排除ISE 3.4 VPN和RADIUS身份验证故障

目录

问题

当辅助管理节点(SAN)出现故障时，ISE 3.4补丁4部署会遇到身份验证故障。定向到主策略管理节点(PPAN)的身份验证请求也会失败，导致ASA VPN连接和RADIUS身份验证中断。SAN节点在ISE部署控制面板中显示为已断开连接，并且日志指示EAP/TLS相关的错误和会话跟踪问题。

环境

- 思科身份服务引擎(ISE)
- 网络接入设备(NAD):包括Meraki设备和/或ASA防火墙
- 拓扑：使用SAN和PPAN的多节点ISE部署

分辨率

1. — 导航到Administration > System > Deployment，通过Cisco ISE管理界面从SAN节点删除所有角色。这会停止对故障节点的身份验证尝试，并允许未受影响的节点恢复处理。

注意：删除角色后，SAN节点在部署控制面板中继续显示为已断开连接（红色X）。

---

2. — 手动强制ASA防火墙将SAN节点视为FAILED，从而阻止进一步的身份验证尝试被定向到不可用的SAN。此操作在ASA配置上执行，确保故障切换到正常运行的ISE节点。

3. — 检查ISE部署是否正确同步，并监控运行状况指标，包括CPU、内存和磁盘利用率。

4. — 通过检查新的Dot1x和RADIUS请求是否由不受影响的ISE节点处理，验证身份验证服务是否正常运行。

5. — 在身份验证失败期间收集DEBUG日志和数据包捕获，以分析EAP/TLS协商计时和会话重置。

6. — 在SAN故障切换事件后，继续监控ISE系统运行状况指标和身份验证行为。

7. — 验证Meraki RADIUS故障切换行为，注意ISE不支持用于服务器可用性检测的“Status-Server”RADIUS数据包。

日志消息示例

```
Accounting start was received for non-existing session
```

```
Error getting peer certificate from SSL Connection
```

```
packet for this endpoint 58-6D-67-XX-XX-XX is being processed right now so drop the new EAP session
```

```
Long step latency ;2=57290
```

```
Endpoint 58-6D-67-XX-XX-XX abandoned EAP session xxxxxxxxx/552628443/4183334 and started EAP session
```

原因

根本原因是ISP链路故障导致SAN节点中断，从而导致会话跟踪不一致以及Supplicant客户端、NAD和ISE节点之间的EAP/TLS协商错误。此外，Meraki设备依靠“Status-Server”RADIUS数据包进行故障切换检测，而Cisco ISE不支持该检测，从而导致对发生故障的SAN节点的持续身份验证尝试。

相关内容

- 如何：将Meraki网络与ISE集成
- 在ISE和组策略映射上配置具有RADIUS身份验证的远程访问VPN
- 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）。