Il valore per l'indicatore KPI aggregato visualizza N/D indipendentemente dalla gravità dell'indicatore KPI dell'entità

Applicabilità

Splunk Enterprise Splunk IT Service Intelligence

Descrizione

Quando i servizi (circa 850) collegati a un modello di servizio vengono visualizzati in Service Analyzer e gli indicatori KPI correlati vengono visualizzati, nel campo Gravità KPI entità viene visualizzato il valore corretto (Info), mentre nel campo Gravità KPI servizio viene visualizzato Sconosciuto. Sia le soglie aggregate che quelle per entità sono impostate su Info per gli indicatori KPI.

Risoluzione

Sono presenti molte entità E molti servizi/indicatori KPI (8 indicatori KPI per modello/servizio). Di conseguenza, ogni esecuzione delle ricerche di base KPI restituisce decine di migliaia di risultati, che possono superare il limite quando ITSI trasporta i risultati della ricerca elaborati nell'indice di riepilogo ITSI

Per evitare il problema: ridurre il numero di risultati, distribuendo i servizi a più ricerche di base condivise.

- identificare le ricerche di base condivise più estese, che restituiscono più di 50000 risultati,

L'ID nel nome della ricerca è l'ID della ricerca di base condivisa.

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

- Determinare il numero di servizi (e di entità per servizio) disponibili e verificare se è possibile eseguirne la metà.
- Clonare le ricerche della base condivisa. Riassegnare quindi metà dei servizi per utilizzare la nuova ricerca di base condivisa.
- Lasciare che venga eseguito, quindi utilizzare la ricerca precedente per visualizzare la nuova partizione dei risultati per ogni ricerca di base condivisa, accertarsi che siano al di sotto del limite
- infine verificare nei servizi che l'indicatore KPI disponga ora di un "valore aggregato del servizio" valido

O

aumentare il limite (non superare 100000)

1. Creare o modificare il file limits.conf in $SPLUNK_HOME/etc/system/local.
2. Aggiungere la seguente stanza:

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

3. Sarà necessario calcolare e adeguare personalmente il numero sopra indicato, che si basa sulla seguente formula:

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

NOTA: In seguito all'aumento di questo limite, l'ITSI utilizzerà più memoria in quanto verrà allocata più memoria per supportare il numero di risultati

4. Riavviare Splunk

Collegamenti correlati

Blog Splunk

Le tre migliori procedure ottimali per la configurazione di Splunk ITSI in un ambiente su larga scala

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).