CISCO SECURE NETWORK ANALYTICS

デスクトップクライアント 7.4 ユーザーガイド

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

CONTENTS

1

このマニュアルについて

概要

このガイドは、Stealthwatch デスクトップクライアントを日常的に使用するユーザーから管理者までを主な対象読者としています。ネットワークの概念に関する全般的な知識があることを前提としています。このガイドでは、ネットワーク パフォーマンスの問題やセキュリティリスクを最小限に抑えるために Stealthwatch デスクトップクライアントを使用する場合の「ベストプラクティス」のガイドラインを示します。ネットワークには複雑な部分が多くさまざまな種類があるため、このガイドは総合的なユーザー ガイドではありません。むしろ、ネットワークのパフォーマンスの問題やネットワークへの脅威の処理や防止に向けて SMC ソフトウェアを使用する最善の方法に関するガイダンスの提供を目的としています。

この章は、次の項で構成されています。

Stealthwatch Web アプリケーションのマニュアルへのアクセス方法

Stealthwatch Web アプリケーションのマニュアルを表示するには、Stealthwatch Web アプリケーション インターフェイスでオンラインヘルプを表示する必要があります。

Stealthwatch Web 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、Stealthwatch Web アプリケーションの任意のページで、そのページの右上隅にあるツールバーの [ユーザー（User）] アイコン（👤）をクリックし、[Stealthwatch オンラインヘルプ（Stealthwatch Online Help）] を選択します。

STEALTHWATCH デスクトップクライアントについて

Stealthwatch デスクトップクライアントは、ネットワーク管理者が 1 つの場所から複数の分散型 Stealthwatch フローコレクタの定義、設定、監視を行える企業レベルのセキュリティ管理システムです。このシステムにより、物理および仮想環境全体のフロー ベースのセキュリティ、ネットワーク、およびアプリケーション パフォーマンス モニターリングが行えます。Stealthwatch によって、ネットワークの運用およびセキュリティのチームは、ネットワークを使用しているユーザー、使用中のアプリケーションとサービス、およびこれらのパフォーマンスの状態を確認できます。

表、円グラフ、グラフ、およびレポートの活用により、セキュリティ上の脅威の速やかな検出と優先順位付け、ネットワークの不正使用と準最適なパフォーマンスの特定、全社でのイベント応答の管理を、管理者が単独のコントロールセンターからすべて行うことができます。Stealthwatch は、異常な動作を迅速に突き止めてコンテキスト情報とともに SMC にアラームを送信し、潜在的な損害を軽減するための決定的なアクションをセキュリティ担当者がただちに取れるようにします。

(注):

Data Store を展開する場合は、Stealthwatch Web アプリケーションを使用して Stealthwatch インストールをモニターおよび設定します。Stealthwatch デスクトップクライアントは Data Store と互換性がありません。

Stealthwatch のインターフェイス

v6.5.0 現在、Stealthwatch は、センサーからのデータを表示して、ポリシー定義などの管理機能を提供するために一定期間 2 つのユーザーインターフェイス(管理コンソール)を使用します。既存のインタ フェースは引き続き使用できますが、段階的に終了する予定です。この機能は、新しい Stealthwatch Web App のインターフェイスに移行中です。移行期間中は両方の UI を使用する必要があります。必要に応じて、各 UI のオンライン ヘルプによって UI の切り替えが必要であることが通知されます。

Stealthwatch デスクトップクライアント: このインターフェイスは情報をグラフ、テーブル、およびフィルタ形式で提供します。フィルタは、個別の(場合により複数の)ページまたはダイアログで構成されます。

Stealthwatch Web アプリケーション: この新しいフォーマットでは、クエリの範囲の絞り込みに使用するフィルタペインなど、商業 Web サイトで見られる要素をはじめとする、より視覚的なアプローチを使用しています。このインターフェイスは、Stealthwatch を起動すると開きます。

（注）:

このマニュアルの使い方

「はじめに」のほかに、このガイドは次の章と索引に分かれています。

章のタイトル	内容
2 - Stealthwatch デスクトップクライアントの操作	SMC 内で共通のナビゲーション要素を使用します。
3 - ホスト管理	ポリシーを使用して動作を制御できるようにホストをグループ化します。
4 - ビューおよびダッシュボード	SMC 内で最も重要なアクティビティを表すデータをさまざまな表形式と図形式で表示します。
5 - インデックス：ランキング動作の変更	インデックスを使用して異常な動作を追跡します。
6 - トラフィックおよびネットワーク パフォーマンスのモニターリング	サーバーとネットワークの応答時間、およびトラフィックを監視します。
7 - フローの分析	傾向を判断するためにホスト間のフローを分析します。
8 - Stealthwatch 脅威インテリジェンス フィード（正式には Stealthwatch Labs Intelligence Center または SLIC）	ネットワークへの脅威に関するグローバルな脅威インテリジェンスフィードから、頻繁に更新される情報を提供するシスコのサービスです。
9 - 原因の特定	アラームを確認して閉じ、自動緩和機能を使用して、手動でソースをブロックします。
10 - アラームへの対応	ポリシーを調整して不要なアラーム表示数を減らします。
11 - 不要なアラームの削減	アラームの原因となった最初のホストとその影響を受けるホストを突き止めます。
12 - ドキュメントの操作	指定のコンポーネントを含むカスタム ドキュメントの保存、共有、スケジュール設定を行います。
13 - デスクトップクライアントのロール	ユーザーが Stealthwatch デスクトップクライアントで表示および設定できる機能（フロー検索、ポリシー管理、レポートなど）を制御するために、デスクトップクライアントのロールを作成します。

ドキュメント アイコン

このドキュメントでは、次のアイコンを使用して重要な情報を示します。

アイコン	意味	説明
	ヒント	特定のタスクを実行するためのショートカットや簡単な方法です。
	コメント	このドキュメントや Stealthwatch を使用するときに役立つ情報です。
	重要	ソフトウェアの誤動作などの重大な結果を防ぐために確認する必要があります。
	注意	ハードウェアの損傷またはデータの損失を防ぐために確認する必要があります。

略語

このガイドでは、次の略語が使用されます。

省略形	定義
AS（番号）	自律システム
CI	リスク インデックス
CIDR	クラスレス ドメイン間ルーティング
CSV	コンマ区切り値
DAR	ディスク アーカイブ
DHCP	ダイナミック ホスト コンフィギュレーション プロトコル
DNS	ドメイン ネーム システム（サービスまたはサーバー）
DoS	Denial of Service; サービス妨害
DSCP	DiffServ コード ポイント
FSI	ファイル共有インデックス
IANA	インターネット割当番号公社
ID	ID
IM	インスタント メッセージ
IP	インターネット プロトコル
MAC	Media Access Control; メディア アクセス コントロール
MPLS	マルチプロトコル ラベル スイッチング
PDF	Portable Document Format; ポータブル ドキュメント フォーマット
P2P	ピアツーピア
RADIUS	Remote Authentication Dial-in User Service; リモート認証ダイヤルイン ユーザー サービス
RFC	コメント要求
RTT	ラウンドトリップ時間
SMC	Stealthwatch Management Console
SNMP	Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
SRT	Server Response Time; サーバー応答時間
TACACS	Terminal Access Controller Access Control System
TCP	伝送制御プロトコル

省略形	定義
TI	ターゲット インデックス
UDP	ユーザー データグラム プロトコル
UI	User Interface; ユーザー インターフェイス
URL	ユニフォーム リソース ロケータ
VLAN	仮想ローカル エリア ネットワーク
VPN	バーチャル プライベート ネットワーク

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ます。

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

2

STEALTHWATCH デスクトップクライアントの操作

概要

Stealthwatch デスクトップクライアントには、ネットワークのモニターリング、保護、および分析に役立つ数多くのドキュメントが含まれています。これらのドキュメントで使用されている共通のナビゲーション要素や汎用インターフェイスに慣れることにより、Stealthwatch を習熟しやすくなり、ネットワーク内のイベントを分析する際の効率を高めることができます。

この章は、次の項で構成されています。

クライアント メモリの割り当て

Stealthwatch デスクトップクライアントを実行するために、クライアントコンピュータで割り当てるランダムアクセスメモリ（RAM）の容量を変更できます。開いている多数のドキュメントや大量のデータ セット（100,000 個を超えるレコードが含まれたフロー クエリなど）を扱う場合は、割り当てるメモリを増やすことを検討してください。

1. **Windows の場合：**

   a. Windows Explorer で、ホームディレクトリに移動します。

   b. パス：AppData > Roaming > Stealthwatch を使用して Stealthwatch フォルダを開きます。

   MacOS の場合：

   a. 検索で、ホーム ディレクトリに移動します。

   b. Stealtwatch フォルダを開きます。

2. Stealthwatch ディレクトリで、目的の Stealthwatch バージョンが含まれているフォルダを開きます。

3. 適切な編集アプリケーションを使用して application.vmoptions ファイルを開き、編集を開始します。（このファイルは、Stealthwatch デスクトップクライアントを最初に開いた後に作成されます）。

   - 最小メモリのサイズ、512 MB 以上を割り当てることをお勧めします。この番号は、ファイルの 3 番目の行に表示されます。コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、どの数字が最小メモリ サイズを表しているかを確認してください。

```
# Enter one VM parameter per line
# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size
-Xms512m
-Xmx2048m
```

   - 最大メモリ サイズには、コンピュータの RAM の最大半分のサイズを割り当てることができます。この番号は、ファイルの 4 番目の行に表示されます。コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、最大メモリサイズを表している数字を確認してください。

```
# Enter one VM parameter per line
# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size
-Xms512m
-Xmx2048m
```

すべての番号を使用します。たとえば、Xmx0.5m ではなく、-xmx512m を入力します。

ビュー ポイント

Stealthwatch デスクトップクライアントにログインしたときに表示されるビューは、ログイン権限（つまり、ビュー ポイント）に応じて異なります。そのため、お使いのコンピュータの Stealthwatch デスクトップクライアントに表示される内容は、このガイドに記載されている内容と多少異なる場合があります。

Stealthwatch 管理者は、[ユーザーとロール管理（User & Role Management）] ダイアログでログイン権限を定義します。詳細については、第 13 章「デスクトップクライアントのロール」。を参照してください。

独自のカスタム ダッシュボードを作成して、それをログイン ドキュメントにすることも、SMC 内ですでに設定されているダッシュボードを選択することもできます。カスタム ダッシュボードは必要な数だけ作成することができます。ダッシュボードとは、必要な SMC コンポーネントと表示する必要のあるデータが含まれている、さまざまなレポートのコレクションです。これにより、確認しておきたい主要な情報のみに集中することができます。

（注）：

- ログインドキュメントの設定については、次を参照してください。第 12 章「ドキュメントの操作」。
- ダッシュボードの作成については、第 4 章「ビューおよびダッシュボード」。を参照してください。

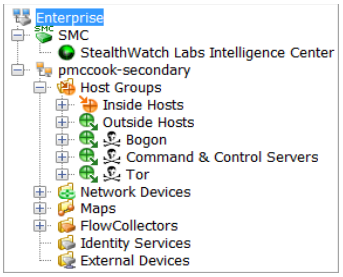
ドメイン ダッシュボードは、ログイン ドキュメントとして活用できるドキュメントの一例であり、ドメイン内の重要なアクティビティに関するデータをグラフィカルに表形式で表示します。表示されるデータは、5 分ごとに SMC から収集されます。ドメイン ダッシュボードはデフォルトで、自動的に管理者ユーザーのログイン ドキュメントに設定されます。また、新規ユーザー用のスケジュール設定されたドキュメントとしてすぐに利用することができます。これには単に、StealthwatchStealthwatch Daily Reports スケジュールを有効にして、そのドキュメントを組み込みます。

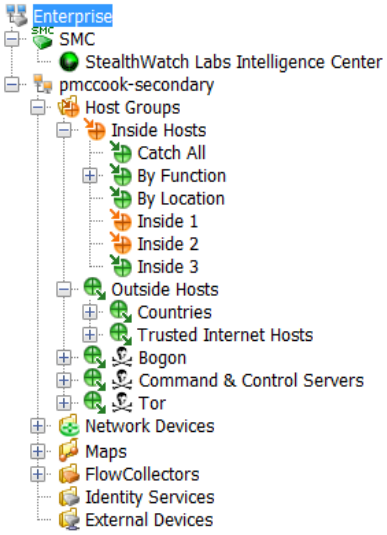
（注）：

ドキュメントの有効化とスケジュール設定については、次を参照してください。第 12 章「ドキュメントの操作」。

企業ツリーとツールのヒント

Stealthwatch デスクトップクライアントの左側のナビゲーションウィンドウにある項目のリストは、企業ツリーと呼ばれることがよくあります。また、企業ページやホスト グループ ツリーと呼ばれることもあります。このツリーは、モニター対象ネットワークの構造を示しています。





企業ツリーのオプションは、デフォルトで折りたたまれています。ツリー内のすべてのオプションを同時に展開するには、ツリー内の任意の項目を右クリックし、[すべて展開(Expand All)] を選択します。すべての項目を同時に折りたたむには、項目を右クリックして [すべて折りたたむ(Collapse All)] を選択します。企業ツリーを完全に非表示にするには、メイン メニューの [表示(View)] > [ツリーを非表示にする(Hide Tree)] をクリックするか、キーボードで **Ctrl+T** を押します。SMC では、展開された状態または折りたたまれた状態のフォルダ設定が保存されます。したがって、次回ログイン時には、企業ツリーが前回ログイン時と同じ状態で表示されます。

ツリー内での検索

企業ツリーで項目を検索するには、企業ツリーの下部にある [検索(Find)] 

フィールドに目的のテキストを入力します。

(注):
[検索(Find)] フィールドは、デフォルトでは表示されません。最初に **Ctrl+F** を押してフィールドを開く必要があります。それ以降は、SMC を開くたびにフィールドが表示されます。

目的のテキストの追加のインスタンスをツリー内で前方および後方検索するには、次のいずれかの方法を使用します。

- [検索(Find)] フィールドの右側にある下向きボタン と上向きボタン をクリックします。
- キーボードの下矢印キー( ) と上矢印キー( ) を押します。

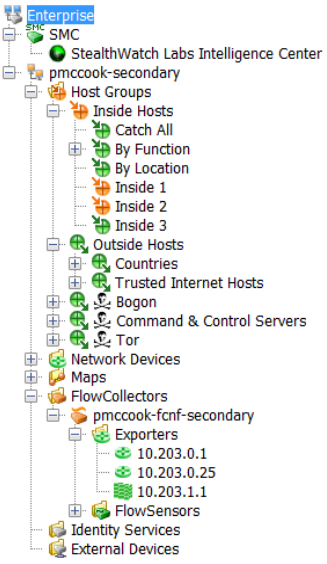
ヒント:
SMC では、検索中でも他の操作を続行できます。

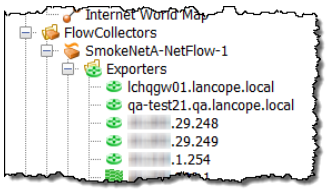
ツリーのブランチ

この例で強調表示されている企業ツリーのブランチは、常に企業ツリーに存在します。このブランチは、すべての SMC 管理オプションの最上位の収集ポイントを表し、SMC のモニター対象であるすべてのドメインが含まれます。

SMC ブランチは、ビュー ポイントに応じて存在する場合と存在しない場合があります。このブランチは、SMC アプライアンスそのものを表します。システムがフェールオーバー SMC を使用している場合は、プライマリとセカンダリの両方の SMC ブランチが表示されます。

他のツリーブランチは、SMC アプライアンスがモニターリングしているドメイン、および、関連付けられたホストグループ、Stealthwatch フローコレクタ、Stealthwatch FlowSensor、マップ、周辺機器、外部デバイスを表します。





ブランチを展開するには、関連付けられているプラス記号 をクリックします。表示されるブランチの 1 つは、[フロー コレクタ(FlowCollectors)] ブランチです。選択したドメインの SMC アプライアンスに情報を送信する Flow Collector(フロー コレクタ)の一覧を表示するには、関連付けられているプラス記号をクリックして [フロー コレクタ(FlowCollectors)] ブランチを展開します。特定の [フロー コレクタ(FlowCollectors)] ブランチを展開すると、関連付けられている [フローセンサ(FlowSensor)] のアプライアンス、エクスポータ、およびファイアウォールが表示されます。

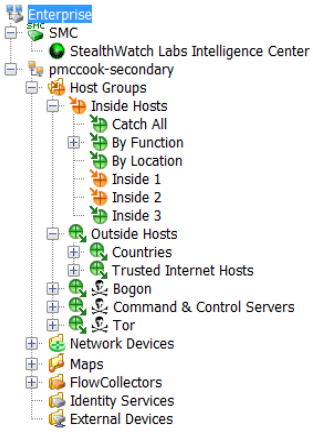
アラームの重大度

企業ツリーのブランチでは、ネットワーク内で発生しているアラームの重大度に応じてアイコンの色が変わるため、アラーム条件が発生しているかどうかをすぐに確認することができます。SMC では、各アラームにすでにデフォルトの重大度が割り当てられています。ただし、ログイン権限によっては、[アラーム設定(Alarm Configuration)] ダイアログを使用して、ネットワーク環境のニーズに合うように重大度の割り当てを変更することができます。次の表に、各種重大度を示します。重大度はそれぞれ、特定の色で示されます。

重大度	関連付けられている色
クリティカル	赤
メジャー	オレンジ
マイナー	黄
通常	青
情報	ライト ブルー
アラームは発生していない	緑

(注):
最上位のブランチ アイコンは、下位のすべてのブランチで発生しているアラームのうち、重大度が最も高いアラームの色で表示されます。

メニューを確認するときには、以下を自問自答してください。

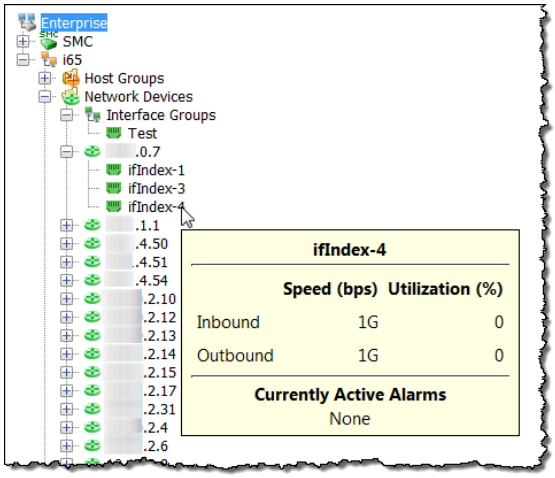


- 赤またはオレンジ色のアイコンはあるか。これらの色のアイコンがある場合は、クリティカルまたはメジャーのアラーム条件が発生しています。
- アイコン  は表示されているか。表示されている場合は、そのアイコンの横にあるデバイスへの接続が失われています。
  - [内部ホスト（Inside Hosts）] サブツリーを展開すると、最も重要なホスト グループでアラームが発生しているかどうかを調べることができます。
  - 詳細については、[ホストグループ（Host Groups）] サブツリーから、[ホストグループダッシュボード（Host Group Dashboard）] ドキュメントの 1 つ（この章で後述）を開いてください。
- SMC のアイコンは何色で表示されているか。緑または灰色以外の色は、SMC アプライアンスでシステム アラームが発生していることを示します。

（注）：

システムは 1 分ごとに企業ツリーを更新します。ただし、企業ツリーはいつでも更新して最新の情報を表示することができます。更新するには、メイン メニューの [表示（View）] > [ツリーを更新（Referesh Tree）] をクリックします。また、企業ツリー内の任意の場所を右クリックして、[ツリーを更新（Refresh Tree）] を選択することもできます。

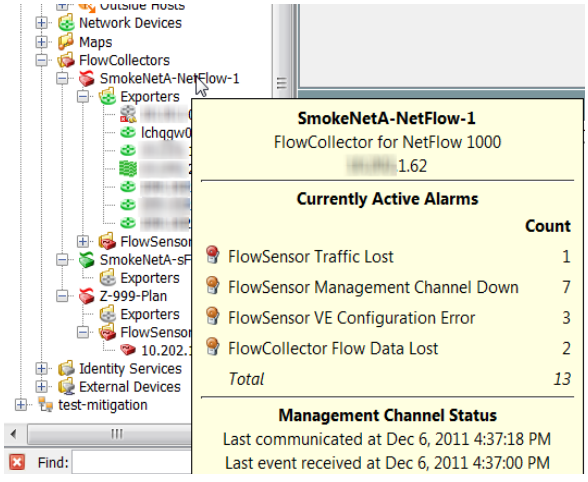
企業ツリー インジケータ



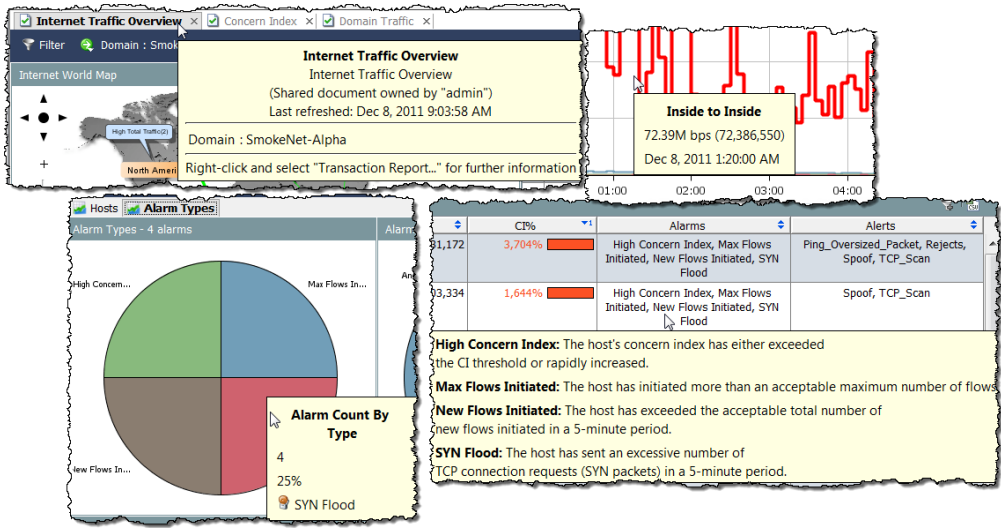
ブランチをマウス オーバーすると、ツールのヒントが表示され、オブジェクトで発生しているアラームの総数とアラームの重大度が表示されます。[フローコレクタ(FlowCollectors)] ブランチの場合は、アラーム情報とステルスウォッチ アプライアンスのアイデンティティが表示されます。さらに、SMC が最後にアプライアンスと通信しようとした日時、SMC が応答を受信した日時、およびアプライアンスが最後にイベントを報告した日時が表示されます。

ツールのヒント

Stealthwatch デスクトップクライアントのさまざまな要素にカーソルを置くと、その要素に関するサマリー情報がツールヒントに表示されます。たとえば、企業ツリーのフローコレクタの名前の 1 つにカーソルを置くと、識別情報とともに、通信ステータス、およびフローコレクタがトリガーしたすべてのアラームが表示されます。



ツールヒントは、Stealthwatch デスクトップクライアントのほぼすべての場所で表示されます。要素（タブ、グラフ、チャート、テーブルのセルなど）をマウスオーバーするだけで、その要素に対応するツール ヒントが表示されます。



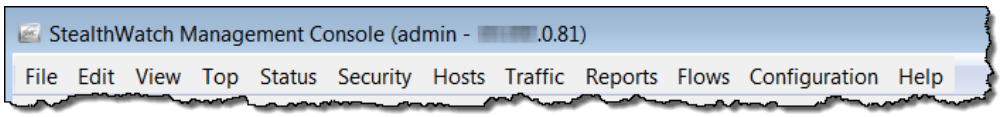
SMC ドキュメントを開く

Stealthwatch デスクトップクライアントを使用すると、メインメニューや右クリック機能など、いくつかの方法でドキュメントを開くことができます。

(注):
ドキュメントはレポートとも呼ばれます。このユーザー ガイドでは、これらの用語が同じ意味で使用される場合があります。

メイン メニュー

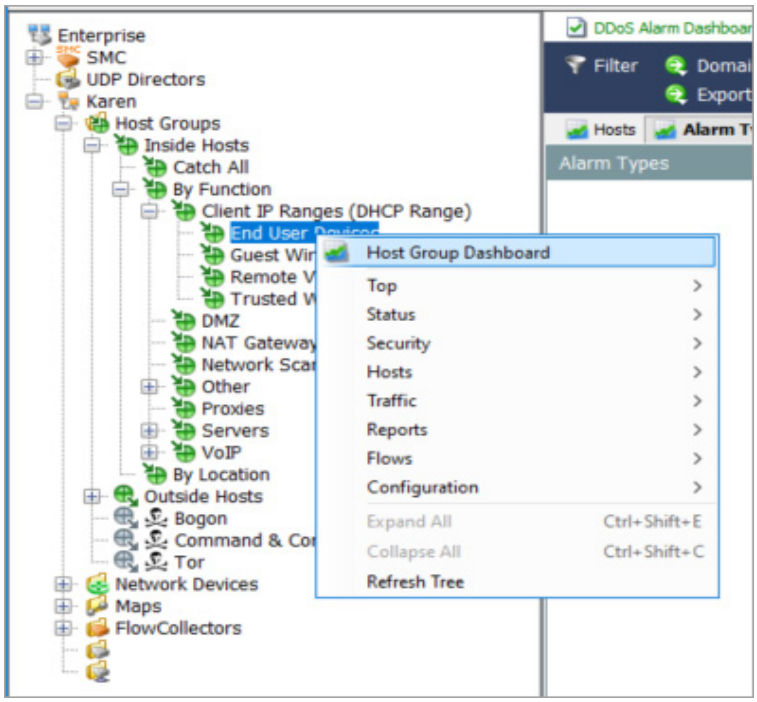
メイン メニューのメニュー項目をクリックして、ドキュメントを開くことができます。



利用可能なオプションは、次の 3 つの主な要因によって異なります。

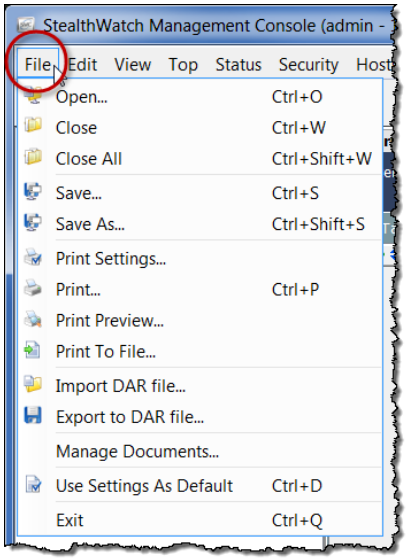
- 企業ツリーでクリックした項目
- 特定の SMC ドキュメントでクリックした項目
- ログイン権限

たとえば、企業ツリーでホスト グループをクリックし、[ホストグループダッシュボード（Host Group Dashboard）] を右クリックすると、そのホスト グループのデータのみが表示されます。



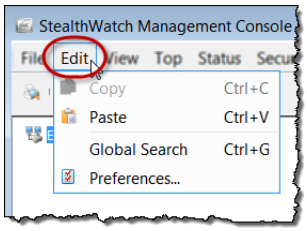
[ファイル（File）] メニュー

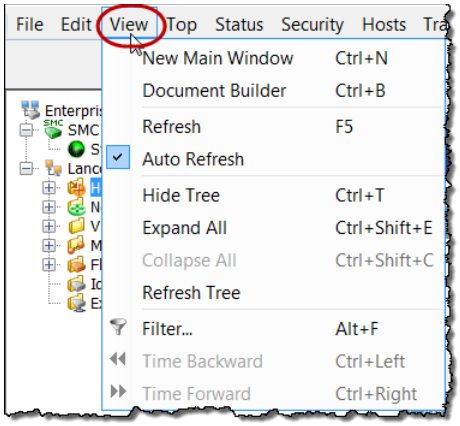
[ファイル（File）] メニューには、SMC ドキュメントを開く、閉じる、保存する、印刷する、他のユーザーと共有するなど、ドキュメントを操作するためのオプションがあります。



[編集（Edit）] メニュー

[編集（Edit）] メニューには、データをコピー、貼り付け、検索、および特定の表示設定を定義するためのオプションがあります。



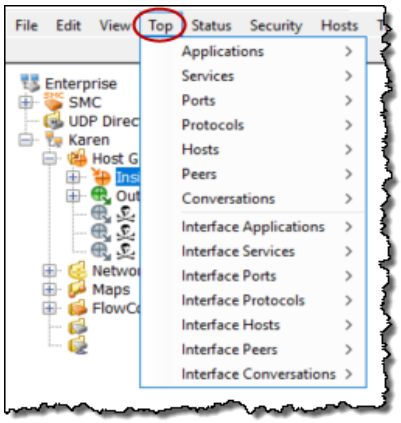


[表示(View)] メニュー

[表示(View)] メニューを使用すると、SMC ユーザー インターフェイスの新しいインスタンスを開いたり、カスタム ダッシュボードを作成したり、自動更新機能を停止または開始したり、手動でデータを更新したり、さまざまな方法で企業ツリーを表示したり、非表示にしたり、データをフィルタ処理したり、以前または以降の時間内のデータを表示したりすることができます。

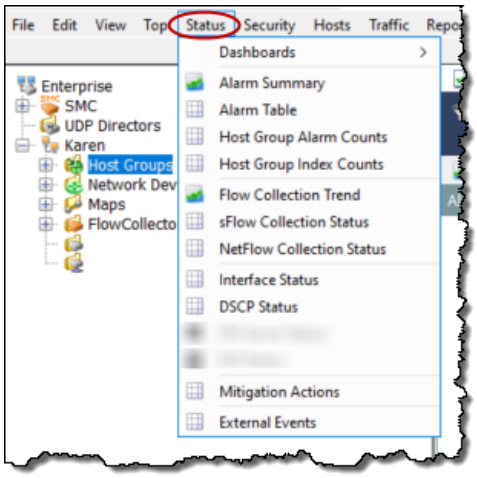
[トップ(Top)] メニュー

[トップ(Top)] メニューでは、使用頻度の最も高いアプリケーション、使用頻度の最も高いサービス、使用頻度の最も高いポート、最もアクティブなホストなど、特定の基準に基づいて最も使用されているデータを表示できます。このデータは、ネットワーク全体で表示することも、着信トラフィック、発信トラフィック、ドメインまたはホスト グループ内のトラフィック、特定のインターフェイスを経由するトラフィックなどに分類して表示することもできます。

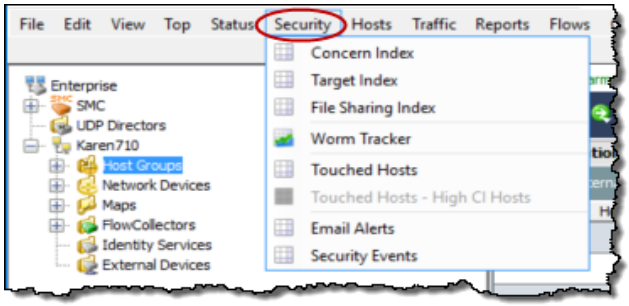


[ステータス(Status)] メニュー

[ステータス(Status)] メニューには、アラーム、トラフィック、データ損失の可能性、インターフェイス、外部イベントなどの特定の基準に基づいて、ネットワークのさまざまな部分のステータスを表示するオプションがあります。



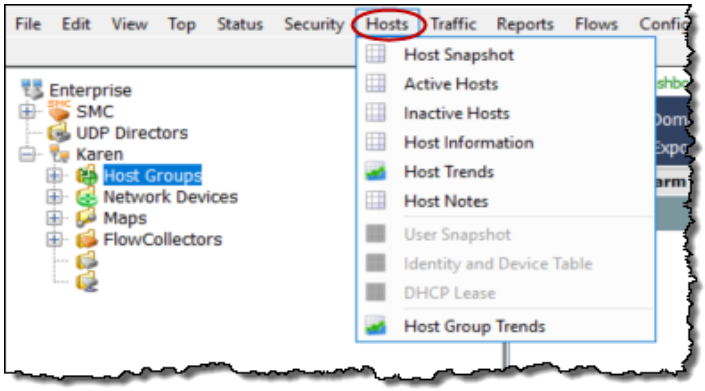
[セキュリティ(Security)] メニュー



[セキュリティ(Security)] メニューでは、高懸念ホスト、ターゲット ホスト、ファイル共有アクティビティ、ワーム アクティビティ、異常なメール トラフィックなどのセキュリティ上の問題に関するデータを表示できます。

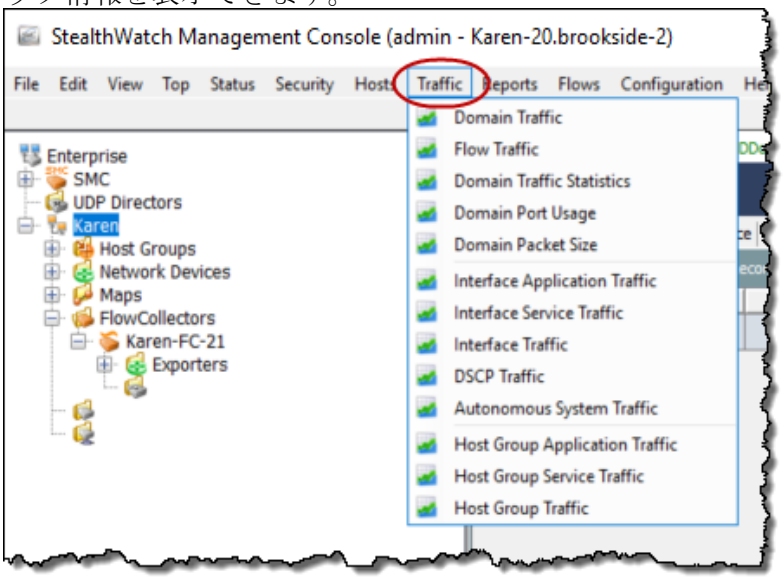
[ホスト(Hosts)] メニュー

[ホスト(Hosts)] メニューには、個々のホストのアクティビティ、ホストの動作の傾向、アクティブまたは非アクティブのホスト、ホストのユーザー アイデンティティなど、ホストに関連するデータを表示するためのオプションがあります。



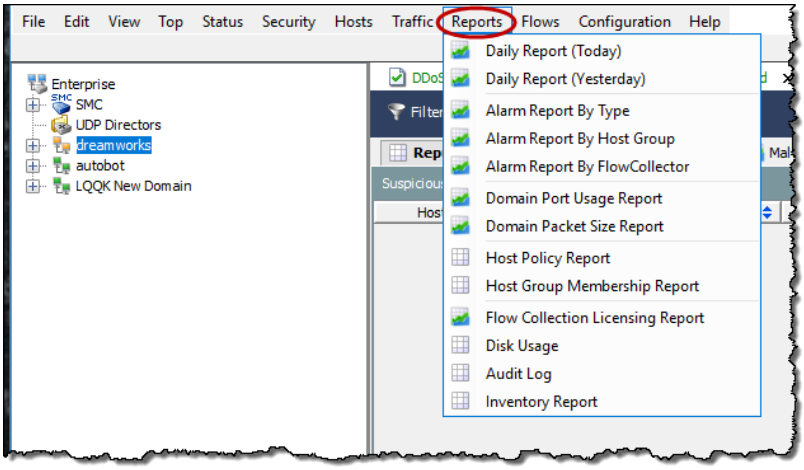
[トラフィック(Traffic)] メニュー

[トラフィック(Traffic)] メニューでは、ドメイン、インターフェイス、ホストグループ、アプリケーション、サービス、ポートなど、さまざまな方法で分類したトラフィック情報を表示できます。



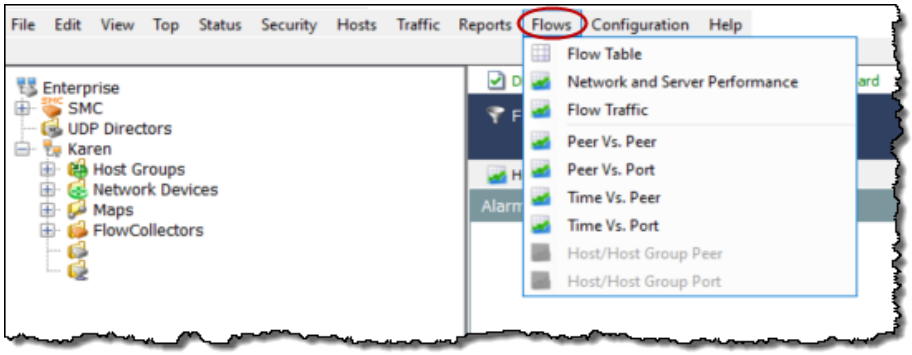
[レポート(Reports)] メニュー

[レポート(Reports)] メニューでは、StealthWatch データベースに対してクエリを実行し、ドメイン アクティビティの日次サマリや、タイプ、ホスト グループ、フロー コレクタ別のアラームのレポートなどを取得することができます。



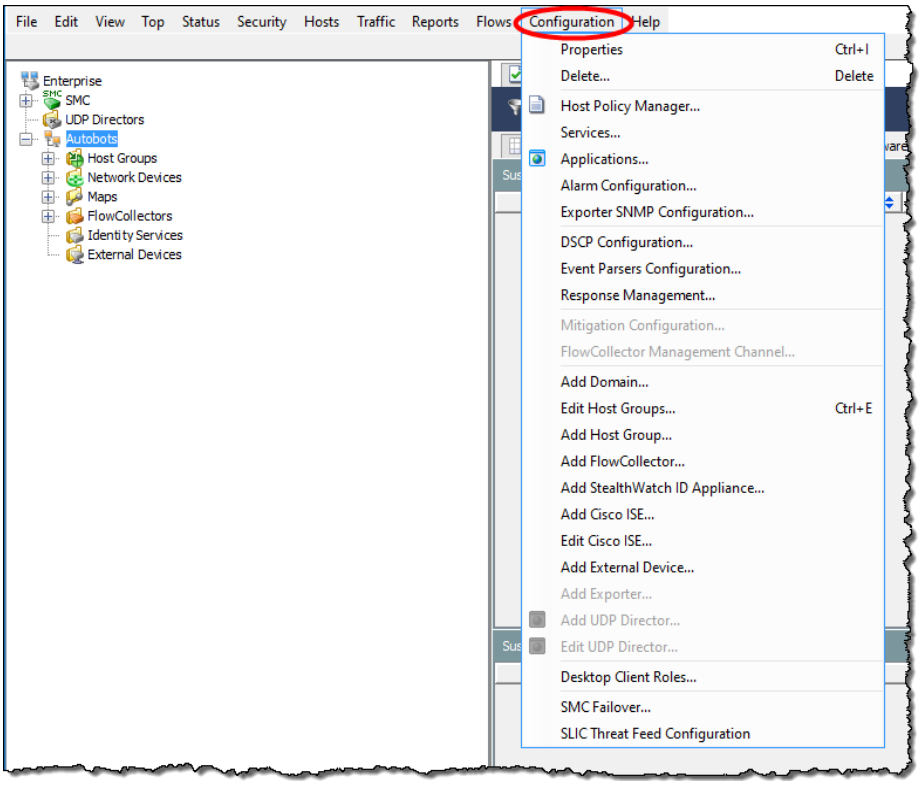
[フロー(Flows)] メニュー

メニュー名からわかるように、[フロー(Flows)] メニューでは、ネットワークおよびサーバーのパフォーマンス フロー データなど、フローを分析するさまざまな方法が提供されます。



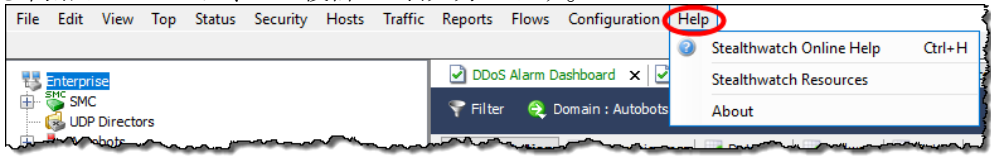
[設定(Configuration)] メニュー

[設定(Configuration)] メニューには、StealthWatch で使用可能な設定オプションの大半が含まれています。モニター対象のネットワークを必要に応じて構造化または絞り込むには、ドメイン、アプライアンス、ホスト グループ、ポリシー、アプリケーション、またはサービス定義を追加、編集、削除します。アクセスを制限するには、ユーザーとそのログイン権限を追加、編集、削除します。Stealthwatch は、アラーム重大度のデフォルトセットを使用します。これらは組織のニーズに応じて変更することができます。



[ヘルプ(Help)] メニュー

[ヘルプ(Help)] メニューには、Stealthwatch デスクトップクライアンのオンラインヘルプと Stealthwatch デスクトップクライアント ソフトウェアのバージョンと説明に関連する情報が含まれています。オンライン ヘルプを使用する利点については、この後詳しく説明します。

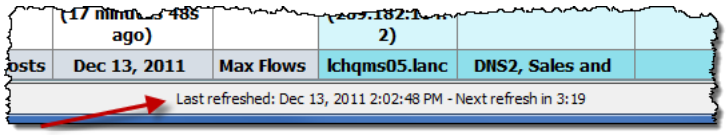


ドキュメントの操作

SMC ドキュメントに表示される共通のナビゲーション要素を確認していきましょう。

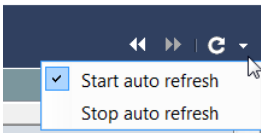
ライブ データと静的データの表示

SMC アプライアンスは、Stealthwatch Flow Collector からデータを収集し、ほとんどの SMC ドキュメントのデータを自動的に更新するため、常に最新の情報が表示されます。次の自動更新がいつ行われるかを確認するには、ウィンドウの下部にあるカウンタを確認します。



[更新(Refresh)] ボタン は、ドキュメント ヘッダーの右端にあります。このボタンをクリックすると、アクティブなドキュメントが最新のデータで更新され(ライブになり)、自動更新機能がリセットされます。

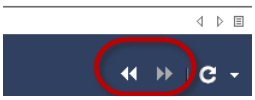
長時間にわたって情報を調べる必要がある場合は、ドキュメントが静的である方が便利です。



ドキュメントを静的またはライブにするには、ドロップダウン メニューから次のいずれかのオプションをクリックします。

- [自動更新を開始(Start auto refresh)]: ドキュメントがライブ(アクティブ)になります。自動更新間隔が終了すると、SMC ソフトウェアはドキュメントを新しいデータで更新します。
- [自動更新を停止(Stop auto refresh)]: ドキュメントが静的(非アクティブ)になります。

ヒント:
[更新(Refresh)] ボタンをクリックすると、データの更新をいつでも開始することができます。



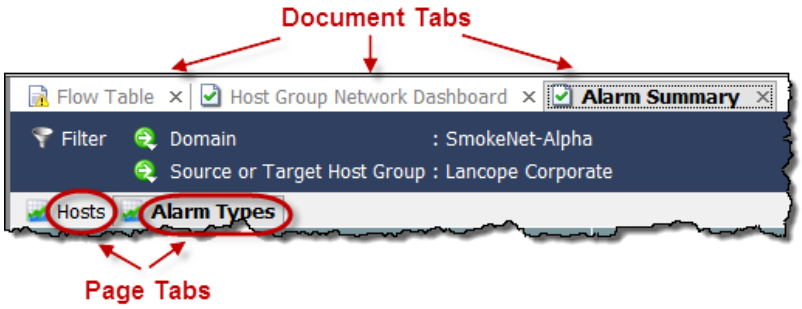
[以前のデータを表示(View Earlier Data)] ボタン と [以降のデータを表示(View Later Data)] ボタン も、ドキュメント ヘッダーの右端にあります。これらのボタンをクリックすると、[フィルタ(Filter)] ダイアログで設定された時間の増分に従って、データ内を前方または後方へ移動することができます。

ヒント:

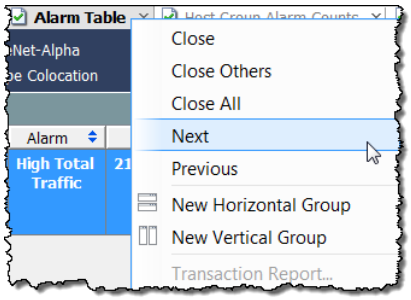
- **Ctrl+ 左矢印キー**を押すと、データ内を時間的に後方へすばやく移動できます。
- **Ctrl+ 右矢印キー**を押すと、データ内を時間的に前方へすばやく移動できます。

タブとドキュメント間の移動

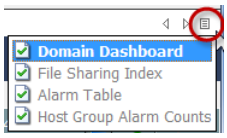
Stealthwatch デスクトップクライアントでは、複数のドキュメントを同時に開くことができます。各ドキュメントはタブで区切られています。次の例に示す [アラームの概要(Alarm Summary)] のような一部のドキュメントには、複数のページがあり、複数のページがタブで区切られています。



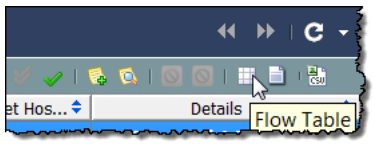
ドキュメント間はいくつかの方法で移動できます。目的のドキュメントのタブをクリックし、ドキュメント タブを右クリックして、[次へ(Next)] または [前へ(Previous)] を選択するか、**Alt** キーとキーボードの左矢印キー ← または右矢印キー → を同時に押します。



開いているドキュメントが多すぎてすべてのタブを表示できない場合、ドキュメント間を移動するには、タブの右側にある右矢印 ▶ または左矢印 ◀ をクリックします。また、[リスト(List)] ボタン をクリックして、開いているドキュメントをドロップダウン リストでクリックすることもできます。



アクティブなドキュメントとは、現在表示されているドキュメントのことです。アクティブなドキュメントのタイトルは、常に黒い太文字で表示されます。アクティブなドキュメントは、対応する更新間隔に基づいて自動的に更新されます。非アクティブなドキュメントは、自動的には更新されません。非アクティブなドキュメントを更新するには、それをアクティブにしてから、手動で更新する必要があります。更新が開始された後、更新が完了されるまで待たなくても、他のドキュメントに移動できます。

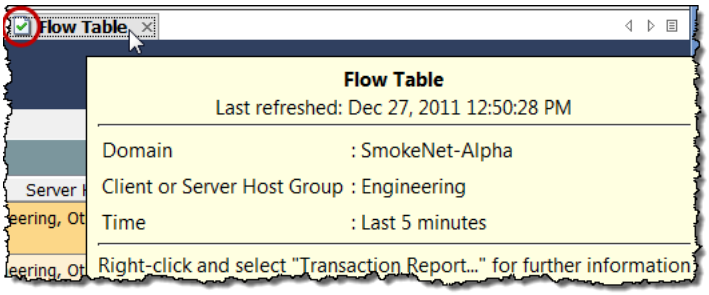


多くのドキュメントには、そのドキュメントに特定の機能が含まれたボタン付きの独自のツールバーが表示されます。いずれかのボタンをマウス オーバーすると、そのボタンについて説明するツール ヒントが表示されます。

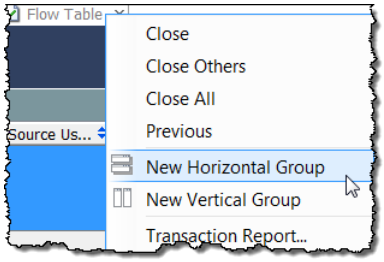
各ドキュメント タブには、ドキュメントの更新ステータスを示すアイコンが表示されます(次の例で、丸で囲んであるアイコンを参照してください)。非アクティブなドキュメントの更新が完了すると、タブのテキストの色が変わり、更新ステータスが示されます。以下のアイコンは、表示される可能性のある更新ステータスです。

- ビジー:ドキュメントが更新中またはその他の操作を実行中です。
- 更新完了:最後の更新が正常に完了しました。非アクティブなタブのテキストは緑色で表示されます。
- 更新完了(エラーあり):最後の更新は正常に完了しましたが、エラーが発生したか、より詳しい情報を入手可能です。非アクティブなタブのテキストは黄色で表示されます。
- エラー:最後の更新を完了できませんでした。非アクティブなタブのテキストは赤色で表示されます。

ドキュメント タブをマウス オーバーすると、そのドキュメントに関するサマリー情報がツール ヒントに表示されます。



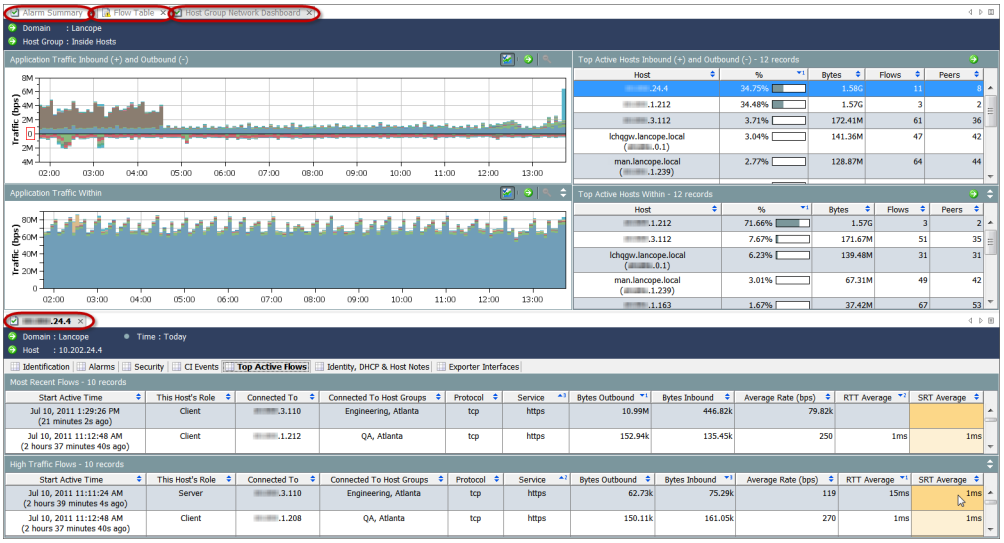
ドキュメントの方向の変更



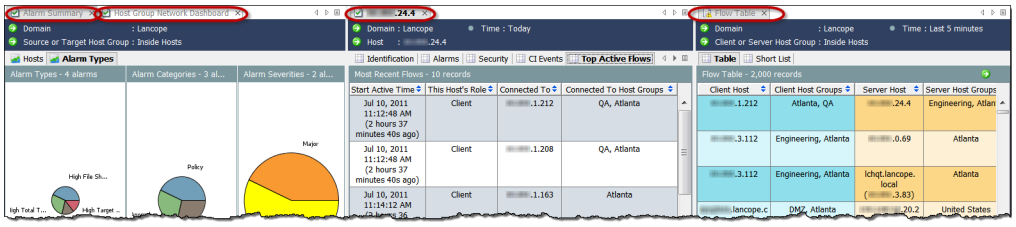
デフォルトでは、複数のドキュメントを開くと、1 つずつ表示され、タブでオフセットされます。この方向は必要に応じて変更でき、ドキュメントを横方向に下に重ねて、または縦方向に並べて表示することができます。方向を選択するには、ドキュメント タブを右クリックして、[新しい横方向グループ(New Horizontal Group)] または [新しい縦方向グループ(New Vertical Group)] をクリックします。

その結果は、次のいずれかの例のようになります。

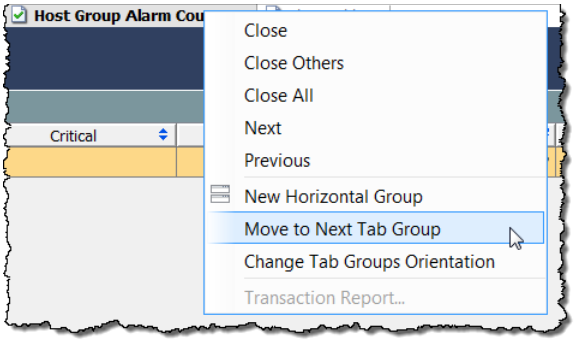
横方向グループ



縦方向グループ



現在の方向に従って、ドキュメントをあるタブ グループから別のタブ グループに移動するには、ドキュメント タブを右クリックして、[次のタブグループに移動（Move to Next Tab Group）]、[前のタブグループに移動（Move to Previous Tab Group）]、または [タブグループの方向を変更（Change Tab Groups Orientation）] を選択します。また、ドキュメント タブをクリックしてドラッグすることによって、開いているドキュメント間で位置を移動することもできます。



ドキュメント ヘッダー

ドキュメント ヘッダーには、ドキュメントが提供するデータに関する情報が記載されています。

上記の例は、フロー テーブル ヘッダーです。ヘッダーには、関連するホストが存在するドメインと、ホスト グループ名がリストされます。さらに、表示されるデータがいつキャプチャされたのかがわかります。

この例の表示データは、SmokeNet-Alpha ドメインの [内部ホスト（Inside Hosts）] ホスト グループで発生したフローです。ドキュメントに表示されているデータは、過去 12 時間以内に取得されたものです。これらのパラメータを変更するには、フィルタを使用します。この方法については、この後すぐに説明します。

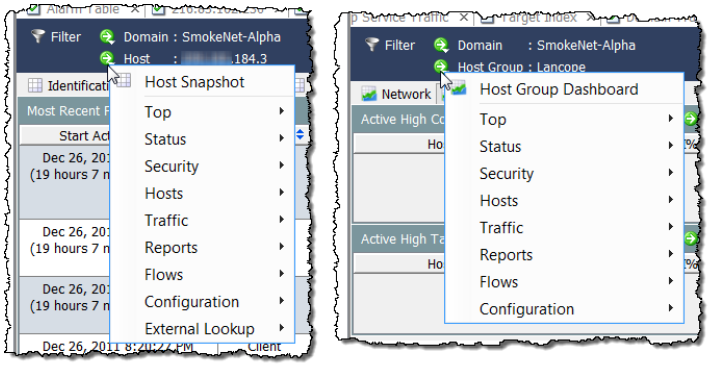
[ドキュメントに移動（Go to Document）] ボタン

[ドキュメントに移動（Go to Document）] ボタン は、Stealthwatch デスクトップ クライアント全体でドキュメントのヘッダーとツールバーに表示されます。このボタンをクリックしたときに表示される内容は、ボタンに関連付けられているオブジェクトによって異なります。

ドキュメント ヘッダー内

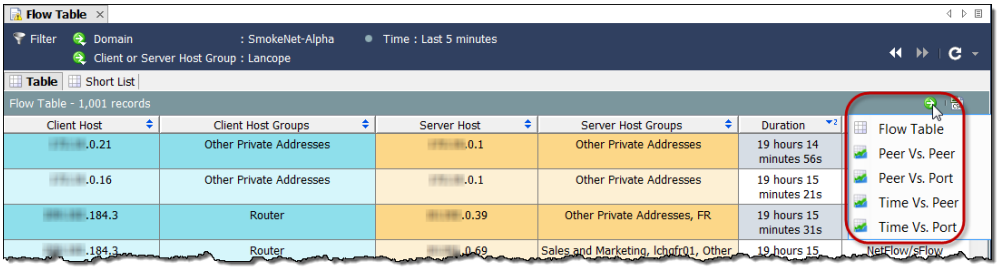
たとえば、ドキュメント ヘッダーでホスト IP アドレスの横にある [ドキュメントに移動(Go to Document)] ボタンをクリックすると、ホストに関連するドキュメント オプションが一覧表示されます。これらのオプションの 1 つをクリックすると、その特定のホストのみに関連するデータが表示されます。

同様に、ヘッダーでホスト グループ名の横にある [ドキュメントに移動(Go to Document)] ボタンをクリックすると、ホスト グループに関連するドキュメント オプションが一覧表示されます。これらのオプションの 1 つをクリックすると、その特定のホスト グループのみに関連するデータが表示されます。

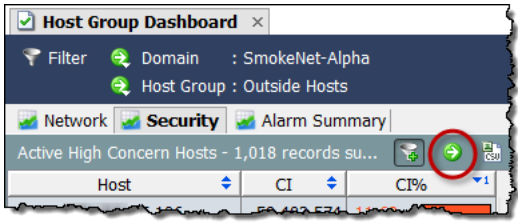


ドキュメント ツールバー内

ドキュメント ツールバーに表示される [ドキュメントに移動(Go to Document)] ボタンを使用すると、データをさまざまな方法で表示できます。たとえば、特定のホスト グループの [フローテーブル(Flow Table)] が表示されているとします。[フローテーブル(Flow Table)] ツールバーに表示されている [ドキュメントに移動(Go to Document)] ボタンをクリックすると、フローに関連するドキュメント オプションが一覧表示されます。これらのオプションの 1 つをクリックすると、このフロー情報が別の形式で表示されます。

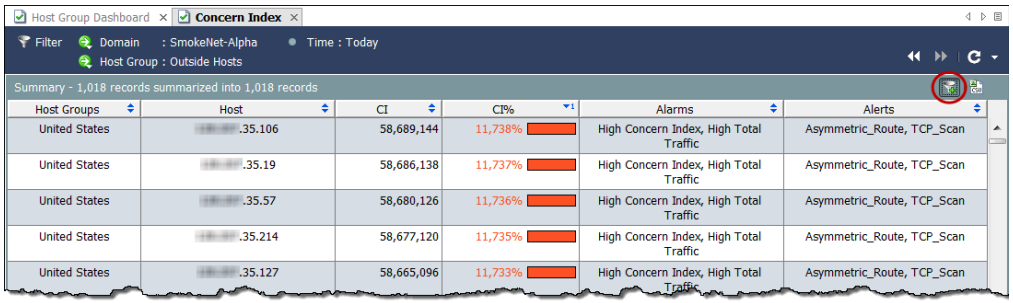


表示されているデータに関連するドキュメントが 1 つしかない場合もあります。その場合、[ドキュメントに移動(Go to Document)] ボタンをクリックすると、そのドキュメントがすぐに開きます。



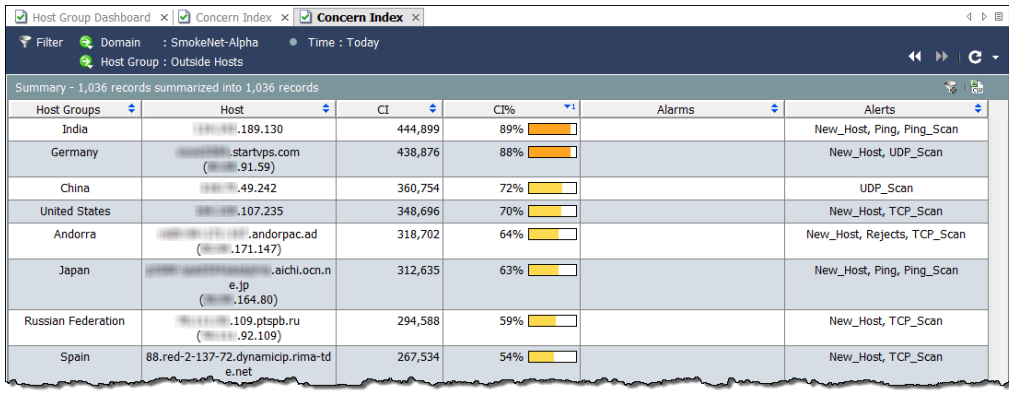
たとえば、ホスト グループ ダッシュボードの各コンポーネントには、[ドキュメントに移動(Go to Document)] ボタンを含む独自のツールバーがあります。[アクティブな高懸念ホスト(Active High Concern Hosts)] コンポーネントのボタンをクリックすると、SMC はただちに [リスクインデックス(Concern Index)] ドキュメントを開き、ホスト グループ ダッシュボードのそのコンポーネントに表示されている情報のみに関連するデータを表示します。

[リスクインデックス(Concern Index)] ドキュメントには、前回のアーカイブ時刻以降に CI ポイント数が最大であったホストの情報が表示されます。



[リスクインデックス(Concern Index)] ドキュメントを開くと、デフォルトで [リスクインデックス(Concern Index)] のフィルタ ボタン (ドキュメントの右上隅)がアクティブになり、[リスクインデックス(Concern Index)] には、[高懸念インデックス(High Concern Index)] アラームがアクティブであるホストのみ(すなわち、CI のパーセンテージが 100 を超えるホスト)が表示されます。CI のパーセンテージが 50 を超えるホストのみを表示するには、[リスクインデックス(Concern Index)] のフィルタ ボタンをクリックします。

[リスクインデックス(Concern Index)] のフィルタ ボタンのプラス記号が灰色 になり、CI のパーセンテージが 50 を超えるホストのみが表示されます。

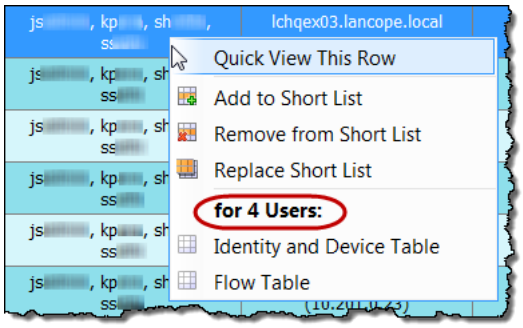


クイック フォーカスの右クリック

Stealthwatch デスクトップクライアント全体で提供されている右クリック機能は、ドキュメントを開くためのもう 1 つの手段です。右クリック メニューでは多くの場合、特定的なデータをメイン メニューよりすばやく見つけ出すことができます。

企業ツリーの要素を右クリックし、ポップアップ メニューから目的のドキュメントを選択します。この時点で、クリックした要素に関連性の高いデータが表示されます。たとえば、企業ツリーでホスト グループ名を右クリックし、[フロー(Flows)] > [フロートラフィック(Flow Traffic)] を選択すると、そのホストグループに関連性の高いフロー トラフィック データが表示されます。

ドキュメントを開くもう 1 つの方法は、ドキュメント内で右クリックして表示されるポップアップ メニューから目的の項目を選択する方法です。たとえば、ドキュメント内の列で 1 つ以上のユーザー名を右クリックすると、次のポップアップ メニューが表示されます。



ポップアップ メニューのラベル(上記の画像で丸で囲んであるラベル)は、ラベルの下にリストされているドキュメントをフィルタ処理できるユーザーの数を示しています。1 つの名前のみをクリックした場合、ラベルにはそのユーザーの名前が示されます。

(注):

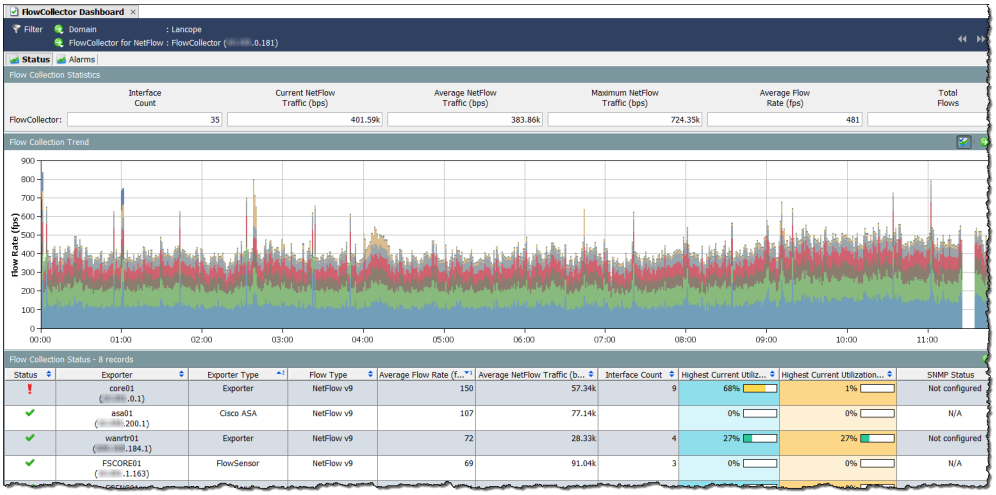
- また、表のセル内の項目をダブルクリックし、[ドキュメントに移動(Go to Document)] ボタンを使用してドキュメントを開くこともできます。

選択したドキュメントのダブルクリック

ダブルクリック機能は、任意の数のドキュメントを開くためのもう 1 つの手段です。企業ツリーのブランチをダブルクリックして開くことができるドキュメントについては、次の表を参照してください。

企業ツリーでダブルクリックするブランチ	表示されるドキュメント
SMC フォルダ	SMC ダッシュボード（SMC Dashboard）
特定のホスト グループ	ホスト グループ ダッシュボード（Host Group Dashboard）
内部/外部ホスト（Inside/Outside Hosts）フォルダ	ホスト グループ ダッシュボード（Host Group Dashboard）
ネットワーク デバイス（Network Devices）フォルダまたは特定のネットワーク デバイス	インターフェイス ステータス
エクスポータ（Exporters）フォルダまたは特定のエクスポータ	インターフェイス ステータス
特定のインターフェイス	インターフェイス サマリー ダッシュボード（Interface Summary Dashboard）
フロー センサー（Flow Sensors）フォルダ	インターフェイス ステータス
特定のマップ	その特定のマップ
特定の Cisco ASA エクスポータ	その ASA によってフィルタ処理された、過去 5 分間のフロー テーブル
Cisco ASA ファイアウォール以外のファイアウォール（Palo Alto ファイアウォールなど）	インターフェイス ステータス
ファイアウォール インターフェイス	インターフェイス サマリー ダッシュボード（Interface Summary Dashboard）
特定のフロー コレクタ	フロー コレクタ ダッシュボード（Flow Collector Dashboard）
特定の Cisco ISE	[アイデンティティとデバイス（Identity and Device）] テーブル
特定のアイデンティティ	[ユーザー アイデンティティ フィルタ（User Identity filter）] ダイアログ
特定の外部デバイス	外部イベント

たとえば、フロー コレクタの 1 つをダブルクリックすると、そのフロー コレクタのフロー コレクタ ダッシュボードが開きます。



ドキュメントの検索

SMC では、企業ツリー内の項目を検索できるだけでなく、特定の項目のすべてのドキュメントを(すべてのドメインにわたって)検索することができます。メイン ツールバーの [検索(Search)] フィールドでは、完全な文字列、部分文字列、またはワイルド カード (*) を含めた部分文字列を使用して、次の項目を検索できます。

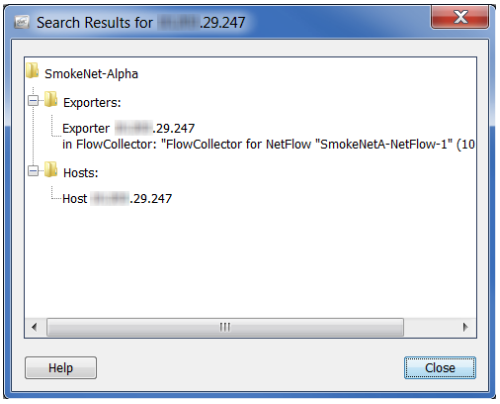
- アラーム ID
- ホストまたはエクスポータの IP アドレス
- 以下の名前:
  - エクスポータ
  - ホスト グループ
  - サーバー
  - ユーザー

(注):

- **検索結果は、ユーザー名に関連付けられているデータの権限と機能の権限に従って制限されます。**

ヒント：

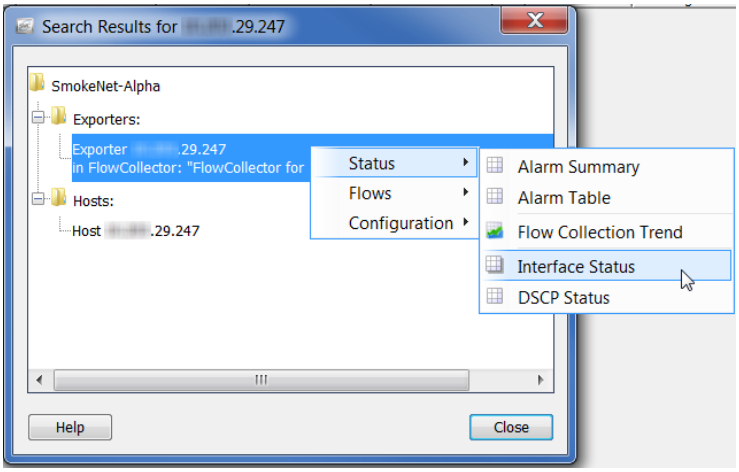
検索するには、[検索（Search）] ドロップダウン リスト ボックスから、以前に検索した項目を選択し、**Enter** キーを押します。



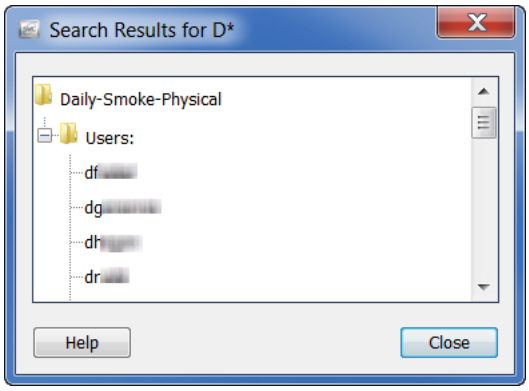
たとえば、[検索（Search）] フィールドにエクスポータの IP アドレスを入力して Enter キーを押すと、[検索結果（Search Results）] ダイアログには、その IP アドレスが表示される SMC 内の場所が一覧表示されます。

一覧の IP アドレスをダブルクリックすると、多くの場合、その項目に関する特定のドキュメントを表示できます。たとえば、ホスト エントリ下の IP アドレスをダブルクリックすると、その IP アドレスのホスト スナップショットが表示されます。

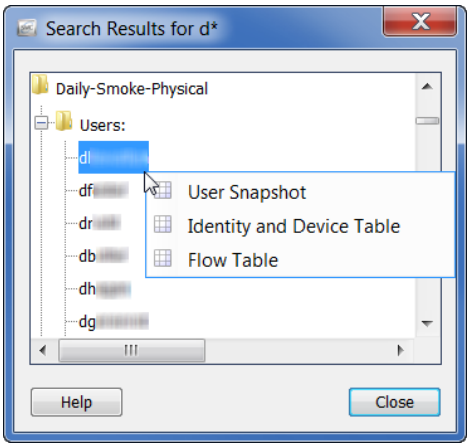
また、IP アドレスを右クリックして、その IP アドレスに関連する、アクセス可能な他の有益なドキュメントを一覧表示することもできます。



ユーザー名を検索すると、各ユーザー名は、[検索結果(Search Results)] ダイアログの「ユーザー(Users)」という名前のフォルダ内に個別の項目として表示されます。



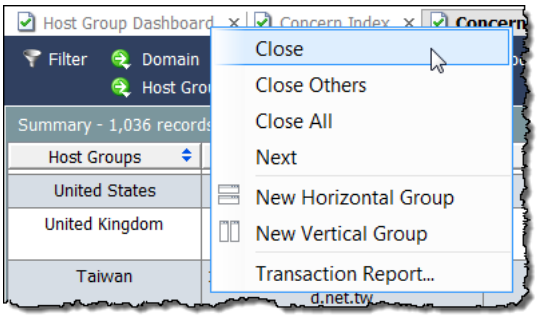
ユーザー名をダブルクリックすると、そのユーザーについて事前にフィルタ処理された状態の [アイデンティティとデバイス(Identity and Device)] テーブルが開きます。ユーザー名を右クリックすると、次のポップアップ メニューが表示されます。このメニューから、対応するユーザーについて事前にフィルタ処理されたドキュメントを選択できます。



ドキュメントを閉じる

SMC ドキュメントを開く方法がいくつかあるように、閉じる方法もいくつかあります。1 つのドキュメントを閉じるには、単にドキュメント タブの右隅にある [X] をクリックします。または、メイン メニューから [ファイル(File)] > [閉じる(Close)] をクリックするか、キーボードで **Ctrl+W** を押します。

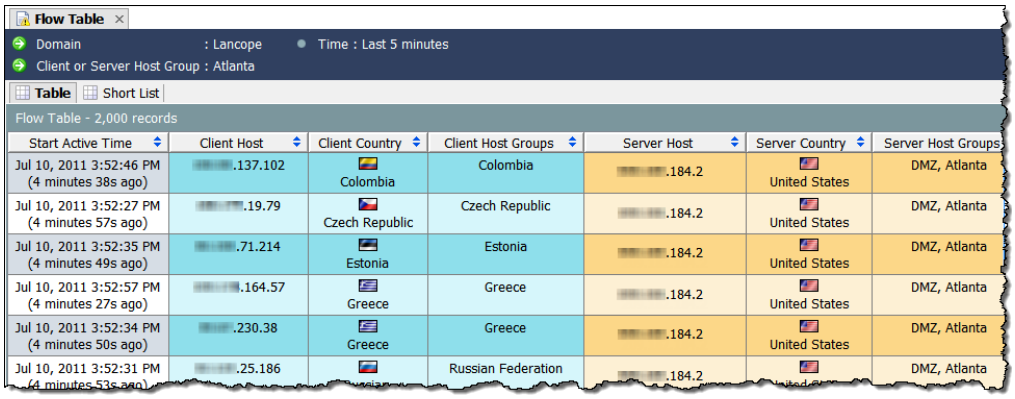
すべてのドキュメントを閉じるには、メイン メニューの [ファイル(File)] > [すべて閉じる(Close All)] をクリックします。また、ドキュメント タブを右クリックし、ポップアップ メニューから適切なオプションを選択することもできます。



(注):
SMC で使用できるキーボード ショートカットの完全なリストについては、「キーボードのショートカット」(80 ページ)を参照してください。

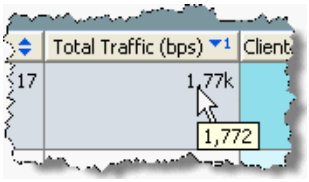
テーブルの操作

テーブルが含まれているドキュメントには、追加のナビゲーション要素があります。重要なグラフィックの標識の 1 つは、次の [フロー テーブル(Flow Table)] のような、表内の行の色分けです。



- 青色はクライアント側のデータを示します。
- 橙黄色はサーバー側のデータを示します。

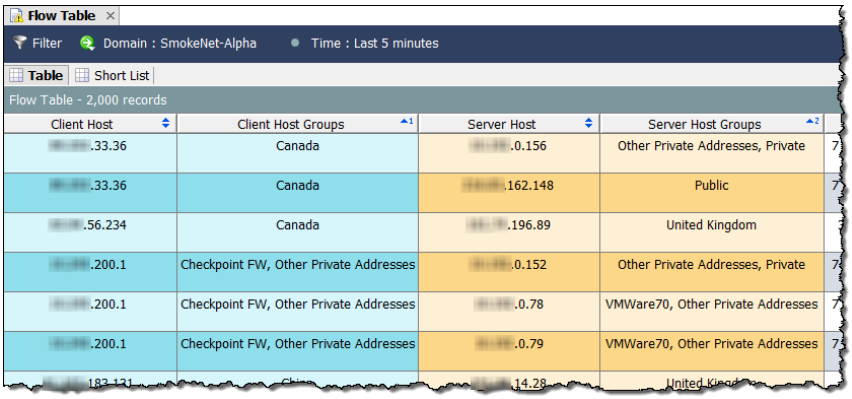
測定単位は、*bps*(1 秒あたりのビット数)のように、列ヘッダーに示されています。対応するセルの数値は四捨五入されます。ただし、四捨五入された値をマウス オーバーすると、ツール ヒントに正確な値が表示されます。



列のソート

列を昇順または降順にソートするには、列ヘッダーの [上/下(Up/Down)] ボタン ⬍ をクリックします。(このボタンは、昇順または降順を示すために切り替わります)。テーブルは、3 つの特定の列を基準にソートすることができます。1 つの列をソートすると、その列に基づいてテーブル全体がソートされます。2 番目の列をソートすると、最初にその列に基づいてテーブル全体がソートされ、次にソートされた最初の列に基づいてテーブル全体がソートされ、以下同様にソートが実行されます。

次の例では、ソートされた最初の列は、[サーバー ホスト グループ(Server Host Groups)] 列であり、英数字の昇順でソートされました。次に [クライアント ホスト グループ(Client Host Groups)] 列が英数字の昇順でソートされると、この列がソートされた最初の列になり、[サーバー ホスト グループ(Server Host Groups)] 列はソートされた 2 番目の列になりました。

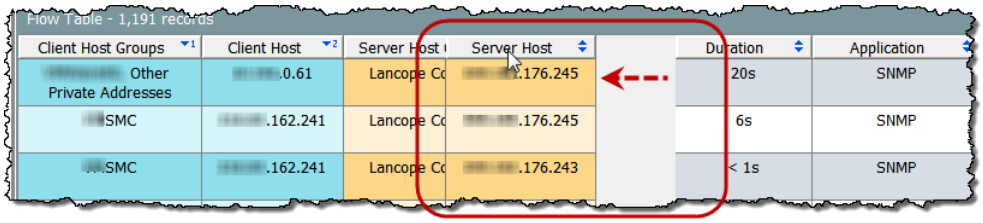


（注）:

列からソート動作を削除するには、キーボードの **Ctrl** キーを押しながら列ヘッダーをクリックします。

列の移動とサイズ変更

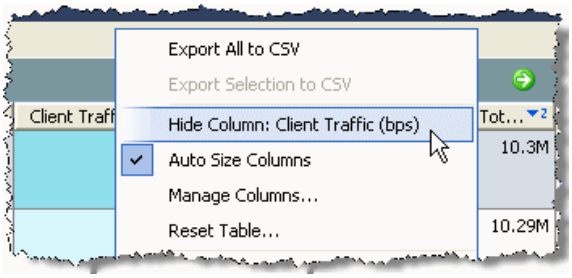
列を左右に移動するには、単に列ヘッダーをクリックして、列を目的の位置までドラッグします。



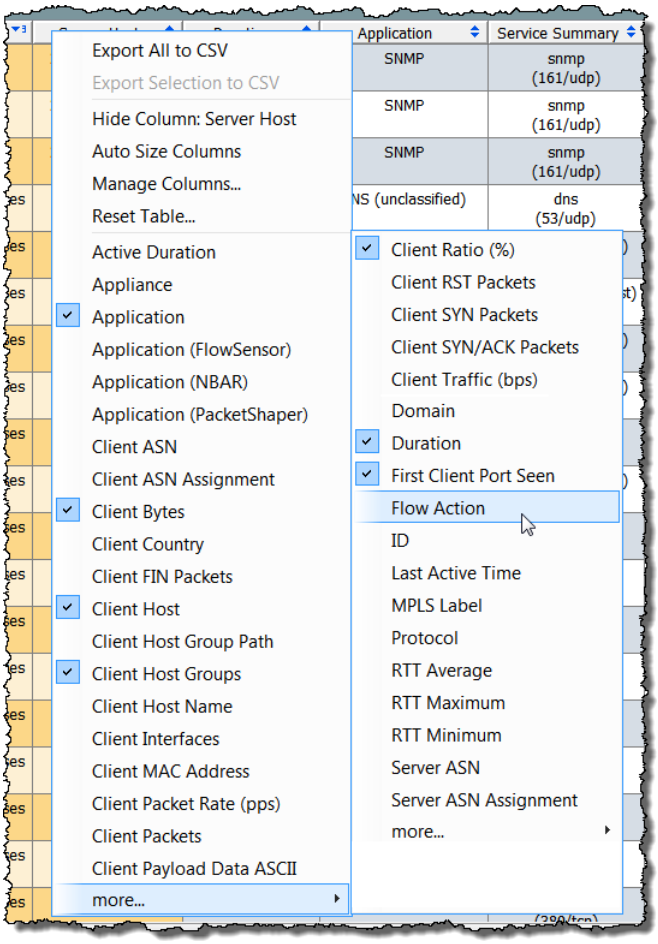
デフォルトでは、列幅は自動的に調整され、すべての列が画面上に可能な限り表示されます。列の幅を手動で拡大または縮小するには、列ヘッダーの境界線をクリックして左右にドラッグし、希望の幅に調整します。

列の非表示と表示

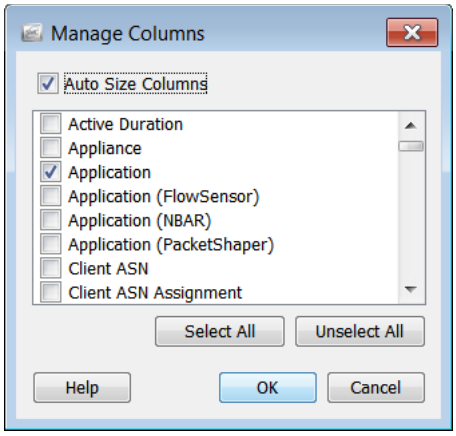
列を非表示にするには、列ヘッダーを右クリックし、[列を非表示:<名前>（Hide Column: <Name>）] を選択します。



列をさらに表示するには、列ヘッダーを右クリックし、ポップアップ メニューから表示する列を選択します。



また、[列を管理(Manage Columns)] ダイアログに移動して、特定の列の非表示と表示を切り替えることもできます。列ヘッダーを右クリックし、[列を管理(Manage Columns)] を選択します。対応するドキュメントで列が表示されるようにするには、そのチェックボックスをクリックしてチェックマークを付けます(チェックマークがまだ付いていない場合)。対応するドキュメントに列が表示されないようにするには、そのチェックボックスをクリックしてチェックマークを外します(チェックマークがまだ付いている場合)。



SMC が列のサイズを自動的に変更するようにするには、ダイアログの上部にある [列のサイズを自動調整(Auto Size Columns)] チェックボックスにチェックマークが付いていることを確認します。SMC は、列が自動的に画面に表示されるように、列のサイズを可能な限り大きくし、水平スクロール バーは表示しません。すべての列のサイズを手動で変更するには、[列のサイズを自動調整(Auto Size Columns)] チェックボックスにチェックマークが付いていないことを確認します。

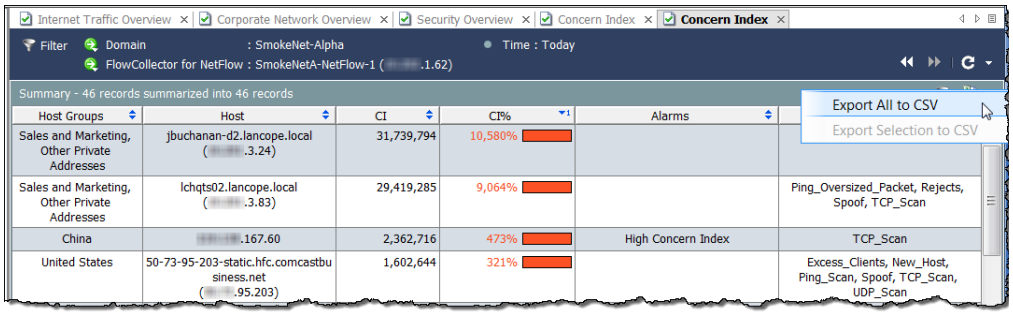
変更が完了したら、[OK] をクリックして変更を適用し、[列を管理(Manage Columns)] ダイアログを閉じます。

ヒント:
テーブルをデフォルト設定に戻すには、列ヘッダーを右クリックして、[テーブルをリセット(Reset Table)] を選択します。

データのエクスポート

SMC テーブルに表示されるデータは、コンマ区切り値(CSV)ファイルに保存できます。CSV ファイルは、後から確認できるように、Microsoft Excel などのほとんどのスプレッドシート プログラムにインポートできます。テーブル内のすべての情報をエクスポートすることも、特定の選択項目のみをエクスポートすることもできます。

テーブルのすべての情報をエクスポートするには、ドキュメントの右上にある [CSV にエクスポート (Export to CSV)] ボタン をクリックし、[すべてを CSV にエクスポート (Export All to CSV)] をクリックします。



(注)

テーブル内の情報の 1 行のみをエクスポートするには、エクスポートするデータの行をクリックします。複数の行を選択するには、**Shift** キーまたは **Ctrl** キーを押しながら選択するか、カーソルをドラッグして必要な選択項目を強調表示します。ドキュメントの右上にある [CSV にエクスポート (Export to CSV)] ボタン をクリックし、[選択項目を CSV にエクスポート (Export Selection to CSV)] をクリックします。

[保存 (Save)] ダイアログが開いたら、情報を保存するディレクトリに移動し、ファイル名を入力します (この形式でファイルを保存するには、ファイル名の最後に **.csv** と入力する必要があります)。[保存 (Save)] をクリックします。これで、選択したスプレッドシート プログラムでその情報を開いて表示することができます。

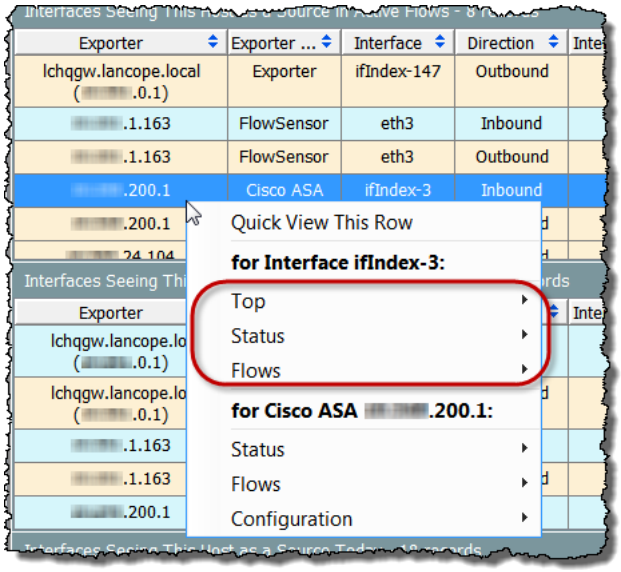
ヒント:

テーブル内の任意のヘッダーを右クリックして、CSV 形式にエクスポートするためのオプションにアクセスすることもできます (オプションはポップアップ メニューに表示されます)。

マルチセクション ポップアップ メニュー

これまで説明したテーブルのポップアップ メニューはかなり単純なものであり、オプションのセクションは 1 つしかありませんでした。ただし、ポップアップ メニューの中には、選択した行の処理方法に基づいて複数のセクションが存在するものがあります。

たとえば、次の例に示すポップアップ メニューを表示するには、ホスト スナップショットの [エクスポータインターフェイス(Exporter Interfaces)] タブでエクスポータをクリックしてから、右クリックする必要があります。

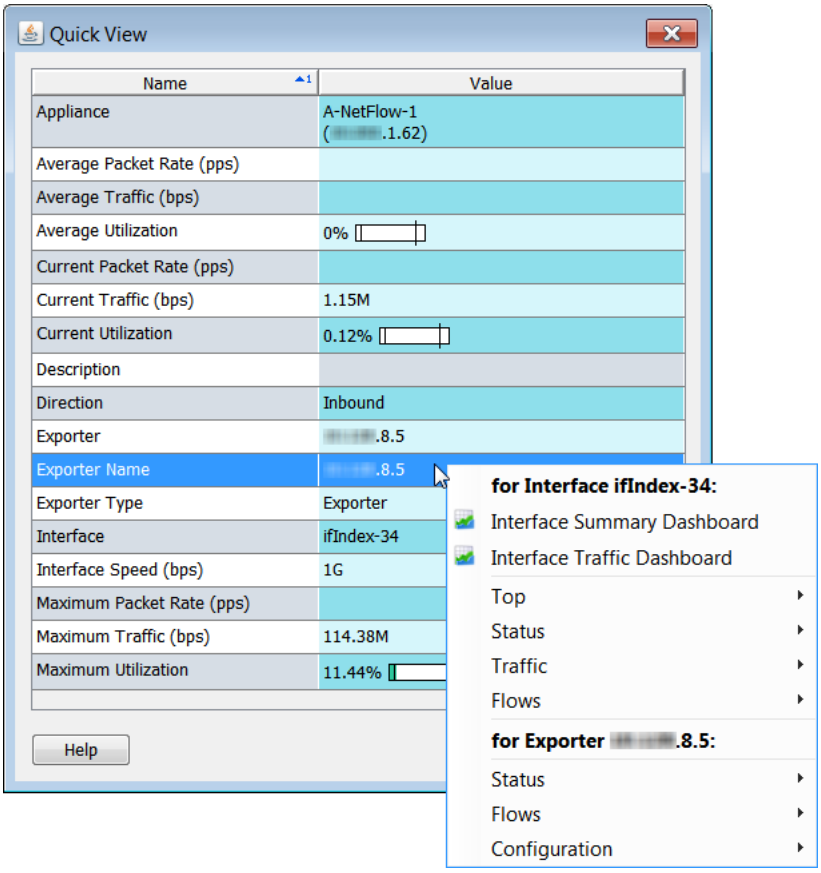


ポップアップ メニューの最上位に表示されるオプションは、行全体に適用されます。ポップアップ メニューの次のレベルに表示されるセクションは、その行の特定のセルに適用されます。前の例では、次のタイプのドキュメントを表示できます。

