在UCSM上配置并排除Radius身份验证故障

目录

简介

本文档介绍使用Windows Server 2022 DataCenter在UCS Manager上配置并排除Radius故障的步骤。

先决条件

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

Windows Server上的配置

安装Active Directory域服务

请参阅Microsoft文档 — 在Windows Server 2022上使用服务器管理器安装AD DS。

创建Active Directory用户（登录帐户）

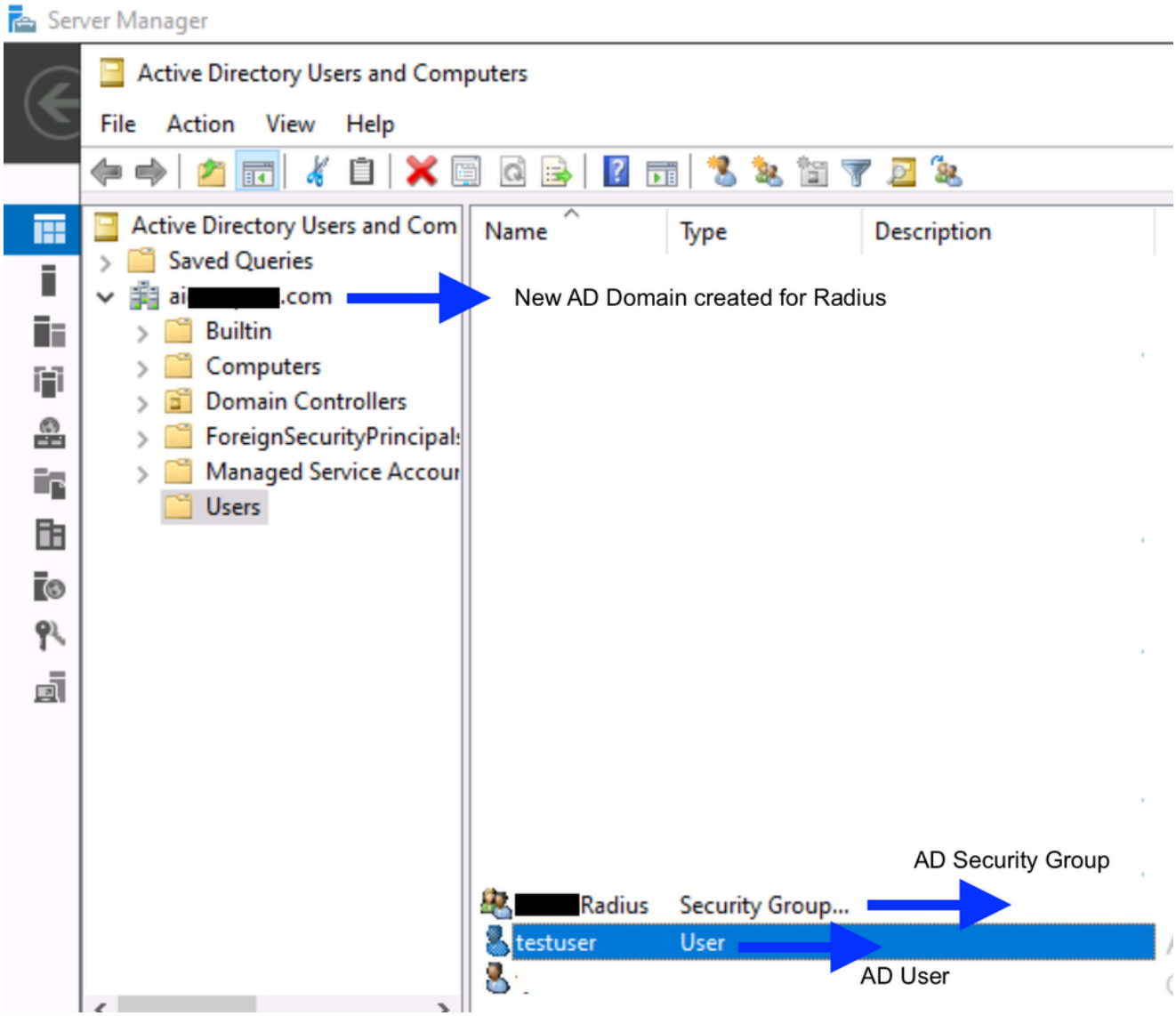
1.打开Server Manager > Tools > Active Directory Users and Computers。

