Cisco Secure Network Analytics

Host Classifier リリースノート v4.0.2

目次

はじめに **3**
- 概要 3
- アプリケーションについて 3
  - アプリケーションの互換性に関する通知 5
- はじめる前に 5
  - ホストグループ 5
- Cisco Software Central からの Host Classifier SWU ファイルのダウンロード 5
- Central Manager での Host Classifier のアップロード 6
  - リソース使用状況 6
  - フェールオーバー 6
  - バックアップ 7
- Host Classifier のインストール 7
- オンライン ヘルプ 7
- 修正点 8
  - バージョン 4.0.2 8
  - バージョン 3.1.1 10
  - バージョン 3.1.0 10
  - バージョン 3.0.0 11
- 連絡先 12

変更履歴 **13**

リリースサポート情報 **14**

はじめに

このドキュメントでは、Host Classifier v4.0.x の一般的な情報と、関連した改善点およびバグ修正について説明します。Host Classifier の最新バージョンは v4.0.2 です。

> Host Classifier は、Secure Network Analytics データストア（v7.3.0 で利用可能）が展開されている Secure Network Analytics では機能しません。

概要

Host Classifier は、トラフィックを監視し、特定のクエリに一致するホストグループを候補として提示することで、ホストを複数の論理グループに分類するのに役立ちます。候補が提示された後、ユーザーはその候補を確認、除外、または無視できます。[選択されたホストを除外（Exclude Selected）] をクリックすると、その時点から 30 日間、Secure Network Analytics には [分類の検索（Classification Searches）] ナビゲーションウィンドウで選択したホストグループの今後の候補に除外したホストが含まれなくなります。30 日が経過すると、このホストは今後のクエリで再び候補として提示され、再評価の対象となる可能性があります。

Host Classifier はすべてのドメインをモニターしますが、Web ビューは確認対象のドメインによって定義されます。ドメインごとに個別の分類タイプを設定できます。

> 個々の分類子の関連付けられたホストグループ（一意の ID）が Secure Network Analytics に存在しない場合、その分類子は機能しません。

アプリケーションについて

Cisco Secure Network Analytics（以前の Stealthwatch）の v7.0.0 でアプリケーションを導入しました。Cisco Secure Network Analytics アプリケーションは、スマートフォンにインストールするアプリケーションと概念的に似ています。これらは、Cisco Secure Network Analytics の機能を強化および拡張するオプションの機能です。これらのアプリケーションのリリーススケジュールは、通常の Cisco 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、これらのアプリケーションは、コアの Cisco Secure Network Analytics リリースにリンクすることなく必要に応じてアプリケーションを更新でき、Cisco Secure Network Analytics システムを更新することなくインストールできます。

[アプリケーションマネージャ（App Manager）] ページを使用して、インストールした Cisco Secure Network Analytics アプリケーションを管理します。このページから、アプリケーションのインストール、更新、アンインストール、またはステータスの確認を実行できます。アプリケーションをインストールすると、Secure Network Analytics Web アプリのダッシュボードにある適切なオプションからアクセスできます。ユーザー権限によって、表示できるアプリケーションが決まります。

Secure Network Analytics を更新しても、現在インストールされているアプリケーションは保持されます。ただし、一部のアプリケーションでは、Cisco Secure Network Analytics の最新バージョンへのアップグレードが必要になる場合があります。さらに、Cisco Secure Network Analytics システムをアップグレードする際に、一部またはすべてのアプリケーションをアップグレードする必要が生じる場合があります。Cisco Secure Network Analytics の特定のバージョンでサポートされるアプリケーションのバージョンを確認するには、「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。

> アプリケーションをインストールまたはアンインストールできるのは、プライマリ管理者だけです。

⚠ アプリケーションを新しいバージョンに更新するには、新しいバージョンを既存のバージョンにそのままインストールします。既存のアプリケーションをアンインストールする必要はありません。アプリケーションをアンインストールすると、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。

