Cisco Secure Network Analytics

Data Store Virtual Edition 導入の概要 7.4.0

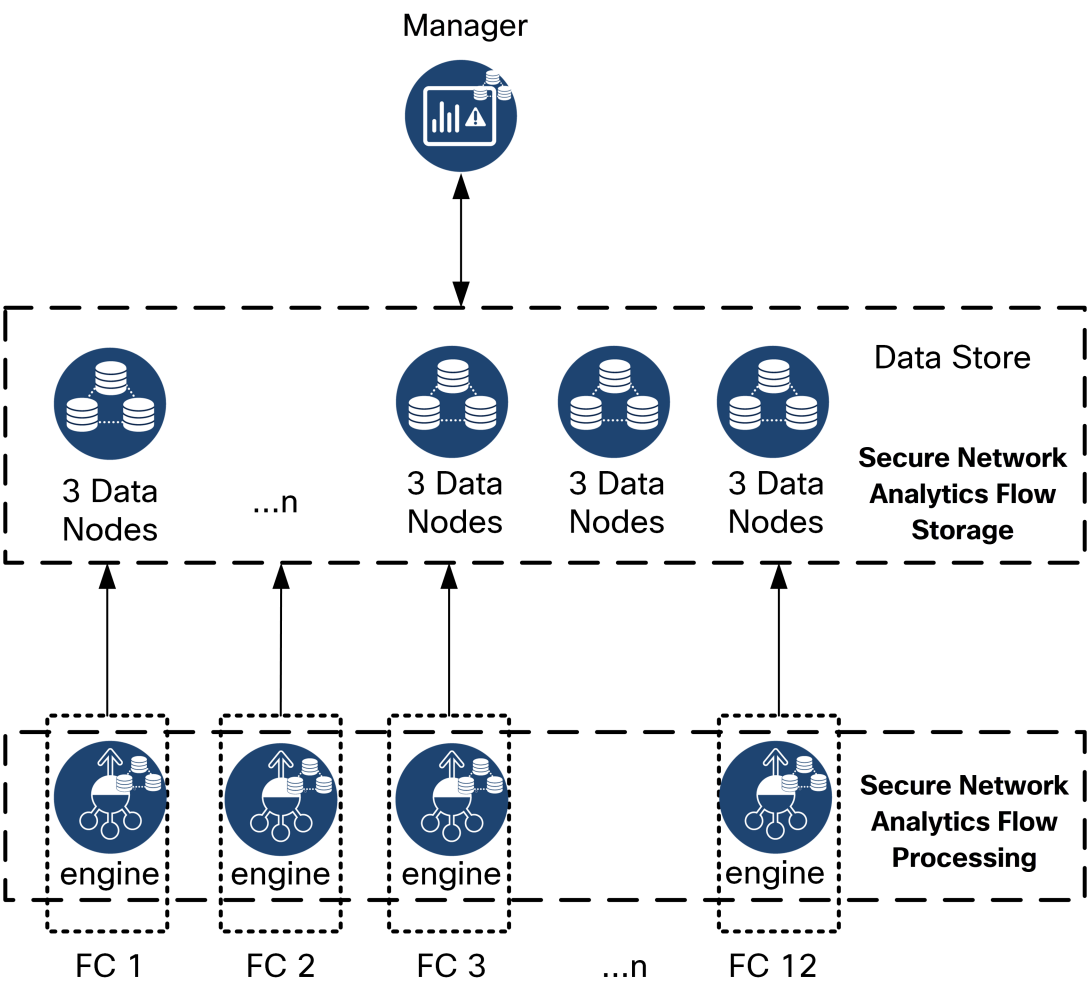
目次

Cisco Secure Network Analytics Data Store の概要

概要

Cisco Secure Network Analytics（旧 Stealthwatch）Data Store は、Secure Network Analytics 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（旧 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 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。



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。 • 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。 • 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』 および『Data Store Hardware Deployment and Configuration Guide』	各 Data Node を展開して構成します。 「**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。 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。 • 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。 • 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。 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』 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)。 1. マネージャ VE 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。 3. Flow Collector VE 4. Data Store を初期化します。 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。 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。 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。

Secure Network Analytics Data Store 仮想アプライアンスの前提条件

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
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、v7.4 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。

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。

Data Store 仮想アプライアンスのパフォーマンスとサイジング

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、予想される同時使用ユーザーの数を決める必要があります。

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。Analytics の詳細については、『Cisco Secure Network Analytics Analytics Beta Guide』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。

1 つのクラスターに最大 3 つの Data Node VE を展開できます。

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	• Data Node あたり 800 GB • 3 つの Data Node で合計 2.4 TB
最大 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 • 3 つの Data Node で合計 5.76 TB
最大 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 • 3 つの Data Node で合計 10.56 TB

Secure Network Analytics Data Store のネットワークとスイッチングに関する考慮事項

次の表に、Data Store の導入に関するネットワーキングとスイッチングの前提条件と考慮事項を示します。

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： • 初期システム設定時に設定：`root`、`sysadmin` • アプライアンス設定ツールを使用して設定：`admin` 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。 • 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 • 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 • 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

Data Store のインストールの次のステップ

このガイドを確認した後の手順：

- 現在の Secure Network Analytics Enterprise バージョンの詳細については、『Cisco Secure Network Analytics リリースノート』を参照してください。
- Data Store の導入の詳細については、『Data Store Virtual Edition の導入および設定ガイド』を参照してください。

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。