Cisco Stealthwatch

更新ガイド 7.2.1

目次

はじめに

概要

次の Stealthwatch アプライアンスを **v7.1.1**（または7.1.2 など、7.1.x の後継バージョン）から **v7.2.1** に更新するには、このガイドを使用します。

- UDP Director（別名 Flow Replicator）
- 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）

v7.2.1 の詳細については、『リリースノート』を参照してください。

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。アプライアンスが SMC によって管理されている場合は、集中管理インベントリに表示されます。

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。

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、および更新を計画するために必要な準備、時間、リソースについて確認してください。

ソフトウェア バージョン

アプライアンスソフトウェアをバージョン 7.2.1 に更新するには、アプライアンスにバージョン **7.1.1**（または 7.1.2 など、7.1.x の後継バージョン）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。

- **アプライアンス ソフトウェア バージョンの段階的更新**：たとえば、Stealthwatch v6.10.x を使用している場合は、各アプライアンスを v6.10.x から v7.0.x に更新した後、v7.0.x を v7.1.x に更新します。各更新ガイドは、Cisco.com で入手できます。
- **パッチ**：アップグレードする前に、ソフトウェアバージョンごとに、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。このガイドの指示に従ってください。
- **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。

VMware

Stealthwatch v7.2.x は VMware v6.5 および v6.7 との互換性があります。Stealthwatch v7.2.x では VMware v6.0 はサポートされていません。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**：Stealthwatch 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、Stealthwatch を v7.2.x にアップグレードする前に、VMware vCenter と ESXi ホストを v6.5 または v6.7 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**：Stealthwatch v7.2.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 か v6.7 であることと、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。

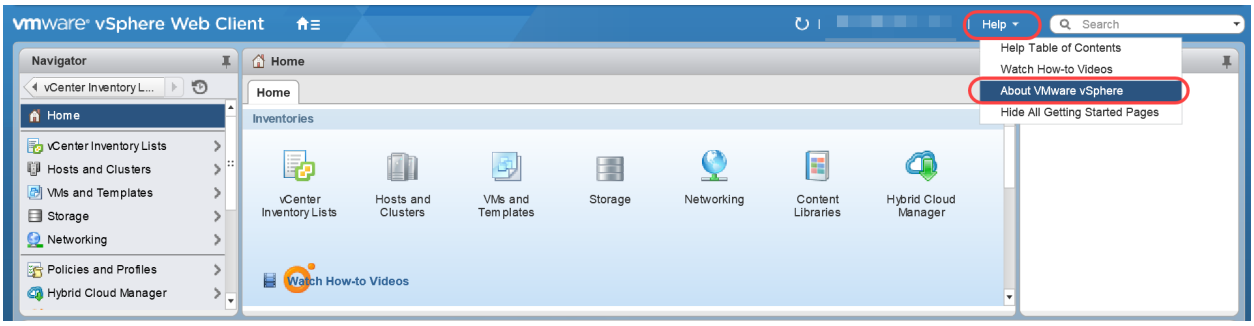
> ⚠ すでにインストールされているカスタム バージョンが上書きされるため、Stealthwatch 仮想アプライアンスに VMware ツールをインストールしないでください。インストールすると、仮想アプライアンスが動作不能になり、再インストールが必要になります。

1. VMware バージョンの確認

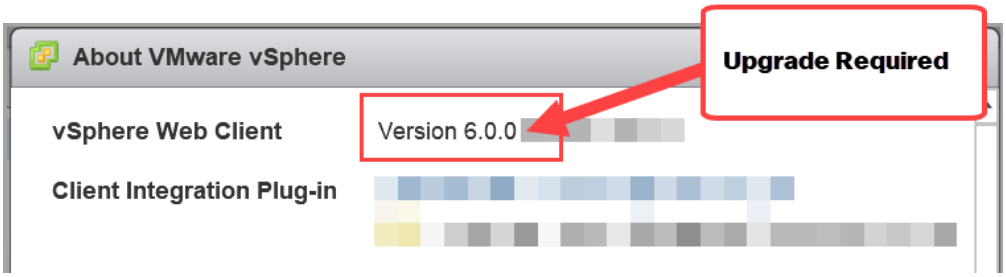
次の手順に従って、VMware vSphere vCenter v6.5 か v6.7 がインストールされていることを確認します。

> 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。バージョンが 6.0 の場合は、v6.5 か v6.7 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。



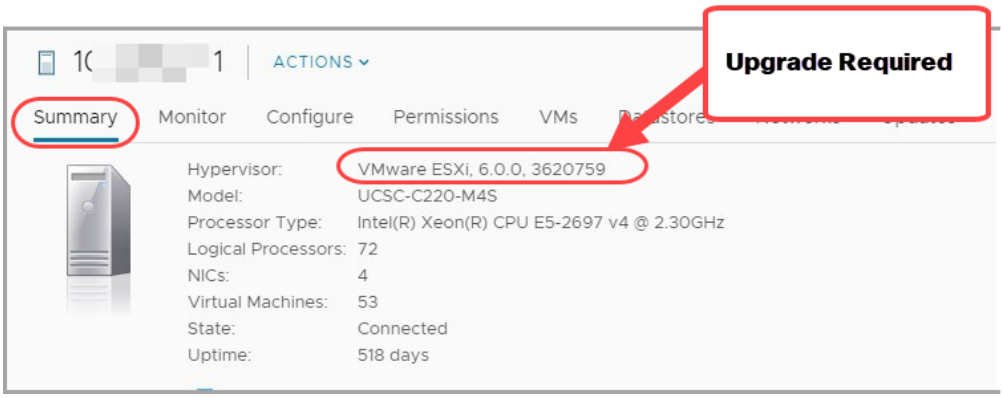
5. 次の項に進みます。

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 か v6.7 がインストールされていることを確認します。Stealthwatch 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、それぞれがオンになっ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. [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。バージョンが 6.0 の場合は、v6.5 か v6.7 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. Stealthwatch 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。

Cisco Software Central

ダウンロードおよびライセンスセンターは、Cisco Software Central に置き換えられました。ライセンスの管理、パッチのダウンロード、および Stealthwatch v7.2.x 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。

バージョン 7.1. x 以前の Stealthwatch のパッチまたはアップデートファイルにアクセスするには、https://stealthwatch.flexnetoperations.com でダウンロードおよびライセンスセンターを引き続き使用します。

TLS

Stealthwatch には TLS v1.2 が必要です。

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。
- **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、別のブラウザからアプライアンスにログインするか、アプライアンス アイデンティティ証明書をカスタム証明書に置き換えるか、または Cisco Stealthwatch サポートに連絡してください。

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。

> ⚠ Dell PowerEdge ハードウェアおよび Flow Collector 5020 は、Stealthwatch v 7.2 ではサポートされていません。ハードウェアの更新については、stealthwatch_renewals@cisco.com で Stealthwatch 更新チームにお問い合わせください。

Stealthwatch ファームウェアおよび Stealthwatch 更新ガイドを使用して、この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。

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。

- **管理対象アプライアンスの確認**: SMC にログインします。[グローバル設定(Global Settings)] アイコン > [集中管理(Central Management)] を選択します。[ライセンス ステータス(License Status)] 列を確認します。
- **スタンドアロン アプライアンスの確認**: 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)] > [ライセンス(Licensing)] を選択します。[機能ライセンスのステータス(Feature License Status)] セクションを確認します。
- **ステータスを使用できません**: v7.1.x では、セカンダリ SMC のライセンスステータスが [集中管理(Central Management)] に [ステータスを使用できません(Status Not Available)] と表示されることがあります。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、『7.1.x ダウンロードおよびライセンスガイド』を参照してください。

スマートライセンシングの準備状況チェック

v7.2 では、Cisco スマート ソフトウェア ライセンシングを使用して、Stealthwatch のアプライアンスおよび機能をライセンシングします。詳細については、cisco.com のスマートライセンシングを参照してください。

更新プロセスの一環として、Stealthwatch 管理コンソールでスマートライセンスの準備状況チェックを実行し、すべての管理対象アプライアンスのライセンスを確認します。手順については、「**4. スマートライセンスの準備状況チェックのインストール**」を参照してください。

互換性のないライセンス

準備状況チェックに失敗した場合は、クラスタ内で互換性のないライセンスが検出されています。ライセンスを再設定する必要がある場合もあれば、新しい期間のライセンシングを購入する必要がある場合もあります。Stealthwatch 更新チーム（stealthwatch_renewals@cisco.com）にご連絡ください。

更新後

スマートライセンシングの詳細については、更新後に『Stealthwatch v7.2.1 リリースノート』と『Stealthwatch Smart Software ライセンスガイド』を参照してください。

- 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、フロー収集が停止します。フロー収集を再度開始するには、製品インスタンスを登録します。
- 評価期間が満了する前に、PAK を転送してスマートライセンスに変換してください。

スタンドアロン アプライアンス

バージョン 7.2 では、スタンドアロン アプライアンスはサポートされていません。このガイドの手順に従ってアプライアンスを設定し、正常に管理および更新できるようにします。

更新の準備の一環として、ライセンス、証明書、ホスト名などを確認します。このガイドの手順に従ってください。

> ⚠ パッチをインストールしてファイルを更新する前に、手順に従ってスタンドアロン アプライアンスを [集中管理（Central Management）]に追加してください。

- **カスタム証明書**：アプライアンスにカスタム証明書がある場合、アプライアンスを [集中管理（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）をそれ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。要件と手順については、「**2. 集中管理 へのスタンドアロン アプライアンスの追加**」を参照してください。

Stealthwatch 管理コンソールが必要

クラスタ内に Stealthwatch 管理コンソールがない場合は、この更新を開始する前に Stealthwatch 管理コンソール VE をインストールします。

- 『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 v7.2』の手順に従って、Stealthwatch 管理コンソール VE をインストールします。Cisco Software Central（https://software.cisco.com）の Cisco スマートアカウントからイメージをダウンロードできます。

- Stealthwatch 管理コンソールに v7.2.1 がインストールされている場合は、「**13. エンドポイントコンセントレータと管理対象外アプライアンスの更新**」の手順に従ってアプライアンスを更新し、v7.2.1 に更新した後に、それらを [集中管理(Central Management)] に追加します。

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。

カスタム証明書を更新するには、プロバイダーの更新された証明書を要求します。

- **管理対象アプライアンスの確認**:SMC にログインします。[グローバル設定(Global Settings)] アイコン > [集中管理(Central Management)] を選択します。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。

  [ヘルプ(Help)] アイコンをクリックします。[Stealthwatch オンライン ヘルプ(Stealthwatch Online Help)] を選択します。要件と手順については、次のヘルプページを確認してください。SSL/TLS のアイデンティティと信頼ストア。

  古い証明書の削除:アプライアンス アイデンティティを置き換えた後、信頼ストアから古い証明書を削除します。アプライアンスの信頼ストア、SMC の信頼ストア、およびその他のアプライアンスの信頼ストアから古い証明書を削除してください。詳細については、信頼ストアのヘルプページのアプライアンス アイデンティティ要件の表を確認します。

  トラブルシューティング:[集中管理(Central Management)] で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)] になっている場合は、[システム設定(System Configuration)] にログインし、[集中管理(Central Management)] からアプライアンスを削除します。手順については、「**2. 集中管理 へのスタンドアロン アプライアンスの追加**」を参照してください。

> ⚠ [集中管理(Central Management)] でアプライアンス アイデンティティを置き換える場合は、新しい証明書(アイデンティティ、ルート、およびチェーン)を追加して、手順をすべて実行するまで、信頼ストアから古い証明書を削除しないでください。

- **スタンドアロン アプライアンスの更新**:手順については、「**2. 集中管理 へのスタンドアロン アプライアンスの追加**」を参照してください。要件については、「**アプライアンス アイデンティティの要件**」を参照してください。

ディスク容量

更新の準備の一環として、パッチとソフトウェア更新ファイルをインストールするための十分な空きディスク容量が各アプライアンスにあることを確認します。手順については、「**8. 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 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、フローコレクタの SWU ファイルが 6 GB の場合、フローコレクタ 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**：たとえば、それぞれ 6 GB の 4 つの SWU ファイルを SMC にアップロードする場合、SMC パーティションで少なくとも 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

- **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。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。
- **管理対象アプライアンスの確認**：SMC にログインします。[グローバル設定（Global Settings）] アイコン > [集中管理（Central Management）] を選択します。各アプライアンスの [ホスト名（Host Name）] 列を確認します。
- **スタンドアロン アプライアンスの確認**：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。
- **管理対象アプライアンスの確認**：SMC にログインします。[グローバル設定（Global Settings）] アイコン > [集中管理（Central Management）] を選択します。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。
- **スタンドアロン アプライアンスの確認**：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**：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。
- **管理対象アプライアンスの確認**：SMC にログインします。[グローバル設定（Global Settings）] アイコン > [集中管理（Central Management）] を選択します。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（NTP Server）] を確認します。
- **スタンドアロン アプライアンスの確認**：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

