Cisco Secure Network Analytics

更新ガイド 7.5.0

目次

はじめに

概要

次の Cisco Secure Network Analytics（旧 Stealthwatch）アプライアンスをバージョン **7.4.0**, **7.4.1**, **7.4.2** to **7.5.0** に更新するには、このガイドを使用します。

- UDP Director（別名 Flow Replicator）
- Data Store

> Data Node の更新手順は、この更新に固有の手順です。Data Store を展開している場合は、必ず手順に従ってください。

- Flow Collector
- Flow Sensor
- マネージャ

v7.4.0 では、Cisco Stealthwatch Enterprise 製品のブランド名を Cisco Secure Network Analytics に変更しました。詳細なリストについては、次を参照してください。リリースノート。このガイドでは、以前の製品名である Stealthwatch が必要に応じて明確さを維持するために使用され、Stealthwatch Management Console や SMC などの用語も使用されています。

対象読者

このガイドは、Secure Network Analytics 製品の更新を担当するネットワーク管理者とその他の担当者を対象としています。

用語

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

また「**クラスタ**」は、Manager が管理するアプライアンスのグループです。アプライアンスが Manager によって管理されている場合は、[集中管理（Central Management）] のインベントリに表示されます。

> Secure Network Analytics v7.5.0 の詳細については、リリースノートを参照してください。

最新情報

システムの更新に慣れている方は、前回のアップグレード以降に以下の変更が行われていることを確認してください。

- アップグレード、更新、および初期状態へのリセットのパフォーマンスが向上しました。
- スマートライセンスのトランスポート設定要件が変更されました。アプライアンスが smartreceiver.cisco.com に接続できることを確認します。
- 更新プロセスを開始する前に、システム内のすべてのアプライアンスが 1 か月（30 日）の基準となる要件を満たしていることを確認してください。

- v7.5.0 の VE 展開には、新しい CPU 命令セット要件があります。CPU が AVX/AVX2 命令セットに対応していることを確認します。ESXi の場合は、VM ハードウェアバージョン 11 以上を選択します。KVM の場合は、ホストパススルーを使用することを推奨します。
- SWU ファイルのインストールを開始する前に、必ず すべての SWU ファイルをアップロードしてください。
- プライマリ Manager が正常に更新されると、正常にアップグレードされたすべてのアプライアンスについて、Appliance Manager のアプライアンスステータスが [接続済み（Connected）] と表示されることに注意してください。詳細については、「**通信**」を参照してください。
- 更新プロセスを開始する前に、必ず**シスコのバンドル**パッチをインストールし、**CIMC ファームウェアバージョン**を更新してください。
- 更新プロセスを開始する前に、ISE 証明書チェーンが完全であることを確認してください。詳細については、「**Identify Services Engine（ISE）または ISE-PIC**」を参照してください。
- v7.4.1 から v7.5.0 にアップグレードする場合、Analytics データは引き継がれません。v7.4.2 の Analytics データは v7.5.0 に引き継がれます。Analytics の詳細については、「Analytics：検出、アラート、および観測」を参照してください。
- 更新の際、MongoDB は v6.0.9 にアップグレードされます。「**MongoDB のアップグレード**」を参照してください。
- 複数の UDP Director がある場合は、「**10. 高可用性の設定**」を参照してください。
- Data Node に v7.4.1 以降がインストールされている場合は、手順に従って、[すべてのData Nodeを更新する（Update all Data Nodes）] ボタンを使用して Data Node を同時に更新します。更新 SWU ファイルが**すべて**のデータノードに正常にインストールされた後に、必ずデータノードで Vertica を再起動してください。
- システムを 7.5.0 に更新すると、ルートユーザーアクセスとアプライアンス セットアップ ツールが削除されます。詳細については、「リリースノート」を参照してください。

はじめる前に

更新プロセスを開始する前に、このガイドを参照してプロセス、および v7.5.0 に正常に更新するために必要な準備、時間、リソースについて確認してください。

ソフトウェア バージョン

アプライアンスソフトウェアをバージョン 7.5.0 に更新するには、アプライアンスにバージョン **7.4.0**、**7.4.1**、または **7.4.2** がインストールされている必要があります。このガイドの手順では、各アプライアンスのソフトウェア バージョンの確認方法について説明します。以下の点にも注意してください。

- **ベースライン**：この更新を開始する前に、アプライアンスが同じバージョンの **v7.4.0**、**v7.4.1**、または **v7.4.2** で 1 か月（30 日）以上実行されていることを確認してください。短期間にシステムを複数のバージョンに更新した場合、システムのベースラインが影響を受ける可能性があります。サポートが必要な場合は、シスコサポートまでお問い合わせください。
- パッチ：更新プロセスの一環として、必要なロールアップパッチをアプライアンスにインストールします。

> ⚠ 必要なパッチが各アプライアンスにインストールされるまでに最大 90 分かかることがあります。

- **ダウングレード**：更新すると、更新時にインストールされる新機能をサポートするために必要な変更がデータ構造や設定に対して行われるため、バージョンのダウングレードはサポートされていません。
- **TLS**：Secure Network Analytics TLS v1.2 が必要です。v7.5.0 へのアップグレード後、TLS v1.2 と TLS v1.3 の両方がデフォルトでサポートされます。手順については、『SSL/TLS Certificates for Managed Appliances Guide』[英語] を参照してください。
- **サードパーティ製アプリケーション**：Secure Network Analytics は、アプライアンスへのサードパーティ製アプリケーションのインストールをサポートしていません。

Cisco Software Central

ライセンスの管理、パッチのダウンロード、および Secure Network Analytics v7.5.0 の更新ファイルのダウンロードについては、https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

スマートライセンス

更新を開始する前に、アプライアンスのライセンスが最新であることを確認します。

- **7.4.0、7.4.1 での確認**：Manager にログインします。[グローバル設定（Global Settings）] アイコン > [Central Management] > [スマートライセンス（Smart Licensing）] を選択します。[スマートライセンスの使用状況（Smart License Usage）] セクションを確認します。
- **7.4.2 での確認**：Manager にログインします。[構成（Configure）] > [グローバル（GLOBAL）] > [集中管理（Central Management）] > [スマートライセンス（Smart Licensing）]を選択します。[スマートライセンスの使用状況（Smart License Usage）] セクションを確認します。
- **手順**：ライセンスがコンプライアンス違反または期限切れと表示されている場合は、スマートソフトウェア ライセンシング ガイド [英語] を参照してください。

スマートライセンスのトランスポート設定

スマートライセンスのトランスポート設定要件が変更されました。

> ⚠ アプライアンスを v7.4.1 以前からアップグレードする場合は、アプライアンスが smartreceiver.cisco.com に接続できることを確認してください。

サポートされているハードウェア プラットフォーム

各システム バージョンでサポートされているハードウェア プラットフォームについては、Hardware and Version Support Matrix を参照してください。

CIMC ファームウェアバージョン

次の表に示すアプライアンスの場合、M4 共通更新プロセスは UCS C シリーズ M4 ハードウェアに適用され、M5 共通更新パッチは M5 ハードウェアに適用され、M6 共通更新パッチは M6 ハードウェアに適用されます。

> ⚠ Cisco.com に掲載されている標準の UCS ファームウェア更新情報は使用しないでください。

M4 ハードウェア	M5 ハードウェア	M6 ハードウェア
SMC 2200（Manager 2200）	SMC 2210（Manager 2210）	SMC 2300（Manager 2300）
FC 4200	FC 4210	FC 4300
FC 5020 エンジン	_	_
FC 5020 データベース	_	_
FC 5200 エンジン	FC 5210 エンジン	_
FC 5200 データベース	FC 5210 データベース	_
FS 1200	FS 1210	FS1300
FS 2200	_	_
FS 3200	FS 3210	FS3300
FS 4200	FS 4210 / FS 4240	FS4300
UD 2200	UD 2210	_
_	DS6200	DN6300

「**2. パッチのダウンロード**」手順に従ってください。ただし、手順 3 では、[すべてのリリース(All Releases)] 列で [ファームウェア(Firmware)] を選択して、最新の CIMC ファームウェアバージョンの共通更新パッチにアクセスします。

詳細については、Cisco.com の「Release Notes」ページの「Common Patch Readmes」セクションに移動して該当する readme を見つけてください。

アプリケーションのバージョンの互換性

> 以前にアプリをインストールしたことがある場合は、インストールする Secure Network Analytics のバージョンと互換性があることを確認します。

インストールされているアプリのリストを確認する方法と最新の Cisco Secure Network Analytics アプリの互換性情報を確認する方法については、Secure Network Analytics アプリのバージョン互換性マトリックスを参照してください。

セキュリティ分析とロギング(オンプレミス)

Secure Network Analytics v7.5.0 に正常に更新されたら、必ず セキュリティ分析とロギング(オンプレミス) v3.3.0 にアップグレードしてください。セキュリティ分析とロギング(オンプレミス) 展開の詳細については、次のドキュメントを参照してください。

- セキュリティ分析とロギング(オンプレミス)のリリースノート
- Cisco Security Analytics and Logging(オンプレミス)スタートアップガイド
- セキュリティ分析とロギング(オンプレミス):Firepower イベント統合ガイド

分析

v7.4.1 から v7.5.0 にアップグレードする場合、Analytics データは引き継がれません。v7.4.2 の Analytics データは v7.5.0 に引き継がれます。Analytics の詳細については、「Analytics:検出、アラート、および観測」を参照してください。

VMware バージョンの互換性

Secure Network Analytics v7.5 は、VMware v7.0 または 8.0 と互換性があります。VMware v6.0、v6.5、または v6.7 と Secure Network Analytics v7.5.x はサポートしていません。詳細については、『vSphere 6.0, 6.5, and 6.7 End of General Support』の VMware のマニュアルを参照してください。

- 更新前:Secure Network Analytics アプライアンスが VMware v6.0、v6.5、または v6.7 にインストールされている場合は、Secure Network Analytics を v7.5.x にアップグレードする前に、VMware vCenter と ESXi ホスト を v7.0 または v8.0 にアップグレードします。
- 確認:「**1. VMware バージョンの確認**」と、「**2. VMware ホストの確認**」を参照して VMware 環境を確認します。
- 更新後:Secure Network Analytics v7.5.x の更新後に、VMware にオペレーティングシステムのエラーが表示される場合があります。VMware の GUI を確認し、VMware vCenter が v7.0 または v8.0 であること、およびオペレーティングシステムが Debian v10 であることを確認します。VMware vCenter またはオペレーティングシステムをアップグレードするには、VMware ガイドを参照してください。
- ホストからホストへのライブマイグレーション(vMotion などを使用)はサポートされていません。
- スナップショット:仮想マシンのスナップショットはサポートされていません。

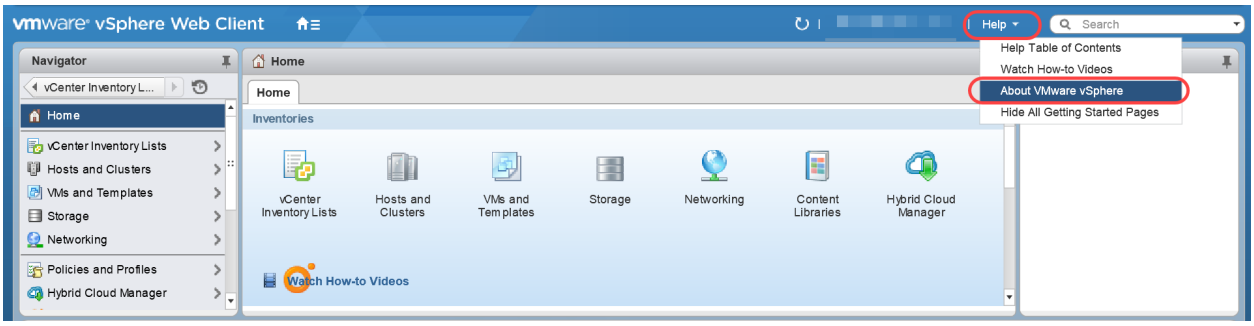
すでにインストールされているカスタムバージョンが上書きされるため、Secure Network Analytics 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

1. VMware バージョンの確認

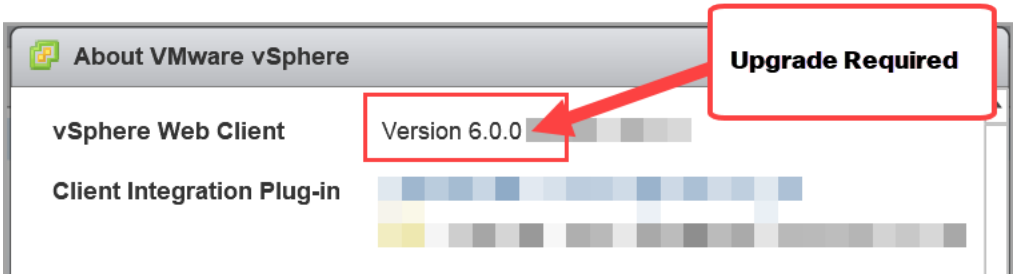
次の手順に従って、VMware vSphere vCenter v7.0 または v8.0 がインストールされていることを確認します。

VMware UI のメニューとグラフィックは、ここに表示されているものと異なる場合があります。ご使用の環境に固有の詳細な点については、VMware ガイドを参照してください。

1. VMware Web クライアントにログインします。
2. [ホーム（Home）] ページで [vCenter インベントリリスト（vCenter Inventory Lists）] を選択します。
3. [ヘルプ（Help）] > [VMware vSphere バージョン情報（About VMware vSphere）] を選択します。



4. **Web クライアント**のバージョンを確認します。v6.0、v6.5、または v6.7 の場合は、v7.0 または v8.0 にアップグレードする必要があります。手順については、VMware ガイドを参照してください。