- ifIndex-3 インターフェイスと関連性の高いドキュメント(前の例で丸で囲んであるオプションのいずれかをクリック)。
- Cisco ASA xxx.xxx.200.1 エクスポータと関連性の高いドキュメント(ポップアップ メニューの最後の 3 つのオプション)。

クイック ビュー

[クイックビュー(Quick View)] ダイアログでは、テーブルの特定の行に表示されるデータをすばやく簡単に表示できます。単に目的の行をクリックし、キーボードのスペースバーを押します。また、行を右クリックして、[この行をクイックビューで表示(Quick View This Row)] を選択することもできます。



クイック ビューには、他のドキュメントのフィルタ処理されたビューへのナビゲーションが表示されることがあります。行内を右クリックすると、関連するドキュメントのポップアップ メニューが表示され、その行のデータの詳細を表示することができます。

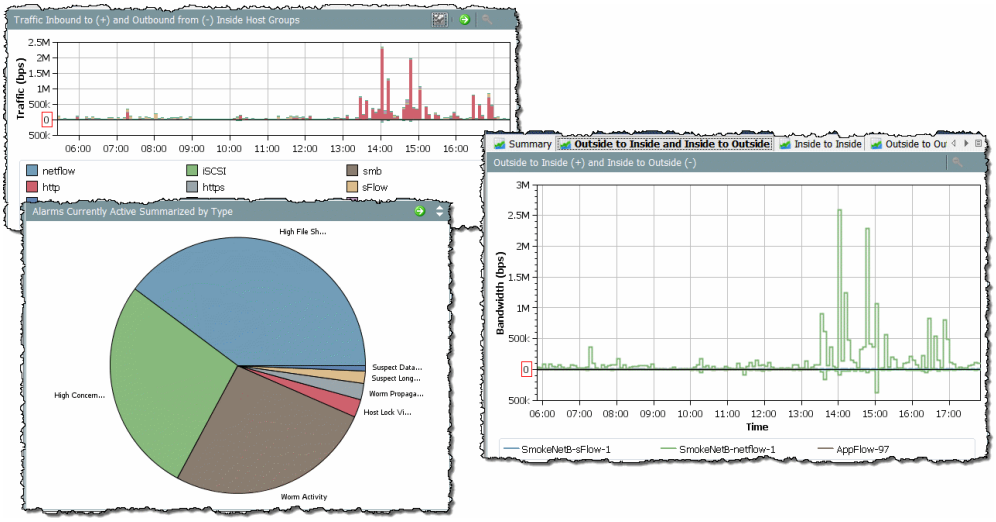
クイック ビューを閉じずに、関連付けられているドキュメントの行間を移動するには、キーボードの **Alt** キーと上下キーを同時に押します。

[クイックビュー(Quick View)] ダイアログを閉じるには、次のいずれかの操作を行います。

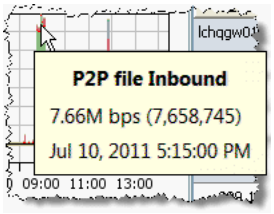
- キーボードのスペースバーを押します。
- キーボードの **Esc** キーを押します。
- 右上隅の ボタンをクリックします。

グラフの使用

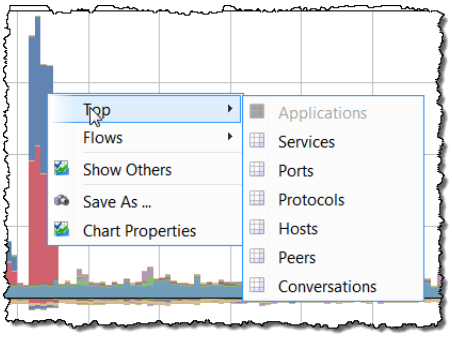
Stealthwatch デスクトップクライアントの一部のドキュメントには、以下の例に示すような棒グラフ、折れ線グラフ、または円グラフが含まれています。



グラフを JPG または PNG ファイルとして保存するには、グラフの任意の場所を右クリックし、[名前をつけて保存(Save As)] を選択します。その後、そのグラフィックを、分析、レポート、アーカイブなどの目的に応じて、別のドキュメントにインポートすることができます。



チャート上の各色は、表示しているチャートに応じて、特定のアプリケーション、サービス、アラーム タイプ、またはアプライアンスを表します。チャート上の特定の項目の詳細を表示するには、色付きの領域をマウス オーバーして、詳細情報を含むツール ヒントを表示します。



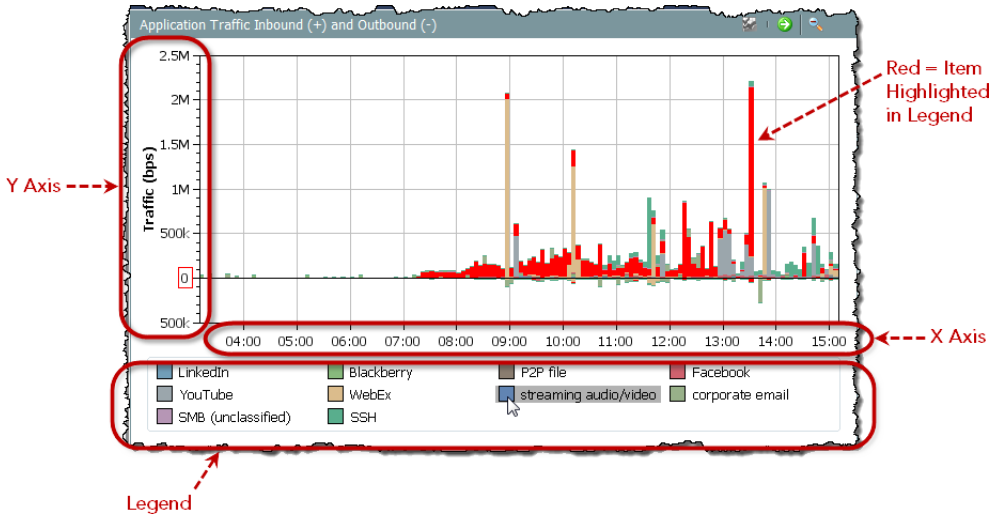
また、色付き領域を右クリックし、表示されるポップアップ メニューからオプションをクリックすることもできます。表示されるドキュメントには、チャート上でクリックした項目と関連性の高いデータが含まれています。

棒グラフまたは折れ線グラフの領域をズーム インするには、その領域を横切るようにカーソルを押したままドラッグします。ズーム インしたら、キーボードの矢印キーを使用してチャート内を上下左右に移動することによって、さまざまな領域を表示できます。通常の倍率に戻すには、キーボードの **F** キーを押すか、チャートの右上隅にある [ズームアウト(Zoom-out)] ボタン をクリックします。

（注）：

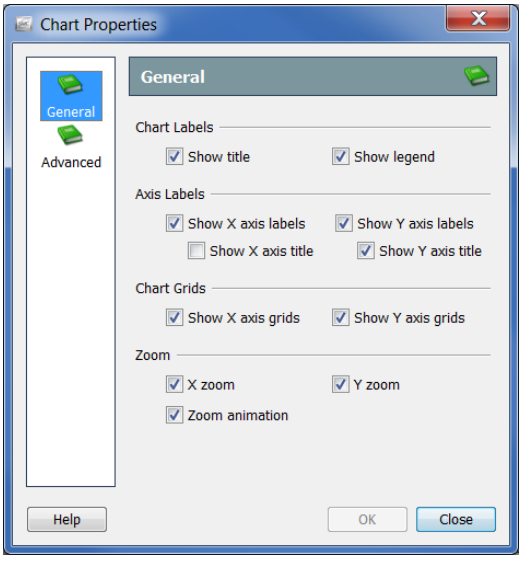
サービス トラフィック データを示すチャートには、右上隅に [表示/非表示（Show/Hide）] ボタン があり、このボタンをクリックすると、一般的に「*その他（Others）*」と表示されているサービス トラフィックの表示と非表示が切り替わります。

棒グラフと折れ線グラフには凡例が付いています。凡例には、さまざまな色とその意味が一覧表示されます。凡例の項目をマウス オーバーすると、チャート内の関連付けられているデータ ポイントが赤で強調表示されます。

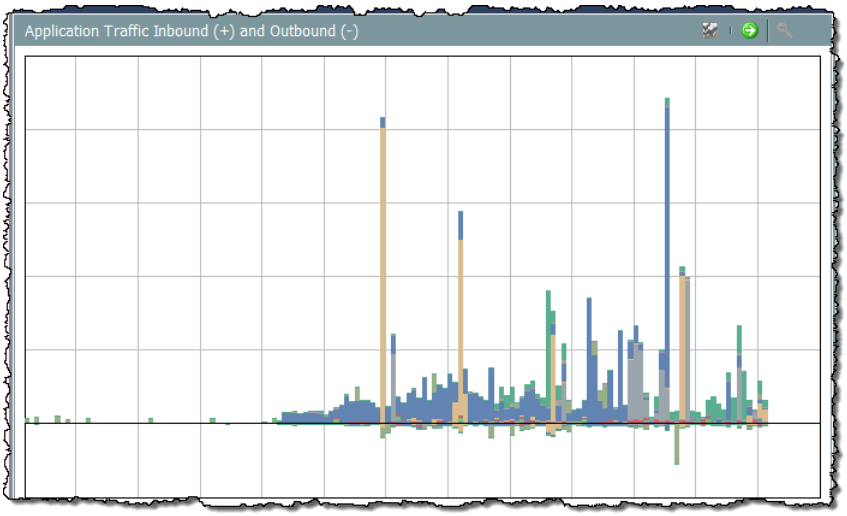


ご覧のように、これらの要素はドキュメント上で多くのスペースを占める場合があります。データ ポイントをマウス オーバーしてツール ヒントを表示すると、ほとんどのアプリケーション情報を確認できるため、凡例や軸を表示する必要がないと判断できる場合があります。

凡例または軸を非表示にするには、チャートの任意の場所を右クリックし、[チャートのプロパティ（Chart Properties）] を選択して、[チャートのプロパティ（Chart Properties）] ダイアログを開きます。[チャートのプロパティ（Chart Properties）] ダイアログで、非表示にする要素に対応するチェックボックスをクリックして、チェックマークを外します。

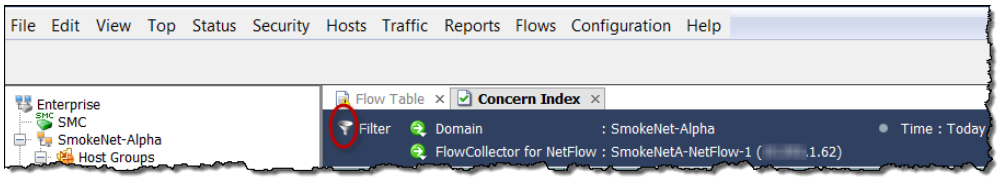


たとえば、ホスト グループ ネットワーク ダッシュボードの [アプリケーショントラフィックインバウンドおよびアウトバウンド（Application Traffic Inbound and Outbound）] チャートで凡例および軸のラベルを非表示にすると、次の例のようになります。

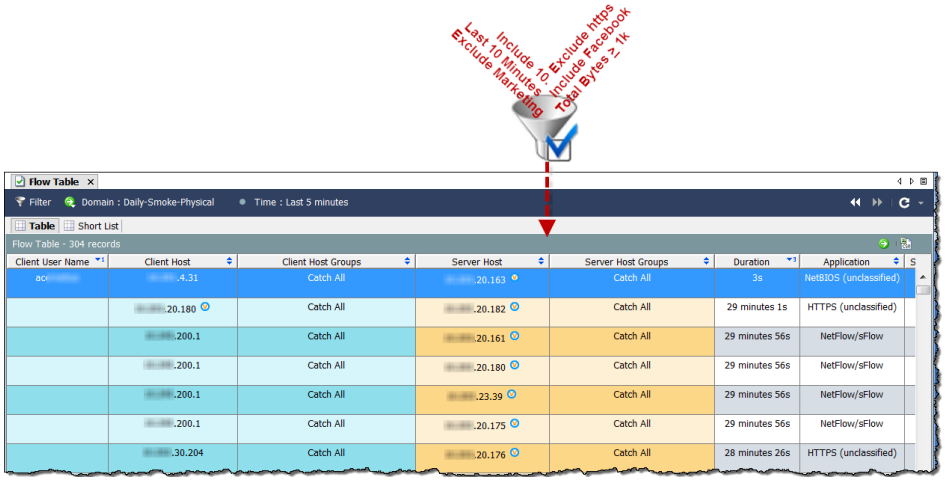


ドキュメント データのフィルタリング

このガイドに記載の情報のうち最も覚えておいていただきたいのは、「フィルタは大変役に立つ」ということです。アクティブな SMC ドキュメントのフィルタを開くには、ドキュメント ヘッダーの [フィルタ (Filter)] ボタン をクリックします。



フィルタをじょうごとして使用して、Stealthwatch から入手できる膨大な量のデータから、必要な情報のみを取得してください。



フィルタは、ほぼすべての SMC ドキュメントに適用できます。フィルタリングではさらに、履歴データを表示することができます。これは、フォレンジックの観点から非常に役立ちます。

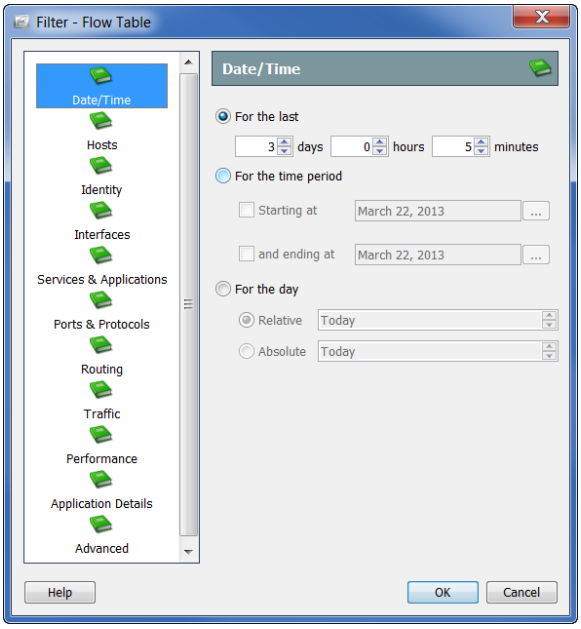
(注):

ドキュメントを共有として保存すると、フィルタ設定も保存されます。詳細については、「ドキュメントの保存」(71 ページ) を参照してください。

すべての SMC ドキュメントに、ほぼ同じ方法で動作するフィルタがあります。[フローテーブル (Flow Table)] に表示される情報をフィルタリングする方法を確認していきましょう。

日時

[日付/時間(Date/Time)] ページでは、[フローテーブル(Flow Table)] をフィルタ処理して、特定の日時に発生したフローの情報から最新の情報までを表示することができます。



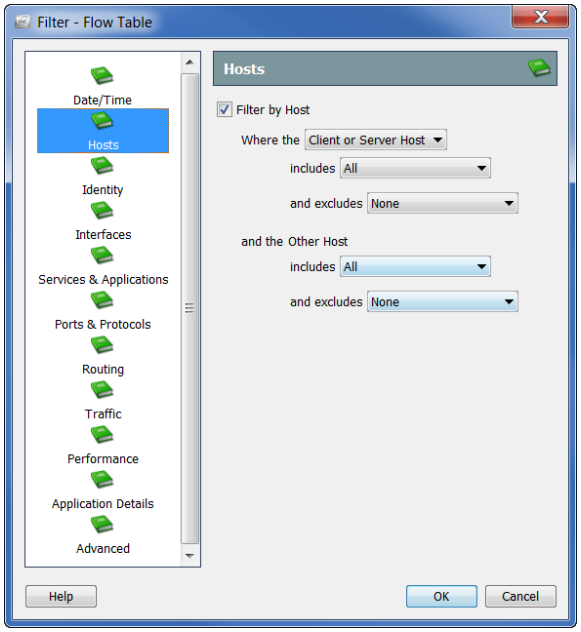
ヒント:

複数日にわたるフローを調べるには、[フローテーブル(Flow Table)] ではなく、[フロートラフィック(Flow Traffic)] ドキュメントを使用すると、よりすばやく必要な情報を入手できます。

ホスト

[フィルタ - フローテーブル(Filter - Flow Table)] の [ホスト(Hosts)] ページでは、特定のホストのみが含まれたフローの情報を表示できます。

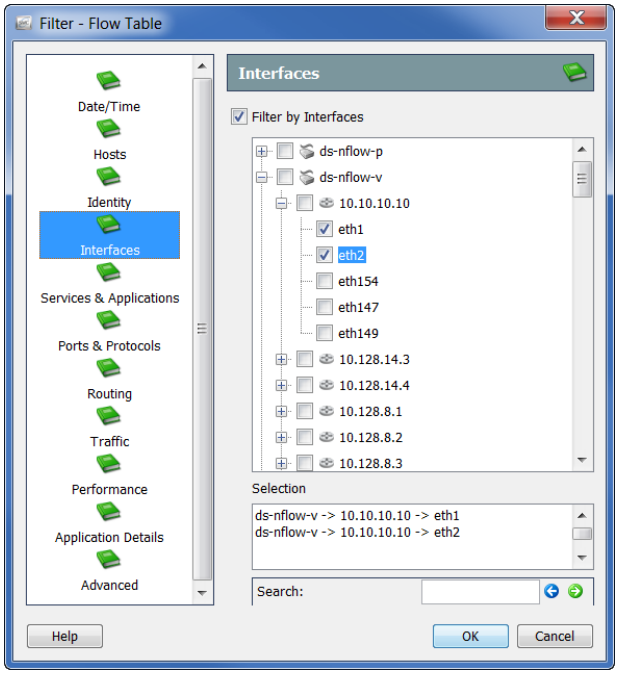
サーバー ホスト、クライアント ホスト、またはその両方をフィルタ処理できます。対象を特定のホスト グループ、IP アドレスの範囲、または特定の IP アドレスに絞り込むことができます。



ヒント:

NATed フローを表示せずに内部ホストに関係するフローを検索するには、[フィルタ - フローテーブル(Filter - Flow Table)] の [ホスト(Hosts)] ページに移動し、ネットワークで使用されている広範な内部 IP アドレス範囲(例:10.0.0.0/8)をフィルタ処理に含めるように指定します。

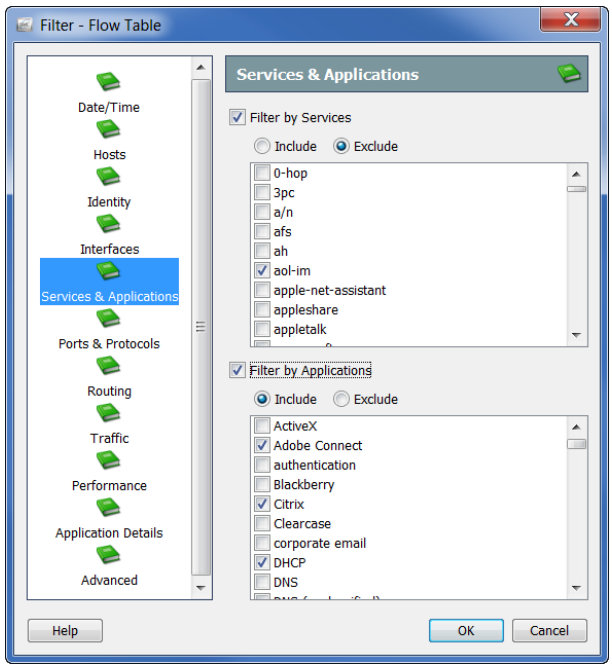
インターフェイス



[フィルタ - フローテーブル(Filter - Flow Table)] の [インターフェイス(Interfaces)] ページでは、特定のフロー コレクタ、エクスポータ、インターフェイスなどに関連するフローの情報を表示できます。フロー コレクタのすべてのエクスポータを選択するには、そのフロー コレクタの対応するチェックボックスをクリックして、チェックマークを付けます。これにより、これらのエクスポータのすべてのインターフェイスも選択されます。

選択した項目がフィルタの [選択(Selection)] フィールドに表示されます。さらに、項目名の一部がわかっている場合は、項目名の下の [検索(Search)] フィールドに項目名を入力すると、インターフェイスの一覧からその項目を見つけ出すことができます。

サービスとアプリケーション



[フィルタ - フローテーブル(Filter - Flow Table)] の [サービスとアプリケーション(Services & Applications)] ページでは、特定のサービスやアプリケーションを使用したフローの情報を表示できます。また、特定のサービスやアプリケーションを使用したフローを除外することもできます。

その他のフィルタ オプション

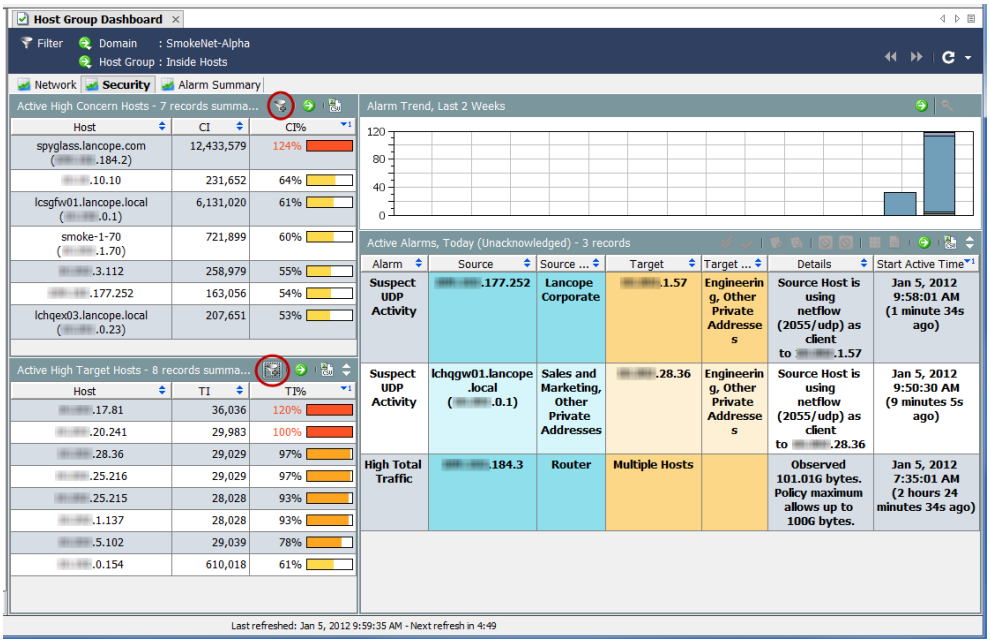
[フィルタ - フロー テーブル(Filter - Flow Table)] 内のその他のページは、これまで説明したフィルタ ページと同様に動作します。次の表で、[フィルタ - フローテーブル(Filter - Flow Table)] の残りのフィルタ ページについて簡単に説明します。

ページ	フローのフィルタ条件
[ID(Identity)]	ユーザー名
[ポートとプロトコル(Ports & Protocols)]	特定の IANA 定義プロトコル、TCP/UDP ポート、クライアントのみが使用するポート。
ルーティング(Routing)	DSCP ポイント、自律システム番号、VLAN ID、MPLS ラベル。
[トラフィック(Traffic)]	合計バイト数、合計パケット数、クライアント バイト数、クライアント パケット数、サーバー バイト数、サーバー パケット数(必要に応じて特定の値の範囲を含む)。 注:[フローテーブル(Flow Table)] には、未加工のトラフィック データが表示されます。
[パフォーマンス(Performance)]	TCP 接続合計、TCP 再送信合計、最小/最大/平均 RTT、最小/最大/平均 SRT(必要に応じて、特定の値の範囲を含む)。
[アプリケーションの詳細(Application Details)]	特定のアプリケーションの詳細文字列(包含または除外)。
[詳細設定(Advanced)]	最大レコード数、特定のフロー レコード フィールド(例えば、バイト数合計、クライアント バイト数など)の最大値または最小値、ファイアウォールによって許可または拒否されるフロー アクション、包含または除外されるフローの重複、包含または除外されるインターフェイス データ、より高速なクエリ(ソートまたはグループ化なし)。

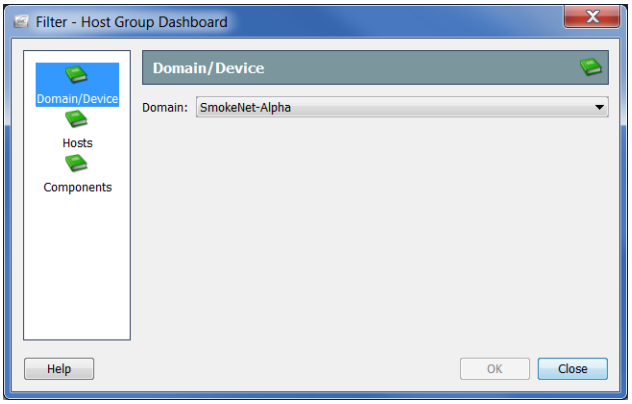
ドキュメント、ダイアログ、またはフィルタに関する質問がある場合は、Stealthwatch デスクトップクライアントのオンラインヘルプをいつでも参照できます。

ダッシュボード フィルタ

ほとんどの SMC ドキュメントのフィルタは、[フィルタ - フローテーブル(Filter - Flow Table)] と非常によく似ています。ただし、ダッシュボード用のフィルタは少し異なります。ダッシュボード フィルタを使用すると、関連付けられているダッシュボード上の各コンポーネントをフィルタ処理できます。例として、ホスト グループ ダッシュボードで情報をフィルタリングする方法を見てみましょう。



ホスト グループ ダッシュボードのドキュメント ヘッダーで、[ダッシュボード フィルタ(Dashboard Filter)] ボタンをクリックしてフィルタを開きます。一般的に、ダッシュボード フィルタには、次の 3 つの画面で示した 3 つのページが含まれています。

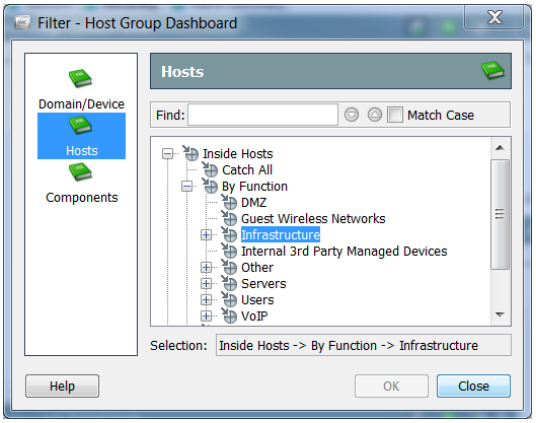


この例では、フィルタの [ドメイン/デバイス(Domain/Device)] ページで、表示するデータのドメインのみを変更できます。前の例では、SmokeNet-Alpha ドメインが選択されていました。ダッシュボードによっては、特定のフロー コレクタ、エクスポータ、またはインターフェイスを選択することもできます。

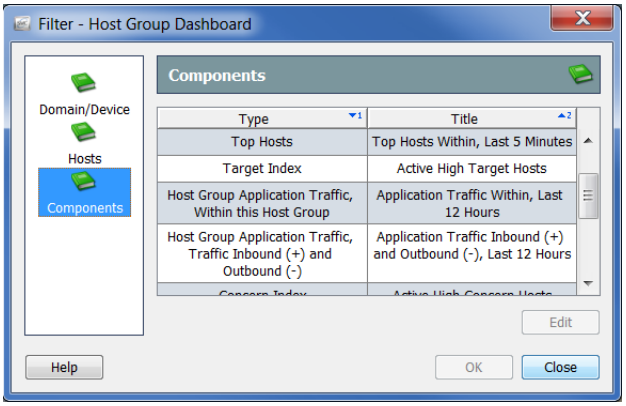
(注):

これらの 3 つのページで指定した内容によって、コンポーネント フィルタの選択が上書きされます。これについては、この後すぐに説明します。

異なるホスト グループのデータを表示するようにダッシュボードをフィルタ処理するには、[ホスト(Hosts)] ページを開きます。ホスト グループの一覧をスクロールして選択することができます。または、[検索(Find)] フィールドにホスト グループの名前を全部または一部入力すると、一覧が自動検索されるため、目的のホスト グループを見つけ出すことができます。ホスト グループをクリックすると、そのホスト グループが画面下部の [選択(Selection)] フィールドに表示されます。この例では、[機能別(By Function)] ホスト グループの [インフラストラクチャ(Infrastructure)] ホスト グループがクリックされています。



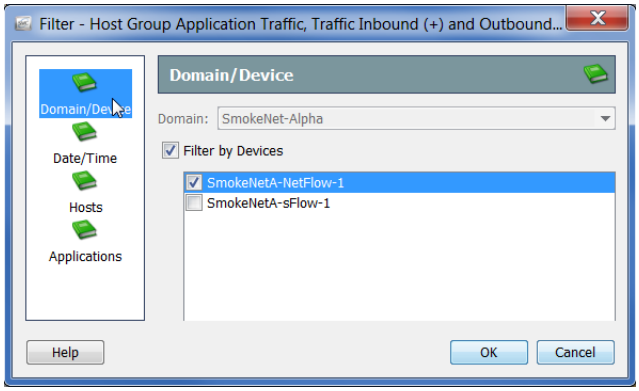
フィルタの [コンポーネント(Components)] ページを開くと、ダッシュボード上の個々のコンポーネントをフィルタ処理できます。



(注):

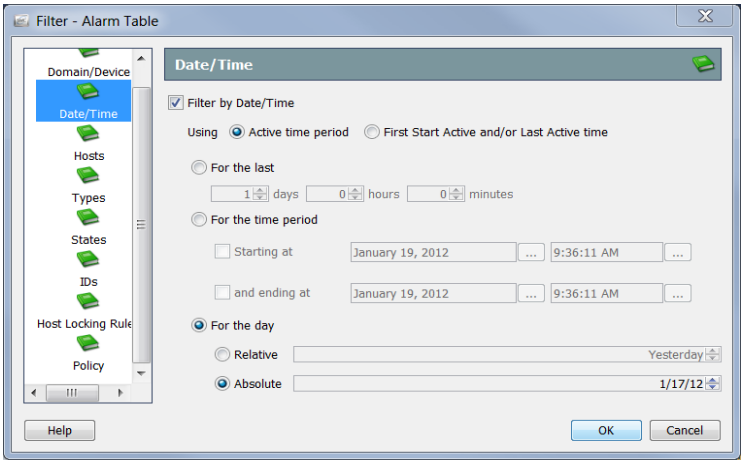
コンポーネントのタイトルをダブルクリックして、ダッシュボードに表示されている名前に変更します。

たとえば、特定の時間内に特定のフロー コレクタによって認識されたプライベート アドレス(Private Addresses)ホスト グループの Facebook アクティビティを表示するとします。この場合、[タイプ(Type)] 列で [ホストグループのアプリケーショントラフィック、トラフィックインバウンド(+)およびアウトバウンド(-)(Host Group Application Traffic, Traffic Inbound (+) and Outbound (-))] をクリックし、[編集(Edit)] をクリックします。



このコンポーネントの [フィルタ(Filter)] ダイアログボックスが開きます。ダッシュボード フィルタですでに SmokeNet-Alpha ドメインをクリックしているため、ここで変更することはできません。ただし、データを表示するフロー コレクタを選択することができます。

表示する時間を指定するには、フィルタの [日付/時刻(Date/Time)] ページを開きます。

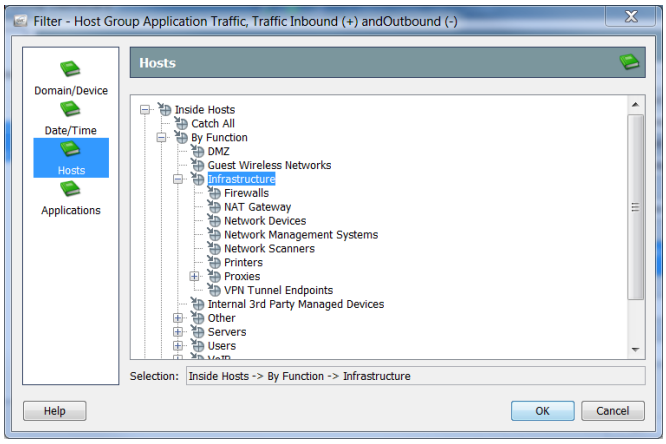


[日付(For the day)] 設定の [相対的(Relative)] および [絶対的(Absolute)] は、将来確認できるように特定のレイアウトやフィルタ設定とともに保存するドキュメントにおいて役立ちます。

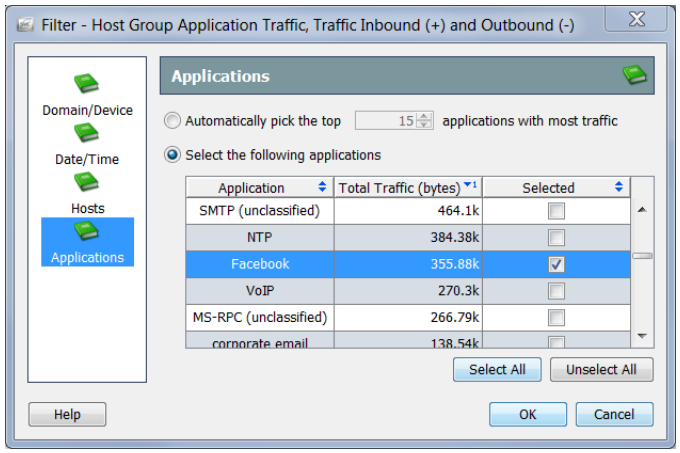
[日付(For the day)] セクションで [絶対的(Relative)] をクリックし、リスト ボックスから [昨日(Yesterday)] を選択するとします。次に、ドキュメントを共有として保存します。そのドキュメントを開くタイミングに関係なく、[昨日(Yesterday)] が選択されたままになります。したがって、このドキュメントは常に前日のデータを表示します。

今度は [日付(For the day)] セクションで [絶対的(Absolute)] をクリックし、リスト ボックスから [2012/1/17(1/17/12)] を選択するとします。次に、ドキュメントを共有として保存します。そのドキュメントを開くタイミングに関係なく、[2012/01/17(1/17/12)] が選択されたままになります。したがって、このドキュメントは常にその日付のデータを表示します。

ダッシュボード フィルタですでにインフラストラクチャ(Infrastructure)ホスト グループをクリックしてあったため、コンポーネント フィルタの [ホスト(Hosts)] ページでそれを変更することはできません。選択項目の表示だけが可能です。



Facebook 以外のすべてのアプリケーションをフィルタで除外するには、コンポーネント フィルタの [アプリケーション(Applications)] ページを開きます。デフォルトでは、このフィルタはトラフィックを最も多く発生させる上位 10 個のアプリケーションを自動的に選択します。[次のアプリケーションを選択する(Select the following applications)] オプションをクリックし、右下隅にある [すべて選択解除(Unselect All)] をクリックして、選択したすべてのアプリケーションをクリアします。最後に、[Facebook] チェックボックスをクリックして、チェックマークを付けます。



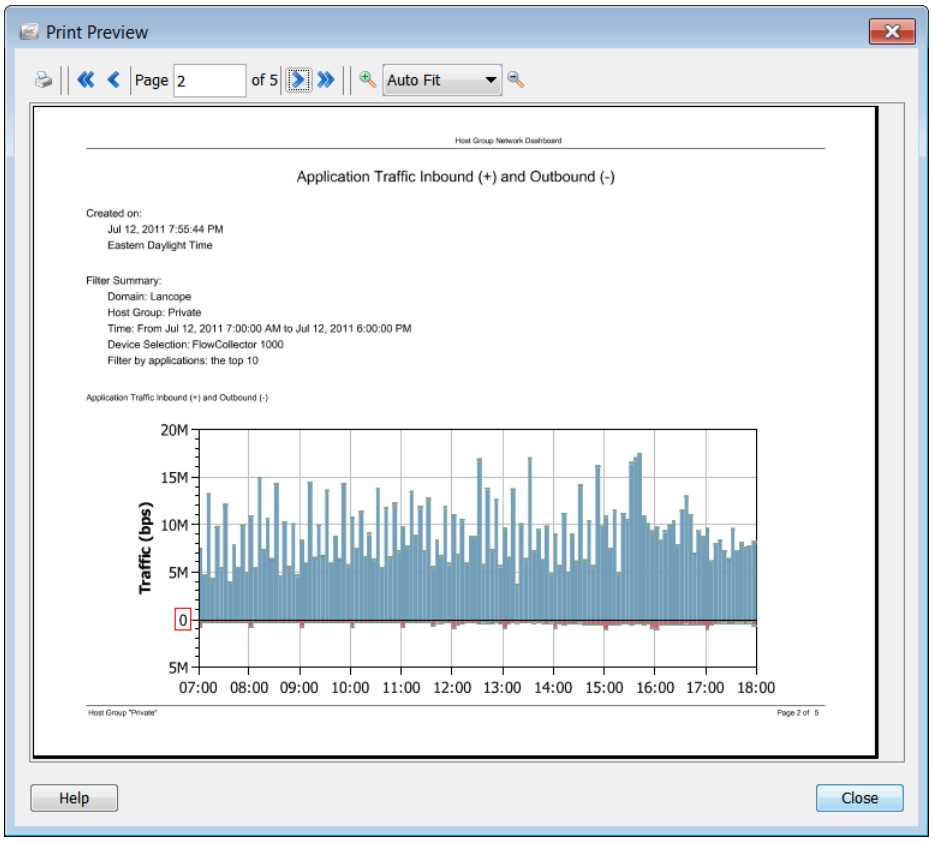
完了したら、[OK] をクリックしてコンポーネント フィルタを閉じ、ダッシュボード フィルタに戻ります。ダッシュボード フィルタで必要に応じて変更を加えたら、[OK] をクリックして、選択したデータ セットでダッシュボードを更新します。

ドキュメントの印刷

後から検討できるように、または同僚に送信するために、アーカイブまたはレポート目的で SMC ドキュメントを印刷することをお勧めします。SMC を使用すると、ドキュメントをプレビューしたり、印刷設定をカスタマイズしたり、印刷したり、PDF ファイルとして保存したりすることができます。

印刷プレビュー

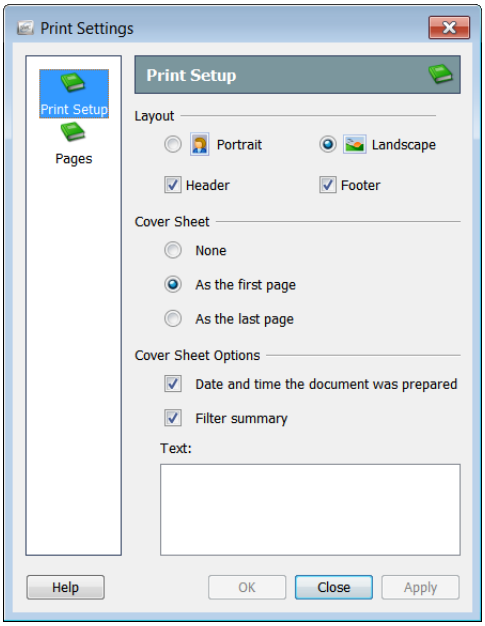
ドキュメントを印刷する前に、印刷状態をプレビューするには、メイン メニューから [ファイル(File)] > [印刷プレビュー(Print Preview)] を選択します。[印刷プレビュー(Print Preview)] ダイアログが開きます。



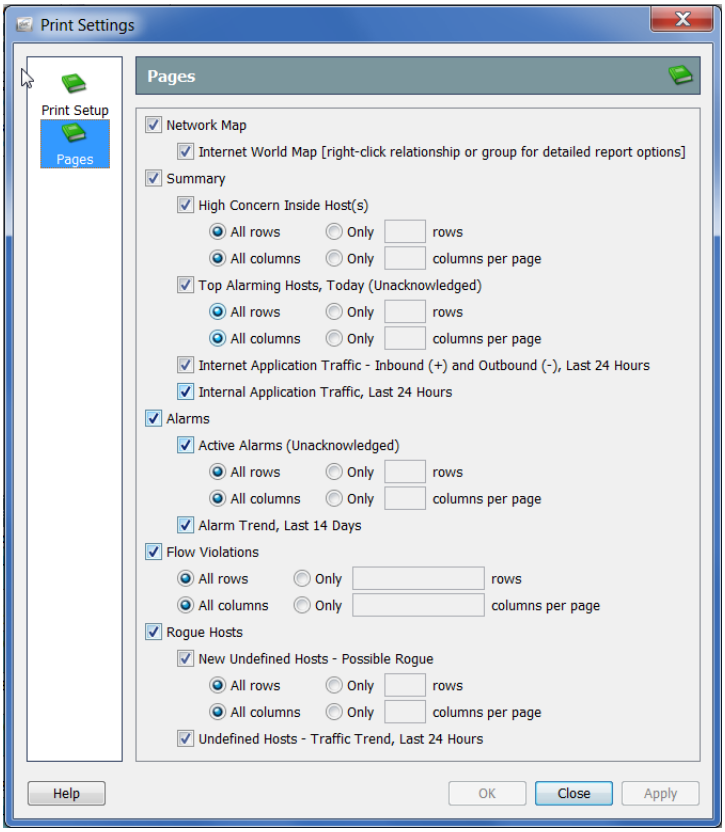
印刷設定

ドキュメントを印刷する前に印刷の外観をカスタマイズするには、[印刷設定(Print Settings)] 機能を使用します。メイン メニューから [ファイル(File)] > [印刷設定(Print Settings)] を選択して、[印刷設定(Print Settings)] ダイアログを開きます。

[印刷設定(Print Setup)] ページでは、ページのレイアウトを [ポートレート(Portrait)] または [ランドスケープ(Landscape)] に設定できます。必要に応じて、ヘッダー、フッターだけでなく、カバー シートを追加することもできます。

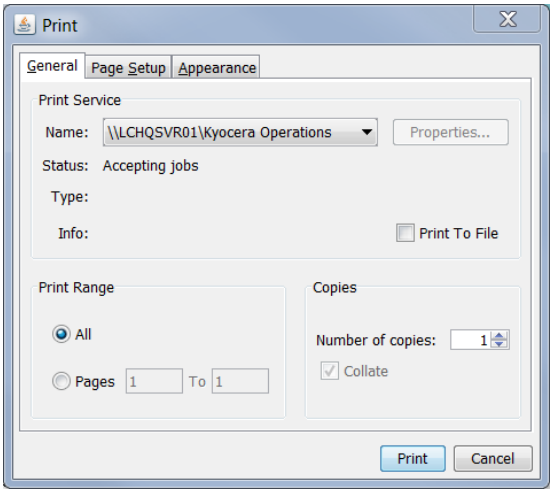


[ページ(Pages)] ページでは、印刷するドキュメントのページ、列、行を選択することができます。



印刷

ドキュメントを印刷するには、メイン メニューから [ファイル(File)] > [印刷(Print)] を選択します。[印刷(Print)] ダイアログが開きます。



(注):

より高品質のフォントを使用するには、[設定: PDF ビューア(Preferences: PDF Viewer)] ダイアログで外部 PDF ビューア(Adobe Acrobat Reader など)のパスを設定します。このダイアログにアクセスするには、メイン メニューで [編集(Edit)] > [設定(Preferences)] を選択します。

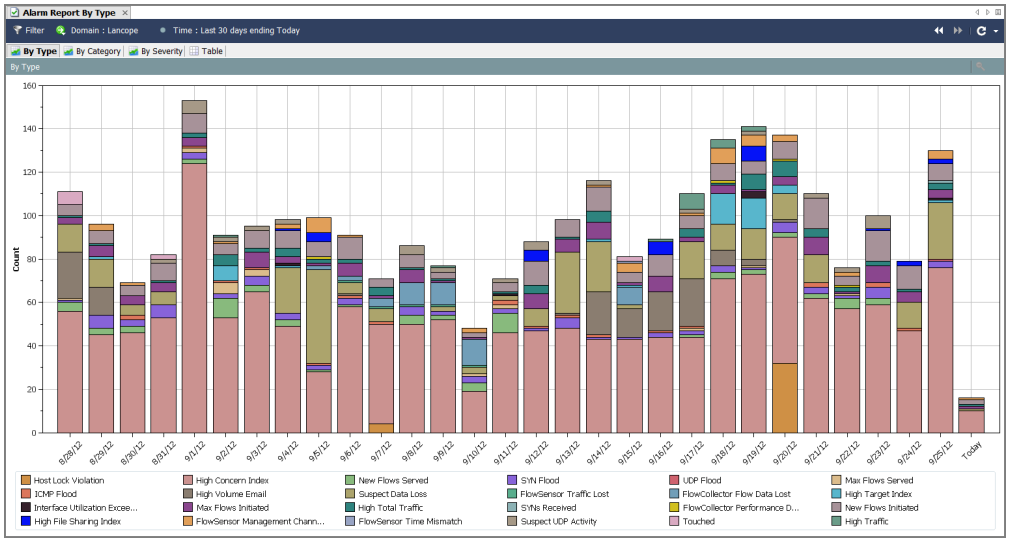
ドキュメントの保存

後から使用できるようにドキュメント レイアウトを保存

SMC ドキュメントのレイアウトを変更し、後で使用するレイアウトを保存したい場合は、ドキュメントを保存します。ドキュメントを保存すると、いつでも検索できるよう、SMC アプライアンスに保存されます。

ドキュメントを保存するには、次の手順に従います。

1. 保存するドキュメントを開きます。たとえば、[種類別アラームレポート(Alarm Report By Type)] ドキュメントを開きます。



2. レイアウトまたはフィルターの設定に必要な変更を加えます。
3. (オプション) SMC のメイン メニューから [ファイル(File)] > [印刷設定(Print Settings)] を選択し、表示されるダイアログ内で、印刷のたびにドキュメントの外観を設定します。[OK] をクリックして、変更を保存します。
4. (オプション) ドキュメントが PDF としてどのように表示されるかを確認するには、[ファイル(File)] > [印刷プレビュー(Print Preview)] を選択します。

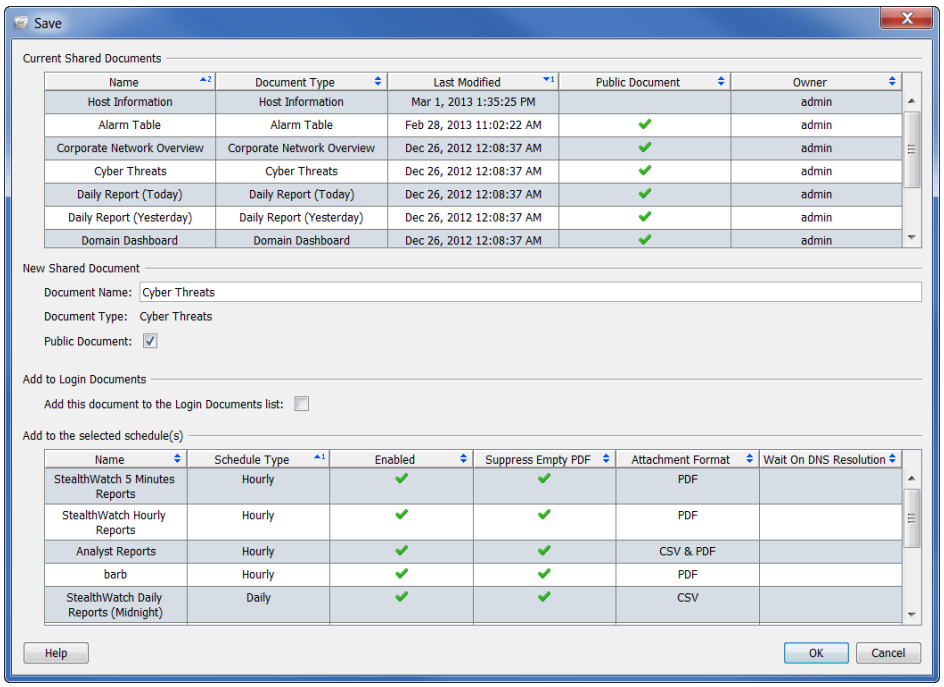
(注):

ドキュメントのレイアウト(列の位置や表示する列など)を変更し、変更を保持するには、[ファイル(File)] > [設定をデフォルトとして使用(Use Settings as Default)] を選択します。この変更は、次にドキュメントを開いたときに有効になります。

5. 次のいずれかを実行します。

   - 同じ名前を使用して以前のバージョンを置き換えるには、SMC のメイン メニューから [ファイル(File)] > [保存(Save)] を選択します。
   - 次のいずれかの状況が該当する場合は、SMC のメイン メニューから [ファイル(File)] > [名前をつけて保存(Save As)] を選択します。
     - 新しい名前でドキュメントのコピーを保存する場合。
     - 新しいドキュメントを作成し、初めてドキュメントを保存する場合。

       [保存(Save)] ダイアログが開きます。



6. [名前(Name)] フィールドに、簡単に識別できるドキュメントの名前を入力します(システムから名前が提案されます)。
7. (オプション)他のユーザーがこのドキュメントを各自のユーザー名で開くことができるようにするには、[パブリック(Public)] チェックボックスをオンにします。

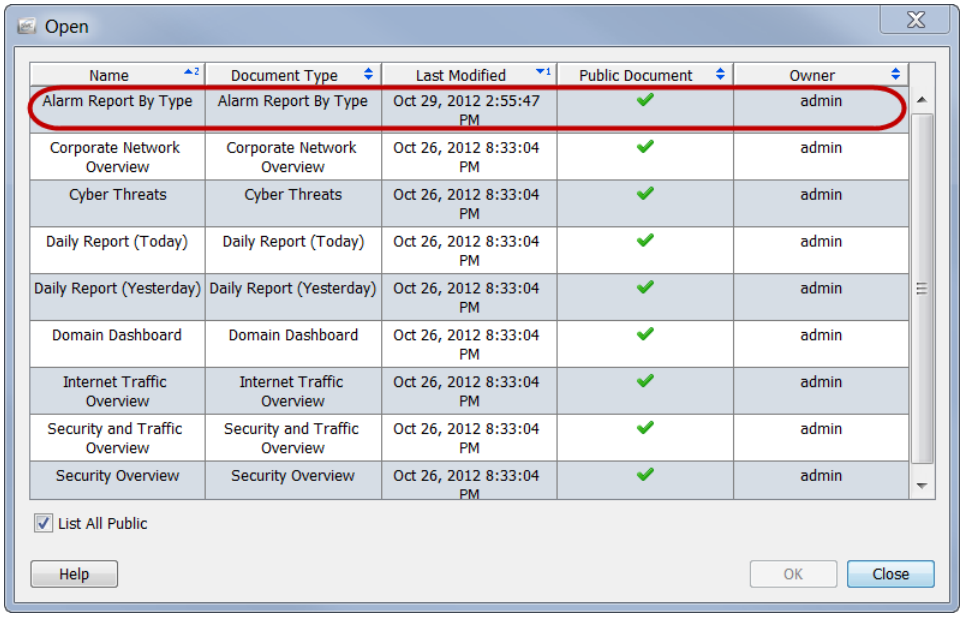
(注)

パブリック ドキュメントの詳細については、第 12 章「ドキュメントの操作」の「パブリック ドキュメント」(304 ページ)を参照してください。

8. (注):(オプション)自分のユーザー名で Stealthwatch デスクトップクライアントにログインするたびにドキュメントを自動的に開くには、[このドキュメントをログインドキュメントリストに追加する(Add this document to the Login Documents list)] チェックボックスをオンにします。

(注):
ログイン ドキュメントの詳細については、第 12 章「ドキュメントの操作」の「ログイン ドキュメント」(299 ページ)を参照してください。

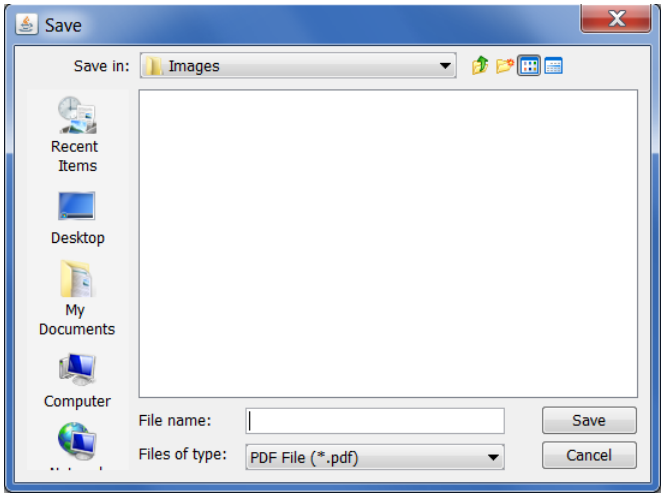
9. [OK] をクリックします。ドキュメントが SMC アプライアンスに保存されます。SMC のアクセスが可能なコンピュータ上で、指定したレイアウトやフィルタの設定を使用して、自分のユーザー名でこのドキュメントを開くことができます。
10. このドキュメントを開くには、SMC のメイン メニューから [ファイル(File)] > [開く(Open)] を選択します。[開く(Open)] ダイアログボックスが開きます。



11. ドキュメントを選択し、[OK] をクリックします。

(注):
デフォルトでは、現在のユーザー名で保存されたドキュメントのみが表示されます。他のユーザーが作成したドキュメントを含めて、すべてのドキュメントを一覧表示するには、[すべてのパブリックを一覧表示する(List All Public)] チェックボックスをオンにします。

ドキュメントを PDF ファイルとして保存

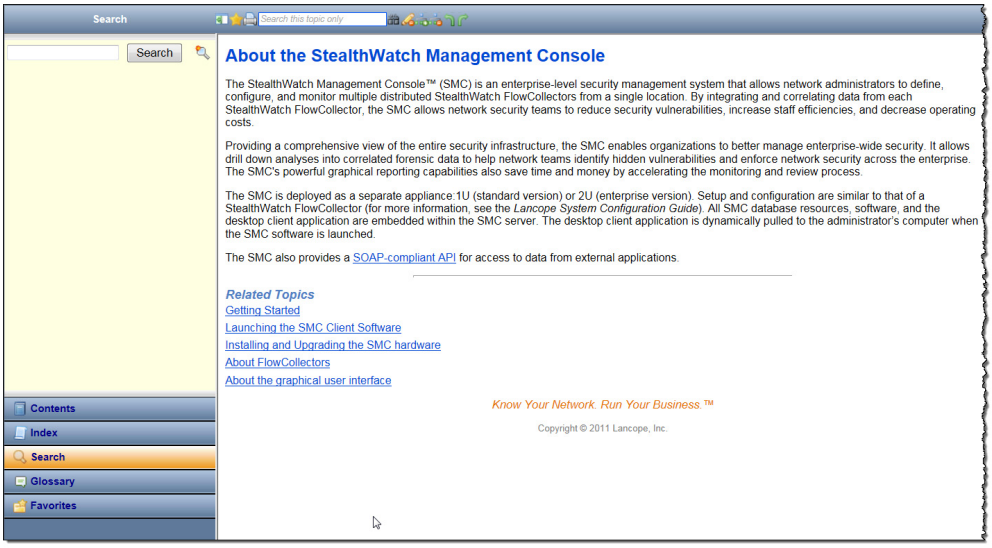


アクティブな SMC ドキュメントを PDF ファイルとして保存するには、メインメニューから [ファイル(File)] > [ファイルに出力(Print to File)] を選択します。[保存(Save)] ダイアログが開きます。

[保存(Save)] ダイアログボックスが表示されたら、ドキュメントを保存するディレクトリとファイル名に移動し、[保存(Save)] をクリックします。PDF ファイルを読み取ることができるツールでドキュメントを開くことができます。

オンライン ヘルプ

SMC ドキュメントの詳細情報が必要な場合は、キーボードの **F1** キーまたは **Ctrl+H** を押して、Stealthwatch デスクトップクライアントのオンラインヘルプを表示します。また、メイン メニューから [ヘルプ(Help)] > [ヘルプ(Help)] を選択することもできます。



ドキュメントがアクティブな状態のときにオンライン ヘルプにアクセスすると、そのドキュメントに関連するヘルプ トピックが表示されます。開いているドキュメントがない場合は、入門向けヘルプ トピック「Stealthwatch Management Console について」を参照してください。

(注):

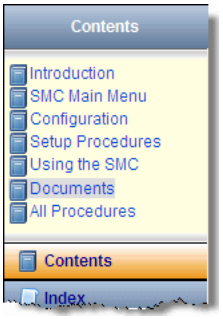
Stealthwatch デスクトップクライアントにログインしたときと同じクレデンシャルを使用してログインしなければならない場合があります。アクティブなドキュメントの情報が表示されない場合は、Stealthwatch デスクトップクライアントに戻り、F1 キーをもう一度押します。

Stealthwatch デスクトップクライアントのオンラインヘルプにアクセスした後、左側のナビゲーションウィンドウの下部にある以下のボタンを使用して、いくつかの方法で情報を検索できます。

- [目次(Contents)]
- [インデックス(Index)]
- [検索(Search)]
- [用語集(Glossary)]
- [お気に入り(Favorites)]

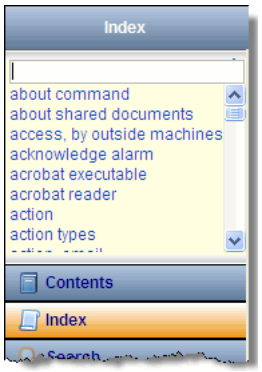
また、項目領域の上部にある [高速検索(Quick Search)] 機能を使用して、開いているトピックを検索することもできます。

[目次(Contents)]



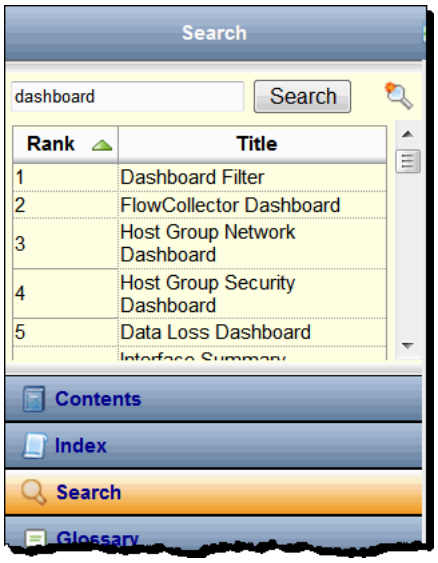
[目次(Contents)] ペインには、書籍の目次のようにまとめられたオンライン ヘルプの目次が用意されています。表示するには、左側のナビゲーション ウィンドウの下部にある [目次(Contents)] をクリックします。リスト内の項目をクリックすると、対応するヘルプ トピックが表示されます。

[インデックス(Index)]



[インデックス(Index)] ペインには、関連項目を検索できる単語のリストが表示されます。表示するには、左側のナビゲーション ウィンドウの下部にある [インデックス(Index)] をクリックします。リスト内の項目をクリックすると、そのヘルプ トピックが表示されます。リストをスクロールして選択するか、または上部のフィールドにテキストを入力して、リスト内のそのテキストにすばやく移動することができます。その後、目的のトピックを選択して表示します。

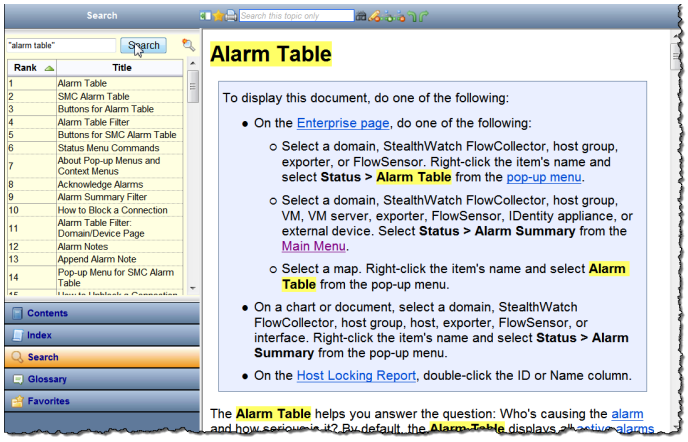
[検索(Search)]



オンライン ヘルプにアクセスしたときにドキュメントが開いていない場合は、[検索(Search)] ペインがデフォルトで開きます。上部のフィールドに、検索するテキストを入力し、左側のナビゲーション ウィンドウの下部にある [検索(Search)] をクリックするか、キーボードの **Enter** キーを押します。項目のリストが表示され、入力したテキストとの関連性に従ってランク付けされます。項目をクリックすると、そのトピックが表示されます。

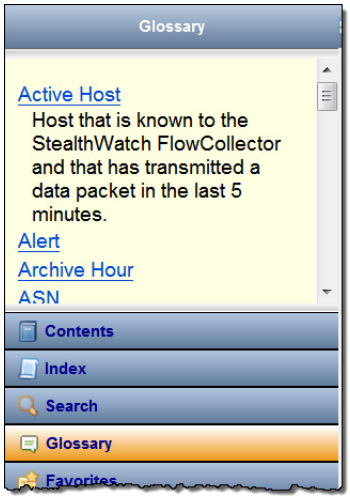
この機能は、一般的な情報を検索できるだけでなく、特定の SMC ドキュメントを開く方法を確認する必要がある場合にも便利です。特定のドキュメントに関連するすべてのヘルプ トピックの最初の段落に、そのドキュメントにアクセスする方法の説明があります。

たとえば、[アラームテーブル（Alarm Table）]を開く必要があるが、その方法がわからない、または覚えていないとします。[検索（Search）]フィールドに「alarm table」と入力し、**Enter** キーを押します。検索結果に [アラームテーブル（Alarm Table）] のヘルプ トピックが表示されたら、その項目名をクリックします。表示されるヘルプ トピックに、[アラームテーブル（Alarm Table）] へのアクセス方法が記載されています。



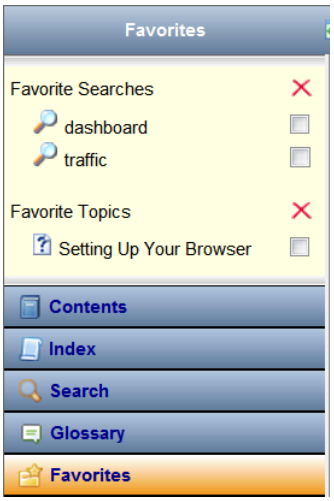
オンライン ヘルプで頻繁に検索する項目がある場合は、検索テキストを [お気に入りリスト（Favorites list）] に追加できます。[検索（Search）] フィールドにテキストを入力し、[お気に入りを検索（Search Favorite）] ボタン をクリックします。次にそのテキストを検索する必要があるときには、[お気に入りリスト（Favorites list）] に移動してそれをクリックするだけです。

[用語集（Glossary）]



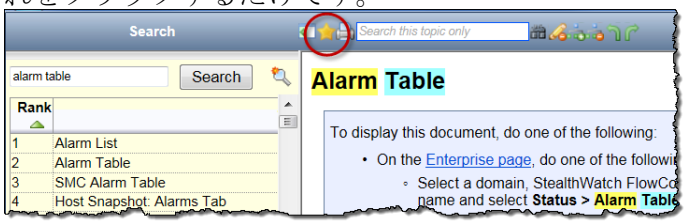
[用語集（Glossary）] ペインには、Stealthwatch でよく使用される単語の定義が表示されます。表示するには、左側のナビゲーション ウィンドウの下部にある [用語集（Glossary）] をクリックします。リスト内の単語をクリックすると、その定義が表示されます。

[お気に入り(Favorites)]



[お気に入り(Favorites)] ペインには、お気に入りとしてマークした検索項目またはトピックが表示されます。表示するには、左側のナビゲーション ウィンドウの下部にある [お気に入り(Favorites)] をクリックします。

お気に入りリストに検索テキストを追加する方法についてはすでに説明しました。リストにはトピックを追加することもできます。この機能は、特定のトピックを頻繁に参照する必要がある場合に役立ちます。お気に入りリストに追加するトピックの上にある [ヘルプ(Help)] ツールバーの [トピックのお気に入り(Topic Favorite)] ボタン をクリックします。次にそのトピックを確認する必要があるときは、お気に入りリストに移動してそれをクリックするだけです。



[お気に入りの検索(Favorite Searches)] 項目をクリックすると、[検索(Search)] ペインが開き、その項目に関連するトピックが一覧表示されます。リスト内の項目をクリックすると、そのヘルプ トピックが表示されます。

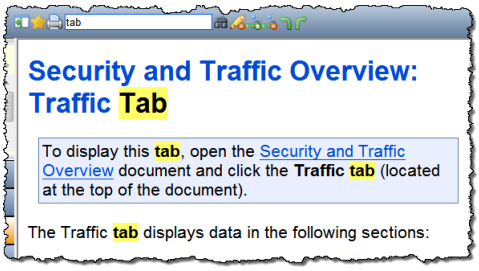
[お気に入りのトピック(Favorite Topics)] 項目をクリックすると、そのヘルプ トピックが開きます。

お気に入りリストから項目を削除するには、対応するチェックボックス をクリックしてチェックマークを付け 、ボタンをクリックします。

[高速検索(Quick Search)]

[高速検索(Quick Search)] フィールドは、[ヘルプ(Help)] ツールバーのヘルプ トピックの上にあります。

このフィールドでは、表示しているヘルプ トピック内のテキストを検索できます。[高速検索(Quick Search)] フィールドにテキストを入力して、[検索(Search)] ボタン をクリックするか、キーボードの **Enter** キーを押します。入力したテキストがトピックに含まれている場合は、次の例のように黄色で強調表示されます。強調表示を解除するには、[ハイライター(Highlighter)] ボタン をクリックします。



（注）:

[ヘルプ（Help）] ツールバーのボタンの詳細については、ボタンをマウスオーバーして、ツール ヒントを表示してください。

キーボードのショートカット

次の表は、Stealthwatch デスクトップクライアントでさまざまな機能を実行するために使用できる、豊富に用意されたキーボードショートカットのリストです。これらのショートカットの多くは、メイン メニューの項目に対応しています。

（注）：

このリストに記載されているすべてのドキュメントについてはまだ説明していませんが、SMC の理解が深まるにつれて、参照情報として役立ちます。

キー	目的
←	チャートの場合：ズームインした領域で後方（左）に移動します。
→	チャートの場合：ズームインした領域で前方（右）に移動します。
↑	チャートの場合：ズームインした領域を上方に移動します。 ツリーの [検索（Find）] フィールドを使用する場合：[検索（Find）] フィールド内のテキストと同じテキストを使用して、ツリー内の前の項目を検索します。
↓	チャートの場合：ズームインした領域を下方に移動します。 ツリーの [検索（Find）] フィールドを使用する場合：[検索（Find）] フィールド内のテキストと同じテキストを使用して、ツリー内の次の項目を検索します。
Alt + ←	複数のドキュメントが開いている場合は、アクティブなドキュメントの左側にあるドキュメントが表示されます。 [フローのクイックビュー（Quick View for Flow）] ダイアログの場合：タブ間を左に移動します。
Alt + →	複数のドキュメントが開いている場合は、アクティブなドキュメントの右側にあるドキュメントが表示されます。 [フローのクイックビュー（Quick View for Flow）] ダイアログの場合：タブ間を右に移動します。
Alt + ↑	[クイックビュー（Quick View）] ダイアログの場合：対応するドキュメント テーブルの行を上に移動します。
- 続く -	

キー	目的
Alt + ↓	[クイックビュー(Quick View)] ダイアログの場合:対応するドキュメント テーブルの行を下に移動します。
Alt + F	エンタープライズ ツリーの [検索(Find)] フィールドが非表示の場合:[検索(Find)] フィールドを表示します。 エンタープライズ ツリーの [検索(Find)] フィールドが表示されている場合:[検索(Find)] フィールドにカーソルが移動します。
Ctrl	テーブルでは、このキーを押しながら列ヘッダーをクリックすると、その列のソート順が解除されます。
Ctrl + ←	以前の時間内にアクティブだったドキュメントのデータを表示します。 このショートカットは、メイン メニューから [表示(View)] > [時間の後方(Time Backward)] を選択するのと同じです。メイン ツールバーの [時間の後方(Time Backward)] ボタン  をクリックすることもできます。
Ctrl + →	以降の時間内にアクティブだったドキュメントのデータを表示します。 このショートカットは、メイン メニューから [表示(View)] > [時間の前方(Time Forward)] を選択するのと同じです。メイン ツールバーの [時間の前方(Time Forward)] ボタン  をクリックすることもできます。
Ctrl + B	独自のカスタム ドキュメントおよびレイアウトを作成できる、ドキュメント ビルダーを開きます。 このショートカットは、メイン メニューから [表示(View)] > [ドキュメントビルダー(Document Builder)] を選択するのと同じです。ドキュメント ビルダーでは、このショートカットは、[表示(View)] > [新規ドキュメントビルダー(New Document Builder)] を選択するのと同じです。
Ctrl + C	選択したテキストをコピーします。 このショートカットは、メイン メニューから [編集(Edit)] > [コピー(Copy)] を選択するのと同じです。
- 続く -	

キー	目的
Ctrl + D	特定の SMC ドキュメントを開くたびに同じレイアウト設定を使用します。 このショートカットは、メイン メニューから [ファイル(File)] > [設定をデフォルトとして使用(Use Settings as Default)] を選択するのと同じです。
Ctrl + E	ホスト グループ エディタを開きます。 このショートカットは、メイン メニューから [構成(Configuration)] > [ホストグループを編集(Edit Host Groups)] を選択するのと同じです。
Ctrl + F	エンタープライズ ツリーの [検索(Find)] フィールドが非表示の場合:[検索(Find)] フィールドを表示します。
Ctrl + G	グローバル検索フィールドにカーソルを置き、すべての SMC ドキュメントから IP アドレスやアラーム ID を検索します。 このショートカットは、メイン メニューから [編集(Edit)] > [グローバル検索(Global Search)] を選択するのと同じです。
Ctrl + H	アクティブなダイアログまたはドキュメントに関連するオンライン ヘルプを表示します。(最初にログインしなければならない可能性があります)。 このショートカットは、メイン メニューまたはドキュメント ビルダーのメイン メニューから [ヘルプ(Help)] > [ヘルプ(Help)] を選択するのと同じです。
Ctrl + I	選択したオブジェクトのプロパティを表示します。 このショートカットは、メイン メニューから [構成(Configuration)] > [プロパティ(Properties)] を選択するのと同じです。
Ctrl + N	Stealthwatch デスクトップクライアントの新しいインスタンスを開きます。 このショートカットは、メイン メニューから [表示(View)] > [新しいメイン ウィンドウ(New Main Window)] を選択するのと同じです。
Ctrl + O	DAR ファイルとして保存されたドキュメントを開きます。 このショートカットは、メイン メニューから [ファイル(File)] > [開く(Open)] を選択するのと同じです。
- 続く -	

キー	目的
Ctrl + P	アクティブなドキュメントを印刷します。 このショートカットは、メイン メニューから [ファイル(File)] > [印刷(Print)] を選択するのと同じです。
Ctrl + Q	Stealthwatch デスクトップクライアントを閉じます(つまり、終了します)。 このショートカットは、メイン メニューから [ファイル(File)] > [終了(Exit)] を選択するのと同じです。
Ctrl + S	アクティブなドキュメントを、レイアウトとフィルタ設定の特定のセットとともに、DAR ファイルとして保存します。 このショートカットは、メイン メニューから [ファイル(File)] > [名前をつけて保存(Save As)] を選択するのと同じです。
Ctrl + T	エンタープライズ ツリーの非表示と表示を切り替えます。 このショートカットは、メイン メニューから [表示(View)] > [ツリーを非表示/表示(Hide/Show Tree)] を選択するのと同じです。
Ctrl + V	コピーしたテキストを編集可能フィールドに挿入(貼り付け)します。 このショートカットは、メイン メニューから [編集(Edit)] > [貼り付け(Paste)] を選択するのと同じです。
Ctrl + W	アクティブ ドキュメントを閉じます。 このショートカットは、メイン メニューから [ファイル(File)] > [閉じる(Close)] を選択するのと同じです。
Ctrl + Shift + C	ツリーで選択したブランチを折りたたむか、ブランチが選択されていない場合はツリーのすべての項目を折りたたみます。 このショートカットは、メイン メニューまたはドキュメント ビルダーのメイン メニューから [表示(View)] > [すべて折りたたむ(Collapse All)] を選択するのと同じです。
- 続く -	

キー	目的
Ctrl + Shift + E	ツリーで選択したブランチを展開するか、ブランチが選択されていない場合はツリーのすべての項目を展開します。 このショートカットは、メイン メニューまたはドキュメント ビルダーのメイン メニューから [表示(View)] > [すべて展開(Expand All)] を選択するのと同じです。
Ctrl + Shift + S	アクティブなドキュメントを、レイアウトとフィルタ設定の特定のセットとともに、新しい名前で DAR ファイルとして保存します。 このショートカットは、メイン メニューから [ファイル(File)] > [名前をつけて保存(Save As)] を選択するのと同じです。
Ctrl + Shift + W	開いているドキュメントをすべて閉じます。 このショートカットは、メイン メニューから [ファイル(File)] > [すべて閉じる(Close All)] を選択するのと同じです。
Delete	選択されている項目を削除します。 このショートカットは、メイン メニューから [構成(Configuration)] > [削除(Delete)] を選択するのと同じです。
Esc	ダイアログ ウィンドウを閉じます。
F	チャートの場合:元のズーム レベルに戻します。
F1	アクティブなダイアログまたはドキュメントに関連するオンライン ヘルプが表示されます。(最初にログインしなければならない可能性があります)。
F3	ドキュメント ビルダーでは、検索フィールド内のテキストと同じテキストを持つ次の項目を検索ツリー内で検索します。 このショートカットは、ドキュメント ビルダーのメイン メニューから [編集(Edit)] > [ツリー内で次を検索(Find Next in Tree)] を選択するのと同じです。
- 続く -	

キー	目的
F5	アクティブなドキュメントのデータを更新します。 このショートカットは、メイン メニューから [表示(View)] > [更新(Refresh)] を選択するのと同じです。メイン ツールバーの [更新(Refresh)] ボタン をクリックすることもできます。
Alt + ←	開いているドキュメントに複数のタブが含まれている場合は、アクティブなタブの左側のタブを表示します。
Alt + →	開いているドキュメントに複数のタブが含まれている場合は、アクティブなタブの右側のタブを表示します。
Shift + F3	ドキュメント ビルダーでは、検索フィールド内のテキストと同じテキストを持つ前の項目を検索ツリー内で検索します。 このショートカットは、ドキュメント ビルダーのメイン メニューから [編集(Edit)] > [ツリー内で前を検索(Find Previous in Tree)] を選択するのと同じです。
Spacebar	一部のテーブルの場合:行内をクリックしてスペースバーを押すと、選択した項目の [クイックビュー(Quick View)] ダイアログが表示されます。[クイックビュー(Quick View)] ダイアログが開いている場合は、スペースバーを押して閉じます。
Z	チャートの場合:X 軸上でズーム インします。

3

ホスト管理

概要

ネットワーク内のすべてのホストを個別に管理することは、非常に大きな負担となります。ただし、StealthWatch は、ホストをホスト グループに編成できるようにすることで、その労力を大幅に軽減します。

ホスト グループを使用すると、ホストを柔軟に編成することができます。一般的に、ホストは複数のグループに属することができます。さらに、ホスト グループごとや、ホストごとに、ポリシーを定義することもできます。

この章では、ホストのグループを論理的に編成して、ネットワークのさまざまな領域をモニターし、ホストの動作をより効率的に管理する方法を学習します。

この章は、次の項で構成されています。

- ホスト グループ
- リレーショナル フロー マップ

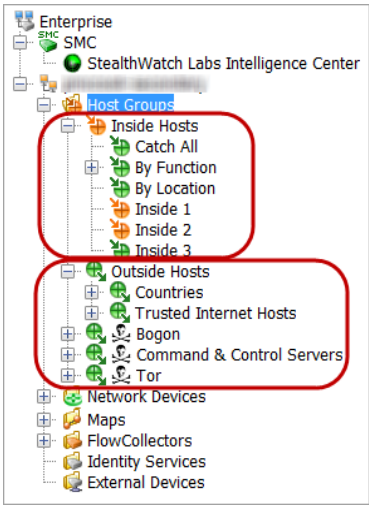
ホスト グループ

ホスト グループは基本的に、場所、機能、トポロジなどの類似の属性を持つ複数のホスト IP アドレスまたは IP アドレス範囲の仮想コンテナです。ホストをグループ化してホスト グループを作成することにより、Stealthwatch Flow Collector が個別にモニターするのではなく、ホストの動作をグループ単位でモニターし、それに応答する方法を制御することができます。

管理者は、組織にとって意味のある方法でホストを編成できます。この自由さから、レポート作成とトラフィック管理には無限の柔軟性がもたらされます。さらに、ポリシー管理ははるかに容易になり、管理者はホストがネットワーク内で果たす役割に基づいてホストのポリシーを設定できます。

Stealthwatch デスクトップクライアントでは、次の例のように、ホストグループ構造とネットワーク構造が企業ツリーに表示されます。各ドメインにはデフォルトで、下位ホスト グループを追加できる最上位ホスト グループが含まれます。

- **[内部ホスト(Inside Hosts)]**:ホストがネットワークの一部として定義されているすべてのホスト グループが含まれます。
- **[外部ホスト(Outside Hosts)]**:ホストがネットワークの一部として特に定義されていないすべてのホスト グループが含まれます。



(注):
エンタープライズ ツリーにすべてのホスト グループが表示されるかどうかは、ログイン権限によって決まります。

ログイン権限に応じて、必要な数の最上位ホスト グループを追加することができ、それらのグループに必要な数のサブホスト グループを含めることができ、さらにそれらのグループにサブホスト グループを含めることができます。特定のホスト グループに対して定義されていない IP アドレスは、自動的に [外部ホスト(Outside Hosts)] ホスト グループの [国(Countries)] サブホスト グループに分類されます。ホスト グループ名は重複してもかまいませんが、同じホスト グループ レベル(つまり、同じ親ホスト グループ下)での重複は許可されません。

(注):
企業ツリーの [ホスト グループ(Host Groups)] ブランチ下の任意のレベルにホスト グループを作成できますが、[内部ホスト(Inside Hosts)] または [外部ホスト(Outside Hosts)] ブランチの下に追加することをお勧めします。

Stealthwatch はデフォルトでは、ネットワーク外のホストに対してはポリシーを作成しません。ただし、ネットワーク上でトラフィックを発生させる外部ホストを定期的に追跡する必要がある場合は、[外部ホスト（Outside Hosts）] ホスト グループにそれらのホストを配置して、そのグループのポリシーを確立することができます。さらに、[内部ホスト（Inside Hosts）] と同じように設定を調整できます。

（注）：

特殊なレポート作成のために必要な場合は、最上位のホスト グループ（つまり、[内部ホスト（Inside Hosts）] または [外部ホスト（Outside Hosts）] と同じレベルのグループ）を作成することもできます。

以下に、特定の外部ホストの動作を追跡する必要があると想定される状況を示します。

- 外部 DNS サーバを使用している場合。
- サードパーティのコンサルタントまたはベンダーが定期的にネットワークにアクセスする場合。
- パートナー企業がネットワークに定期的にアクセスする場合。

[キャッチオール（Catch All）] ホスト グループ

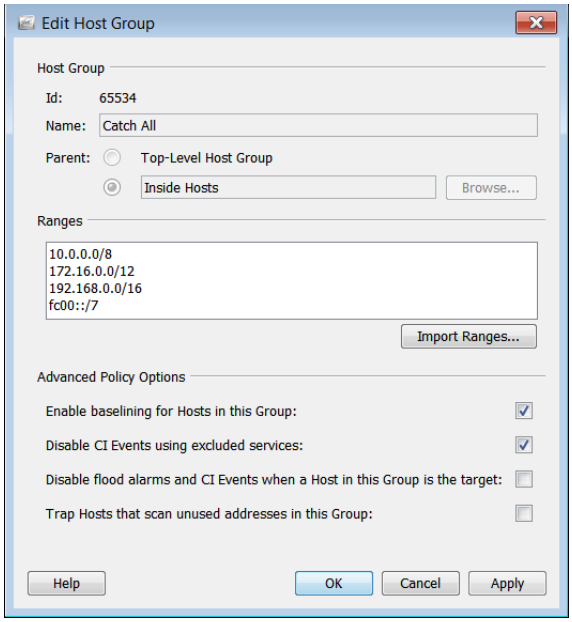
[内部ホスト（Inside Hosts）] ホスト グループには、デフォルトの [キャッチオール（Catch All）] サブホスト グループが含まれます。管理者は、[キャッチオール（Catch All）] ホスト グループを使用して、ホスト グループの構造を絞り込むことができます。

最初に、ネットワークに対応する大規模な IP 範囲をすべて、[キャッチオール（Catch All）] ホスト グループに配置することをお勧めします。次に、絞り込んで定義された IP 範囲または特定の IP アドレスを持つ他のホスト グループを作成すると、それらの範囲やアドレスが、キャッチ オール（Catch All）ホスト グループから自動的に移動します。

Stealthwatch v6 の新しい SMC インストールでは、次の IP 範囲（RFC 1918 と RFC 4193）がデフォルトで、[すべてを捕捉（Catch All）] ホストグループに設定されます。

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- fc00::/7

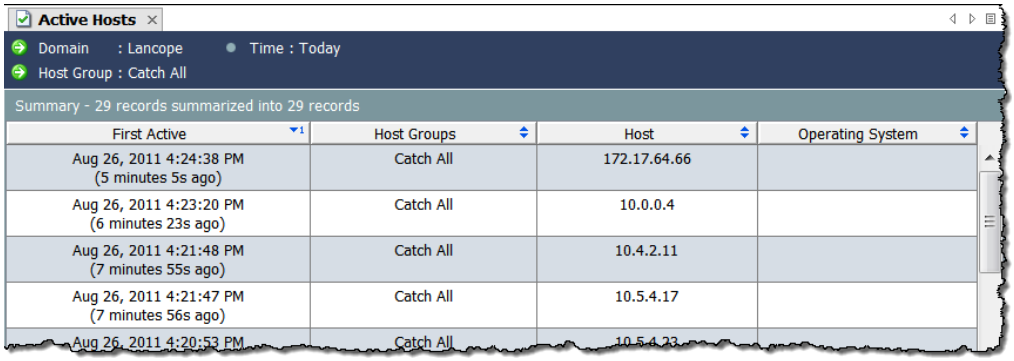
パブリック IP アドレスを登録している場合は、[キャッチオール（Catch All）] ホスト グループにこれらの範囲を手動で配置することをお勧めします。ログイン権限に応じて、[キャッチオール（Catch All）] ホスト グループ内に定義されている IP 範囲/アドレスを確認するには、エンタープライズ ツリーで [キャッチオール（Catch All）] ホスト グループを右クリックし、[構成（Configuration）] > [ホストグループのプロパティ（Host Group Properties）] を選択します。



（注）：

- 任意のホスト グループを編集するには、企業ツリーでホスト グループを右クリックし、[設定（Configuration）] > [ホストグループのプロパティ（Host Group Properties）] を選択します。
- ホスト名には、英数字および以下の特殊文字を使用できます：< , > . ? " ' : ; | { [}] + = _ - ( ) * & ^ % $ # @ ! ~ ‘スペース

ホスト グループ構造の定義が完了した時点で、[キャッチオール（Catch All）] ホスト グループにアクティブな IP アドレスが存在しているのが理想的です。不正なホスト IP アドレスを特定するには、[キャッチオール（Catch All）] ホスト グループの [アクティブホスト（Active Hosts）] ドキュメントを参照してください。単にエンタープライズ ツリーで [キャッチオール（Catch All）] ホスト グループを右クリックし、[ホスト（Hosts）] > [アクティブホスト（Active Hosts）] を選択します。

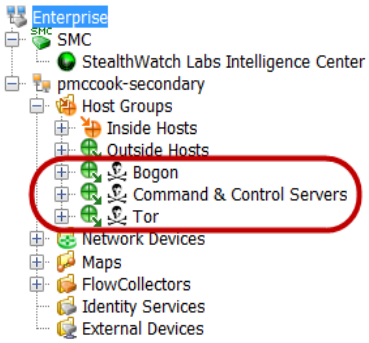


ネットワークは 1 つ 1 つ異なりますが、[キャッチオール(Catch All)] ホスト グループにホストを割り当てる際に考慮すべき共通の事項は次のとおりです。

- ネットワーク内のどの領域が他の領域より重要であるか。
- ネットワークのどの領域が頻繁に変化するか、どの領域の安定性が高いか。
- 重要な資産はどこにありまるか。
- どのホストが同様の機能を果たすか。
- ホストで実行される機能は何か。
- 動作に一貫性がなく日常的に「予測不能」な動作をするホストがあるか。

脅威インテリジェンスフィードのホストグループ

脅威インテリジェンスフィードには、悪意のあるアクティビティに使用されることが知られている IP アドレス、ポート番号、プロトコル、ホスト名、および URL が含まれます。次のホストグループが脅威インテリジェンスフィードに含まれます。



- [Bogon]:bogon は公共のインターネットに公式に割り当てられていない IP アドレスです。
- [コマンドアンドコントロール サーバー(Command & Control Servers)]: C&C は、ボットネットに対して命令を出し、乗っ取られたコンピュータからレポートを受け取る集中型コンピュータです。
- [Tor]:Tor は、インターネットの匿名化サービスです。

(注):

ホストに接続している可能性のある脅威インテリジェンスフィード内の URL を検出するには、IPFIX を(NetFlow に)エクスポートするように設定された FlowSensor またはルータをインストールしておく必要があります(デフォルトでは、FlowSensor が IPFIX をエクスポートするよう設定されています)。

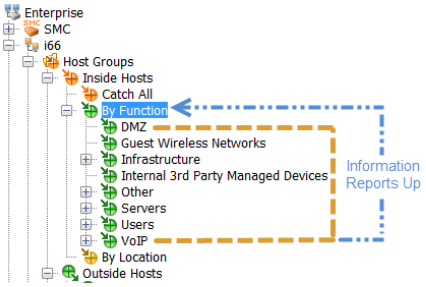
前述のホスト グループのいずれかにある、悪意のあるホストと通信したホストを調査したいが、関連するホスト グループに悪意のあるそのホストが表示されなくなった場合は、アラーム テーブルにアクセスして、次のコンポーネントをフィルタ処理します。

