Cisco Stealthwatch

更新ガイド 7.0.2

目次

はじめに

概要

このガイドは、次の Stealthwatch アプライアンスを v7.0.0 から v7.0.2 に更新する際に参照してください。

- 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）

v7.0.2 の詳細については、『リリース ノート』を参照してください。

対象読者

このガイドは、Stealthwatch 製品の更新を担当するネットワーク管理者とその他の担当者を対象としています。

用語

このガイドでは、Stealthwatch FlowSensor Virtual Edition（VE）などの仮想製品を含むすべての Stealthwatch 製品に対し「アプライアンス」という用語を使用しています。

「クラスタ」は、StealthWatch Management Console（SMC）で管理される Stealthwatch アプライアンスのグループです。アプライアンスが SMC によって管理されている場合は、Central Management 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。

考えられるルート パーティション スペースの不足

次の点に注意してください。

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

ソフトウェア バージョン

アプライアンスソフトウェアをバージョン 7.0.2 に更新するには、アプライアンスにバージョン **7.0.0** がインストールされている必要があります。このガイドの手順では、各アプライアンスのソフトウェア バージョンの確認方法について説明します。以下の点にも注意してください。

- アプライアンスのソフトウェアバージョンの段階的更新: たとえば、Stealthwatch v6.9.x を使用している場合は、各アプライアンスを v6.9.x から v6.10.x に更新してから、v6.10.x を v7.0.x に更新します。各更新ガイドは、Cisco.com で入手できます。
- 同一バージョン: すべてのアプライアンスが同じソフトウェアバージョンを使用していることを確認してください。たとえば、SMC に v7.0.0 がインストールされている場合、クラスタ内の他のアプライアンスには v7.0.0 がインストールされている必要があります。
- 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。

TLS

Stealthwatch には TLS v1.1 または 1.2 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。

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 > [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。
- ステータスを使用できません：セカンダリ SMC のライセンス ステータスが [ステータスを使用できません（Status Not Available）] と表示される場合があります。この状態は、プライマリ SMC とのフェールオーバー関係が原因で発生しますが、セカンダリ SMC の通信ステータスを表してはいません。ライセンスの詳細を表示するには、[ステータス（status）] ボタンをクリックします。
- ガイド：詳細については、ダウンロードおよびライセンスガイド [英語] を参照してください。

ISE または ISE-PIC

- 設定：SMC で ISE または ISE-PIC を使用している場合は、クライアントグループに適応型ネットワーク制御（ANC）が含まれていることを確認してから更新を開始してください。
- 確認：ISEクライアントにログインします。[管理（Administration）] > [pxGrid サービス（pxGrid Services）] の順に選択します。[SMC] > [クライアントグループ（Client Group）] 列を確認します。リスト内の各 SMC を確認します。

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

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

ホスト名

- 設定：各アプライアンスには固有のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは更新できません。
- 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 > [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 > [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：v7.0.2 では、各アプライアンスに少なくとも 1 台の NTP サーバが必要です。
- **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 > [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

v7.0.2 では、すべての Stealthwatch アプライアンスで協定世界時（UTC）が使用されます。

- 設定：更新を開始する前に、アプライアンスが UTC に設定されていることを確認します。
- 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。

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 > [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。SSL/TLS ID および信頼ストアの手順については、後続のヘルプページを参照してください。

- スタンドアロン アプライアンスの更新：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。更新された証明書をプロバイダーからインストールするには、[設定（Configuration）] > [SSL] を選択します。

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

信頼ストア

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

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

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

必要な信頼ストアに証明書を個別にアップロードしてください。

アプライアンスのバックアップ

Stealthwatch システムをバックアップするための時間を計画してください。バックアップファイルは、更新で問題が発生した場合に必要です。診断パックは、Cisco Stealthwatch サポートによるトラブルシューティング時に重要になります。

このガイドでは、次の手順について説明します。

- 各アプライアンスのバックアップ
- SMC データベースのバックアップ
- Flow Collector データベースのバックアップ
- 診断パックの作成

バックアップを作成しない場合、更新プロセス中に問題が発生してもファイルを回復することはできません。また、診断パックは、Cisco Stealthwatch サポートによるトラブルシューティングが必要な場合に役立ちます。

更新に最適な時間

ステルスウォッチ アプライアンスを更新するための時間とリソースを計画する際には、次の点を検討してください。

ソフトウェア アップデート ファイル

ソフトウェア アップデート ファイルのダウンロードには時間がかかります。ファイルは、ダウンロードおよびライセンスセンターから事前にダウンロードできます。

すべてのアプライアンス

- 時間：更新プロセスは、アプライアンスごとに完了するまで約 30 分かかります。ただし、ネットワークの状況によっては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。

- Flow Collector の更新期間：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。

  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。

  Flow Collector 5000 シリーズ：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。次に、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に [アップ（Up）] と表示されていることを確認してください。

通信

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

更新後

システムを v 7.0.2 に更新した後、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。

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

このガイドの手順に従い、Stealthwatch ダウンロードおよびライセンスセンター（Stealthwatch Download and License Center）にあるパッチの Readme ファイルに記載されている手順で詳細を確認してください。

代替アクセス

今後サービスが必要になった場合に備えて、次の手順に従い、ステルスウォッチ アプライアンスにアクセスする別の方法を有効にします。

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

ハードウェア

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

仮想マシン

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

Central Management 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。

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. [Central Management] > [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. クラスタの確認
2. インストールされているソフトウェア バージョンの確認
3. パッチファイルと更新ファイルのダウンロード
4. アプライアンスの設定のバックアップ
5. 診断パックの作成
6. Flow Collector と SMC データベースのバックアップ
7. 使用可能なディスク容量の確認
8. 更新ログのバックアップ
9. パッチのインストール
10. v7.0.2 ソフトウェア更新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。v7.0.2 SWU は、必ず更新順序を使用してインストールしてください。
11. ルートパーティションの確認
12. v7.0.2 パッチのインストール
13. Stealthwatch デスクトップ クライアント のインストール
14. SMC フェールオーバー ロールの確認
15. スタンドアロン アプライアンスを更新します。また、「Central Managementにおける管理対象およびスタンドアロンの要件」を参照して、更新が完了した後に Central Management にアプライアンスを追加する必要があるかどうかを判断してください。

1. クラスタの確認

次の手順を使用して、ステルスウォッチ アプライアンスを確認します。

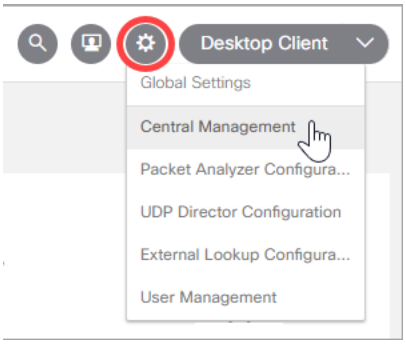
- Central Management：すべての Stealthwatch アプライアンスを Stealthwatch Management Console（SMC）で管理するように設定します。SMC の管理対象であるすべてのアプライアンスを確認するには、[Central Management] > [Appliance Manager] ページを参照します。アプライアンスを Central Management に追加するには、『Stealthwatch インストールおよびコンフィギュレーションガイド』を参照してください。
- SMC の最大数：この更新では 2 つの SMC を更新できます。
- スタンドアロン アプライアンス：管理対象外のままになるエンドポイントコンセントレータまたは別のアプライアンスがある場合は、管理対象アプライアンスに対する 7.0.2 更新の完了後に、このアプライアンスを更新できます。15. スタンドアロン アプライアンスの更新」を参照してください。