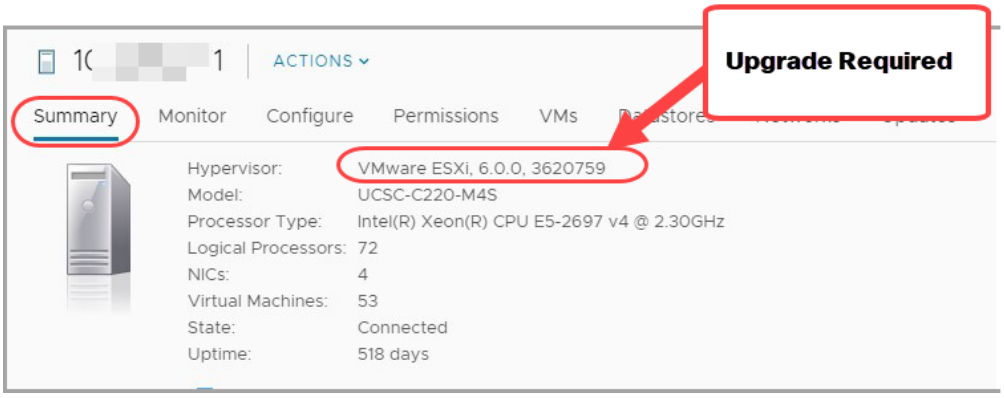
5. 次の項に進みます。

2. VMware ホストの確認

次の手順に従って ESXi ホストを確認し、v7.0 または v8.0 がインストールされていることを確認します。Secure Network Analytics アプライアンスが複数のホストにインストールされている場合は、各ホストを確認します。

VMware UI のメニューとグラフィックの一部は、ここに示す情報とは異なる場合があります。ソフトウェアに関する詳細については、VMware ガイドを参照してください。

1. [ナビゲータ(Navigator)] ペインで [vCenter インベントリリスト(vCenter Inventory Lists)] を選択します。
2. [ホスト(Hosts)] を選択します。
3. ホスト名をクリックします。
4. [サマリー(Summary)] タブをクリックします。



5. **ハイパーバイザ** のバージョンを確認します。v6.0、v6.5、または v6.7 の場合は、v7.0 または 8.0 にアップグレードする必要があります。手順については、VMware ガイドを参照してください。
6. Secure Network Analytics アプライアンスがインストールされている他のホストに対して手順 1 ～ 5 を繰り返します。

互換性のあるブラウザ

- **互換性のあるブラウザ**:Secure Network Analytics は Chrome、Firefox、および Microsoft Edge の最新のラピッドリリースをサポートしています。
- **Microsoft Edge**:Microsoft Edge には、ファイル サイズの制限がある可能性があります。Microsoft Edge を使用して、ソフトウェア アップデート ファイル(SWU)をアップロードしないことをお勧めします。
- **ショートカット**:ブラウザのショートカットを使用して、いずれかの Secure Network Analytics アプライアンスのアプライアンス管理インターフェイスにアクセスしている場合、更新プロセスの完了後はショートカットが機能しないことがあります。その場合は、ショートカットを一旦削除してから再作成してください。
- **証明書**:一部のブラウザでは、アプライアンス アイデンティティ証明書の有効期限の要件が変更されています。アプライアンスにアクセスできない場合は、『SSL/TLS Certificates for Managed Appliances Guide』を参照して証明書を置き換えるか、Cisco サポートまでお問い合わせください。

代替アクセス

> ⚠ 今後のサービスのニーズを想定し、Secure Network Analytics アプライアンスにアクセスする代替方法を有効にしておく必要があります。

次のいずれかのオプションを使用して Secure Network Analytics アプライアンスにアクセスできることを確認してください。

仮想アプライアンス：コンソール（コンソールポートへのシリアル接続）

KVM を介してアプライアンスにアクセスするには、『Virtual Edition Appliance Installation Guide』[英語] を参照してください。または、VMware を介してアプライアンスに接続するには、vSphere の vCenter Server Appliance 管理インターフェイスのドキュメントを参照してください。

ハードウェア：コンソール（コンソールポートへのシリアル接続）

ラップトップまたはモニター付きキーボードを使用してアプライアンスに接続するには、『Install and Upgrade Guides』ページ [英語] に掲載されている最新の Secure Network Analytics ハードウェア設置ガイドを参照してください。

ハードウェア：CIMC（UCS アプライアンス）

CIMC を介してアプライアンスにアクセスするには、『Cisco Integrated Management Controller (CIMC) Configuration Guides』ページにリストされているプラットフォームの最新のガイドを参照してください。

別の方法

今後サービスが必要になった場合に備えて、次の手順に従い、Secure Network Analytics アプライアンスにアクセスする別の方法を有効にします。

仮想またはハードウェアの方法を使用してアプライアンスにログインできない場合は、アプライアンスのネットワーク インターフェイスで一時的に SSH を有効にできます。

> ⚠ 停電後、データベースをアップグレードまたは起動する前に、[SSH の有効化（Enable SSH）] オプションを選択して、すべての Data Node で SSH が有効になっていることを確認する必要があります。SSH を有効にすると、システムの侵害リスクが増加します。SSH は必要な場合のみ有効にすることが重要です。SSH は、使用終了後に無効にします。

次の手順に従って、選択したアプライアンスの SSH を開いて有効にします。

1. [集中管理（Central Management）] > [アプライアンスマネージャ（Appliance Manager）] を開きます。
2. アプライアンスの [アクション（Actions）] メニューをクリックします。
3. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
4. [アプライアンス（Appliance）] タブを選択します。
5. [SSH] セクションを見つけます。
6. アプライアンスへの SSH アクセスを許可するには、[SSHの有効化（Enable SSH）] チェックボックスをオンにします。
7. [設定の適用（Apply settings）] をクリックします。
8. 画面に表示される指示に従って、変更を保存します。

> ⚠ SSH は、使用が終了したら必ず無効にしてください。

証明書の有効性

更新プロセスを開始する前に、アプライアンス アイデンティティ証明書が有効であり、最新のものであることを確認します。無効または期限切れのアプライアンス アイデンティティ証明書では、アプライアンスを更新できません。アプライアンス アイデンティティ証明書を置き換えるには、管理対象アプライアンスの SSL/TLS 証明書ガイド [英語] の手順に従います。

アプライアンス アイデンティティの要件	
フォーマット	PEM（.cer、.crt、.pem）または PKCS#12（.p12、.pfx、.pks）
RSA キーの長さ	4096 ビットまたは 8192 ビット
共通名または **Subject Alternative Name**	共通名またはサブジェクトの別名が FQDN と一致することを確認します。
認証	サーバーとクライアントの認証は、アプライアンス アイデンティティ証明書に必要です。

シスコのバンドル

最新のシスコのバンドルに共通の更新パッチがインストールされていることを確認してください。詳細については、Cisco Bundles Common Update Patch の readme を参照してください。パッチには、以下の特徴があります：

- 厳選したルート認証局（CA）の事前検証済みのデジタル証明書を提供しています。これには、
- シスコのサービスとの接続に使用するコア証明書バンドルと、シスコ以外のサービスとの接続に使用する外部証明書バンドルが含まれます。

「**2. パッチのダウンロード**」手順に従ってください。ただし、手順 3 では、[最新リリース（Latest Release）] 列で [証明書バンドル（Certificate Bundles）] を選択して、最新のシスコのバンドルの共通更新パッチにアクセスします。

Data Store

展開に Data Store が含まれている場合は、更新を開始する前に、すべての Data Node で SSH が有効になっていることを確認してください。

- **SSH の有効化**：「**代替アクセス**」の手順に従って、すべての Data Node で SSH を有効にし、[SSHの有効化（Enabling SSH）] チェックボックスをオンにします。
- **SSH の無効化**：Data Node で SSH を無効にする場合は、アップグレードプロセスとパッチのインストールが完了したら、Data Node ごとに SSH を無効にできます。
- **すべての Data Node v7.4.1 以降を更新する**：v7.4.1 以降がインストールされている場合は、指示に従って、[すべてのData Nodeを更新する（Update all Data Nodes）] ボタンを使用して Data Node を同時に更新します。このボタンを使用して、パッチと SWU ファイルをインストールします。パッチのインストール後に Data Store データベースを開始する必要がある場合がありますが、更新 SWU がすべての Data Node に正常にインストールされた後に自動的に開始されます。

- **ダウンタイム**：この更新に必要なダウンタイムについて懸念がある場合は、シスコサポートにお問い合わせください。

Data Store のプライベート LAN の設定と Data Node の拡張

v7.4.1 以降、Secure Network Analytics は プライベート LAN の IP アドレスに特定の要件を適用します。プライベート LAN の IP アドレスを使用して設定されている Data Node のすべてが次の要件を満たしていることを確認してください。

- 最初の 3 オクテットが **169.254.42** であること。
- サブネットが **/24** であること。

> 例：169.254.42.**x**/24（**x** はサイトによって割り当てられた番号（2 ～ 255））

詳細については、シスコサポートに問い合わせてください。

Identify Services Engine（ISE）または ISE-PIC

> v7.5.0 に更新する前に、ISE の証明書チェーンが完全であることを確認してください。詳細については、Cisco Secure Network Analytics ISE および ISE-PIC コンフィギュレーション ガイド 7.5.0 [英語] の 5 ページから始まる「Option 1 – Deploying Certificates Using ISE Internal Certificate Authority (Recommended)」セクションを参照してください。手動同期を実行して、ISE のレプリケーションアラームの問題も修正してください。詳細については、『リリースノート』の「既知の問題」セクションに記載されている関連する ISE 統合の問題を参照してください。

- **要件**：Manager で ISE または ISE-PIC を使用している場合は、クライアントグループに適応型ネットワーク制御（ANC）が含まれていることを確認してから更新を開始してください。
- **確認**：ISE クライアントにログインします。[管理（Administration）] > [pxGrid サービス（pxGrid Services）] の順に選択します。[Manager] > [クライアントグループ（Client Group）] 列で、リスト内の各 Manager を確認します。シスコ適応型ネットワーク制御（ANC）が表示されていない場合は、[Manager] チェックボックスをオンにして選択します。[グループ（Group）] をクリックして ANC を [グループ（Group）] フィールドに追加し、[保存（Save）] をクリックします。

> ANC はデフォルトで無効になっており、pxGrid が有効になっている場合にのみ有効にできます。ANC を有効にした後で無効にするには、管理ポータルから手動でサービスを無効にしてください。

- **ガイド**：詳細については、Cisco Secure Network Analytics ISE および ISE-PIC コンフィギュレーション ガイド 7.4 [英語] および『Cisco Identity Services Engine Administrator Guide, Release 2.2』[英語] を参照してください。ISEに関する追加の製品情報については、Cisco Identity Services Engine ページにアクセスしてください。

ディスク容量

更新の準備の一環として、パッチとソフトウェア更新ファイルをインストールするための十分な空きディスク容量が各アプライアンスにあることを確認します。詳細については、「**7. 使用可能なディスク容量の確認**」を参照してください。

- **要件**：管理対象アプライアンスごとに、個々のソフトウェア更新ファイル（SWU）の 4 倍以上のサイズが必要です。Manager では、Update Manager にアップロードするすべてのアプライアンス SWU ファイルの 4 倍以上のサイズが必要です。
- **管理対象アプライアンス**：たとえば、Flow Collector の SWU ファイルが 6 GB の場合、Flow Collector（/lancope/var）パーティションで少なくとも 24 GB の空き容量が必要です（1 つの SWU ファイル x 6 GB x 4 = 24 GB）。
- **Manager**：たとえば、それぞれ 6 GB の 4 つの SWU ファイルをアップロードする場合、/lancope/var パーティションに少なくとも 96 GB の空き容量が必要です（4 つの SWU ファイル X 6 GB X 4 = 96 GB）。

ホスト名

- **要件**：各アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは更新できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。
- **確認**：Manager にログインしてから、[グローバル設定（Global Settings）] アイコン > [集中管理（Central Management）] の順に選択します。各アプライアンスの [ホスト名（Host Name）] 列を確認します。

ドメイン名

- **要件**：各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスは更新できません。
- **確認**：Manager にログインしてから、[グローバル設定（Global Settings）] アイコン > [集中管理（Central Management）] の順に選択します。アプライアンスの [アクション（Actions）] 列の [••• （**省略符号**）アイコン] をクリックします。[アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。[アプライアンス（Appliance）] タブで、[ホスト名（Host Naming）] を確認します。

NTP サーバー

- **要件**：各アプライアンスに少なくとも 1 台の NTP サーバーが必要です。
- **確認**：Manager にログインしてから、[グローバル設定（Global Settings）] アイコン > [集中管理（Central Management）] の順に選択します。アプライアンスの [アクション（Actions）] 列の [••• （**省略符号**）アイコン] をクリックします。[アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。[ネットワークサービス（Network Services）] タブで、[NTP サーバー（NTP Server）] を確認します。
- **問題のある NTP**：130.126.24.53 NTP サーバーがサーバーのリストに含まれている場合は削除します。このサーバーには問題があることが判明しており、シスコのデフォルトの NTP サーバー リストからはすでに除外されています。

タイム ゾーン

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

すべてのアプライアンスは協定世界時（UTC）を使用します。

- **要件**：更新を開始する前に、アプライアンスが UTC に設定されていることを確認します。
- **仮想ホストサーバー**：仮想ホストサーバーが、UTC に対して正しい時刻に設定されていることを確認します。

アプライアンスとデータベースのバックアップ

システムをバックアップするための時間を計画してください。バックアップファイルは、更新で問題が発生した場合に必要です。診断パックは、シスコサポートによるトラブルシューティング時に必要になります。

