Secure Network Analyticsにおけるフロー速度使用率の95パーセンタイルを計算する

内容

はじめに

このドキュメントでは、StealthwatchまたはSecure Network Analytics for FlowRate Licensingにおけるフロー速度使用率の95パーセンタイル値を計算する方法について説明します

前提条件

要件

次の項目に関する知識があることが推奨されます。

- スマート ソフトウェア ライセンシング
- メインダッシュボード内のSecure Network Analyticsナビゲーション

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- StealthWatch管理コンソールバージョン7.4.1

次のコマンドも必要です。

- Secure Network Analyticsのスマートライセンス画面への管理アクセス
- StealthWatch Management ConsoleへのCLIアクセス（ルート）
- VSQLデータベースパスワード
- Secure Network Analytics環境がスマートライセンスに登録されている

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

公式の7.4.2スマートライセンスガイド（22ページ）には、Secure Network Analyticsが、過去24時間の期間に基づいて、1日のフロー率（1秒あたりのフロー数）の使用状況の95パーセンタイルをスマートアカウントに報告することが記載されています。

Secure Network Analytics（以降SNAと呼ぶ）は、以前はStealthwatchと呼ばれていましたが、これらの用語は同じ意味で使用できます。

確認

このセクションでは、設定が正常に動作していることを確認します。

Stealthwatch Management Consoleデータベースで95パーセンタイル値を確認する

⚠ 注意：このドキュメントでは、2023年4月18日の単一の例の日について、流量の使用量を計算するプロセスについて説明します。SQLクエリを調整して、ユースケースの使用日に合わせます

Smart License Usageの下のFlow Rate Licenseに表示される値は、Stealthwatch Management Consoleデータベースのflow_collection_summaryテーブルから取得されます。この表を参照するには、SSH経由でStealthWatch Management Consoleにrootとしてログインし、次のコマンドを実行します。

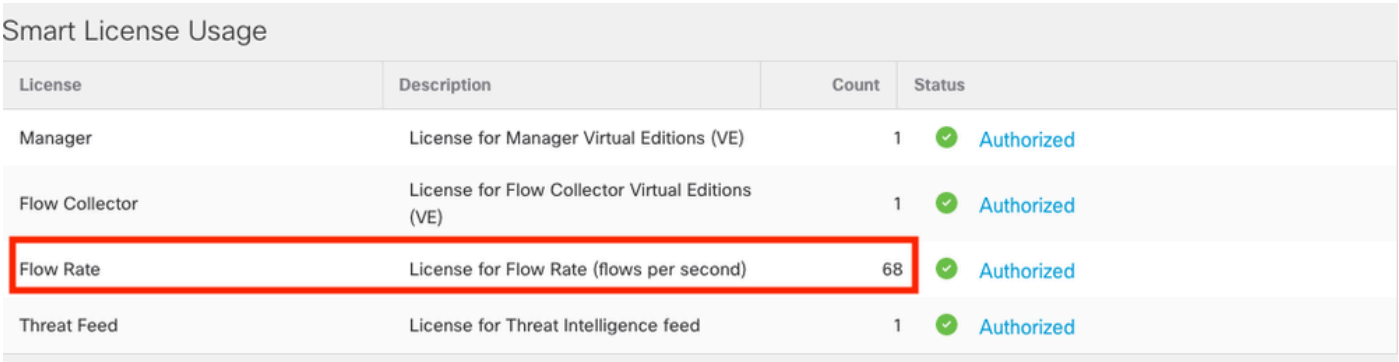
```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select last_time, fps_95 from flow_collection_summary
```

✎ 注：このドキュメントで紹介するコマンドでは、StealthWatch Management Consoleデータベースのデフォルトパスワードを使用します。ご使用の環境でデータベースパスワードが変更されている場合は、正しいパスワードになるようにコマンドを調整します

出力には、最近の5日間のレコードと95パーセンタイルのレコードが最新の順に表示されます。例については、次の図を参照してください。

```
        last_time          | fps_95
---------------------------+--------
 2023-04-18 00:00:00+00    |     68
 2023-04-17 00:00:00+00    |     66
 2023-04-16 00:00:00+00    |     58
 2023-04-15 00:00:00+00    |     66
 2023-04-14 00:00:00+00    |     82
(5 rows)
```

「背景説明」に示されているように、スマートライセンスの画面に表示される毎日のフロー速度の使用状況は、直前の24時間の期間に基づいて計算されます。flow_collection_summary表では、まだ終了していない日の値が表示されるため、日付の不一致が示されます。これは、リセット時間の各日の終わりに00:00:00に使用量が計算されるためです。スマートライセンス画面では、fps_95の値は現在の日の値(2023-04-18)と一致します。次の図を参照してください。


Smart License Usage

License	Description	Count	Status
Manager	License for Manager Virtual Editions (VE)	1	Authorized
Flow Collector	License for Flow Collector Virtual Editions (VE)	1	Authorized
Flow Rate	License for Flow Rate (flows per second)	68	Authorized
Threat Feed	License for Threat Intelligence feed	1	Authorized

flow_collection_summary表の4月18日のfps_95値は、前日の4月17日のフロー・レート使用量に対応します。4月17日のfps_95値は、4月16日の流量に対応します。

