Configurar e solucionar problemas de autenticação Radius no UCSM

Contents

Introdução

Este documento descreve as etapas para configurar e solucionar problemas do Radius no UCS Manager usando um Windows Server 2022 DataCenter.

Pré-requisitos

- UCS Manager - 4.2(3o) ou superior
- Data center do Windows Server 2022

Configuração no Windows Server

Instalar Serviços de Domínio Ative Diretory

Consulte o documento da Microsoft - Instalar o AD DS usando o Gerenciador de Servidores no Windows Server 2022.

Criar o Usuário do Ative Diretory (Conta de Logon)

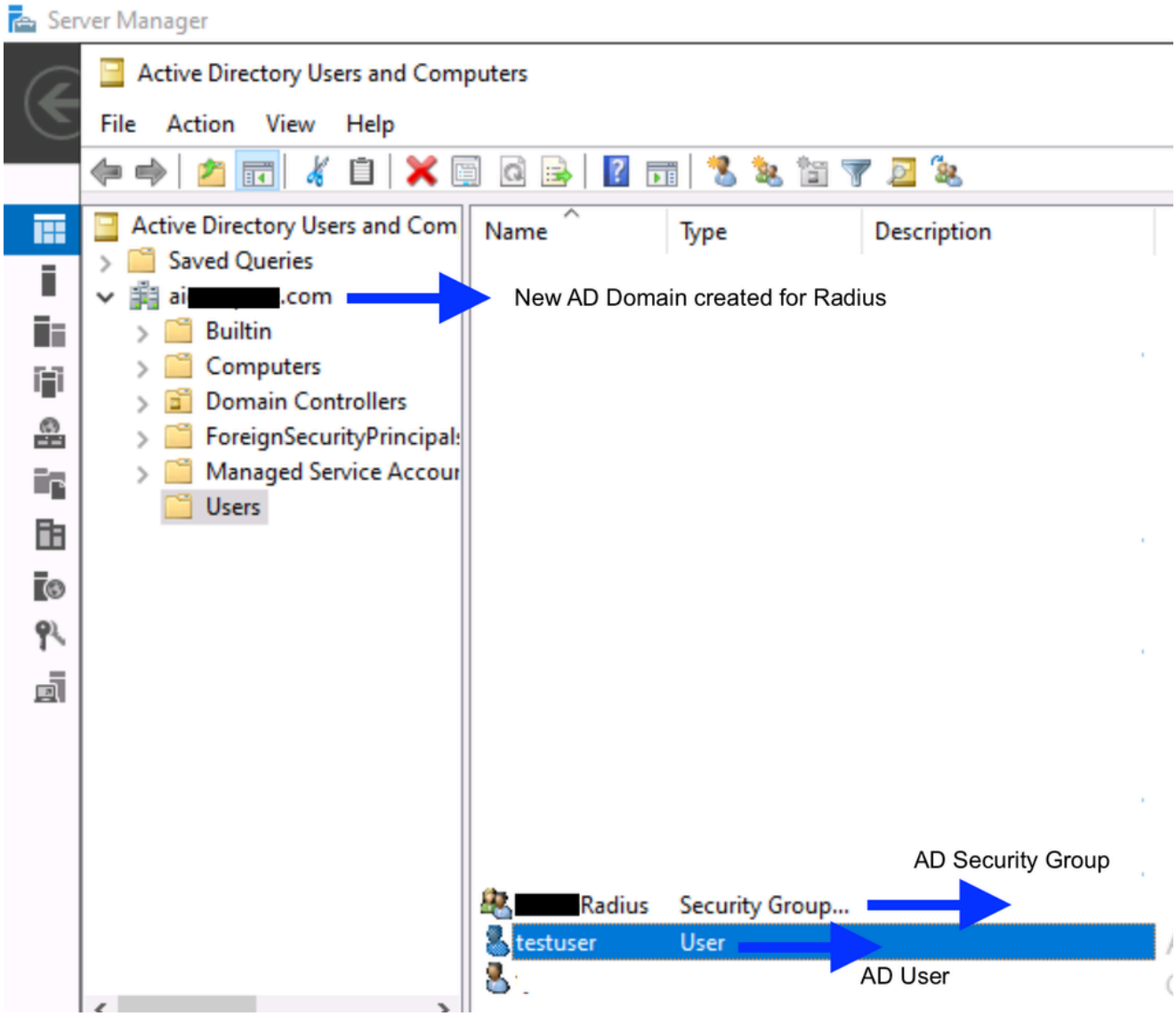
1. Abra Server Manager > Ferramentas > Usuários e Computadores do Ative Diretory.