ステータス	定義	対処
UpToDate	インストール済みのアプリケーションは最新バージョンです。	特に対処の必要はありません。
UpdateAvailable	新しいバージョンの Secure Network Analytics にアップグレードしています。既存のアプリケーションは、このバージョンの Secure Network Analytics でサポートされていますが、このアプリケーションの新しいバージョンがあります。	必要な場合は、Cisco Software Central にアクセスして最新バージョンのダウンロードとインストールを行ってください（これにより既存のバージョンが置き換えられます）。
UpgradeRequired	新しいバージョンの Secure Network Analytics にアップグレードしましたが、既存のアプリケーションは、現在使用している Secure Network Analytics バージョンでサポートされていません。	このアプリケーションを引き続き使用するには、Cisco Software Central にアクセスして最新バージョンのダウンロードとインストールを行ってください（既存のバージョンが置き換えられます）。
AppNotSupported	新しいバージョンの Secure Network Analytics にアップグレードしています。このアプリケーションは、現在使用しているバージョンの Secure Network Analytics でサポートされなくなる可能性があります。このアプリケーションが廃止されたか、このアプリケーションの新しいバージョンがまだリリースされていない可能性があります。	新しいバージョンがリリースされたかどうかを確認するには、Cisco Software Central に移動します。
Error	関連付けられているアプリケーションのインストール、アップグレード、または削除プロセスが正常に完了しませんでした。	シスコのサポートに連絡してください（サポートの連絡先情報については、本書の最後のセクションを参照）。このアプリケーションが、部分的にインストール、アップグレード、または削除された可能性があります。その場合は修正が必要です。

アプリケーションの互換性に関する通知

Cisco Secure Network Analytics のカスタマーエクスペリエンスをシンプルにするため、任意の時点でインストールできる Cisco Secure Network Analytics アプリケーションのバージョンは 1 つのみになります（アプリストアモデルと同様）。アプリケーションの互換性については最大限尽力していますが、アプリケーションのすべてのバージョンが Cisco Secure Network Analytics のすべてのバージョンと互換性があるわけではありません。

シスコでは、Cisco Secure Network Analytics アプリケーションをいつでも中止する権利を留保しています。廃止の根拠には以下の状況が含まれますが、これらに限定されません。

1. アプリケーションによって提供される同等の機能が、アプリケーションの新しいバージョン、新しいアプリケーション、または Cisco Secure Network Analytics の機能を介して、他の方法でも提供されるようになりました。
2. アプリケーションによって提供される機能が、当社のカスタマーベースに関連があるか、または役立つとみなされなくなった場合。

Cisco Secure Network Analytics アプリケーションを中止すると決定された場合、中止が実行される少なくとも 60 日前に通知されます。Cisco Secure Network Analytics アプリケーションは現在 Cisco Secure Network Analytics ライセンスに含まれていますが、今後シスコでは特定の Cisco Secure Network Analytics アプリケーションのライセンス料を請求する権利を留保しています。

はじめる前に

Host Classifier をダウンロードしてインストールする前に、この通知をお読みください。

> Host Classifier は、輸出管理に関する法律および規制の対象となります。Host Classifier をダウンロードすることにより、お客様は、当該政府機関からの事前の書面による許可なく、Host Classifier を禁止された宛先、エンドユーザー、または最終用途向けに故意に（直接的または間接的に）輸出または再輸出しないことに同意したことになります。

ホストグループ

各分類子には、分類子が候補を返すためのデフォルトの「機能別」ホストグループが存在する必要があります。各デフォルトホストグループの名前は、Exchange Server 分類子を除いて、分類子の名前に対応します。ExchangeServer 分類子のデフォルトホストグループの名前は *Mail Servers* です。

