Cisco Stealthwatch

更新ガイド(v6.9.x から v6.10.2)

目次

はじめに

概要

次の Stealthwatch アプライアンスを v6.10.x から v7.0.2（または 7.0.x となるその後のバージョン）に更新するには、このガイドを使用します。

- UDP Director（別名 FlowReplicator）
- エンドポイント コンセントレータ
- Stealthwatch Flow Collector
- Stealthwatch Flow Sensor
- Stealthwatch Management Console（SMC）

V7.0.2 の詳細については、『リリース ノート』を参照してください。

対象読者

このガイドは、Stealthwatch 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、Stealthwatch FlowSensor Virtual Edition（VE）などの仮想製品を含むすべての 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、StealthWatch Management Console（SMC）で管理される Stealthwatch アプライアンスのグループです。

ほとんどのアプライアンスは SMC で管理されます。SMC で管理されないエンドポイント コンセントレータなどのアプライアンスは、「スタンドアロン アプライアンス」と呼ばれています。

新しい更新プロセス

Stealthwatch アプライアンスをバージョン 6.10.x から v7.0.2（または 7.0.x となるその後のバージョン）に更新するための新しいプロセスを導入しました。更新には次の内容が含まれます。

- アプライアンス管理インターフェイス：プライマリ SMC にパッチ（Pre-SWU）ファイルをインストールします。
- Web アプリケーション インターフェイス：クラスタ内の各アプライアンスにパッチ（Pre-SWU）と v7.0.x SWU（ソフトウェア アップデート ファイル）をインストールします。
- 新しいアプライアンスの更新順序：Pre-SWU をインストール後、このガイドの手順および新しい順序に従い、v7.0.x SWU をインストールする必要があります。
- 証明書：アプライアンスソフトウェアを v7.0.x に更新すると、デフォルトのアプライアンス アイデンティティ証明書（旧 Lancope）が一意の自己署名アプライアンス アイデンティティ証明書で置き換えられます。アプライアンスの信頼ストアは、このプロセスの一環として自動的に更新されます。アプライアンスでカスタム証明書を使用している場合、証明書は置き換えられません。
- Central Management：すべての Stealthwatch アプライアンスを v7.0.x に更新すると、プライマリ SMC/Central Manager からアプライアンスを管理できます。

V7.0.2 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、および更新のために計画する必要がある準備、時間、リソースを確認してください。

考えられるルート パーティション スペースの不足

次の点に注意してください。

- SMC に 5 GB または 7.5 GB のルートパーティションがあるシステムの場合、v7.0.2（または 7.0.x となるその後のバージョン）にアップグレードすると、ルートの使用量が最適な範囲に近づくか、超過することがあります。そのため、その後の StealthWatch アプリケーションの更新やインストールに影響が出る可能性があります。システムのルート パーティションに十分なスペースがない場合、重要な機能が停止します。
- 場合によっては、パッチを実行する際に、1 つ以上のアプリケーションをアンインストールして空き領域を確保する必要があります。
- 更新後：このガイドでは、アプライアンスを更新後に、ルート パーティションを確認する方法について説明します。詳細については、「Central Management へのログイン」または「スタンドアロン アプライアンスと接続解除されたアプライアンスの更新」を参照してください。

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 v7.0.x に更新するには、アプライアンスに 6.10.2、6.10.3、または 6.10.x となるその後のバージョン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。

- パッチ：アップグレードする前に、各ソフトウェアバージョンについて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。詳細については、Stealthwatch のダウンロードおよびライセンス センター https://stealthwatch.flexnetoperations.com [英語] にログインして確認してください。

  この更新には次のパッチが必要です。

  - 6.10.2：patch-smc-ROLLUP008-6.10.2-01.swu（または以降）
  - 6.10.4：patch-common-lc-admin-6.10.4-01.swu（または以降）

- **アプライアンスのソフトウェア バージョンは段階的に更新してください。**たとえば、Stealthwatch v6.8.x を使用している場合は、各アプライアンスを v6.8.x から 6.9.x に更新してから、v6.9.x を v6.10.4（または 6.10.x の最新バージョン）に更新します。各更新ガイドは、Customer Community または Cisco.com で入手できます。
- 同一バージョン：すべてのアプライアンスが同じソフトウェアバージョンを使用していることを確認してください。たとえば、SMC に v6.10.3 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は v6.10.3 がインストールされている必要があります。

- 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。

Java

SMC デスクトップ クライアントを実行するためには、Stealthwatch に Java バージョン 8(使用可能な最新の更新)をインストールする必要があります。Java バージョン 9、10、11 はサポートされていません。

次の製品機能を確認して、Java Runtime Environment をインストールする必要があるかどうかを判断してください。

- SMC デスクトップ クライアント: マップ、カスタマイズ可能なダッシュボード、応答の管理、システム アラーム、SLIC の設定、SMC フェールオーバーの設定、クラスタ間のライセンス管理、TACACS と RADIUS の設定、および Stealthwatch ドメインの編集。これらの機能を必要とするユーザにのみ、Java Runtime Environment をインストールします。ここに記載されていない機能があることもあります。
- Web ユーザ インターフェイス: ほとんどの製品機能は Web ユーザ インターフェイスから使用可能なため、Java Runtime Environment は不要な場合があります。

TLS

Stealthwatch には TLS v1.1 以降が必要です。

デフォルト クレデンシャル

ポート 5672 は、pre-SWU のインストール時に RabbitMQ に使用されます。一時的な認証ファイルを、次のデフォルトクレデンシャルと共に使用します。

- ユーザ名 : upgrade
- パスワード : @ist+ipsdishzsfadetidyprizecrag007hm

一時的な認証ファイルを使用することで、更新中に信頼ストアを再構築できます。更新が完了すると、クレデンシャルは置き換えられます。

> ⚠ Pre-SWU のインストールと v7.0.x の更新の間は、短時間ですが公開のリスクが増えることがあります。セキュリティ上の制限により、デフォルト クレデンシャルを使用できない場合は、Cisco Stealthwatch サポートに連絡してカスタム クレデンシャルを設定してください。

ポート 5672

フローコレクタ、フローセンサー、および UDP Director は、**ポート 5672** で SMC との通信が開いている必要があります。通信は暗号化され、TCP アクセスが必要となります。関連情報については、「デフォルトクレデンシャル」を参照してください。

更新中にポートエラーが発生した場合は、ポート 5672 が開いていることを確認するか、システム管理者にお問い合わせください。

サード パーティ製アプリケーション

Stealthwatch 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。

ブラウザ

- 互換性のあるブラウザ： Stealthwatch 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、いずれかのステルスウォッチ 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。

ハードウェア

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、Cisco.com の Hardware and Version Support Matrix を参照してください。

Stealthwatch ファームウェアおよび Stealthwatch 更新ガイド [英語] を使用して、ファームウェアを更新します。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。

Flow Sensor 4000

FlowSensor 4000 モデルを使用している場合は、アプライアンスを v7.0.x に更新後、パッチをインストールします。この手順はこのガイドで説明されています。詳細については、パッチの Readme ファイルを参照してください。

この要件は、FS4000 モデルにのみ適用されます。Flow Sensor 4000 シリーズのその他のモデルには適用されません。

SMC

この更新では、最大 2 つの SMC を更新できます。SMC が 2 つより多い場合は、「1. クラスタの確認」を参照してください。

UDP Director

UDP Director がハイ アベイラビリティ ペアとして設定されている場合は、仮想 IP アドレスで管理されていないことを確認します。詳細については、「1. クラスタの確認」を参照してください。

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 Web アプリケーションにログインします。[グローバル設定（Global Settings）] アイコン > [アプライアンスの管理（Administer Appliance）] の順に選択します。[設定（Configuration）] > [ライセンス（Licensing）] の順に選択します。
- ステータスを使用できません：セカンダリ SMC のライセンス ステータスが [ステータスを使用できません（Status Not Available）] と表示される場合があります。この状態は、プライマリ SMC とのフェールオーバー関係が原因で発生しますが、セカンダリ SMC の通信ステータスを表してはいません。ライセンスの詳細を表示するには、[ステータス（status）] ボタンをクリックします。
- ガイド：詳細については、ダウンロードおよびライセンス ガイド [英語] を参照してください。

ISE または ISE-PIC

- 設定：SMC 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] > [クライアントグループ（Client Group）] 列を確認します。リスト内の各 SMC を確認します。

  ANC が表示されていない場合は、[SMC] チェックボックスをオンにして選択します。[グループ（Group）] をクリックします。[グループ（Group）] フィールドに ANC を追加します。[保存（Save）] をクリックします。

- ガイド：v7.0 の詳細については、Stealthwatch の ISE 統合機能の拡張 [英語] および ANC ポリシーの設定手順 [英語] を参照してください。

ホスト名

- 設定：各アプライアンスには固有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。
- 確認：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。[設定（Configuration）] > [ネーミングと DNS（Naming and DNS）] の順に選択します。

ドメイン名

- 設定：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：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。[設定（Configuration）] > [ネーミングと DNS（Naming and DNS）] の順に選択します。

NTP サーバ

- 設定：7.0 では、各アプライアンスに少なくとも 1 台の NTP サーバが必要です。
- 確認：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。[設定（Configuration）] > [システム時刻とNTP（System Time and NTP）] の順に選択します。
- 問題のある NTP：130.126.24.53 NTP サーバがサーバのリストに含まれている場合は削除します。このサーバ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 リストからはすでに除外されています。

タイムゾーン

v7.0.x では、すべての Stealthwatch アプライアンスで協定世界時（UTC）が使用されます。

- 設定：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。
- 確認：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。[設定（Configuration）] > [システム時刻と NTP（System Time and NTP）] の順に選択します。
- 仮想ホスト サーバ：仮想ホスト サーバが正しい時刻に設定されていることを確認します。

> ⚠ （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。

カスタム証明書

StealthWatch は、RSA で暗号化された PEM 形式の証明書をサポートしています。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。

期限切れの証明書を置き換える場合は、次のオプションを確認してください。

- [証明書の更新（Update Certificate）]：最新の証明書をプロバイダーに要求して、アプライアンス管理インターフェイスにインストールします。[設定（Configuration）] > [SSL証明書（SSL Certificate）] を選択します。
- [デフォルトの復元（Restore Default）]：アプライアンス アイデンティティ証明書のデフォルトを復元します。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。[設定（Configuration）] > [SSL] の順に選択します。[SSLサーバアイデンティティ（SSL Server Identity）] セクションで、[デフォルトの復元（Restore Defaults）] をクリックします。

手順については、SSL 証明書の作成とインストール ガイド [英語] を参照してください。

信頼ストア

各アプライアンス アイデンティティ証明書と証明書チェーン（該当する場合）が、アプライアンス信頼ストア（独自の信頼ストア）と SMC 信頼ストアに保存されていることを確認します。この設定は、すべてのアプライアンスに必要です。

- 設定：更新を開始する前に、アプライアンス アイデンティティ証明書と証明書チェーン（ルートおよび中間）が、アプライアンス信頼ストアと SMC 信頼ストアに保存されていることを確認します。
- 確認：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。[設定（Configuration）] > [認証局証明書（Certificate Authority Certificates）] の順に選択します。

手順については、SSL 証明書の作成とインストール ガイド [英語] を参照してください。

> ⚠ 必要な各信頼ストアに証明書を個別にアップロードするようにしてください。

アプライアンスのバックアップ

Stealthwatch 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、Cisco Stealthwatch サポートによるトラブルシューティング時に重要になります。

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
- SMC 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
- 診断パックの作成

> ⚠ バックアップを作成しない場合、更新プロセス中に問題が発生してもファイルを回復することはできません。また、診断パックは、Cisco Stealthwatch 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。

更新に最適な時間

ステルスウォッチ 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

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。ファイルは、ダウンロードおよびライセンス センターから事前にダウンロードできます。

すべてのアプライアンス

- 時間: 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、SMC Pre-SWU のインストール、Pre-SWU の終了手順、および SWU のインストール後に自動的に再起動します。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 とFlow Collector

- 前回の再起動またはアクティブ: SMC 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。
- Flow Collector: Flow Collector を更新して実行すると、SMC が更新されるまで、SMC 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。

SMC デスクトップ クライアントから Flow Collector を削除しないでください。削除すると、それらのフローコレクタに関する履歴データが SMC から失われます。

通信

- 通信：更新プロセス中は、SMC と Flow Collector 間の通信が停止します。通信が停止すると、SMC デスクトップ クライアントの企業ツリーにある Flow Collector アイコンに赤い「x」が表示され、管理対象アプライアンスのアイコンが緑色ではなくオレンジ色（  ）になります。
- 管理チャネル ダウン：StealthWatch FlowSensor を使用している場合は、SMC デスクトップ クライアントのアラーム テーブルに FlowSensor 管理チャネル ダウン アラームが表示されます。更新が完了すると通信が再確立されてアイコンは通常に戻り、アラームは表示されなくなります。

更新後

システムを v 7.0.2 に更新した後は、次の必須パッチを必ずインストールしてください。

- SMC： patch-smc-ROLLUP003-7.0.2-02.swu

このガイドの手順に従って、詳細を Stealthwatch ダウンロードおよびライセンスセンターにあるパッチの readme ファイルに記載されている指示で確認してください。

代替アクセス

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、ステルスウォッチ 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。

> ⚠ 今後サービスが必要になった場合に備えて、ハードウェアまたは仮想マシンに対して次のいずれかの方法を使用してステルスウォッチ アプライアンスにアクセスする別の方法を有効にしておくことは重要です。

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):ラップトップや、キーボードとモニタを使用してアプライアンスに接続する方法については、最新の Stealthwatch ハードウェア インストレーション ガイド[英語]を参照してください。 https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html
- iDRAC Enterprise(Dell アプライアンス):www.dell.com で、お使いのプラットフォームの最新ドキュメントを参照してください。iDRAC Enterprise にはライセンスが必要です。また、iDRAC Express ではコンソール アクセスはできません。iDRAC Enterprise をお持ちでない場合は、コンソールまたは SSH での直接接続をお使いください。
- CIMC(UCS アプライアンス): 最新の Cisco UCS を参照してください。 https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/b_Cisco_CIMC_CLI_Configuration_Guide/Cisco_CIMC_CLI_Configuration_Guide_chapter1.html で、お使いのプラットフォーム向けの最新の Cisco UCS ガイドを参照してください。

