Calcule o 95o percentil do uso da taxa de fluxo na análise de rede segura

Contents

Introdução

Este documento descreve como calcular o 95o percentil do uso da taxa de fluxo no Stealthwatch ou Secure Network Analytics para o licenciamento da taxa de fluxo

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

- Licenciamento de software inteligente
- Navegação Secure Network Analytics no painel principal

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Stealthwatch Management Console versão 7.4.1

Também é necessário:

- Acesso administrativo à tela Smart Licensing no Secure Network Analytics
- Acesso via CLI como raiz ao Stealthwatch Management Console
- Senha do Banco de Dados VSQL
- Seu ambiente Secure Network Analytics está registrado no Smart Licensing

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O guia oficial de Smart Licensing do 7.4.2, página 22, afirma que o Secure Network Analytics relata o 95º percentil do uso diário da taxa de fluxo (fluxos por segundo) para sua Smart Account, com base no período de 24 horas anterior.

O Secure Network Analytics (a partir de agora conhecido como SNA) era anteriormente chamado de Stealthwatch e esses termos podem ser usados de forma intercambiável.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Confirme o valor do 95º percentil no banco de dados do Stealthwatch Management Console

⚠ Cuidado: este documento descreve o processo para calcular o uso da Taxa de Fluxo para um único dia de exemplo, 18 de abril de 2023. Ajuste as consultas SQL para corresponder ao dia pretendido para seu caso de uso

O valor apresentado na licença de taxa de fluxo, em Uso da licença inteligente, é extraído da tabela flow_collection_summary do banco de dados do Stealthwatch Management Console. Para consultar essa tabela, faça login no Stealthwatch Management Console via SSH como Raiz e execute o comando:

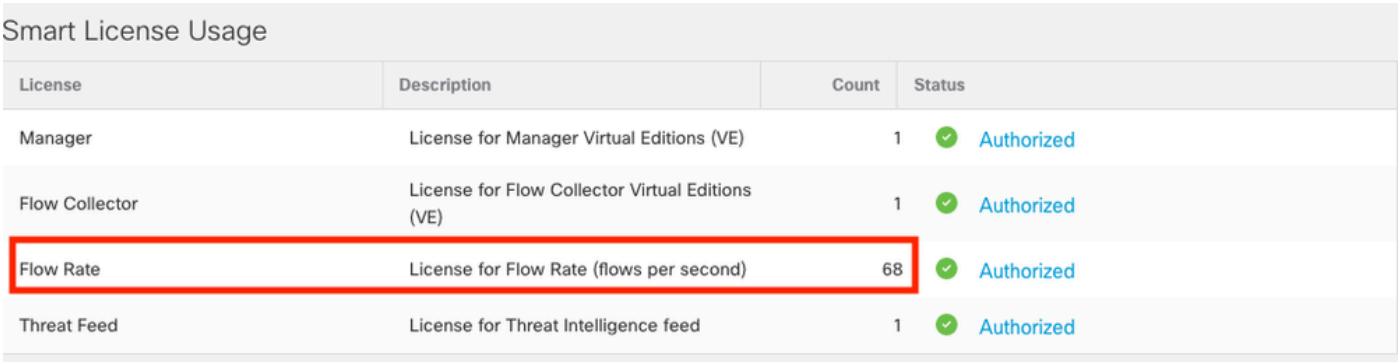
```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select last_time, fps_95 from flow_collection_summary
```

✎ Observação: os comandos apresentados neste documento usam a senha padrão do banco de dados do Stealthwatch Management Console. Se a senha do banco de dados tiver sido alterada no seu ambiente, ajuste os comandos para que ele tenha a senha correta

A saída exibe os registros dos últimos cinco dias e seu percentil 95, ordenados pelo mais recente. Consulte a próxima imagem para obter um exemplo:

```
        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)
```

Como indicado nas Informações de apoio, o uso da taxa de fluxo diário apresentado na tela Smart Licensing é calculado com base no período de 24 horas anterior. Uma discrepância é apresentada entre as datas na tabela flow_collection_summary, pois ela exibe um valor para um dia que ainda não terminou. Isso se deve à forma como o uso é calculado no final de cada dia na hora de redefinição, às 00:00:00. Na tela Smart Licensing, o valor fps_95 coincide com o valor apresentado para o dia atual (18 de abril de 2023). Veja a próxima imagem:


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

O valor fps_95 de 18 de abril na tabela flow_collection_summary corresponde ao uso da Taxa de Fluxo do dia anterior, 17 de abril. O valor fps_95 de 17 de abril corresponde ao Fluxo de 16 de abril e assim por diante.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração

Calcular o 95º percentil para um único dia de uso

O valor fps_95 apresentado na tabela flow_collection_summary é calculado com base nas informações da tabela flow_collection_trend, também disponível no banco de dados do Stealthwatch Management Console. Esta tabela rastreia o uso da taxa de fluxo minuto a minuto

de cada exportador relatado por todos os Flow Collectors no ambiente. Para um único dia, há 1440 registros, para cada um dos 1440 minutos de um dia. Os minutos-fps da tupla na tabela devem parecer com a próxima imagem:

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

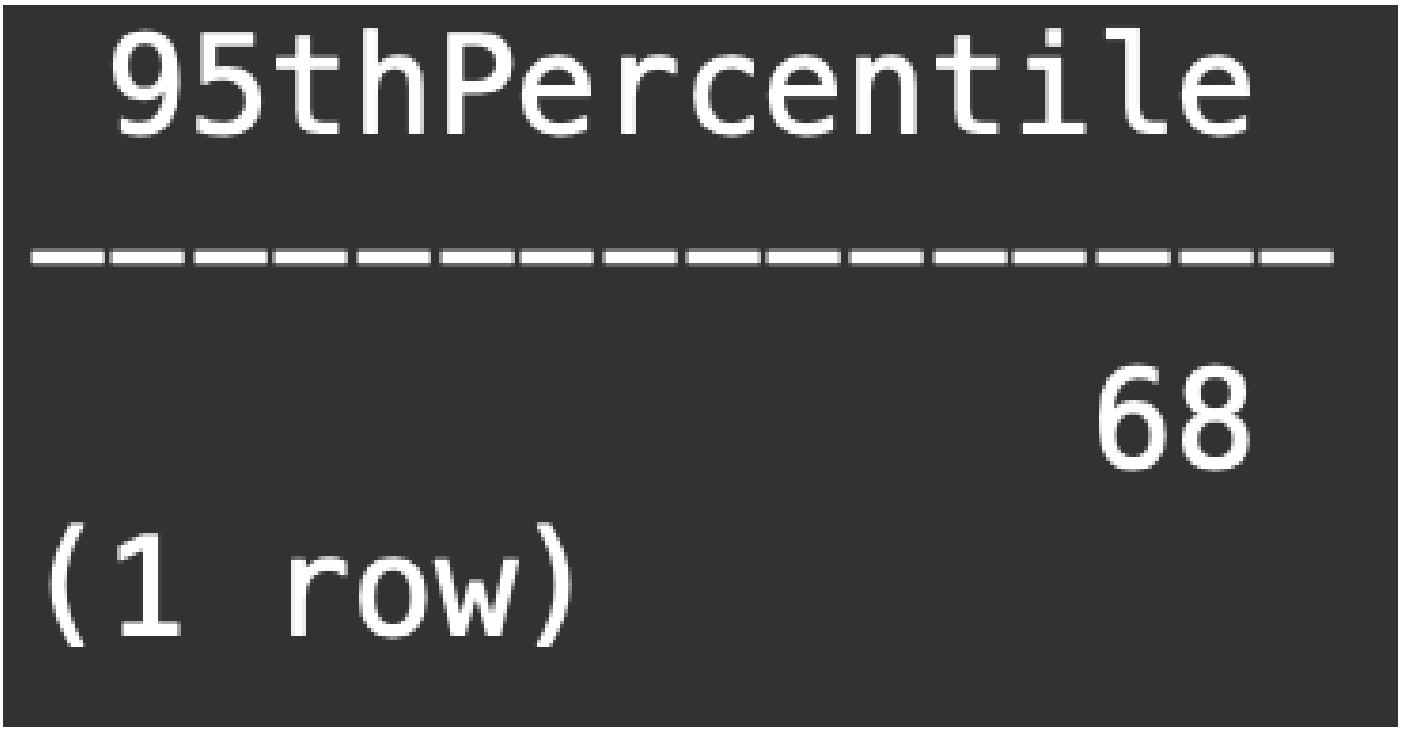
A coluna fps_95 em flow_collection_summary tem seu valor calculado a partir dos registros de 1440 minutos-fps de um único dia. Como apenas o percentil 95 é relatado de volta, isso significa que os primeiros 5% dos registros (primeiras 72 linhas), ordenados pela coluna fps na ordem maior para a menor, são descartados no processo. Assim, a 73ª linha representa o 95º valor do

uso da taxa de fluxo. Há um desvio esperado do valor de fps no 73º de ≈1-2 fps, devido a cálculos decimais.

