故障排除"5440终端已放弃EAP会话并已启动新"由于请求方超时或配置错误

目录

问题

ISE向终端发送RADIUS访问质询。终端不再响应访问质询，而是重复重新启动身份验证过程。思科身份服务引擎(ISE)的终端身份验证最终失败，出现错误。

"5440 – Endpoint abandoned EAP session and started new"

环境

- 思科ISE
- 802.1X身份验证
- 有线或无线网络
- 基于可扩展身份验证协议(EAP)的身份验证
- 终端请求方

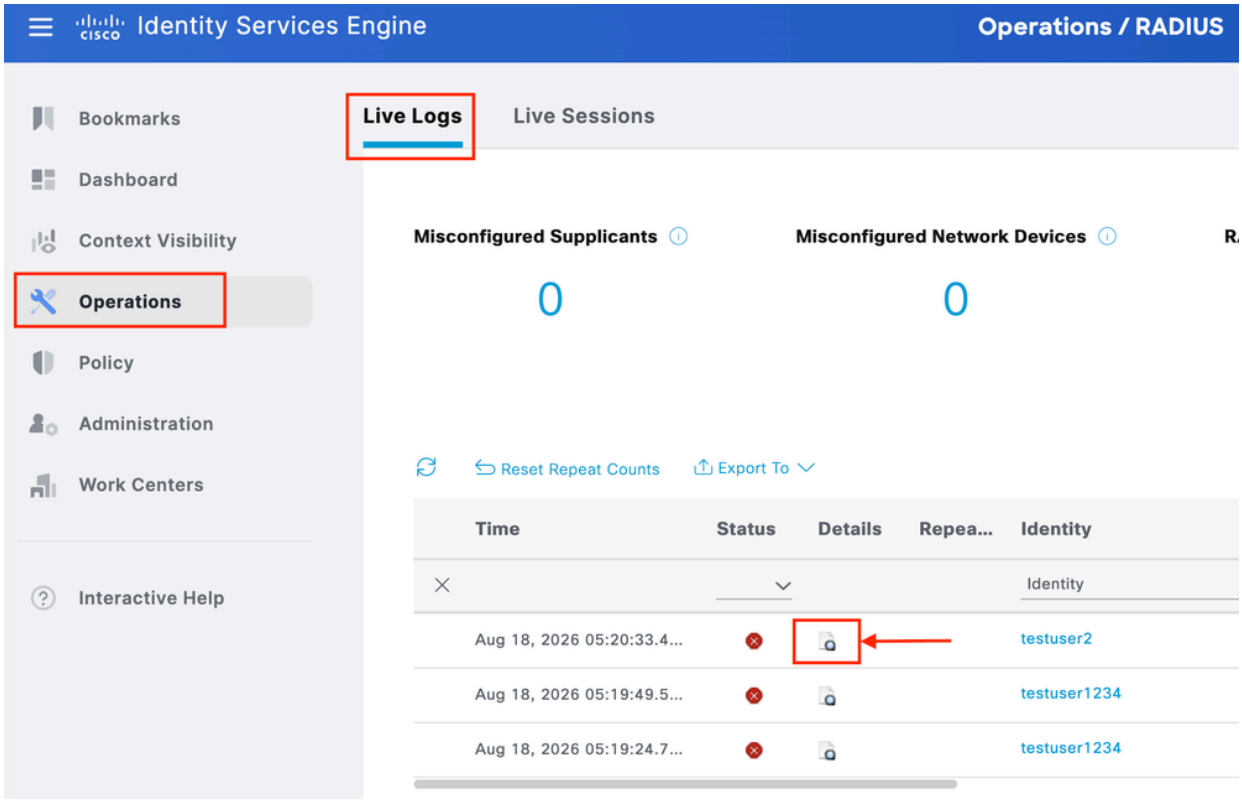
分辨率

使用以下步骤进行故障排除：

1. 检查ISE身份验证详细信息

1. 导航到操作> RADIUS >实时日志。

2. 打开失败的身份验证。



3. 验证ISE是否发送“Access-Challenge”。

4. 确认终端发送新的“Access-Request”而不是响应质询。

5. 记下Access-Challenge与新访问请求之间的时间。

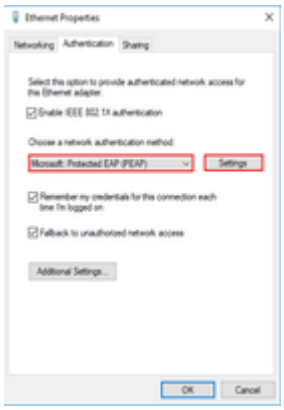
6. 在此映像中，我们可以看到ISE发送“Access-Challenge”，但ISE未收到任何响应。

Cisco Identity Services Engine

11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	1
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	0
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	1
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	1
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
5440	Endpoint abandoned EAP session and started new	58134

2. 验证终端请求方配置

- 确认配置了正确的EAP方法。
- 验证身份验证模式，例如计算机、用户或计算机+用户身份验证。



- 检查请求方超时并重试设置。
- 验证终端是否使用预期的802.1X配置文件。
- 将配置与工作终端进行比较。

3. 检查终端日志

- 查看操作系统和请求方身份验证日志。
- 检查请求方是否收到EAP请求。
- 确定任何超时、身份验证重新启动或EAP相关错误。
- 如果使用Cisco Secure Client，请收集DART捆绑包以进行进一步分析。
    - 收集安全客户端的DART捆绑包

4. 检查网络路径

- 在终端(Wireshark)、NAD（SPAN捕获）和ISE(TCPDump)上同时捕获数据包
- 检验EAPOL流量是否到达NAD。
- 验证来自ISE的RADIUS响应是否到达NAD。

- 检查终端、NAD和ISE之间的数据包丢失或延迟。
- 当终端日志无法识别重启原因时，请使用数据包捕获。

5. 请比较工作端点

- 尽可能使用相同的NAD、ISE PSN和身份验证策略。
- 比较EAP方法、请求方配置、超时值和身份验证顺序。
- 如果只有特定终端失败，则将调查重点放在终端配置或请求方上。

要验证问题是否已解决，请执行新的身份验证并验证终端是否响应ISE访问质询，并成功完成身份验证而不生成5440。

原因

终端请求方未在配置的超时时间内完成EAP身份验证，或者使用的802.1X配置不正确。短暂的请求方超时、不正确的EAP设置或请求方问题可能导致终端在上一个会话完成之前重新启动身份验证。

相关内容

- 了解和配置EAP-TLS

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）。