> ⚠ バックアップしていないと、更新プロセス中に問題が発生した場合にファイルを回復できません。また、診断パックは、シスコサポートによるトラブルシューティングが必要な場合に役立ちます。

このガイドでは、次の手順について説明します。

- 各アプライアンスのバックアップ
- 診断パックの作成
- Manager データベースのバックアップ
- Flow Collector データベースのバックアップ
- Data Store のバックアップ

バックアップ手順の一環として、各データベースのバックアップの前後に、Manager と Flow Collector のデータベース スナップショットを削除します。また、Flow Collector のバックアップ手順には、データベースのトリミングも含まれています。

詳細については、「5. Manager と Flow Collector のデータベースのバックアップ」を参照してください。

> ⚠ Data Store が導入されている場合は、Flow Collector データベースの代わりに Data Store データベースをバックアップします。詳細については、「6. Data Store のバックアップ」を参照してください。

MongoDB のアップグレード

更新の前に CPU 設定の確認が実行されます。更新の際、MongoDB は v6.0.9 にアップグレードされます。

CPU 命令セット要件：CPU が AVX/AVX2 命令セットに対応していることを確認します。ESXi の場合は、VM ハードウェアバージョン 11 以上を選択します。KVM の場合は、ホストパススルーを使用することを推奨します。

更新に最適な時間

アプライアンスを更新するための時間とリソースを計画する際には、次の点を検討してください。

ソフトウェア アップデート ファイル

パッチおよびソフトウェア アップデート ファイルのダウンロードには時間がかかります。これらは事前にダウンロードできます。詳細については、「**2. パッチと更新ファイルのダウンロード**」を参照してください。

すべてのアプライアンス

- **時間**:この更新のパッチが各アプライアンスにインストールされるまでに最大 90 分かかることがあります。ソフトウェアの更新プロセスは、アプライアンスごとに完了するまで約 30 分かかります。ただし、ネットワークの状況によって長くなることがあります。この概算時間には、ユーザー環境によって異なるバックアップと診断パックの作成に必要な時間は含まれていません。
- **少量**:システムのトラフィック量が比較的少ないときに、システム全体を一度に更新することをお勧めします。
- **再起動**:アプライアンスは、再起動プロセス中はデータを収集しません。ただし、現在のデータは保持されます。

Manager と Flow Collector

- **Flow Collector**:Flow Collector を更新して実行すると、Manager が更新されるまで、Manager に送信されるデータが Flow Collector にキャッシュされます。ただし、更新プロセスはできる限り短時間で終わらせたいものです。そのため、すべてのアプライアンスの準備を整えて一度に更新するのが、最も成功するアプローチであると言えます。

> ⚠ [集中管理(Central Management)] から Flow Collector を削除しないでください。削除すると、それらの Flow Collector のすべての履歴データが Manager から消失します。

通信

更新プロセスの実行中は Manager とアプライアンス間の通信が停止し、更新と再起動が行われます。

[集中管理(Central Management)] のインベントリでは、アプライアンスのステータスが [構成チャネルのダウン(Config Channel Down)] に変わります。更新が完了すると、通信が再確立され、アプライアンスのステータスが [接続済み(Connected)] に戻ります。「**9. v7.5.0 ソフトウェアアップデートのインストール**」を参照してください。

> ⚠ クラスタ内で次のアプライアンスを設定する前に、アプライアンスのステータスが [接続済み(Connected)] になっていることを確認します。

更新プロセスの概要

> ⚠ 各パッチおよび SWU ファイルについて、ソフトウェアのインストール順序に必ず従ってください。更新を成功させるためには、このガイドの手順に従うことが重要です。

更新を成功させ、データ損失を最小限に抑えるためには、手順を順番に実行する必要があります。

1. クラスタの確認
2. パッチと更新ファイルのダウンロード
3. アプライアンスの設定のバックアップ
4. 診断パックの作成
5. Manager と Flow Collector のデータベースのバックアップ
6. Data Store のバックアップ
7. 使用可能なディスク容量の確認
8. パッチのインストール
9. v7.5.0 ソフトウェアアップデートのインストール
10. 高可用性の設定
11. デスクトップクライアントのインストール
12. Manager フェールオーバーロールの確認

1. クラスタの確認

> ⚠ すべてのアプライアンスに正しいソフトウェア バージョンがインストールされていることを確認します。これは、更新を成功させるために不可欠な手順です。

クラスタを確認して、各アプライアンスのソフトウェアバージョンを確認します。各アプライアンスの現在のソフトウェアバージョンが **7.4.0**、**7.4.1**、または **7.4.2** であることを確認するには、以下の手順を実行します。

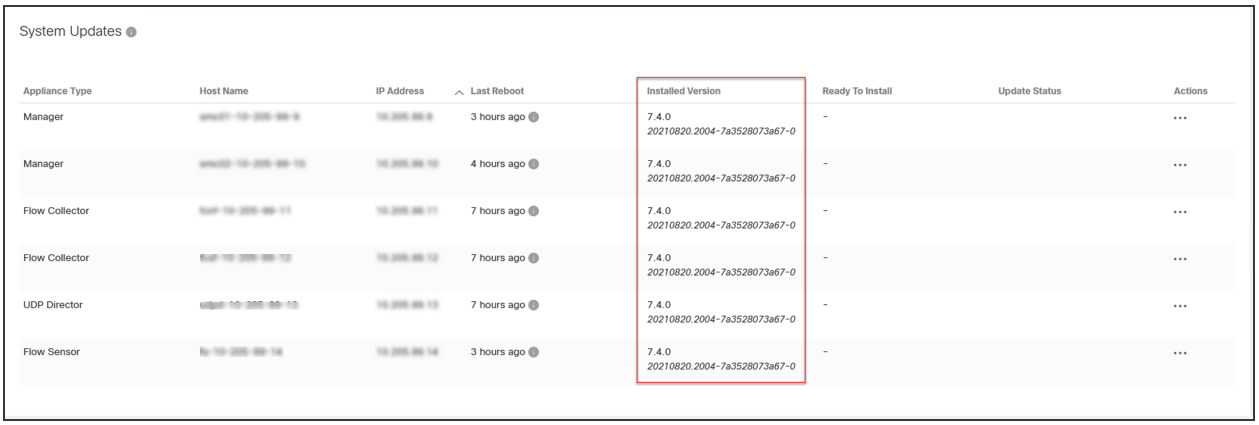
1. Manager の IP アドレスを使用して、管理者として Manager にログインします。

   ブラウザのアドレスバーに https://<Manager IP address> と入力します。

2. **7.4.0 および 7.4.1**：[⚙（**グローバル設定**）アイコン] をクリックします。[集中管理（Central Management）] を選択します。

   7.4.2：[構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] を選択します。

3. [アップデートマネージャ（Update Manager）] タブを選択し、[システムアップデート（System Updates）] セクションを見つけます。



> ⚠ 更新プロセスを開始した後は、アプライアンスの追加または削除、クラスタ設定の変更、アプライアンスでの設定変更、アプライアンスのフェールオーバーロールの変更は行わないでください。

2. パッチと更新ファイルのダウンロード

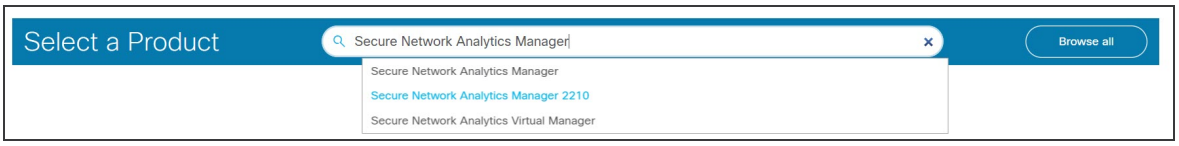
ライセンスを管理するには、パッチをダウンロードし、更新ファイルをダウンロードして、Cisco スマートアカウント（https://software.cisco.com）にログインします。

次の手順に従って、アカウントに記載されているパッチと v7.5.0 SWU をダウンロードします。

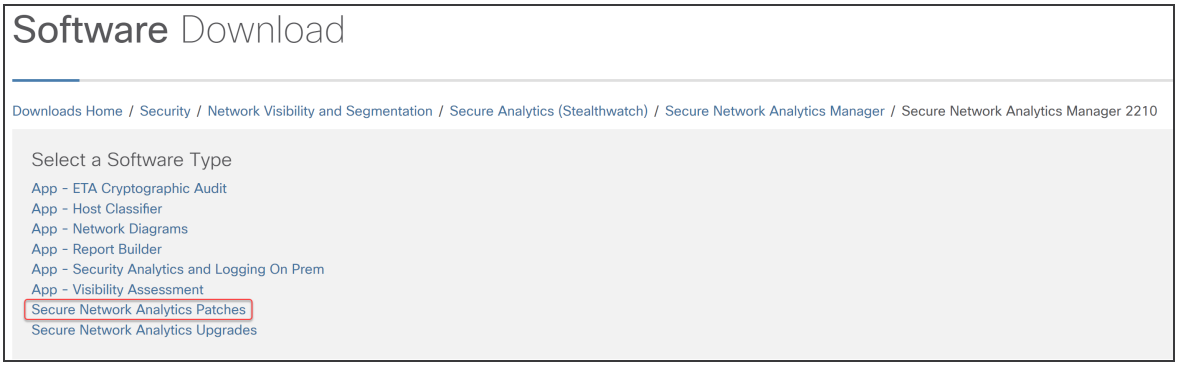
1. Cisco Software Central へのログイン

1. https://software.cisco.com で Cisco Software Central にログインします。
2. [ダウンロードとアップグレード（Download and Upgrade）] セクションの [ダウンロードと管理（Download and manage）] ページで、[ダウンロードにアクセス（Access downloads）] を選択します。
3. [製品の選択（Select a Product）] フィールドに **Secure Network Analytics** と入力し、アプライアンスを選択します。

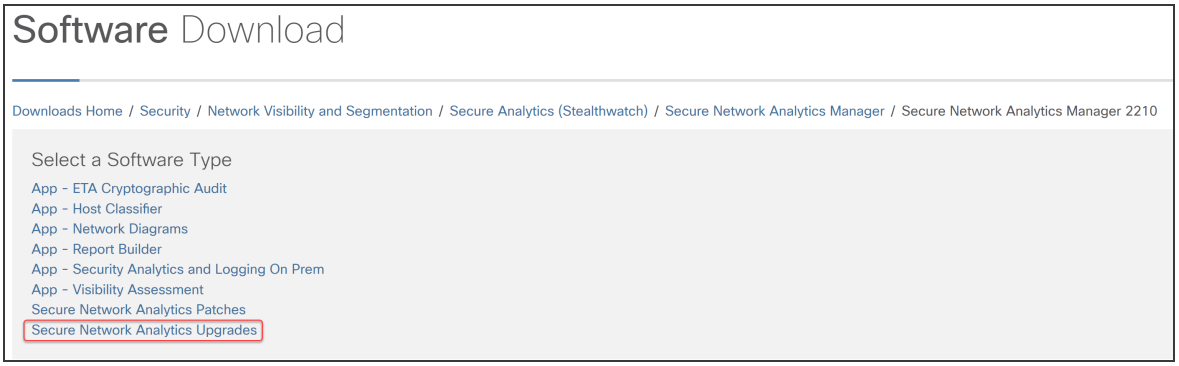
   次の例のように、製品名を入力するときにアプライアンスを含めることもできます。



4. [ソフトウェアのダウンロード（Download Software）] ページが表示されます。
   - 更新プロセスを開始する前に、[Secure Network Analyticsパッチ（Secure Network Analytics Patches）] を選択して適用する必要があるパッチファイルにアクセスします。



- または、[Secure Network Analyticsのアップグレード（Secure Network Analytics Upgrade）]を選択して更新ファイルにアクセスします。

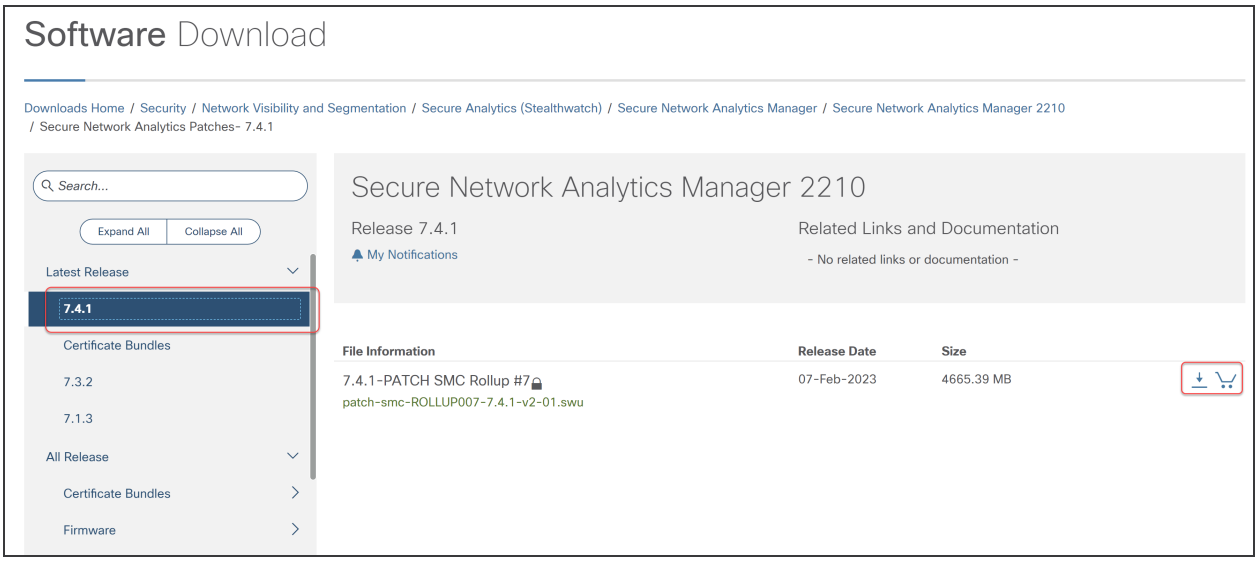


2. パッチのダウンロード

更新プロセスを開始する前に、[Secure Network Analyticsパッチ（Secure Network Analytics Patches）]を選択して適用する必要があるパッチにアクセスします。詳細については、パッチの readme を参照してください。

