

Cisco Stealthwatch

更新ガイド 7.3.0



目次

はじめに	5
概要	5
対象読者	5
用語	5
はじめる前に	6
ソフトウェア バージョン	6
Cisco Software Central	6
TLS	6
サード パーティ製アプリケーション	6
ブラウザ	7
ハードウェア	7
ライセンス	7
カスタム証明書	7
ディスク容量	8
ホスト名	9
ドメイン名	9
NTP サーバ	9
タイムゾーン	9
ISE または ISE-PIC	10
アプライアンスのバックアップ	10
フローコレクタデータベースのバックアップ	10
更新に最適な時間	11
ソフトウェア アップデートファイル	11
すべてのアプライアンス	11
SMC と Flow Collector	11
通信	11
更新後	12
代替アクセス	12
ハードウェア	12
仮想アプライアンス	12
その他のオプション	12
更新の概要	14
更新プロセスの概要	14

1. クラスタの確認	15
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	15
2. 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	17
1. Cisco Software Central へのログイン	17
2. パッチのダウンロード	18
3. 更新ファイルのダウンロード	19
SWU ファイル	20
3. アプライアンスの設定のバックアップ	21
バックアップ設定ファイルの作成	21
4. 診断パックの作成	22
5. Flow Collector と SMC データベースのバックアップ	23
1. SMC の SNMP ポーリングの無効化	23
2. フローコレクタデータベースのトリミング	24
1. データベースストレージの統計情報の確認	24
2. インターフェイスの詳細のトリミング	25
3. フローの詳細と CI イベントデータのトリミング	26
3. データベースのバックアップ	26
4. データベースのスナップショットの削除	28
5. SMC での SNMP ポーリングの再有効化	29
6. 使用可能なディスク容量の確認	30
使用可能なディスク容量の確認	30
7. パッチのインストール	32
ベストプラクティス	32
1. インストールされているバージョンの確認	33
2. SMC への必要なロールアップパッチのインストール	34
3. 必要なロールアップパッチのアップロード	35
4. 必要なロールアップパッチのインストール	35
8. v7.3.0 ソフトウェアアップデートのインストール	38
新しい更新順序の使用	38
ベストプラクティス	40
ソフトウェアアップデートのインストール	40
1. SWU のアップロード	40
2. SWU のインストール	41
3. ソフトウェアアップデートの確認	42
9. v7.3.0 パッチのインストール	46

10. Stealthwatch デスクトップクライアントのインストール	47
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	47
メモリサイズの変更	48
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	48
メモリサイズの変更	49
11. SMC フェールオーバーロールの確認	51
サポートへの問い合わせ	53

はじめに

概要

Stealthwatch アプライアンスを v7.2.1 (または後継バージョン 7.2.x) から v7.3.0 に更新するには、このガイドを使用します。

- UDP Director (別名 Flow Replicator)
- 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)

v7.3.0 の詳細については、『[リリースノート](#)』を参照してください。

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。

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 7.3.0 に更新するには、アプライアンスに 7.2.1 (または後継バージョン 7.2.x) 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 v7.0.x を使用している場合は、各アプライアンスを v7.0.x から v7.1.x に更新した後、v7.1.x を v7.2.x に更新します。各更新ガイドは、[Cisco.com](https://www.cisco.com) で入手できます。
- **パッチ:** 更新プロセスの一環として、アップグレードの前に必要なロールアップパッチをアプライアンスにインストールします。パッチのインストール順序は、この更新に固有です。また、パッチが各アプライアンスにインストールされるまでに最大 90 分かかる場合があります。詳細については、「[7. パッチのインストール](#)」を参照してください。



パッチのインストール順序は、この更新に固有です。また、必要なパッチが各アプライアンスにインストールされるまでに最大 90 分かかることがあります。「[7. 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。

- **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。

Cisco Software Central

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。

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。

- **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)] > [スマートライセンス (Smart Licensing)] を選択します。[スマートライセンスの使用状況 (Smart License Usage)] セクションを確認します。
- **手順** ライセンスがコンプライアンス違反または期限切れと表示されている場合は、『[Stealthwatch スマートソフトウェアライセンシング ガイド](#)』[英語] で詳細を確認してください。

カスタム証明書

アプライアンスにカスタム アプライアンスアイデンティティ証明書がインストールされている場合は、それらの証明書が有効かつ最新であることを確認してから、更新プロセスを開始します。無効または期限切れのアプライアンスアイデンティティ証明書では、アプライアンスを更新できません。


	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。
----	--

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。

- **証明書の更新:** 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。

[ユーザ (User)] 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。

 [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。

- **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)] にシステム管理者としてログインし、[集中管理 (Central Management)] > [復旧 (Recovery)] > [アプライアンスの削除 (Remove Appliance)] からアプライアンスを削除します。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。
 - カスタムアプライアンスのアイデンティティ証明書 (アイデンティティ、ルート、およびチェーン) を必ず保存してください。
 - アプライアンスにログインし、アプライアンス設定ツールを使用して Central Management にアプライアンスを追加します。アプライアンス アイデンティティ証明書は自動的に置き換えられます。
 - デフォルトのアプライアンス 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には、このセクションの「**証明書の更新**」と「**古い証明書の削除**」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、「[6. 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 \times 6 GB \times 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 \times 6 GB \times 4 = 96 GB)。

