Cisco Secure Network Analytics

更新ガイド 7.4.1

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 **7.3.x**（7.3.0、7.3.1、および 7.3.2）または **7.4.0** から **7.4.1** 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
- SMC（v7.4.x への更新後に Manager に名称変更）
- フローセンサー

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、リリース ノートを参照してください。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（旧 Stealthwatch）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。

「**クラスタ**」は、（v7.4.x への更新後に Manager に名称が変更される）SMC によって管理されるアプライアンスのグループです。アプライアンスが SMC（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。

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。

- 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てください。
- 更新プロセスを開始する前に、必ず **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。
- セキュリティ分析とロギング（オンプレミス） アプリケーションをアンインストールしないでください。詳細については、**セキュリティ分析とロギング（オンプレミス）**を参照してください。
- レポートビルダー アプリケーションは削除しないでください。詳細については、**レポートビルダー**を参照してください。

- UDP Director が複数ある場合は、「**10. ハイアベイラビリティの設定**」を参照してください。
- SMTP 設定と監査ログの宛先の更新の一環として、**サーバーの ID 検証（7.3.x ～ 7.4.1 のみ）**を実行します。
- v7.4.0 から更新する場合、Manager または Flow Collector における前回のアプライアンスの再起動が 1 時間以上前、かつ 7 日未満であることを確認する必要がなくなりました。ただし、v7.3.x から更新する場合は、前回の再起動が 1 時間以上前、かつ 7 日未満であることを確認する必要があります。
- プライマリ Manager が v7.4.1 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）］と表示されます。セカンダリ Manager を含むすべてのアプライアンスのステータスは、プライマリ Manager が更新されるまで［アップ（Up）］と表示されます。詳細については、「**通信**」を参照してください。
- Data Node を v7.4.1 に更新する場合、ソフトウェアの更新後に各 Data Node にパッチ SWU をインストールする必要はありません（v7.4.0 では必要でした）。
- v7.3.x か v.7.4.0 のどちらからアップグレードするのかに基づいて、正しい SWU ファイルを選択してください。v7.4.0（以降）の SWU ファイルには、ファイル名に「v2」が含まれます。この更新に必要なファイルを確認するには、**SWU ファイル**の表を参照してください。

Secure Network Analytics v7.4.1 の詳細については、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 v7.4.1 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。

> ⚠ コンプライアンスのお客様：v7.4.1 へのアップグレードを選択した場合、このバージョンにはコンプライアンス違反が含まれていることに注意してください。特に FIPS および CC モードの場合、Cisco Secure Network Analytics TLS クライアントは、FCS_TLSC_EXT.1.4 に違反して、Client Hello メッセージの Supported Groups Extension で非準拠曲線をアドバタイズします。
>
> 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。

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 v7.4.1 に更新するには、アプライアンスに **v7.3.x**（7.3.0、7.3.1、7.3.2）または **v7.4.0** 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。

- **更新ガイド**：アプライアンスに Stealthwatch v7.3.x または v7.4.0 がインストールされていない場合は、Cisco.com の更新ガイドを使用して段階的に更新してください。たとえば、Stealthwatch v7.1.x がインストールされている場合は、各アプライアンスを v7.1.x から v7.2.1 に更新した後で、v7.2.1 から v7.3.x などに更新してください。
- 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 AnalyticsTLS v1.2 が必要です。
- **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 v7.4.1 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。

> ℹ Stealthwatch v7.1.3 のパッチまたは更新ファイルにアクセスするには、引き続きダウンロードおよびライセンスセンターを使用してください。

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。

- **確認**：SMC（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）] > [スマートライセンス（Smart Licensing）] の順に選択します。[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。

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
SMC 2220（Manager 2220）	SMC 2210（Manager 2210）
FC 4200	FC 4210
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
FS 2200	_
FS 3200	FS 3210
FS 4200	FS 4210
UD 2200	UD 2210

「**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。

VMware バージョンの互換性

Secure Network Analytics v7.4.x は、VMware v6.5、v6.7、および v7.0 と互換性があります。VMware v6.0 と Secure Network Analytics v7.4.x はサポートしていません。詳細については、『vSphere 6.0 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 にインストールされている場合は、Secure Network Analytics を v7.4.x にアップグレードする前に、VMware vCenter と ESXi ホストを v6.5、v6.7、または v7.0 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 v7.4.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 v6.5、v6.7、または v7.0 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。

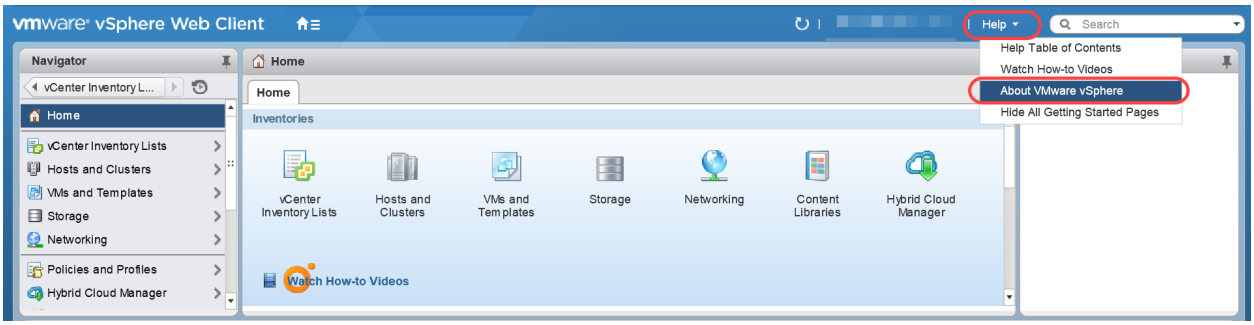
> すでにインストールされているカスタムバージョンが上書きされるため、Secure Network Analytics 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

1. VMware バージョンの確認

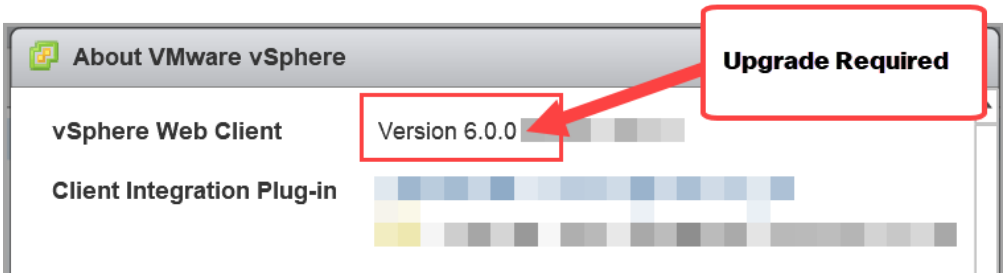
次の手順に従って、VMware vSphere vCenter v6.5、v6.7、または v7.0 がインストールされていることを確認します。

> 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. 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 の場合は、v6.5、v6.7、または v7.0 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。



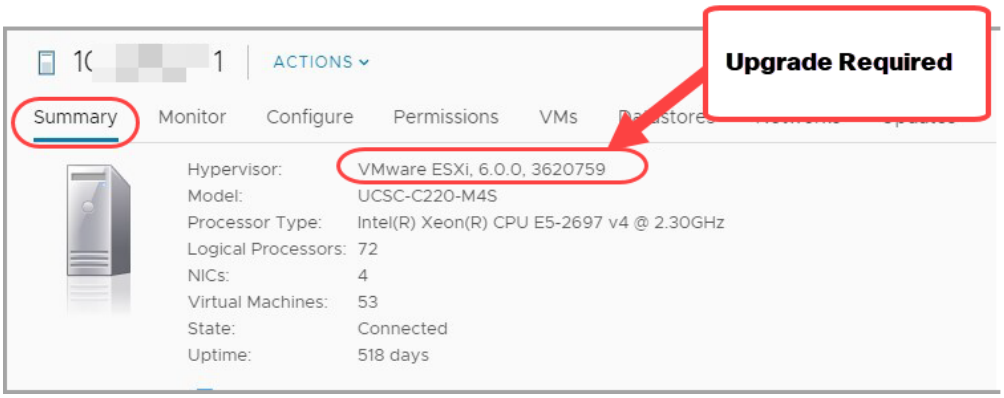
5. 次の項に進みます。

2. VMware ホストの確認

次の手順に従って ESXi ホストを確認し、v6.5、v6.7、または v7.0 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 の場合は、v6.5、v6.7、または v7.0 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 の最新バージョン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 Manager のドキュメント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、「インストールとアップグレードガイド」ページにリストされている最新の『Secure Network Analytics Hardware Installation Guide』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. SSH アクセスのみを有効にするか、ルートアクセスも有効にするかを選択します。
   - [SSH の有効化（Enable SSH）]：アプライアンスへの SSH アクセスを許可するには、このチェックボックスをオンにします。
   - [ルート SSH アクセスの有効化（Enable Root SSH Access）]：アプライアンスへのルートアクセスの有効化を許可するには、この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。

