Configuración y resolución de problemas de autenticación Radius en UCSM

Contenido

Introducción

Este documento describe los pasos para configurar y resolver problemas de Radius en UCS Manager mediante un DataCenter de Windows Server 2022.

Prerequisites

- UCS Manager - 4.2(3o) o superior
- DataCenter de Windows Server 2022

Configuración en Windows Server

Instalar Servicios de dominio de Active Directory

Consulte el documento de Microsoft: Instalación de AD DS mediante el Administrador del servidor en Windows Server 2022.

Crear el usuario de Active Directory (cuenta de inicio de sesión)

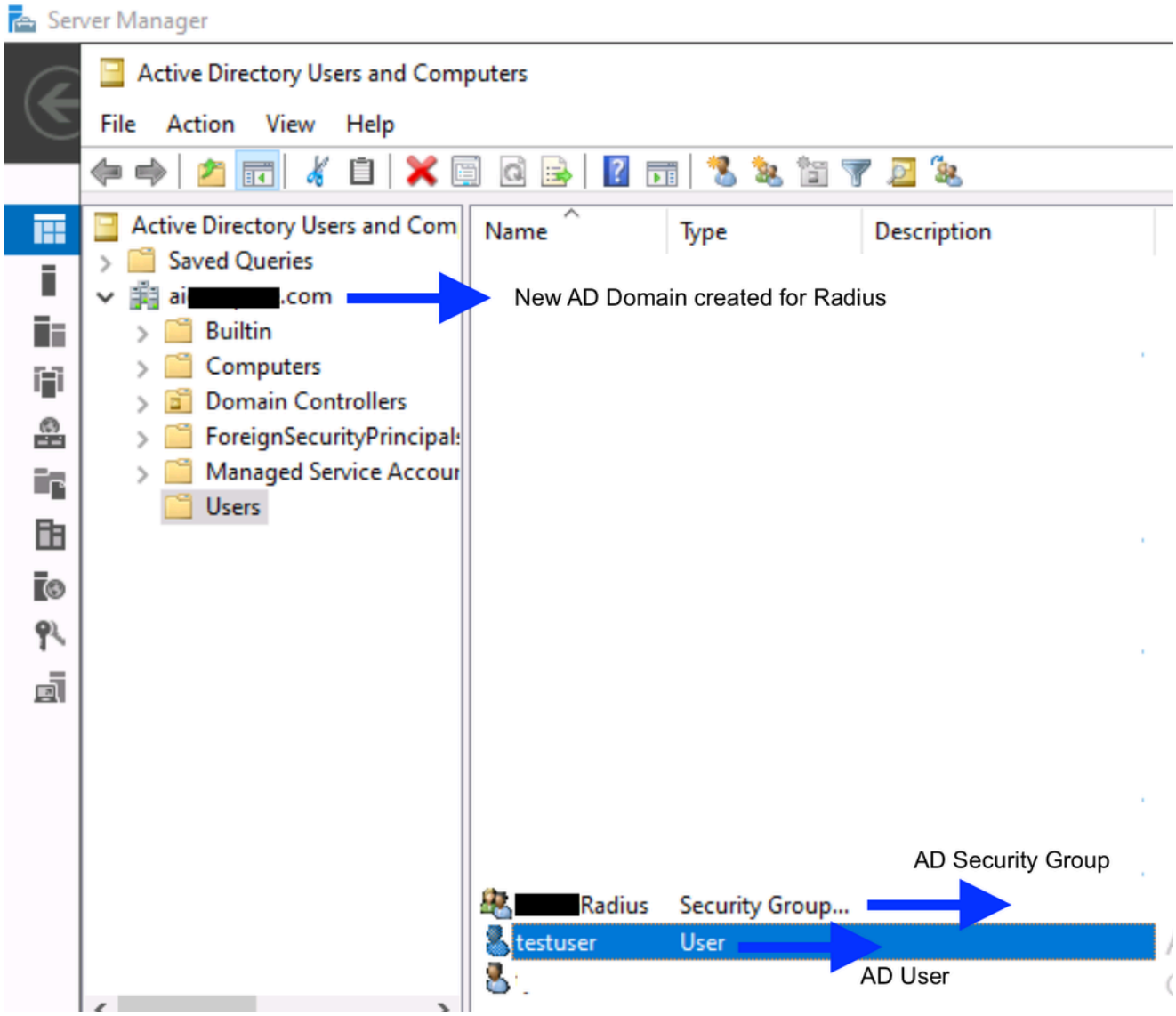
1. Abra Administrador del servidor > Herramientas > Usuarios y equipos de Active Directory.