仮想マシン

- コンソール(コンソール ポートへのシリアル接続):アプライアンスのインストールについては、最新の KVM または VMware のマニュアルを参照してください。
    - KVM の場合は、https://virt-manager.org/ で Virtual Manager のマニュアルを参照してください。
    - VMware の場合は、https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.vcsa.doc/GUID-223C2821-BD98-4C7A-936B-7DBE96291BA4.html で、vSphere 向けの vCenter Server アプライアンス管理インターフェイスのマニュアルを参照してください。

その他のオプション

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。

> ⚠ 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。

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。

SMC：SMC にログインします。[グローバル設定（Global Settings）] アイコン > [アプライアンスの管理（Administer Appliance）] の順にクリックします。

2. [設定（Configuration）] > [サービス（Services）] の順にクリックします。
3. [SSHを有効にする（Enable SSH）] チェックボックスをオンにして SSH を有効にします。

   ルート ユーザによる SSH アクセスを許可するには、[ルートSSHアクセスの有効化（Enable Root SSH Access）] チェックボックスをオンにします。

4. [適用（Apply）] をクリックします。

StealthWatch IDentity アプライアンス(A10)

StealthWatch IDentity アプライアンス(ID-1000、ID-1100)を使用している場合は、次の手順を使用して ID-1000/1100 Lancope Web 証明書を交換してからソフトウェアを v7.0.x に更新します。

クラスタに Stealthwatch IDentity アプライアンスがない場合は、このセクションをスキップして「更新の概要」に進みます。

> ⚠ 以下の手順に従い Lancope Web 証明書を交換してから、バージョン v7.0.x への更新を開始してください。

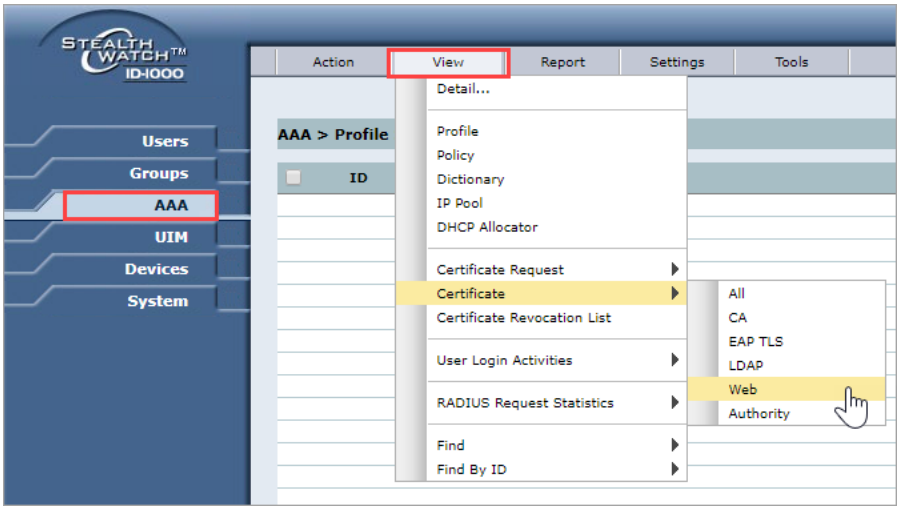
1. ソフトウェアの更新

セキュリティ向上のため、アプライアンスが TSL 1.2 で新しいバージョンの openSSL を使用できるよう、ID-1000 および ID-1100 を更新することをお勧めします。

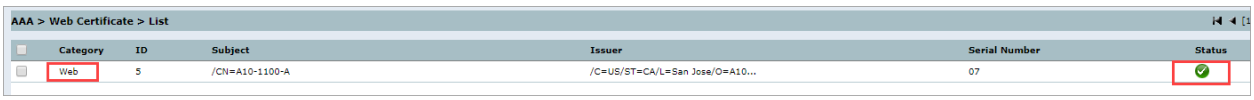
手順については、Stealthwatch IDentity アプライアンスのオンライン ヘルプの「**アップグレード**」のトピックを参照してください。

2. 現在の証明書の確認

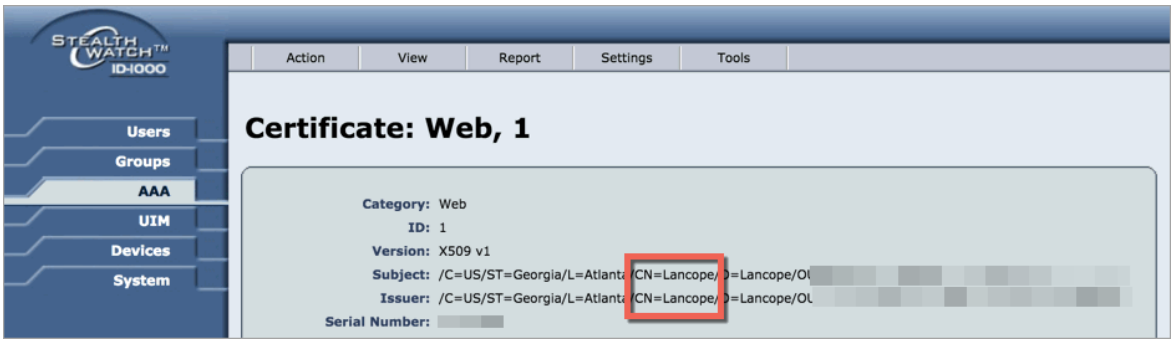
1. Stealthwatch IDentity アプライアンスにログインします。
2. [AAA]をクリックします。
3. [表示(View)]>[証明書(Certificate)]>[Web]の順にクリックします。



4. 現在の証明書のリストを確認します。[カテゴリ(Category)]列で、[ステータス(Status)]列に緑色のチェック マークが付いている[Web]証明書を見つけます。



5. [証明書(Certificate)] アイコンをクリックします。
6. [発行元(Issuer)]セクションを確認します。説明部分に Lancope が含まれている証明書は交換する必要があります。次の項に進みます。



3. 新しい証明書の作成

1. [アクション(Action)]>[新規(New)]>[証明書(Certificate)]の順にクリックします。
2. 次のパラメータを使用して、新しい証明書を作成します。

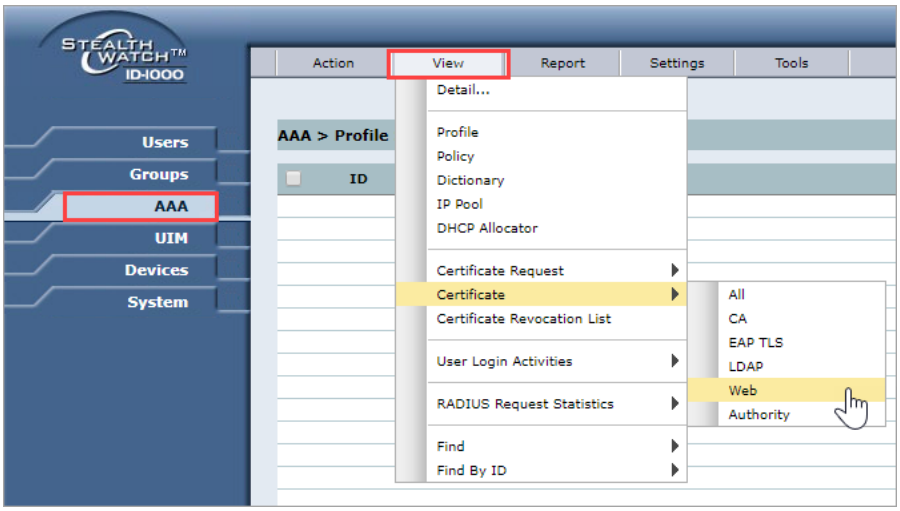
   - [共通名(Common Name)]: 一意の名前を入力します(可能な場合はアプライアンスの完全修飾ドメイン名)。Stealthwatch IDentity アプライアンスが複数ある場合は、アプライアンスごとに一意の名前を使用する必要があります。
   - [有効な日数(Valid Days)]: 1460
   - [キー長(Key Length)]: 4096
   - [署名アルゴリズム(Signature Algorithm)]: SHA256WithRSA(またはより上の SHA)を選択します。

3. [OK]をクリックします。
4. アプライアンスが自動的に再起動します。

4. 新しい証明書の確認

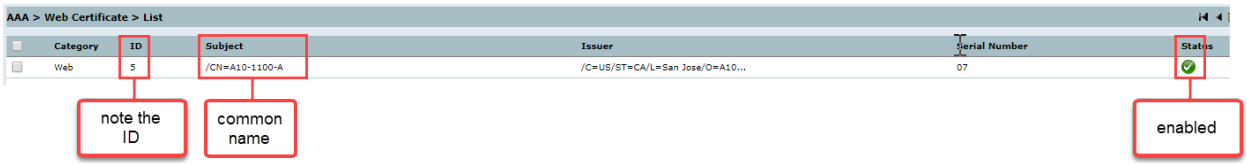
次の手順を使用して、新しい証明書が作成され、有効になっていることを確認します。

1. Stealthwatch IDentity アプライアンスにログインします。
2. [AAA]をクリックします。
3. [表示(View)]>[証明書(Certificate)]>[Web]の順にクリックします。



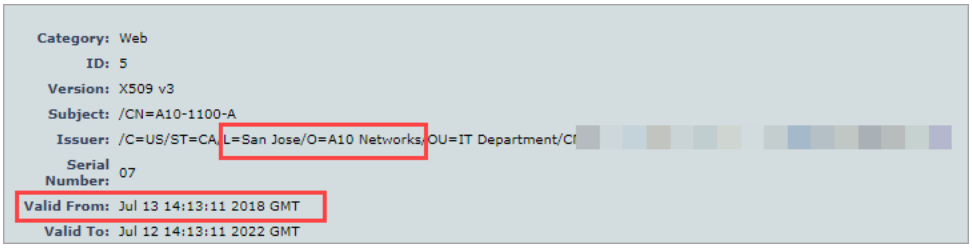
4. 新しい Web 証明書を見つけます。共通名は「CN= ユーザが割り当てた共通名」として表示されています。。

   - [ステータス(Status)] 列に緑色のチェック マークが付いていることを確認します。
   - ID 番号をメモします。ID 番号は次のセクションで使用します。



5. [証明書(Certificate)] アイコンをクリックします。
6. 新しい証明書を確認し、次の情報が表示されていることを確認します。

   - [発行元(Issuer)]: 説明部分に Lancope が表示されていないことを確認します。ほとんどの場合、San Jose と表示されます。
   - [有効開始日(Valid From)]: 新しい証明書を作成した日付が表示されていることを確認します。



5. 証明書の有効化

Web UI に証明書を追加したら、次の手順を使用して端末で証明書を有効にします。

1. Stealthwatch IDentity アプライアンスに SSH ログインします。

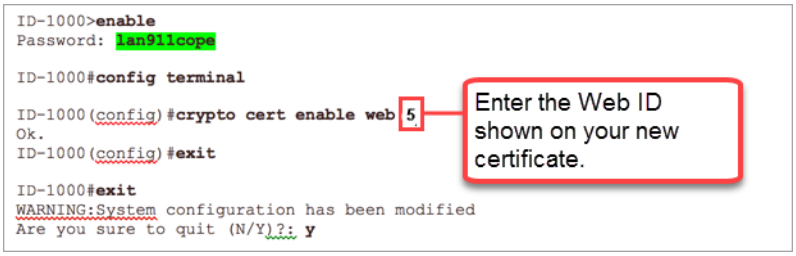
   アプライアンスの再起動が必要な場合があります。

2. アプライアンスの IP アドレスを入力します。Enter キーを押します。
3. 「`enable`」と入力します。Enter キーを押します。
4. アプライアンスのパスワードを入力します。Enter キーを押します。

   デフォルト: lan911cope

5. 「`config terminal`」と入力します。Enter キーを押します。
6. 「`crypto cert enable web ID`」と入力します。Enter キーを押します。

   ID: 前のセクションでメモした証明書の ID 番号を入力します。



7. OK が表示されたら、「`exit`」と入力します。Enter キーを押します。

> ⚠ OK の応答が表示されない場合は、Cisco Stealthwatch サポートにお問い合わせください。

8. ログアウト: 「`exit`」と入力します。Enter キーを押します。

6. 確認およびエクスポート

1. Stealthwatch IDentity アプライアンスにログインします。
2. ブラウザのアドレス バーにある [セキュリティ(Security)] アイコンをクリックします。
3. [証明書(Certificate)] をクリックします。
4. 新しい証明書が表示されていて、古い Lancope 証明書が表示されていないことを確認します。
5. [OK] をクリックして、[証明書(Certificate)] ダイアログボックスを閉じます。
6. [AAA] をクリックします。
7. [表示(View)] > [証明書(Certificate)] > [Web] の順にクリックします。
8. 古い Lancope 証明書を見つけ、[ごみ箱(Trash)] アイコンをクリックして削除します。

9. 新しい証明書を見つけます。
10. [エクスポート(Export)] アイコンをクリックします。[OK]をクリックします。
11. 証明書がダウンロードされます。ファイル名と場所をメモします。
12. [キャンセル(Cancel)]をクリックして前のページに戻ります。

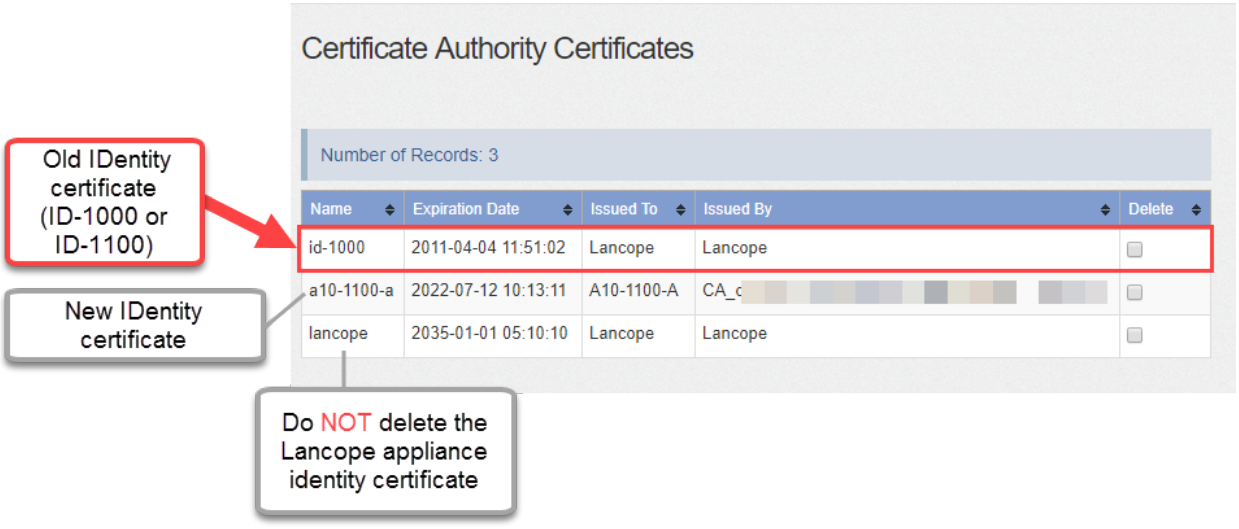
7. SMC での新しい証明書のインストール

1. SMC 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. [アプライアンスの管理(Administer Appliance)]を選択します。
4. [設定(Configuration)]>[認証局証明書(Certificate Authority Certificates)]の順に選択します。
5. [認証局証明書(Certificate Authority Certificates)]セクションで、[ファイルの選択(Choose File)]をクリックします。IDentity アプライアンスからエクスポートした新しい証明書を選択します。
6. [名前(Name)]フィールドに、証明書の名前をスペースを含めずに入力します。