> ⚠ 更新プロセスの開始後は、アプライアンスの追加や削除、クラスタ設定の変更、またはアプライアンスのフェールオーバー ロールの変更は行わないでください。V 7.0.2 の更新が完了したら、スタンドアロン アプライアンスを Central Management に追加できます。

2. インストールされているソフトウェア バージョンの確認

各アプライアンスの現在のソフトウェアのバージョンが v7.0.0 であることを確認するには、以下の手順を実行します。

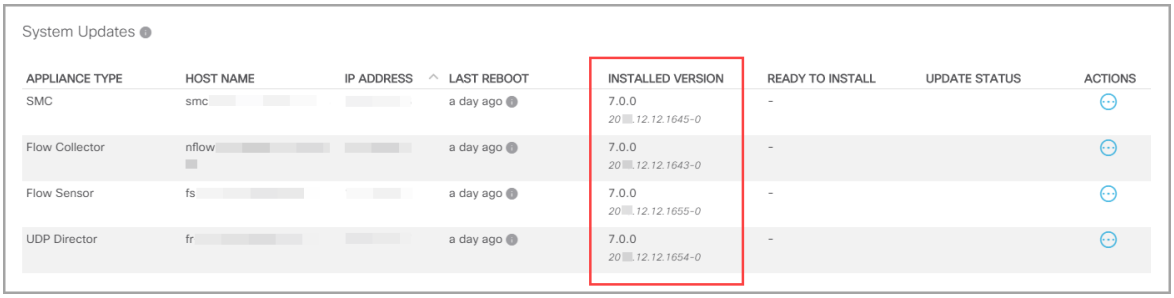
1. SMC にログインします。
   （ブラウザのアドレス フィールドに、https:// およびアプライアンスの IP アドレスを入力し、Enter キーを押します。）
2. [グローバル設定（Global Settings）] アイコンをクリックします。
3. [Central Management] を選択します。



4. [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 v7.0.0 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 v7.0.0 がインストールされている場合、クラスタ内の他のアプライアンスには v7.0.0 がインストールされている必要があります。

   6.10.x 以前：ソフトウェアのバージョンが6.10.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 7.0.0 に更新します。Stealthwatch システム更新ガイド（6.10.x から 7.0.0）[英語] を参照してください。

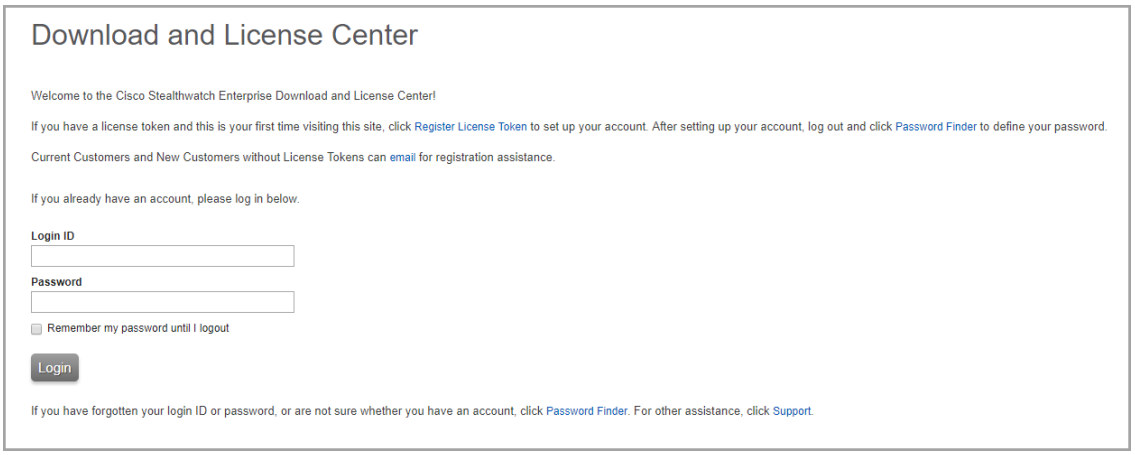


すべてのアプライアンスに正しいソフトウェア バージョンがインストールされていることを確認します。これは、更新を成功させるために不可欠な手順です。

3. パッチ ファイルとアップデート ファイルのダウンロード

次の手順を使用して、アカウントに記載されているパッチとv7.0.2 SWUをダウンロードします。

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



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

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

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

SWU ファイル

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

4. アプライアンスの設定のバックアップ

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

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

バックアップ設定ファイルの作成

次の手順に従って、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. [Central Management] > [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)]: 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 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、「6. 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。

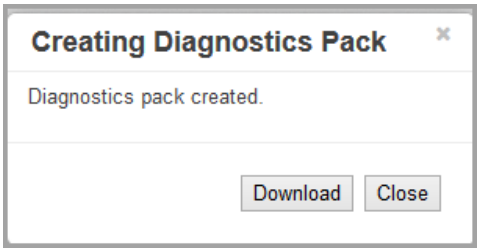
5. 診断パックの作成

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

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

1. 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。

6. Flow Collector とSMC データベースのバックアップ

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

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

このプロセスには、次の手順が含まれます。

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

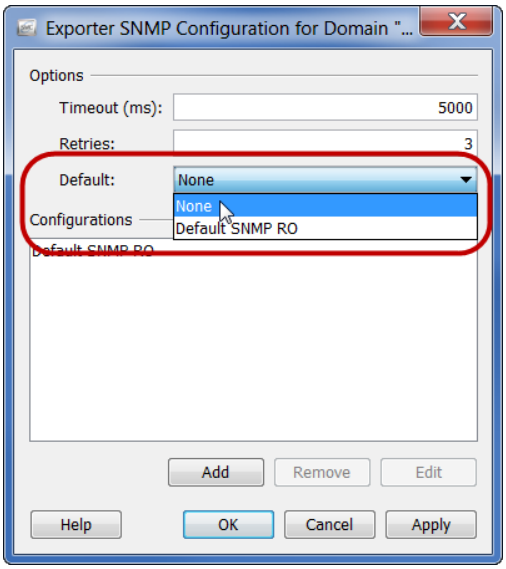
> バックアップしていないと、更新プロセス中に問題が発生した場合にファイルを回復できません。

SMC のSNMP ポーリングの無効化

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

SNMP ポーリングを無効にするには、次の手順を実行します。

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



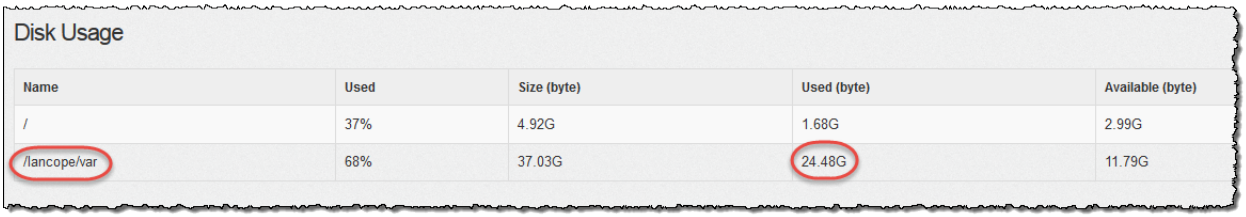
5. [デフォルト(Default)]ドロップダウンリストから[なし(None)]を選択します。このドメインの SNMP ポーリングがオフになりました。
6. [OK]をクリックします。
7. システム上のドメインごとに手順 2 ～ 6 を繰り返します。

