在UCSM上配置Radius身份驗證並對其進行故障排除

目錄

簡介

本文檔介紹使用Windows Server 2022 DataCenter在UCS Manager上配置Radius並對其進行故障排除的步驟。

必要條件

- UCS Manager - 4.2(3o)或更高版本
- Windows Server 2022資料中心

Windows Server上的配置

安裝Active Directory域服務

請參閱Microsoft文檔 — 在Windows Server 2022上使用伺服器管理器安裝AD DS。

建立Active Directory使用者（登入帳戶）

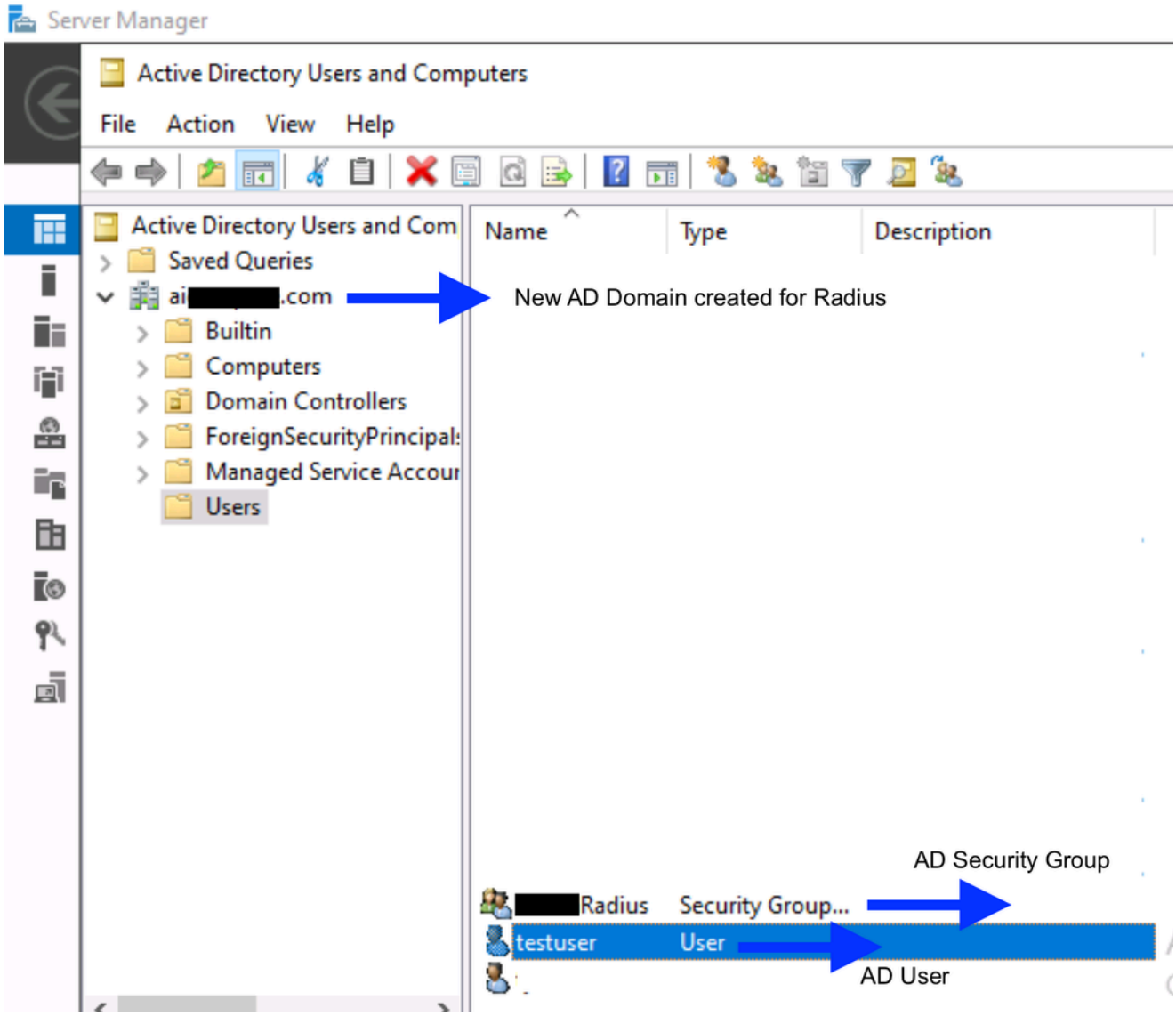
1.開啟「Server Manager」>「Tools」>「Active Directory Users and Computers」。

