

Impossible de rechercher les champs avec "="

Applicabilité

Cloud Splunk Enterprise Splunk

Description

Version du Splunk : 7.0.13

Lorsque vous tentez de rechercher l'un des champs suivants en faisant correspondre une chaîne :

- capsule
- espace de noms
- nom_conteneur
- id_conteneur

Comme `container_id=add1`, ne renvoie pas de résultats.

Enquête

Après quelques recherches, il a été remarqué que les données HEC sur cette configuration sont indexées sans aucun fichier de configuration, mais pour l'utiliser correctement, une certaine configuration est nécessaire. Les champs peuvent en fait être recherchés en configurant avec le `::` sign (spécificateur de champs de métadonnées), mais cela ne résout pas le fait qu'ils ne peuvent pas être recherchés avec le signe `=`.

Pour que cela fonctionne, d'autres configurations doivent être effectuées lors de la recherche. Il semble que lorsqu'il y a des entrées HEC pour les kubernetes GCP, les événements ne sont pas complètement préparés pour être recherchables. En particulier, les champs semblent ne pas rester indexés, ce qui fait partie des données brutes de données mais ne doit pas être spécifié sur la recherche d'obtenir des événements.

Résolution

Puisque les événements n'obtiennent pas les paramètres de configuration indexés, vous devez les ajouter comme suit :

Instance : Tête de recherche

Fichier: `champs.conf`

Chemin : \$SPLUNK_HOME/etc/apps/search/local

Paramètre : Ajoutez chaque champ en tant que strophe avec le paramètre INDEXED=true comme suit.

```
[pod]
INDEXED=true[namespace]
INDEXED=true[container_name]
INDEXED=true[container_id]
INDEXED=true
```

Après cela, la tête de recherche doit être redémarrée, et avec cela, les nouveaux événements à venir seront recherchables avec le signe =.

Liens connexes

Réponses Splunk

Pourquoi dois-je rechercher des métadonnées dans un argument « fields » d'un HEC avec « :: » ?
:

<https://answers.splunk.com/answers/635676/why-do-i-need-to-search-metadata-in-a-fields-argum.html>

Liens externes

Paramètres de journalisation Kubernetes :

<https://github.com/splunk/splunk-connect-for-kubernetes/tree/develop/helm-chart/splunk-kubernetes-logging>

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.