

Récupération des erreurs de synchronisation dans un environnement de clustering des têtes de recherche.

Applicabilité

Splunk Enterprise

Description

Environnement : -

Environ 500+ UF 7.1.2 envoyant des événements à 2 indexeurs 7.1.2 qui avec la fonctionnalité de mise en grappe d'index activée via 2 redirecteurs lourds 7.1.2 et 4 têtes de recherche avec mise en grappe SH.

presque tous les serveurs Splunk et UF sont 7.1.2 à l'exception de quelques redirecteurs universels qui sont 6.3.3, 6.4, 7.1.0.

Quelques-uns des membres de SH ont été arrêtés la semaine dernière en raison de l'opt devenant plein.

Maintenant, les SH sont actifs, mais ils affichent l'erreur ci-dessous sur leur interface utilisateur : -

Erreur lors de l'extraction des configurations du capitaine du cluster de tête de recherche ; pensez à effectuer une resynchronisation de configuration destructive sur ce membre de cluster de tête de recherche.

Le cluster de tête de recherche peut ne pas être synchronisé avec les mises à jour de configuration répertoriées par le capitaine pour diverses raisons : les pannes inattendues, les problèmes de réseau et la grande taille de la réplication ne sont que quelques-unes des raisons pour lesquelles nous constatons que ce problème se produit.

En réalité, le membre tente d'appliquer l'ensemble des modifications répliquées du capitaine. Si l'ensemble dépasse les limites de purge et que le membre et le capitaine ne partagent plus de validation commune, un message de bannière apparaît sur l'interface utilisateur du membre, avec un texte similaire à celui-ci :

Error pulling configurations from the search head cluster captain; consider performing a

Résolution

Confirmez que le message suivant s'affiche sur l'interface utilisateur ou dans le fichier splunkd.log :

Erreur lors de l'extraction des configurations du capitaine du cluster de tête de recherche ; pensez à effectuer une resynchronisation de configuration destructive sur ce membre de cluster de tête de recherche.

Vérifiez quel noeud est le capitaine actuel en exécutant la commande suivante à partir du répertoire bin Splunk :

```
./splunk show shcluster-status
```

Une fois que vous confirmez que quel noeud est le capitaine, puis à partir des noeuds qui ne sont pas synchronisés et obtenir les erreurs, exécutez la commande ci-dessous : -

```
./splunk resync shcluster-replicated-config
```

Liens connexes

Documentation Splunk

Effectuez une resynchronisation manuelle :

https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/HowconfrepoworksinSHC#Perform_a_m

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.