サーバーの ID 検証（7.3.x ～ 7.4.1 のみ）

7.3.x から 7.4.1 への更新の一環として、次の設定を見直してサーバーの ID 検証の要件を満たしていることを確認します。

- [監査ログの保存先（TLS経由のSyslog）（Audit Log Destination（Syslog over TLS））]
- SMTP 設定（応答管理の電子メール通知）

更新を開始する前に、構成を確認してください。構成が要件を満たしていない場合、更新は失敗します。

監査ログの宛先の要件

監査ログの宛先の設定が次の両方の要件を満たしていることを確認してください。

- Syslog over TLS をサポートする syslog サーバーからのルート認証局（CA）SSL 証明書がアプライアンスの信頼ストアに含まれていることを確認します。監査ログの宛先が構成されている各アプライアンスの信頼ストアを確認します。
- syslog サーバーの ID 証明書の [サブジェクト（Subject）] フィールドまたは [サブジェクトの別名（Subject Alternative Name）] フィールドに syslog サーバーの IP アドレスが含まれていない場合は、アドレスを監査ログの保存先が設定されている各アプライアンスの信頼ストアに追加します。

信頼ストアにアクセスするには、SMC（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 ･･･（[省略記号（Ellipsis）]）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。[全般（General）] タブを選択し、[信頼ストア（Trust Store）] セクションまでスクロールします。詳細については、管理対象アプライアンスの SSL/TLS 証明書ガイド v7.3 [英語] を参照してください。

SMTP 設定の要件

サーバーの ID 検証には、次のいずれかのオプションを使用します。

- 認証局（CA）からの SMTP サーバーの ID 証明書に、設定した IP アドレスかホスト名と一致する [サブジェクト（Subject）] または [サブジェクトの別名（Subject Alternative Name）] があることを確認します。**または、**
- 信頼ストアに SMTP サーバーの ID 証明書を追加します。

信頼ストアにアクセスするには、SMC（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。SMC（Manager）の ･･･（[省略記号（Ellipsis）]）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。[全般（General）] タブを選択し、[信頼ストア（Trust Store）] セクションまでスクロールします。詳細については、管理対象アプライアンスの SSL/TLS 証明書ガイド v7.3 [英語] を参照してください。

カスタム証明書

アプライアンスにカスタム アプライアンス アイデンティティ証明書がインストールされている場合は、それらの証明書が有効かつ最新であることを確認してから、更新プロセスを開始します。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。カスタムアプライアンス ID 証明書を置き換えるには、『SSL/TLS Certificates for Managed Appliances Guide』(v7.3 または v7.4)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
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。

証明書チェック

v7.3.0 から v7.3.1、v7.3.2、および v7.4.0 への更新には、シスコのバンドルによって使用中の環境に問題が発生しないことを確認するための証明書チェックが含まれています。

証明書を使用している場合は、証明書の完全なチェーンが(個別のファイルとして)Central Management の信頼ストアに存在することを確認します。信頼ストアにエンドエンティティ証明書のみがある場合は、アップグレードは失敗します。

> ⚠ 追加された証明書の完全なチェーンが Central Manager の信頼ストアに存在しない場合、Secure Network Analytics v7.3.0 からの更新は失敗します。v7.3.1 または v7.3.2 からアップグレードする場合、このチェックは適用されません。

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。

> [集中管理(Central Management)] の [Data Store] > [データベースの更新(Database Update)] タブの「最終ステータス更新(Last Status Change)」および「Data Node の更新ステータス(Data Node Update Status)」フィールドは、Data Node のロールアップインストール後も変更されません。

- 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、[ルート SSH アクセスの有効化(Enable Root SSH Access)] オプションの代わりに、[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。
- 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 Node を v7.4.1 に更新する場合、ソフトウェアの更新後に各 Data Node にパッチ SWU をインストールする必要はありません(v7.4.0 では必要でした)。

新規または既存の Flow Collector を使用した Data Store 環境への拡張

v7.4.1(以降)への更新に続いて、既存の Flow Collector を使用するか、新しい Flow Collector を追加してから Data Node を追加することにより、Secure Network Analytics の非 Data Store 環境を拡張できます。詳細については、『リリースノート』と『システム コンフィギュレーション ガイド』の手順を参照してください。Cisco Secure Network Analytics Data Store の仕組みを理解するには、Data Store のソリューション概要を確認してください。

データストア 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

> v7.4.1 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 7.4 [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**：SMC（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。[SMC]（[Manager]）> [クライアントグループ（Client Group）] 列で、リスト内の各 SMC（Manager）を確認します。Cisco 適応型ネットワーク制御（ANC）が表示されていない場合は、[SMC]（[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 リリース 2.2 管理者ガイド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。

クロスサイト リクエスト フォージェリ（CSRF）に対する保護（7.3.0 および 7.3.1 のみ）

システムを v7.3.0 または v7.3.1 から v7.4.1 に更新する場合は、このセクションの手順に従ってください。v7.3.2 から v7.4.1 に更新する場合、このセクションは省略できます。

CSRF 攻撃に対する保護を強化するために、HTTPS クライアントは状態変更 HTTPS リクエストの一部として CSRF トークンを送信する必要があります。CSRF トークンはセッション固有であり、認証時に「XSRF-TOKEN」という Cookie で返されます。HTTPS クライアントは、HTTPS リクエストを行うときに、HTTPS ヘッダー「X-XSRF-TOKEN」をこの Cookie の値に設定する必要があります。追加されたこの保護の一環として、認証 API スクリプトが HTTP 401 エラーで失敗することがあります。

API スクリプトを更新する手順は、環境によって異なる場合があります。クラスタを v7.3.0 または v7.3.1 から v7.4.0 に更新する前に、API スクリプトに次の変更を加えたことを確認してください。

1. HTTPS クライアントの認証時に、XSRF-TOKEN Cookie で返された CSRF トークンを保存します。
2. すべての HTTPS リクエスト（「GET」を除く）で、スクリプトは「X-XSRF-TOKEN」という HTTP ヘッダーを介してこの保存された値を返す必要があります。
3. スクリプトは再認証のたびに、保存されている CSRF トークンの値を更新する必要があります。

> API スクリプトを更新する前にクラスタを更新する必要がある場合は、シスコサポートにお問い合わせください。

セキュリティ分析とロギング（オンプレミス）

> ⚠ セキュリティ分析とロギング（オンプレミス）の以前のバージョンをアンインストールしないでください。アンインストールすると、既存のデータが削除されます。

Secure Network Analytics v7.4.x 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）を v3.1.0 にアップグレードしてください。アプリケーションの以前のバージョンは、v7.4.x と互換

性がありません。アップグレードしないと セキュリティ分析とロギング（オンプレミス） にアクセスできません。Software Central から必要なファイルをダウンロードしたら、次の手順を実行して セキュリティ分析とロギング（オンプレミス） をインストールします。