2.按一下右鍵您建立的域「新建」>「使用者」。

3.輸入登入名（示例 — testuser），設定密碼，取消選中User must change password at next logon，然後選中Password never expires（對於服務/管理員帳戶）> Finish（根據您的本地安全要求/策略）。

為UCS管理員建立AD安全組

- 在同一控制檯中，按一下右鍵您的域New > Group（示例 — testRadius， Security）。將AD使用者testuser新增到此組。
- 此組名稱是以後必須對映到UCS角色的名稱。

- 

安裝NPS（RADIUS角色）並在Active Directory中註冊NPS

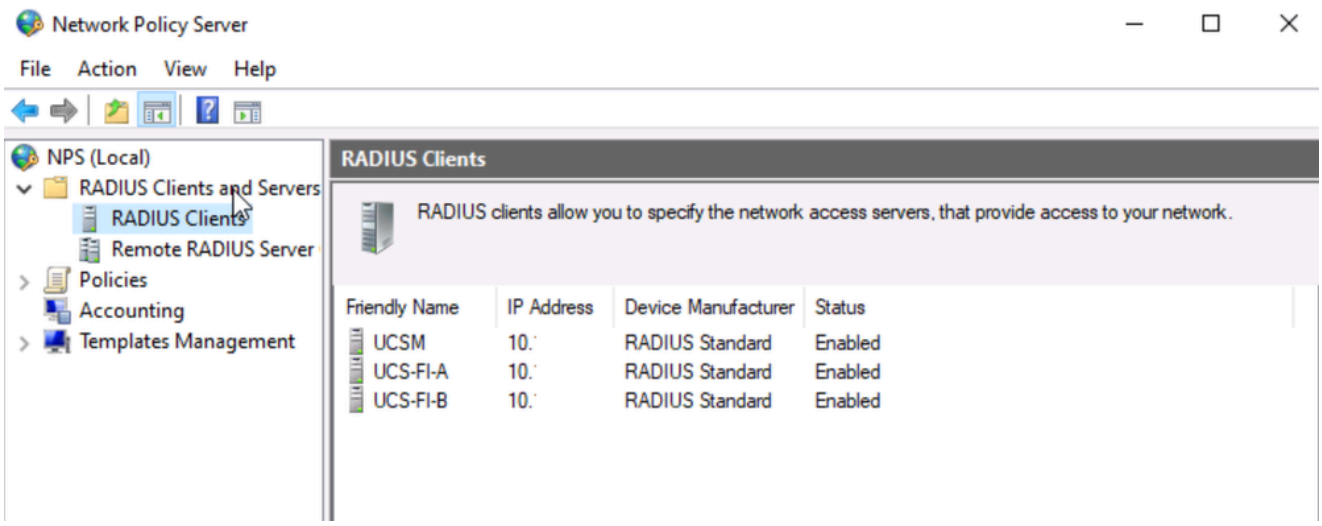
1.導航到Server Manager > Manage > Add Roles and Features。

2.選擇Network Policy and Access Services > Complete the wizard to install Network Policy Server(NPS)。

3.開啟Tools > Network Policy Server。按一下右鍵NPS（本地）> Register server in Active Directory > OK。這樣NPS可以讀取AD使用者/組成員身份。