すべての Stealthwatch アプライアンスは協定世界時（UTC）を使用します。

- **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。
- **仮想ホストサーバ**：仮想ホストサーバが、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。

> ⚠ （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。

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**：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 ロック セキュリティ イベントの変換

v7.2 では、Stealthwatch はホスト ロック セキュリティ イベントを使用しなくなりました。v7.2 にアップグレードすると、ホスト ロック セキュリティ イベントに関連するすべての既存のホストロックルールおよび管理ルールが、カスタム セキュリティ イベントと同等のものに変換されます。

ホストロックイベントを確認し、関連のないものはアップグレード前に削除してください。詳細については、『Release Notes v7.2.1』を参照してください。

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
- フローコレクタ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。

フローコレクタデータベースのバックアップ

フローコレクタデータベースをバックアップする手順には、データベースのトリミングと、バックアップ終了後のスナップショットの削除が含まれます。詳細については、「**7. フローコレクタと SMC データベースのバックアップ**」を参照してください。

> ⚠ 手順に従って、データベースのバックアップのすべての手順を実行してください。サポートが必要な場合は、Cisco Stealthwatch サポートに連絡してください。

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

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、「**3. 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**：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、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。

> ⚠ 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

更新プロセスの実行時は、SMC とアプライアンス間の通信が停止し、更新およびリブートが行われます。

[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。詳細については、「**管理対象アプライアンスでの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。

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 Hardware Installation Guide』を参照してください。https://www.cisco.com/c/ja_jp/support/security/stealthwatch/products-installation-guides-list.html
- CIMC（UCS アプライアンス）：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の最新のシスコガイドを参照してください。

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）：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。
    - たとえば **KVM** については仮想マネージャのマニュアルを参照してください。
    - **VMware** については、VSphere の VCenter サーバ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（セキュアシェル）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。

集中管理での SSH の有効化

このセクションは、SSH（セキュア シェル）を使用してアプライアンスにアクセスできるかどうかを制御する場合に使用します。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、アプライアンスで一時的に SSH を有効にできます。

SSH を開く

次の手順に従って、選択したアプライアンスの SSH を開きます。

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。

SSH の有効化

1. [SSH] セクションを見つけます。
2. 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。
3. [設定の適用(Apply settings)] をクリックします。
4. 画面に表示される指示に従って操作します。

> ⚠ 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。

アプライアンス管理インターフェイスでの SSH の有効化

次の手順に従って、選択したアプライアンスの SSH をアプライアンス管理インターフェイスを使用して開きます。

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)] > [サービス(Services)] の順にクリックします。
3. [SSHの有効化(Enable SSH)] チェックボックスをオンにして SSH へのアクセスを許可します。
4. ルートへのアクセスも許可するには、[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。
5. [適用(Apply)] をクリックします。

> ⚠ 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。

更新の概要

> ⚠ 各 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. クラスタを確認します。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、スタンドアロン アプライアンスを確認します。
2. 集中管理 へのスタンドアロン アプライアンスの追加
3. パッチファイルと更新ファイルのダウンロード
4. スマートライセンスの準備状況チェックのインストール
5. アプライアンス設定のバックアップ
6. 診断パックの作成
7. フローコレクタと SMC データベースのバックアップ
8. 使用可能なディスク容量の確認
9. パッチのインストール
10. v7.2.1 ソフトウェアアップデートをインストールします。Central Management を使用して、各管理対象アプライアンスを更新します。必ず、更新順序を使用して、v7.2.1 SWU をインストールしてください 。
11. Stealthwatch デスクトップ クライアント のインストール
12. SMC フェールオーバー ロールの確認
13. エンドポイントコンセントレータと管理対象外アプライアンスを更新します。管理対象アプライアンスを更新した後で、エンドポイントコンセントレータを更新し、[集中管理(Central Management)] に追加します。更新前に [集中管理(Central Management)] に追加されていないスタンドアロン アプライアンスがある場合は、次の手順に従ってアプライアンスを更新し、[集中管理(Central Management)] に追加します。

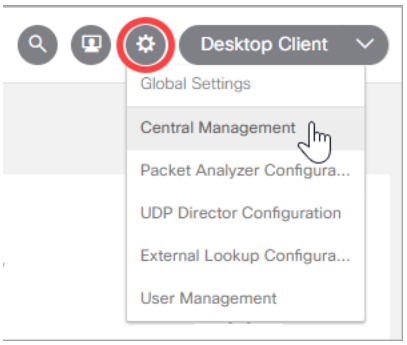
1. クラスタの確認

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、スタンドアロン アプライアンスを確認します。

1. 管理者として Stealthwatch 管理コンソールにログインします。

   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。



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

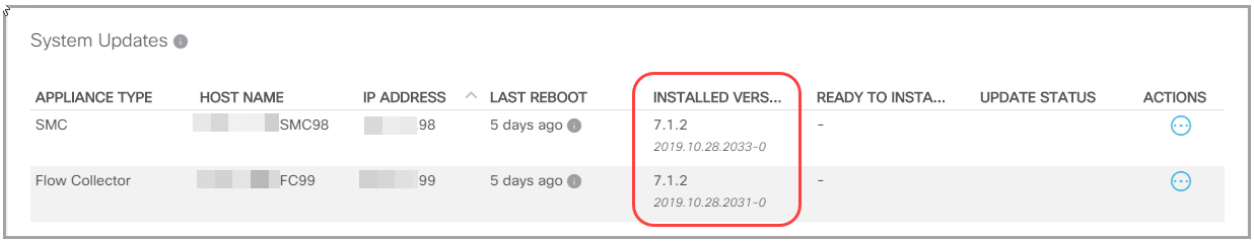
各アプライアンスの現在のソフトウェアバージョンが **v7.1.1**(または 7.1.x の後続バージョン)であることを確認するには、次の手順を実行します。

1. [マネージャの更新(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。
2. [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 v7.1.1(または 7.1.x の後継バージョン)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 v7.1.2 がインストールされている場合は、クラスタ内の他のアプライアンスに 7.1.2 がインストールされている必要があります。

   7.0.x 以前:ソフトウェアバージョンが 7.0.x 以前の場合は、この更新を開始する前に、アプライアンスを 7.1.x に更新します。『Stealthwatch System 更新ガイド』を参照してください。

   Stealthwatch 管理コンソール:Stealthwatch 管理コンソールに **v7.2.1 がインストールされている場合**は、「**13. エンドポイントコンセントレータと管理対象外アプライアンスの更新**」の手順に従ってアプライアンスを更新し、v7.2.1 に更新した後に、それらを [集中管理(Central Management)] に追加します。

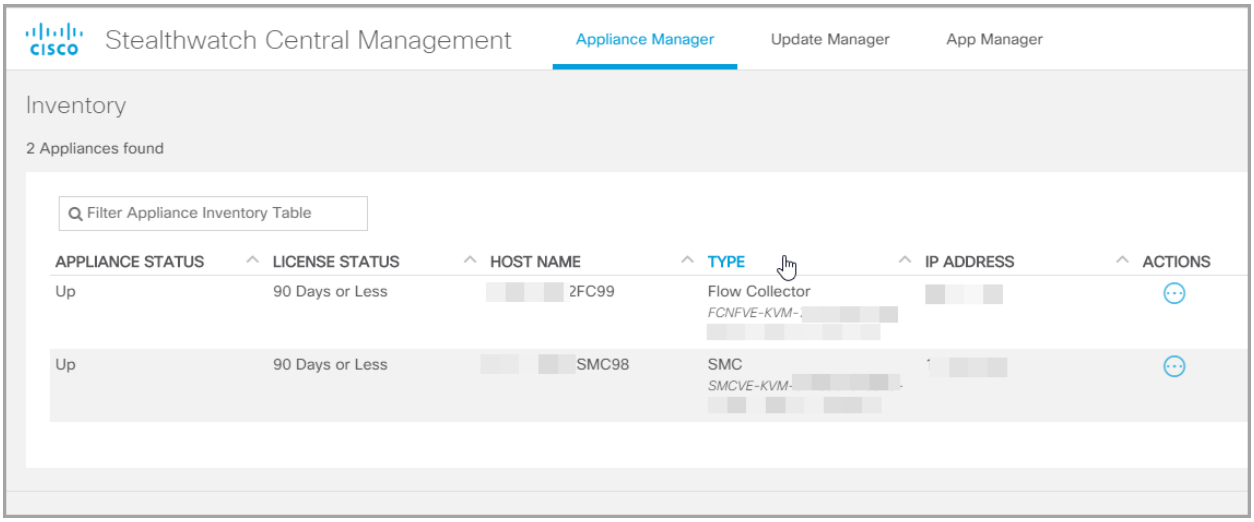


すべてのアプライアンスに正しいソフトウェア バージョンがインストールされていることを確認します。これは、更新を成功させるために不可欠な手順です。

管理対象アプライアンスとスタンドアロン アプライアンスの確認

1. [アプライアンス マネージャ(Appliance Manager)] タブを選択し、インベントリを確認します。

   - **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。[集中管理(Central Management)] に表示されていないアプライアンスがある場合は、「**2. 集中管理 へのスタンドアロン アプライアンスの追加**」の手順を実行します。
   - **管理対象アプライアンス**: すべての Stealthwatch アプライアンスが [集中管理(Central Management)] のインベントリに表示されていて、スタンドアロン アプライアンスがないことを確認した場合は、「**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**」に進みます。



2. 集中管理 へのスタンドアロン アプライアンスの追加

スタンドアロン アプライアンス（フローセンサー、UDP Director など）がある場合は、次の手順に従って、それらのアプライアンスを次の情報を含めて［集中管理（Central Management）］に追加します。

- **ソフトウェアバージョン**：［集中管理（Central Management）］に追加する前に、アプライアンスに Stealthwatch v7.1.1（または 7.1.x の後継バージョン）がインストールされていることを確認します。
- **Stealthwatch 管理コンソール v7.2.1**：プライマリ Stealthwatch 管理コンソールに v7.2.1 がすでにインストールされていて、v7.1.x を搭載したスタンドアロン アプライアンスがある場合は、「**13. エンドポイントコンセントレータと管理対象外アプライアンスの更新**」に進み、スタンドアロン アプライアンスを更新します。
- **ライセンス**：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。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）］>［ライセンス（Licensing）］を選択します。［機能ライセンスのステータス（Feature License Status）］セクションを確認します。詳細については、「**ライセンス**」を参照してください。
- **ホスト名**：アプライアンスごとに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。

  ホスト名を確認するには、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**：アプライアンスごとに完全修飾ドメイン名が必要です。ドメイン名を確認するには、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。
- **カスタム証明書**：スタンドアロン アプライアンスにカスタム証明書がある場合は、アプライアンスを［集中管理（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（ルートと中間）をその独自の信頼ストアと SMC 信頼ストアに個別に保存します。

> **エンドポイントコンセントレータ**がある場合は、管理対象アプライアンスを更新した後にそのコンセントレータを更新して［集中管理（Central Management）］に追加します。次の情報を参照してください。**13. エンドポイントコンセントレータと管理対象外アプライアンスの更新**」を参照してください。

1. 信頼ストアへのカスタム証明書の追加

スタンドアロン アプライアンスにカスタム証明書がある場合は、アプライアンスを [集中管理 (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 (ルートと中間) をその独自の信頼ストアと SMC 信頼ストアに個別に保存します。

> **アプライアンスにカスタム証明書がない場合**は、この手順をスキップできます。「**2. 集中管理へのアプライアンスの追加**」に進みます。

アプライアンス アイデンティティの要件

	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。

アプライアンスのアイデンティティ証明書の確認

更新プロセスを開始する前に、証明書が有効であり、最新のものであることを確認します。

1. 管理者としてアプライアンス管理インターフェイス (https://<IPaddress>) にログインします。
2. [設定 (Configuration)] > [SSL証明書 (SSL Certificate)] を選択します。
3. [SSL サーバ ID (SSL Server Identity)] セクションを確認します。
   - アプライアンスのすべてのアイデンティティ証明書が表示されていることを確認します。
   - 証明書がアプライアンスのアイデンティティ要件を満たしていることを確認します。
   - 証明書の有効期限が切れていないことを確認します。
4. カスタム証明書がアプライアンスのアイデンティティ要件を満たしていない場合、または期限切れになっている場合は、認証局からの更新された証明書を要求します。詳細については、『Creating and Installing SSL Certificates Guide』を参照してください。
5. アプライアンス アイデンティティを置き換えたら、古いアプライアンス アイデンティティ証明書を削除します。アプライアンスの信頼ストア、SMC の信頼ストア、およびその他のアプライアンスの信頼ストアから古い証明書を削除してください。