1. プライマリ Manager にログインします。
2. ［グローバル設定（Global Settings）］アイコンをクリックします。
3. ［集中管理（Central Management）］を選択します。
4. ［アプリケーションマネージャー（App Manager）］タブを選択し、ファイルを参照します。
5. 画面に表示される指示に従って、ファイルをアップロードします。

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

レポートビルダー

> ⚠ 既存の レポートビルダー アプリケーションはアンインストールしないでください。レポートビルダー をアンインストールすると、保存済みのレポートや一時ファイルを含めて、関連付けられているすべてのファイルが削除されます。

v7.4.0 では、レポートビルダーを別のアプリケーションからコアシステムに移動しました。Secure Network Analytics を v7.3.x から v7.4.1 に更新すると、その更新の一環としてアプリケーションは自動的に削除されます。

既存のアプリケーションをアンインストールする必要はありません。レポートビルダー をアンインストールすると、保存済みのレポートや一時ファイルを含めて、関連付けられているすべてのファイルが削除されます。レポートビルダーアプリは削除しないでください。

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。SMC（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）パーティションに少なくとも 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）。
- **SMC（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**：SMC（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**：SMC（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）] メニューをクリックします。[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**：SMC（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）] メニューをクリックします。[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
- SMC（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、SMC（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. SMC（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。

7.4.0 以前のリリースの sFlow アプライアンス

7.4.0 リリース以降、sFlow は個別の ISO イメージとしてリリースされません。Flow Collector NetFlow を sFlow に切り替えることができます。詳細については、オンラインヘルプの「詳細設定」トピックを参照してください。

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。

SMC（Manager）と Flow Collector

- **前回の再起動またはアクティブ**：v7.3.x から更新する場合、SMC（Manager）と Flow Collector は、更新プロセスを開始する前に **1 時間以上 7 日未満**連続で実行されている必要があります。この条件を満たしていない場合、移行の安全スイッチにより SWU ファイルはインストールされません。この再起動の要件は、パッチのインストールには適用されません。
- **Flow Collector**：Flow Collector を更新して実行すると、SMC（Manager）が更新されるまで、SMC（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 SMC（Manager）から消失します。

通信

更新プロセスの実行中は SMC（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［アップ（Up）］に戻ります。「**9. v7.4.1 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。

> ⚠ クラスタ内の次のアプライアンスを更新する前に、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。

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を重要です。

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. SMC（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. v7.4.1 ソフトウェアアップデートのインストール
10. ハイアベイラビリティの設定
11. デスクトップクライアントのインストール
12. SMC（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。

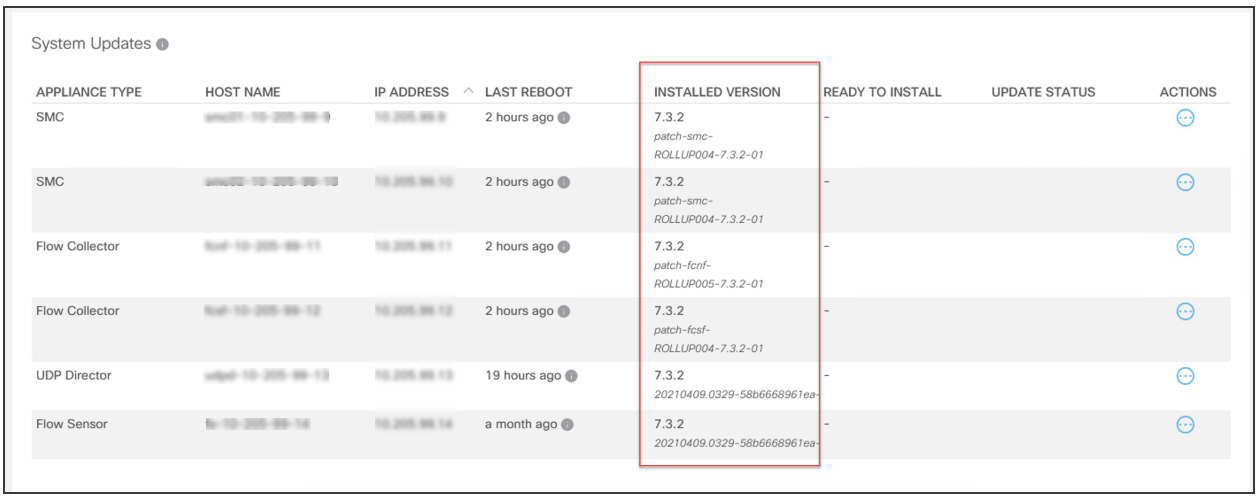
クラスタを確認して、各アプライアンスのソフトウェアバージョンを確認します。各アプライアンスの現在のソフトウェアバージョンが **7.3.x**（7.3.0、7.3.1、7.3.2）または **v7.4.0** であることを確認するには、次の手順を実行します。

1. SMC（Manager）に admin としてログインします。

   https://<SMC IP address>

2. ⚙（[グローバル設定（Global Settings）]）アイコンをクリックします。
3. [集中管理（Central Management）] を選択します。
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）] 列を確認して、すべてのアプライアンスで 7.3.x 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。

   同一バージョン：すべてのアプライアンスで 7.3.x の同じソフトウェアバージョンが使用されていることを確認してください。たとえば、SMC に 7.3.2 がインストールされている場合、クラスタ内の他のアプライアンスにも 7.3.2 がインストールされている必要があります。



> ⚠ 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

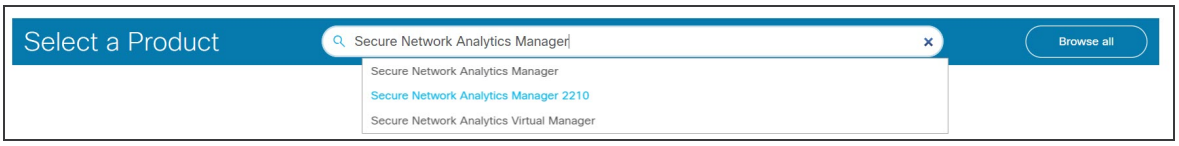
ライセンスを管理するには、パッチをダウンロードし、更新ファイルをダウンロードして、Cisco スマートアカウント（https://software.cisco.com）にログインします。

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 v7.4.1 SWU をダウンロードします。

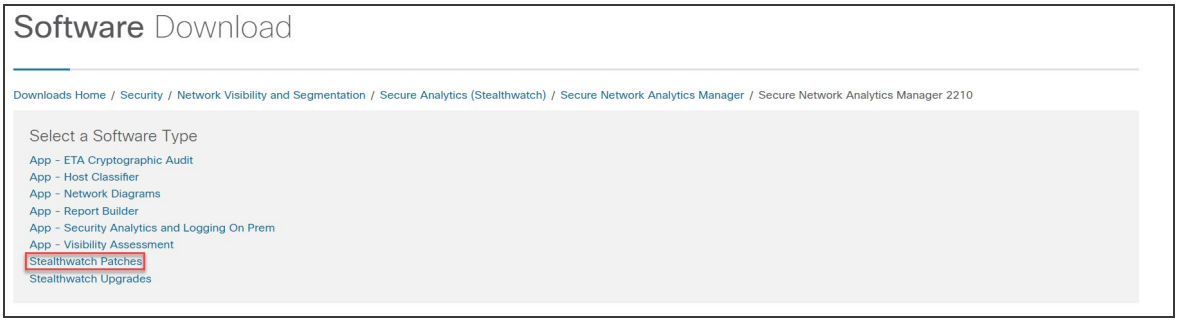
1. Cisco Software Central へのログイン

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。

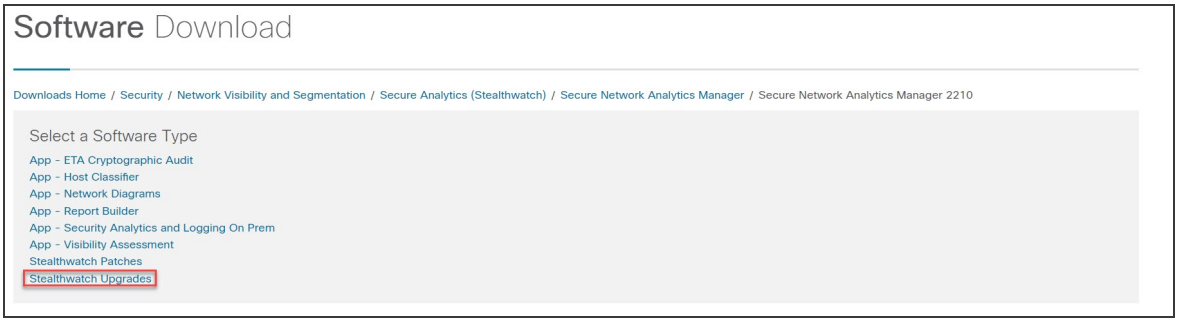
   次の例のように、製品名を入力するときにアプライアンスを含めることもできます。