將UCS交換矩陣互聯新增為RADIUS客戶端

- 這指示NPS信任來自UCSM的請求。在NPS中，展開RADIUS Clients and Servers > RADIUS Clients。按一下右鍵New。

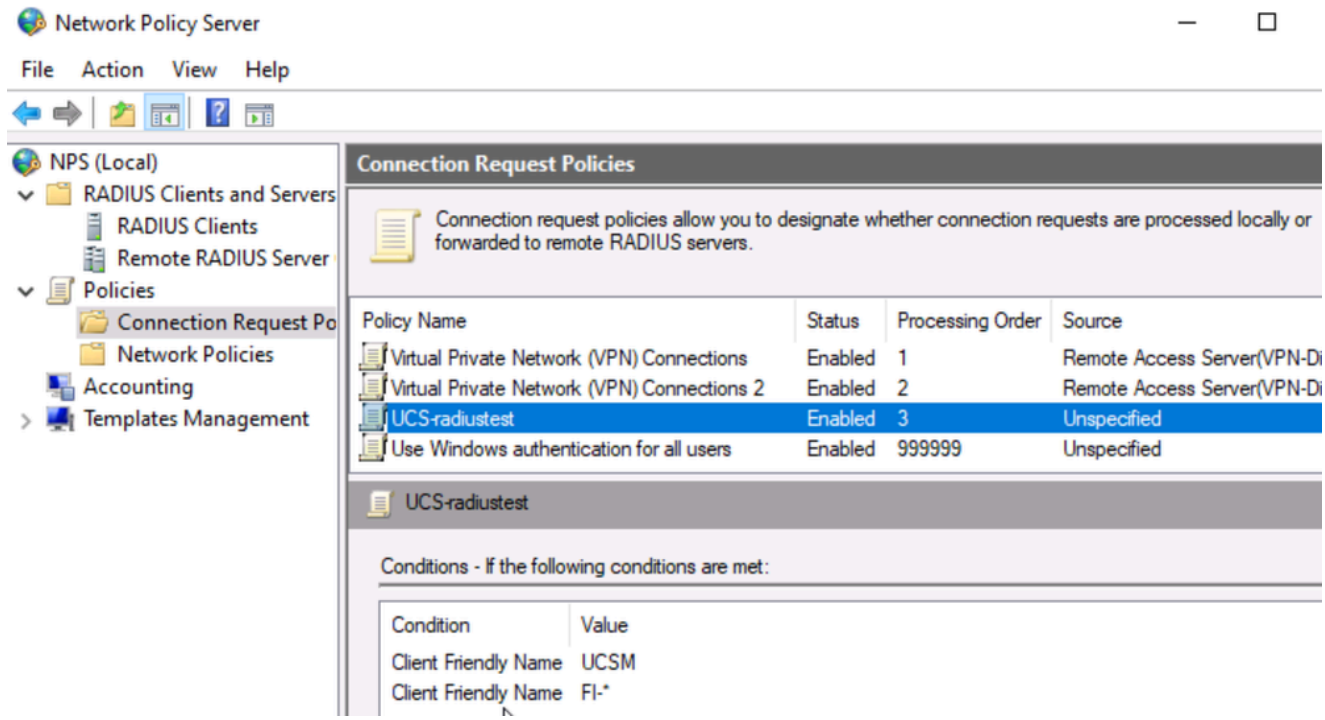
- 提供：
  - 友好名稱：示例 — UCSM
  - 地址(IP):fi-A的管理IP
  - 共用金鑰：建立強金鑰並將其記下 — 您稍後將在UCSM中輸入此確切的共用金鑰字串。
- 對交換矩陣互聯B重複上述操作，如果要根據集群VIP進行身份驗證，請新增該IP。
- 