> ⚠ アプライアンス アイデンティティを置き換える場合は、新しい証明書 (アイデンティティ、ルート、およびチェーン) を追加して、手順をすべて実行するまで、古い証明書を削除しないでください。

アプライアンスのアイデンティティ証明書のダウンロード

この更新を開始する前に、カスタム証明書が保存されていることを確認します。証明書がすでに保存されている場合は、「**アプライアンス信頼ストアへの証明書の追加**」に進みます。

1. ブラウザのアドレスバーで、IP アドレスの後のパスを **/secrets/v1/server-identity** に置き換えます。

   例：https://<IPaddress>/secrets/v1/server-identity

2. 画面に表示される指示に従って証明書を保存します。

   オープン：ファイルを表示するには、テキストファイル形式を選択します。

   トラブルシューティング：証明書をダウンロードするためのプロンプトが表示されない場合は、自動的にダウンロードされている場合があるため、[ダウンロード（Downloads）] フォルダを確認するか、または別のブラウザを試します。

アプライアンス信頼ストアへの証明書の追加

アプライアンスの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に個別に保存します。

1. アプライアンス管理インターフェイスで、[設定（Configuration）] > [認証局証明書（Certificate Authority Certificates）] を選択します。
2. [ファイルの選択（Choose File）] をクリックします。証明書を選択します。
3. [名前（Name）] フィールドに証明書名を入力します。
4. [証明書の追加（Add Certificate）] をクリックします。

> ⚠ 各証明書とチェーン（ルートおよび中間）証明書を個別にアップロードしていることを確認します。

5. [送信（Submit）] をクリックします。
6. 手順 2 ～ 5 を繰り返して、必要なすべての証明書をアプライアンスの信頼ストアに追加します。
7. 必要なすべての新しい証明書をアプライアンスの信頼ストアに追加したら、古いまたは期限切れの証明書を信頼ストアから削除します。

SMC 信頼ストアへの証明書の追加

アイデンティティ証明書と証明書チェーン（ルートと中間）を SMC 信頼ストアに個別に保存します。

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。[集中管理（Central Management）] を選択します。
3. [アプライアンス マネージャ（Appliance Manager）] ページで、SMC の [アクション（Actions）] メニューをクリックします。
4. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。

5. [Appliance Manager] > [全般(General)] タブで、[信頼ストア(Trust Store)] セクションを見つけます。
6. [新規追加(Add New)] をクリックします。

> ⚠ 各証明書とチェーン(ルートおよび中間)証明書を個別にアップロードしていることを確認します。

7. [フレンドリ名(Friendly Name)] フィールドに、証明書の名前を入力します。
8. [ファイルの選択(Choose File)] をクリックします。証明書を選択します。
9. [証明書の追加(Add Certificate)] をクリックします。[信頼ストア(Trust Store)] リストに証明書が表示されていることを確認します。
10. 手順 6 ～ 9 を繰り返して、他の必要な証明書を信頼ストアに追加します。
11. [設定の適用(Apply settings)] 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。
12. [アップ(Up)]:[アプライアンス マネージャ(Appliance Manager)] ページで、SMC が設定変更を終了し、アプライアンスのステータスが [アップ(Up)] に戻っていることを確認します。
13. 必要なすべての新しい証明書をアプライアンスの信頼ストアに追加したら、古いまたは期限切れの証明書を SMC の信頼ストアから削除します。

> ⚠ アプライアンスの信頼ストア、SMC の信頼ストア、およびその他のアプライアンスの信頼ストアから古い証明書を削除してください。

2. 集中管理へのアプライアンスの追加

アプライアンス セットアップ ツールを使用して、スタンドアロン アプライアンスを [集中管理(Central Management)] に追加します。

> ℹ この手順には、v7.1.x の Stealthwatch 管理コンソールが必要です。Stealthwatch 管理コンソールがない場合、詳細については、「**Stealthwatch 管理コンソールが必要**」を参照してください。

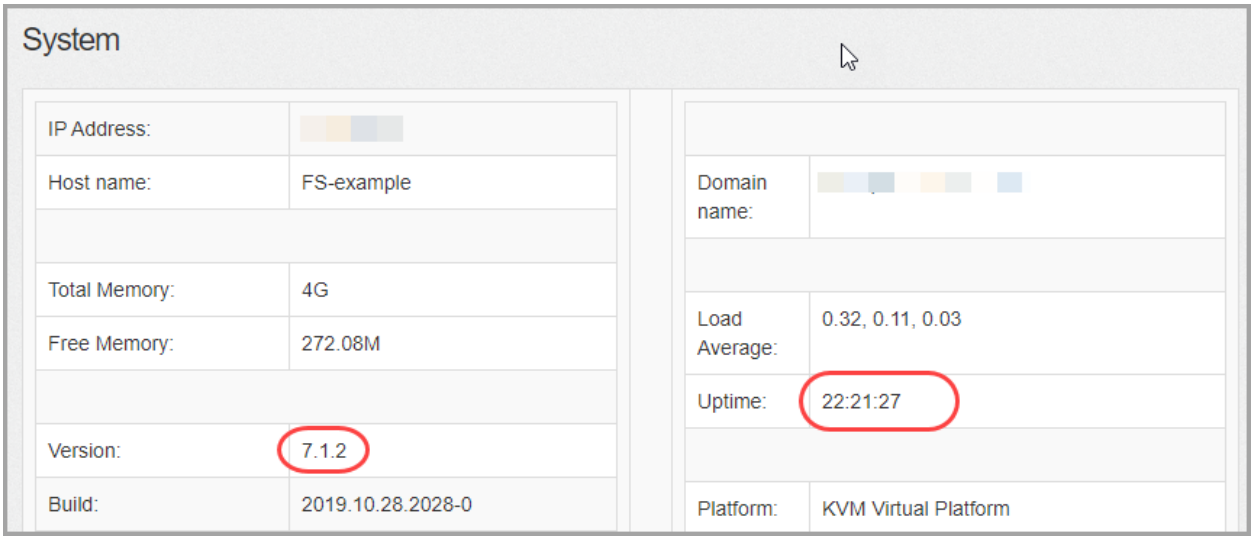
システムを正常に設定するには、次の点に注意してください。

- [集中管理(Central Management)]:SMC IP アドレス、SMC パスワード、および Stealthwatch ドメインが必要です。
- **1 つずつ**:一度に 1 つのアプライアンスを設定します。別のアプライアンスでアプライアンス セットアップ ツールを開く前に、アプライアンスのステータスに [アップ(Up)] と表示されていることを確認します。

> ⚠ アプライアンスにカスタム証明書がある場合は、アプライアンスを [集中管理(Central Management)] に追加する前に、「**1. 信頼ストアへのカスタム証明書の追加**」の手順を実行します。

1. 管理者としてアプライアンス管理インターフェイス（https://<IPaddress>）にログインします。
2. [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。アプライアンスに **v7.1.1**（または 7.1.x の後継バージョン）がインストールされていることを確認します。

   7.0.x 以前：ソフトウェアバージョンが 7.0.x 以前の場合は、[集中管理（Central Management）] に追加する前に、『Stealthwatch 更新ガイド』を使用して アプライアンスを 7.1.x に更新します。



3. [稼働時間（Uptime）] がアクティブであり、表示されていることを確認します。
4. **アプライアンスセットアップツールを開く**：ブラウザのアドレスバーで、IP アドレスの後の URL の末尾を /lc-ast に置き換えます。

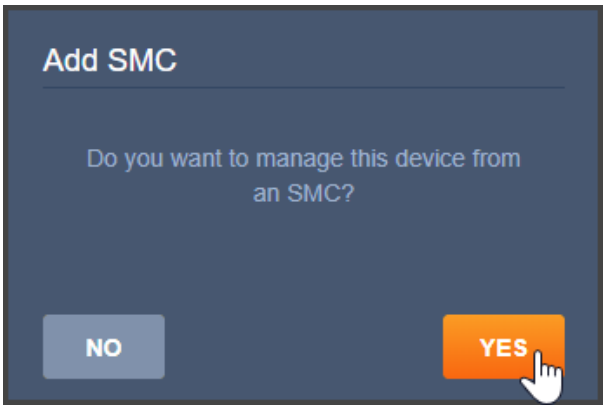
   https://<IPaddress>/lc-ast

5. [続行（Continue）] または [次へ（Next）] をクリックして、アプライアンス設定をスクロールします。詳細については、『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 v7.1.x』を参照してください。

> ⚠ IP アドレス、ホスト名、またはネットワークドメイン名を変更すると、アプライアンスのアイデンティティ証明書が自動的に置き換えられます。カスタム証明書がある場合は、これらのフィールドを変更する前に証明書と秘密キーを保存し、データが失われないようにします。

6. アプライアンスを [集中管理（Central Management）] に追加するには、[SMC の追加（Add SMC）] ダイアログボックスの画面に表示される指示に従うか、または [集中管理（Central Management）] タブを選択します。

   [SMC の追加（Add SMC）] ダイアログボックス：[集中管理（Central Management）] タブで、[はい（Yes）] を選択して SMC からアプライアンスを管理します。



[集中管理(Central Management)] タブ:SMC の IP アドレスを入力します。Stealthwatch ドメインを選択します。

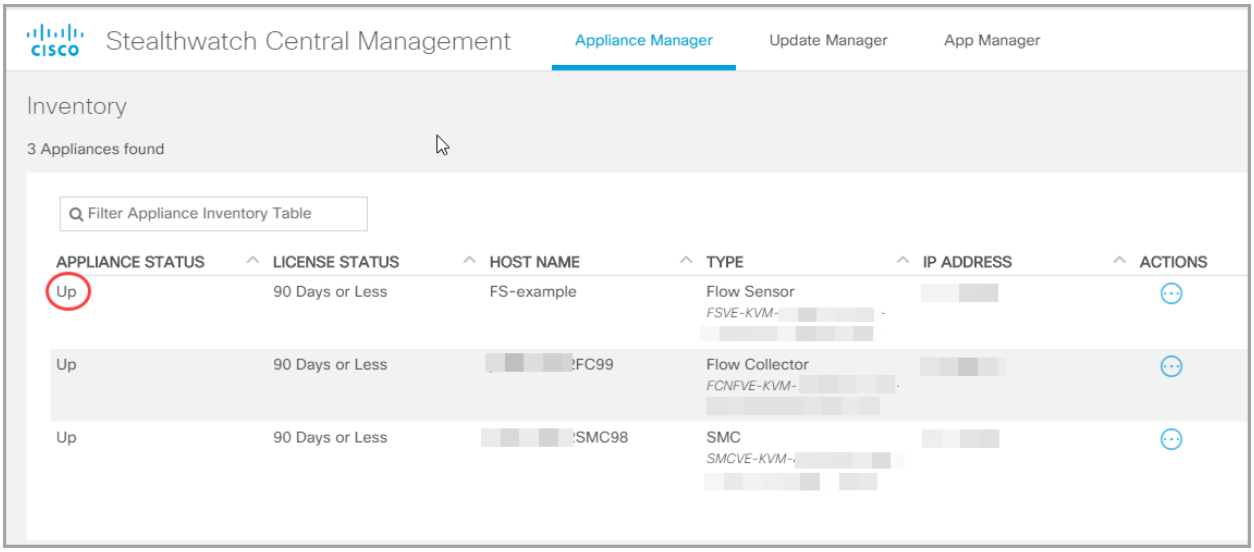
> フィールドに SMC の IP アドレスを入力できない場合は、キャッシュをクリアするか、ブラウザを変更します。

7. 画面に表示される指示に従って、SMC 証明書を信頼し、SMC との通信を許可します。
   - SMC ログイン クレデンシャルを入力します。
   - Stealthwatch ドメインを選択します。

> 画面に表示される指示は、アプライアンスによって異なる場合があります。たとえば、フローセンサーを設定する場合は、フローコレクタを選択します。

8. アプライアンスの再起動中は、画面に表示される指示に従います。新しいシステム設定が有効になるまで数分待ちます。
9. **Stealthwatch 管理コンソール**にログインします。[グローバル設定(Global Settings)] アイコン > [集中管理(Central Management)] をクリックします。[集中管理(Central Management)] のインベントリを確認します。
   - アプライアンスがインベントリに表示されていることを確認します。
   - アプライアンスのステータスが [アップ(Up)] として表示されていることを確認します。