- [種類(Types)]:フィルターを適用したい悪意のあるホストの種類に応じて、該当する bogon、コマンド アンド コントロール、または ToR アラームを選択します。
- [日付/時刻(Date/Time)]:調べたい期間に従ってフィルターを適用します。

(注):
[SLIC 脅威フィード(SLIC Threat Feed)] ホスト グループ ブランチは名前変更、変更、移動、または削除できません。

情報レポートの上位化

ホスト グループの SMC ドキュメントには、そのサブホスト グループ内のすべてのホストに関する情報が含まれています。たとえば、[機能別(By Function)] ホスト グループのホスト情報(Host Information)ドキュメントを(フィルタ設定を変更せずに)開くと、その下にあるすべてのサブホスト グループ内のすべてのホストに関する情報と、[機能別(By Function)] ホスト グループの直下に定義されているすべてのホストに関する情報が表示されます。



ホスト グループ作成のストラテジ

この時点でほとんどの場合、ホスト グループは定義済みだと考えられます。ただし、ホスト グループの仕組みを理解するために、ホスト グループ作成の推奨ストラテジを確認していきましょう。

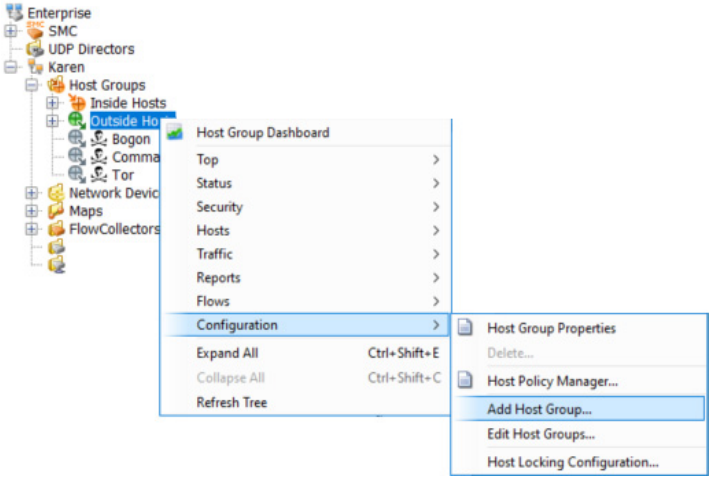
すべての Stealthwatch Flow Collector に、デフォルトのホスト グループ構造が付属しています。ログイン権限に応じて、ネットワークのニーズに適合するようにデフォルト ホスト グループを変更することができます。追加のホスト グループを作成できるだけでなく、[内部ホスト(Inside Hosts)]、[キャッチオール(Catch All)]、[外部ホスト(Outside Hosts)]、[国(Countries)]、[コマンドおよび制御サーバー(Command & Control Servers)] 以外のデフォルト ホスト グループは削除することができます。

ホストを [キャッチオール(Catch All)] ホスト グループに配置するための推奨事項については、先ほど説明しました。さらに、同じように動作するホストをホスト グループにまとめて配置することをお勧めします。ただし、ネットワーク、地理的地域、IP セグメント、または組織にとって意味のあるその他のカテゴリ内に、部門ごとに異なるホスト グループを作成することができます。

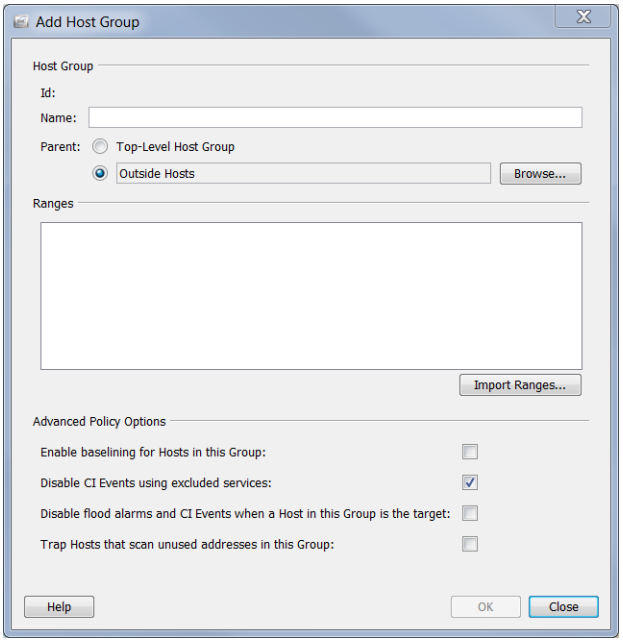
ホスト グループの作成

ホスト グループを作成するには、次の手順を実行します。

1. [エンタープライズ(Enterprise)] ページのツリー メニューで、[内部ホスト(Inside Hosts)] または [外部ホスト(Outside Hosts)] 内でいずれかのフォルダ(別のホスト グループを追加するフォルダ)をクリックします。
2. [内部ホスト(Inside Hosts)] または [外部ホスト(Outside Hosts)] ホスト グループ(いずれか該当する方)を右クリックして、[構成(Configuration)] > [ホストグループの追加(Add Host Group)] を選択します。



[ホストグループの追加(Add Host Group)] ダイアログが開きます。



3. [名前(Name)] フィールドに、追加するホスト グループの名前(例: *Partners*)を入力します。
4. [親(Parent)] フィールドで、新しいホスト グループの親をクリックします(デフォルトが正しくない場合)。
5. [範囲(Ranges)] フィールドに、必要な IP アドレスの範囲を入力します。このホスト グループの IP アドレスが含まれている既存のファイルがある場合は、[範囲をインポート(Import Ranges)] をクリックします。
6. [詳細ポリシーオプション(Advanced Policy Options)] セクションで、新しいホスト グループに適用するオプションをクリックします。
7. [OK] をクリックして [ホストグループの追加(Add Host Group)] ダイアログを閉じます。[エンタープライズ(Enterprise)] ページ ツリー メニューが自動的に更新され、新しいホスト グループが含まれます。

IP アドレス

IPv4 または IPv6 の IP アドレスを、各ホスト グループに含めることができます。IPv4 の IP アドレスを入力する場合は、次の表に記載されている表記法に従う必要があります。

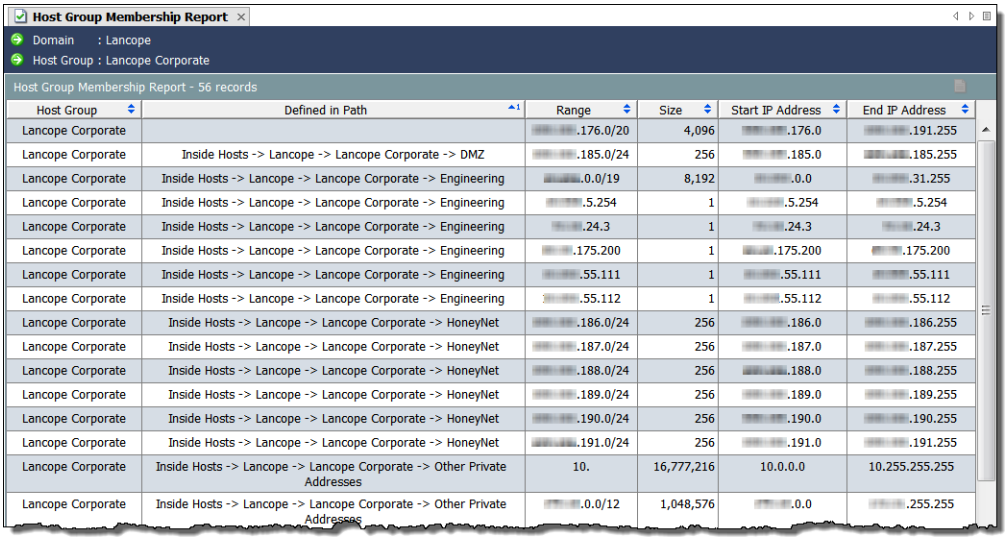
表記法	例
単一 IP アドレス	**10.52.1.55** 10.52.1.55 のホストのみを含む
末尾のドット サブネット	**10.52.** 10.52.0.0 ～ 10.52.255.255 の IP アドレスを含む **注:** 末尾にピリオド(.)を付ける必要があります。
クラスレス ドメイン間ルーティング(CIDR)表記法(つまり、マスクされたビットを「/」で表す)	**10.52.1.0/24** 10.52.1.0 ～ 10.52.1.255 の IP アドレスを含む **注:** 「マスク」を使用して IP アドレスを入力する場合は、この表記法を使用します。CIDR 表記の使用方法の詳細については、Stealthwatch デスクトップクライアントのオンラインヘルプを参照してください。**CIDR** への参照を検索するには、[検索(Search)] 機能を使用します。
ネットワークの範囲	**10-11.** 10.0.0.0 ～ 11.255.255.255 の IP アドレスを含む **10.52-53.** 10.52.0.0 ～ 10.52.255.255 および 10.53.0.0 ～ 10.53.255.255 の IP アドレスを含む **10.52-55.3.** 10.52.3.0 ～ 10.52.3.255、10.53.3.0 ～ 10.53.3.255、10.54.3.0 ～ 10.54.3.255、10.55.3.0 ～ 10.55.3.255 の IP アドレスを含む **注:** 末尾にピリオド(.)を付ける必要があります。
ホストの範囲	**10.52.1.0-10** 10.52.1.0 ～ 10.52.1.10 の IP アドレスを含む **10.52.0.0-10.52.255.255** 10.52.0.0 ～ 10.52.255.255 の IP アドレスを含む **注:** IPv4 アドレスの 2 つまでのオクテットを範囲(たとえば、10.52.100-255.15-255)に置き換えることができます。
複数の範囲	**10.52.100-255.15-255** **10.52.100-255.15-255.3** **1-2.3-4.5-6.7-8**
カンマ区切りリスト	**10.52.1.10,10.52.1.50,10.100.1.20** これらの 3 つのホストのみを含む

IPv6 の IP アドレスを入力する場合は、次の表に記載されている表記法に従う必要があります。

表記法	例
単一 IP アドレス	**2001:0DB8:0000:0056:0000:ABCD:EF12:3456** **2001:DB8:0:56:0:ABCD:EF12:3456** **2001:DB8::56:0:ABCD:EF12:3456** **2001:DB80:0:56::ABCD:EF12:3456** **2001:DB80:0:56::ABCD:239.18.52.86**
グローバル ルーティング プレフィックス サブネット	**2001:DB8:0:56::/64**
ネットワークの範囲	**2001:DB8:0:56-58::/64**
ホストの範囲	**2001:DB8:0:56:ABCD:EF12:3456:1-10** **2001:DB8:0:56:ABCD:EF12:3456:1-** **2001:DB8:0:56:ABCD:EF12:3456:10**
複数の範囲	**2001:DB8:0:56-58:ABCD:EF12:3456:1-10** **2001:DB8:0:56-58:ABCD-ABCF:EF12:3456:1-10**

ホスト グループ メンバーシップ

ホスト グループ構造を表示するには、ホスト グループ メンバーシップ レポートを開きます。一般的にこのレポートにアクセスするには、エンタープライズ ツリーの任意の要素を右クリックし、[レポート（Reports）] > [ホストグループ メンバーシップレポート（Host Group Membership Report）] を選択します。

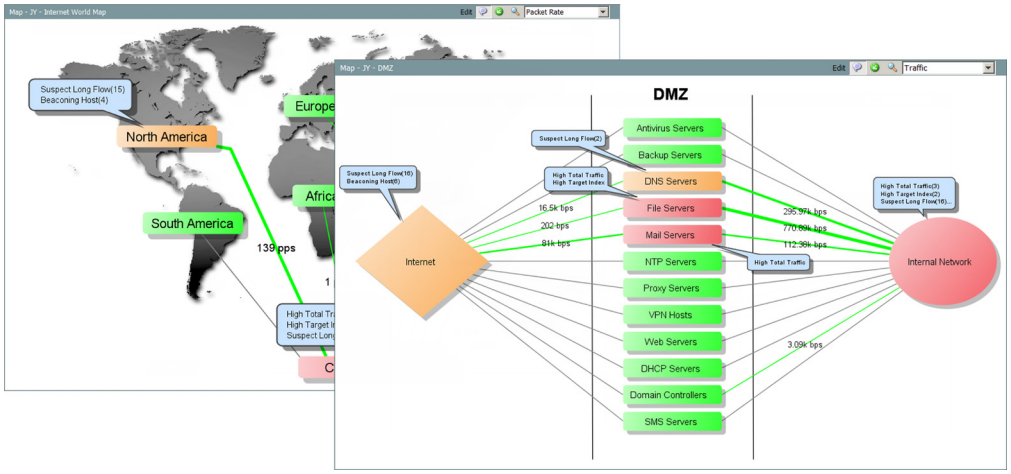


Host Group	Defined in Path	Range	Size	Start IP Address	End IP Address
Lancope Corporate		.176.0/20	4,096	.176.0	.191.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> DMZ	.185.0/24	256	.185.0	.185.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.0.0/19	8,192	.0.0	.31.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.5.254	1	.5.254	.5.254
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.24.3	1	.24.3	.24.3
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.175.200	1	.175.200	.175.200
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.55.111	1	.55.111	.55.111
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.55.112	1	.55.112	.55.112
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.186.0/24	256	.186.0	.186.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.187.0/24	256	.187.0	.187.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.188.0/24	256	.188.0	.188.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.189.0/24	256	.189.0	.189.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.190.0/24	256	.190.0	.190.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.191.0/24	256	.191.0	.191.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Other Private Addresses	10.	16,777,216	10.0.0.0	10.255.255.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Other Private Addresses	.0.0/12	1,048,576	.0.0	.255.255

リレーショナル フロー マップ

リレーショナル フロー マップを使用すると、ネットワーク上のホスト グループ間の現在のトラフィック状態をグラフィカルに表示できるため、どこに注目すべきかをすぐに確認できます。StealthWatch にはいくつかのデフォルト マップが付属しており、管理者は必要に応じてカスタマイズできます。

さらに管理者は、次の例に示すように、場所、機能、または仮想環境などの任意の基準に基づいて新しい関係マップを簡単に作成できます。



マップは重大な疑問を解消するのに役立ちます。2 つのホスト グループ間に関係が確立されるため、それらの間を移動するトラフィックを分析することができます。マップ上のホスト グループをダブルクリックすると、ドリル ダウンして何が起きているかを詳細に把握することができます。関係が確立されたら、関係（ホストグループ間の線）を右クリックし、[関係（Relationship）] > [ポリシー（Policy）] を選択すると、ホスト グループ間の基準および警告機能を有効にすることができます。

4

ビューおよびダッシュボード

概要

SMC のドキュメントには、デフォルトで、ネットワーク上で発生しているすべての単一アクティビティに関する情報が表示されます。しかし、特定のタイプのトラフィックまたはアラームに注意を払う必要がある場合はどうしたらよいでしょうか。また、このドキュメント全体ではなく、ドキュメントの特定の部分のみを表示したい場合はどうでしょうか。SMC では、独自のダッシュボードを構築して、表示したい主な情報のみを表示することができます。

この章は、次の項で構成されています。

SMC のデフォルトのダッシュ ボード

SMC コンソールにはデフォルトのダッシュボードが複数用意されているため、1 つのドキュメントに含まれるさまざまなタイプの情報を簡単に表示できます。これらのダッシュボードにアクセスするには、メインメニューで [ステータス(Status)] > [ダッシュボード(Dashboards)] > デフォルトのダッシュボード名を選択します。

次に、SMC コンソールのデフォルトのダッシュボード(アルファベット順)およびそれぞれの説明のリストを示します。

ダッシュボード名	説明
[アラームダッシュボード(Alarm Dashboard)]	このダッシュ ボードには、選択したドメインのアラーム データが表示されます。データは次のセクション内に表示されます。 ▶ [新しいアラーム(New Alarms)] ▶ [確認済みのアラーム(Acknowledged Alarms)]
[サイバー脅威ダッシュボード(Cyber Threats Dashboard)]	このダッシュ ボードには、ドメインに影響するサイバー脅威に関するデータがグラフおよびテーブルで表示されます。データは、次のタブに表示されます。 ▶ [レピュテーション(Reputation)] ▶ [調査(Reconnaissance)] ▶ [データ損失(Data Loss)] ▶ [マルウェア(Malware)] ▶ [ボットネット(Botnet)]
[データ損失ダッシュボード(Data Loss Dashboard)]	このダッシュ ボードには、選択したドメイン内のデータ転送アクティビティが表示されます。データは次のセクション内に表示されます。 ▶ [データ損失アラーム(今日)(Data Loss Alarms (Today))] ▶ [アクティブなデータ損失アラームのホスト情報(Host Information for Active Data Loss Alarms)] ▶ [データ損失アラームの傾向(Trend of Data Loss Alarms)] ▶ [上位 20 のアップロード(今日)(Top 20 Uploads (Today))]

ダッシュボード名	説明
[DDoS アラームダッシュボード（DDoS Alarm Dashboard）]	このダッシュボードに表示される情報は次のとおりです。 ▶ DDoS 脅威または DDoS 攻撃が行われようとしていることを示している可能性のあるアクティビティ ▶ ネットワークで発生したアラームに関する詳細情報
[DDoS トラフィックダッシュボード（DDoS Traffic Dashboard）]	このダッシュ ボードには、DDoS 攻撃を示している可能性のある、ネットワーク上のトラフィック パターン内のスパイクや変更に関する情報が表示されます。
[フローコレクタダッシュボード（Flow Collector Dashboard）]	このダッシュ ボードには、Stealthwatch フロー コレクタの最も重要なアクティビティがグラフで表示されます。データは次のセクション内に表示されます。 ▶ [状態（Status）] タブ • [フロー収集の統計情報（Flow Collection Statistics）] • [フロー収集のトレンド（Flow Collection Trend）] • [フロー収集のステータス（Flow Collection Status）] ▶ [アラーム（Alarms）] タブ • [フローコレクタアラームのトレンド、過去 30 日間（Flow Alarm Trend, Previous 30 Days）] • [フローコレクタアラーム、過去 30 日間（Flow Collector Alarms, Previous 30 Days）]
[ホストグループダッシュボード（Host Group Dashboard）]	[ホストグループダッシュボード（Host Group Dashboard）] の詳細については、「[ホストグループダッシュボード（Host Group Dashboard）]」（104 ページ）を参照してください。

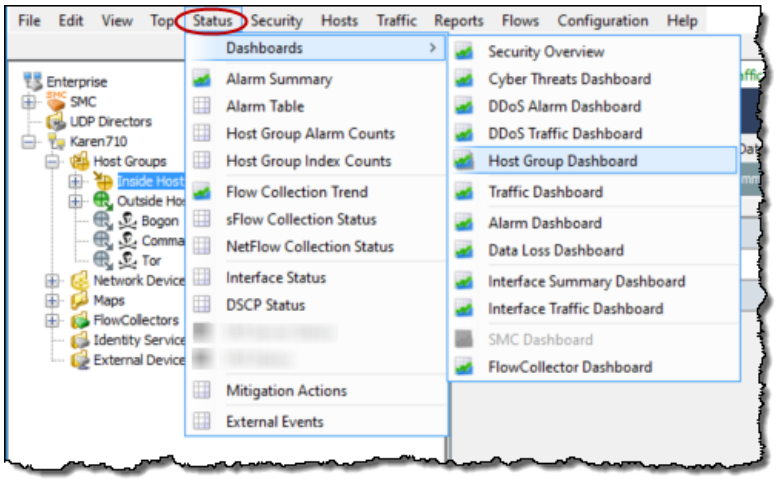
ダッシュボード名	説明
[インターフェイスサマリーダッシュボード（Interface Summary Dashboard）]	このダッシュ ボードには、選択したインターフェイスのトラフィック データがさまざまなグラフおよびテーブルで表示されます。データは次のセクション内に表示されます。 ▶ [トラフィックの統計情報、過去 6 時間（Traffic Statistics, Last 6 Hours）] ▶ [インバウンドおよびアウトバウンドの使用率、過去 6 時間（Utilization Inbound and Outbound, Last 6 Hours）] ▶ [インバウンドおよびアウトバウンドのアプリケーショントラフィック、過去 6 時間（Application Traffic Inbound and Outbound, Last 6 Hours）] ▶ [上位のアクティブな会話、インバウンド（Top Active Conversations, Inbound）] ▶ [上位のアクティブな会話、アウトバウンド（Top Active Conversations, Outbound）]
[インターフェイストラフィックダッシュボード（Interface Traffic Dashboard）]	このダッシュ ボードには、選択したインターフェイスのトラフィック データがさまざまなグラフおよびテーブルで表示されます。データは次のセクション内に表示されます。 ▶ [インターフェイスサービストラフィック（Interface Service Traffic）] ▶ [インターフェイスアプリケーショントラフィック（Interface Application Traffic）] ▶ [インターフェイスの統計情報（Interface Statistics）] ▶ [インターフェイス使用率（Interface Utilization）] ▶ [DSCP トラフィック（DSCP Traffic）]
[セキュリティの概要（Security Overview）]	このダッシュ ボードには、システムのセキュリティに関連するデータがグラフおよびテーブルで表示されます。データは次のセクション内に表示されます。 ▶ [関心のある内部ホスト（Inside Concern Hosts）] ▶ [関心のある外部ホスト（Outside Concern Hosts）] ▶ [上位のアラームホスト（Top Alarming Hosts）] ▶ [タイプ別に要約された現在アクティブなアラーム（Alarms Currently Active Summarized by Type

ダッシュボード名	説明
[SMC ダッシュボード（SMC Dashboard）]	このダッシュ ボードには、SMC コンソールの最も重要なアクティビティがグラフで表示されます。データは次のセクション内に表示されます。 ▶ [SMC のパフォーマンス（SMC Performance）] ▶ [SMC のアラーム（SMC Alarms）] ▶ [処理された SMC イベント（SMC Event Processed）]
[トラフィックダッシュボード（Traffic Dashboard）]	このダッシュ ボードには、選択されたドメインのトラフィックの統計情報がグラフで表示されます。データは次のセクション内に表示されます。 ▶ [プロトコル、内部および外部ホストからのパケット（Protocols, Packets from Inside and Outside Hosts）] ▶ [TCP フラグ、内部および外部ホストからのパケット（TCP Flags, Packets from Inside and Outside Hosts）] ▶ [内部および外部ホストで開始されたアクティブなフロー（Active Flows Initiated by Inside and Outside Hosts）] ▶ [内部および外部のアクティブなホスト（Inside and Outside Active Hosts）]

（注）：
これらのダッシュボードの詳細については、Stealthwatch デスクトップクライアントのオンラインヘルプを参照してください。

[ホストグループダッシュボード（Host Group Dashboard）]

[ホストグループダッシュボード（Host Group Dashboard）] には、選択したホスト グループのネットワーク、セキュリティ、およびアラームに関する重要なアクティビティのデータがグラフおよびテーブルで表示されます。表示されるデータは、5 分ごとに SMC から収集されます。このドキュメントを表示するには、エンタープライズ ツリー内でデータを表示するホストをクリックしてから、SMC のメイン メニューで [ステータス（Status）] > [ダッシュボード（Dashboards）] > [ホストグループダッシュボード（Host Group Dashboard）] を選択します。

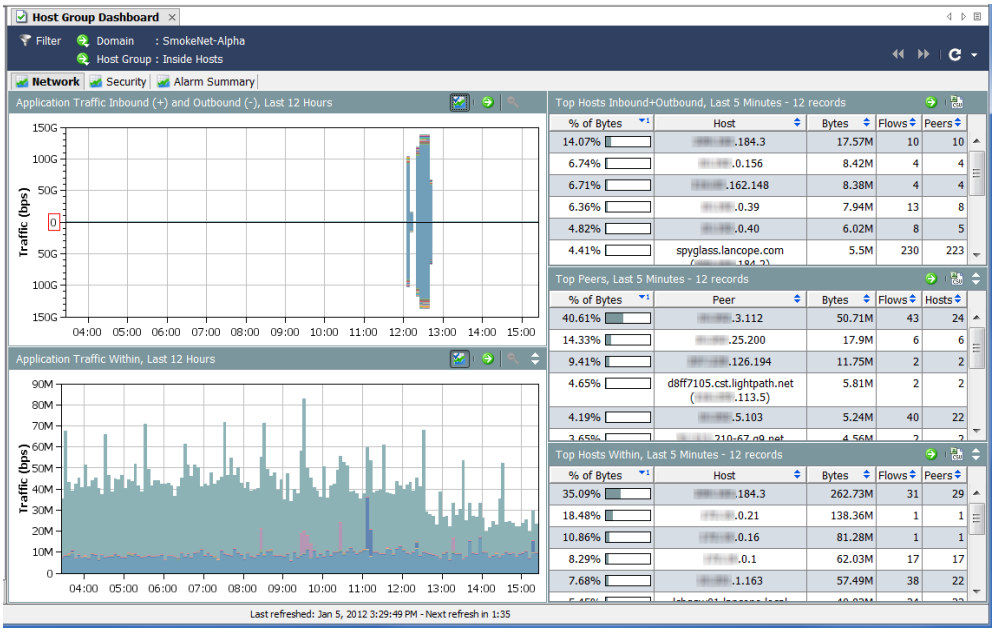


[ホストグループダッシュボード（Host Group Dashboard）] で次のページを表示する方法については、この章の以降の部分の対応するセクションに移動してください。

- [ネットワーク（Network）] ページ
- [セキュリティ（Security）] ページ
- [アラームサマリー（Alarm Summary）] ページ

[ホストグループダッシュボード(Host Group Dashboard)] - [ネットワーク(Network)] ページ

[ホストグループダッシュボード(Host Group Dashboard)]:[ネットワーク(Network)] ページには、選択したホスト グループのネットワークに関連する重要なアクティビティのデータがグラフおよびテーブルで表示されます。このダッシュボードを表示するには、[ネットワーク(Network)] タブをクリックします。



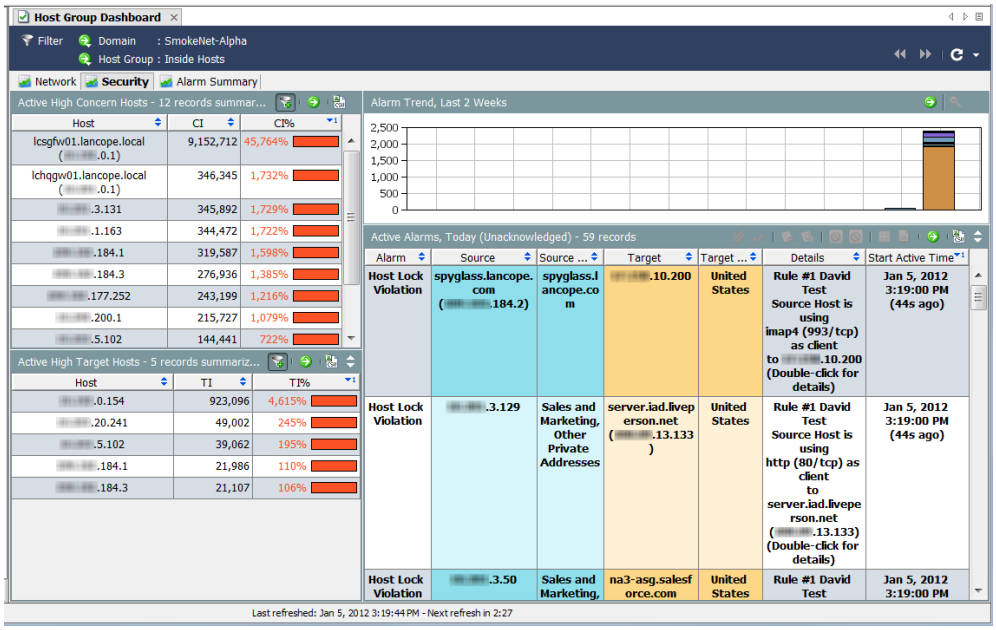
[ネットワーク(Network)] ページを見ながら、次の質問に答えてください。

- アプリケーション グラフに、組織内で通常使用されないアプリケーションのトラフィックが大量に発生していることが示されていますか。
- アプリケーション グラフに、通常使用されないアプリケーションのトラフィックが特定の時刻(通常の就業時間後など)に大量に発生していることが示されていますか。
- アプリケーションのグラフに、未定義のアプリケーションまたはその他のアプリケーションのトラフィックが大量に発生していることが示されていますか。該当する場合は、その他のアプリケーション定義を設定する必要があります。

- [上位のアクティブホスト(Top Active Hosts)] テーブルに、上位のアクティブ ホストのリストに通常は表示されないホストが含まれていますか。
- [上位のアクティブホスト(Top Active Hosts)] テーブルに、少数のホストで非常に大量のトラフィックが処理されていることが示されていますか。

[ホストグループダッシュボード(Host Group Dashboard)] - [セキュリティ(Security)] ページ

[ホストグループダッシュボード(Host Group Dashboard)]:[セキュリティ(Security)] ページは、最初に表示されるダッシュボードです。このドキュメントには、選択したホスト グループのセキュリティに関連する重要なアクティビティのデータがグラフおよびテーブルで表示されます。



(注):

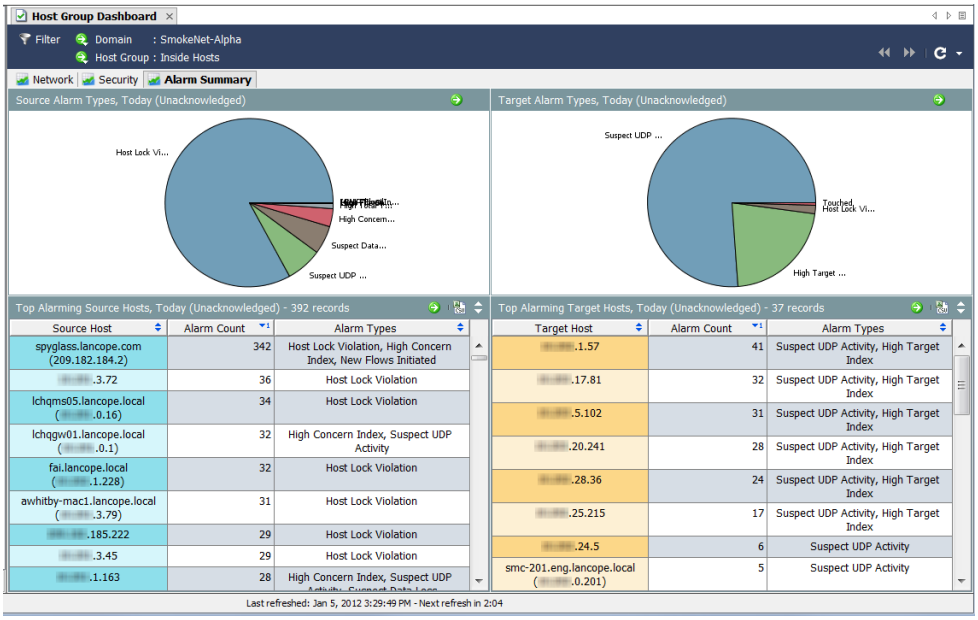
各ドキュメント ヘッダーの [ドキュメントに移動(Go to Document)] ボタン (注):をクリックして、各コンポーネントを独立したドキュメントとして開くことができます。

[セキュリティ(Security)] ページを見ながら、次の質問に答えてください。

- [懸念事項インデックスホスト(High CI Hosts)] テーブルに、組織にとって重要なホストの懸念事項インデックスが示されていますか。
- [ホストグループ別のアラームレポート(Alarm Report by Host Group)] テーブルに、重要なホスト グループの懸念事項インデックス アラームが示されていますか。
- [ホストグループ別のアラームレポート(Alarm Report by Host Group)] テーブルに、特定の日付の懸念事項インデックス アラームにスパイクがあることが示されていますか。
- [アラームを発行中の上位ホスト(Top Alarming Hosts)] テーブルに、組織にとって重要なホストに多数のアラームが発生していることが示されていますか。
- [アラームを発行中のホスト(Alarming Hosts)] テーブルに、特に懸念されるアラームのタイプが示されていますか。
- [上位のスキャン(Top Scans)] テーブルに、組織にとって重要なソース ホストまたはターゲット ホストに対する TCP/UDP アドレス スキャンが大量に発生していることが示されていますか。

[ホストグループダッシュボード(Host Group Dashboard)] - [アラームのまとめ(Alarm Summary)] ページ

[ホストグループダッシュボード(Host Group Dashboard)]:[アラームのまとめ(Alarm Summary)] ページには、選択したホスト グループのアラーム アクティビティのサマリー グラフ、および詳細なテーブル データが表示されます。このダッシュボードを表示するには、[アラームのまとめ(Alarm Summary)] タブをクリックします。



[アラーム(Alarms)] ページを見ながら、次の質問に答えてください。

- テーブルに、組織にとって重要なホストまたはホスト グループに関するアラームが多数示されていますか。
- テーブルに、特に懸念されるアラームのタイプが示されていますか。

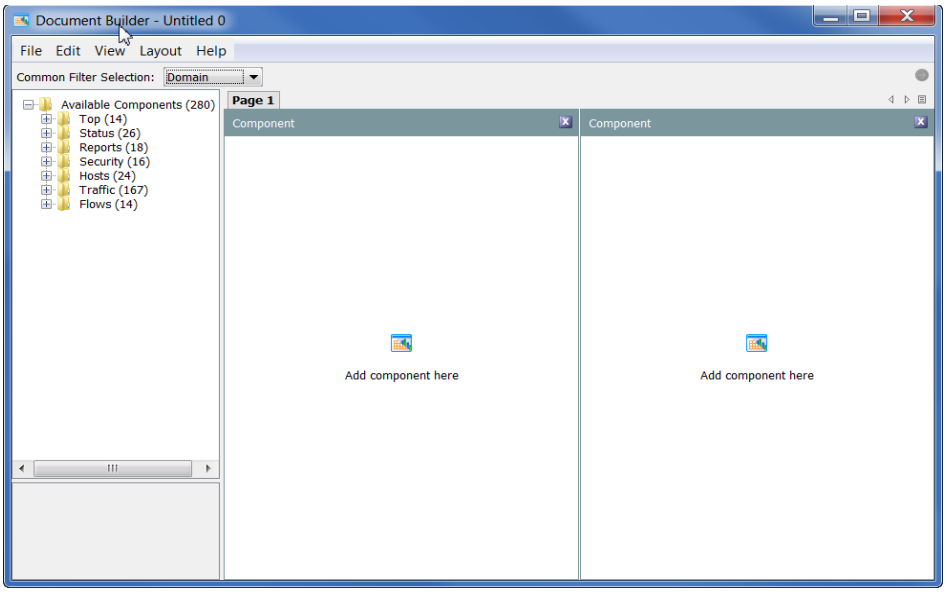
独自のダッシュボードの構築

[ドキュメントビルダー(Document Builder)] を使用すると、必要な SMC コンポーネントと表示したいデータが含まれるカスタム ダッシュボード(ダッシュボードはさまざまなレポートの集まり)を作成できます。これらのコンポーネントの名前を、わかりやすい名前に変更することもできます。

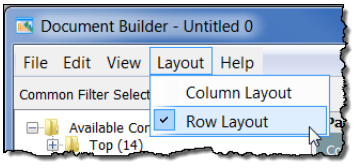
説明のために、セキュリティ アラームのみを扱うセキュリティレポート ダッシュボードを作成します。このサンプル ダッシュボードに複数のタブを配置し、それぞれに複数のコンポーネントが表示されるようにします。ただし、同じ原則に従って、必要な任意のタイプのダッシュボードを構築することができます。

独自のカスタム ダッシュ ボードを構築するには、次の手順を実行します。

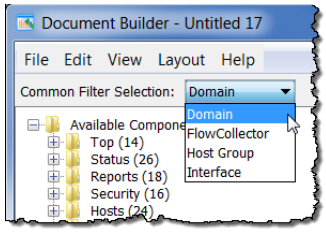
1. SMC のメイン メニュー選択で [表示(View)] > [ドキュメントビルダー(Document Builder)] を選択します。[ドキュメントビルダー(Document Builder)] ダイアログボックスが開きます。



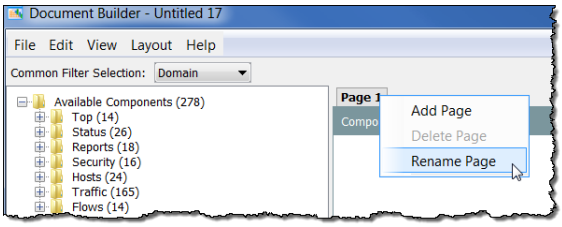
2. ドキュメントを列形式(デフォルト)でなく行形式にする場合は、[ドキュメントビルダー(Document Builder)] のメイン メニューで [レイアウト(Layout)] > [行レイアウト(Row Layout)] を選択します。

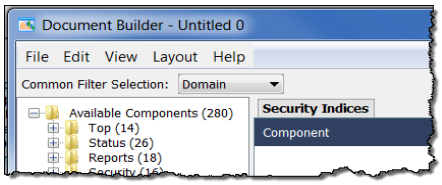


3. [一般的なフィルタ選択(Common Filter Selection)] ドロップダウン リスト内の矢印をクリックして、このドキュメントのデフォルトのフィルタリング基準となるオプションをクリックします。右の例では、ドキュメントは [ドメイン(Domain)] でフィルタリングされます。



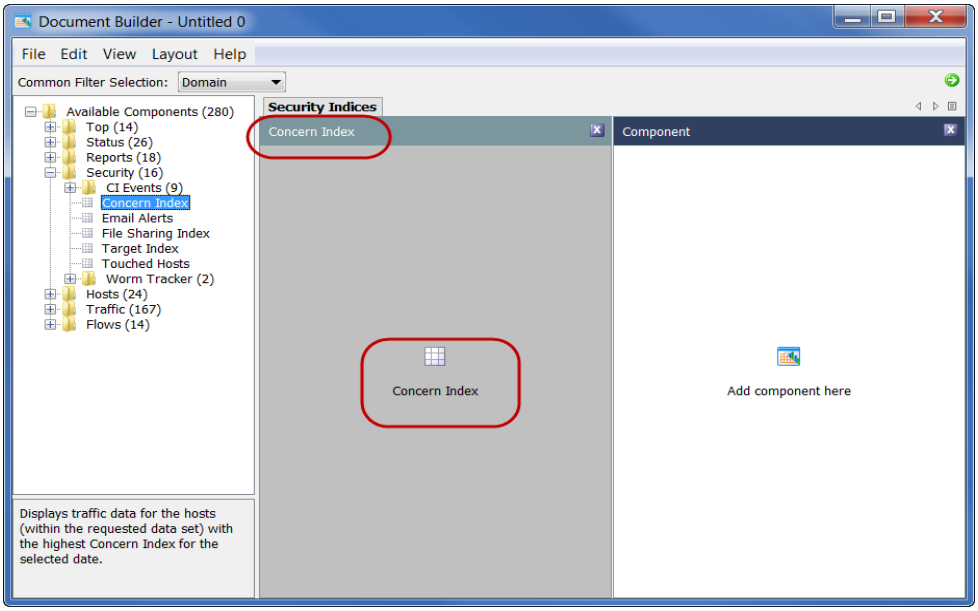
4. ページの名前を変更する場合は、そのページのタブを右クリックして、[ページの名前変更(Rename Page)] を選択します。(タブをダブルクリックして、このタブに新しいページ名を直接入力することもできます。)





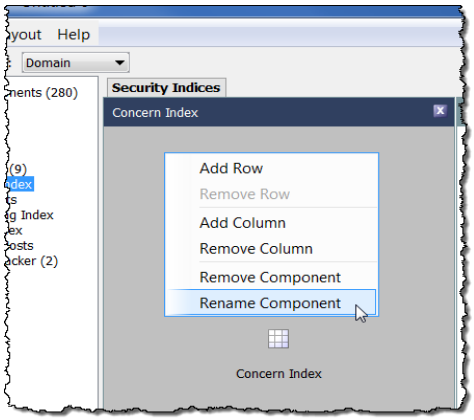
左の例では、ページ タブの名前を [Page 1] から [Security Indices] に変更しました。

5. 左側のツリー メニューで追加するコンポーネントをクリックし、そのコンポーネントを配置先のページ上のエリアにドラッグします。次の例では、左側の列に [リスクインデックス(Concern Index)] コンポーネントをドラッグしました。

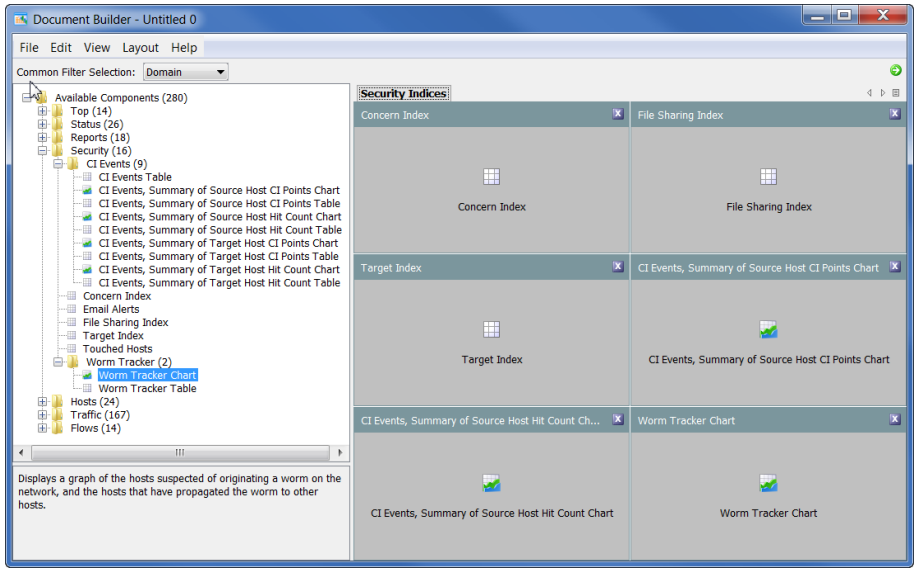


コンポーネントの名前が [Component] から、直前に追加したコンポーネントの名前である [Concern Index] に変更されたことに注意してください。この列の中央にあるアイコンの名前も、直前に追加したコンポーネントの名前に変更されています。

6. コンポーネントの名前を変更する場合は、コンポーネントの本体内で右クリックして、[コンポーネントの名前変更（Rename Component）] を選択します。



7. 操作が終了するまで、このページに引き続きコンポーネントを追加します。デフォルト ページには、コンポーネントのエリアが 2 つのみ表示されています。ただし、3 つ以上のエリアを追加すると、それに応じてページが調整されます。次の例には、6 つのコンポーネントが配置されています。列に新しいコンポーネントを追加すると、この列の最後のエントリの下に追加したコンポーネントが表示されます。レイアウトは必要に応じていつでも変更できます。

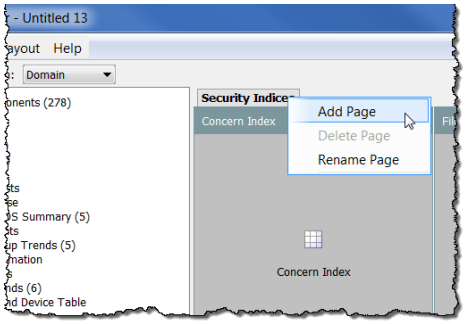


（注）：

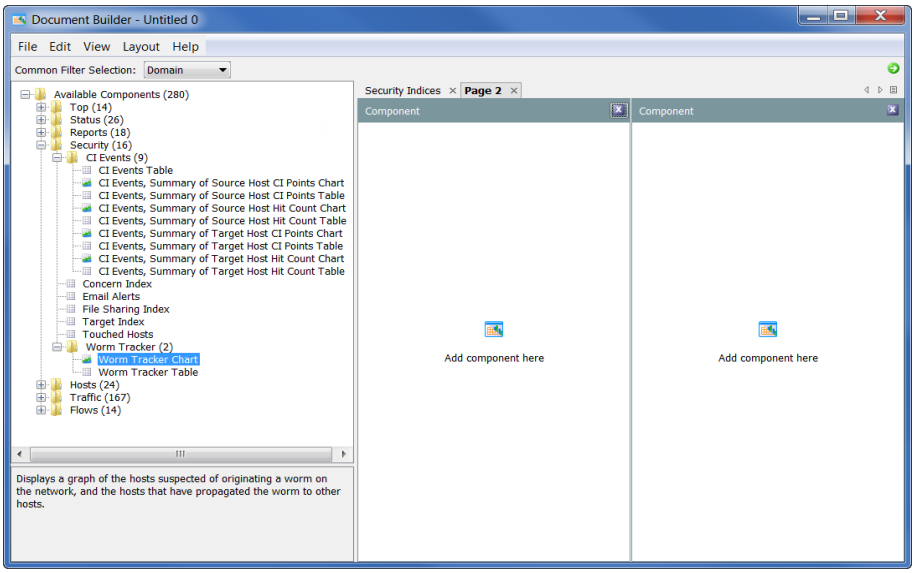
ボタンを 1 回クリックすると、コンポーネント エリアが空になります。

ボタンを 2 回クリックすると、コンポーネント エリアが完全に削除されます。

8. ドキュメントに別のページ(タブ)を追加する場合は、既存のタブを右クリックして、[ページを追加(Add Page)] を選択します。



新しい空白のページが開きます。



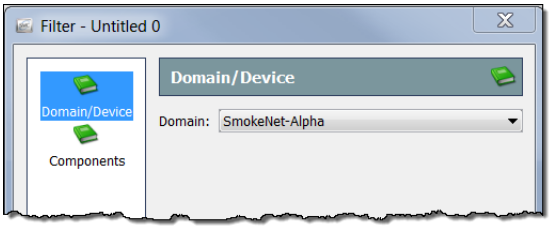
9. 最初のページと同様に、このページ上の目的の場所にコンポーネントをドラッグします。

10. ドキュメントの作成が終了したら、[ファイル(File)] > [名前を付けて保存(Save As)] をクリックして、ハード ドライブに XML テンプレートとして保存します。

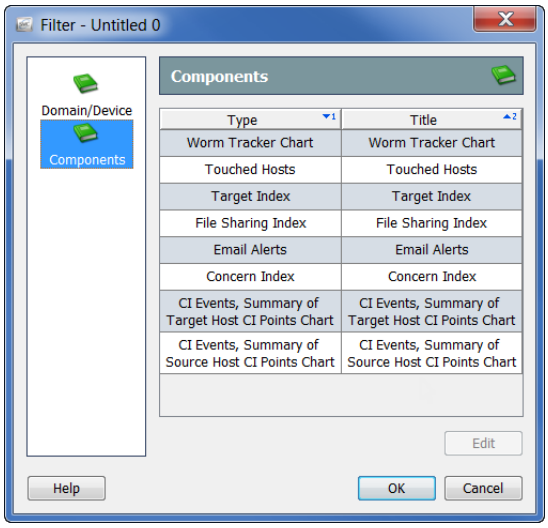
(注):

ファイル名がドキュメント名になります。たとえば、ファイルを *1234* の名前で保存した場合、ドキュメントのタイトルは *1234* になります。したがって、ドキュメントには意味のあるファイル名を付けるようにしてください(*Security Reports* など)。

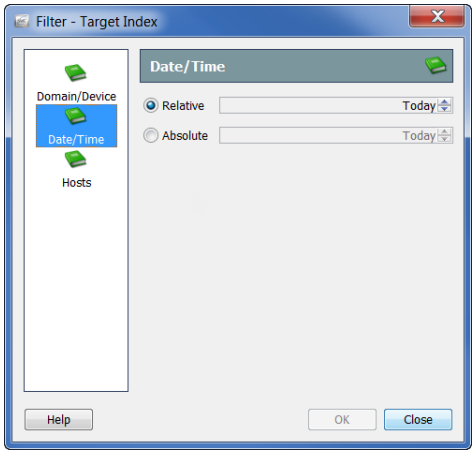
11. [ドキュメントビルダー(Document Builder)] ダイアログボックスの右上にある [ドキュメントに移動(Go to Document)] ボタン をクリックして、Stealthwatch デスクトップクライアント内でドキュメントを起動します。ドキュメントの [フィルタ(Filter)] ダイアログが開きます。[ドメイン/デバイス(Domain/Device)] ボタンがまだ強調表示されていない場合は、このボタンをクリックします。フィルタリングするドメインが選択されていることを確認してください。



12. [コンポーネント(Components)] ボタンをクリックします。ドキュメントに含まれているすべてのコンポーネントがリストされます。

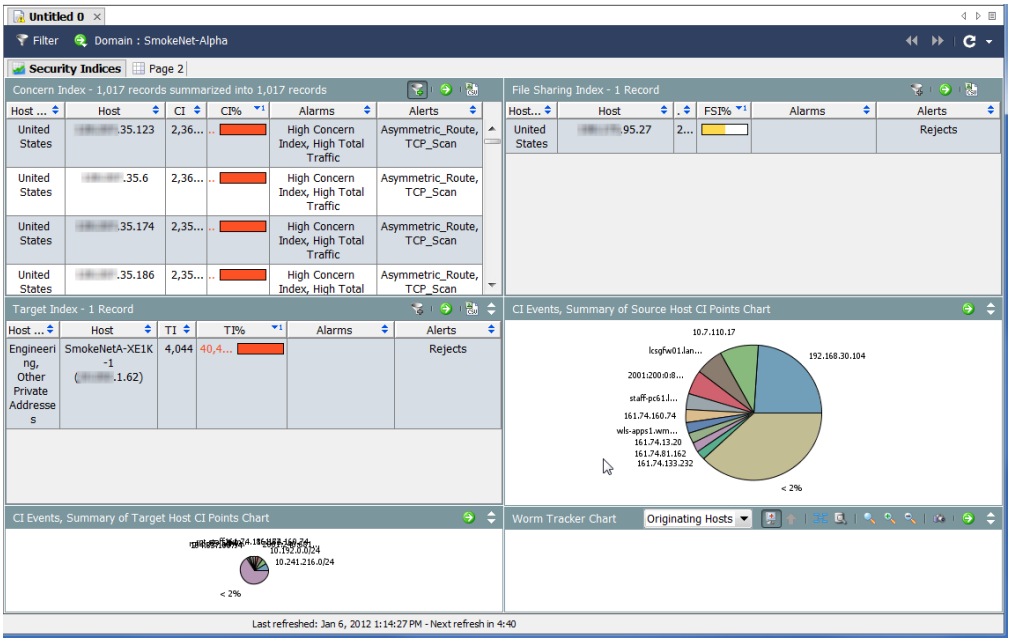


13. フィルタリングするコンポーネントをクリックして、[編集(Edit)] をクリックします。このコンポーネントの [フィルタ(Filter)] ダイアログボックスが開きます(フィルタリングできるオプションは、ダイアログボックスの左側でクリックしたボタンに応じて異なります)。



14. 選択したら、[OK] をクリックします。

15. SMC GUI 内に開かれた新しいドキュメントは、次の例のように表示されます。必要に応じて、列およびコンポーネントのサイズを変更します。



16. 終了したら、SMC のメイン メニューで [ファイル(File)] > [名前を付けて保存(Save As)] を選択して SMC サーバーにドキュメントを保存し、SMC 内でいつでも開けるようにすることができます。

(注):
ファイル名がドキュメント名になります。たとえば、ファイルを *1234* の名前で保存した場合、ドキュメントのタイトルは *1234* になります。したがって、ドキュメントには意味のあるファイル名を付けるようにしてください(*Security Reports* など)。

17. [ドキュメントビルダー(Document Builder)] を閉じます。

(注):
必要に応じて、以前に保存した XML ファイルおよび DAR ファイルを [ドキュメントビルダー(Document Builder)] で開き、編集することができます。

5

インデックス:ランキング動作の変更

概要

Stealthwatch はインデックスを使用して、ネットワーク上のホストの異常を検出します。Stealthwatch フロー コレクタは、独自のヒューリスティックおよびアルゴリズムを使用して使用環境の標準動作の基準を設定します。これにより、禁止されているさまざまなホスト動作に関するリスク インデックス(CI)ポイントをホストに追加します。累積されたインデックス ポイントが許容されるしきい値を超えると、フロー コレクタはアラームを生成します。

インデックスは、動作がどれくらい異常であるのか、および異常なアクティビティの関連性について Stealthwatch がどれくらい確実に判断しているのかを示す際に役立ちます。つまり、インデックを使用することで、調査に優先順位を付けることができます。

たとえば、見知らぬ人が玄関のドアをガラガラと開けたとして、住所が間違っていたとその人が言うなら、警察に通報する理由はないと考えるでしょう。リスク インデックスは比較的低い値になります。ただし、その人がその後も同じ通りにある隣の家のドアで同じことを行った場合は、その人の行動に対する不信感が高まります。

その人がドアに近づくたびに、リスク インデックスが 1 ポイント以上増える可能性が高くなります。その人が 3 番目のドアに近づいたときは、警察に通報する必要があるまでに懸念が高まっています。この場合、その人の行動について心配しなくてもよいのは、2 番目のドアまでです。その人が 3 番目のドアに近づいた場合は、このしきい値を上回るため、何らかの行動が必要となります。

Stealthwatch インデックスは同じ方法でユーザーのネットワークを保護し、異常なアクティビティが禁止レベルに達した場合のみアラームを生成します。基本的に、これらのインデックスに赤色の情報が表示されている場合は、動作について重要な変化が起きています。

たとえば、TCP を 1 回リセットした場合は、Stealthwatch によって CI ポイントが割り当てられるとしても、アラームは生成されません。ただし、TCP を何度もリセットすると、システムで定義された許容レベルに基づいてアラームが生成される可能性があります。

Stealthwatch は次のインデックスを使用して、異常な動作を追跡します。

- リスク インデックス(CI)– ネットワークの整合性を低下させる可能性のあるアクティビティを実行しているホストを追加します。
- ターゲット インデックス(TI)– 他のホストの疑わしい動作の被害を受けるホストを追跡します。
- ファイル共有インデックス(FSI)– ピアツーピア(P2P)アクティビティを示す動作を追跡します。

この章は、次の項で構成されています。

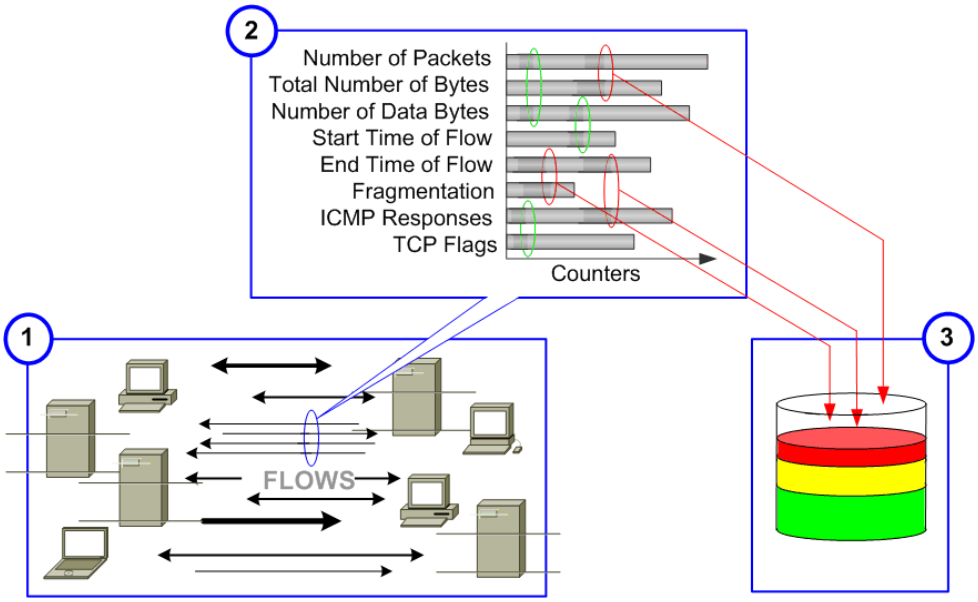
リスク インデックス

リスク インデックス(CI)は、サービス妨害(DoS)やスキャン アクティビティ中にネットワーク ホストから応答を得るために意図的に送信されるパケットのような、疑わしいフロー アクティビティがある場合に、Stealthwatch からユーザーに通知するための主な手段となります。Stealthwatch はこれらのアクティビティに、「セキュリティ イベント」というラベルを付けます。

セキュリティ イベントはセキュリティ違反、デバイスの設定ミス、サーバーの機能不良、またはネットワーキング問題の別の発生元を示す可能性があります。Stealthwatch はこれらのイベントに関連付けられた情報を追跡して、このホストの CI ポイント数を増やします。CI が大きいほど、この動作に対する懸念のレベルが上昇します。

ポイント数が設定されたしきい値を超えると、Stealthwatch はアクティビティの発生元であるホストに対して懸念事項インデックス アラームを生成します。CI 値の有効範囲は、0 から数十万ポイントまでです。

次の図に、CI の増加に関連する 3 つの基本段階を示します。



1. Stealthwatch フロー コレクタは、ホストが関連するフローを観察します。
2. フロー コレクタは、観察されたアクティビティと許容できる動作として設定されたアクティビティを比較します。
3. フロー コレクタは、ホストのアクティビティの一部が許容できないことを検出して、CI を増加させます。

内部ホストで懸念事項インデックス アラームが発生している場合は、通常、ホストが異常な動作を行っていて、侵害、誤使用、ポリシー違反が発生する可能性がないか調べる必要があります。

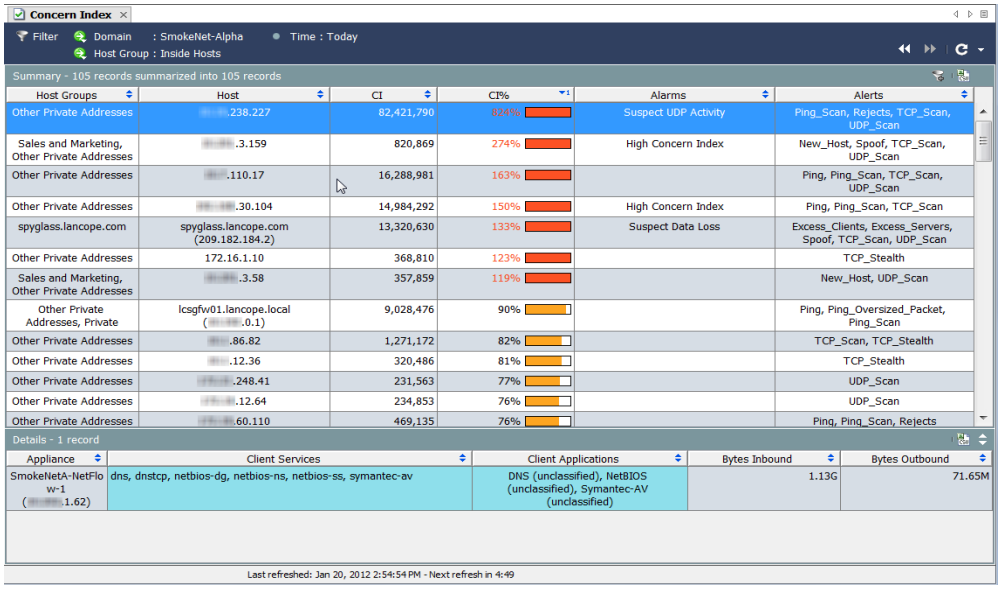
外部ホストで懸念事項インデックス アラームが発生している場合は、通常、ネットワークの整合性違反を引き起こす試みの一環として「不適切な処理」が行われています。いずれの場合も、[リスクインデックス(Concern Index)] ドキュメントを参照することで、ネットワークに攻撃しているホストや、攻撃を受けているホストを特定することができます。

(注):

ホストのアクティビティが CI しきい値を超えていても、関連付けられたホスト グループの懸念事項インデックス アラームが抑制されている場合、フロー コレクタはそのホストに対して懸念事項インデックス アラームを生成しません。

Stealthwatch フロー コレクタは、ユーザーが定義したアーカイブ時刻に、24 時間おきにすべてのインデックス数をクリアします。その時点で、フロー コレクタは過去 24 時間内に収集されたログ ファイルおよび Web ファイルを保存し、翌日のデータ収集を開始します。

[リスクインデックス(Concern Index)] ドキュメントには、前回のアーカイブ時刻以降に CI ポイント数が最大であったホストの情報が表示されます。

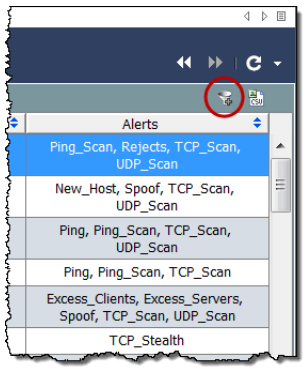


[リスクインデックス(Concern Index)] ドキュメントを表示するには、ドメインまたはホスト グループを右クリックして、[セキュリティ(Security)] > [リスクインデックス(Concern Index)] を選択します。

[リスクインデックス(Concern Index)] ドキュメントを使用することで脅威に優先順位を付けて、実際に問題となるイベントに専念することができます。Stealthwatch では、毎日生成される数千のアラートを表示する代わりに、少数の実用的な項目を、優先度の高い順に表示することができます。

(注):

アラートは異常なネットワーク アクティビティの情報を示すサマリーですが、アラームと異なり、通知として送信されません。



デフォルトでは、[リスクインデックスフィルタ(Concern Index Filter)] ボタン (ドキュメントの右上) が有効になっていて、リスク インデックスには、リスク インデックス アラームがアクティブなホスト (CI のパーセント値が 100 を超えているホスト) のみが表示されます。CI のパーセント値が 50 を超えるホストを表示するには、[リスクインデックスフィルタ(Concern Index Filter)] ボタンをクリックします。[リスクインデックスフィルタ(Concern Index Filter)] ボタンのプラス記号がグレーに変わり、有効な懸念事項インデックス アラームがあるかどうかに関係なく、CI のパーセント値が 50 を超えるホストが表示されます。

(注):

ホストに累積された CI はアーカイブ時刻にクリアされます。

リスク インデックスの上部に [概要(Summary)] セクション、下部に [詳細(Details)] セクションがあることに注意してください。[概要(Summary)] セクション内の行を選択すると、この行に関する詳細が [詳細(Details)] セクションに表示されます。

前の例では、脅威レベルが最高のホストは xxx.xxx.238.227 です。この例の目的に合わせて、このホストは内部ホストであると仮定します。このホストに関する次の情報を簡単に確認できます。

- 前回のアーカイブ時刻以降、このホストでは CI パーセントが累積して約 824 パーセントになりました。
- このホストで 2 つのアラート (Ping_Scan、Rejects、TCP_Scan、UDP_Scan) も発生しました。
- 受信したデータ量は 1.13G です。
- 送信したデータ量は 71.65M です。

CI のパーセント値、アラーム、アラート、およびデータ転送を組み合わせることで、セキュリティ違反が発生した可能性があることがわかります。このホストに侵害、誤使用、またはポリシー違反の可能性があるか調べる必要があります。

ホストの IP アドレスをダブルクリックしてホストのスナップショットを開き、セキュリティ イベントの発生元となるホストを探します。

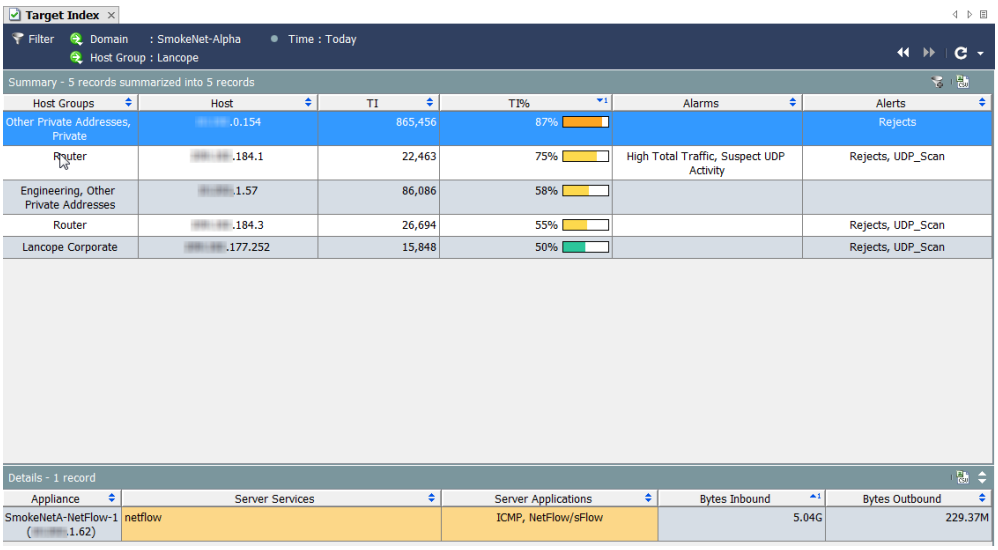
（注）:

[リスクインデックス（Concern Index）] ドキュメントに表示できるさまざまな列の説明については、Stealthwatch デスクトップクライアントのオンラインヘルプを参照してください。

ターゲット インデックス

ターゲット インデックス(TI)に、Stealthwatch フロー コレクタの前回のアーカイブ時刻以降にターゲット インデックスが最大となったホスト(要求されたデータ セット内)が表示されます。ターゲット IP アドレスが複数のセキュリティ イベントまたは他の悪意のある攻撃を受信していて、しきい値を超えている場合、Stealthwatch フロー コレクタはターゲット インデックス アラームをトリガーします。ターゲット インデックスは、単一の内部ホストで複数のホストが転送されることにより分散攻撃が行われる可能性があることをユーザーに警告するために使用されます。

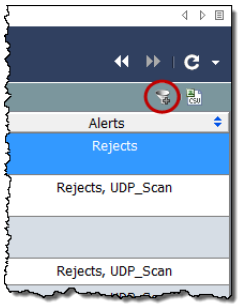
侵害されたホストおよび関連付けられたサービスとポートが特定されたら、使用している機器およびソフトウェアに応じて、ファイアウォールおよびホスト自体で禁止されたポートをブロックすることができます。また、ネットワークからホストを切断して、スクラビング処理を行うこともできます。



ターゲット インデックスを表示するには、ドメインまたはホスト グループを右クリックして、[セキュリティ(Security)] > [ターゲット インデックス(Target Index)] を選択します。

ターゲット インデックス値の有効範囲は、0 から数十万ポイントまでです。ターゲット インデックス ポイントがホストごとに累積されると、TI アラームが生成されることがあります。デフォルトでは、データは TI パーセントを基準として降順に並べ替えられます。データは、前回のアーカイブ時刻以降にドメイン内で観察された最大のデータ値を表します。たとえば、TI パーセント値が 158 のホストは TI しきい値を 58% 超過しているため、さらなる調査が必要になる可能性があります。パーセントの後に、TI しきい値に近づくと色が変化するグラフィックが表示されます(次の表を参照)。

設定されたしきい値に対する割合	テキストの色
設定されたしきい値の 0%	空のグラフィック
設定されたしきい値の 0 ～ 50%	緑
設定されたしきい値の 51 ～ 75%	黄
設定されたしきい値の 76 ～ 99%	オレンジ
設定されたしきい値の 100% 以上	赤



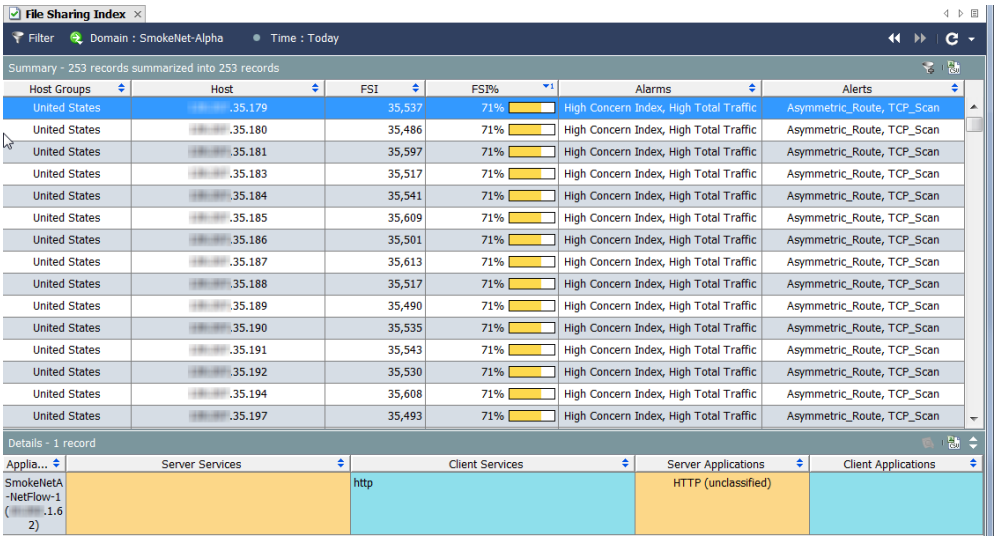
デフォルトでは、[ターゲットインデックスフィルタ(Target Index Filter)] ボタン (ドキュメントの右上)が有効になっていて、ターゲット インデックスには、ターゲット インデックス アラームがアクティブなホスト(TI のパーセント値が 100 を超過しているホスト)のみが表示されます。TI のパーセント値が 50 を超えるホストを表示するには、[ターゲットインデックスフィルタ(Target Index Filter)] ボタンをクリックします。[ターゲットインデックスフィルタ(Target Index Filter)] ボタン のプラス記号がグレーに変わり、TI のパーセント値が 50 を超えるホストが表示されます。

ファイル共有インデックス

ファイル共有インデックス(FSI)の目標は、組織にリスクをもたらす疑わしいファイル共有アプリケーション、特にピアツーピア(P2P)通信を検出することです。この処理は、ネットワークの内部または外部の他のユーザーと著作権情報を共有することによって、機密情報が送信されたり、組織のネットワークが誤って使用されたりする可能性がある場合に発生することがあります。

Stealthwatch フロー コレクタは、ネットワーク上のすべてのホストで確立された接続に関するさまざまな情報を収集します。特定の統計情報を関連付けることにより、ファイル共有インデックスが取得されます。このインデックスは、ファイル転送(通常は P2P アクティビティを示す)に関連する可能性があるホストを識別します。

このインデックスは、関連付けの技術を使用して、最もアクティブなホストを示します。またポイントを追加することで、ファイル共有アクティビティとの関連性が一般に最も高いセンサーの組み合わせを作動させます。この技術は、Stealthwatch フロー コレクタでスキャン アクティビティを示すために使用されるリスク インデックス値の判別技術と似ています。[ファイル共有インデックス(File Sharing Index)] ドキュメントには、調査対象となるホスト、およびオプションのホストレベル アラームの対象となるホストの優先順位付きリストが表示されます。

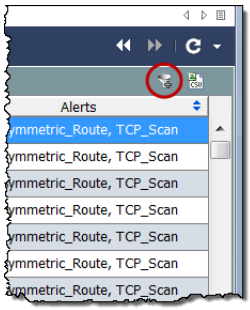


ファイル共有インデックスを表示するには、ドメインまたはホスト グループを右クリックして、[セキュリティ(Security)] > [ファイル共有インデックス(File Sharing Index)] を選択します。

ファイル共有インデックス値の有効範囲は、0 から数十万ポイントまでです。ファイル共有インデックスのポイントがホストごとに累積されると、ファイル共有インデックス アラームが生成されることがあります。デフォルトでは、データは FSI パーセントを基準として降順に並べ替えられます。データは、前回のアーカイブ時刻以降にドメイン内で観察された最大のデータ値を表します。たとえば、FSI パーセント値が 158 のホストは、FSI しきい値を 58% 超過しているため、さらなる調査が必要になる可能性があります。

パーセントの後に、FSI しきい値に近づくと色が変化するグラフィックが表示されます（次の表を参照）。

設定されたしきい値に対する割合	テキストの色
設定されたしきい値の 0%	空のグラフィック
設定されたしきい値の 0 ～ 50%	緑
設定されたしきい値の 51 ～ 75%	黄
設定されたしきい値の 76 ～ 99%	オレンジ
設定されたしきい値の 100% 以上	赤



デフォルトでは、[ファイル共有インデックスフィルタ（File Sharing Index Filter）] ボタン（ドキュメントの右上）が有効になっていて、ファイル共有インデックスには、ファイル共有インデックス アラームがアクティブなホスト（FSI のパーセント値が 100 を超過しているホスト）のみが表示されます。FSI のパーセント値が 50 を超えるホストを表示するには、[ファイル共有インデックスフィルタ（File Sharing Index Filter）] ボタンをクリックします。[ファイル共有インデックスフィルタ（File Sharing Index Filter）] ボタン のプラス記号がグレーに変わり、FSI のパーセント値が 50 を超えるホストが表示されます。

6

トラフィックおよびネットワーク パフォーマンスのモニターリング

概要

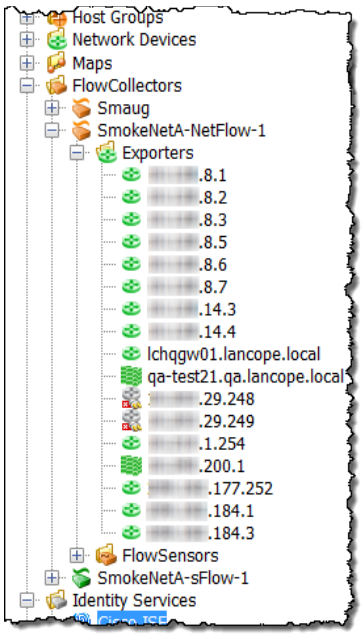
Stealthwatch はネットワーク動作分析を使用してネットワークをモニターし、潜在的な問題があることを示す可能性のある変化が生じた場合にユーザーに通知します。システムはネットワーク上のすべてのホストを継続的に観察し、ホストのアクティブ レベルの増減、ホスト間のデータ送信量、関連するトラフィックの種類などの動作を記録します。

この章では、ネットワーク上のトラフィックを表すグラフ形式およびテーブル形式のデータを利用して、ホストやネットワークの動作の変化を確認する方法について説明します。潜在的な脅威が存在する場合は、これらがネットワークに被害をもたらす前に解決することができます。

この章は、次の項で構成されています。

- トラフィックのモニターリング
- エクスポータ/ネットワーク デバイス
- ネットワーク パフォーマンス

トラフィックのモニターリング

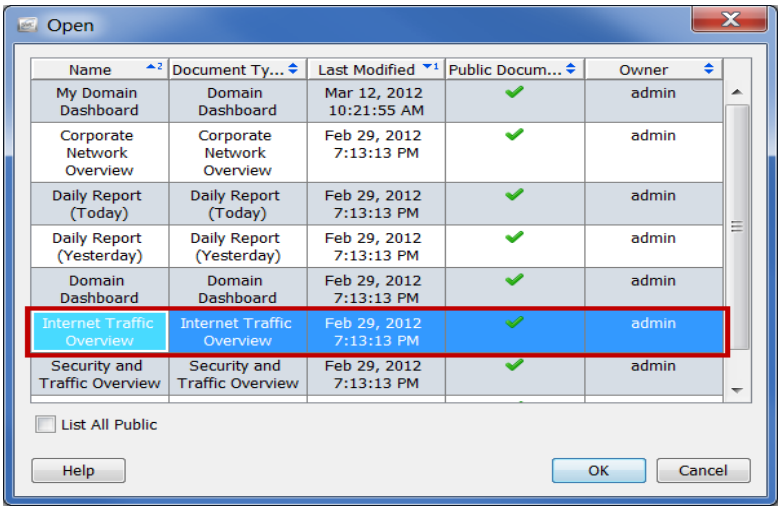


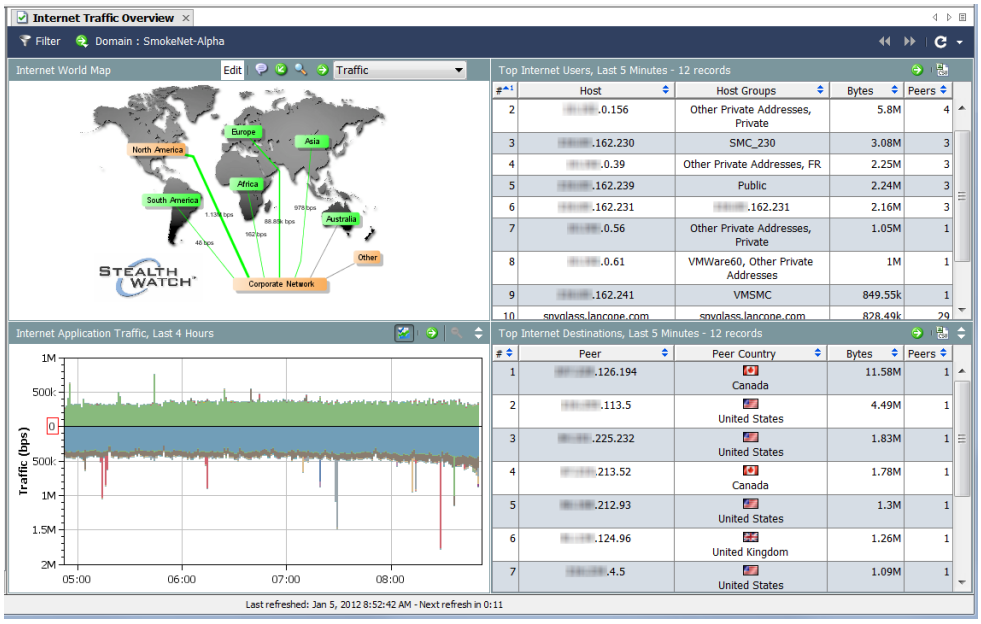
SMC のグラフィカル ユーザー インターフェイスの左側のフレーム内に、エンタープライズ ツリーがあります。このフレームにはツリー メニューが使用されていて、ユーザーは短時間に、かつ簡単な方法でシステムのステータスを表示したり、ドキュメントを要求したりできます。

トラフィックをモニターするための主な対象はエクスポータです。これは、Stealthwatch フロー コレクタにデータを送信するために設定されたルータまたはスイッチです。

インターネット トラフィックの概要

[インターネットトラフィックの概要(Internet Traffic Overview)] には、インターネットに関連付けられたドメイン トラフィックのデータがグラフおよびテーブルで表示されます。このドキュメントを表示するには、メイン メニューで [ファイル(File)] > [開く(Open)] を選択します。次のダイアログボックスが開きます。[インターネットトラフィックの概要(Internet Traffic Overview)] ドキュメントを選択して、[OK] をクリックします。





[インターネットのワールドマップ(Internet World Map)] を見ながら、次の質問に答えてください。

- ホスト グループまたはホスト グループの関係のいずれかに、クリティカル アラームまたはメジャー アラームが発生していることが示されていますか。これは、色およびコールアウトで判別できます。

  これらのアラームが発生している場合は、アラームを生成しているホスト グループまたはホスト グループの関係を右クリックしてから、[アラームテーブル(Alarm Table)] を選択して、詳細を表示します。

- ドキュメント ヘッダーのドロップダウン リスト内の矢印をクリックして、表示されるデータ タイプを変更します。ホスト グループの関係のいずれかに、異常なデータ量が発生していることが示されていますか。これは、線の太さおよび線のステータス テキストで判別できます。

  異常なデータ量が発生している場合は、ホスト グループの関係を右クリックしてから、[ホストグループの関係のダッシュボード(Host Group Relationship Dashboard)] を選択して、詳細を表示します。

[インターネットのアプリケーショントラフィック(Internet Application Traffic)]を見ながら、次の質問に答えてください。

- グラフに、組織で使用されているアプリケーションで異常なスパイクが生じていることが示されていますか。

ヒント:

[その他の非表示(Hide Others)] ボタン  をクリックして、使用されている上位数件に含まれていないアプリケーションのトラフィックを非表示にすることができます。このボタンをクリックすると、データの表示/非表示が切り替わります。

- グラフに、組織内で通常使用されないアプリケーションのトラフィックが大量に発生していることが示されていますか。
- グラフに、未定義のアプリケーションまたはその他のアプリケーションのトラフィックが大量に発生していることが示されていますか。

  該当する場合は、その他のアプリケーション定義を設定する必要があります。

[上位のインターネットユーザー(Top Internet Users)]を見ながら、次の質問に答えてください。

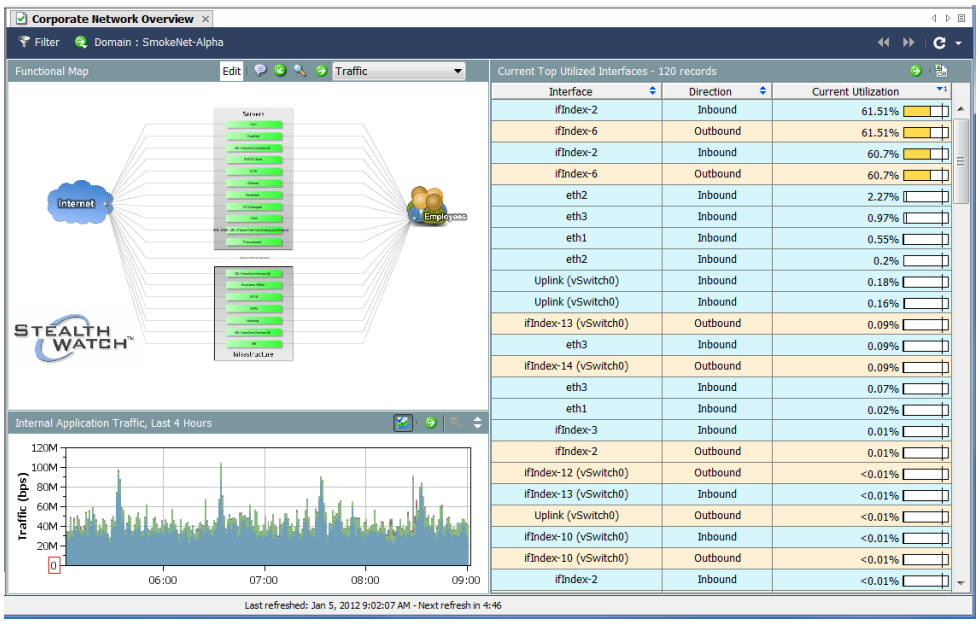
- テーブルに、組織内の上位のインターネット ユーザーに含まれないホストで大量のトラフィックが発生していることが示されていますか。
- テーブルに、サーバーとして機能していて、大量のトラフィックを送信している組織内のホストが示されていますか。
- テーブルに、多数のピアに対してトラフィックを送受信している組織内のホストが示されていますか。

[上位のインターネット接続先(Top Internet Destinations)]を見ながら、次の質問に答えてください。

- テーブルに、組織と通信していないピアに対するトラフィックが大量に発生していることが示されていますか。
- テーブルに、クライアントとして機能していて、組織内のホストから大量のトラフィックを受信しているピアが示されていますか。
- テーブルに、組織内の多数のホストに対してトラフィックを送受信しているピアが示されていますか。

社内ネットワークの概要

[社内ネットワークの概要(Corporate Network Overview)] には、社内ネットワーク全体に関連付けられたドメイン トラフィックのデータがグラフおよびテーブルで表示されます。このドキュメントを表示するには、メイン メニューで [ファイル(File)] > [開く(Open)] を選択します。[開く(Open)] ダイアログボックスが開きます。[社内ネットワークの概要(Corporate Network Overview)] ドキュメントを選択して、[OK] をクリックします。



機能マップを見ながら、次の質問に答えてください。

- ホスト グループまたはホスト グループの関係のいずれかに、クリティカル アラームまたはメジャー アラームが発生していることが示されていますか。これは、色およびコールアウトで判別できます。

  これらのアラームが発生している場合は、アラームを生成しているホスト グループまたはホスト グループの関係を右クリックしてから、[アラームテーブル(Alarm Table)] を選択して、詳細を表示します。

- ドキュメント ヘッダーのドロップダウン リスト内の矢印をクリックして、表示されるデータ タイプを変更します。ホスト グループの関係のいずれかに、異常なデータ量が発生していることが示されていますか。これは、線の太さおよび線のステータス テキストで判別できます。

異常なデータ量が発生している場合は、ホスト グループの関係を右クリックしてから、[ホストグループダッシュボード（Host Group Dashboard）] を選択して、詳細を表示します。

[内部アプリケーショントラフィック（Internal Application Traffic）] を見ながら、次の質問に答えてください。

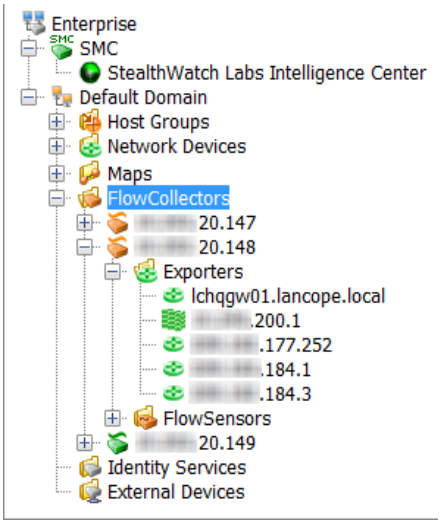
- グラフに、組織で使用されているアプリケーションで異常なスパイクが生じていることが示されていますか。
- グラフに、組織内で通常使用されないアプリケーションのトラフィックが大量に発生していることが示されていますか。
- グラフに、未定義のアプリケーションまたはその他のアプリケーションのトラフィックが大量に発生していることが示されていますか。該当する場合は、その他のアプリケーション定義を設定する必要があります。

[現在の上位の使用済みインターフェイス（Current Top Utilized Interfaces）] を見ながら、次の質問に答えてください。

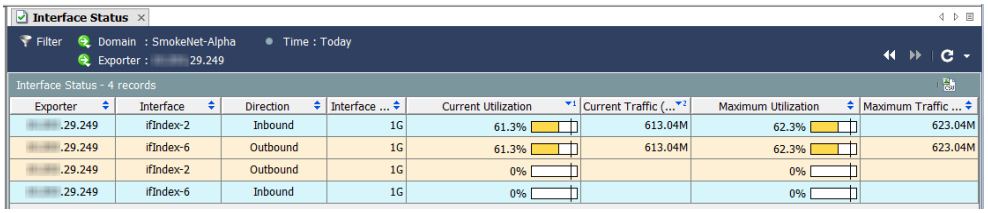
- テーブルに、飽和状態のインターフェイス（使用率が以上に高い割合を示しているもの）が示されていますか。
- テーブルに、上位ユーザーに含まれていないインターフェイスが示されていますか。

エクスポータ/ネットワーク デバイス

エクスポータはデータを受信するStealthwatch フロー コレクタの下のツリー内にあります(右側の例を参照)。

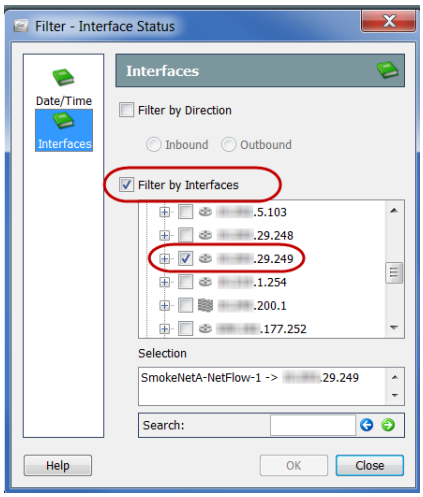


エクスポータのドキュメントに直接移動するには、エンタープライズ ツリー内の該当するホストの下の [ネットワークデバイス(Network Devices)] オプションを展開して、エクスポータをダブルクリックします。[インターフェイスステータス(Interface Status)] ドキュメントが開きます。このドキュメントには、sFlow 用の Stealthwatch フロー コレクタまたは NetFlow 用の Stealthwatch フロー コレクタにデータを送信しているルータまたはスイッチ(エクスポータ)のインターフェイスに関する統計情報が表示されます。

