Waarde voor geaggregeerde KPI toont N/A ongeacht de KPI-ernst van de entiteit

toepasbaarheid

Splunk Enterprise Splunk IT Service Intelligence

Beschrijving

Wanneer de Services (ongeveer 850) die aan een Servicesjabloon zijn gekoppeld, in de Servicemanalist worden bekeken en de bijbehorende KPI's worden weergegeven, geeft de Entity KPI Severity de juiste waarde (Info) weer, maar de Service KPI Severity toont Unknown. Zowel de geaggregeerde drempelwaarden als de drempelwaarden per entiteit zijn ingesteld op Info voor de KPI’s.

resolutie

Er zijn veel entiteiten EN veel diensten/KPI’s (8 KPI’s per template/dienst). Als gevolg hiervan geeft elke run van de KPI-basiszoekopdrachten tienduizenden resultaten terug, die de limiet kunnen overschrijden wanneer ITSI de verwerkte zoekresultaten naar de ITSI-overzichtsindex transporteert

Om het probleem te voorkomen: verminder het aantal resultaten door de services te distribueren naar meerdere gedeelde zoekopdrachten.

- Identificeer de grootste Shared base zoekopdrachten, die meer dan 50000 resultaten opleveren,

De ID in de zoeknaam is de ID van de gedeelde zoekbasis.

```
index=_internal source=*scheduler.log* shared indicator  | stats min(result_count) AS mi
```

- Bepaal hoeveel services (en entiteiten per service) je hebt, kijk of je de helft en de helft kunt doen.
- Klonen van de gedeelde basis zoekopdrachten. Wijs vervolgens de helft van de services opnieuw toe om de nieuwe gedeelde zoekfunctie te gebruiken.
- Laat het uitvoeren en gebruik dan de bovenstaande zoekopdracht om de nieuwe repartitie van resultaten per gedeelde basiszoekopdracht te zien, zorg ervoor dat ze onder de limiet zijn
- ten slotte in de diensten te valideren dat de KPI nu een geldige "totale waarde voor de dienst" heeft

OF

de limiet verhogen (niet verder gaan dan 100000)

1. Maak of bewerk de limits.conf in $SPLUNK_HOME/etc/system/local.
2. Voeg de volgende strofe toe:

```
[scheduler]
* The maximum number of results to load when triggering an alert action.
* Default: 50000
max_action_results = 50000
```

3. U moet het bovenstaande getal zelf berekenen en aanpassen, wat gebaseerd is op de volgende formule:

```
limit = (number of KPIs * number of entities for each service) + (number of services) *
```

OPMERKING: Als gevolg van het verhogen van deze limiet gebruikt ITSI meer geheugen omdat er meer geheugen wordt toegewezen om het aantal resultaten te ondersteunen

4. Splunk opnieuw opstarten

Gerelateerde links

Splunk Blog

Top 3 best practices voor het configureren van Splunk ITSI in een grootschalige omgeving

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.