[Secure Network Analyticsパッチ（Secure Network Analytics Patches）]を選択すると、アプライアンスのページが表示されます。

1. アプライアンスに現在インストールされている Secure Network Analytics のバージョンを選択します。たとえば、アプライアンスに 7.4.1 がインストールされている場合は、[7.4.1] を選択します。



2. **ダウンロード**:[ダウンロード(Download)] アイコンをクリックするか、または [カートに追加(Add to Cart)] アイコンをクリックします。

   選択したアプライアンスのすべてのパッチをダウンロードします。

> 各アプライアンスの最新のロールアップパッチ、および必要な共通更新パッチ、CIMC ファームウェア更新パッチ、およびシスコのバンドルパッチを含む、現在のバージョンのすべてのパッチをダウンロードしてください。

3. これらの手順を繰り返して、クラスタ内のすべてのアプライアンスにすべてのパッチをダウンロードします。この更新に必要なすべてのファイルがダウンロードされていることを確認するには、**SWU ファイル**の表を参照してください。

3. 更新ファイルのダウンロード

> 特定のバージョンのファイルすべてにアクセスする最も効率的な方法としては、最初に Manager を選択します。

[Secure Network Analyticsのアップグレード(**Secure Network Analytics Upgrades**)] を選択すると、アプライアンスページが表示されます。

1. [7.5.0] を選択します。
2. **ダウンロード**:[ダウンロード(Download)] アイコンをクリックするか、または [カートに追加(Add to Cart)] アイコンをクリックします。
   - **選択したアプライアンス**:アプライアンスに表示されている更新ファイルをダウンロードします。
   - **関連ソフトウェア**:[関連ソフトウェア(Related Software)] セクションを使用して、その他すべてのアプライアンスの更新ファイルをダウンロードします。このセクションにパッチが表示されている場合は、更新後にそれらのパッチをインストールします。
3. この更新に必要なすべてのファイルがダウンロードされていることを確認するには、**SWU ファイル**の表を参照してください。何らかの更新ファイルがない場合は、これらの手順を繰り返して、別のアプライアンスの更新ファイルをダウンロードします。

SWU ファイル

この更新に必要なすべてのファイルがダウンロードされていることを確認します。ファイルが不足している場合は、「**2. パッチと更新ファイルのダウンロード**」を参照してください。

アプライアンス	**v7.4.0、v7.4.1、または v7.4.2 からの更新 ソフトウェア更新 ファイル名**
UDP Director （別名 Flow Replicator） UDP Director VE （別名 Flow Replicator VE）	update-udpd-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
データノード	update-dnode-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
Flow Collector データベース 5000 シリーズ	update-fcdb-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
Flow Collector（NetFlow） （Flow Collector 5000 シリーズ エンジンに必要） Flow Collector（NetFlow） VE	update-fcnf-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
Flow Collector（sFlow） Flow Collector（sFlow） VE	update-fcsf-7.5.0.20231114.0021-18dba09f721e-D-v2-01.swu
フローセンサー Flow Sensor VE	update-fsuf-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
Manager Manager VE	update-smc-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu

3. アプライアンスの設定のバックアップ

バックアップしていないと、更新プロセス中に問題が発生した場合にファイルを回復できません。これらの手順は、データ損失を最小限に抑えるために重要です。

> 各アプライアンスの設定を必ずバックアップしてください。

次の手順に従って、[アプライアンス マネージャ(Appliance Manager)] からアプライアンスを選択し、構成時の設定のバックアップ ファイルを作成します。

1. [集中管理(Central Management)] > [アプライアンスマネージャ(Appliance Manager)] を開きます。
2. Manager の [アクション(Actions)] メニューをクリックします。

   - **すべての管理対象アプライアンス**:Central Manager によって管理されているすべてのアプライアンスの設定をバックアップするには、プライマリ Manager を選択します。
   - [個々の管理対象アプライアンス(Individual Managed Appliance)]:[集中管理(Central Management)] の個々のアプライアンスの設定をバックアップするには、アプライアンスの [アクション(Actions)] メニューを選択します。たとえば、フロー センサーのバックアップだけが必要な場合は、フロー センサーの [アクション(Actions)] メニューを選択します。

3. [サポート(Support)] を選択します。
4. [設定ファイル(Configuration Files)] タブを選択します。
5. [バックアップ操作(Backup Actions)] ドロップダウンをクリックします。
6. [バックアップの作成(Create Backup)] を選択します。

   Manager と Central Manager:プライマリ Manager と Central Manager をバックアップすると、Manager のバックアップ設定ファイルと Central Management のバックアップ設定ファイルが作成されます。

> Manager と Flow Collector をバックアップする場合は、データベースもバックアップする必要があります。これらのアプライアンスを完全に復元するには、両方のバックアップが必要です。Manager および Flow Collector データベースのバックアップの詳細については、「5. Manager と Flow Collector のデータベースのバックアップ」を参照してください。

7. 「4. 診断パックの作成」に進みます。

4. 診断パックの作成

診断パックがあると、シスコサポートによる問題のトラブルシューティングが必要な場合に役立ちます。お使いの Secure Network Analytics のバージョンの手順に従ってください。

タイムアウト：大規模なシステムでは、タイムアウトが原因で診断パックの生成に失敗することがあります。これに対処するには、アプライアンスの SSH コンソールを開き、`doDiagPack` コマンドを実行します。これにより、診断パックの生成時にタイムアウトを防ぐことができます。

診断パックは **/lancope/var/admin/diagnostics** にあります。

システム設定を使用して各アプライアンスの診断パックを作成します。

1. アプライアンスコンソールに root としてログインします。
2. SystemConfig と入力します。Enter を押します。
3. [リカバリ（Recovery）] を選択します。
4. [診断パック（Diagnostics Pack）] を選択します。
5. 診断パックをカスタマイズするには、メニューを選択して [編集（Edit）] をクリックします。

メニュー	説明
ファイル名のプレフィックス（File Name Prefix）	診断パックのファイル名にプレフィックスを追加します（最大 127 文字）。
パスワード（Password）	診断パックのファイルパスワードを作成します。ファイルパスワードを作成しない場合、診断パックはデフォルトの方法（Cisco キー）で暗号化されます。
構成のバックアップ（Configuration Backup）	このオプションを選択し、画面の指示に従って診断パックに構成のバックアップを含めます。バックアップの詳細については、ヘルプの「Backup Configuration Files」を参照してください。
モジュール（Modules）	含める特定のモジュールを選択して、診断パックの内容を編集します。

6. [完了（Finish）] をクリックします。画面の指示に従って、診断パックを作成します。

メニュー	説明
ファイル名のプレフィックス（File Name Prefix）	診断パックのファイル名にプレフィックスを追加します（最大 127 文字）。
パスワード（Password）	診断パックのファイルパスワードを作成します。ファイルパスワードを作成しない場合、診断パックはデフォルトの方法（Cisco キー）で暗号化されます。
構成のバックアップ（Configuration Backup）	このオプションを選択し、画面の指示に従って診断パックに構成のバックアップを含めます。バックアップの詳細については、ヘルプの「Backup Configuration Files」を参照してください。
モジュール（Modules）	含める特定のモジュールを選択して、診断パックの内容を編集します。

5. Manager と Flow Collector のデータベースのバックアップ

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

Manager と Flow Collector の診断パックを作成したら、データベースを必ずバックアップしてください。サポートが必要な場合は、シスコサポートまでお問い合わせください。

このプロセスには、次の手順が含まれます。

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

1. Flow Collector データベースのトリミング

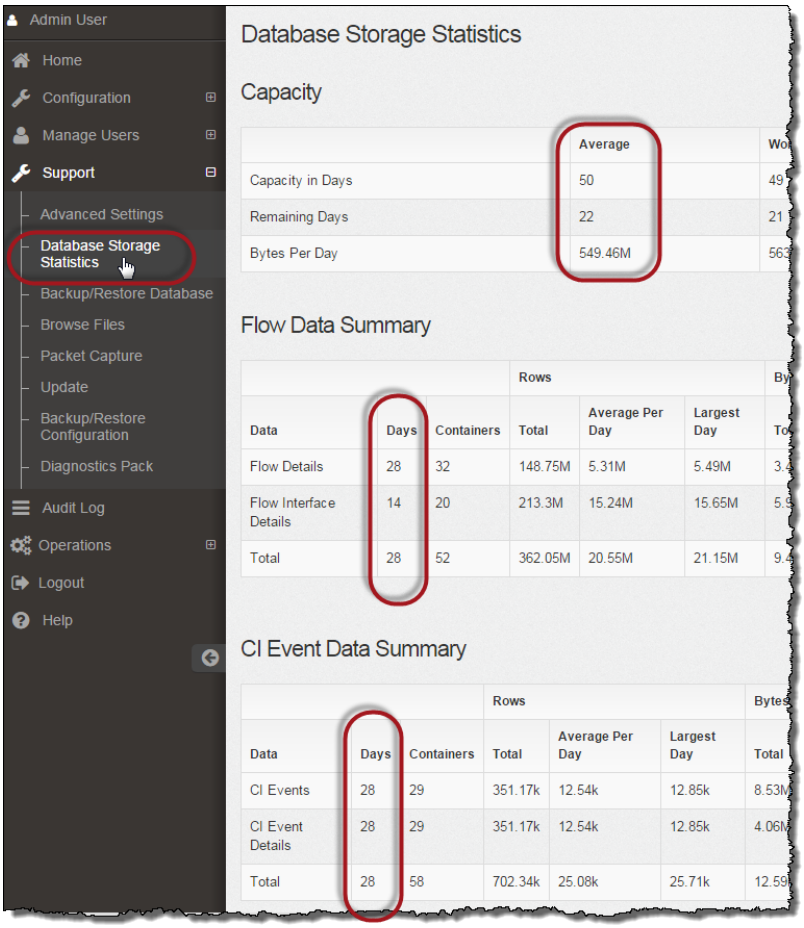
Flow Collector データベースのバックアップは、完了するまでに数日かかる場合があります。また、データベースが大きい場合はネットワークの速度が低下します。データベースをバックアップする前に、Flow Collector データベースをトリミングすることを推奨します。これにより、フローの保存に使用できるディスク容量が解放され、データベースのバックアップにかかる時間が短縮されます。

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

1. データベースストレージの統計情報の確認

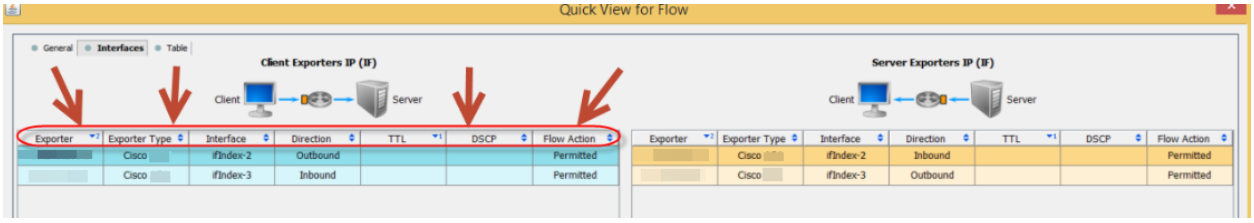
次の手順に従って、データベースストレージを確認します。

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



2. インターフェイスの詳細のトリミング

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



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

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

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

3. フローの詳細と CI イベントデータのトリミング

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

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

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

2. データベースのスナップショットの削除

バックアップファイルを作成する前に、次の手順に従って Manager およびフローコレクタのデータベースに保存されているスナップショットを削除します。

> ⚠ Manager およびフローコレクタのデータベースのスナップショットを必ず削除してください。これは、バックアップを成功させるために不可欠な手順です。

1. Manager およびフローコレクタ アプライアンスのデータベースのコンソールに **admin** としてログインします。
2. **スナップショットの確認**：次のように入力します。

```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from
database_snapshots;"
```

3. リモートファイルシステムへのバックアップ

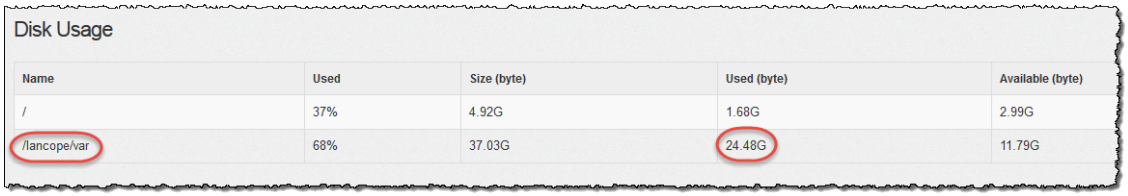
データベースをリモートファイルシステムにバックアップするには、次の手順を実行します。