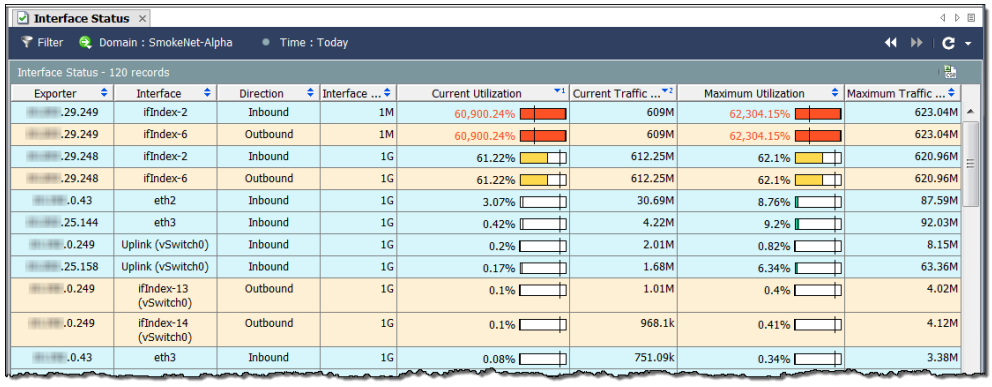


(注):
Cisco ASA エクスポータ タイプでは、[インターフェイスステータス(Interface Status)] ドキュメントを使用できません。

[インターフェイスステータス(Interface Status)]ドキュメントの左上にある[フィルタ(Filter)]ボタン をクリックします。表示された[フィルタ - インターフェイスステータス(Filter - Interface Status)]ダイアログボックス内の[インターフェイス(Interfaces)]ボタンがまだ強調表示されていない場合は、このボタンをクリックします。

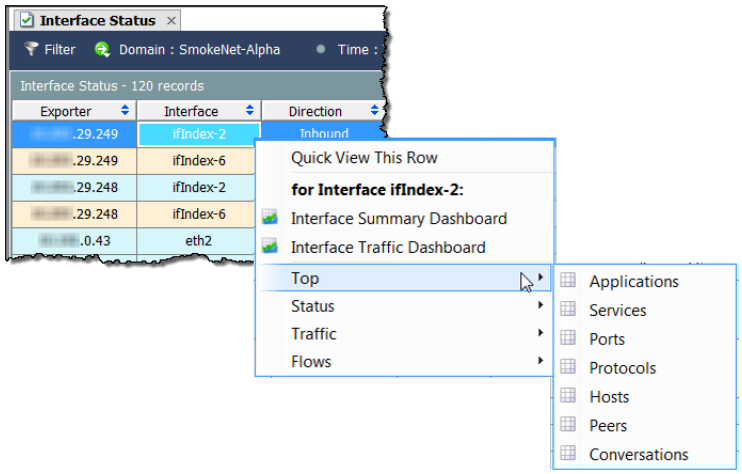


[インターフェイスでフィルタ(Filter by Interfaces)]チェックボックスをクリックして、チェックマークをはずします。次に、ドキュメントの現在のフィルタリング基準となっているエクスポータ(チェックマークが付いている唯一のエクスポータ)を見つけます。このエクスポータのチェックボックスをクリックしてチェックマークをはずし、[OK]をクリックします。[インターフェイスステータス(Interface Status)]ドキュメントにドメイン全体のトラフィックの統計情報が表示されるようになりました(次の例を参照)。

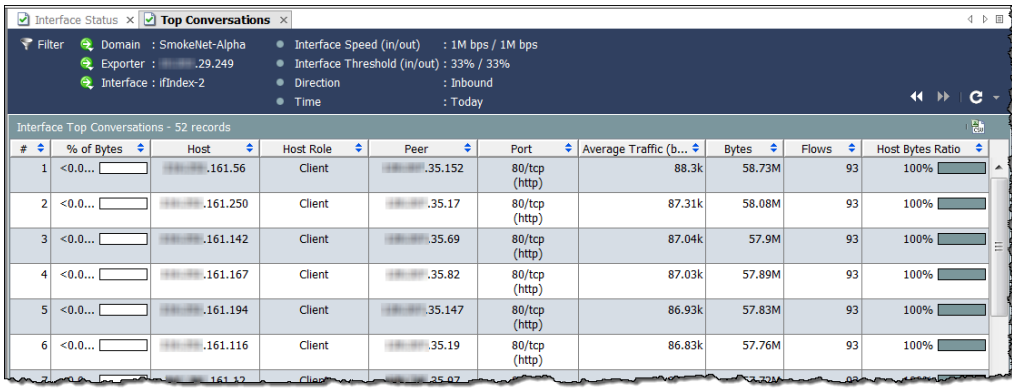


Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic ...	Maximum Utilization	Maximum Traffic ...
.29.249	ifIndex-2	Inbound	1M	60,900.24%	609M	62,304.15%	623.04M
.29.249	ifIndex-6	Outbound	1M	60,900.24%	609M	62,304.15%	623.04M
.29.248	ifIndex-2	Inbound	1G	61.22%	612.25M	62.1%	620.96M
.29.248	ifIndex-6	Outbound	1G	61.22%	612.25M	62.1%	620.96M
.0.43	eth2	Inbound	1G	3.07%	30.69M	8.76%	87.59M
.25.144	eth3	Inbound	1G	0.42%	4.22M	9.2%	92.03M
.0.249	Uplink (vSwitch0)	Inbound	1G	0.2%	2.01M	0.82%	8.15M
.25.158	Uplink (vSwitch0)	Inbound	1G	0.17%	1.68M	6.34%	63.36M
.0.249	ifIndex-13 (vSwitch0)	Outbound	1G	0.1%	1.01M	0.4%	4.02M
.0.249	ifIndex-14 (vSwitch0)	Outbound	1G	0.1%	968.1k	0.41%	4.12M
.0.43	eth3	Inbound	1G	0.08%	751.09k	0.34%	3.38M

インターフェイスの列内でインターフェイスを右クリックして、[トップ(Top)] を選択します。ポップアップ メニューが表示され、いくつかのオプションを選択できます。

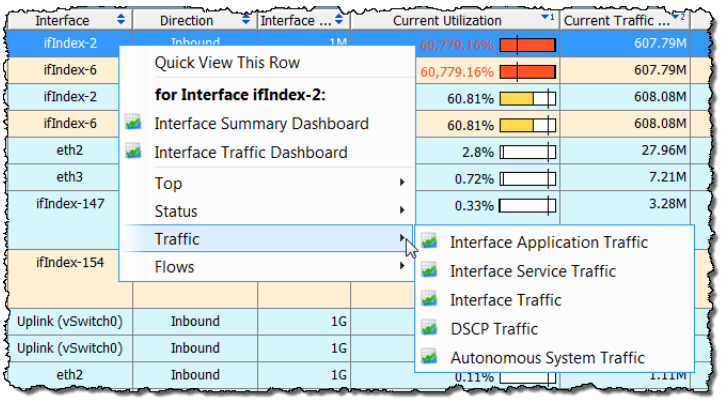


たとえば、[トップ(Top)] > [会話(Conversations)] を選択すると、[上位の会話(Top Conversations)] ドキュメントが表示されます(次の例を参照)。[上位の会話(Top Conversations)] ドキュメントには、上位の会話に従ってフロー データがリストされます。方向(フィルタ内で変更可能)は、選択した項目に対する受信トラフィック、選択した項目からの送信トラフィック、または選択した項目内のトラフィックを含むすべてのトラフィック(合計)がデータに含まれるかどうかを示します。



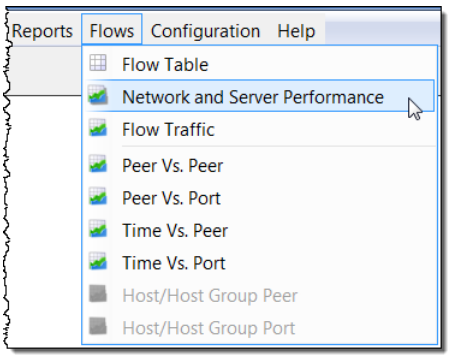
ヒント:
インターフェイスをダブルクリックすると、サマリー レポートを開くことができます。

列内で右クリックし、最初のポップアップ メニューで [トラフィック（Traffic）] を選択して、トラフィックのモニターリングに役立つ他の多数のドキュメントを検索することができます。

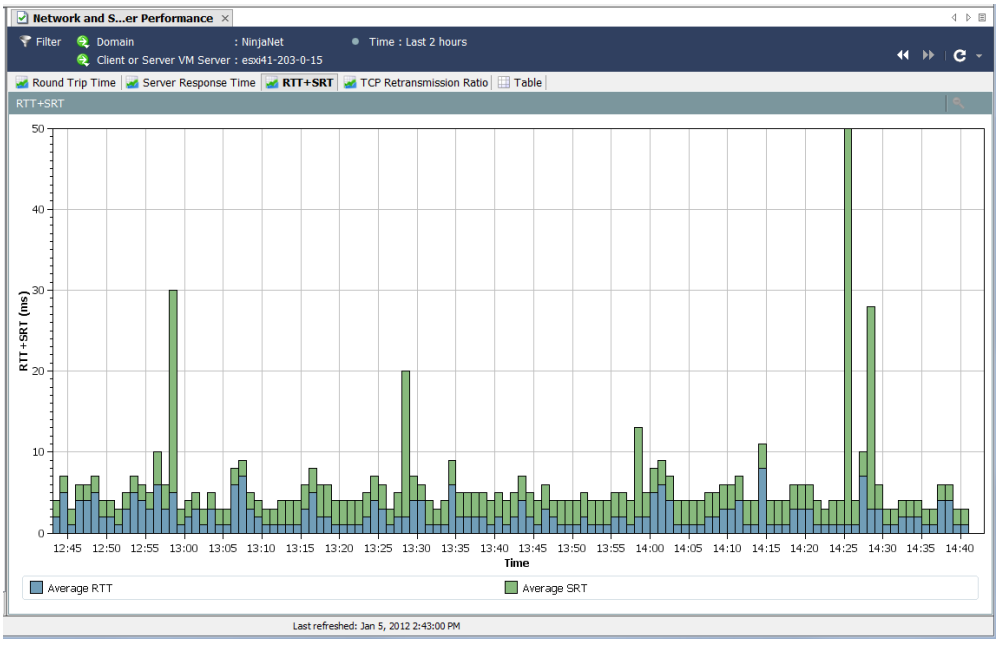


ネットワーク パフォーマンス

「低速なインターネット」に不満を持つ従業員がいるとします。[ネットワークおよびサーバーのパフォーマンス(Network and Server Performance)] ドキュメントを使用して、これらのタイプの問題を調査することができます。このドキュメントにアクセスするには、メインメニューで [フロー(Flows)] > [ネットワークおよびサーバーのパフォーマンス(Network and Server Performance)] を選択します。



(注):
このレポートを表示するには、このレポートに入力する特定の値を収集する Stealthwatch FlowSensor が必要です。

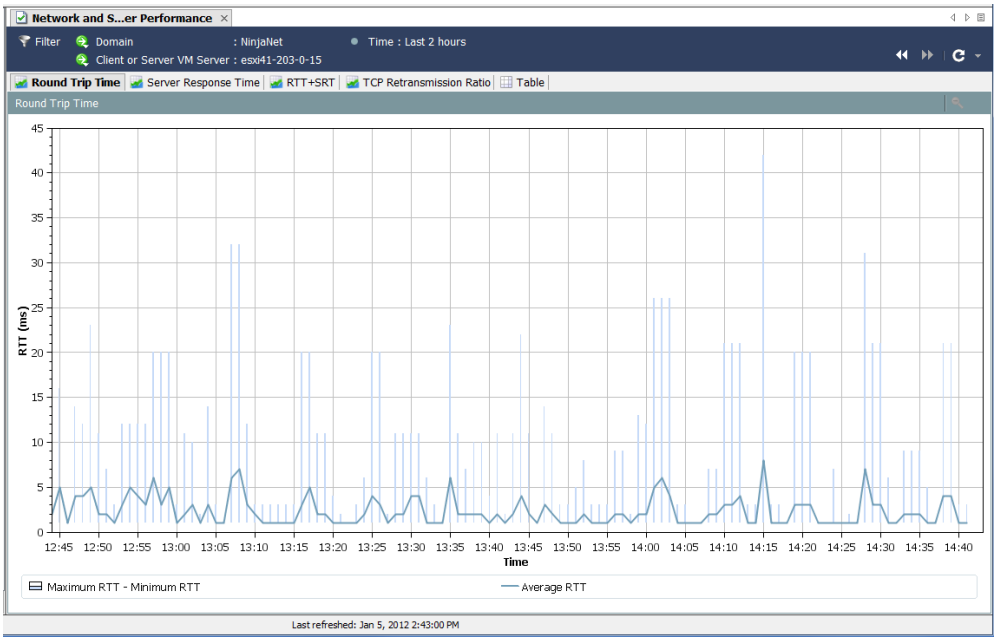


[ネットワークおよびサーバーのパフォーマンス(Network and Server Performance)] ドキュメントには、データベースに保存されたフローに関するさまざまなパフォーマンス データが表示されます。このデータを表示するには、ドキュメントの上部にある次のタブにアクセスします。

- [ラウンドトリップ時間(Round-Trip Time)]
- [サーバー応答時間(Server Response Time)]
- [RTT+SRT]
- [TCP 再送信比率(TCP Retransmission Ratio)]
- [テーブル(Table)]

[ラウンドトリップ時間(Round-Trip Time)]

[ラウンドトリップ時間(Round Trip Time)] タブには、フローのラウンドトリップ時間に関する統計情報がグラフィカルに表示されます。

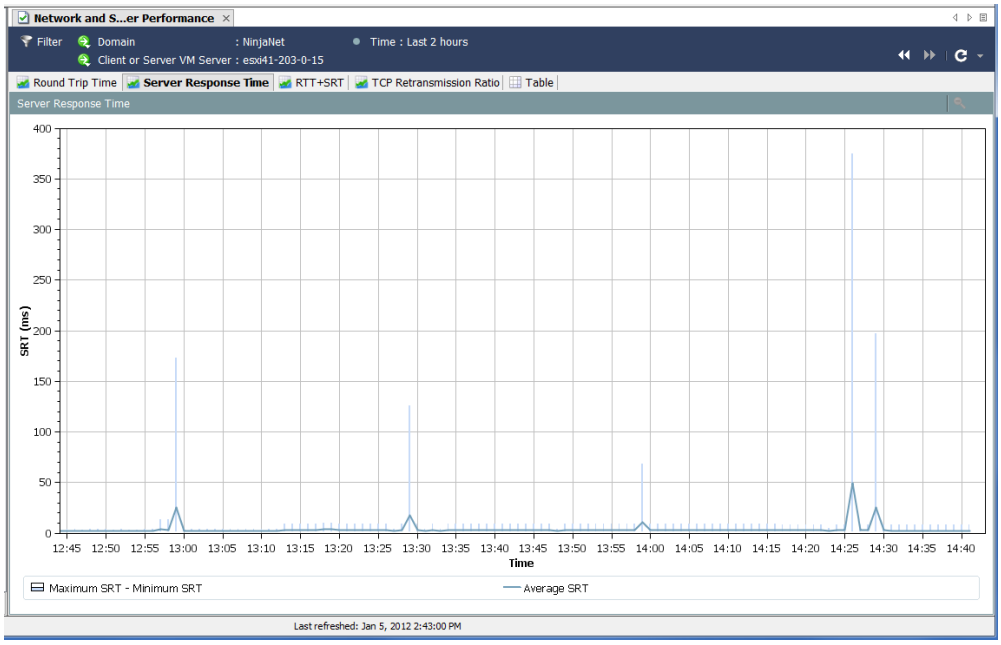


この機能は、離れているホスト グループ間のフローを完了するために必要な期間を測定する場合に役立ちます。この時間を設定するには、[フィルタ(Filter)] の [ホスト(Hosts)] ページを使用します。

グラフの下部にある濃い線は計算された RTT の平均値を表し、長く細い線は計算された毎分の最小 RTT および最大 RTT の間隔を表します。

[サーバー応答時間(Server Response Time)]

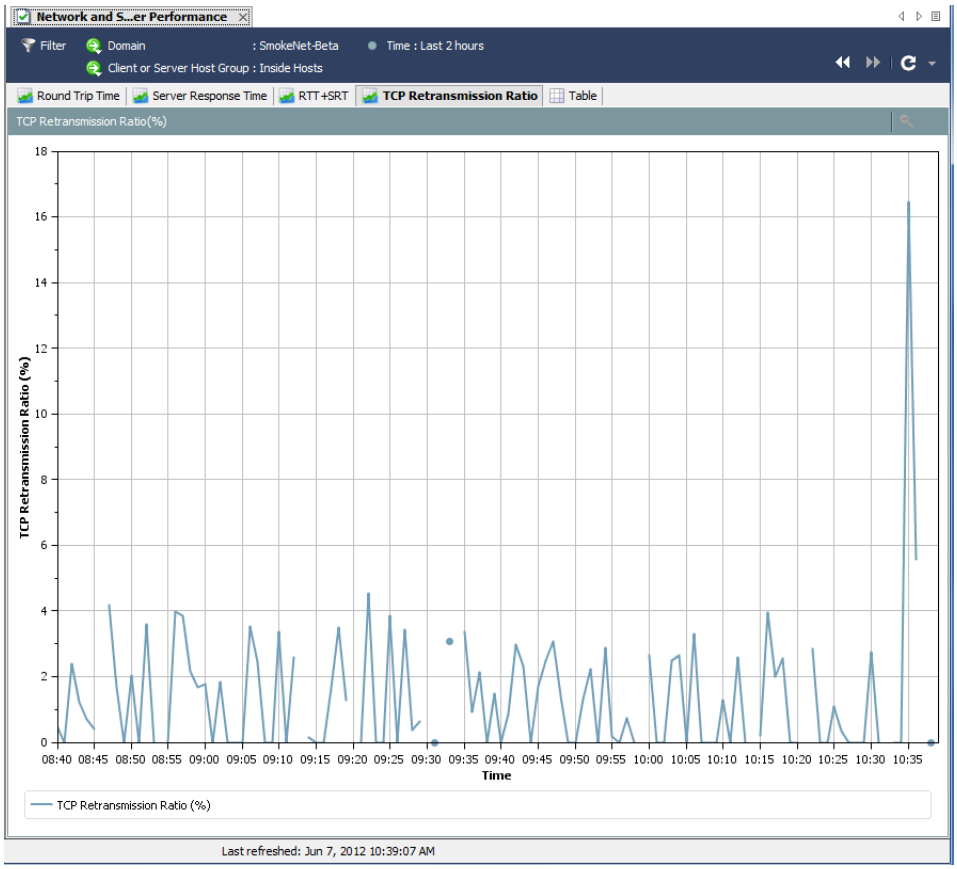
[サーバー応答時間(Server Response Time)] タブには、フローのサーバー応答時間(SRT)に関する統計情報がグラフィカルに表示されます。



この機能は、サーバーが要求に応答するための所要時間を測定する場合に便利です。たとえば、画面が「いつまでたっても読み込まれない」場合、ユーザーは Web ベース アプリケーションのパフォーマンス低下に不満を抱きます。このドキュメントを使用すると、サーバーの SRT を観察し、サーバーから取得したユーザー独自の SRT と平均 SRT を比較することができます。

[TCP 再送信比率(TCP Retransmission Ratio)]

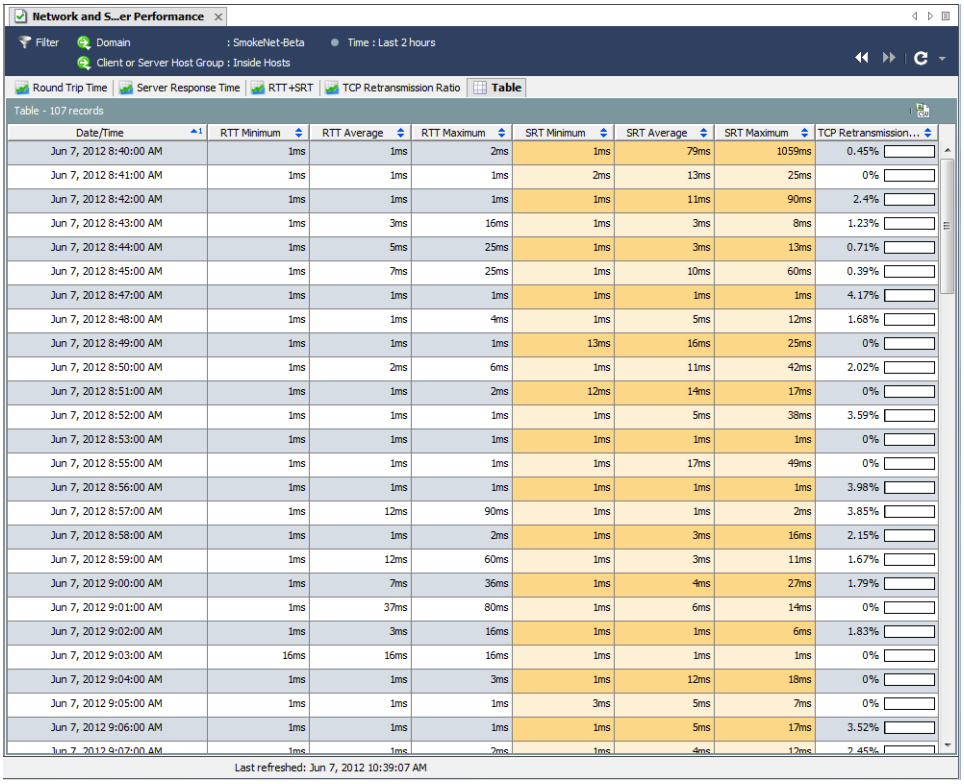
[ネットワークおよびサーバーのパフォーマンス(Network and Server Performance)] ドキュメントの [TCP 再送信比率(TCP Retransmission Ratio)] タブには、再送信されたパケットの割合がグラフィカルに表示されます。デフォルトでは、データの範囲は 2 時間、データ レコードの間隔は 1 分です。通常は、パケットが破損した場合、または失われた場合に再送信が行われます。



(注):
このドキュメントを使用できるのは、Stealthwatch FlowSensor からデータを受信している NetFlow 用 Stealthwatch フロー コレクタが使用されているドメインに限られます。

[テーブル(Table)]

[ネットワークおよびサーバーのパフォーマンス(Network and Server Performance)] ドキュメントの [テーブル(Table)] タブには、フローのパフォーマンス データがリストされます。デフォルトでは、データの範囲は 2 時間、データ レコードの間隔は 1 分です。



Date/Time	RTT Minimum	RTT Average	RTT Maximum	SRT Minimum	SRT Average	SRT Maximum	TCP Retransmission...
Jun 7, 2012 8:40:00 AM	1ms	1ms	2ms	1ms	79ms	1059ms	0.45%
Jun 7, 2012 8:41:00 AM	1ms	1ms	1ms	2ms	13ms	25ms	0%
Jun 7, 2012 8:42:00 AM	1ms	1ms	1ms	1ms	11ms	90ms	2.4%
Jun 7, 2012 8:43:00 AM	1ms	3ms	16ms	1ms	3ms	8ms	1.23%
Jun 7, 2012 8:44:00 AM	1ms	5ms	25ms	1ms	3ms	13ms	0.71%
Jun 7, 2012 8:45:00 AM	1ms	7ms	25ms	1ms	10ms	60ms	0.39%
Jun 7, 2012 8:47:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	4.17%
Jun 7, 2012 8:48:00 AM	1ms	1ms	4ms	1ms	5ms	12ms	1.68%
Jun 7, 2012 8:49:00 AM	1ms	1ms	1ms	13ms	16ms	25ms	0%
Jun 7, 2012 8:50:00 AM	1ms	2ms	6ms	1ms	11ms	42ms	2.02%
Jun 7, 2012 8:51:00 AM	1ms	1ms	2ms	12ms	14ms	17ms	0%
Jun 7, 2012 8:52:00 AM	1ms	1ms	1ms	1ms	5ms	38ms	3.59%
Jun 7, 2012 8:53:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	0%
Jun 7, 2012 8:55:00 AM	1ms	1ms	1ms	1ms	17ms	49ms	0%
Jun 7, 2012 8:56:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	3.98%
Jun 7, 2012 8:57:00 AM	1ms	12ms	90ms	1ms	1ms	2ms	3.85%
Jun 7, 2012 8:58:00 AM	1ms	1ms	2ms	1ms	3ms	16ms	2.15%
Jun 7, 2012 8:59:00 AM	1ms	12ms	60ms	1ms	3ms	11ms	1.67%
Jun 7, 2012 9:00:00 AM	1ms	7ms	36ms	1ms	4ms	27ms	1.79%
Jun 7, 2012 9:01:00 AM	1ms	37ms	80ms	1ms	6ms	14ms	0%
Jun 7, 2012 9:02:00 AM	1ms	3ms	16ms	1ms	1ms	6ms	1.83%
Jun 7, 2012 9:03:00 AM	16ms	16ms	16ms	1ms	1ms	1ms	0%
Jun 7, 2012 9:04:00 AM	1ms	1ms	3ms	1ms	12ms	18ms	0%
Jun 7, 2012 9:05:00 AM	1ms	1ms	1ms	3ms	5ms	7ms	0%
Jun 7, 2012 9:06:00 AM	1ms	1ms	1ms	1ms	5ms	17ms	3.52%
Jun 7, 2012 9:07:00 AM	1ms	1ms	2ms	1ms	4ms	12ms	2.45%

(注):

このドキュメントを使用できるのは、Stealthwatch FlowSensor からデータを受信している NetFlow 用 Stealthwatch フロー コレクタが使用されているドメインに限られます。

7

フロー分析

概要

特定のホストが侵害されたことが判明しました。当該ホストとの双方向の会話を「なかったことに」し、侵害の原因の疑いのあるホストを特定したいと思うでしょう。または、トラフィックが急増し、データを分析して、その急増の原因を突き止めたいと思うでしょう。あるいは、アラームが発生し、あなたのネットワークに対する脅威があるかを判断する必要があるでしょう。

フロー分析プロセスでは、ネットワークを保護するためにこれらの判断を行うことができます。この章では、フロー分析プロセスの概要を説明し、最も一般的な使用のシナリオをいくつか紹介します。

この章は、次の項で構成されています。

フロー フィルター

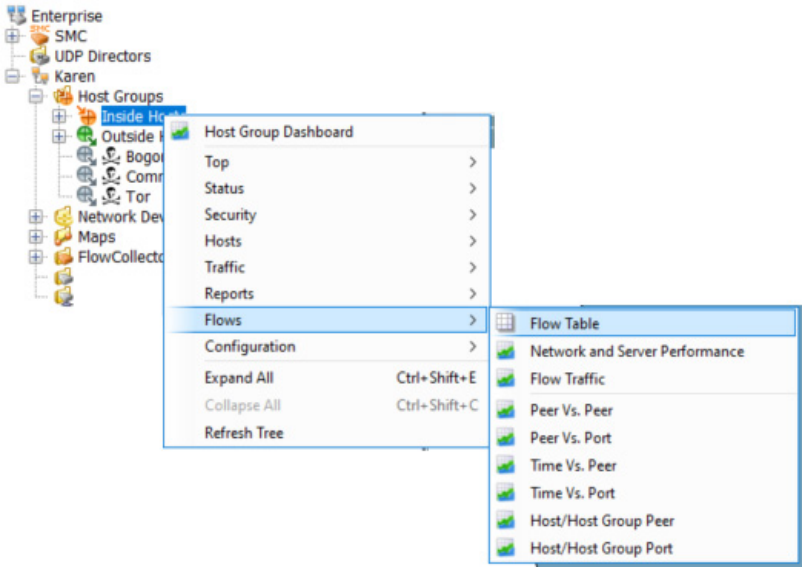
[フローフィルター(Flow Filter)] ダイアログボックスでは、確認したいフロー データを選択して、必要な結果を受け取るために、各種フィルタリングのレベルを設定できます。

フロー クエリの入力

フロー データのクエリを行うには、次の手順を実行します。

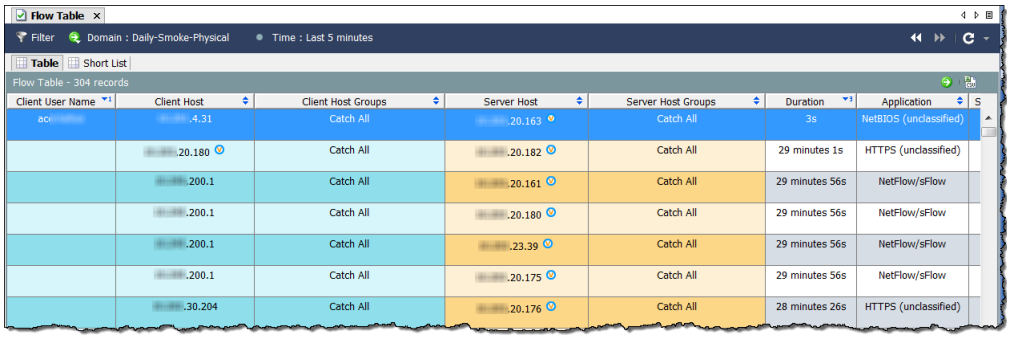
(注):
次の手順で説明するすべての設定を使用する必要はありません。

1. ドメイン、アプライアンス、ホスト グループまたはホストの IP アドレスを右クリックし、[フロー(Flow)] > [テーブル(Table)] を選択します。

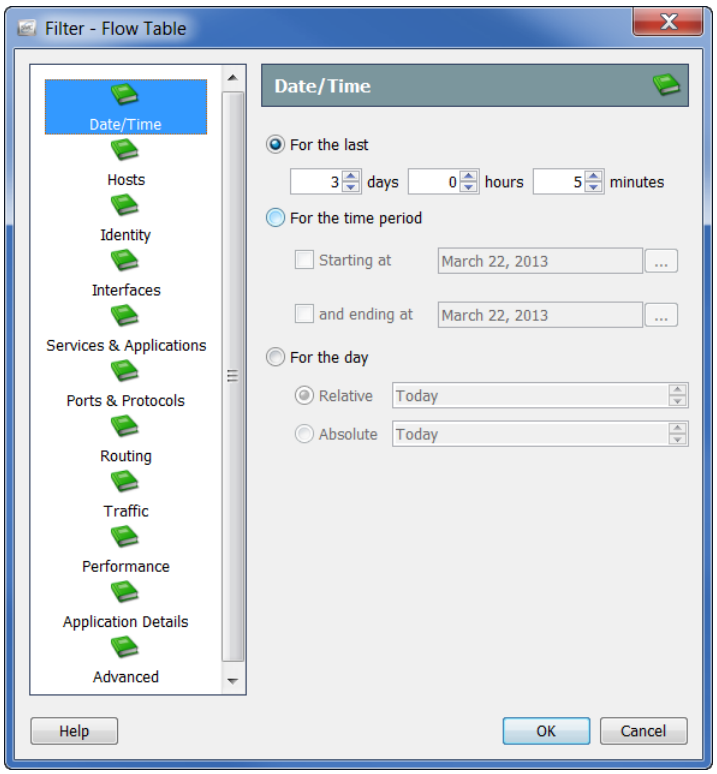


ヒント:
ポップアップ メニューから [フローテーブル(Flow Table)] をクリックする際に、キーボードで **Ctrl** を押すと、フィルタが最初に表示され、検索条件を絞り込むことができます。[OK] をクリックした後、入力した検索条件を使用してフロー テーブルが表示されます。

フロー テーブルが開きます。



2. フロー テーブルの左上角にある [フィルター(Filter)] ボタン をクリックして、[フィルター(Filter)] ダイアログを開き、まだ強調表示されていない場合は、[日時(Date/Time)] アイコンをクリックします。[日時(Date/Time)] ページが開きます。

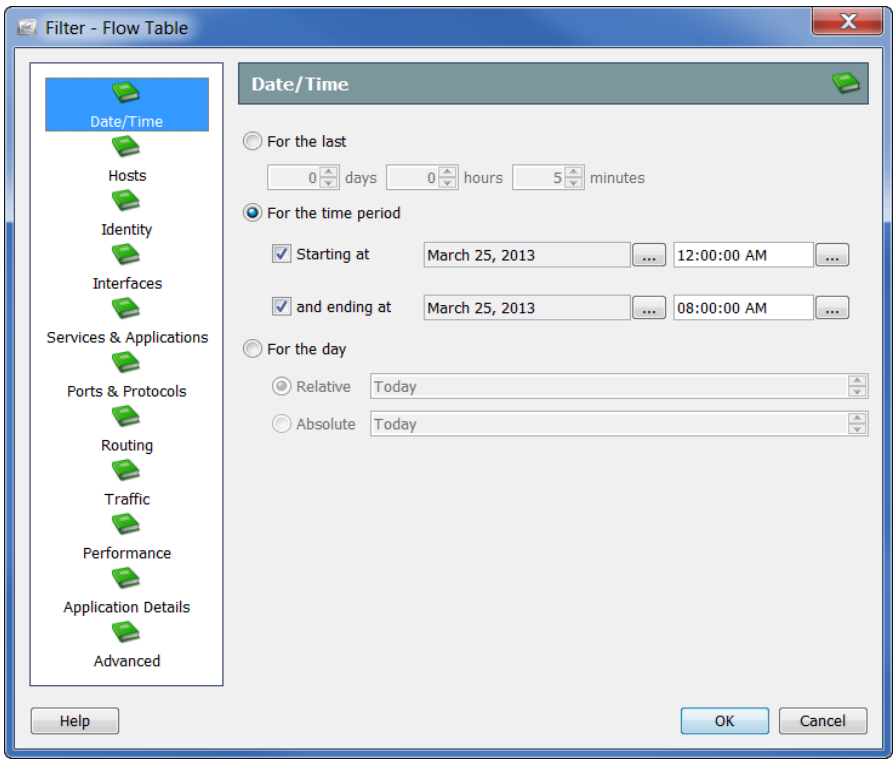


3. 正確な日時、範囲、またはフロー データをフィルター処理する相対設定を指定します。たとえば、特定の日の真夜中と午前 8 時の間のすべてのフローを表示したい場合は、次の手順を実行します。

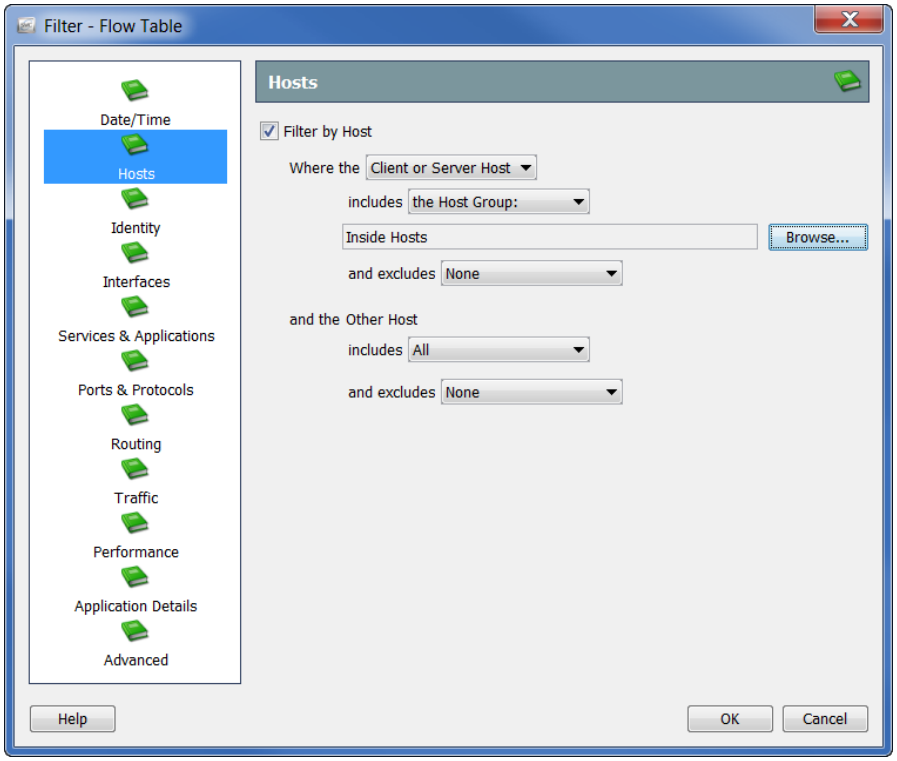
   a. [期間(For the time period)] オプションをクリックします。

   b. [開始日時(Starting at)] オプションをクリックし、フィルタ処理を開始する日付を入力し、時間フィールドに ***12:00:00*** と入力します。

c. [終了日時(and ending at)] オプションをクリックし、フィルタ処理を終了する日付を入力し、そのオプションに対する時間フィールドに ***08:00:00*** と入力します。

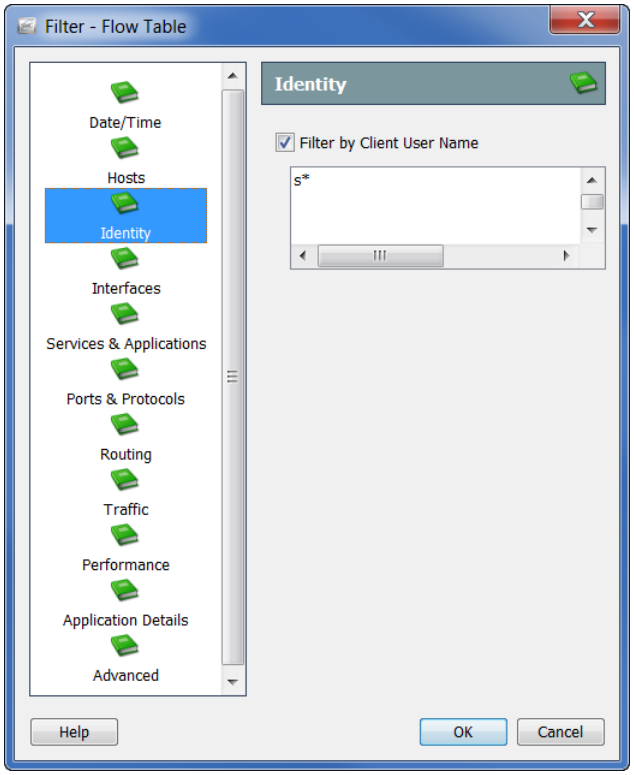


4. [ホスト(Hosts)] アイコンをクリックします。[ホスト(Hosts)] ページが開きます。



フロー データへのフィルター処理に使用したいホストを指定します。ホストグループ、IP アドレスの範囲(CIDR 形式を使用)、または、IP アドレスのリスト(カンマ区切り形式)を含めたり、除外することができます。

5. [ID（Identity）] アイコンをクリックします。[ID（Identity）] ページが開きます。



次の手順を完了することによって、フロー データをフィルター処理するユーザー名を指定します。

1. [クライアントユーザー名（Client User Name）] チェックボックスをクリックして、チェック マークを付けます。
2. 次の内容のいずれかをテキスト フィールドに入力します。
   - jdoe などの 1 つのユーザー名。
   - jdoe、jalpha、jbeta などの複数のユーザー名。名前を入力し、カンマで各名前を区切るか、各名前の後で **Enter** を押します（行ごとに 1 つの名前を入力します）。また、名前のカンマ区切り値一覧 (CSV) から、コピー アンド ペーストすることもできます。
   - ワイルド カードのある部分的な名前。ワイルド カードは、srh * や * doe などの任意の位置に入れることができます。1 つの名前に複数のワイルドカードを使用できます。

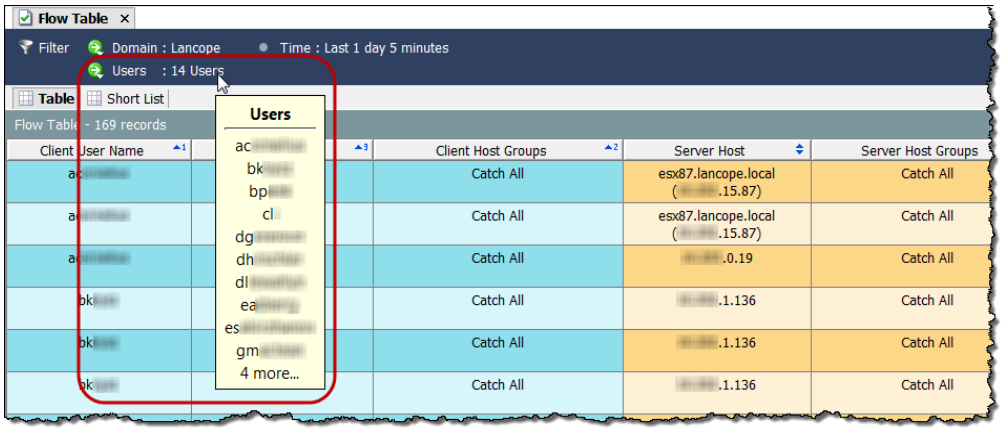
（注）：

- **このフィールドは、大文字と小文字が区別されません。**
- **ユーザー名には、|、+、=、?、“、<、>、(、)、:、; などの文字は使用できません。**

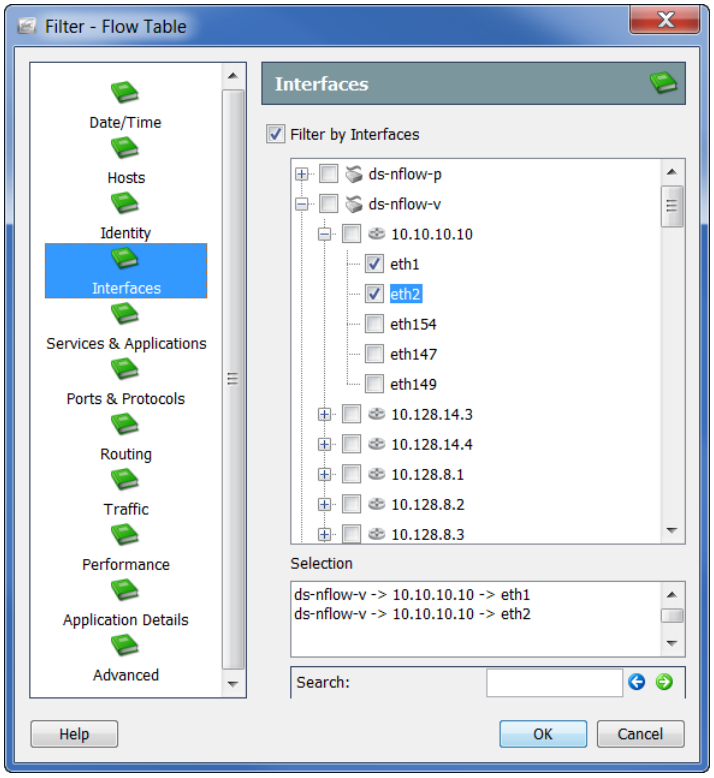
3. [OK] をクリックします。

結果は、[クライアントユーザー名 (Client User Name)] 列に表示されます。1 人のユーザーをフィルター処理した場合、そのユーザーの名前がヘッダーに表示されます。複数のユーザーをフィルター処理した場合、ヘッダーにユーザー名にフィルター処理したユーザー名の数が表示されます。このエントリにカーソルを合わせると、照会した最初の 10 人のユーザーの名前がポップアップ ウィンドウに一覧表示されます (次の画面を参照してください)。

最初の 10 名のユーザーの他、フィルター処理したユーザー名の数がポップアップ ウィンドウの下部に表示されます。下の例では、14 のユーザー名がフィルタ処理されているので、ポップアップ ウィンドウの下部には [あと 4 ユーザー... (4 more...)] が表示されます。が表示されます。

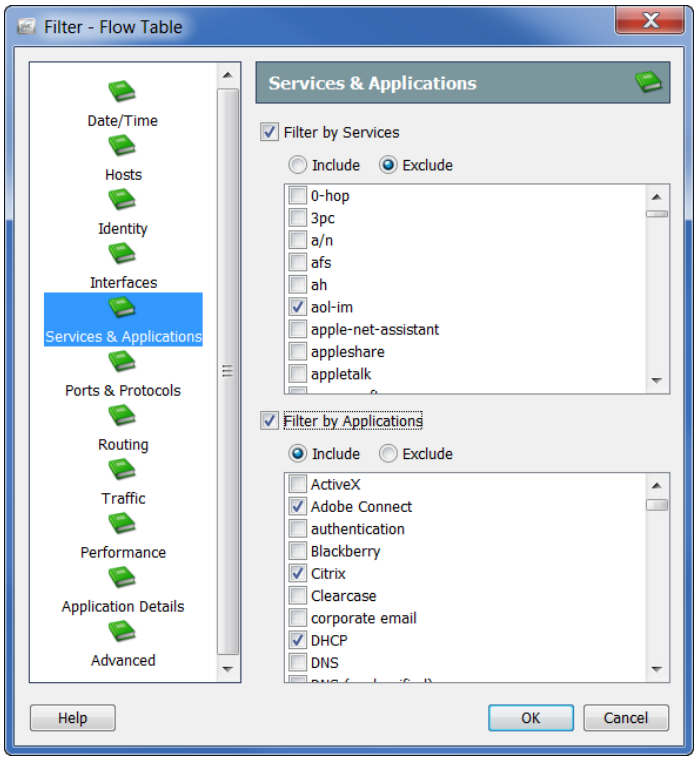


4. [インターフェイス(Interfaces)] アイコンをクリックします。[インターフェイス(Interfaces)] ページが開きます。



フロー データへのフィルター処理に使用したいインターフェイスを指定します。個々のインターフェイス、エクスポータ全体、または Stealthwatch アプライアンスをクリックして指定できます。

5. [サービスとアプリケーション(Services & Applications)] アイコンをクリックします。[サービスとアプリケーション(Services & Applications)] ページが開きます。

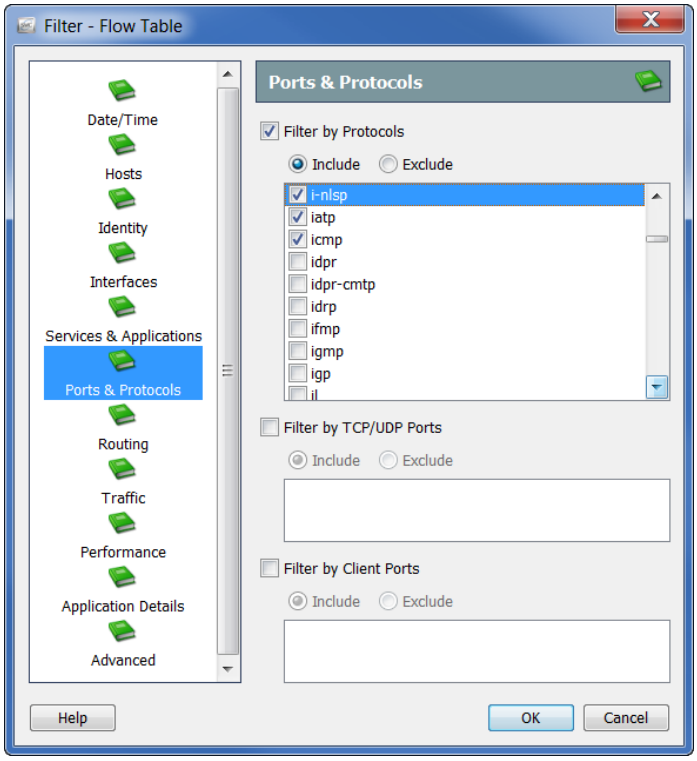


次のチェックボックスの一方または両方をクリックして、チェック マークを付け、フロー データのフィルター処理に使用したいサービスまたはアプリケーションを指定します。

- [サービスでフィルター処理(Filter by Services)]
- [アプリケーションでフィルター処理(Filter by Applications)]

[含める(Include)] または [除外(Exclude)] オプションのいずれかをクリックします。たとえば、Facebook を除くすべてにクエリを制限したいとします。この場合、[アプリケーションでフィルタ処理(Filter by Applications)] チェックボックスをクリックして、[除外(Exclude)] オプションをクリックし、[Facebook] チェックボックスをクリックして、チェック マークを付けます。

6. [ポートとプロトコル(Ports & Protocols)] アイコンをクリックします。[ポートとプロトコル(Ports & Protocols)] ページが開きます。

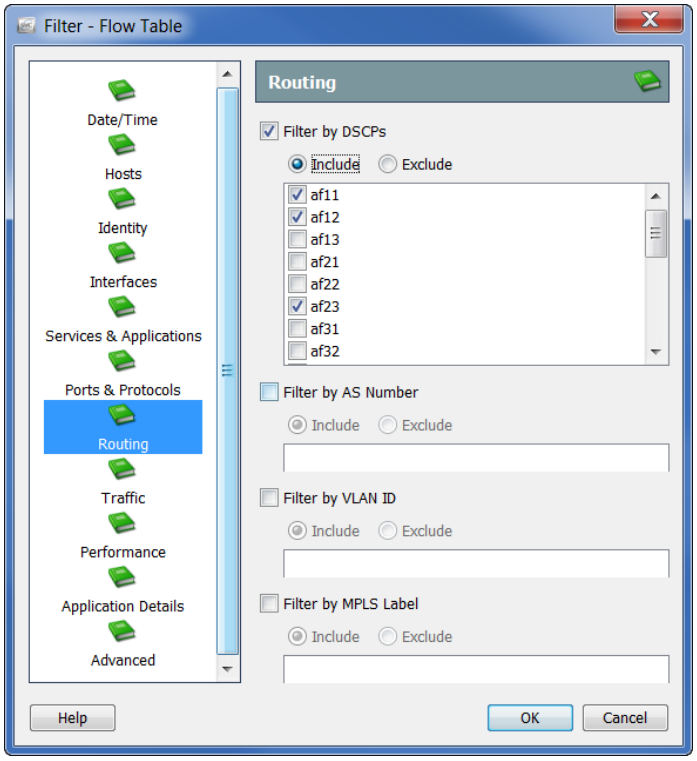


次のチェックボックスのいずれかまたはすべてをクリックして、チェック マークを付け、フロー データのフィルター処理に使用したいポートとプロトコルを指定します。

- [プロトコルでフィルター処理(Filter by Protocols)]
- [TCP/UDP ポートでフィルター処理(Filter by TCP/UDP Ports)]
- [クライアントポートでフィルター処理(Filter by Client Ports)]

[含める(Include)] または [除外(Exclude)] オプションのいずれかをクリックして、クエリをさらにカスタマイズします。

7. [ルーティング(Routing)] アイコンをクリックします。[ルーティング(Routing)] ページが開きます。

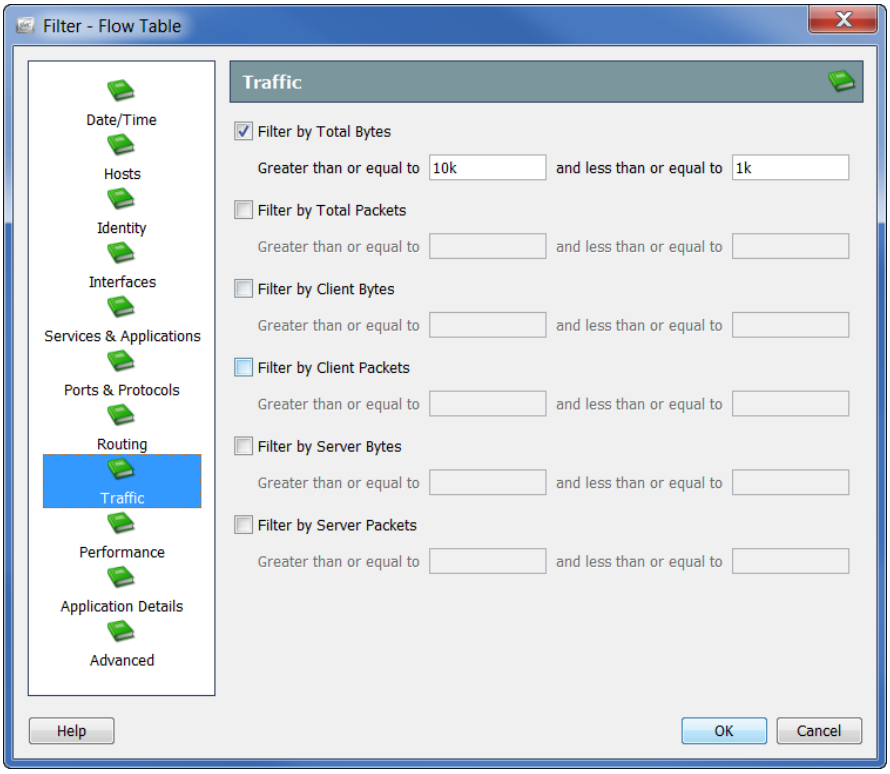


次のチェックボックスのいずれかまたはすべてをクリックして、チェック マークを付け、フロー データのフィルター処理に使用したいパラメータを指定します。

- [DSCP でフィルター処理(Filter by DSCPs)]
- [AS 番号でフィルター処理(Filter by AS Number)]
- [VLAN ID でフィルター処理(Filter by VLAN ID)]
- [MPLS ラベルでフィルター処理(Filter by MPLS Label)]

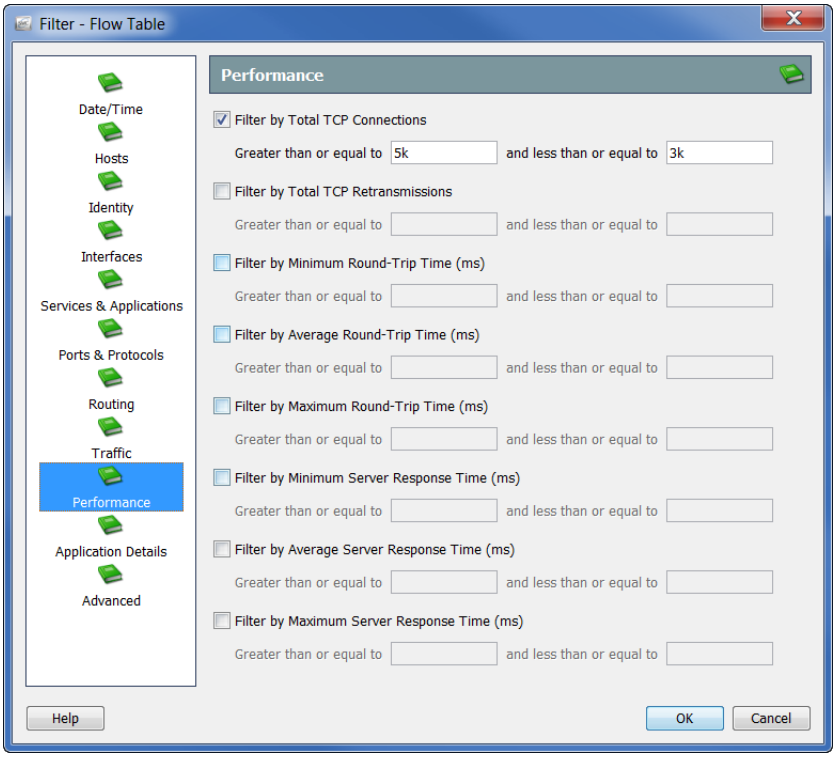
[含める(Include)] または[除外(Exclude)] オプションのいずれかをクリックして、クエリをさらにカスタマイズします。

8. [トラフィック(Traffic)] アイコンをクリックします。[トラフィック(Traffic)] ページが開きます。



フィルター処理するトラフィック データの種類とサイズを指定します。

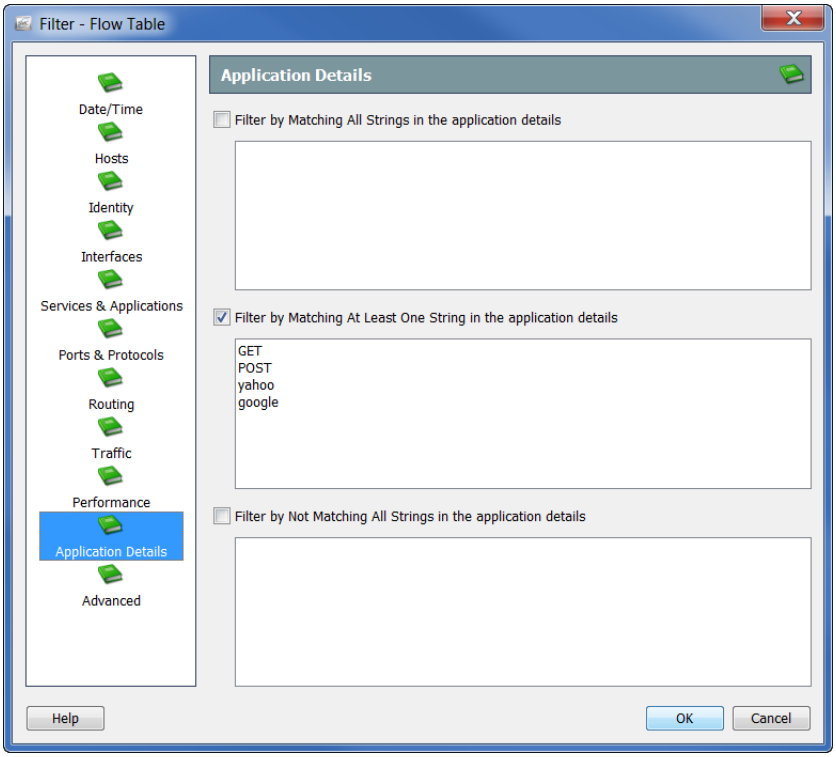
9. [パフォーマンス(Performance)] アイコンをクリックします。[パフォーマンス(Performance)] ページが開きます。



フィルター処理するパフォーマンス データの種類とサイズを指定します。

(注):
[パフォーマンス(Performance)] ページのすべての値には、Stealthwatch FlowSensor によって、この情報を収集および格納する必要があります。

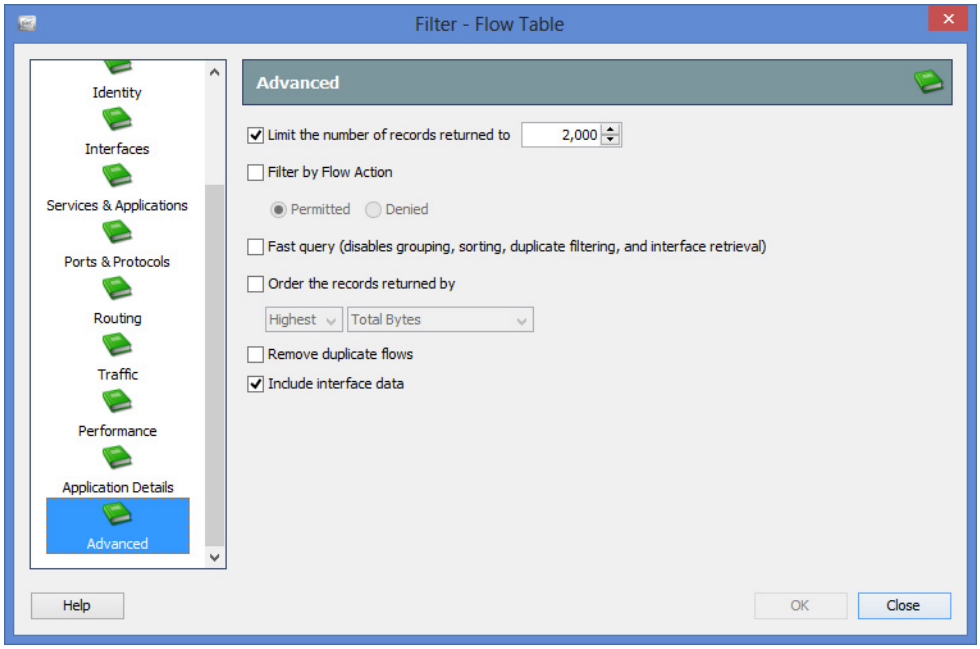
10. [アプリケーション詳細(Application Details)] アイコンをクリックします。[アプリケーション詳細(Application Details)] ページが開きます。



フロー データをフィルター処理するペイロードの情報を指定します。

[アプリケーション詳細(Application Details)] ページのすべての値には、FlowSensor または Flexible NetFlow 内でのペイロードのエクスポートによって、この情報を収集および格納する必要があります。

11. [詳細(Advanced)] アイコンをクリックします。[詳細(Advanced)] ページが開きます。



クエリーをフロー レコードの最大数に制限することができます。(たとえば、データを取得する前にサーバー上で)データをどのように並び替えするか、および結果から重複フローを削除するかどうかも指定できます。

(注):

- [重複フローを削除(Remove duplicate flows)] オプションは、複数のフロー コレクタがある場合にのみ関連があります。1 つのフロー コレクターが自動的に重複解除します。
- インターフェイス データを表示する必要がない場合、[インターフェイスデータを含める(Include interface data)] チェックボックスをクリックして、チェック マークをはずします。これにより、すばやくデータを収集できます。

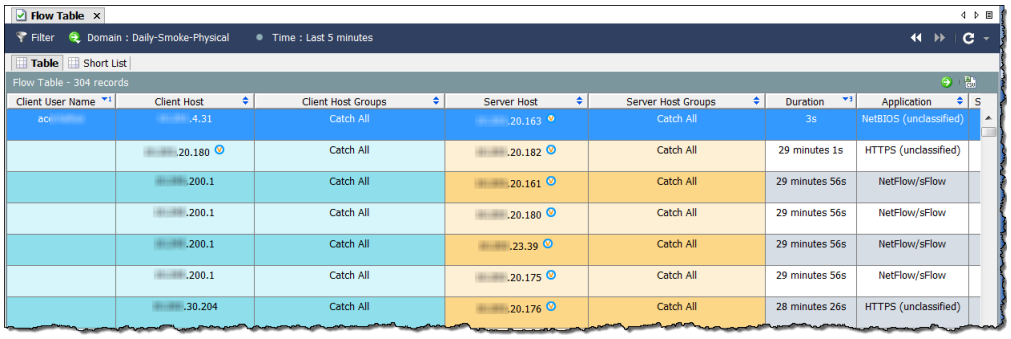
12. [OK] をクリックして、フィルタ処理を実行します。フロー クエリーが送信され、収集したデータがフロー テーブル ドキュメントに表示されます。

次にフロー テーブルにアクセスする際に、指定したフィルター設定のみが、[詳細(Advanced)] ページで有効のままになります。[フィルタ - フローテーブル(Filter - Flow Table)] 内のその他のページでフィルターの設定は維持されません。

フロー テーブルのタブ

[テーブル(Table)] タブ

[フローテーブル(Flow Table)] ドキュメント上にある [テーブル(Table)] タブには、[フィルタ - フローテーブル(Filter - Flow Table)] で指定したオプションに基づいてデータが表示されます。



(注):

ドキュメントの右上隅にある [ドキュメントに移動(Go to Document)] ボタン をクリックして、同じフロー データを使用している他のドキュメントを表示することができます。

インポートしたファイルは、元のアプライアンスやドメイン情報を含んでいないため、この情報を必要とするポップアップ メニュー オプションは、インポートしたフロー ファイルに使用できません(灰色表示になっています)。

(注):

フローファイルのインポートに関する詳細については、Stealthwatch デスクトップクライアントのオンラインヘルプにある「フロー ファイルのインポート方法」を参照してください。

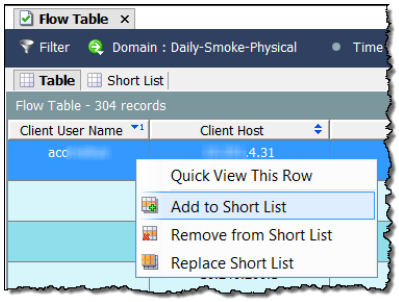
テーブルに表示する列を変更するには、見出しを右クリックし、ポップアップ メニューから目的の列を選択します。名前の横にチェック マークが付いた見出しは、ドキュメントに表示されていることを示しています。

[ショートリスト(Short List)] タブ

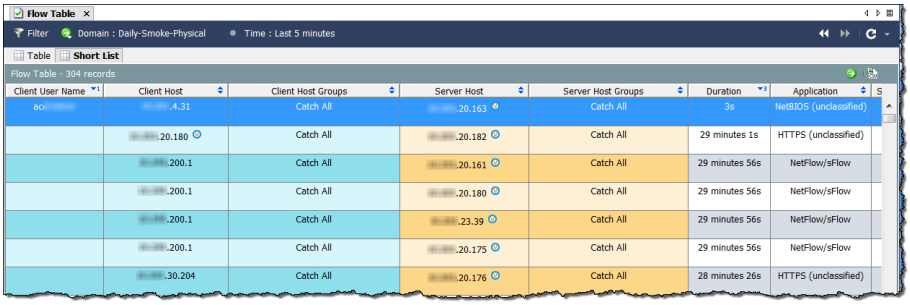
[ショート リスト(Short List)] タブと [テーブル(Table)] タブは同じ構成です。一方で行った変更は、自動的に他方に反映されます。

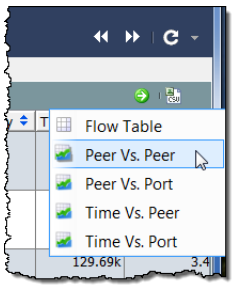
[フローテーブル(Flow Table)] ドキュメント上の [ショートリスト(Short List)] タブでは、フロー テーブルの [テーブル(Table)] ページに表示されるフロー データのサブセットを表示することができます。たとえば、[テーブル(Table)] タブは、数千のフローのレコードを表示できますが、より詳細な分析のために、行数を絞って確認するとよい場合があります。ショート リスト機能では、見やすくするために、特定の行を選択することができます。

[テーブル(Table)] タブで行を右クリックし、右側の例に示すように、[ショートリストに追加(Add to Shortlist)] を選択できます。



フローを表示するには、[ショートリスト(Short List)] タブをクリックして、[フローショートリスト(Flow Shortlist)] を開きます。選択した行は、このドキュメントに表示されます。





データのサブセットをグラフ表示するには、[ドキュメントに移動(Go to Document)] ボタン をクリックして、ポップアップ メニューから希望する分析の種類(たとえば、ピアツーピア)をクリックします。

[フィルタ - フローテーブル（Filter - Flow Table）] で収集したすべてのデータではなく、そのホストに対するデータのみが [ショートリスト（Short List）] に表示されます。

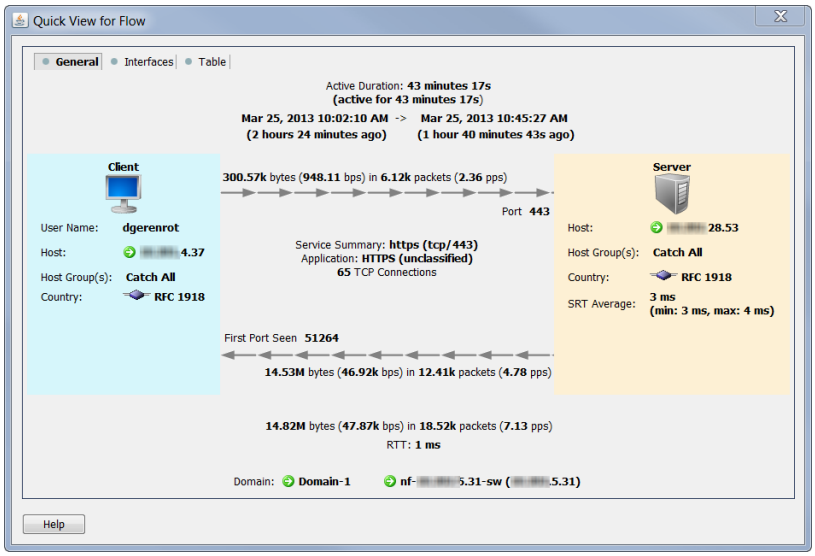
クイック ビュー

[クイックビュー(Quick View)] ダイアログは、表形式のデータをグラフ表示する、迅速で簡単な方法を提供します。また、その他のドキュメントのフィルター処理されたビューにすばやく移動できます。

[クイックビュー(Quick View)] ダイアログボックスを表示するには、テーブルのセルをクリックし、スペースバーを押します。ダイアログを非表示にするには、再度スペースバーまたは Esc キーを押します。

次の例に示すように、[クイックビュー(Quick View)] ダイアログは、次のタブのデータを表示します。

- [全般(General)]
- [インターフェイス(Interfaces)]
- [テーブル(Table)]



キーボードの Alt キーと共に ← 、または → キーを押すことで、タブ間を移動できます。

([クイックビュー(Quick View)] ダイアログを開いたまま)キーボードの Alt キーと共に ↑ 、または ↓ キーを押すことで、フロー間を移動できます。

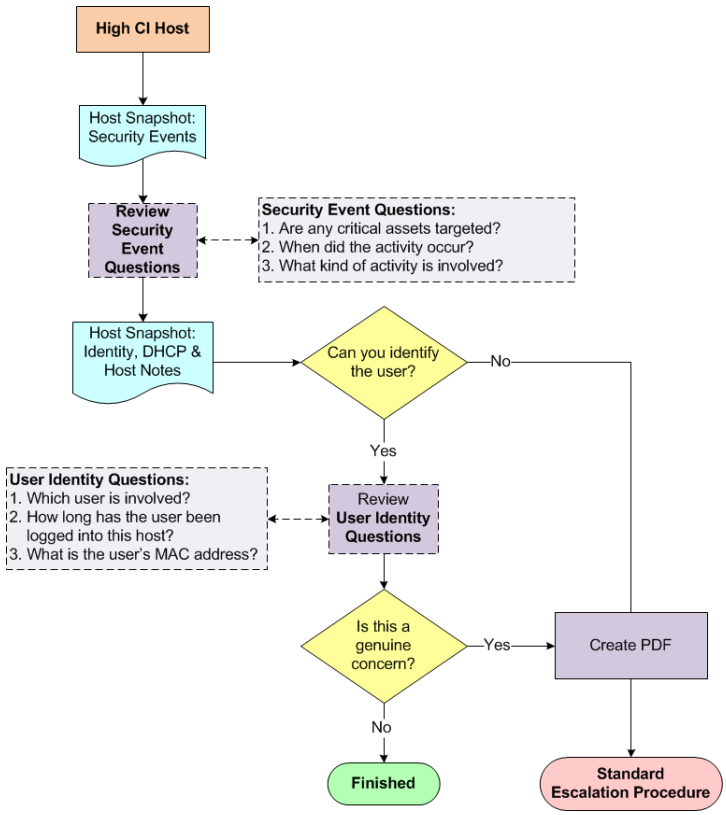
ヒント:
他のテーブルに適用される同じナビゲーション機能(たとえば、他の文書への掘り下げ)もここで適用されます。

フロー分析シナリオ

フロー分析プロセスについて学んだので、いくつかの一般的なシナリオを紹介します。

高懸念インデックス ホスト

高 CI ホストは、疑わしいフロー アクティビティ（セキュリティ イベント）のソースであるホストです。次の図は、脅威が本物かどうかを判定するのに使用できるワークフローを示しています。



ワークフロー概要

次の手順は、上記のワークフロー図に示す手順の概要について説明しています。

1. ソース ホストに対して、ホスト スナップショットの [セキュリティ イベント(Security Events)] ページを開いて、詳細を確認します。次項「セキュリティ イベント アクティビティ(ホスト スナップショット)の検査」を参照してください。
2. [ID と DHCP、ホスト ノート(Identity, DHCP & Host Notes)] タブをクリックします。
3. ユーザーを特定することができますか。
   - 「はい」の場合、手順 4 に進みます。
   - 「いいえ」の場合、手順 6 に進みます。
4. ソース ホストにログインしているユーザーの情報を確認します。「ユーザー ID 情報(ホスト スナップショット)を調べる」(163 ページ)を参照してください。
5. 収集した情報に基づいて、このアクティビティが本当の懸念のように見えますか。
   - 「はい」の場合、または不明な場合は、手順 6 に進みます。
   - 「いいえ」の場合は、ここで終了します。
6. ホスト スナップショットの PDF を作成し、あなたの組織の標準エスカレーション手順に従ってエスカレートします。

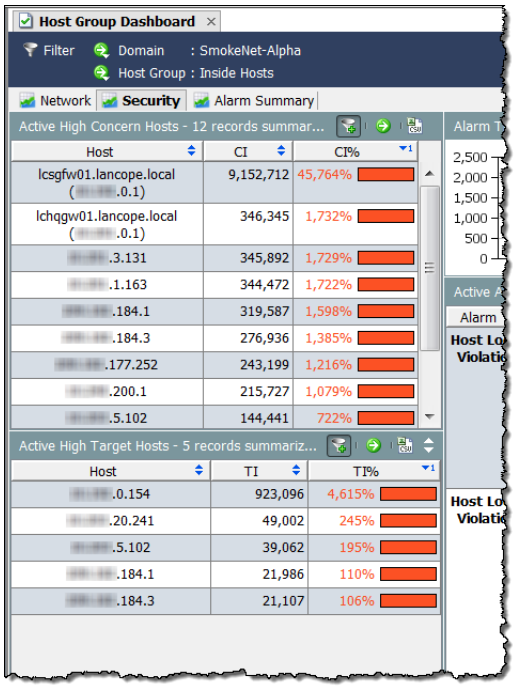
セキュリティ イベント アクティビティ(ホスト スナップショット)の検査

高 CI ホストは、マルウェアに感染するか、何らかの形で侵入されるおそれがあります。SMC は、高 CI ホストを簡単に識別することができる、以下を含むいくつかの方法を提供します。

- リスク インデックス
- アラーム テーブル(アラームが発生した場合)
- ホスト グループ ダッシュボードの [セキュリティ(Security)] ページ

このワークフローは、ホスト グループ ダッシュボードの [セキュリティ(Security)] ページから調査を開始します。高 CI ホストのセキュリティ イベント アクティビティを調べるには、次の手順を実行します。

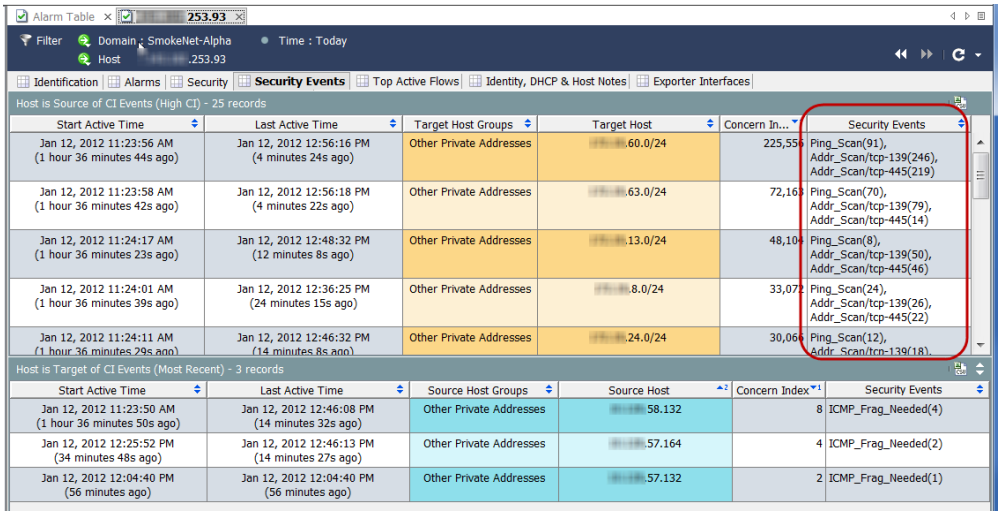
1. ホスト グループ ダッシュボードで、[セキュリティ(Security)] タブをクリックします。[アクティブな高懸念ホスト(Active High Concern Hosts)] と [アクティブな高対象ホスト(Active High Target Hosts)] のセクションに、特定のホスト グループ ダッシュボードに関連付けられているホスト グループに対する高 CI ホストと高 TI ホストが一覧表示されます。



2. 適切なホスト IP アドレスをダブルクリックして、そのホスト スナップショットを開きます。

ヒント：
IP アドレスが分かっている場合は、グローバル検索機能を使用して、ホスト スナップショットを検索することもできます。

3. [セキュリティイベント（Security Events）] タブをクリックします。
4. ホストが [セキュリティイベントのソース（高 CI）（Source of Security Events (High CI)）] セクションにある場合、[セキュリティイベント（Security Events）] 列のエントリを確認します（次の例を参照してください）。次の質問に回答します。
   - すべての重要な資産が対象ですか。
   - アクティビティはいつ発生しましたか。
   - どのようなアクティビティが必要ですか。



(注):

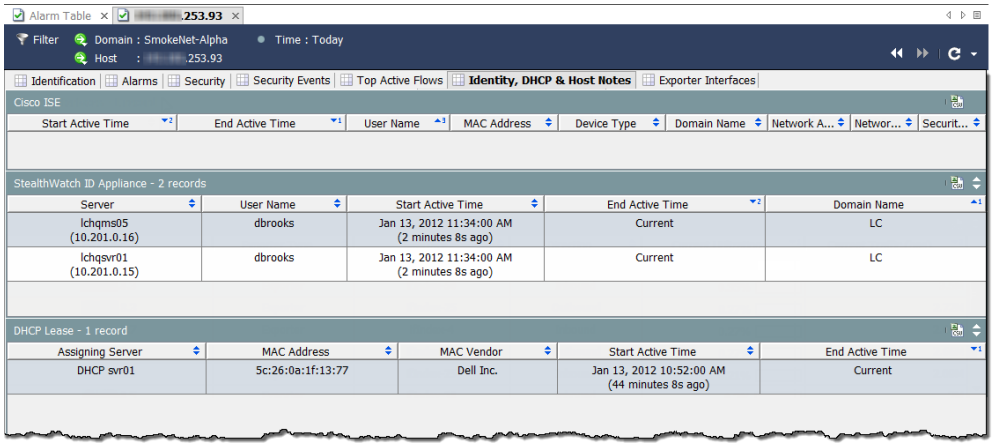
特定のセキュリティイベントの詳しい説明については、Stealthwatch デスクトップクライアントのオンラインヘルプにある「セキュリティイベント」を参照してください。

5. 次のセクションで説明するように、ユーザーの ID 情報を確認します。

ユーザー ID 情報(ホスト スナップショット)を調べる

高 CI ホストのセキュリティ イベント アクティビティを理解したら、次の手順を完了して、そのホストにログインしているユーザーの ID を調べます。

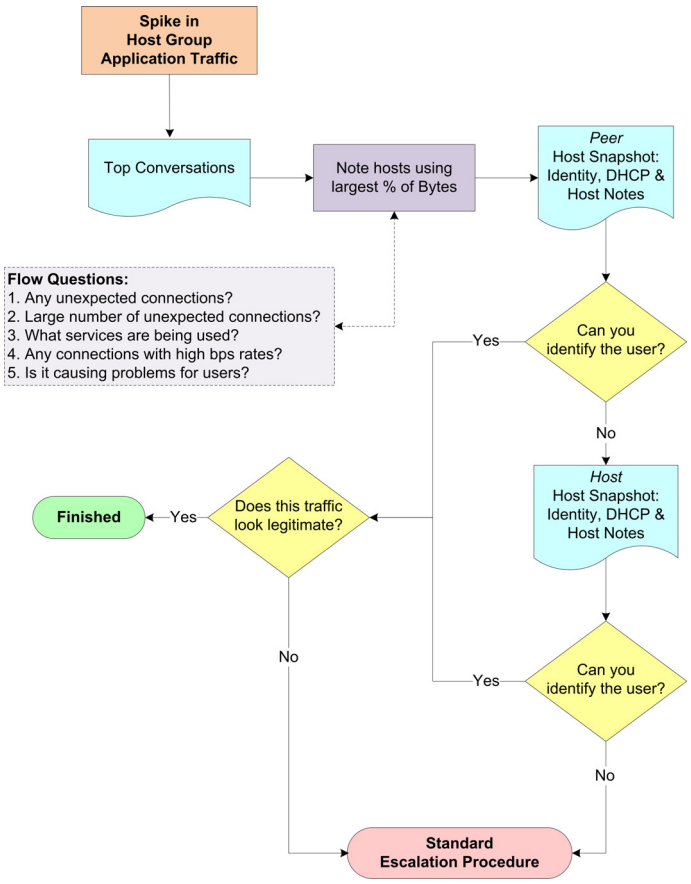
1. ホスト スナップショットで、[ID と DHCP、ホスト ノート (Identity, DHCP & Host Notes)] タブをクリックします。



2. 任意のユーザー情報を見ますか。
   - 「はい」の場合、手順 3 に進みます。
   - 「いいえ」の場合、手順 5 に進みます。
3. 次の質問を念頭に置いて、ユーザー情報を確認します。
   - どのユーザーがこのホストにログインしていますか。
   - どれくらいの時間、ログインしていましたか。
   - ユーザーの MAC アドレスは何ですか。
4. このアクティビティは、このホストについて収集した情報に基づいて、本当の懸念のように見えますか。
   - 「はい」の場合、または不明な場合は、手順 5 に進みます。
   - 「いいえ」の場合は、ここで終了します。
5. ホスト スナップショットの PDF を作成し、あなたの組織の標準エスカレーション手順に従ってエスカレートします。

アプリケーション トラフィックの急激な増加

ネットワークの 1 つのエリア内でトラフィックが急激に増加した場合、次の図に示すワークフローを使用して、この急激な増加の原因や、注意するべきかどうかを決定します。



ワークフロー概要

SMC では、次のようなトラフィックの急激な増加を確認できるいくつかの場所を提供しています。

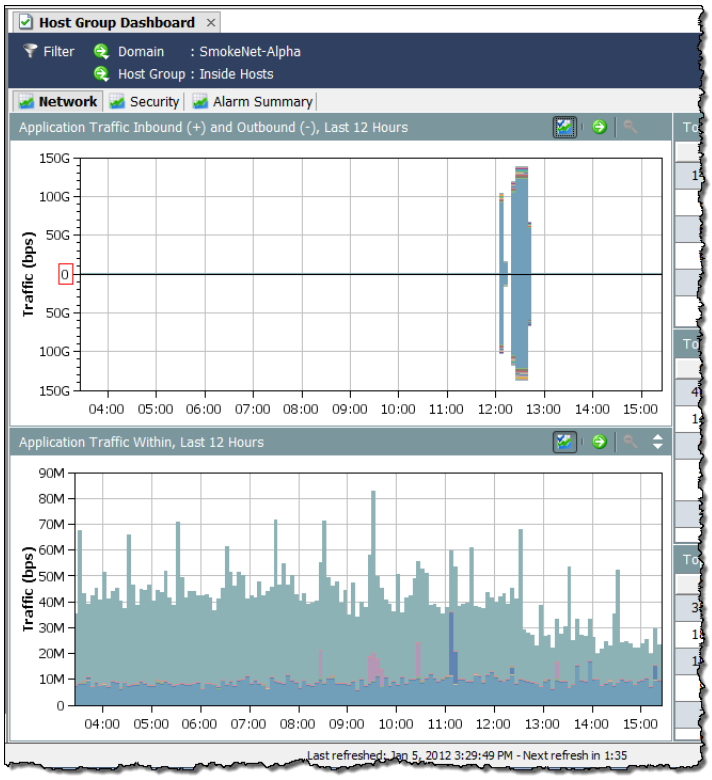
- [トラフィック(Traffic)] メニューを介してアクセスすることができるトラフィック グラフ
- ホスト グループ ダッシュボードの [ネットワーク(Network)] ページ

このワークフローは、[ネットワーク(Network)] ページから調査を開始します。次の手順は、上記のワークフロー図に示す手順の概要について説明しています。

1. [ネットワーク(Network)] ページで、トラフィックの急激な増加が進む方向を決定します。「関係するホストを特定」(168 ページ)を参照してください。
2. トラフィックの急激な増加をダブルクリックして、[上位の会話(Top Conversations)] ドキュメントを開き、どのホストのペアが指摘した方向にある大半の帯域幅を使用しているかを特定します。「関係するホストを特定」(168 ページ)を参照してください。
3. 上記の特定されたホストのペアについて、次の内容を確認します。
   - 予期しない接続(たとえば、不正なホスト グループまたはサーバー)はありますか。
   - 予期しない接続は数多くありますか。
   - どのポートが使用されていますか。
   - 大量のトラフィックが送信または受信されていますか。
   - 高ビットレートの接続はありますか。
   - この急激な増加は、ネットワークに関するユーザーの苦情と相関関係がありますか。
4. ピアに対して、ホスト スナップショットの [ID と DHCP、ホスト ノート(DHCP & Host Notes)] ページを開きます。「関係するユーザーを特定」(169 ページ)を参照してください。
5. 関連するユーザーを特定できますか。
   - 「はい」の場合、手順 8 に進みます。
   - 「いいえ」の場合、手順 6 に進みます。
6. ホストに対して、ホスト スナップショットの [ID と DHCP、ホスト ノート(DHCP & Host Notes)] ページを開きます。「関係するユーザーを特定」(169 ページ)を参照してください。
7. 関連するユーザーを特定できますか。
   - 「はい」の場合、手順 8 に進みます。
   - 「いいえ」の場合、手順 9 に進みます。
8. このトラフィックは、正当なアクティビティに見えますか。
   - 「はい」場合、または不明な場合は、手順 9 に進みます。
   - 「いいえ」の場合は、トラフィックの急激な増加を無視できます。
9. これまで収集した情報を収集して、組織の標準エスカレーション手順に従ってエスカレートします。

トラフィックの方向を特定

ホスト グループ ダッシュボードは、その [ネットワーク(Network)] タブで、ホスト グループ アプリケーション トラフィックの最も包括的なビューを提供します。



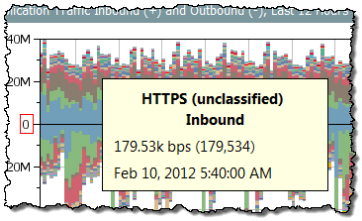
[アプリケーションの受信トラフィック(+)と送信トラフィック(-)(Application Traffic Inbound (+) and Outbound (-))] と [アプリケーションの内部トラフィック(Application Traffic Within)] グラフを見て、トラフィックに急激な増加があるかを直ちに確認し、トラフィックがどの方向に移動しているかを判定します。

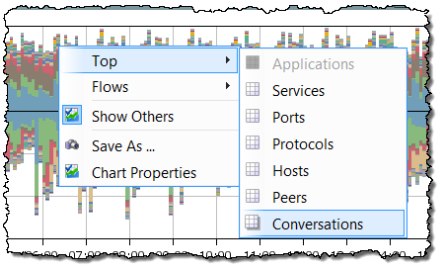
[アプリケーションの受信トラフィック(+)と送信トラフィック(-)(Application Traffic Inbound (+) and Outbound (-))] グラフは、[ホストグループ内(Inside Host Groups)] から [ホストグループ外(Outside Host Groups)]、またはその逆に移動しているトラフィックを示しています。受信トラフィックは、ゼロ(0)の行を越えているように見えます。送信トラフィックは、ゼロ(0)の行未満のように見えます。

[アプリケーションの内部トラフィック(Application Traffic Within)] グラフは、ネットワーク内のサブホスト グループ(内部ホスト グループ間のみを通過する)トラフィックを示しています。

各グラフには、フィルターで設定された期間で使用される上位 15 個のアプリケーションが表示されます。各アプリケーションには、異なる色が使用されます。各グラフの凡例は、最もよく使用されるものから、最も使用されないものの順にサービスを一覧表示します。凡例内のアプリケーションにカーソルを合わせ、グラフ内で強調表示されているアプリケーションを確認します。

