

分散バンドルレプリケーションマネージャ：現在のバンドルディレクトリには、バンドルレプリケーションの失敗を引き起こす可能性のある大きな参照ファイルが含まれています

適用性

SplunkエンタープライズSplunkクラウド

説明

UIの[メッセージ]タブに次のメッセージが表示されます。

```
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
```

調査

次のコマンドを使用して、500MBを超えるファイルを検索します。

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

500 MBを超えるファイルが存在する場合、インデクサで検索を満たす必要がない場合は、`replicationDenyList`に追加することをお勧めします。ルックアップ名（フルパスと.csvを除く）を取得し、この**bttool**コマンドでを使用して、`props.conf`に存在するルックアップのインスタンスを検索します。

```
splunk bttool props list --debug | grep -i
```

バックアップがprops.confで呼び出される場合、検索を満たすために必要になる場合があります。「[参照のKVStoreへの移行](#)」などの代替方法を検討します。

解決方法

denylistの方法

denylistは、distsearch.confの検索ヘッドに適用する必要があります

システムデフォルトバージョンのdistsearch.confの[replicationDenylist]スタanzasは、指定されたすべての.csvファイルを拒否します

これは、特に検索ピアに複製する必要がない非常に大きなファイルの場合に、ナレッジバンドルのサイズを制限する場合に最も役立ちます。拒否リストは、許可リストよりも優先されます。

次に例を示します。

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

警告を変更する方法：

警告のデフォルト値を増やす（推奨しません）

このオプションは、警告メッセージを取り除くためだけのものです。ファイルが増え続けると、インデクサへのレプリケーションが失敗する可能性があります。その結果、Splunkは古いバンドルを使用するため、アプリケーションが見つからない（終了コード=111）などのエラーが発生する可能性があります。

その方法

何かを変更する前に、以下のベストプラクティスを使用してSplunkファイルのバックアップを作成してください。[バックアップ設定](#)

1. CLIへのアクセス
2. /opt/splunk/etc/system/local/に移動します。
3. distsearch.confファイルを編集します
4. 次を追加

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

5.変更を適用するには、保存して再起動します。

関連リンク

Splunkドキュメント
ナレッジバンドルの変更

[知識のバンドル化を制限する](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。