   例:A10-1100-A。

7. [証明書の追加(Add Certificate)]をクリックします。
8. 画面に表示される指示に従って、新しい証明書を確認します。
9. 証明書認証局リストの[名前(Name)]列で、ID-1000 または ID-1100 証明書を見つけます。

   これは古い証明書です。[発行先(Issued To)]と[発行元(Issued By)]の説明に Lancope が表示されています。



10. ID-1000 または ID-1100 の行で、[削除(Delete)]チェックボックスをオンにします。

> ⚠ 必ず、古い ID-1000 または ID-1100 証明書を選択してください。SMC Lancope アプライアンス アイデンティティ証明書は削除しないでください。詳細については、（上記）のスクリーンショットを参照してください。

11. [削除（Delete）]をクリックします。
12. 画面に表示される指示に従って、削除を確認します。

更新の概要

新しいプロセス

アプライアンスをバージョン 6.10.x から v7.0.2（または 7.0.x となるその後のバージョン）に更新するための新しいプロセスを導入しました。新しいプロセスでは、特定の順序で Pre-SWU ファイルと SWU ファイルをアプライアンスにインストールします。

> ⚠ Pre-SWU ファイルと SWU ファイルの両方で、ソフトウェアのインストール順序に従ってください。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。

更新プロセスの概要

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. インストールされているソフトウェア バージョンの確認
3. パッチ ファイルとアップデート ファイルのダウンロード
4. アプライアンスの設定のバックアップ
5. 診断パックの作成
6. Flow Collector と SMC データベースのバックアップ
7. 使用可能なディスク容量の確認
8. アプライアンス管理を使用した SMC での Pre-SWU パッチのインストール
9. [システム管理（System Management）] ページを使用した 管理対象アプライアンスでの Pre-SWU パッチのインストール
10. Pre-SWU のインストールの終了
11. v7.0.x ソフトウェアアップデートをインストールします。SMC の [システム管理（System Management）] ページを使用して各管理対象アプライアンスを更新します。v7.0.x SWU は、必ず新しい順序でインストールしてください。
12. Central Management へのログイン
13. v7.0.2 パッチのインストール
14. SMC デスクトップ クライアントへのログイン：証明書を信頼し、フェールオーバー ロールを確認します。
15. スタンドアロン アプライアンスと接続が解除されたアプライアンスを更新し、必要に応じてスタンドアロン アプライアンスを Central Management に追加します。

1. クラスタの確認

次の手順を使用して、ステルスウォッチ アプライアンスを確認します。

ベスト プラクティス

ベストプラクティスに従い、更新を開始することを推奨します。

- **SMC 管理**:すべてのステルスウォッチ アプライアンスを StealthWatch Management Console(SMC)で管理するように設定します。
- **スタンドアローン アプライアンス**:SMC で管理されないアプライアンスは、スタンドアロン アプライアンスと呼ばれています。エンドポイントコネクタを除くすべてのアプライアンスは、プライマリ SMC で管理されるように設定することをお勧めします。

  スタンドアロン アプライアンスをお使いの場合は、v7.0.x クラスタの更新完了後に更新できます。「15. スタンドアロン アプライアンスと接続解除されたアプライアンスの更新」と「Central Managementにおける管理対象およびスタンドアロンの要件」を参照してください。

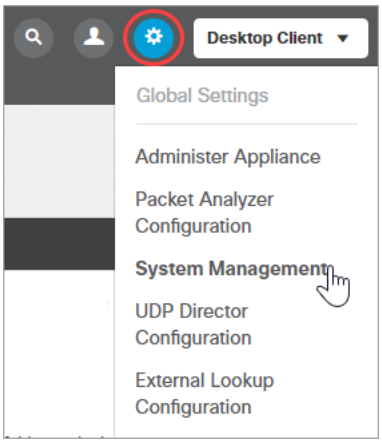
- **接続解除されるアプライアンス**:更新プロセス中に接続が解除されるアプライアンスがある場合、またはクラスタと関連付けられているアプライアンスが SMC で管理されていない場合、更新プロセスの中で、それらのアプライアンスをクラスタから接続解除するように求められることがあります。v7.0.x の更新完了後に、アプライアンスと管理設定を更新できます。「15. スタンドアロン アプライアンスと接続解除されたアプライアンスの更新」と「Central Managementにおける管理対象およびスタンドアロンの要件」を参照してください。
- **SMC の最大数**:この更新では 2 つの SMC を更新できます。
- UDP Director のハイ アベイラビリティ: UDP Director がハイ アベイラビリティ ペアとして設定されている場合は、仮想 IP アドレスで管理されていないことを確認します。 詳細については、「1. 管理対象アプライアンスの確認」を参照してください。

> ⚠ 更新プロセスの開始後は、アプライアンスの追加や削除、クラスタ設定の変更、または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。7.0.x の更新後に、それらのアプライアンスをクラスタに追加できます。

1. 管理対象アプライアンスの確認

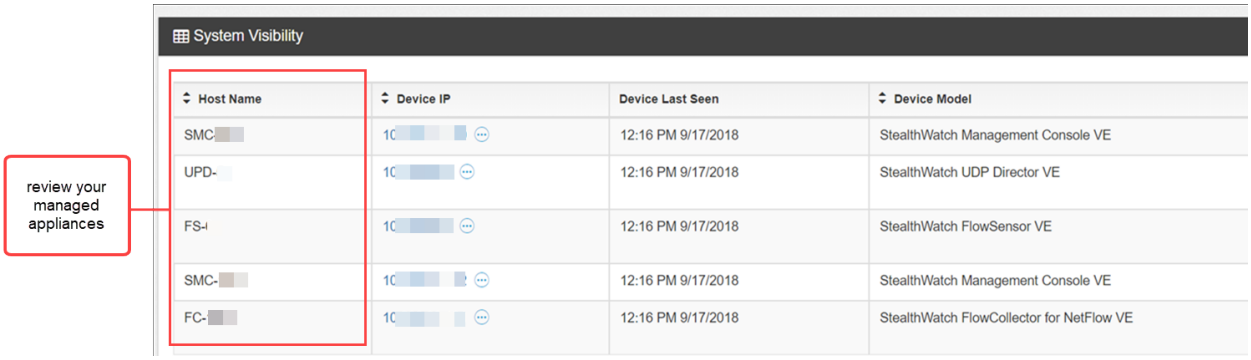
SMC システム管理リストをチェックして、Stealthwatch クラスタ内のアプライアンスを確認します。更新を開始する前に、次の手順を使用して、Stealthwatch クラスタに最終的な変更を加えます。

1. プライマリ SMC Web アプリケーションにログインします(https://[IP address])。
2. [グローバル設定(Global Settings)]アイコンをクリックします。[システム管理(System Management)]を選択します。



3. [システムの可視性(System Visibility)]セクションに表示されているアプライアンスを確認します。

   - 欠落アプライアンス: アプライアンスをこのリストに追加して、SMC の管理対象にするには、「Stealthwatch クラスタへのアプライアンスの追加」に進みます。
   - 旧式のアプライアンス: SMC システム管理からアプライアンスを削除する場合、または、[最後に表示されたデバイス(Device Last Seen)]列の時刻が最新ではない場合は、「Stealthwatch クラスタからのアプライアンスの削除」に進みます。
   - UDP Director のハイ アベイラビリティ: UDP Director がハイ アベイラビリティ ペアとして設定されている場合は、仮想 IP アドレスで管理されていないことを確認します。リストに UDP Director の仮想 IP アドレスが含まれている場合は、「Stealthwatch クラスタからのアプライアンスの削除」の手順に従い削除します。



Stealthwatch クラスタへのアプライアンスの追加

次の手順を使用して、Stealthwatch クラスタにアプライアンスを追加して、SMC の管理対象にします。エンドポイント コネクタを除くすべてのアプライアンスは、プライマリ SMC で管理されるように設定することをお勧めします。

すべてのアプライアンスを SMC の管理対象にするのが、アプライアンスを更新する最も速い方法ですが、必須ではありません。v7.0.x の更新完了後に、スタンドアロンアプライアンスを更新できます。「15. スタンドアロン アプライアンスと接続解除されたアプライアンスの更新」と「Central Managementにおける管理対象およびスタンドアロンの要件」を参照してください。

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. [設定(Configuration)] > [管理システムの設定(Management Systems Configuration)] の順に選択します。
3. [任意の管理システムからの接続を承認する(Accept connections from any management system)] チェックボックスをオフにします。
4. リストの確認: 管理システム設定のリストを確認します。システム内でアクティブになっていない SMC をすべて削除します。
5. [新しい管理システムの追加(Add New Management System)] をクリックします。
6. プライマリ SMC の IP アドレスとその他の必要なフィールドに値を入力します。セカンダリ SMC(フェールオーバー専用)がある場合は、ステップ 5 を繰り返します。
7. [適用(Apply)] をクリックします。画面に表示される指示に従って操作します。
8. SMC の [システム管理(System Management)] ページに戻ります。アプライアンスが表示されていることを確認します。ページの更新が必要な場合があります。

Stealthwatch クラスタからのアプライアンスの削除

次の手順を使用して、Stealthwatch クラスタからアプライアンスを削除して、SMC の管理対象外にします。

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. [設定(Configuration)] > [管理システムの設定(Management Systems Configuration)] の順に選択します。
3. [任意の管理システムからの接続を承認する(Accept connections from any management system)] チェックボックスをオフにします。
4. 管理リストで SMC を見つけます。
5. [削除(Delete)] チェックボックスをオンにします。
6. [適用(Apply)] をクリックします。画面に表示される指示に従って操作します。
7. SMC 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。
   - SMC の [システム管理(System Management)] ページで、[グローバル設定(Global Settings)] アイコンをクリックします。
   - [アプライアンスの管理(Administer Appliance)] を選択します。
8. [ホーム(Home)] ページを選択します。
9. [サービス(Services)] セクションで、次のサービスの [リロード(Reload)] をクリックします。

- upserv_uwsgi
- authserv_uwsgi

10. SMC の [システム管理（System Management）] ページに戻ります。アプライアンスが削除されたことを確認します。ページの更新が必要な場合があります。

    アプライアンスが削除されていない場合は、SMC デスクトップ クライアントにログインして、企業ツリーからアプライアンスを削除します。

    - アプライアンスを右クリックします。
    - [設定（Configuration）] > [削除（Delete）] の順に選択します。

2. FlowSensor の設定の確認

次の手順を使用して、FlowSensor の管理チャネルとトラフィックの設定を確認します。

1. FlowSensor 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. [設定（Configuration）] > [管理システムの設定（Management Systems Configuration）] の順に選択します。
3. 管理システム設定のリストを確認します。

    - FlowSensor が SMC の管理対象の場合は、プライマリ SMC とセカンダリ SMC（使用している場合）がこのリストに表示されていることを確認します。2 つの以上の SMC が表示されている場合は、非アクティブな SMC を削除します。
    - FlowSensor が SMC の管理対象外の場合は、このリストが空であることを確認します。このリストに SMC が含まれている場合は、それらを削除します。

4. [設定（Configuration）] > [NetFlowコレクタ（Net Flow Collectors）] の順に選択します。
5. NetFlow コレクタ リストを確認します。

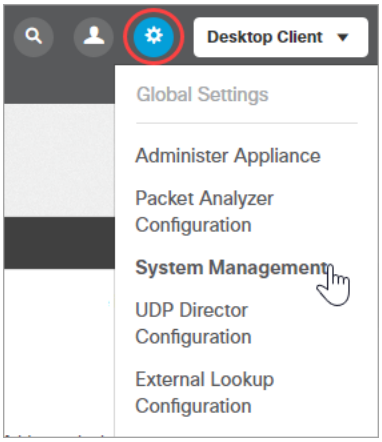
    - リスト内の Flow Collector が FlowSensor からトラフィックを受信していることを確認します。
    - 非アクティブまたは余分な Flow Collector をすべて削除します。

> ⚠ 更新プロセスの開始後は、アプライアンスの追加や削除、クラスタ設定の変更、または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。7.0.x の更新後に、それらのアプライアンスをクラスタに追加できます。

2. インストールされているソフトウェア バージョンの確認

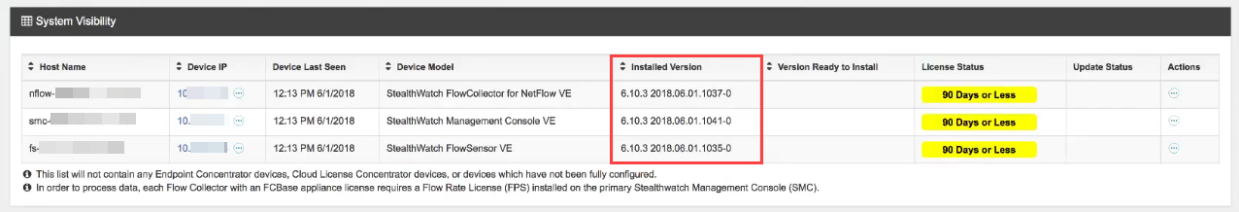
次の手順を実行して、各アプライアンスの現在のソフトウェア バージョンが 6.10.2、6.10.3、または 6.10.x の後続のバージョンであることを確認します。また、すべてのアプライアンスが同じソフトウェアバージョンを使用していることも確認してください。たとえば、SMC に v6.10.3 がインストールされている場合、クラスタ内の他のアプライアンスには v6.10.3 がインストールされている必要があります。

