Cisco Secure Network Analytics

リリースノート 7.5.0

目次

はじめに

概要

このドキュメントでは、Cisco Secure Network Analytics（旧 Stealthwatch）v7.5.0 リリースの新機能と改善点、バグ修正、および既知の問題について説明します。

Secure Network Analytics の詳細については、Cisco.com をご覧ください。

用語

このガイドでは、Secure Network Analytics Flow Sensor Virtual Edition（VE）などの仮想製品を含むすべての Secure Network Analytics 製品に対し「**アプライアンス**」という用語を使用しています。

「**クラスタ**」は、Manager が管理する Secure Network Analytics アプライアンスのグループです。

更新する前に

更新プロセスを開始する前に、『Update Guide』を確認してください。

ソフトウェア バージョン

アプライアンスソフトウェアをバージョン 7.5.0 に更新するには、アプライアンスにバージョン 7.4.0、7.4.1、または 7.4.2 がインストールされている必要があります。以下の点にも注意してください。

VMware 互換性変更の通知

> Secure Network Analytics v7.5.0 は、VMware 7.0 または 8.0 と互換性があります。VMware 6.0、6.5、または 6.7 と Secure Network Analytics v7.5.x はサポートしていません。詳細については、『vSphere 6.0, 6.5, and 6.7 End of General Support』の VMware のマニュアルを参照してください。

サポートされているハードウェア プラットフォーム

Secure Network Analytics は、最新世代の UCS ハードウェア（M6）で使用できます。各システムバージョンでサポートされているハードウェア プラットフォームについては、Hardware and Version Support Matrix を参照してください。

CIMC ファームウェアバージョン

共通の更新プロセスまたはハードウェアに固有の共通の更新パッチを使用して、CIMC ファームウェアバージョンを必ず更新してください。

次の表に示すアプライアンスの場合、M4 共通更新プロセスは UCS C シリーズ M4 ハードウェアに適用され、M5 共通更新パッチは M5 ハードウェアに適用され、M6 共通更新パッチは M6 ハードウェアに適用されます。

M4 ハードウェア	M5 ハードウェア	M6 ハードウェア
SMC 2200（Manager 2200）	SMC 2210（Manager 2210）	SMC 2300（Manager 2300）
FC 4200	FC 4210	FC 4300

M4 ハードウェア	M5 ハードウェア	M6 ハードウェア
FC 5020 エンジン	_	_
FC 5020 データベース	_	_
FC 5200 エンジン	FC 5210 エンジン	_
FC 5200 データベース	FC 5210 データベース	_
FS 1200	FS 1210	FS1300
FS 2200	_	_
FS 3200	FS 3210	FS3300
FS 4200	FS 4210 / FS 4240	FS4300
UD 2200	UD 2210	_
_	DS6200	DN6300

シスコのバンドル

最新のシスコのバンドルに共通の更新パッチがインストールされていることを確認してください。詳細については、Cisco Bundles Common Update Patch の readme を参照してください。このパッチでは、厳選したルート認証局（CA）の事前検証済みのデジタル証明書を提供しています。これにはシスコのサービスとの接続に使用するコア証明書バンドルと、シスコ以外のサービスとの接続に使用する外部証明書バンドルが含まれます。

MongoDB

v7.5.0 への更新の際に、MongoDB は v6.0.9 にアップグレードされます。

CPU 命令セット要件：CPU が AVX/AVX2 命令セットに対応していることを確認します。ESXi の場合は、VM ハードウェアバージョン 11 以上を選択します。KVM の場合は、ホストパススルーを使用することを推奨します。

スマートライセンスのトランスポート設定

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。

> ⚠ アプライアンスを v7.4.1 以前から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。

高可用性

UDP Director で高可用性が構成されていて、Secure Network Analytics を v7.5.0 に更新する予定の場合は、更新を開始する前に、UDP Director の高可用性設定を必ず書き留めておいてください。更新が完了したら、高可用性を再構成する必要があります。Secure Network Analytics の更新の詳細については、更新ガイドを参照してください。

サードパーティ製アプリケーション

Secure Network Analytics は、アプライアンスへのサードパーティ製アプリケーションのインストールをサポートしていません。

アプリケーションのバージョンの互換性

> 以前にアプリをインストールしたことがある場合は、インストールする Secure Network Analytics のバージョンと互換性があることを確認します。