2. Haga clic con el botón derecho del ratón en su dominio creado Nuevo > Usuario.

3. Introduzca el nombre de inicio de sesión (Ejemplo: usuario de prueba), defina una contraseña, desactive El usuario debe cambiar la contraseña en el siguiente inicio de sesión y marque La contraseña nunca caduca (para una cuenta de servicio/administrador) > Finalizar (según sus requisitos o políticas de seguridad locales).

Crear un grupo de seguridad de AD para administradores de UCS

- En la misma consola, haga clic con el botón secundario en el dominio Nuevo > Grupo (Ejemplo: testRadius, Seguridad). Agregue el usuario de AD testuser a este grupo.
- Este nombre de grupo es lo que tiene que asignar posteriormente a una función de UCS.

- 

Instalar NPS (rol RADIUS) y registrar NPS en Active Directory

1. Vaya a Administrador del servidor > Administrar > Agregar funciones y características.

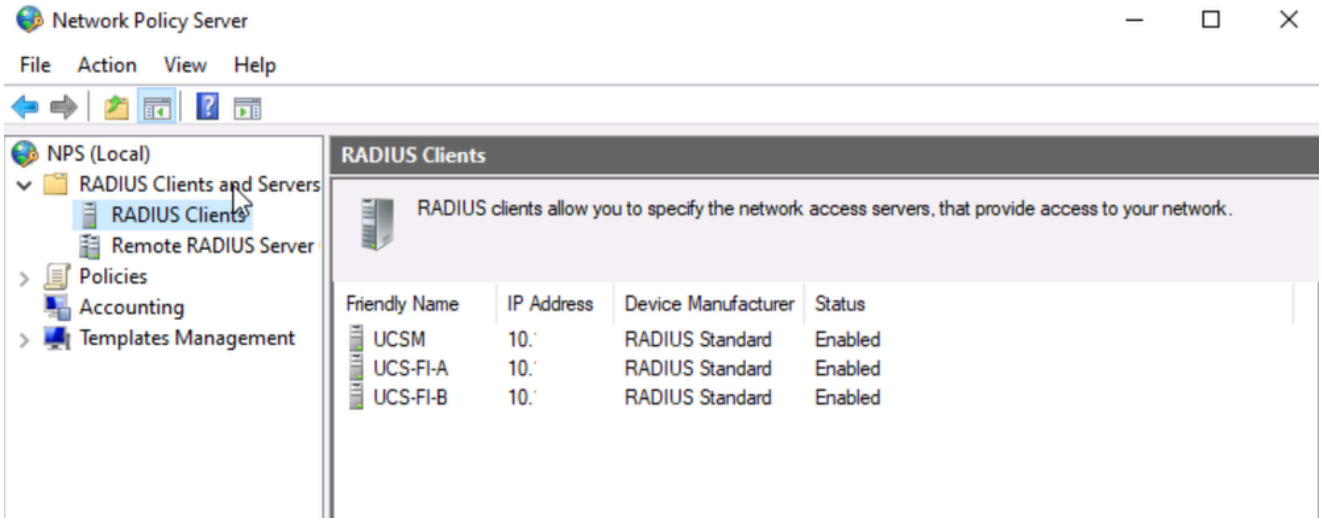
2. Seleccione Network Policy and Access Services > Complete el asistente para instalar Network Policy Server (NPS).

3. Abra Tools > Network Policy Server. Haga clic con el botón derecho del mouse en NPS (Local) > Registrar servidor en Active Directory > Aceptar. Esto permite a NPS leer la pertenencia a usuarios/grupos de AD.