1. SMC Web アプリケーションのダッシュボードに移動します。
2. [グローバル設定（Global Settings）] アイコンをクリックします。[システム管理（System Management）] を選択します。



3. [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 v6.10.2 または 6.10.3（以降）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が同じソフトウェアバージョンを使用していることを確認してください。たとえば、SMC に v6.10.3 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は v6.10.3 がインストールされている必要があります。



   また、各バージョンの次の補足事項を確認してください。

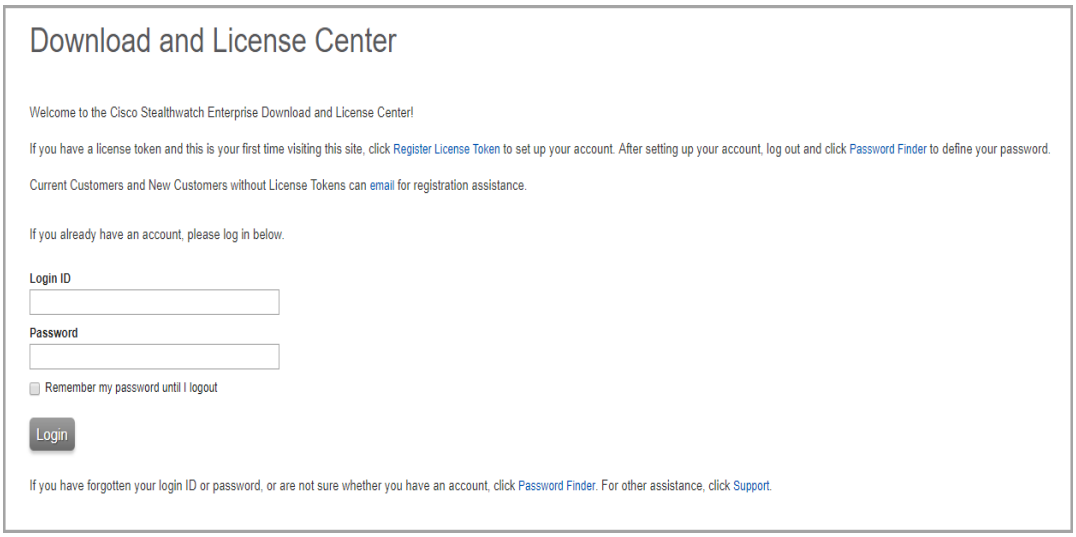
- 6.9.x 以前：インストールされているバージョンが 6.9.x 以前の場合は、Cisco.com にある Stealthwatch 更新ガイド [英語] を参照して、アプライアンスを v6.10.4（または 6.10.x の最新バージョン）に更新します。
- 6.10.2：インストールされているバージョンが 6.10.2 の場合は、Readme ファイルの手順に従い、6.10.2 ロールアップ パッチをインストールします。この更新には、patch-smc-ROLLUP008-6.10.2-01.swu（以降）が必要です。 詳細については、https://stealthwatch.flexnetoperations.com にログインして確認してください。
- 6.10.3：インストールされているバージョンが 6.10.3 の場合は、Readme ファイルの手順に従い、6.10.3 ロールアップ パッチをインストールします。詳細については、https://stealthwatch.flexnetoperations.com にログインして確認してください。
- 6.10.4：インストールされているバージョンが 6.10.4 の場合は、Readme ファイルの手順に従い、6.10.4 ロールアップ パッチをインストールします。この更新には、patch-common-lc-admin-6.10.4-01.swu（以降）が必要です。 詳細については、https://stealthwatch.flexnetoperations.com にログインして確認してください。
- 6.10.x： インストールされているバージョンが 6.10.5 以降の場合は、Readme ファイルの手順に従い、最新のロールアップ パッチをインストールします。詳細については、https://stealthwatch.flexnetoperations.com にログインして確認してください。

> 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。

3. パッチ ファイルとアップデート ファイルのダウンロード

次の手順を使用して、Pre-SWU と v7.0.x の更新 SWU をダウンロードします。

1. https://stealthwatch.flexnetoperations.com に移動します。



2. ダウンロードおよびライセンス センターにログインします。
3. [ダウンロード(Downloads)] > [Stealthwatchのアップグレード(Upgrade Stealthwatch)] の順に選択します。
4. [現在のバージョン(Current Versions)] タブで、アプライアンス名をクリックします。ソフトウェア リリース リンクをクリックしてダウンロードします(または [FTPのダウンロード(FTP Download)] を選択します)。

   - 各アプライアンスには、仮想(VE)アプライアンスと物理アプライアンスの両方に対する統合アップデート ファイルが 1 つあります。
   - すべてのアプライアンスに対する Pre-SWU パッチ ファイルおよびアップデート(SWU)ファイルをダウンロードします。詳細については、SWU ファイルの表を参照してください。
   - 詳細: 各項目の横にある下向き矢印をクリックして、追加のソフトウェア情報を表示します。

> ⚠ アプライアンスのソフトウェア アップデート ファイルを個別にダウンロードして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。

Pre-SWU(パッチ)ファイル

アプライアンス	パッチ ファイル名
SMC	patch-smc-pre-7.0-jumpstart-PATCH1-01.swu
その他すべてのアプライアンス • Flow Collector • Flow Sensor • UDP Director(別名 Flow Replicator) • エンドポイントコンセントレータ	patch-common-pre-7.0-jumpstart-PATCH1-01.swu 1 回だけのダウンロード: この 1 つのファイルを使用して各アプライアンスを更新します。

SWU ファイル

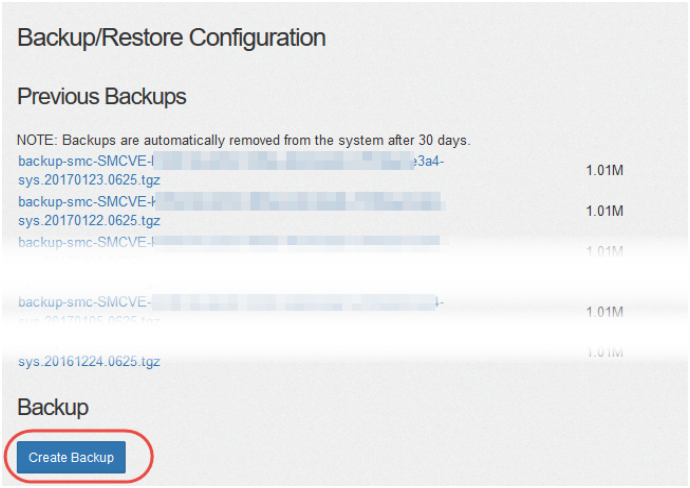
アプライアンス	更新ファイル名
UDP Director (別名 Flow Replicator) UDP Director VE (別名 Flow Replicator VE)	update-udpd-7.0.2.2019.07.05.1352-01.swu
Flow Collector 5000 シリーズ データベース	update-fcdb-7.0.2.2019.07.05.1406-01.swu
NetFlow 向けフローコレクタ (Flow Collector 5000 シリーズ エンジンに必要) NetFlow VE 向けフローコレクタ	update-fcnf-7.0.2.2019.07.05.1356-01.swu
sFlow 向けフローコレクタ sFlow VE 向けフローコレクタ	update-fcsf-7.0.2.2019.07.05.1355-01.swu
エンドポイントコンセントレータ	update-ec-7.0.2.2019.07.05.1352-01.swu
SMC および SMC VE	update-smc-7.0.2.2019.07.05.1359-01.swu
フローセンサーアプライアンス Flow Sensor VE	update-fsuf-7.0.2.2019.07.05.1353-01.swu

4. アプライアンスの設定のバックアップ

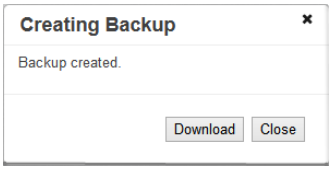
次の手順を実行して、各アプライアンスの設定をバックアップします。これらの手順は、データ損失を最小限に抑えるために重要です。

> ⚠ バックアップを作成しない場合、更新プロセス中に問題が発生してもファイルを回復することはできません。

1. 管理者ユーザとして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)]ページを選択します。
3. IP アドレスとホスト名を確認します。更新対象のアプライアンスであることを確認します。
4. [サポート(Support)]>[設定のバックアップ/復元(Backup/Restore Configuration)]の順にクリックします。
5. [バックアップ(Backup)]セクションで、[バックアップの作成(Create Backup)]をクリックします。



6. バックアップ プロセスが終了したら、[ダウンロード(Download)]をクリックします。バックアップ(TGZ)ファイルを任意の場所に保存します。



7. [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。
8. すべてのアプライアンスに対してステップ 1 ～ 7 を繰り返します。

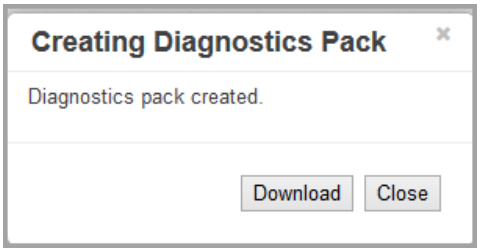
5. 診断パックの作成

診断パックがあると、Cisco Stealthwatch 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。

アプライアンス管理を使用して診断パックを作成するには、次の手順を実行します。

1. [サポート(Support)]>[診断パック(Diagnostics Pack)]の順にクリックします。
2. [診断パックの作成(Create Diagnostics Pack)]をクリックします。

3. [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。このプロセスに数分かかることがあります。



4. [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が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。

6. Flow Collector とSMC データベースのバックアップ

Flow Collector または SMC の診断パックを作成したら、Flow Collector および SMC データベースをバックアップします。

> アプライアンスがフローコレクタまたは SMC ではない場合は、この手順をスキップできます。

このプロセスには、次の手順が含まれます。

1. SNMP ポーリングを無効にする。
2. データベースをバックアップする。
3. SNMP ポーリングを再度有効にする。

> 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。

SMC のSNMP ポーリングの無効化

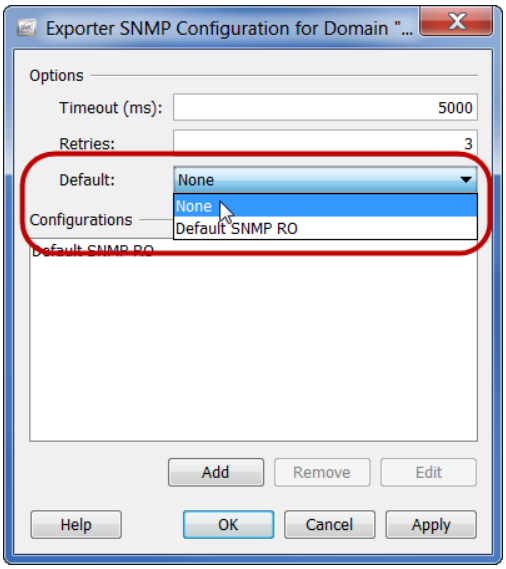
データベースのバックアップには、時間がかかる場合があります。SNMP プロセスによるバックアップの中断を防ぐには、SNMP ポーリングをオフにします。その後、バックアップが終了したら SNMP ポーリングを再度有効にします。

SNMP ポーリングを無効にするには、次の手順を実行します。

1. 管理者ユーザとして SMC デスクトップ クライアントを起動します（ただし、アプライアンス管理インターフェイスは閉じないでください）。
2. 企業ツリーで、エクスポータを右クリックします。

   [設定（Configuration）] > [エクスポータのSNMP設定（Exporter SNMP Configuration）] の順に選択します。

3. [デフォルト（Default）] フィールドのエントリをメモします。この情報は、データベースのバックアップ後に再入力します。



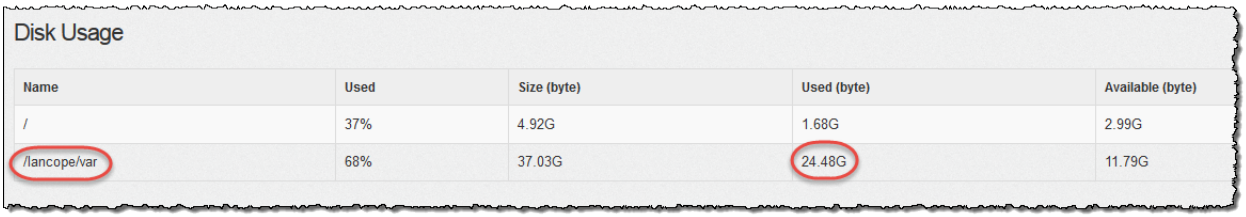
4. [デフォルト(Default)]ドロップダウンリストから[なし(None)]を選択します。このドメインの SNMP ポーリングがオフになりました。
5. [OK]をクリックします。
6. システム上の各ドメインについてステップ 2 ～ 5 を繰り返します。

データベースのバックアップ

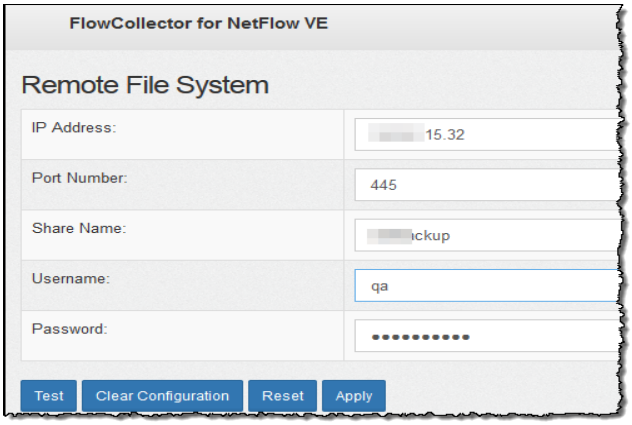
リモートファイル システムにフローコレクタまたは SMC データベースをバックアップするには、次の手順を実行します。

- 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、SMC 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[使用済み(バイト)(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。

   Stealthwatch ファイル共有は CIFS(Common Internet File System)、別名 SMB(Server Message Block)というプロトコルを使用します。

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。

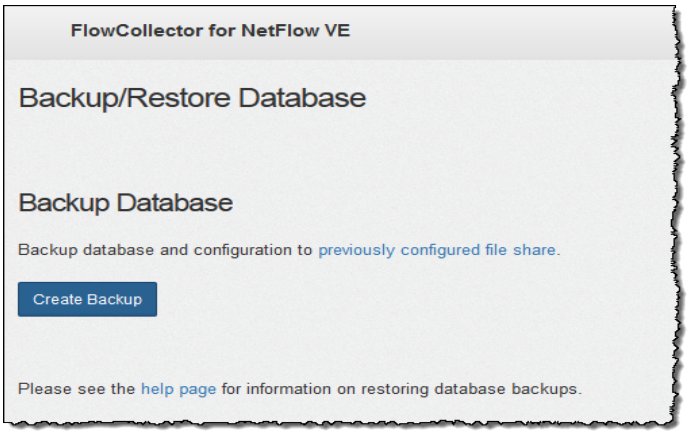
   パスワードを入力しても[適用(Apply)]ボタンが有効にならない場合、[リモートファイルシステム(Remote File System)]ページの空白部分を 1 回クリックすると有効になります。

6. [テスト(Test)]をクリックして、Stealthwatch 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。

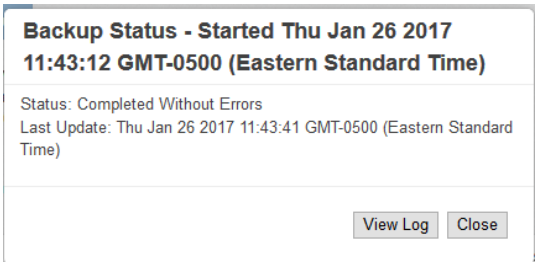
   File sharing appears to be properly configured.