右の例に示すように、データ ポイントにカーソルを合わせて、そのトラフィックに関する詳細を提供するツール ヒントを表示します。



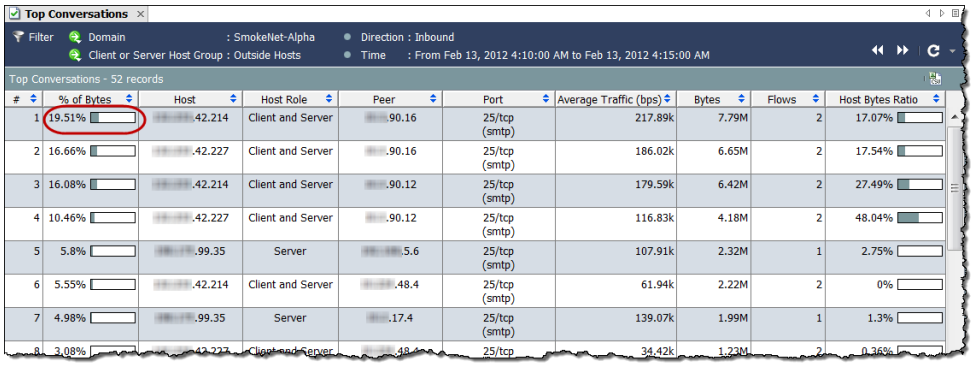


左の例に示すように、データ ポイントをダブルクリックして、トラフィックについてさらに情報を得るためのオプションを選択できるポップアップ メニューを表示します。

関係するホストを特定

トラフィックの移動方向がわかれば、次の手順を完了して、関係するホストのペアを判定します。

1. [ネットワーク(Network)] タブで、トラフィックの急激な増加をダブルクリックして、[上位の会話(Top Conversations)] ドキュメントを開きます。



#	% of Bytes	Host	Host Role	Peer	Port	Average Traffic (bps)	Bytes	Flows	Host Bytes Ratio
1	19.51%	.42.214	Client and Server	.90.16	25/tcp (smtp)	217.89k	7.79M	2	17.07%
2	16.66%	.42.227	Client and Server	.90.16	25/tcp (smtp)	186.02k	6.65M	2	17.54%
3	16.08%	.42.214	Client and Server	.90.12	25/tcp (smtp)	179.59k	6.42M	2	27.49%
4	10.46%	.42.227	Client and Server	.90.12	25/tcp (smtp)	116.83k	4.18M	2	48.04%
5	5.8%	.99.35	Server	.5.6	25/tcp (smtp)	107.91k	2.32M	1	2.75%
6	5.55%	.42.214	Client and Server	.48.4	25/tcp (smtp)	61.94k	2.22M	2	0%
7	4.98%	.99.35	Server	.17.4	25/tcp (smtp)	139.07k	1.99M	1	1.3%
8	3.08%	.42.227	Client and Server	.48.4	25/tcp	34.42k	1.23M	2	0.36%

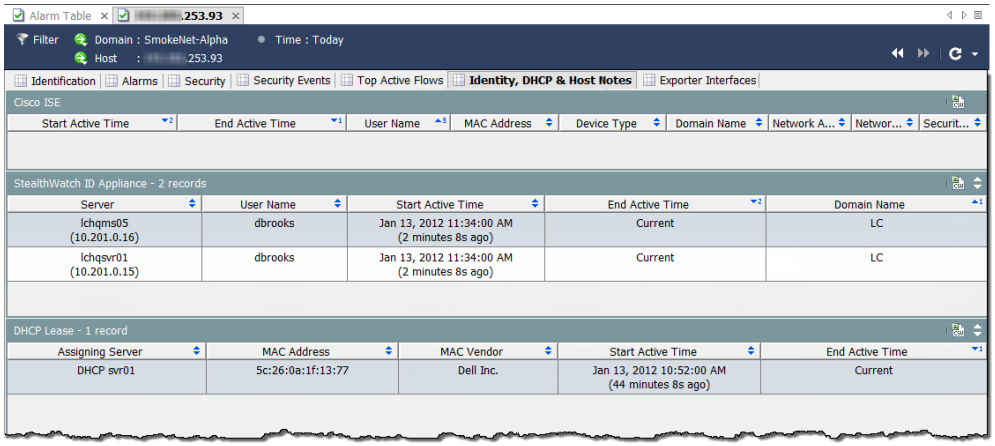
2. 使用しているバイトの割合が最も高いホストとピアを特定します。(デフォルトでは、列 # 内の数字 **1** によって表されています)。
3. 上記の特定されたホストのペアについて、次の内容を確認します。
   - 予期しない接続(たとえば、不正なホスト グループまたはサーバー)はありますか。
   - 予期しない接続は数多くありますか。
   - どのポートが使用されていますか。
   - 大量のトラフィックが送信または受信されていますか。

- 高ビットレートの接続はありますか。
- この急激な増加は、ネットワークに関するユーザーの苦情と相関関係がありますか。

関係するユーザーを特定

トラフィックの急激な増加に関わるホストのペアの IP アドレスを確認した後、次の手順を完了して、どのユーザーが関係しているかやこのアクティビティが問題かどうかを特定できることを確認します。

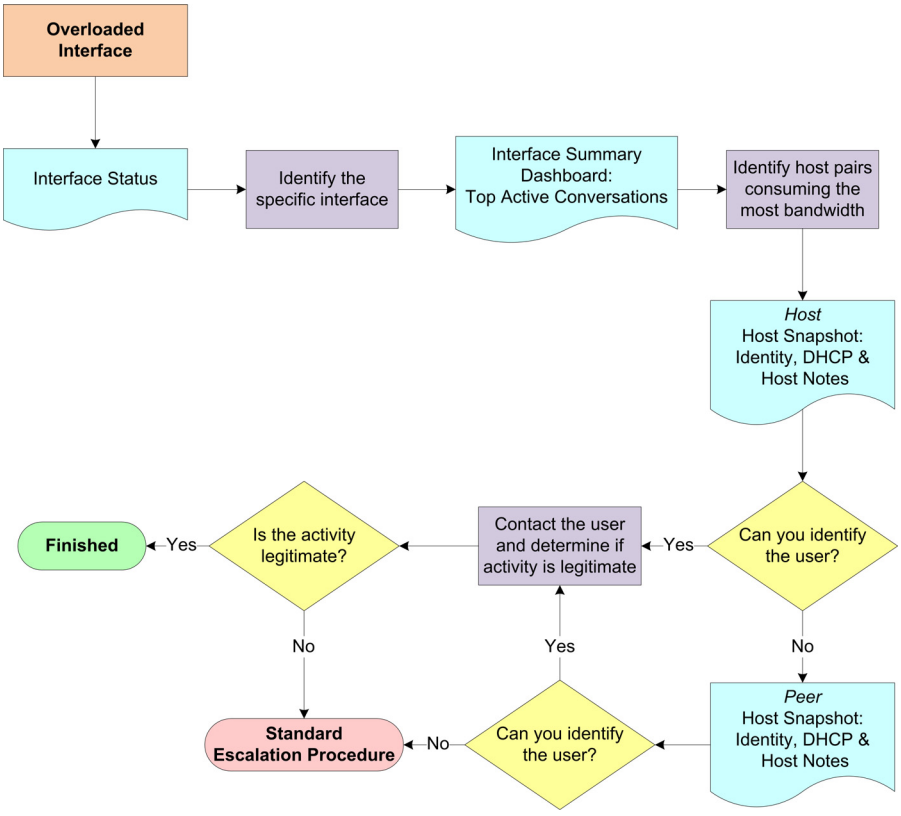
1. 適切なホスト IP アドレスをダブルクリックして、そのホスト スナップショットを開きます。
2. [ID と DHCP、ホスト ノート (Identity, DHCP & Host Notes)] タブをクリックします。



3. 任意のユーザー情報を見ますか。
   - 「はい」の場合、手順 6 に進みます。
   - 「いいえ」の場合、手順 4 に進みます。
4. 適切なピア IP アドレスをダブルクリックして、そのホスト スナップショットを開きます。
5. [ID と DHCP、ホスト ノート (Identity, DHCP & Host Notes)] タブをクリックします。
6. 任意のユーザー情報を見ますか。
   - 「はい」の場合、手順 6 に進みます。
   - 「いいえ」の場合、手順 7 に進みます。
7. このアクティビティは、問題があるように見えますか。
   - 「はい」の場合、または不明な場合は、手順 7 に進みます。
   - 「いいえ」の場合は、ここで終了します。
8. これまでに得られた情報を集約し、組織の標準エスカレーション手順に従ってエスカレートします。

過負荷のインターフェイス

インターフェイスが過負荷になっているか容量に近いことが、わかっているか推測される場合は、次の図に示すワークフローを使用して、問題の原因を特定できます。



ワークフロー概要

SMC では、インターフェイスの使用率が簡単にわかる、次を含むいくつかの方法を提供しています。

- [エンタープライズ(Enterprise)] ツリー内の [ネットワークデバイス(Netwrk Devices]
- [インターフェイスステータス(Interface Status)]
- [アラームテーブル(Alarm Table)]([インターフェイスの使用率を超えています(Interface Utilization Exceeded)] アラームが発生した場合)

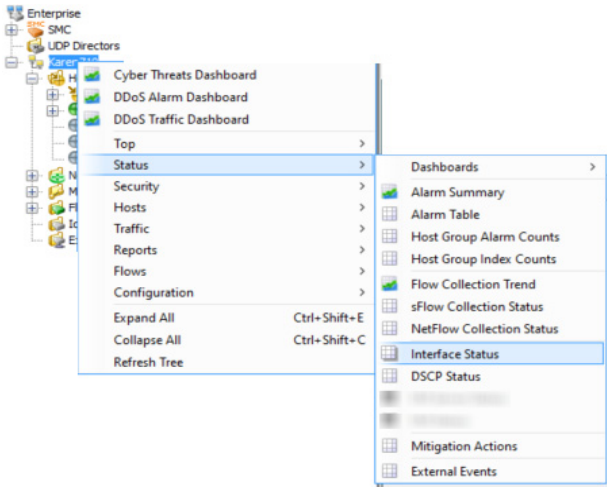
このワークフローは、[インターフェイス状態（Interface Status）] ドキュメントから調査を開始します。次の手順は、上記のワークフロー図に示す手順の概要について説明しています。

1. ドメインに対する [インターフェイス状態（Interface Status）] ドキュメントを開いて、過負荷のインターフェイスを特定します。次項「過負荷のインターフェイスを特定（インターフェイス状態）」を参照してください。
2. 過度に使用されているインターフェイスに対する [インターフェイス概要ダッシュボード（Interface Summary Dashboard）] を開き、上位のアクティブな会話を確認します。
3. 最も帯域幅を消費しているホストのペア（ホストとピア）の IP アドレスを書き留めます。
4. ホストに対して、ホスト スナップショットの [ID と DHCP、ホスト ノート（DHCP & Host Notes）] ページを開きます。「高帯域幅ホストにログインしているユーザーの特定」（180 ページ）を参照してください。
5. ユーザーを特定することができますか。
   - 「はい」の場合、手順 8 に進みます。
   - 「いいえ」の場合、手順 6 に進みます。
6. ピアに対して、ホスト スナップショットの [ID と DHCP、ホスト ノート（DHCP & Host Notes）] ページを開きます。「高帯域幅ホストにログインしているユーザーの特定」（180 ページ）を参照してください。
7. ユーザーを特定することができますか。
   - 「はい」の場合、手順 8 に進みます。
   - 「いいえ」の場合、手順 10 に進みます。
8. ユーザーに連絡し、ユーザーが関係しているアクティビティが正当かどうかを判断します。
9. アクティビティは正当なものですか。
   - 「はい」の場合、ここで終了します。
   - 「いいえ」の場合、手順 10 に進みます。
10. これまでに得られた情報を集約し、組織の標準エスカレーション手順に従ってエスカレートします。

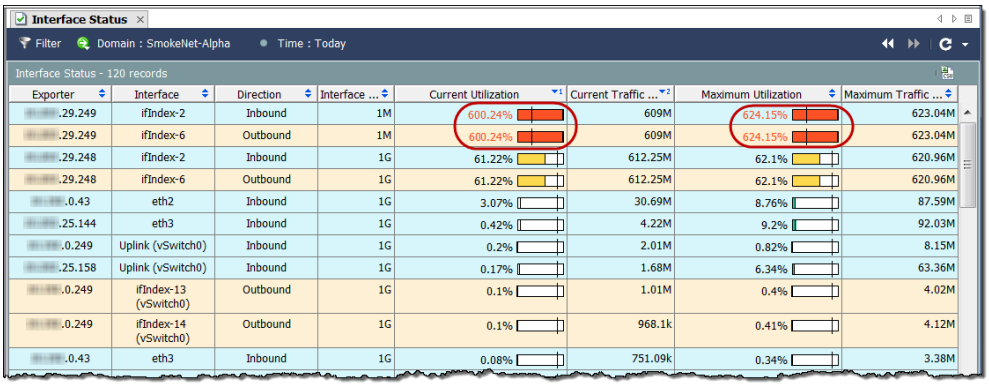
過負荷のインターフェイスを特定(インターフェイス状態)

次の手順を行って、[インターフェイス状態(Interface Status)] ドキュメントを開き、過負荷または容量に近い特定のインターフェイスを特定します。

1. ドメイン名をダブルクリックし、[状態(Status)] > [インターフェイス状態(Interface Status)] を選択します。



2. [インターフェイス状態(Interface Status)] ドキュメントが開いたら、次の例に示すように、過負荷または容量に近いインターフェイスを特定します。(**ヒント:**[現在の使用率と最大使用率(Current Utilization and Maximum Utilization)] 列で、赤色、橙色、または黄色を確認します)。

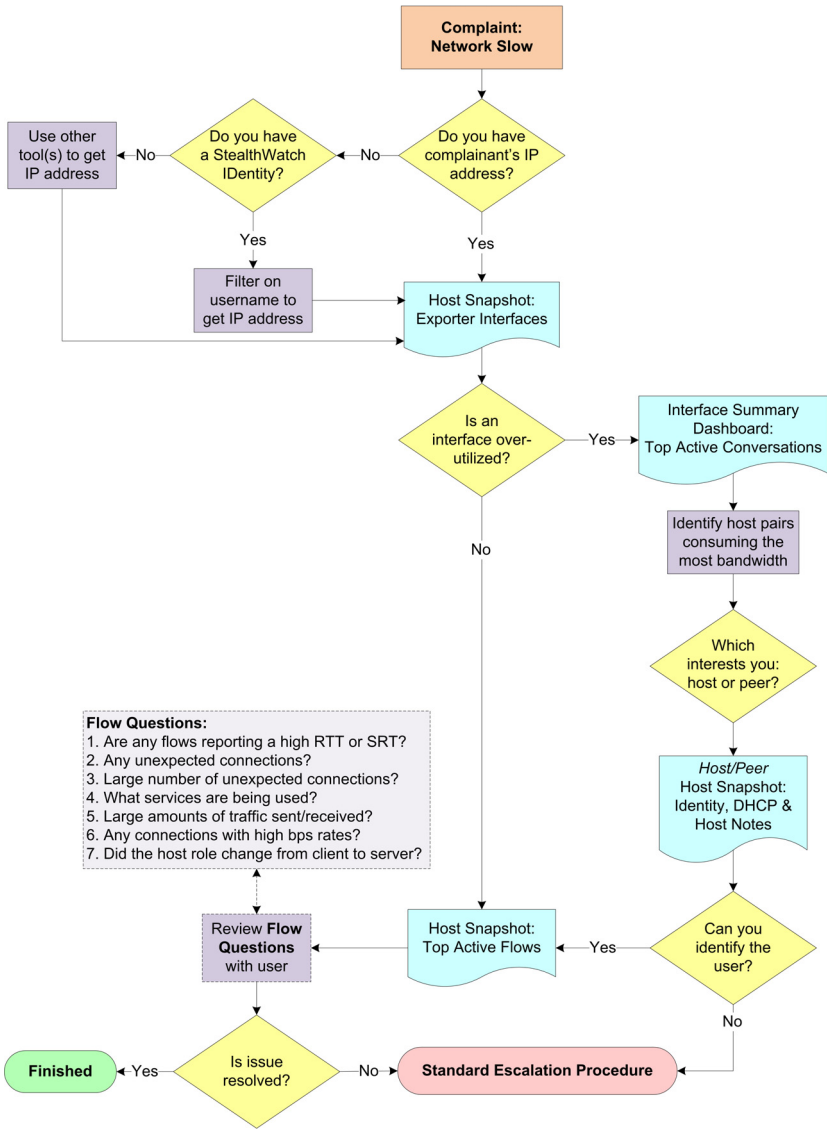


Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic ...	Maximum Utilization	Maximum Traffic ...
.29.249	ifIndex-2	Inbound	1M	600.24%	609M	624.15%	623.04M
.29.249	ifIndex-6	Outbound	1M	600.24%	609M	624.15%	623.04M
.29.248	ifIndex-2	Inbound	1G	61.22%	612.25M	62.1%	620.96M
.29.248	ifIndex-6	Outbound	1G	61.22%	612.25M	62.1%	620.96M
.0.43	eth2	Inbound	1G	3.07%	30.69M	8.76%	87.59M
.25.144	eth3	Inbound	1G	0.42%	4.22M	9.2%	92.03M
.0.249	Uplink (vSwitch0)	Inbound	1G	0.2%	2.01M	0.82%	8.15M
.25.158	Uplink (vSwitch0)	Inbound	1G	0.17%	1.68M	6.34%	63.36M
.0.249	ifIndex-13 (vSwitch0)	Outbound	1G	0.1%	1.01M	0.4%	4.02M
.0.249	ifIndex-14 (vSwitch0)	Outbound	1G	0.1%	968.1k	0.41%	4.12M
.0.43	eth3	Inbound	1G	0.08%	751.09k	0.34%	3.38M

3. 対応するインターフェイスのセルをダブルクリックして、特定したインターフェイスに対して、[インターフェイス概要ダッシュボード(Interface Summary Dashboard)] を開いて、大量のトラフィックがある理由を判定します。「高帯域幅ホスト(インターフェイス概要ダッシュボード)を検索」(179 ページ)を参照してください。

ネットワーク速度の低下

ユーザーの最も一般的な苦情の一つは、ネットワーク速度の低下です。次の図は、問題の原因を特定するのに便利なワークフローを示しています。



ワークフロー概要

次の手順は、上記のワークフロー図に示す手順の概要について説明しています。

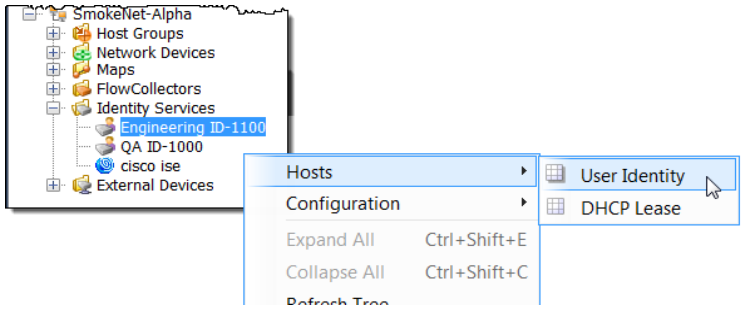
1. 苦情を訴えているユーザーの IP アドレスを把握していますか。
   - 「はい」の場合、手順 3 に進みます。
   - 「いいえ」の場合、手順 2 に進みます。
2. Stealthwatch Identity アプライアンスはありますか。
   - 「はい」の場合は、[ユーザー ID(User Identity)] フィルターを使用して、そのユーザーの IP アドレスを検索します。次項「Stealthwatch Identity を使用した IP アドレスの確認」を参照してください。
   - 「いいえ」の場合は、いずれかのツール(たとえば、ipconfig)を使用して、ユーザーの IP アドレスを取得します。
3. そのユーザーの IP アドレスに対して、ホスト スナップショットの [エクスポータインターフェイス(Exporter Interfaces)] ページを開きます。「過度に使用されているインターフェイス(ホスト スナップショット)のチェック」(177 ページ)を参照してください。
4. 過度に使用されている、または容量に近いインターフェイスはありますか。
   - 「はい」の場合、過度に使用されているインターフェイスに対して、[インターフェイス概要ダッシュボード(Interface Summary Dashboard)] を開き、上位のアクティブな会話を確認してください。「高帯域幅ホスト(インターフェイス概要ダッシュボード)を検索」(179 ページ)を参照してください。
   - 「いいえ」の場合、手順 8 に進みます。
5. 最も帯域幅を消費しているホストのペア(ホストとピア)の IP アドレスを書き留めます。
6. 最も関心のあるホストのペアに基づいて、ホストまたはピアのいずれかに対して、ホスト スナップショットの [ID と DHCP、ホスト ノート(Identity, DHCP & Host Notes)] ページを開いて、その IP アドレスにログインしているユーザーを特定します。「高帯域幅ホストにログインしているユーザーの特定」(180 ページ)を参照してください。
7. ユーザーを特定できますか。
   - 「はい」場合、ユーザーの IP アドレスを取得し、手順 8 に進みます。
   - 「いいえ」の場合、手順 10 に進みます。
8. 関連付けられているホスト スナップショットの [上位のアクティブなフロー(Top Active Flows)] ページを開いて、そのユーザーに関連付けられたフローの詳細を確認し、問題の原因を可能性として判断します。「上位のアクティブなフローの確認」(181 ページ)を参照してください。

9. この問題を解決できましたか。
   - 「はい」の場合、ここで終了します。
   - 「いいえ」の場合、手順 10 に進みます。
10. これまでに得られた情報を集約し、組織の標準エスカレーション手順に従ってエスカレートします。

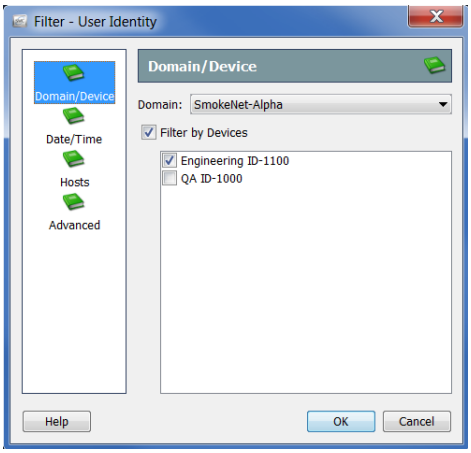
Stealthwatch Identity を使用した IP アドレスの確認

Stealthwatch IDentity アプライアンスがあれば、次の手順を行って、特定のユーザーが使用しているか、または使用していた IP アドレスをすばやく見つけます。

1. [エンタープライズ(Enterprise)] ツリーで、[アイデンティティサービス(Identity Services)] ブランチを展開し、使用したい IDentity アプライアンスを探します。
2. IDentity アプライアンスを右クリックし、[ホスト(Hosts)] > [ユーザー ID(User Identity)] を選択します。



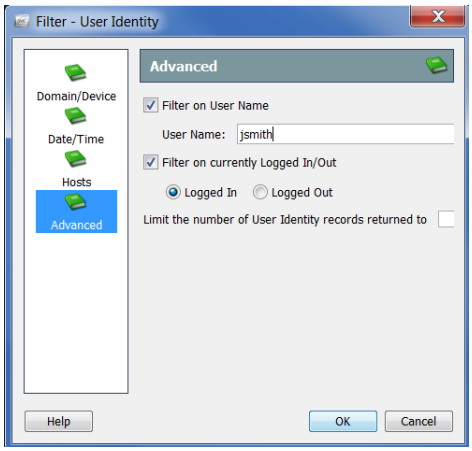
[フィルタ(Filter)] ダイアログ、[ユーザー ID(User Identity)] ページが開きます。[ドメインとデバイス(Domain/Device)] ページでは、選択したドメインとデバイスが自動的に選択されます。



(注):

- 最後にフィルタを閉じたときに見ていた最後のページに対して、フィルタが開きます。フィルターを開いたことがない場合、[ドメインとデバイス(Domain/Device)] ページに対して開きます。
- ユーザーの IP アドレスに対するすべての IDentity アプライアンスを検索するには、[ドメインとデバイス(Domain/Device)] ページ上の [デバイスでフィルタ処理(Filter by Devices)] チェックボックスをクリックして、チェック マークをはずします。

3. [詳細設定(Advanced)] ボタンをクリックします。[詳細(Advanced)] ページが開きます。
4. [ユーザー名でフィルタ処理(Filter on User Name)] チェックボックスをクリックして、チェック マークを付け、[ユーザー名(User Name)] フィールドにユーザーのログイン名を入力します。



5. デフォルトでは、フィルタは、選択した [現在のログインまたはログアウトでフィルタ処理(Filter on currently Logged In/Out)] オプションによって示されるように、クエリ時にログインしているユーザーの IP アドレスのみを検索します。

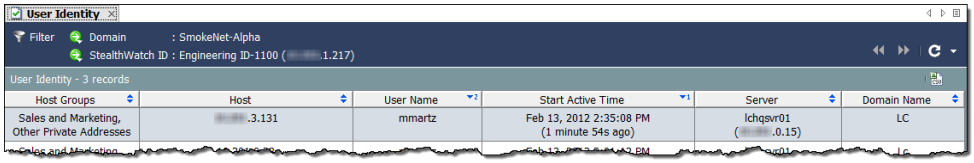
   その他のときにユーザーがログインしていた IP アドレスを検索するには、[現在のログインまたはログアウトでフィルタ処理(Filter on currently Logged In/Out)] チェックボックスをクリックして、チェック マークをはずし、次にフィルターの [日付/時刻(Date/Time)] ページに移動して、期間を指定します。

6. 必要に応じて、[返すユーザー ID レコード数を制限(Limit the number of User Identity records returned to)] フィールド内に値を入力することによって表示される、レコード数を変更します。

(注):

この項で説明した種類の問題を解決するには、一般的に、このフィルター内のその他のパラメータを定義する必要はありません。さらにサポートが必要な場合は、Stealthwatch デスクトップクライアントのオンラインヘルプを参照してください。

7. [OK] をクリックします。[ユーザー ID(User Identity)] ページが開き、指定したユーザー名に関連付けられた IP アドレスが表示されます。



ヒント:

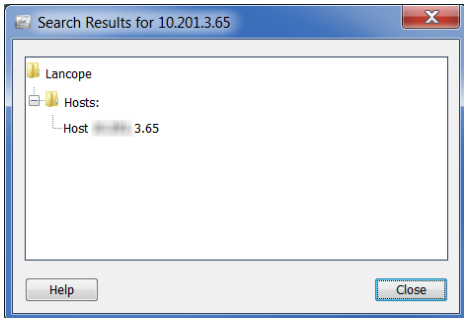
IP アドレスをダブルクリックして、関連付けられているホスト スナップショットを開きます。

過度に使用されているインターフェイス(ホスト スナップショット)のチェック

次の手順を行って、特定の IP アドレスに対して、ホスト スナップショットの [エクスポータインターフェイス(Exporter Interfaces)] ページを開き、インターフェイスが過負荷かどうかを確認します。

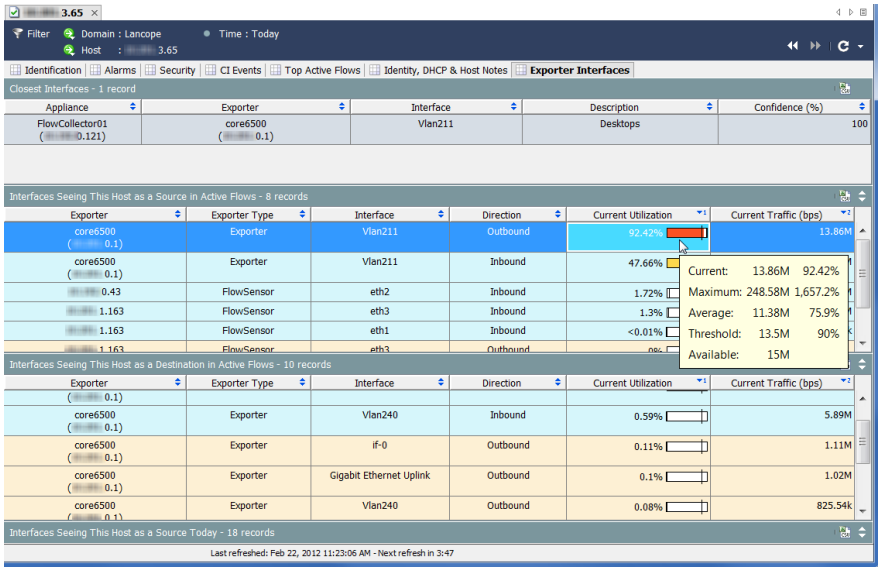
1. IP アドレスを特定するのに [ユーザー ID(User Identity)] ドキュメントを使用しましたか。
   - 「はい」の場合は、IP アドレスをダブルクリックして、ホスト スナップショットを開き、手順 4 に進みます。
   - 「いいえ」の場合、手順 2 に進みます。

2. SMC ツールバーで、[グローバル検索(Global Search)] フィールドに IP アドレスを入力し、**Enter** を押します。右に例に示すように、[検索結果(Search Results)] ダイアログには、そのアドレスが SMC に表示されるそれぞれの場所の一覧が表示されます。



3. ホストの IP アドレスのエントリーをダブルクリックします。

4. ホスト スナップショットが開いたら、[エクスポータインターフェイス(Exporter Interfaces)] タブをクリックします。



ヒント:

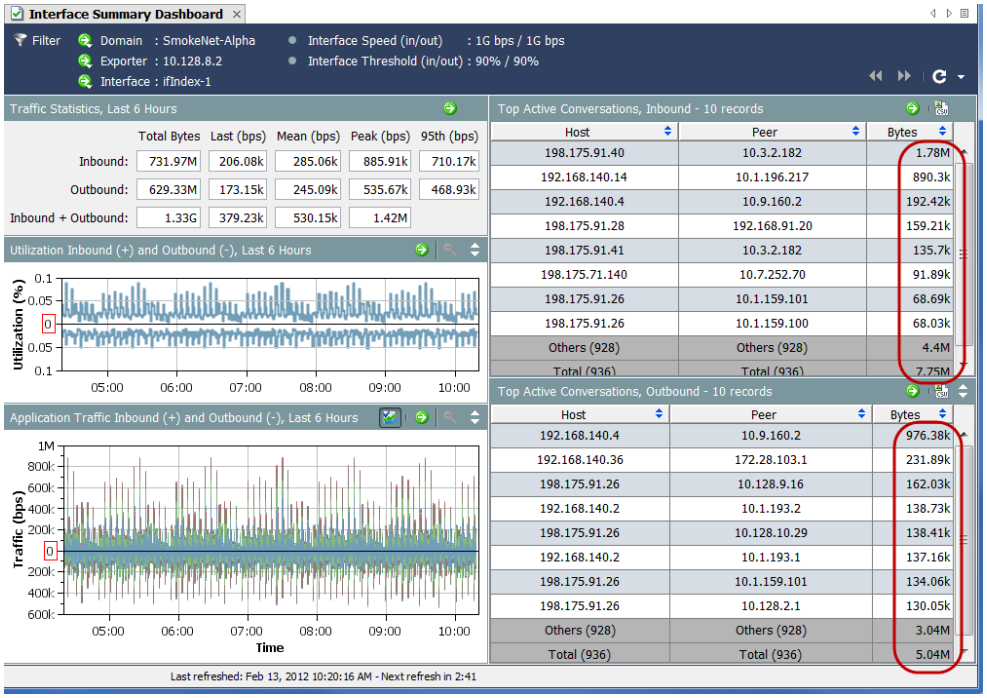
[現在の使用率(Current Utilization)] 列内の値にカーソルを合わせ、関連付けられたインターフェイスに対する容量の可用性と使用率詳細を確認します。

5. インターフェイスは過負荷または容量に近い状態ですか(**ヒント**:[現在の使用率(Current Utilization)] 列で、赤色、橙色、または黄色を確認します)。

   - 「はい」の場合、過負荷のインターフェイスに対して、[インターフェイス概要ダッシュボード(Interface Summary Dashboard)] を開き、大量のトラフィックがある理由を判断します。次項「高帯域幅ホスト(インターフェイス概要ダッシュボード)を検索」を参照してください。
   - 「いいえ」の場合、ホスト スナップショット上の [上位のアクティブなフロー(Top Active Flows)] タブをクリックして、ユーザーに関連付けられたフローの詳細を確認して、問題の原因を可能性として判断します。「上位のアクティブなフローの確認」(181 ページ)を参照してください。

高帯域幅ホスト(インターフェイス概要ダッシュボード)を検索

インターフェイス概要の [エクスポータインターフェイス(Exporter Interfaces)] タブで、過負荷または容量に近いインターフェイス([インターフェイス(Interfaces)] 列内)を確認している場合、ダブルクリックして、関連付けられた [インターフェイス概要ダッシュボード(Interface Summary Dashboard)] を開きます。



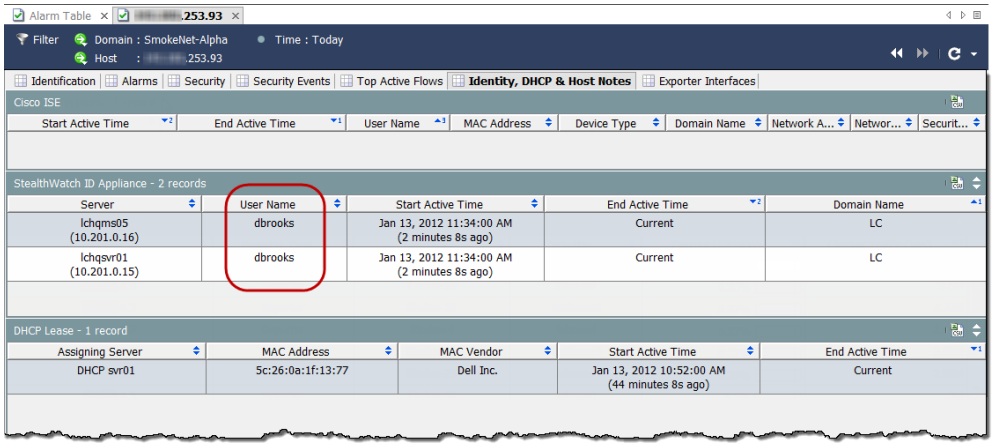
ダッシュボードの右側で、[送受信する上位のアクティブな会話(Top Active Conversations Inbound and Outbound)] を確認します。いずれかの方向でほとんどの帯域幅を使用しているホストのペア(ホストとピア)([バイト(Bytes)] 列を参照)を特定します。

それぞれの IP アドレスにログインしているユーザーを特定するには、それぞれの IP アドレスに対して、ホスト スナップショットの [ID と DHCP、ホスト ノート (Identity, DHCP & Host Notes)] タブを開きます。「高帯域幅ホストにログインしているユーザーの特定」(180 ページ) を参照してください。

高帯域幅ホストにログインしているユーザーの特定

過度な帯域幅を使用しているホストまたはピアに対する IP アドレスを作成したら、そのアドレスに対してホスト スナップショットを開き、[ID と DHCP、ホスト ノート (Identity, DHCP & Host Notes)] タブをクリックします。

ログイン情報がある場合は、その IP アドレスにログインしたユーザーのユーザー名が表示されます。

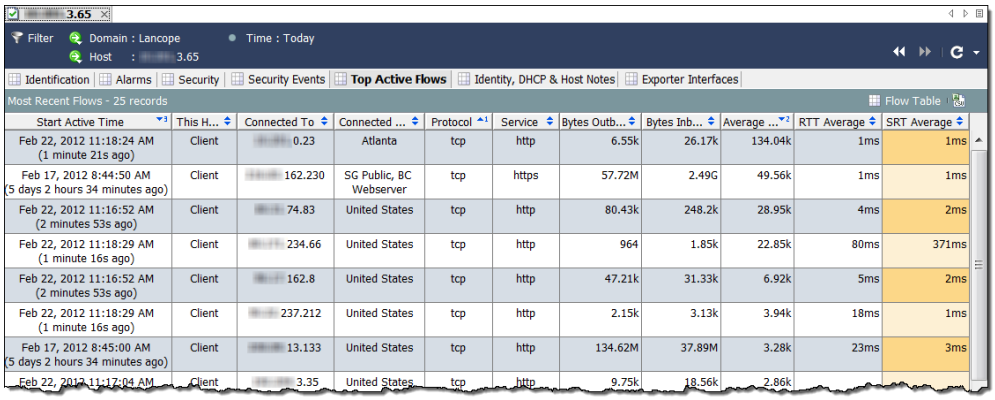


ユーザー情報がない場合は、これまでに得た情報を集約し、あなたの組織の標準エスカレーション手順に従ってエスカレートします。

ヒント:
Stealthwatch IDentity アプライアンスがある場合は、ユーザー名をダブルクリックして、[ユーザーID(User Identity)] ドキュメントを開き、そのユーザーに関連付けられている IP アドレスを確認できます。

上位のアクティブなフローの確認

ホスト スナップショットの [上位のアクティブなフロー(Top Active Flows)] タブは、Stealthwatch アプライアンスごとの 25 件の最新フロー、およびアプライアンスごとの最大トラフィックを持つ 25 件のフローについて、詳細を提供します。



Start Active Time	This H...	Connected To	Connected ...	Protocol	Service	Bytes Outb...	Bytes Inb...	Average ...	RTT Average	SRT Average
Feb 22, 2012 11:18:24 AM (1 minute 21s ago)	Client	0.23	Atlanta	tcp	http	6.55k	26.17k	134.04k	1ms	1ms
Feb 17, 2012 8:44:50 AM (5 days 2 hours 34 minutes ago)	Client	162.230	SG Public, BC Webserver	tcp	https	57.72M	2.49G	49.56k	1ms	1ms
Feb 22, 2012 11:16:52 AM (2 minutes 53s ago)	Client	74.83	United States	tcp	http	80.43k	248.2k	28.95k	4ms	2ms
Feb 22, 2012 11:18:29 AM (1 minute 16s ago)	Client	234.66	United States	tcp	http	964	1.85k	22.85k	80ms	371ms
Feb 22, 2012 11:16:52 AM (2 minutes 53s ago)	Client	162.8	United States	tcp	http	47.21k	31.33k	6.92k	5ms	2ms
Feb 22, 2012 11:18:29 AM (1 minute 16s ago)	Client	237.212	United States	tcp	http	2.15k	3.13k	3.94k	18ms	1ms
Feb 17, 2012 8:45:00 AM (5 days 2 hours 34 minutes ago)	Client	13.133	United States	tcp	http	134.62M	37.89M	3.28k	23ms	3ms
Feb 22, 2012 11:17:04 AM	Client	3.35	United States	tcp	http	9.75k	18.56k	2.86k		

まず、RTT と SRT の値を見てください。SRT の値が許容できないほど高い場合、サーバーに問題があるとわかり、サーバー チームに連絡して、問題を解決することができます。

SRT の値が適切な場合、問題は、ネットワークのどこか、大抵はホスト自体にあります。[上位のアクティブなフロー(Top Active Flows)] タブを見て、次の内容を確認します。確認した内容は、ホストがハイジャックされたか、マルウェアに感染したか、ユーザーが不正な活動に関わっているかを判断するのに役立ちます。

1. 予期しない接続(たとえば、不正なホスト グループまたはサーバー)はありますか。
2. 予期しない接続は数多くありますか。
3. どのようなサービスを使用していますか。
4. 大量のトラフィックが送信または受信されていますか。
5. 高ビットレートの接続はありますか。
6. ホストがロールをクライアントからサーバーに変更しましたか。ワークステーションが突然サーバーとして実行を開始する場合、最も高い可能性は、マルウェアに感染したか、ハイジャックされたかです。

前の質問に対する確認内容に基づいて問題を解決できない場合は、次の手順を実行します。

1. ホストのウイルス対策プログラムまたはファイアウォールが問題のサーバーへのアクセスをブロックしていないかを確認します。
2. ホストのウイルス対策プログラムは、マルウェアを検出できなかったか、侵害された可能性があるため、Malwarebytes の Anti-Malware など、別のアンチウイルス プログラムを使用してウイルス スキャンを実行します。
3. ホスト上で新しいアプリケーションがインストールまたはアップデートされているかを確認します。その場合、アプリケーションが正しく構成されていることを確認します。アプリケーションをアンインストールし、再インストールする必要が生じることがあります。

これらの提案を使用して問題を解決することができない場合は、これまでに得られた情報を集約し、組織の標準エスカレーション手順に従ってエスカレートします。

外部参照

外部参照機能では、IP アドレスに関する追加情報を表示する Web アプリケーション（または内部資産データベース）を起動することができます。この Web アプリケーションまたはデータベースは、Stealthwatch デスクトップクライアントまたは Stealthwatch Web アプリケーションから直接起動できます。

また、外部ルックアップ機能を使用して、Stealthwatch デスクトップクライアントから Stealthwatch Web アプリケーションに即座にジャンプできるショートカットを作成することもできます。

Stealthwatch は、外部ルックアップ機能とともに使用できる次のデフォルト Web アプリケーション（ルックアップオプション）を備えています。それらを Stealthwatch に追加する必要はありません。

- Cisco SenderBase
- DShield
- Host Report

次に、IP アドレスに関する追加情報を表示するために Stealthwatch 管理者が追加できる Web アプリケーションのいくつかの例を示します。

- BigFix
- CiscoWorls
- Cisco ISE（Identity Services Engine）
- スプランク
- トリップワイヤ
- Ziften

重要:

デフォルト以外のルックアップオプションを追加するには、Stealthwatch Web アプリケーションの外部ルックアップ設定ツールを使用する必要があります。この方法については、「外部参照の設定」を参照してください。

外部参照の設定

前述のように、外部ルックアップ機能の使用を想定して Cisco SenderBase、DShield、およびホスト名がデフォルトで含まれているため、Stealthwatch にそれらを追加する必要はありません。この機能で他の Web アプリケーションを使用するには、それを Stealthwatch に追加する必要があります。これを行うには、Stealthwatch Web アプリケーションで外部ルックアップ設定ツールを使用します。

（注）:

v6.7 にアップグレードすると、以前に追加した外部参照オプションごとに、v6.7 では 2 つずつ表示されます。

Stealthwatch では、外部ルックアップ設定を管理するために webLinks.xml ファイルが使用されなくなりました。

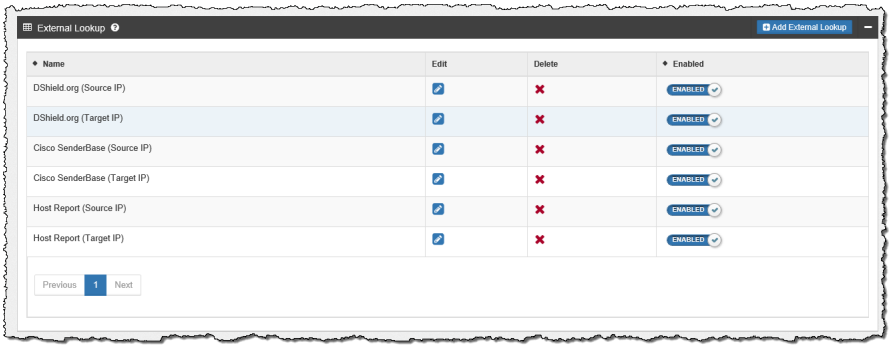
このツールを使って、Web アプリケーションに送信したい特定のパラメーターを構成することもできます。構成するパラメータは、参照を実行する IP アドレスを利用できる場合にのみ送信されます。

参照オプションを追加して、Web アプリケーションに送信したいパラメータを設定するには、次の手順を行います。

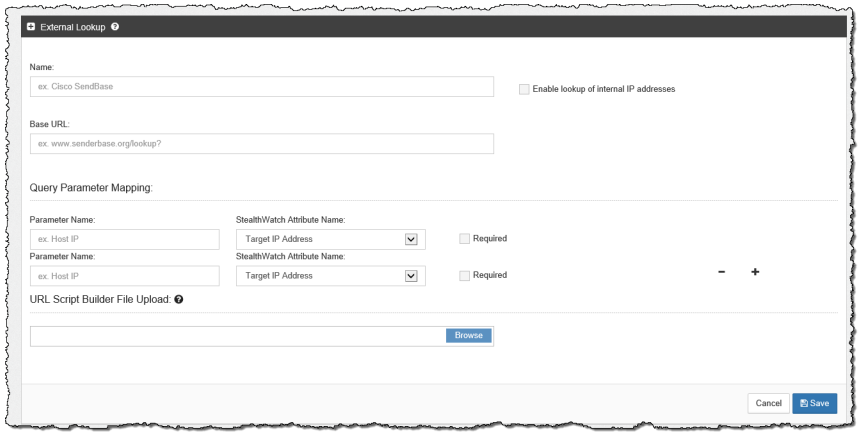
1. Stealthwatch Web アプリケーションで、左側にある [ナビゲーション（Navigation）] ペインの [ツール（Tools）] [設定（Settings）] > [外部ルックアップ設定（External Lookup Configuration）] をクリックします。[外部参照の構成（External Lookup Configuration）] ページが開きます。

   外部参照機能を使用できない参照オプションを無効にする（ただし、後の使用のためにその構成を保持する）には、該当する行で [有効（Enable）] をクリックします。ボタンが [無効（Disabled）] に切り替わります。

   将来、この参照オプションを有効にするには、[無効（Disabled）] をクリックします。ボタンが [有効（Enabled）] に切り替わります。



2. [外部参照を追加(Add External Lookup)] をクリックします。外部参照セクションが開きます。



3. このセクションの上部で、次のフィールドに適切なエントリーを入力します。
   - [名前(Name)]
   - [ベース URL(Base URL)]
4. 内部 Web アプリケーションの IP アドレスについての情報を表示するには、[内部 IP アドレスの参照を有効にする(Enable lookup of internal IP addresses)] チェックボックスを選択します。
5. [クエリパラメータマッピング(Query Parameter Mapping)] セクション内の最初の [Stealthwatch 属性名(Stealthwatch Attribute Name)] フィールドで、[ソース IP アドレス(Source IP Address)] または [ターゲット IP アドレス(Target IP Address)] を選択します。

重要:
追加する参照オプションに対して、ソース IP アドレスまたはターゲット IP アドレスを設定する必要があります。

6. 対応する [パラメータ名(Parameter Name)] フィールドに、前の手順で選択した IP アドレスを指定するのに使用した Web アプリケーションのパラメータ名を入力します。
7. 必要な場合は、IP アドレスの参照を実行する Web アプリケーションに送信したい追加のパラメータのいずれかを設定します。
   - [ターゲット IP アドレス(Target IP Address)]
   - [ターゲットポート番号(Target Port No.)]
   - [ソース IP アドレス(Source IP Address)]
   - [ソースポート番号(Source Port No.)]
   - [ホスト名(Host Name)]

- [タイムスタンプ(UTC)(TimeStamp (UTC))]
- [トランスポートプロトコル(Transport Protocol)]
- [ユーザー(User)]

追加のパラメータを追加するには、最初に設定した行の最後にあるプラス(+)記号をクリックします。設定した行を削除するには、適切な行でマイナス(-)記号をクリックします。

(注):
各参照オプションに対して、最大 20 個のクエリ パラメータをマッピングできます。

8. 特定の Web アプリケーションを使用して、検索を実行する際にパラメータを使用したい場合は、[Required(必須)] チェックボックスを選択します。特定の Web アプリケーションに対して必要となるよう指定したパラメータはすべて、参照を実行する IP アドレスに対して利用できる必要があります。関連する IP アドレスに必要なパラメータのうち 1 つでも使用できない場合、その参照オプションはポップアップ メニューで有効になりません。
9. クエリ パラメータが標準のクエリ パラメータと一致しない場合、カスタマイズしたスクリプト ビルダーを [URL スクリプトビルダーファイルアップロード(URL Script Builder File Upload)] フィールドにアップロードする必要があります。

(注):
次のスクリプトの例では、強調表示されている変数を使用してください。

スクリプト ビルダー ファイルには、Web アプリケーションがクエリを実行するために必要とする URL 形式にクエリ パラメータを設定するスクリプトが含まれています。

スクリプトビルダーファイルをアップロードしなかった場合、Stealthwatch は以下に示すデフォルトの標準クエリパラメータを使用します。

```
BaseURL?[ParameterName1]=[ParameterValue1]&
ParameterName2]=[ParameterValue2]&
ParameterName3]=[ParameterValue3](追加するパラメータに対してなど)
```

URL とスクリプトの例

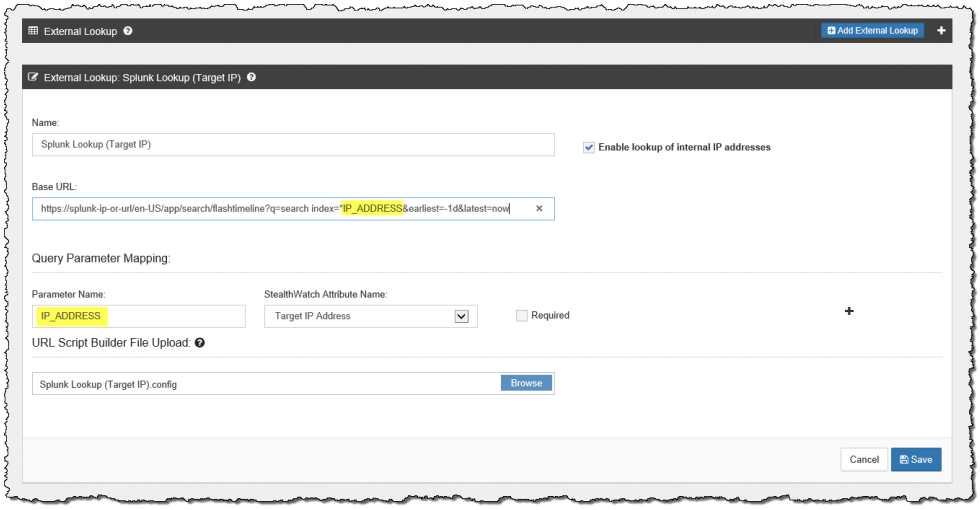
例 1

次の URL とスクリプトの例は、パラメータ名（たとえば、Splunk）のない値を使用する Web アプリケーションに使用されます。

```
https://splunk-ip-or-url/en-US/app/search/flash-timeline
?q=search index=* 192.10.20.43 &earliest=-1d&lastest=now
```

```
def String query = baseUrl;
def String url = baseUrl;

vendorValues.each { valueOperand ->

    if (url.indexOf(valueOperand.getName()) != -1) {
        def String convertedStr = "";
        if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
            convertedStr = valueOperand.getFromValue().toString();
        } else if (valueOperand.getFromValue() instanceof Date) {
            convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
        }
        if (query.indexOf(valueOperand.getName()) != -1) {
            String[] parts = query.split(valueOperand.getName());
            query = "";
            def int i = 0;

            parts.each { part ->
                if (i + 1 < parts.length) {
                    query = query + part + URLEncoder.encode(convertedStr,"UTF-8");
                } else {
                    query = query + part;
                }

                i += 1;
            }

            if (url.endsWith(valueOperand.getName())) {
                query += URLEncoder.encode(convertedStr,"UTF-8");
            }
            url = query;
        }
    }
};

return query;
```

この例で前に示したように、クエリ パラメータを URL 形式に設定するスクリプトを作成するには、次の画像で強調表示されている [パラメータ名（Parameter Name）] フィールド エントリーを使用します。



（注）：

必要な数だけ属性を設定することができますが、同じ数のパラメータを設定してください。

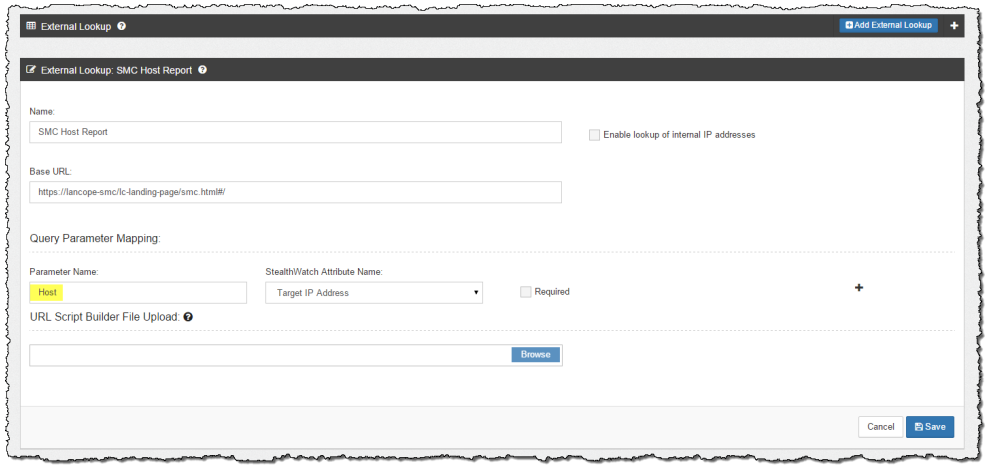
例 2

次の URL とスクリプトの例は、rest-like パスのパラメータ（たとえば、Stealthwatch ホスト レポート）を使用する Web アプリケーションに使用されます。

```
https://lancope-smc/lc-landing-page/smc.html#/host
/172.21.114.17
```

```
def String query = "";

vendorValues.each { valueOperand ->


    query += valueOperand.getName() + "/";
    def String convertedStr = "";
    if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
        convertedStr = valueOperand.getFromValue().toString();
    } else if (valueOperand.getFromValue() instanceof Date) {
        convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
    }
    String.valueOf('java.lang.Integer');
    query += URLEncoder.encode(convertedStr,"UTF-8");
};

def char lastChar = baseUrl.charAt(baseUrl.length() - 1);
if (lastChar != '?' && lastChar != '/' && lastChar != '&') {
    baseUrl = baseUrl + "?";
};

query = baseUrl + query;
return query;
```

この例で前に示したように、クエリ パラメータを URL 形式に設定するスクリプトを作成するには、次の画像で強調表示されている [パラメータ名 (Parameter Name)] フィールド エントリーを使用します。



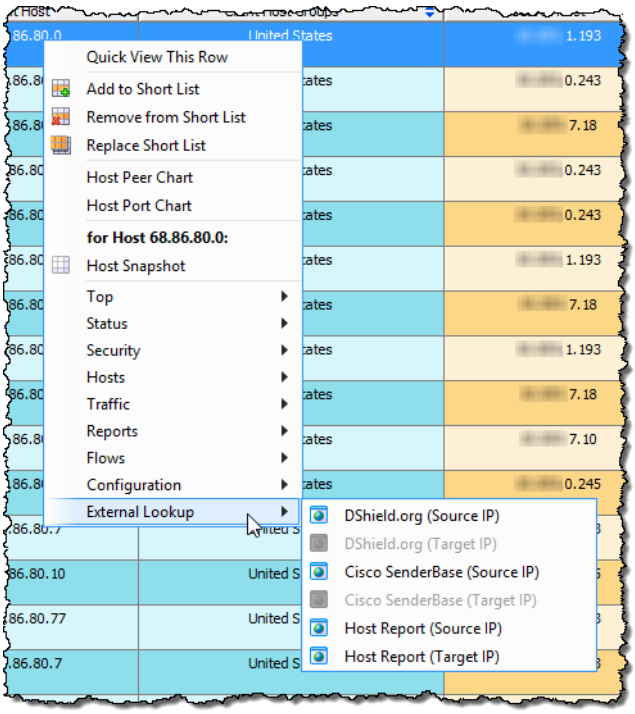
10. 終了したら、[保存 (Save)] をクリックします。[外部参照 (External Lookup)] セクションに戻ります。追加した参照オプションがリストに表示され、デフォルトで有効になります (外部参照機能を使用できます)。

外部参照を実行

IP アドレスに関する追加情報を表示するために、Web アプリケーションにクエリを行うには、次の手順を行います。

1. 次のいずれかを実行します。
   - Stealthwatch デスクトップクライアントの場合は、手順 2 に進みます。
   - Stealthwatch Web アプリケーションの場合は、手順 3 に進みます。
2. 次の手順を実行します。
   a. Stealthwatch デスクトップクライアントで、関連する IP アドレスが含まれているドキュメントを開きます。
   b. IP アドレスを右クリックします。

c. 表示されるポップアップ メニューで、[外部参照(External Lookup)] をクリックします。第 2 のポップアップ メニューが表示されます。

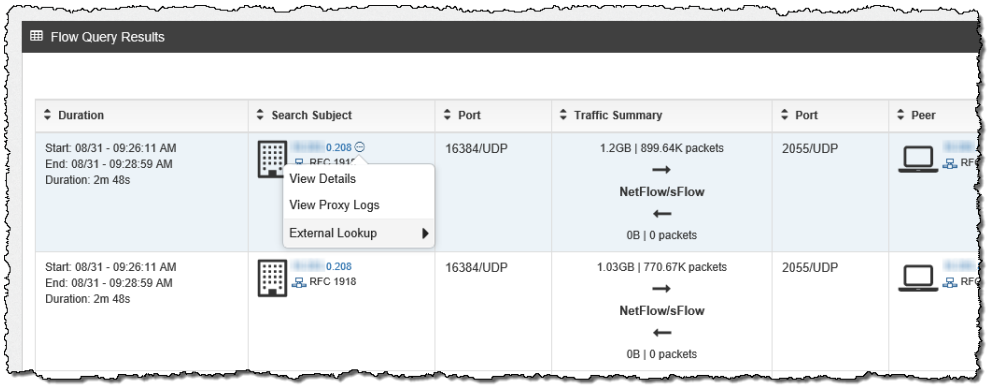


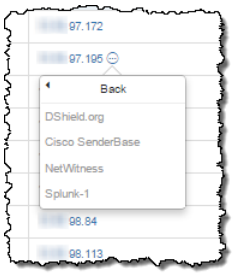
3. 次の手順を実行します。

a. Stealthwatch Web アプリケーションで、[標準のフロークエリ結果(Standard Flow Query Results)] ページまたは [詳細なフロークエリ結果(Advanced Flow Query Results)] ページを開きます。

b. [検索対象(Search Subject)] 列または [ピア(Peer)] 列で、IP アドレスにカーソルを合わせ、楕円をクリックします。

c. 表示されるポップアップ メニューで、[外部参照(External Lookup)] をクリックします。第 2 のポップアップ メニューが表示されます。

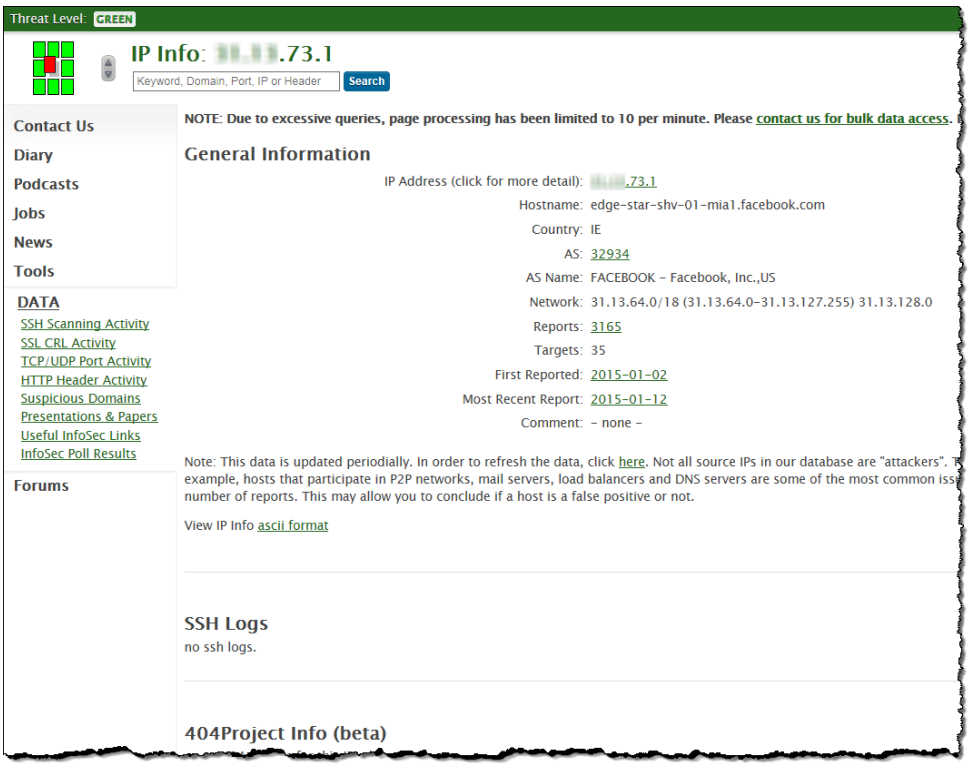




4. 手順 3 で示すように第 2 のポップアップ メニューから目的の参照オプションをクリックします。選択した参照オプションに対する Web アプリケーションが開き（Web アプリケーションにログインするよう求められる場合があります）、参照を実行する IP アドレスに対するクエリ結果が表示されます。

   特定の Web アプリケーションに対して必要となるよう指定したパラメータはすべて、参照を実行する IP アドレスに対して利用できる必要があります。関連する IP アドレスに必要なパラメータのうち 1 つでも使用できない場合、その参照オプションはポップアップ メニューで有効になりません。詳細については、194 ページの「ベンダーの設定」を参照してください。

   次の例では、DShield Web アプリケーションを使用したクエリに対して返される情報について説明します。



8

STEALTHWATCH 脅威インテリジェンスフィード

概要

Stealthwatch 脅威インテリジェンスフィード（正式には Stealthwatch Labs Intelligence Center または SLIC）は、ネットワークに対する脅威に関したグローバルな脅威インテリジェンスフィードから、頻繁に更新される情報を提供するシスコのサービスです。Stealthwatch 脅威フィードは、有害なネットワーク活動を迅速かつ正確に特定するのに Stealthwatch が使用する、マルウェア コマンド アンド コントロール（C&C）サーバーおよび他の対象ホスト（Bogon や Tor など）についてのデータを提供します。

この章は、次の項で構成されています。

脅威インテリジェンスフィードについて

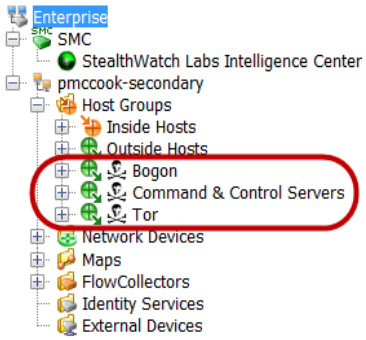
企業ツリー内のアイコン(Stealthwatch Labs Intelligence Center または SLIC という以前の名前が現在も表示されている)は、脅威インテリジェンスフィードが有効になっているかどうか、またはアクティブなアラームがあるかどうかに応じて色が変わります。ガイドラインについては、次の一覧を参照してください。

- 脅威インテリジェンスフィードを無効にすると、SLIC のアイコンがグレーになります。(右側の画像で、アイコンは無効モードで表示されています)
- 脅威インテリジェンスフィードが有効で、アクティブなアラームがない場合は、SLIC のアイコンが緑色になります。
- 脅威インテリジェンスフィードが有効になっていて、SLIC チャネルダウンアラームがある場合は、SLIC のアイコンがグレーになり、このアイコンの下部には赤の背景で白色の X が表示されます。
- SLIC チャネルダウンアラーム以外のアラームが存在する場合、アイコンは最高のアラーム重大度に対応した色になります。

脅威インテリジェンスフィードの機能

次に、脅威インテリジェンスフィードを有効にしたときに発生するイベントを順番に示します。

1. 脅威インテリジェンスフィードが、特定した脅威のリストを SMC にダウンロードします。これらは、右の図に示すように、[エンタープライズ(Enterprise)] ツリーで内の個々のホスト グループ ブランチに表示されます。



2. SMC は、システム内の各フロー コレクタにこのリストを配布します。
3. フロー コレクタは、ネットワークでホストを監視するためにこの情報を使用します。
4. フローコレクタが脅威インテリジェンスフィードにある脅威と通信しているネットワーク内のホストを検出すると、セキュリティイベントがトリガーされます。

(注):

(そのように構成されている場合)これらのセキュリティ イベントにより発生しうるアラームについての詳細、および各アラーム発生の前提となる条件については、「脅威インテリジェンス セキュリティ イベント」(198 ページ)を参照してください。

5. 脅威インテリジェンスフィードが SMC で有効になっていても SMC サーバーが脅威インテリジェンスフィードからデータを取得できない場合は、SLIC チャネルダウンアラームがトリガーされます。企業ツリー内の [SLIC] アイコンがグレーになり、アイコンの下部に X が表示されます。

   次の 2 つの条件のいずれかが満たされると、このアラームは解除されます。

   - SMC サーバーが再び脅威インテリジェンスフィードからのデータの取得を開始する。
   - 脅威インテリジェンスフィードを無効にする。

脅威インテリジェンスフィードのホストグループ

(注):
Stealthwatch Labs Intelligence Center のブランチ内にあるホストグループブランチの名前の変更、変更、移動、または削除はできません。

これらのホストグループには、悪意のあるアクティビティに使用されたことがわかっている IP アドレス、ポート番号、プロトコル、ホスト名、および URL が含まれています。次のホストグループが脅威インテリジェンスフィードに含まれます。

- [Bogon]:bogon は公共のインターネットに公式に割り当てられていない IP アドレスです。
- [コマンドアンドコントロール サーバー(Command & Control Servers)]:C&C は、ボットネットに対して命令を出し、乗っ取られたコンピュータからレポートを受け取る集中型コンピュータです。
- [Tor]:Tor は、インターネットの匿名化サービスです。

(注):
ホストに接続している可能性のある脅威インテリジェンスフィード内の URL を検出するには、IPFIX を(NetFlow に)エクスポートするように設定された FlowSensor またはルータをインストールしておく必要があります(デフォルトでは、FlowSensor が IPFIX をエクスポートするよう設定されています)。

前述のホスト グループのいずれかにある、悪意のあるホストと通信したホストを調査したいが、関連するホスト グループに悪意のあるそのホストが表示されなくなった場合は、アラーム テーブルにアクセスして、次のコンポーネントをフィルタ処理します。

- [種類(Types)]:フィルターを適用したい悪意のあるホストの種類に応じて、該当する bogon、コマンド アンド コントロール、または ToR アラームを選択します。
- [日付/時刻(Date/Time)]:調べたい期間に従ってフィルターを適用します。

脅威インテリジェンスフィードの有効化

脅威インテリジェンスフィードを有効にする方法については、Stealthwatch デスクトップクライアントのオンラインヘルプにある「脅威インテリジェンスフィードの設定」のトピックを参照してください。

脅威インテリジェンス セキュリティ イベント

この項では、脅威インテリジェンスフィードにある脅威のホストによって引き起こされる可能性のあるセキュリティイベントについて説明します。このようなセキュリティ イベントはそれぞれが、(そのように設定されていれば) SMC クライアント インターフェイスでアラームを発生させます(これらは、Stealthwatch デスクトップクライアントのホストポリシーマネージャで設定できます)。発生すると、Stealthwatch デスクトップクライアント内のアラームテーブルに表示されます。

フローコレクタが検出したものや SMC の設定によっては、次のセキュリティイベントでアラームが発生する場合があります。

セキュリティ イベント	説明
[ホストがボットに感染:C&C 行動を試行 (Bot Infected Host – Attempted C&C Activity)]	このアラームは、ネットワーク内のホストが C&C サーバーの一覧に表示される C&C サーバーと通信しようとし、そのためにボットネットのメンバーとなったことを示します。通信は、一方向のみです。 内部ホストは、イニシエータとして、懸念インデックス(CI)ポイントの累積を行います。接続を試みられている C&C サーバーも内部ホストである場合、その C&C サーバーはターゲット インデックス(TI)ポイントの累積を行います。これらのインデックスの詳細については、第 6 章「インデックス:ランキング動作の変更」を参照してください。
[ホストがボットに感染:C&C 行動成功 (Bot Infected Host – Successful C&C Activity)]	このアラームは、ネットワーク内のホストが C&C サーバーの一覧に表示される C&C サーバーと通信し、応答を受信し、そのためにボットネットのメンバーとなったことを示します。C&C サーバーは、ネットワークの内部または外部のいずれかになります。通信は、双方向です。 内部ホストは、イニシエータとして、CI ポイントの累積を行います。接触している C&C サーバーも内部ホストである場合、その C&C サーバーは TI ポイントの累積を行います。
[ボットコマンドアンドコントロールサーバー(Bot Command & Control Server)]	このアラームは、自分のネットワーク内のホストがボットネットの C&C サーバーとして機能していることを示します。このアラームは、SLIC 脅威フィードが C&C サーバーとして特定した IP アドレスにネットワーク上の内部ホストが一致する場合に発生します。このアラームは、ソース IP アドレスだけを特定します。ターゲットは特定されません。

セキュリティ イベント	説明
[Bogon アドレスからの接続試行（Connection from Bogon Address Attempted）]	ネットワーク内のホスト サーバーとの通信を試みたが、失敗した外部 Bogon ホストのインスタンスを検出します。Bogon プレフィックスは、通常はインターネット ルーティング テーブルには現れないルートです。
[Bogon アドレスからの接続成功（Connection From Bogon Address Successful）]	ネットワーク内のホスト サーバーとの通信に成功し、クライアントとして機能している外部 Bogon ホストのインスタンスを検出します。Bogon プレフィックスは、通常はインターネット ルーティング テーブルには現れないルートです。
[ToR からの接続試行（Connection from Tor Attempted）]	何者かが現在の Tor ネットワークの出口ノードからの接続に失敗しました。Tor は、インターネットの匿名化サービスです。
[ToR からの接続成功（Connection from Tor Successful）]	ネットワーク上の 1 つ以上のホストが現在の Tor ネットワーク出口ノードからのトラフィックを受信しています。Tor は、インターネットの匿名化サービスです。
[Bogon アドレスへの接続試行（Connection To Bogon Address Attempted）]	外部 Bogon ホストとの通信に失敗したネットワーク内のホストのインスタンスを検出します。Bogon プレフィックスは、通常はインターネット ルーティング テーブルには現れないルートです。
[Bogon アドレスへの接続成功（Connection To Bogon Address Successful）]	公共のインターネットに割り当てられていない、ネットワーク内部および外部の Bogon IP アドレス間の双方向トラフィックのインスタンスを検出し、その通信が行われたことについてアラートを発生します。Bogon プレフィックスは、通常はインターネット ルーティング テーブルには現れないルートです。
[ToR への接続試行（Connection to Tor Attempted）]	アクティブな内部ホストの 1 つが現在の Tor ネットワーク エントリー ノードへの接続に失敗しました。Tor は、インターネットの匿名化サービスです。
[ToR への接続成功（Connection to Tor Successful）]	ネットワーク上の 1 つ以上のホストが Tor ネットワークにトラフィックを送信しています。Tor は、インターネットの匿名化サービスです。
[内部 Tor エントリー検出（Inside Tor Entry Detected）]	アクティブな内部ホストの 1 つが Tor のエントリー ノードとして機能しています。Tor は、インターネットの匿名化サービスです。
[内部 ToR 発信検出（Inside Tor Exit Detected）]	アクティブな内部ホストの 1 つが Tor の出口ノードとして機能しています。Tor は、インターネットの匿名化サービスです。

（注）:

これらのアラームの詳細については、Stealthwatch Web アプリケーションのオンラインヘルプにある「セキュリティイベントリスト」のトピックを参照してください。

9

原因の特定

概要

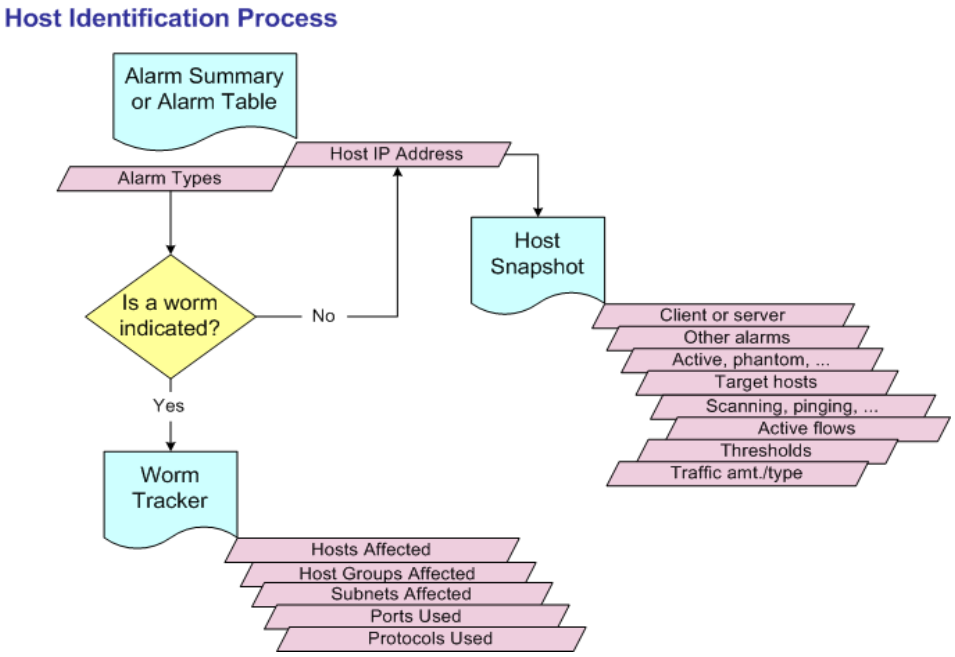
これまで学んできたように、脅威を処理するにはまず、アラームの原因となっているホスト（つまり、「ソース ホスト」）を特定します。この章では、脅威を処理する方法に関して詳細な情報を得た上での決定を行えるよう、SMC を使用して、ソース ホストに関する情報を収集する方法について説明します。

この章は、次の項で構成されています。

- 特定プロセス
- アラームのまとめ
- アラーム テーブル
- グローバル検索
- ホスト スナップショットからの詳細の取得
- 動作は正常か
- どのホストが同じ特性を共有しているか

特定プロセス

アラーム条件に関して何をすべきかについて評価することは、ソース ホストの IP アドレスの検索と同じくらい簡単です。ただし、他の場合に、同様にホストやアラームについての詳細が必要になります。どちらにしても、アラーム概要とアラーム テーブルは、評価に役立ちます。次の図は、不審なホストを特定する上で従うべきプロセスを示しています。

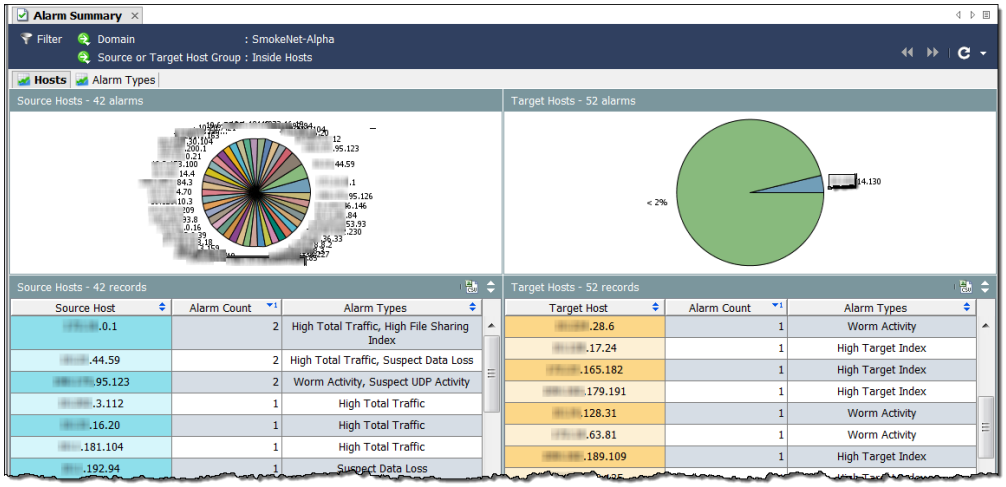


(注):
「再犯者」かどうかが簡単に分かるように、ネットワーク上で問題を起こしたホストの記録を保管します。

アラームのまとめ

おそらく、ホストを特定する最も簡単な方法は、アラームのまとめを使用することです。このドキュメントを開くには、ドメイン、エクスポータ、または FlowSensor を右クリックし、ポップアップ メニューから、[状態(Status)] > [アラームのまとめ(Alarm Summary)] を選択します。

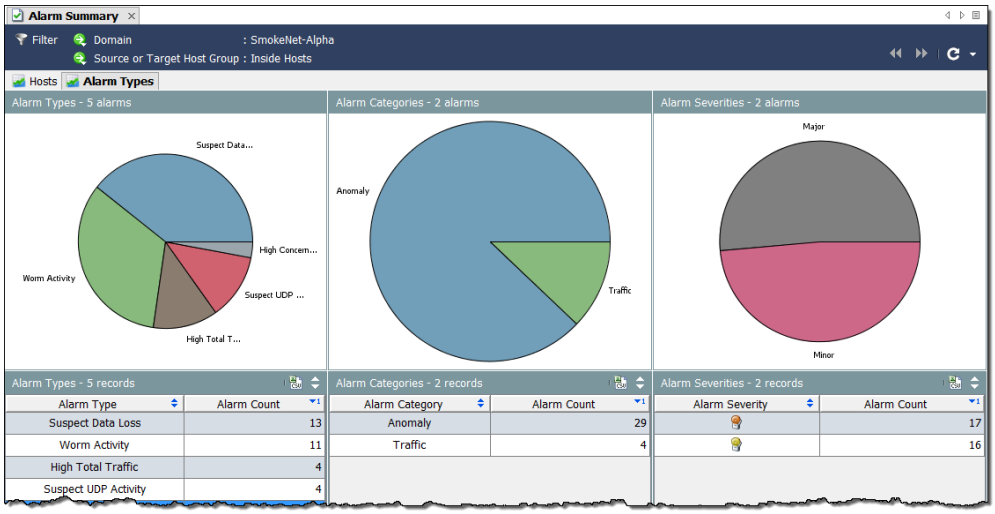
ここでは、種類、カテゴリー、重大度レベル、ソース ホストの IP アドレス、およびターゲット ホストの IP アドレス別のネットワークに上のすべてのアラームのグラフ表示を見ることができます。次の例では、[ホスト(Hosts)] タブで、ソース ホストの IP アドレスを簡単に表示することができます。



このドキュメントから移動するには、次の操作のいずれかを実行します。

- ホスト スナップショットを見るには、[ホスト(Hosts)] タブにあるホストの IP アドレスをダブルクリックします 。
- アラーム テーブルのフィルタ処理されたビューを取得するには、[アラームカウント(Alarm Count)] 列または [アラームの種類(Alarm Types)] 列をダブルクリックします。

[アラームの種類(Alarm Types)] タブをクリックして、別のビューを表示します。



このドキュメントから移動するには、次の操作のいずれかを実行します。

- アラーム テーブルのフィルタ処理されたビューを取得するには、[アラームの種類(Alarm Types)] タブ上のグラフやテーブルの項目をダブルクリックします。
- その項目に関連付けられたアラームのみを表示するよう事前フィルター処理されたアラーム テーブルを表示するには、列または円グラフのいずれかの項目をダブルクリックします。

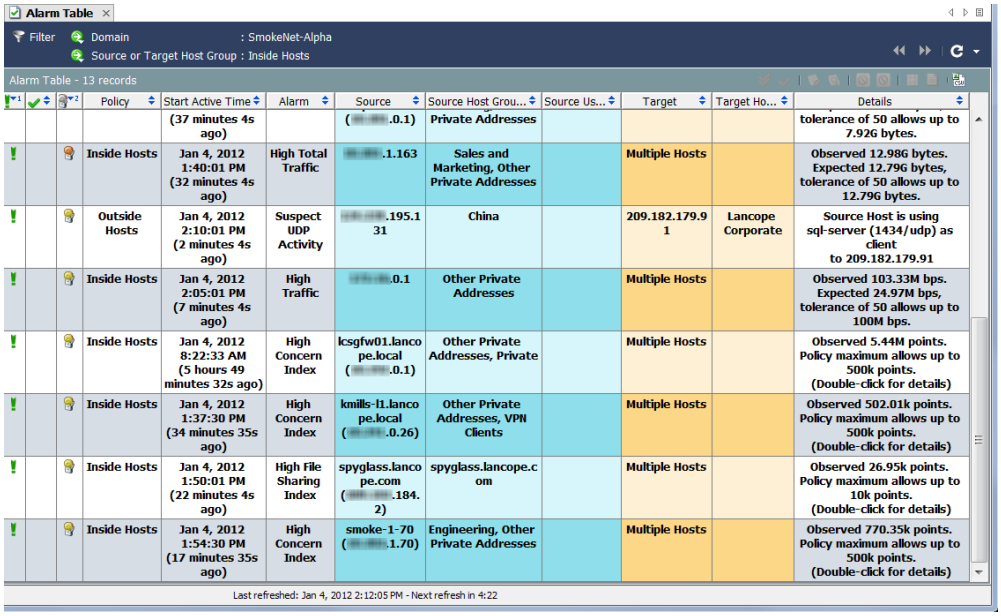
  たとえば、[アラームの種類(Alarm Types)] 列内の [高懸念インデックス(High Concern Index)] アラームをダブルクリックすると、アラーム テーブルには、[高懸念インデックス(High Concern Index)] アラームのみが表示されます。

(注):
各アラームの詳細については、Stealthwatch デスクトップクライアントのオンラインヘルプを参照してください。

アラーム テーブル

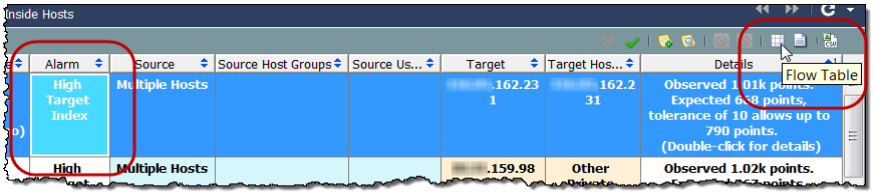
アラームについての詳細については、アラーム テーブルを参照してください。このドキュメントを開くには、ドメイン、Stealthwatch フロー コレクタ、ホスト グループ、エクスポータ、または FlowSensor を右クリックし、ポップアップ メニューから、[状態(Status)] > [アラーム概要(Alarm Summary)] を選択します。

アラーム テーブルは、これらの質問(「アラームの原因はなんですか」や「どのくらい重大ですか」)に回答する上で役に立ちます。デフォルトでは、アラーム テーブルには、発生元である Stealthwatch Flow Collector の最後のアクティブな時間以降発生したすべてのアクティブなアラームが表示されます。



ほとんどの SMC ドキュメントのように、アラーム テーブルには、ドキュメントを開くレベルに対応するデータが表示されます。たとえば、ドメイン レベルでアラーム テーブルを開くと、表示されるアラームは、全体的にドメインに関連したものになります。ホスト グループ レベルでアラーム テーブルを開くと、表示されるアラームは、全体的にホスト グループとそのサブ ホスト グループのみに関連したものになります。

アラームを表示するだけでなく、アラーム テーブルによって、アラームを承認、閉じる、メモの追加を行なうことができます(ログイン権限に応じて)。アラームをクリックして、[フローテーブル(Flow Table)] ボタンをクリックし、そのアラームに関連付けられているすべてのフローを含むフロー テーブルを表示できます。

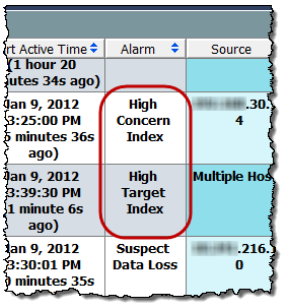


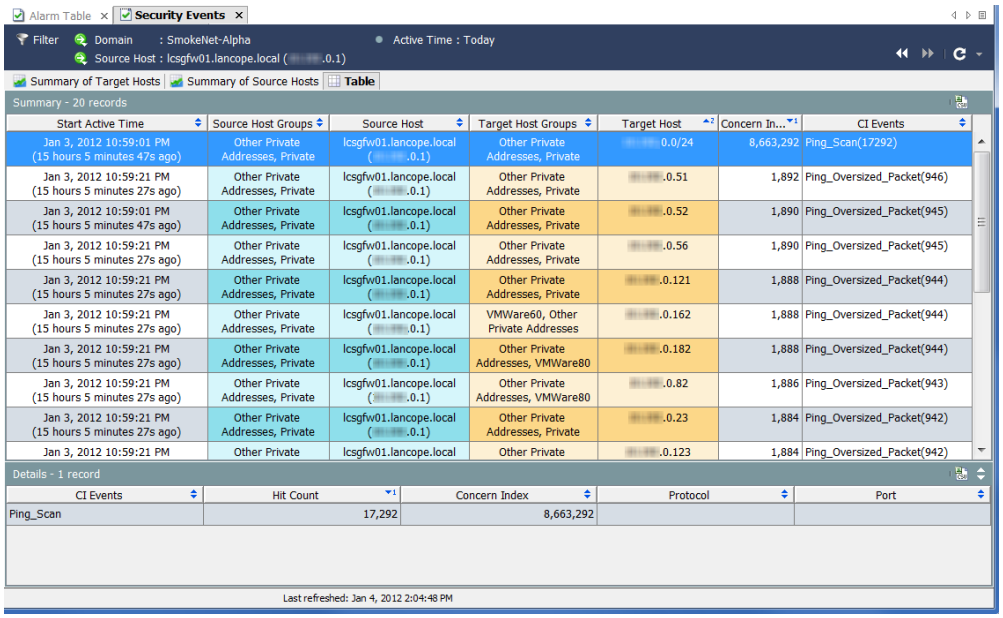
アラームは、アラームの原因となった状態が存在しなくなるまでアクティブなままになります。必要に応じて、アラーム ポイント閉じることができる点で、アラームは、非アクティブになります。アクティブなアラームを承認することができますが、閉じることはできません。非アクティブなアラームのみを閉じることができます。

アラーム テーブルが提供するもう一つの利点は、次の操作を実行できることです。

- アラームの承認または不承認
- アラーム メモの追加または表示
- ホストのブロックまたはブロック解除(つまり、アラーム軽減)

アラーム テーブル内の [高懸念インデックス(High Concern Index)] アラームまたは [高ターゲット インデックス(High Target Index)] アラームをダブルクリックすると、次の例に示すように、[セキュリティ イベント(Security Events)] ドキュメントが表示されます。このドキュメントには、アラームを発生させたセキュリティ イベントのデータが表示されます。





（注）:

アラームへの対応の詳細については、第 10 章「アラームへの対応」。を参照してください。

グローバル検索

グローバル検索機能によって、特定の項目に対する(すべてのドメイン上の)すべてのドキュメントを検索することができます。メイン ツールバーの [検索(Search)] フィールドでは、完全な文字列、部分文字列、またはワイルド カード(*)を含めた部分文字列を使用して、次の項目を検索できます。