データベースのバックアップ

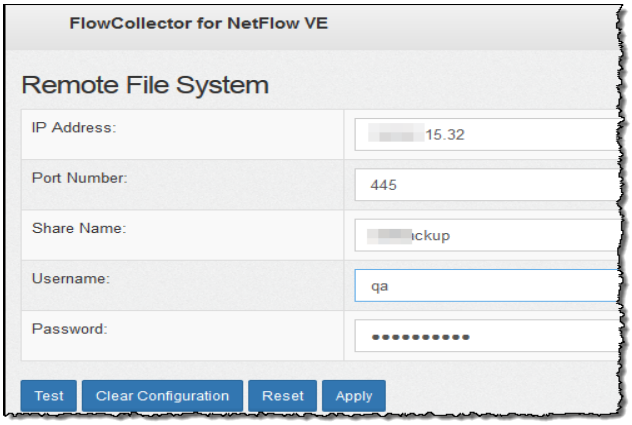
リモートファイルシステムに Flow Collector または SMC データベースをバックアップするには、次の手順を実行します。

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

1. アプライアンス管理インターフェイスに戻ります(ただし、デスクトップクライアントは閉じないでください)。
2. 次の手順を実行して、リモート ファイル システム上に必要となるデータベース バックアップ保存容量を確認します。
    - [ホーム(Home)]をクリックします。
    - [ディスク使用量(Disk Usage)]セクションを見つけます。
    - **/lancope/var** ファイルシステムの[使用済み(バイト)(Used(byte))]列を確認します。データベースのバックアップを保存するためには、リモートファイル システム上に少なくともこの数値にその 15% を足した分の空き容量が必要です。



3. [設定(Configuration)]>[リモートファイルシステム(Remote File System)]の順にクリックします。



4. バックアップファイルを保存するリモートファイル システムの設定を使用して、フィールドに入力します。

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

5. [適用(Apply)]をクリックして、設定ファイルに設定を適用します。

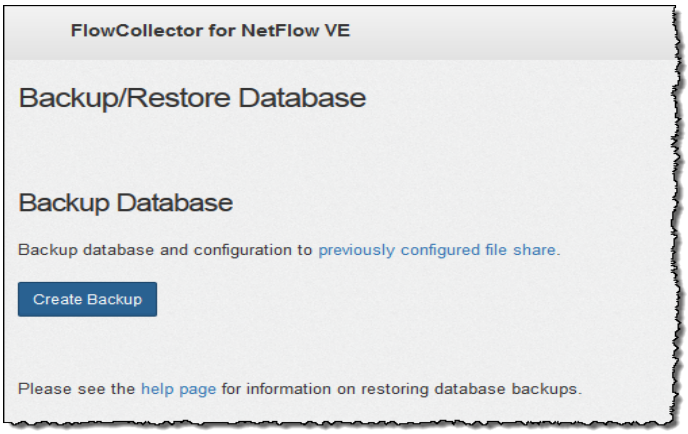
   パスワードを入力しても[適用(Apply)]ボタンが有効にならない場合、[リモートファイルシステム(Remote File System)]ページの空白部分を 1 回クリックすると有効になります。

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

   テストが完了すると、リモートファイル システムのページの下部に次のメッセージが表示されます。

   File sharing appears to be properly configured.

7. [サポート(Support)]>[データベースのバックアップおよび復元(Backup/Restore Database)]の順にクリックします。[データベースのバックアップ(Backup Database)]ページが開きます(次の例を参照)。



8. [Create Backup] をクリックします。このプロセスは長時間かかる場合があります。
   - バックアップ プロセスの開始後は、マウスをページから離してもプロセスは中断されません。ただし、バックアップの実行中に、[キャンセル(Cancel)] をクリックすると、アプライアンスを再起動しないとバックアップを再開できなくなる場合があります。
   - バックアップが完了するまで、画面に表示される指示に従います。
   - バックアッププロセスの詳細を確認するには、[ログの表示(View Log)] をクリックします。
9. [閉じる(Close)] をクリックして進捗状況ウィンドウを閉じます。

SMC でのSNMP ポーリングの再有効化

SNMP ポーリングを再度有効にするには、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。

7. 使用可能なディスク容量の確認

各アプライアンスのディスク容量をチェックして、ソフトウェアアップデート用の容量が十分にあることを確認します。

- **SMC**：SWU が Central Management の 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（Central Management）上に保持されます。

  たとえば、Central Management の 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。

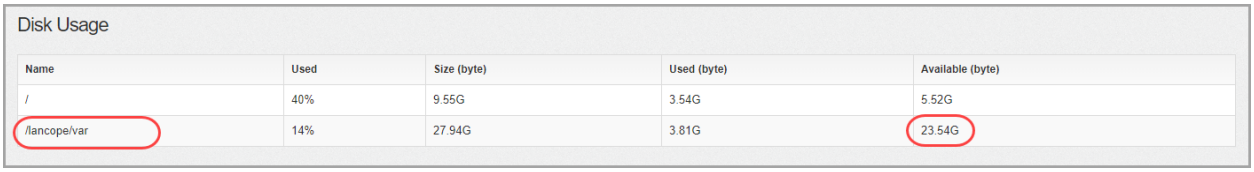
- 管理対象アプライアンス：Central Management の Update Manager を使用してアプライアンスを更新すると、更新が完了した後に SWU がアプライアンスのファイルシステムから削除されます。

  たとえば、Central Management の 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

1. アプライアンス管理インターフェイスにログインします。
2. [ホーム（Home）] をクリックします。
3. [ディスク使用量（Disk Usage）] セクションを見つけます。
4. [使用可能（バイト）（Available（byte））] 列を確認し、/lancope/var/ パーティションにソフトウェア アップデート ファイル（SWU）のサイズの 4 倍以上の空き容量があることを確認します。

   たとえば、ソフトウェア アップデート ファイル（ダウンロードおよびライセンス センターから取得）が 6 GB の場合、パーティションには 24 GB の空き容量が必要です。


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 v7.0 [英語] の「Data Storage」セクションを参照してください。

8. 更新ログのバックアップ

各アプライアンスの更新ログをバックアップするには、次の手順に従います。Stealthwatch クラスタ内のすべてのアプライアンスで更新ログのバックアップを作成してください。

1. アプライアンスに SSH 接続します。
2. root としてログインします。
3. 次のように入力します。

```
cp /lancope/var/admin/upgrade/upgradeOutput.log /lancope/var/
admin/upgrade/upgradeOutputHistory.log
```

4. Enter を押します。
5. アプライアンスを終了します。
6. Stealthwatch クラスタ内のすべてのアプライアンスでこの手順を繰り返します。

⚠ 次の手順「9. パッチのインストール。

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 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。

