UCSM에서 RADIUS 인증 구성 및 문제 해결

목차

소개

이 문서에서는 Windows Server 2022 DataCenter를 사용하여 UCS Manager에서 Radius를 구성하고 문제를 해결하는 단계를 설명합니다.

사전 요구 사항

- UCS Manager - 4.2(3o) 이상
- Windows Server 2022 데이터 센터

Windows Server 구성

Active Directory 도메인 서비스 설치

Microsoft 문서 - Windows Server 2022에서 Server Manager를 사용하여 AD DS를 설치하십시오.

Active Directory 사용자(로그인 계정) 생성

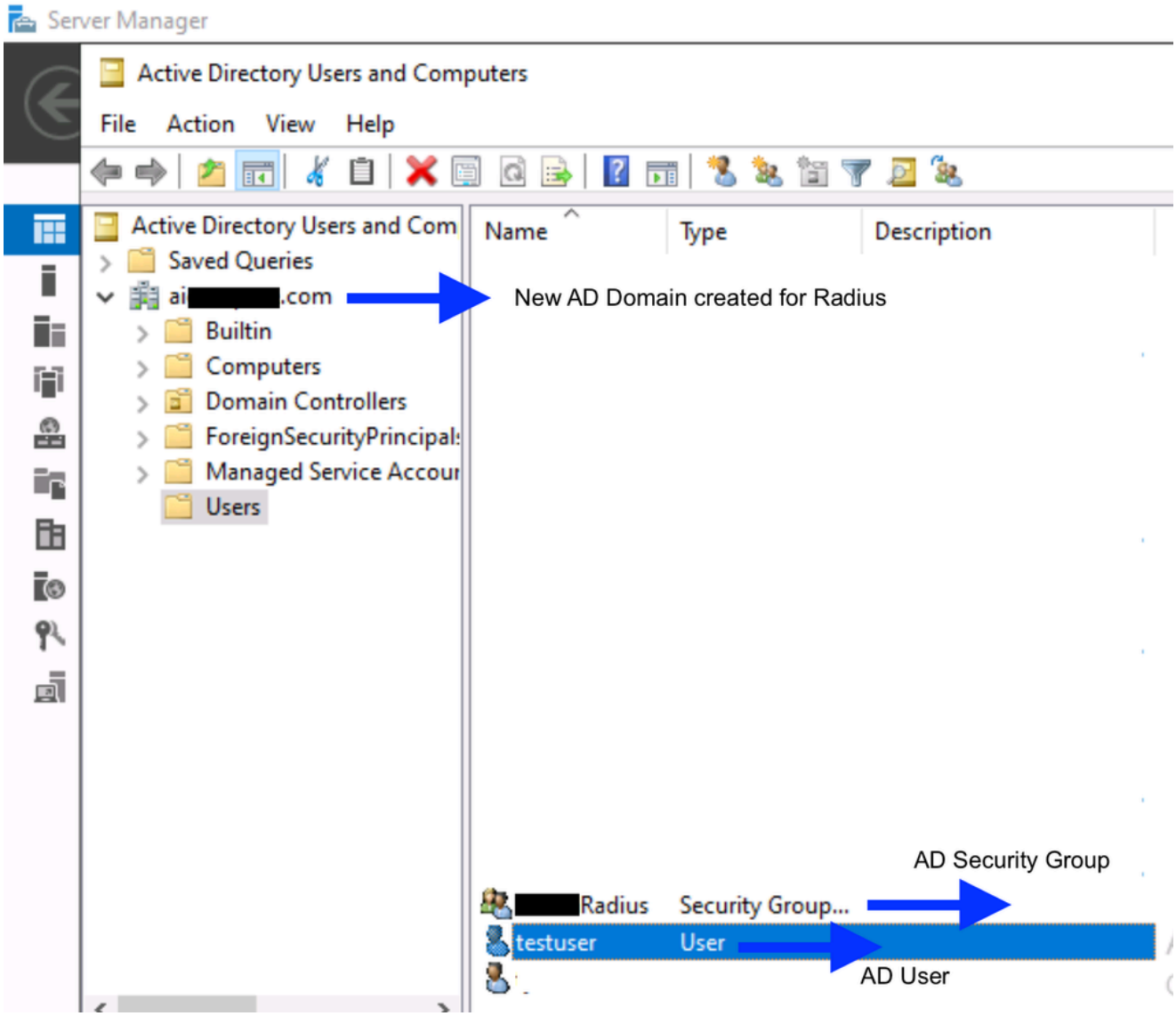
1. 서버 관리자 > 도구 > Active Directory 사용자 및 컴퓨터를 엽니다.