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、[Stealthwatchパッチ（Stealthwatch 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、[Stealthwatchのアップグレード（Stealthwatch 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、[Stealthwatchパッチ(Stealthwatch 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。

[Stealthwatchパッチ(Stealthwatch Patches)] を選択すると、アプライアンス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 7.3.2 がインストールされている場合は、[7.3.2] 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。

> アプライアンス固有のロールアップパッチや一般的なアップデートパッチ(すべてのアプライアンスに適用される CIMC ファームウェアバージョンとシスコのバンドルパッチを含む)を含む、バージョンのすべてのファイル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 SMC(Manager)を選択します。

[Stealthwatchのアップグレード(Stealthwatch 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. [7.4.1] 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**：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**」に進みます。

> Cisco Software Central には、ここに示されている番号よりも新しいパッチロールアップ番号がある可能性があります。最新のパッチをダウンロードしてインストールしてください。

アプライアンス	v7.3.x からの更新 ソフトウェア更新 ファイル名	v7.4.0 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-7.4.1.20220411.1352-0674092e2d2e-0-01.swu	update-udpd-7.4.1.20220411.1352-0674092e2d2e-0-v2-01.swu
Data Node	update-dnode-7.4.1.20220411.1352-0674092e2d2e-0-01.swu	update-dnode-7.4.1.20220411.1352-0674092e2d2e-0-v2-01.swu
Flow Collector データベース 5000 シリーズ	update-fcdb-7.4.1.20220411.1352-0674092e2d2e-0-01.swu	update-fcdb-7.4.1.20220411.1352-0674092e2d2e-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-7.4.1.20220411.1352-0674092e2d2e-0-01.swu	update-fcnf-7.4.1.20220411.1352-0674092e2d2e-0-v2-01.swu
Flow Collector（sFlow） Flow Collector（sFlow）VE	update-fcsf-7.4.1.20220411.1352-0674092e2d2e-0-01.swu	update-fcsf-7.4.1.20220411.1352-0674092e2d2e-0-v2-01.swu

アプライアンス	v7.3.x からの更新 ソフトウェア更新 ファイル名	v7.4.0 からの更新 ソフトウェア更新 ファイル名
フローセンサー フローセンサー VE	update-fsuf-7.4.1.20220411.1352-0674092e2d2e-1-01.swu	update-fsuf-7.4.1.20220411.1352-0674092e2d2e-1-V2-01.swu
SMC（マネージャ） SMC（マネージャ）VE	update-smc-7.4.1.20220411.1352-0674092e2d2e-0-01.swu	update-smc-7.4.1.20220411.1352-0674092e2d2e-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. SMC(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(All Managed Appliances)]: 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 SMC(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。
7. 「**4. 診断パックの作成**」

   SMC(Manager)/Central Manager: プライマリ SMC(Manager)と Central Manager をバックアップすると、SMC(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。

> SMC(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。SMC(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. SMC(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。

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。

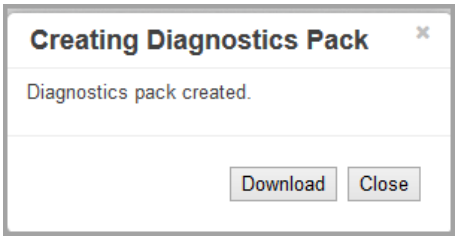
- v7.3.x：v7.3.x での診断パックの作成
- v7.4.0：v7.4.x での診断パックの作成

v7.3.x での診断パックの作成

アプライアンス管理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. アプライアンス管理インターフェイスにログインします。
2. ［サポート（Support）］>［診断パック（Diagnostics Pack）］の順にクリックします。
3. ［診断パックの作成（Create Diagnostics Pack）］をクリックします。

4. ［ダウンロード（Download）］をクリックして、診断パック（GPG）ファイルを任意の場所に保存します。このプロセスには数分かかる可能性があります。



5. ［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。

> **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。

v7.4.x での診断パックの作成

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	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	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	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。

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

> ⚠ 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。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。また、この手順はデータストア以外の Flow Collector にのみ適用されることに注意してください。サポートが必要な場合は、シスコサポートにお問い合わせください。

SMC（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

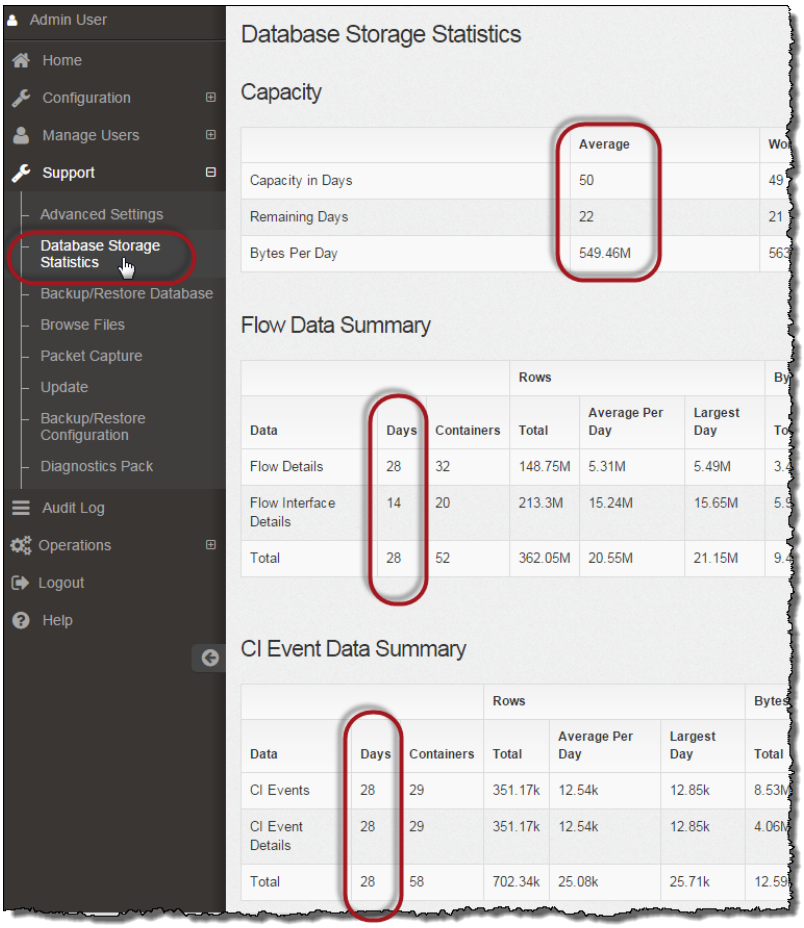
Flow Collector データベースのバックアップは、完了するまでに数日かかる場合があります。また、データベースが大きい場合はネットワークの速度が低下します。データベースをバックアップする前に、Flow Collector データベースをトリミングすることを推奨します。これにより、フローの保存に使用できるディスク容量が解放され、データベースのバックアップにかかる時間が短縮されます。

