

Cisco Secure Network Analytics (旧 Stealthwatch) v7.4.2 Manager 更新パッチ

このドキュメントでは、Cisco Secure Network Analytics Manager (旧 Stealthwatch Management Console) 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。開始する前に、「[はじめる前に](#)」セクションを確認してください。

i このパッチに対する前提条件はありません。

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-smc-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で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-smc-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-19322	IP 範囲での新しいホストグループの作成が失敗するデスクトップクライアントの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 <code>/lancope/info/patch</code> に含まれていない問題を修正しました。

i 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 \times 6 GB \times 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 \times 6 GB \times 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. Cisco Software Central (<https://software.cisco.com>) 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)] エリアで [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-smc-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-smc-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。

 パッチがアプライアンスを再起動します。

スマートライセンスの変更

スマートライセンスのトランスポート設定要件が変更されました。

 アプライアンスを 7.4.1 以前からアップグレードする場合は、アプライアンスが smartreceiver.cisco.com に接続できることを確認してください。

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-18548	デスクトップクライアントで [インターフェイスサービストラフィック (Interface Service Traffic)] ウィンドウの [フィルタ (Filter)] ボタンをクリックすると、フィルタ処理の [フィルタ - インターフェイスサービストラフィック (Filter - Interface Service Traffic)] ダイアログボックスが表示されない問題を修正しました。
SWD-18638	LDAP タイムアウトの問題を修正しました。
SWD-18734	大きな host_groups.xml ファイルを復元した後にホストグループ管理リストが表示されない問題を修正しました。
SWD-18814	Manager が v7.4.2 SWU ファイルの抽出に失敗する問題を修正しました。
SWD-18835	Central Management の [設定の適用 (Apply Settings)] ボタンが、変更されていないインターネットプロキシ設定で使用できる問題を修正しました。
SWD-18868	セキュリティイベントの hopopt が誤ってフローにマッピングされる問題を修正しました。
SWD-18893	Flow Sensor 4240 がシングルキャッシュモードを使用するように設定されている場合、[データロール (Data Roles)] ページに 5020 エラーが表示される問題を修正しました。
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-18922	Subject TrustSec によるフロー検索フィルタ処理が機能しない問題を修正しました。
SWD-18925	エクスポートされた CSV アラームレポートの [詳細 (Details)] 列に改行が含まれていた問題を修正しました。
SWD-18972	レポートが長期間にわたって生成された場合に Manager インターフェイストラフィックレポートに一部のデータが表示されない問題を修正しました。
SWD-19006	Data Store のパスワードに空白が含まれている場合に、Analytics を有効化および無効化できない問題を修正しました。

障害	説明
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-19095	エクスポートした CSV ファイルにプロトコルデータがなく、UI に表示される [ポート (Port)] 列にはポートとプロトコルの両方のデータが表示され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-25712/ SWD-19234	非表示の要素からのクエリが UI でパフォーマンスの問題を引き起こしていた問題を修正しました。
SWONE-25923	[フロー検索結果 (Flow Search Results)] ページに進行中のクエリの最終更新時刻が表示されない問題を修正しました。
SWONE-25924	[ジョブ管理 (Job Management)] ページの [完了したジョブ (Finished Jobs)] テーブルから [%完了 (% Complete)] 列を削除しました。
SWONE-25925	完了したクエリとキャンセルされたクエリの [フロー検索結果 (Flow Search Results)] ページに [クエリ進行中 (Query In Progress)] メッセージが短時間表示される問題を修正しました。
SWONE-25926	[フロー検索 (Flow Search)] ページ、[フロー検索結果 (Flow Search Results)] ページ、および [ジョブ管理 (Job Management)] ページのバナーテキストメッセージを簡素化しました。
SWONE-25956	ホストグループ管理 IP が英数字順にソートされない問題を修正しました。
SWONE-25957	ホストグループ管理 IP の重複が除外されない問題を修正しました。
SWONE-26045	デスクトップクライアントの Azul JRE を更新しました。

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

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)