Cisco Stealthwatch

Data Store ハードウェア導入および構成ガイド 7.3.2

目次

Data Store の設置と構成の概要 **5**
概要 5
対象読者 5
このマニュアルの使い方 5
Data Store の概念とアーキテクチャ **7**
Data Store の導入の前提条件と推奨事項 **12**
Stealthwatch バージョン サポート 12
Stealthwatch ライセンス 12
Stealthwatch ハードウェアの互換性とネットワーキングの要件 12
Stealthwatch Management Console VE 13
Data Store 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 18
Data Store 通信ポート 19
Stealthwatch と Data Store の導入の概要 **21**
Data Store の設置 **22**
Stealthwatch ハードウェアの導入と考慮事項 22
Data Store で使用する SMC の設定 22
Data Store の初期導入と設定 23
Data Store で使用する Flow Collector の設定 24
Data Store の初期化と設定 25
UDP Director（オプション）の導入 28
Flow Sensor（オプション）の導入 28
フェールオーバー Stealthwatch Management Console（オプション）の導入 28
フローインターフェイス統計の保持設定 **29**
Data Store のインストールの次のステップ **34**
Data Store のメンテナンス **35**
Data Node の再起動 35
Data Store の再起動 36
Data Store のバックアップの作成 36
Data Store のバックアップの復元 41
Data Store への 3 つの Data Node の追加 43
Data Node の追加と再調整のための Data Store の準備 43

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Data Store への Data Node の追加 44
Data Store からの Data Node の削除 45
別の IP アドレスを持つスペア Data Node への Data Node の交換 45
障害が発生した Data Node を交換するための Data Store の準備 46
Data Node の交換 46
Data Store の初期化後の SMC および Flow Collector の追加 47
Data Store の導入のトラブルシューティング 49
ハードウェアの導入のトラブルシューティング 49
Data Store トラブルシューティング 49
付録 A. 設置の準備 51
設置に関する警告 51
設置に関するガイドライン 53
安全に関する推奨事項 54
電気製品を扱う場合の注意 54
静電破壊の防止 55
設置場所の環境 55
電源モジュールに関する考慮事項 55
ラックの構成に関する考慮事項 56
付録 B. Stealthwatch ハードウェアの設置 57
アプライアンスのマウント 57
アプライアンスに付属するハードウェア 57
追加で必要なハードウェア 57
ネットワークへのアプライアンスの接続 58
アプライアンスへの接続 59
キーボードとモニタを使用した接続 59
ラップトップを使用した接続 59
初回セットアップを使用したネットワークの設定 60
一般的な Stealthwatch アプライアンスの設定 61
Data Store と互換性のあるアプライアンス（SMC 2210、FC 4210） 62
Data Node 設定 66
sysadmin ユーザパスワードの変更 69
ルートユーザパスワードの変更 69
付録 C. アプライアンスの設定 71
アプライアンス設定ツールの要件 71
管理対象 71

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

SMC フェールオーバー 71
ベストプラクティス 71
設定の順序 72
1. ログイン 73
2. アプライアンスの設定 73
3. Stealthwatch Management Console の登録 75
4. Central Management へのアプライアンスの追加 75
5. アプライアンス ステータスの確認 76

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 システムハードウェアの設置を担当する方を対象にしています。ハードウェアネットワーク機器（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
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、SMC 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 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。
Stealthwatch と Data Store の導入の概要	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。
Data Store の設置	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。
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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

章	説明
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。
付録 A. 設置の準備	ハードウェアの設置に関する警告の情報を提供します。
付録 B. Stealthwatch ハードウェアの設置	Stealthwatch アプライアンスを設置し、IP アドレスおよびその他の関連する管理情報を割り当てるために初期設定を実行する方法の概要を示します。
付録 C. アプライアンスの設定	アプライアンス セットアップ ツールを使用して Stealthwatch アプライアンスを設定する方法の概要を示します。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

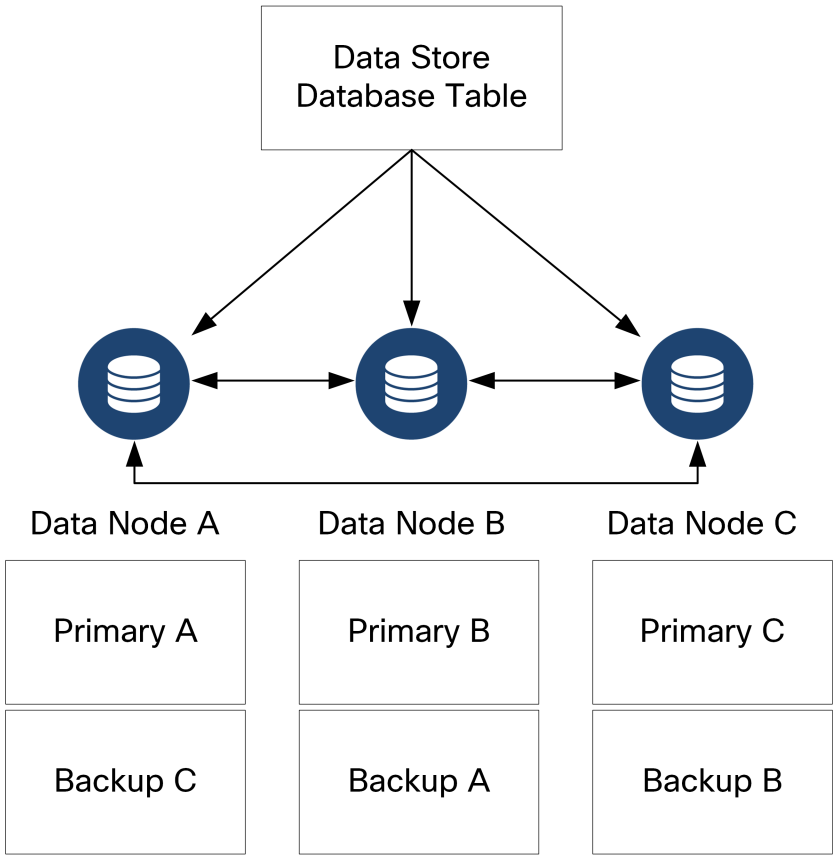
Data Store のストレージと耐障害性

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

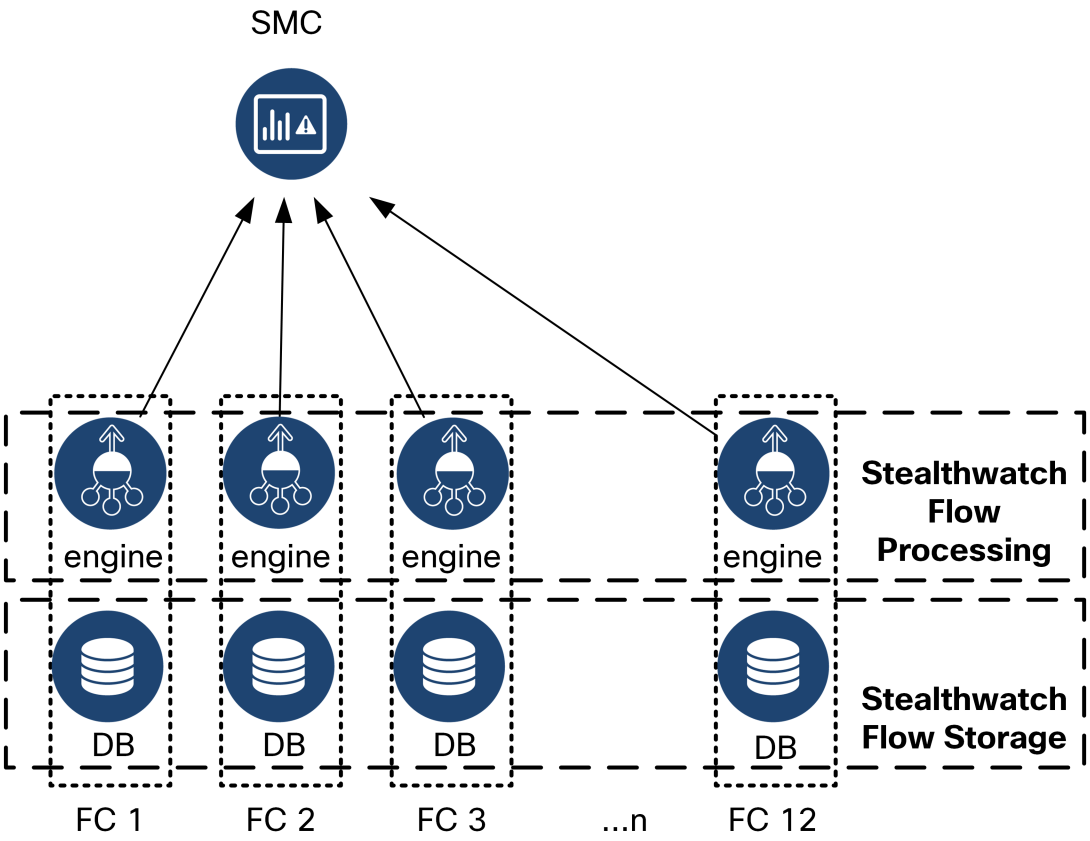
いずれかのノードが停止しても、そのバックアップを格納しているノードがまだ使用可能であり、Data Node の総数の少なくとも半分が稼働していれば、Data Store 全体は稼働状態を維持します。この間に、停止した接続や不具合のあるハードウェアを修復できます。問題がある Data Node を交換すると、そのノードのデータが Data Store の隣接する Data Node に格納されている既存のバックアップから復元され、その Data Node にデータのバックアップが作成されます。Data Node におけるテレメトリの格納方法の例については、次の図を参照してください。



© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

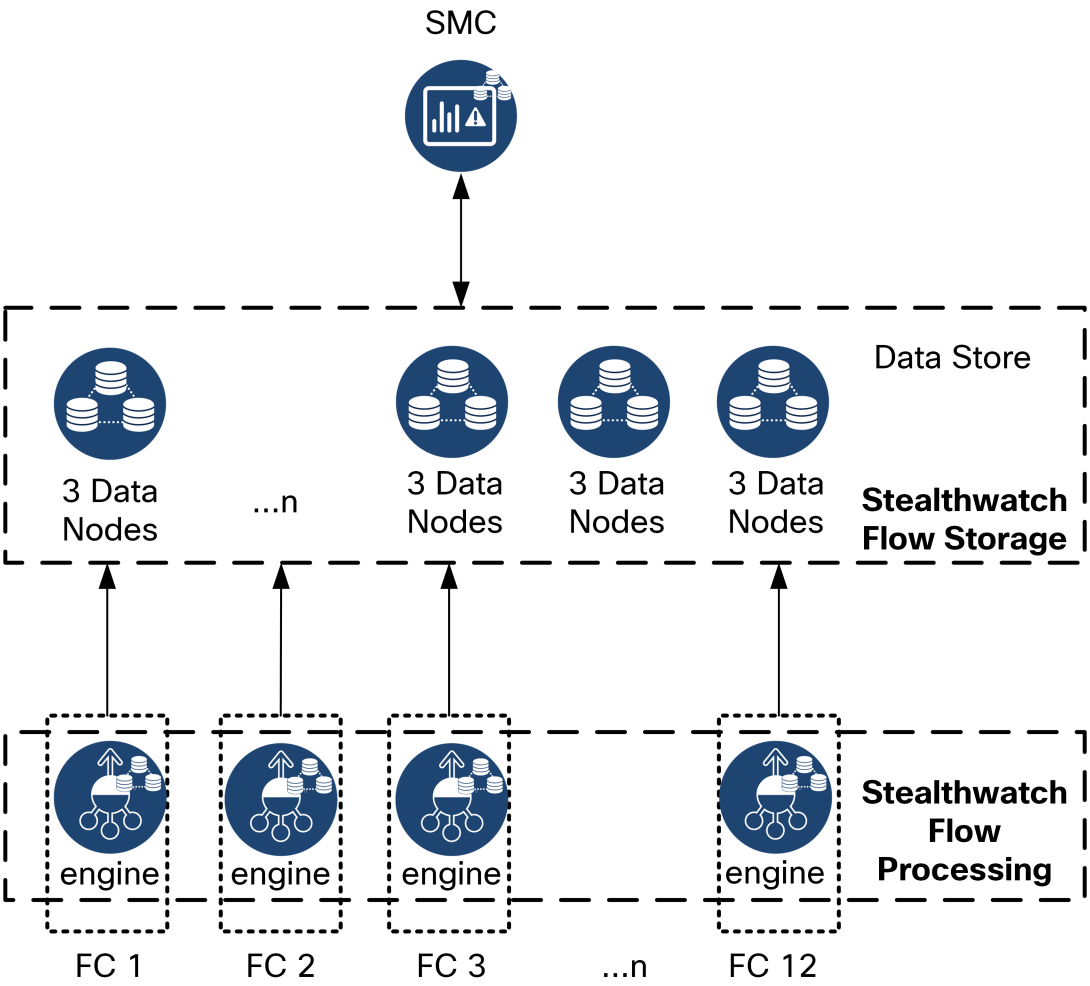
Stealthwatch Data Store の導入アーキテクチャ

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。



© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Data Store を使用した Stealthwatch 展開では、Data Store クラスタは 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 にほぼ均一に分散させます。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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- Data Store 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。
- ハードウェア Data Store（DS 6200）では、3 つのハードウェア Data Node をハードウェア SMC およびハードウェア 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 つ以上の Data Node で構成されます。ハードウェア Data Node は、それぞれが独自のシャーシです。ハードウェア Data Store を購入すると、その Data Store モデルで示されたノード数に対応する複数の Data Node ハードウェアシャーシが提供されます。たとえば、DS 6200 Data Store では 3 つの Data Node ハードウェアシャーシが提供されます。

複数の Data Store を購入して導入できます。Data Node は、Data Store の一部として、最小 3 台から最大 36 台まで 3 の倍数でクラスタ化できます。

> Data Node の構成においては、隣接する番号の Data Node に個別の冗長電源から電力を供給するように構成することをお勧めします。この構成により、データの冗長性と Data Store の全体的な稼働時間が向上します。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 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 10G ネットワーク接続
- （オプション）ハードウェア Data Node のみを対象として、ネットワークの冗長性および Data Node 間通信の重要性に対する、追加の 10G 接続、および Data Node のポートチャネルを確立する追加のスイッチ

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 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 ハードウェアの互換性とネットワーキングの要件

次の表に、Stealthwatch をハードウェア Data Store とともに導入する場合の必要なハードウェアの概要を示します。

ハードウェア コンポーネント	サポートされているキャパシティ
Data Store	• 3 つ以上の Data Node(DS 6200) • Data Store を拡張するための付加的な 3 つの Data Node のセット(Data Node の最大数は 36 個)
Stealthwatch Management Console	• 1 つ以上の Stealthwatch Management Console
Flow Collector	• 1 つ以上の Flow Collector

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。

> ⚠ アプライアンスの機能に問題が発生する可能性があるため、アプライアンスの BIOS を更新しないでください。

Data Store を展開する場合、少なくとも 3 つの Data Node が必要です。Data Store 6200 では、3 つの Data Node で 1 秒あたり約 500,000 フローを処理し、そのデータを約 90 日間保持できます。Data Store は Data Node を 3 の倍数の単位で追加して拡張できます。Data Node の最大数は 36 個です。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

これらの推奨事項では、テレメトリのみを考慮しています。パフォーマンスは、ホスト数、Flow Sensor の使用、トラフィックプロファイル、その他のネットワーク特性など、追加の要因によって異なる場合があります。サイジングについては、シスコサポートまでお問い合わせください。

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。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。

SMC を Data Store とともに展開し、Data Store で使用するように設定する必要があります。SMC のハイアベイラビリティが必要な場合は、フェールオーバー SMC も展開できます。

さらに、少なくとも 1 つの Flow Collector を Data Store とともに展開し、Data Store で使用するように設定する必要があります。

展開する SMC および Flow Collector のそれぞれについて、ルーティング可能なパブリック IP アドレスを `eth0` 管理ポートに割り当てる必要があります。Data Store を展開する場合は、SMC および Flow Collector の `eth0` 管理ポートに BASE-T 銅線 1G/10G ポートまたは SFP+ Twinax ケーブル 10G ポートを使用するように設定できます。Data Store で使用する BASE-T 銅線ポートには 10G のスループットが必要です。Data Store を展開していないユーザは、100Mbps/1Gbps/10Gbps 銅線インターフェイスのみを `eth0` として設定できます。

また、Stealthwatch の展開用に Flow Sensor と UDP Director を展開することもできます。これらのアプライアンスは Data Store と直接通信しないため、Data Store で使用するように設定する必要はありません。

サポートされているプラットフォームの詳細については、関連する仕様シートを参照してください。バージョンの互換性の詳細については、「Stealthwatch Hardware and Software Version Compatibility Matrix」を参照してください。

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、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

- `90` 日間フローを保存
- `3` つの `Data Node` を装備
- `7,200 GB / 3 Data Node = Data Node` あたり 2,400 GB（2.4 TB）

Data Store 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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 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	各 Data Node、Stealthwatch Management Console、および Flow Collector の場合： • 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 間での推奨されるラウンドトリップ時間（RTT）の遅延を 200 マイクロ秒未満に設定します。 • Data Node 間のクロックスキューを 1 秒以下に保ちます。 • Data Node 間での推奨スループットを 6.4 Gbps 以上（10 Gbps 全二重スイッチ接続）に設定します。
Data Node ハードウェア電源	• ハードウェア Data Node の電源が予期せず失われると、データが破損する可能性があります。無停電電源装置と、別回路の電源装置の両方を使用します。 • Data Store クラスタの初期化時に（詳細については「Data Store の初期化と設定」を参照）、各 Data Node が使用する電源に基づいて Data Node の設定を切り替えます。この操作により、電源が失われた場合にダウンする Data Node の数を最小限に抑えることで、耐障害性を最適化できます。
Data Node スイッチング	• Data Node は、Data Node 間通信を可能にするために独自のレイヤ 2 VLAN を必要とします。ハードウェア Data Node は、共有または専用の 10G スイッチに接続できます。 • シスコでは、ハードウェア Data Node を 2 台のスイッチに接続して、スイッチの停止時およびアップグレード時にも接続が保たれるようにすることを推奨しています。Data Node 間通信には低遅延が必要なため、シスコでは、2 台のスイッチが相互接続され両方のスイッチでレイヤ 2 VLAN が伝送される、スイッチの冗長ペアを推奨しています。
Stealthwatch	• 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

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

アプライアンス通信	• SMC と 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、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。

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。

> 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。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`）。SMC および Flow Collector と通信できるように Data Node の `eth0` ポートをネットワークに接続します。Data Node の `eth0` 管理ポートには、BASE-T 銅線 1G/10G ポートまたは SFP+ Twinax ケーブル 10G ポートを使用するように設定できます。