ホスト名

- **要件:**各アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは更新できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。
- **確認:**SMC 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。

ドメイン名

- **要件:**各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスは更新できません。
- **確認:**SMC 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。


NTP サーバ

- **要件:**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:**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。
- **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。

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

- **要件:** 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。

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。手順については、「[5. Flow Collector 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。手順については、「[2. 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。

すべてのアプライアンス

- **時間:** この更新のパッチが各アプライアンスにインストールされるまでに最大 90 分かかることがあります。ソフトウェアの更新プロセスは、アプライアンスごとに完了するまで約 30 分かかります。ただし、ネットワークの状況によって長くなることがあります。この概算時間には、ユーザ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。この再起動の要件は、パッチのインストールには適用されません。
- **Flow Collector:** Flow Collector を更新して実行すると、SMC 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、「[ソフトウェア アップデートのインストール](#)」を参照してください。

 クラスタ内の次のアプライアンスを更新する前に、アプライアンスのステータスが [アップ (Up)] と表示されていることを確認します。

更新後

アプライアンスを更新した後、必要なパッチをインストールしてください。

- patch-smc-ROLLUP001-7.3.0-01.swu 以降
- patch-fcnf-ROLLUP001-7.3.0-02.swu 以降
- patch-fcsf-ROLLUP001-7.3.0-02.swu 以降

このガイドの手順に従い、Cisco Software Central(<https://software.cisco.com>)でパッチの ReadMe の手順を確認します。

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](https://www.cisco.com/c/ja_jp/support/security/stealthwatch/products-installation-guides-list.html)』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。

次の手順に従って、選択したアプライアンスの SSH を開いて有効にします。

1. [集中管理 (Central Management)] > [アプライアンス マネージャ (Appliance Manager)] を開きます。
2. アプライアンスの [アクション (Actions)] メニューをクリックします。
3. [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。
4. [アプライアンス (Appliance)] タブを選択します。
5. [SSH] セクションを見つけます。
6. SSH アクセスのみを有効にするか、ルートアクセスも有効にするかを選択します。
 - [SSHの有効化 (Enable SSH)]: アプライアンスへの SSH アクセスを許可するには、このチェックボックスをオンにします。
 - [ルートSSHアクセスの有効化 (Enable Root SSH Access)]: アプライアンスへのルートアクセスの有効化を許可するには、このチェックボックスをオンにします。
7. [設定の適用 (Apply settings)] をクリックします。
8. 画面に表示される指示に従って操作します。

更新の概要

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

更新プロセスの概要

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**を確認します。各アプライアンスのソフトウェアバージョンを確認します。
2. **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**
3. **アプライアンスの設定のバックアップ**
4. **診断パックの作成**
5. **Flow Collector と SMC データベースのバックアップ**
6. **使用可能なディスク容量の確認**
7. **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。この更新用に示された順序でパッチをインストールしてください。
8. **v7.3.0 ソフトウェアアップデートのインストール**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、v7.3.0 SWU をインストールしてください。
9. **v7.3.0 パッチのインストール**
10. **Stealthwatch デスクトップクライアントのインストール**
11. **SMC フェールオーバーロールの確認**

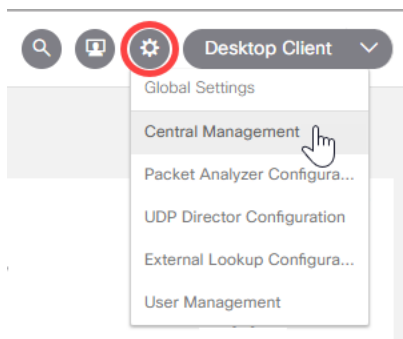
1. クラスタの確認

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 v7.2.1 (または 7.2.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 v7.2.1 (または 7.2.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 v7.2.1 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 7.2.1 がインストールされている必要があります。

7.1.x 以前: ソフトウェアバージョンが 7.1.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 7.2.x に更新します。『[Stealthwatch System 更新ガイド](#)』を参照してください。

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
Endpoint Concentrator	20	.20	8 days ago	7.2.1	-		
Flow Sensor	2	.22	8 days ago	7.2.1	-		
SMC	c24	.24	2 hours ago	7.2.1	-		
Flow Collector	5	.25	4 hours ago	7.2.1	-		
UDP Director		.94	8 days ago	7.2.1	-		



