Configuración de la autenticación de UCSM mediante RADIUS (FreeRADIUS)

Contenido

Introducción

Este documento describe la configuración de la autenticación UCSM mediante RADIUS.

Prerequisites

Requirements

- FreeRADIUS está operativo.
- UCS Manager, Fabric Interconnects y el servidor FreeRADIUS se comunican entre sí.

El público objetivo son los administradores de UCS que tienen conocimientos básicos de las funciones de UCS.

Cisco recomienda que tenga conocimientos o esté familiarizado con estos temas:

- Edición del archivo de configuración de Linux
- UCS Manager
- FreeRADIUS
- Ubuntu o cualquier otra versión de Linux

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- UCS Manager (UCSM) 4.3(3a) o superior.
- Fabric Interconnect 6464

- Ubuntu 22.04.4 LTS
- FreeRADIUS versión 3.0.26

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuración de FreeRADIUS para la Autenticación UCSM

Estos pasos requieren el privilegio de acceso raíz al servidor freeRADIUS.

Paso 1. Configure el dominio UCSM como cliente.

Navegue hasta el archivo clients.conf ubicado en el directorio /etc/freeradius/3.0 y edite el archivo usando un editor de texto de su preferencia. Para este ejemplo, se ha utilizado el editor 'vim' y se ha creado el cliente 'UCS-POD'.

<#root>

```
root@ubuntu:/etc/freeradius/3.0#

vim clients.conf
*Inside clients.conf file*

client UCS-POD {
ipaddr = 10.0.0.100/29
secret = PODsecret
}
```

El campo ipaddr sólo puede contener la IP de la Fabric Interconnect principal. En este ejemplo, se utilizó la IP 10.0.0.100/29 IP para incluir la IP VIP + mgmt0 de ambos FI.

El campo secret contiene la contraseña que se utiliza en la configuración RADIUS de UCSM (Paso 2).

Paso 2. Configure la lista de usuarios con permiso para autenticarse en UCSM.

En el mismo directorio - /etc/freeradius/3.0 - abra el archivo users y cree un usuario. Para este ejemplo, se definió el usuario 'alerosa' con la contraseña 'password' para iniciar sesión como administrador en el dominio UCSM.

<#root>

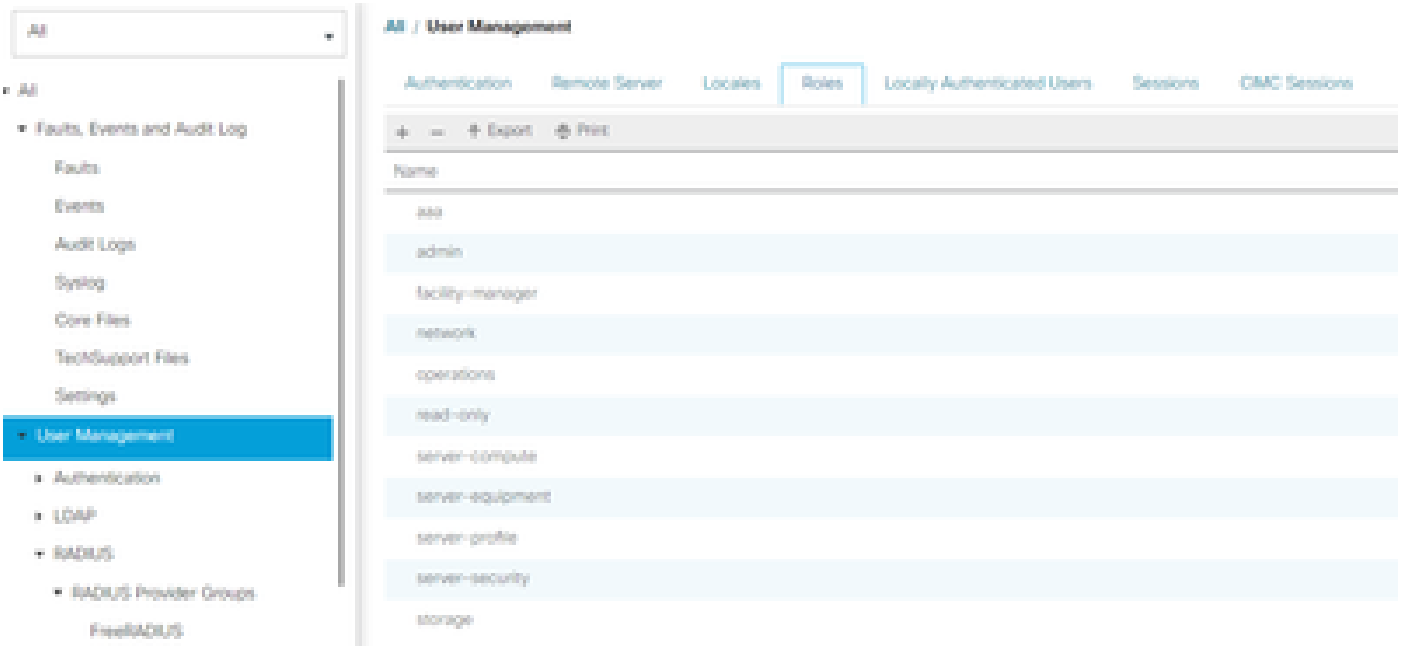
```
root@ubuntu:/etc/freeradius/3.0#
```

```
vim users
*Inside users file*


alerosa Cleartext-Password := "password"
Reply-Message := "Hello, %{User-Name}",
cisco-avpair = "shell:roles=admin"
```

El atributo cisco-avpair es obligatorio y debe seguir la misma sintaxis.