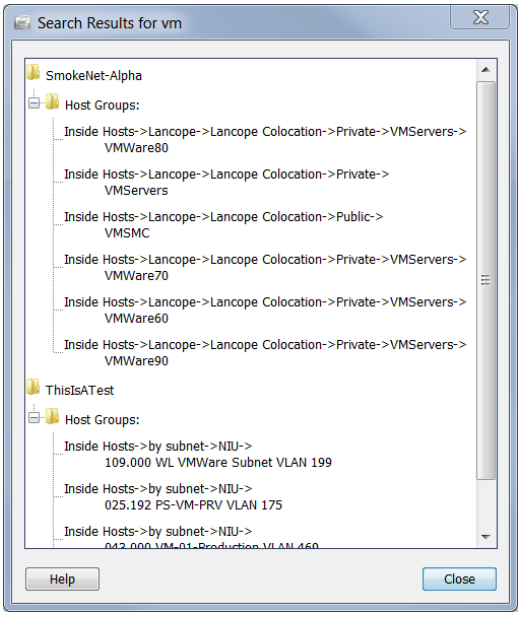
- アラーム ID
- ホストまたはエクスポータの IP アドレス
- 以下の名前:
  - エクスポータ
  - ホスト グループ
  - サーバー
  - ユーザー

(注):
検索結果は、ユーザー名に関連付けられているデータの権限と機能の権限に従って制限されます。

ヒント:
検索するには、[検索(Search)] ドロップダウン リスト ボックスから、以前に検索した項目を選択し、**Enter** キーを押します。

検索を実行するには、ツールバーの [グローバル検索(Global Search)] ボックス内をクリックします。

検索項目を入力して、**Enter** を押します。[検索結果（Search Results）] ダイアログが開きます。

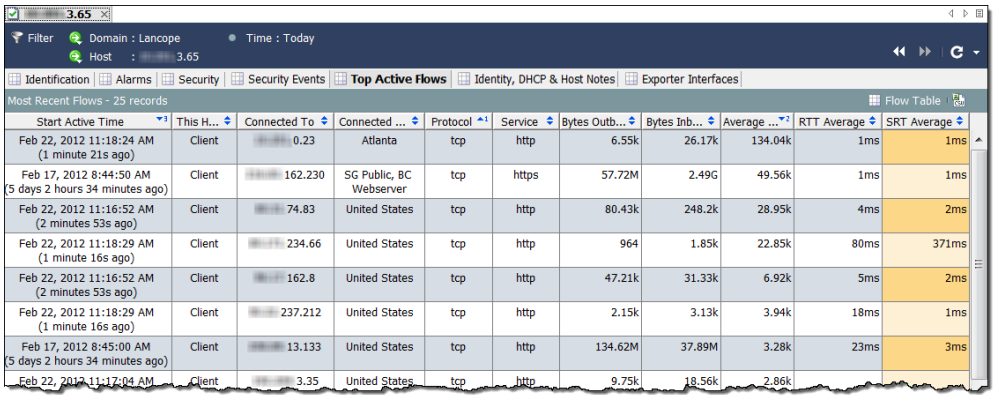


次のいずれかを実行します。

- 検索結果をダブルクリックします。
- 検索結果を右クリックし、ポップアップ メニューから目的の項目を選択します。

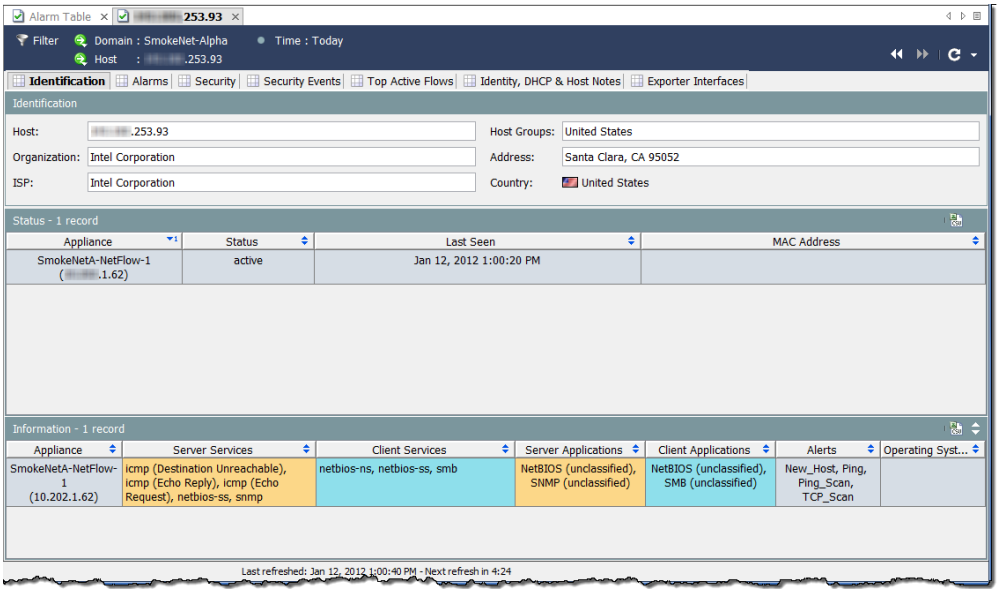
ホスト スナップショットからの詳細の取得

ホストの行動の変化を調査する際、ホスト スナップショット ドキュメントで最初に立ち止まることが多くあります。このドキュメントは、ネットワーク内の各ホストの最も包括的な情報を提供します。



ほとんどの場合、Stealthwatch デスクトップクライアント内の任意の場所にあるホストの IP アドレスをダブルクリックするだけで、そのホストのホスト スナップショットを参照できます。ホスト スナップショットには、次の情報が含まれています。

- ホストに関連付けられた最近のフロー
- 今日まで最高量のトラフィックをもつフロー
- ホストにログオンしたユーザーの名前
- ホストに関連付けられているアラーム
- フローを運んでいるエクスポータ インターフェイス
- アドレスとインターネット サービス プロバイダ（ISP）と併せた、ホストの IP アドレスが割り当てられている組織（該当する場合）
- ホストの状態とネットワーク上で最近確認された通信
- ホストに関連付けられているアラートの他、ホストのサーバーまたはクライアント プロファイルとオペレーティング システム（OS）

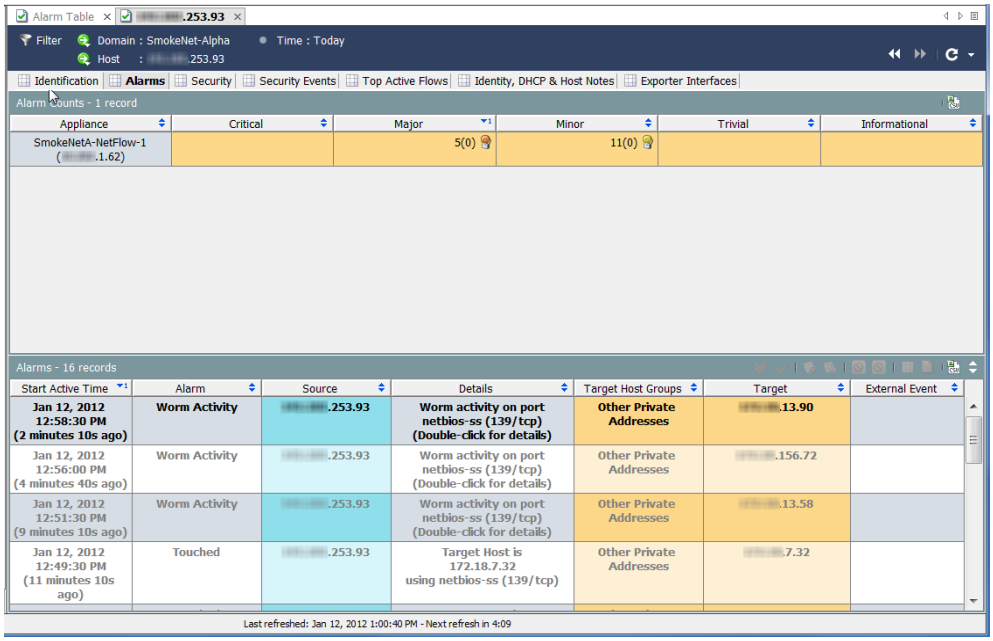


上記の例では、[識別(Identification)] タブで選択したホストに関する次の情報を見ることができます、

- ホストには、プライベート IP アドレスがあります。
- システムは最後に、2012 年 1 月 12 日にこのホストに対する行動を見ました。
- システムは、他の多くのサービスの中で、netbios トラフィックがサーバーとクライアントの両方としてホストの発生を報告しました。

ホストが他のアラームを発生させたか

ホスト スナップショットの [アラーム(Alarms)] タブは、問題のホストが他のアラームを発生させたかどうか、その場合の回数と種類を示します。



ホストが発生させるアラームの数が多いほど、心配が多くなります。特定の状況に調整できるよう、重大度を調整できます。

上記の例では、選択したホストに関する次の情報を参照してください。

- [アラーム カウント(Alarm Counts)] テーブルには、アラームの種類とカテゴリーに基づいて、対応する Stealthwatch アプライアンスによって報告されるように、選択したホストが発生させたアラーム数が表示されます。この例では、Stealthwatch アプライアンスは、11 個の軽度のアラーム状態と 5 個の重度のアラーム状態を報告しました。

(注):
列の見出しを右クリックし、テーブルに表示したい特定のアラームの種類に列を選択できます。

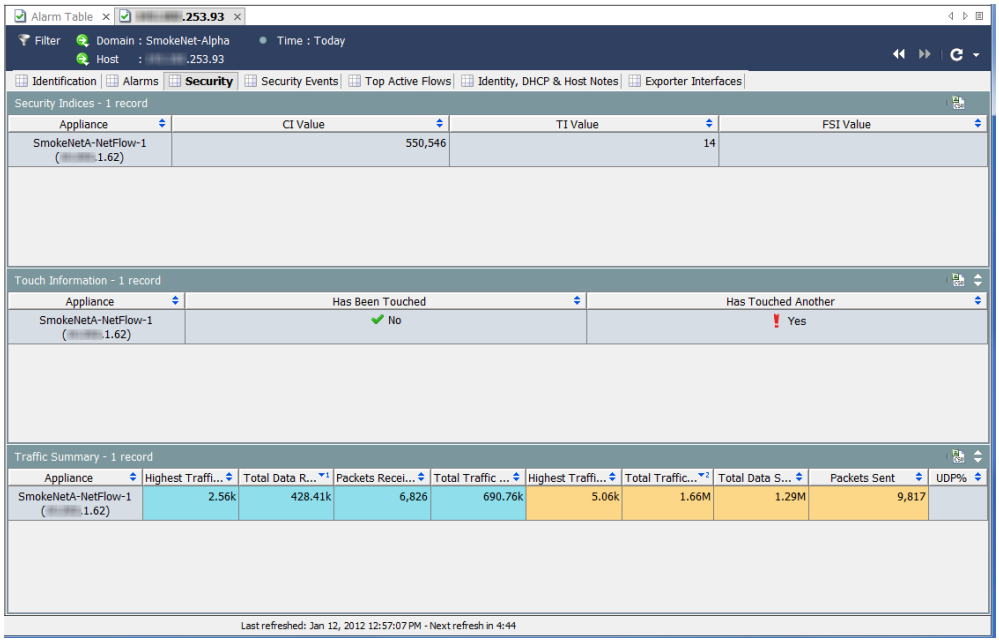
- アラーム テーブルには、最後のアーカイブ時間以降に選択したホストが発生させた個々のアラームに関する詳細なデータが表示されます。この場合、このホストがいくつかの [ワームの活動(Worm Activity)] アラームを発生させたことが分かります。

(注):
ホスト ポリシー マネージャーを開いて、これらの値に対してなされたポリシー設定を確認および調整できます。

このホストが感染している可能性があると疑っているため、次の手順は、感染源と影響を受けているホストの数を特定します。

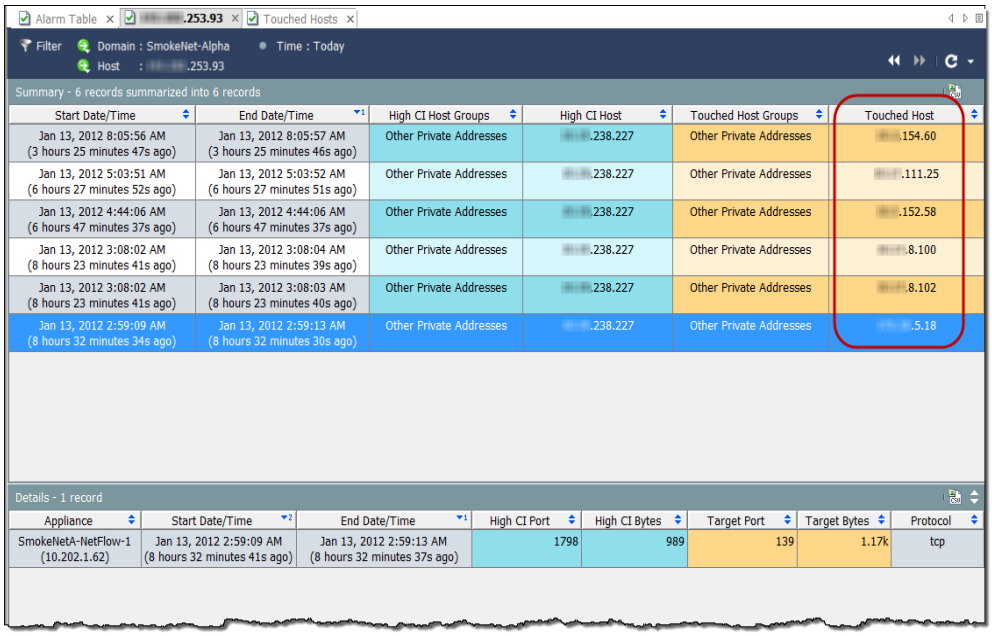
脅威はどのくらい広まっているか

ワームが表示されているかどうかに関係なく、例に示すホスト スナップショットの [セキュリティ(Security)] タブに移動して、問題のホストがその他のホストに接触したか、あるいはその他のホストに接触されたかを確認できます。[接触情報(Touch Informatio)] テーブルは、このホストがその脅威を他のホストに広めたかどうかの他、このホストに対する脅威が他の何処かに発生したかを判断でする上で役に立ちます。



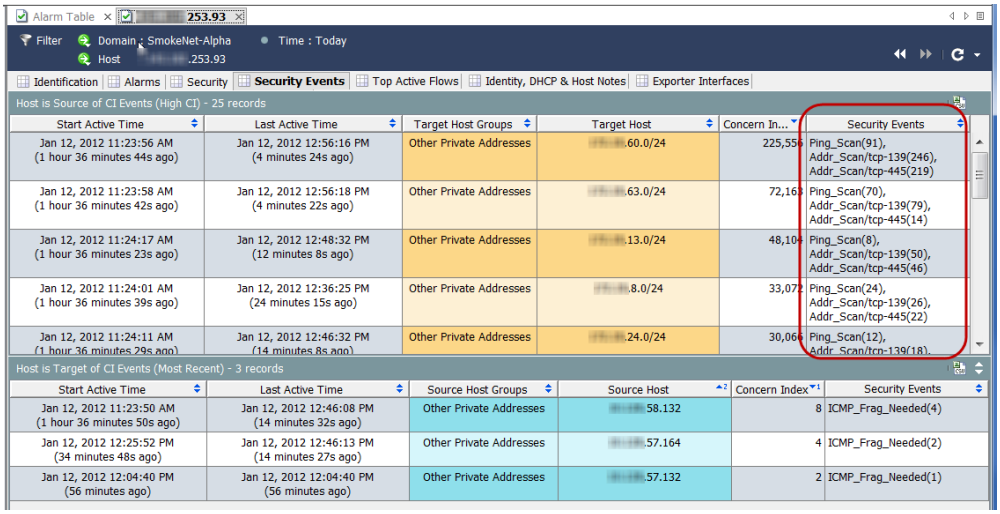
さらに、[セキュリティ インデックス(Security Index)] テーブルには、このホストが Stealthwatch アプライアンスあたり各種インデックスを制限をどれだけ超えたかが示されます。[トラフィックの概要(Traffic Summary)] テーブルには、このホストがどのくらいの量のトラフィックを送受信したかが示されますが。これは、ファイル共有の活動を決定する上で役に立ちます。

上記の例では、このホストが接触したその他のホストの数を確認する必要があります。これを行うには、[他に接触した(Has Touched Another)] 列に移動し、[はい(Yes)] をクリックします。[接触されたホスト(Touched Hosts)] ドキュメントが開きます。高 CI ホストが少なくとも 6 回ターゲット ホストに触れたことを [接触されたホスト(Touched Hosts)] 列で確認できます。

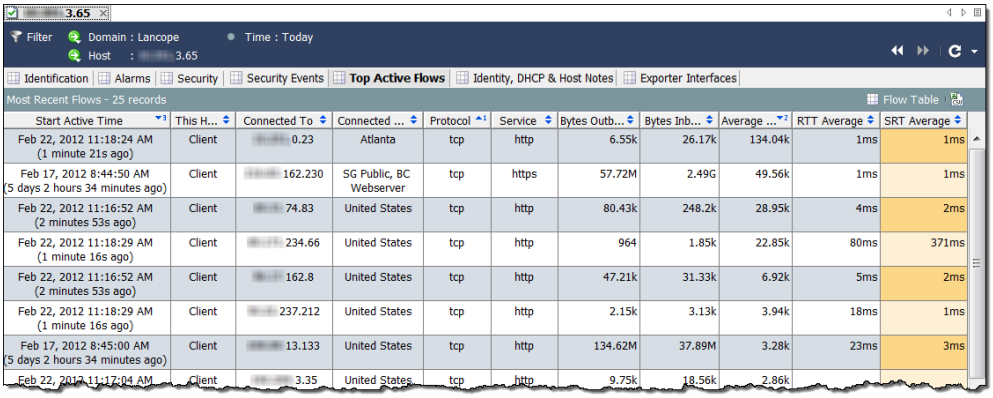


前のテーブルの行のいずれかを選択すると、下部にある [詳細(Details)] セクションで、高 CI ポートとバイト、ターゲット ポートとバイト、および影響を受けているホストに使用されているプロトコルなどの詳細を確認できます。

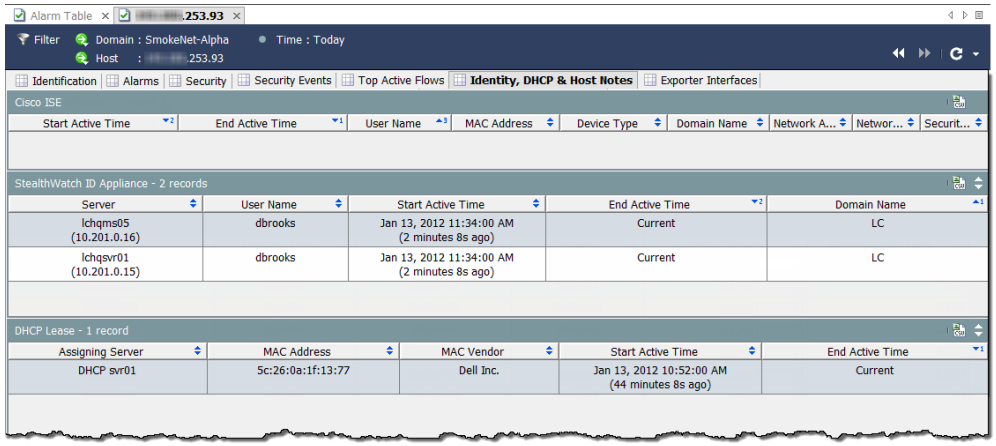
セキュリティ イベントの種類を確認するには、ホスト スナップショットの [セキュリティイベント(Security Events)] タブをクリックします。例では、セキュリティ イベントの種類は、アドレス スキャンと Ping スキャンになります。



このホストに対する上位のアクティブなフローを表示する場合は、[上位のアクティブなフロー(Top Active Flows)] タブをクリックします。

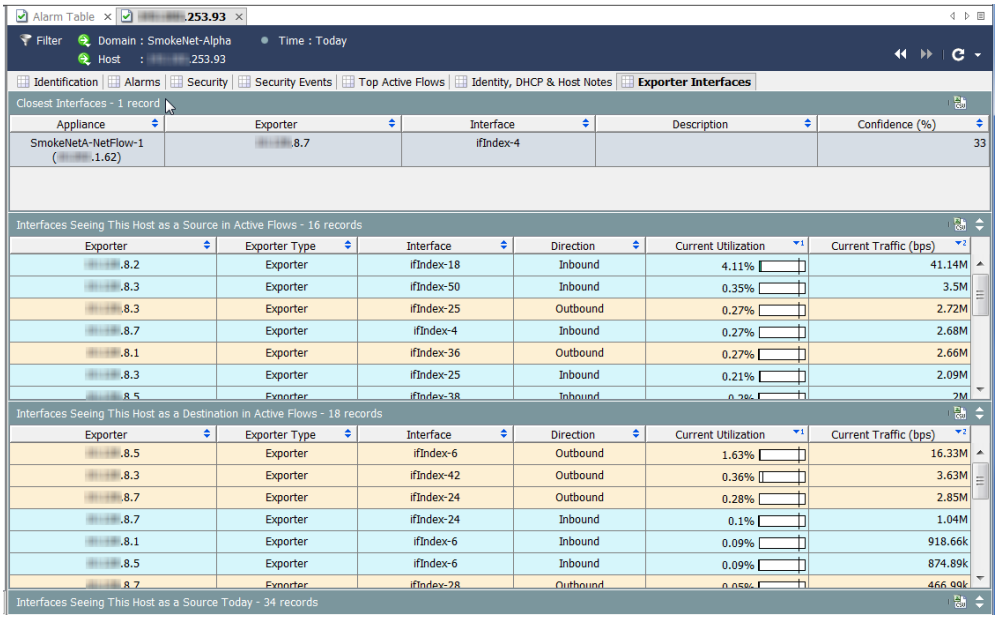


ドメイン内のどのユーザーが IP アドレスに関連付けられているかを特定する場合、[ID と DHCP、ホストノート(Identity, DHCP & Host Notes)] タブをクリックします。



(注):
ユーザー ID データを取得するには、Stealthwatch IDentity アプライアンスまたはシスコ ISE アプライアンスが必要です。

最も近いエクスポータに関する追加情報を表示し、ホストがアクティブなフローのソースまたは宛先のどちらとして見られているかを判別する場合は、[エクスポータインターフェイス(Exporter Interfaces)] タブをクリックします。



この時点で、ソース ホストとターゲット ホストの両方を特定する十分な情報があります。これで、組織のポリシーあたりのクリーンアップ処理を開始できます。たとえば、次のいずれかの動作を実行できます。

- 各ホスト上でのアンチ ウイルス ソフトウェアの実行
- すべてのホストが同じホスト グループにある場合のホスト グループ全体のブロックまたは分離
- データが交換されているポートのブロック

動作は正常か

この時点までは、アラーム状態は、脅威の結果と仮定してきました。しかし、アラームの原因となった動作が問題のホストにとって完全に正常の場合はどうなるでしょうか。

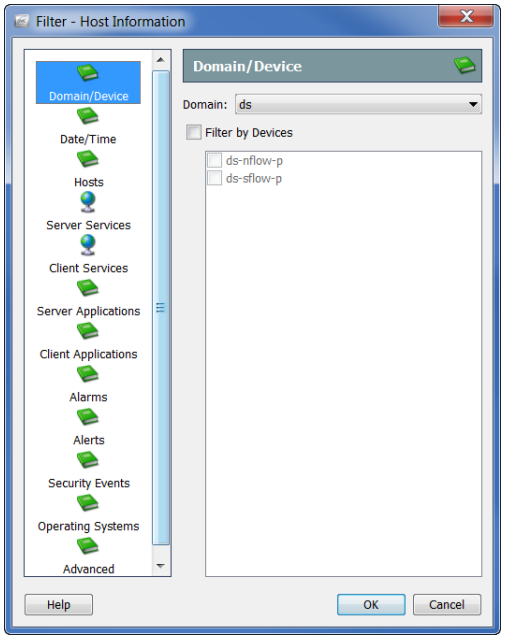
たとえば、電子メール サーバーは、特に電子メール トラフィックなど多くの確認をします。ただし、そのサーバーに対するパラメータ設定が低すぎると、そのサーバーに対して複数のメールおよびトラフィックのアラームが表示されます。この場合、パラメータをより現実的な限界まで上げ、確認している不要なアラームの数を減らすだけで解決できます。その他の場合、ポリシーを編集するする必要がある場合があります。

（注）：

パラメータの調整およびポリシーの編集の詳細については、第 10 章「アラームへの対応」。を参照してください。

どのホストが同じ特性を共有しているか

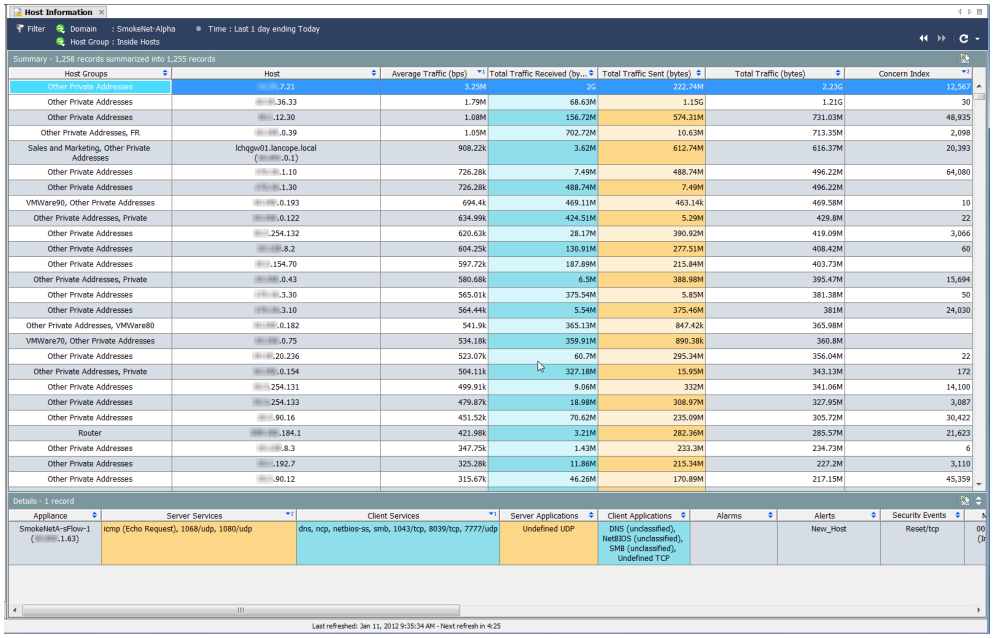
特定のサービスを使用するか、またはその他の一般的な特性を共有して、特定のアラームを発生させているホストをすべて見るには、[ホスト情報(Host Information)] フィルターを使用します。このフィルタにアクセスするには、メイン メニューから、[ホスト(Hosts)] > [ホスト情報(Host Information)] を選択します。



[フィルター(Filter)] の [ホスト情報(Host Information)] ダイアログでは、これらのパラメータ内に収まるすべてのホストに対してクエリーを実行する特定のパラメータを選択することができます。たとえば、許可されていないサービスまたはアプリケーションを使用しているまたはワームの活動アラームを発生させている特定のホスト グループ内のすべてのホストにフィルター処理を行えます。

(注):
情報クエリー(IQ)を実行しているため、このプロセスは、「ホスト IQ の実行」と呼ばれることがあります。

目的のパラメータを指定した後、[OK] をクリックして、要求されたデータのあるホスト情報ドキュメント（つまり、ホスト IQ）を表示します。



（注）：

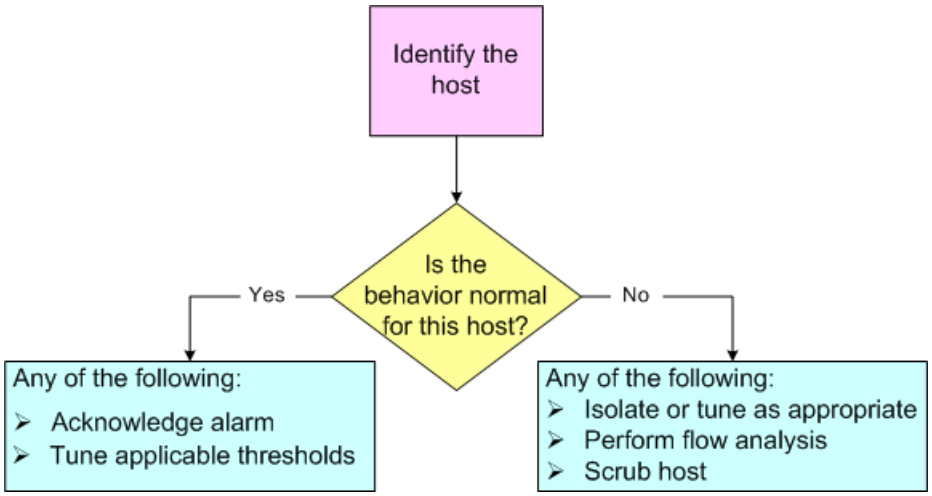
高懸念インデックス アラームとして TCP_Scan アラートを引き起こしているすべてのホストをフィルター処理する場合、最も可能性の高いいくつかの方法で感染しているホストの一覧が結果に含まれます。

10

アラームへの対応

概要

次の図は、ネットワークへの脅威に対処する場合の基本的な手順を示しています。



ご覧の通り、アラームに対処するには、次の 3 つの質問に回答する必要があります。

- どのホストがアラームの原因となりましたか。
- このアラームを発生させた動作は、このホストには正常ですか。
- 他にどのホストが影響を受けますか（存在する場合）。

（注）：
問題ないと分かっている活動に対して大量の不要なアラームが発生していると分かる場合もあるでしょう。確認している不要なアラームの数の削減の詳細については、第 11 章「不要なアラームの削減」を参照してください。

上記の質問に回答したら、次に、SMC のソフトウェアを使用して、アラームに対応する方法を決定できます。この章には、アラームに対応する際に取る最も一般的な措置が含まれています。

（注）:
アラームに対応するときに実行することがあるその他の手順については、Stealthwatch デスクトップクライアントのオンラインヘルプを参照してください。

この章は、次の項で構成されています。

- アラームに対応する方法
- Stealthwatch 軽減機能

アラームに対応する方法

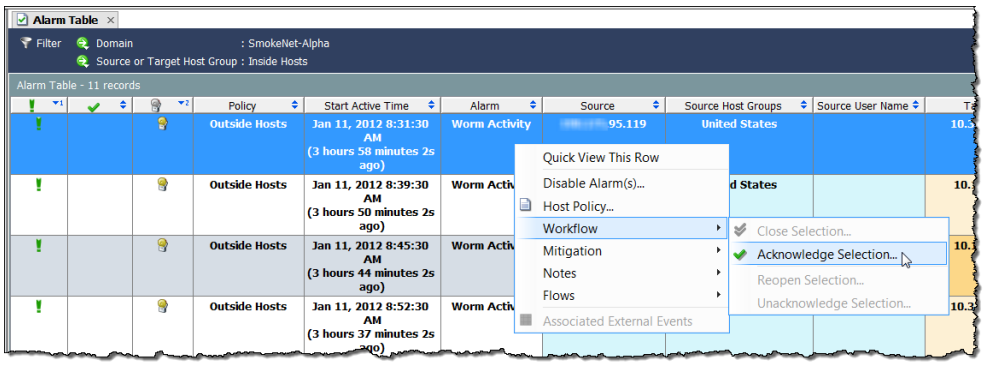
アラームに対応する方法はいくつかあります。アラームを承認する、アラームを承認しない、アラームを閉じる、および閉じたアラームを再度開くことができます。これらの特定の手順については、次のセクションを参照してください。

アラームを承認

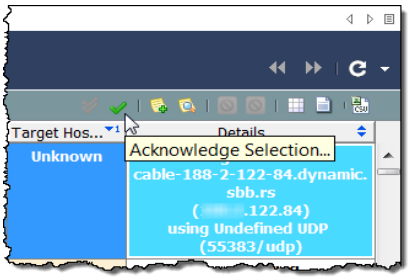
アラームを承認すると、そのアラームを調査していることを示すことになります。これは、ワークフローやアラームは調査されていることを他のチーム メンバーに意識させることにとって有益です。アラームを承認する前に、アラームの承認は、必要に応じて取り消すことができることに留意してください。

アラームは、アラームがアクティブまたは非アクティブであるかに関係なく、承認済みまたは未承認にできます。SMC を使用して、アラームに応答するには、次の手順を実行します。

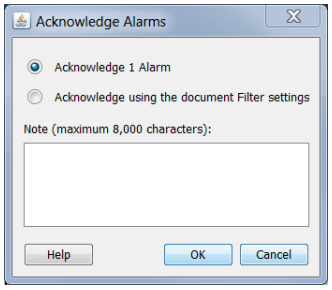
1. アラーム テーブルで、アラームを右クリックして、[ワークフロー（Workflow）] > [承認（Acknowledge）] を選択します。



また、アラームをクリックして、[アラームテーブル（Alarm Table）] ツールバーの [承認選択（Acknowledge Selection）] ボタンをクリックします。



[アラームを承認] ダイアログが開き、アラームが閉じられる理由を説明するメモを入力することを求められます。

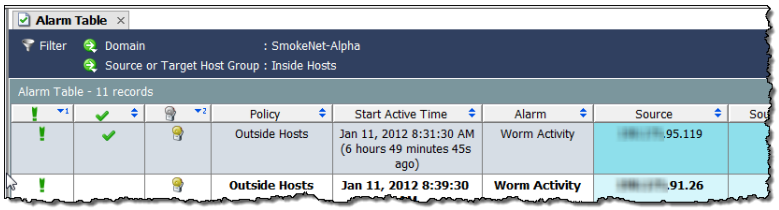


2. アラームを承認するか、ドキュメント フィルター内の設定を使用することを承認するかを指定します。アラームを承認する場合の意味を意識するよう、利用できるオプションの次の説明を参照してください。

   - [(x 個の)アラームを承認(Acknowledge [x] Alarm(s))]: アラーム テーブルに現在表示されているアラームのみを承認します。ここでの x は、選択したアラームの総数です。これをクリックすると、システムは、各アラームを 1 つずつ承認します。そのため、1,000 以上などの大量のアラームがある場合、システムは、このプロセスを完了するのにかなりの時間を要します。
   - [ドキュメントのフィルタ設定を使用を承認する(Acknowledge using the document Filter settings)] – 承認プロセス中に*発生する可能性のある新しいアラームを含め*、1 つずつではなく、現在のフィルタ設定内に含まれるすべてのアラームを一括で承認します。たとえば、アラーム テーブル フィルターを [通常(Trivial)] アラームのみを表示するよう設定すると仮定し、この設定に基づいて、すべてのアラームを承認することを選択します。システムは、アラーム テーブルで確認している [通常(Trivial)] アラームだけでなく、確認していない承認プロセスが進行中である間に生成される可能性のある [通常(Trivial)] アラームも承認します。

   (注):
   [ドキュメントフィルタ設定を使用した承認(Acknowledge using the document Filter settings)] オプションは、アラームを一括で承認するため、特に 1,000 個以上のアラームがある場合には、その他のオプションよりもはるかに高速です。しかし、このオプションを選択することで、確認したことのないアラームを承認できることを知る必要があります。

3. Click テキスト入力フィールド内をクリックして、アラームを承認する理由を入力し、[OK] をクリックします。これらの列を表示した場合は、[確認済み(Acknowledge)] 列にチェックマーク が表示され、[最後のメモ(Last Note)] 列にメモが表示されます。そのアラームのテーブル行内のテキストは、太字解除されます。



(注):

[承認済み(Acknowledge)] および [最後のメモ(Last Note)] 列を見るには、列のヘッダーを右クリックし、ポップアップ メニューから適切なオプションを選択します。

アラームを不承認

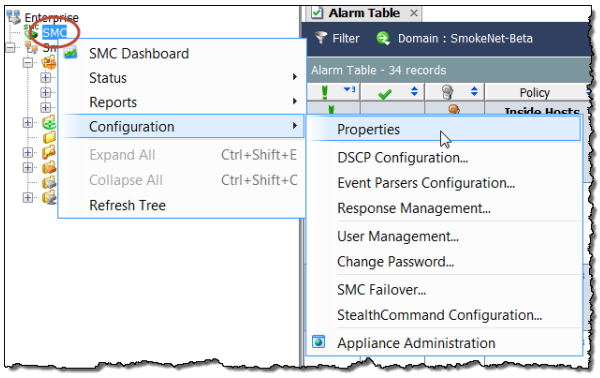
SMC によって、1 つ以上の承認済みアラームを未承認にできます。たとえば、誤って、いずれかのアラームを承認した場合、次の手順を実行したい場合があります。

1. アラーム テーブルには、未承認にしたい承認済みアラームが表示されます。必要に応じて、アラーム フィルターを使用します。
2. 未承認にしたいアラームを右クリックして、[ワークフロー(Workflow)] > [不承認選択(Unacknowledge Selection)] を選択します。[アラームを不承認(Unacknowledge Alarms)] ダイアログが開きます。
3. アラーム メモを入力し、[OK] をクリックします。
4. 承認したい各アラームに対して、手順 2 および 3 を繰り返します。

アラームを閉じる

アラームが解決されたことに満足していることを示したい場合、アラームを閉じることができます。アラームを手動で閉じる必要はありません。

アラームが非アクティブになると、SMC プロパティの [データ保持(Data Retention)] 上のアラーム テーブルに指定されている日数よりも古い場合は、自動的にデータベースから削除されます。このページにアクセスするには、[エンタープライズ(Enterprise)] ツリーで SMC のアイコンを右クリックして、[設定(Configuration)] > [プロパティ(Properties)] をクリックします。

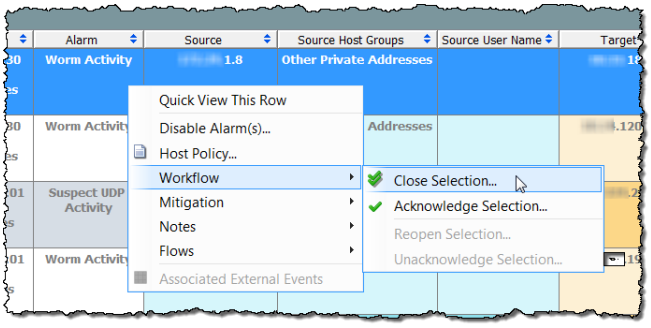


アラームを閉じる前に、次の点に注意してください。

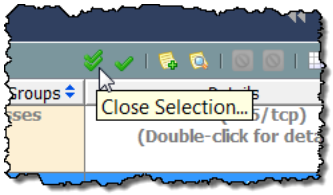
- アクティブなアラームは閉じることができません。
- 特定のホストに対するアラームを閉じた場合、そのホストが次のアクティブな時間の前に再度そのアラームを発生させる場合があります。
- 必要な場合、アラームを閉じても、取り消すことができます。

SMC を使用して、アラームを閉じるには、は、次の手順を実行します。

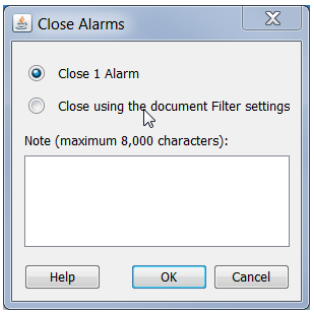
1. 非アクティブなアラームが表示されるように、[アラーム テーブル フィルター(Alarm Table filter)] を変更します。これを行なうには、[アラーム テーブルフィルタ(Alarm Table filter)] ダイアログの [状態(States)] ページで、[現在のアクティブなアラームに基づくフィルタ(Filter on currently Active)]チェックボックスをクリックして、チェック マークを追加し、[非アクティブ(Inactive)] オプションをクリックします。
2. アラーム テーブルで、アラームを右クリックして、[ワークフロー(Workflow)] > [選択を閉じる(Close Selection)] をクリックします。



また、アラームをクリックして、[アラームテーブル(Alarm Table)] ツールバーの [選択を閉じる(Close Selection)] ボタンをクリックします。



[アラームを閉じる(Close Alarms)] ウィンドウが開き、アラームを閉じている理由を説明するメモを入力することを要求されます。



3. アラームを閉じるか、ドキュメント フィルターの設定を使用して閉じるかを指定します。アラームを閉じる意味を意識するよう、利用可能なオプションの次の説明を参照してください。

   - [(x 個の)アラームを閉じる(Close [x] Alarm(s))]:アラーム テーブルに現在表示されているアラームのみを承認し、閉じます。ここでの [x] は、選択したアラームの総数です。このオプションをクリックすると、システムは、1 つずつ各アラームを承認し、閉じます。そのため、1,000 以上などの大量のアラームがある場合、システムは、このオプションでこのプロセスを完了するのにかなりの時間を要します。
   - [ドキュメントフィルタ設定を使用して閉じる(Close using the document Filter settings)] :閉鎖プロセス中に*発生する可能性のある新しいアラームを含め*、1 つずつではなく、現在のフィルタ設定内に含まれるすべてのアラームを一括で承認し、閉じます。たとえば、アラーム テーブル フィルターを [軽度(Minor)] アラーム タイプのみを表示するよう設定すると仮定し、この設定に基づいて、すべてのアラームを閉じることを選択します。システムは、アラーム テーブルで確認している [軽度(Minor)] アラームだけでなく、確認していない閉鎖プロセスが進行中である間に生成される可能性のある [軽度(Minor)] アラームも閉じます。

(注):

「ドキュメントのフィルター設定を使用してを閉じる(Close using the document Filter settings)」オプションは、一括でアラームを閉じる、特に 1000 以上アラームがあれば他のオプションよりもはるかに高速です。しかし、このオプションを選択することで、確認したことのないアラームを閉じることができます。

4. Click テキスト入力フィールド内をクリックして、アラームを閉じる理由を入力し、[OK] をクリックします。これらの列を表示しなかった場合は、[終了(Closed)] 列にチェックマーク が表示され、[最後のメモ(Last Note)] 列にメモが表示されます。

(注):

[承認済み(Acknowledge)] および [最後のメモ(Last Note)] 列を見るには、列のヘッダーを右クリックし、ポップアップ メニューから適切なオプションを選択します。

閉じたアラームを再度開く

SMC では、1 つ以上の閉じたアラームを再度開くことができます。たとえば、誤って、いずれかのアラームを閉じた場合、次の手順を実行したい場合があります。

1. アラーム テーブルには、再度開きたい閉じたアラームが表示されます。必要に応じて、アラーム フィルターを使用します。
2. 再度開きたいアラームを右クリックして、[ワークフロー(Workflow)] > [選択を再度開く(Reopen Selection)] を選択します。
3. アラーム メモを入力し、[OK] をクリックします。
4. 承認したい各アラームに対して、手順 2 および 3 を繰り返します。

STEALTHWATCH 軽減機能

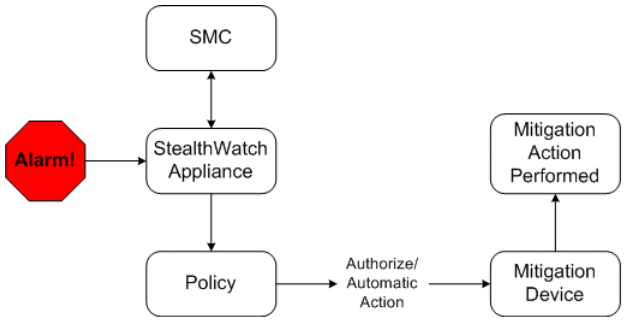
Stealthwatch ソフトウェアには、さまざまな脅威に対するシステムの対応を自動化するための脅威軽減機能があります。この機能を使用することで、特定のアラームに対応する方法について決定を下すのに必要な時間を減らすことができます。アラームが発生するとすぐにシステムがこれを行います。

Stealthwatch 軽減機能は、秒単位でインシデントを解決するのに役立ちます。希望する場合、この機能を設定して、すぐに軽減を実行するか（自動モード）、または最初に承認を求める（承認または手動モード）にできます。

Stealthwatch 軽減機能は、デフォルトでは無効になっています。これを有効にするには、このセクションで後述する次の手順を完了する必要があります。

1. 軽減を使用したいアプライアンスそれぞれに対して軽減装置を設定します（たとえば、ファイアウォールを定義します）。
2. 軽減機能を使用したいポリシーに対して軽減機能を有効にします。
3. 個々のアラームに対して必要な軽減動作を定義します。

次の図は、Stealthwatch 軽減機能のしくみの概要を示しています。



この機能を有効にし、その後で指定したアラームが発生すると、Stealthwatch は緩和デバイスに対し、設定されている緩和アクションの実行を要求するシグナルを送信します。この装置は、そのアラームに指定したポリシー設定に基づいて要求された動作を実行します。

（注）：
システムでは、放送リスト、または軽減ホワイト リストにあるホストに対して軽減を実行しません。これらのリストの詳細については、Stealthwatch デスクトップクライアントのオンラインヘルプを参照してください。

軽減装置の設定

Stealthwatch と緩和デバイス間の通信をセットアップするように SMC を設定する必要があります。いくつかのアプライアンスに同じ軽減装置を使用させたい場合、その装置に対して、それぞれのアプライアンスを個別に設定する必要があります。

(注):

また、軽減装置自体を設定して、Stealthwatch 装置から情報を受け取る必要がある場合もあるでしょう。詳細については、『Mitigation Device Configuration guide』を参照してください。このドキュメントは、Stealthwatch ユーザー コミュニティ Web サイトで検索できます(https://community.Cisco.com)。

アプライアンスごとに次の内、5 つまでの軽減装置の種類を設定できます。

- ブロケード INM
- シスコ ASA
- シスコ ガード
- シスコ ルータ(インターネットワーキング オペレーティング システム 11.3 以降)
- カスタム(Custom)
- ラドウェア ディフェンス プロ
- Stealthwatch SNMP 軽減インターフェイス

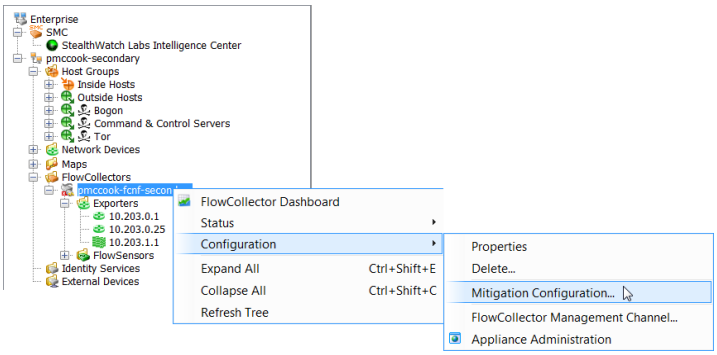
(注):

- これらの軽減装置の種類(ラドウェア ディフェンス プロを除く)はすべて、Stealthwatch モジュールでのみ使用できます。ラドウェア ディフェンス プロは、DDoS モジュールでのみ使用できます。
- Expect スクリプトを使用して、軽減アクションをカスタマイズする場合は、[カスタム(Custom)] オプションを選択します。ただし、予想されるスクリプトを使用する前に、サポートのためにシスコ カスタマー サポートに連絡することをお勧めします。

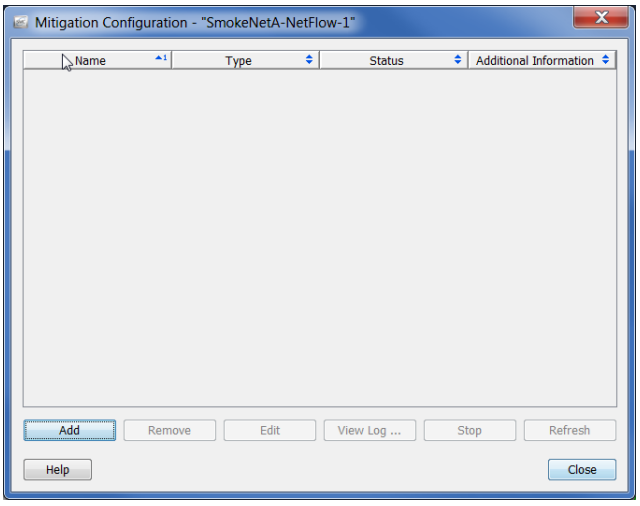
選択した軽減装置選択の種類によって、システムが実行できる軽減処置の種類が決まります。たとえば、特定の装置がソース IP アドレスからくるトラフィックのブロックをサポートするだけの場合があります。

SMC で軽減装置を設定するには、次の手順を実行します。

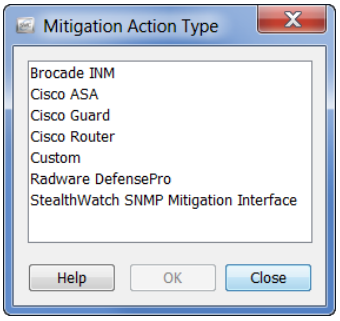
1. アプライアンス名を右クリックし、[設定(Configuration)] > [軽減設定(Mitigation Configuration)] を選択します。



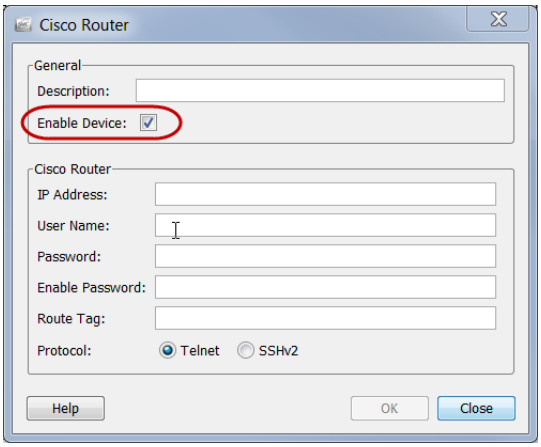
[軽減設定(Mitigation Configuration)] ダイアログが開きます。



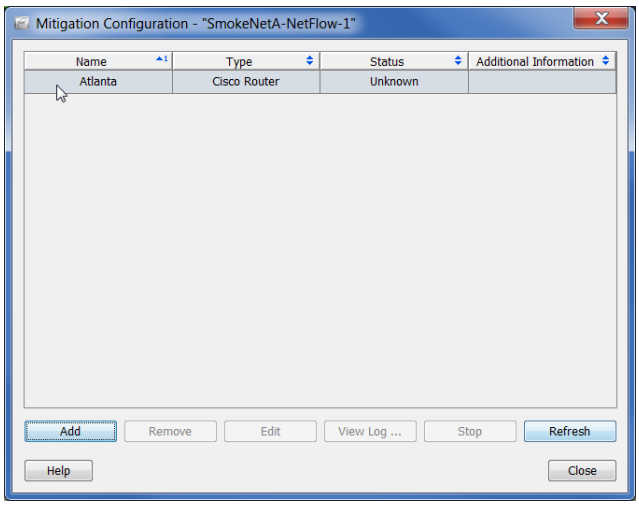
2. [追加(Add)] をクリックします。[軽減動作の種類(Mitigation Action Type)] ダイアログが開きます。



3. 使用したい軽減装置の種類をクリックして、[OK] をクリックします。選択したデバイス タイプに対して、デバイスの情報ダイアログが開きます。たとえば、[シスコルータ（Cisco Router）] をクリックした場合、シスコルータの情報ダイアログが開きます。



4. 上記の例で示すように、[装置を有効化（Enable Device）] チェックボックスにチェック マークが入っているかを確認します。この選択を行わない場合、デバイスは、Stealthwatch から情報を受信せず、緩和機能は作動しません。
5. 選択した装置に対する特定の ID 情報をすべて完了し、[OK] をクリックします。装置情報ダイアログが閉じ、追加した装置が [軽減設定（Mitigation Configuration）] ダイアログに含まれます。



6. このアプライアンスに追加する必要がある軽減装置のすべてを追加するまで、手順 2 ～ 5 を繰り返します。
7. 終了したら、[閉じる（Close）] をクリックして、[軽減設定（Mitigation Configuration）] ダイアログを閉じます。

次項で説明するように、これでホスト グループあたり軽減機能を有効にする準備が整いました。

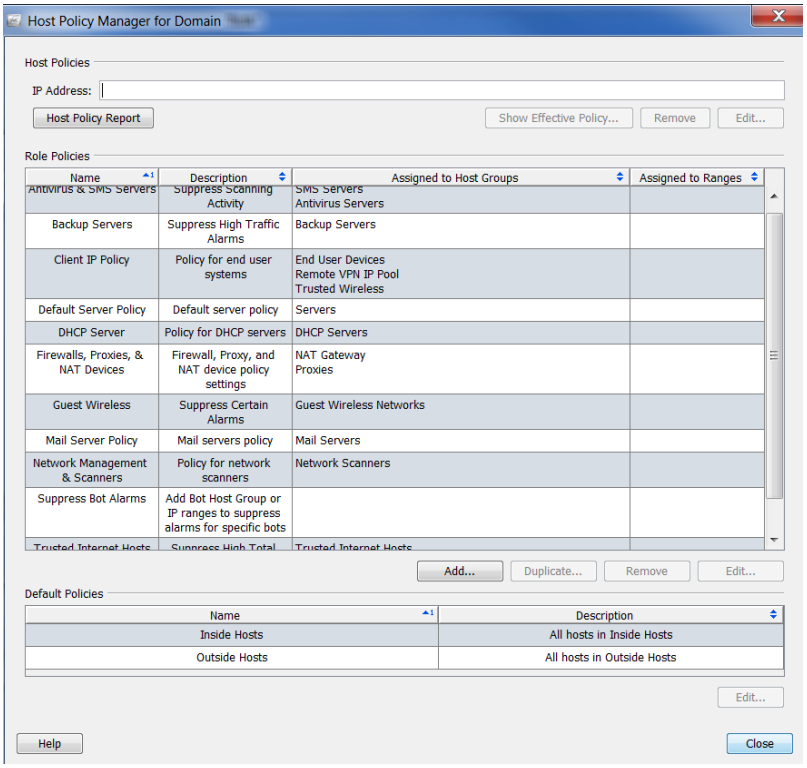
（注）：
軽減機能が作動するには、軽減装置を作動させる必要があります。

ポリシーに対する軽減機能の有効化

軽減装置を設定すると、1 つ以上のホスト グループに割り当てることができる、特定のポリシーに対して、Stealthwatch 軽減機能を有効にできます。たとえば、内部ホストのデフォルト ポリシーに軽減機能を有効したい場合があります。少数のホスト グループのみに対して、または特定のホスト IP アドレスに対してもこの機能を有効にすることができます。

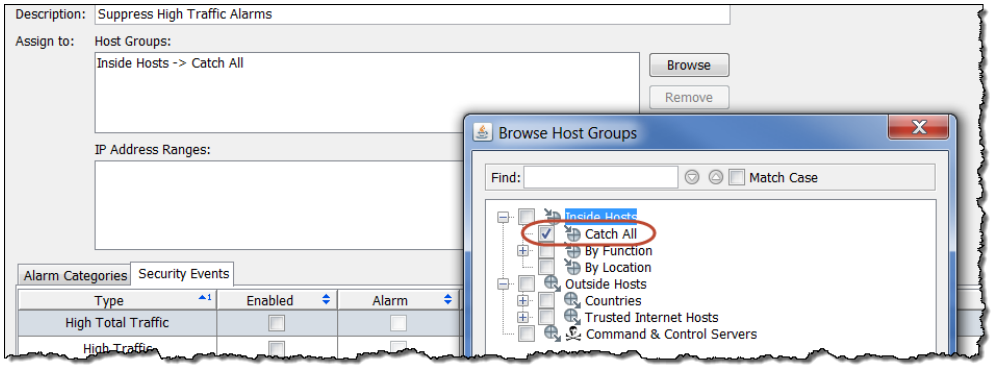
次の例では、特定のロール ポリシーに対して軽減機能を有効にすると仮定します。これを行うには、次の手順を実行します。

1. メイン メニューから、[設定（Configuration）] > [ホストポリシーマネージャ（Host Policy Manager）] を選択します。[ホスト ポリシー マネージャー（Host Policy Manager）] ダイアログが開きます。

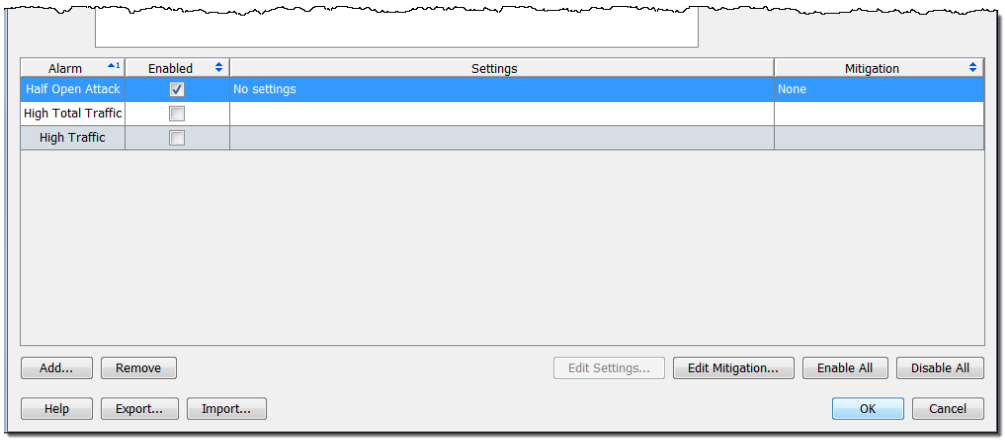


2. [ロールポリシー（Role Policies）] セクションで、必要なロール ポリシーをクリックして、[編集（Edit）] をクリックします。[ロール ポリシーを編集（Edit Role Policy）] ダイアログが開きます。

3. [割り当て先(Assign to)] の [ホストグループ(Host Groups)] セクションで、[参照(Browse)] をクリックして、ポリシーを適用するホスト グループを選択し、[OK] をクリックして、[ロールポリシーを編集(Edit Role Policy)] ダイアログに戻ります。(特定のホスト IP アドレスまたは [IP アドレスの範囲(IP Address Ranges)] フィールドで範囲を指定することもできます)



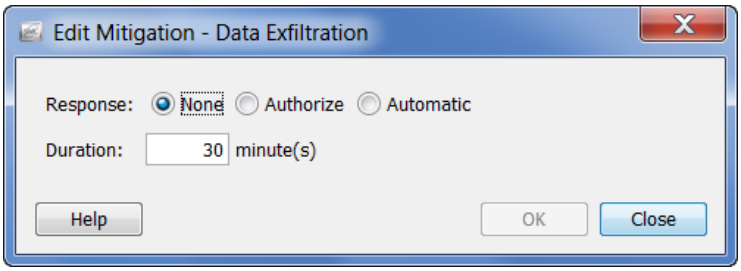
4. [ロール ポリシーを編集(Edit Role Policy)] ダイアログで、チェックボックスをクリックして、軽減を有効にしたい各アラームに対して、[有効(Enabled)] 列内にチェック マークを追加します。(必要なアラームが記載されていない場合、[追加(Add)] をクリックして、追加します)



アラームに対する軽減動作の定義

必要な個々のアラームに対して、軽減処置を定義できます。これを行うには、次の手順を実行します。

1. 前項の手順 4 からの続きですが、開く [ロールポリシーを編集(Edit Role Policy)] ダイアログから、軽減を有効にしたいアラームを含む行を選択して、[軽減を編集(Edit Mitigation)] をクリックします。[軽減を編集(Edit Mitigation)] ダイアログが開きます(アラームによって内容が異なる場合があります)。



(注):
シスコは、各軽減動作に推奨されるデフォルトの設定を提供します。必要性に応じて、ネットワークに対応するように、これらの設定を変更できます。

2. 次の説明に基づいて、ポップアップ メニューで、必要な軽減応答をクリックします。

対応	説明
[なし(None)]	アラームに対するすべての軽減動作を無効にするには、[なし(None)] をクリックします。
[承認する(Authorize)]	アラームが発生する際に、選択した軽減動作が実行される前にシステムに承認を求めさせるには、[承認する(Authorize)] をクリックします。システムに自動的にブロックさせるのではなく、手動で接続をブロックしたい場合に、この設定を使用します。
[自動(Automatic)]	アラームが発生する際に、システムにただちに、かつ自動的に選択した軽減動作を行わせるには、[自動(Automatic)] をクリックします。

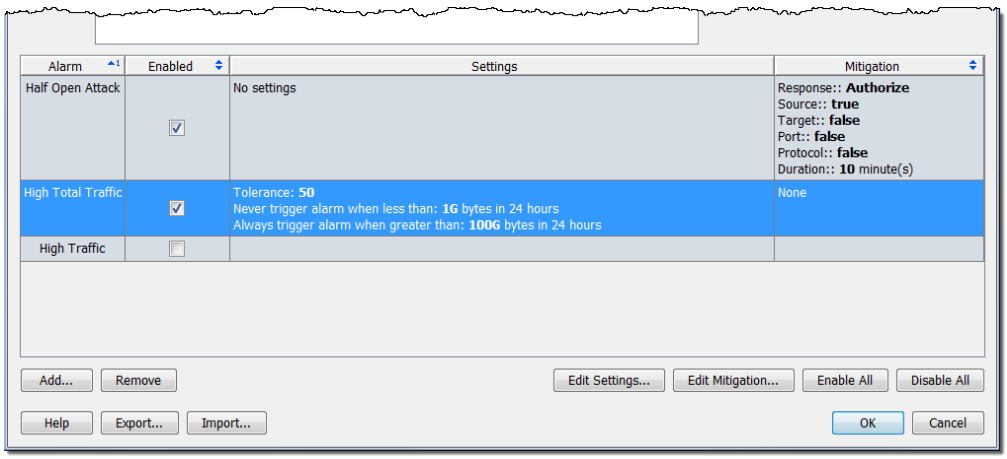
3. 次の表に示すように、軽減設定を指定します。ソースまたはターゲット IP アドレス、プロトコル、およびポート番号の組み合わせに基づいて、各アラームに対する軽減動作をカスタマイズできます。軽減動作を実行する時間を指定することもできます。

軽減オプション	目的
[ソース (Source)]	不審な行動が発生したホストからくるトラフィックをブロックします。
[ターゲット (Target)]	不審な行動のターゲットであるホストに向かうトラフィックをブロックします。
[ポート (Port)]	不審なトラフィックが通過しているインターフェイスをブロックします。
[プロトコル (Protocol)]	不審なトラフィックを送信するのに使用されるプロトコルをブロックします。
[時間 (Duration)]	ブロックを有効にしたい時間(分単位)。この期間が経過すると、軽減プロセスが終了します。 **注:この時間が 0 (ゼロ) の場合、軽減動作は、軽減プロセスを手動で終了するまで有効になります。**

(注):

- シスコのルータは、ポートまたはプロトコルの軽減動作には対応していません。
- OPSEC 装置は、ソースおよびターゲット軽減動作の両方を有効にする必要があります。それ以外の場合、これらの装置は、接続をブロックできません。

4. アラームに対して軽減の設定を指定したら、[OK] をクリックします。設定は、[ロール ポリシーを編集 (Edit Role Policy)] ダイアログに表示されます。



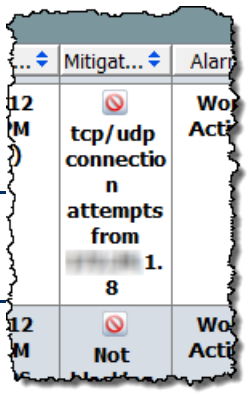
5. 軽減を設定したい各アラームに対して、手順 1 ～ 4 を繰り返します。
6. 終了したら、[OK] をクリックし、[閉じる(Close)] をクリックして、ホスト ポリシー マネージャーを閉じます。

軽減とアラーム テーブル

承認または自動モードで軽減動作を有効にしたかどうかに基づいて、対応するアラームが発生した際に、アラーム テーブルには、ブロック動作が実行されているかどうかが表示されます。

承認(手動)モード

承認モードで軽減動作のあるアラームが発生すると、アラーム テーブルの [軽減(Mitigation)] 列に赤色の [ブロックされていません(Not Blocking)] アイコンが表示されます。

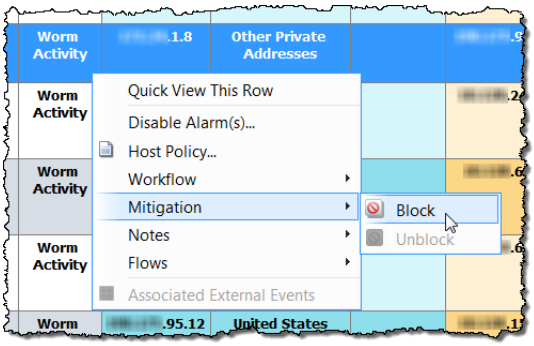


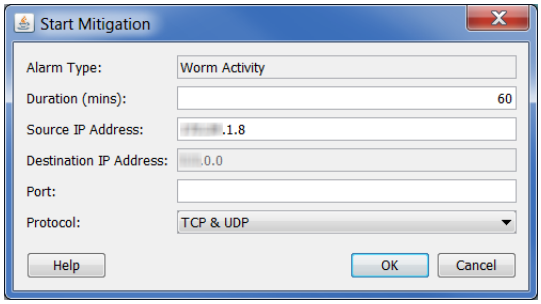
(注):
[軽減(Mitigation)] 列を表示するには、列ヘッダー内を右クリックして、[軽減(Mitigation)] を選択します。

軽減動作が承認モードの時に、アラーム テーブル内の特定のアラームを手動で軽減するには、次の手順を実行します。

1. アラームを右クリックして、[軽減(Mitigation)] > [ブロック(Block)] を選択します。

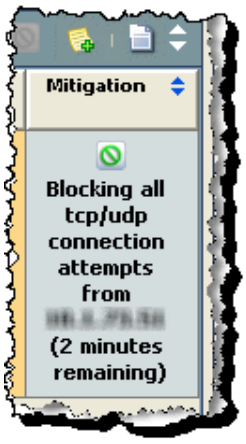
   [軽減を開始(Start Mitigation)] ダイアログが開きます。





2. 必要に応じて、緩和アクションのパラメータを変更して、[OK] をクリックします。[軽減を開始(Start Mitigation)] ダイアログが閉じ、アラーム テーブルが更新されます。

3. アラーム条件を見つけます。赤色の [ブロックされていません(Not Blocking)] アイコンは、緑色の [ブロック中(Blocking)] アイコンに置き換えられました。



(注):
軽減動作の有効期限が切れる前に、接続のブロックを解除したい場合は、アラームを右クリックして、[軽減(Mitigation)] > [ブロック解除(Unblock)] を選択するだけです。

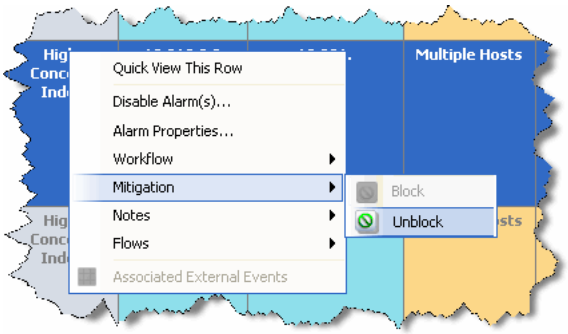
自動モード

自動モードで軽減動作のあるアラームが発生すると、アラーム テーブルの [軽減(Mitigation)] 列に緑色の [ブロック中(Blocking)] アイコンが表示されます。

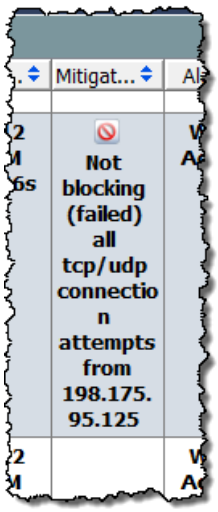
(注):
[軽減(Mitigation)] 列を表示するには、列ヘッダー内を右クリックして、[軽減(Mitigation)] を選択します。

軽減動作が自動モードのため、アラームが発生しても何も行う必要はありません。ただし、軽減動作を停止する必要が有る場合、次の手順を実行します。

1. アラーム テーブルで、アラームを右クリックして、[軽減(Mitigation)] > [ブロック解除(Unblock)] を選択します。アラーム テーブルが更新されます。

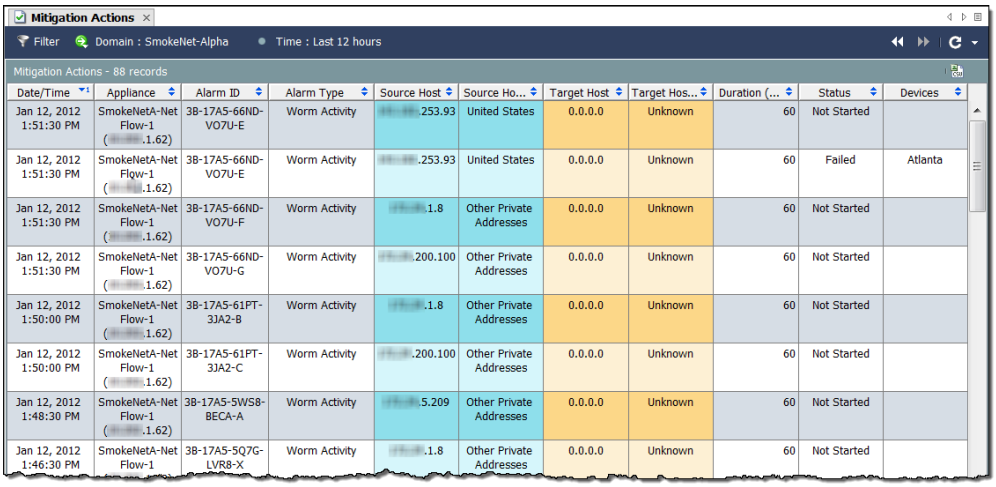


2. 再度、ドキュメントを更新し、アラーム条件を再選択します。緑色の [ブロック中(Blocking)] が赤色の [ブロックされていません(Not Blocking)] アイコンに置き換わりました。



軽減動作ドキュメント

軽減動作ドキュメントによって、最後のアーカイブ時間以降にドメインで発生したすべての軽減動作の状態を確認できます。軽減動作ドキュメントにアクセスするには、問題のドメインを右クリックして、[ステータス(Status)] > [軽減動作(Mitigation Actions)] を選択します。軽減文書が開きます。



Date/Time	Appliance	Alarm ID	Alarm Type	Source Host	Source Ho...	Target Host	Target Hos...	Duration (...	Status	Devices
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-E	Worm Activity	.253.93	United States	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-E	Worm Activity	.253.93	United States	0.0.0.0	Unknown	60	Failed	Atlanta
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-F	Worm Activity	.1.8	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:51:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-66ND-VO7U-G	Worm Activity	.200.100	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:50:00 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-61PT-3JA2-B	Worm Activity	.1.8	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:50:00 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-61PT-3JA2-C	Worm Activity	.200.100	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:48:30 PM	SmokeNetA-Net Flow-1 (.1.62)	3B-17A5-5WS8-BECA-A	Worm Activity	5.209	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	
Jan 12, 2012 1:46:30 PM	SmokeNetA-Net Flow-1	3B-17A5-5Q7G-LVR8-X	Worm Activity	.1.8	Other Private Addresses	0.0.0.0	Unknown	60	Not Started	

11

不要なアラームの削減

概要

特定のポリシー設定が低すぎるか、または問題がないと識別されたサービス/アプリケーションが特定のホスト グループに対して誤って却下された場合、実際には行動が正常である場合でも、疑わしく見える行動の結果としてアラームが発生します。この章では、不要なアラーム表示の数を減らす方法について説明します。

この章は、次の項で構成されています。

- ベースラインの設定
- ホスト ポリシー管理
- ポリシーの作成および編集
- アラーム
- 推奨事項

ベースラインの設定

ベースラインの設定は、ネットワークの正常動作のプロファイルを構築するため、ネットワークの監視には不可欠です。これによって、Stealthwatch は、異常な行動を観測した場合にアラームを発生させることができます。

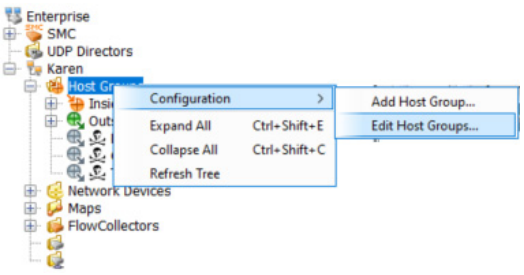
Stealthwatch をネットワークにインストールすると、そのネットワーク上のすべてのホストの識別を開始します。Stealthwatch では、最初の 7 日間で約 90 個の属性に基づいて正常なネットワークのベースラインを確立します。それらの属性には、次のものが含まれます。

- 通常の帯域幅使用量
- 他のホストとの通信
- 同時フローの数
- 秒あたりのパケット数

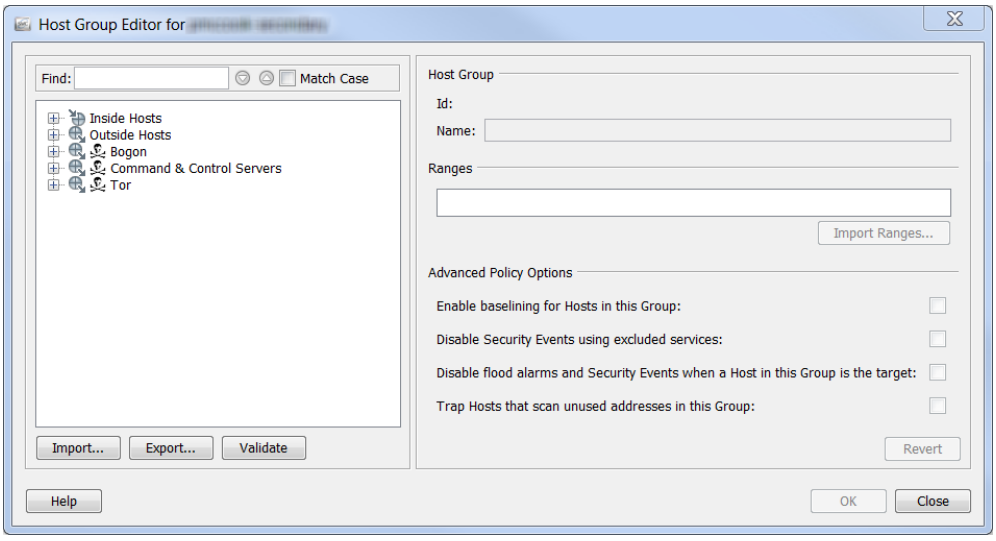
このベースラインは、その日の予想される動作を表しています。ベースラインは、その日に使用する閾値を計算するために、許容差と組み合わせて使用します。

(注):
アラームに関連する許容範囲の概念については、「アラーム」(279 ページ)を参照してください。

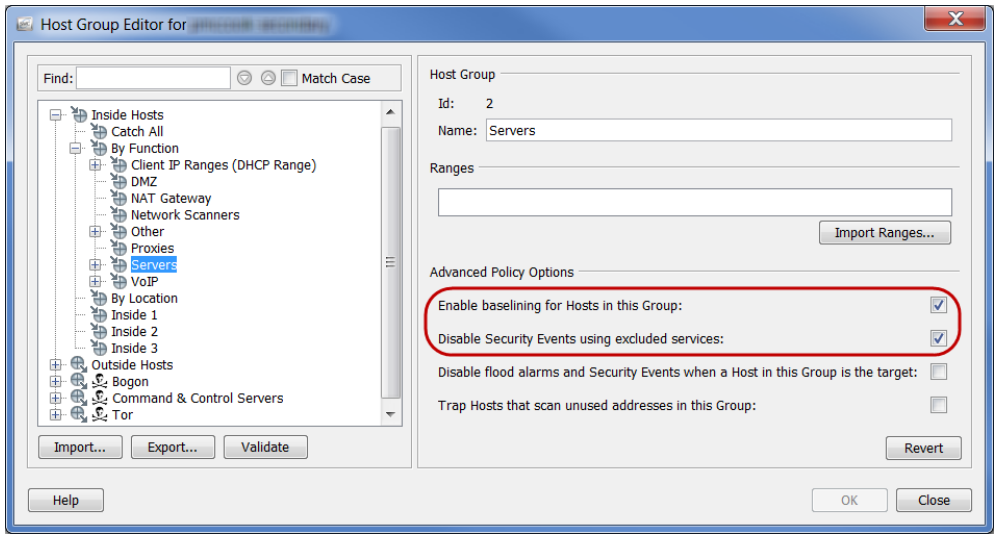
これらの 90 個の属性は、前述のホスト プロファイルの一部になります。デフォルトでは、Stealthwatch は、[内部ホスト(Inside Hosts)] ホスト グループ内のすべてのホストのベースラインになります。ただし、[外部ホスト(Outside Hosts)] ホスト グループの場合は、Stealthwatch ベースラインは、そのホスト グループ レベルでのみホスト動作を集計します。ベースラインの設定方法は、[ホスト グループ エディター(Host Group Editor)] ダイアログボックスでいつでも変更できます。



このダイアログにアクセスするには、[エンタープライズ(Tree)] ツリーで、[ホストグループ(Host Group)] を右クリックして、[設定(Configuration)] > [ホストグループを編集(Edit Host Groups)] を選択します。



ダイアログの左側にある [エンタープライズ(Tree)] ツリーで、ベースラインを設定する方法を変更するホストをクリックします。[詳細なポリシー オプション] セクションで、チェックボックスには、クリックしたホストに対する現在の設定を示すためのチェック マークが自動的に入力されます。



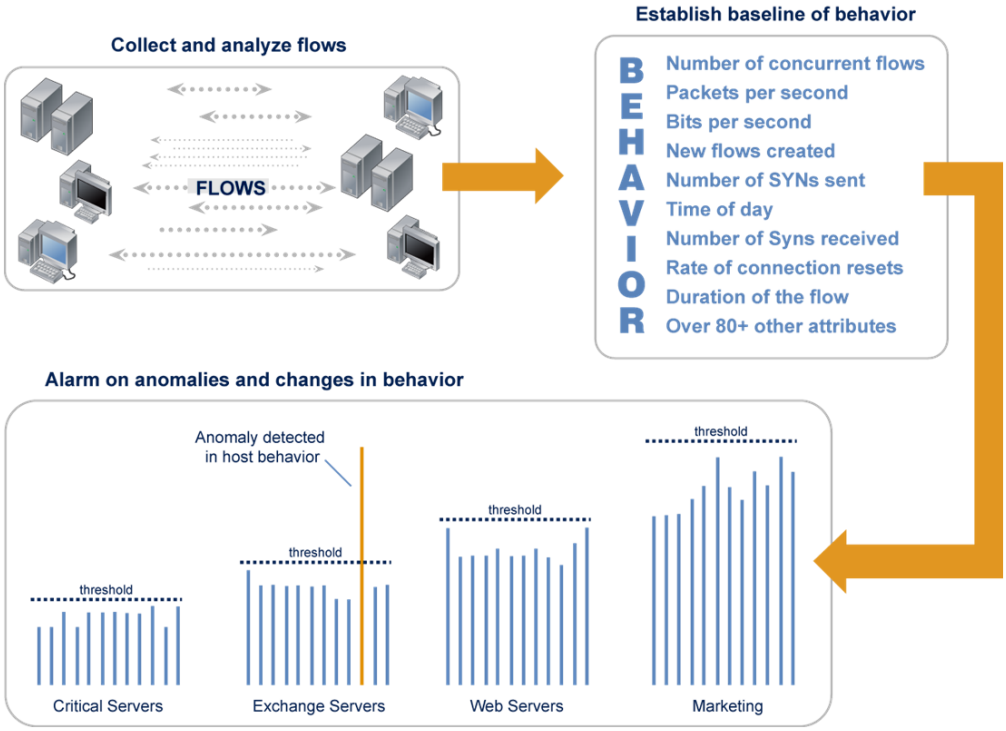
[このグループ内のホストに対するベースライン設定を有効にする(Enable baselining for Hosts in this Group)] チェックボックスにチェックマークがある*場合にのみ*、ホスト グループ内の各ホストに対して一意のホスト レベル ベースラインが確立されます。そうでない場合は、Stealthwatch ベースラインがそのホスト グループ レベルでホストの動作を集計します。

前述したように、デフォルトでは、Stealthwatch は、[内部ホスト（Inside Hosts）] ホスト グループ内のすべてのホストのベースラインになります。そのため、デフォルトでは、このオプションは、内部ホストに対して有効になります（前の例の円で囲われた箇所を参照してください）。

（注）：
IP が頻繁に変わる、DHCP スコープなどの非常に動的な環境に対してこの機能を無効にできます。無効にすると、DHCP ホストの予想された動作に対するベースラインが、他のすべての DHCP ホストのように動作します。

ただしデフォルトでは、Stealthwatch ベースラインは、[外部ホスト（Outside Hosts）] グループに対するホスト グループ レベルでのみホスト動作を集計します。そのためデフォルトでは、このオプションは外部ホストに対して無効になります。

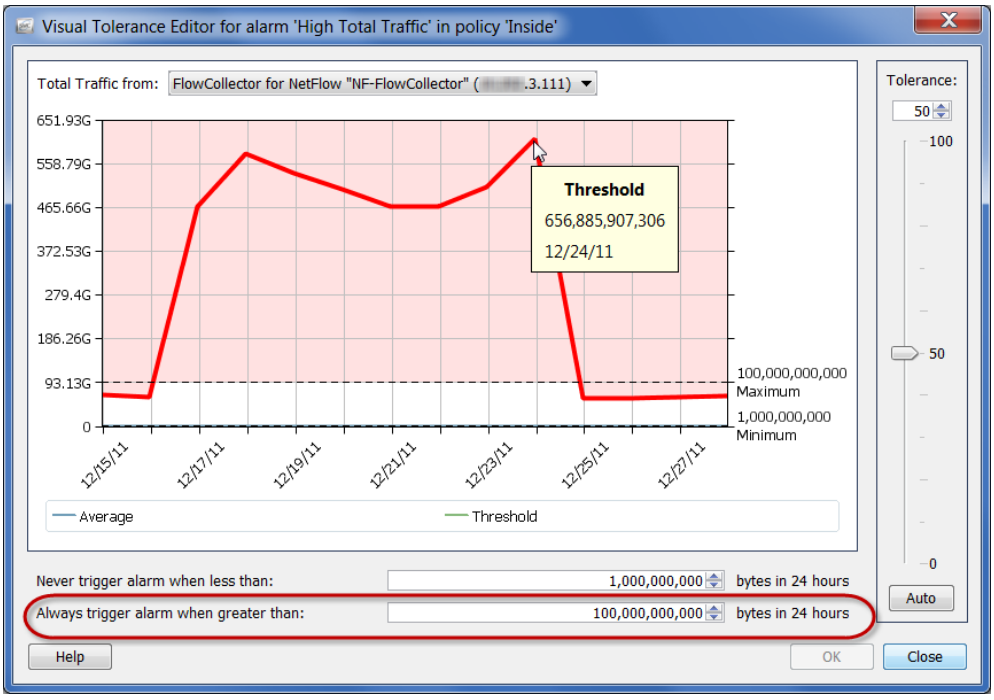
次の図は、ベースライン設定プロセスを示しています。



最初の 7 日後、Stealthwatch は、次の 28 日間ベースラインを作成するため、14 個のキー属性を追跡します。このベースラインは、最後の 7 日間に対して大きく重み付けされた、過去 28 日間の（日単位の）属性値の平均です。ベースラインには最後の 7 日間が組み込まれているため、これらは週単位の値を表します。そのため、ベースラインには前月の値が含まれますが、最後の週の比重が高くなります。

Stealthwatch は、ベースラインの設定に次のガイドラインを使用しています。

- ホストのベースライン設定の場合、Stealthwatch は、有効になっている各アラーム（[高合計トラフィック（High Total Traffic）] アラームなど）に確認されたホストの日単位の最大値を記憶します。
- ホスト グループのベースライン設定の場合、Stealthwatch は、有グループ内のすべてのホスト（すべてのホストに対する最大高合計トラフィック、平均化など）に対する平均値を記憶します。
- ホストに日単位の値がない場合は、属するホストの数が最も少ないグループからのベースラインを使用します。たとえば、ホストが 2 つのグループ（10.201.0.0/16 として定義されているグループ A と 10.201.3.0/24 として定義されているグループ B）に属している場合、ベースラインは、ホストの数が少ないグループ B を継承します。
- ホスト グループのベースラインが、ゼロ（0）の場合、最大値が使用されます（たとえば、24 時間単位の高合計トラフィック最大バイト数）。
- 新規インストールの初日は、ベースラインが確立されるまでの間、すべてのホストが構成ポリシーを最大限に活用します。ホストは、最大値（次の例の丸で囲んだオプションを参照してください）を超える場合を除き、アラームを発生させません。



今後は、Stealthwatch は、次のような動作における変更を検索し、強調表示します。

- 短時間にその他の多くのホストと連絡を取る 1 つのホスト（ピア ツー ピア アプリケーションやワームなど）
- 長いフロー期間（秘密チャンネル、Vpn など）
- 不正なポート（不正なサーバやアプリケーションなど）の使用
- 帯域幅の異常（Warezserver、サービス拒否攻撃など）
- 不正な通信（アカウンティング サーバと通信する VPN ホスト）

ホストが Stealthwatch が「正常な」動作としてベースライン設定したものの閾値を越えた場合、Stealthwatch は常にはアラームを発生させます。動作が発生した時にホストの動作を観察し、いくつかの専用アラームを使用することで、Stealthwatch は、署名ベースのソリューションによって生じることの多い誤検出アラームを発生させないようにします。

ホスト ポリシー管理

ログインの権限に応じて、ポリシーを使用して、Stealthwatch がホスト動作をどのように監視し、対応するかを制御できます。ポリシーには、Stealthwatch が特定の動作を監視する際に反応する方法を決定する設定が含まれています。Stealthwatch は、次の 3 つのポリシーを使用しますが、これらは、必要な時にいつでも編集できます。

- デフォルト ポリシー: 内部および外部ホストすべてに関連しています。
- ロール ポリシー: 一般的な目的 (Web サーバー、ファイアウォール、信頼できるインターネット ホストなど) を提供するホスト (IP アドレス) の集合に関連しています。
- ホスト ポリシー: 特定の IP アドレスに関連しています。

ホスト ポリシーは、他のすべてのポリシーよりも優先されます。そのため、ホスト ポリシーは、ロール ポリシーよりもより具体的で、ロール ポリシーは、デフォルト ポリシーよりもより具体的になります。ホストに対する最も具体的なポリシー設定のみがアラームを発生させます。

(注):
ホストには、複数のホスト ポリシーを割り当てることはできません。

たとえば、アラームをロール ポリシーに追加する場合、無効有効に関係なく、またはそのアラーム設定が変更されているかいなかに関係なく、デフォルト ポリシーでは同じアラームは無効になります。

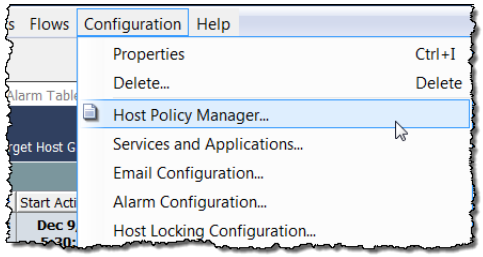
同様に、アラームを特定のホストに対するホスト ポリシーに追加する場合、無効有効に関係なく、またはそのアラーム設定が変更されているかいなかに関係なく、そのホストに適用されるいずれかのロール アラームまたはデフォルト ポリシー内の同じアラームは無効になります。

ホストがホストポリシーには割り当てられていないが、2 つ以上のロールポリシーに割り当てられている場合、Stealthwatch は、各アラームに対して、どのポリシーの設定がホストの有効なポリシーで使用されるかを決定します。有効なポリシーを決定する方法の詳細については、「有効なホスト ポリシー」(251 ページ) を参照してください。

