の導入の前提条件と推奨事項</b> .....	<b>11</b>
Stealthwatch バージョン サポート .....	11
Stealthwatch ライセンス .....	11
Stealthwatch 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 .....	11
Stealthwatch Management Console VE .....	11
Flow Collector VE .....	12
Data Node VE .....	12
Data Store の導入に必要なログイン情報 .....	13
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 .....	14
Data Store の導入の要件と考慮事項 .....	16
Data Store 通信ポート .....	17
<b>Stealthwatch と Data Store の導入の概要</b> .....	<b>19</b>
<b>Data Store の設置</b> .....	<b>20</b>
Stealthwatch 仮想アプライアンスの導入と考慮事項 .....	20
Data Store で使用する SMC の設定 .....	20
Data Store の初期導入と設定 .....	21
Data Store で使用する Flow Collector の設定 .....	22
Data Store の初期化と設定 .....	23
UDP Director (オプション) の導入 .....	26
Flow Sensor (オプション) の導入 .....	26
フェールオーバー Stealthwatch Management Console (オプション) の導入 .....	26
<b>フローインターフェイス統計の保持設定</b> .....	<b>27</b>
<b>Data Store のインストールの次のステップ</b> .....	<b>32</b>
<b>Data Store のメンテナンス</b> .....	<b>33</b>
Data Node の再起動 .....	33
Data Store の再起動 .....	34
Data Store のバックアップの作成 .....	34
Data Store のバックアップの復元 .....	39

---

Data Store からの Data Node の削除 .....	41
別の IP アドレスを持つスペア Data Node への Data Node の交換 .....	42
障害が発生した Data Node を交換するための Data Store の準備 .....	42
Data Node の交換 .....	42
Data Store の初期化後の SMC および Flow Collector の追加 .....	44
<b>Data Store の導入のトラブルシューティング .....</b>	<b>46</b>
仮想アプライアンスの導入のトラブルシューティング .....	46
Data Store トラブルシューティング .....	46

# Data Store の設置と構成の概要

## 概要

このガイドでは、Stealthwatch システムの導入の一環として Stealthwatch Data Store を設置する方法について説明します。Stealthwatch システム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](#)
- [このマニュアルの使い方](#)

## 対象読者

このガイドは、Stealthwatch 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 (Flow Collector および 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。

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

## このマニュアルの使い方

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
<a href="#">Data Store の概念とアーキテクチャ</a>	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、SMC や Flow Collector と関連付けて説明します。
<a href="#">Data Store の導入の前提条件と推奨事項</a>	Data Store と互換性がある Stealthwatch 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。
<a href="#">Stealthwatch と Data Store の導入の概要</a>	Data Store で使用する Stealthwatch 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。
<a href="#">Data Store の設置</a>	Data Store で使用する Stealthwatch 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。
<a href="#">フローインターフェイス統計の保持設定</a>	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。

---

章	説明
<a href="#">Data Store のインストールの次のステップ</a>	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。
<a href="#">Data Store のメンテナンス</a>	Data Store のメンテナンスタスクについて説明します。
<a href="#">Data Store の導入のトラブルシューティング</a>	Data Store の導入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

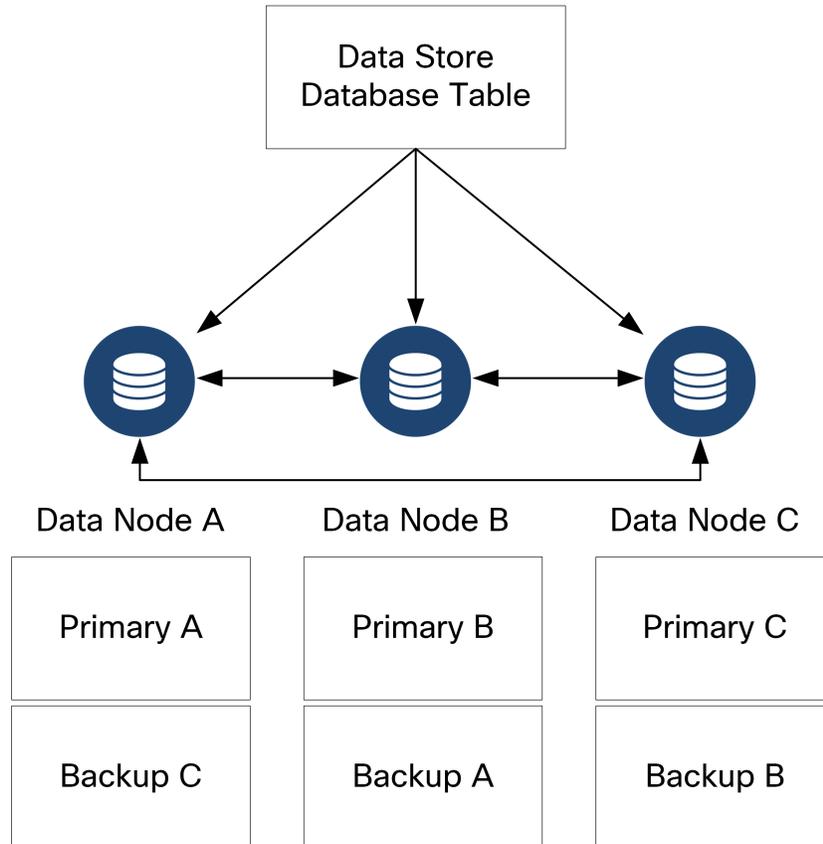
Stealthwatch Data Store は、Stealthwatch Flow Collector によって収集されたネットワークのテレメトリを保存する中央リポジトリを提供します。Data Store は、Data Node のクラスタで構成されます。各クラスタには、データの一部と個別 Data Node のデータのバックアップが含まれます。すべてのデータが 1 つの集中型データベースに存在し、複数の Flow Collector に分散されていないため、Stealthwatch Management Console はすべての Flow Collector に個別にクエリする場合よりも 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。

