将部署从FMC升级到FTD失败后的SFTUNNEL通信问题故障排除

目录

问题

尝试将部署推送到多个防火墙威胁防御(FTD)设备失败，部署失败发生率介于8%和20%之间。FMC日志未提供导致这些失败的明确原因。

环境

- 思科安全防火墙Firepower(FMC)
- FMC和FTD通过MPLS路径通信
- FMC和FTD之间的sftunnel/管理流量不进行防火墙检查
- FMC和FTD之间足够的带宽用于安全隧道通信
- 已注意到部署故障

分辨率

此工作流提供全面而详细的过程，用于标识并解决与sftunnel进程通信问题相关的从FMC到FTD设备的部署故障。每个步骤都详细介绍，包括示例命令输出作为说明。

以超级根用户身份访问FTD CLI

要执行高级诊断和流程操作，请登录FTD设备CLI并将权限提升到root。

```
> expert
device$ sudo su
Password:
root@device:/Volume/home/admin#
```

检查FTD sftunnel状态

运行`sftunnel_status.pl`脚本以检查sftunnel进程的运行状况和通信状态。

```
root@device:/Volume/home/admin# sftunnel_status.pl
OR
root@device:/Volume/home/admin# sftunnel_status.pl PEERIPADDRESS
```

```
OR
root@device:/Volume/home/admin# sftunnel_status.pl PEERUUID
```

指示RPC状态故障的示例输出：

```
peer UUID did not reply at /ngfw/usr/local/sf/bin/sftunnel_status.pl line 309.
Retry rpc status poll at /ngfw/usr/local/sf/bin/sftunnel_status.pl line 315.
**RPC STATUS****PEERIP*************
RPC status :Failed
**RPC STATUS****PEERIP*************
RPC status :Failed
```

确保最近没有对FMC或FTD管理进行IP地址或网络更改，因为这需要手动更改FMC System / Configuration / Management Interfaces页面或FTD CLISH上的IP地址，具体取决于需要更改的设备。

FTD CLISH上的管理IP地址更改示例：

```
> configure network ipv4 manual IPADDRESS NETMASK GATEWAYIP
> show network
```

确定sftunnel进程的当前进程ID(PID)

要监控和验证sftunnel进程，请使用pmtool检索其PID。

```
root@device:/Volume/home/admin# pmtool status | grep sftunnel
```

示例输出：

```
sftunnel      Running     PID: 12345
```

重新启动sftunnel进程并验证PID更改

重新启动sftunnel进程以重置其通信状态。重新启动后，重新运行PID检查以确认新进程处于活动状态。

```
root@device:/Volume/home/admin# pmtool restartbyid sftunnel
```

在短暂时间段后，再次检查进程状态：

```
root@device:/Volume/home/admin# pmtool status | grep sftunnel
```

示例输出（PID必须与之前的不同）：

```
sftunnel      Running     PID: 67890
```

等待2分钟，使sftunnel流程稳定并尝试从FMC到受影响的FTD进行新部署

请等待大约两分钟，以便sftunnel进程完全重新初始化并重新建立通信。然后，启动从FMC到FTD的新部署。

部署脚本示例：

```
===============TRANSACTION INFO===============
Device UUID: PEERUUID
Transaction ID: 4075925334520
Selected policy group list: Access Control Policy, Intrusion Policy, Network Analysis Policy, Intrusion
Out-of-date policy group list: Access Control Policy, Intrusion Policy, Network Analysis Policy, Intrus
Deployment Type: Full Deployment
================================================================
```

如果成功，部署完成时不会出现错误，并且策略会在FTD上更新。

重新启动后验证sftunnel和RPC通信

成功部署后，再次使用`sftunnel_status.pl`确认sftunnel进程和RPC状态正常。

```
root@device:/Volume/home/admin# sftunnel_status.pl
```

表示成功的示例输出：

```
**RPC STATUS****PEERIP*************
  'ipv4_1' => 'PEERIP',
  'uuid' => 'PEERUUID',
  'ipv6' => 'IPv6 is not configured for management',
```

```
  'active' => 1,
  'ip' => 'PEERIP',
  'last_changed' => 'Thu Nov 13 23:22:43 2025',
  'name' => 'PEERNAME',
  'uuid_gw' => ''
```

对所有受影响的FTD重复sftunnel重新启动过程

如果多个FTD受到影响，请对每个受影响的设备执行上述步骤以恢复部署功能。

带宽和连接验证

运行bandwidth_analyzer.pl —size SIZEINMB -p PEERIP，确保FMC和FTD之间具有足够的带宽和基本网络连接。思科文档建议至少使用5 Mbps的吞吐量来实现稳定的管理连接。

带宽分析输出示例：

```
======== Bandwidth Analysis Result  ========
$VAR1 = {
          'PEERIP' => [
                                {
                                  'download' => '3.81 Mbps'
                                },
                                {
                                  'upload' => '4.24 Mbps'
                                },
                                {
                                  'rpcStatus' => 'Up'
                                }
                              ]
        };
```

原因

部署失败的根本原因可能是由于：

- 特定FTD或FMC设备上的sftunnel进程故障。
- 对管理TLS流量的干扰（例如来自中间防火墙检查的干扰），导致对RPC状态检查的错误响应。
- 网络更改（例如IP地址更改、迁移或添加设备），导致设备之间无法连通。

在受影响的FTD/FMC上重新启动sftunnel进程可以恢复正确的通信并允许从FMC成功部署策略。

否则，请通过验证IP地址和明确的网络路径来确保设备之间的正确连接。

相关内容

- 思科技术支持和下载

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）。