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。



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

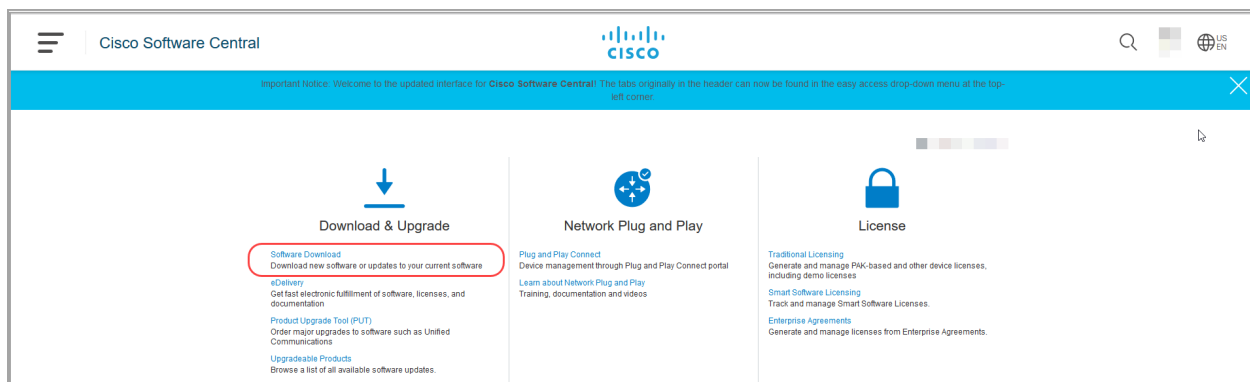
2. パッチ ファイルとアップデート ファイルのダウンロード

ライセンスを管理するには、パッチをダウンロードし、Stealthwatch 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 v7.3.0 SWU をダウンロードします。

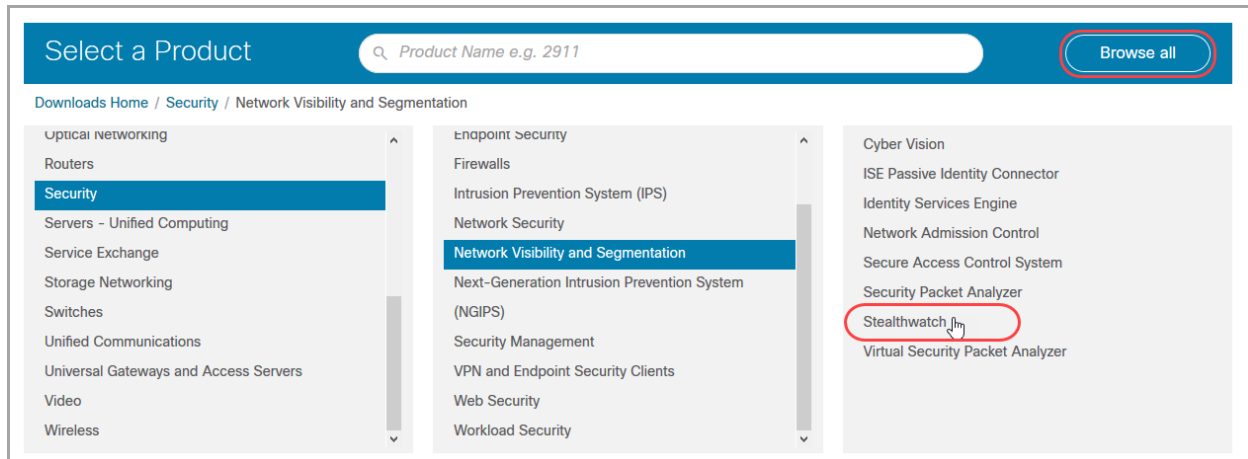
1. Cisco Software Central へのログイン

1. <https://software.cisco.com> で Cisco Software Central にログインします。
2. [ダウンロードとアップグレード (Download and Upgrade)] セクションで、[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。

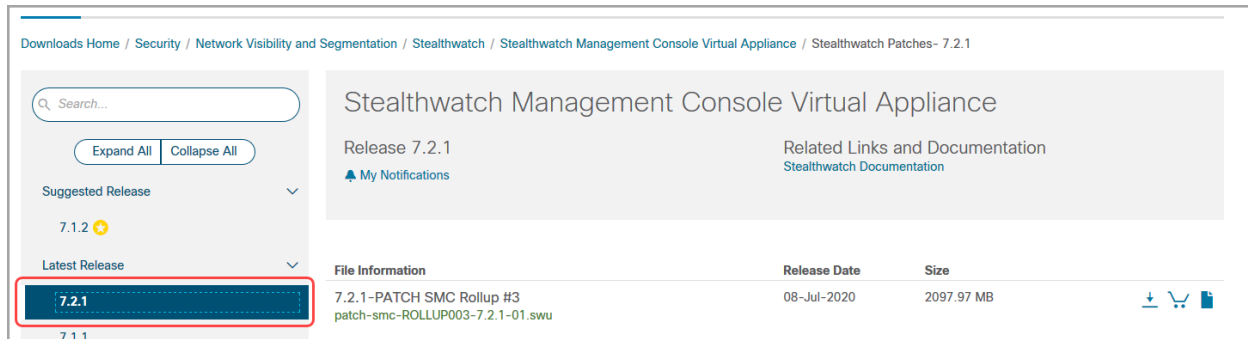


2. パッチのダウンロード

1. [Stealthwatch] メニューから、アプライアンスモデルを選択します。

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 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 7.2.1 がインストールされている場合は、[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。この更新に必要なすべてのファイルがダウンロードされていることを確認するには、[SWU ファイル](#)の表を参照してください。

