

Pacote distribuído do Replication Manager: O diretório do pacote atual contém um arquivo de pesquisa grande que pode causar falha na replicação do pacote

Aplicabilidade

Splunk Enterprise Splunk Cloud

Descrição

A seguinte mensagem é exibida na guia Mensagens na UI:

```
Distributed Bundle Replication Manager: The current bundle directory contains a large lo
The path to the directory is /opt/splunk/var/run/<cloudstack>.splunkcloud.com-1573504421
```

Investigação

Localize arquivos maiores que 500 MB usando o seguinte comando:

```
find /opt/splunk/etc -type f -size +500M -exec ls -lh {} \;
```

Se os arquivos existirem acima de 500 MB, é recomendável adicioná-los à replicationDenyList se eles não forem necessários no indexador para satisfazer a pesquisa. Use o nome da pesquisa (excluindo o caminho completo e .csv) e use-o neste comando btool para procurar instâncias da pesquisa existente em props.conf:

```
splunk btool props list --debug | grep -i <lookup>
```

Se a pesquisa for chamada no props.conf, talvez ela seja necessária para satisfazer as pesquisas. Procure alternativas como [migração de pesquisas para o KVStore](#)

Resolução

Como recusar a lista

A lista de negação deve ser aplicada no cabeçalho de pesquisa em distsearch.conf

A estrofe [replicationDenylist] na versão padrão do sistema de distsearch.conf negará todos os arquivos .csv especificados

Isso é mais útil para limitar o tamanho do pacote de conhecimento, especialmente no caso de arquivos muito grandes que não precisam ser replicados para os peers de pesquisa. A lista de negação tem precedência sobre qualquer lista de permissão.

A seguir, está um exemplo:

```
[replicationDenylist]
my_lookup = apps/search/lookups/my_lookup.csv
```

Como alterar o aviso:

Aumentando o número padrão do aviso (Não recomendado)

Essa opção serve apenas para eliminar a mensagem de aviso. Se o arquivo continuar crescendo, a replicação para os indexadores pode começar a falhar. O resultado final é o Splunk usando pacotes desatualizados que podem levar a erros de aplicativo não encontrado (código de saída=111) e muito mais.

Como fazer isso

Antes de alterar algo, certifique-se de fazer um backup dos arquivos Splunk com as melhores práticas aqui: [Configurações de backup](#)

1. Obtenha acesso ao CLI
2. Mover para /opt/splunk/etc/system/local/
3. Edite o arquivo distsearch.conf
4. Adicione o seguinte

```
[replicationSettings]
concerningReplicatedFileSize = 2000
maxBundleSize = 4096
```

5. Salve e reinicie o para aplicar as alterações.

Links relacionados

Documentação do Splunk
Modificar o pacote de conhecimento

[Limitar o tamanho do pacote de conhecimento](#)

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.