Utilisation excessive intermittente du disque sur le capitaine en chef de recherche

Applicabilité

Splunk Enterprise

Description

Dans un cluster de tête de recherche, il a été constaté que l'utilisation du disque dans le système de fichiers utilisé par Splunk lors de la recherche
le capitaine en chef augmentait par intermittence et remplissait presque le système de fichiers, avant de diminuer par la suite,
puis en augmentant à nouveau

Enquête

Plusieurs fichiers .bundle (de réplication) de 2 Go chacun ont été trouvés dans les répertoires suivants

```
/data/splunk/var/run
/data/splunk/var/run/snapshot
```

Une liste de ces fichiers .bundle (tar) contenant des objets de connaissances pour la réplication contenait des fichiers anciens (plus utilisés) volumineux
fichiers de recherche de /data/splunk/etc/users, qui dans ce cas pourraient être supprimés, réduisant ainsi les futures tailles de bundle et
arrêt des pics d'utilisation du disque.

Résolution

De gros fichiers binaires dans etc/apps peuvent causer le même problème. Les binaires ne peuvent pas être supprimés, mais comme ils n'ont pas besoin
être inclus dans les bundles, éviter qu'ils ne soient inclus en les ajoutant à une liste noire via la `strophe [replicationBlacklist] dans distsearch.conf :`

https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Limittheknowledgebundlesize

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.