- **領域**：リモート ファイル システムに、データベースのバックアップを保存するための十分な空き領域があることを確認します。

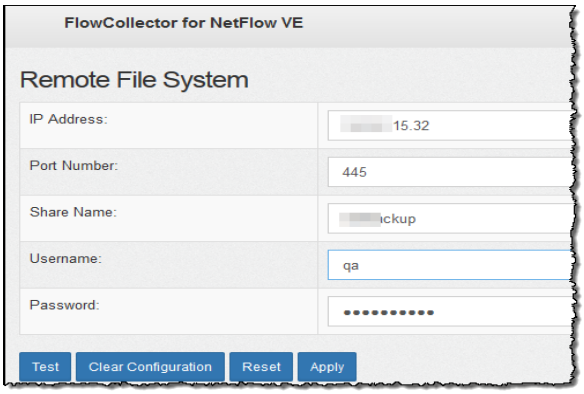
- **時間**：データベースを 1 回バックアップすると、以後は前回のバックアップからの変更点だけがバックアップされるため、バックアップにかかる時間は短くなります。このプロセスでは、1 分あたり約 0.5 GB ～ 2 GB のデータがバックアップされます。

1. アプライアンス管理インターフェイスに戻ります（ただし、デスクトップクライアントは閉じないでください）。
2. 次の手順を実行して、リモート ファイル システム上に必要となるデータベース バックアップ保存容量を確認します。

    - [ホーム（Home）] をクリックします。
    - [ディスク使用量（Disk Usage）] セクションを見つけます。
    - **/lancope/var** ファイルシステムの [Used（byte）] 列を確認します。データベースのバックアップを保存するためには、リモート ファイル システム上に少なくともこの数値にその 15% を足した分の空き容量が必要です。



3. [設定（Configuration）] > [リモートファイルシステム（Remote File System）] の順にクリックします。



4. バックアップ ファイルを保存するリモート ファイル システムの設定を使用して、フィールドに入力します。

    ファイル共有では CIFS（Common Internet File System）、別名 SMB（Server Message Block）というプロトコルが使用されます。

5. [適用（Apply）] をクリックして、設定ファイルに設定を適用します。

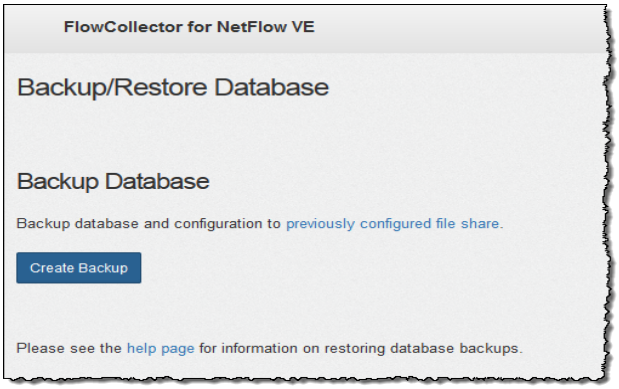
パスワードを入力しても [適用(Apply)] ボタンが有効にならない場合、[リモートファイルシステム(Remote File System)] ページの空白部分を 1 回クリックすると有効になります。

6. [テスト(Test)] をクリックして、アプライアンスとリモートファイルシステムが相互に通信できることを確認します。

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

   File sharing appears to be properly configured.

7. [サポート(Support)] > [データベースのバックアップおよび復元(Backup/Restore Database)] の順にクリックします。[データベースのバックアップ(Backup Database)] ページが開きます(次の例を参照)。



8. [バックアップの作成(Create Backup)] をクリックします。このプロセスは長時間かかる場合があります。

   - バックアップ プロセスの開始後は、マウスをページから離してもプロセスは中断されません。ただし、バックアップの実行中に、[キャンセル(Cancel)] をクリックすると、アプライアンスを再起動しないとバックアップを再開できなくなる場合があります。
   - バックアップが完了するまで、画面に表示される指示に従います。
   - バックアッププロセスの詳細を確認するには、[ログの表示(View Log)] をクリックします。

9. [閉じる(Close)] をクリックして進捗状況ウィンドウを閉じます。

> 終了する前にバックアップをキャンセルする場合は、必ずデータベースのスナップショットを再度削除してください。詳細な手順については、「**4. データベースのスナップショットの削除**」を参照してください。

4. データベースのスナップショットの削除

バックアップファイルを保存したら、次の手順に従って Manager またはフローコレクタのデータベースのスナップショットを削除します。

> ⚠ Manager およびフローコレクタのデータベースのスナップショットを必ず削除してください。これは、更新を成功させるために不可欠な手順です。

1. Manager またはフローコレクタ アプライアンスのデータベースのコンソールに **admin** としてログインします。
2. **スナップショットの確認**：次のように入力します。

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from database_snapshots;"
   ```

3. **スナップショット（存在する場合）の削除**：次のように入力します。

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_database_snapshot('StealthWatchSnap1');"
   ```

4. **スナップショットフォルダが削除されるまで待機**：次を確認します。

   ```
   ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
   ```

   結果が空でない場合は、そのまま待機します。データベースのサイズによっては、フォルダが削除されるまで数分かかる場合があります。

5. 手順 1 ～ 4 を繰り返して、保存されているすべての Manager およびフローコレクタのデータベースのスナップショットを削除します。

6. Data Store のバックアップ

> Data Store を初めて使用する場合、各タスクの計画と実装については、シスコ 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 データベースのバックアップの詳細については、『System Configuration Guide』[英語] を参照してください。

Data Store をバックアップするには、次の手順を実行します。

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

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

3. **dbadmin のパスワードレス SSH アクセスを有効にする**。すべての Data Node 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します。
4. **バックアップホストのバックアップディレクトリを初期化する**
5. **データストアデータベースのバックアップ**

1. バックアップホストのストレージ要件を見積もる

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

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

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

2. バックアップホストを準備する

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

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

2. バックアップホストのコンソールに次の権限でログインします：`root`。
3. コマンドプロンプトから、`python3 --version` と入力して Enter を押し、インストールされている Python のバージョンを確認します。次の選択肢があります。

- Python 3.7 以降がインストールされている場合は、手順 6 に進みます。
- それ以外の場合は、手順 4 から Python 3.7 をインストールします。

4. `sudo apt-get update` と入力して Enter を押し、Python を含むパッケージの更新バージョンをダウンロードします。プロンプトが表示されたら、パスワードを入力します。
5. `sudo apt-get install python3.7` と入力して Enter を押し、Python 3.7 をインストールします（違うバージョンをインストールする場合はコマンドを修正してください）。
6. コマンドプロンプトから、`rsync --version` と入力して Enter を押し、インストールされている rsync のバージョンを確認します。次の選択肢があります。

   - rsync 3.0.5 以降がインストールされている場合は、手順 9 に進みます。
   - それ以外の場合は、rsync 3.0.5 をインストールします。手順 7 に進みます。

7. `sudo apt-get update` と入力して Enter を押し、rsync を含むパッケージの更新バージョンをダウンロードします。プロンプトが表示されたら、パスワードを入力します。
8. `sudo apt-get install rsync` と入力して Enter を押し、rsync をインストールします。
9. コマンドプロンプトから、`getent passwd | grep dbadmin` と入力して Enter を押し、`dbadmin` ユーザーアカウントがこのホストに存在するかどうかを確認します。次の選択肢があります。
   - もし `dbadmin` ユーザーアカウントが存在していれば、バックアップホストの準備は完了です。**3. dbadmin のパスワードレス SSH アクセスを有効にする**に進みます。
   - それ以外の場合は、`dbadmin` ユーザーアカウントをこのホスト上に作成します。手順 10 に進みます。
10. コマンドプロンプトから、`adduser dbadmin` と入力して Enter を押し、`dbadmin` ユーザーアカウントを作成します。
11. `passwd dbadmin` と入力して Enter を押し、次にパスワードを割り当てます。`dbadmin`。
12. **新しいパスワード（New password）**を入力します。入力後、Enter を押して次を設定します。`dbadmin` password. プロンプトが表示されたら、確認のためにパスワードを再入力します。

3. dbadmin のパスワードレス SSH アクセスを有効にする

1. SSH 用にバックアップホストと各データノードの間でポート 22/TCP を開き、rsync 用にバックアップホストと各データノードの間でポート 50000/TCP を開きます。
2. 次の OpenSSH ドキュメントを確認します。`ssh-copy-id dbadmin@ <hostname>` を参照してください。
3. 最初の Data Node に次の権限でログインします。`dbadmin` 次のように入力します。

   ```
   su dbadmin
   ```

4. 次のコマンドをコピーし、プレーンテキストエディタに貼り付けます。

   `ssh-copy-id dbadmin@[hostname]` ここで `[hostname]` は、バックアップホストのホスト名または IP アドレスです。

5. 更新したコマンドをコピーし、コマンドプロンプトに貼り付けて Enter を押し、dbadmin SSH 認証キーをバックアップホストにコピーします。
6. 次のコマンドをコピーし、プレーンテキストエディタに貼り付けます。

   ssh 'dbadmin@[hostname]' ここで [hostname] は、バックアップホストのホスト名または IP アドレスです。
7. 更新したコマンドをコピーし、コマンドプロンプトに貼り付けて Enter を押して、この Data Node からリモートホストのコンソールに SSH を介してパスワードなしでログインできることを確認します。

4. バックアップホストのバックアップディレクトリを初期化する

1. 最初の Data Node コンソールに次の権限でログインします。root。

> バックアップディレクトリの初期化に使用する Data Node をメモします。同じ Data Node を使用して、次の手順で Data Node データベースにバックアップします：**5. データストアデータベースのバックアップ**。

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

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

8. 次の行をプレーンテキストエディタにコピーします。

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

9. [dbadmin-password] を次の Data Store パスワードに更新します：dbadmin。
10. 更新した行をコピーし、pw.ini バックアップ パスワード ファイルに貼り付けます。
11. Esc を押して、:wq と入力して Enter を押し、変更を保存して終了します。
12. chmod 640 pw.ini と入力して Enter を押し、pw.ini ファイル権限を変更して、dbadmin ユーザーがファイルの読み取りと編集を実行できるようにします。v7.4.2 ソフトウェ

アを使用している場合は、手順 15 に進みます。それ以外の場合は、次のステップに進みます。

13. ノードごとに、SSHD_OPTS を /etc/default/ssh ファイルで次のように編集/変更します。このプロセスを完了するには、root としてログインする必要があります。

    作業前:

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

    作業後:

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

14. 次のように ssh サービスを再起動します。

    ```
    systemctl restart ssh
    ```

15. 次の行をコピーし、プレーンテキストエディタに貼り付けます。

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

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

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

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

- Data Node コンソールに次の権限で接続します。`root`
  - `su dbadmin` と入力します。
  - `admintools -t node_map` と入力します。
- 次のエントリの「NODENAME」列にはノード名を使用します。`[Mapping]` エントリ

例:

```
dbadmin@sdbn-742-10-0-56-133-5:/root$ admintools -t node_map
DATABASE    | NODENAME                | HOSTNAME
-------------------------------------------------------
sw          | v_sw_node0001           | 169.254.42.10
sw          | v_sw_node0002           | 169.254.42.12
sw          | v_sw_node0003           | 169.254.42.15
```

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

5. データストアデータベースのバックアップ

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

1. Data Node のコンソールに `root` としてログインします。このコンソールは、次の手順で初期化したものです。**4. バックアップホストのバックアップディレクトリを初期化する**。
2. `su - dbadmin` と入力して Enter を押し、以降のコマンドを `dbadmin` ユーザーとして実行します。
3. `vbr -t backup -c config.ini --debug 3 --dry-run` と入力して Enter を押し、バックアップを作成せずにバックアップのテストを実行します。次のオプションがあります。
   - バックアップのテストに成功した場合は、Data Store をバックアップし、手順 4 に進みます。
   - バックアップテストが失敗した場合は、スナップショットファイルが作成されている可能性があるため、削除する必要があります。「Data Store のバックアップの失敗」で削除の手順を確認してください。バックアップテストが解決しない場合は、`/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、もう一度バックアップをテストしてください。シスコ サポートに連絡してサポートを依頼してください。
4. `vbr -t backup -c config.ini` と入力して Enter を押し、バックアップホストの `/home/dbadmin/backups` ディレクトリに Data Store をバックアップします。

5. 「7. 使用可能なディスク容量の確認」に進みます。

Data Store のバックアップの失敗

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

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

   ```
   select * from database_snapshots;
   ```

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

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

4. 次のコマンドを実行して終了します。

   ```
   \q
   ```

7. 使用可能なディスク容量の確認

各アプライアンスのディスク容量をチェックして、パッチとソフトウェア更新ファイル用の十分な空き容量があることを確認します。

> ⚠ Update Manager にアップロードするすべてのアプライアンス SWU ファイルについて、Manager に十分な空き容量があることを確認します。また、各アプライアンスに十分な空き容量があることを確認します。

- **Manager**：SWU が [集中管理（Central Management）] の Update Manager にアップロードされると、更新中に Manager の追加容量が使用されます。ファイルは、同じタイプの別のファイルによって置き換えられるまで、[集中管理（Central Management）] の Manager で保持されます。

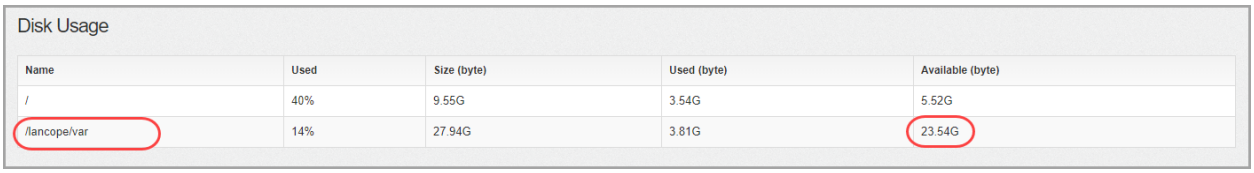
  Update Manager にアップロードするすべてのアプライアンス SWU ファイルについて、Manager に十分な空き容量があることを確認します。たとえば、[集中管理（Central Management）] の [アップデートマネージャ（Update Manager）] を使用して Flow Collector を更新した場合、新しい Flow Collector SWU ファイルをアップロードするまで、ファイルは Manager ファイルシステムで保持されます。