2. Clique com o botão direito do mouse no domínio criado Novo > Usuário.

3. Insira o nome de logon (Exemplo - testuser), defina uma senha, desmarque O usuário deve alterar a senha no próximo logon e marque A senha nunca expira (para uma conta de serviço/administrador) > Concluir (sujeito aos seus requisitos/políticas de segurança locais).

Criar um grupo do AD Security para administradores do UCS

- No mesmo console, clique com o botão direito do mouse no seu domínio Novo > Grupo (Exemplo - testRadius, Segurança). Adicione o usuário do AD testuser) a este grupo.
- Esse nome de grupo é o que você terá que mapear posteriormente para uma função do UCS.

- 

Instalar o NPS (função RADIUS) e Registrar o NPS no Ative Diretory

1. Navegue até Server Manager > Manage > Add Roles and Features.

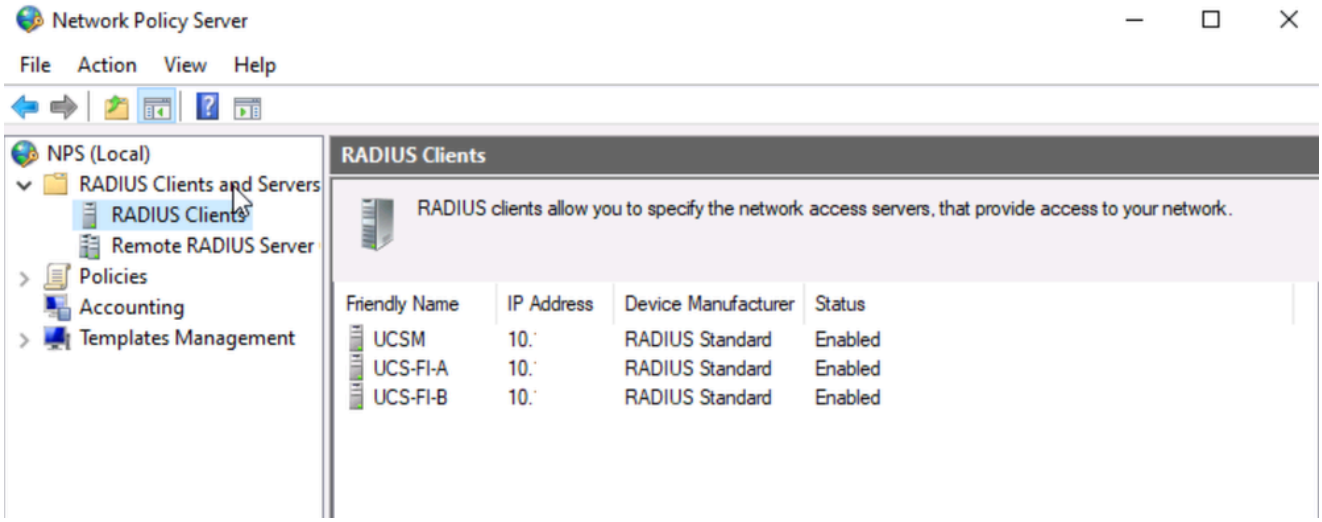
2. Selecione Serviços de Acesso e Diretiva de Rede > Concluir o assistente para instalar o NPS (Servidor de Diretivas de Rede).

3. Abra Ferramentas > Servidor de Políticas de Rede. Clique com o botão direito do mouse em NPS (Local) > Registrar servidor no Ative Diretory > OK. Isso permite que o NPS leia a associação de usuário/grupo do AD.