Cisco Software Central からの Host Classifier SWU ファイルのダウンロード

1. Cisco Software Central 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）] 検索バーで、**Cisco Secure Network Analytics** と入力して Enter を押します。
4. リストから [Cisco Secure Network Analytics Manager 2210] を選択します。
5. リストから [アプリケーション – Host Classifier（App – Host Classifier）] を選択します。
6. 右側のウィンドウで、Host Classifier SWU ファイルの  （[ダウンロード（Download）] ）アイコンをクリックし、選択した場所にダウンロードします。

Central Manager での Host Classifier のアップロード

- 通常、アプリケーションのアップロードとインストールには数分を要します。
- アプリケーションのアップロードとインストールは、システム管理者だけが行えます。

1. 現在の Cisco Secure Network Analytics のバージョンと互換性があるアプリケーションをインストールしていることを確認します。『Cisco Secure Network Analytics アプリケーションバージョン互換性マトリックス』を参照してください。
2. [集中管理(Central Management)] に移動します。
3. [アプリケーションマネージャ(App Manager)] タブで [参照(Browse)] をクリックして SWU ファイルを選択します。
4. アプリケーションファイルを選択します。

   アップロードとインストールのプロセスが自動的に始まります。
5. アップロードプロセスをキャンセルする場合は、[アップロード(Upload)] ダイアログで [キャンセル(Cancel)] をクリックします(必要な場合)。

   アプリケーションをインストールすると、[ダッシュボード(Dashboard)] メニューの下にあるメインメニューからアクセスできます。

リソース使用状況

Host Classifier

- 複数のフローコレクタおよびドメインをサポートします。
- 次のディスク容量が必要です。
  - /lancope : 50 MB
  - /lancope/var : 10 MB(このディスク容量は開始点であり、システムにデータが蓄積されるにつれて消費量が増加することに注意)

アプライアンスのディスク使用状況の統計情報を取得するには、次の手順を実行します。

1. Web アプリで、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. [Inventory] タブをクリックします。
3. アプライアンスの [アクション(Actions)] メニューをクリックし、メニューから [アプライアンス統計情報の表示(View Appliance Statistics)] を選択します。
4. プロンプトが表示されたら、関連付けられたインターフェイスにログインします。
5. [ディスク使用量(Disk Usage)] セクションまでスクロールします。

フェールオーバー

インストール時に、プライマリ SMC とセカンダリ SMC の両方にアプリケーションがインストールされます。ただし、アプリケーションはプライマリ Manager のみで動作します。セカンダリ Manager がプライマリ Manager になると、新しいプライマリ Manager 上のアプリが新しくインストールされたかのように動作します。アプリケーション関連のデータはフェールオーバーペア間では転送されないため、履歴データは保持されません。元のプライマリ Manager が再びプライマリ Manager になると、この元のプライマリ Manager の機能が復元されます。これは、セカンダリ Manager になる前に保持していた履歴データのみを保持します。

- プライマリとセカンダリの Manager のアプリケーションまたはアプリケーションのバージョンが一致しない場合、そのアプリケーションは正常に機能しない可能性があります。不一致がある場合は、アプリケーションまたはアプリケーションのバージョンを同期するように求めるメッセージが表示されます。

バックアップ

Host Classifier のデータと設定をバックアップできるかどうかを確認するには、次の表を参照してください。

このタイプのバックアップを実行すると…	関連するデータはバックアップされますか。
設定	• インストールはバックアップされません。 • 変更が Host Classifier によって行われたかどうかにかかわらず、Secure Network Analytics を使用して行われたホストグループの変更はバックアップされます。 • アプリケーション固有の設定はバックアップされません。
データベース	• すべての候補、確認、および除外がバックアップされます。 • 分類子固有の設定はバックアップされます（例：オン/オフ、自動または手動）。