- **管理対象アプライアンス**：[集中管理（Central Management）] の [アップデートマネージャ（Update Manager）] を使用してアプライアンスを更新すると、更新が完了した後に SWU がアプライアンスのファイルシステムから削除されます。たとえば、[集中管理（Central Management）] の [アップデートマネージャ（Update Manager）] を使用して Flow Collector を更新した場合、更新が完了すると、そのファイルは Flow Collector ファイルシステムから削除されます。

以下の手順に従って、Manager と各管理対象アプライアンスにパッチとソフトウェア更新ファイルをインストールするための十分な空き容量があることを確認します。

1. アプライアンス管理インターフェイスにログインします。
2. [ホーム（Home）] をクリックします。
3. [ディスク使用量（Disk Usage）] セクションを見つけます。
4. [空き容量（バイト）（Available (byte)）] 列を確認し、**/lancope/var/** パーティションに必要な空き容量があることを確認します。

   - **要件**：管理対象アプライアンスごとに、個々のソフトウェア更新ファイル（SWU）の 4 倍以上のサイズが必要です。Manager では、Update Manager にアップロードするすべてのアプライアンス SWU ファイルの 4 倍以上のサイズが必要です。
   - **管理対象アプライアンス**：たとえば、Flow Collector の SWU ファイルが 6 GB の場合、Flow Collector（/lancope/var）パーティションで少なくとも 24 GB の空き容量が必要です（1 つの SWU ファイル x 6 GB x 4 = 24 GB）。
   - **Manager**：たとえば、それぞれ 6 GB の 4 つの SWU ファイルを Manager にアップロードする場合、/lancope/var パーティションに少なくとも 96 GB の空き容量が必要です（4 つの SWU ファイル X 6 GB X 4 = 96 GB）。



Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	40%	9.55G	3.54G	5.52G
/lancope/var	14%	27.94G	3.81G	23.54G

5. アプライアンスのディスク容量を拡張する必要がある場合は、使用しているアプライアンスのインストールガイド [英語] の「Data Storage」セクションを参照してください。
6. 手順 1 ～ 5 を繰り返して、各アプライアンスの空き容量を確認します。

8. パッチのインストール

ソフトウェアアップデートを開始する前に、アプライアンスに最新のパッチをインストールしていることを確認してください。パッチのダウンロードについては、「**2. パッチと更新ファイルのダウンロード**」で詳細を参照してください。

> ⚠ パッチをインストールする前に、クラスタ内のすべての管理対象アプライアンスで手順 3 ～ 7 が完了していることを確認してください。

パッチをインストールするときは、次のベストプラクティスに従うことをお勧めします。

- Readme：特定のアプライアンスの更新パッチ SWU ファイルをアップロードするか、または [集中管理（Central Management）] 内のすべてのアプライアンスに適用される共通の更新パッチをアップロードします。特定の更新パッチの詳細については、cisco.com にある readme を参照してください。
- **順序**：このセクションで指定された順序でパッチをアプライアンスにインストールします。この更新では、最初にセカンダリ Manager にロールアップパッチをインストールします。
- **時間**：これらのパッチが各アプライアンスにインストールされるまでに最大 90 分かかることがあります。設定の変更が保留中、または設定チャネルがダウンしている場合は、アプライアンスを再起動しないでください。
- **確認**：次のパッチのインストールを開始する前に、パッチがインストールされ、各アプライアンスのステータスが [アップ（Up）]（v7.4.0）または [接続済み（Connected）]（v7.4.1、v7.4.2）と表示されていることを確認します。
- **Data Node（v7.4.1）**：v7.4.1 がインストールされた Data Node がある場合は、必ず [すべての Data Nodeを更新する（Update All Data Nodes）] ボタンを使用してください。

1. インストールされているバージョンの確認

[集中管理（Central Management）] の [アップデートマネージャ（Update Manager）] にパッチをアップロードするには、次の手順を使用します。

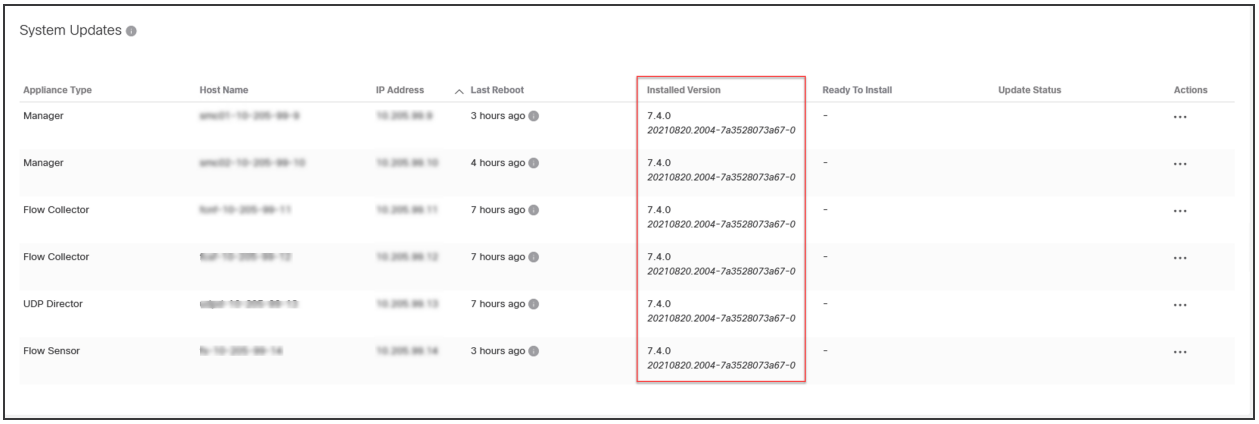
1. プライマリ Manager にログインします。

   ブラウザのアドレスバーに https://<Manager IP address> と入力します。

2. **7.4.0 および 7.4.1**：[⚙（**グローバル設定**）アイコン] をクリックします。[集中管理（Central Management）] を選択します。

   7.4.2：[構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] を選択します。
3. [アプライアンスステータス（Appliance Status）] 列を確認し、各アプライアンスが [アップ（Up）]（v7.4.0）または [接続済み（Connected）]（v7.4.1、v7.4.2）と表示されていることを確認します。
4. [アップデートマネージャ（Update Manager）] タブを選択し、[システムアップデート（System Updates）] セクションを見つけます。
5. [インストールされているバージョン（Installed Version）] 列を確認します。バージョン **7.4.0**、**7.4.1**、または **v7.4.2** のみがインストールされ、各アプライアンスに一貫性があることを確認します。

次の例は、すべてのアプライアンスのインストールされているバージョンが v7.4.0 であることを示しています。



2. 必要なパッチのインストール

v7.5.0 に更新する前に、必要な **v7.4.x**（v7.4.0、v7.4.1、または v7.4.2）パッチをインストールしてください。

> ⚠ プライマリ Manager にパッチをインストールする前に**セカンダリ** Manager にパッチをインストールし、インストールが完了したことを確認します。

[アップデートマネージャ（Update Manager）] ページで、次の手順を実行します。

1. [アップロード（Upload）] をクリックします。
2. Manager の最新のロールアップパッチ SWU ファイルを選択します。
3. [アップデートマネージャ（Update Manager）] > [システムの更新（System Update）] セクションで、Manager の [インストールの準備完了（Ready to Install）] 列を見てパッチが表示されていることを確認します。
4. セカンダリ Manager の [アクション（Actions）] メニューをクリックしてから、[更新のインストール（Install Update）] を選択します。

    - **プライマリ Manager**：セカンダリ Manager でのパッチのインストールがすでに完了している場合は、プライマリ Manager の [アクション（Actions）] メニューをクリックします。
    - **Data Node v7.4.1 以降**：[すべてのData Nodeを更新する（Update all Data Nodes）] ボタンをクリックします。
    - **他のすべてのアプライアンスとバージョン**：[アクション（Actions）] 列で、アプライアンスの [••• （**省略符号**）アイコン] をクリックします。[更新のインストール（Install Update）] を選択します。

5. 画面に表示される指示に従って、更新を確認します。

   - **更新ステータス**:[更新ステータス(Update Status)] 列は、[インストール待機中... (Waiting to Install...)] から [インストール中(Installing)] に変わります。
   - **再起動**:アプライアンスが自動的に再起動します。

   すべてのパッチがアプライアンスを再起動するわけではありません。変更中はアプライアンスを再起動しないでください。

> ⚠ パッチが各アプライアンスにインストールされるまでに最大 90 分かかることがあります。設定の変更が保留中、または設定チャネルがダウンしている場合は、アプライアンスを再起動しないでください。アプライアンスのステータスが [アップ(Up)](v7.4.0)または [接続済み(Connected)](v7.4.1、v7.4.2)であることを確認するには、[集中管理(Central Management)] > [アプライアンスマネージャ(Appliance Manager)] ページを参照します。

6. **インストールの確認**:

   - Manager の [アクション(Actions)] メニューをクリックします。
   - [更新ログの表示(View Update Log)] を選択します。
   - パッチが「正常」または「インストール済み」として表示されていることを確認します。パッチが失敗した場合、エラーを修正して再度試行してください。詳細については、「**障害対応**」を参照してください。

7. [集中管理(Central Management)] > [アプライアンスマネージャ(Appliance Manager)] ページで Manager を確認します。アプライアンスのステータスが [アップ(Up)](v7.4.0)または [接続済み(Connected)](v7.4.1、v7.4.2)と表示されていることを確認します。
8. 2 つの Manager をフェールオーバー用に設定している場合は、手順 4 ～ 7 を繰り返して、プライマリ Manager にパッチをインストールします。

9. クラスタ内の他のすべてのアプライアンスについて、次の順序でこれらの手順を繰り返します。

順序	アプライアンス	注意
1.	すべての UDP Director（別名 Flow Replicator）	高可用性クラスタ環境の場合は、最初にセカンダリ UDP Director にパッチをインストールします。
2.	すべての Data Node または Flow Collector 5000 シリーズ データベース	7.4.1 よりも前のバージョンの場合、クラスタに Data Node と Flow Collector 5000 シリーズ データベースの両方が存在することはありません。 **Data Node** Data Store 内のすべての Data Node にパッチを適用します。続行する前に、[集中管理（Central Management）] ですべての Data Node アプライアンスのステータスが [アップ（Up）] または [接続済み（Connected）] と表示されるのを待ちます。 **すべての Data Node を更新する（v7.4.1 以降）** v7.4.1 以降がインストールされている場合は、手順に従って、[すべてのData Nodeを更新する（Update all Data Nodes）] ボタンを使用して Data Node にパッチを同時にインストールします。更新パッチが**すべての** Data Node に正常にインストールされた後に、必ず Data Node で Vertica を再起動してください。 **Flow Collector 5000 シリーズ データベース** エンジンの更新を開始する前に、Flow Collector シリーズ データベースがパッチのインストールを完了し、アプライアンスのステータスが [アップ（Up）] または [接続済み（Connected）]と表示されていることを確認します。
3.	Flow Collector 5000 シリーズ エンジン	エンジンの更新を開始する前に、Flow Collector シリーズ データベースがパッチのインストールを完了し、アプライアンスのステータスが [アップ（Up）] または [接続済み（Connected）]と表示されていることを確認します。
4.	その他のすべての Flow Collector（NetFlow および sflow）	クラスタ内の次のアプライアンスにパッチをインストールする前に、Flow Collector がパッチのインストールを完了し、アプライアンスのステータスが [アップ（Up）] または [接続済み（Connected）] と表示されていることを確認します。
5.	Flow Sensor	

10. **インストールの確認**:

    - アプライアンスの [アクション(Actions)] メニューをクリックします。
    - [更新ログの表示(View Update Log)] を選択します。
    - パッチが「正常」または「インストール済み」として表示されていることを確認します。パッチが失敗した場合、エラーを修正して再度試行してください。詳細については、「**障害対応**」を参照してください。

11. [アップデートマネージャ(Update Manager)] > [システムの更新(System Update)] セクションで、各アプライアンスの [インストールの準備完了(Ready to Install)] 列を確認し、表示されているロールアップパッチを確認します。

> ⚠ パッチが各アプライアンスにインストールされるまでに最大 90 分かかることがあります。設定の変更が保留中、または設定チャネルがダウンしている場合は、アプライアンスを再起動しないでください。アプライアンスのステータスが [アップ(Up)](v7.4.0)または [接続済み(Connected)](v7.4.1、v7.4.2)であることを確認するには、[集中管理(Central Management)] > [アプライアンスマネージャ(Appliance Manager)] ページを参照します。

12. **Data Node v7.4.x**: パッチファイルがすべての Data Node に正常にインストールされた後に、Data Node で Vertica を再起動します。

    - [集中管理(Central Management)] > [Data Store] > [データベースコントロール(Database Control)] に進みます。
    - データベースの [アクション(Actions)] 列の ••• (**省略符号**)アイコンをクリックします。
    - [スタート(Start)] を選択します。
    - データベースのステータスが [アップ(Up)] と表示されていることを確認します。

