

Eliminazione degli errori di sincronizzazione in un ambiente cluster Search Head.

Applicabilità

Splunk Enterprise

Descrizione

Ambiente:

Circa 500+ UF 7.1.2 inviano eventi a 2 indicizzatori 7.1.2 che con funzionalità di clustering dell'indice abilitata tramite 2 inoltri pesanti 7.1.2 e 4 head di ricerca con clustering SSH. quasi tutti i server Splunk e UF sono 7.1.2, ad eccezione di alcuni server d'oltreo universali 6.3.3, 6.4, 7.1.0.

Alcuni membri del team SSH sono stati fermati la settimana scorsa a causa del riempimento /opt.

Ora gli SSH sono attivi ma sull'interfaccia utente viene visualizzato l'errore seguente:-

Errore durante il pull delle configurazioni dal capitano del cluster di testa di ricerca; valutare la possibilità di eseguire una risincronizzazione della configurazione distruttiva su questo membro del cluster head di ricerca.

Il cluster della testa di ricerca può non essere sincronizzato con gli aggiornamenti di configurazione indicati dal capitano per diversi motivi: interruzioni non sospettate, problemi di rete e dimensioni elevate per la replica sono solo alcuni dei motivi per cui questo problema si verifica. In realtà, il membro sta tentando di applicare il set di modifiche replicate dal capitano e, se il set supera i limiti di eliminazione e il membro e il capitano non condividono più un commit comune, nell'interfaccia utente del membro viene visualizzato un messaggio banner, con testo simile al seguente:

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

Risoluzione

Verificare che il seguente messaggio sia visualizzato nell'interfaccia utente o in splunkd.log:

Errore durante il pull delle configurazioni dal capitano del cluster di testa di ricerca; valutare la possibilità di eseguire una risincronizzazione della configurazione distruttiva su questo membro del cluster head di ricerca.

Confermare quale nodo è il capitano corrente eseguendo il seguente comando dalla directory Splunk bin:

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

Una volta confermato che quale nodo è il capitano, quindi dai nodi che non sono sincronizzati e ottenere gli errori, eseguire il seguente comando:-

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

Collegamenti correlati

Documentazione relativa a Splunk

Eseguire una risincronizzazione manuale:

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

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).