El valor de KPI agregado muestra N/A independientemente de la gravedad de KPI de entidad

Aplicabilidad

Splunk Enterprise Inteligencia de servicios de TI Splunk

Descripción

Cuando los servicios (alrededor de 850) vinculados a una plantilla de servicio se ven en Service Analyzer y se muestran los KPI relacionados, Entity KPI Severity muestra el valor correcto (Info) pero Service KPI Severity muestra Unknown. Tanto Aggregate Threshold como Per Entity Threshold están establecidos en Info para los KPI.

Resolución

Hay muchas entidades Y muchos servicios/KPI (8 KPI por plantilla/servicio). Como resultado, cada ejecución de las búsquedas de base de KPI devuelve decenas de miles de resultados, que pueden superar el límite cuando ITSI transporta los resultados de búsqueda procesados al índice de resumen de ITSI

Para evitar el problema: reducir el número de resultados mediante la distribución de los servicios a varias búsquedas de shared base.

- Identificar las búsquedas de base compartida más grandes que devuelven más de 50000 resultados.

El ID del nombre de búsqueda es el ID de la búsqueda de la base compartida.

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

- Averigüe cuántos servicios (y entidades por servicio) tiene, a ver si puede prestar la mitad y la otra mitad.
- Clonar las búsquedas de base compartida. A continuación, reasigne la mitad de los servicios para utilizar la nueva búsqueda de base compartida.
- Déjela ejecutar y, a continuación, utilice la búsqueda anterior para ver la nueva repartición de resultados por búsqueda de base compartida; asegúrese de que estén por debajo del límite
- valide finalmente en los servicios que el KPI tiene ahora un "valor agregado de servicio" válido

O bien

aumente el límite (no supere los 100000)

1. Haga o edite limits.conf en $SPLUNK_HOME/etc/system/local.
2. Añádase la siguiente estrofa:

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

3. Tendrá que calcular y ajustar el número anterior usted mismo, que se basa en la siguiente fórmula:

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

NOTE: Como resultado del aumento de este límite, ITSI utilizará más memoria, ya que se asignará más memoria para admitir el número de resultados

4. Reiniciar Splunk

Enlaces relacionados

Blog de Splunk

Las 3 mejores prácticas para configurar Splunk ITSI en un entorno a gran escala

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).