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します

1日の使用について95パーセンタイルを計算する

flow_collection_summaryテーブルに表示されるfps_95値は、flow_collection_trendテーブルの情報に基づいて計算されます。このテーブルは、Stealthwatch Management Consoleデータベースでも入手できます。このテーブルは、環境内のすべてのフローコレクタによって報告された各エクスポータの分単位の流量の使用状況を追跡します。1日に1,440分のレコードが1,440個あります。表のタプルminute-fpsは、次の図のようになります。

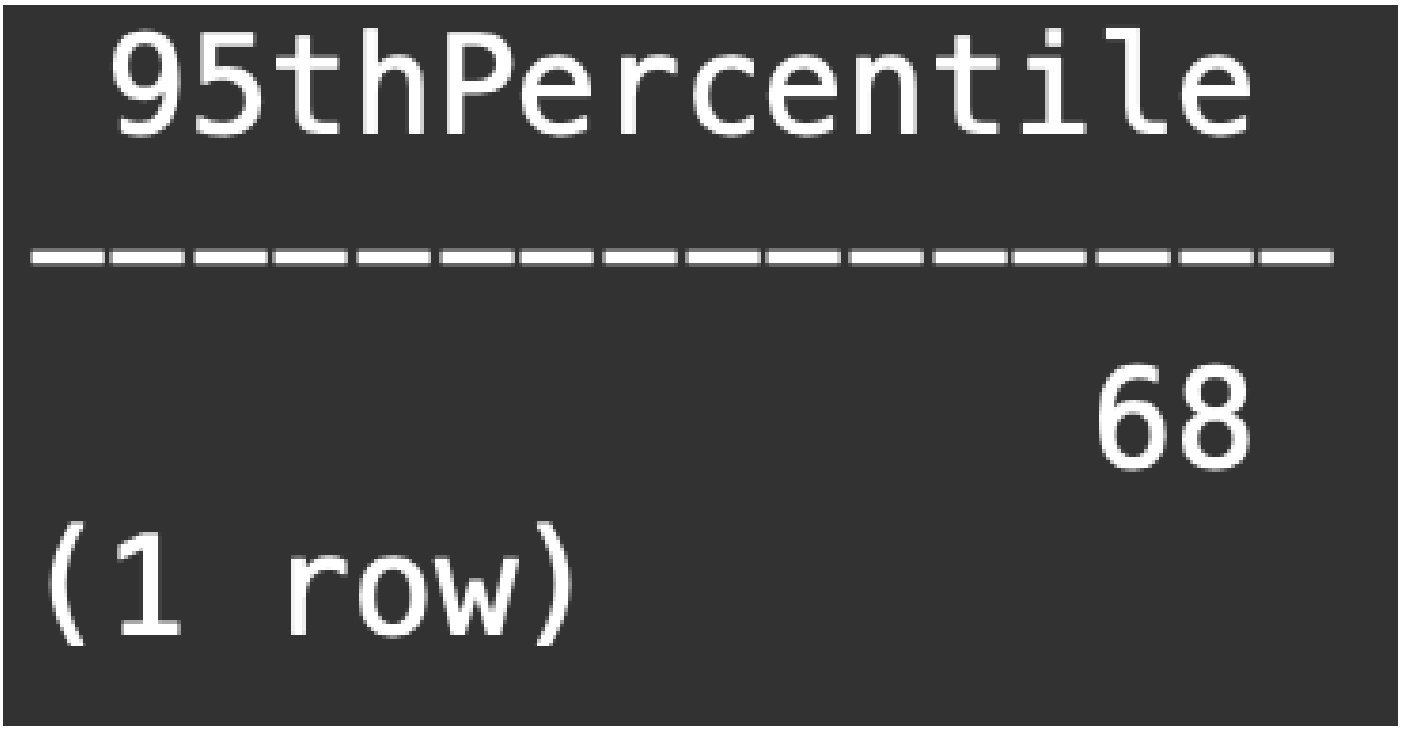
last_time	fps
2023-04-17 07:36:00+00	94
2023-04-17 00:48:00+00	88
2023-04-17 14:24:00+00	86
2023-04-17 23:28:00+00	85
2023-04-17 15:33:00+00	85
2023-04-17 00:01:00+00	85
2023-04-17 20:11:00+00	79
2023-04-17 00:50:00+00	79
2023-04-17 11:00:00+00	78
2023-04-17 20:13:00+00	77
2023-04-17 20:05:00+00	77
2023-04-17 20:15:00+00	76
2023-04-17 23:22:00+00	75
2023-04-17 16:36:00+00	75
2023-04-17 00:51:00+00	75
2023-04-17 15:32:00+00	74

flow_collection_summaryのfps_95カラムの値は、1日の1440 minute-fpsレコードから計算されます。95番目のパーセンタイルのみが報告されるため、これはfps列で最大から最小の順に並べられたレコードの最初の5%（最初の72行）がプロセスで破棄されることを意味します。したがって、73行目は流量使用率の95番目の値を表します。10進数計算により、≈1 ~ 2 fpsの73番目のfps値に予想されるずれがあります。