Host Classifier のインストール

Host Classifier をインストールするには、Central Management にアクセスし、[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。Host Classifier をインストールすると、すぐに Manager の実行が開始されます。結果が表示されるまでしばらく時間がかかります。結果が表示された後、Host Classifier は、6 時間ごとに 1 つずつ、開始時刻を 10 分ずつずらしながら、各分類子のクエリを開始します。クエリを停止するには、各分類子の [有効（Enabled）] ステータスを [オン（ON）] から [オフ（OFF）] に変更するか、アプリケーションをアンインストールします。

- Secure Network Analytics の使用可能なディスク容量が 100 ～ 300 MB の場合、Secure Network Analytics の残りのディスク容量を示すメッセージが表示されます。こうした状況では、現在使用可能なディスク容量よりも多くのディスク容量を Host Classifier アプリケーションが必要としている可能性があります。Host Classifier アプリケーションに必要なディスク容量を確認するには、このドキュメントの「**リソース使用状況**」を参照してください。
- Secure Network Analytics が使用可能なディスク容量が 100 MB 未満の場合、このアプリケーションはインストールできません。

オンライン ヘルプ

このアプリケーションのオンラインヘルプにアクセスするには、ページの右上隅にある ?（[ヘルプ（Help）]）アイコンをクリックします。

修正点

このセクションでは、今回のリリースで実施された修正の概要を示します。参照用に Secure Network Analytics の事例番号を示します。

バージョン 4.0.2

障害	説明
LVA-2374	パッケージ libidn の脆弱性を修正しました。任意のドメインを偽装することはできなくなりました。
LVA-2376	GNU Bash の脆弱性を修正しました。権限が削除されることはなくなりました。
LVA-2378	libexpat の脆弱性を修正しました。巧妙に細工された XML 入力によって、パーサーが早期に解析を開始することはなくなりました。
LVA-2380	サービス妨害攻撃（DoS）を引き起こす可能性のある glibc の脆弱性を修正しました。
LVA-2446	lodash の脆弱性を修正しました。
LVA-2660	攻撃者がプログラムをクラッシュさせたり、コードを実行したりする可能性がある iptables の脆弱性を修正しました。
LVA-2661	iproute の脆弱性を修正しました。
LVA-2698	targetUrl Cookie の脆弱性を修正しました。HttpOnly 属性と SameSite 属性が存在しませんでした。
LVA-2748	OpenPGP に対するクロス構成攻撃の発生を可能にする libgcrypt の脆弱性が修正されました。
LVA-2756	整数オーバーフローの可能性を生じさせる PCRE の libpcre の脆弱性が修正されました。
LVA-2761	異なるサービスが所有するリソースに攻撃者が将来アクセスする可能性を生じさせる systemd サービスの脆弱性を修正しました。
LVA-2779	攻撃者が偽造された証明書署名を作成する可能性がある脆弱性を生じさせる GnuPG の脆弱性を修正しました。
LVA-2829	LDAP サーバーからロードされた任意のコードを実行する悪意のある設定を攻撃者が作成することを可能にする logback-core の脆弱性を修正しました。

障害	説明
LVA-2878	桁上げ伝播バグを含む openssl の脆弱性が修正されました。
LVA-2931	Java StackOverflow 例外と、ネストされたオブジェクトが深い場所にあることを利用したサービス妨害を可能にする jackson-databind の脆弱性を修正しました。
LVA-2951	離れた位置の一致が入力に多数含まれる場合にデフレート（圧縮）するとメモリ破損が発生する zlib の脆弱性を修正しました。
LVA-2956	moment.js の脆弱性を修正しました。
LVA-2977	攻撃者が任意のコマンドを実行する可能性を生じさせる openssl の脆弱性を修正しました。
LVA-3013	攻撃者が整合性を侵害する可能性を生じさせる ramda の脆弱性を修正しました。
LVA-3094	ヒープベースバッファの過剰読み込みまたはインフレート時のバッファオーバーフローを含む zlib の脆弱性が修正されました。
LVA-3332	攻撃者がステータス行への挿入を利用して署名の偽造を行う可能性を生じさせる GnuPG の脆弱性を修正しました。
SWAPP-478	メールサーバー分類子を修正しました。偽陽性の結果が生成されることはなくなりました。
SWAPP-479	以前はインターフェイスになかったボタンとチェックボックスを復元しました。
SWAPP-480	表のすべての列が正しく配置されるようになりました。
SWAPP-484	ホームページのツールチップテキストが適切に配置されるようになりました。
SWD-18122	グリッドフィルタのドロップダウンリストとボタンが SNA で正しく表示されるようになりました。
SWONE-20416	BouncyCastle ライブラリの基本イメージを v1.0.2.3 に更新しました。