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

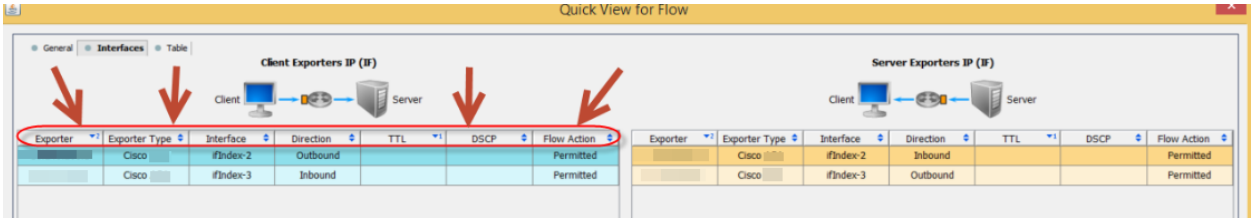
次の手順に従って、データベースストレージを確認します。

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 SMC（Manager）および Flow Collector 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。

> ⚠ SMC（Manager）および Flow Collector データベースのスナップショットを削除してください。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. SMC（Manager）および Flow Collector 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 SMC（Manager）および Flow Collector データベースのスナップショットを削除します。

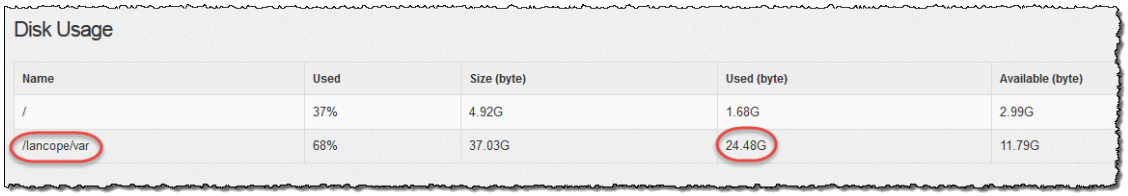
3. リモートファイルシステムへのバックアップ

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。

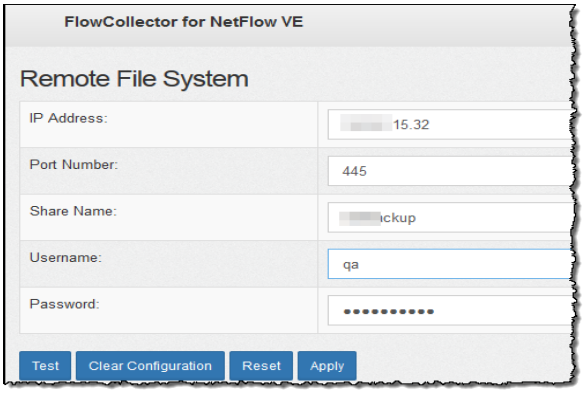
- **領域**：リモート ファイル システムに、データベースのバックアップを保存するための十分な空き領域があることを確認します。
- **時間**：データベースを 1 回バックアップすると、以後は前回のバックアップからの変更点だけがバックアップされるため、バックアップにかかる時間は短くなります。このプロセスでは、1 分あたり約 0.5 GB ～ 2 GB のデータがバックアップされます。

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。

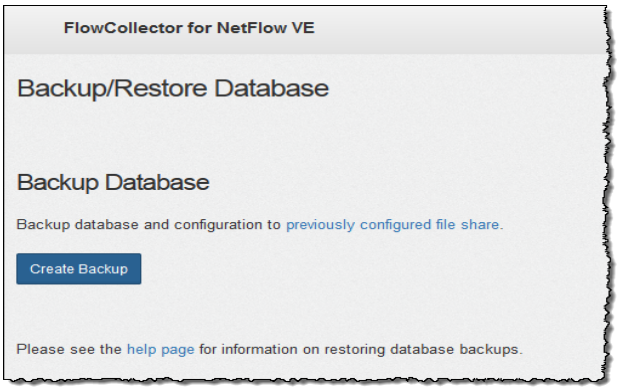
   パスワードを入力しても［適用（Apply）］ボタンが有効にならない場合、［リモートファイルシステム（Remote File System）］ページの空白部分を 1 回クリックすると有効になります。

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 SMC（Manager）または Flow Collector データベースのスナップショットを削除します。

SMC（Manager）および Flow Collector データベースのスナップショットを削除してください。これは、更新を成功させるために不可欠な手順です。

1. SMC（Manager）または Flow Collector 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 SMC（Manager）および Flow Collector 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 を始めて使用する場合、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、Data Store ハードウェア導入およびコンフィギュレーション ガイド [英語] または Data Store Virtual Edition 導入および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。

Data Store をバックアップするには、以下の手順を実行する必要があります。

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に Python 3.7 と rsync 3.0.5 をインストールする
3. バックアップホストを準備する
4. dbadmin のパスワードレス SSH アクセスを有効にする
5. 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
6. Data Store データベースをバックアップする

1. バックアップホストのストレージ要件を見積もる

バックアップサイズを見積もるには、次の手順を実行します。

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

> バックアップホストにバックアップサイズの少なくとも 2 倍のストレージ容量があることを確認してください。

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。

> 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。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。

2. 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

Stealthwatch アプライアンスとは別の Linux ベースのホストを使用していることを確認してから、バックアップホストに Python 3.7 と rsync 3.0.5 をインストールします。

1. 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。
2. 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。
   - Python 3.7 がインストールされていない場合は、手順 3 に進みます。
   - Python 3.7 がすでにインストールされている場合は、手順 5 に進みます。
3. `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。
4. `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。
5. 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。
   - rsync 3.0.5 がインストールされていない場合は、手順 6 に進みます。
   - rsync 3.0.5 がすでにインストールされている場合は、「**3. バックアップホストを準備する**」に進みます。
6. `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。
7. `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。

3. バックアップホストを準備する

バックアップホストを準備するには、次の手順を実行します。

1. バックアップホストのコンソールに `root` としてログインします（まだログインしていない場合）。
2. コマンドプロンプトで `getent passwd | grep dbadmin` と入力して Enter を押し、このホストに `dbadmin` ユーザーアカウントが存在するかどうかを確認します。
   - `dbadmin` ユーザーアカウントが存在しない場合は、このホストに `dbadmin` ユーザーアカウントを作成してください。手順 3 に進みます。
   - `dbadmin` ユーザーアカウントが存在している場合、バックアップホストの準備は完了です。「**4. 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。
3. コマンドプロンプトで `useradd dbadmin` と入力して Enter を押し、`dbadmin` ユーザーアカウントを作成します。
4. `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。
5. 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。
6. 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。

4. dbadmin のパスワードレス SSH アクセスを有効にする

`dbadmin` ユーザーアカウントのパスワードレス SSH アクセスを有効にするには、次の手順を実行します。

1. バックアップホストのコンソールに `root` としてログインします（まだログインしていない場合）。
2. 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。
3. OpenSSH の `ssh-copy-id` に関するドキュメントで詳細を確認します。
4. 最初の Data Node に `root` としてログインします。
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。

   ```
   ssh-copy-id -i dbadmin@[hostname]
   ```

6. `[hostname]` をバックアップホスト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、`dbadmin` の SSH 認証キーをバックアップホストにコピーします。
8. 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]'
   ```

9. `[hostname]` をバックアップホストのホスト名に置き換えます。
10. 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、この Data Node からパスワードなしで SSH 経由でリモートホストのコンソールにログインできることを確認します。

> パスワードなしで SSH 経由でリモートホストのコンソールにログインできることを確認してください。

5. 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

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には、次の手順を実行します。

1. 最初の Data Node のコンソールに `root` としてログインします。
2. 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。

> Data Node にバックアップするときに同じ Data Node を使用するため、バックアップディレクトリの初期化に使用する Data Node を書き留めておきます（「6. Data Store データベースをバックアップする」）。

3. `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。
4. 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]`
5. `[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。

6. 更新したコマンドをコピーしてコマンドプロンプトに貼り付けてから Enter を押し、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。
7. `cd /home/dbadmin` と入力して Enter を押し、ディレクトリを変更します。
8. `mkdir backups` と入力して Enter を押し、`backups` ディレクトリを作成します。
9. `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。
10. `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。

11. 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]
```

