Cisco Secure Network Analytics（旧 Stealthwatch）v7.4.0 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 v7.4.0 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-fcnf-ROLLUP009-7.4.0-v2-01.swu）には、次の修正が含まれています。

障害	説明
SWD-17799/ SWD-17756	バージョン 9 でサポートされている IPFIX AVC/ART フィールドの Flow Collector エンジンへのサポートが追加されました。
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-fcnf-ROLLUP009-7.4.0-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. ⚙（[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-fcnf-ROLLUP009-7.4.0-v2-01.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。

パッチによって Flow Collector エンジンが停止し、アプライアンスが再起動します。

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-16260	アプライアンスのアップグレード後に csm-statsd サービスを開始でき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-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-16856	スマート ライセンス マネージャで、エンドポイントライセンスの使用数が実際に使用されているライセンス数ではなく 0 と表示されていた問題を修正しました。
SWD-16876	nvm_netflow_port の [詳細設定（Advanced Setting）] が「ゼロ以外」の値に設定されていた場合に、それ以降 [詳細設定（Advanced Setting）] で変更を行うとエンジンが再起動されていた問題を修正しました。
SWD-16886	CSM 統計に影響を与える日次リセットとカウンターリセットの問題を修正しました。
SWD-16942	[FlowCollectorインターフェイス数の超過（FlowCollector Interfaces Count Exceeded）] で、数を超えていない場合にもアラームが発生する問題を修正しました。

障害	説明
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-17102	Flow Collector エンジンが exporter_inactivity_timeout の詳細設定を認識しない問題を修正しました。
SWD-17142	エンジンが無効な JSON 変数を含む flex_security_events ファイルを生成する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-17236	Network Based Application Recognition（NBAR）機能と Secure Network Analytics をより完全に統合する方法を見直しました。
SWD-17239	URL データのホスト名を特定するときに、Flow Collector エンジンが「http://」と「https://」の両方を検索する必要があった問題を修正しました。
SWD-17309	Flow Collector の再起動後にアクティブなユーザーセッションからフィールド（SGT、SGT ID、およびユーザー名）が欠落する問題を修正しました。
SWD-17353	Flow Collector、Flow Sensor、および UDP Director のログがホストマシンからアクセス可能なファイルに確実に記録されるようになりました。

障害	説明
SWD-17361	Flow Collector 5K アプライアンスでホストおよびフローキャッシュが適切にスケーリングされるようにするために、エンジンのスケーリング上限の問題を修正しました。
SWD-17377	Flow Collector エンジンが、ホストグループ構成の更新中に SWAAgent メッセージサーバーをリセットする問題を修正しました。
SWD-17378	Secure Analytics and Logging（SAL）に入る ASA および FTD イベントのヘッダーからセッション情報が欠落していた問題を修正しました。
SWD-17405	シャットダウン後に svc_fc_engine を再起動するまでの待機時間が短縮されました。
SWD-17409	サポートされていないメッセージをエンジンに送信した Follow Collector エージェント（fc-core）がハングする可能性がある問題を修正しました。
SWD-17439	現在のグループ数より大きいグループ ID がベースラインファイルから削除されるたびに発生する SIGABRT の問題を修正しました。
SWD-17450	エンジンのシャットダウンプロセスの非グレースフルシャットダウンで stop_smc_agent() 関数を呼び出す必要がある問題を修正しました。
SWD-17458	詳細設定が 1 回しかだけ実行されない問題を修正しました。
SWD-17493	SIGABRT シグナルが強化され、log_backtrace 関数を無効または有効にできるようになりました。
SWD-17517	MAX_FAKE_APP_EXCLUDE 値に基づいて、fake_app_exclude_list 配列のサイズを設定するために、Flow Collector エンジンが必要だった問題を修正しました。
SWD-17552	[詳細設定（Advanced Settings）] の restart_hour を 0..23 にバインドする必要があった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-17628	ベースラインファイルのグループインデックスがホストグループの数と同じである場合、SIGABRT 問題が発生する問題を修正しました。

障害	説明
SWD-17663	flow_stats テーブルに誤った値が表示される問題を修正しました。
SWD-17711/ SWD-17718	insane_average_packet_size の詳細設定構成を 16 ビット値から 32 ビット値に増やしました。
SWD-17734	Avro ファイルが重複する問題を修正しました。
SWD-17743/ SWD-17762	すべてのインターフェイス（eth0 および eth1）ですべてのテレメトリ（NVM を含む）を確実に処理するように Flow Collector エンジンを強化しました。
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-17788/ SWD-17791	AnyConnect バージョン 4.10.0407 以降によってエクスポートされるテンプレート 272 および 273 を確実に受け入れるように Flow Collector エンジンを強化しました。
SWD-17973	ディスク容量の不足が原因でアプライアンス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-18467	パフォーマンスを向上させるために ignorelist の処理を変更して bsearch 関数を利用する必要があった問題を修正しました。
SWONE-19230/ SWONE-19530	NATed フローが、宛先 IP アドレスとして実際の宛先 IP を表示せず、代わりにファイアウォール IP を表示していた問題を修正しました。
SWONE-19509	エンジンで exporters.xml ファイルにアクセス許可を設定できなかった場合に、sw.log に書き込まれたエラーに errno と strerror を追加する必要があった問題を修正しました。
SWONE-19511	debug_sflow の詳細設定を追加しました。
SWONE-19512	NetFlow と sFlow エクスポータの両方を同じ操作ロジックで非アクティブ状態に設定する必要があった問題を修正しました。
SWONE-19513	SGT タグにデータ検証を追加する必要があった問題を修正しました。

障害	説明
SWONE-20633	Flow Collector エンジンが MAX_FAKE_APP を増やす必要があった問題を修正しました。
SWONE-21198	Flow Collector エンジンの Debian パッケージ sw.log ファイルの収集期間が 3 日から 30 日に延長されたため、アプライアンスの診断パックには 30 日間の sw.log ファイルが含まれるようになりました。
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