> パッチをインストールする前に、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。

ベスト プラクティス

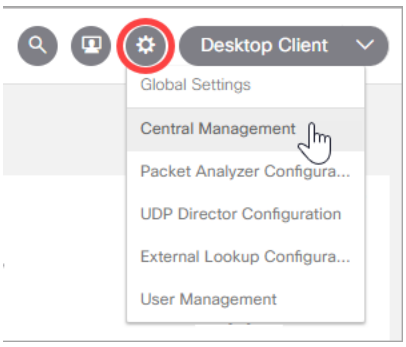
- Readme: 詳細については、パッチの Readme ノートを参照してください。
- 順序: アプライアンスにパッチを順番に適用します。開始する前に、アプライアンスの更新順序で詳細を確認してください。
- 待機: パッチをインストールする前に、SMC と Flow Collector が1 時間以上 7 日未満実行されていることを確認してください。
- 確認: 次のアプライアンスの更新を開始する前に、更新がインストールされていて、各アプライアンスのステータスが [アップ(Up)] と表示されていることを確認してください。

1. パッチのアップロード

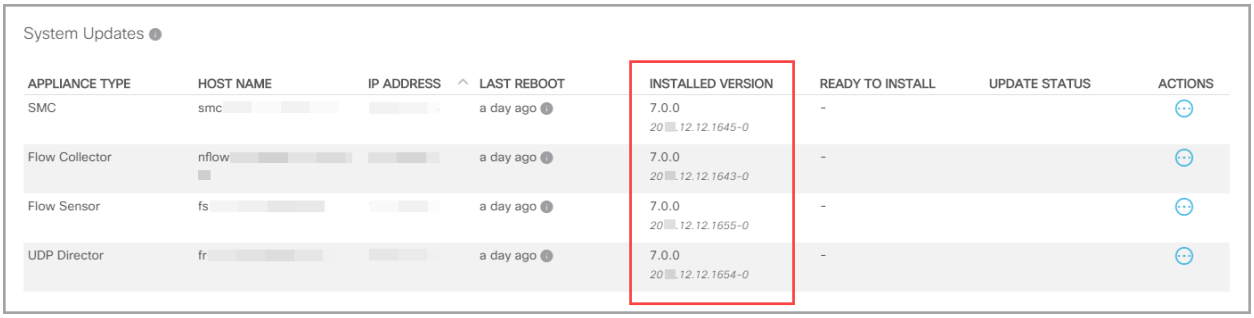
次の手順を使用して、Central Management の Update Manager にパッチをアップロードします。

> パッチをインストールする前に、SMC と 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。

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. [Central Management] を選択します。



4. [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 v7.0.0 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 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、Central Management を使用してパッチを適用します。

1. [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。
    - 最後の再起動(SMC および Flow Collector): 最後の再起動が 1 時間以上前、かつ 7 日未満であることを確認します。

        - 1 時間未満の場合は、処理の終了を待ちます。
        - 7 日以上経過している場合は、[アクション(Actions)] メニュー > [アプライアンスの再起動(Reboot Appliance)] の順にクリックして、アプライアンスを再起動します。少なくとも 1 時間待ってから、すべてのプロセスと安全性チェックの準備ができていることを確認します。

> ⚠ 設定の変更が保留中、または設定チャネルがダウンしている場合は、アプライアンスを再起動しないでください。アプライアンスのステータスが Up であることを確認するには、[Central Management] > [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。

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

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. 7.0.2 ソフトウェア アップデートのインストール

v7.0.2 ソフトウェアアップデートでも、引き続き [Update Manager] ページを使用します。

> ⚠ v7.0.2 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 が 1 時間以上 7 日未満稼働していることを確認します。

新しい更新順序の使用

次の順序で、アプライアンスを更新します。

順序	アプライアンス	注意
1.	UDP Director (別 名 Flow Replicators)	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。更新は、完了までに最大 2 時間かかる場合があります。
3.	Flow Collector 5000 シリーズ エンジン	エンジンの更新を開始する前に、Flow Collector 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。更新は、完了までに最大 2 時間かかる場合があります。
4.	その他 のすべての Flow Collector	更新を開始する前に、フローコレクタが 1

	(NetFlow および sflow)	時間以上 7 日未満稼働していることを確認します。 クラスタ内の次のアプライアンスを更新する前に、Flow Collector の更新が完了し、アプライアンスのステータスが Up と表示されていることを確認してください。更新は、完了までに最大 2 時間かかる場合があります。
5.	セカンダリ SMC (使用する場合)	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、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から、プライマリ SMC の更新を開始します。 更新が完了すると、両方の SMC がセカンダリ ロールで再起動する可能性があります。これが発生した場合は、「14. 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 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)] 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、「14. 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.	スタンドアロン アプライアンス	例：エンドポイントコンセントレータ、またはいずれかのアプライアンスが SMC で管理されていない。 注：これらのアプライアンスは、すべての管理対象アプライアンスの更新終了後に更新します。スタンドアロン アプライアンスは、アプライアンス管理者インターフェイスを使用して更新します。

ベスト プラクティス

- 順序：アプライアンスを順番通りに更新します。開始する前に、アプライアンスの更新順序で詳細を確認してください。
- 待機：7.0.x ソフトウェアアップデートを開始する前に、SMC および Flow Collector が 1 時間以上 7日未満稼働していることを確認します。
- 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。

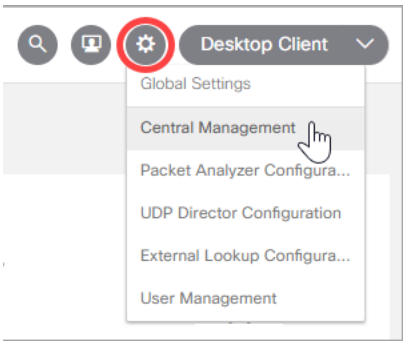
  たとえば、クラスタ内に複数のフロー センサーがある場合は、すべてのフロー センサーを同時に更新できます。ただし、最初にクラスタ内のすべてのフローコレクタの更新が完了していることを確認してください。

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

次の手順を使用して、Central Management のアプライアンスに v7.0.2 ソフトウェアをインストールします。

1. SWU のアップロード

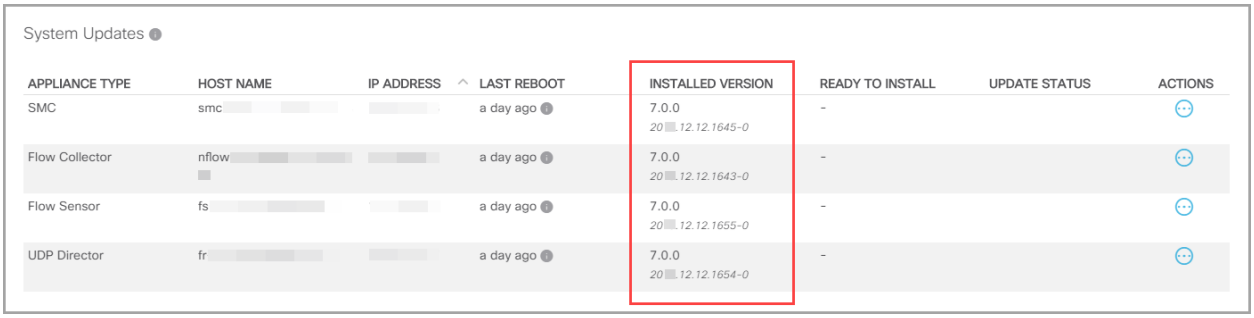
1. SMC にログインします。
   （ブラウザのアドレス フィールドに、https:// およびアプライアンスの IP アドレスを入力し、Enter キーを押します。）
2. [グローバル設定（Global Settings）] アイコンをクリックします。
3. [Central Management] を選択します。