9. v7.5.0 ソフトウェアアップデートのインストール

ソフトウェアアップデートでは、引き続き [アップデートマネージャ(Update Manager)] ページを使用します。

ソフトウェアアップデートをインストールするときは、次のベストプラクティスに従うことをお勧めします。

- **順序**:アプライアンスを順序どおりに更新します。開始する前に「**更新の順序**」セクションで詳細を確認してください。
- **確認**:次のアプライアンスの更新を開始する前に、更新がインストールされており、各アプライアンスのステータスが [接続済み(Connected)] と表示されていることを確認します。
- **複数のアプライアンス**:Manager、Flow Collector 5000、高可用性(HA)の UDP Director、および Data Node を除き、アプライアンスタイプが同じである場合は、複数のアプライアンスを同時に更新できます。
- Data Store:Data Store が展開されている場合は、停電後にデータベースをアップグレードまたは起動する前に必要な、すべての Data Node で SSH が有効になっていることを確認します([SSH の有効化(Enable SSH)] オプションを選択します)。

  「**代替アクセス**」の手順に従って、すべての Data Node で SSH を有効にし、[SSHの有効化(Enabling SSH)] チェックボックスをオンにします。Data Node で SSH を無効にする場合は、アップグレードプロセスが完了したら、各 Data Node の SSH を再度無効にできます。

更新の順序

次の順序で、アプライアンスを更新します。

> SWU ファイルのインストールを開始する前に、必ずすべての SWU ファイルをアップロードしてください。

順序	アプライアンス	注意
1.	UDP Director (別名 Flow Replicator)	高可用性クラスタ環境の場合は、最初にセカンダリ UDP Director を更新します。 更新が完了し、セカンダリ UDP Director アプライアンスのステータスが [アップ(Up)] または [接続済み(Connected)] と表示されていることを確認してから、プライマリ UDP Director を更新します。 プライマリ UDP Director をアップグレードする場合、プライマリ UDP Director とセカンダリ UDP Director の両方のアップグレードが完了するまで、セカンダリ UDP Director には [構成チャネルのダウン(Config Channel Down)] というアプライアンスステータスが表示されます。両方のアプライアンスがアップグレードされ、自動再起動が行

		われると、両方の UDP Director のアプライアンスステータスが [接続済み(Connected)] に変わります。
2.	すべての Data Node または Flow Collector 5000 シリーズ データベース	7.4.1 よりも前のバージョンの場合、クラスタに Data Node と Flow Collector 5000 シリーズ データベースの両方が存在することはありません。 **Data Node** 更新を開始する前に、各 Data Node で SSH が有効になっていることを確認してください。詳細については、「はじめに」の「Data Store」を参照してください。 **すべての Data Node を更新する(v7.4.1 以降)** v7.4.1 以降がインストールされている場合は、手順に従って、[すべてのData Nodeを更新する(Update all Data Nodes)] ボタンを使用して Data Node を同時に更新します。更新 SWU ファイルが**すべて**のデータノードに正常にインストールされた後に、必ずデータノードで Vertica を再起動してください。 **Flow Collector 5000 シリーズ データベース** エンジンの更新を開始する前に、Flow Collector シリーズ データベースの更新が完了し、アプライアンスのステータスが [アップ(Up)] または [接続済み(Connected)] と表示されていることを確認します。
3.	Flow Collector 5000 シリーズ エンジン	クラスタ内の次のアプライアンスを更新する前に、エンジンの更新が完了しており、アプライアンスのステータスが [アップ(Up)] または [接続済み(Connected)] と表示されていることを確認します。
4.	その他のすべての Flow Collector (NetFlow および sflow)	クラスタ内の次のアプライアンスを更新する前に、Flow Collector の更新が完了し、アプライアンスのステータスが [アップ(Up)] または [接続済み(Connected)] と表示されていることを確認します。
5.	Flow Sensor	Flow Collector SWU ファイルをアップロードします。

6.	セカンダリ Manager *使用している場合	システムでセカンダリ Manager を使用している場合は、プライマリ Manager の更新を開始する前に、セカンダリ Manager の更新が完了しており、セカンダリ Manager アプライアンスのステータスが [アップ(Up)] または [接続済み(Connected)] と表示されていることを確認します。 更新が完了すると、両方の Manager がセカンダリロールで再起動することがあります。その場合は、「12. Manager フェールオーバーロールの確認」で詳細を確認してください。フェールオーバーロールは、両方の Manager が更新されるまで変更しないでください。
7.	プライマリ Manager	システムでセカンダリ Manager を使用している場合は、プライマリ Manager の更新を開始する前に、セカンダリ Manager の更新が完了しており、セカンダリ Manager アプライアンスのステータスが [アップ(Up)] または [接続済み(Connected)] と表示されていることを確認します。 更新が完了すると、両方の Manager がセカンダリロールで再起動することがあります。その場合は、「12. Manager フェールオーバーロールの確認」で詳細を確認してください。フェールオーバーロールは、両方の Manager が更新されるまで変更しないでください。

ソフトウェアアップデートのインストール

次の手順に従って、[集中管理(Central Management)] 内のアプライアンスにソフトウェアアップデートをインストールします。

> ⚠ アプライアンスソフトウェアのアップデートファイルを個別にインストールします。ファイルサイズや Web アプリケーションの制限があるため、ソフトウェア更新ファイルの圧縮やバンドリングは推奨されません。

1. 7.5.0 SWU のアップロード

1. Manager にログインします。

   ブラウザのアドレスバーに https://<Manager IP address> と入力します。

2. **7.4.0 および 7.4.1**:[⚙ (**グローバル設定**) アイコン] をクリックします。[集中管理(Central Management)] を選択します。

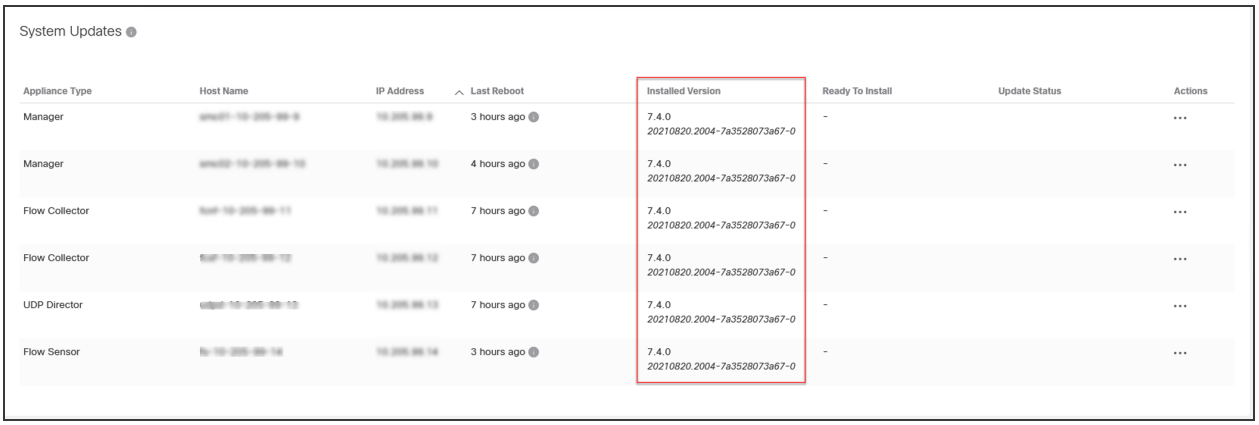
   7.4.2:[構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。

3. [アップデートマネージャ(Update Manager)] タブを選択し、[システムアップデート(System Updates)] セクションを見つけます。

> ⚠ 開始する前に、アプライアンスを順序通りに更新して詳細を確認してください。次のアプライアンスの更新を開始する前に、更新がインストールされており、各アプライアンスのステータスが [接続済み(Connected)] と表示されていることを確認します。

4. [インストールされているバージョン(Installed Version)] 列を確認します。各アプライアンスに **7.4.0**、**7.4.1**、または**v7.4.2** の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ます。

   この例は、すべてのアプライアンスに同じバージョン(7.4.0)がインストールされていることを示しています。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ということに注目してください。



5. [アップロード(Upload)] をクリックします。
6. 画面に表示されるプロンプトに従って SWU ファイルを選択します。一度に 1 つのファイルをアップロードします。

> SWU ファイルのインストールを開始する前に、必ずすべての SWU ファイルをアップロードしてください。

- **更新**:[集中管理(Central Management)] 内の各アプライアンスに SWU ファイルをアップロードします。
- ディスク容量:詳細については、「**7. 使用可能なディスク容量の確認**」をチェックしてください(十分なディスク容量があることを確認する必要がある場合)。

2. 7.5.0 SWU のインストール

次の手順に従い、[集中管理(Central Management)] を使用してソフトウェアを更新します。

> アプライアンスは順序どおりに更新します。注記の情報を確認してください。「**更新の順序**」を参照してください。

1. すべてのアプライアンスのステータスが [アップ(Up)](v7.4.0)または [接続済み(Connected)](v7.4.1、v7.4.2)と表示されていることを確認します。
2. [アップデートマネージャ(Update Manager)] タブを選択します。
3. [システムの更新(System Updates)] セクションを確認します。アプライアンスの次の列をチェックして、更新準備ができていることを確認します

- [インストール準備完了（Ready to Install）]：7.5.0 SWU ファイルが表示されていることを確認します。
- **Manager と Flow Collector の最後のリブート**：
  - 1 時間未満の場合は、処理の終了を待ちます。
  - 7 日以上経過している場合は、[アクション（Actions）] メニュー > [アプライアンスの再起動（Reboot Appliance）] の順にクリックして、アプライアンスを再起動します。少なくとも 1 時間待ってから、すべてのプロセスと安全性チェックの準備ができていることを確認します。

⚠ 設定の変更が保留中、または設定チャネルがダウンしている場合は、アプライアンスを再起動しないでください。アプライアンスのステータスが [アップ（Up）]（v7.4.0）または [接続済み（Connected）]（v7.4.1、v7.4.2）であることを確認するには、[集中管理（Central Management）] > [アプライアンスマネージャ（Appliance Manager）] ページを参照します。

4. **Data Node v7.4.1 以降**：[すべてのData Nodeを更新する（Update all Data Nodes）] ボタンをクリックします。

   他のすべてのアプライアンスとバージョン：[アクション（Actions）] 列で、アプライアンスの [••• （**省略符号**）アイコン] をクリックします。[更新のインストール（Install Update）] を選択します。

5. 画面に表示される指示に従って、更新を確認します。

   - **更新ステータス**：[更新ステータス（Update Status）] 列は、[インストール待機中...（Waiting to Install...）] から [インストール中（Installing）] に変わります。画面は 1 分ごとに更新されます。
   - **再起動**：アプライアンスは、ソフトウェアアップデートのために自動的に再起動します。

⚠ アプライアンスが自動的に再起動します。設定の変更が保留中の間は、アプライアンスを再起動させないでください。

6. [インストールされているバージョン（Installed Version）] 列をチェックして、バージョン 7.5.0 ソフトウェアアップデートが表示されていることを確認します。

   - [インストールに成功しました（Installation Successful）]：アプライアンスの [インストールされているバージョン（Installed Version）] として 7.5.0 が表示されている場合は、次の手順に進み、アプライアンスのステータスを確認します。
   - [インストールに失敗しました（Installation Failed）]：[更新ステータス（Update Status）] 列に [インストールに失敗しました（Install Failed）] と表示されている場合は、[アクション（Actions）] メニューの [更新ログの表示（View Update Log）] をクリックして詳細を確認します。問題を解決できる場合は、更新を再試行してください。詳細については、「**障害対応**」を参照してください。

7. [セキュリティ分析ダッシュボード（Security Insight Dashboard）] で、[構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] を選択し、インベントリでアプライアンスを見つけます。
   - [アップ（Up）] または [接続済み（Connected）]：アプライアンスのステータスが [アップ（Up）]（v7.4.0）または [接続済み（Connected）]（v7.4.1、v7.4.2）と表示されていることを確認します。プライマリ Manager をインストールすると、v7.5.0 に正常にインストールされたすべてのアプライアンスのアプライアンスステータスが [接続済み（Connected）] と表示されます。
   - **プライマリ Manager**：プライマリ Manager のアプライアンスステータスが [接続済み（Connected）] と表示されていることを確認します。プライマリ Manager が更新されるまで、セカンダリ Manager のステータスは [アップ（Up）] のままです。その後、すべてのアプライアンスのステータスが [接続済み（Connected）] と表示されます。
8. **Data Node v7.4.1 から v7.5.0**：すべての Data Node について、次のステータスを確認します。
   - [Data Store] > [データベース更新ステータス（Database Update Status）] タブに移動します。すべての Data Node の [更新ステータス（Update Status）] に [成功（Succeeded）] と表示されており、最後のステータス変更が最新であることを確認します。最新のステータスを確認するには、ページを更新する必要がある場合があります。
   - [データベースコントロール（Database Control）] タブをクリックします。[データベースのステータス（Database Status）] に [アップ（Up）] と表示されていることを確認します。すべての Data Node のステータスが [アップ（Up）] になっていることを確認します。
9. このセクション「2. 7.5.0 SWU のインストール」の全手順を次のアプライアンスのために繰り返します。アプライアンスは順番に更新してください。
   - [集中管理（Central Management）] ですべてのアプライアンスを v7.4.2 に更新した場合は、「10. 高可用性の設定」に進みます（UDP Director のみ）。
   - 展開に UDP Director が含まれていない場合は、「11. デスクトップクライアントのインストール」を参照してください。

