

Splunk转发器未向Splunk云发送事件

适用范围

Splunk云

描述

Splunk转发器不再向Splunk Cloud发送事件。这可能会影响通用转发器、重型转发器或中间转发层。

splunkd.log中出现以下错误：

```
ERROR TcpOutputFd - Connection to host=1.22.122.222:9997 failed. sock_error = 104. SSL Error = No error
```

sock_error = 104消息表明当转发器尝试与Splunk云接收终端通信时，TCP连接已重置。

调查

验证从受影响转发器到Splunk云输入终端的基本网络连接：

```
telnet inputs1.<stack_id>.splunkcloud.com 9997
```

成功建立telnet连接可确认该端口可访问。但是，它不会完全验证SSL/TLS连接或确认中间网络设备未重置流量。

要进一步验证连接，请从受影响的转发器运行以下命令之一：

```
openssl s_client -connect inputs1.<stack_id>.splunkcloud.com:9997
```

或者

```
$SPLUNK_HOME/bin/splunk cmd openssl s_client -connect inputs1.<stack_id>.splunkcloud.com
```

如果返回以下输出，连接将被重置：

```
CONNECTED(00000003)  
write:errno=104
```

这确认转发器最初可以建立TCP连接，但连接在SSL/TLS会话完成之前被强制关闭。

另请查看受影响的转发器上的转发配置（包括`outputs.conf`），以确认转发器正在使用正确的Splunk云接收端点和端口。

分辨率

错误104是ECONNRESET，这意味着“连接由对等体重置”。这表示使用TCP重置数据包强制关闭连接。重置可以由目标终端或中间网络设备（例如防火墙、代理、负载均衡器、IDS/IPS、SSL检查设备或网络设备）发送。

查看受影响转发器和Splunk云之间的完整网络路径。确认：

- 端口9997上允许到Splunk云输入终端的出站流量。
- 防火墙、代理或网络设备未重置TCP会话。
- SSL检查不会干扰Splunk转发连接。
- 会检查任何最近的网络、防火墙、代理、路由或与证书相关的更改。
- Splunk云转发器应用和证书是最新且正确部署的。
- 中间转发器可以与Splunk云通信，不会丢弃或阻止转发流量。

纠正网络、防火墙或证书配置后，根据需要重新启动受影响的转发器，或允许它自动重新连接。然后确认事件已在Splunk云中成功建立索引。

相关链接

[Linux ARM通用转发器和Splunk云的连接问题（SSL错误）](#)

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）。