Adición de Fabric Interconnects UCS como clientes RADIUS

- Esto indica a NPS que confíe en las solicitudes de UCSM. En NPS, expanda Clientes y

servidores RADIUS > Clientes RADIUS. haga clic con el botón secundario en Nuevo.

- Proporcionar:
  - Nombre descriptivo: Ejemplo: UCSM
  - Dirección (IP): la IP de administración de FI-A
  - secreto compartido: cree un secreto seguro y anótelo: debe introducir esta cadena secreta compartida exacta en UCSM más adelante.
- Repita este procedimiento para Fabric Interconnect B y, si desea autenticarse con el VIP del clúster, agregue también esa IP.
- 

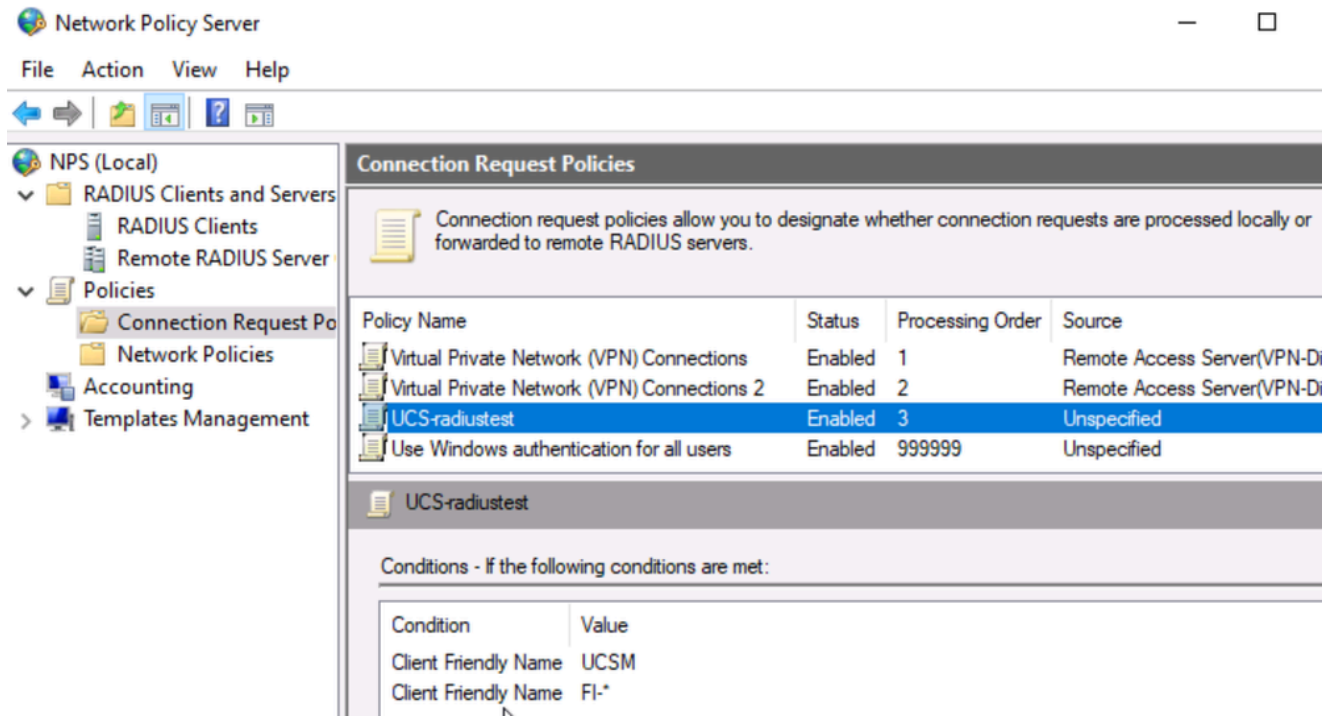
Clientes Radius

Crear una directiva de solicitud de conexión y una directiva de red (autorización y asignación de funciones)