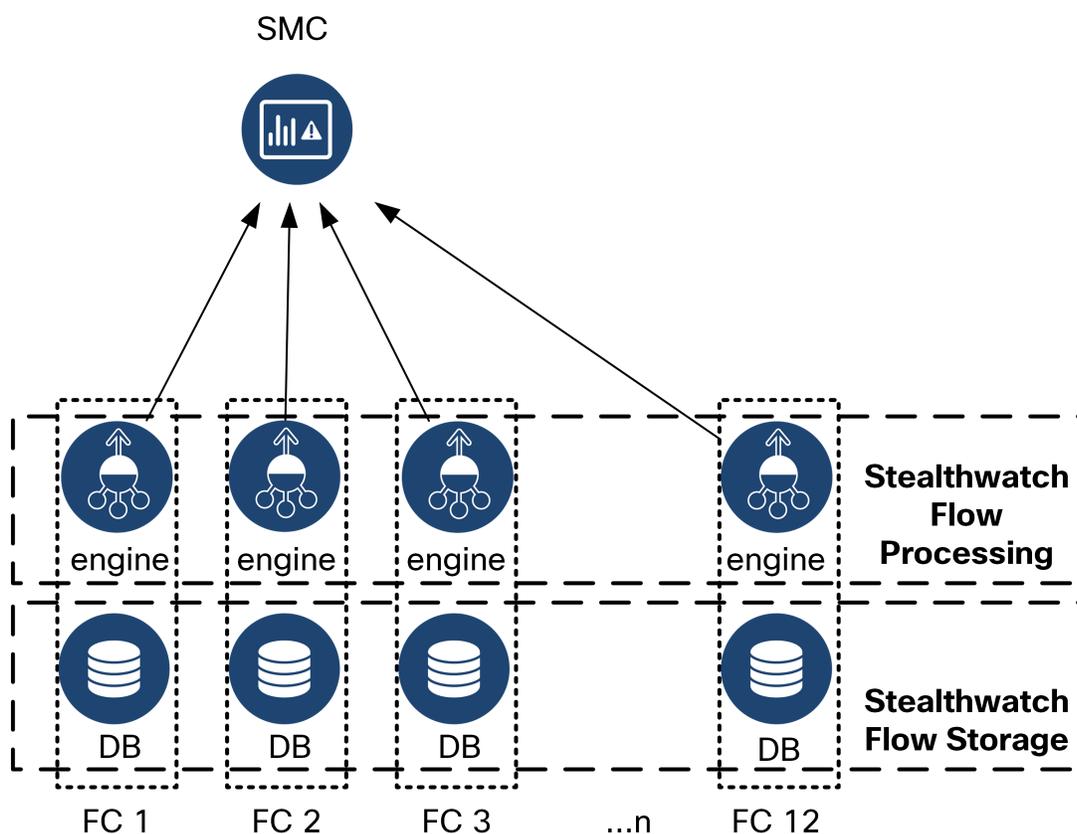
- ロードバランシングに役立ちます。
- 各ノードに処理が分散されます。
- Data Store に取り込まれたすべてのデータのバックアップが保持され、耐障害性が確保されます。
- Data Node の数を増やすことで、全体的なストレージとクエリのパフォーマンスを向上させることができます。

