排除會話重新身份驗證後未觸發的ISE無代理狀態故障

目錄

問題

身份服務引擎(ISE)3.3中的無代理狀態功能在會話重新身份驗證事件後無法觸發。在初始身份驗證期間，無代理狀態工作正常，端點變得合規。但是，發生重新驗證時，端點會收到RADIUS記帳臨時更新事件而不是記帳開始事件，從而導致不呼叫無代理狀態流。因此，終端匹配未知的終端安全評估策略並保持未知的終端安全評估狀態，從而影響受影響裝置的網路訪問。

問題顯現為，重新身份驗證後，終端處於「狀態暫掛」或「未知」狀態，在報告環境中1200個終端中有大約800個受到影響。日誌分析顯示，在重新身份驗證期間，ISE接收具有agentlessEnabled=true的ACCOUNTING_UPDATE事件，但不會針對現有會話ID重新呼叫狀態流。

環境

- 身分識別服務引擎(ISE)版本3.3補丁4
- 採用MAC驗證略過(MAB)的有線802.1X驗證
- 已啟用無代理狀態配置
- 已配置會話重新身份驗證計時器（420秒超時）
- 用作網路接入裝置的Cisco Catalyst交換機
- 環境中約有1200個端點

解析

此行為在ISE中設計為預期行為。無代理狀態僅由RADIUS Accounting Start事件觸發，並且當已框架的IP地址保持不變時，不會在會話重新身份驗證期間由記帳臨時更新事件重新呼叫。

技術分析

ISE NetAccessEventHandler代碼路徑僅在新的RADIUS Accounting-Start資料包上重新處理無代理狀態流。在重新身份驗證期間，網路裝置通常使用相同的Acct-Session-Id傳送Accounting Interim-Update資料包，這會導致shouldInvokePostureFlow()函式返回false，從而阻止狀態重新評估。

記錄顯示行為的證據：

初始身份驗證（無代理狀態觸發）：

```
2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle

2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

重新身份驗證（未觸發無代理狀態）：

```
2026-04-01 11:35:37,669 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

建議的解決方法

要緩解此行為的影響，請配置終端安全評估租賃設定以在重新身份驗證方案期間保持終端合規性：

步驟 1:在ISE終端安全評估策略中配置適當的終端安全評估租用持續時間，以確保終端在終端安全評估之間不會丟失網路訪問。

步驟 2:根據組織的安全要求和重新身份驗證頻率，監控終端安全狀態並調整租用計時器。

原因

此行為預期記錄在Cisco錯誤ID CSCwu48086中。ISE中的無代理狀態設計為僅在RADIUS記帳開始事件上觸發，而不是由臨時記帳更新事件觸發。在會話重新身份驗證期間，網路接入裝置會傳送具有相同框架IP地址和會話ID的記帳臨時更新，這些更新不會重新呼叫無代理狀態評估過程。ISE代碼

專門檢查新會話（ACCOUNTING_START事件），然後啟動無代理狀態流。

相關內容

- 思科錯誤ID CSCwu48086
- 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）。