2.右键单击您创建的域“新建”>“用户”。

3.输入登录名（示例 — testuser），设置密码，取消选中User must change password at next logon，然后选中Password never expires（对于服务/管理员帐户）> Finish（根据您的本地安全要求/策略）。

为UCS管理员创建AD安全组

- 在同一控制台中，右键单击您的域New > Group（示例 — testRadius， Security）。将AD用户testuser添加到此组。
- 此组名称是稍后必须映射到UCS角色的名称。

- 

安装NPS（RADIUS角色）并在Active Directory中注册NPS

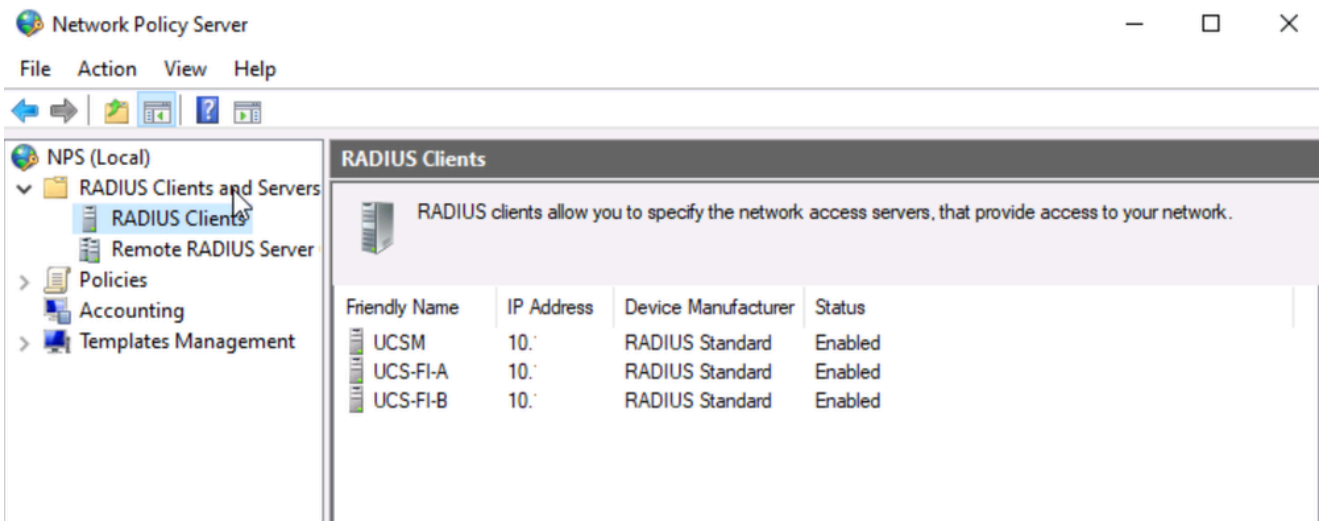
1.导航到服务器管理器>管理>添加角色和功能。

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

3.打开Tools > Network Policy Server。右键单击NPS（本地）> Register server in Active Directory > OK。这样NPS可以读取AD用户/组成员身份。

将UCS交换矩阵互联添加为RADIUS客户端

- 这会告知NPS信任来自UCSM的请求。在NPS中，展开RADIUS Clients and Servers > RADIUS Clients。右键单击New。