障害	説明
SWONE-21589	Host Classifier が、SNA 内部 HTTP(S)呼び出しにアプライアンスゲートウェイを使用するようになりました。
SWONE-22827	Vertica を v11.1.1-0 にアップグレードしました。

バージョン 3.1.1

障害	説明
SWAPP-477	v3.1.0 では、システムに複数の Data Store ドメインと非 Data Store ドメインの組み合わせが含まれている場合、5 分ごとに実行されるドメインモニターが 1 分間隔でループし始め、大量のログが生成されていました。その結果、Manager のディスク使用量が増加しました。 この問題は v3.1.1 で修正されています。

バージョン 3.1.0

障害	説明
LVA-2372	パッケージ zlib の脆弱性を修正しました。
LVA-2373	パッケージ bzip2 の脆弱性を修正しました。
LVA-2375	パッケージ libbsd の脆弱性を修正しました。
LVA-2377	パッケージ avahi の脆弱性を修正しました。
LVA-2379	パッケージ openssl の脆弱性を修正しました。
LVA-2654	ライブラリを v1.8.4-5 + deb10u1 に更新しました。mpi-pown に対するサイドチャネル攻撃を防止できるように、指数バインドを含むようになりました。
LVA-2657	ライブラリが脆弱性のないバージョンの E2fsprogs 1.45.3 にアップグレードされたため、スタックでの境界外書き込みは発生しなくなりました(攻撃者はパーティションを壊してこの脆弱性をトリガーすることができなくなりました)。
LVA-2763	パッケージ akka の脆弱性を修正しました。

障害	説明
SWAPP-423	複数の転送エンコーディングヘッダーが、package.comtypesafe.akka-http-core によって許可されるようになりました。
SWAPP-445	パスワードポリシーに関するドメインコントローラクエリの制限を緩和しました。
SWAPP-452	パッケージ commons-io の脆弱性を修正しました。
SWAPP-453	パッケージ guava の脆弱性を修正しました。
SWONE-6998	スクリプトがアップグレードされ、Python 3 を使用するようになりました。
SWONE-18556	FIPS 認定要件を満たすために基本画像を更新しました。
SWONE-19907	次の 2 つのホスト分類子のタイプが Host Classifier に追加されました。 • 信頼できるインターネットホスト • 未分類の上位サーバー
SWONE-20090	ユーザーがデータストアドメインで Host Classifier を使用しようとすると、Host Classifier は、データストアが展開されているシステムでは Host Classifier が機能しないことを示すメッセージをユーザーインターフェイスで提供するようになりました。

バージョン 3.0.0

障害	説明
SWAPP-460	[分類(Classification)] ページにチェック ボックスが表示されるようになりました。
SWONE-12914	Host Classifier がインストール時にソフトウェアの署名を検証するようになりました。

連絡先

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。

コール

- 最寄りのシスコ パートナー
- シスコ サポート
  - （米国）1-800-553-2447
  - 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

ケースのオープン

- Web：http://www.cisco.com/c/en/us/support/index.html
- 電子メール：tac@cisco.com

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 3 月 1 日	最初のバージョン

リリースサポート情報

リリース 4.0.2 の公式一般公開（GA）日は 2023 年 3 月 1 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