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。

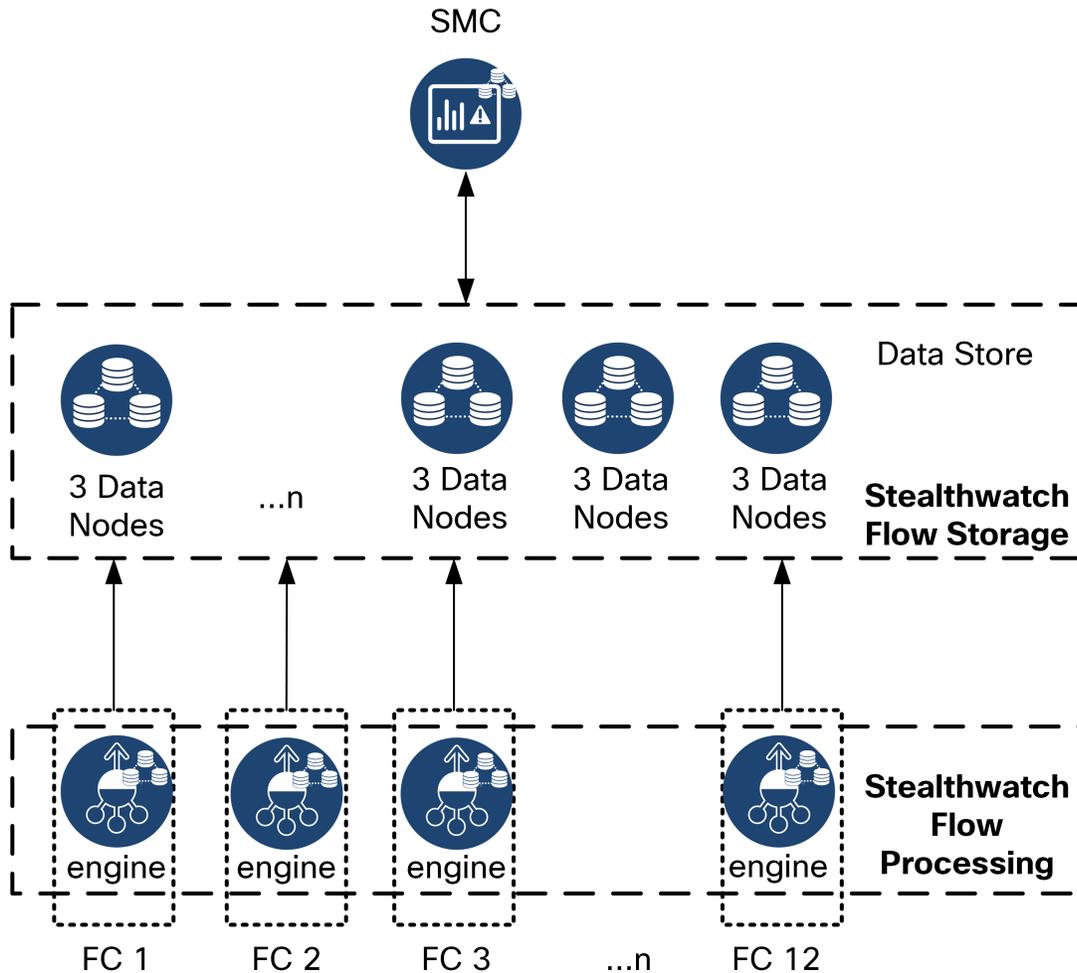


## Stealthwatch Data Store の導入アーキテクチャ

Data Store なしの Stealthwatch の展開では、1つ以上の Flow Collector がデータを取り込んで重複排除し、分析を実行し、データと結果を SMC に直接レポートします。グラフやチャートを含むユーザが送信したクエリを解決するために、SMC 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 SMC に返します。SMC 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 Stealthwatch 展開では、Data Store クラスターは SMC と Flow Collector の間に配置されます。1 つ以上の Flow Collector 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 Data Node にほぼ均等に分散させます。Data Store は、Data Storage 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が送信したクエリを解決するために、SMC 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 SMC に返します。SMC 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。

## Stealthwatch Enterprise の導入の考慮事項

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。ストレージ統計情報をモニタする場合は、レポートビルダーアプリを SMC にダウンロードします。
- データストアを展開する場合は、Stealthwatch Web アプリケーションを使用して Stealthwatch インストールをモニタおよび設定します。Stealthwatch 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 SMC 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 のアーキテクチャでは、SMC 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 SMC、および仮想 Flow Collector とともに展開できます。ハードウェア Data Store で仮想アプライアンスを導入することはできません。また、仮想 Data Store でハードウェアアプライアンスを導入することもできません。

## Stealthwatch Data Store アーキテクチャ

各 Data Store は 3 つの Data Node で構成されます。

仮想 Data Store を購入すると、3 つの Data Node 仮想エディション (VE) を展開できます。

Data Store を展開するには、それぞれの Data Node について以下を割り当てる必要があります。

- Stealthwatch 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。

## Stealthwatch バージョン サポート

Stealthwatch を Data Store とともに導入する場合、Stealthwatch のすべてのアプライアンスが同じバージョン (7.3.x) である必要があります。使用可能な 7.3.x の最新バージョンは 7.3.2 です。