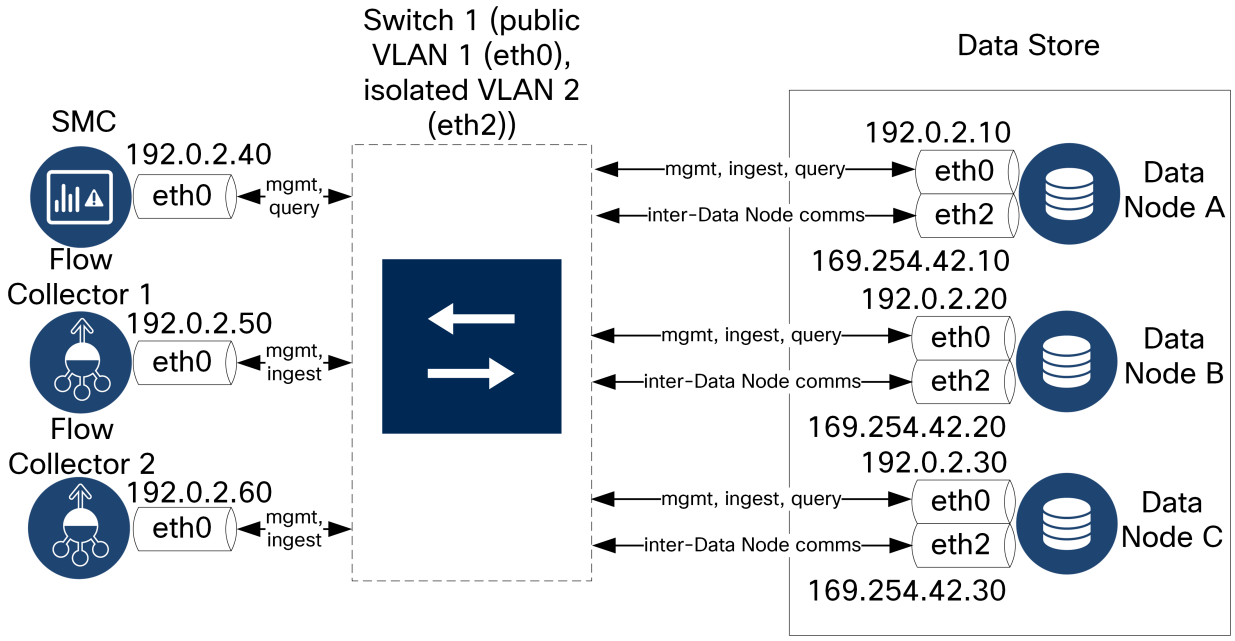
  Data Store の展開と設定においては、Data Node `eth0` IP アドレスを Data Store の名前にマッピングして、テレメトリの保存やクエリの要求と応答がより均等に分散されるようにします。詳細については、「Data Store の初期化と設定」を参照してください。
- Data Node 間の通信に使用するプライベート LAN または VLAN 内のルーティング不可の IP アドレス（`eth2`、またはスループットとパフォーマンスを高めるには `eth2` と `eth3` を含むポートチャネル）。Data Node 間の通信用に Data Node の `eth2` ポートまたは `eth2` と `eth3` を含むポートチャネルをスイッチに接続します。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。

  ハードウェア Data Node の場合、通常の Data Node 間の通信には、`eth2` ポートで 10G のスループットを設定すれば十分です。最大 20G のスループットを実現する `eth2/eth3` ポートチャネルを作成すると、Data Node 間の高速な通信が可能になり、新しい各 Data Node が隣接する Data Node からトラフィックを受信してデータを取り込むため、Data Store への Data Node の追加や交換が迅速になります。

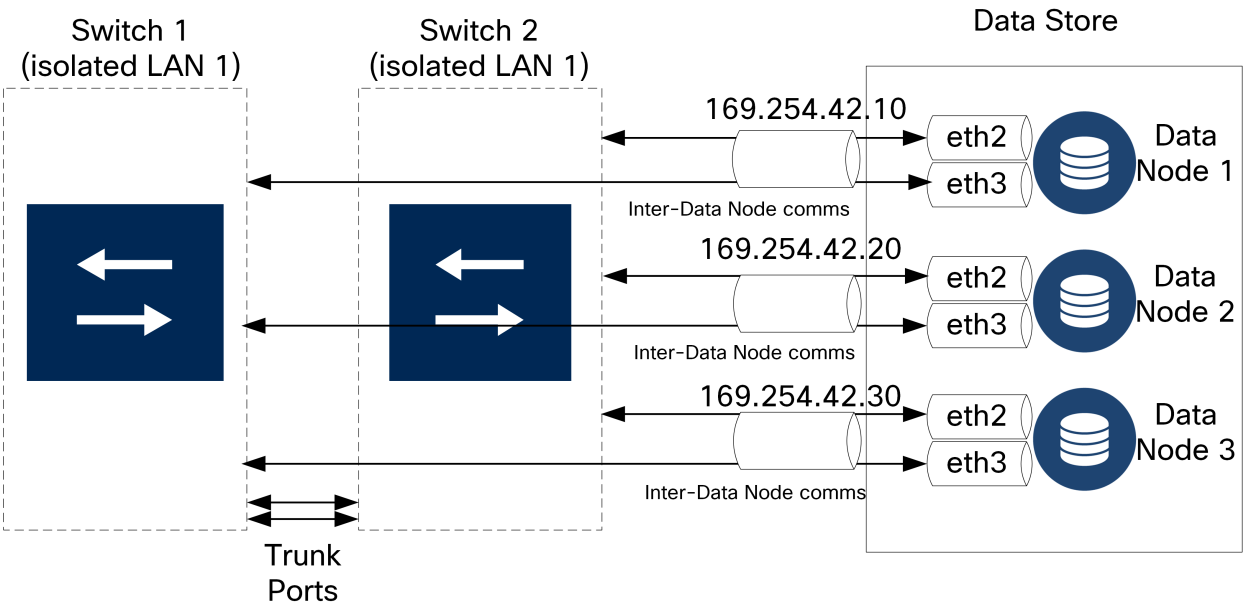
© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

eth2 または eth2/eth3 ポートチャネルを介した Data Node 間の通信を有効にするには、10G の速度をサポートするスイッチを 1 つ導入する必要があります。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、Data Node 間の通信用に独立した LAN または VLAN を設定します。これらのスイッチは他のアプライアンスと共有できますが、追加のアプライアンストラフィックには別の LAN または VLAN を作成してください。例として次の図を参照してください。



© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。スイッチの更新や計画的停止に備えてネットワークの冗長性をさらに高める場合は、Data Node で Data Node 間の通信専用のポートチャネルを設定することをお勧めします。それぞれの Data Node について、各物理ポートを異なるスイッチに接続して 2 つのスイッチに接続します。例として次の図を参照してください。



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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

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。

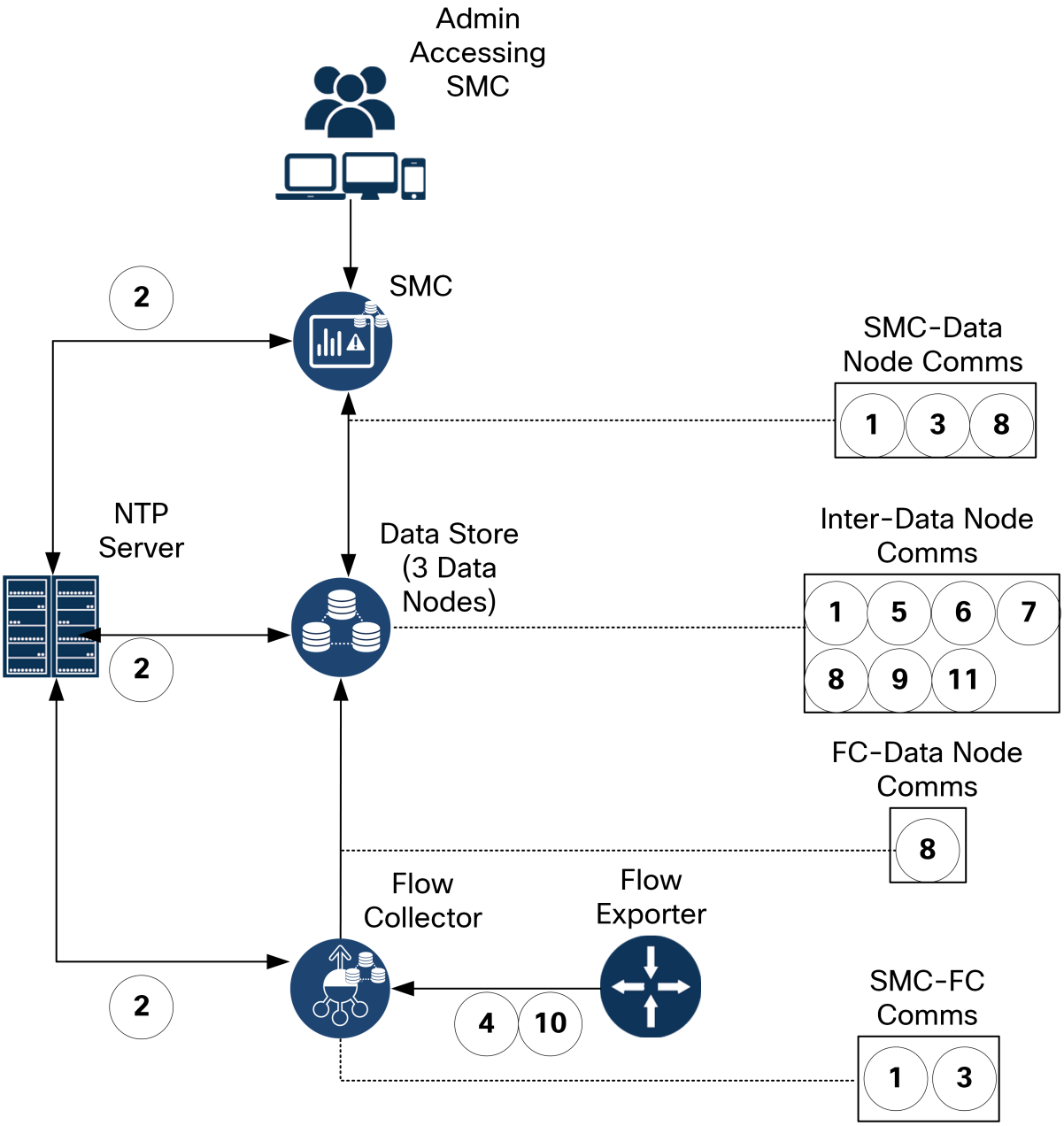
以下の点に注意してください。

- ハードウェア Data Node の電源復元ポリシーが［最後の状態の復元（Restore Last State）］に設定されていることを確認します。この設定の場合、電源喪失後に Data Node が自動的に再起動し、実行中のプロセスの復元が試行されます。CIMC での電源復元ポリシーの設定の詳細については、『UCS C-Series GUI Configuration Guide』を参照してください。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 x2xx Series (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

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 エクスポータ	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 エクスポータ	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

