

Stealthwatch® システムのバージョン 6.10.x から 6.10.3 への更新ガイド

このガイドは、次のステルスウォッチ アプライアンスを v6.10.x から V6.10.3 に更新する際に参照してください。

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

V6.10.3 の詳細については、[リリースノート](#)を参照してください。

重要： お使いのアプライアンスにバージョン 6.9.x がインストールされている場合は、『[Stealthwatch システムのバージョン 6.9.x から 6.10.3 への更新ガイド](#)』を使用してアプライアンスを更新してください。このガイドは使用しないでください。

注意！

- 更新すると、新しくインストールされた機能をサポートするためにデータ構造や構成に変更が加えられるため、バージョンのダウングレードはサポートされません。
- システムを更新する前に、設定をバックアップし、このガイドで説明されている手順に従って診断パックを作成してください。フローコレクタと SMC のデータベースのバックアップも強く推奨します。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。また、診断パックはトラブルシューティングが必要になった場合に役立ちます。
- SMC とフローコレクタは、更新のプロセスを開始する前に **1 時間以上 7 日未満**連続して実行されている必要があります。この条件が満たされていない場合、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。
- 次の順序でアプライアンスを更新することが重要です。すべての UDP Director(別名 FlowReplicator)、フローコレクタ 5000 シリーズ データベース、フローコレクタ 5000 シリーズ エンジン、その他すべてのフローコレクタ(NetFlow および sFlow)、Cloud License コンセントレータ、エンドポイント コンセントレータ、続けてセカンダリ SMC、プライマリ SMC、最後に Flow Sensor。

重要：

- 更新プロセスが完了すると、アプライアンスは自動的に再起動します。再起動プロセス中は、新しいデータは収集されません。ただし、現在のデータは保持されます。
- セキュリティ向上のため、新しいバージョンの openSSL を TLS 1.2 で使用できるよう、**IDentity**

1000/1100 アプライアンスを v3.3.0.x に更新することをおすすめします。

- ステルスウォッチ アプライアンスの NTP 設定を確認し、サーバー一覧の中に 130.126.24.53 の NTP サーバがあれば削除してください。このサーバには問題があることが判明しており、Cisco 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。

(注)

- このガイドにおいて、「アプライアンス」という語は Stealthwatch Flow Sensor Virtual Edition(VE) を含むあらゆる Stealthwatch 製品を指して使用されます。
- StealthWatch システムには、Java バージョン 8 Update 161(v1.8.0_161) 以降が必要です。
- 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、Customer Community で [ハードウェアおよびバージョンのサポート一覧表](#) をご覧ください。

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。

画像

このガイドで使用される画像は基本的にフローコレクタ NetFlow VE の管理インターフェイスのものです。これは全アプライアンスの代表例として使用されています。特に記載がない限り、アプライアンスの更新手順はすべて同じです。

更新の前に: 確認事項

更新プロセスを開始する前に、次の各項目を確認してください。


更新に最適な時間

通常、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。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。

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すすめします。フローコレクタが更新され、実行されると、SMC に送信されるデータはコレクタでキャッシュされ、SMC が更新されるまで保持されます。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。

注意! SMC クライアント インターフェイスからフロー コレクタ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。

設定

更新プロセスの実行中は、SMC とフロー コレクタ間の通信が停止します。通信が停止すると、SMC クライアント インターフェイスの企業 ツリーのフロー コレクタ アイコンに赤い「x」が表示され、管理対象のアプライアンスのアイコンが緑からオレンジ色に変わります()。

さらに、Stealthwatch Flow Sensor を使用している場合は、SMC クライアント インターフェイスのアラーム テーブルにフロー センサー 管理 チャネル ダウン アラームが表示されます。更新が完了すると通信が再確立されてアイコンは通常に戻り、アラームは表示されなくなります。

ブラウザのショートカット

ブラウザのショートカットを使用してステルスウォッチ アプライアンスの管理 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そのショートカットが機能しないことがあります。その場合、一度ショートカットを削除してから作成し直してください。

代替アクセス

警告!

今後必要になった場合に備えて、次のいずれかの手順を使ってステルスウォッチ アプライアンスにアクセスする別の方法を有効にしておくことは重要です。

ハードウェア*

- **コンソール(コンソールポートへのシリアル接続)** : ラップトップや、キーボードとモニタを使用してアプライアンスに接続する方法については、最新の Stealthwatch ハードウェア インストール ガイドを参照してください。 <https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html>
- **iDRAC Enterprise(Dell アプライアンス)** : www.dell.com で、お使いのプラットフォームの最新ドキュメントを参照してください。iDRAC Enterprise にはライセンスが必要です。また、iDRAC Express でコンソール アクセスはできません。iDRAC Enterprise をお持ちでない場合は、コンソールまたは SSH での直接接続をお使いください。
- **CIMC(UCS アプライアンス)** : 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 Cisco UCS ガイドを参照してください。

仮想マシン*

- **コンソール(コンソールポートへのシリアル接続)** : インストールされているアプライアンスに関する KVM または VMware の最新ドキュメンテーションを参照してください。
 - たとえば、KVM をお使いの場合は、<https://virt-manager.org/> で Virtual Manager のドキュメンテーションを参照してください。
 - VMware をお使いの場合は、<https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.vcsa.doc/GUID-223C2821-BD98-4C7A-936B-7DBE96291BA4.html> で vSphere での vCenter Server アプライアンス管理インターフェイスのドキュメンテーションを参照してください。

