搜索头上断断续续的过度磁盘使用

适用范围

Splunk企业

描述

在搜索头群集中，发现Splunk在搜索中使用的文件系统中的磁盘使用情况
机长间歇地增加，几乎填满文件系统，然后逐渐减少，
然后再次增加

调查

在以下目录中找到几个（复制）大小最高为2 GB的.bundle文件

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

包含用于复制的知识对象的这些.bundle(tar)文件的列表包含旧的（不再使用）大文件
从/data/splunk/etc/users查找文件，在这种情况下，可以删除这些文件，从而减少将来的捆绑包大小和
停止磁盘使用率峰值。

分辨率

etc/apps中的大型二进制文件可能导致相同的问题。无法删除二进制文件，但是它们不需要
包含在捆绑包中，通过以下方式将其添加到黑名单来避免包含它们：
distsearch.conf中的 `[replicationBlacklist] stanza:`

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。