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Data Store の設置

> 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 ハードウェアの導入と考慮事項

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、ネットワークに Data Store 用のスイッチを設置します。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（v7.3.2）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設置と設定の詳細については、『Stealthwatch x2xx Series Hardware (with Data Store) Appliance Installation Guide』または「**付録 A. 設置の準備**」と「**付録 B. Stealthwatch ハードウェアの設置**」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』を参照してください。

> 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。

> 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。

1. 最初に、SMC をネットワークに展開します。その後、CIMC、キーボードとモニタ、またはラップトップを使用してアプライアンスに接続し、コンソールに `root` としてログインします。`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 での使用方法、および `root` ユーザと `sysadmin` ユーザのパスワードを更新します。ハードウェア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 x2xx Series Hardware (with Data Store) Appliance Installation Guide』または「**付録 A. 設置の準備**」と「**付録 B. Stealthwatch ハードウェアの設置**」を参照してください。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

> 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 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。

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』または「**付録 C. アプライアンスの設定**」を参照してください。
3. 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。

各 Data Node について、次の手順を実行します。

1. 最初に、Data Node をネットワークに展開します。その後、CIMC、キーボードとモニタ、またはラップトップを使用して Data Node アプライアンスに接続し、コンソールに `root` としてログインします。`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。ハードウェア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 x2xx Series Hardware (with Data Store) Appliance Installation Guide』または「**付録 A. 設置の準備**」と「**付録 B. Stealthwatch ハードウェアの設置**」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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 』または「**付録 C. アプライアンスの設定** 」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。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。
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

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。

1. 最初に、Flow Collector をネットワークに展開します。その後、CIMC、キーボードとモニタ、またはラップトップを使用して Flow Collector に接続し、コンソールに root としてログインします。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 での使用方法、および root ユーザと sysadmin ユーザのパスワードを更新します。ハードウェア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 x2xx Series Hardware (with Data Store) Appliance Installation Guide』または「**付録 A. 設置の準備**」と「**付録 B. Stealthwatch ハードウェアの設置**」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 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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 』または「**付録 C. アプライアンスの設定** 」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。

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

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。

1. 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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

UDP Director（オプション）の導入

UDP Director を導入する場合は、『Stealthwatch x2xx Series Hardware (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 x2xx Series Hardware (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 x2xx Series Hardware (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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

リソース	説明
URI パラメータ	• *[smc-eth0-ip]*：SMC の eth0 管理 IP アドレス
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）SMC の admin ユーザ • *[password]*：（必須）SMC の admin ユーザ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]*：SMC の 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

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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]*：SMC の 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	`{ "interfaceRetentionType":"[type]", "interfaceRetentionAmount":"[#]" }`

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。
	  • 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。
	  • 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。
	• *[#]*：（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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

リソース	説明
	`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、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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Data Store のインストールの次のステップ

Stealthwatch を展開して Data Store で使用するように設定したら、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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

> 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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

- 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

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

  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

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 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。

  > 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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 `dbadmin` の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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 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、「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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 への 3 つの Data Node の追加

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

ハードウェア Data Store は Data Node を追加して拡張できます。Data Node は 3 の倍数の単位で追加します。Data Store の Data Node の数を増やすには、次のタスクを実行します。

Data Node の追加と再調整のための Data Store の準備

Data Node を追加する前に、次の手順を実行します。

- 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。
- 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。
- 使用していない古いデータパーティションを削除します。これらのパーティションの識別については、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。
- ローカルセグメントを無効にします。vsql から SELECT DISABLE_LOCAL_SEGMENTS(); を発行します。
- リソースプールの設定を更新します。vsql から alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '70%; を発行します。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Data Store への Data Node の追加

次に、ネットワークに Data Node をまだ展開していない場合は、3 の倍数の単位で展開します。初回セットアップを使用してシステム設定で初期設定を実行し、アプライアンス セットアップ ツールで初期設定を完了します。詳細については、「**付録 B. Stealthwatch ハードウェアの設置**」と「**付録 C. アプライアンスの設定**」または『VE Installation Guide』を参照してください。

Data Node の設定（ルーティング可能な `eth0` 管理 IP アドレスとルーティング不可能な 2 番目のポートの IP アドレスの割り当てなど）が完了したら、SMC から SystemConfig を使用して Data Store に Data Node を追加します。

Data Store に Data Node を追加する

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。数分待ちます。
4. [データストア（Data Store）] メニューから、[新しいデータノードの設定（Config new Data Nodes）] を選択します。数分待ちます。

Data Node をデータベースに追加したら、各 Data Node に均等にデータが保存されるように Data Node 間でデータを再調整します。

Data Store のデータを再調整する

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/vsql --timing -x -c "SELECT rebalance_
   cluster()" -a -d sw -U dbadmin -w [dbadmin-password]
   ```

3. `[dbadmin-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、データの再調整を開始します。これには、プロジェクションの数やデータの量などのさまざまな要因により、しばらく時間がかかる場合があることに注意してください。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

5. 再調整が完了したら、リソースプールの設定を更新します。vsql から `alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '0%;` を発行します。

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

```
/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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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 と Data Store の間のセキュアな通信を設定する

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 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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Data Store の導入のトラブルシューティング

ハードウェアの導入のトラブルシューティング

SMC または Flow Collector の導入と設定に関する問題の詳細については、『Stealthwatch x2xx Series Hardware (with Data Store) Appliance Installation Guide』および『Stealthwatch System Configuration Guide』を参照してください。

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。

再起動する前に、Data Node の電源復元ポリシーの更新が必要になる場合もあります。電源復元ポリシーが [電源オフ（Power Off）] に設定されている場合は、電源喪失後に Data Node を手動で再起動する必要があります。CIMC での電源復元ポリシーの設定の詳細については、『UCS C-Series GUI Configuration Guide』を参照してください。

