Cisco Secure Network Analytics（旧 Stealthwatch）v7.4.2 Flow Collector NetFlow 更新パッチ

このドキュメントでは、Cisco Secure Network Analytics Flow Collector NetFlow アプライアンス v7.4.2 のパッチとインストール手順について説明します。

> このパッチの前提条件はありませんが、開始する前に「**はじめる前に**」セクションを必ずお読みください。

パッチ名とサイズ

- **名前**：パッチ名が「patch」ではなく「update」で始まるように変更されました。このロールアップの名前は、**update-fcnf-ROLLUP20230727-7.4.2-v2-01.swu** です。
- **サイズ**：パッチ SWU ファイルのサイズを増やしました。ファイルのダウンロードに以前より時間がかかる場合があります。また、**使用可能なディスク容量の確認**セクションの手順に従って、新しいファイルサイズで使用可能なディスク容量が十分にあることを確認してください。

パッチの説明

このパッチ（update-fcnf-ROLLUP20230727-7.4.2-v2-01.swu）には、次の修正が含まれています。

障害	説明
SWD-19193	データベースのディスク容量アラームが Flow Collectorで正しく機能していなかった問題を修正しました。
SWD-19265	Manager が信頼ストアで 40 を超える証明書を処理できない問題を修正しました。
SWD-19375	v7.4.2 ROLLUP パッチの最新のインストール済みパッチ情報が **/lancope/info/patch** に含まれていない問題を修正しました。

> このパッチに含まれる以前の修正については、「**以前の修正**」で説明します。

はじめる前に

> ⚠ 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、Manager 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。

使用可能なディスク容量の確認

これらの手順を使用して、使用可能なディスク容量が十分にあることを確認します。

1. アプライアンス管理インターフェイスにログインします。
2. [ホーム（Home）] をクリックします。
3. [ディスク使用量（Disk Usage）] セクションを見つけます。
4. [空き容量（バイト）（Available (byte)）] 列を確認し、**/lancope/var/** パーティションに必要な空き容量があることを確認します。
    - **要件**：管理対象アプライアンスごとに、個々のソフトウェア更新ファイル（SWU）の 4 倍以上のサイズが必要です。Manager では、Update Manager にアップロードするすべてのアプライアンス SWU ファイルの 4 倍以上のサイズが必要です。
    - **管理対象アプライアンス**：たとえば、Flow Collector の SWU ファイルが 6 GB の場合、Flow Collector（/lancope/var）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）。
    - **Manager**：たとえば、それぞれ 6 GB の 4 つの SWU ファイルを Manager にアップロードする場合、/lancope/var パーティションに少なくとも 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）。

次の表に、新しいパッチファイルのサイズを示します。

アプライアンス	ファイル サイズ（File size）
Manager	5.7 GB
フロー コレクタ NetFlow	2.6 GB
フローコレクタ sFlow	2.4 GB
フローコレクタデータベース	1.9 GB
フローセンサー	2.7 GB
UDP Director	1.7 GB
データストア	1.8 GB

ダウンロードとインストール

ダウンロード

パッチ更新ファイルをダウンロードするには、次の手順を実行します。

1. シスコ ソフトウェア セントラル（https://software.cisco.com）に移動します。
2. [ダウンロードとアップグレード（Download and Upgrade）] セクションで、[ダウンロードにアクセス（Access downloads）] を選択します。
3. [製品の選択（Select a Product）] 検索ボックスに「**Secure Network Analytics**」と入力します。
4. ドロップダウンリストからアプライアンスモデルを選択し、Enter キーを押します。
5. [ソフトウェアタイプの選択（Select a Software Type）] で [Secure Network Analytics パッチ（Secure Network Analytics Patches）] を選択します。
6. [最新リリース（Latest Releases）] エリアから [7.4.2] を選択してパッチを見つけます。
7. パッチ更新ファイル（update-fcnf-ROLLUP20230727-7.4.2-v2-01.swu）をダウンロードし、任意の場所に保存します。

インストール

パッチ更新ファイルをインストールするには、次の手順を実行します。

1. Manager にログインします。
2. メインメニューで、**[設定（Configure）] > [グローバル 集中管理（GLOBAL Central Management）]** を選択します。
3. [Update Manager] タブをクリックします。
4. [アップデートマネージャ（Update Manager）] ページで **[アップロード（Upload）]** をクリックし、保存したパッチ更新ファイル（update-fcnf-ROLLUP20230727-7.4.2-v2-01.swu）を開きます。
5. **[アクション（Actions）]** 列で、アプライアンスの ••• （[省略記号（Ellipsis）]）アイコンをクリックし、**[更新をインストール（Install Update）]** を選択します。

> パッチはアプライアンスを再起動します。

以前の修正

次の項目は、このパッチに含まれている以前の障害の修正です。

障害	説明
SWD-18633/ SWD-18629	Flow Collector エンジンの詳細設定に **ignore_syn_flag_for_cs** を追加しました。

障害	説明
SWD-18869	Manager で無効な重大アラーム SMC_DBMAINT_DSTORE_COMMUNICATION_DOWN が発生する問題を修正しました。
SWD-18884	必須ではないファイルを Flow Collector エンジンの診断パックから除外しました。
SWD-18949	フラッディング sw.log を処理するために sw.log が拡張される問題を修正しました。
SWD-18955	Data Store を使用して Flow Collector にスプリットトンネルが設定されている場合、sw.log の NetFlow カスタマーサクセス メトリック統計に信頼できるフロー数のみが表示される問題を修正しました。
SWD-19026	NVM に関連する統計が NetFlow トラフィックについて誤って更新される問題を修正しました。
SWD-19029	「JOIN Inner がメモリに収まりませんでした」というエラーが原因で Data Store フロークエリが失敗する問題を修正しました。
SWD-19030	NVM データの処理中、Flow Collector エクスポータの数が時間の経過とともに増加し続ける問題を修正しました。
SWD-19064	オーバーロードされた Flow Collector 4000 で set_src_host_exporter() の SIGFPE が発生していた問題を修正しました。
SWD-19065	NetFlow テンプレートデータをまだ送信していないフロー センサーの Flow Collector エンジンデバイス統計を修正しました。
SWD-19100	NVM NetFlow トラフィックが Manager のフロートレンドグラフに表示されることがある問題を修正しました。
SWD-19230/ SWONE-25442	新しいデータを収集し、データベース容量が不足している場合に古いパーティションデータを削除するための保持管理を強化しました。
SWONE-24802	Flow Collector エンジンが NVM を正しく検出および軽減しない問題を修正しました。
SWONE-26094	信頼できない NVM フローが Data Store および非 Data Store の展開でキャッシュされる問題を修正しました。

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ください。
- シスコサポートの連絡先
- 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