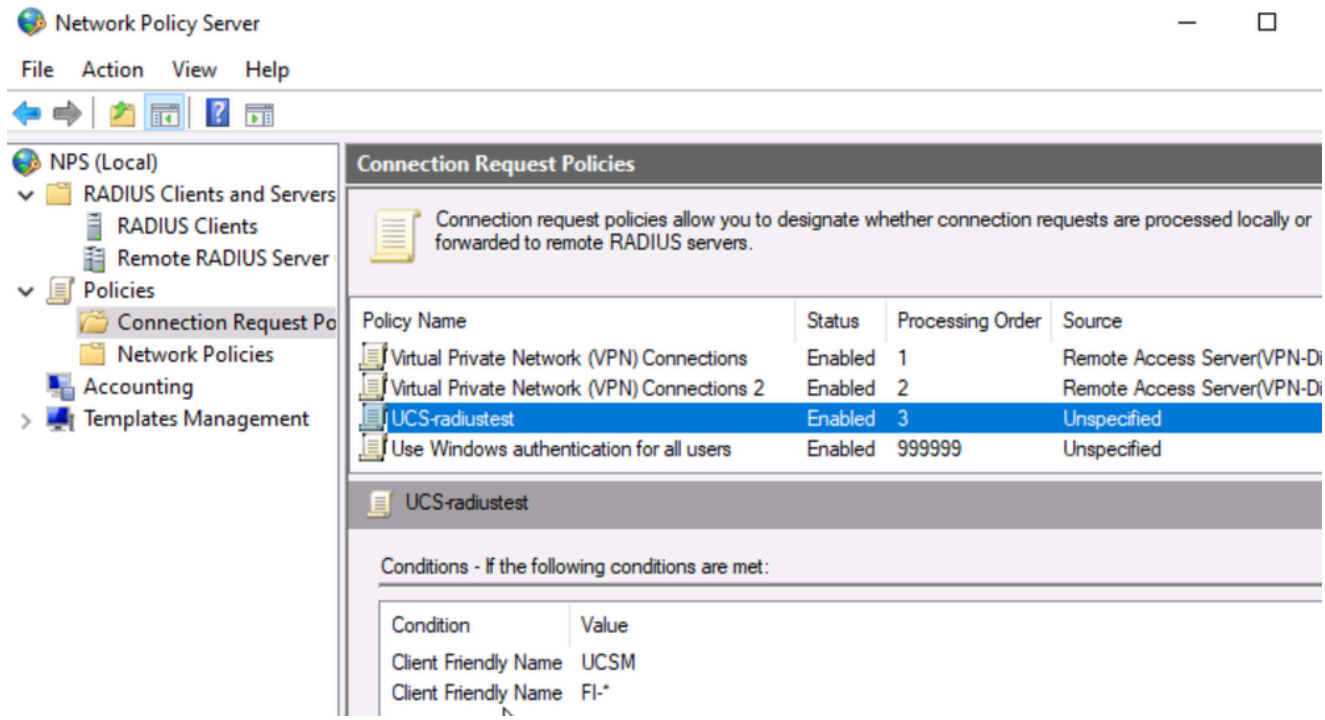
- 提供：
  - 友好名称：示例 — UCSM
  - 地址(IP):fi-A的管理IP
  - 共享密钥:创建强加密并记下 — 稍后您将在UCSM中输入此确切的共享加密字符串。
- 对交换矩阵互联B重复上述步骤，如果要根据集群VIP进行身份验证，请同时添加该IP。
- 