Radius使用者端

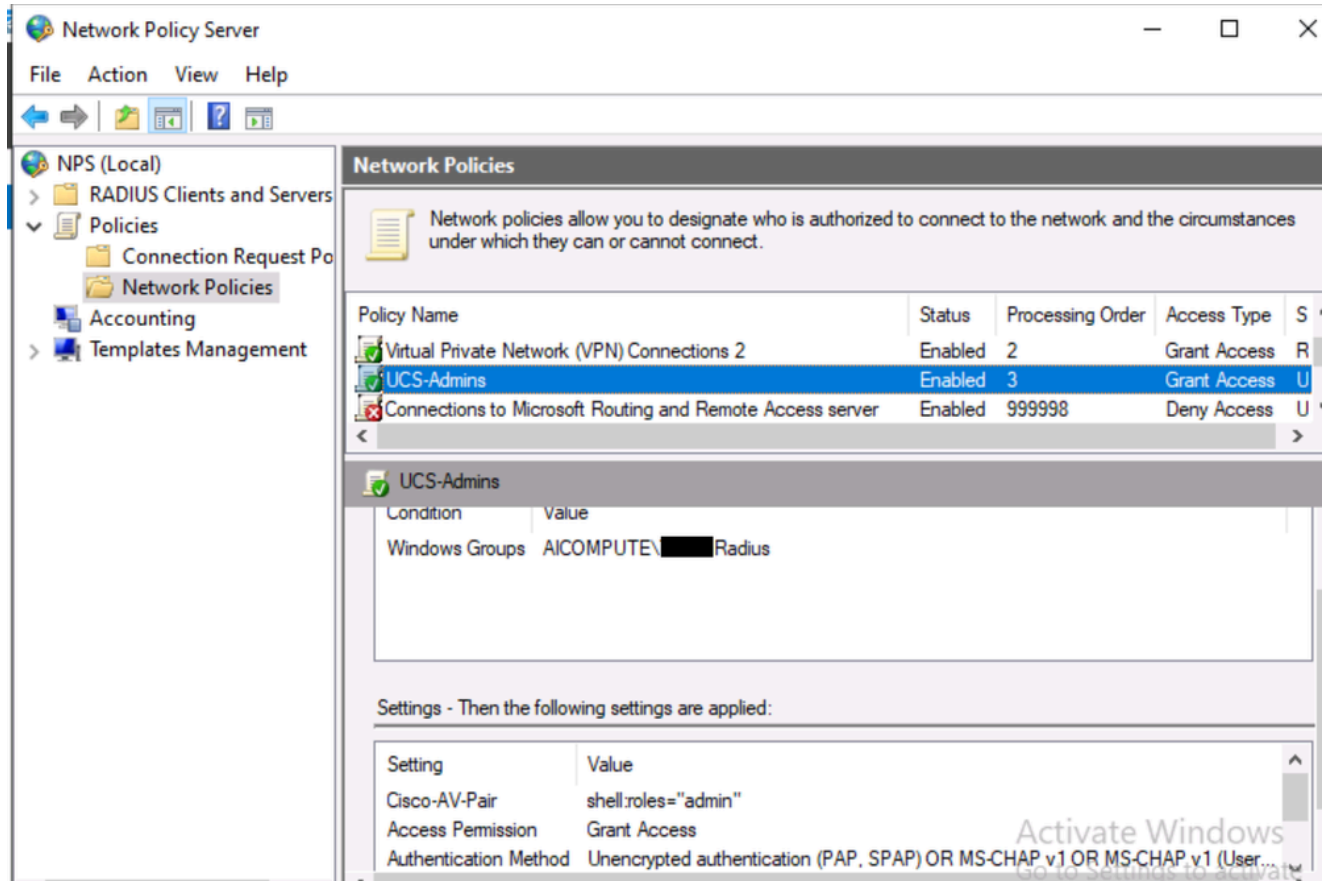
建立連線請求策略和網路策略（授權和角色對映）

- Policies > Connection Request Policies > New > Name it（示例 — UCS-radiustest），新增「Client Friendly Name」（客戶端友好名稱）條件，使其能夠在本地進行身份驗證。舉例來說：FI-*或UCSM、
- Policies > Network Policies > New > Policy name
  - 狀況:新增Windows組。選擇您在步驟3中建立的testRadius組。
  - 訪問許可權：授予訪問許可權
  - 身份驗證方法：啟用未加密身份驗證(PAP/SPAP)和/或UCS使用的方法。（UCS RADIUS通常使用PAP。）
- Configure Settings > Vendor Specific Attributes（這是將AD使用者對映到UCS角色的關鍵部分）：新增特定供應商的屬性> Cisco AV配對
  - 將該值設定為UCS角色/區域設定字串，示例 — shell:roles="admin"（如果跳過此屬性，則使用者以只讀方式登入）。