Adicione as interconexões em malha do UCS como clientes RADIUS

- Isso instrui o NPS a confiar em solicitações do UCSM. No NPS, expanda Clientes e

servidores RADIUS > Clientes RADIUS. clique com o botão direito do mouse em New.

- Fornecer:
  - Nome amigável: Exemplo - UCSM
  - Endereço (IP) o IP de gerenciamento do FI-A
  - shared secret: crie um segredo forte e anote-o — você deve digitar essa sequência de segredo compartilhada exata no UCSM posteriormente.
- Repita o procedimento para o Interconector de estrutura B e, se você for autenticar no VIP do cluster, adicione esse IP também.
- 

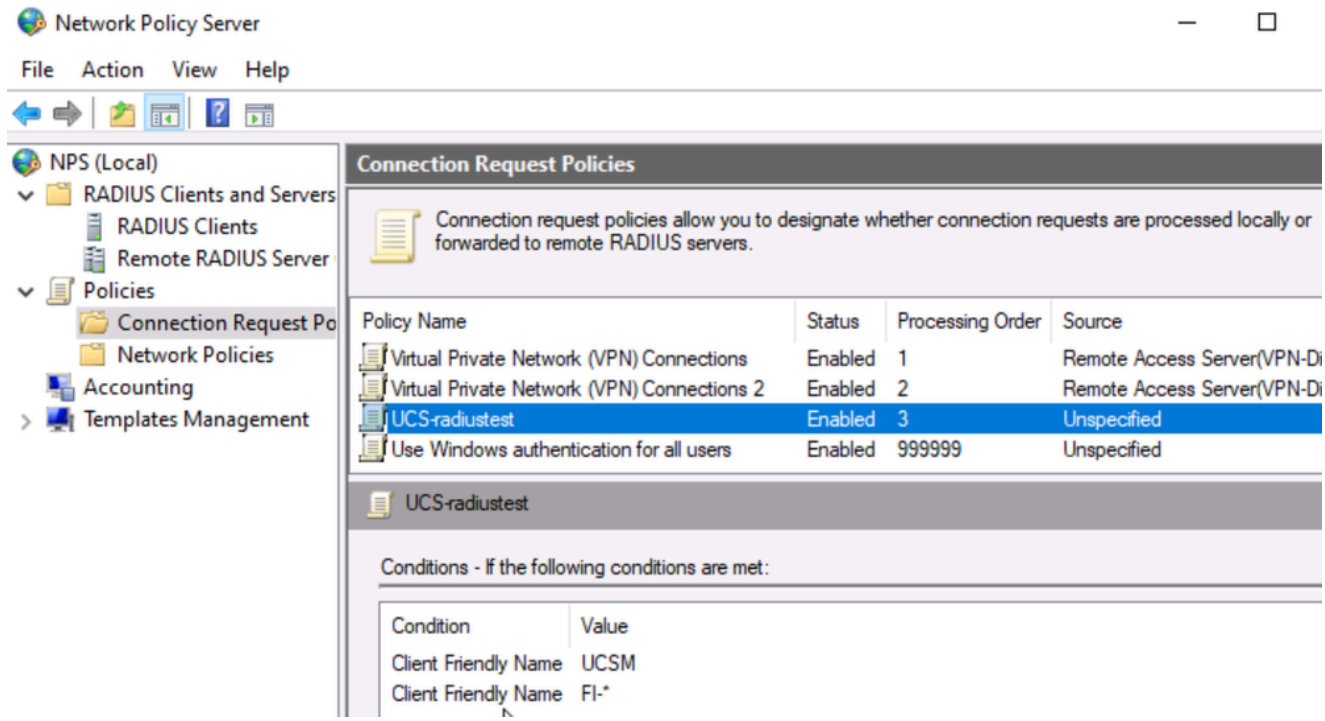
Clientes Radius

Criar uma Política de Solicitação de Conexão e uma Política de Rede (Autorização e Mapeamento de Função)