Radius客户端

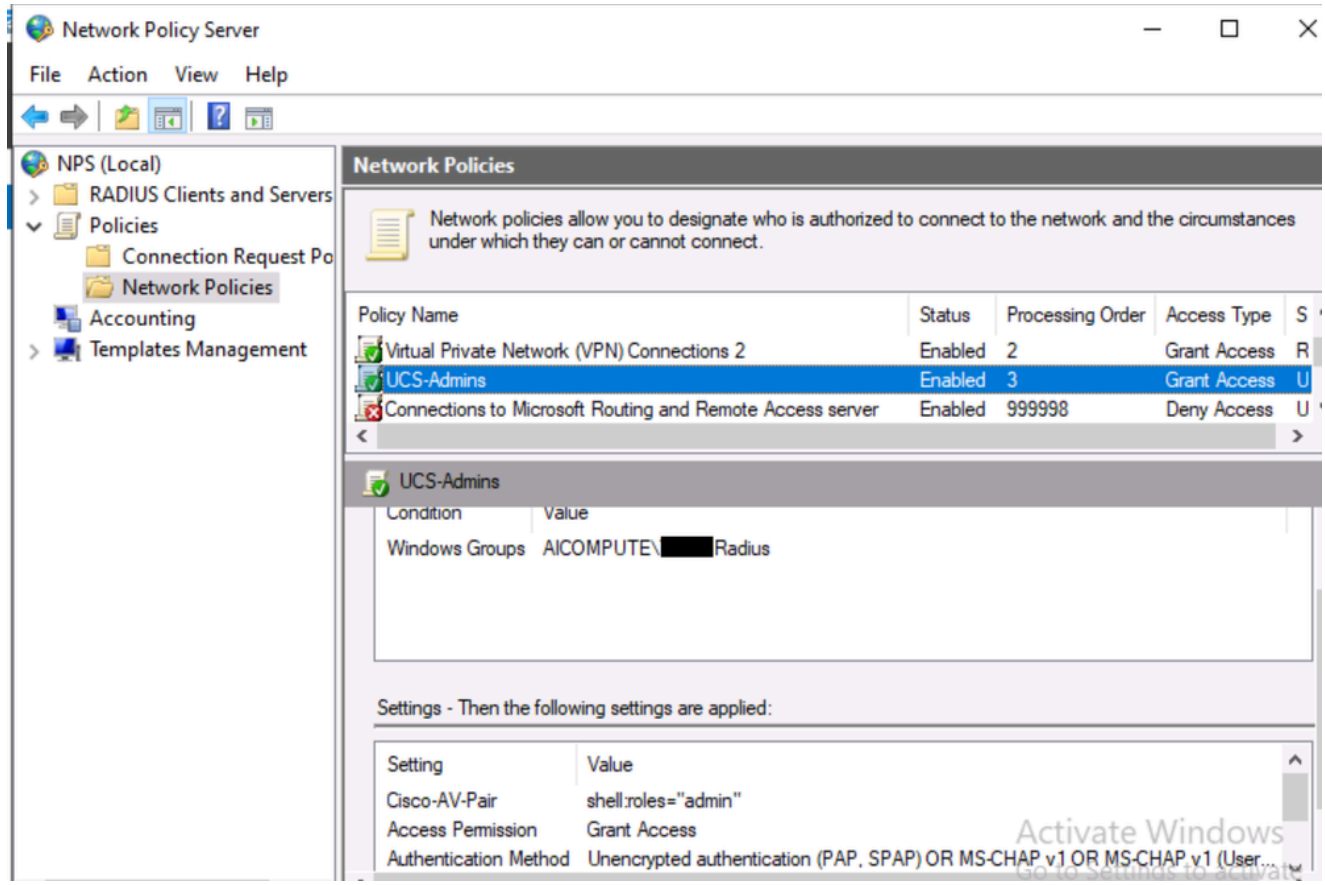
创建连接请求策略和网络策略（授权和角色映射）

- Policies > Connection Request Policies > New > Name it（示例 — UCS-radiustest），添加“Client Friendly Name”（客户端友好名称）的条件，使其能够在本地进行身份验证。例如：FI-*或UCSM、
- Policies > Network Policies > New > Policy name
  - 条件:添加Windows组。选择您在第3步中所创建的testRadius组。
  - 访问权限：授权访问
  - 身份验证方法：启用未加密身份验证(PAP/SPAP)和/或UCS使用的方法。（UCS RADIUS通常使用PAP。）
- Configure Settings > Vendor Specific Attributes（这是将AD用户映射到UCS角色的关键部分）：添加供应商特定属性> Cisco AV-Pair
  - 将该值设置为UCS角色/区域设置字符串，例如 — shell:roles="admin"（如果跳过此属性，用户将以只读身份登录）。