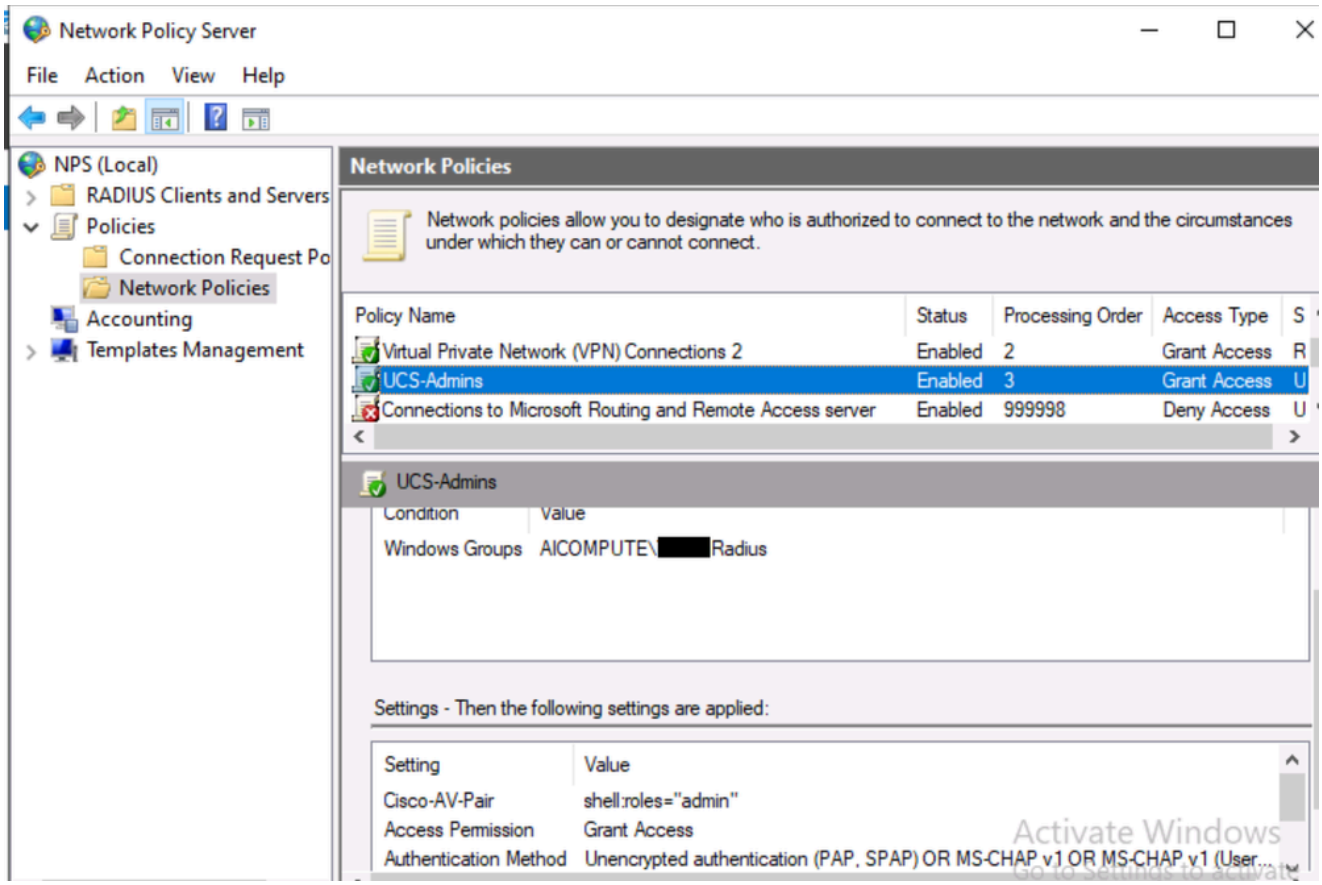
- Policies > Connection Request Policies > New > Name it (Example - UCS-radiustest), agregue la condición para 'Client Friendly Name' que le permite autenticarse localmente. Por ejemplo: FI-* o UCSM,
- Políticas > Políticas de red > Nuevo > Nombre de política
  - Condiciones: agregar grupos de Windows. Seleccione el grupo testRadius que realizó en el paso 3.
  - Permiso de acceso: Conceder acceso
  - Métodos de autenticación: habilitar la autenticación sin cifrar (PAP/SPAP) o los métodos que utiliza UCS. (UCS RADIUS suele utilizar PAP.)
- Configuración > Atributos específicos del proveedor (esta es la parte clave que asigna el usuario de AD a una función de UCS): Agregar un atributo específico del proveedor > Par AV de Cisco
  - Establezca el valor en la cadena de función/configuración regional de UCS, Ejemplo -