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. [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。

SMC でのSNMP ポーリングの再有効化

SNMP ポーリングを再び有効化するには、次の手順を実行します。

1. SMC デスクトップ クライアントに戻ります(ただし、アプライアンス管理インターフェイスは閉じないでください)。
2. 適切なドメインを右クリックし、[設定(Configuration)]>[エクスポータのSNMP設定(Exporter SNMP Configuration)]の順に選択します。そのドメインの[エクスポータのSNMP構成(Exporter SNMP Configuration)]ページが開きます。
3. [デフォルト(Default)]ドロップダウンリストから、選択したドメインの元のエントリを選択します(「SNMPポーリングの無効化」のステップ 3 を参照)。このドメインの SNMP ポーリングが再度有効になりました。
4. [OK]をクリックします。

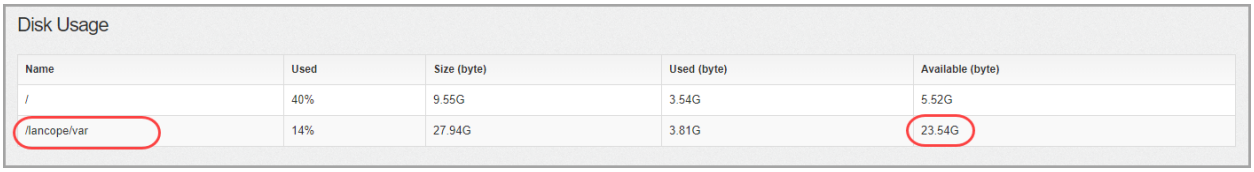
5. システム上の各ドメインについて、この手順のステップ 2 ～ 4 を繰り返します。
6. SMC デスクトップ クライアントを閉じます。

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、ソフトウェア アップデート用の十分なディスク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. [使用可能(バイト)(Available(byte))]列を確認し、/lancope/var/ パーティションにソフトウェア アップデート ファイル(SWU)のサイズの 4 倍以上の空き容量があることを確認します。

    - たとえば、ソフトウェア アップデート ファイル(ダウンロードおよびライセンス センターから取得)が 6 GB の場合、パーティションには 24 GB の空き容量が必要です。
    - SWU が SMC にアップロードされる際、更新中に追加の容量が使用されます。更新が完了すると、SWU はファイル システムから削除されます。


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 Stealthwatch の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「Data Storage」セクションを参照してください。

8. SMC でのPre-SWU パッチのインストール

次の手順に従い、アプライアンス管理者インターフェイスを使用して、StealthWatch Management Console（SMC）でPre-SWU パッチをインストールします。

SMC フェールオーバー ペアがある場合は、最初にセカンダリ SMC でPre-SWU をインストールしてください。

> ⚠ 更新プロセスの開始後は、アプライアンスの追加や削除、クラスタ設定の変更、または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。これらのアプライアンスは、7.0.x クラスタの更新後にクラスタに追加できます。

1. 管理者として SMC にログインします（https://[IP address]）。

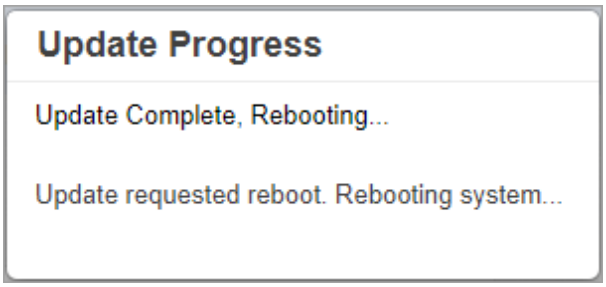
   SMC フェールオーバー ペアがある場合は、最初にセカンダリ SMC にログインします。

2. [グローバル設定（Global Settings）] アイコンをクリックします。[アプライアンスの管理（Administer Appliance）] を選択します。
3. [サポート（Support）] > [更新（Update）] の順にクリックします。
4. [ファイルの選択（Choose File）] をクリックします。
5. Pre-SWU パッチ ファイルを選択します。

   patch-smc-pre-7.0-jumpstart-PATCH1-01.swu

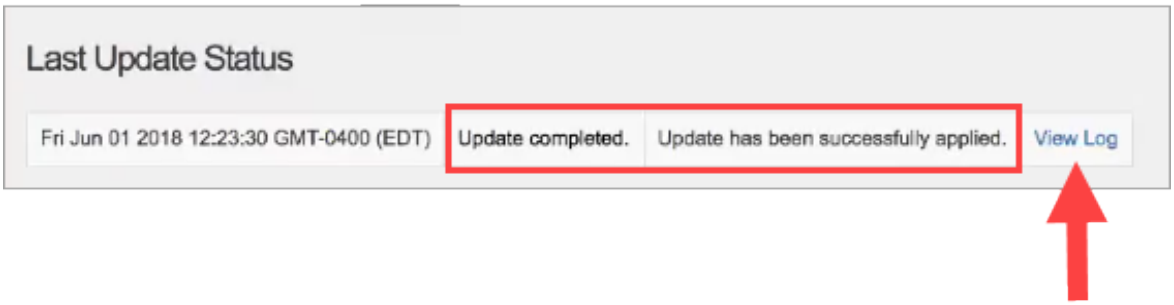
6. [開く（Open）] をクリックします。
7. [自動的に実行（Automatically Execute）] チェックボックスをオンにします。
8. [アップロード（Upload）] をクリックします。画面に表示される指示に従って、インストールを開始します。

9. [更新の進捗状況（Update Progress）] に [完了（Complete）] および [再起動（Rebooting）] が表示されたら、ページを更新します。



- これは、一般的なパッチよりも時間がかかる場合があります。
- 再起動：システムは自動的に再起動します。
- 更新：アプライアンスとサービスの再起動中に、ページが一時停止することがあります。ページを更新して、進捗状況を確認します。

10. インストールの確認：SMC 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。
    - [サポート（Support）]>[更新（Update）]の順に選択します。
    - [前回の更新ステータス（Last Update Status）]セクションで、Pre-SWU が正常に適用されたと表示されていることを確認します。[ログの表示（View Log）]をクリックして、詳細を確認します。



⚠ Pre-SWU のインストールが失敗した場合は、再度インストールせずに、Cisco Stealthwatch サポートに連絡してください。

11. SMC フェールオーバー ペアがある場合は、手順「8. SMC での Pre-SWU パッチのインストール」を繰り返して、プライマリ SMC で Pre-SWU パッチをインストールします。

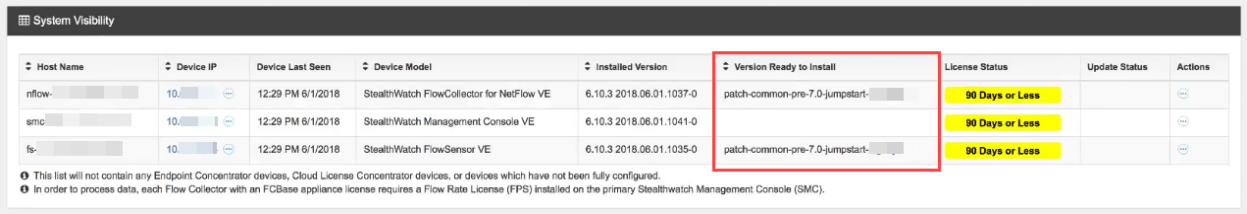
9. 管理対象アプライアンスでの Pre-SWU パッチのインストール

プライマリ SMC アプライアンス管理で Pre-SWU パッチをインストールすると、[システム管理(System Management)] ページでの Pre-SWU インストールに対する管理対象アプライアンスの準備が行われます。次の手順を使用して、管理対象アプライアンスで Pre-SWU パッチをインストールします。

1. プライマリ SMC Web アプリケーション ダッシュボードに移動します。
2. [グローバル設定(Global Settings)] アイコンをクリックします。[システム管理(System Management)] を選択します。
3. [システムの可視性(System Visibility)] で、アプライアンスのリストを確認します。

    - 各アプライアンスの [インストール可能なバージョン(Version Ready to Install)] 列に patch-common-pre-7.0-jumpstart-PATCH1-01.swu が表示されていることを確認します。

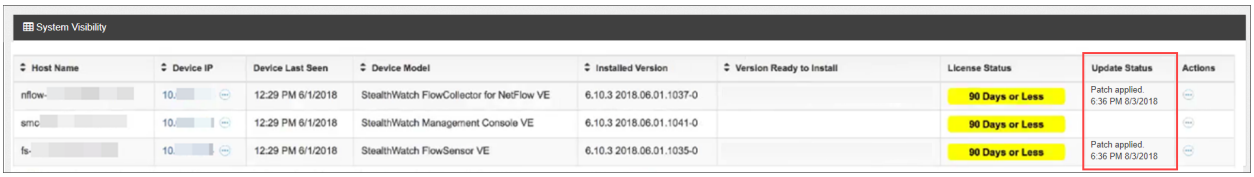
    - SMC: SMC の [インストール可能なバージョン(Version Ready to Install)] は、すでにインストールされているため空白になります。



4. 参考として使用するために、[システムの可視性(System Visibility)] リストのスクリーンショットを取ります。
5. 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。[更新のインストール(Install Update)] を選択します。

    - 順序: SMC を最初に更新するならば、任意の順序でアプライアンスで Pre-SWU をインストールできます。
    - 複数のアプライアンス: 同時に複数のアプライアンスで Pre-SWU をインストールできます。
    - ステータス: [更新ステータス(Update Status)] 列をチェックし、ページを更新して更新の進捗状況を確認します。

6. [システムの可視性(System Visibility)] でアプライアンスごとにステップ 5 を繰り返します。
7. [更新ステータス(Update Status)] 列を確認します。すべてのアプライアンス(SMC を除く)で [パッチ適用済み(Patch Applied)] が表示されていることを確認します。

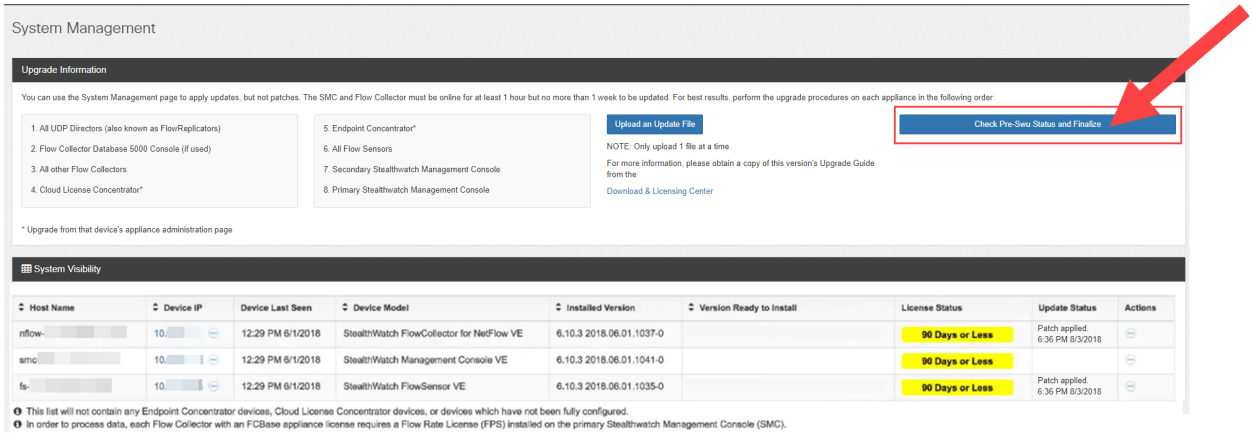


10. Pre-SWU のインストールの終了

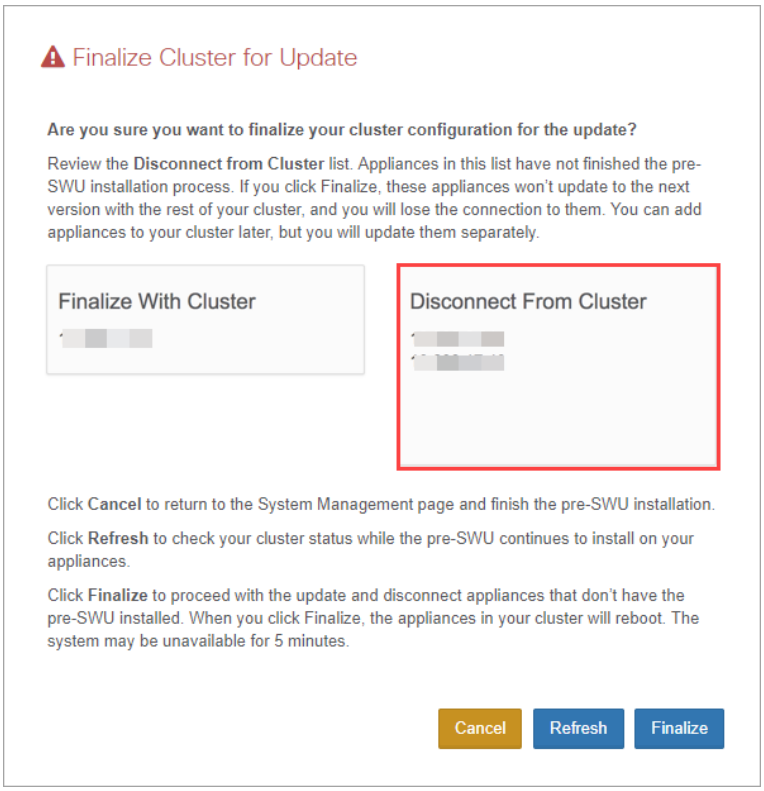
次の手順を使用して、クラスタでの Pre-SWU のインストールを終了し、v7.0.2 へのアップグレードの準備をします。