4. [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 v7.0.0 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(Updates)]: 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。
   - 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、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. [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：7.0.2 SWU ファイルが掲示されていることを確認します。
- 最後の再起動（SMC および Flow Collector）：最後の再起動が 1 時間以上前、かつ 7 日未満であることを確認します。
  - 1 時間未満の場合は、処理の終了を待ちます。
  - 7 日以上経過している場合は、[アクション（Actions）] メニュー > [アプライアンスの再起動（Reboot Appliance）] の順にクリックして、アプライアンスを再起動します。少なくとも 1 時間待ってから、すべてのプロセスと安全性チェックの準備ができていることを確認します。

> ⚠ 設定の変更が保留中、または設定チャネルがダウンしている場合は、アプライアンスを再起動しないでください。アプライアンスのステータスが Up であることを確認するには、[Central Management] > [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

[インストールバージョン（Installed Version）] 列をチェックして、新しい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。

1. [Appliance Manager] ダッシュボードでアプライアンスを見つけます。
   - Up：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。
   - 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。
   - Flow Collector データベース：このソフトウェアアップデートの一環として、Flow Collector データベースのプロセスを改善しました。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。これには最大 2 時間かかる場合があります。
2. 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。

3. Central Management ですべてのアプライアンスを更新したら、「11. ルートパーティションの確認」に進みます。

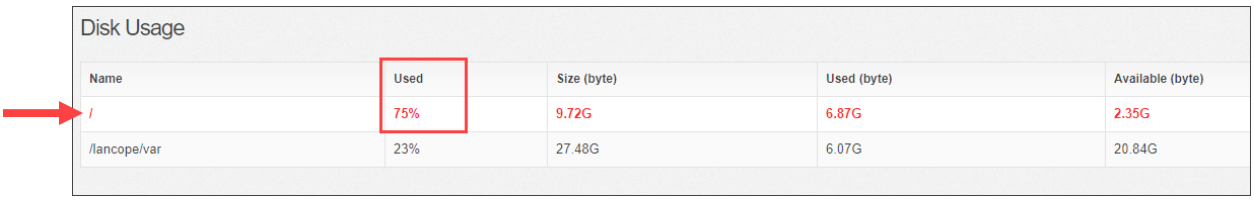
11. ルートパーティションの確認

ルートパーティションを確認するには、次の手順を使用します。

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

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. [アプライアンス統計情報の表示（View Appliance Statistics）] を選択します。
3. 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。
4. [ホーム（Home）] ページで、[ディスク使用量（Disk Usage）] セクションを見つけます。
5. 上の行 / を確認し、[使用済み（Used）] 列のパーセンテージをチェックします。

   使用率が 75 % 以上の場合、このルートパーティションのデータは赤で表示されます。ルートパーティションが埋まった状態が続くと、重要な機能が停止することがあります。使用率が 100 % に近づくに従い、アプライアンスの更新を検討する必要が生じます。



12. v7.0.2 パッチのインストール

1. 「9. パッチのインストール」手順を使用して、次のパッチをインストールします。
    - SMC： patch-smc-ROLLUP003-7.0.2-02.swu

詳細については、Stealthwatch ダウンロードおよびライセンスセンター（Stealthwatch Download and License Center）にあるパッチの readme ファイルで確認してください。

13. 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ページの右上隅にある [デスクトップクライアント（Desktop Client）] 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。

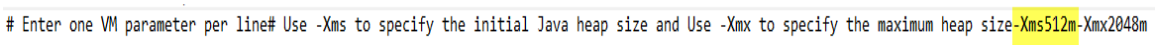
1. Windows Explorer で、ホームディレクトリに移動します。
2. これらのフォルダを次の順に開きます。AppData > ローミング > Stealthwatch。

   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）。

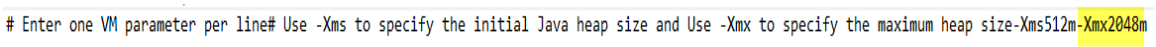
   最小メモリサイズ（Xms）：512 MB 以上を割り当てることをお勧めします。この番号は、ファイルの 3 番目の行に表示されます。

   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。

   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、どの数字が最大メモリサイズを表しているのか確認してください。

