Stealthwatch Management Console v7.3.1 更新パッチ

このドキュメントでは、Stealthwatch Management Console アプライアンス v7.3.1 のパッチとインストール手順について説明します。

> 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-ROLLUP013-7.3.1-01.swu）には、次の修正が含まれています。

障害	説明
SWD-16951	最新のシスコのバンドルを最初にインストールすると ROLLUP パッチのインストールが失敗する問題を修正しました。
SWD-16131	[エクスポータおよびインターフェイス（Exporters & Interfaces）] が選択されているときにフロー検索の結果が表示されず、代わりに応答しないスクリプトに対して黄色のバナー警告がポップアップ表示される問題を修正しました。（LSQ-5388）

> このパッチに含まれる以前の修正については、次のページの表で説明します。

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. シスコ ソフトウェア セントラル（https://software.cisco.com）に移動します。
2. [ダウンロードとアップグレード（Download and Upgrade）] セクションで、[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）] フィールドに「**Secure Analytics (Stealthwatch)**」と入力し、**Enter** を押します。
4. アプライアンスモデルを選択します。
5. [ソフトウェアタイプの選択（Select a Software Type）] の下にある [Stealthwatchパッチ（Stealthwatch Patches）] を選択します。
6. [すべてのリリース（All Release）] を選択し、リリースバージョンを選択します。
7. パッチ更新ファイル（patch-smc-ROLLUP013-7.3.1-01.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. SMC 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、[中央管理(Central Management)] をクリックします。
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-ROLLUP013-7.3.1-01.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)] の順にクリックします。

> 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-1706	SNMP ポーリングの問題を修正しました。(LSQ-5521、LSQ-5496)
SWD-11169	Flow Collector がダウンしたときにエラーメッセージを表示する IP アドレス検索機能の問題を修正しました。
SWD-14160	セッションタイムアウトが 0 に設定されていても、非アクティブであるためユーザがセッションからログアウトされていた問題を修正しました。
SWD-15440	ANC クエリの要求とドキュメントの更新に関する問題を修正しました。(LSQ-5020)
SWD-15815	パケットリスナーで例外(UnknownHostException: 0xffbef43d18)が発生する問題を修正しました。
SWD-15831	ユーザがスマート ライセンス トランスポート ゲートウェイをカスタム トップレベル ドメイン(TLD)に登録できない問題を修正しました。(LSQ-5147)
SWD-15842	ラボの移動後にシステムアラームが Flow Collector でクリアされない問題を修正しました。
SWD-15918	CDS フロー検索にアプリケーションを含めると予期した結果が返されない問題を修正しました。

障害	説明
SWD-15934	SMC が約 200 万のユーザセッションを受信したときに、[ユーザのモニタ(Monitor Users)] ページがデータを返さない問題を修正しました。(LSQ-5102)
SWD-15963	[ホストに対してビーコンを実行(Beaconing Host)] セキュリティイベントから [関連フロー(Associated Flows)] テーブルに切り替えると結果が表示されない問題を修正しました。(LSQ-5248)
SWD-15777	権限エラーのために SecureX ピボットメニューにアクセスできない問題を修正しました。
SWD-15981	「Config changes failed(設定変更の失敗)」エラーで示される、パススループロキシの設定時にプロキシ設定が適切に保存されない問題を修正しました。(LSQ-5305)
SWD-15995	7.2.1 からのアップグレード時に SMC の [trust_sec_matrix] テーブルが表示されない問題を修正しました。
SWD-16012	パブリック SSL 証明書を使用して CTR サービスと通信しない SSE コネクタに関する問題を修正しました。
SWD-16014	SSE デバイスの登録に失敗する問題を修正しました。
SWD-16024	システム設定でデータストア アドバンス オプションの有効化を誤って妨げてしまう問題を修正しました。
SWD-16025	データベースバックアップの実行に失敗する問題を修正しました。(LSQ-5358)
SWD-16028	自己割り当て証明書が SAN フィールドと一致しない問題を修正しました。(LSQ-5375)
SWD-16049	Flow Collector の swe-detections-worker サービスが監視結果を登録していなかった問題を修正しました。

