

Calculez le 95e centile de l'utilisation du débit dans Secure Network Analytics

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Vérifier](#)

[Confirmez la valeur du 95e centile dans la base de données de la console de gestion StealthWatch](#)

[Dépannage](#)

[Calculez le 95e centile pour une seule journée d'utilisation](#)

Introduction

Ce document décrit comment calculer le 95e centile de l'utilisation du débit dans StealthWatch ou Secure Network Analytics pour les licences FlowRate

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Licences logicielles Smart
- Navigation Secure Network Analytics dans le tableau de bord principal

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles et matérielles suivantes :

- Console de gestion StealthWatch version 7.4.1

Il est également nécessaire :

- Accès administratif à l'écran Smart Licensing dans Secure Network Analytics
- Accès CLI en tant que racine à la console de gestion StealthWatch
- Mot de passe VSQL Database
- Votre environnement Secure Network Analytics est enregistré dans 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le guide officiel 7.4.2 Smart Licensing Guide, page 22, indique que Secure Network Analytics indique le 95e centile du débit journalier (flux par seconde) utilisé sur votre compte Smart, sur la base de la période précédente de 24 heures.

Secure Network Analytics (désormais appelé SNA) s'appelait auparavant StealthWatch et ces termes peuvent être utilisés indifféremment.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Confirmez la valeur du 95e centile dans la base de données de la console de gestion StealthWatch

 Attention : ce document décrit le processus de calcul de l'utilisation du débit pour un seul exemple de jour, le 18 avril 2023. Ajustez les requêtes SQL en fonction du jour prévu pour votre exemple d'utilisation

La valeur présentée dans Flow Rate License, sous Smart License Usage, est extraite de la table `flow_collection_summary` de la base de données de la console de gestion StealthWatch. Pour consulter cette table, connectez-vous à la console de gestion StealthWatch via SSH en tant que racine et exécutez la commande suivante :

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

 Remarque : les commandes présentées dans ce document utilisent le mot de passe par défaut de la base de données StealthWatch Management Console. Si le mot de passe de la base de données a été modifié dans votre environnement, ajustez les commandes de sorte qu'il possède le bon

Le résultat affiche les enregistrements des cinq derniers jours et son 95e centile, triés par ordre décroissant. Reportez-vous à l'image suivante pour obtenir un exemple :

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)

Comme indiqué dans les Informations générales, l'utilisation quotidienne du débit présentée dans l'écran Licence intelligente est calculée en fonction de la période de 24 heures précédente. Un écart est présenté entre les dates de la table flow_collection_summary, car il affiche une valeur pour un jour qui n'est pas encore terminé. Cela est dû à la façon dont l'utilisation est calculée à la fin de chaque jour à l'heure de réinitialisation, à 00:00:00. Sur l'écran Smart Licensing, la valeur fps_95 coïncide avec la valeur présentée pour le jour en cours (2023-04-18). Voir l'image suivante :

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

La valeur fps_95 du 18 avril dans la table flow_collection_summary correspond à l'utilisation du débit du jour précédent, le 17 avril. La valeur fps_95 du 17 avril correspond au débit du 16 avril, etc.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration

Calculez le 95e centile pour une seule journée d'utilisation

La valeur fps_95 présentée dans la table flow_collection_summary est calculée à partir des informations de la table flow_collection_trend, également disponibles dans la base de données StealthWatch Management Console. Ce tableau permet de suivre l'utilisation du débit minute par

minute de chaque exportateur signalé par tous les collecteurs de flux de l'environnement. Pour une seule journée, il y a 1440 enregistrements, pour chacune des 1440 minutes d'une journée. Le nombre de minutes-ips dans le tableau doit ressembler à l'image suivante :