インストールされているアプリケーションのリストを確認する方法と最新の Cisco Secure Network Analytics アプリケーションの互換性情報を確認する方法については、Secure Network Analytics アプリケーションのバージョン互換性マトリックスを参照してください。

ブラウザ

- **互換性のあるブラウザ**：Secure Network Analytics は Chrome、Firefox、および Edge の最新のラピッドリリースをサポートしています。
- **Microsoft Edge**：Microsoft Edge には、ファイル サイズの制限がある可能性があります。Microsoft Edge を使用して、ソフトウェア アップデート ファイル（SWU）をアップロードしないことをお勧めします。
- **ショートカット**：ブラウザのショートカットを使用して、いずれかの Secure Network Analytics アプライアンスのアプライアンス管理インターフェイスにアクセスしている場合、更新プロセスの完了後はショートカットが機能しないことがあります。その場合は、ショートカットを一旦削除してから再作成してください。
- **証明書**：一部のブラウザでは、アプライアンス アイデンティティ証明書の有効期限の要件が変更されています。アプライアンスにアクセスできない場合は、『SSL/TLS Certificates for Managed Appliances Guide』を参照して証明書を置き換えるか、Cisco サポートまでお問い合わせください。

代替アクセス

> 今後のサービスのニーズを想定し、Secure Network Analytics アプライアンスにアクセスする代替方法を有効にしておく必要があります。

次のいずれかのオプションを使用して Secure Network Analytics アプライアンスにアクセスできることを確認してください。

仮想アプライアンス：コンソール（コンソールポートへのシリアル接続）

KVM を介してアプライアンスにアクセスするには、Virtual Manager のドキュメントを参照してください。または、**VMware** を介してアプライアンスに接続するには、vSphere の vCenter Server Appliance 管理インターフェイスのドキュメントを参照してください。

ハードウェア：コンソール（コンソールポートへのシリアル接続）

ラップトップまたはモニター付きキーボードを使用してアプライアンスに接続するには、「インストールとアップグレードガイド」ページにリストされている最新の『Secure Network Analytics Hardware Installation Guide』を参照してください。

ハードウェア：CIMC（UCS アプライアンス）

CIMC を介してアプライアンスにアクセスするには、『Cisco Integrated Management Controller (CIMC) Configuration Guides』ページにリストされているプラットフォームの最新のガイドを参照してください。

別の方法

今後サービスが必要になった場合に備えて、次の手順に従い、Secure Network Analytics アプライアンスにアクセスする別の方法を有効にします。

仮想またはハードウェアの方法を使用してアプライアンスにログインできない場合は、アプライアンスのネットワーク インターフェイスで一時的に SSH を有効にできます。

> ⚠ SSH を有効にすると、システムの侵害リスクが増加します。必要な場合にのみ SSH を有効にし、使用が終了したら無効にすることが重要です。

1. Manager にログインします。
2. **[構成（Configure）]** > **[グローバル集中管理（GLOBAL Central Management）]** を選択します。
3. アプライアンスの [アクション（Actions）] 列の [••• （**省略符号**）アイコン] をクリックします。
4. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
5. [アプライアンス（Appliance）] タブを選択します。
6. [SSH] セクションを見つけます。
7. [SSHの有効化（Enable SSH）] チェックボックスをオンにして、アプライアンスへの SSH アクセスを許可します。
8. [設定の適用（Apply settings）] をクリックします。
9. 画面に表示される指示に従って、変更を保存します。

> ⚠ SSH は、使用が終了したら必ず無効にしてください。

Data Store のプライベート LAN の設定と Data Node の拡張

v7.4.1 以降、Secure Network Analytics は プライベート LAN の IP アドレスに特定の要件を適用します。プライベート LAN の IP アドレスを使用して設定されている Data Node のすべてが次の要件を満たしていることを確認してください。

