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

このドキュメントでは、Cisco Secure Network Analytics フローセンサー 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-fsuf-ROLLUP007-7.4.0-v2-01.swu）には、次の修正が含まれています。

障害	説明
SWD-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-17936	v7.4.1 へのアップグレード時に、フローセンサー 4240 アプライアンスコンソールに [UNREG] または [未登録（Unregistered）] が表示される問題を修正しました。
SWD-18018	フローセンサー がラウンドトリップ時間（RTT）を処理していない問題を修正しました。
SWD-18028	フローセンサー バーチャルエディションが eth2 インターフェイスからの着信トラフィックを処理していない問題を修正しました。
SWD-18036	フローセンサー 4240 の nicspeed 属性が削除される問題を修正しました。
SWD-18037	Psiphon トラフィックの フローセンサー アプリケーション識別が間違っている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-fsuf-ROLLUP007-7.4.0-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-fsuf-ROLLUP007-7.4.0-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。

ℹ パッチによって Flow Sensor 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-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-16906	フローセンサー が同じサブネット上の管理/データインターフェイスをサポートしていない問題を修正しました。
	パラメータ情報の調整を flowsensor.xml に追加する手順
	1. /lancope/var/flowsensor/config/flowsensor.xml を編集します。
	2. sysctl_arp_fix value="1" を 0 から 1 に変更するか、存在しない場合は次の変数をもう 1 つ追加します。
	`<sysctl_arp_fix value="1" min="0" max="1" default="0"/>`
	`systemctl restart engine`

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-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-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。
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-17613	Flow Senor エンジンのパケットキャプチャページが読み込まれていない問題を修正しました。
SWD-17734	Avro ファイルが重複する問題を修正しました。
SWD-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-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