Calculate the 95Th Percentile of the Flow Rate Usage in Secure Network Analytics

Contents

Introduction

This document describes how to calculate the 95th percentile of the Flow Rate Usage in Stealthwatch or Secure Network Analytics for FlowRate Licensing

Prerequisites

Requirements

Cisco recommends that you have knowledge in this topics:

- Smart Software Licensing
- Secure Network Analytics navigation within the main dashboard

Components used

The information in this document is based on these software and hardware version:

- Stealthwatch Management Console version 7.4.1

It is also required:

- Administrative access to the Smart Licensing screen in Secure Network Analytics
- CLI access as Root to the Stealthwatch Management Console
- VSQL Database Password
- Your Secure Network Analytics environment is registered in Smart Licensing

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The official 7.4.2 Smart Licensing Guide, page 22, states that Secure Network Analytics reports the 95th

percentile of the daily Flow Rate (flows per second) usage to your Smart Account, based on the previous 24-hour period.

Secure Network Analytics (from now on referenced as SNA) was formerly called Stealthwatch and these terms can be used interchangeably.

Verify

Use this section to confirm that your configuration works properly.

Confirm the 95th percentile value at the Stealthwatch Management Console Database
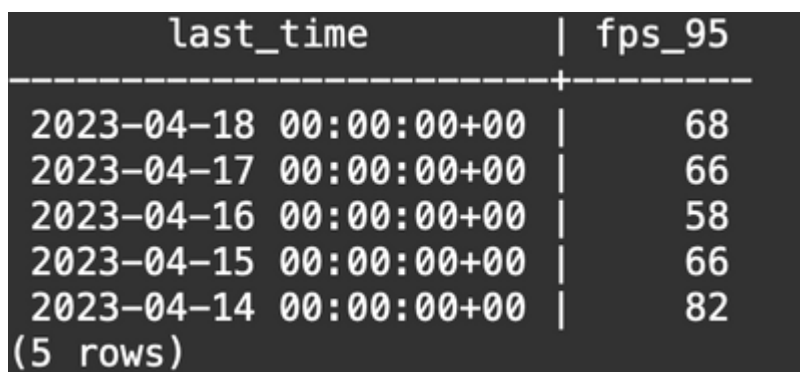

Caution: This document describes the process to calculate the Flow Rate usage for a single example day, April 18, 2023. Adjust the SQL queries to match the intended day for your use case

---

The value that is presented at Flow Rate License, under the Smart License Usage, is pulled from the flow_collection_summary table from the Stealthwatch Management Console Database. To consult this table, log into the Stealthwatch Management Console via SSH as Root and run the command:

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

Note: The commands presented in this document use the default password of the Stealthwatch Management Console database. If the database password has been changed in your environment, adjust the commands so it has the correct

---

The output displays the records of the last five days and its 95th percentile, ordered by most recent. Refer to the next image for an example:

```
       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)
```

As indicated in the Background Information, the daily Flow Rate Usage presented on the Smart Licensing screen is calculated based on the previous 24-hour period. A discrepancy is presented between the dates on the flow_collection_summary table, since it displays a value for a day that has not ended yet. This is due to how the usage is calculated at the end of each day at reset hour, at 00:00:00. At the Smart Licensing screen, the fps_95 value coincides with the value presented for the current day (2023-04-18). See the next image:

Smart License Usage

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

The fps_95 value of April 18 in the flow_collection_summary table corresponds to the Flow Rate usage of the previous day, April 17. The fps_95 value of April 17 corresponds to the Flow Rate of April 16 and so on.

Troubleshoot

This section provides information you can use to troubleshoot your configuration

Calculate the 95th percentile for a single day of usage

The fps_95 value presented at the flow_collection_summary table is calculated based on the information of the flow_collection_trend table, also available at the Stealthwatch Management Console database. This table keeps track of the minute-by-minute flow rate usage of each exporter reported by all Flow Collectors in the environment. For a single day, there are 1440 records, for each one of the 1440 minutes of a day. The tuple minute-fps in the table must look like the next image:
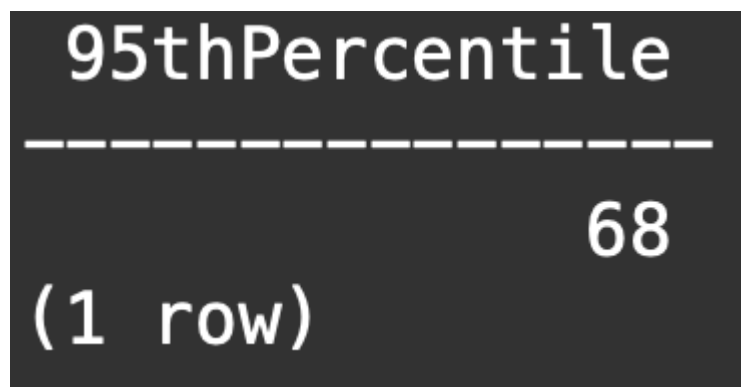


```
       last_time        | fps
------------------------+-----
2023-04-17 07:36:00+00  |  94
2023-04-17 00:48:00+00  |  88
2023-04-17 14:24:00+00  |  86
2023-04-17 23:28:00+00  |  85
2023-04-17 15:33:00+00  |  85
2023-04-17 00:01:00+00  |  85
2023-04-17 20:11:00+00  |  79
2023-04-17 00:50:00+00  |  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
```

The fps_95 column in the flow_collection_summary has its value calculated from the 1440 minute-fps records of a single day. Since only the 95th percentile is reported back, this means that the first 5% of the records (first 72 rows), ordered by the fps column in largest-to-smallest order, are discarded in the process. Thus, the 73th row represents the 95th value of the flow rate usage. There is an expected deviation of the fps value in the 73th of ≈1-2 fps, due to decimal calculations.

The next command displays the aggregated fps value of the 73th row of the flow_collection_trend, grouped by minute and ordered by fps in largest-to-smallest order:

```
/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 RowNumber
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;"
```

The output must look like the next image:

This value represents the 95th percentile of the flow rate usage for a single day (2023-04-18), which matches with what is presented both at the flow_collection_summary table and at the Smart Licensing Screen.