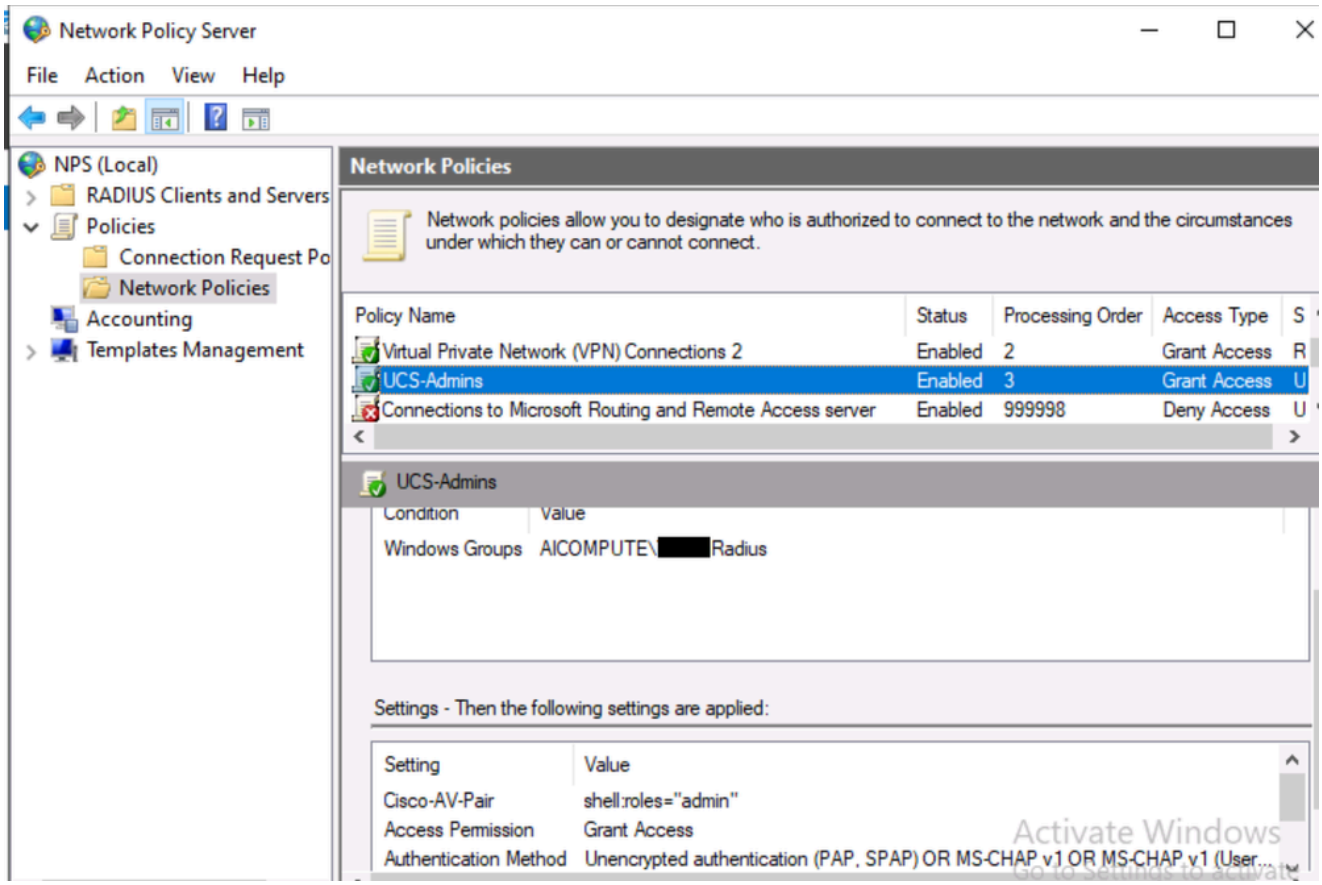
- Policies > Connection Request Policies > New > Name it (Example - UCS-radiustest), adicione a condição para 'Client Friendly Name', que permite a autenticação local. Por exemplo: FI-* ou UCSM,
- Políticas > Políticas de rede > Novo > Nome da política
  - Condições: adicionar Grupos do Windows. Selecione o grupo testRadius criado na Etapa 3.
  - Permissão de acesso: Conceder acesso
  - Métodos de autenticação: habilite a autenticação sem criptografia (PAP/SPAP) e/ou os métodos que o UCS usa. (O UCS RADIUS geralmente usa PAP.)
- Configurar Configurações > Atributos específicos do fornecedor (esta é a parte chave que mapeia o usuário do AD para uma função do UCS): Adicionar um atributo específico do fornecedor > Cisco AV-Pair
  - Defina o valor para a string de função/local do UCS, Exemplo - shell:roles="admin" (Se