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

```
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。

再起動する前に、Data Node の電源復元ポリシーの更新が必要になる場合もあります。電源復元ポリシーが [電源オフ(Power Off)] に設定されている場合は、電源喪失後に Data Node を手動で再起動する必要があります。CIMC での電源復元ポリシーの設定の詳細については、『UCS C-Series GUI Configuration Guide』を参照してください。

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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

付録 A. 設置の準備

設置に関する警告

Stealthwatch Data Store アプライアンスを設置する前に、『Regulatory and Compliance Safety Information』のドキュメントをお読みください。

次の警告に注意してください。

ステートメント 1071：警告の定義

安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。警告の各国版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

ステートメント 1005：回路ブレーカー

この製品は、設置する建物にショート（過電流）保護機構が備わっていることを前提に設計されています。この保護装置の定格が USA：120、15 A（EU：250 V、16 A）以下であることを確認します。

ステートメント 1004：設置方法

設置手順を読んでから、システムを使用、取り付け、または電源に接続してください。

ステートメント 12：電源の切断に関する警告

シャーシの作業や電源モジュール周辺の作業を行う前に、AC 装置の電源コードを外し、DC 装置の回路ブレーカーの電源を切ってください。

ステートメント 43：装身具の取り外しに関する警告

電力系統に接続された装置で作業する場合は、事前に、指輪、ネックレス、腕時計などの装身具を外してください。金属は電源やアースに接触すると、過熱して重度のやけどを引き起こしたり、金属類が端子に焼き付いたりすることがあります。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ステートメント 94：リスト ストラップの警告

作業中は、カードの静電破壊を防ぐため、必ず静電気防止用リスト ストラップを着用してください。感電する危険があるので、手や金属工具がバックプレーンに直接触れないようにしてください。

ステートメント 1045：短絡保護

この製品は、設置する建物に回路短絡（過電流）保護機構が備わっていることを前提に設計されています。一般および地域の電気規格に準拠するように設置する必要があります。

ステートメント 1021：SELV 回路

感電を防ぐため、安全超低電圧（SELV）回路を電話網電圧（TNV）回路に接続しないでください。LAN ポートには SELV 回路が、WAN ポートには TNV 回路が組み込まれています。一部の LAN ポートおよび WAN ポートでは、共に RJ-45 コネクタが使用されています。ケーブルを接続する際は、注意してください。

ステートメント 1024：アース導体

この装置は、接地させる必要があります。絶対にアース導体を破損させたり、アース線が正しく取り付けられていない装置を稼働させたりしないでください。アースが適切かどうかはっきりしない場合には、電気検査機関または電気技術者に確認してください。

ステートメント 1040：製品の廃棄

本製品の最終処分は、各国のすべての法律および規制に従って行ってください。

ステートメント 1074：地域および国の電気規則への適合

機器の取り付けは各地域および各国の電気規格に適合する必要があります。

ステートメント 19：TN 電源に関する警告

この装置は TN 電源システムで動作するように設計されています。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

設置に関するガイドライン

次の警告を記録しておいてください。

> ステートメント 1047：過熱の防止
>
> システムの過熱を防ぐため、周囲温度が推奨範囲の最大値である 5 ～ 35° C（41 ～ 95° F）度を超える場所ではシステムを使用しないでください。

> ステートメント 1019：主要な切断装置
>
> いつでも装置の電源を切断できるように、プラグおよびソケットにすぐ手が届く状態にしておいてください。

> ステートメント 1005：回路ブレーカー
>
> この製品は、設置する建物にショート（過電流）保護機構が備わっていることを前提に設計されています。この保護デバイスの定格が USA：120、15 A（EU：250 V、16 A）以下であることを確認します。

> ステートメント 1074：地域および国の電気規則への適合
>
> 機器の取り付けは各地域および各国の電気規格に適合する必要があります。

> ステートメント 371：電源コードおよび AC アダプタ
>
> 製品を設置する際は、同梱または指定のケーブル、電源ケーブル、および AC アダプタ/バッテリを使用してください。他のケーブルやアダプタを使用すると、誤動作や発火が生じることがあります。電気用品安全法により、シスコによって指定された製品以外の電気製品で、UL 認定のケーブル（コードに「UL」または「CSA」と記載）を使用することは禁じられています。同法で規制されていないものはコードに「PSE」と表示されます。

> ステートメント 1073：ユーザが保守可能な部品なし
>
> スイッチ内部にはユーザが保守できる部品はありません。筐体を開けないでください。

シャーシを設置するときは、次のガイドラインに従ってください。

- シャーシの作業に支障がないように、また適切なエアーフローが確保されるように、アプライアンス周辺に十分なスペースを確保できることを確認してください。シャーシのエアーフローは、前面から背面に向かいます。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

> シャーシを取り付ける際は、適切なエアーフローを確保するために、レール キットを使用する必要があります。レール キットを使用せずに、ユニットを別のユニットの上に物理的に置く、つまり積み重ねると、シャーシの上部にある通気口がふさがれ、過熱したり、ファンの回転が速くなったり、電力消費が高くなったりする原因となる可能性があります。シャーシをラックに取り付けるときは、これらのレールによりシャーシ間で必要な最小の間隔が提供されるので、レール キットにシャーシをマウントすることを推奨します。レール キットを使用してマウントする場合は、シャーシ間の間隔を余分にとる必要はありません。

- 空調が 5 ～ 35° C（41 ～ 95° F）の温度でシャーシを維持できることを確認します。
- キャビネットまたはラックが、ラック要件に適合していることを確認します。
- 設置場所の電源が、「仕様シート」に記載された電源要件に適合していることを確認します。使用可能な場合は、電源障害に備えて UPS を使用してください。

> 鉄共振テクノロジーを使用する UPS タイプは使用しないでください。このタイプの UPS は、システムに使用すると、データトラフィック パターンの変化によって入力電流が大きく変動し、動作が不安定になるおそれがあります。

安全に関する推奨事項

次の情報により、安全を確保し、シャーシを保護することができます。この情報には、作業環境で生じる可能性のある危険な状況がすべて網羅されているわけではありません。絶えず注意して、的確な判断を心がけてください。

これらの安全に関する注意事項を遵守してください。

- 設置作業中および作業後は、設置場所を整理し、埃のない状態に保ってください。
- 工具は、通行の邪魔にならない場所に置いてください。
- ゆったりとした衣服やイヤリング、ブレスレット、ネックレスなどの装飾品は身につけず、シャーシに引っかかることがないようにしてください。
- 目が危険にさらされる状況で作業する場合は、保護眼鏡を着用してください。
- 人身事故や装置障害を引き起こす可能性のある作業は行わないでください。
- 重量が 1 人で扱える範囲を超えているものを、単独で持ち上げないでください。

電気製品を扱う場合の注意

> ⚠ シャーシの作業を行う前に、必ず電源コードを抜いてください。

電気機器を取り扱う際には、次の注意事項に従ってください。

- 危険を伴う作業は、一人では行わないでください。
- 電源が切断されていると思い込まずに、必ず確認してください。
- 床が濡れていないか、アースされていない電源延長コード、すり減った電源コード、保護アースの不備などがないかどうか、作業場所の安全を十分に確認してください。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 電気事故が発生した場合は、次のように対処してください。
  - 負傷しないように注意してください。
  - システムの電源を切断してください。
  - 可能であれば、だれかに頼んで救護を呼んでもらいます。それができない場合は、負傷者の状況を見極めてから救援を要請してください。
  - 負傷者に人工呼吸または心臓マッサージが必要かどうかを判断し、適切な処置を施してください。
- シャーシは、指定された定格電力の範囲内で、製品の使用説明書に従って使用してください。

静電破壊の防止

電子部品の取り扱いが不適切な場合、ESD が発生し、機器の損傷や電気回路の破損を引き起こす可能性があります。その結果、機器の断続的障害または完全な故障を引き起こします。

部品の取り外しまたは交換を行うときは、必ず静電気防止手順に従ってください。シャーシが電気的にアースに接続されていることを確認してください。静電気防止用リスト ストラップを肌に密着させて着用してください。アースクリップをシャーシフレームの塗装されていない表面に止めて、静電気が安全にアースに流れるようにします。静電放電による損傷とショックを防止するには、リストストラップとコードを効果的に作用させる必要があります。リストストラップがない場合は、シャーシの金属部分に触れて、身体を接地してください。

安全を確保するために、静電気防止用ストラップの抵抗値を定期的にチェックしてください。抵抗値は 1 ～ 10 MΩ である必要があります。

設置場所の環境

機器故障を予防し、環境に起因するシャットダウンを防ぐため、注意して設置場所のレイアウトや機器の配置を検討してください。既存の装置で停止やエラーが頻繁に起きている場合にも、この考慮事項を参考にすることにより、障害の原因を突き止め、今後問題が起きないように予防できます。

電源モジュールに関する考慮事項

シャーシを設置する際には、以下のことを考慮してください。

- シャーシを設置する前に、設置場所の電源を調べ、スパイクやノイズがないかどうかを確認してください。必要に応じて電源調整器を設置し、アプライアンス入力電圧にて適切な電圧および電力レベルを確保してください。
- 設置場所で適切にアースし、雷や電力サージによる損傷を防止してください。
- シャーシでは、ユーザが動作範囲を選択できません。シャーシの正確なアプライアンス入力所要電力については、そのラベルを参照してください。
- 複数の種類の AC 入力電源コードをアプライアンスに使用できます。設置場所に適したタイプを使用してください。
- デュアル冗長（1＋1）電源を使用している場合は、各電源に独立した電気回路を使用することを推奨します。
- できるだけ、無停電電源装置を使用してください。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ラックの構成に関する考慮事項

ラックの構成を決めるときは、次のことを考慮してください。

- 開放型ラックにシャーシをマウントする場合、ラックのフレームで吸気口や排気口をふさがないように注意してください。
- 閉鎖型ラックに十分な通気があることを確認してください。各シャーシで熱が発生するため、ラック内に装置を詰め込みすぎないように注意してください。冷気が回るように、閉鎖型ラックにはルーバーが付いた側面とファンが必要です。
- 閉鎖型ラックの上部に換気用ファンが付いている場合には、ラックの下段に設置した装置の熱が上昇し、上段の装置の吸気口から入り込む可能性があります。ラック下段の装置に対して、十分な換気が行われるようにしてください。
- バッフルは吸気から排気を分離するときに役立ちます。また、シャーシ内に冷気を取り込むためにも役立ちます。隔壁は、シャーシ内に冷気を行き渡らせるためにも有効です。隔壁の最適な取り付け位置は、ラック内の空気がどのように流れるかによって異なります。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

付録 B. Stealthwatch ハードウェアの設置

このセクションでは、ご使用の環境へのアプライアンスの設置について説明します。内容は次のとおりです。

- **アプライアンスのマウント**
- **ネットワークへのアプライアンスの接続**
- **アプライアンスへの接続**
- 初回セットアップを使用したネットワークの設定 **初回セットアップを使用したネットワークの設定**

アプライアンスのマウント

Stealthwatch アプライアンスは、標準の 19 インチラックまたはキャビネット、その他の適切なキャビネット、または平らな面に直接マウントすることができます。ラックまたはキャビネット内にアプライアンスをマウントする場合は、レール マウント キットに含まれている手順に従ってください。アプライアンスの配置場所を決める場合は、前面および背面パネルまでのスペースが以下の要件を満たしていることを確認します。

- 前面パネルのインジケータが見やすいこと。
- 背面パネルのポートに無理なくケーブルを接続できること。
- 背面パネルの電源コネクタが調整済み AC 電源の近くにあること。
- アプライアンスの周囲および通気口を通過するエアーフローが妨げられないこと。

アプライアンスに付属するハードウェア

Stealthwatch アプライアンスには、次のハードウェアが含まれます。

- AC 電源コード
- アクセス キー（前面プレート）
- ラック マウント用のレール キットまたは小型アプライアンス用のマウント用取り付け金具
- Flow Collector 5210 シリーズ アプライアンスの場合は、10 GB SFP ケーブル

追加で必要なハードウェア

以下のハードウェアを追加で用意する必要があります。

- 標準の 19 インチ ラック用取り付けネジ。
- 設置している 各 Stealthwatch システム製品の無停電電源装置（UPS）。
- （オプション）ローカルに設定するには、次のいずれかの方法を使用します。
    - ラップトップとビデオ ケーブルおよび USB ケーブル（キーボード用）
    - ビデオ モニタとビデオ ケーブルおよびキーボードと USB ケーブル

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ネットワークへのアプライアンスの接続

各アプライアンスを同じ方法でネットワークに接続します。接続に関する唯一の相違点は、使用するアプライアンスのタイプです。

> ⚠ アプライアンスの機能に問題が発生する可能性があるため、アプライアンスの BIOS を更新しないでください。

各アプライアンスの仕様に関する詳細については、Stealthwatch の仕様シートを参照してください。