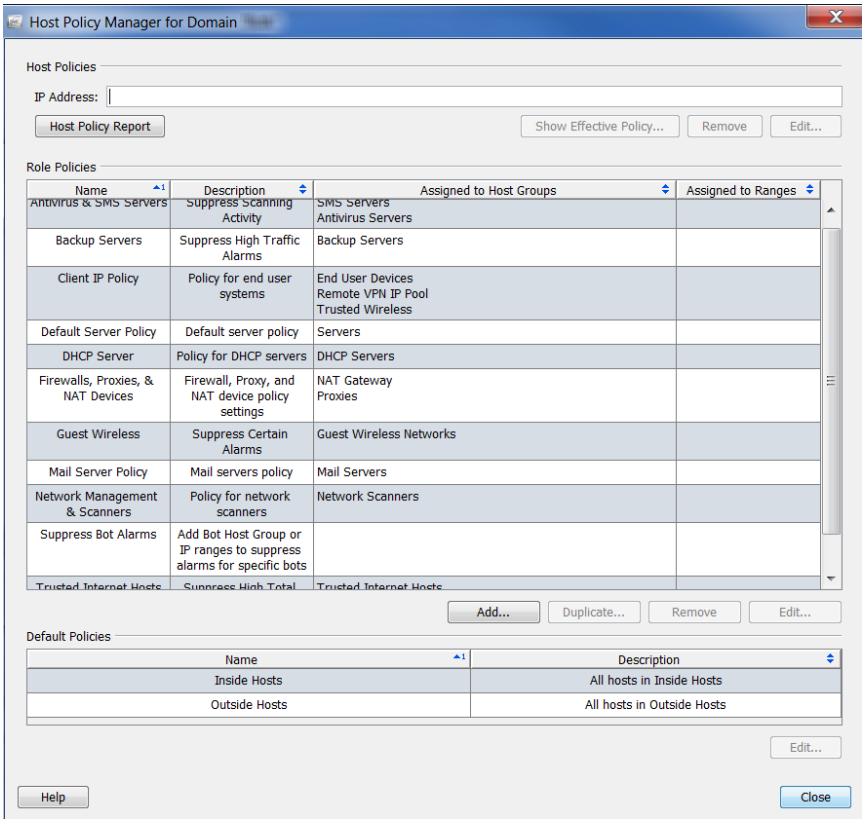
ドメイン、ホスト グループ、または特定のホストに許可されている動作のしきい値を変更したい場合は、影響を与えたいホスト グループまたはホストの数に応じて、適切なポリシーの種類を作成または編集する必要があります。

Stealthwatch 内には、内部ホストのデフォルトポリシーと外部ホストのデフォルトポリシーの 2 つのデフォルトポリシーが存在します。これらの設定は、ロール ポリシーまたはホスト ポリシーが作成されていない場合に適用されます。

これらのグループのいずれかまたは両方に対してデフォルト ポリシーを編集する必要があると判断する場合があるでしょう。これを行うには、ホスト ポリシー マネージャーにアクセスする必要があります。このダイアログにアクセスするには、メイン メニューから、[設定(Configuration)] > [ホストポリシーマネージャ(Host Policy Manager)] を選択します。



[ホスト ポリシー マネージャー(Host Policy Manager)] ダイアログが開きます。



このダイアログでは、次のセクションを使用して、ポリシーを設定することができます。

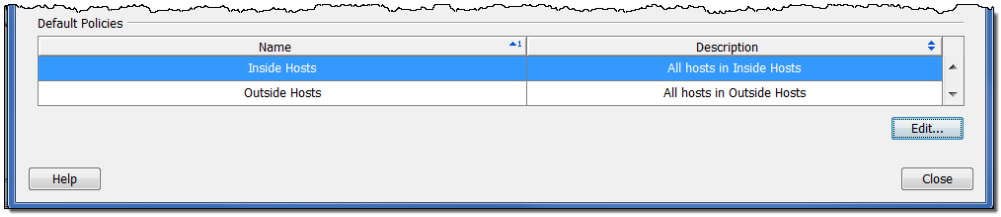
- [ホスト ポリシー(Host Policies)]:1 つのホスト ポリシーを管理することができます。
- [ロール ポリシー(Role Policies)]:お使いのシステムで実行するロールによって、ホスト ポリシーを管理することができます。
- [デフォルト ポリシー(Default Policies)]:内部または外部ホストに対するデフォルト ポリシーを管理することができます。

(注):
ロール ポリシーとホスト ポリシーの作成および編集の詳細については、「ポリシーの作成および編集」(262 ページ)を参照してください。

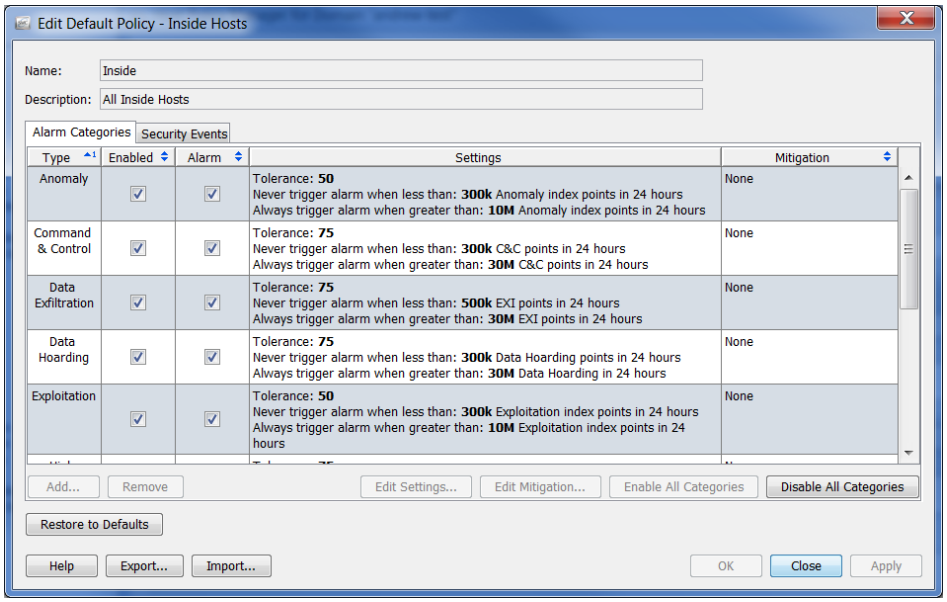
内部および外部ホストのデフォルト ポリシーの編集

内部ホストのデフォルト ポリシーまたは外部ホストのデフォルト ポリシーを編集するには、次の手順を実行します。

1. メイン メニューから、[設定(Configuration)] > [ホストポリシーマネージャ(Host Policy Manager)] を選択します。前の画面で示したように、[ホスト ポリシー マネージャー(Host Policy Manager)] ダイアログが開きます。
2. [デフォルトポリシー(Default Policies)] セクションで、デフォルト ポリシーを編集するホストの名前を選択し、[編集(Edit)] をクリックします。



[デフォルト ポリシーを編集(Edit Default Policy)] ダイアログが開きます。



注意:

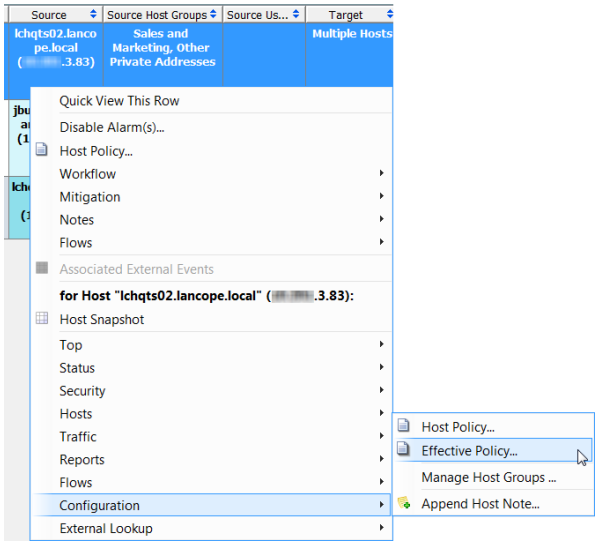
[デフォルトに戻す(Restore to Defaults)] をクリックすると、現在のポリシーは工場出荷時のデフォルト ポリシー設定で置き換えられるため、この機能を使用する時には特に注意してください。

3. アラームのカテゴリーをポリシーに追加したい場合は、設定またはアラームのカテゴリーに関連付けられているアラームの軽減を編集するか、アラームのカテゴリーを有効または無効にし、「ホスト ポリシーでのアラーム カテゴリーの設定」(255 ページ)に進みます。
4. ポリシーが使用するセキュリティ イベントを設定する場合は、設定またはは CI に関連付けられているアラームの軽減を編集し、セキュリティ イベントを有効または無効にし、「ホスト ポリシーでのセキュリティ イベントの設定」(259 ページ)に進みます。

有効なホスト ポリシー

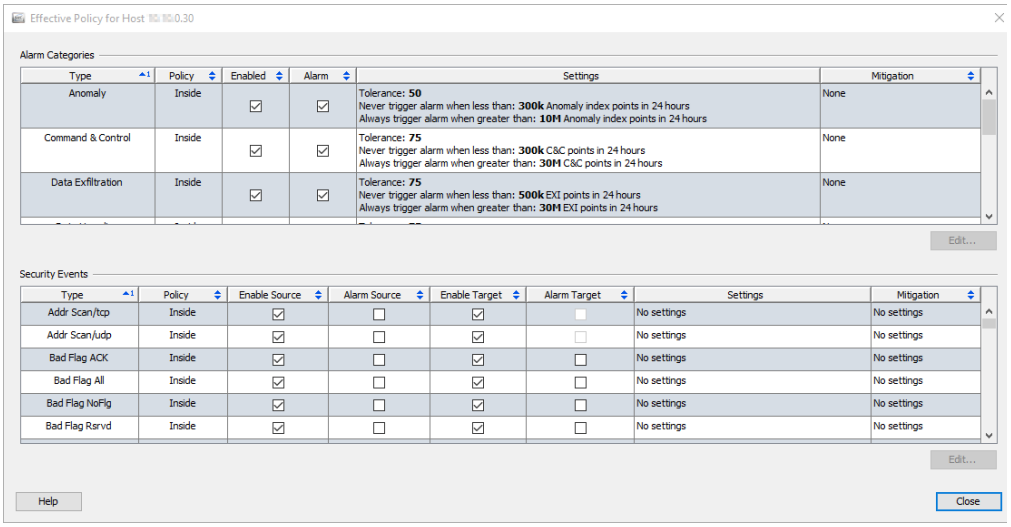
アラームに応答する場合、最初にどのポリシーがそのアラームを発生させたかを判定する必要があります。IP アドレスが表示されている場合、IP アドレスを右クリックし、[設定(Configuration)] > [有効なポリシー(Effective Policy)] を選択できます。

次の例に示すように、[有効なホスト(Effective Host)] ダイアログが開きます。



ヒント:

アラーム テーブルにいる場合、制御ポリシーをすばやく検索する方法は、ヘッダー内で右クリックし、ポップアップ メニューから [ポリシー(Policy)] を選択して、[ポリシー(Policy)] 列を表示します。この列を見て、アラームをどのポリシーで制御するかを決定できます。この時点から、特定のポリシーに対するポリシー設定を表示する場合は、[ポリシー(Policy)] 列内のポリシー名をダブルクリックします。



前の例で分かるように、[高ファイル共有インデックス(High File Sharing Index)] アラームは、サーバー ロール ポリシーによって制御され、[高トラフィック(High Traffic)] アラームは、内部ホスト ポリシーによって制御されます。

ホストがホスト ポリシーに割り当てられていないが、2 つ以上の構成の異なるロール ポリシーに割り当てられている状況があるかもしれません。これが発生すると、Stealthwatch は、そのホストが割り当てられているロールポリシーのいずれかで最初に次の 4 つの列のいずれかが選択解除されるかをチェックします。

- [ソースを有効にする(Enable Source)]
- [アラーム ソース(Alarm Source)]
- [ターゲットを有効にする(Enable Target)]
- [アラーム ターゲット(Alarm Target)]

ポリシーのいずれかで以前のビュレット リストで名付けた 4 つの列の内の 1 つだけでもだけでも選択解除されると、有効なポリシーでもその列は選択解除されます。つまり、選択解除されている(「偽」設定と同等)列は、その列が選択されると(「真」設定と同等)、ホストが割り当てられるその他のロール ポリシーを無効にします。つまり、偽設定は真設定を無効にします。

割り当てられたロール ポリシーのすべてで選択された列は、有効なポリシーで選択されたままになります。

例 1

ロール ポリシー 1 が次の場合			
[ソースを有効にする(Enable Source)]	**[アラーム ソース(Alarm Source)]**	**[ターゲットを有効にする(Enable Target)]**	**[アラーム ターゲット(Alarm Target)]**
○	○	×	×
ロール ポリシー 2 は			
[ソースを有効にする(Enable Source)]	**[アラーム ソース(Alarm Source)]**	**[ターゲットを有効にする(Enable Target)]**	**[アラーム ターゲット(Alarm Target)]**
×	×	○	○
次に、有効なポリシーは			
[ソースを有効にする(Enable Source)]	**[アラーム ソース(Alarm Source)]**	**[ターゲットを有効にする(Enable Target)]**	**[アラーム ターゲット(Alarm Target)]**
×	×	×	×

例 2

ロール ポリシー 1 が次の場合			
[ソースを有効にする(Enable Source)]	[アラーム ソース(Alarm Source)]	[ターゲットを有効にする(Enable Target)]	[アラーム ターゲット(Alarm Target)]
○	○	○	×
ロール ポリシー 2 は			
[ソースを有効にする(Enable Source)]	[アラーム ソース(Alarm Source)]	[ターゲットを有効にする(Enable Target)]	[アラーム ターゲット(Alarm Target)]
○	×	○	○
次に、有効なポリシーは			
[ソースを有効にする(Enable Source)]	[アラーム ソース(Alarm Source)]	[ターゲットを有効にする(Enable Target)]	[アラーム ターゲット(Alarm Target)]
○	×	○	×

ホストに対する有効なポリシーは、[ポリシー(Policy)] 列にすべての有効なポリシーの名前を表示します。セキュリティ イベントに対してソース ポリシーとターゲット ポリシーが存在する場合、[ポリシー(Policy)] 列には、最初にソース ポリシーが次にターゲット ポリシーが一覧表示されます。

(注):
アラームへの対応の次の手順については、「ポリシーの作成および編集」(262 ページ)を参照してください。

アラーム カテゴリー

このセクションを使用して、このロール ポリシーが使用されるアラーム カテゴリーを設定します。カテゴリーは、特定の種類のセキュリティ イベントをグループ化する方法を提供します。アラーム カテゴリーはそれぞれ発生するイベントの数と種類に応じて、アラームを生成できます。

次を実行できます。

- アラーム カテゴリー設定の追加または編集
- アラーム カテゴリーに関連付けられたアラームの緩和の編集
- アラーム カテゴリーの有効化または無効化

次のアラーム カテゴリーが利用できます。

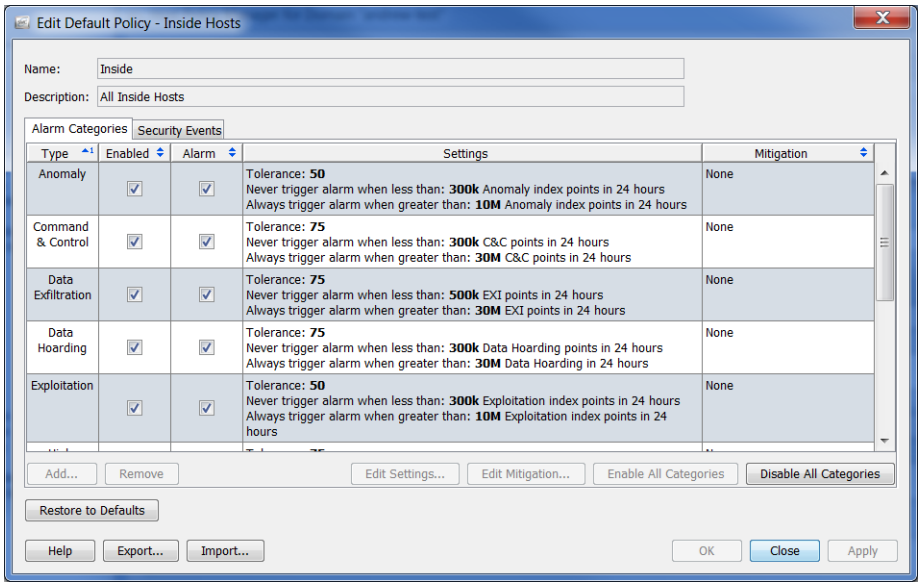
項目	説明
[異常(Abnormaly)]	ホストが異常な動作をしているか、普通ではないトラフィックを生成している活動の別のカテゴリーと一致していないことを示すイベントを追跡します。
[C&C(コマンドとコントロール(Command & Control))]	C&C サーバーと連絡を取ろうとするネットワーク内のボットに感染したサーバーまたはホストの存在を示しています。
[データの漏洩(Data Exfiltration)]	異常な量のデータが転送された先の内部と外部のホストを追跡します。 ホストが設定した閾値を超えるこれらのイベントを多く発生させた場合、高漏洩アラームが発生します。
[データの蓄積(Data Hoarding)]	ネットワーク内のソース ホストまたはターゲット ホストが 1 つ以上のホストから異常な量のデータがダウンロードしたことを示しています。
[エクスプロイト(Exploitation)]	ワームの増殖や総当りのクラッキングなどを通じた、ホストによる相互に侵入しようとする直接の試みを追跡します。
[高懸念インデックス(High Concern Index)]	懸念インデックスが CI しきい値を超過しているか、または急速に増加したかホストを追跡します。 [高懸念インデックス(High Concern Index)] と [高ターゲット インデックス(High Target Index)] カテゴリーは、同じイベントを使用します。イベントがソース ホストによって発生させられた場合、[高 CI(High CI)] カテゴリー アラームが発生します。イベントがターゲット ホストによって発生させられた場合、[高 TI (High TI)] アラームが発生します。
[高 DDoS ソース インデックス(High DDoS Source Index)]	ホストが DDoS 攻撃のソースであると判明したことを示しています。
[高 DDos ターゲット インデックス(High DDoS Target Index)]	ホストが DDoS 攻撃のターゲットであると判明したことを示しています。
[高ターゲット インデックス(High Target Index)]	内部ホストが複数の許容可能なスキャンまたはその他の悪意のある攻撃の受信者であったことを示しています。 [高懸念インデックス(High Concern Index)] と [高ターゲット インデックス(High Target Index)] カテゴリーは、同じイベントを使用します。イベントがソース ホストによって発生させられた場合、[高 CI(High CI)] カテゴリー アラームが発生します。イベントがターゲット ホストによって発生させられた場合、[高 TI (High TI)] アラームが発生します。

項目	説明
[ポリシー違反（Policy Violation）]	サブジェクトは、通常のネットワーク ポリシーに違反する動作を示しています。
[偵察（Recon）]	TCP または UDP を使用し、組織のホストと対立している不正で、潜在的に悪意のあるスキャンの存在を示しています。これらのスキャンは、「偵察」とも呼ばれますが、ネットワークに対する攻撃の早期指標であり、このスキャンは、組織の内外からくる場合があります。

ホスト ポリシーでのアラーム カテゴリーの設定

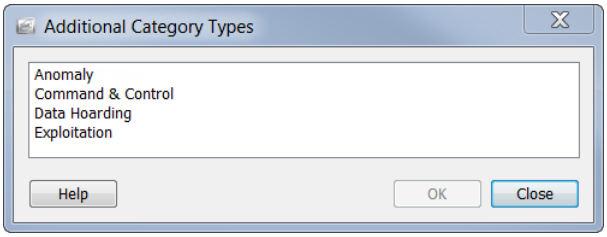
アラーム カテゴリーを設定するには、次の手順を実行します。

1. [ポリシーを編集（Edit Policy）] ダイアログで、[アラームカテゴリ（Alarm Category）] タブをクリックします。



2. 次のいずれかを実行します。
   - アラーム カテゴリーを追加する必要がある場合は、手順 3 に進みます。
   - アラーム カテゴリーを編集する必要がある場合は、手順 5 に進みます。

3. アラーム カテゴリを追加するには、[追加(Add)] をクリックします。[アラーム カテゴリー(Alarm Categories)] ダイアログが開きます。

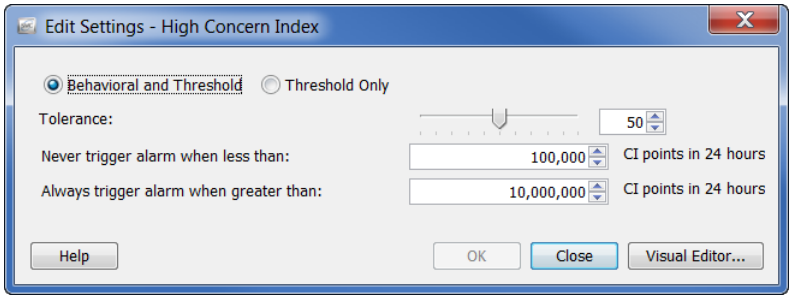


4. 1 つ以上のアラーム カテゴリーを選択し、[OK] をクリックします。

   [ポリシーを編集(Edit Policy)] ダイアログに戻ります。

5. アラーム カテゴリーに対して、動作、許容差、または閾値設定を編集するには、編集したいアラーム カテゴリーを選択します。

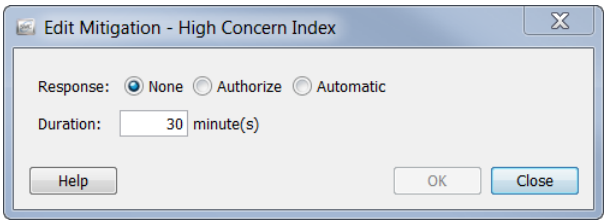
6. [設定の編集(Edit Settings)] をクリックします。[設定を編集(Edit Settings)] ダイアログが開きます。



7. 必要に応じて、設定を変更して、終了したら、[OK] をクリックします。[ポリシーを編集(Edit Policy)] ダイアログに戻ります。

8. 軽減が発生するタイミングを指定するには、編集したいアラーム カテゴリーを選択します。

9. [軽減を編集(Edit Mitigation)] をクリックします。[軽減を編集(Edit Mitigation)] ダイアログが開きます。



10. 必要に応じて、設定を変更して、終了したら、[OK] をクリックします。[ポリシーを編集(Edit Policy)] ダイアログに戻ります。

(注):

- アラーム カテゴリに対して設定がなされていない場合、[設定(Settings)] 列に [設定なし(No Settings)] が表示されます。
- アラーム カテゴリに対して軽減設定がなされていない場合、[軽減(Mitigation)] 列に [なし(None)] が表示されます。

11. アラーム カテゴリーを有効にするには、[有効(Enabled)] 列でそのアラーム カテゴリーのチェックボックスを選択します。

ヒント:

[すべてのカテゴリーを有効にする(Enable All Categories)] ボタンまたは [すべてのカテゴリーを無効にする(Disable All Categories)] ボタンを使用して、一度にすべてのアラーム カテゴリーに影響を与えます。

12. セキュリティ イベントに対してアラームを出すには、[警報(Alarm)] 列でチェックボックスを選択します。
13. 次のいずれかを実行します。
    - [ポリシーを編集(Edit Policy)] ダイアログを終了せずに、設定を適用するには、[適用(Apply)] > [閉じる(Close)] をクリックします。
    - 設定を適用して、[ポリシーを編集(Edit Policy)] ダイアログを閉じるには、[OK] をクリックします。

(注):

- アラームの設定の各種設定の詳細については、「アラーム」(279 ページ)を参照してください。
- 特定のアラームの推奨設定については、「推奨事項」(285 ページ)を参照してください。

セキュリティ イベント

このセクションを使用して、ポリシーが使用するセキュリティ イベントの設定、CI に関連付けられているアラームの設定または軽減の編集、セキュリティ イベントの有効化または無効化を行います。[セキュリティ イベント(Security Events)] タブのチェックボックスの説明については、次の表を参照してください。

選択するチェックボックス	行える操作
[ソース ポリシーに影響(Impact Source Policy)]	ホスト ポリシーまたはロール ポリシーに既存の有効なポリシーで定義されたソース設定を無効にさせたい場合。 **注:** この列は、ホスト ポリシーまたはロール ポリシーを編集するのみ使用できます。
[ソースを有効にする(Enable Source)]	ソースに対して有効になっているセキュリティ イベントに該当するアラーム カテゴリーにポイントを提供させたい場合。
[アラーム ソース(Alarm Source)]	ソースに対して有効になっているセキュリティ イベントに関連するアラームを発生させたい場合。
[ソース ターゲットに影響(Impact Source Target)]	ホスト ポリシーまたはロール ポリシーに既存の有効なポリシーで定義されたソース設定を無効にさせたい場合。 **注:** この列は、ホスト ポリシーまたはロール ポリシーを編集するのみ使用できます。
[ターゲットを有効にする(Enable Target)]	ターゲットに対して有効になっているセキュリティ イベントに該当するアラーム カテゴリーにポイントを提供させたい場合。
[アラーム ターゲット(Alarm Target)]	ターゲットに対して有効になっているセキュリティ イベントに関連するアラームを発生させたい場合。

特定の種類のセキュリティ イベントがアラームを発生させない状況については、次を参照してください。

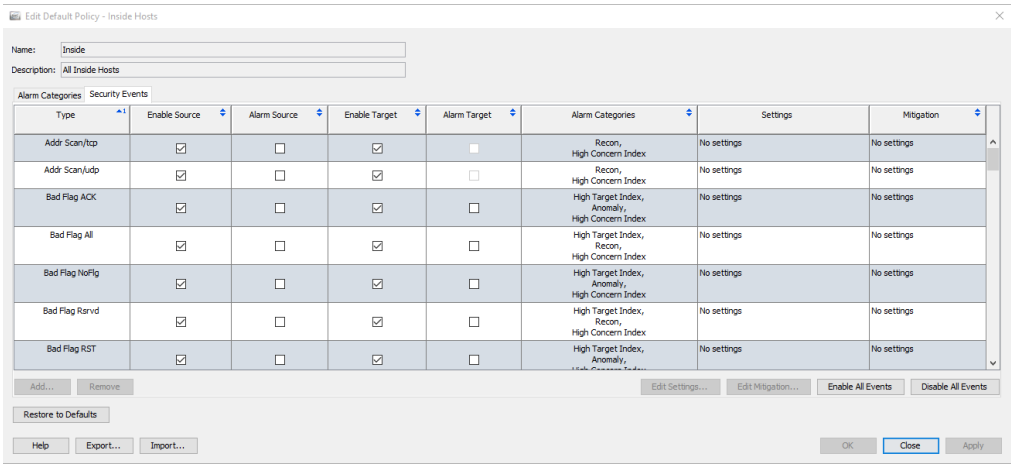
- 一対多([最大フロー開始(Max Flows Initiated)] など):この種類のセキュリティ イベントはターゲットでアラームを発生させることができないため、このセキュリティ イベントには [アラーム ターゲット(Alarm Target)] チェックボックスを選択できません。
- 多対一([SYNs 受信(SYNs Received)] など):この種類のセキュリティ イベントはソースでアラームを発生させることができないため、このセキュリティ イベントには [アラーム ソース(Alarm Source)] チェックボックスを選択できません。

[アラームを無効にする(Disable Alarm(s))] を右クリックし、選択して、[アラーム テーブル(Alarm Table)] 内のアラームを無効にできます。これによって、対応するセキュリティ イベントに対して、[アラーム ソース(Alarm Source)] および [アラーム ターゲット(Alarm Target)] チェックボックスの選択が解除され、[ソースを有効にする(Enable Source)] および [ターゲットを有効(Enable Target)] チェックボックスは選択されたままになります。これによって、[ソースを有効にする(Enable Source)] および [ターゲットを有効にする(Enable Target)] 列が選択される新しいホスト ポリシーが作成されますが、[アラーム ソース(Alarm Source)] および [アラーム ターゲット(Alarm Target)] 列は選択解除されます。

ホスト ポリシーでのセキュリティ イベントの設定

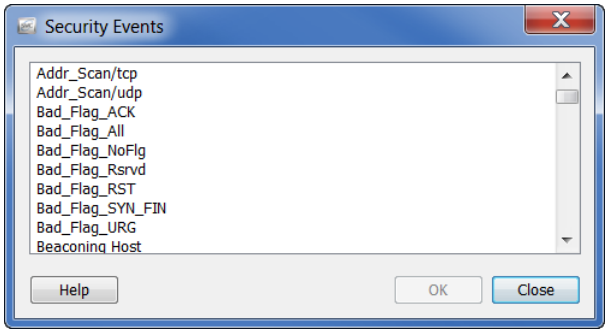
セキュリティ イベントを設定するには、次の手順を実行します。

1. [ポリシーを編集(Edit Policy)] ダイアログで、[セキュリティイベント(Security Events)] タブをクリックします。



2. 次のいずれかを実行します。
   - セキュリティ イベントを追加する必要がある場合は、手順 3 に進みます。
   - セキュリティ イベントを編集する必要がある場合は、手順 5 に進みます。

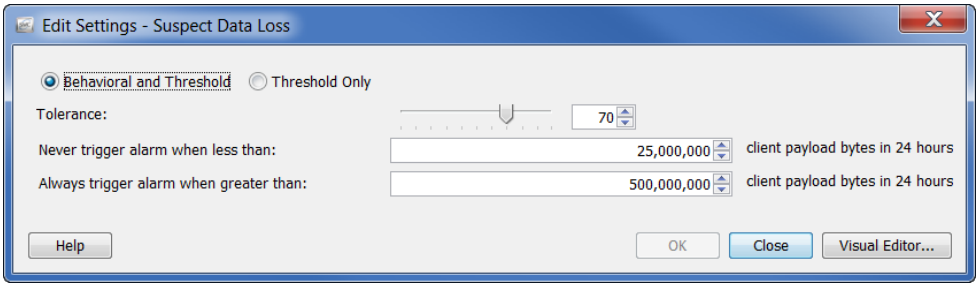
3. セキュリティ イベントを追加するには、[追加(Add)] をクリックします。[セキュリティ イベント(Security Events)] ダイアログが開きます。



4. 次のいずれかを実行します。
   - 1 つのセキュリティ イベントを追加するには、そのイベントを選択して、[OK] をクリックします。
   - 順に一覧表示されている複数のイベントを追加するには、最初のイベントを選択して、**Shift** キーを押し、その順内の最後のイベントを選択して、[OK] をクリックします。
   - 順に一覧表示されていない複数のイベントを追加するには、**Ctrl** キーを押し、各イベントを選択して、[OK] をクリックします。

   [セキュリティ イベント(Security Events)] タブに戻ります。
5. セキュリティ イベントに対して、動作、許容差、または閾値設定を編集するには、編集したいセキュリティ イベントを選択します。
6. [設定の編集(Edit Settings)] をクリックします。

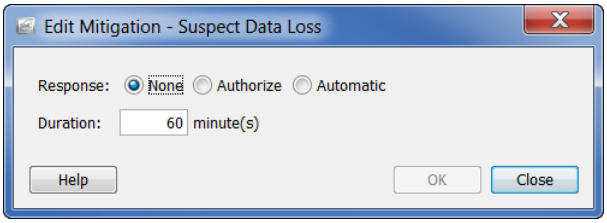
   [設定を編集(Edit Settings)] ダイアログが開きます。



7. 必要に応じて、設定を変更して、終了したら、[OK] をクリックします。[ポリシーを編集(Edit Policy)] ダイアログに戻ります。
8. 軽減が発生するタイミングと方法を指定するには、編集したいセキュリティ イベントを選択します。

9. [軽減を編集(Edit Mitigation)] をクリックします。

   [軽減を編集(Edit Mitigation)] ダイアログが開きます。



10. 必要に応じて、設定を変更して、終了したら、[OK] をクリックします。[ポリシーを編集(Edit Policy)] ダイアログに戻ります。

(注):

- アラーム カテゴリに対して設定がなされていない場合、[設定(Settings)] 列に [設定なし(No Settings)] が表示されます。
- アラーム カテゴリに対して軽減設定がなされていない場合、[軽減(Mitigation)] 列に [なし(None)] が表示されます。

11. ソース セキュリティ イベント、ターゲット セキュリティ イベント、またはその両方に該当するアラーム カテゴリーにポイントを提供させたいかどうかに応じて、該当する [有効化(Enable)] チェックボックスをクリックします。

ヒント:

[すべてのイベントを有効にする(Enable All Events)] ボタンまたは [すべてのイベントを無効にする(Disable All Events)] ボタンを使用して、一度にすべてのイベントに影響を与えます。

12. ソース セキュリティ イベント、ターゲット セキュリティ イベント、またはその両方に対して、アラームを発生させたいかに応じて、該当する [アラーム(Alarm)] チェックボックスをクリックします。

13. 次のいずれかを実行します。

    - [ポリシーを編集(Edit Policy)] ダイアログを終了せずに、設定を適用するには、[適用(Apply)] > [閉じる(Close)] をクリックします。
    - 設定を適用して、[ポリシーを編集(Edit Policy)] ダイアログを閉じるには、[OK] をクリックします。

(注):

- アラームの設定の各種設定の詳細については、「アラーム」(279 ページ)を参照してください。
- 特定のアラームの推奨設定については、「推奨事項」(285 ページ)を参照してください。

ポリシーの作成および編集

前項で説明したように、アラームに応答する際は、特定のアラームをどのポリシーが発生させたかを判定する必要があります。アラームを編集または無効にする準備ができている場合、アラーム テーブル、またはホスト スナップショットの [アラーム(Alarm)] セクション内にいる可能性が高くなります。そのため、次の例では、ユーザーがアラーム テーブル内にいて、アラームを編集または無効にする準備ができているシナリオを使用します。

アラームに応答する際は、次の手順を実行します。

1. 発生させているホストを判定します。サーバー、デスクトップなど。また、動作が通常かどうかを判定します。動作が正常の場合は、次の手順に進みます。動作が正常ではない場合は、標準的なエスカレーション手順に従って、アラームの原因を調査します。
2. 発生させているホストがそれに対して作成されたデフォルトのロール ポリシーをすでに持っているが、論理的に属することができない事前定義されたグループ(バックアップ サーバー、ファイアウォール、プロキシなど)のメンバーでない場合、このホストを論理的に適切なその事前定義されたグループに割り当てます。(「事前定義されたグループへのホストの割り当て」(263 ページ)を参照)。

   たとえば、発生させているホストがバックアップ サーバーの場合、「バックアップ サーバー」と呼ばれる事前定義されたグループがあるため、デフォルトのロール ポリシーはそれに対してすでに作成されています。そのため、この発生させているホストをバックアップ サーバー グループに割り当てることができます。次に、バックアップ サーバーに対して、デフォルトのロール ポリシーに自動的に割り当てられます。
3. 発生させているホストが事前定義されたグループのメンバーではなく、論理的に適切でないが、別のロール ポリシーに属している場合、属するロール ポリシーを編集します。(「ロール ポリシーの編集」(271 ページ)を参照)。

   発生させているホストが事前定義されたグループのメンバーではなく、論理的に適切でないが、ホスト ポリシーに属している場合、属するホスト ポリシーを編集します。(「ホスト ポリシーの編集」(277 ページ)を参照)。

4. 発生させているホストがどのロール ポリシーまたはホスト ポリシーにも属していない場合、次のいずれかを行なうことができます。

   - (いずれか適用されても)このホストを管理する内部ホストのデフォルト ポリシーまたは外部ホストのデフォルト ポリシーのいずれかの編集(「内部および外部ホストのデフォルト ポリシーの編集」(249 ページ)を参照)

注意:
内部ホストのデフォルト ポリシーまたは外部ホストのデフォルト ポリシーに行った編集は、グローバル設定に影響することに注意してください。

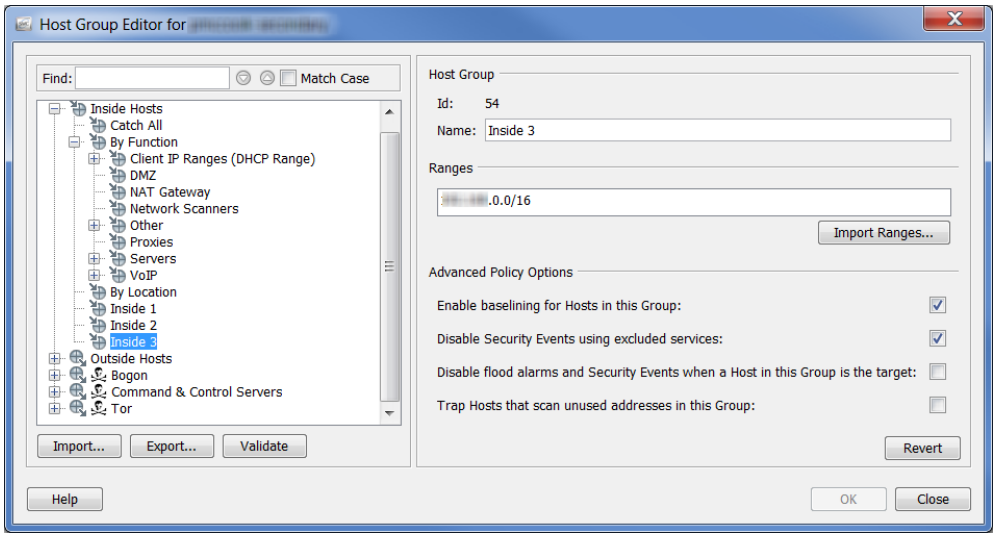
   - このホストのロール ポリシーの作成(「ロール ポリシーの作成」(265 ページ)を参照)。
   - このホストのホスト ポリシーの作成(「ホスト ポリシーの作成」(274 ページ)を参照)。

事前定義されたグループへのホストの割り当て

事前定義されたグループにホストを割り当てるには、次の手順を実行してください。

1. [エンタープライズ(Enterprise)] ページのツリー メニューで、発生させているホストが属するドメインをクリックします。
2. メイン メニューから、[設定(Configuration)] > [ホストグループを編集(Edit Host Groups)] を選択します。[エンタープライズ(Tree)] ツリーでクリックしたドメインに [ホスト グループ エディター(Host Group Editor)] ダイアログが開きます。

3. 左側のウィンドウで、発生させているホストを割り当てたいグループをクリックします。すでのこのグループのメンバーであるホストの IP アドレスは、ダイアログの右側にある [範囲(Range)] フィールドに表示されます。



ヒント:

1 つのホストをグループにすばやく移動させるには、ドキュメント内にあるホストを右クリックして、[設定(Configuration)] > [ホストグループを編集(Edit Host Groups)] を選択します。そのホストの [ホストグループ(Host Groups)] ダイアログが開いたら、ダイアログの最上部のセクションから目的のグループを選択し、[OK] をクリックします。

4. 手順 3 で指定したグループに IP アドレスを追加するには、次の手順のいずれかを実行します。
   - [範囲(Range)] フィールドに、発生させているホストの IP アドレスを入力します。
   - 複数のホストを追加し、これらが範囲内にある場合、[範囲(Range)] フィールドに、発生させているホストの IP アドレスを入力します。
   - 複数のホストを追加し、発生させているホストの IP アドレスを含む既存のファイルがある場合、[範囲をインポート(Import Ranges)] をクリックして、IP アドレスをインポートします。
5. [OK] をクリックします。[エンタープライズ(Enterprise)] ページのツリーメニューが自動的にアップデートされ、手順 3 で指定したグループに新たに追加したすべての IP アドレスが含まれます。

ロール ポリシーの作成

一般的な関数または類似の属性を共有するホストのグループに同じアラーム閾値を割り当てたい場合は、ロール ポリシーを作成することに注意してください。

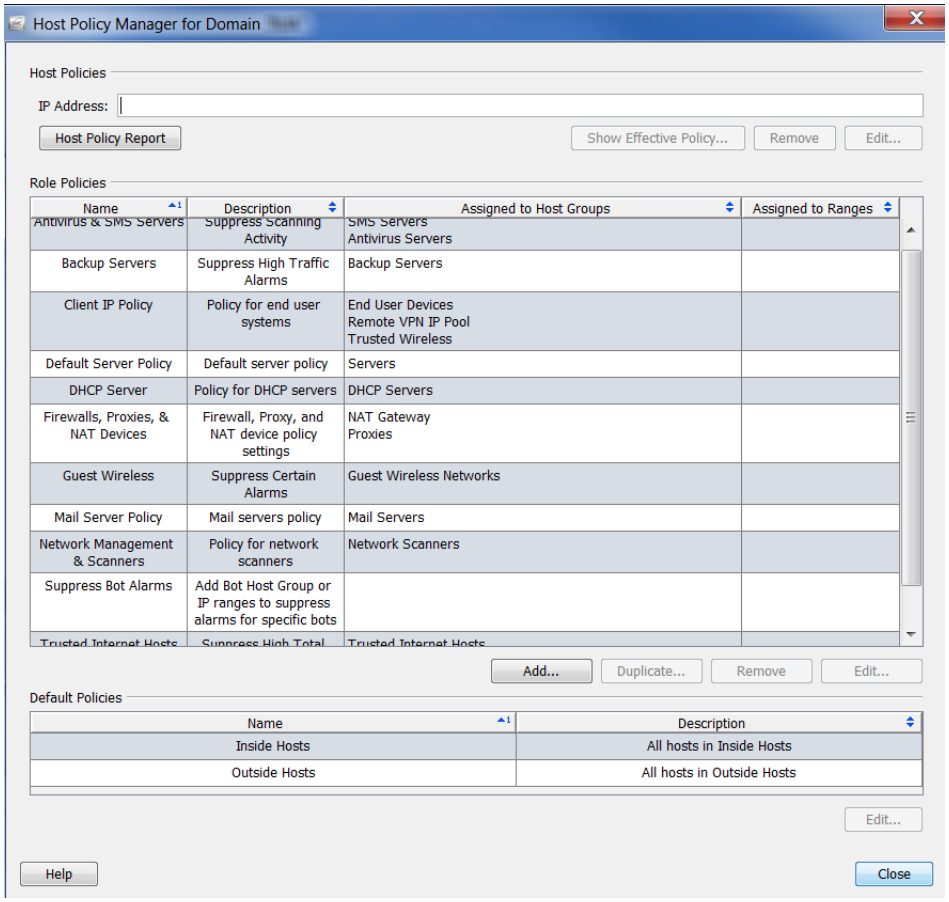
IP アドレスにホスト ポリシーが存在しない場合、Stealthwatch は、そのホストを管理するロール ポリシーから対応するアラームの設定を使用します。ホストは複数のロール ポリシーに存在し、ロール ポリシーの**すべての**設定を継承する場合があります。そのため、複数のロール ポリシーを特定のホストに適用でき、各ポリシーに対する閾値設定が異なる場合があるため、ホストの動作が各ロール ポリシー内で定義されている値を超えている場合、複数のアラームが発生する可能性があります。

（注）：

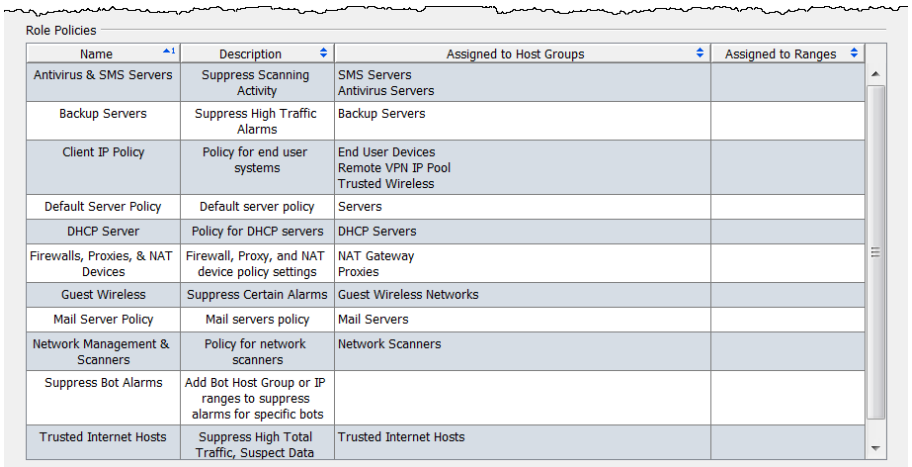
混乱を防ぐため、異なる値（異なるチームなど）に基づいて、アラームを発生させる必要がない限りは、同じアラームのある複数のロール ポリシーを使用しないことが最適です。

ロール ポリシーを追加するには、次の手順を実行します。

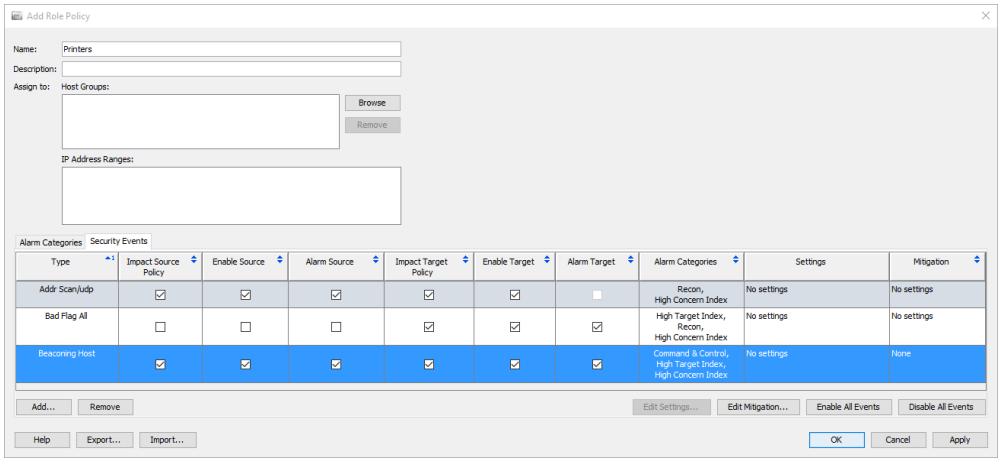
1. メイン メニューから、[設定(Configuration)] > [ホストポリシーマネージャ(Host Policy Manager)] を選択します。[ホスト ポリシー マネージャー(Host Policy Manager)] ダイアログが開きます。



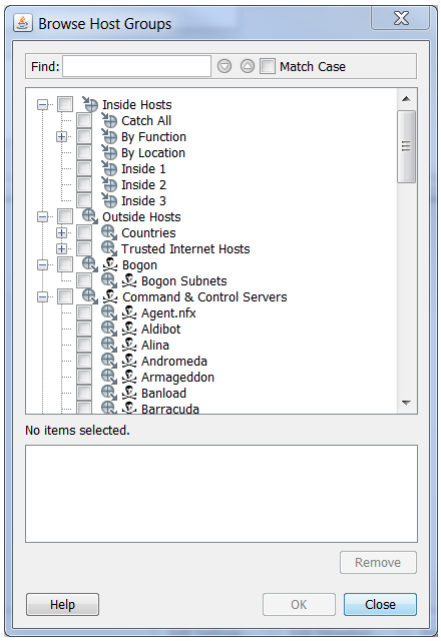
2. [ホストポリシーマネージャ(Host Policy Manager)] ダイアログで、[ロールポリシー(Role Policies)] セクション内の [追加(Add)] をクリックします。



[ロール ポリシーを追加(Add Role Policy)] ダイアログが開きます。



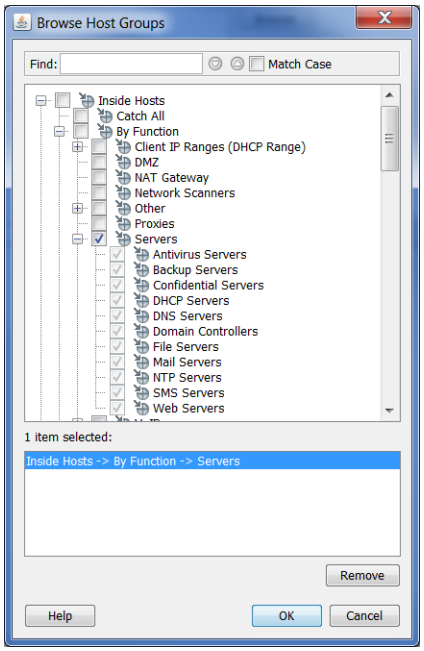
3. [名前(Name)] フィールドに、追加するポリシーの名前(会計部門など)を入力します。
4. [説明(Description)] フィールドに、説明を入力します(省略可能)。
5. 次のいずれかの手順を実行します。
   - [IP アドレスの範囲(IP Address Range)] フィールドに、特定のホストの IP アドレスまたは範囲を入力します。
   - [割当先:ホストグループ(Assign to: Host Groups)] フィールドで、[参照(Browse)] をクリックします。[ホスト グループを参照(Browse Host Group)] ダイアログが開きます。



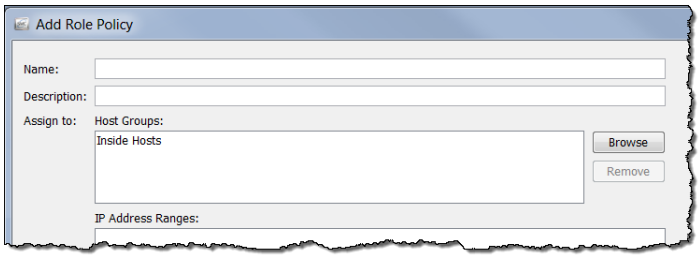
（注）:

各ホスト グループには、特定のアラームを防ぐことができるプロパティ設定があります。これらの設定を表示するには、[エンタープライズ（Enterprise）] ツリー メニュー内のホスト グループを右クリックし、[設定（Configuration）] > [ホストグループのプロパティ（Host Group Properties）] を選択します。[ホスト グループを編集（Edit Host Group）] ダイアログが開きます。[詳細なポリシー オプション（Advanced Policy Options）] は、下部に表示されます。

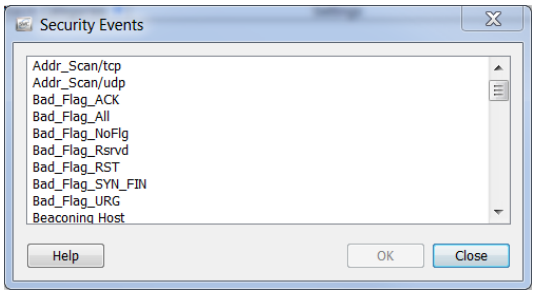
6. ポリシーが適用されるホスト グループをクリックします。親ホストをクリックすると、それの下にあるすべてのホストが自動的に選択されます。



7. [OK] をクリックします。[ロールポリシーを追加（Add Role Policy）] ダイアログの [割当先：ホストグループ（Assign to: Host Groups）] セクションにグループが表示されます。



8. [ロールポリシーを追加(Add Role Policy)] ダイアログの下部の [追加(Add)] をクリックします。[セキュリティ イベント(Security Events)] ダイアログが開きます。

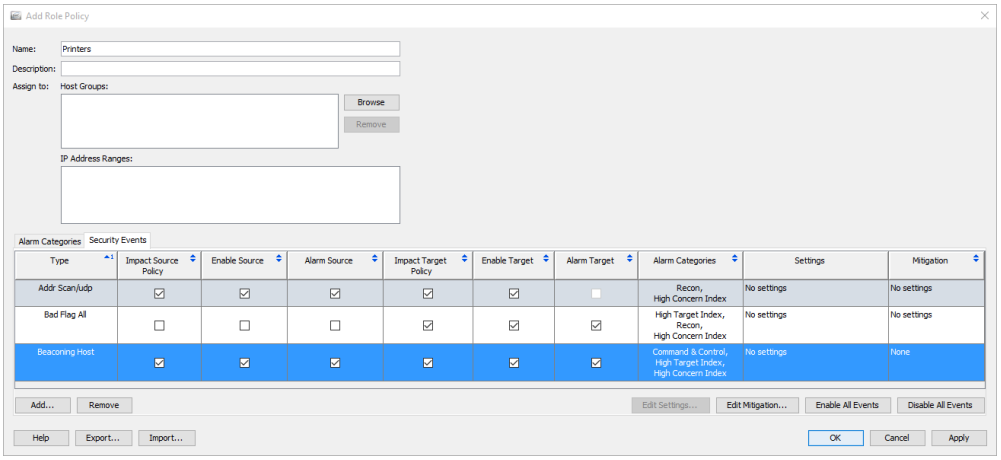


9. 編集するアラームをクリックして、[OK] をクリックします。

(注):

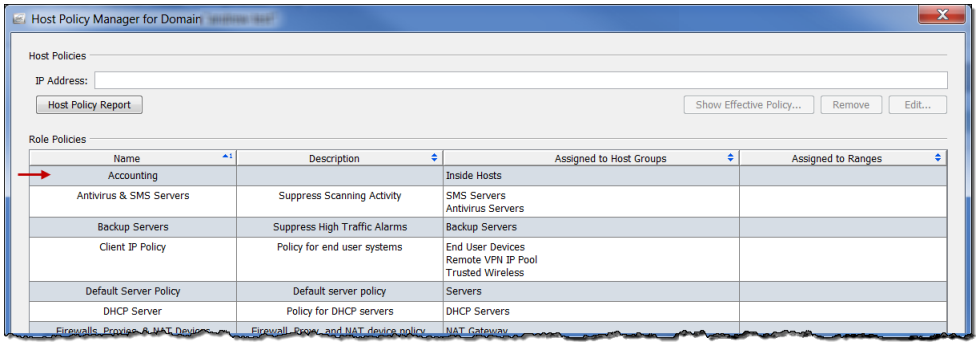
複数のアラームを選択するには、Ctrl キーを押したまま、追加する各アラームをクリックします。一定範囲内のアラームを選択するには、選択する範囲の一番上にあるアラームをクリックし、Shift キーを押したまま、選択する範囲の一番下にあるアラームをクリックします。

アラームは、[ロール ポリシーを追加(Add Role Policy)] ダイアログに表示されます。



10. このポリシーに発生させたい各アラームのチェックボックスを選択します。

11. [適用(Apply)] > [閉じる(Close)] をクリックします。ポリシーは、[ロール ポリシー(Role Policies)] セクションの [ホスト ポリシー マネージャー(Host Policy Manager)] ダイアログに表示されます。



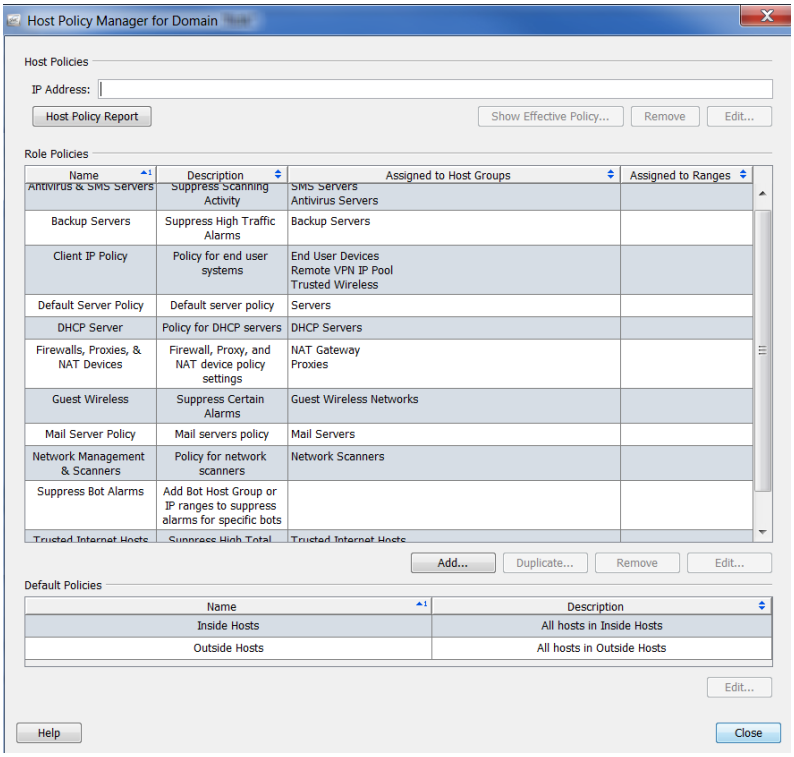
ヒント:

ロール ポリシーを一定の範囲内の IP アドレス、または複数の範囲の IP アドレスに割り当てようとしていると気づいた場合、代わりに、これらの IP アドレスに対してホスト グループを作成し、ポール ポリシーをこのホスト グループに割り当てます。

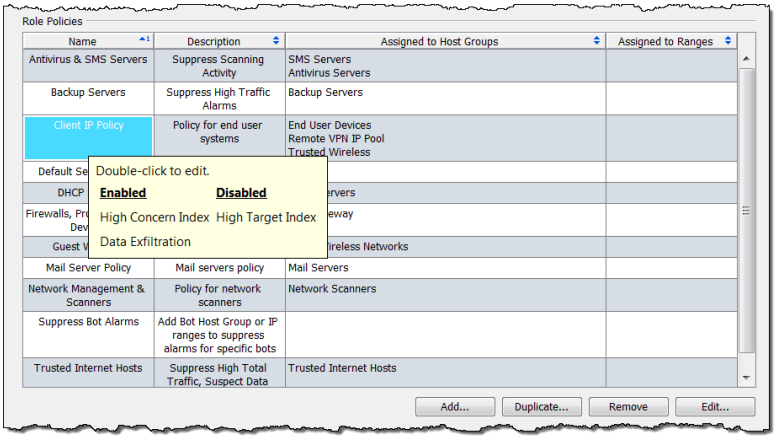
ロール ポリシーの編集

ロール ポリシーを編集するには、次の手順を実行します。

1. メイン メニューから、[設定(Configuration)] > [ホストポリシーマネージャ(Host Policy Manager)] を選択します。[ホスト ポリシー マネージャー(Host Policy Manager)] ダイアログが開きます。



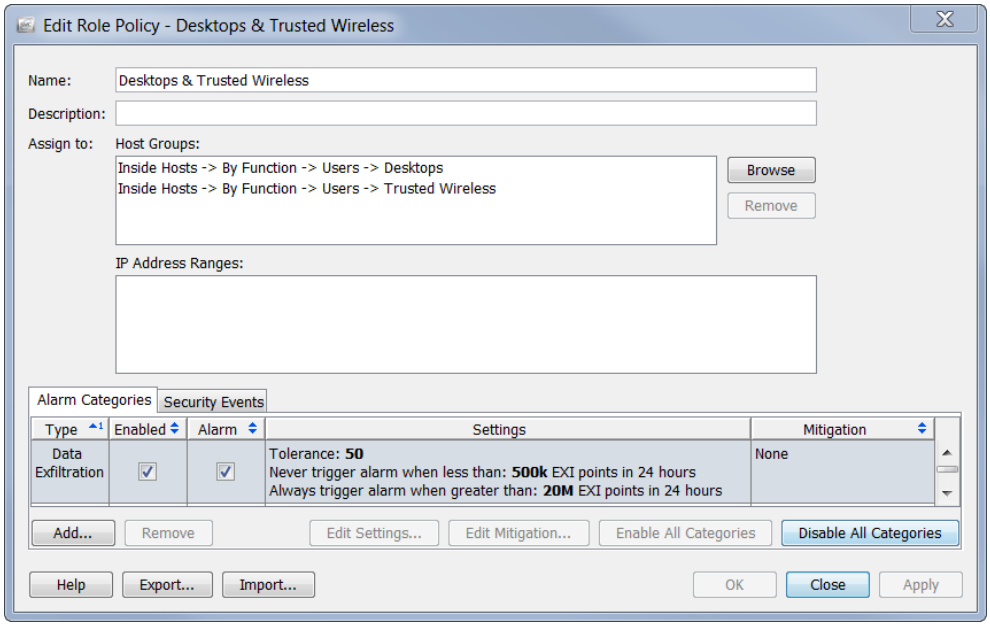
2. [ホストポリシーマネージャ(Host Policy Manager)] ダイアログの [ロールポリシー(Role Policies)] セクション内で、編集するロール ポリシーの名前をクリックして、[編集(Edit)] をクリックします。



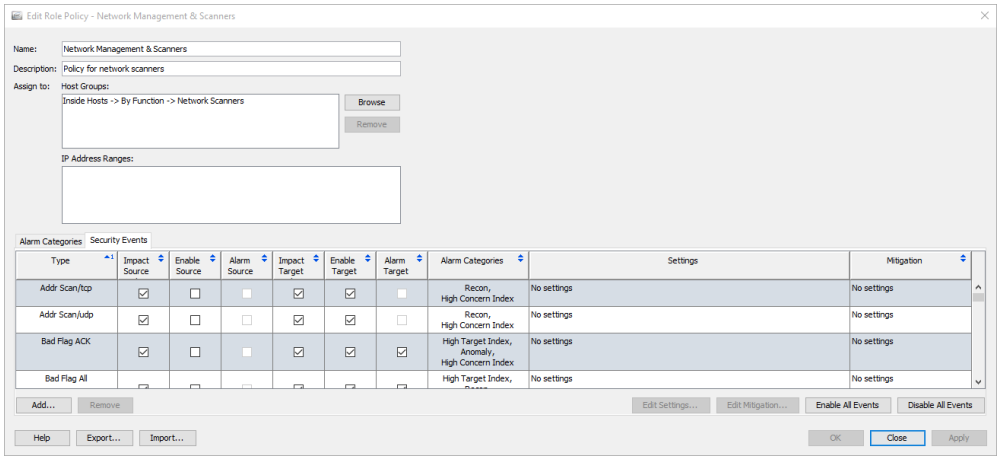
(注):

エントリーにカーソルを合わせると、すべての有効および無効になっているアラームのリストが表示されます。前の例では、アラームが無効になってないため、無効になったアラームは一覧表示されていません。

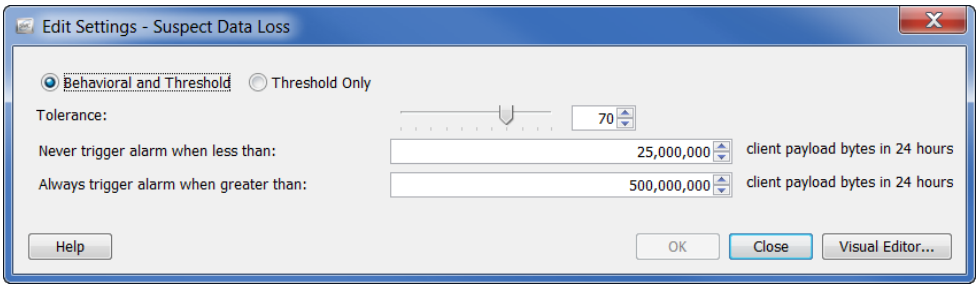
[ロール ポリシーを編集(Edit Role Policy)] ダイアログが開きます。デフォルトでは、[アラーム カテゴリー(Alarm Categories)] タブが開きます。



編集したいアラームに応じて、[セキュリティ イベント（Security Events）] タブをクリックする必要がある場合あります。



3. 編集したいアラームをダブルクリックします（必ず [設定（Setting）] 列内をクリックするようにしてください）。そのアラームの [設定を編集（Edit Settings）] ダイアログが開きます。



4. 編集を完了し、終了したら、[閉じる] をクリックします。

（注）：

- アラームの設定の各種設定の詳細については、「アラーム」（279 ページ）を参照してください。
- 特定のアラームの推奨設定については、「推奨事項」（285 ページ）を参照してください。

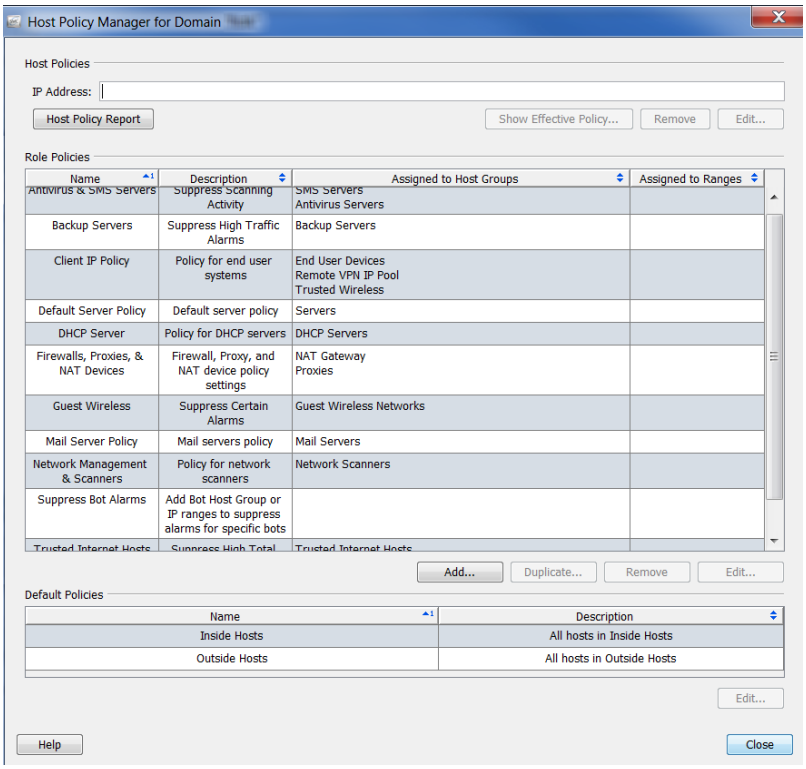
ホスト ポリシーの作成

これまで学んできたように、IP アドレスにホスト ポリシーが存在する場合、この IP アドレスがロールまたはデフォルト ポリシーのレベルでその他のアラームに割り当てられているかに関係なく、Stealthwatch は、ホスト ポリシーから対応するアラーム カテゴリーを使用して、そのホストに対してアラームを発生させるタイミングを決定します。ホスト ポリシーは、常にロール ポリシーおよびデフォルト ポリシーよりも優先されることに注意してください。

(ロール ポリシーまたはデフォルト ポリシーの編集とは対照的に)個々のホストに対して、ホスト ポリシーを編集したいでしょう。個々のアラームや、例えば、アラーム テーブルで、発生すべきではない、または、異なる閾値で発生すべき特定のアラームが特定のホストに対して発生しているとの通知を見ると、その特定のホストに対して、有効的なホスト ポリシーを修正したいと思うでしょう。

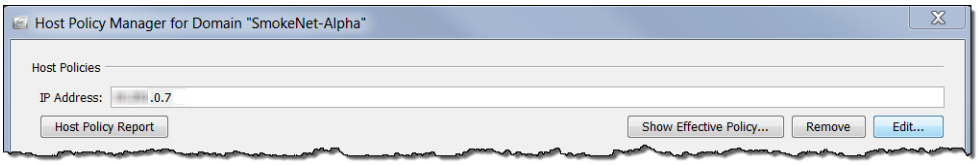
ホスト ポリシーを追加するには、次の手順に従います。

1. メイン メニューから、[設定(Configuration)] > [ホストポリシーマネージャ(Host Policy Manager)] を選択します。[ホスト ポリシー マネージャー(Host Policy Manager)] ダイアログが開きます。

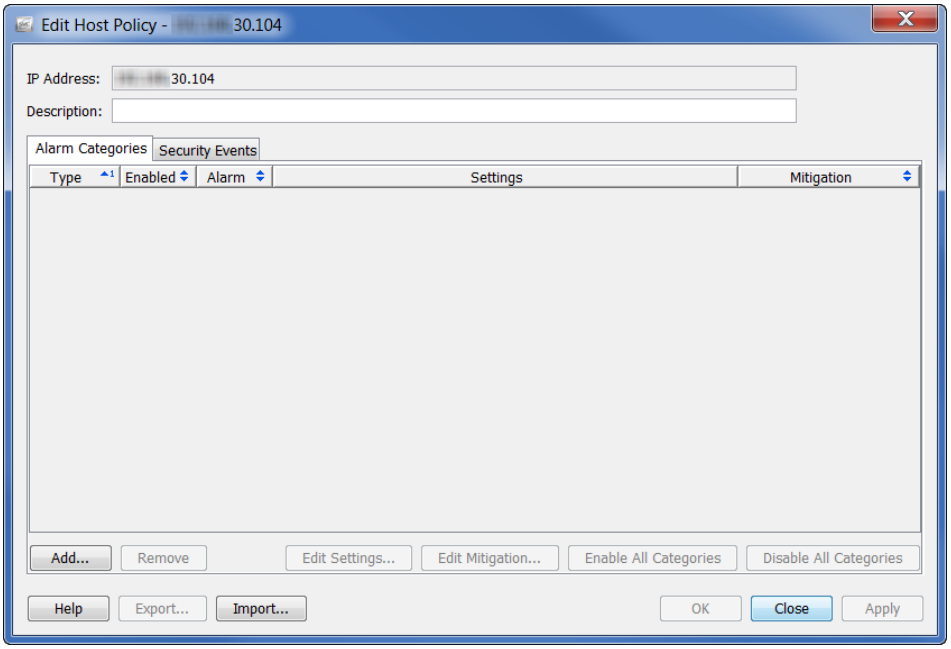


2. [ホストポリシー(Host Policies)] セクション内で、ホスト ポリシーを追加するホストの IP アドレスを入力します。

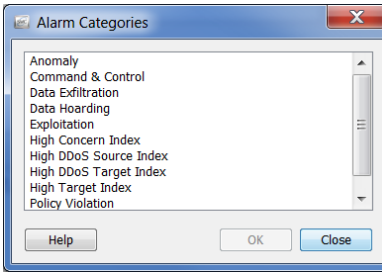
3. [編集(Edit)] をクリックします。



[ホスト ポリシーを編集(Edit Host Policy)] ダイアログが開きます。デフォルトでは、[アラーム カテゴリー(Alarm Categories)] タブが開きます。

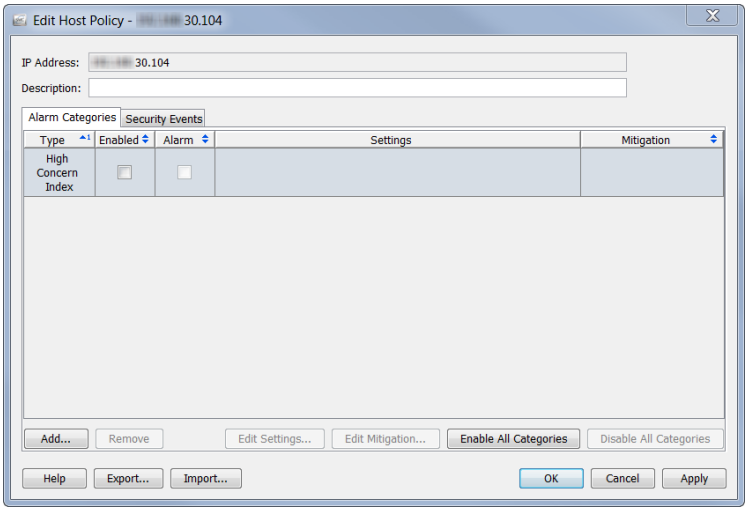


4. [追加(Add)] をクリックします。[アラーム カテゴリー(Alarm Categories)] ダイアログが開きます。
5. このアラーム カテゴリに追加するアラーム カテゴリをクリックして、[OK] をクリックします。



(注):
複数のアラームを選択するには、**Ctrl** キーを押したまま、追加する各アラームをクリックします。一定範囲内のアラームを選択するには、選択する範囲の一番上にあるアラームをクリックし、**Shift** キーを押したまま、選択する範囲の一番下にあるアラームをクリックします。

アラーム カテゴリーは、[ホスト ポリシーを編集(Edit Host Policy)] ダイアログに表示されます。

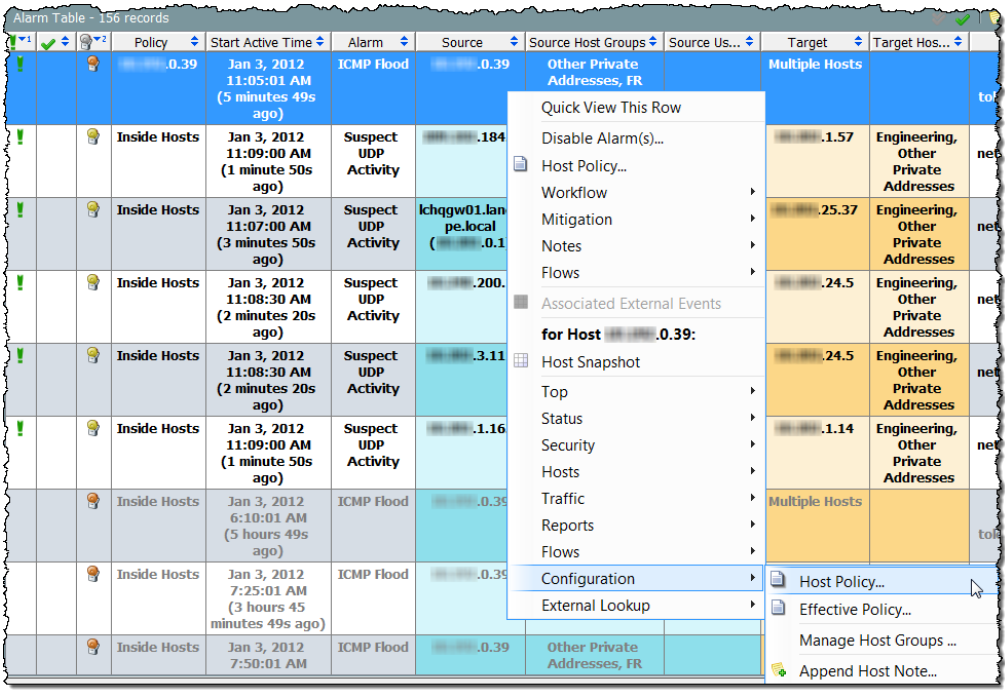


(注):
[有効(Enabled)] 列に、このポリシーを発生させたいすべてのアラームに対するチェック マークが含まれていることを確認します。

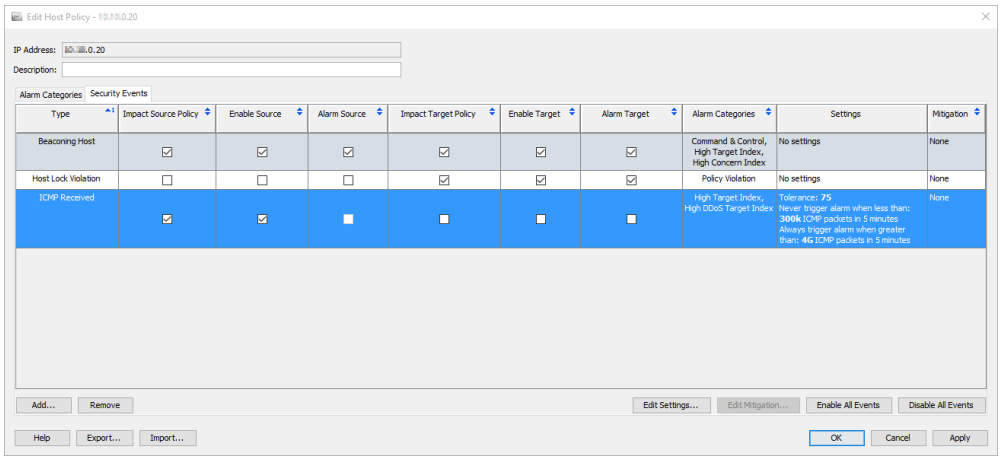
ホスト ポリシーの編集

ホスト ポリシーを編集するには、次の手順を実行します。

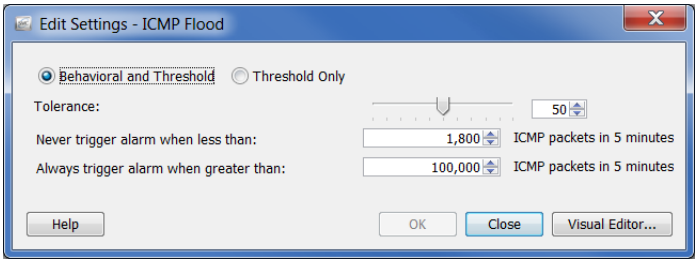
1. ホストの IP アドレスを右クリックし、[設定(Configuration)] > [ホストポリシー(Host Policy)] を選択します。



そのホストの [ホスト ポリシー(Host Policies)] ダイアログが開きます。



2. 修正したいアラームをダブルクリックします。そのアラームの [設定を編集(Edit Settings)] ダイアログが開きます。



3. 変更を加えて、[閉じる(Close)] をクリックします。

(注):

- アラームの設定の各種設定の詳細については、「アラーム」(279 ページ)を参照してください。
- 特定のアラームの推奨設定については、「推奨事項」(285 ページ)を参照してください。

アラーム

分散によるアラーム対オンまたはオフ アラーム

ホストの活動に過去の動作からの大幅な変更があると、アラームが発生します。これらの種類のアラームの許容差(つまり、感度)は、ホスト ポリシー マネージャーを使用して変更できます。これらのアラームは、分散によるアラームと呼ばれます。次の表に分散によるアラームを示します。

(注):
アラーム カテゴリーも分散によるアラームです。

分散によるアラーム	
[異常(Abnormaly)]	[ポート スキャン(Port Scan)]
[総当たりログイン(Brute Force Login)]	[相関高合計トラフィック(Relational High Total Traffic)]
[コマンドおよびコントロール(Command & Control)]	[相関高トラフィック(Relational High Traffic)]
[データの漏洩(Data Exfiltration)]	[相関 ICMP フラッド(Relational ICMP Flood)]
[データの蓄積(Data Hoarding)]	[相関低トラフィック(Relational Low Traffic)]
[エクスプロイト(Exploitation)]	[相関最大フロー開始(Relational Max Flows Initiated)]
[高懸念インデックス(High Concern Index)]	[相関最大フロー供給(Relational Max Flows Served)]
[高 DDoS ソース インデックス(High DDoS Source Index)]	[相関 SYN フラッド(Relational SYN Flood)]
[高 DDos ターゲット インデックス(High DDoS Target Index)]	[相関 UDP フラッド(Relational UDP Flood)]
[高ファイル共有インデックス(High File Sharing Index)]	[相関往復時間(Relational Round Trip Time)]
[高 SMC ピア(High SMC Peers)]	[相関サーバー応答時間(Relational Server Response Time)]
[高ターゲット インデックス(High Target Index)]	[相関 TCP 再送率(Relational TCP Retransmission Ratio)]

分散によるアラーム	
[高トラフィック(High Traffic)]	[相関高合計トラフィック(Relational High Total Traffic)]
[大容量電子メール(High Volume Mail)]	[低速接続フラッド(Slow Connection Flood)]
[ICMP フラッド(ICMP Flood)]	[SPAN ソース(Span Source)]
[ICMP 受信(ICMP Received)]	[SSH リバース シェル(SSH Reverse Shell)]
[メール拒否(Mail Rejects)]	[データの蓄積の疑い(Suspect Data Hoarding)]
[メール リレー(Mail Relay)]	[データの損失の疑い(Suspect Data Loss)]
[最大フロー開始(Max Flows Initiated)]	[SYN フラッド(SYN Flood)]
[最大フロー供給(Max Flows Served)]	[SYN 受信(SYNs Received)]
[パケット フラッド(Packet Flood)]	[ターゲット データの蓄積(Target Data Hoarding)]
[新フロー開始(New Flows Initiated)]	[接触(Touched)]
[新フロー供給(New Flows Served)]	[閉じ込められたホスト(Trapped Host)]
[ポリシー違反(Policy Violation)]	[UDP フラッド(UDP Flood)]
[偵察(Recon)]	[UDP 受信(UDP Received)]

この手法の主な利点は、発生するアラームの数が組織のニーズに合致するよう、システムを調整できるという点です。つまり、アラームが多い方がいい(つまり、予想される動作からのわずかな変更だけ許容できる)場合に、関連するポリシー内で許容差設定を下げることができます。逆に、アラームが少ない方がいい(つまり、予想される動作からの大幅な変更を許容できる)場合、許容差設定を上げることができます。基本的には、分散によるアラームに対する設定はそれぞれ、数値に割り当てられ、この値は、上方または下方調整できます。

分散によるアラームに使用される閾値は、最近の活動や設定した許容差に生成されます。これにより、ホストは、その動作がその動作が完全に変更されても、アラームを発生する能力を失うことなく、時間と共にその動作を変更できます。許容差は、どのくらい変更が許容可能かを制御する方法を提供します。基本的に、アラームの閾値レベルの感度を調整することができます(つまり、必要なレベルにまで「ノイズを下げる」ことができます)。

分散によるアラームで、アラームを発生させる前にホストは、ベースラインからの一定の偏差を到達する必要があります。たとえば、[高合計トラフィック(High Total Traffic)] アラームに対する許容差レベルが 50 に設定されている場合、システムは、期待値(ホストのベースライン)を超える値の 50% を無視しますが、その値を超える値にもアラームを発生させます。

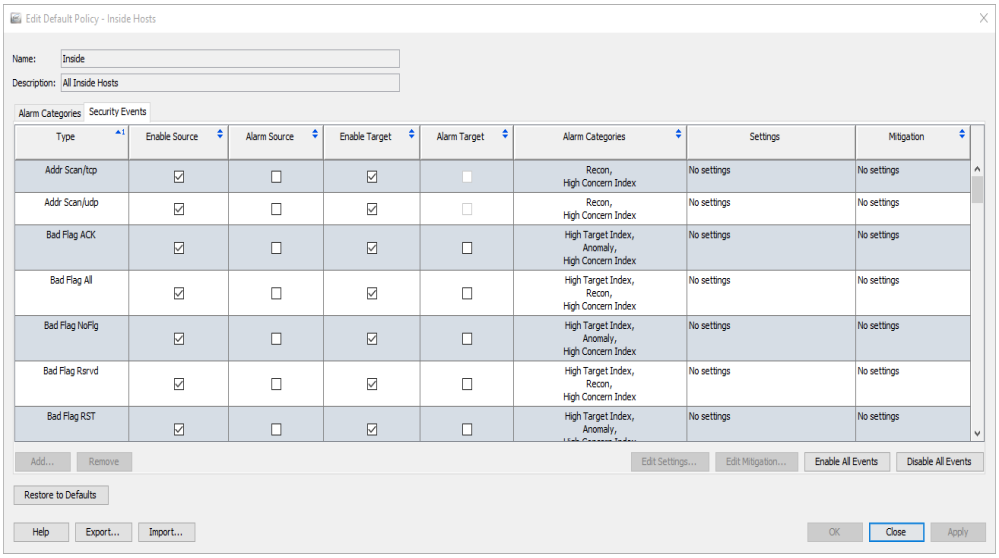
(注):
アラーム設定の詳細については、「分散によるアラームの設定」(282 ページ)を参照してください。

アラームの 2 つ目の種類は、オンまたはオフのいずれかにできるアラームです。この種類のアラームを発生させる基準は、分散によるアラームの基準によって異なります。単にオンまたはオフ設定のあるアラームの場合、ホストの動作は、この種類のアラームが発生する前に、すべて相互に一致する必要がある一定の条件に一致する必要があります。これらすべての条件が存在しない場合、アラームを発生しません。たとえば、ワームの活動アラームを発生するには、次の動作が**すべて** 発生している必要があります。

- ソース ホストが複数のサブネットをスキャンしている。
- 少なくとも 1 つのターゲット ホストがソース ホストに接続している。
- このターゲット ホストがソース ホストに情報を転送している。

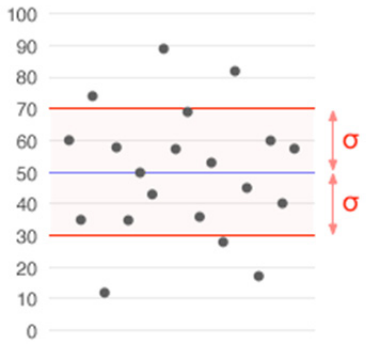
これらの条件の 1 つでも存在しない場合、アラームを発生しません。

どのアラームが分散によるアラームか、オンまたはオフ アラームかは、[デフォルト ポリシーを編集(Edit Default Policy)] ダイアログ内の [設定(Settings)] 列を見ればわかります。アラームが分散によるアラームの場合、そのアラームに対して表示されている許容差値が表示されます。アラームがオンまたはオフの場合、エントリー「設定なし」が表示されます。



分散によるアラームの設定

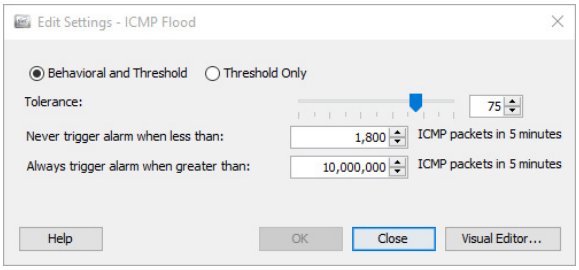
前項で述べたように、分散によるアラームで使用されている閾値は、最近の活動と設定された許容差に基づいてベースラインから生成されます。許容差は、「最頻値からの標準偏差の数」として定義され、アラームの閾値レベルの感度を調整する方法を提供します。



A data set with a mean of 50 (shown in blue) and a standard deviation (σ) of 20.