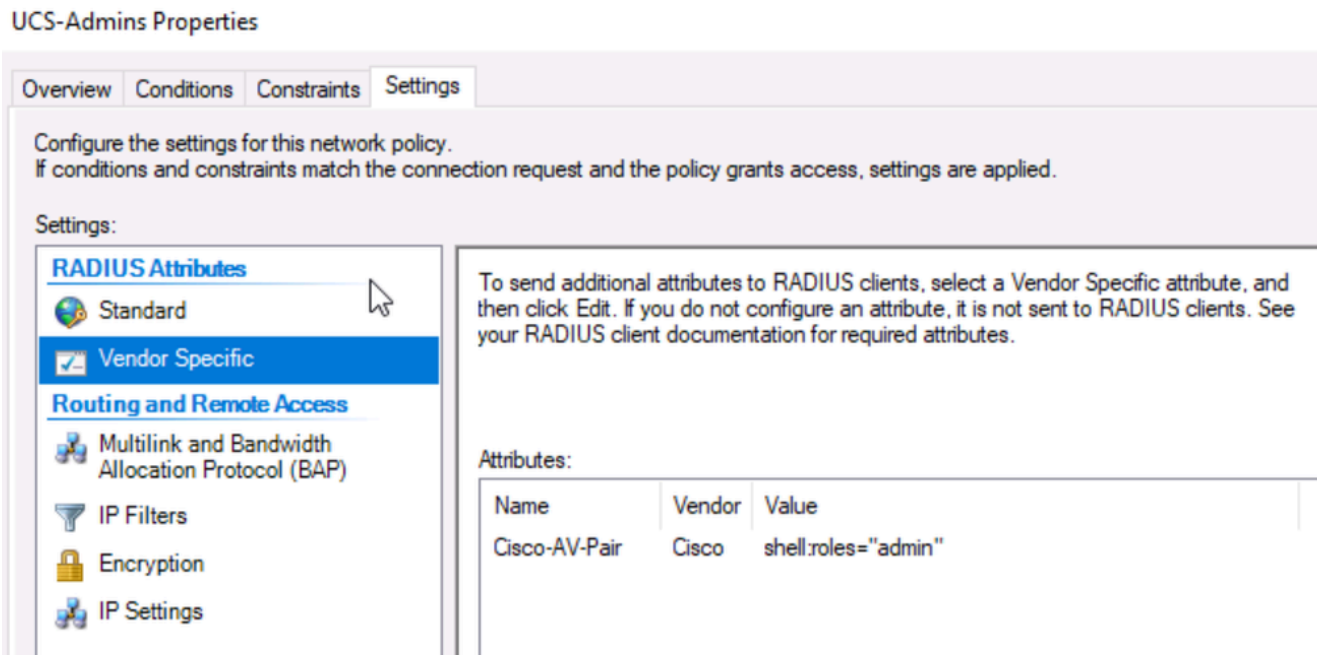
连接请求策略

- 

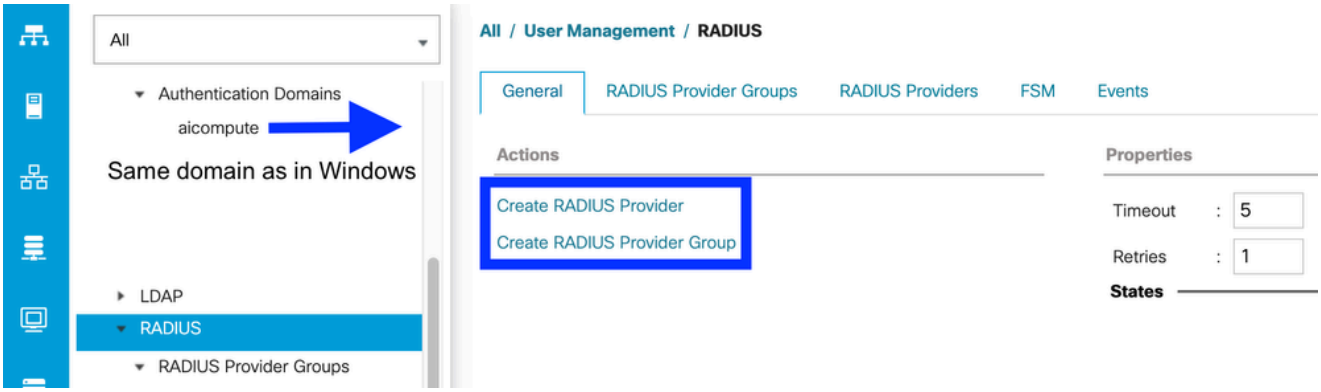
网络策略

- 

供应商特定属性



UCSM上的配置



创建Radius提供程序并添加到提供程序组

1.登录到UCS Manager GUI，然后导航到Admin > User Management > RADIUS。

2.单击创建RADIUS提供程序（ +/ Create选项）并填写：

- 主机名/FQDN或IP:Windows NPS服务器。
- 密钥:在NPS步骤5中设置的完全共享密钥。
- 授权端口:1812（必须与NPS匹配）
- 超时/重试:保留默认值为开始。