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

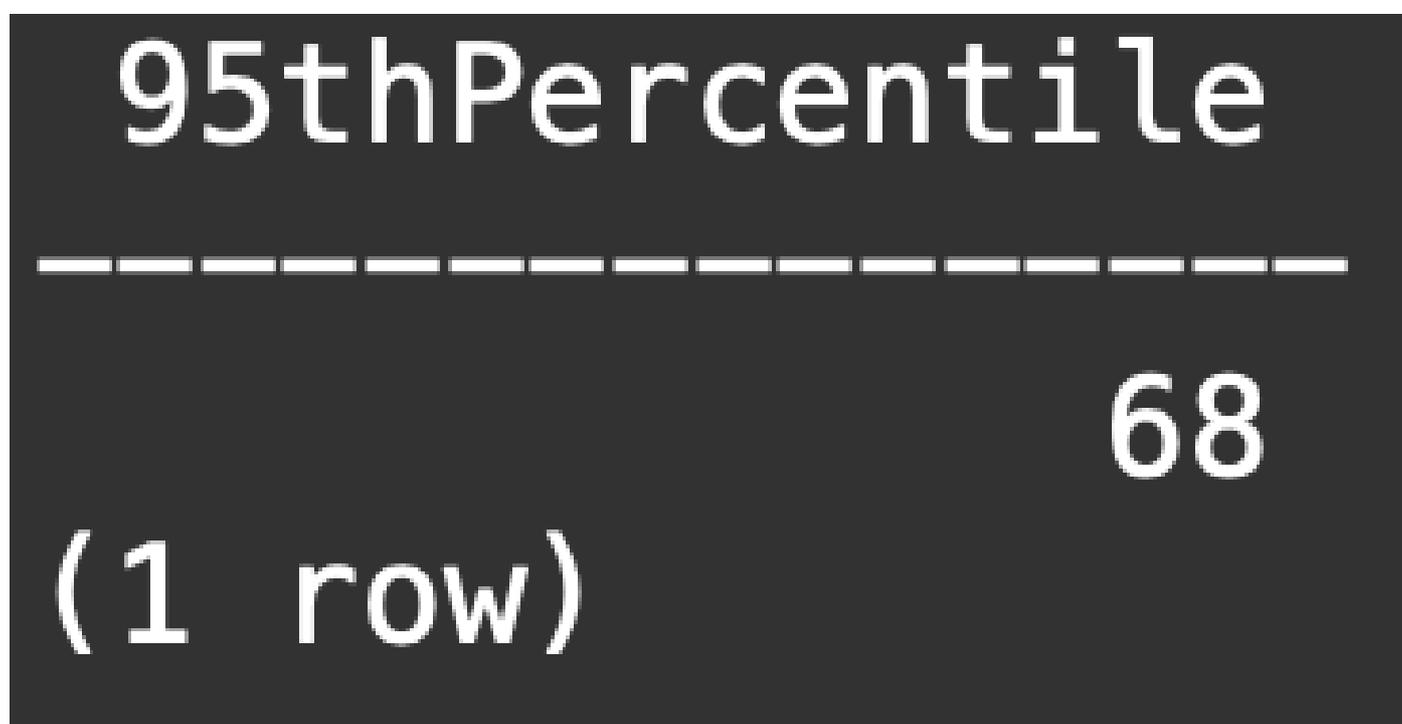
La valeur de la colonne `fps_95` de `flow_collection_summary` est calculée à partir des enregistrements 1440 minutes-fps d'une seule journée. Puisque seul le 95e centile est retourné, cela signifie que les 5 premiers % des enregistrements (72 premières lignes), classés par la colonne `fps` dans l'ordre du plus grand au plus petit, sont rejetés dans le processus. Ainsi, la 73e

ligne représente la 95e valeur de l'utilisation du débit. Il y a un écart prévu de la valeur fps dans le 73ème de $\approx 1-2$ fps, en raison de calculs décimaux.

