

ISE RCM功能导致基于证书的身份验证期间删除终端

目录

问题

在从JAMF迁移到Intune MDM for macOS设备期间，思科ISE会意外删除或合并终端记录，并在EAP-TLS身份验证期间更改终端身份组分配。

受影响的终端从DB_Authorized_Devices身份组移动到Profiled触发CoA事件，原因为“删除终端”。这会导致终端从ISE内部数据库中删除，并导致受影响设备的身份验证中断。当设备使用包含主题备用名称(SAN)URI字段的相同证书在无线和有线连接之间切换时，会出现此问题，ISE将此类字段解释为随机和更改MAC(RCM)功能的GUID。

环境

- 思科身份服务引擎(ISE)版本3.2
- 使用EAP-TLS身份验证的MACos终端
- 使用包含设备标识符的SAN URI字段进行基于证书的身份验证
- 在无线和有线网络连接之间切换的设备
- MDM从JAMF迁移到Microsoft Intune
- ISE 3.2中默认启用RCM (随机和更改MAC) 功能
- 通过具有自定义属性的REST API管理的终端

分辨率

此问题由ISE 3.2中的RCM功能引起，该功能根据证书SAN URI字段合并终端记录。有两个分辨率选项可用。

选项 1：禁用RCM功能（建议小心使用）

步骤 1：访问ISE Swagger API接口

导航到Administration > Settings > API Settings，然后单击/swagger-ui链接。

步骤 2：检查当前LSD设置

在Swagger界面中，查找LSD Settings并执行GET请求以查看当前配置：

```
GET /api/v1/lsd/settings
```

步骤 3：修改RCM设置

使用此请求正文执行PUT请求以禁用RCM:

```
{
  "enableEPO": true,
  "enableRCM": false
}
```

步骤 4：检验配置更改

再次执行GET请求以确认RCM已禁用且LSD保持启用状态。

步骤 5：执行清理脚本

在RCM禁用后运行建议的脚本操作以修复属性差异。监控此过程中任何角落案例的基础设施。



警告：有可能。此处提到的详细信息似乎包含执行后可能会产生重大影响的过程或命令。请确保SME或业务部门在执行或建议之前已评估程序或命令。

选项 2：修改授权策略

通过为有线和无线身份验证流创建单独的授权逻辑，调整策略集以考虑RCM行为，确保合并的终端根据连接类型而不是仅根据身份组成员资格接收适当的访问决策。

证书SAN URI处理

ISE使用特定逻辑处理证书SAN URI字段以提取GUID。对于包含Microsoft Entra ID段的证书，ISE使用regex模式删除临时身份段：

```
tag:[a-zA-Z0-9.,-]+:sid:S-[0-9-]+[:,:]?
```

SAN URI处理示例：

- 输入："ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482"
- 存储在会话中："ID:Meraki:GUID:673288144292101809"

原因

ISE 3.2中默认启用的RCM (随机和更改MAC) 功能将证书SAN URI字段解释为用于终端识别的GUID。当使用相同证书的设备通过无线和有线接口连接时，RCM会根据共享GUID合并终端记录。在此合并过程中，无线终端的属性会迁移到有线终端，并且无线MAC条目会从终端数据库中删除。此行为发生在CoA或DHCP探测之前，会导致丢失最初通过REST API配置的自定义属性和身份组分配。合并进程不会保留不属于分析策略的自定义属性，从而导致终端身份重置和后续身份验证失败。

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）。