## Stealthwatch ライセンス

Stealthwatch 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。

SMC VE を導入する場合は、[software.cisco.com](https://software.cisco.com) でアカウントを登録すると、SMC VE のライセンスが付与されます。

## Stealthwatch 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 Stealthwatch 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
Data Store	<ul style="list-style-type: none"> <li>3 つの Data Node VE まで</li> </ul>
Stealthwatch Management Console	<ul style="list-style-type: none"> <li>1 つ以上の Stealthwatch Management Console VE</li> </ul>
Flow Collector	<ul style="list-style-type: none"> <li>1 つ以上の Flow Collector VE</li> </ul>

v7.3.1 または v7.3.2 では、Data Store は Flow Sensor および UDP Director をサポートしています。Data Store を使用する場合は、どちらも展開する必要はありません。アプライアンスをクラスターに追加する場合は、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。

## Stealthwatch Management Console VE

Stealthwatch Management Console 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	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、モニタする見込みのホストとエクスポート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	エクスポート	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。

$$[(\text{日時平均 FPS} / 1,000) \times 1.6 \times \text{日数}] / \text{Data Node 数}$$

- 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 Data Node 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。

$[(50,000/1,000) \times 1.6 \times 90] / 3 = \text{Data Node あたり } 2,400 \text{ GB (2.4 TB)}$   
Data Node

- 日時平均 FPS = 50,000
- 日時平均 50,000 FPS / 1,000 = 50
- $50 \times 1.6 \text{ GB} = 1 \text{ 日あたりのストレージ相当量 } 80 \text{ GB}$
- Data Store あたり 80 GB X 90 日 = Data Store あたり 7,200 GB
- $7,200 \text{ GB} / 3 \text{ Data Node} = \text{Data Node あたり } 2,400 \text{ GB (2.4 TB)}$

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 50,000	Data Node VE あたり 32 GB	Data Node VE あたり 6	<ul style="list-style-type: none"> <li>• Data Node あたり 800 GB Data Node</li> <li>• 3 つの Data Node で合計 2.4 TB</li> </ul>
最大 120,000	Data Node VE あたり 32 GB	Data Node VE あたり 12	<ul style="list-style-type: none"> <li>• Data Node あたり 1.92 TB</li> <li>• 3 つの Data Node で合計 5.76 TB</li> </ul>
最大 220,000	Data Node VE あたり 64 GB	Data Node VE あたり 16	<ul style="list-style-type: none"> <li>• Data Node あたり 3.52 TB</li> <li>• 3 つの Data Node で合計 10.56 TB</li> </ul>

## Data Store の導入に必要なログイン情報

次のユーザアカウントのパスワードを準備します。

- それぞれの SMC、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 SMC、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、Stealthwatch 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	<p>各 Data Node、Stealthwatch Management Console、および Flow Collector の場合：</p> <ul style="list-style-type: none"> <li>初期システム設定時に設定: <code>root</code>、<code>sysadmin</code></li> <li>アプライアンス設定ツールを使用して設定: <code>admin</code></li> </ul> <p>Data Store の初期化時に設定: <code>dbadmin</code>、<code>readonlyuser</code></p>
Data Node 間通信	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
Stealthwatch アプライアンス通信	<ul style="list-style-type: none"> <li>SMC、Data Node、Flow Collector に必要で、SMC から設定される SSH および SSH ルートアクセス</li> <li>SMC と Flow Collector は、すべての Data Node に到達できる必要があります。</li> <li>Data Node は、SMC、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。</li> </ul>

全 Stealthwatch 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。

**i** 現在、Data Store では、プライマリ Data Node が停止した場合の自動交換としてのスベア Data Node の導入はサポートされていません。ガイダンスについては、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。