você ignorar este atributo, o usuário fará login como somente leitura).

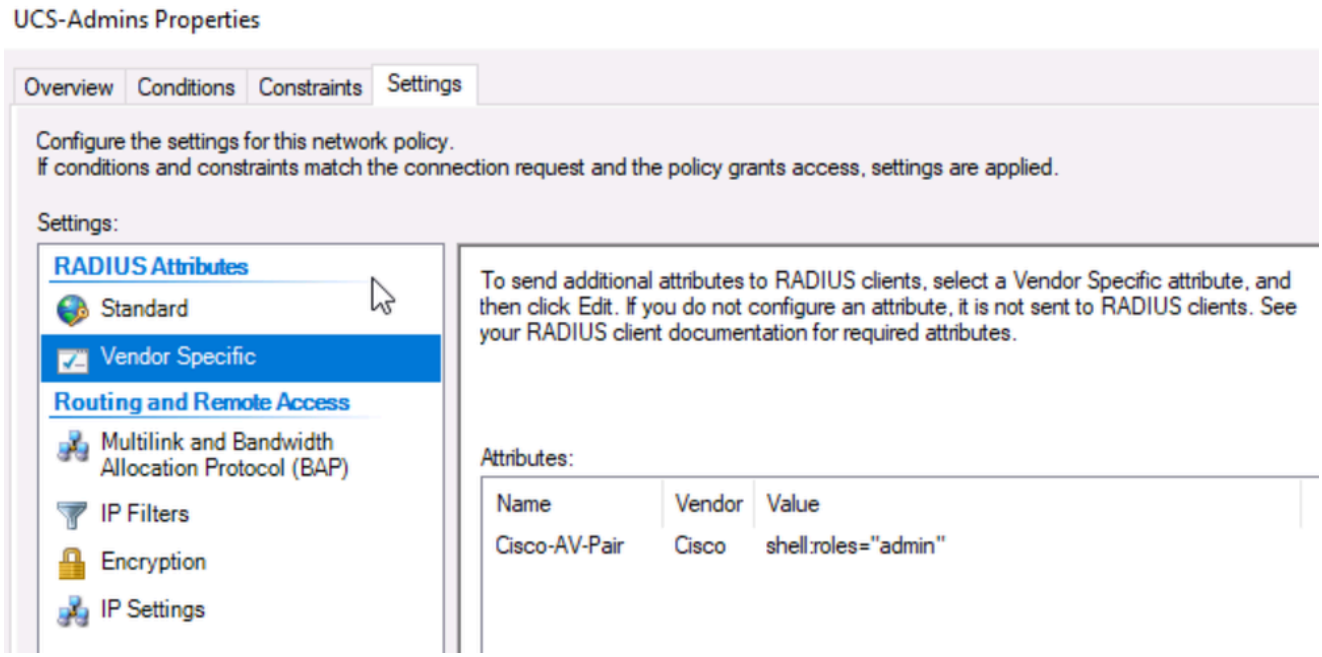
Política de Solicitação de Conexão

- 

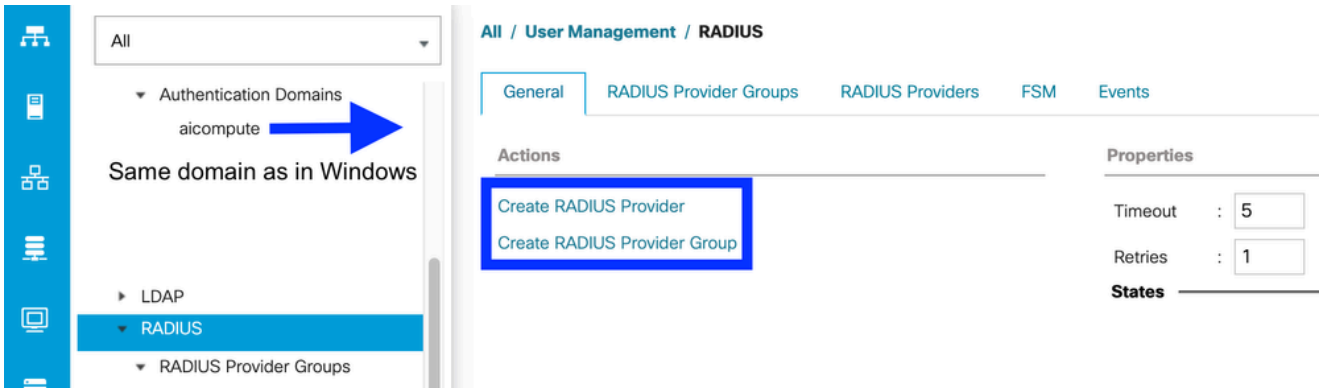
Política de rede



Atributo Específico do Fornecedor



Configuração no UCSM

- 

Crie um provedor Radius e adicione a um grupo de provedores

1. Faça login na GUI do UCS Manager e navegue até Admin > User Management > RADIUS.

2. Clique em Criar Provedor RADIUS (a opção +/ Criar) e preencha:

- Nome de host/FQDN ou IP: seu servidor Windows NPS.
- Chave: o segredo compartilhado exato definido na Etapa 5 do NPS.
- Porta de autorização: 1812 (deve corresponder ao NPS)
- Tempo limite / Novas tentativas: deixe os padrões para iniciar.

3. Em Admin >User Management > RADIUS, crie um Grupo de Provedores (Exemplo - RADIUS-Grp) e adicione o provedor a partir de anterior.

Criar um domínio de autenticação

Esta é a peça que une tudo.