- 最初の 3 オクテットが **169.254.42** であること。
- サブネットが **/24** であること。

> ⓘ 例：169.254.42.**x**/24（**x** はサイトによって割り当てられた番号（2 ～ 255））

詳細については、シスコサポートに問い合わせてください。

Data Store アプライアンスのサポート

次の表で、Data Store アプライアンスのサポートについて説明します。

アプライアンス	必須かどうか	サポートされるモデル
Data Store	Yes	• DS 6200 マルチノード（v7.4 以降）またはシングルノード（v7.4.1 以降）、バーチャルエディション • DN 6300 マルチノードまたはシングルノード（v7.4.2 以降）、バーチャルエディション
Manager	Yes	• Manager 2200、バーチャルエディション • Manager 2210 または Manager バーチャルエディション（v7.4 以降）。バーチャルエディションでは 4 つのモデルが利用可能 • Manager 2300 または Manager バーチャルエディション（v7.4.2 以降）。
Flow Collector	Yes	• Flow Collector 4200 番台、5200 番台、Virtual Edition • Flow Collector 4210 番台または Flow Collector Virtual Edition（v7.4 以降）* • Flow Collector 4300 番台または Flow Collector Virtual Edition（v7.4.2 以降）* • Flow Collector 5210 番台または Flow Collector Virtual Edition（v7.4 以降）* * バーチャルエディションでは 4 つのモデルが利用可能
Flow Sensor	No	• M5SX 以前の世代の場合、v7.4 以降の任意のモデルです。 • M6SX 世代の場合、Flow Sensor は v7.4.2 以降でのみサポートされます。
UDP Director	No	• v7.3 以降のすべてのモデル

Data Node の混在はサポートされていません。データストアはすべて仮想ハードウェアであるか、すべてハードウェアである必要があり、同じ世代のハードウェア（すべて DS 6200 またはすべて DN 6300）である必要があります。

新機能

Secure Network Analytics v7.5.0 リリースの新機能と改善点は次のとおりです。

Analytics

Cisco XDR へのアラートの送信

Manager 内の Analytics 機能を使用して、Cisco Secure Network Analytics アラートを Cisco XDR に送信できるようになりました。Cisco XDR にアラートを送信すると、SecureX にも送信されることに注意してください。

初期設定

Cisco XDR にアラートを送信するには、ユーザーにアクセス権が必要です。ユーザーにアクセス権を付与するには、API クライアントを設定する必要があります。

Cisco XDR にログインし、新しい API クライアント設定を完了します（[管理（Administration）] > [API クライアント（API Clients）]）。[クライアント名（Client Name）] フィールドに、エントリを入力します。このエントリは、単に、XDR の [クライアント（Client）] 列に表示されるラベルになります。[スコープ（Scopes）] セクションで、[すべて選択（Select All）] をクリックして、すべてのチェックボックスをオンにします。Cisco XDR の詳細については、Cisco XDR のサイトを参照してください。

Cisco XDR へのアラートの送信

Analytics 内で Cisco Secure Network Analytics アラートを送信するには、[アラートの詳細（Alert Details）] ページの [インシデントの送信（Post an Incident）] フィールドを使用するか、応答管理でルールを作成します。

- [アラートの詳細（Alert Details）] ページにアクセスするには、メインメニューから [モニター（Monitor）] > [アラート（Alerts）] を選択します。[アラート概要（Alerts Summary）] が開きます。アラートを選択すると、そのアラートの [アラートの詳細（Alert Details）] ページが開きます。
- [応答管理ルール（Response Management Rules）] ページにアクセスするには、[設定（Configure）] > [検出（DETECTION）] > [応答管理（Response Management）] > [ルール（Rules）] を選択します。

> [インシデントの送信（Post an Incident）] フィールドを使用するには、まず SecureX 設定を作成する必要があります。方法については、『Cisco SecureX Integration Guide』を参照してください。

Secure Network Analytics アラートを Cisco XDR に送信する方法の詳細については、ヘルプの「Analytics：Cisco XDR へのアラートの送信」トピックを参照してください。

応答管理を使用したアラートの送信

また、応答管理内で電子メール、syslog、および webhook アクションタイプを使用して Cisco Secure Network Analytics アラートを送信できるようになりました（現在、これらのアクションタイプを使用して Cisco Secure Network Analytics アラームを投稿できるのと同様です）。応答管理を使用した Secure Network Analytics アラートの送信の詳細については、ヘルプの「応答管理：ワークフロー」トピックを参照してください。

アプライアンス セットアップ ツール

アプライアンスの設定にアプライアンス セットアップ ツールは使用されなくなりました。アプライアンスへの初回ログイン時に、初回セットアップツールを使用して各アプライアンスを設定し、Manager で管理できるようにします。詳細については、『 System Configuration Guide』を参照してください。