*これらの方法を使用してアプライアンスにログインできない場合は、アプライアンスのネットワークインターフェイスで一時的に SSH を有効にできます。

警告! SSH を有効にすると、システムの侵害リスクが増加します。SSH は必要な場合のみ有効にすることが重要です。SSH は、使用終了後に無効にします。

1. アプライアンス管理インターフェイスにログインします。
SMC : SMC にログインします。[設定 (Settings)] アイコン > [アプライアンスの管理 (Administer Appliance)] をクリックします。
2. [構成 (Configuration)] > [サービス (Services)] をクリックします。
3. SSH を有効化するには、[SSH を有効にする (Enable SSH)] チェックボックスをオンにします。
ルート ユーザによる SSH アクセスを許可するには、[ルート SSH アクセスの有効化 (Enable Root SSH Access)] チェックボックスをオンにします。
4. [適用 (Apply)] をクリックします。

更新プロセス

注意! 更新を実行するときには、このガイドで説明されている順序でシステム全体を更新する必要があります。そうしないと、システムは、不明な状態のままになる可能性があります。

重要: 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 を更新する前に、セカンダリ SMC を更新します。更新が完了すると、両方の SMC がセカンダリ権限で再起動される場合があります。この場合、管理者ユーザとして SMC クライアント インターフェイスにログインし、プライマリ SMC をリセットしてプライマリフェールオーバー権限にします。両方の SMC が更新されるまでは、フェールオーバー権限を変更しないでください。

(注)

- Flow Sensor のみを使用している場合、この手順を使用して Flow Sensor のみを更新できま

す。

- フローコレクタ 5000 シリーズ エンジンを更新する前に、フローコレクタ 5000 シリーズ データベースを更新する必要があります。すべてのフローコレクタは、SMC を更新する前に更新する必要があります。

更新を正常に完了し、データ損失を最小限に抑えるには、このガイドのすべての手順を以下の順序で実行します。

1. [ステルスウォッチ アプライアンスの現在のバージョンが 6.10.x であることを確認する](#)。
2. [更新するステルスウォッチ アプライアンス用の更新ファイルを取得する](#)。
3. [アプライアンスの構成をバックアップする](#)。
4. [アプライアンスの診断パックを作成する](#)。
5. [アプライアンスデータベース\(フローコレクタおよび SMC\)をバックアップし利用可能なディスク容量を確認する](#)。
6. [アプライアンスを再起動してすべてのプロセスが正常な状態にあることを確認し、1 時間待つ](#)。
7. [アプライアンスを更新する](#)。SMC の[システム管理 (System Management)] ページを使用して、各アプライアンスを更新する。SMC で管理されていないアプライアンスの場合は、アプライアンス管理インターフェイスを使用します。
8. [更新を確認する](#)。
9. システム内の次のアプライアンスについて、この手順を繰り返します。最良の結果を得るには、次に示す順序で、これらの手順を各アプライアンスに対して実行してください。
 - すべての UDP Director(別名 FlowReplicator)
 - フローコレクタ 5000 シリーズ データベース
 - フローコレクタ 5000 シリーズ エンジン
 - その他あらゆるフローコレクタ(NetFlow や sFlow)
 - Cloud License コンセントレータ: アプライアンス管理から更新
 - エンドポイント コンセントレータ: アプライアンス管理から更新
 - セカンダリ SMC(使用している場合)
 - プライマリ SMC
 - すべての Flow Sensor

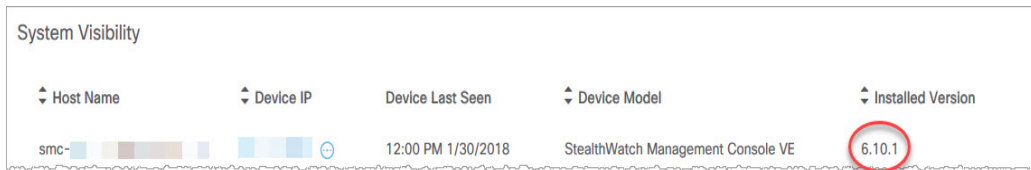
アプライアンスの現在のバージョンの確認

アプライアンスの現在のバージョンを確認するには、SMC Web アプリケーション インターフェイスで [システム管理 (System Management)] ページに移動します。[システム管理 (System Management)] ページに表示されない他のアプライアンスについては、現在のバージョンを確認するための以前の操作と同様、アプライアンス管理インターフェイスにアクセスします。

以下の手順を実行し、更新するすべてのアプライアンスの現在のソフトウェアのバージョンが6.10.1 または 6.10.2 であることを確認します。

1. SMC ダッシュボード ページに移動します。
2. [設定 (Settings)] アイコンをクリックして、[システム管理 (System Management)] を選択します。

[システム管理 (System Management)] ページが開きます。



3. エンドポイント コンセントレータを更新しますか。
 - 「はい」の場合、次の手順に進みます。
 - 「いいえ」の場合、このガイドの次のセクション「[更新ファイルの取得](#)」に進みます。
4. エンドポイント コンセントレータでは、そのアプライアンス管理 インターフェイスのログイン ページ([https://\[IP アドレス\]](https://[IP アドレス])) に移動します。右側の例で示すように、現在のソフトウェアのバージョンはアプライアンス名の下に表示されます。
5. 現在のバージョンは6.10.1 または 6.10.2 ですか。
 - 「はい」の場合、他のすべてのアプライアンスが同じバージョンで、最新のパッチ ロールアップが適用されていることを確認します。確認できたら、次の手順に進みます。
 - 「いいえ」の場合は、『[Stealthwatch System Version 6.9.x to 6.10.3 Update Guide](#)』を使用する必要があります。
6. このガイドの次のセクション「[更新ファイルの取得](#)」に進みます。

更新ファイルの取得

更新するすべてのアプライアンスの現在のソフトウェアのバージョンがv6.10.x であることが確認できたら、次の手順を実行してソフトウェア更新 (SWU) ファイルを取得します。

1. <https://stealthwatch.flexnetoperations.com> に移動します。Download and License Center のログイン ページが開きます。

Download and License Center

Welcome to Lancope's Download and License Center!