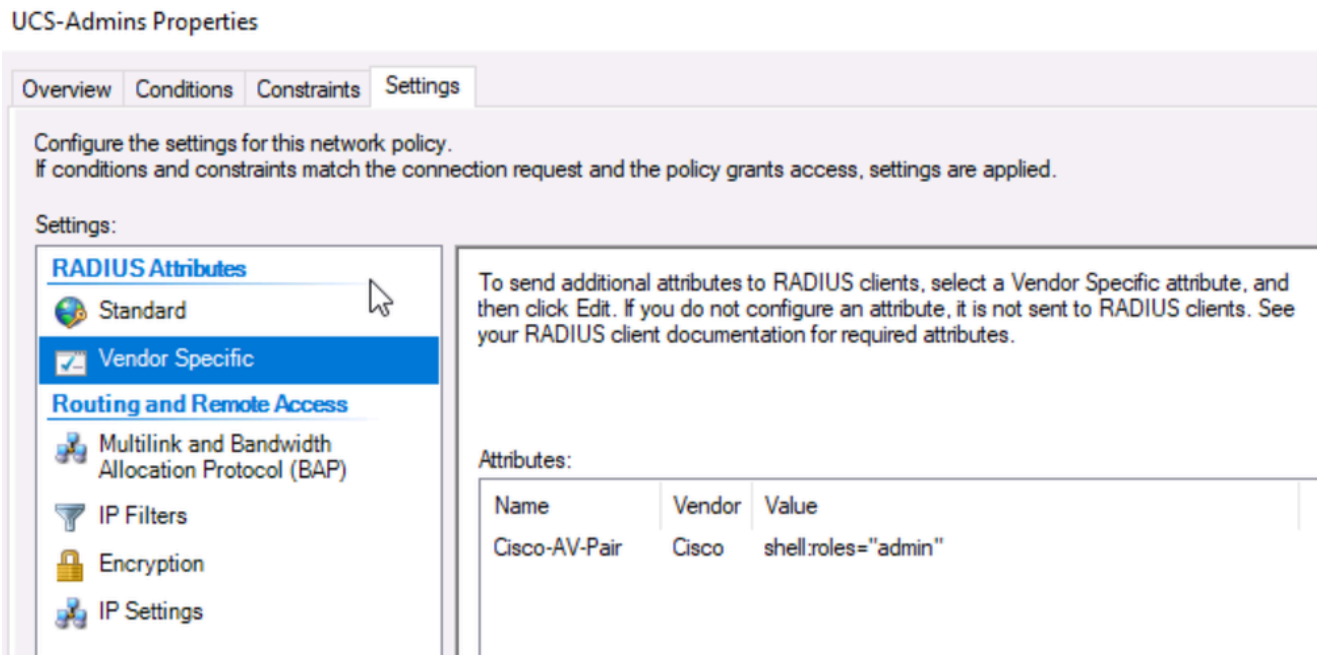
連線請求策略

- 

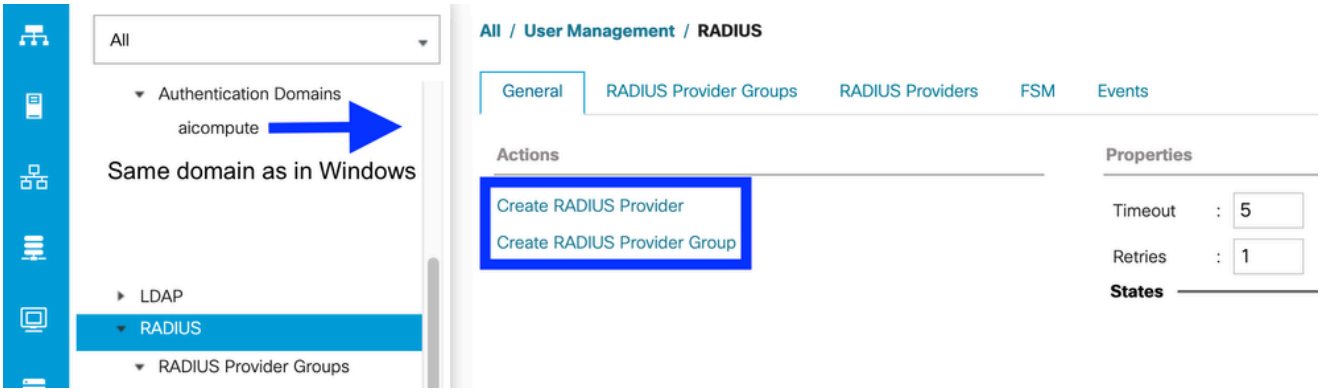
網路策略

- 

供應商特定屬性



UCSM上的配置



建立Radius提供程式並新增到提供程式組

1.登入到UCS Manager GUI，然後導航至Admin > User Management > RADIUS。

2.按一下建立RADIUS提供程式(+/ Create 選項)並填寫：

- 主機名/FQDN或IP:Windows NPS伺服器。
- 主要:您在NPS步驟5中設定的確切共用金鑰。
- 授權埠:1812（必須與NPS匹配）
- 逾時/重試:保留預設值為開始。