データベースのバックアップ（非 Data Store ドメイン）

非 Data Store ドメインのデータベースバックアップを作成するときに、データベースのスナップショットを削除する必要がなくなりました。詳細については、『 System Configuration Guide』を参照してください。

Data Store のバックアップ

Data Store のバックアッププロセスが更新され、アプライアンスコンソール（SystemConfig）を介して実行されるようになりました。[Data Storeのバックアップ（Data Store Backup）] メニューが追加されました。このメニューでは、リモートホストの設定、バックアップのテストとサイズの見積もりのための Data Store バックアップのリハーサルの実行、バックアップ操作の管理、およびバックアップの実行を行うことができます。詳細については、『System Configuration Guide』を参照してください。

エンドポイントライセンスと Network Visibility Module

v7.5.0 では、Cisco Secure Client（AnyConnect を含む） Network Visibility Module（NVM）トラフィックを取り込む Data Store 展開に次の機能が追加されました。

- NVM トラフィックエンドポイント IP を介したホストグループへのエンドポイントの追加
- エンドポイント接続に基づくカスタム セキュリティ イベントの作成
- NVM トラフィックに基づく NetFlow 検出
- Report Builder でのオフネットワークフローの保存と表示

Flow Collector の詳細設定に、**nvm_to_flow_cache** と **nvm_filter_untrusted_flows** の 2 つの新しいフィールドが追加されました。どちらもデフォルトは **0** であり、NVM の信頼できないトラフィックの処理を改善するには **1** に変更する必要があります。詳細については、『Secure Network Analytics Endpoint License and Network Visibility Module Configuration Guide v7.5.0』を参照してください。

ネットワーク検出のファイアウォールログ

Cisco Security Analytics and Logging（オンプレミス） データに基づくネットワーク検出を追加しました。この設定を有効にすると、トラフィックパターン、リスク、および攻撃の範囲をより詳細に把握できます。

- **設定**：『Cisco Security Analytics and Logging (On Premises): Firewall Event Integration Guide』の指示に従ってください。
- **クエリ**：フロー検索、カスタム セキュリティ イベント、およびレポートビルダーでファイアウォールログをクエリできます。

ホストグループ管理

ホストグループ管理が更新され、IP アドレスが英数字順にソートされるようになりました。ホストグループ管理の詳細については、ヘルプの「ホストグループの管理と設定」を参照してください。

IPv6 のサポート

v7.5.0 では、IPv6 およびデュアルスタックに対して次のサポートが提供されます。

アプライアンス/ デスクトップクライアント	IPv6 およびデュアルスタックの サポート	IPv4 のみサポート
Manager	✓	✓
Flow Collector	✓	✓
Flow Sensor	✓	✓
Data Node		✓
デスクトップ クライアント		✓
UDP Director*		

*UDP Director サポート

- **M5 UDP Director**：M5 UDP Director（UD2210）を設定する際には、[IPv4] と [デュアルスタック（Dual Stack）] が選択できます。[デュアルスタック（Dual Stack）] オプションを選択すると、UDP は IPv4 経由でのみ転送を行います。ただし、管理には IPv6 を使用できます。UDP Director の IPv6 転送の詳細については、『Cisco Telemetry Broker ユーザーガイド』を参照してください。
- **M4 UDP Director**：M4 UDP Director（UD2200）を設定する場合、IPv4 のみがサポートされます。M4 および M5 UDP Director の詳細については、「**CIMC ファームウェアバージョン**」を参照してください。
- **ネットワークモードの変更**：アプライアンスのネットワークモードの変更については、『System Configuration Guide』を参照してください。

ネットワーク管理

アプライアンスのネットワークモードは次のいずれかの方法で変更できます（Data Node アプライアンスと UDP Director を除きます）。

- 「IPv4 のみ」から「デュアルスタック」
- 「IPv4 のみ」から「IPv6 のみ」
- 「デュアルスタック」から「IPv6 のみ」
- 「デュアルスタック」から「IPv4 のみ」
- 「IPv6」から「IPv4 のみ」
- 「IPv6 のみ」から「デュアルスタック」

Data Node でサポートされるネットワークモードは IPv4 のみです。Data Node のネットワークモードの変更は、v7.5.0 ではサポートされていません。

M5 UDP Director（UD2210）を設定する際には、[IPv4] と [デュアルスタック（Dual Stack）] が選択できます。[デュアルスタック（Dual Stack）] オプションを選択すると、UDP は IPv4 経由でのみ転送を行います。ただし、管理には IPv6 を使用できます。UDP Director の IPv6 転送の詳細については、『Cisco Telemetry Broker ユーザーガイド』を参照してください。