> ⚠ Pre-SWU のインストールが終了したら、できるだけ早くアプライアンスをアップグレードすることをお勧めします。Pre-SWU と v7.0.x SWU の更新の間もアプライアンスは使用できますが、機能は制限されます。

1. [Pre-SWUのステータスの確認と終了（Check Pre-SWU Status and Finalize）]をクリックします。



2. [クラスタリストからの接続解除(Disconnect From Cluster List)]を確認します。



[接続解除(Disconnect)]リストにアプライアンスが含まれていない場合は、ステップ 3 に進みます。

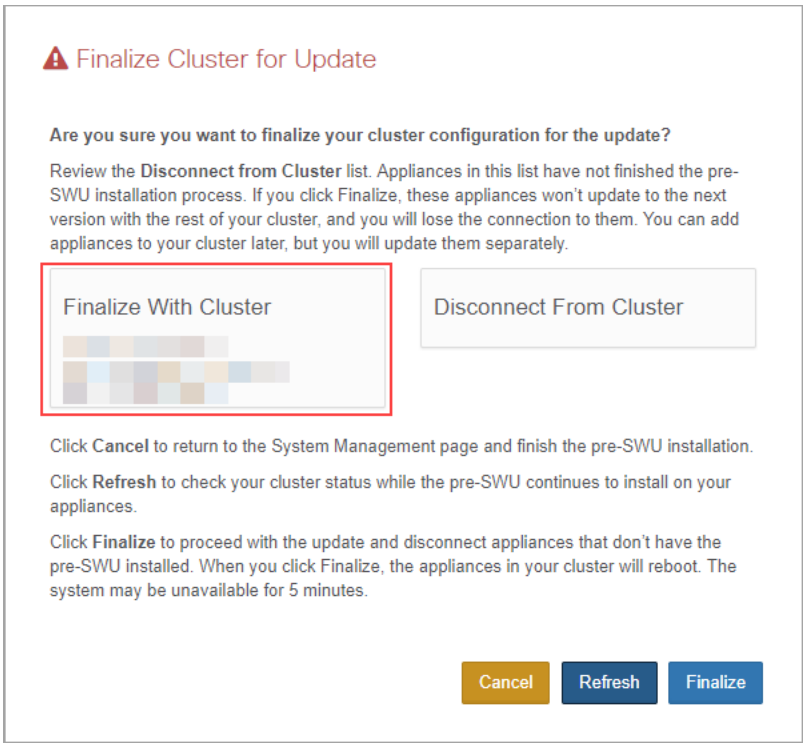
[接続解除(Disconnect)]リストにアプライアンスが含まれている場合、それらのアプライアンスでは Pre-SWU のインストールは完了していません。

- 必要に応じて、[更新(Refresh)]をクリックし、アプライアンスが[クラスタの処理終了(Finalize With Cluster)]リストに移動するまで待ちます。
- 次のオプションを参照して、アプライアンスを Stealthwatch クラスタに保持する必要があるか、アプライアンスを接続解除するかを判断します。

オプション	詳細
クラスタ内で保持	Stealthwatch クラスタでアプライアンスを保持するには、必要に応じて[更新(Refresh)]をクリックし、アプライアンスが[クラスタの処理終了(Finalize With Cluster)]リストに移動するまで待ちます。

クラスタからの接続解除	Stealthwatch クラスタからアプライアンスを接続解除し、それらのアプライアンスでの Pre-SWU のインストールを省略するには、ステップ 3 に進みます。 **アプライアンスを接続解除する場合:** • 接続解除したアプライアンスは、他のクラスタで次のバージョンに更新されません。 • 接続解除したアプライアンスへの接続は失われます。 • 後でクラスタにアプライアンスを追加することはできますが、それらのアプライアンスは個別に更新します。 • リストのスクリーンショットを取り、IP アドレスをなくさないようにします。
トラブルシューティング	[クラスタからの接続解除(Disconnect From Cluster)]リストに含まれているアプライアンスをクラスタで更新する必要があるが、それらのアプライアンスが[クラスタの処理終了(Finalize With Cluster)]リストに移動していない場合は、[キャンセル(Cancel)]をクリックします。Cisco Stealthwatch サポートに連絡して、サポートを受けてください。 ポートの警告: アプライアンスは、この更新のために**ポート 5672** を使用して通信しています。詳細については、「ポート 5672」を参照してください。更新中にポート エラーが発生した場合は、このポートが開いていることを確認するか、システム管理者にお問い合わせください。 SMC フェールオーバー: SMC フェールオーバーの設定に失敗した場合、またはフェールオーバー ペアのいずれかの SMC を失った場合は、Cisco Stealthwatch サポートに連絡して、サポートを受けてください。

3. クラスタ内のすべてのアプライアンスが[クラスタの処理終了(Finalize With Cluster)]セクションに表示されていることを確認します。表示されている場合、Pre-SWU のインストールを完了し、更新に進むことができます。



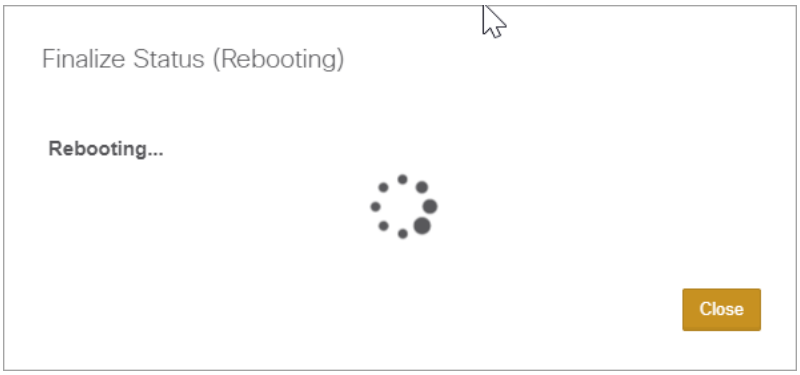
⚠ [終了(Finalize)]をクリックすると[クラスタからの接続解除(Disconnect From Cluster)]リストに含まれているアプライアンスが接続解除されて、Stealthwatch クラスタから削除されます。それらのアプライアンスは個別に更新できます。

4. [終了(Finalize)]をクリックします。

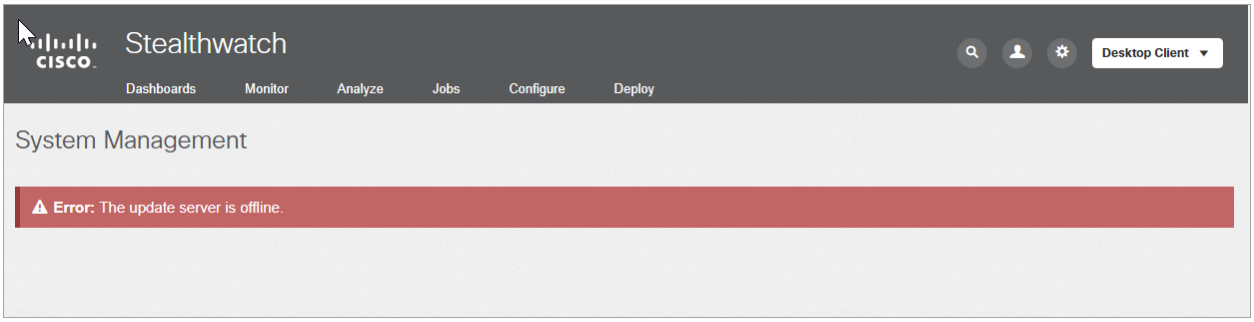
   再起動: システムは自動的に再起動します。

   更新: アプライアンスとサービスの再起動中に、ページが一時停止することがあります。[更新(Refresh)]をクリックして、Pre-SWU の終了プロセスの進捗状況を表示します。

5. [終了ステータス(Finalize Status)]に[再起動中(Rebooting)]と表示されたら、[閉じる(Close)]をクリックします。

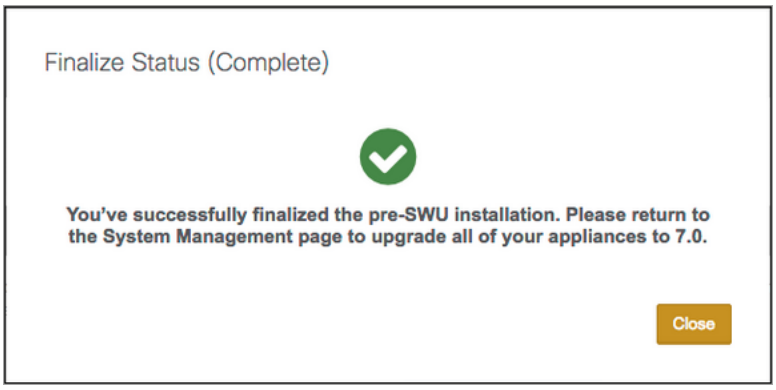


6. [システム管理(System Management)]ページに、サーバがオフラインであることを示すエラーが表示されます。ページを更新します。



7. プライマリ SMC Web アプリケーションにログインします(https://[IP address])。
8. [システム管理(System Management)]ページに戻ります。
   - [グローバル設定(Global Settings)]アイコンをクリックします。
   - [システム管理(System Management)]を選択します。
9. [Pre-SWUのステータスの確認と終了(Check Pre-SWU Status and Finalize)]をクリックします。

   完了:[終了ステータス(Finalize Status)]に、[完了(Complete)]と表示されていることを確認します。



   未完了:[終了ステータス(Finalize Status)]が[完了(Complete)]でない場合は、[システム管理(System Management)]ページに戻ります。Pre-SWU インストールのステータスを確認するか、または Cisco Stealthwatch サポートに連絡します。

> ⚠ SMC での Pre-SWU のインストールが失敗した場合は、再度インストールせずに、Cisco Stealthwatch サポートに連絡してください。

11. 7.0 ソフトウェア アップデートのインストール

7.0.2（または 7.0.x であるその後のバージョン）のソフトウェアアップデートでも、引き続き [システム管理（System Management）] ページを使用します。

> ⚠ v7.0.x ソフトウェアアップデートを開始する前に、SMC およびフローコレクタが 1 時間以上稼働していることを確認します。

新しい更新順序の使用

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	詳細
1.	UDP Director （別名 FlowReplicators）	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 が再稼動していることを確認したら、プライマリ UDP Director を更新します。
2.	Flow Collector 5000 シリーズ データベース	更新を開始する前に、Flow Collector が 1 時間以上稼働していることを確認します。
3.	Flow Collector 5000 シリーズ エンジン	Flow Collector 5000 シリーズ データベースの更新が完了し、再稼働していることを確認してから、エンジンの更新を開始します。
4.	その他のすべての Flow Collector （NetFlow および sflow）	更新を開始する前に、Flow Collector が 1 時間以上稼働していることを確認します。
5.	Flow Sensor	
6.	セカンダリ SMC （使用する場合）	更新を開始する前に、SMC が 1 時間以上稼働していることを確認します。 システムでセカンダリ SMC を使用している場合は、セカンダリ SMC の更新が完了し、セカンダリ SMC が再稼動していることを確認してから、プライマリ SMC の更新を開始します。

		更新が完了すると、両方の SMC がセカンダリ ロールで再起動する可能性があります。再起動した場合は、「SMC 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 SMC 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	更新を開始する前に、SMC が 1 時間以上稼働していることを確認します。 システムでセカンダリ SMC を使用している場合は、セカンダリ SMC の更新が完了し、セカンダリ SMC が再稼動していることを確認してから、プライマリ SMC の更新を開始します。 更新が完了すると、両方の SMC がセカンダリ ロールで再起動する可能性があります。再起動した場合は、「SMC 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 SMC が更新されるまで変更しないでください。
8.	スタンドアロン アプライアンスと接続解除されたアプライアンス	例：エンドポイント コンセントレータ、またはいずれかのアプライアンスが SMC で管理されていない。 注：これらのアプライアンスは、すべての管理対象アプライアンスの更新終了後に更新します。スタンドアロン アプライアンスは、アプライアンス管理者インターフェイスを使用して更新します。

ベスト プラクティス

- **順序**：アプライアンスを順番通りに更新します。開始する前に、アプライアンスの更新順序で詳細を確認してください。
- **待機**：v7.0.x ソフトウェアアップデートを開始する前に、SMC およびフローコレクタが 1 時間以上稼働してい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、更新が完了し、各アプライアンスが稼動していることを確認します。
- **複数のアプライアンス**：SMC と Flow Collector 5000 シリーズを除き、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い、複数のアプライアンスを同時に更新できます。

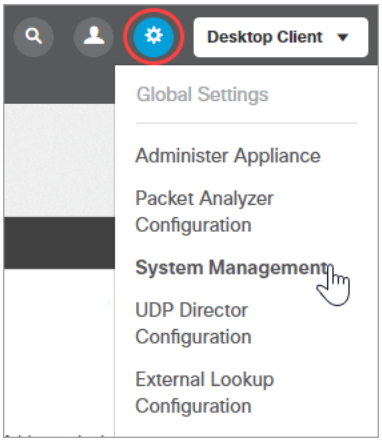
  たとえば、クラスタ内に複数のフロー センサーがある場合は、すべてのフロー センサー

を同時に更新できます。ただし、最初にクラスタ内のすべてのフローコレクタの更新が完了していることを確認してください。

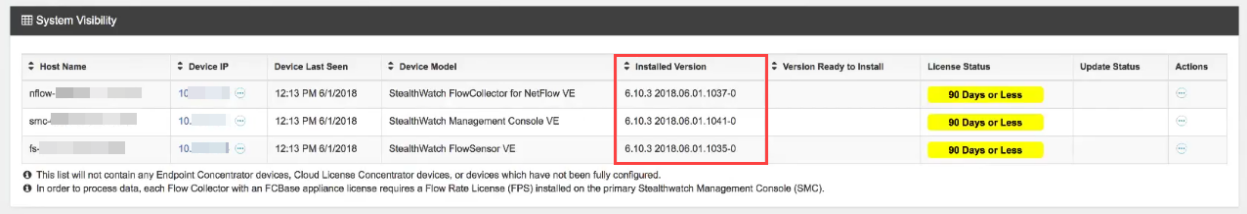
管理対象アプライアンスでのv7.0.2 更新プログラムのインストール

次の手順に従い、[システム管理(System Management)]ページを使用して、SMC の管理対象アプライアンスに v7.0.2 ソフトウエア(または 7.0.x であるその後のバージョン)をインストールします。