3.在Admin >User Management > RADIUS下，建立提供程式組（示例 — RADIUS-Grp）並從早期

版本新增提供程式。

建立身份驗證域

這是把所有東西綁在一起的部件。

1.導航到Admin > User Management > Authentication > Authentication Domains。

2.按一下Create a Domain（示例 — RADIUS — 建議與NPS中建立的域相同的域名）。

3.設定領域= RADIUS。

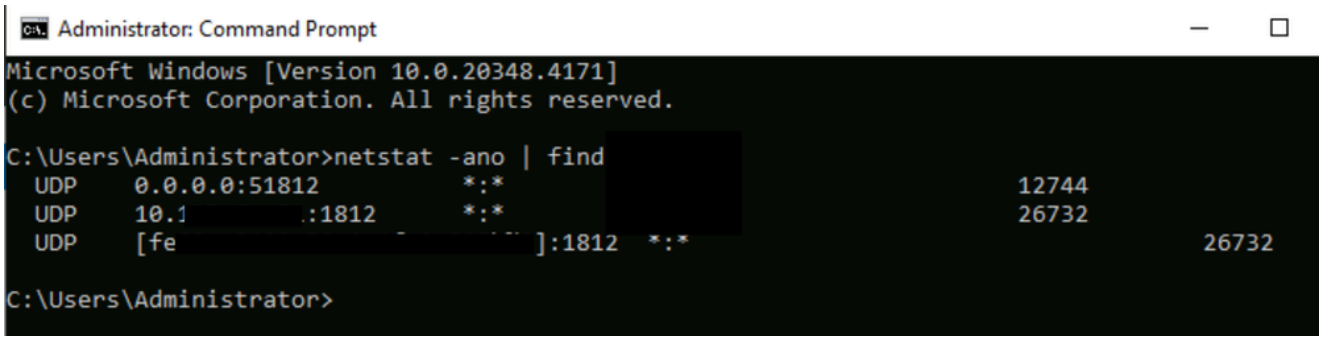
4.分配您建立的提供商組(RADIUS-Grp)並儲存。

驗證

在Windows Server上 — 確認防火牆/埠

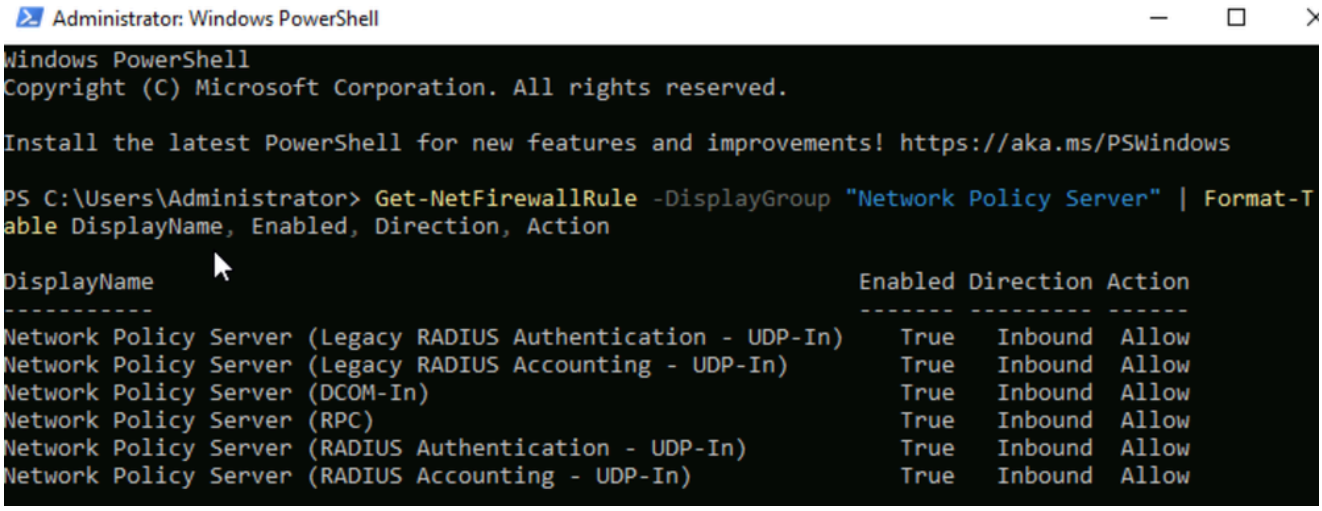
RADIUS驗證使用UDP連線埠1812（和計量1813）。 確保Windows防火牆和任何網路防火牆都允許從FI管理IP獲取這些資訊。