M4 UDP Director（UD2200）を設定する場合は、IPv4 のみがサポートされます。M4 および M5 UDP Director の詳細については、「**CIMC ファームウェアバージョン**」を参照してください。

アプライアンスのネットワークモードの変更については、『System Configuration Guide』を参照してください。

詳細については、『System Configuration Guide』を参照してください。

パケットキャプチャ

パケットキャプチャのプロセスは v7.5.0 で更新されました。詳細については、ヘルプの「パケットキャプチャ」および「Manager でのパケットキャプチャ」のトピックを参照してください。

パスワード

v7.5.0 では、次のパスワード変更が行われました。

- root のデフォルトパスワードがなくなり、root パスワードアクセスが制限されました。詳細については、「**制限されたコマンド ライン インターフェイス アクセス**」を参照してください。
- パスワード リセット ブート オプションと関連する SystemConfig プラグインが削除されました。
- admin と sysadmin パスワードをデフォルトにリセットできます。root アカウントにはパスワードを使用してアクセスできないため、パスワードのリセットメカニズムはありません。詳細については、「**制限されたコマンド ライン インターフェイス アクセス**」を参照してください。
- Manager での admin パスワードをリセットするためのプロセスを変更しました。このプロセスは、[セキュリティ（Security）] メニューのアプライアンスコンソール（SystemConfig）を介して処理されるようになりました。詳細については、『System Configuration Guide』を参照してください。

制限されたコマンド ライン インターフェイス アクセス

v7.5.0 リリースでセキュリティ対策が追加されたため、コマンド ライン インターフェイス アクセスが制限されました。トラブルシューティングと シスコ サポート には、引き続きアプライアンスコンソール（SystemConfig）を使用できます。次の状況では、シスコ サポート を使用して一時的なコマンド ライン インターフェイス アクセスを取得できます。

- アクセスは、トラブルシューティングまたはリカバリにのみ使用されます。
- アクセスは、シスコのコマンド ライン インターフェイス アクセス ポリシーに従って使用されます。

Cisco Secure Network Analytics から次へのオンプレミスフローの送信：Secure Cloud Analytics

オンプレミスフローを送信するための Flow Collector 設定を、Cisco Secure Network Analytics から Cisco Secure Cloud Analytics に移動しました。手順の一環として、Flow Collector アプライアンスコンソール（SystemConfig）にログインします。詳細については、『Send On-Premises Flows from Cisco Telemetry Broker or Secure Network Analytics to Secure Cloud Analytics Guide』を参照してください。

SSL/TLS 証明書

SSL/TLS アプライアンス ID 証明書の要件、セキュリティチェック、およびワークフローを更新しました。すべてのワークフローで正常に設定するために、必ず『SSL/TLS Certificates for Managed Appliances Guide』に記載されている手順に従ってください。

TLS のバージョン

アプライアンスの TLS バージョン設定を次のように選択できます。v7.5.0 にアップグレードすると、バージョン 1.2 および 1.3 がデフォルトでサポートされます。

- TLS 1.2 および 1.3（デフォルト）
- TLS 1.3 のみ（Data Store ではサポートされていません）

信頼ストアへの証明書の追加（カスタム証明書）

アプライアンス アイデンティティ証明書をカスタム証明書に置き換えるには、以前はアイデンティティ証明書とチェーン（ルート証明書と中間証明書）を各アプライアンスの信頼ストアに個別にアップロードする必要がありました。

v7.5.0 では、選択した手順に応じて、自己署名証明書またはルート証明書をアプライアンスの信頼ストアに追加するだけで済みます。証明書の要件および手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

Central Management へのアプライアンスの追加

多くの証明書関連のワークフローには、Central Management へのアプライアンスの追加が含まれています。このメニューは、アプライアンス セットアップ ツールからアプライアンスコンソール（SystemConfig）に移動されました。

期限が切れていないシスコの自己署名アプライアンス アイデンティティ証明書の置換（証明書の更新）

> ⚠ アプライアンス アイデンティティ証明書は、期限切れになる前に必ず置き換えてください。期限日を確認するには、『SSL/TLS Certificates for Managed Appliances Guide』に記載されている手順に従います。

