

由于客户端抑制和软件缺陷，ISE 3.2 MDM合规性查询失败

目录

问题

某些终端在思科身份服务引擎(ISE)上通过EAP-TLS进行身份验证，即使它们在Intune控制面板中显示为合规状态，也会间歇性地从Microsoft Intune接收合规状态。因此，这些终端会达到默认无线授权策略，而不是预期的状况合规或状况不合规策略。受影响的终端不会在ISE实时日志或外部MDM报告中显示移动设备管理(MDM)合规性属性，并且该问题仅影响部署中的客户端子集。

观察到的具体症状包括：

- 异常客户端在外部移动设备管理报告中的ISE报告中没有日志。
- 异常客户端在实时日志详细信息中没有诸如MDM合规状态或设备合规状态之类的属性。
- 异常客户端命中无线802.1x_EAP-TLS_toyotawifi授权策略而不是状态合规策略。
- 日志中的错误消息显示“无法连接到MDM服务器：404 Not Found”。

环境

- 思科ISE多节点集群版本3.2补丁6
- 集群中的8个ISE节点，全部显示绿色状态
- 与Microsoft Intune集成的11,000个无线/有线客户端
- 客户端使用EAP-TLS（计算机证书）身份验证
- ISE使用客户端的MAC地址进行Intune查询
- 所有客户端在Microsoft Intune控制面板上都具有合规状态
- 问题影响某些客户端，但不是所有客户端

分辨率

通过上述步骤解决了此问题。

步骤 1：确定根本原因

对ISE日志的分析显示，受影响的终端具有过时的MDM服务器ID，无法执行MDM查询。

日志显示：

```
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MDMUtil -:::- M
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MdmServersCache -
2026-06-15 13:35:14,344 ERROR [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.pip.MdmPartnerPIPHandl
```

此外，发现部署遇到思科漏洞ID CSCwv51917，这会影响使用MAC地址时的MDM服务器ID过时的MDM合规性查找。

步骤 2：临时解决方法

作为临时解决方法：

1. — 从情景可视性中删除终端并重新进行身份验证。发现此错误是为了解决查询MDM服务器和获取合规性状态的问题。
2. — 导航到Context Visibility。
3. — 选择终端mac地址并将其删除。
4. — 重新验证终端。

步骤 3：永久解决方案 — 软件升级

永久解决方案在Cisco Bug ID CSCwv51917 (仅限注册用户) 下跟踪。

原因

在身份验证期间，ISE尝试查询过时的MDM服务器引用，但相应的MDM服务器对象不再存在或处于非活动状态。因此，ISE不会从Intune检索MDM合规性属性。

相关内容

- [思科漏洞ID CSCwv519173134](#)
- [ISE 3.2版本说明 — 已解决的警告](#)
- [ISE 3.2生命周期终止通知](#)
- [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）。