

使用PingID聯合RADIUS令牌登入ISE管理員GUI失敗

目錄

問題

當使用PingID聯合作為RADIUS令牌時，管理員GUI登入思科ISE失敗，儘管資料包捕獲顯示Ping聯合返回訪問接受響應。即使RADIUS身份驗證從網路角度顯示成功，也會發生登入失敗，從而阻止對ISE介面的管理訪問。網路資料包分析確認PingID伺服器(10.32.154.200)將預期的訪問接受響應傳送到ISE(10.2.200.241)，但ISE管理員登入過程仍無法成功完成。

環境

- 思科身分識別服務引擎(ISE)版本3.3補丁7
- 4節點虛擬機器部署
- 配置為RADIUS令牌身份驗證的PingID聯盟
- ISE IP地址：10.2.200.241
- PingID伺服器IP地址：10.32.154.200
- 在Administration > Admin Access下檢視管理員訪問配置

解析

通過應用啟用成功管理員登入功能的解決方法，問題得以解決。下面幾節中介紹的步驟已用於解決此問題。

步驟 1:證據收集與分析

收集並分析資料包捕獲證據以確認ISE和PingID伺服器之間的RADIUS身份驗證流程。分析驗證了Ping聯盟是否正確傳送了Access-Accept響應。

步驟 2:來自prrt-server.log的證據

###

prrt-server.log

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

###

步驟 3:什麼是Message-Authenticator?

Message-Authenticator是RADIUS資料包中使用的安全屬性，用於確保網路裝置和RADIUS伺服器之間交換的消息的完整性和真實性。它是使用HMAC-MD5在整個RADIUS資料包上使用共用金鑰計算的加密簽名。此屬性有助於防止RADIUS消息的篡改和欺騙，尤其是那些涉及可擴展身份驗證協定(EAP)身份驗證流的消息。

步驟 4:因應措施實施

禁用「響應時需要消息驗證器」：管理/身份管理/外部身份源/RADIUS令牌。點選RADIUS令牌名稱，然後轉到Authentication。取消選中「Message Authenticator Required On Response」。

步驟 5:驗證測試

應用該解決方法後，執行管理員登入測試以驗證解決方案。這些測試確認身份驗證成功以及使用 PingID聯盟作為RADIUS令牌訪問ISE管理員GUI成功。

步驟 6:監控期間

為確保應對措施的穩定性，建立了監測和驗證期。在此期間，繼續進行了管理員登入測試，未報告錯誤或故障。

原因

ISE管理員GUI登入失敗是由思科ISE 3.3補丁7和PingID (Ping聯盟) 在MFA身份驗證期間的RADIUS協定安全實施不匹配引起的。

具體為：

- 思科ISE要求外部RADIUS令牌伺服器的Access-Accept響應中存在RADIUS Message-Authenticator屬性。
- PingID返回的Access-Accept響應沒有Message-Authenticator屬性。
- 因為ISE啟用了Message Authenticator Required On Response設定，所以它以靜默方式拒絕RADIUS響應無效，即使身份驗證本身在PingID端成功也是如此。
- 此實施是Cisco ISE安全加固的一部分，可緩解Blast-RADIUS漏洞(CVE-2024-3596)。

相關內容

- [Blast-RADIUS協定欺騙緩解\(CVE-2024-3596\)](#)

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）。