3. 更新ファイルのダウンロード

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、[7.3.0] 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

この更新に必要なすべてのファイルがダウンロードされていることを確認します。ファイルが不足している場合は、「[2. パッチ 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。




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

アプライアンス	パッチ SWU ファイル名	ソフトウェア アップデート ファイル名
UDP Director (別名 Flow Replicator) UDP Director VE (別名 Flow Replicator VE)	patch-udp-ROLLUP001-7.2.1-02.swu	update-udp-7.3.0-2020.06.12.1944-01.swu
Flow Collector 5000 シリーズ データベース	patch-fcdb-ROLLUP001-7.2.1-02.swu	update-fcdb-7.3.0-2020.06.12.1945-01.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	patch-fcnf-ROLLUP001-7.2.1-02.swu	update-fcnf-7.3.0-2020.06.12.1947-01.swu
sFlow 向けフロー コレクタ sFlow VE 向けフロー コレクタ	patch-fcsf-ROLLUP001-7.2.1-02.swu	update-fcsf-7.3.0-2020.06.12.1946-01.swu
エンドポイント コンセントレータ	patch-ec-ROLLUP001-7.2.1-01.swu	update-ec-7.3.0-2020.06.12.1943-01.swu
SMC および SMC VE	patch-fcnf-ROLLUP006-7.2.1-04.swu	update-smc-7.3.0-2020.06.12.1949-01.swu
フロー センサー アプライアンス Flow Sensor VE	patch-fsuf-ROLLUP001-7.2.1-02.swu	update-fsuf-7.3.0-2020.06.12.1945-01.swu

3. 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。

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。

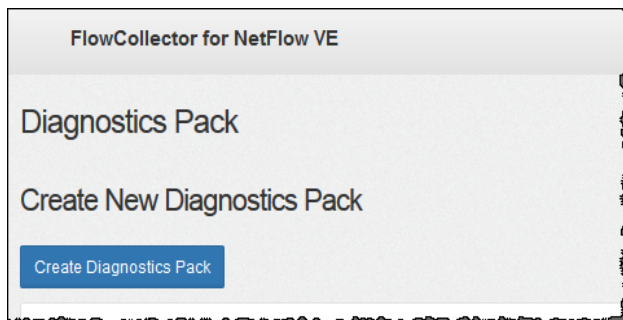
 SMC やフローコレクタをバックアップする場合は、データベースもバックアップする必要があります。これらのアプライアンスを完全に復元するには、両方のバックアップが必要です。手順については、「[5. Flow Collector と SMC データベースのバックアップ](#)」を参照してください。

4. 診断パックの作成

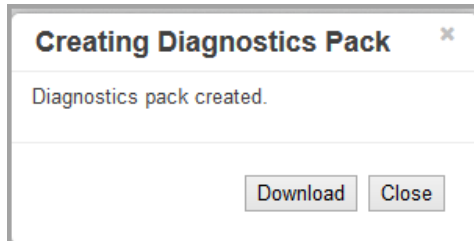
診断パックがあると、[Cisco Stealthwatch サポート](#)による問題のトラブルシューティングが必要な場合に役立ちます。

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 `/lancopce/var/admin/diagnostics` にあります。


5. Flow Collector 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

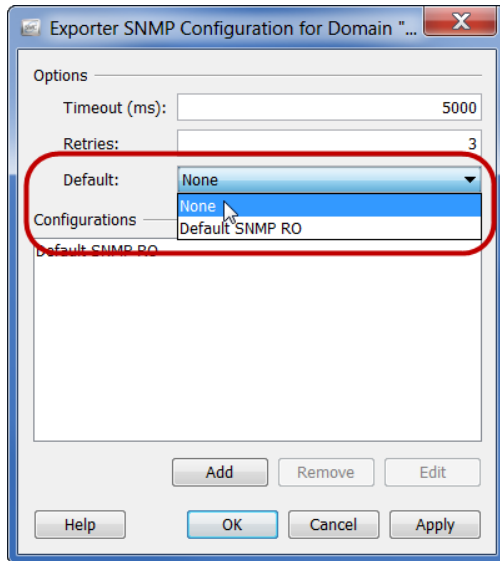
 バックアップしていないと、更新プロセス中に問題が発生した場合にファイルを回復できません。手順に従って、データベースのバックアップのすべての手順を実行してください。サポートが必要な場合は、[Cisco Stealthwatch サポート](#)に連絡してください。