shell:roles="admin" (Si omite este atributo, el usuario inicia sesión como de solo lectura).

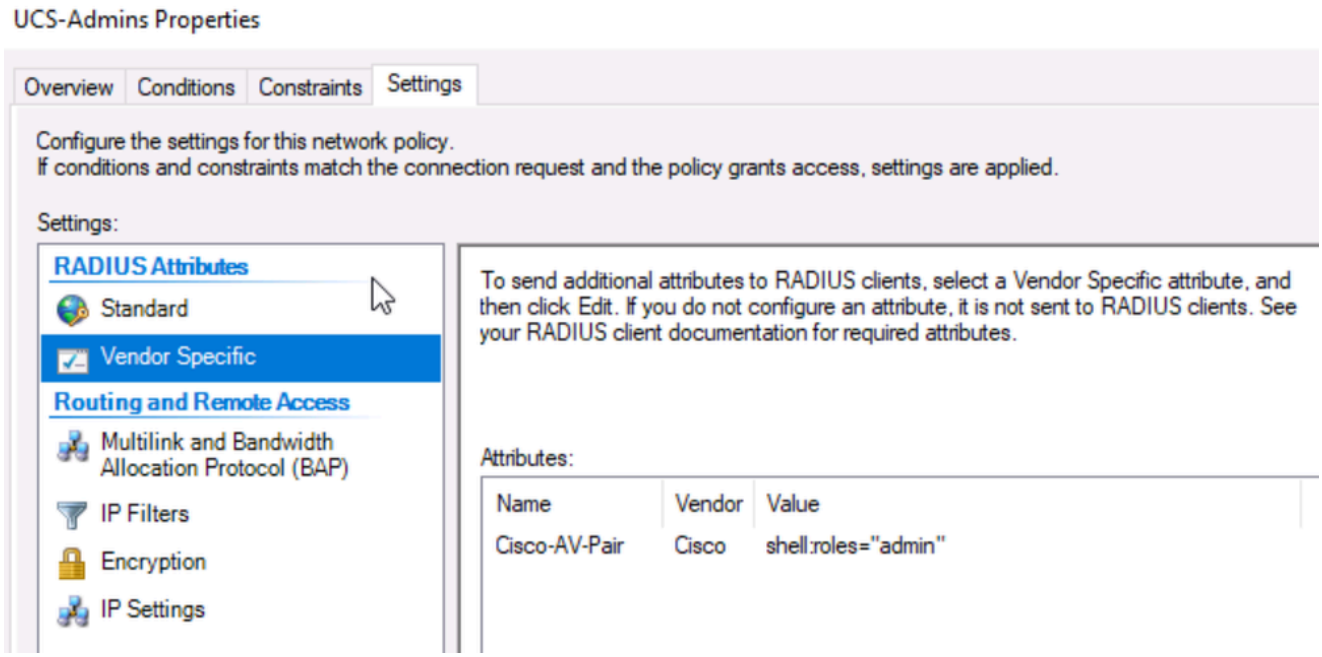
Directiva de solicitud de conexión

- 

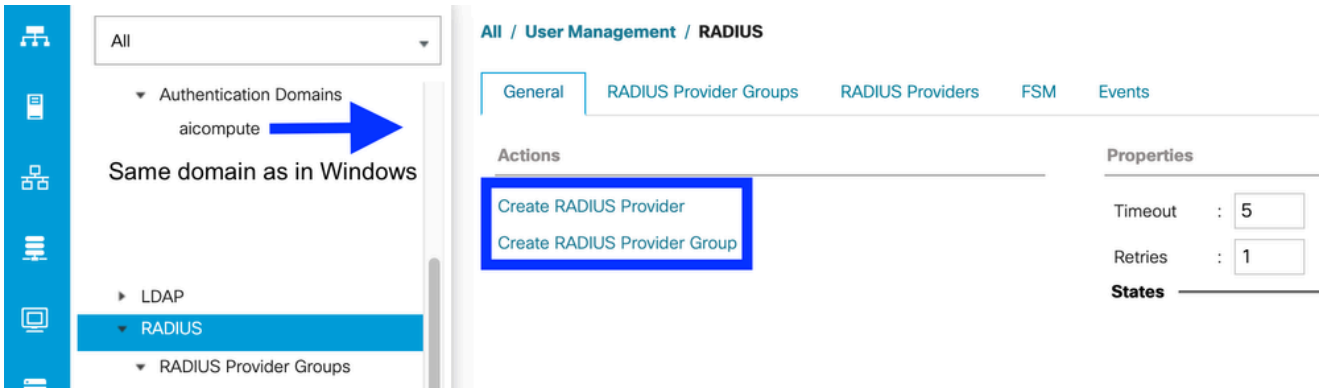
Política de red

- 

Atributo específico del proveedor

- 

Configuración en UCSM

- 

Creación de un proveedor Radius y adición a un grupo de proveedores

1. Inicie sesión en la GUI de UCS Manager y navegue hasta Admin > User Management > RADIUS.

2. Haga clic en Create RADIUS Provider (la opción +/ Create) y rellene:

- Nombre de host/FQDN o IP: el servidor NPS de Windows.
- Clave: Seleccione la clave secreta compartida exacta que haya establecido en el paso 5 de NPS.
- Puerto de autorización: 1812 (debe coincidir con NPS)
- Tiempo de espera/reintentos: deje los valores predeterminados para iniciar.

3. En Admin >User Management > RADIUS, cree un grupo de proveedores (Ejemplo: RADIUS-Grp) y agregue el proveedor de la versión anterior.

Crear un dominio de autenticación

Esta es la pieza que lo une todo.

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

2. Haga clic en Create a Domain (Ejemplo: RADIUS; se recomienda que el nombre de dominio sea el mismo que el dominio creado en NPS).

