

tstats search with large lookup as sub-search failed with error "exit with code 255" (将大型查找作为子搜索的tstats搜索失败，错误为“exit with code 255”)

适用范围

Splunk Enterprise Splunk Search Splunk Subsearch Splunk tstats

描述

在tstats命令的where子句中使用子搜索时，如果搜索过大（看起来超过5,000行），搜索将失败并引发错误：

搜索进程未干净退出，exit_code=255, description="exit with code 255"。请在“作业检查器”中的search.log中查找此对等体以了解详细信息。

```
| tstats count from datamodel=Web where NOT  
[| inputlookup lookup.csv  
| fields dest  
| rename dest as Web.dest  
| format ] by Web.src Web.dest
```

在此示例中，lookup_name.csv有大约110k行。

调查

当搜索失败并出现以下错误时。

```
[<INDEXER_NAME>] Search process did not exit cleanly, exit_code=255, description="exited
```

该错误消息意味着索引器INDEXER_NAME上的搜索过程出现了问题 — 在大多数情况下，搜索过程会崩溃（或中断）。

如果没有crash.log，则意味着该splunk已在外部被终止，或者我们在保存crash.log时遇到问题。但是，查看搜索字符串（OR数） — 它极有可能由于递归而造成堆栈溢出。

分辨率

递归可能会导致崩溃（即，包含大量或/和搜索的无效搜索字符串），这是一个已知问题

[SPL-144975跟踪器：Splunk的重新设计部分并删除递归](#)

解决此问题的一种方法是增加堆栈的极限值，默认值为8064，而增强值（如128k或256k）可以解决此问题。

相关链接

[SPL-144975：重新设计Splunk零件并删除递归](#)

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）。