標準偏差は、統計で広く使用されている変動または多様性の測定値です。平均からどのくらいの変化があるが(つまり、平均または期待値)を示しています。低い標準偏差は、データ ポイントが平均に非常に近い傾向にあることを示し、一方で、高い標準偏差は、データ ポイントが広い範囲の値に広がっていることを示しています。

次の例では、分散によるアラームに対する [設定を編集(Edit Settings)] ダイアログを示します。



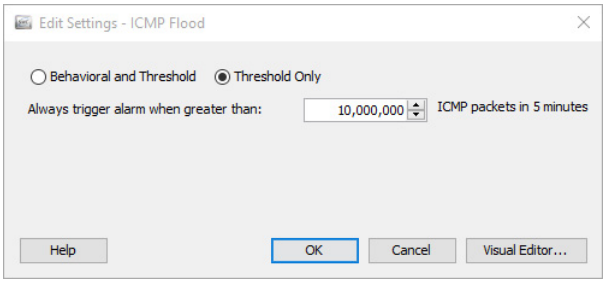
分散によるアラームには、次の調整可能な設定が含まれています。

- [動作と閾値(Behavioral and Threshold)]: このオプションを選択した場合、ダイアログに許容差の設定、最小閾値と最大閾値が表示されます。
  - [許容差(Tolerance)]: アラームを発生する前に、動作がどれほど予想される動作を超えることができるかを示す、0 ～ 100 の相対的な数。これにより、ユーザーは、何に「有意差」があるかを定義できます。
    - 許容差 0 は、期待値を超える値に対してアラームが発生することを意味していますが、これは非常に敏感で、多くのアラームが発生します。

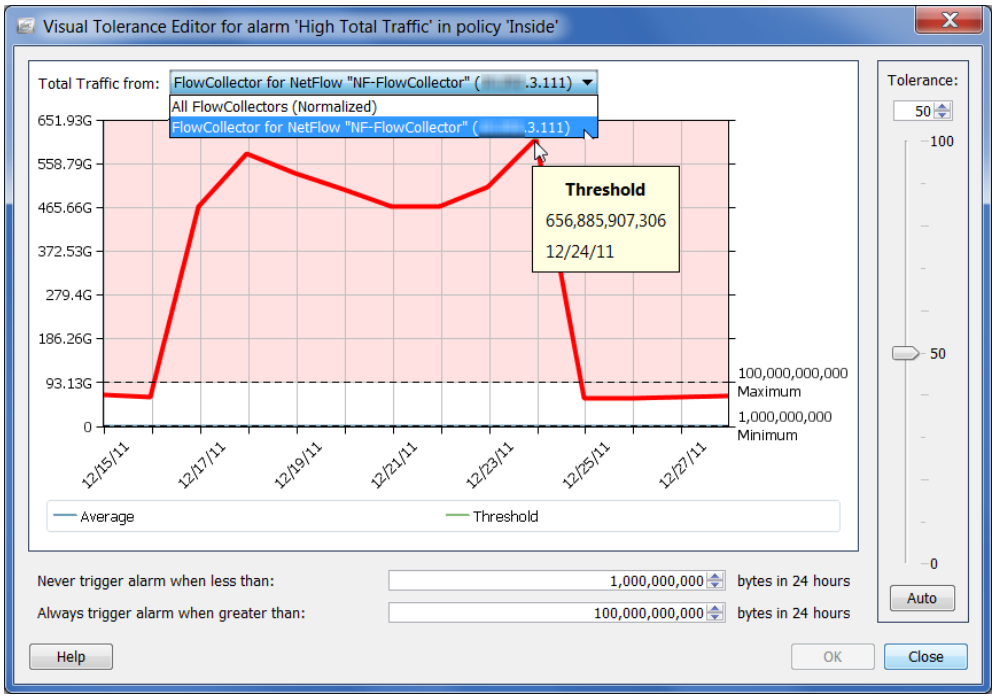
- 許容差 100 は、アラームが許容される最高レベルです。アラームが発生する回数が大幅に減りますが、アラームを無効にしただけでは、アラームが発生しないということにはなりません。
- 許容差 50 は、ホストが期待値を超える値の最低 50% を無視しますが、その値を超える値に対してアラームを発生させます。

- [次の値未満の場合はアラームを発生させない(Never trigger alarm when less than)]:「*最小しきい値*」とも呼ばれ、アラームを発生させることができる最小値を示す静的値です。測定値がこの設定を下回ると、アラームは発生しません。つまり、たとえホストがその期待値を大幅に超えても、このダイアログに示す最小値以下であれば、アラームは発生しません。
- [次の値を超える場合は常にアラームを発生させる(Always trigger alarm when greater than)]:「*最大しきい値*」とも呼ばれ、アラームを発生させずに可能な最大値を示す静的値です。この設定では、測定値を超えると、アラームが発生します。つまり、ホストがこのダイアログに示す最大値を超えると、そのホストに予想されているとしても、アラームが発生します。

▶ [閾値のみ(Threshold Only)]: このオプションを選択すると、ダイアログは、最大閾値設定のみを示します。



[ビジュアルエディタ(Visual Editor)] をクリックして、[ビジュアルエディタ(Visual Editor)] ダイアログにアクセスします。ビジュアル許容差エディターは、次の例に示すように、特定のアラームに対するホストまたはホスト グループ ポリシーの設定を調整するグラフィカルな方法です。



(注):

フロー コレクタを 1 つだけ使用している場合は、画面上部にある [合計トラフィック(Total Traffic from)] ドロップダウン リストから、[フローコレクタ(Flow Collector)] オプションをクリックして、関連するアラームの実際の値を確認します。複数のフロー コレクタを使用している場合、[正規化(Normalized)] オプションをクリックして、値を正規化します。

推奨事項

この項では、過剰な数の不要なアラームを受信している場合のネットワークの微調整に関する推奨事項について説明しています。この項における推奨事項は、アルファベット順に、最も一般的なアラームの種類に従って分類されています。

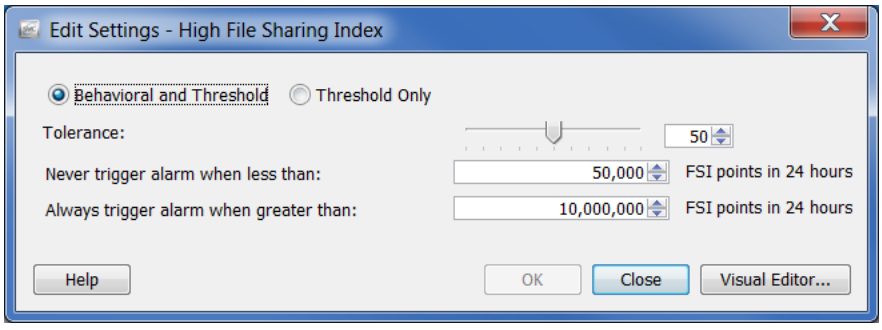
(注):

- これらのアラームやその他のアラームの詳細については、Stealthwatch デスクトップクライアントのオンラインヘルプにある「アラームリスト」を参照してください。
- 次に示すアラームの設定を調整する方法の詳細については、「分散によるアラームの設定」(282 ページ)を参照してください。

[高ファイル共有インデックス(High File Sharing Index)]

[高ファイル共有インデックス(High File Sharing Index(FSI)] アラームは、ファイル共有活動がホスト ポリシー マネージャーで定義した FSI 閾値を超えたことを示します。高 FSI アラームを発生させているホストをファイル共有に使用している場合、次の手順のいずれかを実行して、確認している不要なアラームの数を減らすことができます。

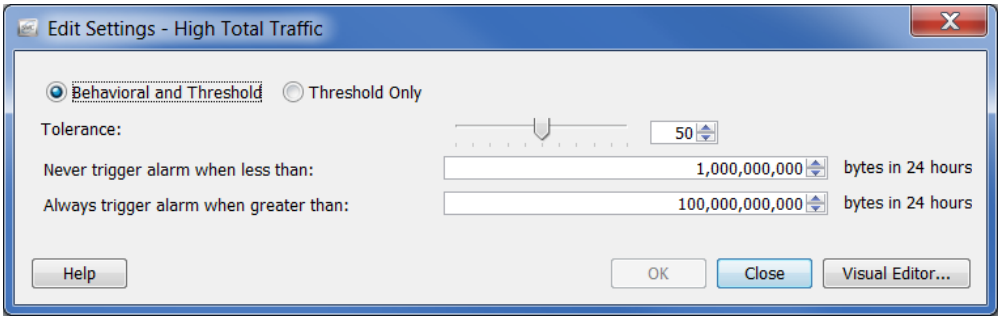
- 対応するポリシー内の [有効(Enabled)] チェックボックスをクリックして、チェック マークを外すことで、対象のホストまたはホスト グループに影響を与えるポリシーに対して、[高ファイル共有インデックス(High File Sharing Index)] アラームを無効にします。
- 問題のホストまたはホスト グループに影響を与えているポリシーに対する [高ファイル共有インデックス(High File Sharing Index)] アラームのしきい値または許容差設定を上げます。



[高合計トラフィック(High Total Traffic)]

[高合計トラフィック(High Total Traffic)] アラームは、合計受信トラフィックと合計送信トラフィックがホストに対するポリシー設定を超えていることを示します。確認されている高合計トラフィック アラームの量に不満の場合は、対応するポリシーの設定を調整します。

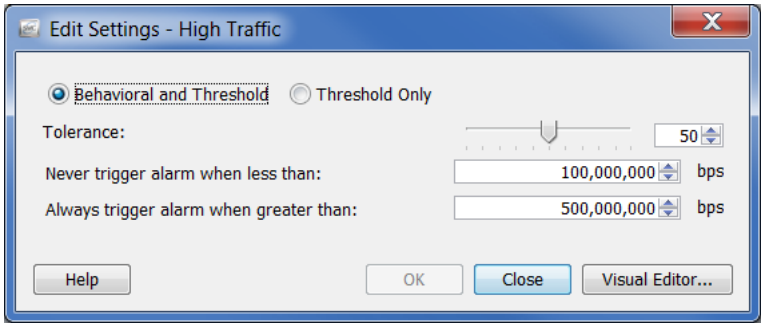
報告されている平均バイト数を超えている問題のホストまたはホスト グループのポリシー設定を上げます。



[高トラフィック(High Traffic)]

[高トラフィック(High Traffic)] アラームは、5 分間の平均ホスト トラフィック率が許容可能なトラフィック値の限界を超えていることを示します。確認されている高トラフィック アラームの量に不満の場合は、対応するポリシーの設定を調整します。

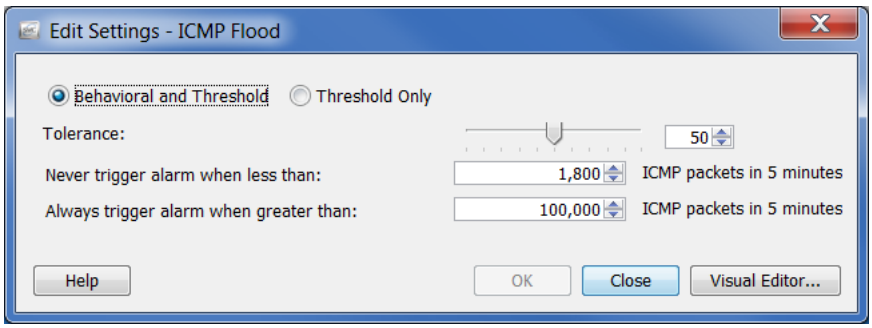
報告されている平均バイト数を超えている問題のホストまたはホスト グループのポリシー設定を上げます。



[ICMP フラッド(ICMP Flood)]

[ICMP フラッド(ICMP Flood)] アラームは、ソース ホストが最後の 5 分で過剰な数の ICMP パケットを送信したことを示します。サービス拒否(DoS)攻撃や非ステルス スキャン活動の可能性があることを示す場合があります。このような状況を解決するには、どのようなホストがアラームを引き起こしているかを特定します。ネットワーク上のホストに大量の ping を送信する管理サーバーの場合があります。

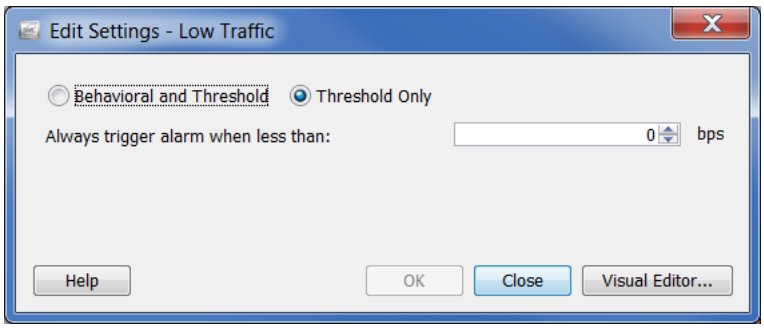
このアラームを停止するには、対応するポリシー内の [有効(Enabled)] チェックボックスをクリックして、チェック マークを外し、問題のホストまたはホスト グループに対する ICMP フラッド アラームを無効にします。



[低トラフィック(Low Traffic)]

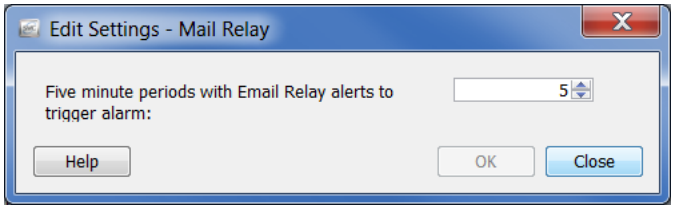
[低トラフィック(Low Traffic)] アラームは、5 分間の平均ホスト トラフィック率が許容可能な最小トラフィック値未満であったことを示します。確認されている低トラフィック アラームの量に不満の場合は、対応するポリシーの設定を調整します。

報告されている平均バイト数を超えている問題のホストまたはホスト グループのポリシー設定を上げます。



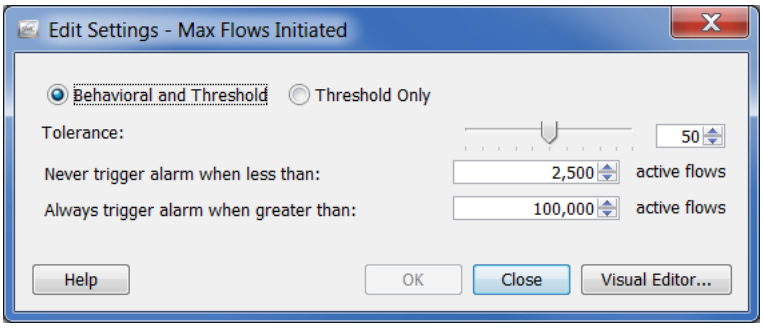
[メール リレー(Mail Relay)]

[メール リレー(Mail Relay)] アラームは、ターゲット ホストがメール リレーとして動作している可能性があることを示します。これらが本当のメール サーバーの場合、対応するポリシー内の [有効(Enabled)] チェックボックスをクリックして、チェック マークを外し、問題のホストまたはホスト グループに対するメール リレー アラームを無効にします。



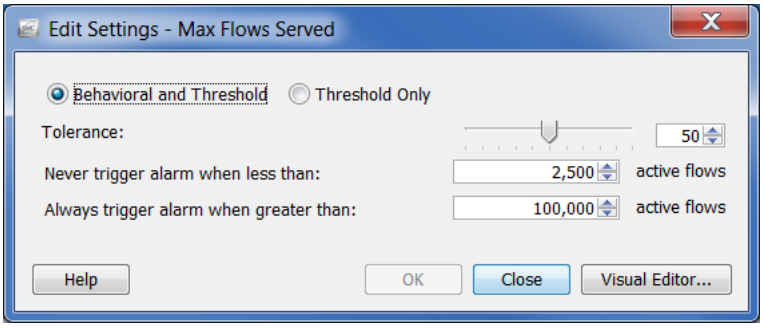
[最大フロー開始(Max Flows Initiated)]

[最大フロー開始(Max Flows Initiated)] アラームは、ホストが対応する [次の値を超える場合は常にアラームを発生させる(Always trigger alarm when greater than)] ポリシー設定で指定されている、許可されている数よりも多くのフローを開始したことを示します。特にこれがドメイン コントローラーの場合は、この設定を調整します。



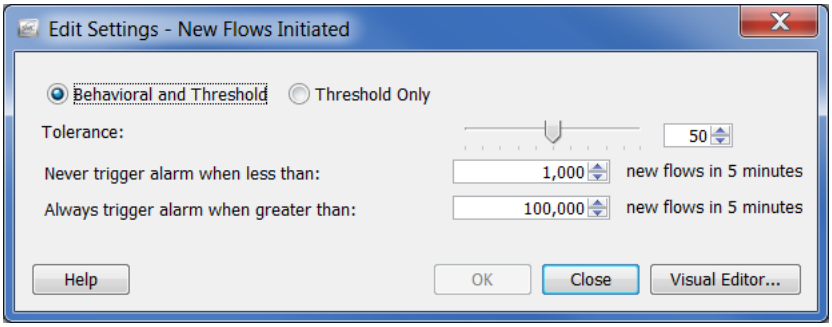
[最大フロー供給(Max Flows Served)]

[最大フロー供給(Max Flows Served)] アラームは、ホストが対応する [次の値を超える場合は常にアラームを発生させる(Always trigger alarm when greater than)] ポリシー設定で指定されている、許可されている数よりも多くのフローを供給したことを示します。特にこれがドメイン コントローラーの場合は、この設定を調整します。



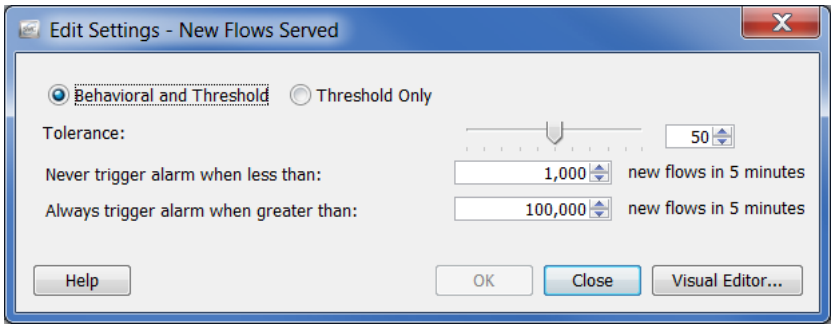
[新フロー開始(New Flows Initiated)]

[新フロー開始(New Flows Initiated)] アラームは、ホストが 5 分間で開始された新しいフローの合計数に対するポリシー設定を超えたことを示します。特にこれがドメイン コントローラーの場合は、この設定を調整します。



[新フロー供給(New Flows Served)]

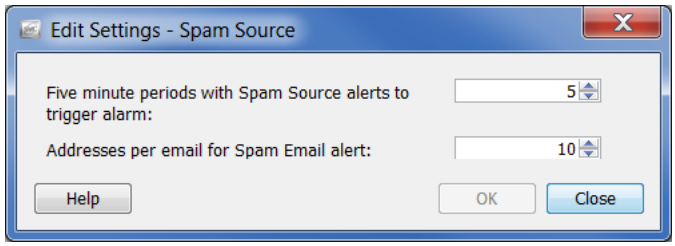
[新フロー供給(New Flows Served)] アラームは、ホストが 5 分間で供給した新しいフローの合計数に対するポリシー設定を超えたことを示します。特にこれがドメイン コントローラーの場合は、この設定を調整します。



[スパム ソース(Spam Source)]

[スパム ソース(Spam Source)] アラームは、ソース ホストがスパム メールを送信している可能性があることを示します。ホストがメール サーバーの場合は、対応するポリシー内の [有効(Enabled)] チェックボックスをクリックして、チェック マークを外し、問題のホストまたはホスト グループに対するスパム ソース アラームを無効にします。

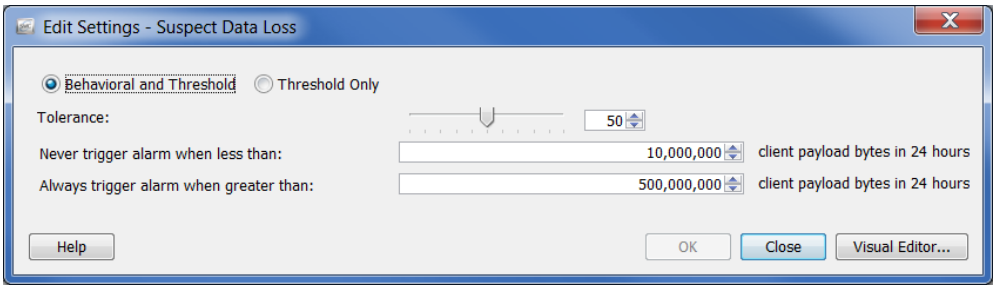
ホストがメール サーバーではない場合は、感染している可能性があります。



[データの損失の疑い(Suspect Data Loss)]

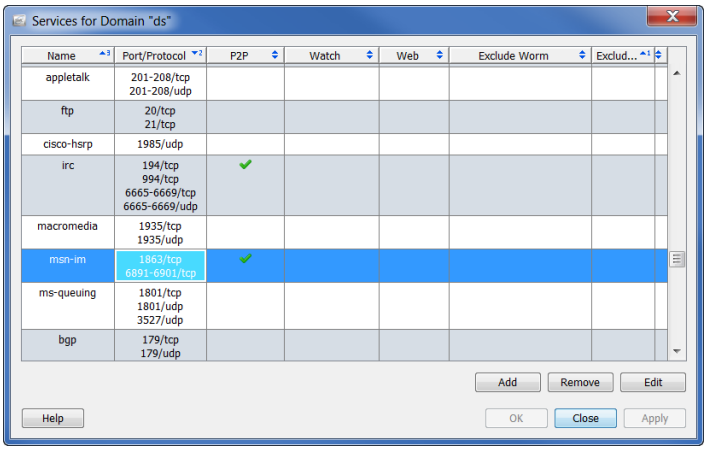
[データの損失の疑い(Suspect Data Loss)] アラームは、外部のホスト グループに対する TCP および UDP ペイロード データの合計がポリシー設定を超えていることを示します。確認されているデータ損失の疑いアラームの数に不満の場合は、ホスト グループ(YouTube、Facebook、ビジネス パートナーなどの)外部の既知の高トラフィックに対して、このアラームを無効にします。

その後、重要なホストまたはホスト グループに対するポリシー設定を調整します。閾値を報告されている平均バイト数以上に上げます。

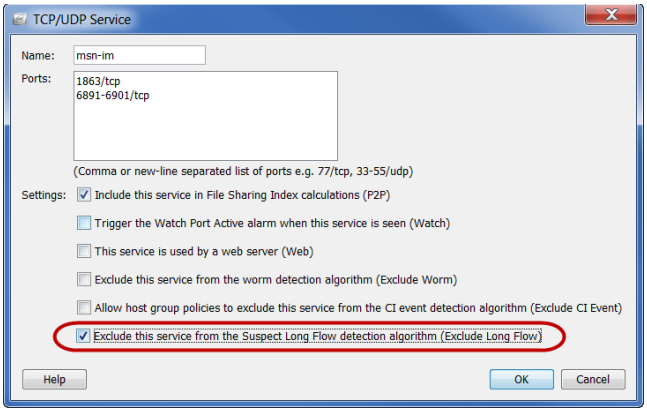


[長フローの疑い(Suspect Long Flow)]

[長フローの疑い(Suspect Long Flow)] アラームは、フローを長い期間とするのに必要な「秒」の間に、内部および外部のホスト間の IP 通信が設定を超えていることを示します。このアラームは、スパイウェアや遠隔デスクトップ技術(gotomypc.com など)、VPN、IRC ボットネット、およびその他の隠れた通信手段などの疑わしい通信チャンネルを検出します。IM 技術を使用している内部ホストは、最大許容値(デフォルトは、9 時間)よりも長いフローによって、この種のアラームを発生しやすい傾向にあります。



設定されたサービスを変更することによって、AOL AIM(ポート 5190)、Yahoo IM(TCP ポート 5050)、MSN メッセンジャー(TCP ポート 1863)などの IM 技術が長フローの疑いアラームを発生させないようにできます。メイン メニューから、[設定(Configuration)] > [サービス(Service)] を選択します。該当するドメインの [サービス(Service)] ダイアログボックスを開きます。



編集しているサービスの名前を含む行を選択して、画面下部にある [編集(Edit)] をクリックします。[このサービスを長フローの疑い検出アルゴリズムから除外(長フローを除外) (Exclude this service from the Suspect Long Flow detection algorithm (Exclude Long Flow))] チェックボックスをクリックして、チェック マークを追加します。

代わりに、ビジネス パートナーなどの権限のあるネットワークに対して外部ホスト グループを作成して、対応するポリシーで長フローの疑いアラームを無効にします。

(注):

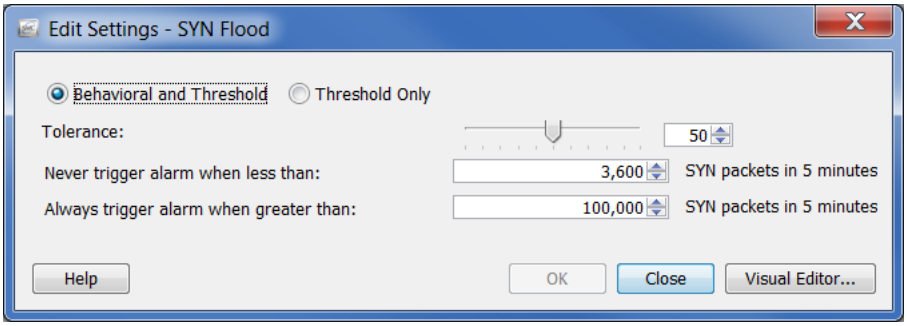
長フローの疑いアラームは、クライアントとサーバーの関係に関係なく、内部ホストに対して常に発生します。外部ホストに対してこのアラームを無効にすると、その外部ホストに接続している内部ホストは、このアラームから除外されます。

[UDP の活動の疑い(Suspect UDP Activity)]

[UDP の活動の疑い(Suspect UDP Activity)] アラームは、UDP ポート上でスキャニングを行っているホストが別のホストに 1 つの大きなパケットを送信したことを示します。このタイプの動作は、SQL Slammer や Witty などの多くのシングルパケット UDP ベースのワームに合致しています。このアラームをただちに調査してください。

[SYN フラッド（SYN Flood）]

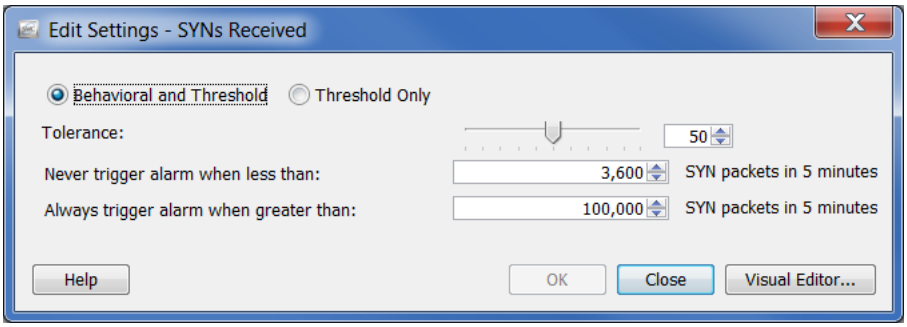
[SYN フラッド（SYN Flood）] アラームは、ホストが 5 分間で過剰な数の TCP 接続要求（SYN パケット）のを送信したことを示します。このアラームを調査して、DOS 攻撃または非ステルス スキャン活動が進行中かどうかを確認してください。



[SYN 受信（SYNs Received）]

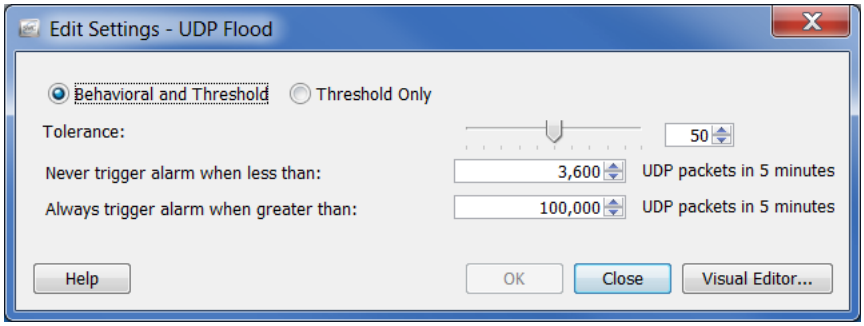
[SYN 受信（SYNs Received）] アラームは、ホストが 5 分間にあまりにも多くの未回答 TCP 接続要求（SYN パケット）を受信したことを示します。このアラームは、分散（多対一）DoS 攻撃を示している可能性があります。

ただし、サーバーが大量の SYN パケットを受信するのは一般的です。この場合、[次の値未満の場合はアラームを発生させない（Never trigger alarm when less than）] 設定を確認しているアラームの平均数よりも上げます。その他のサーバーよりも多くの SYN パケットを受信するサーバーを、Web サーバーやアプリケーション サーバーなどの別のホスト グループに分離したい場合があります。



[UDP フラッド（UDP Flood）]

[UDP フラッド（UDP Flood）] アラームは、ソース IP が最後の 5 分間で過剰な数の UDP パケットを送信したことを示します。このアラームを調査して、DOS 攻撃または非ステルス スキャン活動が進行中かどうかを確認してください。



[ワームの活動（Worm Activity）]

[ワームの活動（Worm Activity）] アラームは、ホストが複数のサブネットで、特定のポートでスキャンと接続を行ったことを示します。このアラームの詳細部は、活動が確認されたポートを指定します。

ドメイン コントローラーが UDP ポートでアドレス スキャンおよび ping スキャンを実行するのは正常です。[ワームの活動（Worm Activity）] アラームがドメイン コントローラのあるホスト グループで発生した場合、対応するポリシー内の [高懸念インデックス（High Concern Index）] アラームに対する [セキュリティイベント（Security Events）] タブにある [Addr_Scan/udp] および [Ping] チェックボックスを削除することで、これらのアラームを防ぐことができます。

12

ドキュメントの操作

概要

この章では、レイアウト設定やフィルター設定の特定のセットがある SMC ドキュメントを保存する方法やログイン ドキュメントの一覧にドキュメントを追加する方法、DAR ファイルの作成方法、ドキュメントの共有方法、定期的なドキュメントの生成方法や他の人間へのドキュメントを電子メールで送信する方法などプロセスについて説明します。

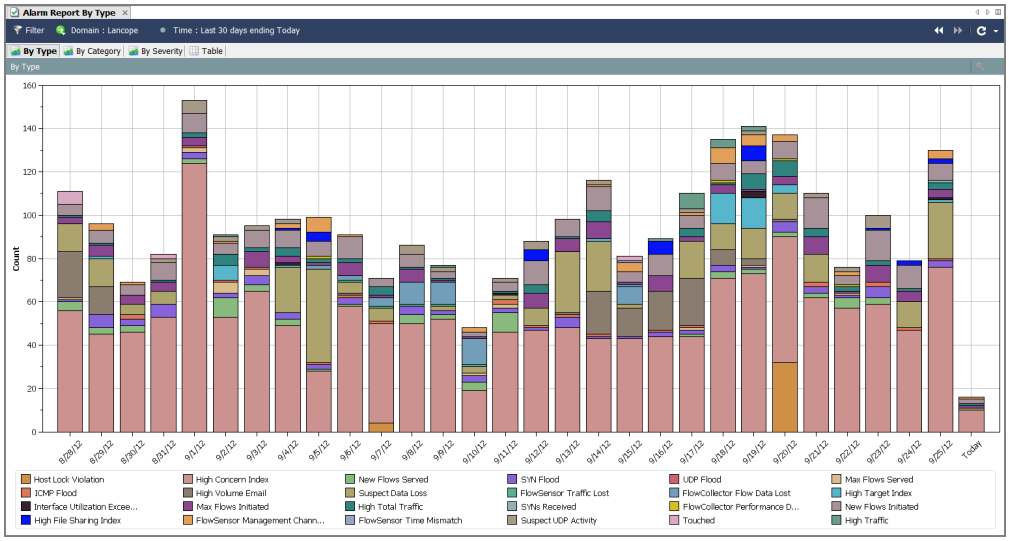
この章は、次の項で構成されています。

ドキュメントの保存

SMC ドキュメントのレイアウトを変更し、後で使用するレイアウトを保存したい場合は、ドキュメントを保存します。ドキュメントを保存すると、いつでも検索できるよう、SMC アプライアンスに保存されます。

ドキュメントを保存するには、次の手順に従います。

1. 保存するドキュメントを開きます。たとえば、[種類別アラームレポート(Alarm Report By Type)] ドキュメントを開きます。



2. レイアウトまたはフィルターの設定に必要な変更を加えます。
3. (オプション) SMC のメイン メニューから [ファイル(File)] > [印刷設定(Print Settings)] を選択し、表示されるダイアログ内で、印刷のたびにドキュメントの外観を設定します。[OK] をクリックして、変更を保存します。
4. (オプション) ドキュメントが PDF としてどのように表示されるかを確認するには、[ファイル(File)] > [印刷プレビュー(Print Preview)] を選択します。

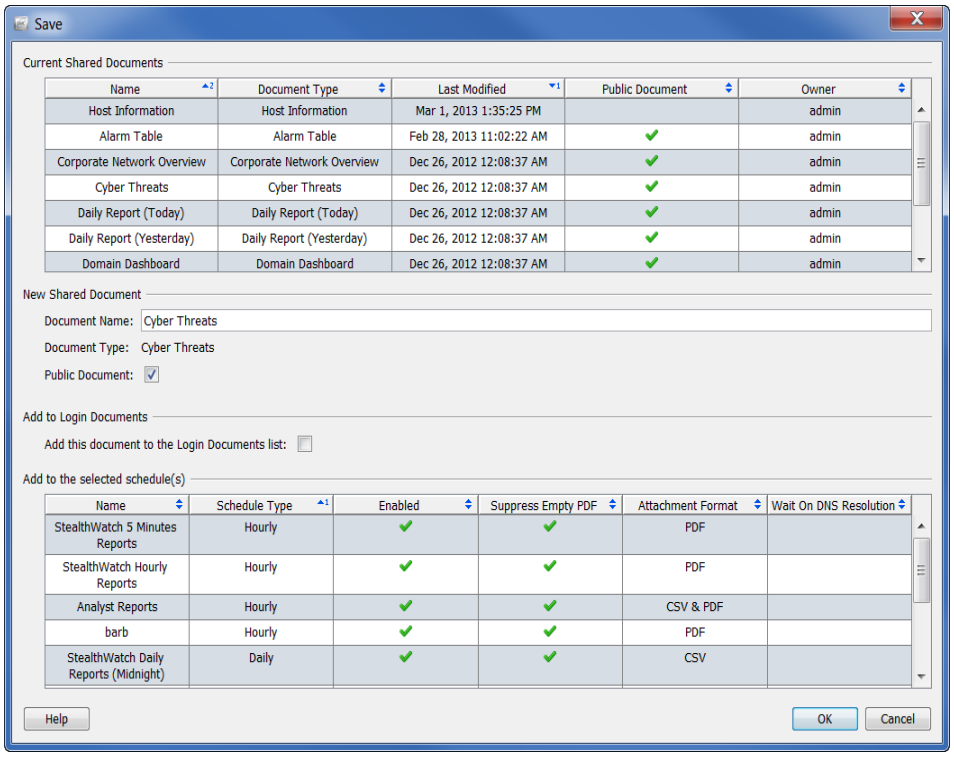
(注):

ドキュメント レイアウトに変更を行い、それを保持したい場合(列位置の変更または表示する列の変更など)、[ファイル(File)] > [設定を規定として使用(Use Settings as Default)] を選択します。この変更は、次にドキュメントを開いたときに有効になります。

5. 次のいずれかを実行します。

   - 同じ名前を使用して以前のバージョンを置き換えるには、SMC のメイン メニューから [ファイル(File)] > [保存(Save)] を選択します。
   - 次のいずれかの状況が該当する場合は、SMC のメイン メニューから [ファイル(File)] > [名前をつけて保存(Save As)] を選択します。
     - 新しい名前でドキュメントのコピーを保存する場合。
     - 新しいドキュメントを作成し、初めてドキュメントを保存する場合。

     [保存(Save)] ダイアログが開きます。



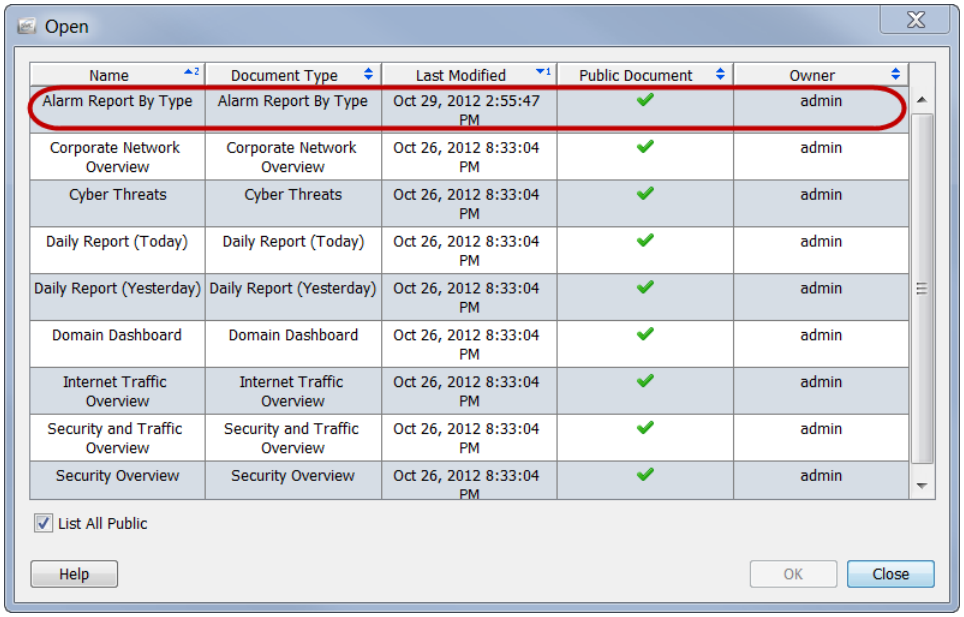
6. [名前(Name)] フィールドに、簡単に識別できるドキュメントの名前を入力します(システムから名前が提案されます)。
7. (オプション)他のユーザーがこのドキュメントを各自のユーザー名で開くことができるようにするには、[パブリック(Public)] チェックボックスをオンにします。

(注):
パブリック ドキュメントの詳細については、「パブリック ドキュメント」(304 ページ)を参照してください。

8. （オプション）自分のユーザー名で Stealthwatch デスクトップクライアントにログインするたびにドキュメントを自動的に開くには、[このドキュメントをログインドキュメントリストに追加する（Add this document to the Login Documents list）] チェックボックスをオンにします。

（注）：
ログイン ドキュメントの詳細については、「ログイン ドキュメント」（299 ページ）を参照してください。

9. [OK] をクリックします。ドキュメントが SMC アプライアンスに保存されます。SMC のアクセスが可能なコンピュータ上で、指定したレイアウトやフィルタの設定を使用して、自分のユーザー名でこのドキュメントを開くことができます。
10. このドキュメントを開くには、SMC メイン メニューから [ファイル（File）] > [開く（Open）] を選択します。[開く（Open）] ダイアログボックスが開きます。



11. ドキュメントを選択し、[OK] をクリックします。

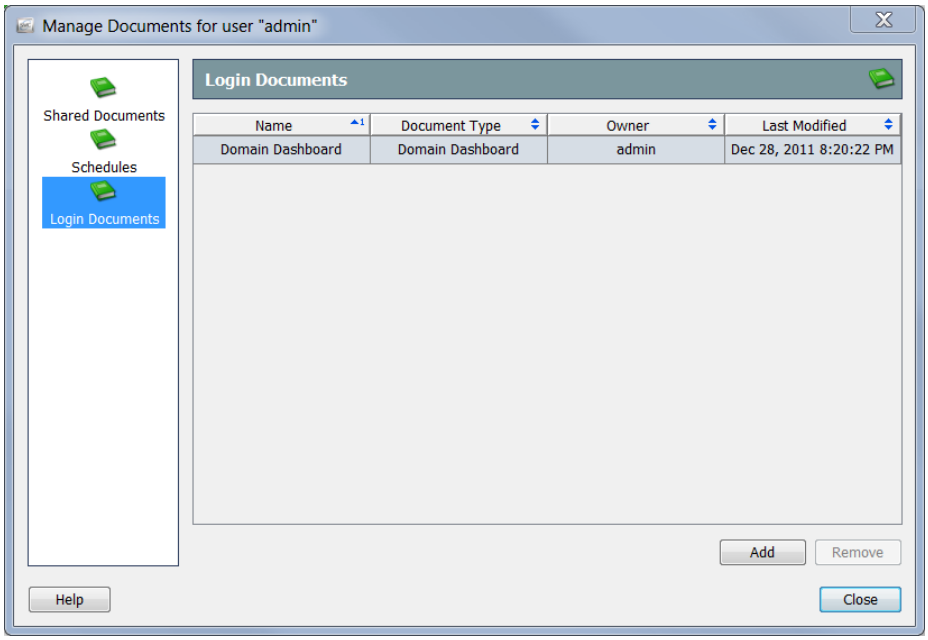
（注）：
デフォルトでは、現在のユーザー名で保存されたドキュメントのみが表示されます。他のユーザーが作成したドキュメントを含めて、すべてのドキュメントを一覧表示するには、[すべてのパブリックを一覧表示する（List All Public）] チェックボックスをオンにします。

ログイン ドキュメント

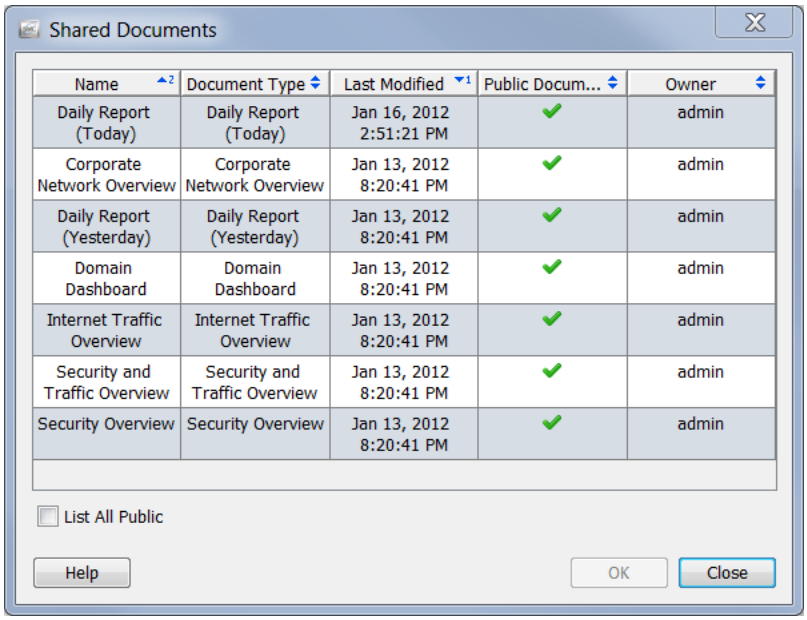
ログイン ドキュメントの一覧にドキュメントを追加できます。ログイン ドキュメントは、Stealthwatch デスクトップ クライアントにログインするたびに自動的に開きます。この機能は、定期的に手動で開くドキュメントを表示するのに便利です。

ドキュメントをログイン ドキュメントにするには、次の手順を実行します。

1. SMC メイン メニューから、[ファイル(File)] > [ドキュメントの管理(Manage Documents)] を選択します。[ドキュメントの管理(Manage Documents)] ダイアログが開きます。
2. [ログインドキュメント(Login Documents)] アイコンをクリックします。[ログイン ドキュメント(Login Documents)] ページが開きます。



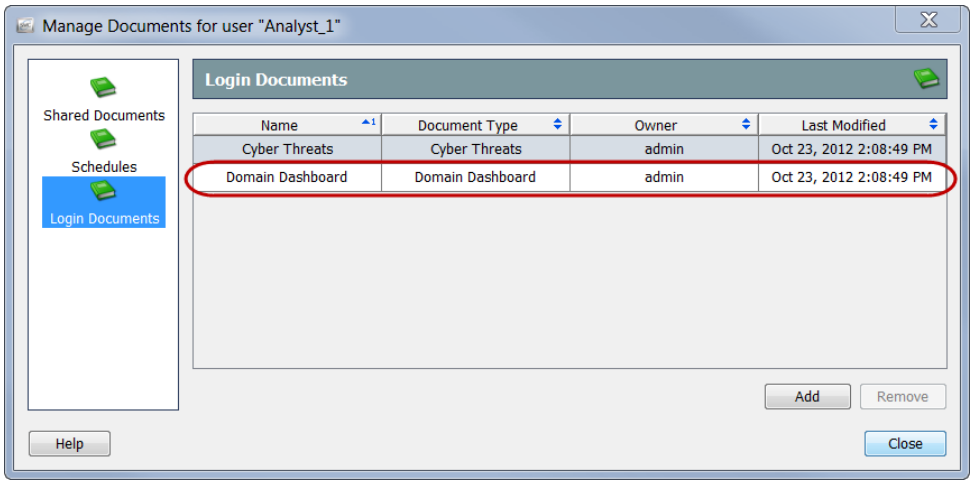
3. [追加(Add)] をクリックします。[共有ドキュメント(Shared Documents)] ダイアログが開きます。



4. [公開ドキュメントをすべてリスト(List All Public)] チェックボックスをオンにして、他のユーザーによって保存されているすべての公開ドキュメントを表示します。
5. ユーザーのログイン ドキュメントのリストに追加するドキュメントを選択します。この例では、[ドメインのダッシュ ボード(Domain Dashboard)] のドキュメントを選択します。

(注):
複数のドキュメントを選択するには、Ctrl キーを押した状態で、追加するドキュメントをそれぞれクリックします。ドキュメントの範囲を選択するには、選択する範囲の一番上にあるドキュメントをクリックし、Shift キーを押した状態で、選択する範囲の一番下にあるドキュメントをクリックします。

6. [OK] をクリック[共有ドキュメント(Shared Documents)] ダイアログが閉じます。選択したドキュメントは、ユーザーのログイン ドキュメントの一覧に表示されます。



7. [閉じる(Close)] をクリックして、[ドキュメントの管理(Manage Documents)] ダイアログを終了します。

ドキュメントの共有

他のユーザーとドキュメントを共有するには、次の 2 つの方法があります。

- DAR ファイルとしてエクスポート
- パブリックに変更

DAR ファイル

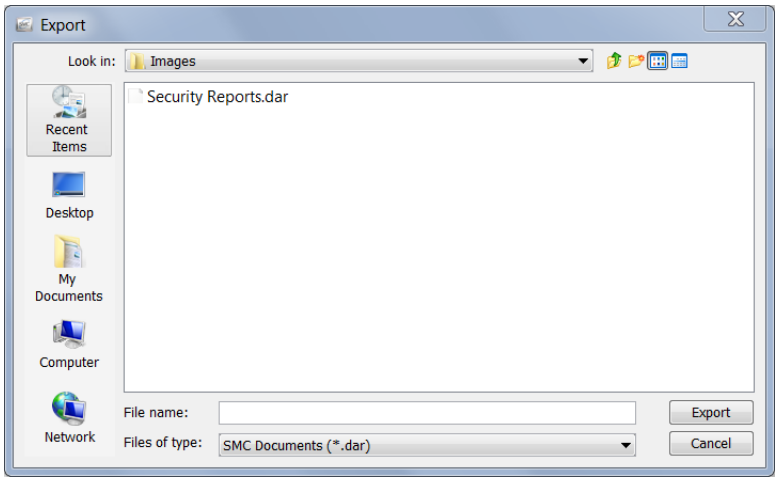
DAR ファイルとしてドキュメントをエクスポートすると、次のようドキュメントで物事を行うことができます。

- お使いのコンピュータのハード ドライブにコピーします。
- SMC アプライアンスにアクセスできる別のコンピュータで使用するために、フラッシュ ドライブにコピーします。
- 誰かと共有します。

DAR ファイルのエクスポート

DAR ファイルとしてドキュメントをエクスポートするには、次の手順を実行します。

1. エクスポートしたいドキュメントを開きます。
2. レイアウトまたはフィルターの設定に必要な変更を加えます。
3. SMC メイン メニューから、[ファイル(File)] > [DAR ファイルへのエクスポート(Export to DAR file)] を選択します。[エクスポート(Export)] ダイアログが開きます。



4. ドキュメントをエクスポートしたい場所に移動します。
5. [ファイル名(File Name)] フィールドに、ファイルの名前を入力します。

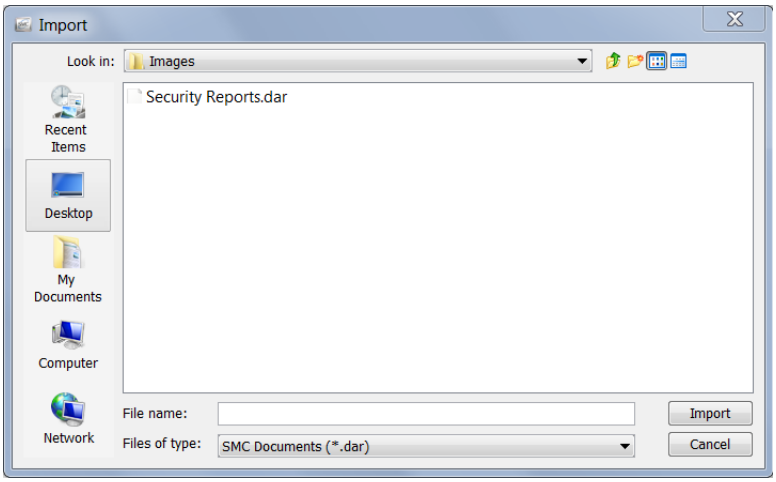
6. [エクスポート(Export)]をクリックします。ドキュメントは、選択した場所にDARファイルとして保存されます。また、[ドキュメント(Document)]タブには新しい名前が付きます。

(注):
[ドキュメント(Document)]タブの上にカーソルを置くと、元のドキュメント名や作成者などのドキュメントについての詳細を示すツール ヒントが表示されます。

DARファイルのインポート

誰かがDARファイルとしてドキュメントをエクスポートし、提供した場合、そのファイルをインポートすれば、Stealthwatchデスクトップクライアントで開くことができます。これを行うには、次の手順を実行します。

1. SMC メイン メニューから、[ファイル(File)] > [DARファイルをインポート(Import DAR file)]を選択します。[インポート(Inport)]ダイアログが開きます。



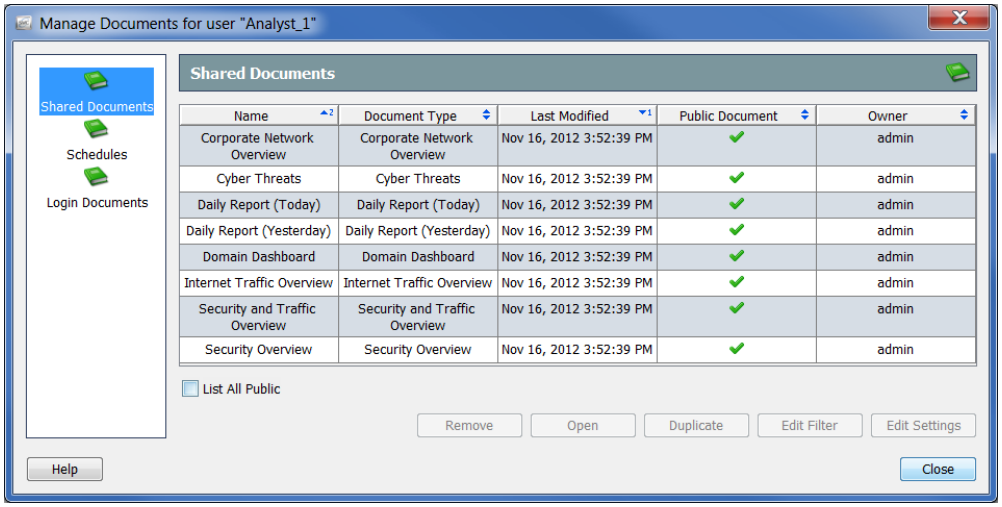
2. DARファイルのある場所に移動します。
3. DARファイルを選択します。
4. [インポート(Import)]をクリックします。Stealthwatchデスクトップクライアントでドキュメントが開きます。

パブリック ドキュメント

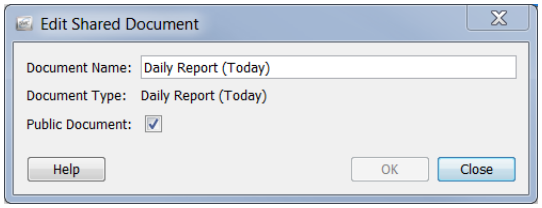
ドキュメントをパブリックにすると、SMC アプライアンスにアクセスできるその他のユーザーが自身のユーザー名でそのドキュメントを表示できます。

「ドキュメントの保存」(296 ページ)で説明したように、保存する際にドキュメントをパブリックにすることができます。次の手順を完了することによって、以前に保存したドキュメントをパブリックにすることができます。

1. メイン メニューから、[ファイル(File)] > [ドキュメントの管理(Manage Documents)] を選択します。[ドキュメントの管理(Manage Documents)] ダイアログが開きます。



2. [共有ドキュメント(Shared Documents)] アイコンをクリックします。[共有ドキュメント(Shared Document)] ページが開きます。
3. 必要なドキュメントを選択します。
4. [設定の編集(Edit Settings)] をクリックします。[設定を編集(Edit Settings)] ダイアログが開きます。



5. [パブリックドキュメント(Public Document)] チェックボックスを選択します。
6. [OK] をクリックして、[編集(Edit)] ダイアログを終了します。
7. [閉じる(Close)] をクリックして、[ドキュメントの管理(Manage Documents)] ダイアログを終了します。

Stealthwatch デスクトップクライアントにアクセスできるユーザーは、このドキュメントとパブリックになったその他すべてのドキュメントを表示することができます。

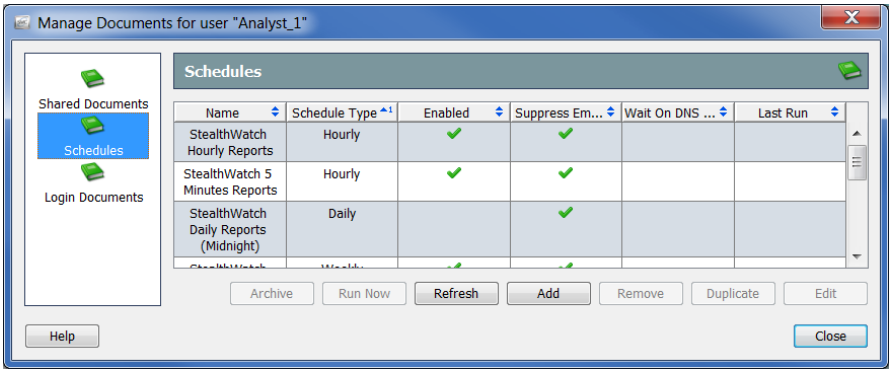
ドキュメントのスケジューリング

毎回同じ設定(フィルタ、レイアウト、時間間隔など)を使用して自動的にドキュメントを生成できると便利な場合があります。これを行うには、必要な設定が含まれているスケジュールにドキュメントを追加する必要があります。

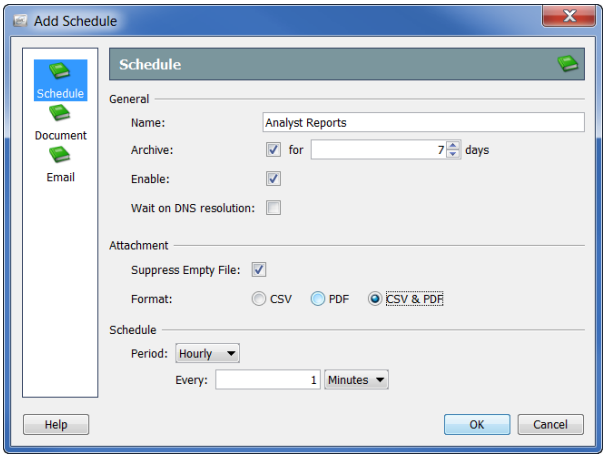
新しいスケジュールの追加

新しいスケジュールを追加するには、次の手順を実行します。

1. SMC メイン メニューから、[ファイル(File)] > [ドキュメントの管理(Manage Documents)] を選択します。[ドキュメントの管理(Manage Documents)] ダイアログが開きます。



2. [スケジュール(Schedules)] アイコンをクリックします。[スケジュール(Schedules)] ページが開きます。
3. [追加(Add)] をクリックします。[スケジュールの追加(Add Schedule)] ダイアログが開きます。



4. [スケジュール(Schedule)] アイコンをクリックします。[スケジュール(Schedule)] ページが開きます。

5. [名前(Name)] フィールドにスケジュールの名前を入力します。この例では、スケジュールに「アナリスト レポート」と名前を付けます。
6. 次の表に示すように、[全般(General)] セクションでパラメータを定義します。

必要な設定	選択するもの
SMC データベースにこのスケジュールによって生成されたドキュメントを保存する	[アーカイブ(Archive)] チェックボックス。次に、対応するドロップダウン リストをクリックし、ドキュメントを保存する日数を選択します。
作成とともにこのスケジュールをアクティブにする	[有効(Enable)] チェックボックス。
ドキュメント内で参照される IP アドレスの名前が解決されるまでスケジュールされたドキュメントの生成をシステムで待機する場合	[DNS 解決を待機(Wait on DNS resolution)] チェックボックス。 **注**: この機能を有効にすると、ドキュメントの生成が遅延する可能性があります。各 IP アドレスは、解決までに最大 2 秒かかることがあります。2 秒以内に IP アドレスが解決しない場合、DNS 名なしで IP アドレスが表示されます。
SMC が生成されたデータのないドキュメントをアーカイブまたは電子メールで送信できないようにする	[空のファイルを制御する(Suppress Empty File)] チェックボックス。
- 続く -	

必要な設定	選択するもの
印刷したいデータの種類を指定する	▶ CSV(コンマ区切り値)- 生成されたドキュメントに含まれているテーブルのデータのみを印刷する場合は、このオプションを選択します。 • 各テーブルは CSV ファイルで格納されます。 • その他すべての種類のデータ (地図、グラフ、図表など) は印刷されません。 • ドキュメントごとにすべての CSV ファイルが 1 つのファイル(ドキュメントあたり 1 つの圧縮ファイル)に圧縮されます。 • 選択したスケジュールで生成されたドキュメントのコピーを電子メール受信するように指定された各ユーザーに、すべての圧縮ファイルが電子メールで送信されます。
	▶ PDF:生成されたドキュメントに含まれるデータをすべて印刷する場合は、このオプションを選択します。 • 生成された各ドキュメントは PDF ファイルで格納されます。 • PDF ファイルはそれぞれ 1 つのファイルに圧縮されます。 • 選択したスケジュールで生成されたドキュメントを電子メールで受信するように指定された各ユーザーに、すべての圧縮ファイルが電子メールで送信されます。
印刷したいデータの種類を指定する	▶ CSV & PDF:テーブルのデータを CSV 形式で、その他のすべてのデータを PDF 形式で印刷する場合は、このオプションを選択します。 • 各テーブルは CSV ファイルで格納されます。 • 生成された各ドキュメント内のその他のすべての種類のデータは、PDF ファイル(ドキュメントあたり 1 つの PDF ファイル)で格納されます。 • ドキュメントに属するすべてのファイルが、1 つのファイル(ドキュメントあたり 1 つの圧縮ファイル)に圧縮されます。 • 選択したスケジュールで生成されたドキュメントのコピーを電子メール受信するように指定された各ユーザーに、すべての圧縮ファイルが電子メールで送信されます。

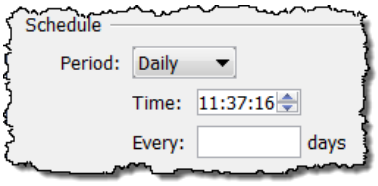
(注):

- [印刷設定(Print Settings)] ダイアログの [ページ(Pages)] ページのテーブルを有効にしていない場合、CSV ファイルを作成するようにスケジュールが設定されていてもこのテーブルの CSV ファイルが作成されません。

- [印刷設定(Print Settings)] ダイアログの [プリンタの設定(Print Setup)] ページで指定すると、生成されるドキュメントにフィルタ サマリーが含まれます。([カバー シート オプション(Cover Sheet Options)] セクションで)[フィルタ サマリー(Filter summary)] チェックボックスを選択できるように、([カバー シート (Cover Sheet)] セクションで)[最初のページ(As the first page)] オプションまたは [最後のページ(As the last page)] オプションのいずれかを選択する必要があることに注意してください。

7. [期間(Period)] ドロップダウン リストをクリックし、このスケジュールに関連付けられているドキュメントを SMC で生成する頻度を選択します。時間単位、日単位、週単位、または月単位でスケジュールされたドキュメントを生成することができます。選択したオプションに応じて、異なるフィールドが表示されて詳細を指定できます。

   たとえば、[毎日(Daily)] を選択すると、2 つのフィールドが表示されるので、スケジュールを実行する時刻を指定できます。毎日、1 日おき、3 日おきなどの実行間隔も指定できます。

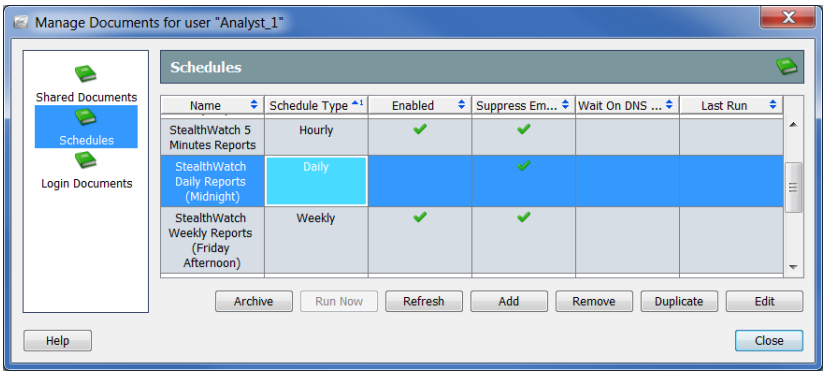


8. 「スケジュールへのドキュメントの追加」(311 ページ) に進みます。

既存スケジュールの編集

自身のアカウントに関連付けたいスケジュールがすでに存在する場合は、それに応じて、次の手順を実行して、スケジュールを編集します。

1. SMC メイン メニューから、[ファイル(File)] > [ドキュメントの管理(Manage Documents)] を選択します。[ドキュメントの管理(Manage Documents)] ダイアログが開きます。

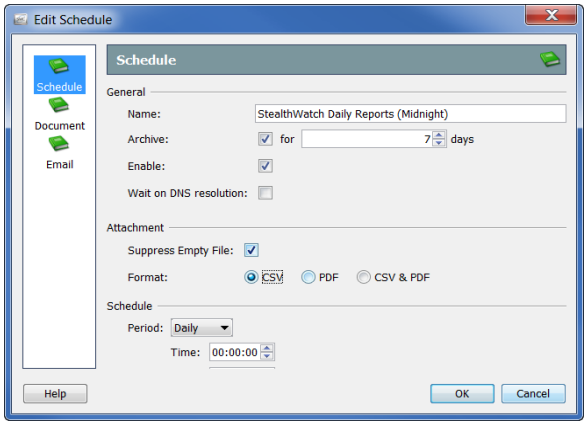


2. [スケジュール(Schedules)] アイコンをクリックします。[スケジュール(Schedules)] ページが開きます。
3. 編集するスケジュールを選択します。

(注):

上記の例では、[Stealthwatch 日次レポート(深夜)(tealthwatch Daily Reports (Midnight)] のスケジュールが選択されています。このスケジュールが自身のアカウントに対して有効になっていないことを示す、[有効(Enabled)] 列にチェック マークがないことに注意してください。スケジュールが有効でない場合、このスケジュールのドキュメントは何も生成されません。

4. [編集(Edit)] をクリックします。[スケジュールの編集(Edit Schedule)] ダイアログが開きます。

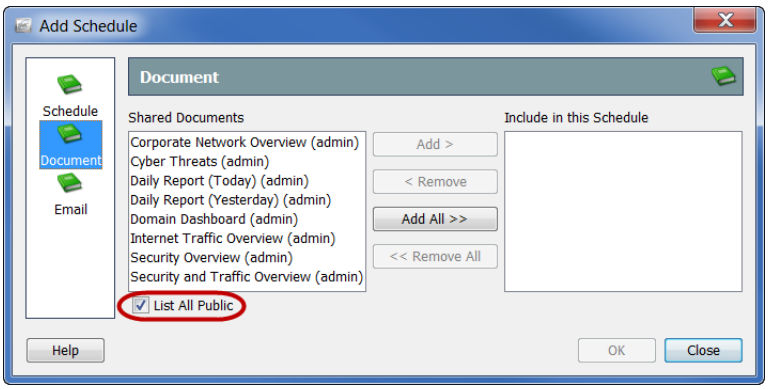


5. [スケジュール(Schedule)] アイコンをクリックします。[スケジュール(Schedule)] ページが開きます。
6. 必要に応じて設定を変更します。オプションの詳細については、[ヘルプ(Help)] をクリックしてください。
7. この章の「スケジュールへのドキュメントの追加」に続きます。

スケジュールへのドキュメントの追加

1 つ以上のドキュメントをスケジュールに追加するには、次の手順を実行します。

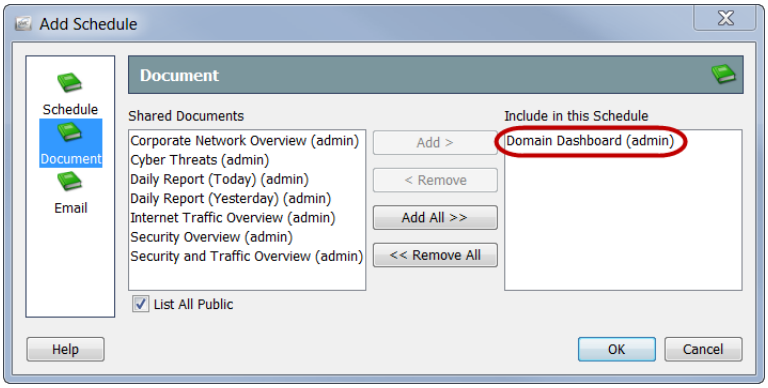
1. [スケジュールを追加(または編集)(Add (or Edit) Schedule] ダイアログで、[ドキュメント(Document)] アイコンをクリックします。[ドキュメント(Document)] ページが開きます。



2. 選択していない場合、[パブリックをすべて一覧表示(List All Public)] チェックボックスを選択します。(詳細については、「パブリック ドキュメント」(304 ページ)を参照してください)。
3. スケジュールに追加するドキュメントを選択します。この例では、[ドメインのダッシュ ボード(Domain Dashboard)] のドキュメントを選択します。

(注):
複数のドキュメントを選択するには、Ctrl キーを押した状態で、追加するドキュメントをそれぞれクリックします。ドキュメントの範囲を選択するには、選択する範囲の一番上にあるドキュメントをクリックし、Shift キーを押した状態で、選択する範囲の一番下にあるドキュメントをクリックします。

4. [追加(Add)] をクリックします。ドキュメントが [スケジュール含める(Include in this Schedule)] フィールドに表示されます。



5. SMC にスケジューリングされたドキュメントを自身に電子メールでさせたいですか。
   - 「はい」の場合は、「スケジュールにユーザーの電子メール アドレスを追加」(314 ページ)に進みます。
   - 「いいえ」の場合、[OK] をクリックして、情報を保存し、[追加(Add)(または編集(Edit))] ダイアログを終了して、[文書の管理(Manage Documents)] ダイアログに戻ります。
6. 残りのダイアログを閉じます。

スケジューリングされたドキュメントを電子メールで送信

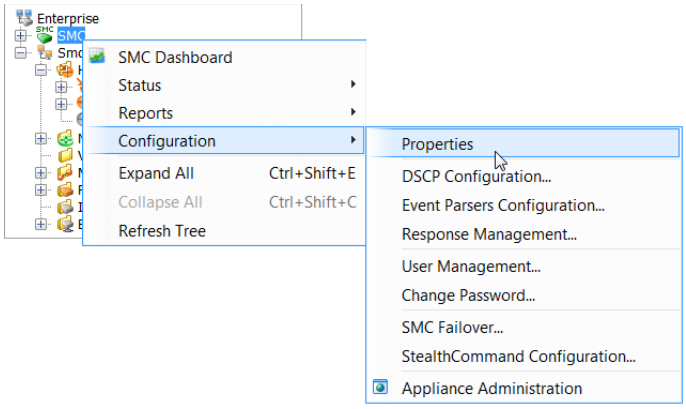
SMC にスケジューリングされたドキュメントを自身に自動的に電子メールで送信させたい場合は、次の 2 つの手順を行なう必要があります。

1. SMC に電子メール サーバーの IP アドレスを追加します。(次項「SMC に電子メール サーバーを追加」を参照してください)。
2. スケジュールにユーザーの電子メール アドレスを追加します。(「スケジュールにユーザーの電子メール アドレスを追加」(314 ページ)を参照)。

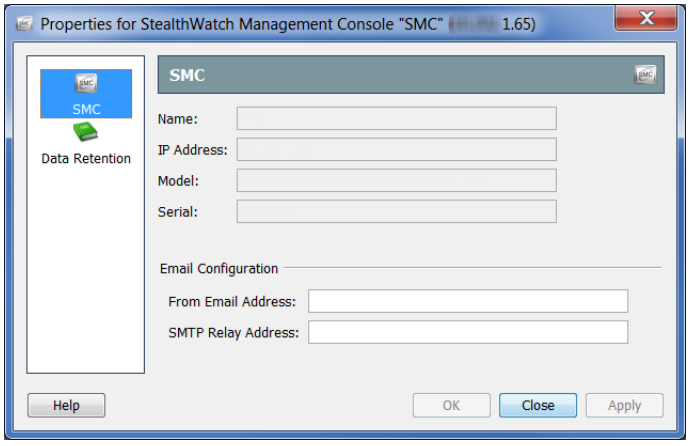
SMC に電子メール サーバーを追加

以前そうしていない場合、SMC がスケジューリングされたドキュメントを送れるようにするには、SMC に電子メール サーバーの IP アドレスを追加する必要があります。これを行うには、次の手順を実行します。

1. [エンタープライズ(Enterprise)] ツリーの [SMC] ブランチで右クリックして、ポップアップ メニューから、[構成(Configuration)] > [プロパティ(Properties)] を選択します。[プロパティ(Properties)] ダイアログが開きます。



2. [SMC] アイコンをクリックします。[SMC] ページが開きます。



3. (省略可能)[差出人の電子メール アドレス(From Email Address)] フィールドに、次の形式を使用してアドレスを入力します。

   [FromUser]@[hostname].[domain]

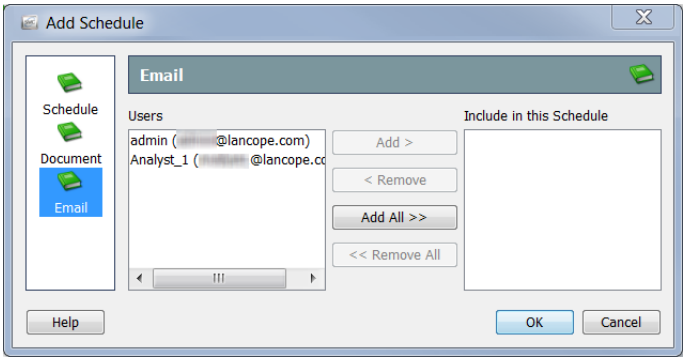
4. [SMTP リレー アドレス(SMTP Relay Address)] フィールドに電子メール サーバーの IP アドレスを入力します。

5. [OK] をクリックして情報を保存し、[プロパティ(Properties)] ページを閉じます。

スケジュールにユーザーの電子メール アドレスを追加

SMC にスケジューリングされたドキュメントを自身に自動的に電子メールで送信させたい場合は、次の 2 つの手順を行って、自身の電子メール アドレスを追加する必要があります。

1. [スケジュールの追加(Add Schedule)] または [スケジュールの編集(Edit Schedule)] ダイアログで、[電子メール(Email)] アイコンをクリックします。[電子メール(Email)] ページが開きます。



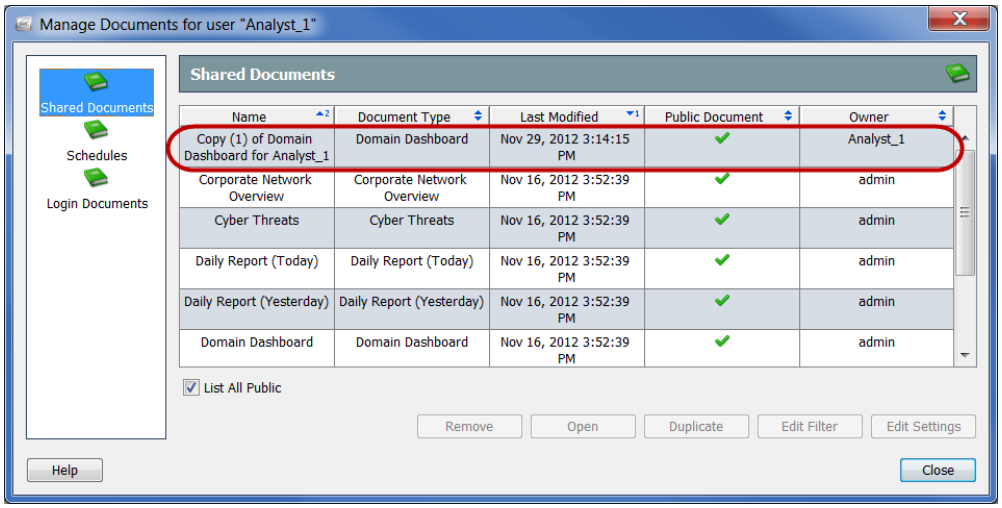
2. [ユーザー(Users)] フィールドで、自身のメール アドレスを選択します。
3. [追加(Add)] をクリックします。[このスケジュール(This Schedule)] フィールドに自身のメール アドレスが表示されます。
4. [OK] をクリックして情報を保存し、[スケジュールの追加(Add Schedule)] または [スケジュールの編集(Edit Schedule)] ダイアログを閉じて [ドキュメントの管理(Manage Messages)] ダイアログに戻ります。
5. 残りのダイアログを閉じます。

共有ドキュメントの事前フィルター処理

スケジュールごと生成される際に、任意の共有ドキュメントのフィルター設定を自動的に使用するよう、そのフィルター設定を編集できます。

これらの編集内容は、次の方法のいずれかで保存されます。

- ドキュメントの所有者でない場合、元のドキュメントは変更されないままで、新しいフィルター設定で重複ドキュメントが作成されます。重複ドキュメントにのみ新しいフィルター設定が含まれます。

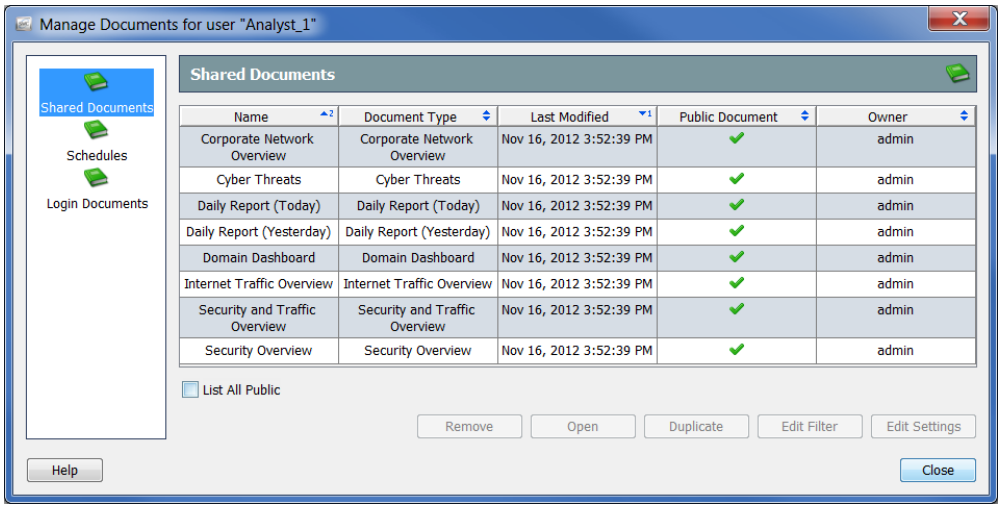


- ドキュメントの所有者の場合、新しいフィルター設定は、元が反映されます。この時点からこのドキュメントがこのドキュメントにアクセスする権限のある人間によって生成または開かれるたびに、新しいフィルター設定が有効になります。

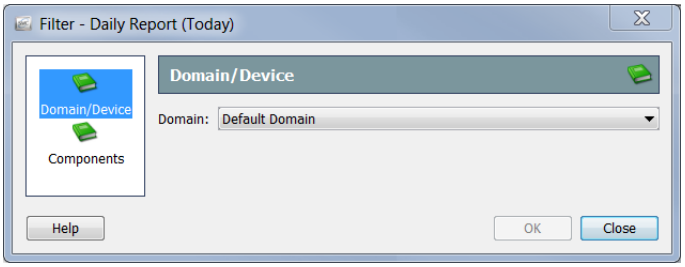
スケジュールごと生成される際に、共有ドキュメントのフィルター設定を自動的に使用するよう、そのフィルター設定を編集できます。これを行うには、次の手順を実行します。

(注):
ドキュメントのフィルター処理の詳細については、「ドキュメント データのフィルタリング」(第 2 章「Stealthwatch デスクトップクライアントの操作」内)を参照してください。

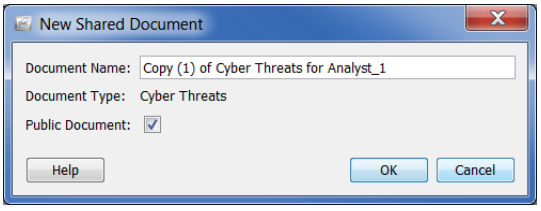
1. メイン メニューから、[ファイル(File)] > [ドキュメントの管理(Manage Documents)] を選択します。[ドキュメントの管理(Manage Documents)] ダイアログが開きます。



2. [共有ドキュメント(Shared Documents)] アイコンをクリックします。[共有ドキュメント(Shared Documents)] ページが開きます。
3. 必要なドキュメントを選択します。
4. [Edit Filter] をクリックします。[フィルター(Filter)] ダイアログが開きます。



5. フィルターの設定に必要な変更を加えます。他の人間が所有するドキュメントのフィルター設定を編集する場合、次の例に示すように、[新しい共有ドキュメント(New Shared Document)] ダイアログが開きます。



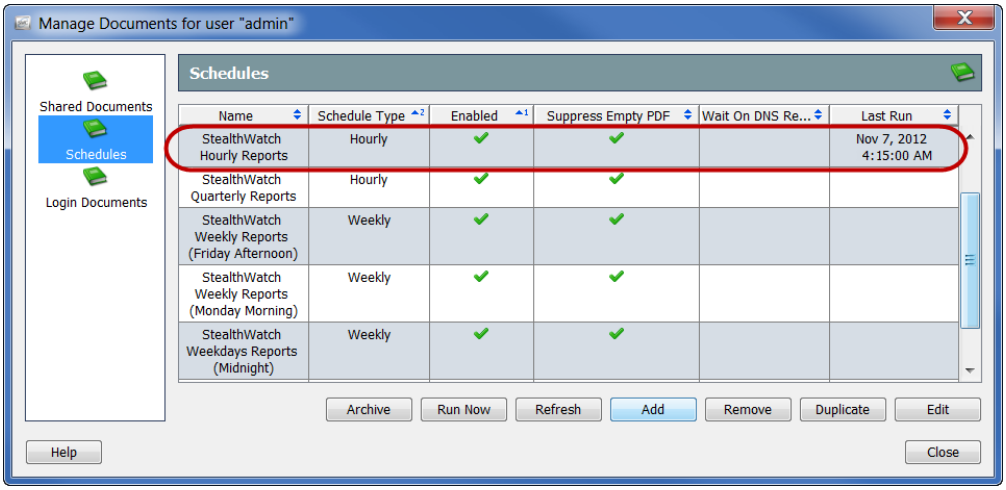
6. 次のいずれかを実行します。
   - [OK] をクリックして、[ドキュメント名 (Document Name)] フィールド内のデフォルトの名前を受け入れ、[新しい共有ドキュメント (New Shared Document)] ダイアログを終了します。
   - [ドキュメント名 (Document Name)] フィールド内の名前を変更し、[OK] をクリックして、[新しい共有ドキュメント (New Shared Document)] ダイアログを閉じます。
7. [OK] をクリックして、[管理されたドキュメント (Managed Documents)] ダイアログを閉じます。

アーカイブされたドキュメントを取得

SMC にスケジューリングされたドキュメントを自身に自動的に電子メールで送信させたくない場合、または SMC からの電子メールを収集できない場合、自身の都合でスケジューリングされたドキュメントを収集するよう選択できます。

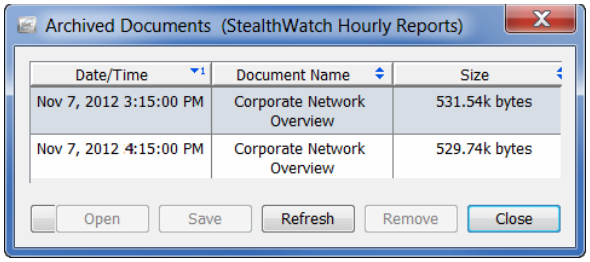
生成されたドキュメントを収集するには、次の手順に従います。

1. SMC メイン メニューから、[ファイル (File)] > [ドキュメントの管理 (Manage Documents)] を選択します。[ドキュメントの管理 (Manage Documents)] ダイアログが開きます。

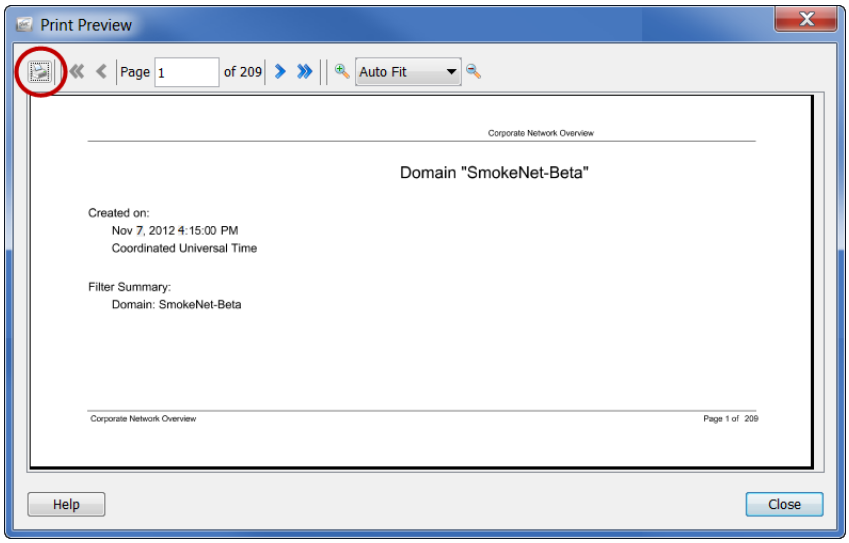


2. [スケジュール (Schedules)] アイコンをクリックします。[スケジュール (Schedules)] ページが開きます。
3. 表示したい生成されたドキュメントを含むスケジュールをクリックします。[最後の実行 (Last Run)] 列には、スケジュールが最後に実行された日時が含まれていることに注意してください。

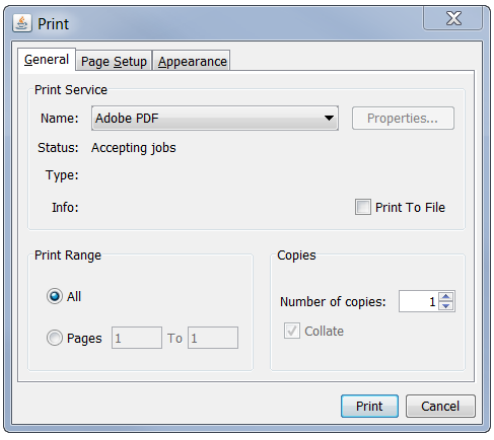
4. [アーカイブ(Archive)] をクリックします。右に示すように、[アーカイブされたドキュメント(Archived Documents)] ダイアログが開きます。



5. 表示したいドキュメントをクリックします。
6. [開く(Open)] をクリックします。[印刷プレビュー(Print Preview)] ダイアログが開きます。



7. [印刷(Print)] アイコンをクリックします(前の画像の円内)。[印刷(Print)] ダイアログが開きます。



ドキュメントのハード コピーを印刷するか、またはローカルのハード ドライブにダウンロードできます。

13

デスクトップクライアントのロール

概要

Stealthwatch 管理コンソール(SMC)では、さまざまなレベルの権限を持つユーザーを非常に柔軟に設定できます。たとえば、あるユーザーに対してネットワーク エリアすべての表示および変更を許可できます。あるいは、ネットワークの特定エリアを表示できるほかは何もできないように特定のユーザーを制限することもできます。

デスクトップクライアントのロール(正式にはユーザー機能ロールと呼ばれる)は、ユーザーが Stealthwatch デスクトップクライアントで表示および設定できる機能(フロー検索、ポリシー管理、レポートなど)を制御します。

(注):

ユーザー、データのロール、および認証サービスを管理するには、Stealthwatch Web アプリケーションの使用が必要になりました。詳細については、Stealthwatch Web アプリケーションのオンラインヘルプを参照してください。

唯一の例外として、デスクトップクライアントのロール(正式にはユーザー機能ロールと呼ばれる)は Stealthwatch デスクトップクライアントで作成および編集できます。ただし、デスクトップクライアントのロールをユーザーに割り当てるには、Stealthwatch Web アプリケーションを使用する必要があります。

この章は、次の項で構成されています。

デスクトップクライアントのロール

Stealthwatch デスクトップクライアントでデスクトップクライアントロール（正式にはユーザー機能ロールと呼ばれる）を作成および編集すると、これらの変更が Stealthwatch Web アプリケーション（[ユーザー管理（User Management）] の [ユーザー（User）] ページにある [デスクトップ（Desktop）] タブ）にも表示されます。

Stealthwatch デスクトップクライアントの [デスクトップクライアントのロール（Desktop Client Roles）] ダイアログにアクセスするには、次のいずれかを実行します。

- 企業ツリーで、コンテキストメニューから [Configuration（設定）] > [デスクトップクライアントのロール（Desktop Client Roles）] を選択します。
- メインメニューから、[設定（Configuration）] > [デスクトップクライアントのロール（Desktop Client Roles）] を選択します。

デスクトップクライアントのロールを変更した場合は、該当するロールが割り当てられているユーザーがログインするまで、その変更は適用されません。したがって、変更が行われた時点でログインしているすべてのユーザーは、ログアウトしてから再度ログインする必要があります。

Stealthwatch には、デフォルトセットとして次のデスクトップクライアントロールが設定されています。

選択オプション	ユーザーによる表示を許可
デスクトップ クライアント マネージャ（Desktop Client Manager）	すべてのメニュー項目と Stealthwatch デスクトップクライアント内のすべての変更。
設定マネージャ（Configuration Manager）	すべてのメニュー項目と、すべてのアプライアンス、デバイス、およびドメインの設定の構成。
ネットワークエンジニア（Network Engineer）	Stealthwatch デスクトップクライアント内のすべてのトラフィック関連のメニュー項目、アラームとホストノートの追加、緩和を除くすべてのアラームアクションの実行。
セキュリティ アナリスト（Security Analyst）	すべてのセキュリティ関連のメニュー項目、アラームとホストノートの追加、緩和を含むすべてのアラームアクションの実行。
Stealthwatch パワーユーザー（Stealthwatch Power User）	すべてのメニュー項目、確認アラーム、アラームとホストノートの追加。ただし、変更機能はなし。

デスクトップクライアントのロールの追加と編集

デスクトップクライアントのロールを追加、編集、削除するには、[デスクトップクライアントロールの追加（Add Desktop Client Role）] ダイアログを使用します。デスクトップクライアントのロールは、ユーザーが Stealthwatch デスクトップクライアントで表示および設定できる機能（フロー検索、ポリシー管理、レポートなど）を制御します。

[デスクトップクライアントのロールの追加（Add Desktop Client Role）] ダイアログにアクセスするには、次の手順を実行します。

- [デスクトップクライアントのロール（Desktop Client Roles）] ダイアログで、[追加（Add）] を選択するか、またはテーブル内のエントリを強調表示し、[編集（Edit）] を選択します。

親関数を選択すると、その子が自動的に選択されます。親関数の子を選択する場合は、最初に親関数の選択を解除する必要があります。

デスクトップクライアントのロールを複製した後、デフォルトでは、名前（複製するデスクトップクライアントのロール名の [x] のコピー）が重複したデスクトップクライアントのロールに割り当てられます。テーブル内の複製されたロールをダブルクリックし、[編集（Edit）] をクリックして名前を変更します。

INDEX

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

ね

は

ひ

ふ

へ

ほ

み

め

ゆ

ら

り

れ

ろ

わ