If you have a license token and this is your first time visiting this site, click [Register License Token](#) to set up your account. After setting up your account, log out and click [Password Finder](#) to define your password.

If you already have an account, please log in below.

Login ID

Password

Remember my password until I logout

If you have forgotten your login ID or password, or are not sure whether you have an account, click [Password Finder](#). For other assistance, click [Support](#).

(注) 初めてパスワードを設定する場合や、ログイン ID またはパスワードを忘れてしまった場合は、[パスワードを忘れた場合 (Password Finder)] リンクをクリックして画面の指示に従ってください。

2. ログイン ID とパスワードを該当するフィールドに入力し、[ログイン(Login)] をクリックします。製品ホームページが開きます。
3. [ソフトウェアアップデート (Software Updates)] セクションで、該当する Stealthwatch リリースのリンクをクリックします。[製品検索 (Product Search)] ページが開き、選択したリリースに関連付けられているすべてのダウンロード可能ファイルのリストが表示されます。
4. 以下の表を確認して適切な更新 (SWU) ファイルを見つけたら [ダウンロード (Download)] をクリックします。

(注)

- 各種類のアプライアンスに提供されている更新ファイルは 1 つだけです。その更新ファイルで仮想 (VE) アプライアンスと物理アプライアンスの両方に対応します。
- SWU ファイルのファイルサイズを確認します。その数値を使用して、更新に十分なディスク容量がアプライアンス上にあることを確認します。

重要: アプライアンスのソフトウェアアップデート ファイルを個別にダウンロードしてインストールします。ファイルサイズや Web アプリケーションの制限があるため、ソフトウェア更新ファイルの圧縮やバンドリングは推奨されません。

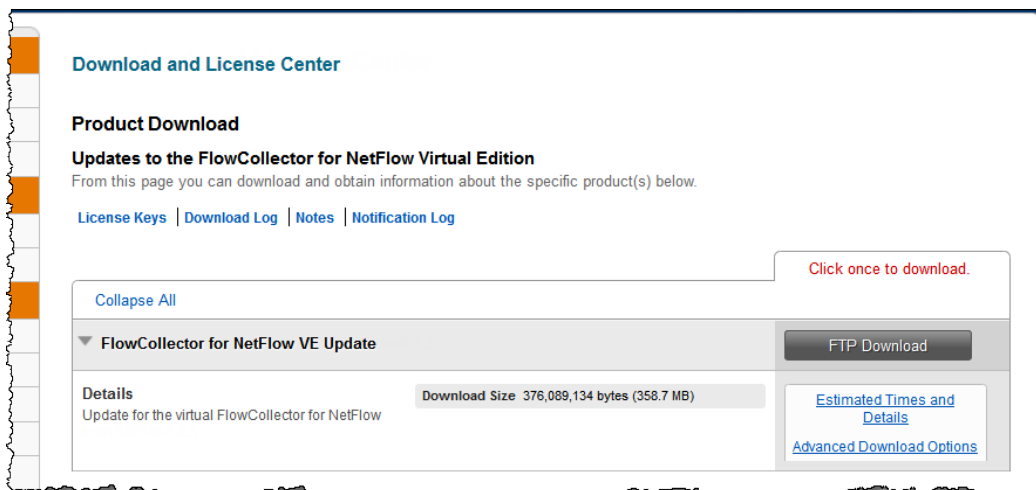
アプライアンス	更新ファイル名
システム更新ファイル (SMC、フローコレクタ、Flow Sensor、UDP Director/FlowReplicator 用)	system-upmanrepo-6.10.3-RC3-01.swu
NetFlow 向けフローコレクタ	update-fcnf-6.10.3.2018.08.08.1941-

アプライアンス	更新ファイル名
(フローコレクタ 5000 シリーズ エンジンに必要) NetFlow VE 向けフローコレクタ	01.swu
sFlow 向けフローコレクタ sFlow VE 向けフローコレクタ	update-fcsf-6.10.3.2018.08.08.1941-01.swu
フローコレクタ 5000 シリーズ データベース	update-fcdb-6.10.3.2018.08.08.1937-01.swu
SMC および SMC VE	update-smc-6.10.3.2018.08.08.1941-01.swu
Flow Sensor アプライアンス Flow Sensor VE	update-fsuf-6.10.3.2018.08.08.1936-01.swu
UDP Director (別名 FlowReplicator) UDP Director VE (別名 FlowReplicator VE)	update-udpd-6.10.3.2018.08.08.1936-01.swu
エンドポイント コンセントレータ	update-ec-6.10.3.2018.08.08.11937-01.swu

[[エクスポートに関するコンプライアンス\(Export Compliance\)](#)] ページが開きます。



5. [同意します(I Agree)] をクリックします(他のコンプライアンス ページやライセンス契約が開いた場合も同様に同意します)。選択したファイルの[製品のダウンロード(Product Download)] ページが表示されます。



(注) 各項目の横にある下向き矢印をクリックすると、ソフトウェアの詳細を確認できます。

6. [FTPでダウンロード (FTP Download)] をクリックします。SWU ファイルを保存するオプションのダイアログが表示されます。
7. 任意の場所にファイルを保存します。
8. 別の更新ファイルをダウンロードする必要がありますか。
 - 「はい」の場合、左側のナビゲーション ウィンドウで [製品 ホーム (Product Home)] をクリックし、手順 3～7 を繰り返します。
 - 「いいえ」の場合、左側のナビゲーション ウィンドウの下部にある [ログアウト (Logout)] をクリックします。
9. このガイドの次のセクション「[アプライアンスの構成のバックアップ](#)」に進みます。