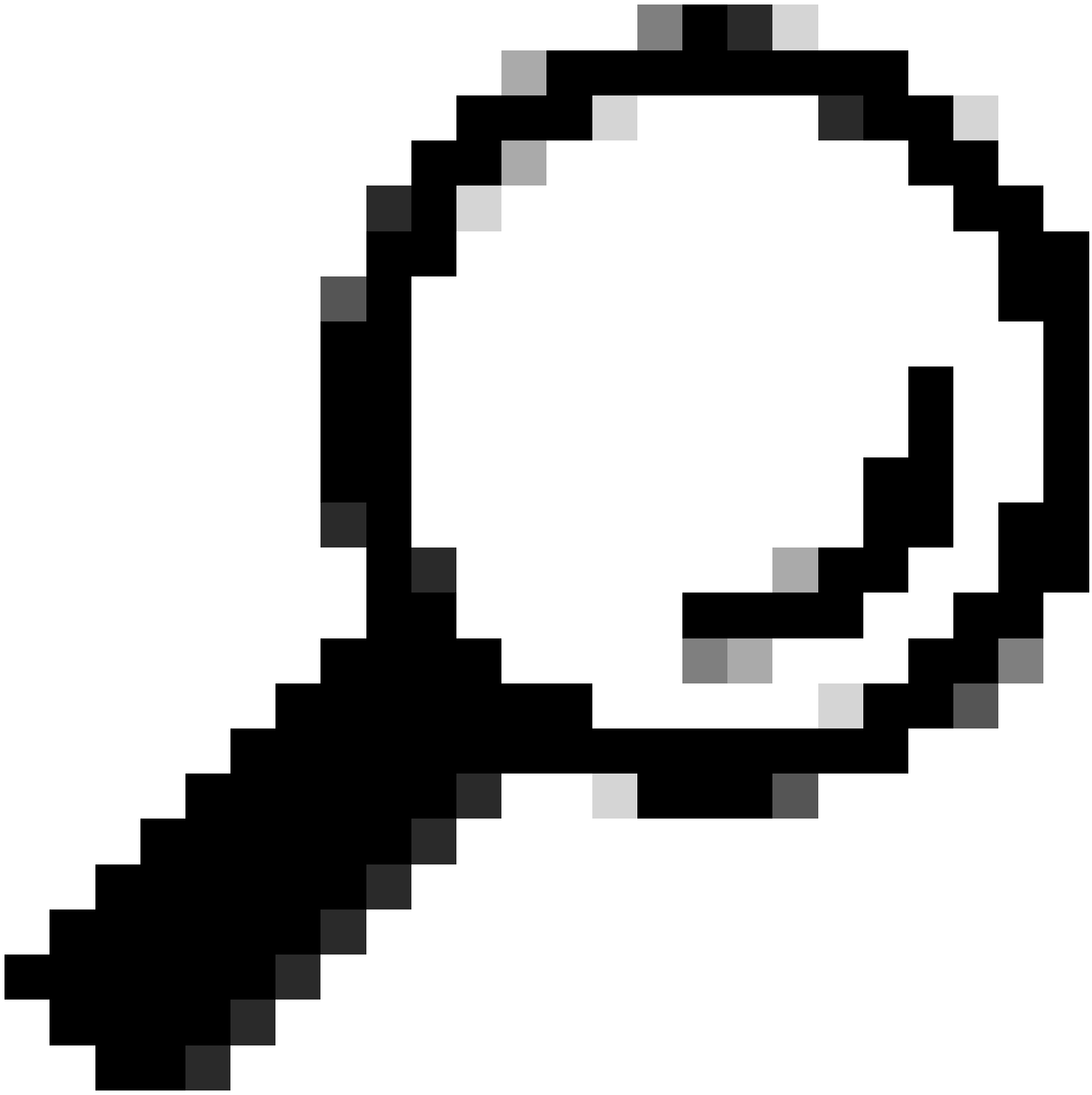
O próximo comando exibe o valor fps agregado da 73ª linha de flow_collection_trend, agrupado por minuto e ordenado por fps na ordem do maior para o menor:

```
/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;"
```

A saída deve ser semelhante à próxima imagem:



Esse valor representa o 95o percentil do uso da taxa de fluxo para um único dia (18 de abril de 2023), que corresponde ao que é apresentado na tabela flow_collection_summary e na tela Smart Licensing.



Dica: observe que a configuração avançada do Flow Collector "Ignore List" pode ser usada para filtrar a captura de fluxo indesejado com base no IP ou no intervalo de IP. Adicionar espaço de rede à lista de ignorados pode ser usado para reduzir efetivamente o gerenciamento de FPS conforme relatado pelo Smart Licensing

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.