排除ISE 3.4 VPN和RADIUS身份驗證故障

目錄

問題

ISE 3.4補丁4部署在輔助管理節點(SAN)出現故障時會發生身份驗證失敗。定向到主策略管理節點(PPAN)的身份驗證請求也會失敗，導致ASA VPN連線和RADIUS身份驗證中斷。SAN節點在ISE部署控制面板中顯示為已斷開連線，日誌顯示EAP/TLS相關錯誤和會話跟蹤問題。

環境

- 思科身分識別服務引擎(ISE)
- 網路存取裝置(NAD):包括Meraki裝置和/或ASA防火牆
- 拓撲：採用SAN和PPAN的多節點ISE部署

解析

1. — 導航到Administration > System > Deployment，通過思科ISE管理介面從SAN節點刪除所有角色。這將停止對故障節點的身份驗證嘗試，並允許未受影響的節點恢復處理。

附註：在刪除角色後，SAN節點在部署控制面板中繼續顯示為已斷開連線（紅色X）。

---

2. — 手動強制ASA防火牆將SAN節點視為FAILED（失敗），以防止進一步身份驗證嘗試被定向到不可用的SAN。此操作在ASA配置上執行，確保故障轉移到可運行的ISE節點。

3. — 檢查ISE部署是否正確同步，並監控運行狀況指標，包括CPU、記憶體和磁碟利用率。

4. — 檢查新的Dot1x和RADIUS請求是否由不受影響的ISE節點處理，驗證身份驗證服務是否正常運行。

5. — 在身份驗證失敗期間收集DEBUG日誌和資料包捕獲，以分析EAP/TLS協商計時和會話重置。

6. — 在SAN故障切換事件之後，繼續監視ISE系統運行狀況指標和身份驗證行為。

7. — 驗證Meraki RADIUS故障轉移行為，注意ISE不支援「Status-Server」 RADIUS資料包進行伺服器可用性檢測。

日誌消息示例

```
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

根本原因是因為ISP鏈路故障而導致SAN節點中斷，從而導致會話跟蹤不一致以及請求方、NAD和ISE節點之間的EAP/TLS協商錯誤。此外，Meraki裝置依靠「Status-Server」RADIUS資料包進行故障切換檢測，而Cisco ISE不支援該功能，從而導致對出現故障的SAN節點的持續身份驗證嘗試。

相關內容

- 如何：將Meraki網路與ISE整合
- 在ISE和組策略對映上配置具有RADIUS身份驗證的遠端訪問VPN
- 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）。