障害	説明
SWD-16057	idgen.txt の値が不必要に増加する SWD-13346 に関連した問題を修正しました。(LSQ-5237) ⚠ この問題が原因で CPU 平均負荷が通常よりも高くなっている場合には、このパッチをインストールしてから、エクスポータの XML ファイルを正しく再生成するための付加的なアクションを完了する必要があります。以下の「SWD-16057 のエクスポータの特定と削除」の手順を確認してください。この問題がお客様の環境に影響しているかどうかが不明な場合や、関連している可能性のあるエクスポータの特定に対する支援については、Stealthwatch カスタマーサポートまでお問い合わせください。
SWD-16062	サービス初期化中の再起動時にアクティブセッションがデータベースに保存されない問題を修正しました。
SWD-16068	パッケージのアップグレード中に Docker イメージがクリーンアップされない問題を修正しました。
SWD-16087	フローベースのアイデンティティがユーザレポートにない問題を修正しました。
SWD-16146	フローコレクタチャネルのダウンアラームが非アクティブになる問題を修正しました。
SWD-16175	dbadmin および読み取り専用ユーザパスワードがログにクリアテキストで表示される問題を修正しました。
SWD-16226/ SWD-16324	SNMP ポーリングの問題を修正しました。(LSQ-5521、LSQ-5496)
SWD-16340	「関連付けられたフロー」検索で、ユーザがフロー検索でフィルタリングする IP アドレスまたはプロトコルを選択できない問題を修正しました。
SWD-16406/ 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-16442	SMC がライセンスの自動再認証を行わない問題を修正しました。ライセンスの再認証は、毎日午前 0 時に行われます。(LSQ-5575)

障害	説明
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-16643	結果が CSV ファイル形式にエクスポートされたときには [ポート (Port)] 列にポートデータのみが表示され、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。(LSQ-4714)。
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。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。
SWONE-7221	SecureX セキュリティリボンのマルチユーザサポートが追加されました。これにより、SecureX、コラボレーション ソリューション アナライザ (CSA)、または Thread Grid のアカウントを持つユーザは、Stealthwatch Enterprise のセキュリティリボンを使用して認可を実行できます。 パッチのインストール後、Oauth 範囲を使用して SecureX 上で API クライアントのログイン情報を再生成し、新しいログイン情報で Stealthwatch および SecureX の設定を更新する必要があります。詳細については、『SecureX Integration Guide』を参照してください。
SWONE-11515	v7.3.1 メンテナンスに特定の TrustSec 機能が追加されました。
SWONE-12050	違反を含む TrustSec のデータアグリゲータが強化されました。
SWONE-12159	機能の向上したデータサービスバックポート TrustSec がさらに強化されました。
SWONE-12549	ヘルプの証明書情報が、証明書ガイドへのリンクに置き換わる問題を修正しました。
SWONE-12550	ホストネーミングとネットワーク インターフェイスのヘルプで、信頼ストアの順序が正しくない問題を修正しました。
SWONE-12633	拡張フロー検索 UI が強化され、選択した接続プロトコルの除外がサポートされるようになりました。

障害	説明
SWONE-12910	シスコのバンドルが更新され、core.keystore の PEM ファイルが提供されるようになりました。
SWONE-13187	セッションの期限が切れたときにログインページにリダイレクトされる機能が追加されました。
SWONE-14903/SWONE-18750	svc-db-ingest に対する 3 つのメモリ関連の変更に関する問題を修正しました。

SWD-16057 のエクスポータの特定と削除

SWD-16057 の CPU の負荷を軽減するため、次の手順を実行して、エクスポータを特定し削除します。

> ⚠ 次の手順を確認してください。この問題がお客様の環境に影響しているかどうかが不明な場合や、関連している可能性のあるエクスポータの特定に対する支援については、Stealthwatch カスタマーサポートまでお問い合わせください。

