在安全网络分析中计算流量使用率的第95个百分点

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

验证

- 在Stealthwatch管理控制台数据库中确认第95个百分位值

故障排除

- 计算一天使用量的第95个百分点

简介

本文档介绍如何计算Stealthwatch或适用于FlowRate许可的安全网络分析中的流量使用率的第95个百分点

先决条件

要求

Cisco建议您了解以下主题：

- 智能软件许可
- 主控制面板中的Secure Network Analytics导航

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Stealthwatch管理控制台版本7.4.1

此外，还需要执行以下操作：

- 对“安全网络分析”(Secure Network Analytics)中的“智能许可”(Smart Licensing)屏幕的管理访问
- 以Root用户身份访问Stealthwatch管理控制台的CLI
- VSQL数据库密码
- 您的安全网络分析环境已在智能许可中注册

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

官方7.4.2智能许可指南（第22页）指出，安全网络分析会根据之前的24小时时段向智能帐户报告每日流量（每秒流量）使用量的第95个百分点。

安全网络分析（从现在起称为SNA）以前称为Stealthwatch，这些术语可以互换使用。

验证

使用本部分可确认配置能否正常运行。

在Stealthwatch管理控制台数据库中确认第95个百分位值

⚠ 注意：本文档介绍计算单个示例日（2023年4月18日）的流量使用情况的流程。调整SQL查询以匹配您的使用案例的预定日期

在智能许可证使用情况下的流量许可证中显示的值取自Stealthwatch管理控制台数据库的flow_collection_summary表。要查询此表，请以Root身份通过SSH登录到Stealthwatch管理控制台并运行以下命令：

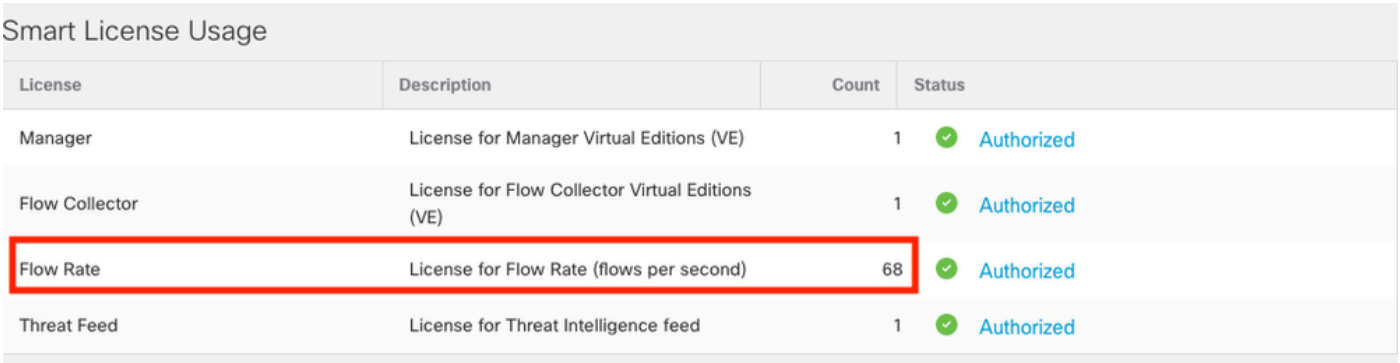
```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select last_time, fps_95 from flow_collection_summary
```

注意：本文档中显示的命令使用Stealthwatch管理控制台数据库的默认密码。如果在您的环境中更改了数据库口令，请调整命令以使其正确

输出显示最近五天的记录和第95个百分位数的记录，按最近时间排序。有关示例，请参阅下一张图片：

```
        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)
```

如背景信息所示，智能许可屏幕上显示的每日流量使用率是根据之前的24小时时段计算的。在flow_collection_summary表的日期之间显示差异，因为它显示尚未结束的日期的值。这是由于在重置时每天结束时的使用率计算方式(00:00:00)。在智能许可屏幕上，fps_95值与当前日显示的值(2023-04-18)一致。请参阅下一张图片：


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表中的fps_95值4月18日对应于前一天（4月17日）的流量使用情况。4月17日的fps_95值对应于4月16日的Flow Rate，依此类推。

故障排除

本部分提供可用于对配置进行故障排除的信息

计算一天使用量的第95个百分点

在flow_collection_summary表中显示的fps_95值基于flow_collection_trend表的信息（也在Stealthwatch Management Console数据库中提供）进行计算。此表跟踪环境中所有流量收集器报告的每个导出器的每分钟流量使用情况。一天中的1440分钟分别有1440条记录。表中的元组minute-fps必须类似于下一个图像：