12. `[dbadmin-password]` を Data Store の `dbadmin` パスワードに更新します。
13. 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。
14. 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。
15. `chmod 640 pw.ini` と入力して Enter を押し、`pw.ini` ファイルの権限を変更して、`dbadmin` ユーザーにファイルの読み取りと編集を許可します。
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作成して編集します。
17. 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
```

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. `[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。

> 4 つ以上の Data Node を環境に展開した場合は、各 Data Node のエントリがあることを確認します。

20. 更新した行をコピーし、`config.ini` ファイルに貼り付けます。
21. Esc を押してから、`:wq` と入力して Enter を押し、変更を保存して終了します。
22. `vbr -t init -c config.ini` と入力して Enter を押し、Data Store のバックアップを受信するバックアップホストの `/home/dbadmin/backups` ディレクトリを初期化します。

6. Data Store データベースをバックアップする

1. バックアップ ホスト ディレクトリの初期化に使用したのと同じ Data Node のコンソールに `root` としてログインします（「**5. 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。
   - バックアップのテストに成功した場合は、Data Store をバックアップします。手順 4 に進みます。
   - バックアップの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。

4. `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。
5. 「**7. 使用可能なディスク容量の確認**」に進みます。

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、SMC（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。

- **SMC（Manager）**：SWU が Central Management の Update Manager にアップロードされると、更新中に SMC（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、Central Management の SMC（Manager）上に保持されます。

  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、SMC（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 SMC（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、SMC（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。SMC（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）。
   - **SMC（Manager）**：たとえば、それぞれ 6 GB の 4 つの SWU ファイルを SMC（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. ステップ 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。

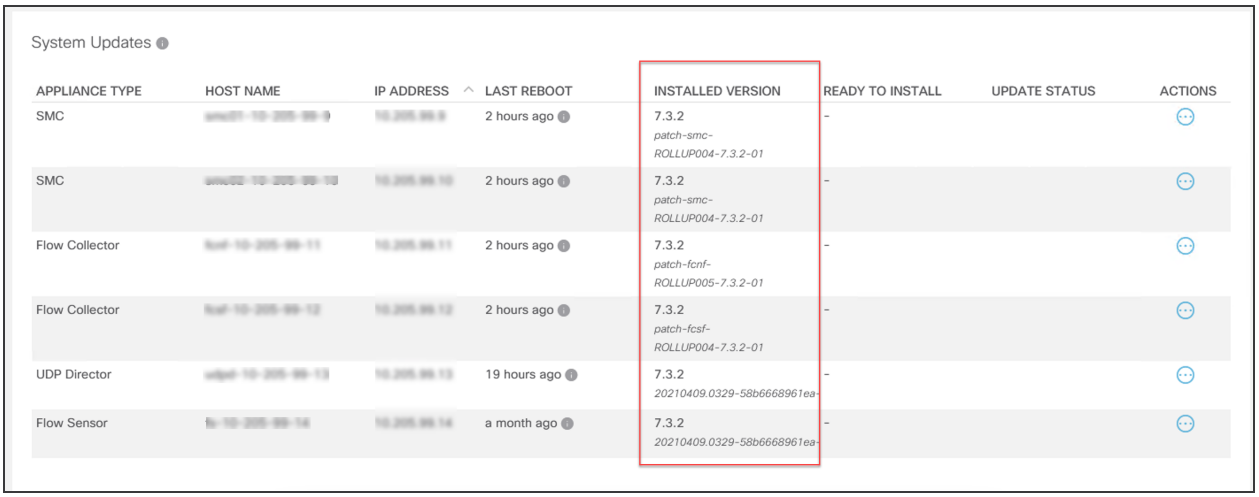
- Readme：特定のアプライアンスの更新パッチ SWU ファイルをアップロードするか、または [集中管理（Central Management）] 内のすべてのアプライアンスに適用される共通の更新パッチをアップロードします。特定の更新パッチの詳細については、cisco.com にある readme を参照してください。
- **順序**：このセクションで指定された順序でパッチをアプライアンスにインストールします。この更新では、最初に**セカンダリ** SMC（Manager）にロールアップパッチをインストールします。
- **時間**：これらのパッチが各アプライアンスにインストールされるまでに最大 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）] と表示されていることを確認します。

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 SMC（Manager）にログインします。
2. ⚙（[グローバル設定（Global Settings）]）アイコンをクリックします。
3. [集中管理（Central Management）] を選択します。
4. [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 [Up] と表示されていることを確認します。
5. [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。
6. [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 **7.3.x**（7.3.0、7.3.1、7.3.2）または **7.4.0** のみがインストールされており、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 v7.3.2 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

v7.4.1 に更新する前に、必要な **v7.3.x**（v7.3.0、v7.3.1、v7.3.2）または **v7.4.0** パッチをインストールしてください。

次の手順に従って、SMC（Manager）に最新のロールアップパッチをインストールします。2 つの SMC（Manager）がフェールオーバー用に設定されている場合は、プライマリ SMC（Manager）の前にセカンダリ SMC（Manager）にパッチをインストールします。

> ⚠ プライマリ SMC（Manager）にパッチをインストールする前に**セカンダリ** SMC（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. SMC（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、SMC（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 SMC（Manager）の［アクション（Actions）］メニューをクリックします。

   プライマリ SMC（Manager）：セカンダリ SMC（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 SMC（Manager）の［アクション（Actions）］メニューをクリックします。

5. ［更新のインストール（Install Update）］を選択します。
6. 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)] 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。

7. **インストールの確認:**
   - SMC(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、「トラブルシューティング」を参照してください。
8. [集中管理(Central Management)] > [アプライアンスマネージャ(Appliance Manager)] ページで SMC(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)] と表示されていることを確認します。
9. 2 つの SMC(Manager)をフェールオーバー用に設定している場合は、手順 4 ～ 8 を繰り返して、プライマリ SMC(Manager)にパッチをインストールします。
10. 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)	ハイアベイラビリティ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	ℹ 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、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)] と表示されるのを待ちます。 **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)] 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)] 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)] と表示されていることを確認します。
5.	Flow Sensor	

11. **インストールの確認:**

    - SMC(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、「トラブルシューティング」を参照してください。

12. [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)] 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。

9. v7.4.1 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。

> ⚠ (v7.3.x から更新する場合)ソフトウェアアップデートを開始する前に、SMC(Manager)と Flow Collector の稼働時間が 1 時間以上 7 日未満であることを確認してください。

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通りに更新します。開始する前に「**更新順序**」セクションで詳細を確認してください。
- **待機**:v7.3.x から更新する場合は、7.4.1 ソフトウェアアップデートを開始する前に、SMC と Flow Collector の稼働時間が 1 時間以上 7 日未満であることを確認します。
- **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 [アップ(Up)] 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**:SMC(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、アプライアンスの更新順序と注記に従って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、[ルート SSH アクセスの有効化(Enable Root SSH Access)] オプションの代わりに、[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。

更新順序

次の順序で、アプライアンスを更新します。

順序	アプライアンス	注意
1.	UDP Director (別名 Flow Replicator)	ハイアベイラビリティ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)] 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。
2.	すべての Data Node または Flow Collector 5000 シリーズ データベース	ℹ 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。 **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)] 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)] 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)	(v7.3.x から更新する場合)更新を開始する前に、Flow Collector の稼働時間が 1 時間以上 7 日未満であることを確認します。 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)] 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。v7.3.x からアップグレードする場合、Flow Collector のアプライアンスステータスが [設定の変更を保留中(Config Changes Pending)] と表示されることがあります。
6.	セカンダリ SMC(Manager) *使用している場合	(v7.3.x から更新する場合)更新を開始する前に、SMC(Manager)の稼働時間が 1 時間以上 7 日未満であることを確認します。 システムでセカンダリ SMC(Manager)を使用している場合は、プライマリ SMC(Manager)の更新を開始する前に、セカンダリ SMC(Manager)の更新が完了しており、セカンダリ SMC(Manager)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。 更新が完了すると、両方の SMC(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(旧 SMC)フェールオーバーロールの確認」を参照してください。フェールオーバーロールは、両方の SMC(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 SMC（Manager）	（v7.3.x から更新する場合）更新を開始する前に、SMC（Manager）の稼働時間が 1 時間以上 7 日未満であることを確認します。 システムでセカンダリ SMC（Manager）を使用している場合は、プライマリ SMC（Manager）の更新を開始する前に、セカンダリ SMC（Manager）の更新が完了しており、セカンダリ SMC（Manager）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。 更新が完了すると、両方の SMC（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（旧 SMC）フェールオーバーロールの確認」を参照してください。フェールオーバーロールは、両方の SMC（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。