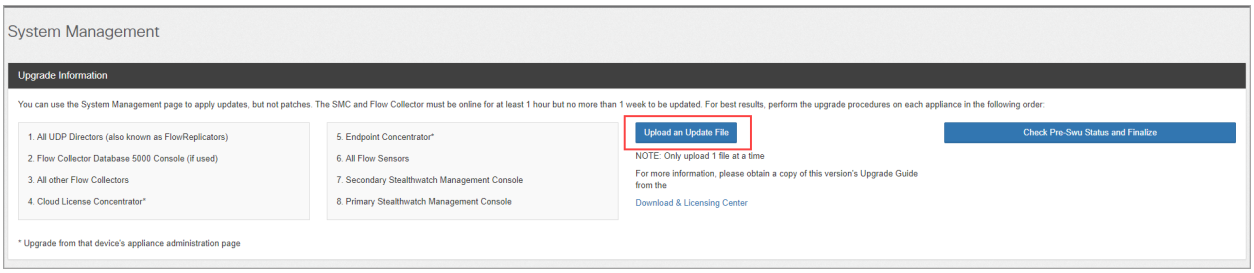
1. プライマリ SMC Web アプリケーションにログインします(https://[IP address])。
2. [グローバル設定(Global Settings)]アイコンをクリックします。[システム管理(System Management)]を選択します。



[システムの可視性(System Visibility)]セクションの[インストールされているバージョン(Installed Version)]列には、引き続き v6.10.x がインストール バージョンとして表示されます。

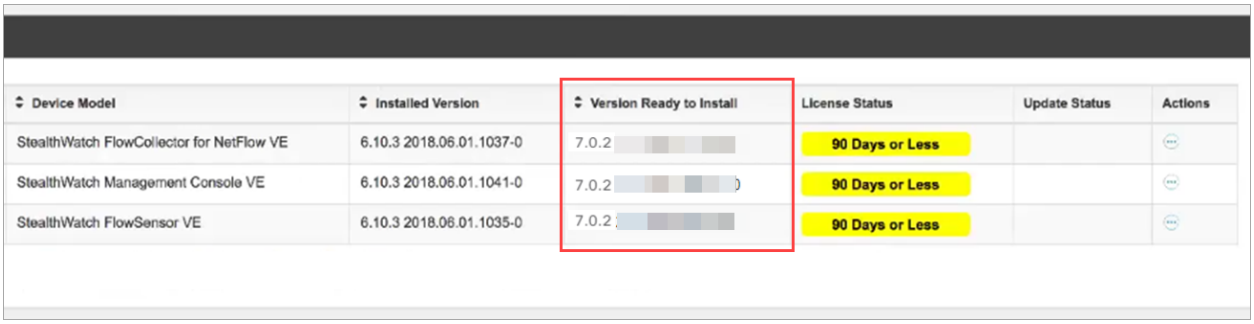


3. [アップデートファイルのアップロード(Upload an Update File)]をクリックします。



- ファイルの選択：ダウンロードおよびライセンスセンターからダウンロードした v7.0.2 ソフトウェア アップデート ファイル（SWU）を選択します。
- 各アプライアンスに対してこのステップを繰り返して、v7.0.2 SWU ファイルをアップロードします。詳細については、SWU ファイルの表を参照してください。

4. [システムの可視性（System Visibility）] セクションでアプライアンス リストを確認します。[インストール可能なバージョン（Version Ready to Install）] 列に v7.0.x ソフトウェアバージョンが表示されていることを確認します。



5. アプライアンスの更新順序を使用して、アプライランスの [アクション（Actions）] メニューをクリックします。[更新のインストール（Install Update）] を選択します。

> ⚠ アプライアンスを順番通りに更新します。開始する前に、アプライアンスの更新順序で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、更新が完了し、各アプライアンスが稼動していることを確認します。この情報を確認するには、ステップ 6 および 7 を参照してください。

6. [システムの可視性（System Visibility）] **セクションで、[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。アプライアンスに v7.0.x がインストールされていることを確認します。

   更新：アプライアンスとサービスの再起動中に、ページが一時停止することがあります。ページを更新して、現在の [更新ステータス（Update Status）] を表示します。

7. 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。アプライアンス管理インターフェイスが開きます。

   - **ログイン**：管理者ユーザとして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。
   - **成功**：[前回の更新ステータス（Last update Status）] セクションで、更新が正常に完了または適用されたことを確認します。

- **稼働時間**: [ホーム(Home)]をクリックします。[稼働時間(Uptime)]のセクションを見つけます。アプライアンスが稼働中であることを確認します。稼働時間は 60 秒ごとに更新されます。

8. [システム管理(System Management)]ページに表示されているすべてのアプライアンスに対してステップ 5 ～ 7 を繰り返します。

   リロード: ページのロード中に問題が発生した場合は、ブラウザのキャッシュをクリアし、ブラウザを閉じて再度開いてから、もう一度ログインします。

9. アプライアンスの更新順序の最後にあるプライマリ SMC を更新すると、システムが再起動します。再度ログインすると、新しい [Central Management アップデート マネージャ(Central Management Update Manager)]ページが開きます。

12. Central Management へのログイン

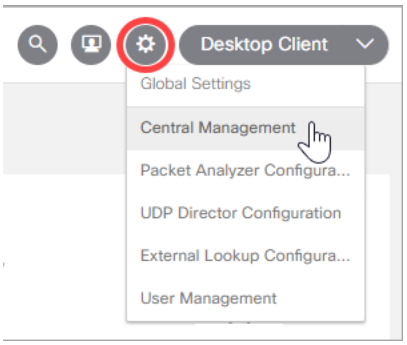
アプライアンス ソフトウェアを v7.0.x に更新すると、Central Management がプライマリ SMC に追加されます。

- Central Management について：アプライアンスが Central Management によって管理されている場合、それらのアプライアンスのステータスを確認できるのに加えて、アプライアンス設定の編集、ソフトウェアの更新、再起動、シャットダウンなどを管理できます。
- Stealthwatch のヘルプ：各ページの詳細については、[ヘルプ（Help）] アイコンをクリックして、[Stealthwatch オンライン ヘルプ（Stealthwatch Online Help）] を選択します。

1. 最後の手順（管理対象アプライアンスでの v7.0.2 更新プログラムのインストール）では、Central Management アップデートマネージャに移動します。[Appliance Manager] タブをクリックします。

   ログインする必要がある場合：

   - SMC Web アプリケーションにログインします。
   - [グローバル設定（Global Settings）] アイコンをクリックします。
   - [Central Management] を選択します。

2. [Appliance Manager] ダッシュボードでアプライアンスを確認します。

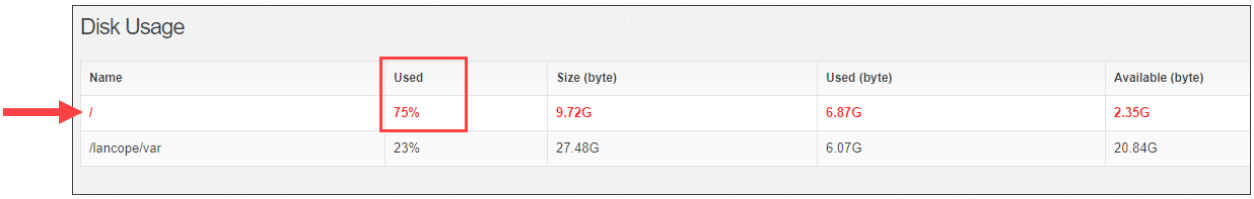
   - 管理対象アプライアンス：Stealthwatch クラスタ内のすべてのアプライアンスが表示されていることを確認します。[アプライアンス ステータス（Appliance Status）] 列を確認し、各アプライアンスが [Up] と表示されていることを確認します。

   - SMC：プライマリ SMC とセカンダリ SMC がある場合は、各 SMC の [アプライアンス ステータス（Appliance Status）] が [Up] と表示されていることを確認します。

3. ルート パーティション：すべてアプライアンスに対してこのステップを繰り返して、ルート パーティションを確認します。

   - 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。

- [アプライアンス統計情報の表示（View Appliance Statistics）]を選択します。
- 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。
- [ホーム（Home）]ページで、[ディスク使用量（Disk Usage）]セクションを見つけます。
- 上の行 / を確認し、[使用済み（Used）]列のパーセンテージをチェックします。使用率が 75 % 以上の場合、このルート パーティションのデータは赤で表示されます。ルート パーティションが埋まった状態が続くと、重要な機能が停止することがあります。使用率が 100 % に近づくに従い、アプライアンスの更新を検討する必要が生じます。



13. v7.0.2 パッチのインストール

1. Stealthwatch ダウンロードおよびライセンスセンターにあるパッチの readme ファイルの指示に従って、Central Management の [アップデートマネージャ(Update Manager)] ページを使用して次のパッチをインストールします。

   - **SMC**: patch-smc-ROLLUP003-7.0.2-02.swu

2. Flow Sensor 4000: Flow Sensor 4000 を使用している場合は、Central Management の [アップデートマネージャ(Update Manager)] ページを使用して、必要なパッチをインストールします。

   - 詳細については、パッチの Readme ファイルを参照してください。
   - この要件は、FS4000 モデルにのみ適用されます。Flow Sensor 4000 シリーズのその他のモデルには適用されません。
   - 詳細については、Stealthwatch のダウンロードおよびライセンス センター https://stealthwatch.flexnetoperations.com [英語] にログインして確認してください。

3. SMC デスクトップ クライアントまたは SMC フェールオーバー ペアを使用する場合は、次の手順「14. SMC デスクトップ クライアントへのログイン」に進みます。

   - SMC デスクトップ クライアントまたは SMC フェールオーバー ペアを使用しない場合は、管理対象アプライアンスでの v7.0.x アップグレードは終了です。
   - スタンドアロン アプライアンスを更新する場合は、「15. スタンドアロン アプライアンスと接続解除されたアプライアンスの更新」を繰り返します。
   - 接続解除されたアプライアンスまたはスタンドアロン アプライアンスを集中管理に追加する場合は、「15. スタンドアロン アプライアンスと接続解除されたアプライアンスの更新」を繰り返します。

14. SMC デスクトップ クライアントへのログイン

SMC デスクトップ クライアントまたは SMC フェールオーバーの設定を使用しない場合、この手順はスキップできます。SMC デスクトップ クライアント製品機能のリストについては、開始する前に「Java」セクションを参照してください。

SMC デスクトップ クライアントの証明書を信頼

v7.0.x の更新の一環として、デフォルトのアプライアンス アイデンティティ証明書（旧 Lancope）が新しい一意の自己署名アプライアンス アイデンティティ証明書で置き換えられます。次の手順を使用して、SMC デスクトップ クライアントで証明書を受け入れます。

- アプライアンスでカスタム証明書を使用している場合、証明書は置き換えられません。ただし、場合によっては、SMC デスクトップ クライアントを開いて、証明書を確認する必要があります。
- デスクトップ クライアントにログインできない場合は、正しいバージョンの Java をインストールしていることを確認します。

1. SMC Web アプリケーションにログインします。
2. [デスクトップクライアント（Desktop Client）] をクリックします。
3. 画面に表示される指示に従って、新しい証明書を確認して信頼します。

   新しい証明書を信頼することを要求されず、SMC デスクトップ クライアントでデータにアクセスできる場合、アクションは不要です。

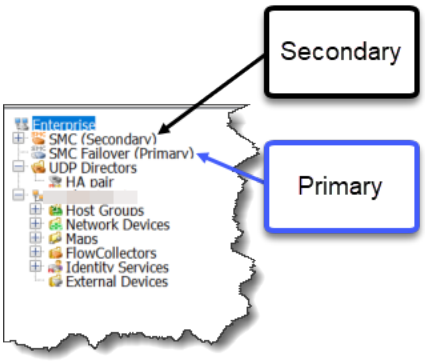
SMC フェールオーバー ロールの確認

フェールオーバー ロールは、両方の SMC 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 SMC アプライアンスのステータスが [Up] と表示されるまで行わないでください。

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

1. 管理者レベルのユーザ名とパスワードを使用して、セカンダリ SMC にログインします。
2. デスクトップ クライアントを開きます。
3. 企業ツリーで、SMC フェールオーバー（プライマリ）と SMC（セカンダリ）が表示されている各ブランチを確認します。



4. 両方の SMC 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 SMC と 1 つセカンダリ SMC がある状態にします。SMC デスクトップ クライアントのヘルプの手順に従っていることを確認します。

> 詳細については、SMC デスクトップ クライアントのヘルプを参照してください。

5. セカンダリ SMC Web アプリケーションにログインします。
6. [フローコレクションの傾向(Flow Collection Trend)]を確認します。

7. 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、Central Management を使用して Flow Collector とセカンダリ SMC を再起動します。

   - プライマリ SMC にログインします。
   - Central Management を開きます。
   - [Appliance Manager] ページで Flow Collector を見つけます。
   - [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、Central Management ですべての Flow Collector を再起動します。
- セカンダリ SMC：手順を繰り返して、セカンダリ SMC を再起動します。

8. プライマリ SMC にログインします。
9. [Central Management] > [Appliance Manager]を確認します。 セカンダリ SMC アプライアンスのステータスが [Up] と表示されていることを確認します。

15. スタンドアロン アプライアンスと接続解除されたアプライアンスの更新

次の手順を使用して、次の状況のアプライアンスを v7.0.2（または 7.0.x であるその後のバージョン）に更新します。

- アプライアンスがエンドポイントコンセントレータの場合
- Pre-SWU のインストール中に、クラスタからアプライアンスを接続解除した場合
- SMC で管理されていないために、他のクラスタで更新されなかったスタンドアロン アプライアンスがある場合

エンドポイントコネクタを除くすべてのアプライアンスは、プライマリ SMC で管理されるように設定することをお勧めします。更新が完了した後に、Central Management にアプライアンスを追加する必要があるかどうかを判断するには、「Central Managementにおける管理対象およびスタンドアロンの要件」を参照してください。

> 接続解除されたアプライアンスも、スタンドアロン アプライアンスもない場合、v7.0.x Stealthwatch の更新は終了です。

1. ソフトウェア バージョンの確認

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（https://[IP address]）。[ホーム（Home）] ページに表示されているソフトウェア バージョンを確認します。