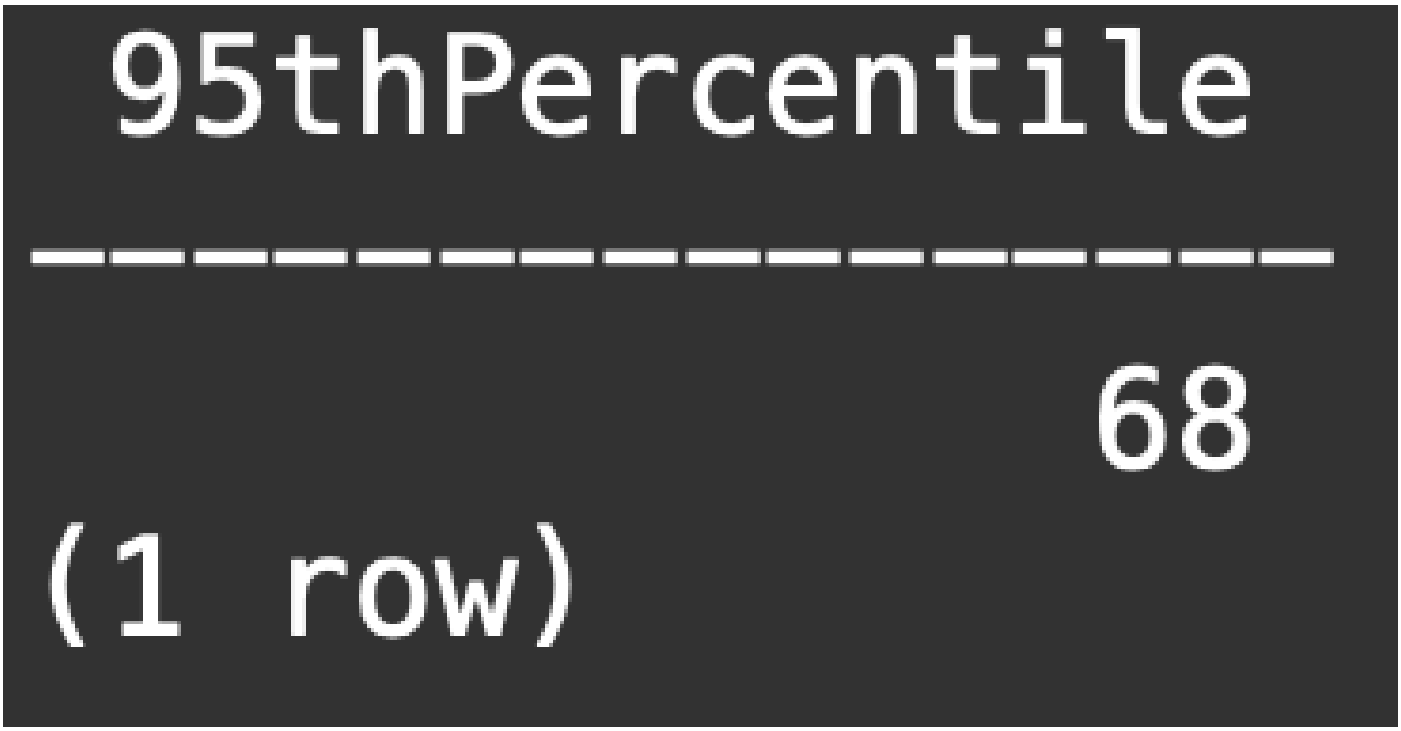
last_time	fps
2023-04-17 07:36:00+00	94
2023-04-17 00:48:00+00	88
2023-04-17 14:24:00+00	86
2023-04-17 23:28:00+00	85
2023-04-17 15:33:00+00	85
2023-04-17 00:01:00+00	85
2023-04-17 20:11:00+00	79
2023-04-17 00:50:00+00	79
2023-04-17 11:00:00+00	78
2023-04-17 20:13:00+00	77
2023-04-17 20:05:00+00	77
2023-04-17 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中的fps_95列的值是根据一天中的1440分钟fps记录计算的。由于只报告第95个百分位数，这意味着在此过程中将丢弃按fps列从大到小的顺序排序的前5%的记录（前72行）。因此，第73行代表流量使用的第95个值。由于十进制计算，fps值在≈1-2 fps的第73次会出现预期偏差。

