

Erros de falta de sincronização em um Ambiente de clustering de Cabeçalho de Pesquisa.

Aplicabilidade

Empresa Splunk

Descrição

Ambiente:-

Cerca de 500+ UF 7.1.2 enviando eventos para 2 indexadores 7.1.2 que com recurso de clustering de índice habilitado via 2 Forwarders pesados 7.1.2 e 4 cabeça de pesquisa com clustering SH.

quase todos os servidores Splunk e UF são 7.1.2, exceto alguns encaminhadores universais que são 6.3.3, 6.4, 7.1.0.

Alguns dos membros do SH foram impedidos na semana passada devido ao fato de o /opt ficar cheio.

Agora os SHs estão ativos, mas estão mostrando o erro abaixo em sua interface do usuário:-

Erro ao extrair configurações do capitão do cluster principal de pesquisa; considere executar uma ressincronização de configuração destrutiva neste membro do cluster de cabeçote de pesquisa.

O Cluster do Cabeçalho de Pesquisa pode ficar fora de sincronia com o que o capitão listou como atualizações de configuração por vários motivos: paralisações não suspeitas, problemas de rede e grande porte para replicação são apenas alguns dos motivos pelos quais podemos ver esse problema ocorrendo.

O que está realmente ocorrendo é que o membro está tentando aplicar o conjunto de alterações replicadas de intervenção do capitão e se o conjunto exceder os limites de purgação e o membro e o capitão não compartilharem mais um comprometimento comum, uma mensagem de banner aparece na interface do usuário do membro, com texto semelhante ao seguinte:

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

Resolução

Confirme se a seguinte mensagem está sendo exibida na interface do usuário ou no splunkd.log:

Erro ao extrair configurações do capitão do cluster principal de pesquisa; considere executar uma resincronização de configuração destrutiva neste membro do cluster de cabeçote de pesquisa.

Confirme qual nó é o capitão atual executando o seguinte comando a partir do diretório Splunk bin:

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

Depois de confirmar que o nó é o capitão, execute o comando abaixo nos nós que estão fora de sincronia e recebendo os erros:-

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

Links relacionados

Documentação do Splunk

Execute uma resincronização manual:

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.