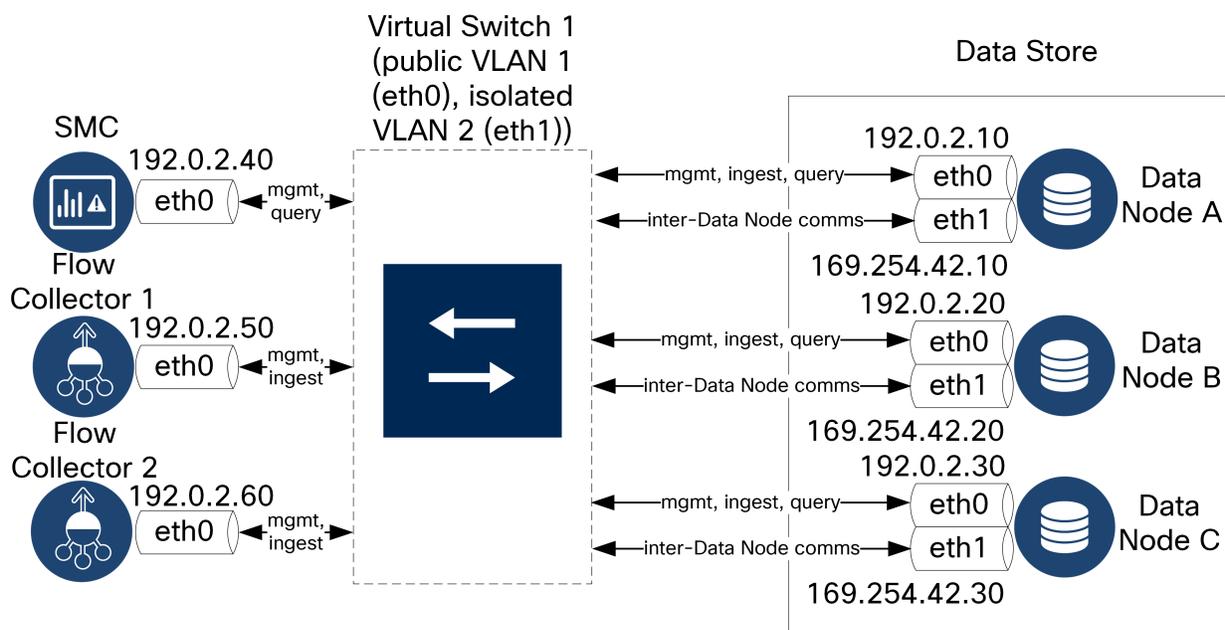
- Stealthwatch アプライアンスとの通信に使用するルーティング可能な IP アドレス (`eth0`)。

Data Store の展開と設定においては、Data Node `eth0` IP アドレスを Data Store の名前にはマッピングして、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。

**i** 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 間の通信専用になります。また、Data Node の SMC 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。

**i** 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、SMC、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 SMC 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 Node VE 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。

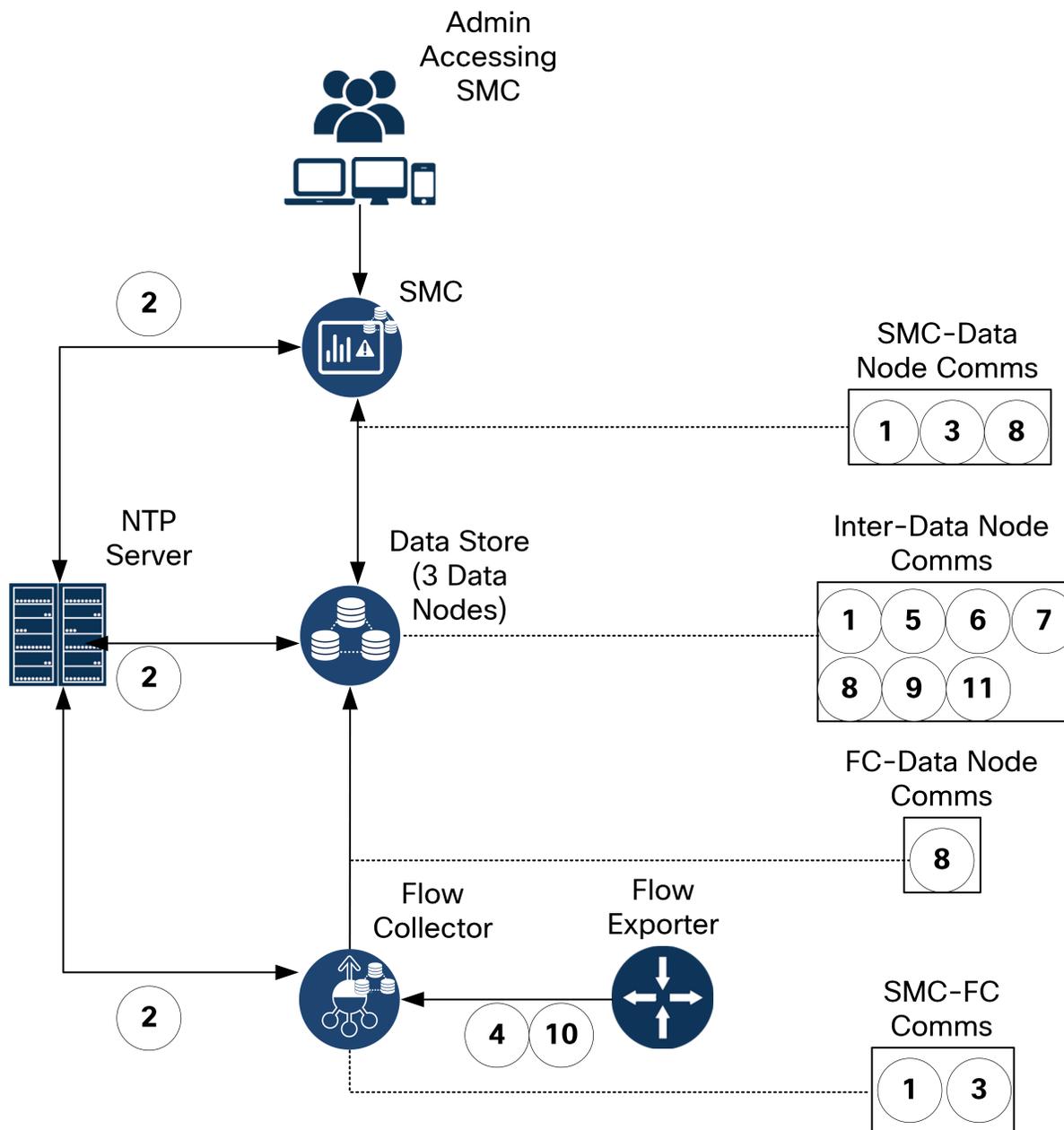
電力の喪失やハードウェアの障害が原因で Data Store が停止すると、データ破損やデータ損失のリスクが高くなります。Data Node の導入は、常時稼働の状態で行うよう考慮をお勧めします。