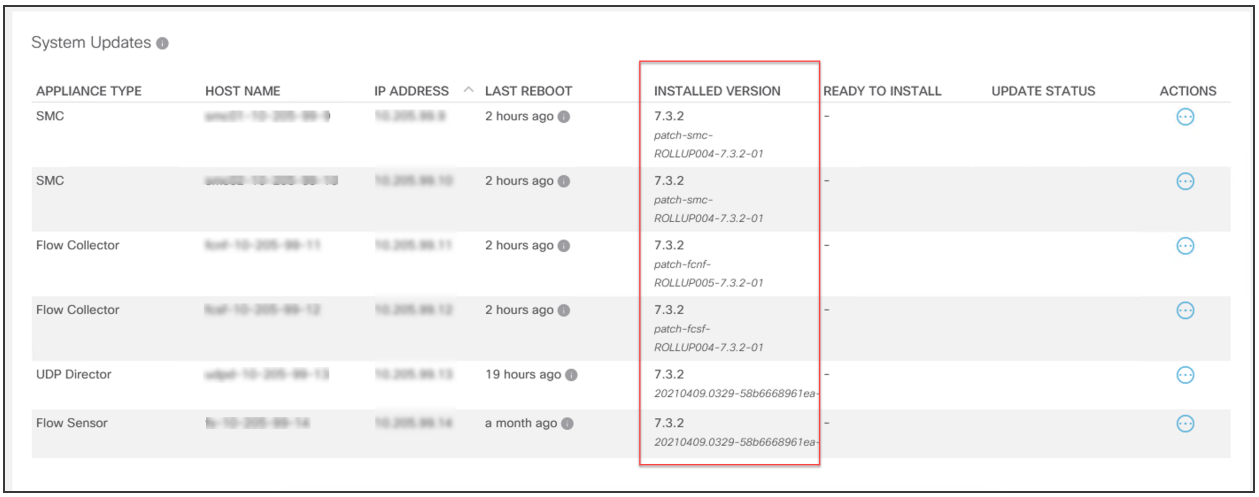
1. 7.4.1 SWU のアップロード

1. SMC（Manager）にログインします。
2. ブラウザのアドレスバーに https://<SMC IP address> と入力します。
3. ⚙（［グローバル設定（Global Settings）］）アイコンをクリックします。
4. ［集中管理（Central Management）］を選択します。
5. ［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、各アプライアンスが［アップ（Up）］と表示されていることを確認します。

6. ［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 7.3.x の同じバージョン（**7.3.0**、**7.3.1**、**7.3.2**）または **7.4.0** 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（7.3.2）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。



System Updates

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	[illegible]	[illegible]	2 hours ago	7.3.2 patch-smc-ROLLUP004-7.3.2-01	-		
SMC	[illegible]	[illegible]	2 hours ago	7.3.2 patch-smc-ROLLUP004-7.3.2-01	-		
Flow Collector	[illegible]	[illegible]	2 hours ago	7.3.2 patch-fcnf-ROLLUP005-7.3.2-01	-		
Flow Collector	[illegible]	[illegible]	2 hours ago	7.3.2 patch-fcsf-ROLLUP004-7.3.2-01	-		
UDP Director	[illegible]	[illegible]	19 hours ago	7.3.2 20210409.0329-58b6668961ea-	-		
Flow Sensor	[illegible]	[illegible]	a month ago	7.3.2 20210409.0329-58b6668961ea-	-		

7. [アップロード(Upload)] をクリックします。
8. 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。

    - **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。
    - **Flow Sensor**:SMC(Manager)を更新した後、Flow Sensor 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**」を参照してください。

2. 7.4.1 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通りに更新して注記に従ってください。

1. [アプライアンスマネージャ(Appliance Manager)] タブを選択します。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 [アップ(Up)] 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)]:7.4.1 SWU ファイルが表示されていることを確認します。**Flow Sensor** SWU ファイルが送信されていない場合は、SMC(Manager)を更新した後にアップロードします。
    - [最後の再起動(Last Reboot)](SMC(Manager)と Flow Collector):(7.3.x から更新する場合)最後の再起動が 1 時間以上前、かつ 7 日未満であることを確認します。
        - 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)] 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. 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。
5. [更新のインストール(Install Update)] を選択します。
6. 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。

7. [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 7.4.1 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 7.4.1 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、「トラブルシューティング」を参照してください。

8. [アプライアンスマネージャ(Appliance Manager)] タブを選択します。インベントリでアプライアンスを見つけます。
   - **アップ**または**接続済み**: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。
     プライマリ Manager をインストールすると、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 マネージャ**:プライマリ マネージャ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。

9. このセクション「2. 7.4.1 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。

10. [集中管理(Central Management)] ですべてのアプライアンスを v7.4.1 に更新した場合は、「**10. ハイアベイラビリティの設定**」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**」に進みます。

トラブルシューティング

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、SMC(Manager)を更新した後に SWU ファイルをアップロードします。 また、[最後の再起動(Last Reboot)] 列で SMC(Manager)と Flow Collector の最後の再起動が 1 時間以上前、かつ 7 日未満であることを確認します(v7.3.x から更新する場合)。 • 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、アプライアンスインベントリに移動します。[アクション(Actions)] メニュー > [アプライアンスの再起動(Reboot Appliance)] を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。
SMC(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、各アプライアンスがアプライアンスインベントリに [アップ(Up)] 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、インストールおよびコンフィギュレーション ガイド [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)	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。

エラーの説明またはカテゴリ	詳細
（ディスク容量）	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。SMC（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）。 • **SMC（Manager）**：たとえば、それぞれ 6 GB の 4 つの SWU ファイルを SMC（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 各アプライアンスがアプライアンスインベントリに［アップ（Up）］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、インストールおよびコンフィギュレーション ガイド［英語］の「Troubleshooting」セクションを参照してください。 また、［最後の再起動（Last Reboot）］列で SMC（Manager）と Flow Collector の最後の再起動が 1 時間以上前、かつ 7 日未満であることを確認します（v7.3.x から更新する場合）。 • 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、アプライアンスインベントリに移動します。［アクション（Actions）］メニュー > ［アプライアンスの再起動（Reboot Appliance）］を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。

エラーの説明またはカテゴリ	詳細
SIVR-CHECK Warning! 次の統合を壊す証明書の検証の問題が見つかりました。(We found certificate validation issues that will break the following integrations.)	監査ログの宛先または SMTP 設定の設定が、サーバーの ID 検証の要件を満たしていませんでした。詳細については、サーバーの ID 検証（7.3.x ～ 7.4.1 のみ）を参照してください。設定を修正して、更新を再試行してください。
アップロードに失敗しました(Upload Failed)	一度に 1 つのファイルをアップロードします。複数の SWU ファイルを同時にアップロードすることはできません。 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。「9. v7.4.1 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。

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. ハイ アベイラビリティの設定

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)を使用すると、ユーザーは冗長 UDP Director の設定を行えます。両方のノードには完全な冗長性がありますが、一度にオンラインにできるのは 1 つのノードのみです。

> 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**」の手順に従って高可用性を再設定します。

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。

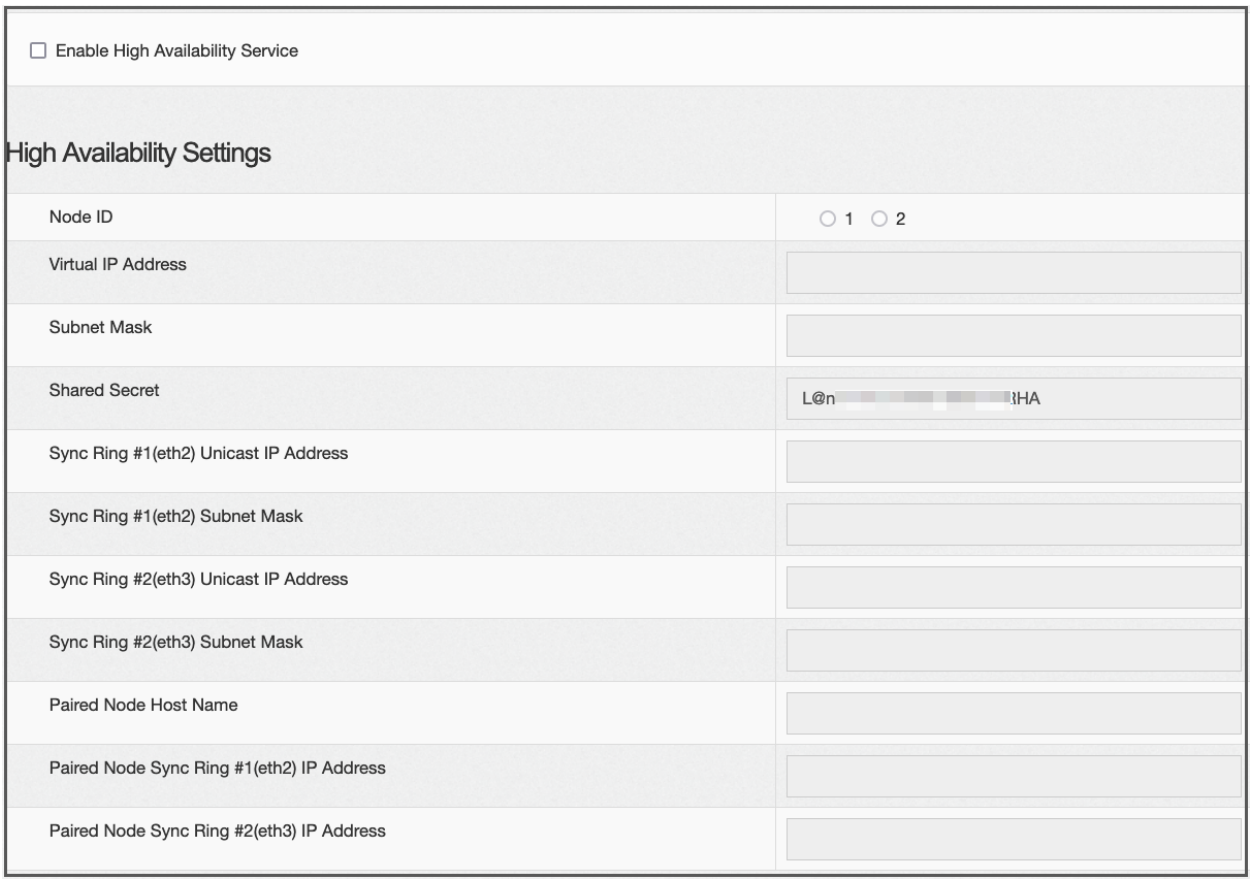
要件

- 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 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の場合は、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。プライマリ UDP Director の場合は、1 を選択します。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）] フィールドに、両方の UDP Director の文字列を入力します（これは暗号化されるため、安全に転送できます）。
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

> 前述の手順 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。

変更履歴

リビジョン	改訂日	説明
1_0	2022 年 4 月 18 日	最初のバージョン
1_1	2022 年 5 月 9 日	一般提供（GA）。
1_2	2022 年 8 月 5 日	「概要」セクションの Data Node に関連する注記を更新しました。SWU ファイル名を更新しました。
1_3	2022 年 11 月 1 日	「Data Store」セクションに注記を追加しました。
1_4	2022 年 12 月 12 日	「Data Store」セクションの注記を変更しました。

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 の名称はマネージャに変更されています。このセクション内では、SMC をマネージャと記載しています。

Data Store Flow Collector を使用して Secure Network Analytics を展開した場合、デスクトップ クライアント は使用しません。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、各マネージャにおいて異なる実行ファイルが必要になります。
- プライマリおよびセカンダリ マネージャの両方を使用している場合は、一方のマネージャをログオフしてからもう一方のマネージャ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 からメモリサイズを変更する**

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. マネージャにログインします。
2. ［ダウンロード（Download）］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、マネージャ 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. マネージャ ユーザ名とパスワードを入力します。
8. 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。

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. マネージャにログインします。
2. [ダウンロード(Download)] 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、マネージャ 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. マネージャ ユーザ名とパスワードを入力します。
8. 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。

Finder 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. 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。

   ```
   # 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。