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、エクスポートを右クリックします。
3. [設定 (Configuration)] > [エクスポートの 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

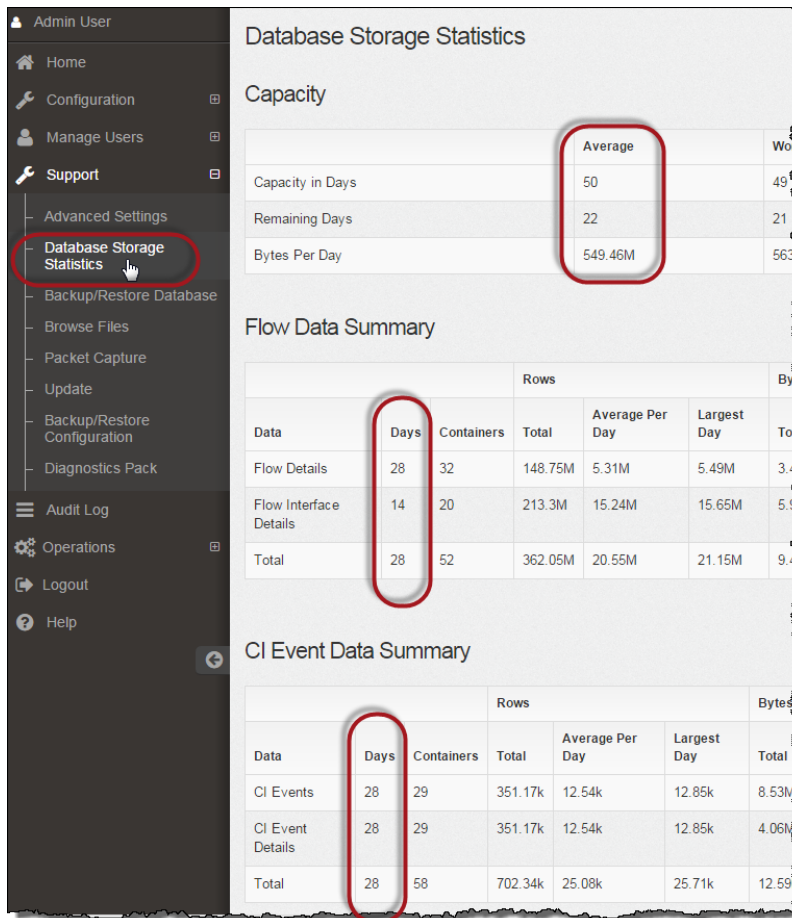
フローコレクタデータベースのバックアップが完了するまでに数日かかる場合があります。また、データベースが大きい場合はネットワークの速度が低下します。データベースをバックアップする前に、フローコレクタデータベースをトリミングすることを推奨します。これにより、フローの保存に使用できるディスク容量が解放され、データベースのバックアップにかかる時間が短縮されます。

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、エクスポート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。

Quick View for Flow

Exporter	Exporter Type	Interface	Direction	TTL	DSCP	Flow Action
Cisco	Cisco	#Index-2	Outbound			Permitted
Cisco	Cisco	#Index-3	Inbound			Permitted

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

フローコレクタのデータベースまたは 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。
 - `/lancopex/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。

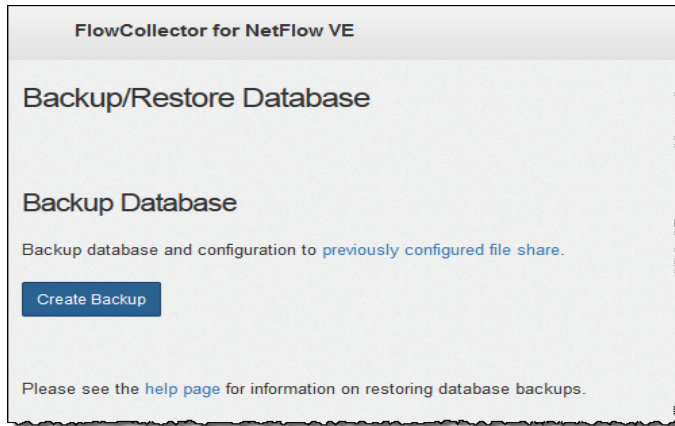
パスワードを入力しても [適用 (Apply)] ボタンが有効にならない場合、[リモートファイルシステム (Remote File System)] ページの空白部分を 1 回クリックすると有効になります。

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 lanlcope -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 lanlcope -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)] > [エクスポートの SNMP 設定 (Exporter SNMP Configuration)] の順に選択します。そのドメインの [エクスポートの 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。

6. 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、/lancopex/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 7.2.x インストールおよびコンフィギュレーション ガイド](#)』の「データストレージ」セクションを参照してください。
6. ステップ 1 ~ 5 を繰り返して、各アプライアンスの空き容量を確認します。