1.確認NPS/Radius服務正在通過netstat -ano | findstr 1812 命令。

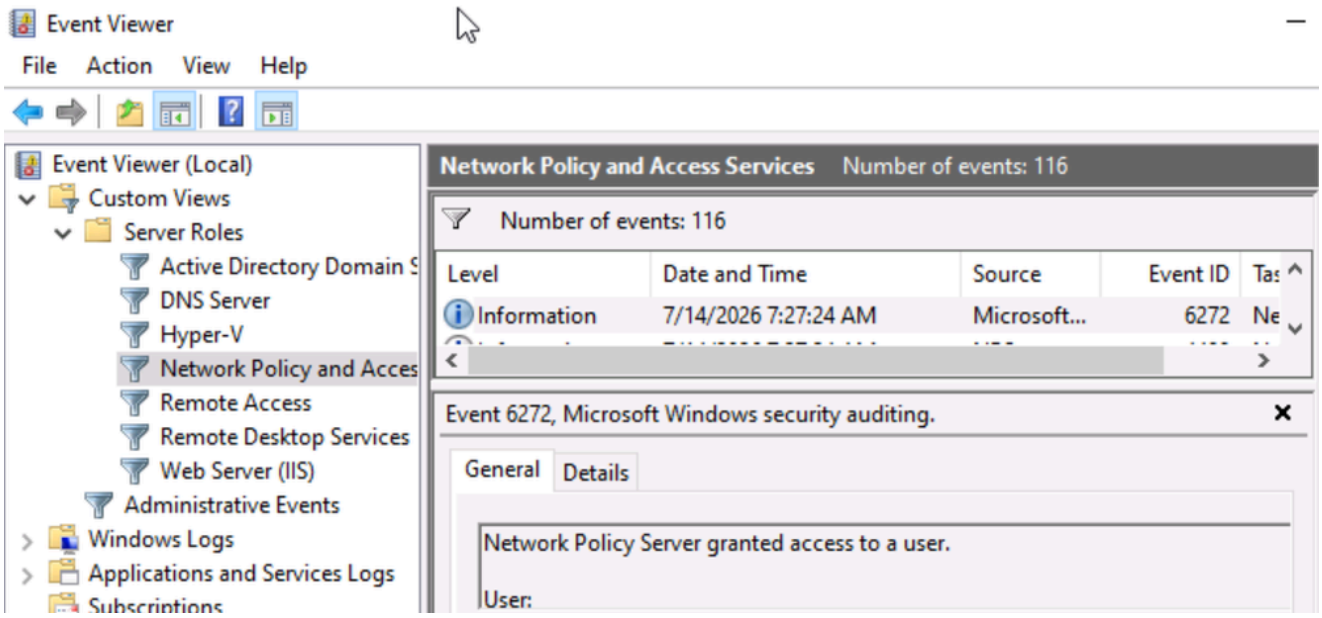
- (您將看到一行帶有UDP和*:1812（或伺服器IP:1812）。 這確認NPS/RADIUS服務正在主動偵聽。
- 如果未顯示，則NPS無法運行 — 請選中Services > Network Policy Server(IAS)is Started。)
- 

- 在Windows Powershell上，運行命令：

- Get-NetFirewallRule -DisplayGroup "網路策略伺服器" | Format-Table DisplayName、Enabled、Direction、Action。



- 在Windows事件檢視器上：
  - Custom Views > Server Roles > Network Policy and Access Services > Packets are reaching。



從UCSM測試登入

1.根據建立的Radius域，通過選擇Domain下拉選單註銷並登入。

2.配置使用者密碼。（請參閱Windows配置步驟2）。

- 如果登入工作正常且您具有管理員許可權，則Cisco AV對對映（Windows配置步驟6）是正確

的。

Radius驗證疑難排解

在Windows Server上

1.在Powershell中執行以下命令以捕獲資料包：

- pktmon過濾器add -p 1812
- pktmon start —capture —pkt-size 0 -f C:\radius_capture.etl