2. 생성된 도메인 New(새로 만들기) > User(사용자)를 마우스 오른쪽 버튼으로 클릭합니다.

3. 로그인 이름(예 - testuser)을 입력하고, 비밀번호를 설정하고, 다음 로그온 시 사용자가 비밀번호를 변경해야 함을 선택 취소하고, 비밀번호가 만료되지 않음(서비스/관리자 계정의 경우) > 마침(로컬 보안 요구 사항/정책에 따라)을 선택합니다.

UCS 관리자용 AD 보안 그룹 만들기

- 동일한 콘솔에서 도메인 New(새로 만들기) > Group(예: testRadius, Security)을 마우스 오른쪽 단추로 클릭합니다. 이 그룹에 AD 사용자 testuser(testuser)를 추가합니다.
- 이 그룹 이름은 나중에 UCS 역할에 매핑해야 하는 이름입니다.

- 

NPS(RADIUS 역할)를 설치하고 Active Directory에 NPS 등록

1. 서버 관리자 > 관리 > 역할 및 기능 추가로 이동합니다.

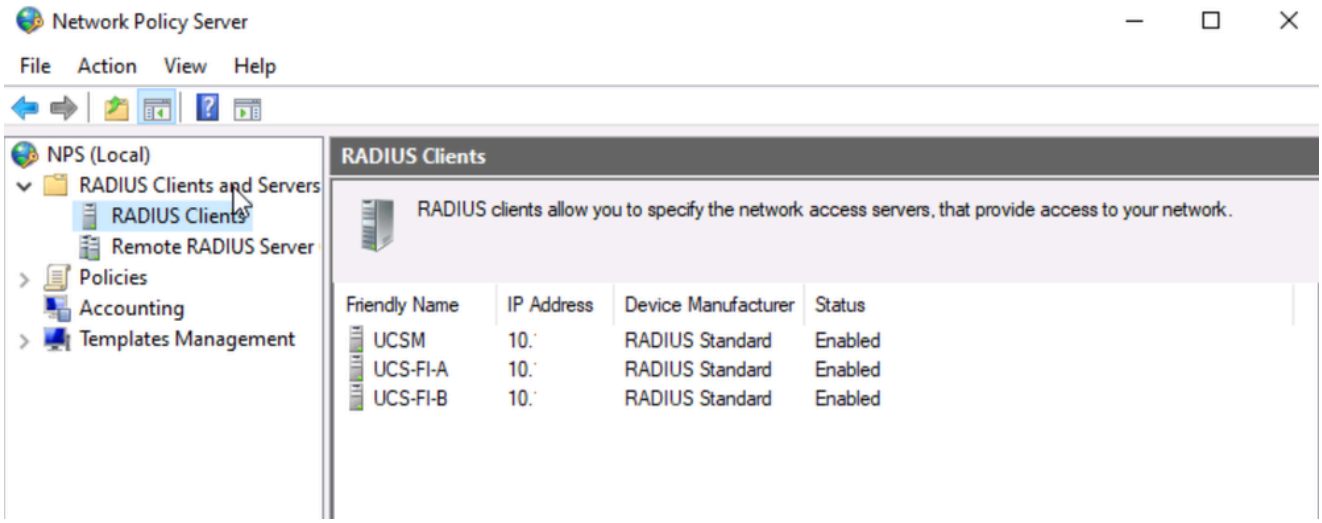
2. 네트워크 정책 및 액세스 서비스 > 네트워크 정책 서버(NPS)를 설치하려면 마법사 완료를 선택합니다.

3. 도구 > 네트워크 정책 서버를 엽니다. NPS (Local) > Register server in Active Directory > OK를 마우스 오른쪽 버튼으로 클릭합니다. 이렇게 하면 NPS가 AD 사용자/그룹 멤버십을 읽을 수 있습니다.