7. パッチのインストール

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



パッチをインストールする前に、Stealthwatch 内のすべての管理対象アプライアンスで手順 3 ～ 6 が完了していることを確認してください。

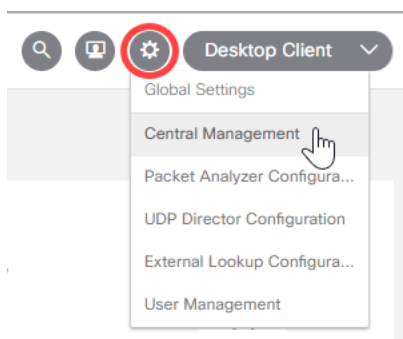
ベスト プラクティス

- **Readme:** 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。
- **順序:** ここで指定された順序でパッチをアプライアンスにインストールします。この更新では、最初にセカンダリ SMC にロールアップパッチをインストールします。
- **時間:** これらのパッチが各アプライアンスにインストールされるまでに最大 90 分かかることがあります。設定の変更が保留中、または設定チャンネルがダウンしている場合は、アプライアンスを再起動しないでください。
- **確認:** 次のパッチのインストールを開始する前に、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. インストールされているバージョンの確認

[集中管理 (Central Management)] の [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. プライマリ 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。
3. [集中管理 (Central Management)] を選択します。




4. [アプライアンスステータス (Appliance Status)] 列を確認し、各アプライアンスが [Up] と表示されていることを確認します。
5. [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。
6. [インストールされているバージョン (Installed Version)] 列を確認します。各アプライアンスに v7.2.1 (または最新バージョンの 7.2.x) がインストールされていることを確認します。

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
Endpoint Concentrator	20	.20	8 days ago	7.2.1	-		
Flow Sensor	2	.22	8 days ago	7.2.1	-		
SMC	c24	.24	2 hours ago	7.2.1	-		
Flow Collector	5	.25	4 hours ago	7.2.1	-		
UDP Director		.94	8 days ago	7.2.1	-		

2. SMC への必要なロールアップパッチのインストール

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

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

1. [アップロード(Upload)] をクリックします。
2. SMC の最新のロールアップパッチ SWU ファイルを選択します。

詳細については、「[SWU ファイル](#)」を参照してください。


3. [アップデートマネージャ(Update Manager)] > [システムの更新(System Update)] セクションで、SMC の [インストールの準備完了(Ready to Install)] 列を確認し、表示されているパッチを確認します。
4. **セカンダリ SMC** の [アクション(Actions)] メニューをクリックします。

プライマリ SMC: セカンダリ SMC でのパッチのインストールがすでに完了している場合は、プライマリ SMC の [アクション(Actions)] メニューをクリックします。

5. [更新のインストール(Install Update)] を選択します。
6. 画面に表示される指示に従って、更新を確認します。

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

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

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

7. インストールの確認:

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

8. [集中管理 (Central Management)] > [アプライアンスマネージャ (Appliance Manager)] ページで SMC を確認します。アプライアンスのステータスが [アップ (Up)] と表示されていることを確認します。
9. 2 つの SMC をフェールオーバー用に設定している場合は、手順 4 ～ 8 を繰り返して、プライマリ SMC にパッチをインストールします。

3. 必要なロールアップパッチのアップロード

次の手順に従って、クラスタ内の各アプライアンスに最新のロールアップパッチをアップロードします。これらの手順は SMC には適用されません。これらの手順を開始する前に、SMC でのパッチのインストールが完了していることを確認してください。

1. [アップロード (Upload)] をクリックします。
2. 選択したアプライアンスの最新のパッチ SWU ファイルを選択します。

詳細については、「[SWU ファイル](#)」を参照してください。

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

4. 必要なロールアップパッチのインストール

次の手順に従って、クラスタ内の各アプライアンスに必要なロールアップパッチをインストールします。これらの手順は SMC には適用されません。これらの手順を開始する前に、SMC でのパッチのインストールが完了していることを確認してください。



パッチが各アプライアンスにインストールされるまでに最大 90 分かかる場合があります。インストールの進行中は、アプライアンスを強制的に再起動しないでください。

各アプライアンスでは必ず次の順序で手順に従ってください。

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 にパッチをインストールします。
2.	Flow Collector 5000 シリーズ データベース	エンジンの更新を開始する前に、データベースがパッチのインストールを完了し、アプライアンスのステータスが [アップ (Up)] と表示されていることを確認してください。
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 データベースがパッチのインストールを完了し、アプライアンスのステータスが [アップ (Up)] と表示されていることを確認してください。

		クラスタ内の次のアプライアンスにパッチをインストールする前に、エンジンがパッチのインストールを完了し、アプライアンスのステータスが[アップ(Up)]と表示されていることを確認してください。
4.	その他のすべての Flow Collector (NetFlow および sflow)	クラスタ内の次のアプライアンスにパッチをインストールする前に、Flow Collector がパッチのインストールを完了し、アプライアンスのステータスが[アップ(Up)]と表示されていることを確認してください。
5.	エンドポイント コンセントレータ	クラスタ内の次のアプライアンスにパッチをインストールする前に、エンドポイント コンセントレータがパッチのインストールを完了し、アプライアンスのステータスが[アップ(Up)]と表示されていることを確認してください。
6.	Flow Sensor	

