Cisco Secure Network Analytics（旧 Stealthwatch）v7.4.1 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 v7.4.1 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-ROLLUP012-7.4.1-v2-02.swu）には、次の修正が含まれています。

障害	説明
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。

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）。

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 [7.4.1] 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-ROLLUP012-7.4.1-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-ROLLUP012-7.4.1-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。

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。

> ⚠ Rollup008 より前の Rollup からアプライアンスを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-16516	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-16606	Manager でフロー検索が日本語で機能しない問題を修正しました。（LSQ-5106）
SWD-16618	バックスラッシュ（¥）文字を含む SMTP ユーザー名で電子メールのアクションを編集または作成しようとすると、応答管理が警告メッセージを表示する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-17345	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-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-17612	アップデートマネージャの [すべてのデータノードを更新する（Update All Data Nodes）] ボタンを使用してソフトウェアアップデートをインストールするときに、インストールエラーのバナーが表示されない問題を修正しました。
SWD-17614	データノードを削除するときに集中管理でエラーが表示される問題を修正しました。

障害	説明
SWD-17623	データノードが接続されていないときにユーザーに通知するバナーメッセージを追加しました。
SWD-17653	引用符付きで作成されたウェルカム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-17681	エクスポータで特定のアラームが表示されたときに、[モニター（Monitor）] > [インターフェイス（Interfaces）] を選択すると「5020 内部サーバーエラー」が表示される問題を修正しました。
SWD-17717	Manager のセットアップ時に管理ポートを切り替えるオプションが提供されました。
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-17832	v7.4.1 の診断パックに system-stats フォルダがない問題を修正しました。
SWD-17874	マネージャに保存されている TrustSec データが、Vertica データベーステーブルで許可されているストレージを超えていた問題を修正しました。
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-17972	Manager で構成の復元が失敗する問題を修正しました。
SWD-17973	ディスク容量の不足によりマネージャがパッチロールアップのインストールに失敗する問題を修正しました。
SWD-18068	マネージャの上位レポート検索がポート/プロトコルフィルタリングをサポートしていなかった問題を修正しました。
SWD-18136	ホストサマリ REST エンドポイントがアラームに対して不要なデータベースクエリを行う問題を修正しました。
SWD-18166	[イベントアラーム（Event Alarms）] 列のエントリをクリックしてもポリシー違反のアラームが表示されない問題を修正しました。

障害	説明
SWD-18297	新しい応答管理ルールを作成するときに、「413 ペイロードが大きすぎます」というエラーメッセージが表示される問題を修正しました。
SWD-18342	ドメインにホストロック違反のセキュリティイベントが存在するために、フロー検索が「500 内部サーバーエラー」を返す問題を修正しました。
SWD-18356	Celery のリソース制限を減らすことで、マネージャのメモリの問題を修正しました。
SWD-18357	アップデートのインストール後に SMTP 設定がデフォルト設定に再初期化される問題を修正しました。
SWD-18424	API が、マルチバイト文字コードではなくホストグループ名の誤った文字を表示する問題を修正しました。
SWD-18522	集中管理のバックアップ構成から managementChannel.json ファイルが欠落していた問題を修正しました。
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-18553	アプライアンスの再起動後に仮想インターフェイスの順序が正しくない問題を修正しました。
SWD-18574	エクスポータを一覧表示するときに、［設定（Configure）］>［エクスポータ（Exporters）］タブにアクセスするとサーバー例外エラーが表示される問題を修正しました。
SWD-18589	フローセンサー 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-18612	アプライアンスのアップグレード後にライセンス付きアプライアンスが評価ライセンスモードに変更される問題を修正しました。
SWD-18620	検索フィルタの IP 範囲によってエラーが発生する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。

障害	説明
SWD-18722/ SWD-18657	バックアップの復元後に保存されたレポートが自動的に削除される問題を修正しました。
SWD-18782/ SWD-18488	宛先ポート 80 がブロックされたときにマネージャが脅威フィードサーバーとの通信を停止する問題を修正しました。
SWD-18817	フロー検索ジョブのデータ保持設定が 48 時間に延長されました。
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-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。
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いにもかかわらず、UI に表示される [ポート（Port）] 列に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。
SWONE-21790	Update Manager の [すべてのデータノードを更新する（Update All Data Nodes）] ボタンの可視性が向上しました。
SWONE-22943/ SWONE-23817	レポートされたシリアル番号が完全なハードウェアシリアル番号を使用するように変更される問題を修正しました。
SWONE-23314	データストアのヘルプトピックの問題を修正しました。
SWONE-24754	アラーム発行ホストの調査に関するヘルプトピックの問題を修正しました。
SWONE-25452	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