2.從UCSM啟動登入並使用命令停止捕獲：

- pktmon stop
- pktmon etl2pcap C:\radius_capture.etl -o C:\radius_capture.pcap

3.在Wireshark中開啟radius_capture.pcap: RADIUS > Attribute Value Pairs > Confirm Message-Authenticator(或屬性80)。這表示NPS正在簽署回覆。

在UCSM CLI上

在Windows上同時從UCSM CLI運行pktmon時，

1.執行：

- connect nxos
- 終端監視器
- debug radius all

2.啟動調試後嘗試UCSM登入。

成功登入看起來類似於2026年7月3日09:54:02.917044 radius:Verified Message Authenticator ，響應來自：10.xxx.xx.xx。

- 如果傳送和接收封包但登入失敗，則訊息驗證器可能不正確。在debug輸出中 — 這表示連線埠和可達性良好。
    - 再次嘗試在Windows NPS伺服器中重新配置共用金鑰和UCSM金鑰（需要完全匹配）。

- 如果在重新配置後登入時問題仍然存在，我們可能會遇到已知的Cisco錯誤ID CSCwm80801 :使用者在Microsoft補丁KB5040434後無法使用Radius登入UCSM，需要升級至上述固定版本。

相關資訊

- Cisco UCS管理器管理管理指南4.2 — 遠端身份驗證

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）。