3. Establezca Rango = RADIUS.

4. Asigne el grupo de proveedores que ha creado (RADIUS-Grp) y guarde.

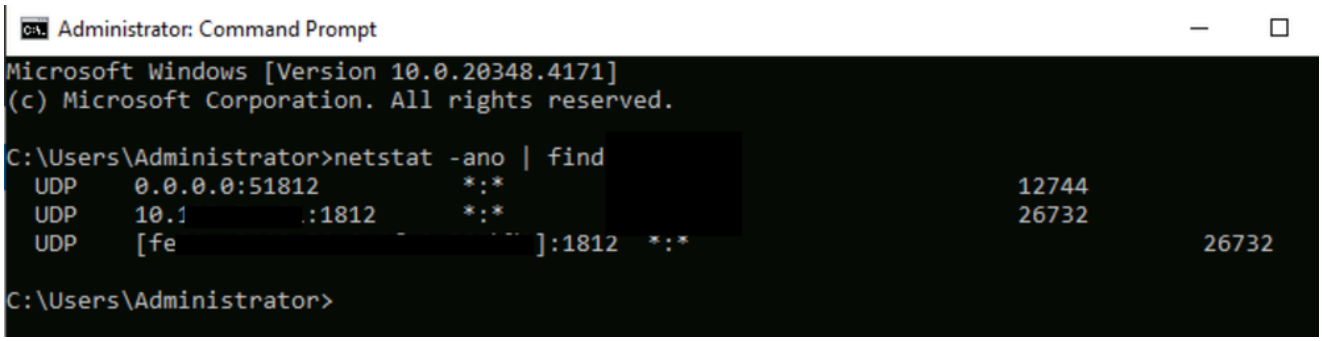
Verificación

Desde Windows Server - Confirmar firewall / puertos

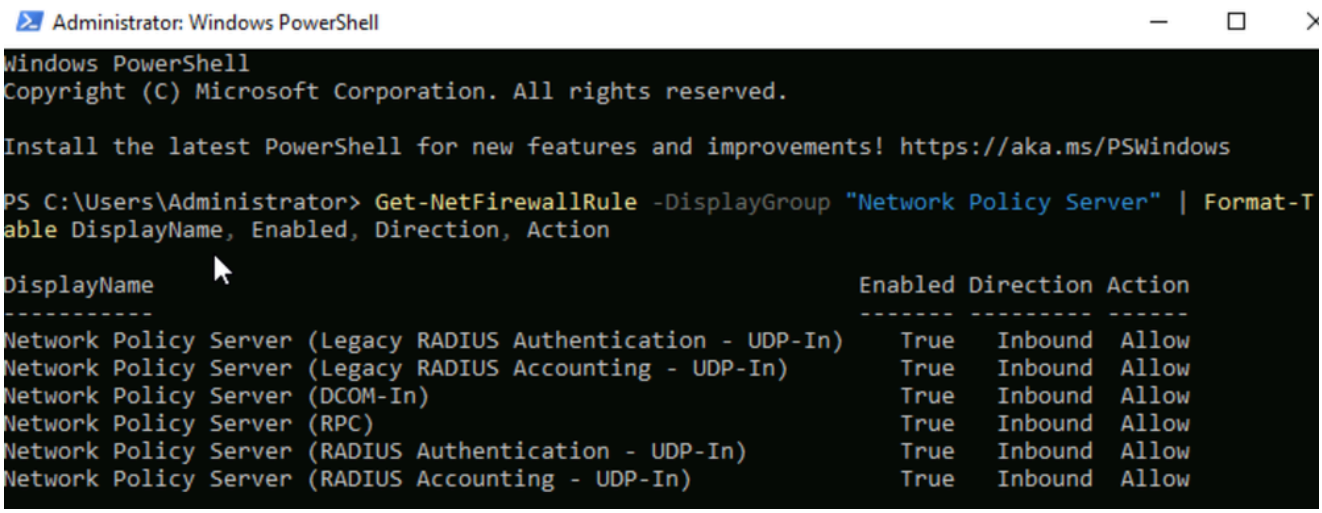
La autenticación RADIUS utiliza el puerto UDP 1812 (y la contabilización 1813). Asegúrese de que el firewall de Windows y cualquier firewall de red lo permitan desde las IP de administración de FI.