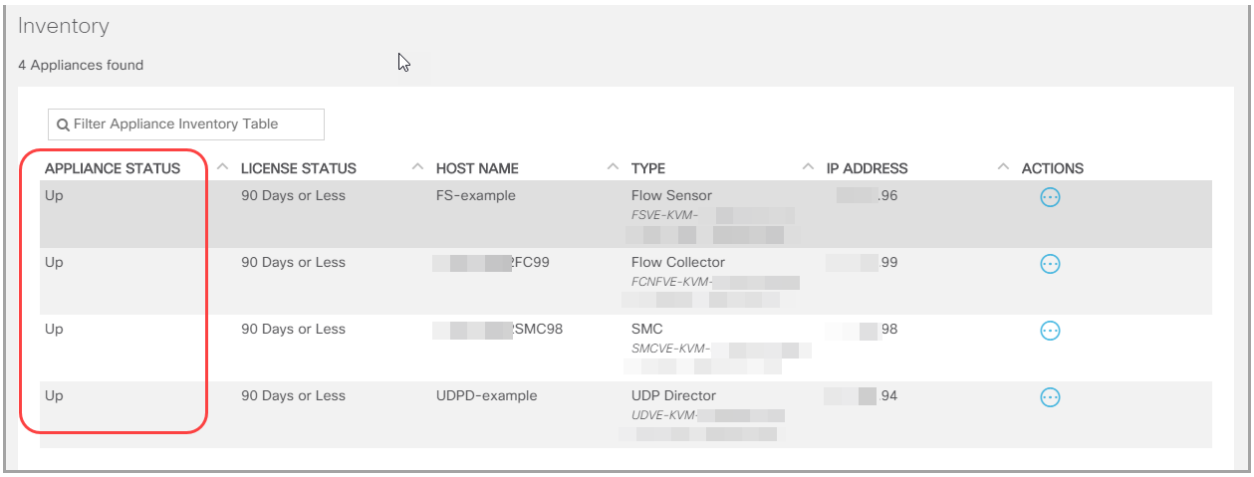
[アプライアンスのステータス(Appliance Status)] が [アップ(Up)] と表示されていることを確認する



> 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)] から [アップ(Up)] に変わります。続行する前に、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てください。

10. すべてのスタンドアロン フロー センサーと UDP Director を [集中管理(Central Management)] に追加するまで、「**2. 集中管理 へのスタンドアロン アプライアンスの追加**」の手順を繰り返します。
11. すべてのアプライアンス(SMC、フローコレクタ、フローセンサー、および UDP Director)が [集中管理(Central Management)] のインベントリに表示されていることを確認します。

    - [アップ(Up)]: すべてのアプライアンスが [アップ(Up)] として表示されていることを確認します。
    - **エンドポイントコンセントレータ**: エンドポイント コンセントレータがある場合は、管理対象アプライアンスを更新した後にそのコンセントレータを更新して [集中管理(Central Management)] に追加します。詳細については、「**13. エンドポイント コンセントレータと管理対象外アプライアンスの更新**」を参照してください。



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。v7.2.1 の更新が完了した後、エンドポイントのコンセントレータと残りの管理対象外のアプライアンスを集中管理に追加できます。

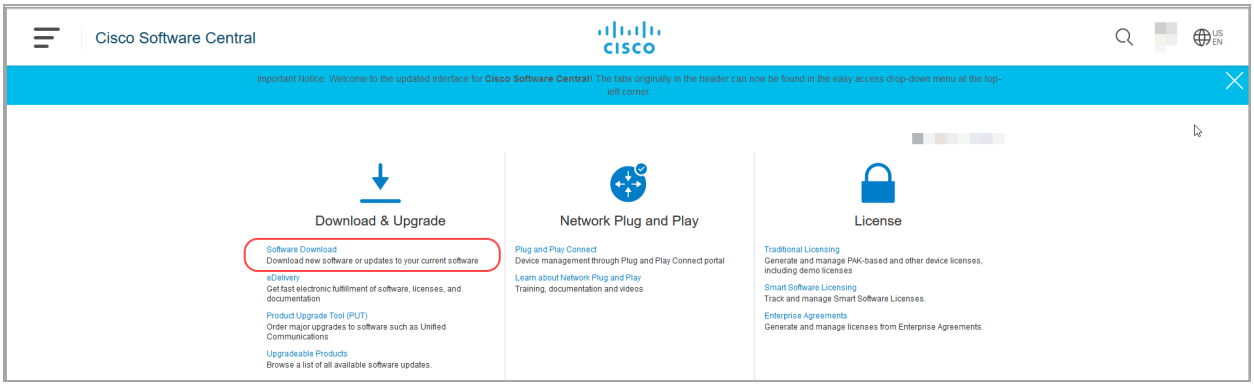
3. パッチ ファイルとアップデート ファイルのダウンロード

ライセンスを管理するには、パッチをダウンロードし、Stealthwatch v7.2 用の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 v7.2.1 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）］セクションで、［ソフトウェアのダウンロード（Software Download）］を選択します。

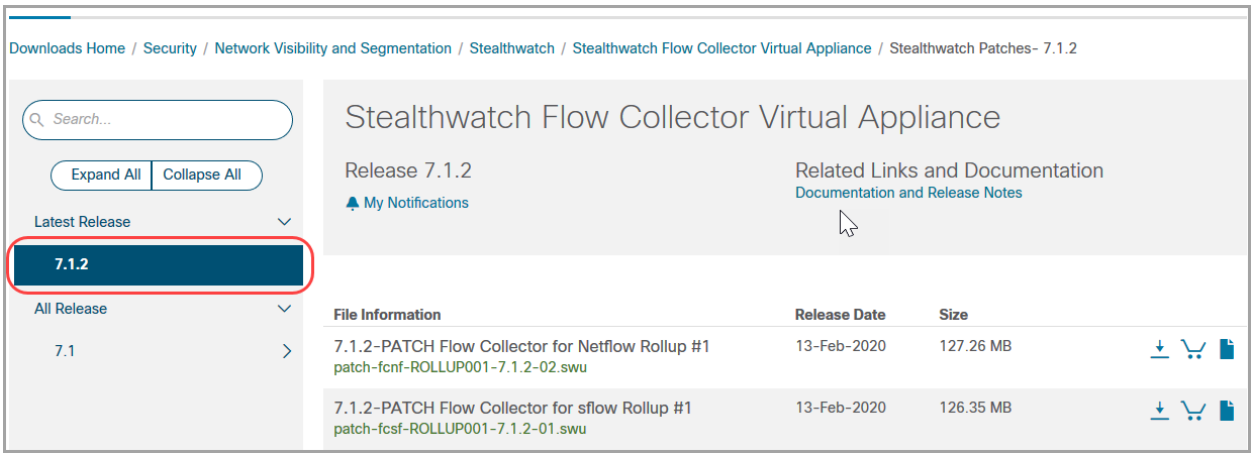


3. ［製品の選択（Select a Product）］フィールドが表示されるまで下にスクロールします。
4. Stealthwatch パッチにアクセスし、ファイルを更新するには、次の 2 つの方法があります。

   - **名前で検索**：［製品の選択（Select a Product）］フィールドに **Stealthwatch** と入力します。Enter を押します。
   - **メニューで検索**：［すべてを参照（Browse All）］をクリックします。［セキュリティ（Security）］>［ネットワークの可視性とセグメンテーション（Network Visibility and Segmentation）］>［Stealthwatch］の順に選択します。

2. パッチのダウンロード

1. [Stealthwatch] メニューから、アプライアンスモデルを選択します。
2. [ソフトウェアタイプの選択(Select a Software Type)] の下にある [Stealthwatch パッチ(Stealthwatch Patches)] を選択します。
3. [最新リリース(Latest Release)] 列で、アプライアンスにインストールされている現在のソフトウェアバージョンを選択します。たとえば、アプライアンスに 7.1.2 がインストールされている場合は、[7.1.2] を選択します。



4. **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、すべてのアプライアンスに適用する共通パッチが表示される場合があります。必ずすべてのパッチをダウンロードしてください。

5. 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。

3. 更新ファイルのダウンロード

1. [Stealthwatch] メニューに戻ります。アプライアンスタイプとアプライアンスモデルを選択します。

   SMC VE：Stealthwatch 管理コンソール仮想アプライアンス（VE）がある場合は、最初にそれを選択します。これは、更新のためにファイルにアクセスするのに最も効率的な方法です。

2. [ソフトウェアタイプの選択（Select a Software Type）] の下にある [Stealthwatch アップグレード（Stealthwatch Upgrades）] を選択します。
3. [最新リリース（Latest Release）] 列で、[7.2.1] を選択します。
4. **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、他のすべての Stealthwatch 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。

5. 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

アプライアンス	ファイル名
スマートライセンシングの準備状況チェック （SMC で実行され、すべての管理対象アプライアンスを確認する）	patch-smc-SmartLicensingReadinessCheck-04.swu
UDP Director （別名 Flow Replicator） UDP Director VE （別名 Flow Replicator VE）	update-udpd-7.2.1.2020.05.15.2357-01.swu
Flow Collector 5000 シリーズ データベース	update-fcdb-7.2.1.2020.05.15.2359-02.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-7.2.1.2020.05.15.2359-02.swu
sFlow 向けフローコレクタ sFlow VE 向けフローコレクタ	update-fcsf-7.2.1.2020.05.15.2359-02.swu
エンドポイントコンセントレータ	update-ec-7.2.1.2020.05.15.2356-01.swu
SMC および SMC VE	update-smc-7.2.1.2020.05.16.0002-02.swu
フローセンサーアプライアンス Flow Sensor VE	update-fsuf-7.2.1.2020.05.15.2357-01.swu

4. スマートライセンスの準備状況チェックのインストール

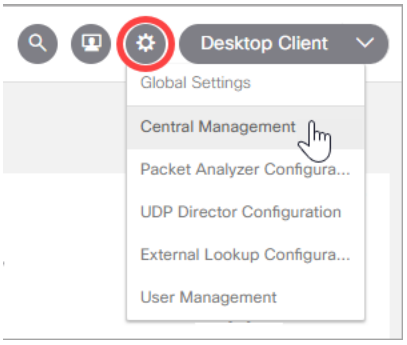
Stealthwatch 管理コンソールでスマートライセンスの準備状況チェックを実行します。管理対象アプライアンスで互換性のないライセンスが検出された場合は、アップグレードを行う前にライセンスを更新する必要があります。スマートライセンスの準備状況チェックをダウンロードするには、「**3. パッチ ファイルとアップデート ファイルのダウンロード**」で詳細を参照してください。

1. マネージャの更新を開

1. SMC にログインします。

   ブラウザのアドレスフィールドに、https://とアプライアンスの IP アドレスを入力します。Enter を押します。

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. [マネージャの更新(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。

2. スマートライセンスの準備状況チェックのインストール

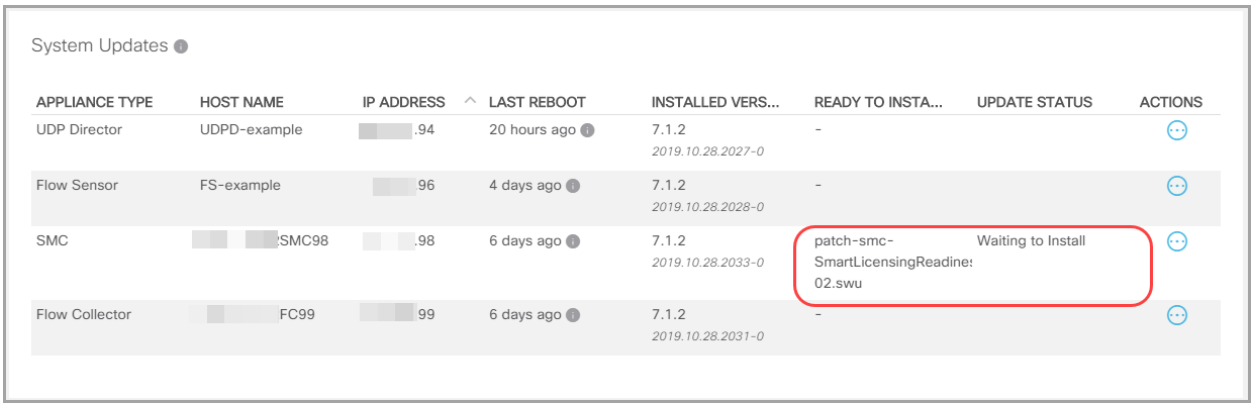
1. [システムの更新(System Updates)] セクションで、[インストールされているバージョン(Installed Version)] 列を確認します。

   - 各アプライアンスに **v7.1.1**(または最新バージョンの 7.1.x)がインストールされていることを確認します。
   - 詳細については、「**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**」を参照してください。

2. [アップロード(Upload)] をクリックします。
3. [スマートライセンスの準備状況チェック(Smart Licensing Readiness Check)] を選択します。

4. [マネージャの更新(Update Manager)]>[システムの更新(System Updates)]セクションで、[Stealthwatch 管理コンソール(Stealthwatch Management Console)]の次の列を確認して、更新の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)]:スマートライセンスの準備状況チェックファイルが SMC に表示されていることを確認します。
   - [更新ステータス(Update Status)]:[インストールを待機中(Waiting to Install)]

> ⚠ 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。



5. SMC の[アクション(Actions)]メニューをクリックします。
6. [更新のインストール(Install Update)]を選択します。
7. 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。