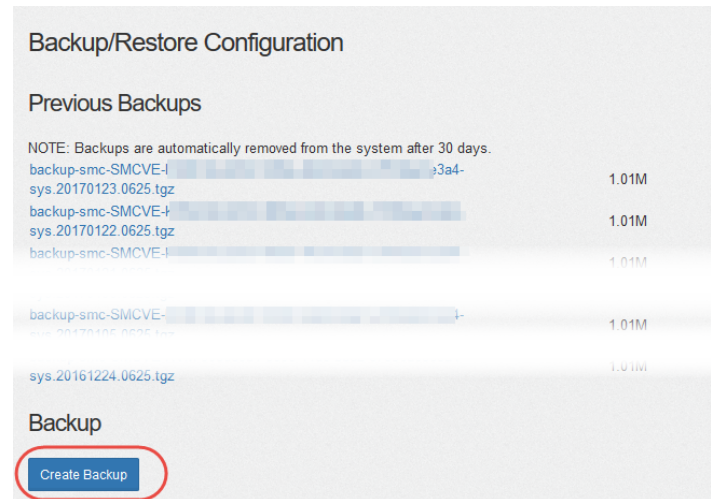
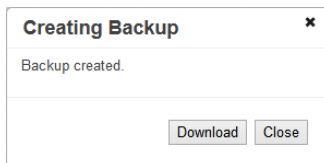
アプライアンスの構成のバックアップ

次の手順を実行して構成をバックアップします。

注意! 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。ホームページが開きます。
2. ホームページに表示されている IP アドレスとホスト名を確認します。それが変更対象のアプライアンスであることを確認します。

3. [サポート (Support)] > [構成のバックアップ/復元 (Backup/Restore Configuration)] をクリックします。右側の例のように、[バックアップ/復元 (Backup/Restore)] ページが開きます。
4. [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。進行状況ウィンドウが開き、処理が終了したことを下の例のように示します。



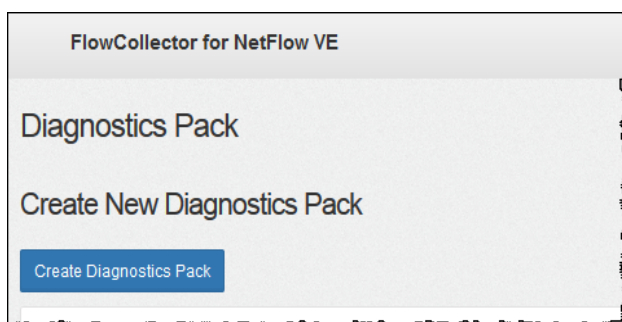
5. [ダウンロード (Download)] をクリックして、バックアップ (TGZ) ファイルを適当な場所に保存します。
6. [閉じる (Close)] をクリックして進行状況ウィンドウを閉じます。
7. このガイドの次のセクション「[診断パックの作成](#)」に進みます。

診断パックの作成

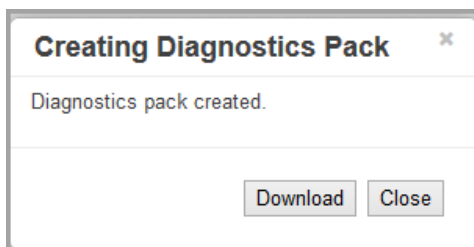
アプライアンスの構成をバックアップしたら、次の手順を実行して、更新するアプライアンスの診断パックを作成します。診断パックを作っておくと、トラブルシューティングが必要になった場合に役立ちます。

重要： 大規模なシステムでは、タイムアウトにより診断パックの生成が失敗することがあります。これに対処するには、アプライアンスのSSHコンソールを開き、doDiagPack コマンドを実行します。これにより、診断パックの生成時にタイムアウトを防ぐことができます。診断パックは /lancope/var/admin/diagnostics に格納されます。

1. [サポート (Support)] > [診断パック (Diagnostics Pack)] をクリックします。次の例のような [診断パック (Diagnostics Pack)] ページが表示されます。



2. [診断パックの作成 (Create Diagnostics Pack)] をクリックします。進行状況ウィンドウが開き、処理が終了したことを示します。



3. [ダウンロード (Download)] をクリックして、診断パック (GPG) ファイルを適当な場所に保存します。このプロセスに数分かかることがあります。
4. [閉じる (Close)] をクリックして進行状況ウィンドウを閉じます。
5. フローコレクタか SMC を更新しますか。
 - 「はい」の場合、このガイドの次のセクション「[フローコレクタまたは SMC のデータベースのバックアップ](#)」に進みます。
 - 「いいえ」の場合、「[ステルスウォッチ アプライアンスの更新](#)」に進みます。

フローコレクタまたは SMC のデータベースのバックアップ

フローコレクタまたは SMC の診断パックを作成したら、フローコレクタと SMC のデータベースをバックアップする必要があります。このプロセスでは、次の手順を実行します。

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

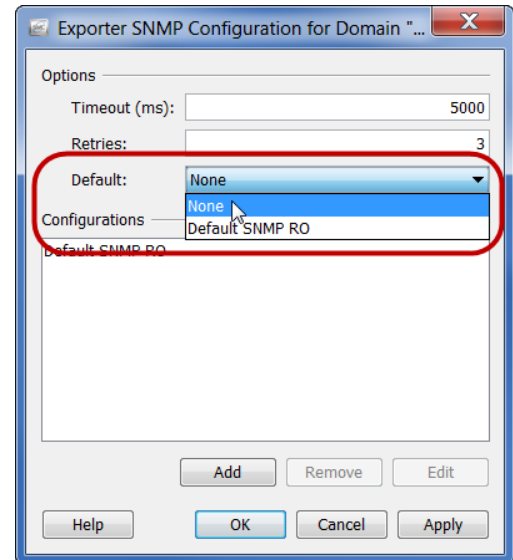
警告! バックアップを作成しない場合、更新プロセス中に問題が発生してもファイルを回復することはできません。