1. Navegue até Admin > User Management > Authentication > Authentication Domains.

2. Clique em Criar um Domínio (Exemplo - RADIUS - recomenda-se que o nome de domínio seja o mesmo que o criado no NPS).

3. Definir Território = RADIUS.

4. Atribua o Grupo de Provedores que você criou (RADIUS-Grp) e Salve.

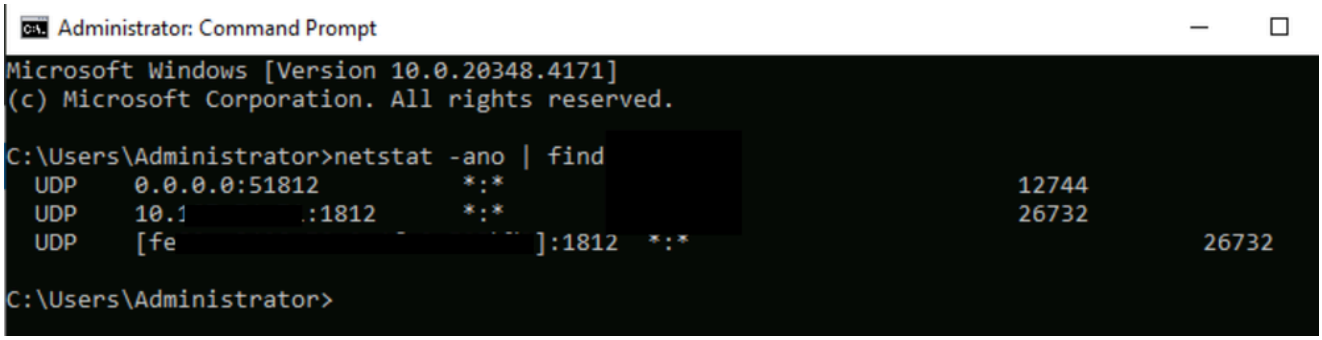
Verificar

A partir do Windows Server - Confirmar firewall/portas

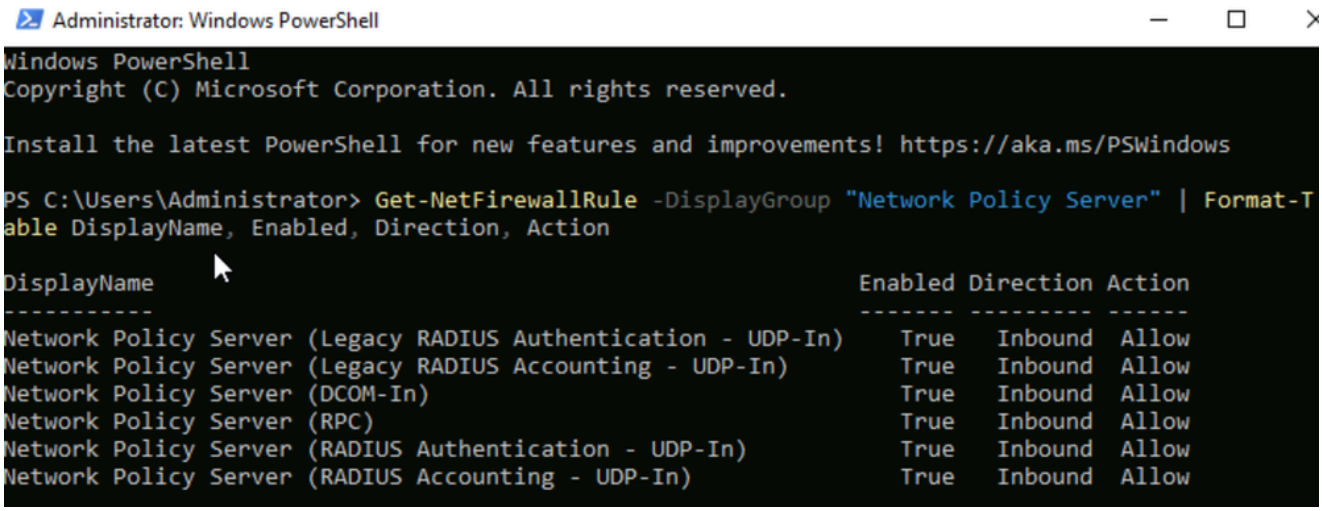
A autenticação RADIUS usa a porta UDP 1812 (e a contabilidade 1813). Verifique se o firewall do Windows e qualquer firewall de rede permitem isso nos IPs de gerenciamento de FI.