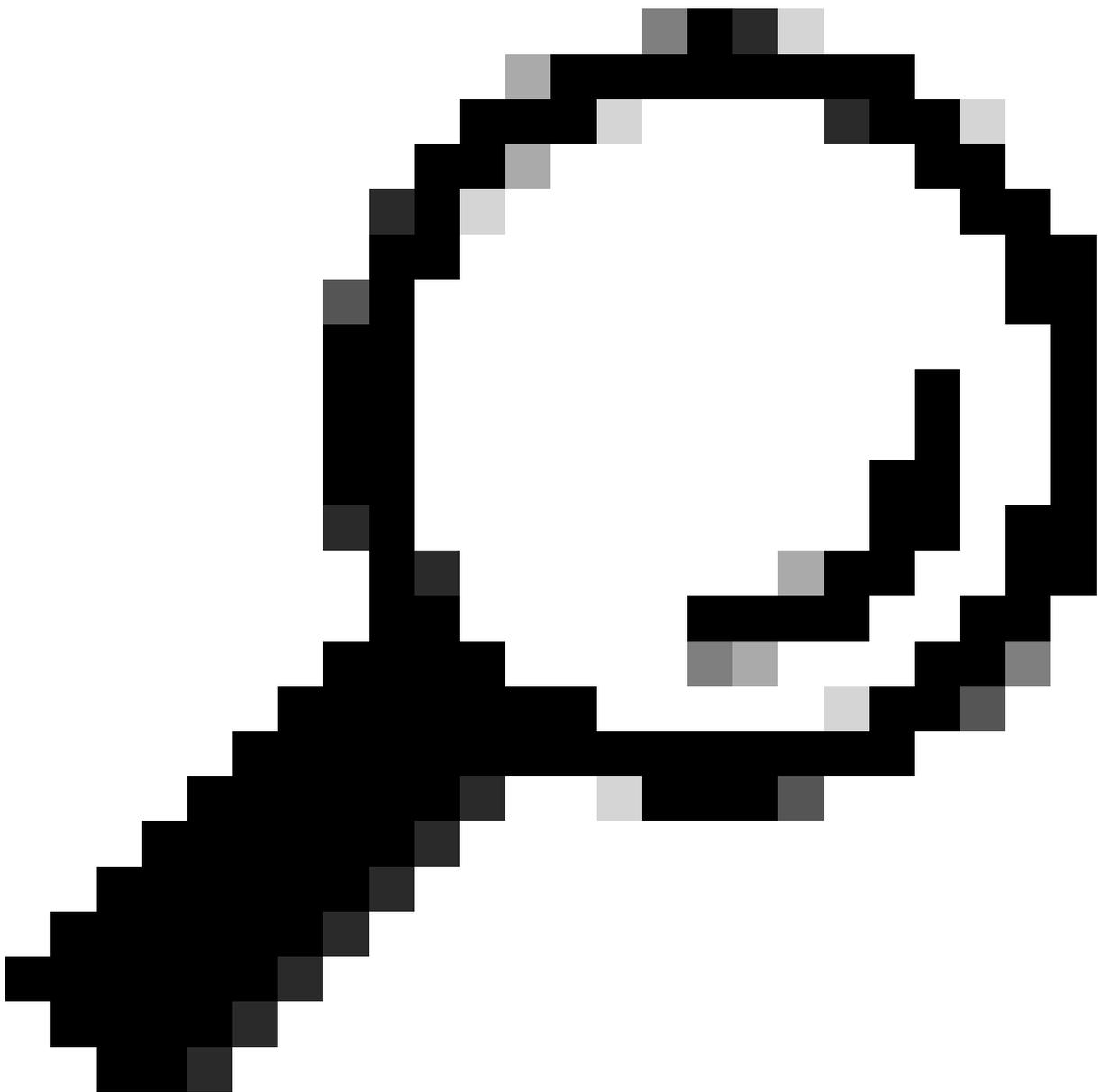
La commande suivante affiche la valeur fps agrégée de la 73e ligne de flow_collection_trend, groupée par minute et ordonnée par fps dans l'ordre du plus grand au plus petit :

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -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;"
```

Le résultat doit ressembler à l'image suivante :



Cette valeur représente le 95e centile de l'utilisation du débit pour une seule journée (2023-04-18), qui correspond à ce qui est présenté à la fois dans le tableau flow_collection_summary et dans l'écran Smart Licensing.



Conseil : notez que le paramètre avancé du collecteur de flux « Ignorer la liste » peut être utilisé pour filtrer les captures de flux indésirables en fonction de l'IP ou de la plage d'IP. L'ajout d'un espace réseau à la liste d'exclusion peut être utilisé pour réduire efficacement la taille de la gestion FPS, comme indiqué par Smart Licensing

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.