UCS Fabric Interconnect를 RADIUS 클라이언트로 추가

- 그러면 NPS가 UCSM의 요청을 신뢰하게 됩니다. NPS에서 RADIUS Clients and

Servers(RADIUS 클라이언트 및 서버) > RADIUS Clients(RADIUS 클라이언트)를 확장합니다. 새로 만들기를 마우스 오른쪽 단추로 클릭합니다.

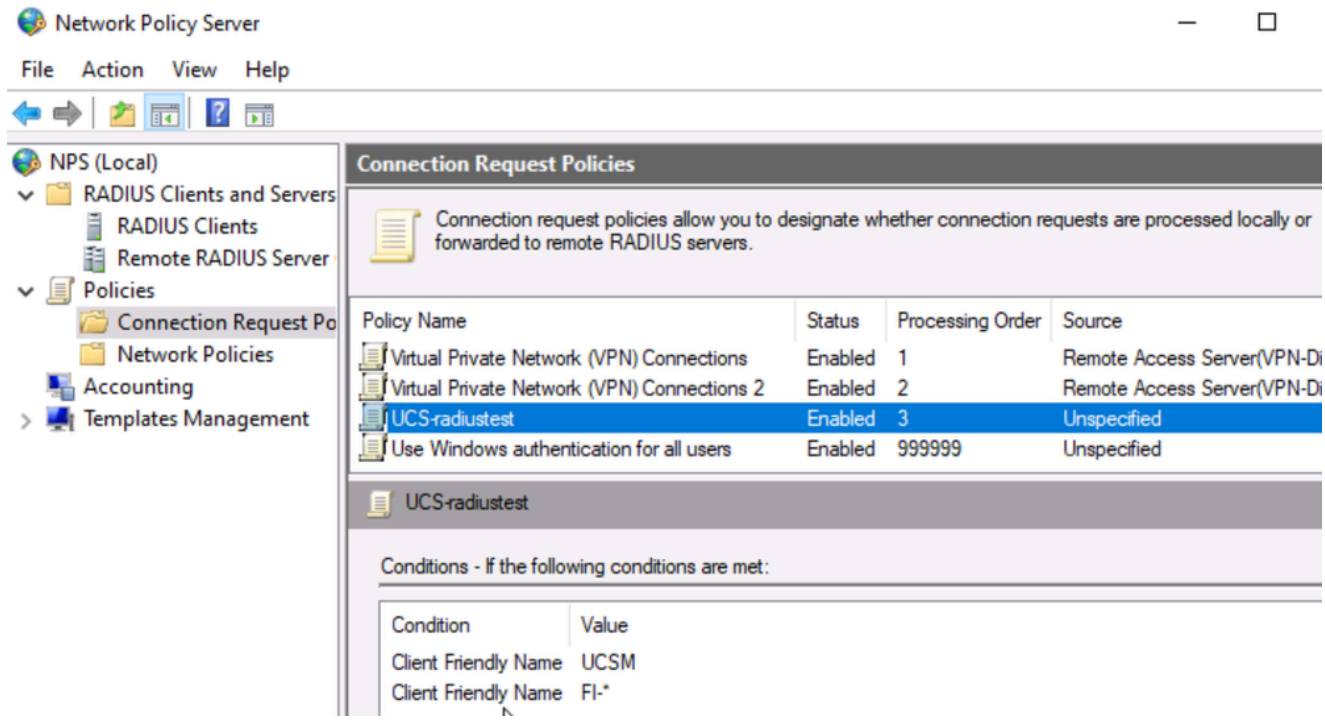
- 제공:
  - 이름: 예 - UCSM
  - 주소(IP): FI-A의 관리 IP
  - 공유 암호: 강력한 암호를 만들고 기록해 두십시오. 나중에 UCSM에서 이 정확한 공유 암호 문자열을 입력해야 합니다.
- 패브릭 인터커넥트 B에 대해 를 반복하고 클러스터 VIP에 대해 인증할 경우 해당 IP도 추가합니다.
- 