SMC の SNMP ポーリングを無効にする

データベースのバックアップは長時間を要することがあります。SNMP プロセスによりバックアップが中断されないようするため、SNMP ポーリングをオフにする必要があります。その後、バックアップが終了したら SNMP ポーリングを再び有効にします。

SNMP ポーリングを無効にするには、次の手順を実行します。

1. 管理者ユーザとして SMC クライアント インターフェイスを起動します(アプライアンス管理インターフェイスは閉じません)。
2. 企業ツリーでエクスポートをクリックし、[構成 (Configuration)] > [エクスポートのSNMP構成 (Exporter SNMP Configuration)] を選択します。右側の例で示すように、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)] フィールドの設定をメモします。データベースをバックアップした後で、この情報を再入力する必要があります。
4. [デフォルト (Default)] ドロップダウンリストから [なし (None)] を選択します。このドメインのSNMP ポーリングはオフになります。
5. [OK] をクリックします。
6. システム上の各ドメインについて手順 2 ~ 5 を繰り返します。



データベースをバックアップする

フローコレクタまたは SMC の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。

重要： リモート ファイルシステムには、データベースのバックアップを保存する十分な空き領域が必要です。このプロセスでは、毎分 0.5 ~ 2 GB 程度のデータがバックアップされます。データベースを 1 回バックアップすると、以後は前回バックアップからの変更点のみ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。

1. バックアップを開始する前に、**フローコレクタのデータベースをトリミング**することをおすすめします。これによりフローの保存に利用可能なディスク容量が解放され、データベースバックアップの所要時間が削減されます。手順については、[Customer Community](#) の投稿を参照してください。
2. アプライアンス管理インターフェイスに戻ります(SMC クライアント インターフェイスは閉じません)。
3. 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。

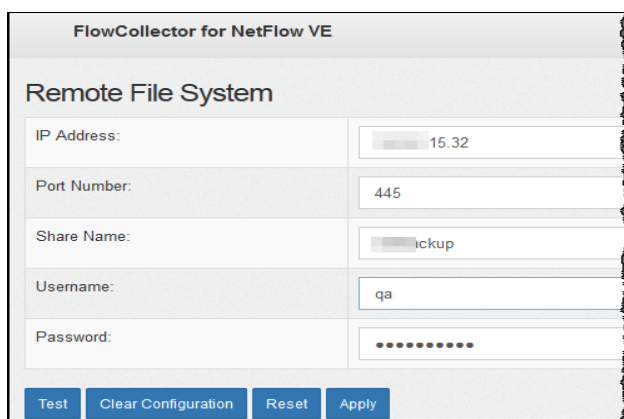
Disk Usage				
Name	Used	Size (byte)	Used (byte)	Available (byte)
/	37%	4.92G	1.68G	2.99G
/lancope/var	68%	37.03G	24.48G	11.79G

- a. [ホーム (Home)] をクリックします。ホームページが開きます。
- b. 例に示すように、[ディスク使用量 (Disk Usage)] セクションまで下にスクロールします。

- c. 右側の例で示すように、/lancope/var ファイルシステムの [使用 (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。

重要: さらに、ソフトウェア更新ファイル (SWU) のサイズの少なくとも 3 倍の容量が /lancope/var/ パーティション上にあることを確認してください。空き容量は [利用可能 (Available)] 列で確認できます。たとえば、ソフトウェア更新ファイル (Download and License Center から取得) が 6 GB の場合、パーティション上に 18 GB の空き容量が必要になります。これが SMC にアップロードされると、更新できる種類のデバイス用に SWU の展開が開始されます。展開処理中には、ギガバイト単位のスペースが追加で必要になります。展開が完了すると、SWU はファイルシステムから削除されます。アプライアンスのディスク容量を拡大する必要がある場合は、『[Stealthwatch Management Console VE and Flow Collector VE Installation and Configuration Guide](#)』の「Data Storage」セクションを参照してください。

4. [構成 (Configuration)] > [リモートファイルシステム (Remote File System)] をクリックします。次の例で示すように、[リモートファイルシステム (Remote File System)] ページが開きます。



5. 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。

(注) 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。

6. 完了したら、[適用 (Apply)] をクリックして設定ファイルに構成を保存します。

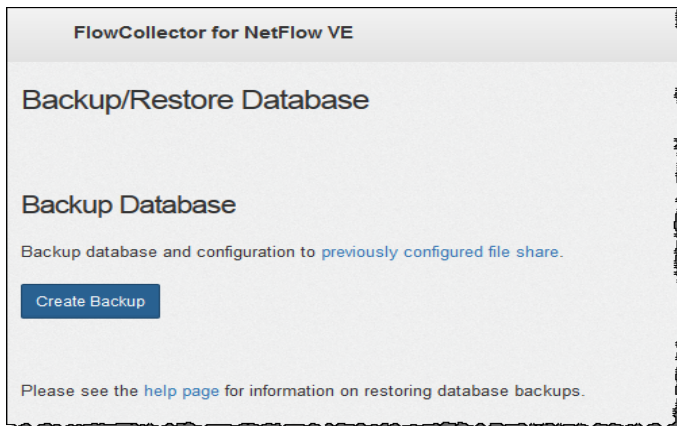
(注) パスワードを入力しても [適用 (Apply)] ボタンがクリックできるようにならない場合、[リモートファイルシステム (Remote File System)] ページの空白領域を 1 回クリックすると、ボタンをクリックできるようになります。

「変更を適用しています (Applying changes)」というメッセージが短時間表示され、設定が適用されます。

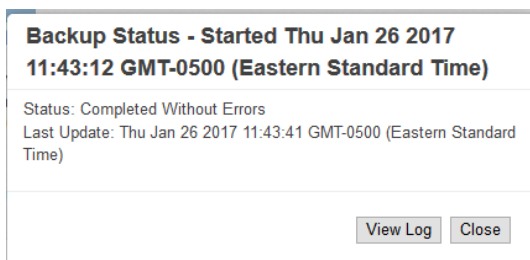
7. [テスト (Test)] をクリックして、ステルスウォッチ アプライアンスとリモート ファイルシステムが相互に通信できることを確認します。[テスト (Test)] をクリックして、ステルスウォッチ アプライアンスとリモート ファイルシステムが相互に通信できることを確認します。

File sharing appears to be properly configured.