障害対応

エラーの説明またはカテゴリ	詳細
[更新のインストール(Install Update)] ボタンは使用できません。	[更新のインストール(Install Update)] ボタンがグレー表示されているためにクリックできない場合は、[インストール準備完了(Ready to Install)] 列にアプライアンスの SWU ファイルが表示されていることを確認します。アプライアンスが Flow Sensor の場合は、Manager を更新した後に SWU ファイルをアップロードします。
Manager と管理対象アプライアンス間のネットワーク接続の切断	ネットワーク接続を回復し、アプライアンスインベントリで各アプライアンスが [アップ(Up)] または [接続済み(Connected)] と表示されていることを確認します。アプライアンスのステータスが [構成チャネルのダウン(Config Channel Down)] の場合は、『System Configuration Guide』[英語] の「Troubleshooting」セクションを参照してください。 ネットワーク接続が回復したことを確認してから、パッチまたはソフトウェア更新ファイルのインストールを再試行します。
失敗:このファイルとデジタル署名を照合できませんでした。ファイルを再度アップロードしてみてください。問題が解決しない場合は、シスコサポートにお問い合わせください。	正しい SWU があることを確認します。正しい SWU があるかどうかを判断できない場合は、シスコサポートに問い合わせます。
デバイスに空き容量がありません (No space left on device) (ディスク容量)	各アプライアンスのディスク容量をチェックして、パッチとソフトウェア更新ファイルのインストールに十分な空き容量があることを確認します。 管理対象アプライアンスごとに、個々のソフトウェア更新ファイル(SWU)の 4 倍以上のサイズが必要です。Manager では、Update Manager にアップロードするすべてのアプライアンス SWU ファイルの 4 倍以上のサイズが必要です。 • **管理対象アプライアンス**:たとえば、Flow Collector の SWU ファイルが 6 GB の場合、Flow Collector (/lancope/var) パーティションで少なくとも 24 GB の空き容量が必要です(1 つの SWU ファイル x 6 GB x 4 = 24 GB)。 • **Manager**:たとえば、それぞれ 6 GB の 4 つの SWU ファイルを Manager にアップロードする場合、/lancope/var パーティションに少なくとも 96 GB の空き容量が必要です(4 つの SWU ファイル X 6 GB X 4 = 96 GB)。 • その他の情報:詳細については、「**7. 使用可能なディ**

エラーの説明またはカテゴリ	詳細
	スク容量の確認」を参照してください。
予期せぬ終了ステータス (Unexpected exit status!)	このエラーが発生した場合は、以下の原因が考えられます。 • インストールの準備中にサービスを正常に停止できなかった • 更新がリブート要件を満たす前に開始された アプライアンスインベントリで各アプライアンスが [アップ(Up)] または [接続済み(Connected)] と表示されていることを確認します。アプライアンスのステータスが [構成チャネルのダウン(Config Channel Down)] の場合は、『System Configuration Guide』[英語] の「Troubleshooting」セクションを参照してください。
アップロードに失敗しました (Upload Failed)	別の SWU ファイルのアップロードを開始する前に、各アップロードが完了し、[インストール準備完了(Ready to Install)] 列に表示されていることを確認します。ログファイル /lancope/var/logs/containers/svc-central-management.log を確認して、アップロードが失敗した理由を確認することもできます。 「**9. v7.5.0 ソフトウェアアップデートのインストール**」を参照してください。このエラーメッセージが引き続き表示される場合は、シスコサポートにお問い合わせください。

エラー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。

10. 高可用性の設定

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

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

UDP Director 高可用性（HA）では、冗長 UDP Director を設定できます。両方のノードが完全冗長ですが、任意の時点で 1 つのノードだけがオンラインになります。

> UDP Director で高可用性が設定されており、Cisco Secure Network Analytics を v7.4.0 以降に更新する場合は、更新後に「**1. プライマリ UDP Director 高可用性の設定**」を参照して高可用性を再設定してください。

プライマリノードとセカンダリノード

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

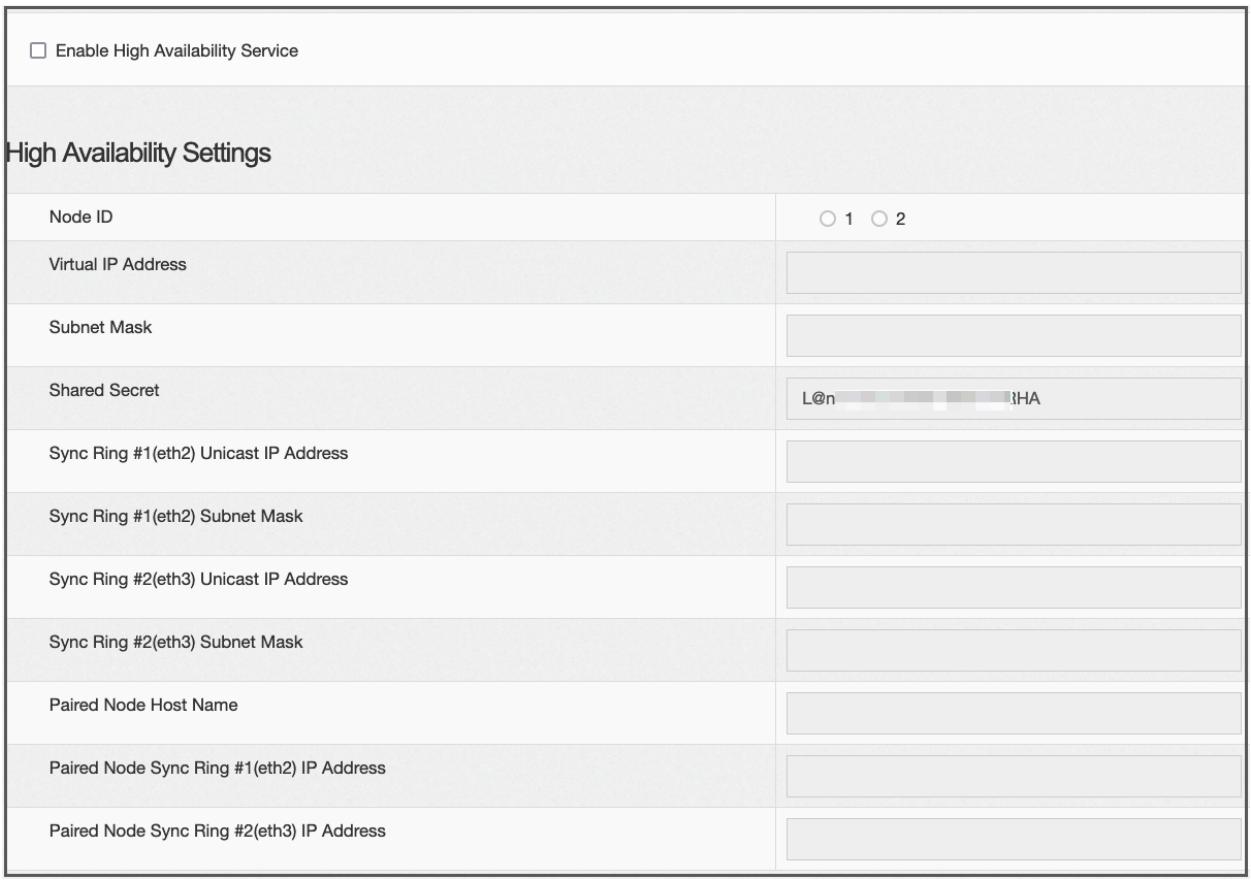
要件

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

1. プライマリ UDP Director 高可用性の設定

1. プライマリ UDP Director にログインします。
2. [設定（Configuration）] > [高可用性（High Availability）] をクリックします。

高可用性設定の [高可用性サービスの有効化（Enable High Availability Service）] チェックボックスをオンにします。



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

仮想 IP アドレスが両方のノードで同じであることを確認します。

5. [共有秘密（Shared Secret）] フィールドで、両方の UDP Director 用の文字列を入力します。（これはセキュアな転送用に暗号化されます。）
6. [同期リング1（eth2）ユニキャストIPアドレス（Sync Ring #1 (eth2) Unicast IP Address）] のフィールドに、IP アドレスとサブネットマスクを入力します。（ユニキャスト IP アドレスは単一のネットワーク宛先を識別します。）
7. [同期リング2（eth3）ユニキャストIPアドレス（Sync Ring #2 (eth3) Unicast IP Address）] のフィールドに、IP アドレスとサブネットマスクを入力します。
8. 各 IP アドレス（eth0、eth02、eth03）は、それぞれ別個のユニキャスト サブネット上である必要があります。[ペアリングされたノード同期リング#1（eth2）のIPアドレス（Paired Node Sync Ring #1(eth2) IP Address）] フィールドに、セカンダリ UDP Director の Eth2 IP アドレスを入力します。
9. [ペアリングされたノードのホスト名（Paired Node Host Name）] フィールドに、セカンダリ UDP Director のホスト名を入力します。

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

2. セカンダリ UDP Director 高可用性の設定

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

セカンダリ UDP Director を設定するには次の手順を実行します。

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

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

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

11. デスクトップクライアントのインストール

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

Data Store Flow Collector のみを使用して Secure Network Analytics システムを展開する場合、デスクトップ クライアントを使用することはありません。ハイブリッド Data Store/非 Data Store システムの場合、デスクトップ クライアントは 非 Data Store ドメインのみと連携します。

次の情報は、デスクトップクライアントのインストールと使用に適用されます。

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

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

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

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

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

Windows を使用したデスクトップクライアントのインストール

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

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

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

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

Windows Explorer からメモリサイズを変更する

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

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

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

   フォルダが非表示の場合は、「Stealthwatch」を検索する必要がある場合があります。
3. Stealthwatch ディレクトリで、目的の Stealthwatch バージョンが含まれているフォルダを開きます。
4. 適切な編集アプリケーションを使用して **application.vmoptions** ファイルを開き、編集を開始します(このファイルは、デスクトップクライアントを最初に開いた後に作成されます)。

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

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

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

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

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

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

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

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

macOS を使用したデスクトップクライアントのインストール

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

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

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

   アイコンとフォルダは、以下に示すようにモニターに表示されます。

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

   アイコンは、スタート パッドに追加されます。

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

Finder からのメモリサイズの変更

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

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

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

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

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

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

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

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

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

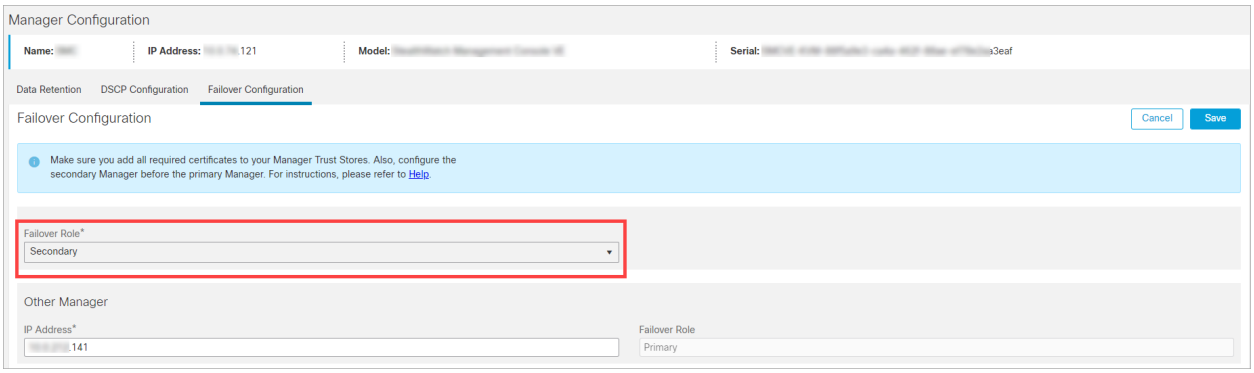
12. Manager フェールオーバーロールの確認

⚠ フェールオーバーロールは、両方の Manager が更新されるまで変更しないでください。

⚠ [集中管理（Central Management）] でのアプライアンスの追加や削除は、フェールオーバーの設定を完了し、[集中管理（Central Management）] でセカンダリ Manager のアプライアンスステータスが [接続済み（Connected）] と表示されていることを確認するまで実行しないでください。

次の手順を使用して、更新後のプライマリ Manager とセカンダリ Manager のロールが変わっていないことを確認します。

1. 管理者ユーザーとして**セカンダリ** Manager にログインします。
2. [構成（Configure）] > [グローバルマネージャ（GLOBAL Manager）] を選択します。
3. [フェールオーバー設定（Failover Configuration）] タブをクリックします。
4. フェールオーバーロールがセカンダリとして表示されていることを確認します。



5. **プライマリ** Manager にログインします。手順 2 ～ 4 に従って、**フェールオーバーロール**が**プライマリ**として表示されることを確認します。
6. 両方の Manager がセカンダリとして表示されている場合は、フェールオーバーロールを変更して、1 つのプライマリ Manager と 1 つのセカンダリ Manager がある状態にします。フェールオーバー コンフィギュレーション ガイド [英語] の設定の順序と手順に従ってください。

ℹ 手順については、フェールオーバー コンフィギュレーション ガイド [英語] を参照してください。

7. **セカンダリ Manager** にログインします。
8. [フローコレクションの傾向（Flow Collection Trend）] を確認します。

9. フロー コレクションが進行中の場合、アクションは不要です。次のステップに進みます。

   フローコレクションが停止している場合は、[集中管理（Central Management）] を使用して Flow Collector とセカンダリ Manager を再起動します。

   - プライマリ Manager にログインします。
   - [構成（Configure）] > [グローバル集中管理（GLOBAL Central Management）] を選択します。
   - インベントリで Flow Collector を見つけます。
   - ••• （**省略符号**）アイコンをクリックします。
   - [アプライアンスの再起動（Reboot Appliance）] を選択します。画面に表示される指示に従って操作します。
   - Flow Collector：手順を繰り返して、[集中管理（Central Management）] ですべての Flow Collector を再起動します。
   - **セカンダリ Manager**：手順を繰り返して、セカンダリ Manager を再起動します。

10. プライマリ Manager にログインします。
11. [集中管理（Central Management）] のインベントリを確認します。セカンダリ Manager のアプライアンスステータスが [接続済み（Connected）] と表示されていることを確認します。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 12 月 13 日	最初のバージョン。

著作権情報