3.在Admin >User Management > RADIUS下，创建提供程序组（示例 — RADIUS-Grp）并从之前

添加提供程序。

创建身份验证域

这是把所有事情都联系在一起的部件。

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

2.单击Create a Domain（示例 — RADIUS — 建议与NPS中创建的域相同的域名）。

3.设置领域= RADIUS。

4.分配您创建的提供商组(RADIUS-Grp)并保存。

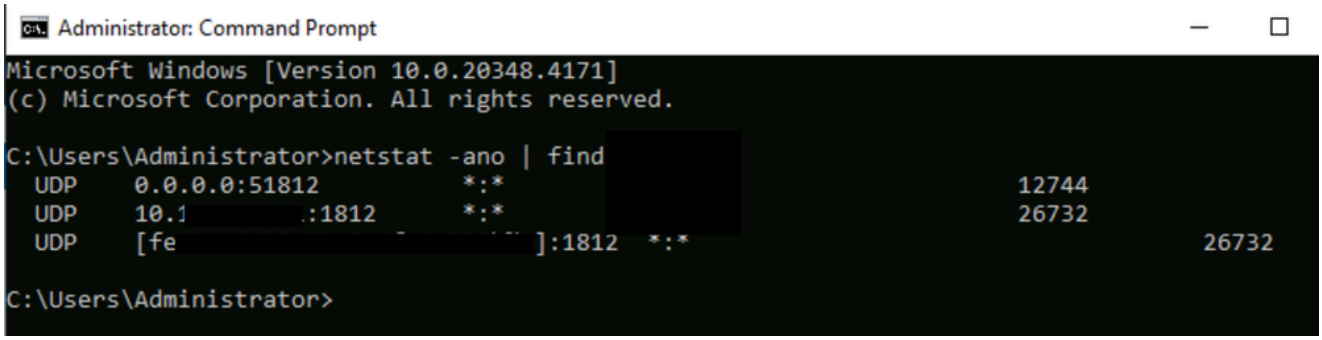
验证

从Windows Server — 确认防火墙/端口

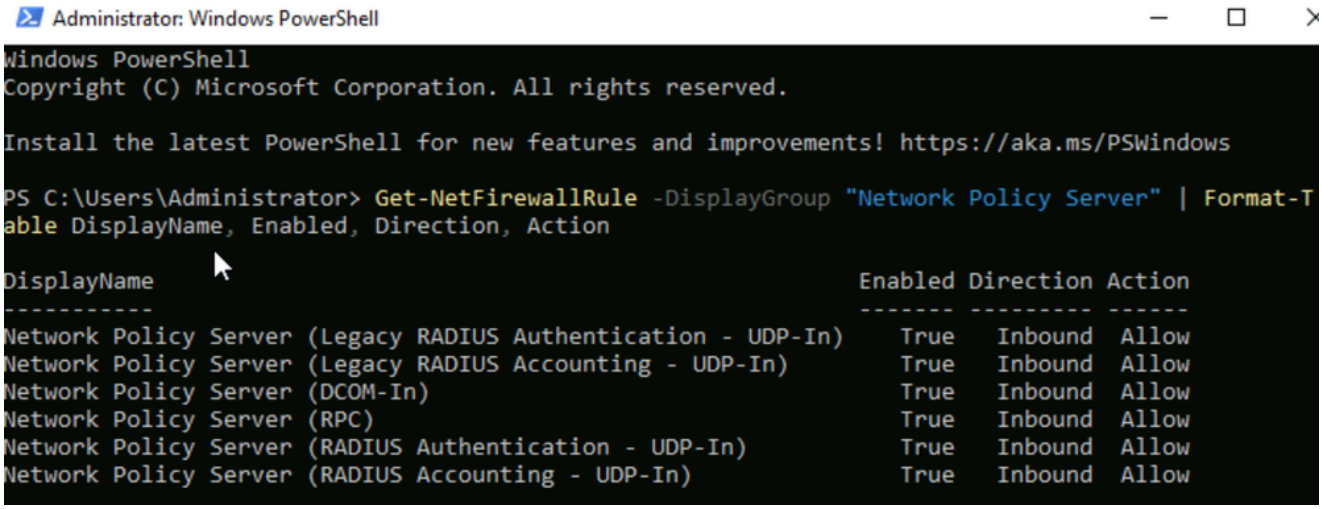
RADIUS身份验证使用UDP端口1812（和记帐1813）。 确保Windows防火墙和任何网络防火墙都允许从FI管理IP进行这些配置。