   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ページの右上隅にある [デスクトップクライアント（Desktop Client）] 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、どの数字が最大メモリサイズを表しているのか確認してください。

```
# 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。

14. SMC フェールオーバーロールの確認

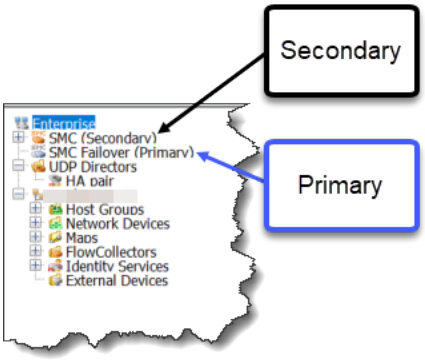
SMC フェールオーバーの設定を使用しない場合、この手順は省略できます。

> ⚠ 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。

> ⚠ Central Management でのアプライアンスの追加や削除は、フェールオーバーの設定を完了し、Central Management でセカンダリ SMC アプライアンスのステータスが [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、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。[Central Management] を選択します。
   - [Appliance Manager] ページで Flow Collector を見つけます。
   - [アクション（Actions）] メニューをクリックします。
   - [アプライアンスの再起動（Reboot Appliance）] を選択します。画面に表示される指示に従って操作します。
   - Flow Collector：手順を繰り返して、Central Management ですべての Flow Collector を再起動します。
   - セカンダリ SMC：手順を繰り返して、セカンダリ SMC を再起動します。

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

15. スタンドアロン アプライアンスの更新

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

- アプライアンスがエンドポイントコンセントレータの場合
- 現在 SMC で管理されていないために、他のクラスタで更新されなかったスタンドアロン アプライアンスがある場合。

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

> スタンドアロン アプライアンスがない場合、Stealthwatch の更新は終了です。

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

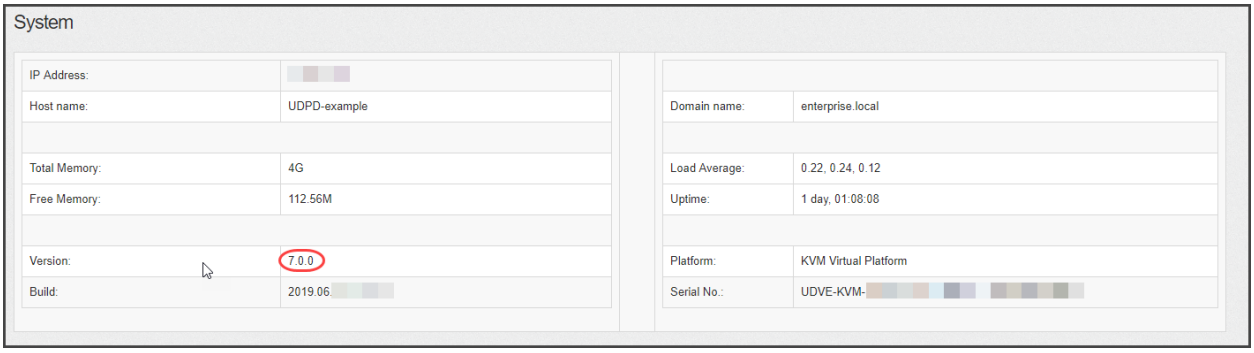
「パッチファイルとアップデートファイルのダウンロード」手順を使用して、パッチファイルとアップデートファイルをダウンロードします。

2. ソフトウェア バージョンの確認

次の手順を使用して、スタンドアロン 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 7.0.0（またはその後のバージョン 7.0.x）がインストールされていることを確認します。

   6.10.x 以前：ソフトウェアのバージョンが 6.10.x 以前の場合は、この更新を開始する前に、Stealthwatch 更新ガイド [英語] を使用して、アプライアンスを 7.0.0（または 7.0.x の後継バージョン）に更新します。

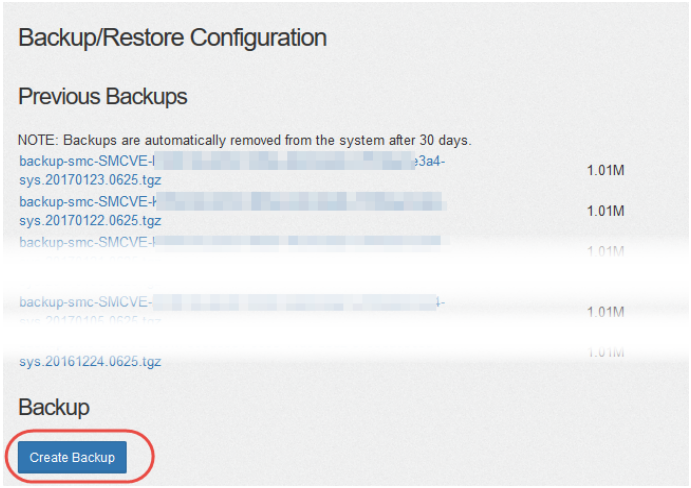


3. アプライアンスの設定のバックアップ

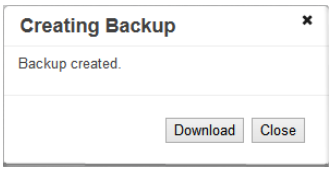
次の手順を実行して、スタンドアロン アプライアンスの設定をバックアップします。これらの手順は、データ損失を最小限に抑えるために重要です。

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

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



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



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

> ⚠ 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

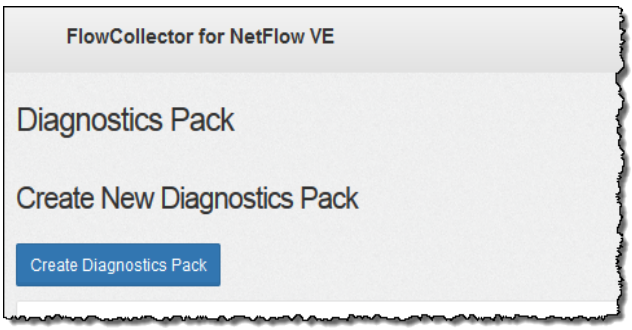
が必要です。手順については、「5. Flow Collector と SMC データベースのバックアップ」を参照してください。

4. 診断パックの作成

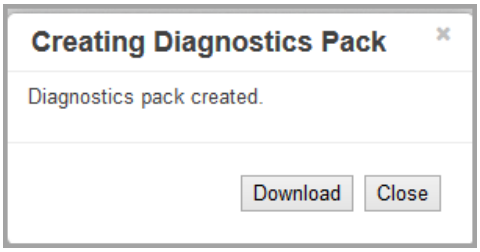
診断パックがあると、Cisco Stealthwatch サポートによる問題のトラブルシューティングが必要な場合に役立ちます。

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 /lancope/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

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

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

このプロセスには、次の手順が含まれます。

