Cisco Stealthwatch

ホスト分類子リリースノート v2.0

目次

はじめに

v2.0.x では、Host Classifier が Stealthwatch v7.2.x と互換性を持つようにリファクタリングされました。Stealthwatch v7.2.x では、Stealthwatch 管理コンソール（SMC）に基本的なアーキテクチャの変更が加えられました。

Host Classifier は、Stealthwatch データストア（v7.3.0 で利用可能）が展開されている Stealthwatch システムでは機能しません。

このドキュメントでは、Host Classifier v2.0.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 v2.0.4 です。

概要

> 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 Stealthwatch に存在しない場合、その分類子は機能しません。

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、[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。

はじめる前に

Host Classifier をインストールする前に、このセクションをお読みください。

> 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、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。

Stealthwatch とアプリケーションの互換性

Stealthwatch の更新の際、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、アプリケーションと新しい Stealthwatch バージョンとの間に互換性がない場合があります。Stealthwatch 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、「Stealthwatch 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。

SMC にインストールできるアプリケーションのバージョンは 1 つのみです。インストール済みのアプリケーションを管理するには、[アプリケーションマネージャ(App Manager)] ページを使用します。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。確認可能なアプリケーションのステータスについては、以下の表を参照してください。

より新しいバージョンのアプリケーションがあっても [アプリケーションマネージャ(App Manager)] に表示されないことがあるため、必ず Cisco Software Central で新しいバージョンがないかどうかを確認してください。

> ⚠ 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。Host Classifier 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 Stealthwatch にアップグレード済みです。既存のアプリケーションは、このバージョンの Stealthwatch 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 Stealthwatch 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 Stealthwatch 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 Stealthwatch にアップグレード済みです。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 Stealthwatch 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。

ステータス	定義	対処
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。	Cisco Stealthwatch 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。

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. SMC Web アプリケーションで、[グローバル設定（Global Settings）] アイコンをクリックし、ドロップダウンメニューから [集中管理（Central Management）] を選択します。
2. [Appliance Manager] 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、コンテキストメニューから [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、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。
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 SMC のみで動作します。セカンダリ SMC がプライマリ SMC になると、新しいプライマリ SMC が改めてインストールされたかのように機能します。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 SMC が再びプライマリ SMC になると、元のプライマリ SMC の機能が復元されます。この SMC は、セカンダリ SMC 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 Stealthwatch 管理コンソールとセカンダリ Stealthwatch 管理コンソール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、アプリケーションは正常に機能しません。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、Stealthwatch 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 Stealthwatch 管理コンソール（SMC）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。

- Stealthwatch の使用可能なディスク領域が 100 ～ 300 MB の場合、Stealthwatch 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。
- Stealthwatch 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。

アプリの互換性に関する注意事項

Stealthwatch アプリケーションは、Cisco Stealthwatch の v7.0.0 で導入されました。

Stealthwatch 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と概念が似ています。Cisco Stealthwatch の機能を強化および拡張する、別個にリリース可能なオプションの機能です。アプリケーションマネージャを使用して Stealthwatch アプリケーションをインストール、更新、削除できます。また、[集中管理（Central Management）] メニューオプションから SMC Web アプリケーションにアクセスすることもできます。

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

Stealthwatch 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 Stealthwatch アプリケーションのバージョンは 1 つのみになっています（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、すべてのバージョンのアプリケーションが Stealthwatch 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。Stealthwatch 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、「Stealthwatch 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。

一部のアプリケーションでは、Cisco Stealthwatch 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、Stealthwatch 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。

シスコは、Stealthwatch アプリケーションを任意の時点で廃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ものと同等の機能が、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 Stealthwatch の機能を介して、他の方法で提供されるようになった場合。
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。

Stealthwatch アプリケーションを廃止すると決定された場合、廃止が実行される少なくとも 60 日前に通知されます。Stealthwatch アプリケーションは現在 Cisco Stealthwatch ライセンスに含まれていますが、シスコは、将来特定の Stealthwatch 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。

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 Stealthwatch 事例番号が表示されています。

バージョン 2.0.3

障害	説明
SWAPP-1	ページ上部のタブのいずれかをクリックしても、ページがすぐに更新されませんでした。 ページ上部のタブのいずれかをクリックすると、ページがすぐに更新されます。

バージョン 2.0.4

障害	説明
SWAPP-362	Vertica ドライバを v9.3 に更新しました。
SWONE-3671	インバウンド TLS クライアント用のシスコ標準キーストアにアップグレードすることで、クラスタのセキュリティを強化しました。
SWONE-9534	包括性に関するシスコの標準規格を組み込み、フォーマットを変更することにより、ヘルプファイルが更新されました。

サポートに連絡

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
- Cisco Stealthwatch 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

著作権情報