> ⓘ すべての Cisco x2xx ハードウェアは、UCSC-C240-M5SX を使用する Flow Collector 5210 DBを除いて、同じ UCS プラットフォーム（UCSC-C220-M5SX）を使用します。アプライアンスの違いは、NIC カード、プロセッサ、メモリ、ストレージおよび RAID にあります。

> ⓘ Flow Collector 5210 は、接続された 2 台のサーバ（エンジンおよびデータベース）で構成されており、これらのサーバは単一のアプライアンスとして機能します。このため、他のアプライアンスとは設置方法が若干異なります。まず、両サーバを 10G SFP+ DA クロス接続ケーブルで相互に直接接続します。次に、ネットワークに接続します。

アプライアンスをネットワークに接続するには、次の手順に従います。

1. イーサネットケーブルをアプライアンスの背面にある管理ポートに接続します。
2. Flow Sensor と UDP Director の少なくとも 1 つのモニタ ポートを接続します。

   UDP Director HA の場合は、クロス ケーブルで 2 つの UDP Director を接続します。1 つの UDP Director の eth2 ポートを 2 つ目の UDP Director の eth2 ポートに接続します。同様に、2 本目のクロス ケーブルで各 UDP Director の eth3 ポートを接続します。ケーブルには、光ファイバまたは銅線を使用できます。

   各ポートのイーサネット ラベル（eth2、eth3 など）に注意してください。これらのラベルは表示されるネットワーク インターフェイス（eth2、eth3 など）を表し、アプライアンス管理インターフェイスのホーム ページから設定できます。

3. イーサネット ケーブルのもう一方の端をネットワークのスイッチに接続します。
4. 電源コードを電源に接続します。一部のアプライアンスには、電源 1 と電源 2 の 2 つの電源接続があります。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

アプライアンスへの接続

このセクションでは、デフォルトのユーザパスワードを変更するためにアプライアンスに接続する方法を説明します。

アプライアンスに接続するには、次のいずれかの方法を使用します。

- キーボードとモニタを使用する
- ラップトップ（およびターミナル エミュレータ）を使用する

新しいアプライアンスの場合、SSH は無効になっています。有効にするには、アプライアンスの管理 Web インターフェイスにログインする必要があります。

キーボードとモニタを使用した接続

IP アドレスをローカルに設定するには、次の手順を実行します。

1. 電源ケーブルをアプライアンスに差し込みます。
2. 電源ボタンを押してアプライアンスをオンにします。起動が完全に終了するまで待機します。起動プロセスを中断しないでください。

> 場合によっては、電源を適用するために前面パネルを取り外す必要があります。
>
> 一部のモデルでは、システムの電源が入っていないときに電源ファンがオンになります。前面パネルの LED がオンになっているか確認します。
>
> アプライアンスを必ず無停電電源装置（UPS）に接続してください。電源には電力が必要です。電力がない場合、エラーが表示されます。

3. 次の手順でキーボードを接続します。

- 標準キーボードの場合は、標準のキーボード コネクタに接続します。
- USB キーボードの場合は、USB コネクタに接続します。

4. ビデオ コネクタにビデオ ケーブルを接続します。ログイン プロンプトが表示されます。
5. セクション「**初回セットアップを使用したネットワークの設定**」に進みます。

ラップトップを使用した接続

ターミナルエミュレータを搭載したラップトップを使用して、アプライアンスに接続することもできます。

ラップトップを使用してアプライアンスに接続するには、次の手順を実行します。

1. 次のいずれかの方法を使用してラップトップをアプライアンスに接続します。

- ラップトップのシリアル ポート コネクタ（DB9）からアプライアンスのコンソール ポートに RS232 ケーブルを接続します。
- ラップトップのイーサネット ポートからアプライアンスの管理ポートにクロス ケーブルを接続します。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

2. 電源ケーブルをアプライアンスに差し込みます。
3. 電源ボタンを押してアプライアンスをオンにします。起動が完全に終了するまで待機します。起動プロセスを中断しないでください。

> 場合によっては、電源を適用するために前面パネルを取り外す必要があります。
>
> 一部のモデルでは、システムの電源が入っていないときに電源ファンがオンになります。前面パネルの LED がオンになっているか確認します。アプライアンスを必ず無停電電源装置(UPS)に接続してください。電源には電力が必要です。電力がない場合、エラーが表示されます。

4. ラップトップで、アプライアンスへの接続を確立します。

   任意のターミナル エミュレータを使用して、アプライアンスと通信できます。

5. 次の設定を適用します。

- BPS:115200
- データビット:8
- ストップ ビット:1
- パリティ:なし
- フロー制御:なし

ログイン画面とログイン プロンプトが表示されます。

6. 次のセクション「**初回セットアップを使用したネットワークの設定**」に進みます。

初回セットアップを使用したネットワークの設定

アプライアンスに接続した後、初回セットアップを使用して、IP アドレスを含むネットワークの設定を行います。次の点に注意してください。

- Data Store を使用して SMC 2210 または Flow Collector 4210 を導入する場合は、IP アドレスの設定に加えて、Data Store 用の SMC または Flow Collector、および `eth0` 管理ポートに使用する物理ポートのタイプも設定できます。

  > SMC または Flow Collector を Data Store 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。

- アプライアンスが Data Node の場合、`eth0` 管理ポートに使用する物理ポートのタイプ、および Data Node 通信用の `eth2` または `eth2/eth3` ポートチャネルの IP アドレスと関連情報を設定できます。

SMC 2210、FC 4210、および Data Node アプライアンスの設置に関する詳細については、『Stealthwatch Data Store Hardware Deployment and Configuration Guide』を参照してください。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

IP アドレスとポートを設定した後、ユーザパスワードを変更します。

> 初めてシステム設定を開始すると、初回セットアップウィザードが起動し、アプライアンスの初期設定をガイドします。このウィザードが完了する前に初回セットアップを終了すると、次にシステム設定を開始したときに、初回セットアップウィザードが再度起動します。

ご使用のアプライアンスに応じて、次のセクションに移動します。

- Data Store と互換性のあるアプライアンス（SMC 2210、FC 4210） **Data Store と互換性のあるアプライアンス（SMC 2210、FC 4210）**
- 一般的な Stealthwatch アプライアンスの設定 **一般的な Stealthwatch アプライアンスの設定**
- **Data Node 設定**

一般的な Stealthwatch アプライアンスの設定

Data Node、SMC 2210、および FC 4210 を除くすべてのアプライアンスで、初回セットアップ時に次の構成が表示されます。

- アプライアンスの IP アドレスと管理情報の設定

アプライアンスの IP アドレスと管理情報の設定

初回セットアップで、アプライアンスの eth0 管理 IP アドレスと関連情報を設定します。大多数のアプライアンスで、これは初回セットアップにおける最初の設定になります。

はじめる前に

- Data Node を設定する場合は、「Data Node の設定」に移動します。
- Data Store と互換性のある SMC または Flow Collector を設定する場合は、「Data Store と互換性のあるアプライアンス（SMC 2210、FC 4210）」に移動します。
- 他の Stealthwatch アプライアンスを設定する場合は、ステップ 1 から開始します。

手順

1. システム設定プログラムにログインします。
   - Data Node または Data Store と互換性のあるアプライアンスを設定する場合は、`root` と入力してから **Enter** を押します。他のアプライアンスを設定している場合は、「`sysadmin`」と入力してから **Enter** を押します。

     > Data Store と Data Store との互換性を適切に設定するには、`root` 権限が必要です。

   - パスワードプロンプトが表示されたら、**lan1cope** と入力して Enter を押します。
   - 次のプロンプトで、**SystemConfig** と入力し、Enter を押します。
2. このアプライアンスでシステム設定を初めて入力した場合は、初回セットアップが開始されます。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

そうでない場合、[システム設定(System Configuration)]メニューが開きます。[管理(Management)]を選択し、Enter を押します。

3. このアプライアンスの **IP アドレス**を入力します。
4. ネットワークの**ネットマスク**を入力します。
5. アプライアンスの IP アドレスの**ゲートウェイ**アドレスを入力します。
6. アプライアンスの**ブロードキャスト**アドレスを入力します。
7. アプライアンスの**ホスト名**を入力します。
8. アプライアンスの**ドメイン**を入力します。
9. [選択(Select)]を選択してから、[はい(Yes)]を選択してエントリを確定します。

   これが初回セットアップの最後の設定オプションです。アプライアンスが再起動して変更が実装されます。完了すると、[ログイン(Login)]ページが開きます。

次の作業

- ユーザパスワードを変更します。詳細については、「**sysadmin ユーザパスワードの変更**」を参照してください。

Data Store と互換性のあるアプライアンス(SMC 2210、FC 4210)

SMC 2210 および FC 4210 の場合、初回セットアップ時には次の設定が表示されます。

1. eth0 管理物理ポートの設定
2. アプライアンスの IP アドレスと管理情報の設定
3. Data Store との互換性の設定
4. Security Analytics and Logging(オンプレミス)の使用の設定

eth0 管理物理ポートの設定

Data Store と互換性のある SMC または Flow Collector を設定して、Data Store を導入する場合は、必要に応じて、デフォルトの BASE-T 銅線ポートの代わりに `eth0` を SFP+ DAC ポートとして設定できます。これらのアプライアンスの場合、これは初回セットアップにおける最初の設定になります。

はじめる前に

- Data Node、または Data Store と互換性のある SMC または Flow Collector を設定する場合、サポートされている SFP+ および BASE-T ポートの詳細については、ご使用のアプライアンスの Stealthwatch 仕様シートを参照してください。
- Data Node を設定する場合は、「Data Node の設定」に移動します。
- Data Store と互換性のあるアプライアンス以外の Stealthwatch アプライアンスを設定する場合は、「一般的な Stealthwatch アプライアンスの構成」を参照してください。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

手順

1. システム設定プログラムにログインします。
   - 「**root**」と入力してから **Enter** を押します。

     > Data Store との互換性を適切に設定するには、`root` 権限が必要です。

   - パスワード プロンプトが表示されたら、**lan1cope** と入力して Enter を押します。
   - 次のプロンプトで、**SystemConfig** と入力し、Enter を押します。
2. このアプライアンスでシステム設定を初めて入力した場合は、初回セットアップが開始され、ポート順序の設定が表示されます。ステップ 5 に進みます。

   そうでない場合、[システム設定(System Configuration)] メニューが開きます。[管理(Management)] を選択し、Enter を押します。
3. [システム設定(System Configuration)] メニューで、[ネットワーク(Network)] を選択してから、**Enter** を押します。
4. [ポートの順序(Port Order)] を選択してから、Enter を押します。
5. 次の選択肢があります。
   - eth0 に BASE-T 銅線ポートを使用するようにアプライアンスを設定するには、[LOM] を選択します。
   - eth0 に SFP+ ファイバポートを使用するようにアプライアンスを設定するには、[SFP+] を選択します。
6. [OK] を選択して選択を確定します。

次の作業

- eth0 管理ポートの IP アドレスと管理情報を設定します。次の手順を参照してください。

アプライアンスの IP アドレスと管理情報の設定

初回セットアップで、アプライアンスの eth0 管理 IP アドレスと関連情報を設定します。Data Store と互換のあるアプライアンスの場合、この構成は eth0 物理管理ポートの設定後に行われます。

はじめる前に

- Data Store と互換性のある SMC または Flow Collector を設定している場合、ポートの順序を設定すると、初期設定ウィザードに `eth0` 管理構成が表示されます。ステップ 3 に進みます。

手順

1. システム設定プログラムにログインします。
   - Data Store と互換性のあるアプライアンスを設定する場合は、`root` と入力してから **Enter** を押します。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

> Data Store と Data Store との互換性を適切に設定するには、`root` 権限が必要です。

- パスワードプロンプトが表示されたら、**lan1cope** と入力して Enter を押します。
- 次のプロンプトで、**SystemConfig** と入力し、Enter を押します。

2. このアプライアンスでシステム設定を初めて入力した場合は、初回セットアップが開始されます。

   そうでない場合、[システム設定(System Configuration)]メニューが開きます。[管理(Management)]を選択し、Enter を押します。