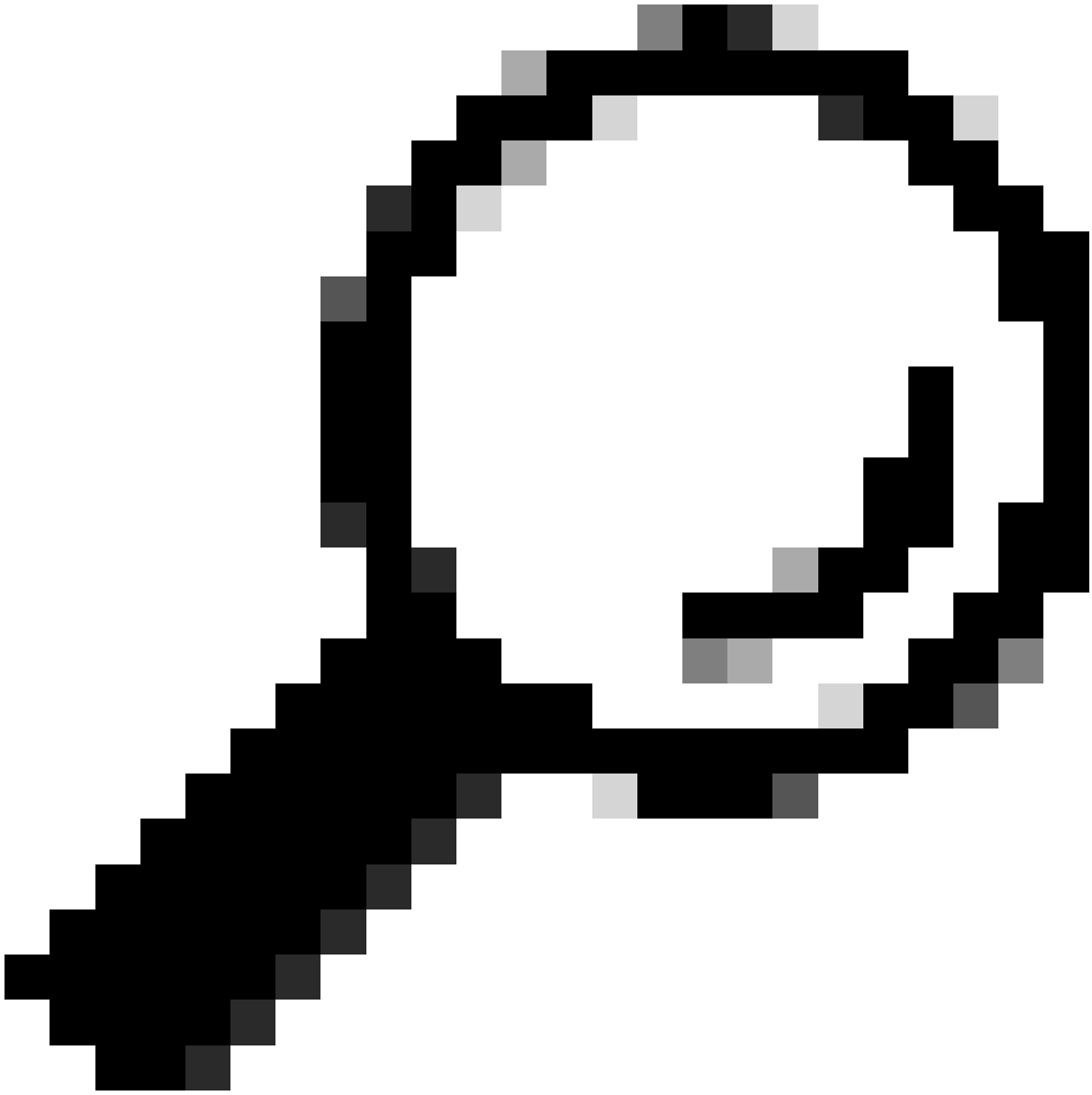
下一命令显示flow_collection_trend第73行的聚合fps值，按分钟分组，并按从大到小的顺序按fps排序：

```
/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;"
```

输出必须类似于下一个映像：



此值表示一天内流量使用情况的第95个百分点(2023-04-18)，与flow_collection_summary表和智能许可屏幕中显示的内容匹配。



提示：请注意，流量收集器高级设置“忽略列表”可用于根据IP或IP范围过滤掉不需要的流量捕获。向忽略列表添加网络空间可用于有效降低管理智能许可所报告的FPS

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。