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、Stealthwatch のアーキテクチャと開く必要がある通信ポートの例を示します。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 Stealthwatch の展開全体で開く通信ポートについては、『[Stealthwatch 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)	ポート	プロトコルまたは目的

1	SMC	Flow Collector および Data Node	22/TCP	SSH (Data Store データベースの初期化に必要)
1	Data Node	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	SMC、Flow Collector、および Data Node	NTP サーバ	123/UDP	NTP (時刻同期に必要)
2	NTP サーバ	SMC、Flow Collector、および Data Node	123/UDP	NTP (時刻同期に必要)
3	SMC	Flow Collector および 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	SMC	443/TCP	HTTPS (アプライアンス間のセキュア通信に必要)
3	Data Node	SMC	443/TCP	HTTPS (アプライアンス間のセキュア通信に必要)
4	NetFlow エクスポート	Flow Collector: NetFlow	2055/UDP	NetFlow の取り込み
5	Data Node	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	Data Node	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	Data Node	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	SMC、Flow Collector、および Data Node	Data Node	5433/TCP	Vertica クライアント接続
9	Data Node	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リング
10	sFlow エクスポート	Flow Collector: sFlow	6343/UDP	sFlow の取り込み
11	Data Node	他のすべての Data Node	6543/UDP	Data Node 間メッセージングサービス

# Stealthwatch と Data Store の導入の概要

次に、Stealthwatch 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 SMC の設定](#) : SMC 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 Stealthwatch 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 Stealthwatch Management Console \(オプション\) の導入](#)

## Data Store の設置

- i** Stealthwatch Data Store の購入を計画している場合は、Cisco プロフェッショナル サービスに連絡し、全体的な Stealthwatch 導入の範囲内および導入の一環として、配置、導入、および設定の支援を受けてください。詳細については、シスコサポートまでお問い合わせください。

### Stealthwatch 仮想アプライアンスの導入と考慮事項

SMC、Data Node、および Flow Collector の各 Stealthwatch 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。SMC、Data Node、および Flow Collector は同じバージョン(7.3.2)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、『[Stealthwatch Virtual Edition \(with Data Store\) Installation Guide v7.3.2](#)』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、『[Stealthwatch System Configuration Guide v7.3.2](#)』を参照してください。

SMC および Flow Collector の初回セットアップでの設定時は、Security Analytics and Logging (オンプレミス)を有効にするオプションもあります。Security Analytics and Logging (オンプレミス)を有効にする場合は、Stealthwatch の展開を使用して Firepower イベント情報を保存します。また、SMC 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。

- i** Data Store を導入する場合は、Stealthwatch Web アプリケーションを使用して Stealthwatch インストールをモニタおよび設定します。Stealthwatch 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 SMC の設定

Data Store で Data Node と Flow Collector の管理に使用する SMC を展開して設定します。

- i** Data Store と連携するセカンダリ SMC 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 Stealthwatch Management Console \(オプション\) の導入](#)」を参照してください。

次の手順を実行します。

- 最初に、SMC 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 Security Analytics and Logging (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 ユーザと sysadmin ユーザ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、『[Stealthwatch Virtual Edition \(with Data Store\) Installation Guide v7.3.2](#)』を参照してください。

Security Analytics and Logging(オンプレミス)を有効にする場合は、Stealthwatch の展開を使用して Firepower イベント情報を保存します。また、SMC 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。