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

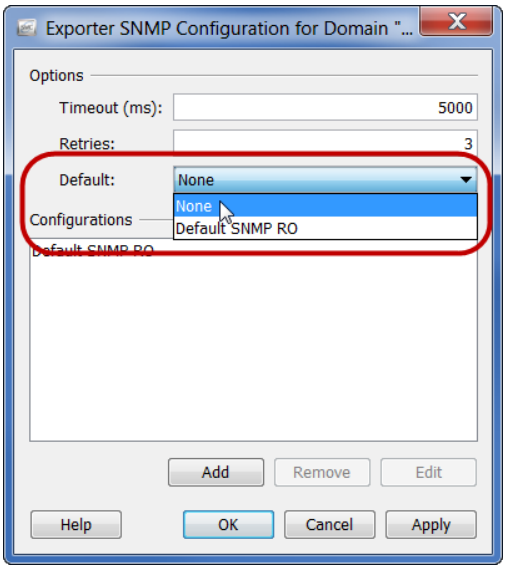
> バックアップしていないと、更新プロセス中に問題が発生した場合にファイルを回復できません。

SMC のSNMP ポーリングの無効化

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

SNMP ポーリングを無効にするには、次の手順を実行します。

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



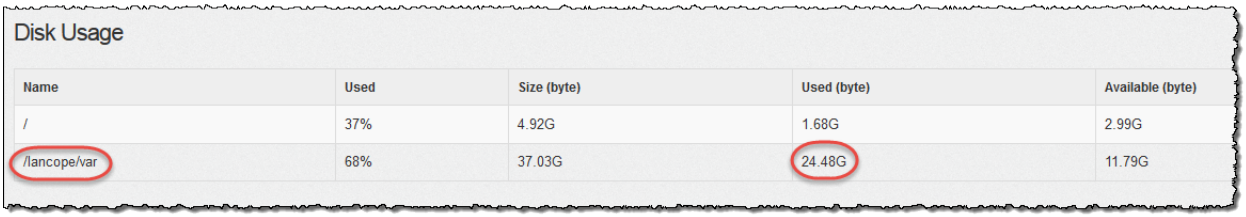
5. [デフォルト(Default)]ドロップダウンリストから[なし(None)]を選択します。このドメインの SNMP ポーリングがオフになりました。
6. [OK]をクリックします。
7. システム上のドメインごとに手順 2 ～ 6 を繰り返します。

データベースのバックアップ

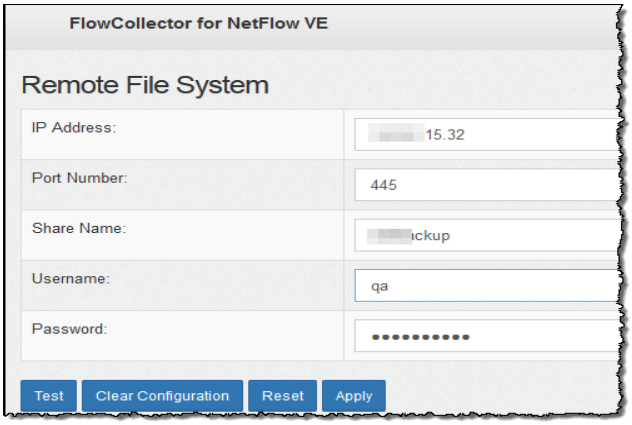
Flow Collector または SMC データベースをリモートファイルシステムにバックアップするには、次の手順を実行します。

- 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。



3. [設定(Configuration)]>[リモートファイルシステム(Remote File System)]の順にクリックします。



4. バックアップ ファイルを保存するリモート ファイル システムの設定を使用して、フィールドに入力します。

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

5. [適用(Apply)]をクリックして、設定ファイルに設定を適用します。

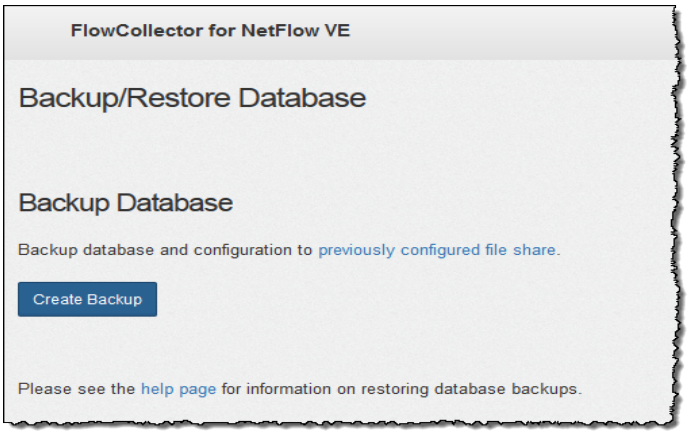
   パスワードを入力しても[適用(Apply)]ボタンが有効にならない場合、[リモートファイルシステム(Remote File System)]ページの空白部分を 1 回クリックすると有効になります。

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

   テストが完了すると、リモート ファイル システムのページの下部に次のメッセージが表示されます。

   File sharing appears to be properly configured.

7. [サポート(Support)]>[データベースのバックアップおよび復元(Backup/Restore Database)]の順にクリックします。[データベースのバックアップ(Backup Database)]ページが開きます(次の例を参照)。



8. [Create Backup]をクリックします。このプロセスは長時間かかる場合があります。

   - バックアップ プロセスの開始後は、マウスをページから離してもプロセスは中断されません。ただし、バックアップの実行中に、[キャンセル(Cancel)]をクリックすると、アプライアンスを再起動しないとバックアップを再開できなくなる場合があります。
   - バックアップが完了するまで、画面に表示される指示に従います。
   - バックアッププロセスの詳細を確認するには、[ログの表示(View Log)]をクリックします。

9. [閉じる(Close)]をクリックして進捗状況ウィンドウを閉じます。

SMC でのSNMP ポーリングの再有効化

SNMP ポーリングを再度有効にするには、次の手順を実行します。

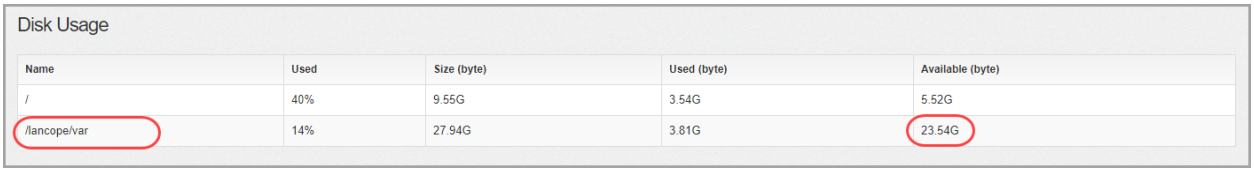
1. デスクトップクライアントに戻ります(ただし、アプライアンス管理インターフェイスは閉じないでください)。
2. 適切なドメインを右クリックし、[設定(Configuration)]>[エクスポータの SNMP 設定(Exporter SNMP Configuration)]の順に選択します。そのドメインの[エクスポータのSNMP構成(Exporter SNMP Configuration)]ページが開きます。
3. [デフォルト(Default)]ドロップダウンリストから、選択したドメインの元のエントリを選択します(「SNMPポーリングの無効化」の手順 4 を参照)。このドメインの SNMP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

6. 使用可能なディスク容量の確認

スタンドアロン アプライアンスのディスク容量をチェックして、ソフトウェアアップデート用の十分なディスク容量があることを確認します。

1. アプライアンス管理インターフェイスにログインします。
2. [ホーム(Home)]をクリックします。
3. [ディスク使用量(Disk Usage)]セクションを見つけます。
4. [使用可能(バイト)(Available(byte))]列を確認し、/lancope/var/ パーティションにソフトウェア アップデート ファイル(SWU)のサイズの 4 倍以上の空き容量があることを確認します。

   たとえば、ソフトウェア アップデート ファイル(ダウンロードおよびライセンス センターから取得)が 6 GB の場合、パーティションには 24 GB の空き容量が必要です。


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。

7. 更新ログのバックアップ

次の手順を使用して、各スタンドアロン アプライアンスの更新ログをバックアップします。

1. アプライアンスに SSH 接続します。
2. root としてログインします。
3. 次のように入力します。