3. 結果の確認

1. SMC の[更新ステータス(Update Status)]を確認します。

[正常にインストールされました(Install Successful)]:準備状況チェックで問題がなかった場合は、[更新ステータス(Update Status)]は空白になります。

- ログでステータスを確認するには、SMCで[アクション(SMC Actions)]メニュー>[更新ログの表示(View Update log)]をクリックします。[スマートライセンスの準備状況チェック(Smart Licensing Readiness Check)](ログ #42)までスクロールして、要件が満たされていることを確認します。
- 要件が満たされている場合は、準備と更新のプロセスを開始する準備が整っています。「**5. アプライアンス設定のバックアップ**」に進みます。

System Updates

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERS...	READY TO INSTA...	UPDATE STATUS	ACTIONS
UDP Director	UDPD-example	.94	15 minutes ago	7.1.2 2019.10.28.2027-0	-		
Flow Sensor	FS-example	.96	3 days ago	7.1.2 2019.10.28.2028-0	-		
SMC	SMC98	.98	5 days ago	7.1.2 2019.10.28.2033-0	-		
Flow Collector	FC99	.99	5 days ago	7.1.2 2019.10.28.2031-0	-		

```
*** Normal exit status.
*** Running [./EXEC/42-SMART-LICENSING-READINESS-CHECK]
Command produced the following output on stdout:
>Executing 42-SMART-LICENSING-READINESS-CHECK with arg: /lancope/var/admin/upgrade/extract/patch-smc-SmartLicensingReadinessCheck-04/swu.ini
>Performing Smart Licensing Readiness Checks: Running Smart Licensing Readiness Check
>LICENSING CHECK: Requirements for Smart Licensing Readiness satisfied.
>
```

[インストールに失敗しました（Installation Failed）]：準備状況チェックが失敗した場合は、[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）] と表示されます。次のステップに進みます。

System Updates

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERS...	READY TO INSTA...	UPDATE STATUS	ACTIONS
UDP Director	UDPD-example	.94	20 hours ago	7.1.2 2019.10.28.2027-0	-		
Flow Sensor	FS-example	96	4 days ago	7.1.2 2019.10.28.2028-0	-		
SMC	SMC98	.98	6 days ago	7.1.2 2019.10.28.2033-0	patch-smc-SmartLicensingReadiness 02.swu	Install Failed	
Flow Collector	FC99	99	6 days ago	7.1.2 2019.10.28.2031-0	-		

2. スマートライセンスの準備状況チェックで障害が表示された場合は、SMC で [アクション (Actions)] メニュー > [更新ログの表示 (View Update Log)] をクリックします。
3. [スマートライセンス準備状況チェック (Smart Licensing Readiness Check)] (ログ #42) までスクロールして詳細を確認します。

   準備状況チェックに失敗した場合は、クラスタ内で互換性のないライセンスが検出されています。ライセンスを再設定する必要がある場合もあれば、新しい期間のライセンシングを購入する必要がある場合もあります。Stealthwatch 更新チームに stealthwatch_renewals@cisco.com からお問い合わせください。

```
We cannot update this cluster. Please contact the Stealthwatch Renewals team (stealthwatch_renewals@cisco.com) for licensing assistance.

We found the following permanent licenses installed:

Appliance Type                  | Serial Number                                  | Name    | IP Address | License Name
=================================================================================================================================
FlowCollector for NetFlow       | FCNFVE-KVM-[redacted]                          | [redacted] | [redacted] | FCNFVE
---------------------------------------------------------------------------------------------------------------------------------
FlowSensor                      | FSVE-KVM-[redacted]                            | [redacted] | [redacted] | FSVE
---------------------------------------------------------------------------------------------------------------------------------
StealthWatch Management Console | SMCVE-KVM-[redacted]                           | [redacted] | [redacted] | SMCVE
                                |                                                |         |            | FPS1000
                                |                                                |         |            | FPS100
---------------------------------------------------------------------------------------------------------------------------------
StealthWatch Management Console | SMCVE-KVM-[redacted]                           | [redacted] | [redacted] | SMCVE
                                |                                                |         |            | FPS1000
                                |                                                |         |            | FPS100
```

5. アプライアンス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。

バックアップ設定ファイルの作成

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 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 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。

   SMC/Central Manager: プライマリ SMC/Central Manager をバックアップすると、SMC のバックアップ コンフィギュレーション ファイルと集中管理のバックアップ コンフィギュレーション ファイルが作成されます。

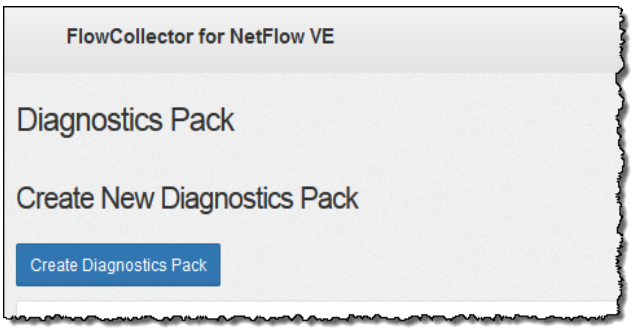
> ⚠ SMC やフローコレクタをバックアップする場合は、データベースもバックアップする必要があります。これらのアプライアンスを完全に復元するには、両方のバックアップが必要です。詳細については、「7. フローコレクタと SMC データベースのバックアップ」を参照してください。

6. 診断パックの作成

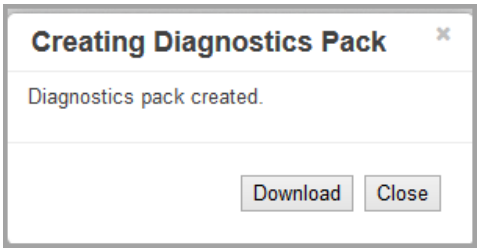
診断パックがあると、Cisco Stealthwatch サポートによる問題のトラブルシューティングが必要な場合に役立ちます。

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. 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。このプロセスに数分かかることがあります。



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。

7. フローコレクタと SMC データベースのバックアップ

フローコレクタまたは Stealthwatch 管理コンソール（SMC）の診断パックを作成した後、フローコレクタデータベースと SMC データベースをバックアップします。サポートが必要な場合は、Cisco Stealthwatch サポートに連絡してください。

> 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. SMC の SNMP ポーリングの無効化
2. フローコレクタデータベースのトリミング
3. データベースのバックアップ
4. データベースのスナップショットの削除
5. SMC での SNMP ポーリングの再有効化

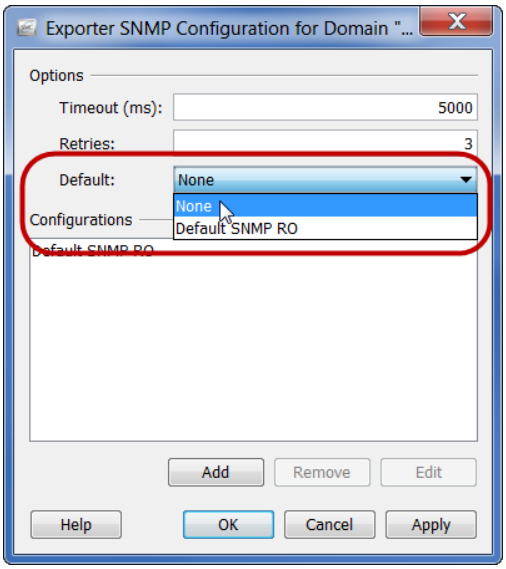
> バックアップしていないと、更新プロセス中に問題が発生した場合にファイルを回復できません。手順に従って、データベースのバックアップのすべての手順を実行してください。サポートが必要な場合は、Cisco Stealthwatch サポートに連絡してください。

1. 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 Stealthwatch デスクトップクライアントにログインします（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。
3. [設定（Configuration）] > [エクスポータの SNMP 設定（Exporter SNMP Configuration）] の順に選択します。
4. [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。



5. [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。
6. [OK]をクリックします。
7. システム上のドメインごとに手順 2 ～ 6 を繰り返します。

2. フローコレクタデータベースのトリミング

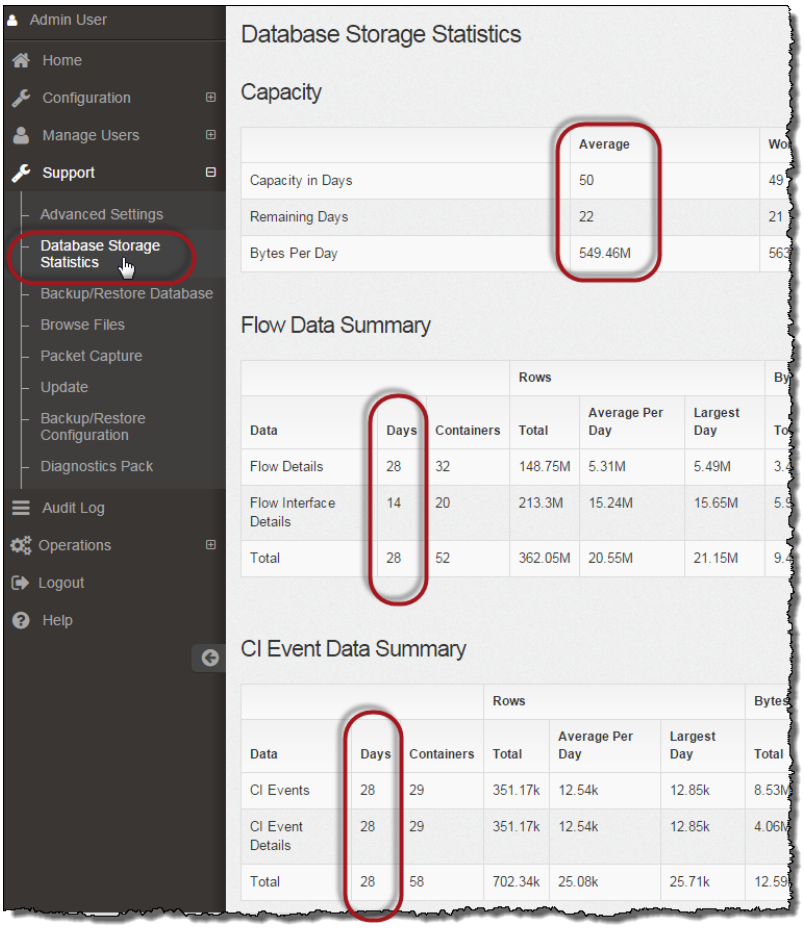
フローコレクタデータベースのバックアップが完了するまでに数日かかる場合があり、また、データベースが大きい場合はネットワークの速度が低下します。データベースをバックアップする前に、フローコレクタデータベースをトリミングすることを推奨します。これにより、フローの保存に使用できるディスク容量が解放され、データベースのバックアップにかかる時間が短縮されます。

フローコレクタには、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(/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

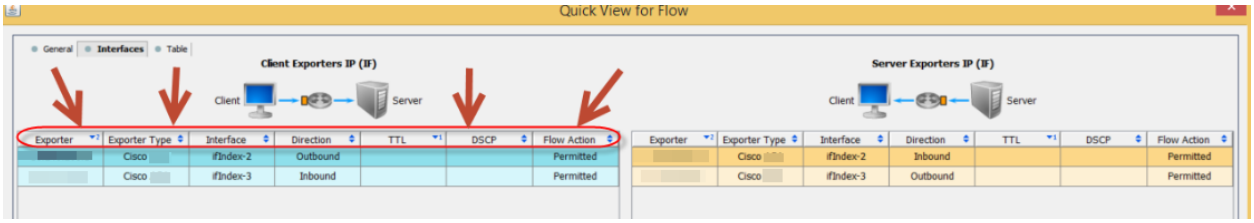
次の手順に従って、データベースストレージを確認します。

1. フローコレクタ 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 は、フロー インターフェイス データと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. 管理者ユーザとして Stealthwatch デスクトップクライアントにログインします。
2. [企業(Enterprise)]ツリーでフローコレクタを見つけます。プラス(+)記号をクリックしてコンテナを展開します。

3. [フローコレクタ(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. [フローコレクタのプロパティ(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

フローコレクタ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、Cisco Stealthwatch 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、フローコレクタ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。