既存の証明書の有効期限が切れていない場合に、新しいシスコの自己署名アプライアンス アイデンティティ証明書を生成するためのワークフローが簡素化されました。

Manager アプライアンスコンソール（SystemConfig）の［証明書の更新（Certificate Refresh）］メニューを使用して、すべての管理対象アプライアンスまたは選択した個々のアプライアンスのアイデンティティ証明書を生成できます。

- **ホスト情報**:アプライアンスのホスト情報(IP アドレス、ホスト名、ドメイン名)は保持されます。
- **手順**:『SSL/TLS Certificates for Managed Appliances Guide』[英語] の手順に従います。
- **カスタム証明書**:アプライアンス アイデンティティ証明書は、この証明書更新手順でシスコの自己署名アプライアンス アイデンティティ証明書に自動的に置き換えられます。カスタム証明書を使用するには、『SSL/TLS Certificates for Managed Appliances Guide』[英語] の「SSL/TLS アプライアンス アイデンティティ証明書の置換」の手順に従います。

Manager ユーザーインターフェイス

Manager UI のフォントと色を変更しました。

Network Diagrams

v7.5.0 では、Network Diagrams を別のアプリケーションからコアの Secure Network Analytics に移動しました。Secure Network Analytics を v7.4.x から v7.5.0 に更新する場合、すべての図が保持されます。ただし、この更新の一環として、メニューの別の場所から Network Diagrams アプリケーションにアクセスするようになりました(以下を参照)。

> ⚠ 既存の Network Diagrams アプリケーションはアンインストールしないでください。Network Diagrams をアンインストールすると、お使いの図や一時ファイルを含めて、関連付けられているすべてのファイルが削除されます。

『更新ガイド』の手順に従ってください。Secure Network Analytics を v7.5.0 に更新したら、次のように Network Diagrams にアクセスします。

1. マネージャ にログインします。
2. [レポート(Report)] メニューを選択します。
3. [Network Diagrams] を選択します。
4. 手順については、?(**ヘルプ**)アイコン > **[ヘルプ(Help)]** をクリックしてください。

Secure Network Analytics アプリケーション

Secure Network Analytics アプリケーションは、Secure Network Analytics の機能を強化および拡張する、独自にリリース可能なオプションの機能です。

Secure Network Analytics アプリケーションのリリーススケジュールは、通常の Secure Network Analytics のアップグレードプロセスとは無関係です。そのため、Secure Network Analytics のコアリリースとリンクさせなくても、必要に応じて Secure Network Analytics アプリケーションを更新できます。

Secure Network Analytics の新しいリリースに対応するように設計されたアプリが、すぐにインストールできない場合があります。アプリケーションの最新バージョンが提供されるまでに数週間かかる場合もあります。

最新の Secure Network Analytics アプリケーションの情報と可用性については、次を参照してください。

- Secure Network Analytics アプリケーションのバージョン互換性マトリクス
- Secure Network Analytics アプリケーションのリリースノート

アプリケーションへのアクセス

v7.5.0 にアップグレードしたら、次の手順を実行してアプリケーションにアクセスします。

1. メインメニューから [構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
2. Secure Network Analytics [アプリケーションマネージャ(App Manager)] タブをクリックします。

ヘルプへのガイドの移動

以前は、次のガイドを cisco.com に掲載していました。v7.5.0 では、この情報はヘルプでのみ使用できます。

ガイドの名前	ヘルプトピック
アラーム抑制	アラーム抑制の概要
デフォルトのカスタム セキュリティ イベントの設定	• カスタムポリシーの設定(カスタム セキュリティ イベント) • ホストグループの管理および設定
外部ルックアップ機能の使用	外部ルックアップの管理

既知の問題:カスタム セキュリティ イベント

サービス、アプリケーション、またはホストグループを削除しても、カスタム セキュリティ イベントからは自動的に削除されません。そのため、カスタム セキュリティ イベントの設定が無効になり、アラームの欠落や誤報が発生する可能性があります。同様に、脅威フィードを無効にすると、追加されたホストグループのスレッドフィードが削除されるため、カスタム セキュリティ イベントを更新する必要があります。

推奨事項は次のとおりです。

- **確認**:次の手順を使用して、すべてのカスタム セキュリティ イベントを確認し、それらが正確であることを確認します。
- **計画**:サービス、アプリケーション、またはホストグループを削除する前、または脅威フィードを無効にする前に、カスタム セキュリティ イベントを確認して、それらを更新する必要があるかどうかを判断してください。

