Calcolare il 95° percentile dell'utilizzo della velocità di flusso in Secure Network Analytics

Sommario

Introduzione

Questo documento descrive come calcolare il 95° percentile del tasso di utilizzo in Stealthwatch o Secure Network Analytics per FlowRate Licensing

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Licenze software Smart
- Navigazione di Analisi della rete protetta nel dashboard principale

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Stealthwatch Management Console versione 7.4.1

È inoltre necessario:

- Accesso amministrativo alla schermata di Smart Licensing in Secure Network Analytics
- Accesso CLI come root a Stealthwatch Management Console
- Password database VSQL
- L'ambiente Secure Network Analytics è registrato in Smart Licensing

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La 7.4.2 Smart Licensing Guide ufficiale, pagina 22, afferma che Secure Network Analytics riporta il 95° percentile dell'utilizzo giornaliero della velocità di flusso (flussi al secondo) sullo Smart Account, in base al precedente periodo di 24 ore.

Secure Network Analytics (d'ora in avanti indicata come SNA) un tempo era chiamata Stealthwatch e questi termini possono essere usati in modo intercambiabile.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Confermare il valore del 95° percentile nel database di Stealthwatch Management Console

---

⚠ Attenzione: in questo documento viene descritto il processo per calcolare l'utilizzo del tasso di flusso per un singolo giorno di esempio, il 18 aprile 2023. Regolare le query SQL in modo che corrispondano al giorno previsto per lo Use Case

---

Il valore presentato in Flow Rate License, in Uso licenza intelligente, viene ricavato dalla tabella flow_collection_summary dal database di Stealthwatch Management Console. Per consultare questa tabella, accedere a Stealthwatch Management Console come root tramite SSH ed eseguire il comando:

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

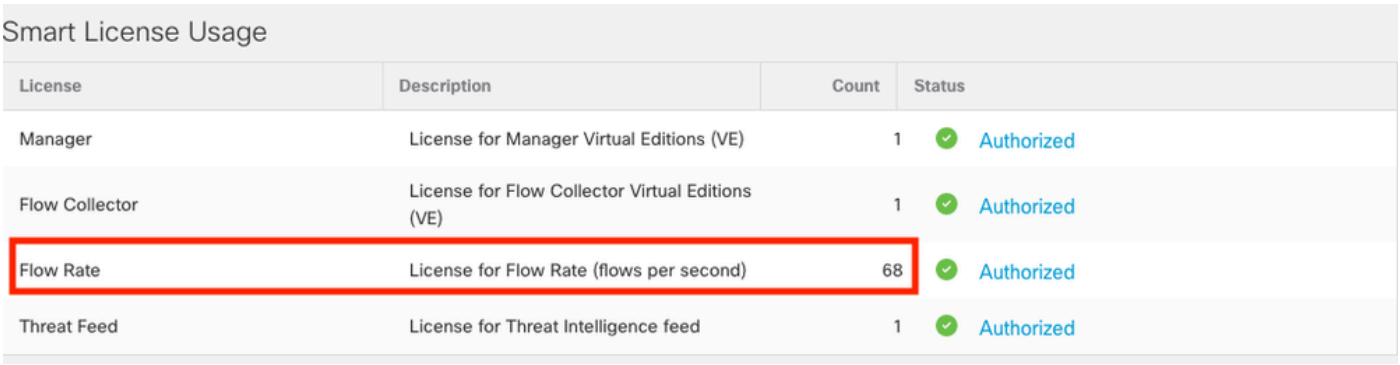
✎ Nota: i comandi presentati in questo documento utilizzano la password predefinita del database di Stealthwatch Management Console. Se la password del database è stata modificata nell'ambiente in uso, modificare i comandi in modo che disponga della password corretta

---

L'output visualizza i record degli ultimi cinque giorni e il relativo 95° percentile, ordinati in base alla data più recente. Per un esempio, fare riferimento all'immagine successiva:

```
        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)
```

Come indicato nelle informazioni preliminari, l'utilizzo giornaliero della velocità di flusso visualizzato nella schermata Smart Licensing viene calcolato in base al periodo di 24 ore precedente. Viene visualizzata una discrepanza tra le date nella tabella flow_collection_summary, poiché viene visualizzato un valore per un giorno non ancora terminato. Ciò è dovuto alla modalità di calcolo dell'uso alla fine di ogni giorno all'ora di ripristino, alle 00:00:00. Nella schermata Smart Licensing, il valore fps_95 coincide con il valore presentato per il giorno corrente (2023-04-18). Vedere l'immagine successiva:


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

Il valore fps_95 del 18 aprile nella tabella flow_collection_summary corrisponde all'utilizzo del tasso di flusso del giorno precedente, il 17 aprile. Il valore fps_95 del 17 aprile corrisponde al tasso di flusso del 16 aprile e così via.