- [サポート (Support)] > [バックアップ/データベースの復元 (Backup/Restore Database)] をクリックします。[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)。



- [バックアップの作成 (Create Backup)] をクリックします。経過表示ウィンドウが開き、ステータスが表示されます。データベースのサイズやバックアップの頻度によって、このプロセスには長時間かかる場合があります。バックアップのプロセスが完了すると、下の例のように別の進行状況ウィンドウが表示され、バックアップのプロセスが完了したことを示します。



重要: 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。

- 必要に応じて、[ログの表示 (View Log)] をクリックして、バックアッププロセスの詳細を確認します。
- [閉じる (Close)] をクリックして進行状況ウィンドウを閉じます。[データベースのバックアップ (Backup Database)] ページが更新され、バックアップの完了と経過時間が表示されます。

SMC で SNMP ポーリングを再度有効化する

SNMP ポーリングを再び有効化するには、次の手順を実行します。

- SMC クライアント インターフェイスに戻ります(アプライアンス管理インターフェイスは閉じません)。
- 適切なドメインを右クリックして [構成 (Configuration)] > [エクスポートのSNMP構成 (Exporter SNMP Configuration)] を選択します。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で、選択したドメインの以前の設定を選択します(このガイドの「SNMP ポーリングを無効にする」の手順 3 を参照)。このドメインの SNMP ポーリングが再度有効になりました。
4. [OK] をクリックします。
5. システム上の各ドメインについて、この手順の 2 ~ 4 を繰り返します。
6. SMC クライアント インターフェイスを閉じます。
7. このガイドの次のセクション「ステルスウォッチ アプライアンスの再起動」に進みます。

ステルスウォッチ アプライアンスの再起動

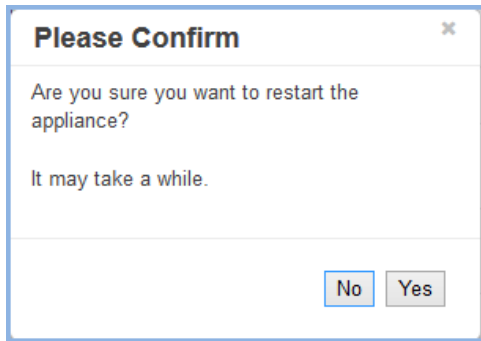
更新するステルスウォッチ アプライアンスを再起動するには、次の手順を実行します。再起動によりディスクチェックが行われるのに加え、すべてのプロセスが正常な状態で更新を開始するのに役立ちます。更新するすべてのアプライアンスに対してこの手順を実行してください。

重要: アプライアンスは、再起動中はデータを収集しません。そのアプライアンスのそれまでの稼働時間によって、再起動には数分から最長で 45 分程度かかります。

(注) SMC の場合は [管理者ユーザ (Admin User)] ドロップダウンリストをクリックし、[アプライアンスの管理 (Administer Appliance)] を選択します。次に、アプライアンス管理 インターフェイスに管理者ユーザとしてログインします。

1. 更新する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、管理者ユーザとしてログインします。右側の例で示すように、ホームページが開きます。
2. [操作 (Operations)] > [アプライアンスの再起動 (Restart Appliance)] をクリックします。次の例で示すように、確認ウィンドウが開きます。





3. [はい (Yes)] をクリックします。進行状況ウィンドウが開き、アプライアンスの再起動プロセスが開始されます。そのアプライアンスのそれまでの稼働時間によって、再起動には数分から最長で 45 分程度かかります。完了すると、アプライアンス管理インターフェイスのログイン ページが開きます。
4. このガイドの次のセクション「[ステルスウォッチ アプライアンスの更新](#)」に進みます。

ステルスウォッチ アプライアンスの更新

診断パックの作成 (およびフローコレクタまたは SMC のデータベースのバックアップ) が完了したら、次の手順を実行してステルスウォッチ アプライアンスを更新します。

アプライアンスの種類によって、更新には 2 つの方法があります。[システム管理 (System Management)] ページからはどちらの方法でも開始できますが、2 番目の方法を実行する場合は [アプライアンスの管理 (Appliance Admin)] ページにアクセスする必要があります。

1. SMC によって管理されているアプライアンス (SMC、フローコレクタ、UDP Director/FlowReplicator、Flow Sensor) の場合は、SMC の [システム管理 (System Management)] ページを使用します。次のセクション「[\[システム管理 \(System Management\)\] ページからステルスウォッチ アプライアンスを更新する](#)」に進みます。
2. 他のすべてのアプライアンスの場合は、対応するアプライアンス管理インターフェイスにアクセスする必要があります。

重要:

- SMC とフローコレクタは、このセクションで説明する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。この条件が満たされていない場合、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。SWU ファイルには安全チェックがあるため、システムが再起動されて一定以上の時間が経過し、プロセスがこの段階に到達しないと更新プロセスを開始できません。アップグレード プロセスでこの段階に到達するまでに 6 日以上を必要とした場合、このセクションで説明する更新プロセスを開始する前にもう一度システムを再起動して 1 時間待機する必要があります。
- 更新プロセスが完了すると、ステルスウォッチ アプライアンスは自動的に再起動します。アプライアンスは、再起動プロセス中にはデータの収集を行いません。再起動は通常 10 分程度で完了します。

[システム管理 (System Management)] ページからステルスウォッチ アプライアンスを更新する

[システム管理 (System Management)] ページを使用して、そのページに表示されているすべてのアプライアンスに更新をインストールできます。

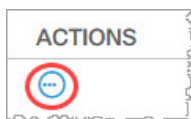
重要:

- UDP Director(別名 FlowReplicator) が高可用性 (HA) クラスタとして構成されている場合は、最初にセカンダリUDP Director を更新します。更新を確認し、完了してセカンダリUDP Director が再度起動したら、プライマリUDP Director を更新します。
- 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 を更新する前に、セカンダリSMC を更新します。

注: アプライアンスの更新は次の順序で実行する必要があります。

1. すべてのUDP Director(別名 FlowReplicator)
2. フローコレクタ 5000 シリーズ データベース
3. フローコレクタ 5000 シリーズ エンジン
4. すべてのNetFlow および sFlow フローコレクタ
5. Cloud License コンセントレータ: アプライアンス管理 インターフェイスから更新
6. エンドポイント コンセントレータ: アプライアンス管理 インターフェイスから更新
7. セカンダリSMC(使用している場合)
8. プライマリSMC
9. すべてのFlow Sensor

1. 必要に応じてSMCに再度ログインし、[管理 (Admin)] > [システム管理 (System Management)] をクリックして [システム管理 (System Management)] ページを開きます。
2. [更新ファイルのアップロード (Upload an Update File)] ボタンをクリックして、Download and License Center からダウンロードしたソフトウェア更新ファイル (SWU) を選択します。
3. [続行 (Continue)] をクリックします。アップロードの進行状況ウィンドウが表示されます。
4. SWU アプライアンスがアップロードされたら、[システムの可視性 (System Visibility)] セクションで目的のアプライアンスを探します。[インストール可能なバージョン (Version Ready to Install)] 列にソフトウェアのバージョンが表示されていることを確認します。
5. アプライアンスの [アクション (Action)] 列で、[アクション (Actions)] メニューをクリックします。[更新のインストール (Install Update)] をクリックします。



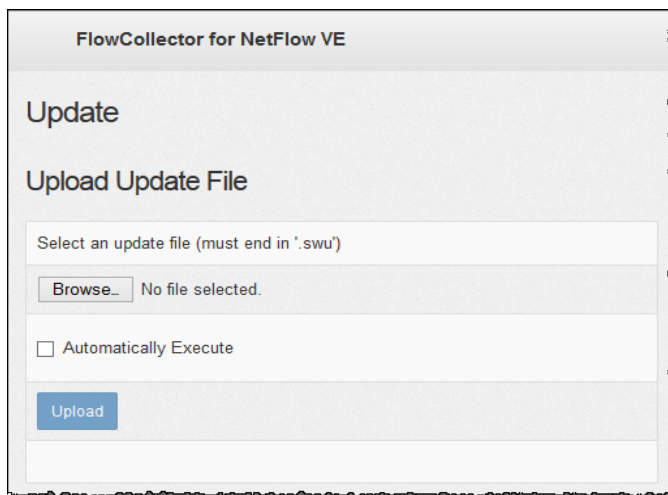
[更新ステータス (Update Status)] には、アプライアンスの更新中には更新中であることが、更新の完了後には結果 (成功/失敗) とその理由が表示されます。

6. [システム管理 (System Management)] ページに表示されているすべてのアプライアンスについて上の手順を繰り返します。
7. [システム管理 (System Management)] ページに表示されていない他のアプライアンスを使用していますか。
 - 「はい」の場合、「[アプライアンス管理 インターフェイスからステルスウォッチ アプライアンスを更新する](#)」に進みます。
 - 「いいえ」の場合、次の手順に進みます。
8. 次のセクションに進み、システム内の他のアプライアンスを更新します。

アプライアンス管理 インターフェイスからステルスウォッチ アプライアンスを更新する

[システム管理 (System Management)] ページに表示されていない各アプライアンスに対して、次の手順を実行します。

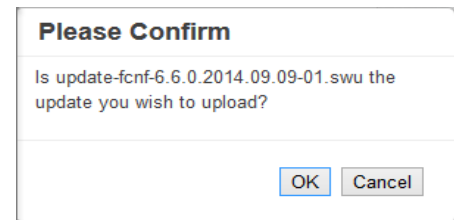
1. アプライアンス管理 インターフェイスにログインします。
2. [サポート (Support)] > [更新 (Update)] をクリックします。以前の更新が適用されている場合、それらの更新が一覧表示され、[ログの表示 (View Log)] リンクをクリックすると詳細を確認できます。



3. [アップデート ファイルをアップロードする (Upload Update File)] セクションで、[参照 (Browse)] をクリックします。
4. 前述の手順でダウンロードした更新 (SWU) ファイルに移動して選択し、開きます。[アップデート ファイルをアップロードする (Upload Update File)] フィールドにファイル名が表示され、[アップロード (Upload)] ボタンがアクティブになります。
5. [アップロード (Upload)] をクリックしたときにすぐ更新プロセスを自動的に開始しますか。
 - 「はい」の場合、[自動的に実行 (Automatically Execute)] チェックボックスを選択します。
 - 「いいえ」の場合 (つまり、更新プロセスを後で起動したい場合) は、[自動的に実行 (Automatically Execute)] チェックボックスをオフのままにします。
6. [アップロード (Upload)] をクリックします。確認ウィンドウが開き、選択したファイル名が表示されます。