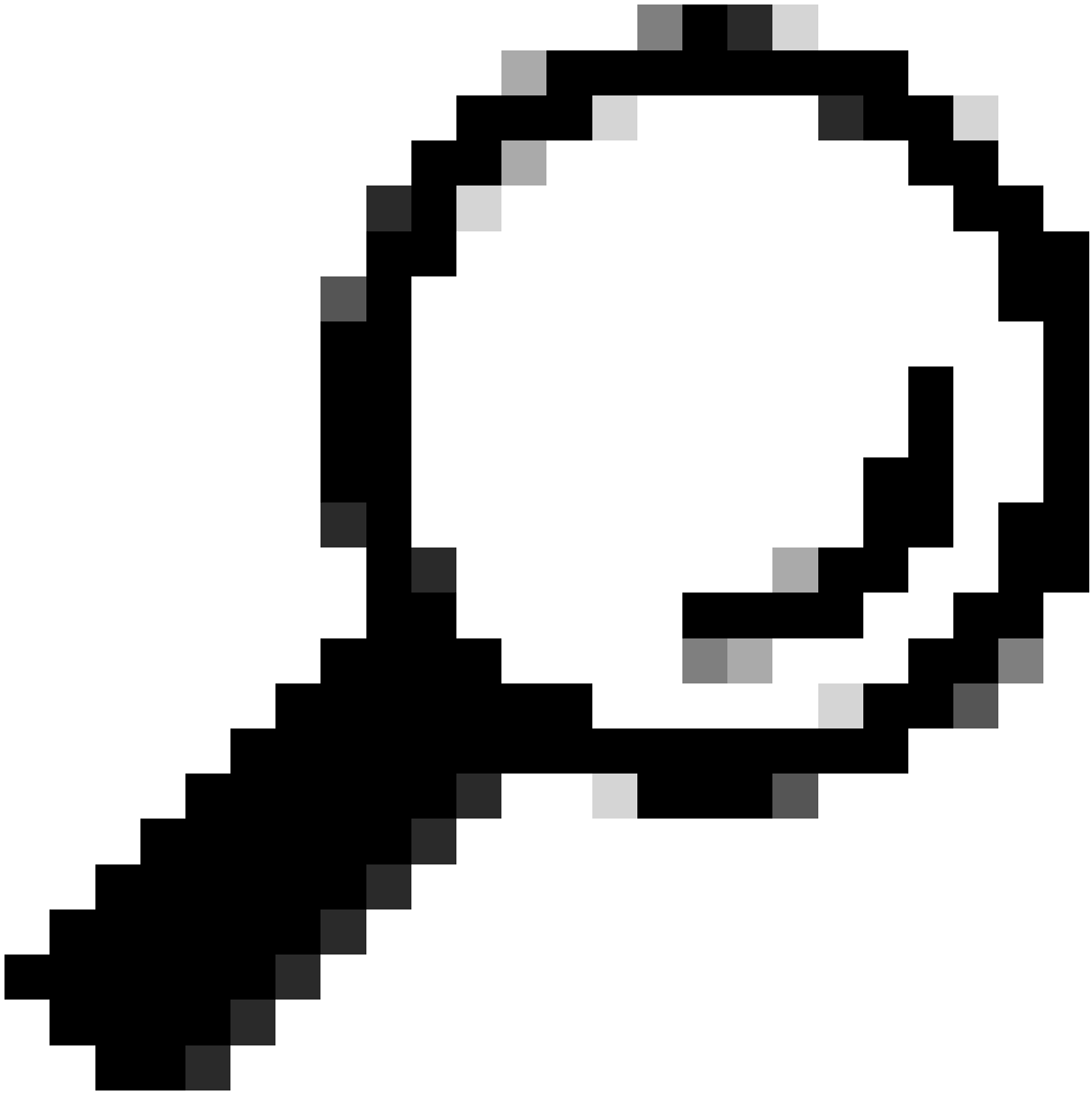
次のコマンドは、flow_collection_trendの73行目の集約fps値を分でグループ化し、fpsで大きい順から小さい順に表示します。

```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "WITH minutes as
(select last_time as Timestamp, sum(fps) as fps, ROW_NUMBER() OVER (order by sum(fps) desc) as RowNumbe
from flow_collection_trend
where last_time >= '2023-04-17 00:00' and last_time < '2023-04-18 00:00'
group by last_time)
select fps as '95thPercentile' from minutes where RowNumber=73;"
```

出力は次の図のようになります。



この値は、1日(2023-04-18)のフロー・レート使用率の95パーセンタイルを表し、
flow_collection_summary表およびSmart Licensing画面の両方に表示される値と一致します。



ヒント：フローコレクタの詳細設定の「Ignore List」を使用すると、IPまたはIP範囲に基づいて不要なフローキャプチャをフィルタリングできます。無視リストにネットワーク領域を追加すると、Smart Licensingで報告されるFPSを効果的に削減して管理できます

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。