3. このアプライアンスの **IP アドレス**を入力します。
4. ネットワークの**ネットマスク**を入力します。
5. アプライアンスの IP アドレスの**ゲートウェイ**アドレスを入力します。
6. アプライアンスの**ブロードキャスト**アドレスを入力します。
7. アプライアンスの**ホスト名**を入力します。
8. アプライアンスの**ドメイン**を入力します。
9. [選択(Select)]を選択してから、[はい(Yes)]を選択してエントリを確定します。

次の作業

- Data Store なしで使用するようにアプライアンスを設定します。詳細については、次の手順を参照してください。

Data Store の使用の設定

Data Store と連動するように SMC 2210 または FC 4210 を設定します。Flow Collectorが Data Store に接続し、SMC が Data Store をクエリするようになります。

> SMC または Flow Collector を Data Store 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。

> Data Store を導入する場合は、Data Store と連携するようにすべての SMC と Flow Collector を設定する必要があります。一部の Flow Collector は、Data Store に接続するように設定できません。SMC に直接接続するように設定できないものもあります。

はじめる前に

- 初回セットアップの場合は、アプライアンスの IP アドレスの設定が完了すると、[システム設定(System Configuration)]に Data Store の設定が表示されます。ステップ 3 に進みます。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

手順

1. [システム設定(System Configuration)]メニューから次の操作を実行します。[詳細(Advanced)]を選択してから、**Enter** を押します。
2. [データストア(Data Store)]を選択してから、Enter を押します。
3. Data Store との互換性を持つようにアプライアンスを設定するには、[はい(Yes)]を選択します。

> ⚠ SMC または Flow Collector を Data Store 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。

4. [OK]を選択して選択を確定します。

次の作業

- Security Analytics and Logging(オンプレミス) を設定します。詳細については、次の手順を参照してください。

Security Analytics and Logging(オンプレミス)の使用の設定

SMC 2210 または FC 4210 を Security Analytics and Logging(オンプレミス)用に設定することで、Stealthwatch の展開を使用して Firepower イベント情報を保存します。Flow Collectorが Firepower イベント情報を取り込み、Data Store に送信して保存します。この Firepower イベント情報を Stealthwatch Management Console または Firepower Management Center からクエリできます。

Security Analytics and Logging(オンプレミス)を設定する場合は、Stealthwatch Management Console にも Security Analytics and Logging(オンプレミス)アプリケーションをインストールする必要があります。詳細については、『Security Analytics and Logging: Firepower Event Integration Guide』を参照してください。

> ⚠ SMC または Flow Collector を Security Analytics and Logging(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。Security Analytics and Logging(オンプレミス)に Stealthwatch を使用して Firepower イベント情報を保存する場合に**のみ**、この機能を有効にしてください。

はじめる前に

- 初回セットアップの場合は、Data Store の使用の設定が完了すると、[システム設定(System Configuration)]に Security Analytics and Logging(オンプレミス)の設定が表示されます。

手順

1. [はい(Yes)]を選択して Security Analytics and Logging(オンプレミス)を有効にし、Firepower の展開からファイアウォールイベント情報を取り込みます。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。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

> ⚠ SMC または Flow Collector を Security Analytics and Logging（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。Security Analytics and Logging（オンプレミス）に Stealthwatch を使用して Firepower イベント情報を保存する場合に**のみ**、この機能を有効にしてください。

2. [いいえ（No）] を選択して Security Analytics and Logging（オンプレミス）を無効にします。Flow Collector で NetFlow を取り込むことができます。Firepower の展開からファイアウォールイベント情報を取り込むことはできません。
3. [OK] を選択して選択を確定します。

   これが初回セットアップの最後の設定オプションです。アプライアンスが再起動して変更が実装されます。完了すると、[ログイン（Login）] ページが開きます。

Data Node 設定

Data Node の場合、初回セットアップ時には次の設定が表示されます。

1. eth0 管理物理ポートの設定
2. アプライアンスの IP アドレスと管理情報の設定
3. Data Node 間通信用の eth2 および eth3 の設定

eth0 管理物理ポートの設定

Data Node を設定する場合、必要に応じて、デフォルトの SFP+ DAC ポートの代わりに `eth0` を BASE-T 銅線ポートとして設定できます。これらのアプライアンスの場合、これは初回セットアップにおける最初の設定になります。

はじめる前に

- Data Node を設定する場合、サポートされている SFP+ および BASE-T ポートの詳細については、ご使用のアプライアンスの Stealthwatch 仕様シートを参照してください。
- Data Store と互換性のある SMC または Flow Collector を設定する場合は、「Data Store と互換性のあるアプライアンス（SMC 2210、FC 4210）」に移動します。
- Data Store と互換性のあるアプライアンス以外の Stealthwatch アプライアンスを設定する場合は、「一般的な Stealthwatch アプライアンスの構成」を参照してください。

手順

1. システム設定プログラムにログインします。
   - 「**root**」と入力してから **Enter** を押します。

     > ⓘ Data Store との互換性を適切に設定するには、`root` 権限が必要です。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- パスワードプロンプトが表示されたら、**lan1cope** と入力して Enter を押します。
- 次のプロンプトで、**SystemConfig** と入力し、Enter を押します。

2. このアプライアンスでシステム設定を初めて入力した場合は、初回セットアップが開始され、ポート順序の設定が表示されます。ステップ 5 に進みます。

   そうでない場合、[システム設定(System Configuration)]メニューが開きます。[管理(Management)]を選択し、Enter を押します。
3. [システム設定(System Configuration)]メニューで、[ネットワーク(Network)]を選択してから、**Enter** を押します。
4. [ポートの順序(Port Order)]を選択してから、Enter を押します。
5. 次の選択肢があります。
   - eth0 に SFP+ ファイバポートを使用するようにアプライアンスを設定するには、[SFP+]を選択します。
   - eth0 に BASE-T 銅線ポートを使用するようにアプライアンスを設定するには、[LOM]を選択します。
6. [OK]を選択して選択を確定します。

次の作業

- eth0 管理ポートの IP アドレスと管理情報を設定します。次の手順を参照してください。

アプライアンスの IP アドレスと管理情報の設定

初回セットアップで、アプライアンスの eth0 管理 IP アドレスと関連情報を設定します。

はじめる前に

- Data Node を設定している場合、ポートの順序を設定すると、初回セットアップウィザードに `eth0` 管理設定が表示されます。ステップ 3 に進みます。

手順

1. システム設定プログラムにログインします。
   - Data Node を設定している場合、`root` と入力してから **Enter** を押します。

     > Data Store と Data Store との互換性を適切に設定するには、`root` 権限が必要です。

   - パスワードプロンプトが表示されたら、**lan1cope** と入力して Enter を押します。
   - 次のプロンプトで、**SystemConfig** と入力し、Enter を押します。
2. このアプライアンスでシステム設定を初めて入力した場合は、初回セットアップが開始されます。

   そうでない場合、[システム設定(System Configuration)]メニューが開きます。[管理(Management)]を選択し、Enter を押します。
3. このアプライアンスの **IP アドレス**を入力します。
4. ネットワークの**ネットマスク**を入力します。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

5. アプライアンスの IP アドレスの**ゲートウェイ**アドレスを入力します。
6. アプライアンスの**ブロードキャスト**アドレスを入力します。
7. アプライアンスの**ホスト名**を入力します。
8. アプライアンスの**ドメイン**を入力します。
9. [選択(Select)]を選択してから、[はい(Yes)]を選択してエントリを確定します。

次の作業

- Data Node の通信ポート管理情報を設定します。詳細については、「**Data Node 間通信用の eth2 および eth3 の設定**」を参照してください。

Data Node 間通信用の eth2 および eth3 の設定

Data Node アプライアンスを設定する場合は、ルーティング不可能な IP アドレスを使用して Data Node 間通信ポートを設定します。次のいずれかを設定できます。

- `eth2`
- `eth2` と `eth3` を含むポートチャネル

> `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。

はじめる前に

- `eth2` および `eth3` SFP+ ポートの詳細については、ご使用のアプライアンスの Stealthwatch 仕様シートを参照してください。`eth2` と `eth3` は、`eth0` の設定方法の影響を受けることに注意してください。
- 初回セットアップの場合、アプライアンスの `eth0` 管理情報の設定が終了すると、[システム設定(System Configuration)]に `eth2` または `eth2/eth3` ポートチャネルの設定が表示されます。ステップ 3 に進みます。

手順

1. [システム設定(System Configuration)]メニューで、[ネットワーク(Network)]を選択してから **Enter** を押します。
2. [ノード通信(Node Communications)]を選択してから、Enter を押します。
3. Data Node 間通信ポートの設定を選択します。次の選択肢があります。
   - Data Node 間通信のポートチャネルとして `eth2` と `eth3` を集約するには、[はい(Yes)]を選択します。
   - Data Node 間通信に `eth2` を使用するには、[いいえ(No)]を選択します。
4. ルーティング不可能な**IP アドレス**を `169.254.42.0/24` CIDR ブロックから `eth2` または `eth2/eth3` ポートチャネル用に入力します。
5. この IP アドレスの**ネットマスク** `255.255.255.0` を入力します。
6. この IP アドレスの**ゲートウェイ**アドレスを入力します。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

7. この IP アドレスの**ブロードキャスト**アドレスを入力します。
8. [選択(Select)]を選択してから、[はい(Yes)]を選択してエントリを確定します。

   これが初回セットアップの最後の設定オプションです。アプライアンスが再起動して変更が実装されます。完了すると、[ログイン(Login)]ページが開きます。

次の作業

- ユーザパスワードを変更します。詳細については、「**sysadmin ユーザパスワードの変更**」を参照してください。

sysadmin ユーザパスワードの変更

ネットワークの安全性を確保するため、アプライアンスのデフォルトの sysadmin パスワードを変更します。

sysadmin パスワードを変更するには、次の手順を実行します。

はじめる前に

- アプライアンスのコンソールに **sysadmin** としてログインします。
- システム設定を開始します。

手順

1. [システム設定(System Configuration)]メニューで、[パスワード(Password)]を選択して Enter を押します。

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

   現在のパスワードのプロンプトがメニューの下に表示されます。
2. 現在のパスワードを入力して、Enter を押します。

   新しいパスワードのプロンプトが表示されます。
3. 新しいパスワードを入力して、Enter を押します。

   パスワードは、スペースを含めずに 8 ～ 30 文字の英数字にする必要があります。次の特殊文字も使用できます。`$.~!@#%_=?:,{}()`
4. パスワードを再度入力して、Enter を押します。
5. パスワードが受け入れられたら、Enter をもう一度押して[システム設定(System Configuration)]メニューに戻ります。