1. Manager にログインします。
2. [設定(Configure)] > [検出ポリシー管理(DETECTION Policy Management)] を選択します。
3. カスタム セキュリティ イベントごとに、⋯ (**省略符号**)アイコンをクリックし、[編集(Edit)] を選択します。
    - **確認**:カスタム セキュリティ イベントが空白であるかルール値がない場合は、イベントを削除するか、イベントを編集して有効なルール値を使用します。
    - **計画**:削除または無効化する予定のルール値(サービスやホストグループなど)がカスタム セキュリティ イベントに含まれている場合は、イベントを削除するか、イベントを編集して有効なルール値を使用します。

詳細な手順については、? (**ヘルプ**)アイコンをクリックしてください。

既知の問題

このセクションでは、このリリースに存在する可能性のあるバグ（欠陥）に関する情報を提供します。各欠陥には、対応する Cisco Defect and Enhancement Tracking System（CDETS）番号があります。CDETS リンクをクリックすると、問題の詳細が表示されます。

CDETS	タイトル
CSCwi37680	Data Node がリカバリしている場合、Data Store Retention Manager がドロップするデータが多すぎることがある
CSCwi33350	FQDN サーバーアドレスを使用して LDAP ユーザー認証サービスを追加すると、Manager に default_error が表示される
CSCwi37953	フィルタを使用したレポートビルダーの検索結果にデータが表示されない
CSCwi37948	Flow Collector の［設定（Configuration）］ページで変更を保存すると、Flow Collector に 500 エラーが表示される
CSCwi37946	SWAEntity（または SWAType）の XSD で partner-ip-address が許可されず、アップグレードの問題が発生する
CSCwi37945	アップグレード後に、セカンダリ Manager が Flow Collector 5000 の認識に失敗する
CSCwi37950	Update Manager が swu（ファームウェアやパッチ更新ファイル）をアップロードできない
CSCwi39002	レポートビルダーに、スペースで区切られた IP アドレスの無効な IP アドレスまたは範囲エラーが表示されない
CSCwi37944	Central Management のバックアップ設定を復元すると、グローバル脅威アラートの設定が無効になる
CSCwi37947	Central Management の［アプライアンス設定の編集（Edit Appliance Configuration）］の IPv6 専用モードのアプライアンスに、eth0 の IPv4 と IPv6 の両方が表示される
CSCwi37952	IPv6 専用モードで IPv6 アドレスを変更すると、システムが常にユーザーに証明書の再生成を求めるプロンプトを表示する
CSCwi19387	レポートビルダーのフロー収集ステータスレポートがすべての NetFlow バージョンをサポートしていない
CSCwi37949	アプライアンス アイデンティティを置き換えるときにカスタム証明書が拒否された場合、Central Management によって新しいファイルのアップロードがブロックされる

CDETS	タイトル
CSCwi39016	デスクトップクライアントの異なるドメインから ISE を編集すると、デフォルトのドメイン ISE ページが開く
CSCwi37951	Network Diagrams から [ポリシー管理（Policy Management）] を選択すると、リレーションシップポリシーにホストグループが表示されない
CSCwi37954	アップグレード後に IPv6 プロキシを使用すると、デバイス登録ステータスが [登録済み（Enrolled）] から [使用不可（Unavailable）] に変更される
CSCwh66159	ホストグループの設定に失敗すると、Manager のファイルシステムがリカバリファイルで 100% 埋め尽くされる
CSCwe25793	FIPS/CC モードが有効になっている場合、Data Node が UI からのファイルの閲覧をブロックできない

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。
- 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

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 12 月 13 日	最初のバージョン。
1_1	2024 年 1 月 22 日	一般提供（GA）。「新機能」セクションの「Analytics」の内容を更新しました。

リリースサポート情報

リリース 7.5.0 の公式一般公開（GA）日は 2024 年 1 月 22 日です。

一般的なソフトウェアのメンテナンスサポート、パッチ、一般的なメンテナンスリリースに関するサポートタイムライン情報、もしくは Cisco Secure Network Analytics ソフトウェア ライフサイクル サポートに関するその他の情報については、『Cisco Secure Network Analytics® Software Lifecycle Support Statement』[英語] を参照してください。

著作権情報