Cisco Stealthwatch

レポートビルダー 1.4 リリースノート

目次

はじめに

このドキュメントでは、Stealthwatch レポートビルダー v1.4 のすべての機能およびメンテナンスリリースに関する一般的な情報と、改善点およびバグ修正について説明します。レポートビルダー の最新バージョンは v1.4.5 です。

概要

Stealthwatch レポートビルダー を使用して、レポートを作成およびカスタマイズします。レポートとパラメータを作成し、検索条件を定義するためのテンプレートが用意されています。

レポートの結果は、Stealthwatch のデータおよびデータロール権限に基づきます。

レポートを定期的に実行する場合でも、問題を調査する場合でも、クエリを編集したり、チャートやテーブルビューを変更したりすることで詳細を確認できます。

各レポートの詳細については、「**レポート テンプレート**」を参照してください。

新機能

レポートビルダー v1.4.5 には、次の修正が含まれています。

障害	説明
LVA-2811	Apache Log4J 2 を v2.15 に更新しました。

以前のバージョンの v1.4.x がインストールされている場合（Stealthwatch v7.3.2 と互換性あり）は、レポートビルダー v1.4.5 をインストールします。手順については、「**アプリケーションのダウンロード**と**レポートビルダーのインストール**」を参照してください。

> ⚠ 既存の レポートビルダー 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。レポートビルダー をアンインストールすると、保存済みのレポート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。

はじめる前に

レポートビルダー 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。

> レポートビルダー は、輸出管理に関する法律および規制の対象となります。レポートビルダー 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、レポートビルダー 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。

アプリケーションのダウンロード

Stealthwatch アプリケーションをダウンロードするには、https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

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. [Secure Network Analytics Virtual Manager] または [Secure Network Analytics Manager] を選択します。
5. [ソフトウェアタイプの選択(Select a Software Type)] で、[アプリのレポートビルダー(App-Report Builder)] を選択します。
6. [すべてのリリース(All Release)] を選択し、[1.4.5] を選択します。
7. app-smc-sw-report-builder-1.4.5.swu をダウンロードして、任意の場所に保存します。

Stealthwatch とアプリケーションの互換性

Stealthwatch を更新すると、現在インストールされているアプリケーションが保持されます。ただし、このアプリケーションは新しい Stealthwatch バージョンとは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。

Stealthwatch 管理コンソール(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。アプリケーションの想定されるステータスについては、以下の表を参照してください。また、次の点についても注意してください。

- **確認する**: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。
- **閉じる**:レポートビルダーを閉じてから更新を開始してください。
- **インストール**:既存のバージョンを上書きして新しいバージョンを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。レポートビルダー をアンインストールすると、保存済みのレポート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。レポートビルダーアプリは削除しないでください。

> ⚠ 既存の レポートビルダー 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。レポートビルダー をアンインストールすると、保存済みのレポート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。

ステータス	定義	アクション
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。	アプリケーションを更新する場合は、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（これにより、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。
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。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

レポートビルダー アプリケーションをインストールする前に、必要な空きディスク領域があることを確認します。

- **必要な空きディスク領域**: /lancope/var に 600 MB
- **詳細**:レポートビルダー では複数のフローコレクタとドメインをサポートします。レポートに示されているトラフィックは、現在のドメインとそれに関連するすべてのフローコレクタで観測されたデータを表します。また、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してください。

空きディスク領域を確認するには、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 をクリックします。
2. [集中管理(Central Management)] を選択します。
3. [アプライアンスマネージャ(Appliance Manager)] タブを選択します。
4. アプライアンスの [アクション(Actions)] メニューをクリックします。
5. [アプライアンス統計情報の表示(View Appliance Statistics)] を選択します。
6. 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。
7. [ディスク使用量(Disk Usage)] セクションまでスクロールします。
8. /lancope/var に 600 MB の空きディスク領域があることを確認します。

フェールオーバー

フェールオーバーを設定している場合、アプリケーションをインストールすると、プライマリ SMC とセカンダリ SMC の両方に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 でのみ動作します。

- 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、この元のプライマリ 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 SMC とセカンダリ SMC 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

レポートビルダー 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。 • 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	• アプリケーション固有のデータはバックアップされません。

レポートビルダーのインストール

Central Management のアプリケーションマネージャを使用して レポートビルダー をインストールします。ブラウザは Chrome または Firefox を使用することをお勧めします。

1. プライマリ Stealthwatch 管理コンソールにログインします。
2. ⚙ ([グローバル設定(Global Settings)]) アイコンをクリックします。
3. [Central Management] を選択します。
4. [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。
5. [参照(Browse)] をクリックします。
6. 画面に表示される指示に従って、アプリケーションファイルをアップロードします。
    - [応対不可(Unavailable)]: Stealthwatch 管理コンソール(SMC)は、インストール後すぐに実行を開始します。ページが数分間使用できなくなる場合があります。
    - [ディスク容量(Disk Space)]: Stealthwatch のディスク容量が 100 MB 未満の場合は、このアプリケーションをインストールできません。空きディスク領域が 100 ～ 600 MB の場合は、ディスク容量を追加する必要が生じる可能性があります。詳細については、「**リソース使用状況**」を参照してください。
    - [更新(Refresh)]: アプリケーションで作業しているときに、レポートビルダー と Stealthwatch Web アプリケーションまたはその他のアプリケーションとの切り替えを開始した場合、システムの応答が遅くなります。この問題を解決するには、ページを更新します。