Radius 클라이언트

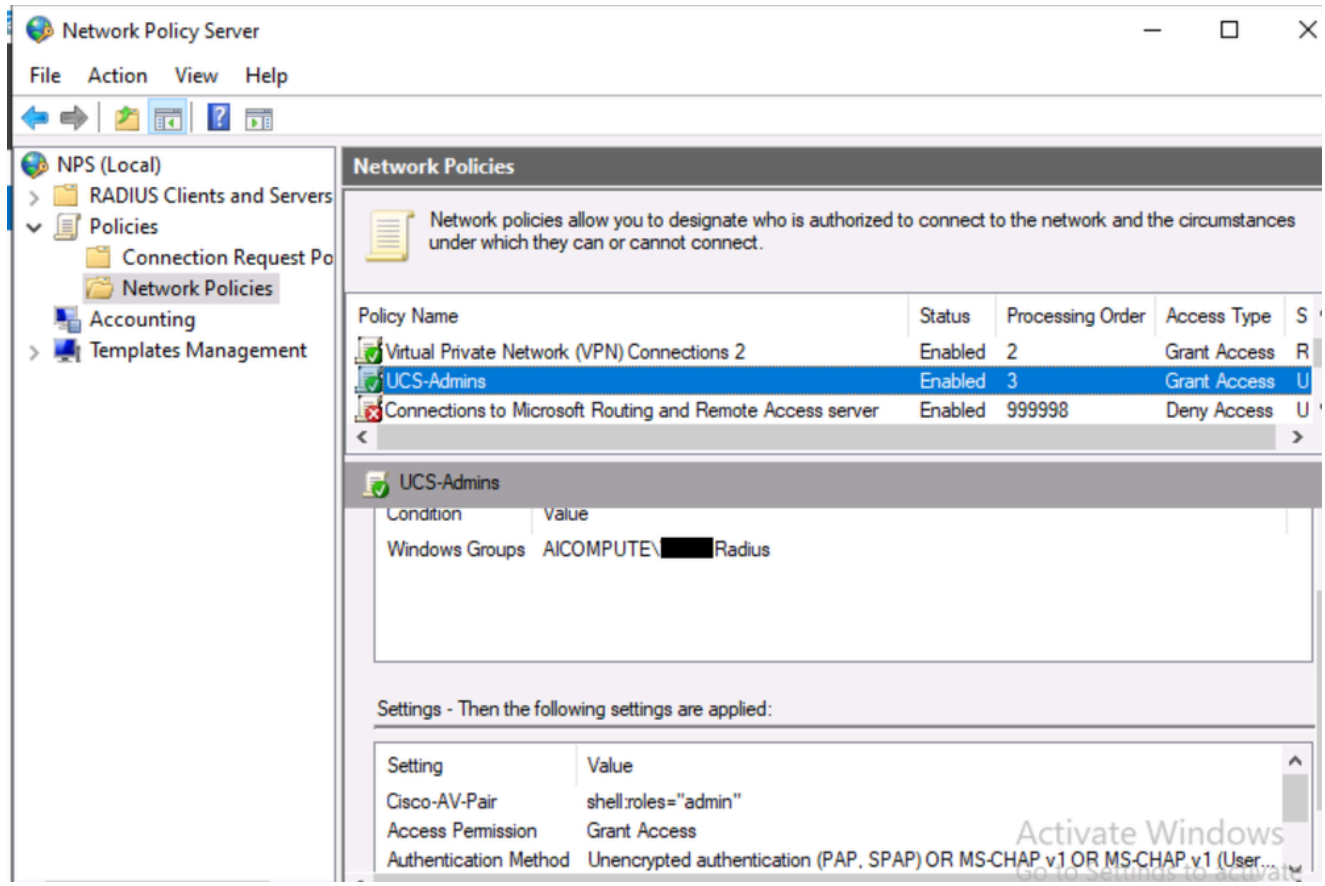
연결 요청 정책 및 네트워크 정책 생성(권한 부여 및 역할 매핑)