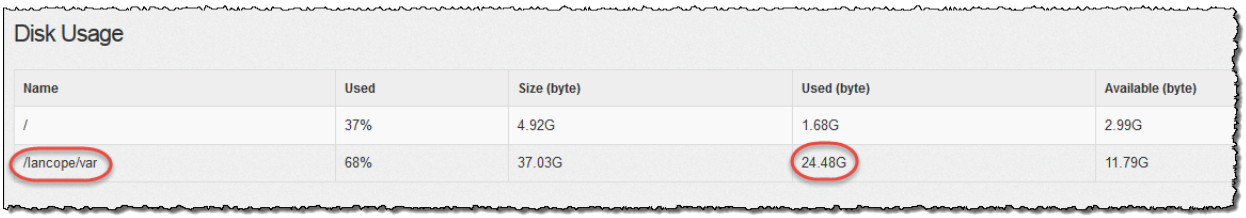
3. データベースのバックアップ

Flow Collector または SMC 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。

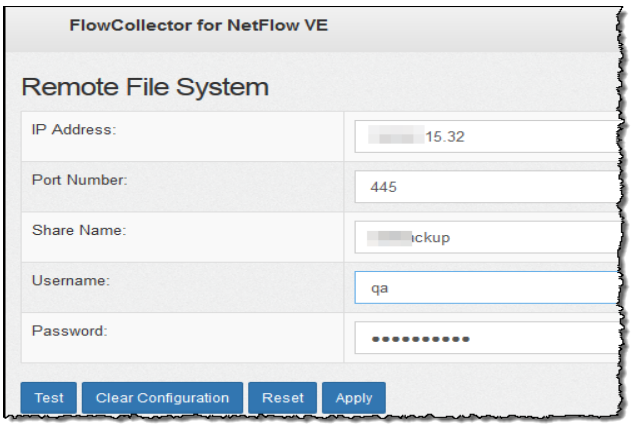
   - [ホーム(Home)]をクリックします。
   - [ディスク使用量(Disk Usage)]セクションを見つけます。
   - **/lancope/var** ファイルシステムの[使用済み(バイト)(Used(byte))]列を確認します。データベースのバックアップを保存するためには、リモートファイル システム上に少なくともこの数値にその 15% を足した分の空き容量が必要です。



Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	37%	4.92G	1.68G	2.99G
/lancope/var	68%	37.03G	24.48G	11.79G

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。

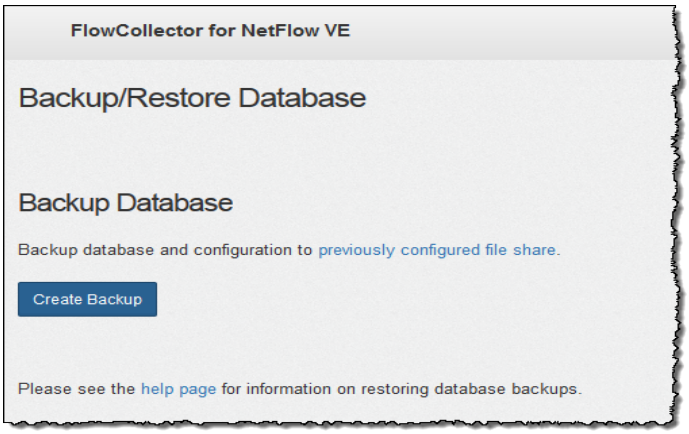
   パスワードを入力しても[適用(Apply)]ボタンが有効にならない場合、[リモートファイルシステム(Remote File System)]ページの空白部分を 1 回クリックすると有効になります。

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. [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。

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後、次の手順に従って SMC またはフローコレクタデータベースのスナップショットを削除します。

> ⚠ SMC またはフローコレクタ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 またはフローコレクタコンソールに**管理者**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. 手順 1 ～ 3 を繰り返して、保存されているすべての SMC およびフローコレクタデータベースのスナップショットを削除します。

5. SMC での SNMP ポーリングの再有効化

SNMP ポーリングを再度有効にするには、次の手順を実行します。

1. 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」の手順 4 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 2 ～ 4 を繰り返します。
6. デスクトップクライアントを閉じます。

8. 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 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**：SWU が [集中管理（Central Management）] の [マネージャの更新（Update Manager）] にアップロードされると、更新中に SMC 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、SMC（[集中管理（Central Management）]）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 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 [マネージャの更新（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 ファイルシステムに残ります。

- **管理対象アプライアンス**：[集中管理（Central Management）] の [マネージャの更新（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 [マネージャの更新（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。

使用可能なディスク容量の確認

以下の手順を使用して、SMC 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（Available）]（バイト）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 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、フローコレクタの SWU ファイルが 6 GB の場合、フローコレクタ 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**：たとえば、それぞれ 6 GB の 4 つの SWU ファイルを SMC にアップロードする場合、SMC パーティションで少なくとも 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『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 v7.1.2』の「Data Storage」の項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。

9. 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、「**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**」で詳細を参照してください。

特定のアプライアンスのパッチ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パッチをアップロードします。詳細については、パッチの Readme ノートを参照してください。

> ⚠ 「**9. パッチのインストール**」の手順を開始する前に、Stealthwatch クラスタ内の管理対象アプライアンスすべてで手順 3 ～ 8 を実行したことを確認します。

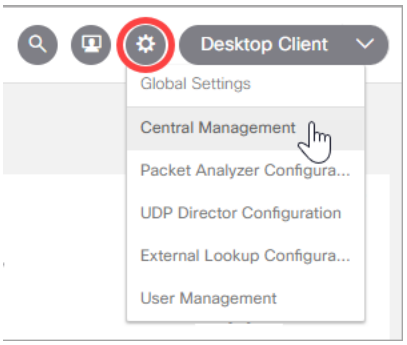
ベスト プラクティス

- **Readme**:詳細については、パッチの Readme ノートを参照してください。
- **順序**:アプライアンスにパッチを順番に適用します。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**:パッチをインストールする前に、SMC および Flow Collector の稼働時間が 1 時間以上かつ 7 日未満であることを確認してください。
- **確認**:次のアプライアンスの更新を開始する前に、更新がインストールされ、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. パッチのアップロード

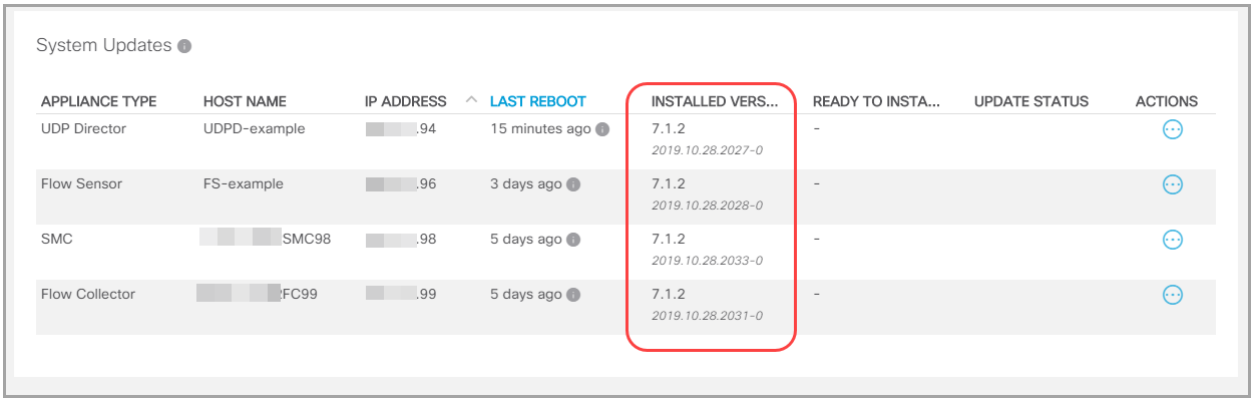
[集中管理(Central Management)] の [マネージャの更新(Update Manager)] にパッチをアップロードするには、次の手順を使用します。

1. SMC にログインします。
   (ブラウザのアドレス フィールドに、https:// およびアプライアンスの IP アドレスを入力し、Enter を押します。)
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. [マネージャの更新(Update Manager)] タブを選択し、[システムアップデート(System Updates)] セクションを見つけます。

5. [インストールされているバージョン(Installed Version)] 列を確認します。各アプライアンスに **v7.1.1**(または最新バージョンの 7.1.x)がインストールされていることを確認します。



6. [アップロード(Upload)] をクリックします。
7. 画面に表示される指示に従って、パッチ 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。

    - [パッチ(Patches)]:特定のアプライアンスのパッチ 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パッチをアップロードします。詳細については、パッチの Readme ノートを参照してください。

    - **ディスク容量**:詳細については、「使用可能なディスク容量の確認」を参照してください。

2. パッチのインストール

次の手順に従い、[集中管理(Central Management)] を使用してパッチを適用します。

1. [マネージャの更新(Update Manager)] > [システム更新(System Updates)] セクションで、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**:パッチファイルが掲示されていることを確認します。
    - [最後のリブート(Last Reboot)](SMC およびフローコレクタ):最後のリブートから 1 時間以上かつ 7 日未満経過してい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。

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. [更新のインストール(Install Update)] を選択します。
4. 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。詳細については、パッチの Readme ノートを参照してください。

3. パッチのインストールの確認

パッチを適用しても、[インストール済みバージョン(Installed Version)] 列に表示される情報は変わりません。次の手順に従って更新ログを確認します。

1. 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。
2. [更新ログの表示(View Update Log)] を選択します。
3. 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。

    失敗: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、「エラーのトラブルシューティング」を参照してください。

4. [集中管理(Central Management)] > [アプライアンス マネージャ(Appliance Manager)] ページでアプライアンスを確認します。

    - **アプライアンスステータス**:[アプライアンスステータス(Appliance Status)] 列を確認し、各アプライアンスが [アップ(Up)] 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 [アップ(Up)] と表示されていることを確認します。

5. このセクションのすべての手順を繰り返し、クラスタ内の各アプライアンスに最新のパッチをインストールします。

10. v7.2.1 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 [マネージャの更新 (Update Manager)] ページを使用します。

> ⚠ ソフトウェアアップデートを開始する前に、SMC とフローコレクタが 1 時間以上、7 日未満実行され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	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.	Flow Collector 5000 シリーズ データベース	更新を開始する前に、Flow Collector の稼働時間が 1 時間以上かつ 7 日未満であることを確認してください。 エンジンの更新を開始する前に、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てください。
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 5000 シリーズの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、エンジンの更新が完了し、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てください。
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 の稼働時間が 1 時間以上かつ 7 日未満で

		あることを確認してください。 クラスタ内の次のアプライアンスを更新する前に、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てください。
5.	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 7 日未満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、プライマリ SMC の更新を開始する前に、セカンダリ SMC の更新が完了し、セカンダリ SMC アプライアンスのステータスが [アップ(Up)] と表示されていることを確認してください。 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。これが発生した場合は、「12. 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。
6.	プライマリ SMC	更新を開始する前に、SMC の稼働時間が 1 時間以上かつ 7 日未満であることを確認してください。 システムでセカンダリ SMC を使用している場合は、プライマリ SMC の更新を開始する前に、セカンダリ SMC の更新が完了し、セカンダリ SMC アプライアンスのステータスが [アップ(Up)] であることを確認してください。 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。これが発生した場合は、「12. 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.	Flow Sensor	
8.	エンドポイント コンセントレータ	管理対象アプライアンスを更新した後、エンドポイント コンセントレータを更新し

		ます。詳細については、「**13. エンドポイントコンセントレータと管理対象外アプライアンスの更新**」を参照してください。

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**：7.1.x ソフトウェアアップデートを開始する前に、SMC および Flow Collector の稼働時間が 1 時間以上かつ 7 日未満であることを確認してください。
- **Flow Collector**：このソフトウェアアップデートの一環として、Stealthwatch Flow Collector のプロセスを改善しました。更新は、完了までに最大 2 時間かかる場合があります。開始する前に、アプライアンスの更新順序で Flow Collector の詳細を確認します。
- **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、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 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。

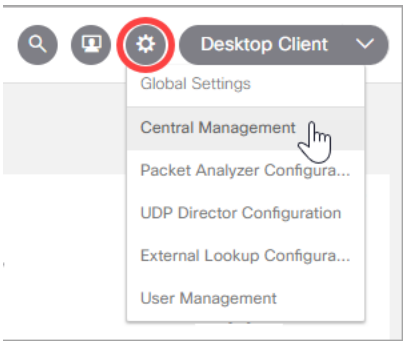
管理対象アプライアンスでのソフトウェアアップデートのインストール

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. SWU のアップロード

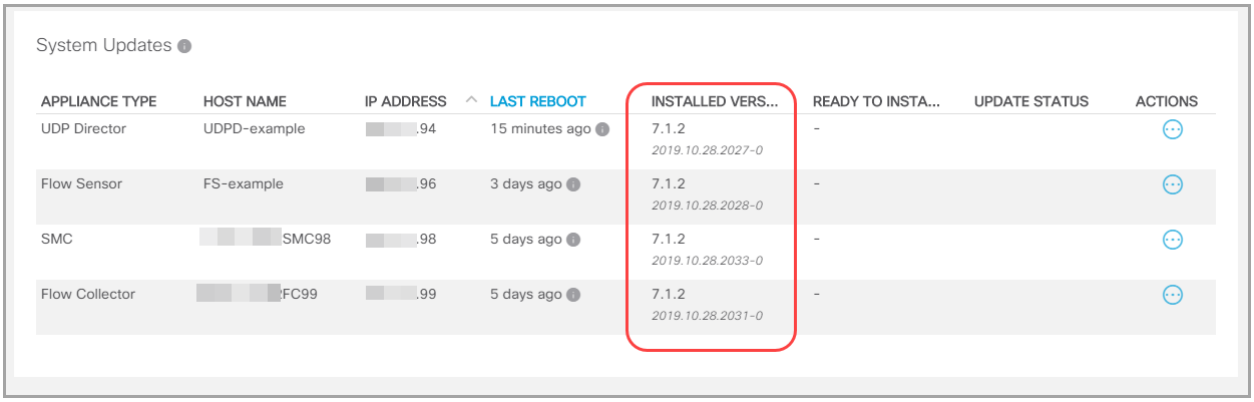
1. SMC にログインします。
   （ブラウザのアドレス フィールドに、https:// およびアプライアンスの IP アドレスを入力し、Enter を押します。）
2. [グローバル設定（Global Settings）] アイコンをクリックします。
3. [集中管理（Central Management）] を選択します。



