splunk由于splunkd.log中的“系统中打开的文件太多”消息而崩溃。

适用范围

Splunk企业

描述

由于splunkd.log中的“ Too many open files in system”消息，Splunk 间歇性崩溃。

splunkd.log中的日志示例：

```
ERROR ProcessRunner - child's last words: ^@^@^@^@cannot create a pipe: Too many open fi
ERROR ProcessRunner - parent/child protocol error: read reply from child "s" (ASCII 0x73
ERROR ProcessRunner - parent/child protocol error: read reply from child "t" (ASCII 0x74
ERROR ProcessRunner - parent/child protocol error: read reply from child "e" (ASCII 0x65
ERROR ProcessRunner - parent/child protocol error: read reply from child "m" (ASCII 0x6D
FATAL ProcessRunner - Unexpected EOF from process runner child!
```

调查

在系统级别检查打开的文件后，每次崩溃时显示的打开文件接近8k，打开文件的硬限制从4096增加到64000。 打开文件的ulimit值反映在splunkd .log中，如下所示。

```
INFO  ulimit - Limit: open files: 64000 files
INFO  ulimit - Limit: open files: 64000 files
```

Splunk在接近8k打开的文件中不断崩溃。

在内核级别上检查了“file-max”，在本例中将其配置为8192，这是在内核级别上实施的最大文件描述符(FD)，请使用下一命令验证此值：

```
$ cat /proc/sys/fs/file-max
8192
```

分辨率

要解决此问题，需要增加file-max，请使用以下命令：

```
sysctl -w fs.file-max=64000
```

然后重新启动系统。

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）。