12. Manager（旧 SMC）フェールオーバーロールの確認

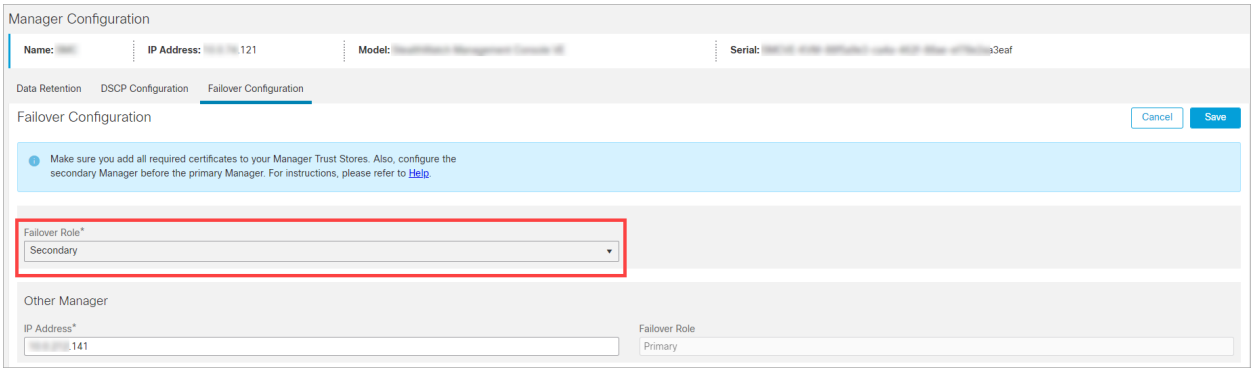
リマインダ：v7.4.0 以降、SMC の名称はマネージャに変更されています。このセクション内では、SMC をマネージャと記載しています。

フェールオーバーロールは、両方のマネージャが更新されるまで変更しないでください。

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、Central Management でセカンダリ マネージャ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 マネージャとセカンダリ マネージャのロールが変わっていないことを確認します。

1. **セカンダリ** マネージャに管理者ユーザーとしてログインします。
2. ［グローバル設定（Global Settings）］アイコンをクリックします。
3. ［Manager設定（Manager Configuration）］を選択します。
4. ［フェールオーバー設定（Failover Configuration）］タブをクリックします。
5. 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。



6. **プライマリ** マネージャにログインします。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。
7. 両方のマネージャ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 マネージャと 1 つのセカンダリ マネージャ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。

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。

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

10. 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 マネージャを再起動します。

    - プライマリ マネージャにログインします。
    - [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。
    - [アプライアンスマネージャ（Appliance Manager）] ページで Flow Collector を見つけます。
    - ••• （[省略記号（Ellipsis）]）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 マネージャ：手順を繰り返して、セカンダリ マネージャを再起動します。

11. プライマリ マネージャにログインします。
12. [集中管理（Central Management）] > [アプライアンスマネージャ（Appliance Manager）] を確認します。 セカンダリ マネージャ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

著作権情報