1. [アップデートマネージャ (Update Manager)] > [システムの更新 (System Updates)] セクションに戻ります。
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:** アプライアンスが自動的に再起動します。

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



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

5. インストールの確認:

- アプライアンスの [アクション (Actions)] メニューをクリックします。

-
- [更新ログの表示 (View Update Log)] を選択します。
 - パッチが「正常」または「インストール済み」として表示されていることを確認します。パッチが失敗した場合、エラーを修正して再度試行してください。詳細については、「[エラーのトラブルシューティング](#)」を参照してください。
6. [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。
7. 手順 1 ~ 6 を繰り返して、各アプライアンスにロールアップパッチを順番にインストールします。
8. この更新用に他のパッチが提供されている場合は、それらをインストールしてからソフトウェアアップデートに進みます。

8. v7.3.0 ソフトウェアアップデートのインストール

ソフトウェアアップデートでは、引き続き [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)	<p>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。</p> <p>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。</p>
2.	Flow Collector 5000 シリーズ データベース	<p>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。</p> <p>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。</p>
3.	Flow Collector 5000 シリーズ エンジン	<p>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。</p> <p>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。</p>
4.	その他のすべての Flow Collector (NetFlow および sflow)	<p>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</p>

		<p>あることを確認してください。</p> <p>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。</p>
5.	エンドポイント コンセントレータ	
6.	セカンダリ SMC (使用する場合)	<p>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。</p> <p>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。</p> <p>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。この場合は、「11. 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。</p>
7.	プライマリ SMC	<p>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。</p> <p>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。</p> <p>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。この場合は、「11. 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。</p>
8.	Flow Sensor	<p>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。</p>

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:** 7.2.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。
- **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。

ソフトウェアアップデートのインストール

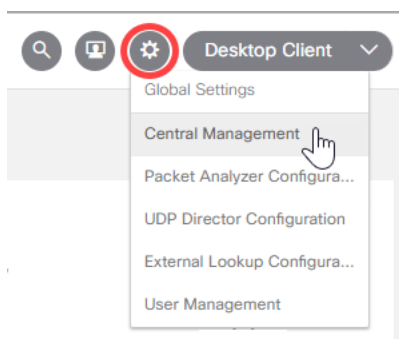
次の手順に従って、[集中管理 (Central Management)] 内のアプライアンスにソフトウェアアップデートをインストールします。



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 キーを押します)
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 v7.2.1 (または最新バージョンの 7.2.x) がインストールされていることを確認します。

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
Endpoint Concentrator	20	.20	8 days ago	7.2.1	-		
Flow Sensor	2	.22	8 days ago	7.2.1	-		
SMC	c24	.24	2 hours ago	7.2.1	-		
Flow Collector	5	.25	4 hours ago	7.2.1	-		
UDP Director		.94	8 days ago	7.2.1	-		

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)]: 7.3.0 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、または設定チャン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。

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、v7.3.0 ソフトウェアアップデートが表示されていることを確認します。

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
Endpoint Concentrator	20	.20	2 hours ago	7.3.0	-		
Flow Sensor	2	.22	4 hours ago	7.3.0	-		
SMC	c24	.24	2 hours ago	7.3.0	-		
Flow Collector	5	.25	4 hours ago	7.3.0	-		
UDP Director		.94	2 hours ago	7.3.0	-		

- [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 7.3.0 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
<p>[更新のインストール (Install Update)] ボタンは使用できません。</p>	<p>[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。</p> <p>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。</p> <ul style="list-style-type: none"> 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。
<p>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</p>	<p>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。</p> <p>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。</p>
<p>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)</p>	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 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)。

エラーの説明またはカテゴリ	詳細
	<ul style="list-style-type: none"> • 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)。 • その他の情報:手順については、「6. 使用可能なディスク容量の確認」を参照してください。
<p>予 期 せぬ終了ステータス (Unexpected exit status!)</p>	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。
<p>アップロードに失敗しました (Upload Failed)</p>	<p>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。</p> <p>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。手順については、「8. v7.3.0 ソフトウェアアップデートのインストール」を参照してください。</p>



エラーを解決できない場合は、[Cisco Stealthwatch サポート](#)に連絡してください。

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. 次のアプライアンスに対し、この「[ソフトウェアアップデートのインストール](#)」セクションの手順をすべて繰り返します。アプライアンスは順番に更新してください。
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、「[9. v7.3.0 パッチのインストール](#)」を参照してください。

9. v7.3.0 パッチのインストール

システムを 7.3.0 に更新したら、「[7. パッチのインストール](#)」手順を使用して、次の必須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。