- Policies(정책) > Connection Request Policies(연결 요청 정책) > New(새로 만들기) > Name it(이름 지정)(예 - UCS-radiustest)에서 'Client Friendly Name(클라이언트 친화적 이름)' 조건을 추가합니다. 그러면 로컬에서 인증할 수 있습니다. 예를 들면 다음과 같습니다. FI-* 또는 UCSM,
- Policies(정책) > Network Policies(네트워크 정책) > New(신규) > Policy name(정책 이름)
  - 조건: Windows 그룹을 추가합니다. 3단계에서 만든 testRadius 그룹을 선택합니다.
  - 액세스 권한: 액세스 권한 부여
  - 인증 방법: unencrypted authentication(PAP/SPAP) 및/또는 UCS에서 사용하는 방법을 활성화합니다. (UCS RADIUS는 일반적으로 PAP를 사용합니다.)
- Configure Settings(설정) > Vendor Specific Attributes(공급업체별 특성)(AD 사용자를 UCS 역할에 매핑하는 핵심 부분): 공급업체별 특성 추가 > Cisco AV-Pair
  - 값을 UCS role/locale 문자열로 설정합니다(예: shell:roles="admin"). 이 특성을 건너뛰면 사용자가 읽기 전용으로 로그인합니다.

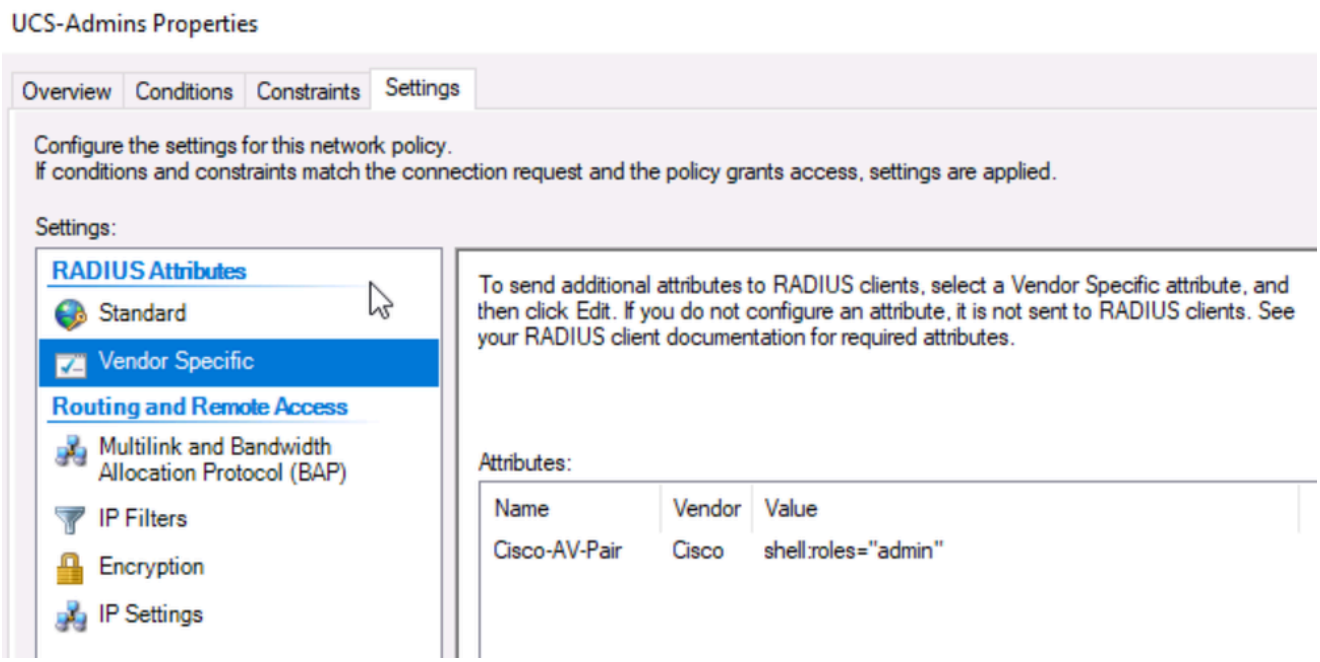
연결 요청 정책

- 

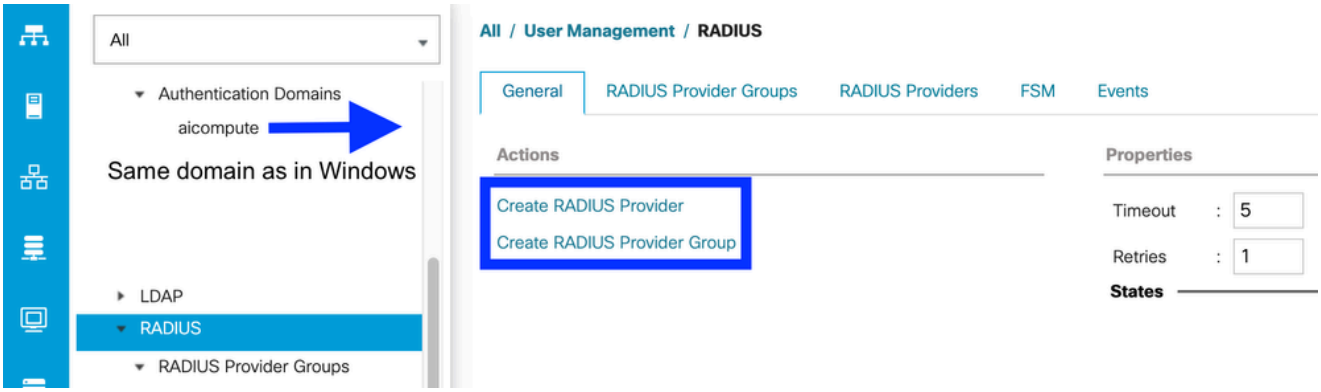
