Cisco Secure Network Analytics（旧 Stealthwatch）v7.4.0 の Manager 更新パッチ

このドキュメントでは、Cisco Secure Network Analytics Manager（旧 SMC）アプライアンス v7.4.0 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。

> このパッチに対する前提条件はありません。

パッチの説明

このパッチ（patch-smc-ROLLUP008-7.4.0-v2-02.swu）には、次の修正が含まれています。

障害	説明
SWD-17653	引用符付きで作成されたメッセージを編集または保存できない問題を修正しました。
SWD-17672	フローの検索結果にフローの負の TCP 再送信値が表示される問題を修正しました。
SWD-17874	マネージャ（旧 SMC）vertica データベーステーブルに格納されている TrustSec データのサイズが大きすぎました。
SWD-17888	オペレーティング システム カーネルが許可する任意の有効な MTU 範囲を許可する問題を修正しました。
SWD-18110	postinst（svc-legacy-auth および svc-token-authority）が以前の Docker イメージを削除できない問題を修正しました。
SWONE-23527	CiscoSSL の rdcpu オプションを有効にしました。

> 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（Available）]（バイト）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）。

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 [7.4.0] を選択してパッチを見つけます。
7. パッチ更新ファイル（patch-smc-ROLLUP008-7.4.0-v2-02.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. ⚙（[グローバル設定（Global Settings）]）アイコン をクリックし、[集中管理（Central Management）] を選択します。
3. [アップデートマネージャ（Update Manager）] 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（patch-smc-ROLLUP008-7.4.0-v2-02.swu）を開きます。
5. アプライアンスの [アクション（Actions）] メニュー、[更新をインストール（Install Update）] の順に選択します。

> このパッチは、5 分後に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
LVA-2811	Apache Log4J 2 を v2.15 に更新しました。
LVA-2825	Apache Log4J 2 を v2.17.1 に更新しました。
LVA-2844	v7.4.0 から log4j 1.x を削除しました。
LVA-3021	TLS クライアントが FIPS/CC モードで非準拠の EC 曲線を提供していた問題を修正しました。
SWD-15482/ SWD-16898	インジケーターが、イベントの説明や Cisco Secure Network Analytics Manager の UUID ではなく、短い形式の古い説明のままになっていた問題を修正しました。
SWD-15993	高速で ISE ユーザーセッションを行うと、サーバー（Super Tomcat）がメモリ不足になり、さまざまなクラッシュ/エラーが発生する問題を修正しました。
SWD-16599	アップグレード後にログインページがロードされない問題を修正しました。
SWD-16634	SSE コネクタがパブリック証明書を使用して svc-ctr-service と通信できない問題を修正しました。

障害	説明
SWD-16687	Swing クライアントがハングし、多数のユーザーセッションでデータを返さない問題を修正しました。
SWD-16706	構成の更新が失敗したときに、Cisco Secure Network Analytics が監査ログの宛先接続をロールバックする問題を修正しました。
SWD-16715	PDT/PST タイムゾーンのお客様が、メインダッシュボードの［日別アラーム（Alarms by Day）］ウィジェットで翌日のアラームの日付が正しく表示されない問題を修正しました。（LSQ-5440）
SWD-16802	SecureX ポータルおよびウィジェットで、一部のフィールド値など再ブランディングの変更が行われない問題を修正しました。
SWD-16828	インターフェイスの上位レポートに誤った結果が表示される問題を修正しました。これまでは、特定のホストまたはホストグループと、クライアントまたはサーバーを検索するときに、行（すべてのデータ）が欠落していました。
SWD-16923	［Central Managerのアップグレード（Central Manager Upgrade）］ページで、稼働要件（1 時間から 7 日）に関するテキストを 7.4.0 から削除したにもかかわらず引き続き表示される問題を修正しました。
SWD-16929	pxGrid 2.0 で ISE セッションを受信するためのバッファサイズが不十分だった問題を修正しました。
SWD-16966	マネージャ（旧 SMC）の画像が 10 GB パーティションに収まらない問題を修正しました。
SWD-16967	Flow Collector データベースバックアップ機能レポートが、Central Manager で分散データストアデータベースのパスワードを変更した後にデータベースが実行されていないことを示す問題を修正しました。
SWD-16969	フローコレクタデータベース統計の Web UI ページでエラーが表示され、Central Manager で分散データストアデータベースのパスワードを変更した後もロードされない問題を修正しました。
SWD-17028	マネージャ（旧 SMC）の CSM コレクタで S3 の AVRO が検証されない問題を修正しました。
SWD-17089	データストアに新しく追加された dnode に secret.store ファイルがない問題を修正しました。

障害	説明
SWD-17101	HG_CHANGES_COUNT を正しく実装するための問題を修正しました。
SWD-17138	エクスポートされた CSV ファイルからポートデータが欠落していた問題を修正しました。
SWD-17143	フロークエリの単方向フィルタ SQL が正しくなかった問題を修正しました。
SWD-17178	GRUB がコードタイプ 0x0700 のディスクパーティションを認識しない問題を修正しました。
SWD-17320/ SWD-17648	MongoDB の Web UI トップレポートの保持設定を 24 時間から 48 時間に延長し、顧客が長時間実行されているレポートにアクセスするためにより多くの時間を提供します。
SWD-17583	Akka ログの初期化のタイムアウト エラーにより、起動中に svc-ise-client サービスが失敗する問題を修正しました。
SWD-17593	TLS が再接続されても、監査ログが再接続されない問題を修正しました。
SWD-17599	macOS Monterey バージョン 12.2.1 および 12.3 でのデスクトップクライアントの機能が改善されました。 環境にデスクトップクライアントが含まれている場合は、最新バージョンをダウンロードしてください。
SWD-17734	Avro ファイルが重複する問題を修正しました。
SWD-17745	ユーザーがアプライアンス セットアップ ツール（AST）にアクセスすることを妨げる VMware での UEFI モードの有効化に関連する問題を修正しました。
SWD-17759	パッチの再インストールを妨げていた問題を修正しました。
SWD-17973	ディスク容量の不足が原因で Manager がパッチをインストールできない問題を確認しました。
SWONE-20990	Firepower 統合で postinst のクリーンアップが必要だった問題を修正しました。
SWONE-21225	log4j 2 ファイルが逆方向にローテーションす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：www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

著作権情報