- patch-smc-ROLLUP001-7.3.0-01.swu 以降
- patch-fcnf-ROLLUP001-7.3.0-02.swu 以降
- patch-fcsf-ROLLUP001-7.3.0-02.swu 以降

このガイドの手順に従い、Cisco Software Central (<https://software.cisco.com>) でパッチの ReadMe の手順を確認します。

10. 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。
- データストアを展開する場合は、Stealthwatch Web アプリケーションを使用して Stealthwatch インストールをモニタおよび設定します。Stealthwatch デスクトップクライアントは データストア と互換性がありません。


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。

- SMC にログインします。
- [ダウンロード (Download)] アイコンをクリックします。



- .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。
- 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。
- 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。
- SMC ユーザ名およびパスワードを入力します。
- SMC サーバ名または IP アドレス (IPv4 または IPv6) を入力します。
- 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. SMC にログインします。
2. [ダウンロード(Download)] アイコンをクリックします。



3. .dmg ファイルをクリックして、インストール プロセスを開始します。

アイコンとフォルダは、以下に示すようにモニタに表示されます。



4. 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。

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

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。

11. SMC フェールオーバーロールの確認

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。

SMC フェールオーバー設定を使用しない場合、Stealthwatch の更新は完了です。

⚠ 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。

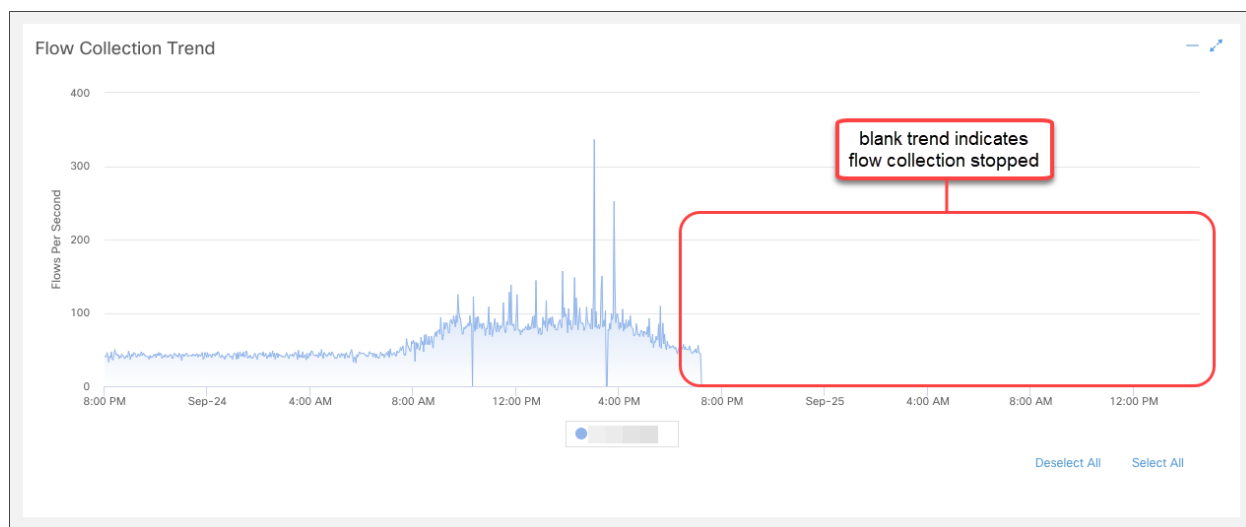
1. 管理者ユーザとしてセカンダリ SMC にログインします。
2. [グローバル設定 (Global Settings)] アイコンをクリックします。
3. [SMC 設定 (SMC Configuration)] を選択します。
4. [フェールオーバー設定 (Failover Configuration)] タブをクリックします。
5. フェールオーバーロールがセカンダリとして表示されていることを確認します。

The screenshot shows the 'SMC Configuration' page with the 'Failover Configuration' tab selected. A blue informational banner at the top states: 'Make sure you add all required certificates to your Stealthwatch Management Console (SMC) Trust Stores. Also, configure the secondary SMC before the primary SMC. For instructions, please refer to [Stealthwatch Help](#)'. Below this, the 'Failover Role' dropdown menu is highlighted with a red box and is set to 'Secondary'. At the bottom, the 'Other SMC' section displays 'IP Address' as 141 and 'Failover Role' as Primary.

6. プライマリ SMC にログインします。手順 2 ～ 4 に従って、フェールオーバーロールがプライマリとして表示されることを確認します。
7. 両方の 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 Failover Configuration Guide](#)』での設定の順序と手順に従ってください。

i 手順については、『[Stealthwatch Failover Configuration Guide](#)』を参照してください。

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



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

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

11. プライマリ SMC にログインします。

12. [集中管理 (Central Management)] > [アプライアンス マネージャ (Appliance Manager)] を確認します。セカンダリ 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。

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

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL: <https://www.cisco.com/go/trademarks> をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)