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione

Calcolare il 95° percentile per un singolo giorno di utilizzo

Il valore fps_95 presentato nella tabella flow_collection_summary viene calcolato in base alle informazioni della tabella flow_collection_trend, disponibile anche nel database di Stealthwatch Management Console. In questa tabella viene registrato l'utilizzo della velocità di flusso minuto per

minuto di ogni esportatore segnalato da tutti i Flow Collector nell'ambiente. Per un singolo giorno, sono disponibili 1440 record, ciascuno dei 1440 minuti di un giorno. I minuti-fps di tupla nella tabella devono essere simili all'immagine successiva:

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

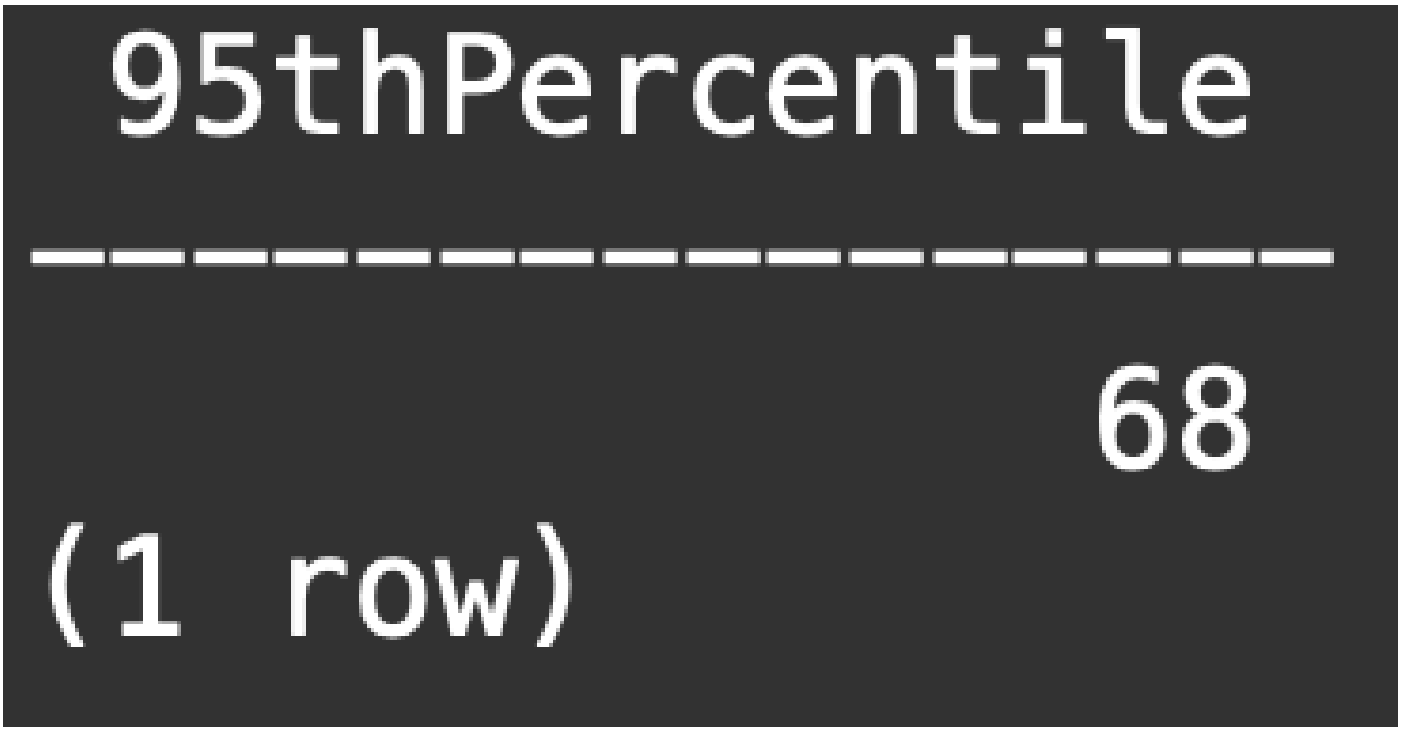
Il valore della colonna fps_95 in flow_collection_summary viene calcolato a partire dai record da 1440 minuti al secondo di un singolo giorno. Poiché viene restituito solo il 95° percentile, ciò significa che il primo 5% dei record (le prime 72 righe), ordinato in base alla colonna fps in ordine crescente, viene scartato nel processo. Pertanto, la 73a riga rappresenta il 95o valore dell'utilizzo

della velocità di flusso. C'è una deviazione prevista del valore fps nel 73esimo di ~1-2 fps, a causa dei calcoli decimali.