レポートビルダーを開く

1. プライマリ Stealthwatch 管理コンソールにログインします。
2. [ダッシュボード(Dashboards)] メニューを選択します。
3. [レポートビルダー(Report Builder)] を選択します。

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、? ([ヘルプ(Help)]) アイコンをクリックします。ヘルプには、各レポートの説明と詳細が含まれています。

レポート テンプレート

次のレポートテンプレートが レポートビルダー に付属しています。

名前	説明
アラームレポート	このレポートを使用して、セキュリティおよびフローコレクタアラームの概要を確認します。選択した Flow Collector のアラームを調査することも、すべてのフローコレクタを検索することも可能です。
データストア保持レポート	このレポートを使用して、データストアのすべてのノードについてデータストア保持統計情報とキャパシティを確認します。データストア保持レポートでは、過去 24 時間のデータを収集し、さまざまなデータタイプのストレージの詳細とキャパシティの残り日数を表示します。これは、分析や調整に役立ちます。
DSCP ステータスレポート	このレポートを使用して、Differentiated Services Code Point（DSCP; DiffServ コードポイント）ステータスを確認します。これは、標準的なネットワーク情報やネットワークの正常性を確認するのに役立ちます。具体的には、選択したインターフェイスのトラフィック、帯域幅、および使用率を確認できます。
エンドポイントトラフィック（NVM）レポート	このレポートを使用して、Network Visibility Module（NVM）からのエンドポイントトラフィックを確認します。ユーザー、デバイス、アプリケーション、場所、宛先のデータが収集されるため、ネットワーク内でもネットワーク外でもユーザーの行動を調査できます。 **要件：** • このレポートのデータを受信するには、Data Store を導入した Stealthwatch が必要です。詳細および手順については、『Stealthwatch Data Store Installation and Configuration Guides』を参照してください。 • Network Visibility Module からデータを受信するようにFlow Collectorが設定されていることを確認してください。手順については、『Endpoint License and NVM Configuration Guide v7.3.2』を参照してください。

名前	説明
フロー収集のトレンドレポート	このレポートを使用して、Flow Collector および選択したエクスポータのフロー収集データの合計を表示します。この情報を使用して、フローコレクタの使用状況がキャパシティプランを下回っているか上回っているかを評価できます。これは、キャパシティプランにおいて重要な点です。
ホスト グループ アプリケーション トラフィック レポート	このレポートを使用して、選択したホストグループのアプリケーション トラフィックを確認します。アプリケーションを含めるか除外するかを選択できます。 これは、データを毎日監視し、大まかな概要を確認するのに適したレポートです。データが急増している場合は、詳細に焦点を当て、問題があるかどうかを判断できます。
ホスト グループ フロー トラフィック レポート	このレポートを使用して、選択したホストグループまたは複数のホストグループのホスト グループ フロー トラフィックを確認します。特定のホストグループを含めるか除外して、検索を絞り込みます。アプリケーション、サービス、およびプロトコルを含めたり除外したりすることも可能です。 データが急増している場合は、詳細に焦点を当て、問題があるかどうかを判断します。
インターフェイス アプリケーション トラフィック レポート	このレポートを使用して、選択したインターフェイスのアプリケーション トラフィックを確認します。
インターフェイス サービス トラフィック レポート	このレポートを使用して、選択したインターフェイスのサービストラフィックを確認します。
NetFlow コレクション ステータス レポート	このレポートを使用して、フローコレクタのエラーとパフォーマンスの問題を確認します。各エクスポータのステータスにマウスポインタを合わせると、問題を調査できます。
ネットワークおよびサーバーのパフォーマンスレポート	このレポートを使用して、フローコレクタ、フローセンサー、およびエクスポータのパフォーマンスを確認します。たとえば、レビューのラウンドトリップ時間（RTT）が長いか増加している場合は、ネットワークの遅延が発生している可能性があります。 **要件**：このレポートを実行するには、ラウンドトリップ時間（RTT）とサーバー応答時間（SRT）に関するデータが含まれた Stealthwatch ネットワークのフローセンサーとエクスポータが必要です。