```
cp /lancope/var/admin/upgrade/upgradeOutput.log /lancope/var/admin/upgrade/upgradeOutputHistory.log
```

4. Enter を押します。
5. アプライアンスを終了します。

> ⚠ 次の手順「8. パッチのインストール」を開始する前に、Stealthwatch クラスタ内のすべての管理対象アプライアンスで手順 1 ～ 8 が完了していることを確認します。

8. パッチのインストール

ソフトウェアアップデートを開始する前に、アプライアンスに最新のパッチをインストールしていることを確認してください。

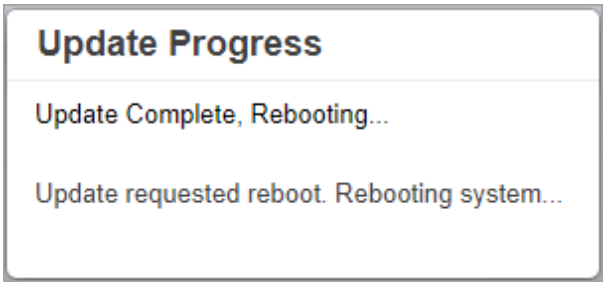
> ℹ 詳細については、パッチの Readme ノートを参照してください。

1. SMC および Flow Collector: 管理アプライアンスの**ホーム** ページで、[稼働時間(Uptime)]を確認します。更新を開始する前に、アプライアンスの稼働時間が 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。

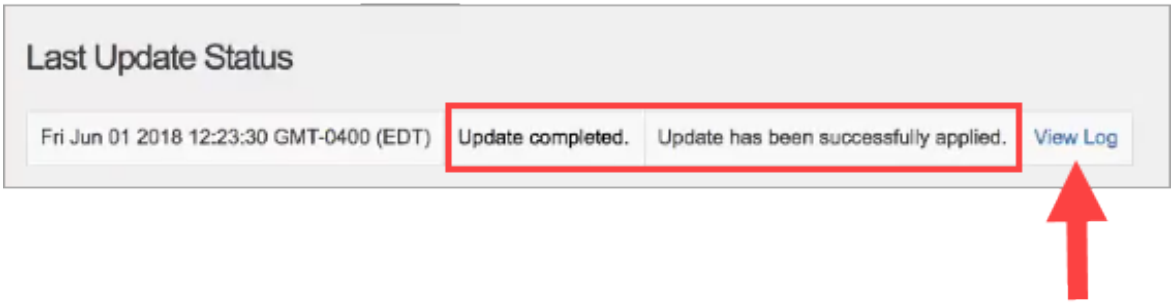
- 1 時間未満の場合は、処理の終了を待ちます。
- 7 日以上経過している場合は、[操作(Operations)]>[アプライアンスの再起動(Restart Appliance)]の順にクリックしてアプライアンスを再起動します。少なくとも 1 時間待ってから、すべてのプロセスと安全性チェックの準備ができていることを確認します。

⚠ 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。

2. 管理アプライアンスの [サポート(Support)]>[更新(Update)]ページで、
3. [ファイルの選択(Choose File)]をクリックします。
4. アプライアンスのパッチ SWU ファイルを選択します。
5. [自動的に実行(Automatically Execute)]チェックボックスをオンにします。
6. [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。
7. [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。



8. 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. 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。
10. [サポート(Support)]>[更新(Update)]の順に選択します。
11. [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。

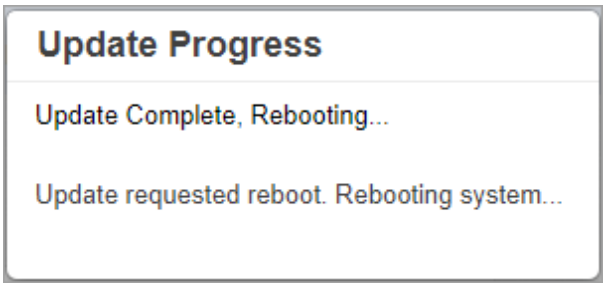


9.v7.0.2 ソフトウェアアップデートをインストールします。

1. SMC および Flow Collector：管理アプライアンスの**ホーム** ページで、[稼働時間（Uptime）] を確認します。更新を開始する前に、アプライアンスの稼働時間が 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。
   - 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、[操作（Operations）] > [アプライアンスの再起動（Restart 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。

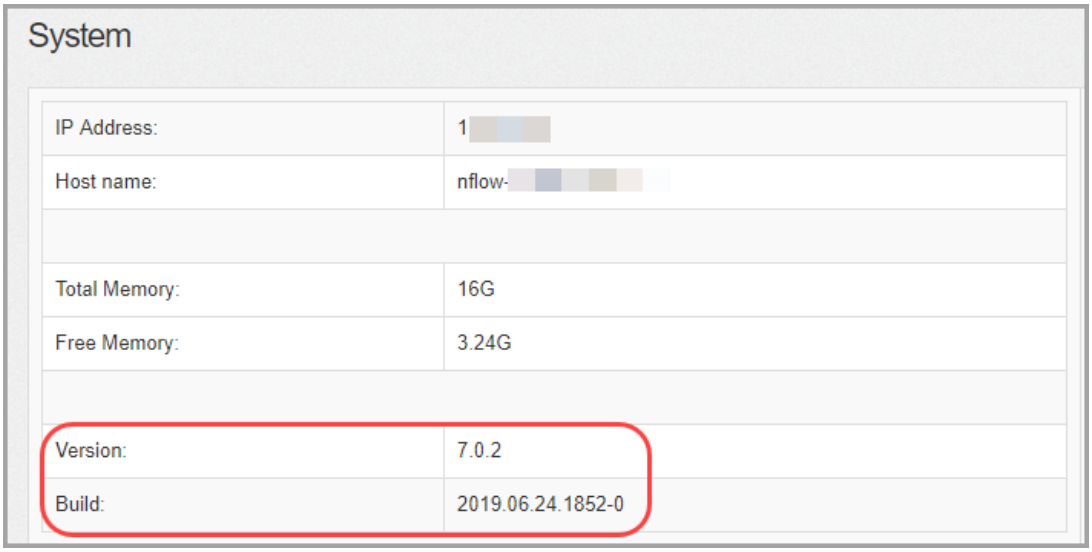
2. 管理アプライアンスの [サポート（Support）] > [更新（Update）] ページで、[ファイルの選択（Choose File）] をクリックします。
3. アプライアンスの v7.0.2 SWU ファイルを選択します。
4. [自動的に実行（Automatically Execute）] チェックボックスをオンにします。
5. [アップロード（Upload）] をクリックします。画面に表示される指示に従って操作します。
   - アップロードの進捗状況はページの下部に表示されます。
   - 安全性の確認と更新には数分かかる場合があります。
6. [更新の進捗状況（Update 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。



> ⚠ 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。アプライアンスが Flow Collector の場合は、更新が完了するまでに最大 2 時間かかることがあります。詳細については、「**更新に最適な時間：SMC および Flow Collector**」セクションを参照してください。

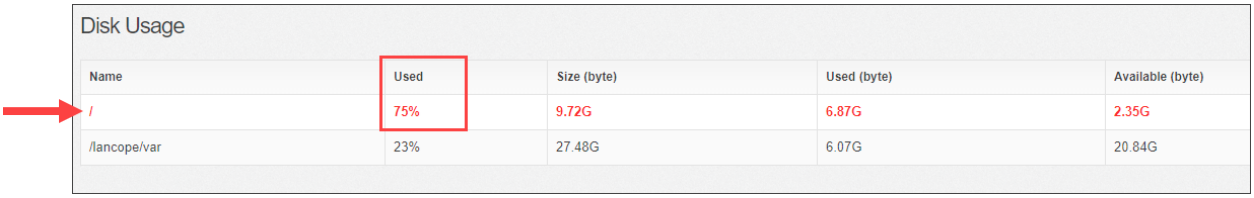
7. アプライアンス管理インターフェイスにログインします。
8. [ホーム（Home）] ページに表示されているソフトウェア バージョンを確認します。[バージョン（Version）] フィールドに v7.0.2 と表示されていることを確認します。

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



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

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



10. アプライアンスが SMC の場合は、「13. Stealthwatch デスクトップクライアントのインストール」手順を使用して Stealthwatch デスクトップ クライアントをインストールします（オプション）。

10. v7.0.2 パッチのインストール

「8. パッチのインストール」手順を使用して、次のパッチをインストールします。

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

詳細については、Stealthwatch ダウンロードおよびライセンスセンター（Stealthwatch Download and License Center）にあるパッチの readme ファイルで確認してください。

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

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

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

ベスト プラクティス

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

推奨事項は次のとおりです。

- **1 つずつ**: 一度に 1 つのアプライアンスを設定します。お使いのクラスタ内で次のアプライアンスの設定を開始する前に、アプライアンスが [稼動中（Up）] ステータスであることを確認します。
- **順序**: 1 つ以上のアプライアンスを Central Management に追加する場合は、設定の順序に従います。
- **アクセス**: Central Management にアクセスするための管理者権限が必要です。
- **カスタム証明書**: アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン（ルートおよび中間）をその独自の信頼ストアおよび SMC 信頼ストアに個別に保存してください。Stealthwatch のオンライン ヘルプの信頼ストアの手順を参照してください。詳細については、「開始する前に」セクションおよび StealthWatch オンラインヘルプの「カスタム証明書」を参照してください。

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

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

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

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

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

Central Management へのアプライアンスの追加

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

   https://<IPaddress>/lc-ast

2. アプライアンス設定ツールを使用して、プライマリ SMC/Central Manager にアプライアンスを追加します。詳細については、アプライアンスのインストールおよびコンフィギュレーション ガイド [英語] を参照してください。
3. 更新する別のスタンドアロン アプライアンスがある場合は、手順「15. スタンドアロン アプライアンスの更新」を繰り返します。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- Cisco Stealthwatch サポートのお問い合わせ先:
- Web でケースを開く場合:http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合:tac@cisco.com
- 電話でサポートを受ける場合:800-553-2447(米国)
- ワールドワイド サポート番号:https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

著作権情報