네트워크 정책

- 

공급업체별 특성

- 

UCSM의 컨피그레이션

- 

Radius 제공자 생성 및 제공자 그룹에 추가

1. UCS Manager GUI에 로그인하고 Admin(관리) > User Management(사용자 관리) > RADIUS로 이동합니다.

2. RADIUS 제공자 생성(+/ 생성 옵션)을 클릭하고 다음을 입력합니다.

- 호스트 이름/FQDN 또는 IP: Windows NPS 서버
- 키: nps 5단계에서 설정한 정확한 공유 암호.

- 권한 부여 포트: 1812(NPS와 일치해야 함)
- 시간 초과/재시도: 기본값을 start(시작)로 둡니다.

3. Admin(관리) > User Management(사용자 관리) > RADIUS에서 제공자 그룹(예 - RADIUS-Grp)을 생성하고 이전 제공자를 추가합니다.

인증 도메인 생성

이 조각은 이 모든 것을 하나로 묶어줍니다.

1. Admin(관리) > User Management(사용자 관리) > Authentication(인증) > Authentication Domains(인증 도메인)로 이동합니다.

2. Create a Domain (Example - RADIUS - domain name recommended to be the same in NPS)을 클릭합니다.

3. 영역 = RADIUS를 설정합니다.

4. 생성한 제공 기관 그룹(RADIUS-Grp)을 지정하고 저장합니다.

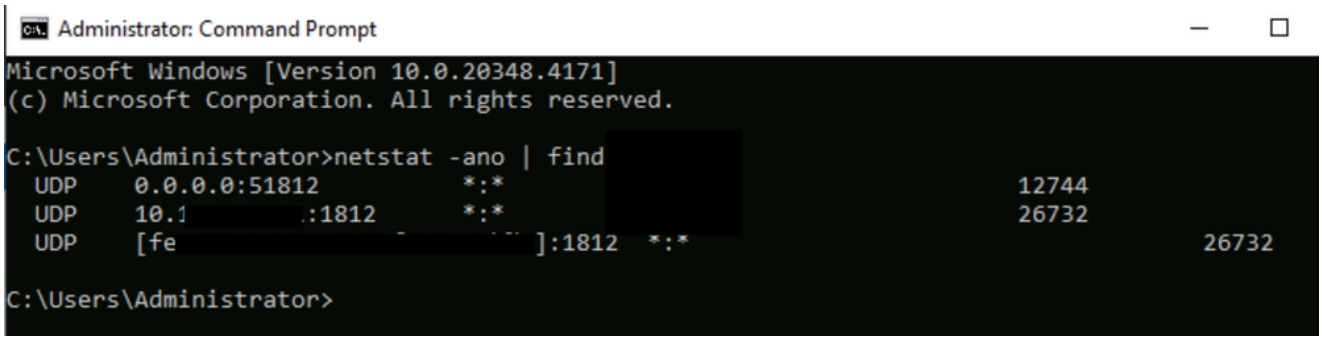
다음을 확인합니다.