1. Confirme que el servicio NPS / Radius está escuchando a través de netstat -ano | findstr 1812 command.

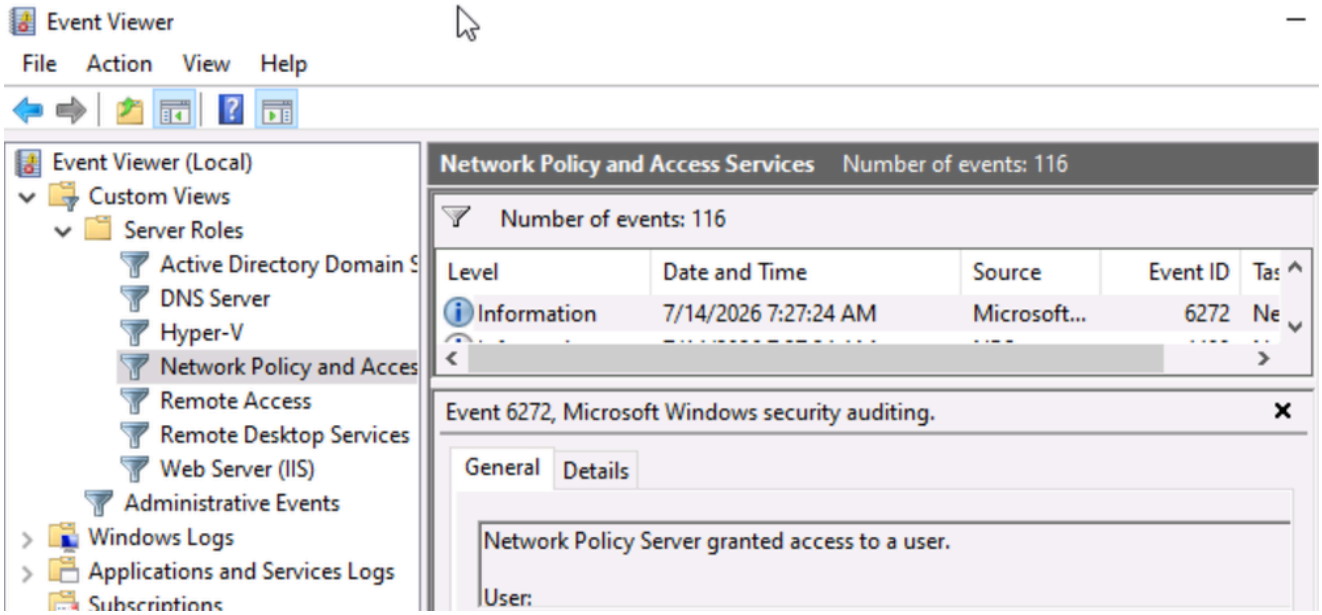
- (Verá una línea con UDP y *:1812 (o la IP del servidor: 1812). Esto confirma que el servicio NPS/RADIUS está escuchando activamente.
- Si no se muestra nada, no se puede ejecutar NPS. Compruebe Services > Network Policy Server (IAS) is Started.)



- En Windows PowerShell, ejecute el comando :
  - Get-NetFirewallRule -DisplayGroup "Servidor de directivas de red" | Format-Table DisplayName, Enabled, Direction, Action.



- En el Visor de eventos de Windows:
  - Vistas personalizadas > Funciones de servidor > Servicios de acceso y políticas de red > Los paquetes están llegando.



Probar conexión desde UCSM

1. Desconéctese e inicie sesión seleccionando el menú desplegable Domain según el dominio Radius creado.

2. Configure la contraseña de usuario. (Consulte el paso 2 de la configuración de Windows).

- Si el inicio de sesión funciona y aterriza con privilegios de administrador, la asignación AV-Pair de Cisco (paso 6 de la configuración de Windows) es correcta.

Troubleshooting de Radius Authentication

Desde Windows Server

1. Ejecute estos comandos en Powershell para la captura de paquetes:

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

2. Inicie la conexión desde UCSM y detenga la captura mediante los comandos :

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

3. Abra radius_capture.pcap en Wireshark: RADIUS > Pares de valores de atributo > confirm Message-Authenticator (o atributo 80) está presente. Esto implica que NPS está firmando la respuesta.

Desde UCSM CLI

Al ejecutar pktmon en Windows, simultáneamente desde UCSM CLI,

1. ejecute:

- connect nxos
- terminal monitor
- debug radius all

2. intente un inicio de sesión de UCSM después de iniciar la depuración.

Un login exitoso parece similar a 2026 Jul 3 09:54:02.917044 radius:Verified Message Authenticator en respuesta de: 10.xxx.xx.xx.

- Si se envían y reciben paquetes pero falla el login con el autenticador de mensaje probablemente sea incorrecto. en la salida de debug - esto implica que el puerto y la disponibilidad están bien.
    - Intente volver a configurar el secreto compartido en el servidor NPS de Windows y la clave UCSM (deben coincidir exactamente).
    - Si el problema persiste mientras se inicia sesión luego de la reconfiguración, podríamos estar encontrando un ID de bug de Cisco conocido CSCwm80801 : El usuario no puede iniciar sesión en UCSM con Radius después de que el parche KB5040434 de Microsoft requiera una actualización a una versión fija mencionada.

Información Relacionada

- Guía de administración y administración de Cisco UCS Manager 4.2: autenticación remota

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).