1. Confirme se o serviço NPS / Radius está escutando através do netstat -ano | comando findstr 1812.

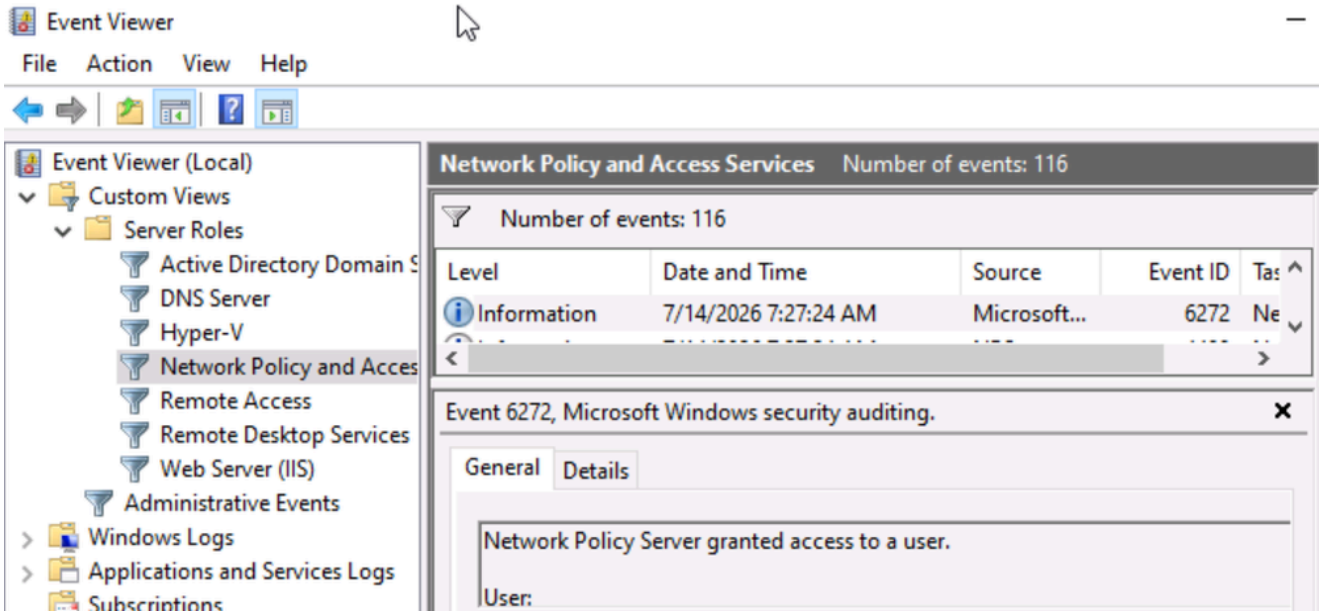
- (Você verá uma linha com UDP e *:1812 (ou o IP do servidor:1812). Isso confirma que o serviço NPS/RADIUS está escutando ativamente.
- Se nada aparecer, o NPS não pôde ser executado — verifique Services > Network Policy Server (IAS) is Started.)



- No Windows Powershell, execute o comando:
  - Get-NetFirewallRule -DisplayGroup "Servidor de Diretiva de Rede" | Format-Table DisplayName, Enabled, Direction, Action.



- No Visualizador de Eventos do Windows:
  - Custom Views > Server Roles > Network Policy and Access Services > Packets are reach (Exibições personalizadas > Funções do servidor > Serviços de acesso e política de rede > Pacotes estão chegando).



Testar login do UCSM

1. Faça logoff e logon escolhendo a lista suspensa Domínio de acordo com o domínio Radius criado.

2. Configure a senha do usuário. (Consulte a etapa 2 da configuração do Windows).

- Se o login funcionar e você chegar com privilégios de administrador, o mapeamento do par AV da Cisco (etapa 6 da configuração do Windows) está correto.

Identificar e solucionar problemas de autenticação Radius

Do Windows Server

1. Execute estes comandos no Powershell para captura de pacotes:

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

2. Inicie o login a partir do UCSM e pare a captura usando comandos :

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

3. Abra radius_capture.pcap no Wireshark: RADIUS > Attribute Value Pairs > confirm Message-Authenticator (ou attribute 80) está presente. Isso significa que o NPS está assinando a resposta.

Da CLI do UCSM

Ao executar o pktmon no Windows, simultaneamente a partir da CLI do UCSM,

1. executar:

- connect nxos
- monitor de terminal
- debug radius all

2. tente um login UCSM após iniciar a depuração.

Um login bem-sucedido se parece com 2026 Jul 3 09:54:02.917044 radius:Verified Message Authenticator em resposta de: 10.xxx.xx.xx.

- Se os pacotes forem enviados e recebidos, mas o login estiver falhando com o autenticador de mensagem provavelmente está incorreto. na saída de depuração - isso implica que a porta e o alcance estão bem.
  - Tente reconfigurar o segredo compartilhado no servidor Windows NPS e a chave UCSM novamente (eles precisam ser exatamente correspondentes).
  - Se o problema persistir durante o login após a reconfiguração, podemos estar atingindo um bug da Cisco ID CSCwm80801 : O usuário não pode fazer login no UCSM usando Radius após o patch KB5040434 da Microsoft exigir uma atualização para uma versão fixa mencionada.

Informações Relacionadas

- Guia de gerenciamento de administração do Cisco UCS Manager 4.2 - Autenticação remota

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.