Utilizzo eccessivo intermittente del disco sul Capitano della testa di ricerca

Applicabilità

Splunk Enterprise

Descrizione

In un cluster di testine di ricerca, è stato rilevato che l'utilizzo del disco nel file system utilizzato da Splunk nella ricerca
il capo-capitano stava aumentando a intermittenza e quasi riempendo il file system, prima di poi diminuire,
e aumentare di nuovo

Indagine

Diversi file .bundle (di replica) di un massimo di 2 GB ciascuno sono stati trovati nelle seguenti directory

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

Un elenco di questi file .bundle (tar) contenenti oggetti di conoscenza per la replica conteneva vecchi (non più utilizzati) file di grandi dimensioni
ricerca di file da /data/splunk/etc/users, che in questo caso potrebbero essere eliminati, riducendo le dimensioni e
arresto dei picchi di utilizzo del disco.

Risoluzione

Binari di grandi dimensioni in etc/apps possono causare lo stesso problema. Non è possibile eliminare i file binari, ma non è necessario
essere inclusi nei pacchetti, evitare di essere inclusi aggiungendoli a una lista nera tramite
la `stanza [replicationBlacklist] in distsearch.conf:`

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).