Intermitterend excessief schijfgebruik op zoekkopkapitein

toepasbaarheid

Splunk Enterprise

Beschrijving

In een zoekkopcluster werd gevonden dat het schijfgebruik in het bestandssysteem dat door Splunk bij de zoekopdracht wordt gebruikt
hoofd kapitein was met tussenpozen toe te nemen en bijna het vullen van het bestandssysteem, voordat vervolgens afnemen,
En dan weer toenemen

onderzoek

Verschillende (replicatie) .bundel bestanden van maximaal 2 GB elk werden gevonden in de volgende directories

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

Een lijst van deze .bundle (tar) bestanden met kennisobjecten voor replicatie bevat oude (niet meer gebruikt) grote
opzoekbestanden van /data/splunk/etc/gebruikers, die in dit geval kunnen worden verwijderd, waardoor toekomstige bundelgroottes en
het stoppen van de pieken in het schijfgebruik.

resolutie

Grote binaries in etc / apps kunnen hetzelfde probleem veroorzaken. De binaries kunnen niet worden verwijderd, maar omdat ze niet nodig zijn
in de bundels worden opgenomen, vermijd ze door ze aan een zwarte lijst toe te voegen via de `stanza [replicationBlacklist] in distsearch.conf:`

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.