Windows Server에서 방화벽/포트 확인

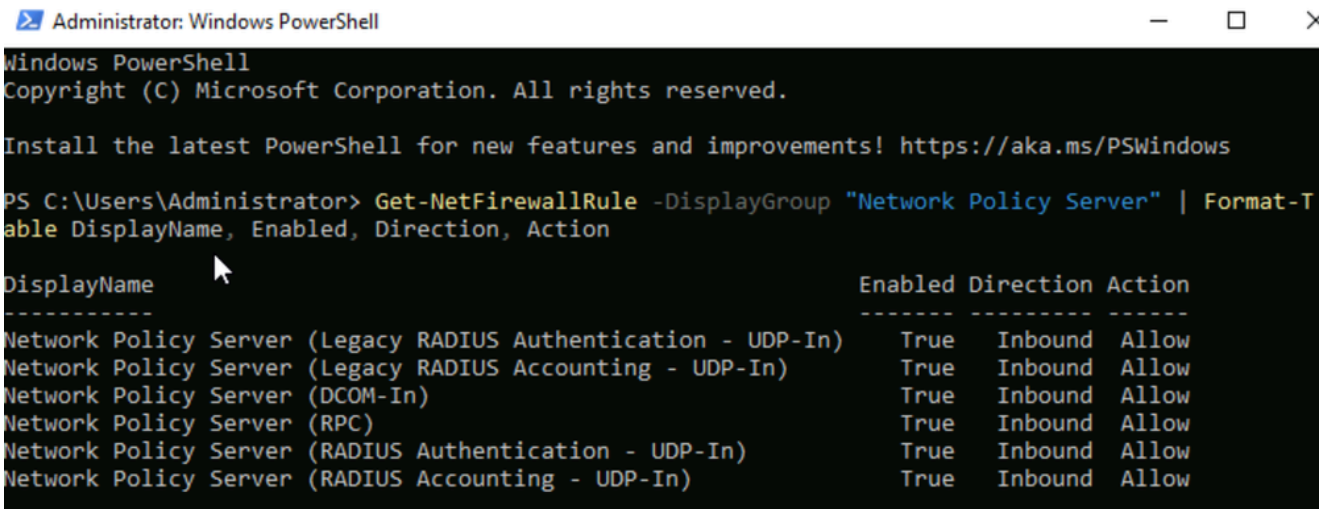
RADIUS 인증에서는 UDP 포트 1812(및 어카운팅 1813)를 사용합니다. Windows 방화벽과 모든 네트워크 방화벽에서 FI 관리 IP에서 이러한 방화벽을 허용하는지 확인합니다.

