

ISE RCM功能在基於證書的身份驗證期間導致終端刪除

目錄

問題

在從JAMF遷移到Intune MDM for macOS裝置期間，思科ISE會意外刪除或合併終端記錄，並在EAP-TLS身份驗證期間更改終端身份組分配。

受影響的端點從DB_Authorized_Devices身份組移動到Profiled，觸發CoA事件，原因為「刪除端點」。這會導致終端從ISE內部資料庫中刪除，並導致受影響裝置的身份驗證中斷。當裝置使用包含主體備用名稱(SAN)URI欄位的同一證書在無線和有線連線之間切換時，會出現此問題，ISE將此類欄位解釋為隨機和更改MAC(RCM)功能的GUID。

環境

- 思科身分識別服務引擎(ISE)版本3.2
- 使用EAP-TLS身份驗證的MACos端點
- 使用包含裝置識別符號的SAN URI欄位進行基於證書的身份驗證
- 在無線和有線網路連線之間切換的裝置
- MDM從JAMF遷移到Microsoft Intune
- ISE 3.2中預設啟用RCM (隨機和更改MAC) 功能
- 通過具有自定義屬性的REST API管理的終端

解析

此問題是由ISE 3.2中的RCM功能引起的，該功能根據證書SAN URI欄位合併終端記錄。有兩種解析度選項可用。

選項 1:禁用RCM功能 (建議小心使用)

步驟 1:訪問ISE Swagger API介面

導航到Administration > Settings > API Settings，然後按一下/swagger-ui連結。

步驟 2:檢查當前LSD設定

在Swagger介面中，查詢LSD Settings並執行GET請求以檢視當前配置：

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

步驟 3:修改RCM設定

使用此請求正文執行PUT請求以禁用RCM:

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

步驟 4:驗證配置更改

再次執行GET請求以確認RCM已禁用並且LSD保持啟用狀態。

步驟 5:執行清理指令碼

在RCM禁用後運行建議的指令碼操作來修復屬性差異。在此過程中，監控基礎架構是否有任何拐角案例。



注意：有可能。此處提到的詳細資訊似乎包含執行後可能會產生重大影響的過程或命令。請確保程式或命令已由SME或業務單位評估，然後執行或推薦。

選項 2:修改授權策略

通過為有線和無線身份驗證流建立單獨的授權邏輯，調整策略集以考慮RCM行為，確保合併的終端接收基於連線型別而不是單獨身份組成員資格的相應訪問決策。

憑證SAN URI處理

ISE使用特定邏輯處理證書SAN URI欄位以提取GUID。對於包含Microsoft Entra ID段的證書，ISE使用regex模式刪除臨時身份段：

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

SAN URI處理示例：

- 輸入："ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482"
- 儲存在會話中："ID:Meraki:GUID:673288144292101809"

原因

ISE 3.2中預設啟用的RCM (隨機和更改MAC) 功能將證書SAN URI欄位解釋為GUID用於終端標識。當使用相同證書的裝置同時通過無線和有線介面連線時，RCM會根據共用GUID合併終端記錄。在此合併過程中，無線端點的屬性將遷移到有線端點，並且從端點資料庫中刪除無線MAC條目。此行為發生在CoA或DHCP探測之前，會導致丟失最初通過REST API配置的自定義屬性和身份組分配。合併進程不會保留不屬於分析策略的自定義屬性，從而導致端點身份重置和後續身份驗證失敗。

相關內容

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。