 SMC または Flow Collector を Data Store および Security Analytics and Logging(オンプレミス) で使用するよう設定した後に、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。この設定は、ネットワークに Data Store を導入する場合にのみ有効にしてください。

- 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 ユーザと sysadmin ユーザのパスワード)の割り当て、Stealthwatch 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、SMC 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、『[Stealthwatch System Configuration Guide](#)』を参照してください。
- 最後に、SMC 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。

SMC 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

SMC 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 Node VE 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、『[Stealthwatch Virtual Edition \(with Data Store\) Installation Guide v7.3.2](#)』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、次の手順を実行します。

- 最初に、Data Node をネットワークに展開します。Data Node VE 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 ユーザと sysadmin ユーザ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、『[Stealthwatch Virtual Edition \(with Data Store\) Installation Guide v7.3.2](#)』を参照してください。

**i** 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。

- 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 ユーザと sysadmin ユーザのパスワード)の割り当て、Stealthwatch 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、Data Node 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、『[Stealthwatch System Configuration Guide](#)』を参照してください。
- 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。

**i** 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。Data Node の更新プロセスでは、Stealthwatch 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。

- 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

Data Node と UDP Director (展開した場合) の設定が完了したら、Flow Collector を展開して設定します。

各 Flow Collector について、次の手順を実行します。

- 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 Security Analytics and Logging (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 ユーザと sysadmin ユーザ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、『[Stealthwatch Virtual Edition \(with Data Store\) Installation Guide v7.3.2](#)』を参照してください。

Security Analytics and Logging (オンプレミス) を有効にする場合は、Stealthwatch の展開を使用して Firepower イベント情報を保存します。また、SMC 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。

**i** 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。

 SMC または Flow Collector を Data Store および Security Analytics and Logging (オンプレミス) で使用するよう設定した後に、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。この設定は、ネットワークに Data Store を導入する場合にのみ有効にしてください。

- 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 ユーザと sysadmin ユーザのパスワード) の割り当て、Stealthwatch 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、『[Stealthwatch System Configuration Guide](#)』を参照してください。

 Data Store で使用するよう 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。ストレージ統計情報をモニタする場合は、レポートビルダーアプリを SMC にダウンロードします。

- 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。

- 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

SMC、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 SMC、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。

- 最初に、Central Management で、必要なアプライアンスが SMC 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 SMC (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 SMC 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 SMC 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 SMC 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、SMC から `SystemConfig` を使用して、SMC、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。

## Stealthwatch 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

- SMC 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 SMC、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 間の通信が設定されます。
- 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。これで、Data Store を含む Stealthwatch の導入は完了です。

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。これで、Data Store を含む Stealthwatch の導入は完了です。

## 次の作業

- UDP Director、Flow Sensor、またはセカンダリ SMC 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 SMC がある場合は、以降のセクションの説明に従って展開します。

## UDP Director(オプション)の導入

UDP Director を導入する場合は、『[Stealthwatch Virtual Edition \(with Data Store\) Appliance Installation Guide](#)』および『[Stealthwatch 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 を導入するかどうかに関係なく同じになります。UDP Director を Data Store で使用するための設定は必要ありません。

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 SMC を設定するか、「[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 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 を導入する場合は、『[Stealthwatch Virtual Edition \(with Data Store\) Appliance Installation Guide](#)』および『[Stealthwatch 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。Flow Sensor を Data Store で使用するための設定は必要ありません。

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 SMC をフェールオーバー SMC 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 Stealthwatch Management Console(オプション)の導入

フェールオーバー SMC として設定するセカンダリ SMC がある場合は、『[Stealthwatch Virtual Edition \(with Data Store\) Appliance Installation Guide](#)』、『[Stealthwatch System Configuration Guide](#)』、および『[Stealthwatch Failover Configuration Guide](#)』の手順に従います。

セカンダリ SMC の設定が完了し、Central Management でプライマリ SMC 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、複数のエクスポートや同じエクスポート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、Stealthwatch 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 Stealthwatch 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。

### SMC 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	<code>https://[smc-eth0-ip]/token/v2/authenticate</code>
説明	SMC の REST API に対して認証を行います。

リソース	説明
URI パラメータ	<ul style="list-style-type: none"> <li><code>[smc-eth0-ip]</code>: SMC の eth0 管理 IP アドレス</li> </ul>
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	<ul style="list-style-type: none"> <li><code>[username]</code>: (必須) SMC の admin ユーザ</li> <li><code>[password]</code>: (必須) SMC の admin ユーザアカウントのパスワード</li> </ul>