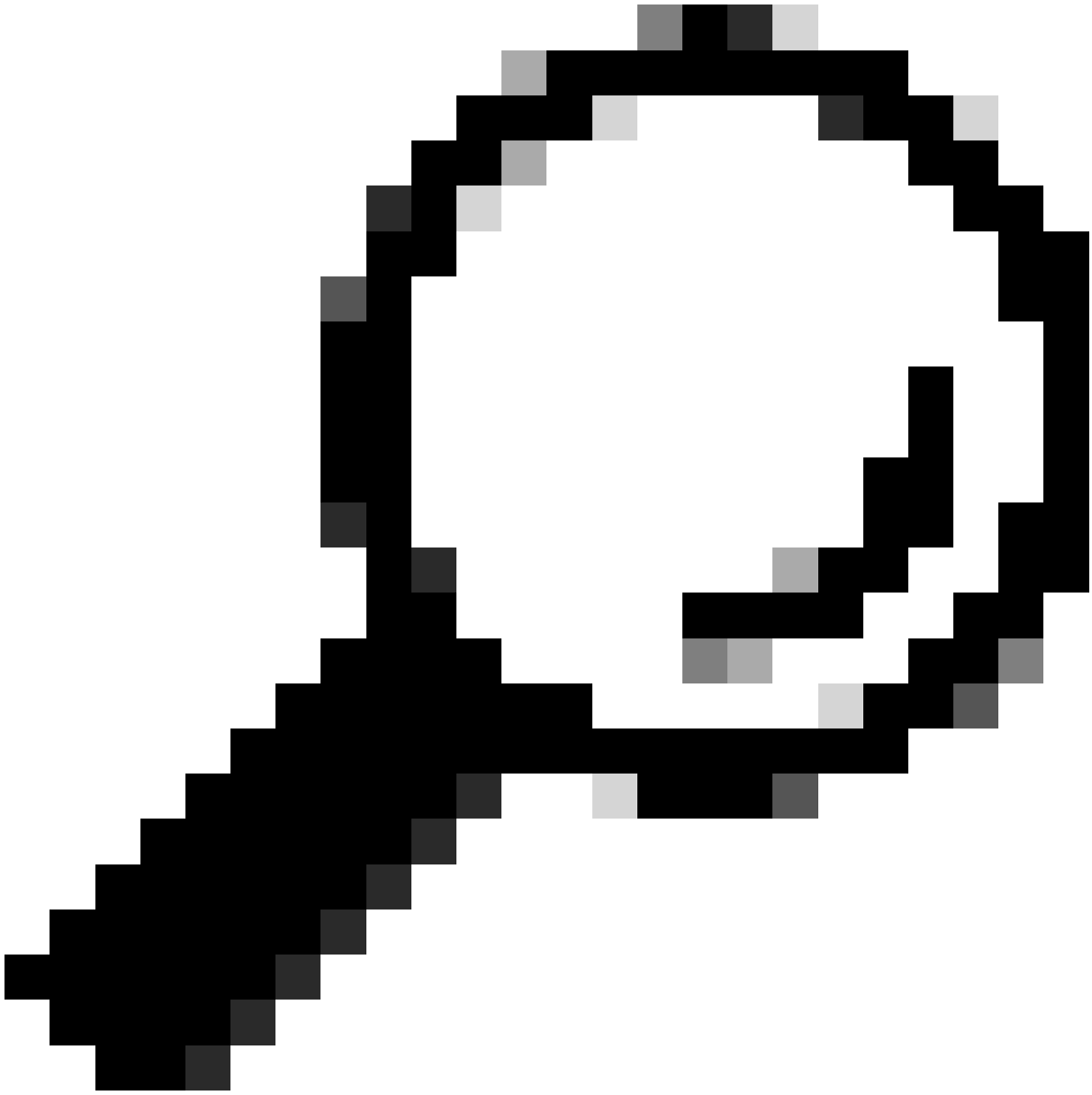
Il comando successivo visualizza il valore fps aggregato della settantatreesima riga di flow_collection_trend, raggruppato per minuto e ordinato per fps in ordine crescente:

```
/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;"
```

L'output deve essere simile all'immagine successiva:



Questo valore rappresenta il 95° percentile dell'utilizzo della velocità di flusso per un singolo giorno (2023-04-18), che corrisponde a quanto presentato sia nella tabella flow_collection_summary che nella schermata Smart Licensing.



Suggerimento: si noti che l'impostazione avanzata del Flow Collector "Ignora elenco" può essere utilizzata per filtrare l'acquisizione di flusso indesiderata basata su IP o intervallo IP. L'aggiunta di spazio di rete all'elenco dei server da ignorare può essere utilizzata per ridurre in modo efficace la gestione di FPS, come segnalato da Smart Licensing

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).