6. 次の「**ルートユーザパスワードの変更**」に進みます。

ルートユーザパスワードの変更

ネットワークのセキュリティをさらに強化するため、デフォルトの sysadmin ユーザパスワードを変更した後、デフォルトのルートユーザパスワードを変更します。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

ルートユーザパスワードを変更するには、次の手順を実行します。

はじめる前に

- アプライアンスのコンソールに **sysadmin** としてログインします。
- システム設定を開始します。

手順

1. ルートシェルに移動します。
2. [システム設定(System Configuration)]メニューで、[詳細設定(Advanced)]を選択し、Enter を押します。[詳細設定(Advanced)]メニューが表示されます。
3. [ルートシェル(RootShell)]を選択して Enter を押します。

   ルート パスワードのプロンプトが表示されます。
4. 現在のルート パスワードを入力して、Enter を押します。ルート シェルのプロンプトが表示されます。
5. **SystemConfig** と入力して、Enter を押します。

   これによって、[システム設定(System Configuration)]メニューに戻り、ルート パスワードを変更できます。
6. [パスワード(Password)]を選択して、Enter を押します。パスワードのプロンプトがメニューの下に表示されます。
7. 新しいルート パスワードを入力して、Enter を押します。2 番目のプロンプトが表示されます。
8. 新しいルート パスワードを再入力して、Enter を押します。
9. パスワードの変更が成功したら、Enter を押します。これで、デフォルトの sysadmin パスワードとルート パスワードの両方が変更されました。これで、[システム設定コンソール(System Configuration Console)]メニューに戻ります。
10. [キャンセル(Cancel)]を選択し、Enter を押します。[システム設定(System Configuration)]コンソールが閉じ、ルート シェル プロンプトが表示されます。
11. **exit** と入力して、Enter キーを押します。ログイン プロンプトが表示されます。
12. Ctrl + Alt を押してコンソール環境を終了します。

アプライアンスを設定できるようになりました。アプライアンスの設定方法については、ご使用のソフトウェアバージョンに該当する『Stealthwatch システム コンフィギュレーション ガイド』を参照してください。x2xx シリーズには、Stealthwatch 7.x ソフトウェアバージョンとの互換性があります。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

付録 C. アプライアンスの設定

初めてアプライアンスにログインする場合、アプライアンス設定ツールを使用してアプライアンス設定を構成します。

アプライアンス設定ツールの要件

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

管理対象

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

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

SMC フェールオーバー

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

- 各 SMC を設定するには、アプライアンス設定ツールを使用します。
- プライマリにする SMC とセカンダリにする SMC を計画します。
- 個々の SMC を設定したら、Central Management 信頼ストアおよび Stealthwatch デスクトップ クライアントを使用して SMC フェールオーバー関係を設定します。

ベスト プラクティス

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

推奨事項は次のとおりです。

- **1 つずつ**：一度に 1 つのアプライアンスを設定します。お使いのクラスタ内で次のアプライアンスの設定を開始する前に、アプライアンスが [アップ（Up）] ステータスであることを確認します。
- **順序**：設定の順序に従います。
- **複数の Central Manager**：システムには複数の Central Manager を設定できます。ただし、各アプライアンスは 1 つのプライマリ SMC/Central Manager のみによって管理できま

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

す。

- **アクセス**: Central Management にアクセスするための管理者権限が必要です。

設定の順序

次の順序でアプライアンスを設定し、各アプライアンスの詳細を書き留めます。

順序	アプライアンス	詳細
1.	プライマリ SMC	プライマリ SMC は、Central Manager です。 システム内で次のアプライアンスの設定を開始する前に、SMC が [アップ(Up)] として表示されていることを確認します。
2.	UDP Director (別名 FlowReplicators)	
3.	Data Node	
4.	Flow Collector 5000 シリーズ データベース	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [アップ(Up)] として表示されていることを確認します。
5.	Flow Collector 5000 シリーズ エンジン	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [アップ(Up)] として表示されていることを確認します。
6.	その他のすべての Flow Collector (NetFlow および sflow)	
7.	Flow Sensor	Flow Sensor の設定を開始する前に、Flow Collector が [アップ(Up)] として表示されていることを確認します。
9.	セカンダリ SMC (使用する場合)	セカンダリ SMC の設定を開始する前に、プライマリ SMC が [アップ(Up)] として表示されていることを確認します。 セカンダリ SMC は、自身を Central Manager として選択します。すべてのアプライアンスの設定後にフェールオーバーを設定します。

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

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

1. ログイン

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

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

   - **プライマリ SMC**：最初にプライマリ SMC を設定します。
   - **アップ**：お使いのクラスタ内で次のアプライアンスの設定を開始する前に、アプライアンスが [アップ（Up）] ステータスであることを確認します。
   - **順番**：アプライアンスが正常に通信するように、必ずそれらを順番どおり設定します。

2. 次のクレデンシャルを入力して、ログインします。

   - **ユーザ名**：admin
   - **パスワード**：lan411cope

2. アプライアンスの設定

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

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

   次の基準を使用します。

   - **長さ**：8 ～ 30 文字
   - **変更**：新しいパスワードがデフォルト パスワードと最低 4 文字異なっていることを確認します。

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

すでにハードウェア設置時にデフォルト パスワードを変更している場合は、[sysadmin] メニューと [root] メニューは使用できません。詳細については、『Stealthwatch x210 Series Hardware Installation Guide』を参照してください。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

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

3. **ホスト名とドメイン**：ホスト名とネットワークドメイン名を入力します。[次へ（Next）] をクリックします。

   - **ホスト名**：各アプライアンスには一意のホスト名が必要です。複数のアプライアンスに同じホスト名を割り当てた場合、それらは正常にインストールされません。
   - **ネットワークドメイン**：各アプライアンスには完全修飾ドメイン名が必要です。
   - **Stealthwatch ドメイン（SMC のみ）**：Stealthwatch アプライアンスの Stealthwatch ドメインを入力します。
   - **IP アドレスの範囲（SMC のみ）**：Stealthwatch ネットワークの IP アドレス範囲を選択します。

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

   DNS サーバの追加または削除（オプション）

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

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

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

   NTP サーバの追加または削除（オプション）

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

6. アプライアンスが SMC の場合は、「3. Stealthwatch Management Console の登録」に進みます。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

アプライアンスが SMC でない場合は、「4. Central Management へのアプライアンスの追加」に進みます。

3. Stealthwatch Management Console の登録

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

   アプライアンスの再起動中は、画面に表示される指示に従います。

   新しいシステム設定が有効になるまで数分待ちます。ページの更新が必要な場合があります。

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

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

6. アプライアンスの設定が完了したら、[ダッシュボードに移動(Go to Dashboard)]をクリックします。
7. [グローバル設定(Global Settings)]アイコンをクリックします。[集中管理(Central Management)]を選択します。
8. インベントリを確認します。SMC アプライアンスのステータスが [アップ(Up)]と表示されていることを確認します。

> ⚠ クラスタ内の次のアプライアンスの設定を開始する前に、プライマリ SMC と各アプライアンスのステータスが [アップ(Up)]として表示されていることを確認してください(設定の順序と詳細を使用)。

9. Data Store を展開して設定します。「Stealthwatch Data Store の導入の概要」に戻って導入プロセスを確認します。

4. Central Management へのアプライアンスの追加

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

1. [集中管理(Central Management)]タブで、プライマリ SMC の IP アドレスを入力します。

   プライマリ SMC は、Central Manager です。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

2. **[保存(Save)]**をクリックします。
3. 画面に表示される指示に従って、プライマリ SMC アプライアンスのアイデンティティ証明書を信頼します。[はい(Yes)]をクリックして証明書を信頼し、アプライアンスと SMC との通信を許可します。
4. プライマリ SMC のログイン クレデンシャルを入力します。
5. Stealthwatch ドメインを選択します。

    - [フローコレクタ(Flow Collectors)]: フロー収集のポート番号を入力します。

      NetFlow のデフォルト: 2055

      sFlow のデフォルト: 6343

    - [フローセンサー(Flow Sensors)]: Flow Collector を選択します。

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

5. アプライアンス ステータスの確認

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

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

    - プライマリ Stealthwatch Management Console にログインします。
    - [グローバル設定(Global Settings)]アイコンをクリックします。
    - [集中管理(Central Management)]を選択します。

2. Appliance Manager インベントリでアプライアンスを確認します。

    - アプライアンスがインベントリに表示されていることを確認します。
    - アプライアンスのステータスが [アップ(Up)]として表示されていることを確認します。

> ⚠ クラスタ内の次のアプライアンスの設定を開始する前に、プライマリ SMC と各アプライアンスのステータスが [アップ(Up)]として表示されていることを確認してください(設定の順序と詳細を使用)。

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

    セットアップするアプライアンスがほかになければ、『Stealthwatch System Configuration Guide』でアプライアンス設定を完了する方法の詳細を確認します。または、「Stealthwatch Data Store の導入の概要」に戻って導入プロセスを確認します。

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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）

© 2021 Cisco Systems, Inc. and/or its affiliates.
All rights reserved.