#### 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	<ul style="list-style-type: none"> <li><code>[smc-eth0-ip]</code>: SMC の eth0 管理 IP アドレス</li> </ul>
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	<code>https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings</code>
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	<ul style="list-style-type: none"> <li><code>[smc-eth0-ip]</code>: SMC の eth0 管理 IP アドレス</li> </ul>
HTTP メソッド	PUT
要求本文 MIME タイプ	application/json
要求本文	<pre>{   "interfaceRetentionType": "[type]",   "interfaceRetentionAmount": "[#]" }</pre>
要求本文パラメータ	<ul style="list-style-type: none"> <li><code>[type]</code>: (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。 <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> </li> <li><code>[#]</code>: (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。</li> </ul>

リソース	説明
	<div style="border: 1px solid #00a0e3; padding: 10px;"> <p><b>i</b> <code>interfaceRetentionType</code> を <code>FOREVER</code> に設定する場合も、<code>interfaceRetentionAmount</code> を渡す必要があります。この値は無視されます。この場合、<code>interfaceRetentionAmount</code> 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。</p> </div>

### 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、[Stealthwatch Enterprise 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 SMC の admin ユーザのユーザ名に置き換えます。
3. `[password]` を SMC の admin ユーザのパスワードに置き換えます。
4. `[smc-eth0-ip]` を SMC 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、SMC 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 SMC 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 "Content-Type:application/json" -d '{"interfaceRetentionType": "[type]", "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. `[#]` を 1-3000 の範囲の保持日数を示す整数に置き換えます。
- 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。
12. `[smc-eth0-ip]` を SMC の `eth0` IP アドレスに置き換えます。
13. 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 Stealthwatch 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

Stealthwatch を展開して Data Store で使用するよう設定したら、以下を行います。

- **レポートビルダーアプリケーション**: Stealthwatch レポートビルダー アプリケーションを SMC にインストールして、Stealthwatch 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**: Stealthwatch の使用方法については、Stealthwatch Web アプリケーションのオンラインヘルプを参照してください。

# 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 および Data Store の再起動
- Data Store 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 SMC および Flow Collector の追加

**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。

## Data Node の再起動

**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。

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

始める前に

- 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 -s [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。
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

**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。

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

- 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。
- SMC が Data Store に接続されておらず、Data Store のクエリや更新を行っ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 -d sw` 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 -d sw -F` と入力して Enter を押し、Flow Collector や SMC 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

**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。

Data Store をバックアップするには、次の手順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

**i** Stealthwatch 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、`vsq1` 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/vs1 -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。

**i** Stealthwatch 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 `python --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、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。

- 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

- su - dbadmin と入力して Enter を押し、以降のコマンドを dbadmin ユーザとして実行します。
- 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]
- [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。
- 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。
- cd /home/dbadmin と入力して Enter を押し、ディレクトリを変更します。
- mkdir backups と入力して Enter を押し、backups ディレクトリを作成します。
- 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。
- 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。

- 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]
```

- [dbadmin-password] を Data Store dbadmin のパスワードに更新します。
- 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。
- 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. 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. `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。
17. `[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。
18. 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。
19. 更新した行をコピーし、`config.ini` ファイルに貼り付けます。
20. 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。
21. `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 SMC 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。

## 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。
- SMC が Data Store に接続されておらず、Data Store のクエリや更新を行っ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 -d sw` 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 -d sw -F` と入力して Enter を押し、Flow Collector や SMC の接続を無効にして Data Store を停止します。

## バックアップから Data Store を復元する

### 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、「[Update the Data Store dbadmin and readonlyuser passwords after initialization](#)」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-file.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。

### 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。
- SMC 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

- Data Node 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。
- Data Store にスペア Data Node を追加します。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 Vertica を停止する

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 を交換する

### 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。

## Data Store の初期化後の SMC および Flow Collector の追加

Data Store を初期化した後に SMC 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、SMC 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 SMC または Flow Collector があり、それらを Stealthwatch 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. 「[Data Store で使用する SMC の設定](#)」および「[Data Store で使用する Flow Collector の設定](#)」の手順に従って、SMC 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SMCとFCの設定(Config new SMC, FCs)] を選択します。SMC 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。

## 新しい SMC または Flow Collector を Data Store で使用するセキュアな通信用に設定する

展開していない新しい SMC または Flow Collector がある場合は、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します。

### 手順

1. 「[Data Store で使用する SMC の設定](#)」および「[Data Store で使用する Flow Collector の設定](#)」の手順に従って、SMC または Flow Collector を展開して Data Store で使用するよう設定し、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 SMC 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SMCとFCの設定(Config new SMC, FCs)]を選択します。SMC 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 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

SMC VE または Flow Collector VE の導入と設定に関する問題の詳細については、『[Stealthwatch Virtual Edition \(with Data Store\) Appliance Installation Guide](#)』を参照してください。

Data Node VE 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 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ます。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 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。

---

# 著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL: <https://www.cisco.com/go/trademarks> をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)