1. NPS/Radius 서비스가 netstat -ano를 통해 수신 대기 중인지 확인합니다. | findstr 1812 명령입니다.

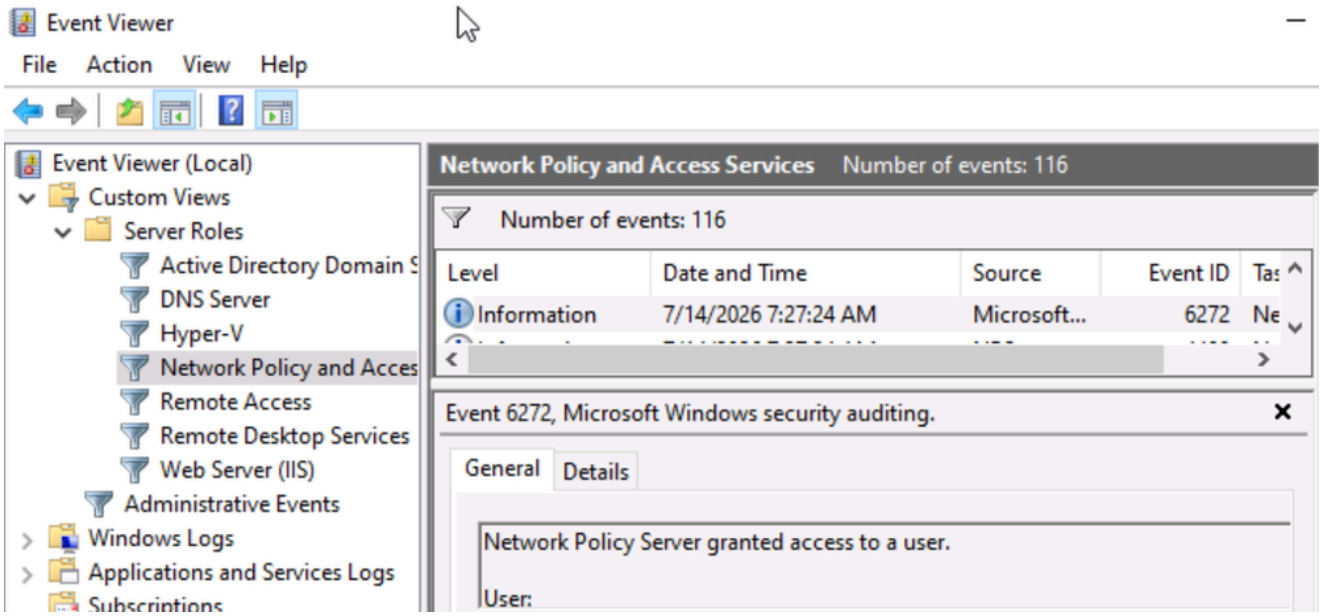
- UDP 및 *:1812(또는 서버 IP:1812)가 있는 줄이 표시됩니다. 이는 NPS/RADIUS 서비스가 능동적으로 수신 대기하고 있음을 확인합니다.
- 아무것도 표시되지 않으면 NPS를 실행할 수 없습니다. Services(서비스) > Network Policy Server (IAS) is Started(네트워크 정책 서버(IAS)가 시작됨)를 확인하십시오.)



- Windows Powershell에서 다음 명령을 실행합니다.
  - Get-NetFirewallRule -DisplayGroup "네트워크 정책 서버" | Format-Table DisplayName, Enabled, Direction, Action.



- Windows 이벤트 뷰어:
  - Custom Views(맞춤형 보기) > Server Roles(서버 역할) > Network Policy and Access Services(네트워크 정책 및 액세스 서비스) > Packets(패킷)가 표시됩니다.



UCSM에서 로그인 테스트

1. 로그아웃한 후 생성된 Radius 도메인에 따라 도메인 드롭다운을 선택하여 로그인합니다.

2. 사용자 비밀번호를 구성합니다. (Windows 구성 2단계 참조).

- 로그인이 작동하고 관리자 권한으로 랜딩하는 경우 Cisco AV 쌍 매핑(Windows 구성 6단계)이 정확합니다.

Radius 인증 문제 해결

Windows 서버에서

1. 패킷 캡처를 위해 Powershell에서 다음 명령을 실행합니다.

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

2. UCSM에서 로그인을 시작하고 명령을 사용하여 캡처를 중지합니다.

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

3. Wireshark에서 radius_capture.pcap를 엽니다. RADIUS > 속성 값 쌍 > 메시지 인증자 확인(또는 속성 80)이 있습니다. 이는 NPS가 회신에 서명하고 있음을 의미합니다.

UCSM CLI에서

UCSM CLI에서 Windows에서 pktmon을 동시에 실행할 경우

1. 실행:

- nxos 연결
- 단말기 모니터
- 모두 RADIUS 디버그

2 . 디버그를 시작한 후 UCSM 로그인을 시도합니다.

성공적인 로그인은 2026년 7월 3일 09:54:02.917044 radius:Verified Message Authenticator의 응답과 유사합니다. 10.xxx.xx.xx

- 패킷을 보내고 받았지만 메시지 인증자로 로그인이 실패하는 경우는 올바르지 않을 수 있습니다. 디버그 출력에서 이는 포트 및 연결성이 정상임을 의미합니다.
  - Windows NPS 서버 및 UCSM 키에서 공유 암호를 다시 한 번 재구성합니다(정확히 일치해야 함).
  - 사후 재구성에 로그인하는 동안 문제가 지속되면 알려진 Cisco 버그 ID CSCwm80801에 도달할 수 있습니다. Microsoft 패치 KB5040434가 언급된 고정 릴리스로 업그레이드해야 하는 경우 사용자는 Radius를 사용하여 UCSM에 로그인할 수 없습니다.

관련 정보

- Cisco UCS Manager 관리 관리 가이드 4.2 - 원격 인증

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.