7. 確認ウィンドウは正しい更新 (SWU) ファイル名を表示していますか。
 - はいの場合は [OK] をクリックして、ステップ 8 に進みます。
 - 正しくない場合、[キャンセル (Cancel)] をクリックして確認ウィンドウを閉じます。ステップ 2 に戻ります。
8. [自動的に実行 (Automatically Execute)] チェックボックスを選択しましたか。
 - はいの場合は、アップロード ステータスを示す経過表示ウィンドウが最初に表示され、次に更新ステータスが表示されます。手順 12 に進みます。
 - いいえの場合は、アップロード ステータスを示す経過表示ウィンドウが開きます。SWU ファイルに応じて、アップロード プロセスが完了するまでに最大 5 分かかる場合があります。アップロード プロセスが終了したら、[閉じる (Close)] をクリックして、進行状況ウィンドウを閉じます。[更新 (Update)] ページに [アップデート ファイルの実行 (Execute Update File)] セクションが表示されるようになったことを確認してください。手順 9 に進みます。
9. 更新プロセスを起動する準備ができたなら、[更新 (Update)] ページの [アップデート ファイルの実行 (Execute Update File)] セクションのドロップダウン ボックスを選択し、正しい更新ファイルを選択します。

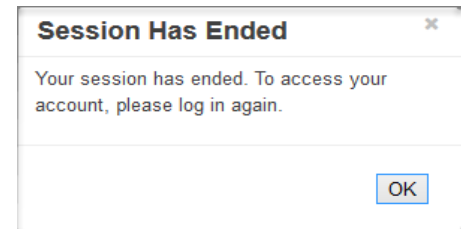
10. [適用 (Apply)] をクリックします。確認ウィンドウが開き、右側の例で示すように、選択したファイル名が表示されます。



11. 確認ウィンドウは正しい更新 (SWU) ファイル名を表示していますか。

- 受け入れる場合は、[OK] をクリックします。経過表示ウィンドウが開き更新ステータスが表示されます。次のステップに進みます。
- 正しくない場合、[キャンセル (Cancel)] をクリックして確認ウィンドウを閉じます。ステップ 2 に戻ります。

12. SWU ファイルおよびアプライアンスに応じて、更新プロセスが完了するまでに最大 30 分かかる場合があります。更新プロセスが完了すると、アプライアンスは自動的に再起動します。再起動プロセスが完了すると、右側の例で示すようにセッションタイムアウト メッセージが表示されます。



13. [OK] をクリックします。アプライアンス管理 インターフェイスのログインウィンドウが開き、次の例に示すように新しいソフトウェアのバージョンが表示されます。



The image shows the login page for Stealthwatch. At the top, it features the 'STEALTH WATCH' logo with 'By Lancope' underneath. Below the logo, it says 'FlowCollector for NetFlow VE' and '6.10.3'. There are two input fields: 'Username:' and 'Password:'. A blue 'Login >>' button is located at the bottom right of the form.

14. 次のセクション「[更新の確認](#)」に進みます。

更新の確認

アプライアンスが再起動してアプライアンス管理 インターフェイスのログイン ウィンドウが表示されたら、次の手順を実行して、更新が正しく行われたことを確認します。

1. admin ユーザとしてログインします。[更新 (Update)] ページが開きます。

(注) ページのロード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き、もう一度ログインします。

2. [最終更新ステータス (Last Update Status)] セクションで、更新が完了し、適用されたことを確認します(次の例を参照)。更新プロセスの詳細を表示するには、[ログの表示 (View Log)] リンクをクリックします。

Last Update Status			
Thu Aug 31 2017 13:03:51 GMT-0400 (Eastern Daylight Time)	Update completed.	Update has been successfully applied.	View Log

3. [ホーム (Home)] をクリックします。ホームページが開きます。
4. [バージョン (Version)] フィールドに新しいソフトウェアのバージョンが表示されていることを確認します(下図)。

System	
IP Address:	
Host name:	
Total Memory:	8G
Free Memory:	221.29M
Version:	6.10.3
Build:	2018.07.19.1330-0
Domain name:	
Load Average:	0.14, 0.14, 0.10
Uptime:	1 day, 04:30:22
Platform:	KVM Virtual Platform
Serial No.:	

5. 更新するアプライアンスは他にもありますか。

- 「はい」の場合、このガイドの「[更新プロセス](#)」に戻り、手順に従って次のアプライアンスですべての手順を繰り返します。
- 「いいえ」の場合、手順 6 に進みます。

6. [ログアウト (Logout)] をクリックし、ブラウザを閉じます。

7. 更新した SMC はフェールオーバー ペアのプライマリ SMC ですか。

重要： 両方の SMC が更新されるまでは、フェールオーバー権限を変更しないでください。

- 「はい」の場合、SMC は以前にプライマリフェールオーバー権限であったとしても、再起動後にセカンダリのフェールオーバー権限になっている可能性があり、そうするとセカンダリ SMC が 2 つになってしまいます。この場合、SMC クライアント インターフェイスに管理者ユーザとしてログインし、それぞれの SMC に目的のフェールオーバー権限を構成します。詳しくは、『SMC Client Online Help』を参照してください。
- 「いいえ」の場合、これで更新の確認は完了です。

おめでとうございます。システムの更新が完了しました。

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
- 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 : www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html
- Stealthwatch Customer Community の Web サイトからケースを送信
(<https://lancope.force.com/Customer/CustomerCommLogin>)

ドキュメント フィードバック

このドキュメントに関するコメントは、StealthWatch Customer Community の Web サイト (<https://lancope.force.com/Customer/CustomerCommLogin>) からお寄せください。ご協力をよろしくお願いいたします。