4. [マネージャの更新(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、各アプライアンスが [アップ(Up)] として表示されていることを確認します。

5. [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 **v7.1.1**(または 7.1.2 など、最新バージョンの 7.1.x)がインストールされていることを確認します。



6. [アップロード(Upload)] をクリックします。
7. 画面に表示される指示に従って、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。
   - **フローセンサー**:SMC を更新した後、フローセンサーの 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、「使用可能なディスク容量の確認」を参照してください。

2. 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番に更新してください。

1. [マネージャの更新(Update Manager)]>[システム更新(System Updates)]セクションで、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)]: 7.2.1 SWU ファイルが表示されていることを確認します。**フローセンサー**の SWU ファイルが送信されていない場合は、SMC を更新した後にアップロードします。
   - [最後のリブート(Last Reboot)](SMC およびフローコレクタ):最後のリブートから 1 時間以上かつ 7 日未満経過してい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。

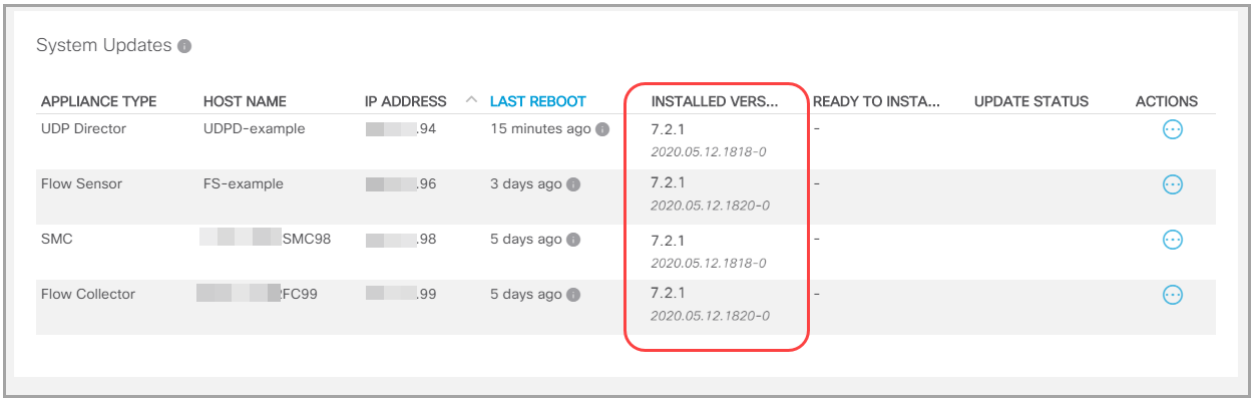
> ⚠ 設定の変更が保留中、または設定チャネルがダウンしている場合は、アプライアンスを再起動しないでください。アプライアンスのステータスが[アップ(Up)]であることを確認するには、[集中管理(Central Management)]>[アプライアンス マネージャ(Appliance Manager)]ページを参照します。

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. [更新のインストール(Install Update)]を選択します。
4. 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。Flow Collector データベースを更新する場合、更新には最大 2 時間かかることがあります。

3. ソフトウェアアップデートの確認

1. [インストールバージョン(Installed Version)] 列をチェックして、**v7.2.1** 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。



- [正常にインストールされました(Installation Successful)]:インストールされているバージョンが **7.2.1** の場合は、次のステップに進んで、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。
- **エラーのトラブルシューティング**:ログまたは UI に次のエラーのどれかが表示される場合があります。

エラーの説明またはカテゴリ	詳細
ハードウェア	Dell PowerEdge または Flow Collector 5020 が検出された場合、これらは Stealthwatch v7.2 でサポートされていないことに注意してください。ハードウェアの更新については、次のメールアドレスから Stealthwatch 更新チームにお問い合わせください。(stealthwatch_renewals@cisco.com)。
[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。アプライアンスがフローセンサーの場合は、SMC を更新した後に SWU ファイルをアップロードします。 また、[最後のリブート(Last Reboot)] 列で SMC およびフローコレクタの最後のリブートから 1 時間以上かつ 7 日未満経過してい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。

エラーの説明またはカテゴリ	詳細
	• 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 > [アプライアンスのリブート(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。
ライセンシング	ライセンス上の理由によってアップグレードが失敗した場合は、ライセンスの再設定か、または新しい期間ライセンスの購入が必要な場合があります。stealthwatch_renewals@cisco.com で Stealthwatch 更新チームにお問い合わせください。ログの詳細については、「確認の結果」を参照してください。
SMC 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、『Stealthwatch インストールおよびコンフィギュレーション ガイド』の「トラブルシューティング」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。
デバイスに空き容量がありません (No space left on device) (ディスク容量)	各アプライアンスのディスク容量をチェックして、パッチとソフトウェア更新ファイルのインストールに十分な空き容量があることを確認します。 管理対象アプライアンスごとに、個々のソフトウェア更新ファイル(SWU)の 4 倍以上のサイズが必要です。SMC 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 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**:たとえば、それぞれ 6 GB の 4 つの SWU ファイルを SMC にアップロードする場合、SMC パーティションで少なくとも 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

エラーの説明またはカテゴリ	詳細
	GB）。 • **その他の情報**：手順については、「**8. 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、『Stealthwatch インストールおよびコンフィギュレーション ガイド』の「トラブルシューティング」セクションを参照してください。 また、［最後のリブート（Last Reboot）］列で SMC およびフローコレクタの最後のリブートから 1 時間以上かつ 7 日未満経過してい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＞［アプライアンスのリブート（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。
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。詳細については、「**10. v7.2.1 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。

> 更新の失敗がハードウェアまたはライセンスに関連せず、解決できない場合は、Cisco Stealthwatch サポートにお問い合わせください。

2. ［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**：アプライアンスのステータスが［アップ（Up）］になっていることを確認します。
- **Stealthwatch 管理コンソール**：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が［アップ（Up）］と表示されていることを確認します。

3. このセクションのすべての手順を繰り返し、次のアプライアンスに対し、「**管理対象アプライアンスでのソフトウェアアップデートのインストール**」を行います。アプライアンスは順番に更新してください。
4. ［集中管理（Central Management）］ですべてのアプライアンスを更新した場合は、「**11. Stealthwatch デスクトップクライアントのインストール**」に進みます。

11. Stealthwatch デスクトップクライアントのインストール

以下の手順で、Windows または macOS を使用して Stealthwatch デスクトップ クライアントをインストールします。次の点に注意してください。

- Stealthwatch 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することができます。
- Stealthwatch 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 SMC 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 SMC とセカンダリ SMC の両方を使用している場合は、一方の SMC をログオフして、その後もう一方の SMC にログインする必要があります。
- Stealthwatch 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。
- Stealthwatch の最新のバージョンに更新する場合は、Stealthwatch 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。
- すでに Stealthwatch デスクトップクライアントがあり、v7.1 に更新する場合、Stealthwatch デスクトップクライアントで Oracle Java を使用できなくなります。

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

- Stealthwatch デスクトップ クライアントをインストール可能な権限を持っている必要があります。
- Stealthwatch 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。

1. Stealthwatch Web アプリケーションの任意のページの右上隅にある [ダウンロード (Download)] アイコンをクリックします。

2. .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。
3. ウィザードの手順を実行して Stealthwatch デスクトップ クライアントをインストールします。
4. デスクトップ上の Stealthwatch デスクトップ クライアント アイコン をクリックします。
5. SMC ユーザ名およびパスワードを入力します。
6. SMC サーバ名または IP アドレス(IPv4 または IPv6)を入力します。
7. 画面に表示される指示に従ってデスクトップ クライアントを開き、アプライアンスのアイデンティティ証明書を信頼します。

メモリサイズの変更

Stealthwatch 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. これらのフォルダを次の順に開きます。AppData > ローミング > 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、Stealthwatch 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。

> - Stealthwatch 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

- Stealthwatch デスクトップ クライアントをインストール可能な権限を持っている必要があります。
- Stealthwatch 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。

1. Stealthwatch Web アプリケーションの任意のページの右上隅にある [ダウンロード (Download)] アイコンをクリックします。

2. .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に表示されます。

3. Stealthwatch デスクトップ クライアントのアイコンを ( ) アプリケーションの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。

4. デスクトップ上の Stealthwatch デスクトップ クライアント アイコン をクリックします。
5. SMC ユーザ名およびパスワードを入力します。
6. SMC サーバ名または IP アドレス (IPv4 または IPv6) を入力します。
7. 画面に表示される指示に従ってデスクトップ クライアントを開き、アプライアンスのアイデンティティ証明書を信頼します。

メモリサイズの変更

Stealthwatch 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、Stealthwatch 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。

- Stealthwatch 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. SMC フェールオーバーロールの確認

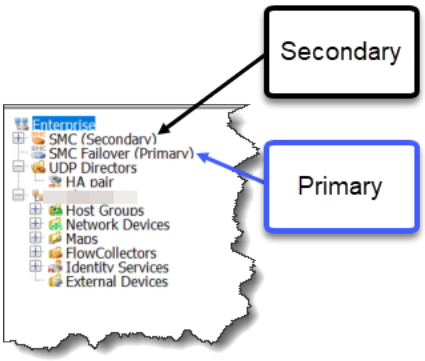
SMC フェールオーバーの設定を使用しない場合、この手順は省略できます。

> ⚠ 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。

> ⚠ [集中管理(Central Management)] でのアプライアンスの追加や削除は、フェールオーバーの設定を完了し、[集中管理(Central Management)] でセカンダリ SMC アプライアンスのステータスが [アップ(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。Stealthwatch 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。

> ℹ 手順については、Stealthwatch 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**(Stealthwatch 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、[集中管理(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。
   - [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。
   - [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、[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 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. [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 SMC アプライアンスのステータスが[アップ(Up)]と表示されていることを確認します。

13. エンドポイント コンセントレータと管理対象外アプライアンスの更新

次の手順に従って、アプライアンスを **v7.1.x から v7.2.1** に更新し、それらを v7.2.1 の Stealthwatch 管理コンソール（Central Manager）に追加します。これらの手順は、次のシナリオのアプライアンスに使用できます。

- **エンドポイントコンセントレータ**：v7.1.x がインストールされたエンドポイントコンセントレータがある場合は、それらを 7.2.1 に更新し、[集中管理（Central Management）] に追加します。
- **管理対象外アプライアンス**：他の管理対象アプライアンスで更新されていない v7.1.x フローセンサーまたは UDP Director がある場合は、次の手順を実行します。アプライアンスを v7.2.1 に更新し、それを v7.2.1 Stealthwatch 管理コンソール（Central Manager）に追加します。

> エンドポイントコンセントレータまたは残りの管理対象外アプライアンスがない場合は、Stealthwatch の更新が終了します。

はじめる前に

はじめる前に、**Stealthwatch 管理コンソールに v7.2.1 がインストールされていることを確認**します。詳細については、「**Stealthwatch 管理コンソールが必要**」を参照してください。

また、アプライアンスの更新準備が整っていることを確認します。

- **ライセンス**：ライセンスが最新であることを確認します。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）] > [ライセンス（Licensing）] を選択します。[機能ライセンスのステータス（Feature License Status）] セクションを確認します。詳細については、「**ライセンス**」を参照してください。
- **ホスト名**：アプライアンスごとに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。

  ホスト名を確認するには、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**：アプライアンスごとに完全修飾ドメイン名が必要です。ドメイン名を確認するには、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。
- **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は、アプライアンスを [集中管理（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（ルートと中間）をその独自の信頼ストアと SMC 信頼ストアに個別に保存します。詳細については、「**1. 信頼ストアへのカスタム証明書の追加**」を参照し、手順を確認します。