- 6.9.x 以前：インストールされているバージョンが 6.9.x 以前の場合は、Cisco.com にある Stealthwatch 更新ガイド [英語] を参照して、アプライアンスを v6.10.4（または 6.10.x の最新バージョン）に更新します。
- 6.10.2：インストールされているバージョンが 6.10.2 の場合は、Readme ファイルの手順に従い、6.10.2 ロールアップ パッチをインストールします。この更新には、patch-smc-ROLLUP008-6.10.2-01.swu（以降）が必要です。 詳細については、https://stealthwatch.flexnetoperations.com にログインして確認してください。
- 6.10.3：インストールされているバージョンが 6.10.3 の場合は、Readme ファイルの手順に従い、6.10.3 ロールアップ パッチをインストールします。詳細については、https://stealthwatch.flexnetoperations.com にログインして確認してください。
- 6.10.4：インストールされているバージョンが 6.10.4 の場合は、Readme ファイルの手順に従い、6.10.4 ロールアップ パッチをインストールします。この更新には、patch-common-lc-admin-6.10.4-01.swu（以降）が必要です。 詳細については、https://stealthwatch.flexnetoperations.com にログインして確認してください。
- 6.10.x：インストールされているバージョンが 6.10.5 以降の場合は、Readme ファイルの手順に従い、最新のロールアップ パッチをインストールします。詳細については、https://stealthwatch.flexnetoperations.com にログインして確認してください。

> すべてのアプライアンスが同じソフトウェアバージョンを使用していることを確認してください。たとえば、SMC に v6.10.3 がインストールされている場合、スタンドアロン アプライアンスには v6.10.3 がインストールされている必要があります。

2. アプライアンスの準備

このガイドの前述の手順を使用して、更新するアプライアンスを準備します。以下の手順は、正常に更新し、データ損失を最小限に抑えるために重要です。

- 3. パッチ ファイルとアップデート ファイルのダウンロード
- 4. アプライアンスの設定のバックアップ
- 5. 診断パックの作成
- 6. Flow Collector と SMC データベースのバックアップ
- 7. 使用可能なディスク容量の確認

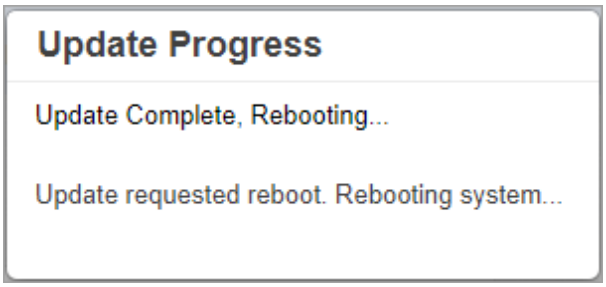
3. Pre-SWU のインストール

1. [サポート(Support)] > [更新(Update)] の順にクリックします。
2. [ファイルの選択(Choose File)] をクリックします。
3. Pre-SWU パッチファイル(patch-common-pre-7.0-jumpstart-PATCH1-01.swu)を選択します。

   SMC: スタンドアロン SMC を更新している場合は、patch-smc-pre-7.0-jumpstart-PATCH1-01.swu を選択します。

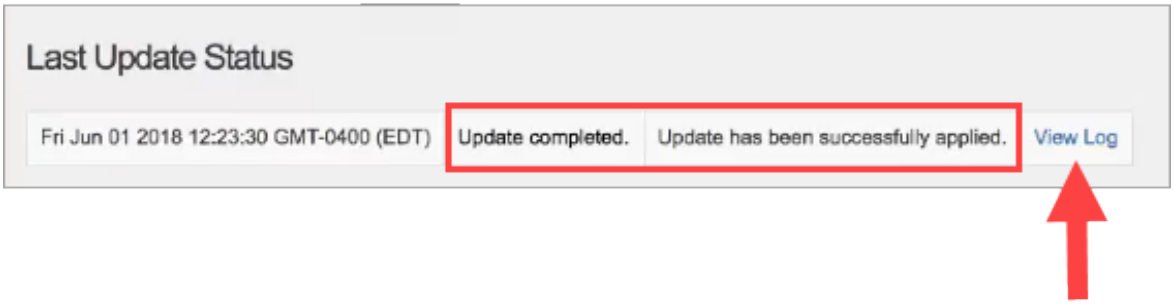
4. [自動的に実行(Automatically Execute)] チェックボックスをオンにします。
5. [アップロード(Upload)] をクリックします。画面に表示される指示に従って、インストールを開始します。

6. [更新の進捗状況(Update Progress)] に [完了(Complete)] および [再起動(Rebooting)] が表示されたら、ページを更新します。



7. 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。
8. [サポート(Support)]>[更新(Update)]の順に選択します。

   - [前回の更新ステータス(Last Update Status)]セクションで、Pre-SWU が正常に適用されたと表示されていることを確認します。[ログの表示(View Log)]をクリックして、詳細を確認します。
   - リロード: ページのロード中に問題が発生した場合は、ブラウザのキャッシュをクリアし、ブラウザを閉じて再度開いてから、もう一度ログインします。
   - ログ: [ログの表示(View Log)]をクリックします。



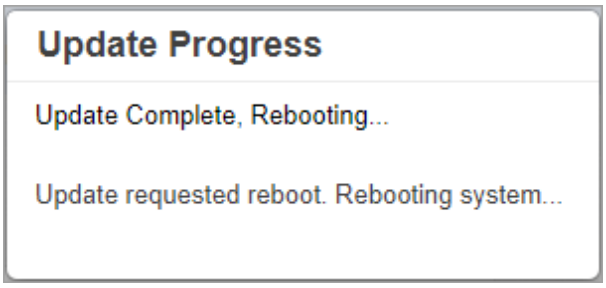
⚠ Pre-SWU のインストールが失敗した場合は、再度インストールせずに、Cisco Stealthwatch サポートに連絡してください。

4. v7.0.x SWU のインストール

1. 管理アプライアンスの [サポート(Support)]>[更新(Update)]ページを表示します。[ファイルの選択(Choose File)]をクリックします。
2. アプライアンスの v7.0.x SWU アップデートファイルを選択します。
3. [自動的に実行(Automatically Execute)]チェックボックスをオンにします。
4. [アップロード(Upload)]をクリックします。画面に表示される指示に従って操作します。

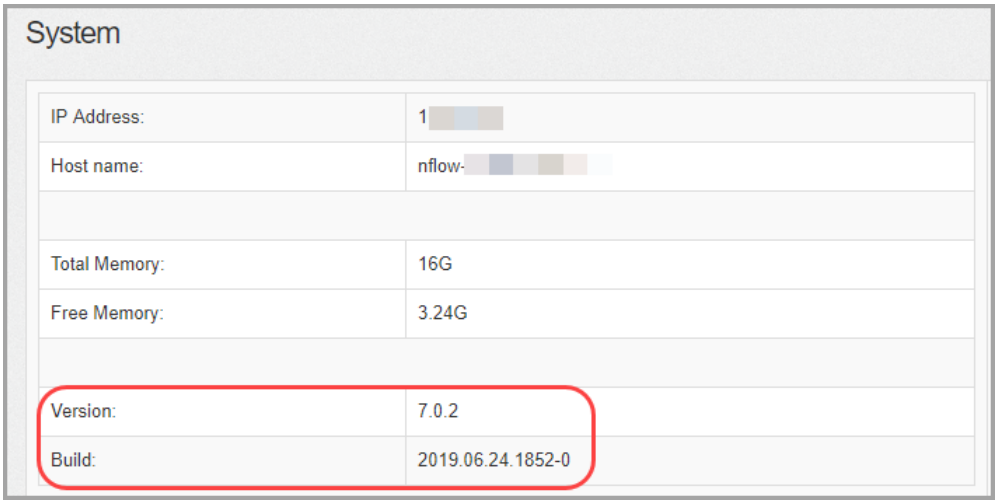
   - アップロードの進捗状況はページの下部に表示されます。
   - 安全性の確認と更新には数分かかる場合があります。

5. [更新の進捗状況(Update Progress)]に[完了(Complete)]および[再起動(Rebooting)]が表示されたら、ページを更新します。



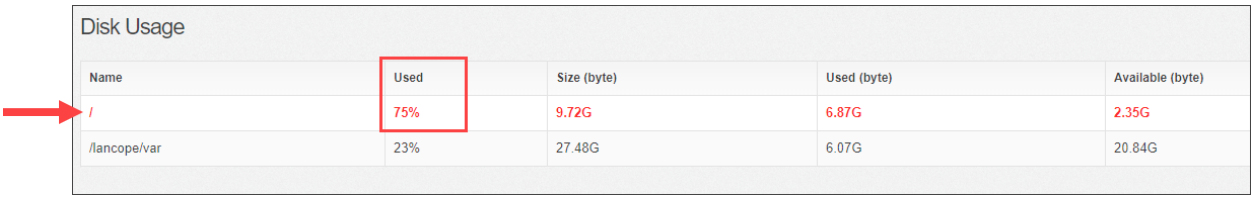
6. アプライアンス管理インターフェイスにログインします。
7. [ホーム(Home)]ページに表示されているソフトウェア バージョンを確認します。[バージョン(Version)]フィールドに v7.0.2 と表示されていることを確認します。

   - ログ: [サポート(Support)]>[更新(Update)]の順にクリックします。[ログの表示(View Log)]をクリックして、詳細を確認します。
   - リロード: ページのロード中に問題が発生した場合は、ブラウザのキャッシュをクリアし、ブラウザを閉じて再度開いてから、もう一度ログインします。



8. ルート パーティション: アプライアンスのルート パーティションを確認します。

   - [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。
   - 上の行 / を確認し、[使用済み(Used)]列のパーセンテージをチェックします。使用率が 75 % 以上の場合、このルート パーティションのデータは赤で表示されます。ルート パーティションが埋まった状態が続くと、重要な機能が停止することがあります。使用率が 100 % に近づくに従い、アプライアンスの更新を検討する必要が生じます。



5. v7.0.2 パッチのインストール

1. Stealthwatch ダウンロードおよびライセンスセンターにあるパッチの readme ファイルの指示に従って、スタンドアロンの SMC がある場合は次のパッチをインストールします。

    - SMC： patch-smc-ROLLUP003-7.0.2-02.swu

6. Central Management へのアプライアンスの追加

すべてのアプライアンスを、プライマリ SMC である Central Manager で管理されるように設定することをお勧めします。Central Management にアプライアンスを追加する必要があるかどうかを判断するには、「Central Managementにおける管理対象およびスタンドアロンの要件」を参照してください。

- **SMC 管理**：アプライアンスが Stealthwatch Central Management によって管理されている場合、Central Management を使用してアプライアンス設定の編集、ソフトウェアの更新、再起動、シャットダウンなどを管理できます。
- **スタンドアロン アプライアンス**：SMC で管理されないアプライアンスは、スタンドアロン アプライアンスと呼ばれています。スタンドアロンとして動作できるアプライアンスのリストについては、「Central Managementにおける管理対象およびスタンドアロンの要件」（Central Management の要件列）を参照してください。

> エンドポイントコネクタを除くすべてのアプライアンスは、プライマリ SMC で管理されるように設定することをお勧めします。

ベスト プラクティス

システムを正常に設定するには、『Stealthwatch Installation and Configuration Guide』の手順に従います。

推奨事項は次のとおりです。

- **1 つずつ**：一度に 1 つのアプライアンスを設定します。お使いのクラスタ内で次のアプライアンスの設定を開始する前に、アプライアンスが [稼動中（Up）] ステータスであることを確認します。
- **順序**：1 つ以上のアプライアンスを Central Management に追加する場合は、設定の順序に従います。
- **管理対象**：可能な場合はプライマリ SMC で管理されるようにアプライアンスを設定します。

- **複数の Central Manager**：システムには複数の Central Manager を設定できます。ただし、各アプライアンスは 1 つのプライマリ SMC/Central Manager のみによって管理できます。
- **アクセス**：Central Management にアクセスするための管理者権限が必要です。
- **カスタム証明書**：アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン（ルートおよび中間）をその独自の信頼ストアおよび SMC 信頼ストアに個別に保存してください。Stealthwatch のオンライン ヘルプの信頼ストアの手順を参照してください。詳細については、「開始する前に」の「カスタム証明書」の項を参照してください。

Central Managementにおける管理対象およびスタンドアロンの要件

次の表を参照して、アプライアンスを Central Management に追加する必要があるかどうかを確認します。

複数のアプライアンスを Central Management に追加する場合は、アプライアンスを順番通り設定し、各アプライアンスの詳細を確認してください。詳細については、『Stealthwatch インストールおよびコンフィギュレーションガイド』を参照してください。

順序	アプライアンス	Central Management	詳細
1.	プライマリ SMC	管理対象 (Managed)	プライマリ SMC は、Central Manager です。 システム内で次のアプライアンスの設定を開始する前に、SMC が [アップ (Up)] として表示されていることを確認します。
2.	UDP Director (別名 FlowReplicators)	管理対象 (Managed) または スタンドアロン	
3.	Flow Collector 5000 シリーズ データベース	管理対象 (Managed)	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [アップ (Up)] として表示されていることを確認します。
4.	Flow Collector 5000 シリーズ エンジン	管理対象 (Managed)	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [アップ (Up)] として表示されていることを確認します。
5.	その他のすべての Flow Collector (NetFlow および sflow)	管理対象 (Managed)	
6.	Flow Sensor	管理対象 (Managed) または スタンドアロン	フローセンサーの設定を開始する前に、フローコレクタが [アップ (Up)] として表示されていることを確認します。

7.	エンドポイント コンセントレータ	スタンドアロン	
8.	セカンダリSMC (使用する場合)	管理対象(Managed)	セカンダリ SMC の設定を開始する前に、プライマリ SMC が [アップ(Up)] として表示されていることを確認します。

Central Management へのアプライアンスの追加

1. アプライアンス設定ツールを開く: ブラウザのアドレス バーに、自分の IP アドレスに続けて `/lc-ast` を入力します。

   https://<IPaddress>/lc-ast

2. アプライアンス設定ツールを使用して、プライマリ SMC/Central Manager にアプライアンスを追加します。詳細については、アプライアンスの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] を参照してください。
3. 更新する別のスタンドアロン アプライアンスがある場合は、手順「15. スタンドアロン アプライアンスと接続解除されたアプライアンスの更新」を繰り返します。

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。
- Cisco Stealthwatch サポートのお問い合わせ先:
- 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