名前	説明
セキュリティ イベント	このレポートを使用して、選択した期間のすべてのセキュリティイベントに関する概要を確認します。
システム アラーム	このレポートを使用して、アクティブなシステムアラームの概要を確認します。すべてのシステムアラームを調査することも、特定のアラームを選択してクエリを実行することも可能です。
TrustSec 分析	TrustSec 分析レポートには、セキュリティグループタグ（SGT）間のトラフィック量と、それらの間のアプリケーションフローに関する詳細が表示されます。このレポートを使用して、ネットワーク上の通信を把握し、ISE ポリシーが適用されているかどうかを確認します。 **要件**：Cisco Identity Services Engine（ISE）に Stealthwatch を設定します。
TrustSec ポリシー分析	このレポートを使用して、選択した Cisco Identity Services Engine（ISE）イーグレス ポリシー マトリックスで可能性があるポリシー違反、誤設定、または展開の問題を特定します。 このレポートを実行するには、調査するセキュリティグループタグ（レポートパラメータ内）も選択します。セキュリティグループ間のフローを分析し、単一のセキュリティグループ アクセス コントロール リスト（SGACL）に基づく現在のポリシーにトラフィックが準拠しているかどうかを判断します。 **要件**：Cisco Identity Services Engine（ISE）に Stealthwatch を設定します。

ベスト プラクティス

レポートを効率的に実行するには、次の点を確認してください。

- **レポート/編集レポートの合計数を制限**：レポートを作成するか編集するかにかかわらず、開くレポートの合計数を制限します。
- **時間範囲パラメータ**：レポートテンプレートにカスタム時間範囲が含まれている場合は、短い時間範囲を選択します。これにより、パフォーマンスを最大化できます。
- **パラメータの包含/除外**：Applications などのパラメータの**包含**を選択した場合は、少なくとも 1 つのパラメータをフィールドに追加します。追加しないと、レポートがそのカテゴリ内のすべてのデータを検索するため、実行に時間がかかり、大量のリソースを使用することになります。

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的に似ています。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簡素化するため、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 つのみとします(アプリストアモデルに似ています)。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。

シスコでは、Stealthwatch 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。

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。

v1.1.5

障害	説明
SWONE-9882	NetFlow コレクションレポートを実行すると、504 のタイムアウトエラーが返されることがあります。
SWONE-10221	アクティブなアラームの終了時間が 12/31/1969 と表示されていました。「-」と表示されるように更新しました。
SWONE-10213	ピボットからフロー/上位レポートを、ホスト グループ フロートラフィック レポートで使用できませんでした。
SWONE-10322	アクティブなアラーム期間が 00:00:00.xxxx と表示されていました。

v1.1.6

障害	説明
n/a	

v1.2.1

障害	説明
n/a	

v1.3.1

障害	説明
SWONE-13307	[すべてのレポート(All Reports)]リストからレポートを編集すると、新しいレポートが作成される場合があります。レポートを編集すると、適切なレポートが変更されるようになりました。
SWONE-10141	以前は、保存されたレポートのメニューで削除が使用できませんでした。開いたレポートを削除できるようになりました。
SWONE-13187	[レポート(Report)]タブをクリックし、セッションの有効期限が切れた場合は、再度ログインするように求められます。

v1.3.2

障害	説明
SWAPP-414	一部のレポートで、フロー検索へのリンクが壊れていました。
SWAPP-429	Google アナリティクスライブラリを更新しました。
SWAPP-430	TrustSec 分析レポートで自動セキュリティグループタグ(SGT)の選択が正しく機能していませんでした。
SWAPP-439	レポートに列フィルタを適用すると、空白のページが表示されていました。
SWONE-13681	カスタムの日付範囲を使用したときに、TrustSec レポートの結果が開始日から 1 日後に表示される場合がありました。

v1.3.4

障害	説明
SWAPP-449	システムアラームレポートを実行すると、[アラームID（Alarm ID）] 列フィルタでは整数値しか受け取りませんでした。任意の文字列でフィルタリングできるようになりました。
SWAPP-450	システムアラームレポートの実行時に、システム アラーム タイプ フィルタのエントリが考慮されていませんでした。
SWAPP-461	シスコのバンドルをインストールすると、新しいレポートの作成を妨げる内部サーバーエラーが発生していました。

v1.4.1

障害	説明
SWAPP-414	フロー検索で [フロー検索にピボット（Pivot to Flow Search）] リンクが開きませんでした。
SWONE-8462	フロー収集のトレンドレポートでは、複数のエクスポータを使用できる必要があります。

v1.4.4

障害	説明
SWAPP-439	レポートに列フィルタを適用すると、空白のページが表示されていました。
SWAPP-447	エンドポイントトラフィック（NVM）レポートで、送信元または宛先ポートフィルタに複数のポート番号を使用すると、フィルタを合計に適用しても結果が表示されませんでした。
SWAPP-449	システムアラームレポートを実行すると、[アラームID（Alarm ID）] 列フィルタでは整数値しか受け取りませんでした。任意の文字列でフィルタリングできるようになりました。

障害	説明
SWAPP-450	システムアラームレポートの実行時に、システム アラーム タイプ フィルタのエントリが考慮されていませんでした。
SWAPP-461	シスコのバンドルをインストールすると、新しいレポートの作成を妨げる内部サーバーエラーが発生していました。

v1.4.5

障害	説明
LVA-2811	Apache Log4J 2 を v2.15 に更新しました。

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：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

著作権情報