> アプライアンスでカスタム証明書を使用する場合は、このガイドの手順に従ってください。

1. 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

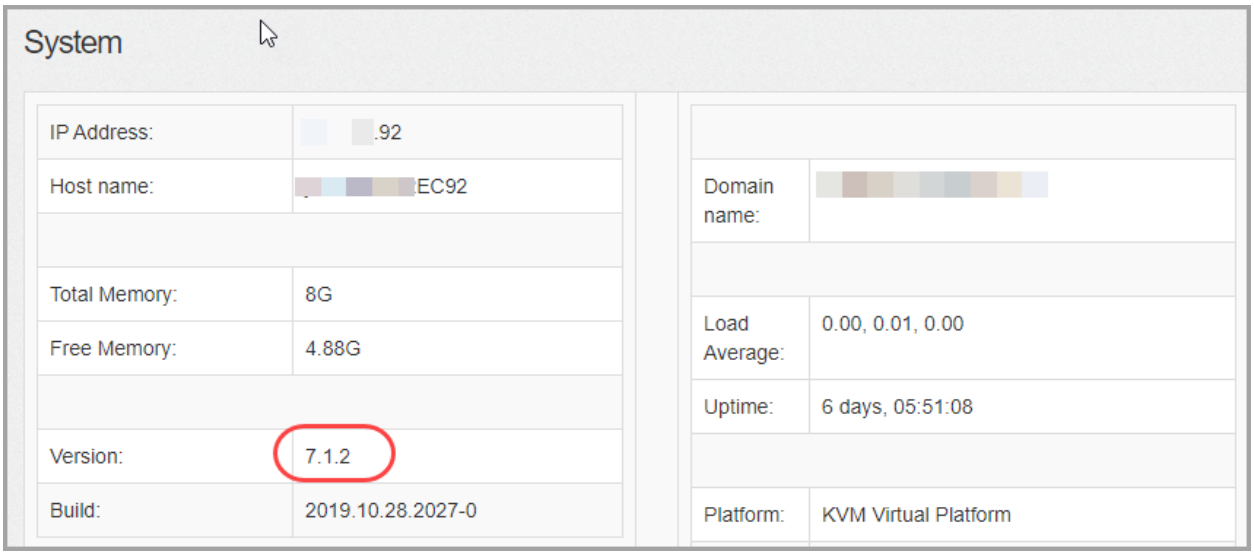
「パッチファイルとアップデートファイルのダウンロード」手順を使用して、パッチファイルとアップデートファイルをダウンロードします。

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

次の手順に従って、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。

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>)。
2. [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。アプライアンスに **v7.1.1**(または 7.1.x の後継バージョン)がインストールされていることを確認します。

   7.0.x 以前:ソフトウェアのバージョンが 7.0.x 以前の場合は、この更新を開始する前に、『Stealthwatch 更新ガイド』を使用して、アプライアンスを 7.1.1(または最新バージョンの 7.1.x)に更新します。



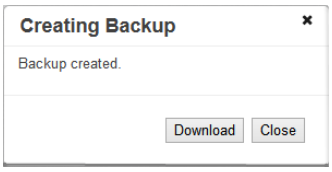
3. アプライアンス設定のバックアップ

管理対象外アプライアンスの設定をバックアップするには、次の手順を実行します。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。



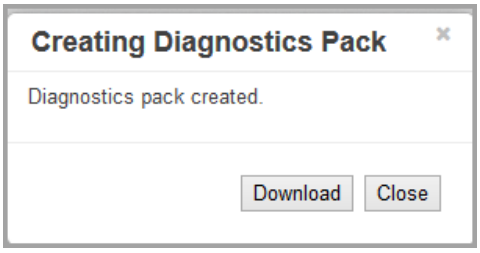
7. [閉じる(Close)] をクリックして進捗状況ウィンドウを閉じます。

4. 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. 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。このプロセスに数分かかることがあります。



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。

5. 使用可能なディスク容量の確認

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。

SWU ファイルをインストールするのに十分な空き容量がアプライアンスに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、ソフトウェア更新ファイルが 6 GB の場合、パーティションには 24 GB の空き容量(1 つの SWU ファイル x 6 GB x 4 = 24 GB)が必要です。

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。

「**6. パッチのインストール**」を開始する前に、アプライアンスに対して手順 1 ～ 6 が完了していることを確認します。

6. 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。

詳細については、パッチの Readme ノートを参照してください。

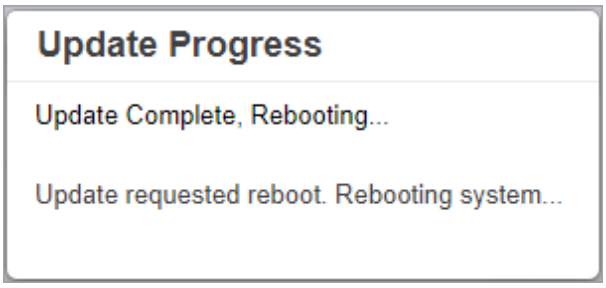
設定の変更が保留中、または設定チャネルがダウンしている場合は、アプライアンスを再起動しないでください。

1. 管理アプライアンスの [サポート(Support)] > [更新(Update)] ページで、
2. [ファイルの選択(Choose File)] をクリックします。
3. アプライアンスのパッチ SWU ファイルを選択します。
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。

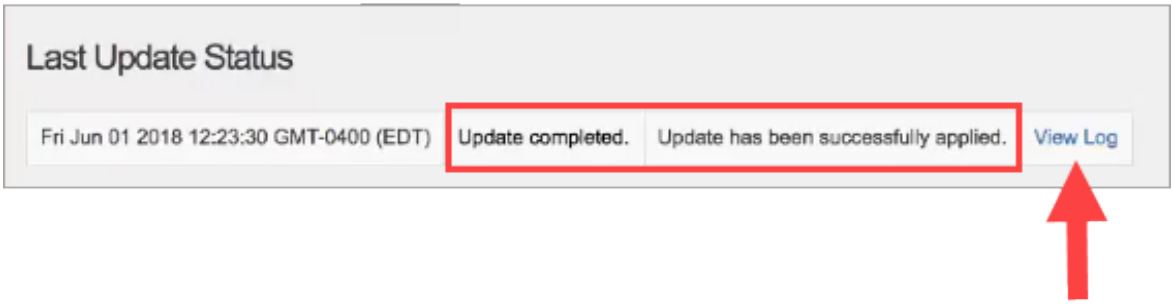
   - アップロードの進捗状況はページの下部に表示されます。

- 安全性の確認と更新には数分かかる場合があります。

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. インストールの確認: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。
9. [サポート(Support)]>[更新(Update)]の順に選択します。
10. [前回の更新ステータス(Last Update Status)]セクションで、パッチ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。



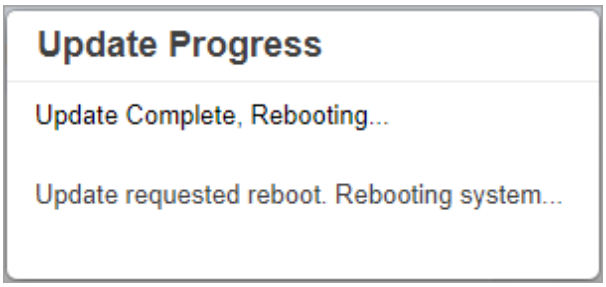
7. 7.2.1 ソフトウェアアップデートのインストール

> ⚠ 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。

1. 管理アプライアンスの[サポート(Support)]>[更新(Update)]ページで、[ファイルの選択(Choose File)]をクリックします。
2. アプライアンスに v7.2.1 SWU 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。

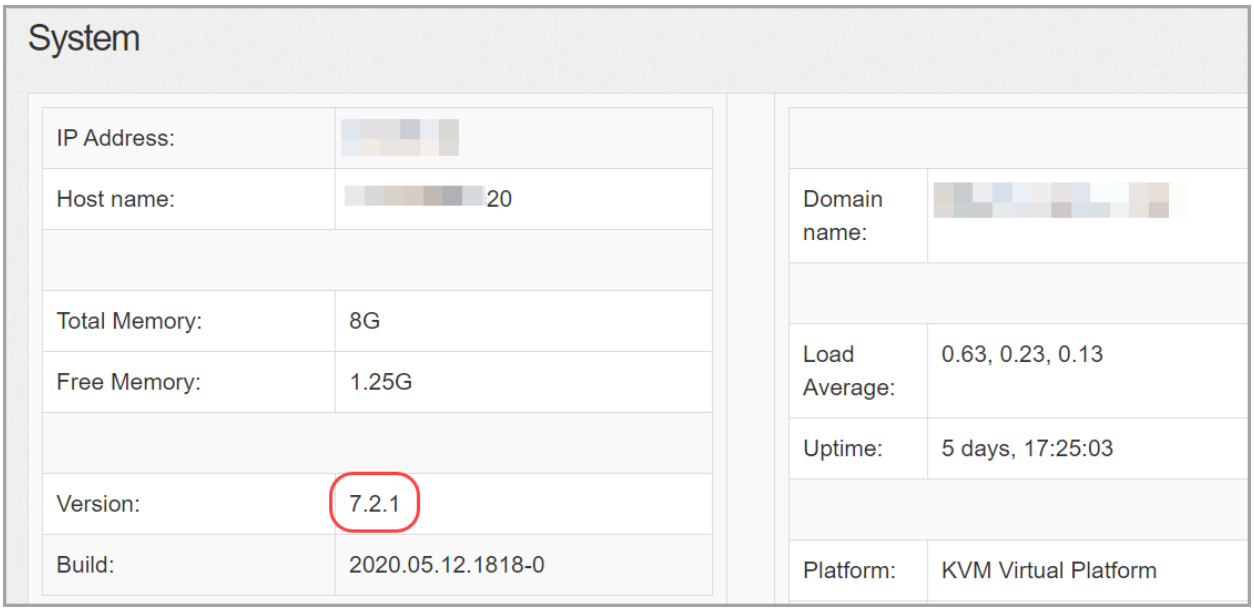
5. [更新の進捗状況(Update Progress)]に[完了(Complete)]および[再起動(Rebooting)]が表示されたら、ページを更新します。



⚠ 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。

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 **v7.2.1** が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. 集中管理へのアプライアンスの追加

すべてのアプライアンスを設定して、プライマリ SMC である Central Manager によって管理されるようにします。

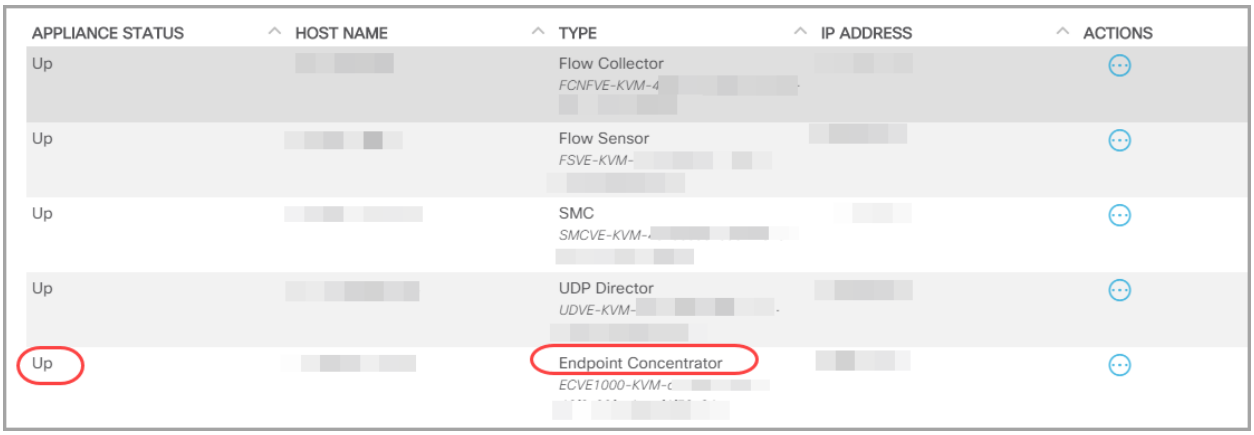
> ⚠ Stealthwatch v7.2.1 を使用するには、すべてのアプライアンスが [集中管理(Central Management)] に追加されていることを確認します。

1. 「**2. 集中管理 へのスタンドアロン アプライアンスの追加**」の手順に従ってエンドポイントコンセントレータ(またはその他の管理対象外フローセンサーまたは UDP Director)を [集中管理(Central Management)] に追加します。

> ⚠ **[集中管理(Central Management)] に追加する前に、アプライアンスに Stealthwatch v7.2.1 が** インストールされていることを確認します。

2. 完了したら、集中管理インベントリにアプライアンスが表示され、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。

   すべての Stealthwatch アプライアンスが [集中管理(Central Management)] に表示されている場合は、Stealthwatch の更新が完了しています。



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