La valeur de l'indicateur de performance clé agrégé indique N/A indépendamment de la gravité de l'indicateur

Applicabilité

Splunk Enterprise Splunk IT Service Intelligence

Description

Lorsque les services (environ 850) liés à un modèle de service sont affichés dans l'Analyseur de services et que les indicateurs associés sont affichés, la gravité de l'indicateur d'entité affiche la valeur correcte (Infos), mais la gravité de l'indicateur de service indique Inconnu. Les seuils d'agrégation et les seuils par entité sont définis sur Infos pour les indicateurs.

Résolution

Il existe de nombreuses entités ET de nombreux services/indicateurs de performance clés (8 indicateurs de performance clés par modèle/service). Par conséquent, chaque exécution des recherches de base d'indicateurs de performance clés renvoie des dizaines de milliers de résultats, ce qui peut dépasser la limite lorsque l'ITSI transporte les résultats de recherche traités vers l'index de synthèse de l'ITSI

Pour éviter le problème : réduire le nombre de résultats, en distribuant les services à plusieurs recherches de base partagée.

- Identifiez les recherches de base partagée les plus importantes, qui renvoient plus de 50000 résultats,

L'ID dans le nom de recherche est l'ID de la recherche de base partagée.

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

- Figure combien de services (et d'entités par service) vous avez, voir si vous pouvez faire moitié moitié.
- Clonez les recherches dans la base partagée. Réaffectez ensuite la moitié des services pour utiliser la nouvelle recherche de base partagée.
- Laissez-le s'exécuter, puis utilisez la recherche ci-dessus pour voir la nouvelle répartition des résultats par recherche de base partagée, assurez-vous qu'ils sont sous la limite
- enfin valider dans les services que l'indicateur de performance clé a désormais une « valeur agrégée de service » valide

OU

augmenter la limite (ne pas dépasser 100000)

1. Créez ou modifiez le fichier limits.conf dans $SPLUNK_HOME/etc/system/local.
2. Ajouter la strophe suivante :

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

3. Vous devrez calculer et ajuster vous-même le nombre ci-dessus, qui est basé sur la formule suivante :

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

NOTE: Suite à l'augmentation de cette limite, l'ITSI utilisera plus de mémoire, car plus de mémoire sera allouée pour prendre en charge le nombre de résultats

4. Redémarrez le Splunk

Liens connexes

Splunk Blog

Les 3 meilleures pratiques de configuration de Splunk ITSI dans un environnement à grande échelle

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.