1.确认NPS/Radius服务正在通过netstat -ano侦听 | findstr 1812命令。

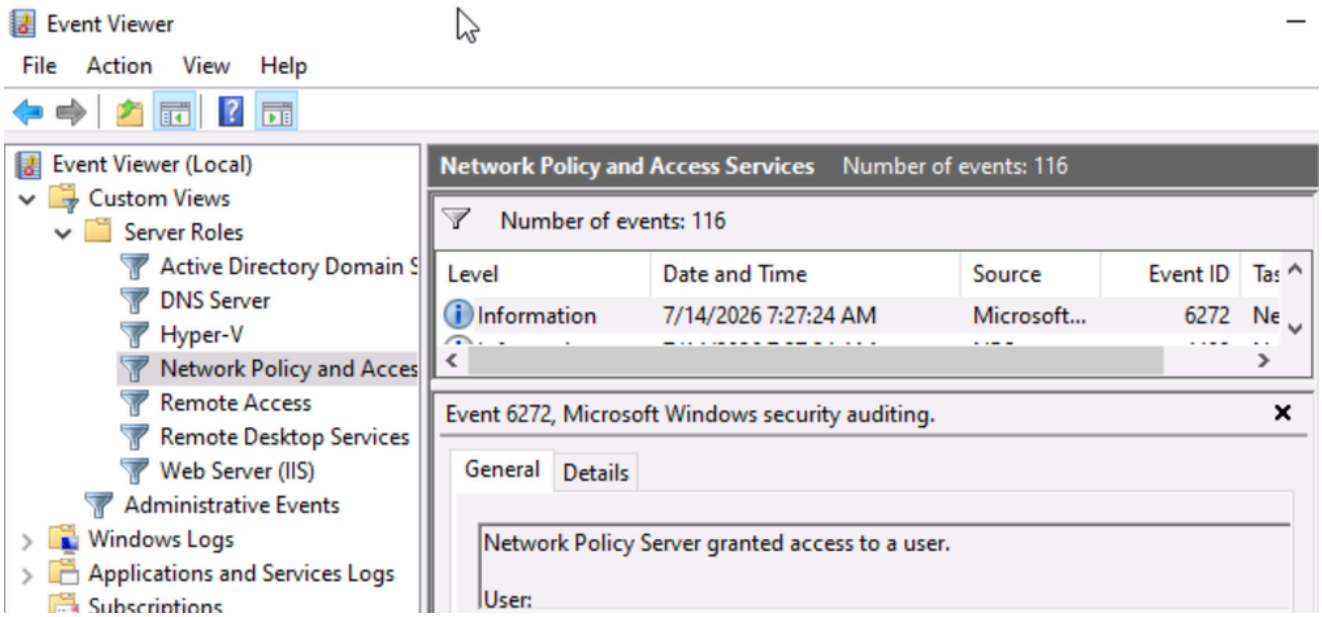
- (您将看到一条带有UDP和*:1812（或服务器IP:1812）的线路。 这确认NPS/RADIUS服务正在主动侦听。
- 如果未显示任何内容，则NPS无法运行 — 选中Services > Network Policy Server(IAS)is Started。）



- 在Windows Powershell上，运行命令：
  - Get-NetFirewallRule -DisplayGroup "网络策略服务器" | Format-Table DisplayName、Enabled、Direction、Action。



- 在Windows事件查看器上：
  - Custom Views > Server Roles > Network Policy and Access Services > Packets are reaching。



从UCSM测试登录

1.根据创建的Radius域，选择Domain下拉菜单以注销并登录。

2.配置用户密码。（请参阅Windows配置步骤2）。

- 如果登录工作正常且您具有管理员权限，则思科AV对映射（Windows配置步骤6）是正确的。

排除Radius身份验证故障

从Windows Server

1.在Powershell中执行以下命令以捕获数据包：

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

2.从UCSM启动登录并使用命令停止捕获：

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

3.在Wireshark中打开radius_capture.pcap:RADIUS > Attribute Value Pairs > confirm Message-Authenticator（或属性80）。这意味着NPS正在签署回复。

从UCSM CLI

在Windows上同时从UCSM CLI运行pktmon时，

1.运行：

- connect nxos
- terminal monitor
- debug radius all

2.在启动调试后尝试UCSM登录。

成功登录看起来类似于2026年7月3日09:54:02.917044 radius:Verified Message Authenticator，响应自：10.xxx.xx.xx。

- 如果发送和接收数据包，但登录失败，则消息验证器可能不正确。在debug输出中，这意味着端口和可达性良好。
    - 再次尝试在Windows NPS服务器中重新配置共享密钥和UCSM密钥（需要完全匹配）。

- 如果在重新配置后登录时问题仍然存在，我们可能会遇到已知的Cisco Bug ID CSCwm80801（仅限注册用户）：在Microsoft补丁KB5040434要求升级到上述固定版本后，用户无法使用Radius登录UCSM。

相关信息

- Cisco UCS Manager管理管理指南4.2 — 远程身份验证

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。