この問題が原因で CPU 平均負荷が通常よりも高くなっている場合には、このパッチをインストールしてから、エクスポータの XML ファイルを正しく再生成するための付加的なアクションを完了する必要があります。以下の手順を確認してください。この問題がお客様の環境に影響しているかどうかが不明な場合や、関連している可能性のあるエクスポータの特定に対する支援については、Stealthwatch カスタマーサポートまでお問い合わせください。

1. この問題に対処するために Tomcat を定期的に再起動する目的で作成された外部 cron ジョブを削除します（該当する場合）。
2. 次の手順に従って、patch-smc-ROLLUP001-7.3.1-02.swu をインストールします。インストールが完了したら、ステップ 3 に進みます。
3. いずれかのエクスポータに ID エクスポータとしてフラグが設定されているかどうかを確認するには、次のコマンドを使用して、SMC のコマンド ライン インターフェイスにログインします。

   ```
   #grep 'identity-source="true"'
   /lancope/var/smc/config/domain_*/exporter*.xml
   ```

   例：#grep 'identity-source="true"' /lancope/var/smc/config/domain_*/exporter*.xml
   /lancope/var/smc/config/domain_102/exporter_1855_192.168.1.1.xml:<exporter
   ip="192.168.1.1" exporter-type="exporter" identity-source="true">

   疑わしいエクスポータは、エクスポータの行の末尾に [ID] フィールドがないことで識別できます（上の例を参照）。

   新しく生成された XML がどのように表示されるか、一例を下に示します。

例：<exporter ip="192.168.1.1" exporter-type="exporter" identity-source="true" id="1">

ファイルが特定された場合には、ステップ 4 に進みます。ファイルが特定されなかった場合、それ以上のアクションは必要ありません。

4. 次のコマンドを使用して Tomcat プロセスを停止します。

```
#systemctl stop smc-manifest
```

5. ステップ 3 のファイル出力のリストを参照し、次のコマンドを使用して削除します。

```
#rm -f <path_to_xml_file>
```

6. ステップ 3 で見つかったエクスポータからフローを受信するフローコレクタのコマンド ライン インターフェイスにログインします。同じエクスポータを .xml ファイルから手動で削除します。
   a. フローコレクタエンジンを停止して、次のコマンドを使用します。
      `>service engine stop`
   b. 次のコマンドを使用して、フローコレクタの設定ディレクトリに移動します。
      `>cd /lancope/var/sw/today/config`
   c. exporters.xml のバックアップコピーを作成します。
      `>cp exporters.xml /lancope/var/exporters.xml.bak`
   d. ステップ 3 で見つかったエクスポータを削除するには、vi または任意のエディタを使用します。特定のエクスポータスタンザの表示例を以下に示します。疑わしい IP を検索し、[エクスポータ（exporter）] タグ間のコンテンツを削除します。完了したら、必ずファイルを保存してください。

      例：<exporter ip="192.168.1.1">
      <interface if-index="1" active="1" speed-in="1000000000" speed-out="1000000000" threshold-in="90" threshold-out="90"/>
      </exporter>

7. 次のコマンドを使用して、フローコレクタエンジンを再起動します。

```
service engine start
```

8. SMC SSH コンソールに戻り、次のコマンドを入力します。

```
systemctl start smc-manifest
```

9. 両方のコンソールからログアウトします。これらの変更により、ID タイプアプライアンスに関連したエクスポータ コンフィギュレーション ファイルの再作成が可能になります。

新しい設定ファイルが正しくフォーマットされ、この問題が原因で発生していた CPU の負担が軽減されます。

> idgen.txt が 65,000 を超える場合は、再作成が必要な構成ファイルが存在する可能性があるため、Cisco Stealthwatch サポートにお問い合わせください。

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。
- Cisco Stealthwatch サポートのお問い合わせ先:
  - 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