El rol de administrador se puede cambiar para cualquier rol configurado en UCSM en Admin > User Management > Roles. En esta configuración específica, existen estos roles



Si un usuario necesita tener varias funciones, se puede utilizar una coma entre las funciones y la sintaxis debe ser similar a cisco-avpair = "shell:roles=aaa,facility-manager,read-only". Si se define en el usuario una función que no se ha creado en UCSM, la autenticación en UCSM falla.

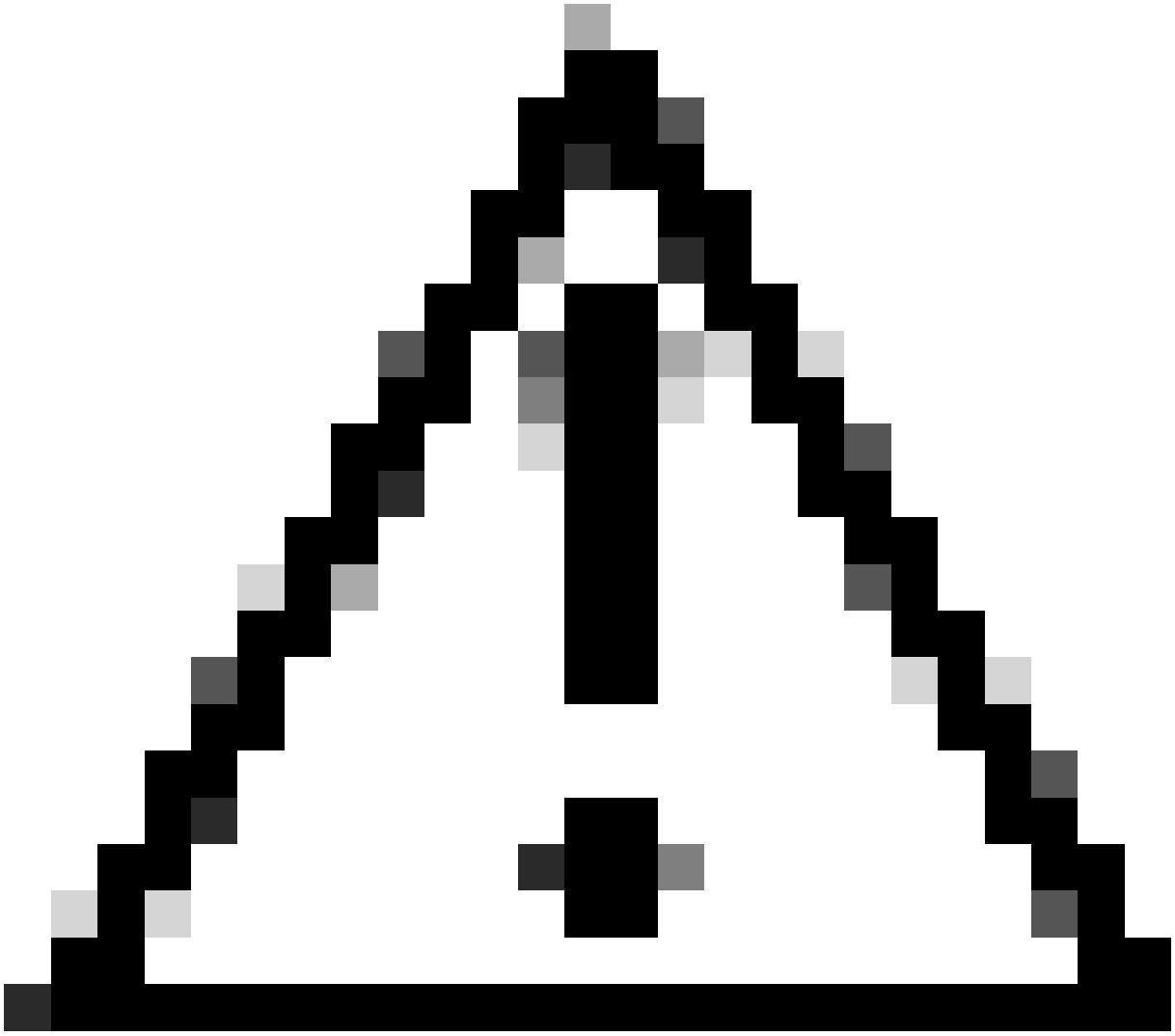
Paso 3. Habilite/Inicie FreeRADIUS daemon.

Active el inicio automático para FreeRADIUS en el arranque del sistema.

```
systemctl enable freeradius
```

Inicie el daemon FreeRADIUS:

```
systemctl restart freeradius
```



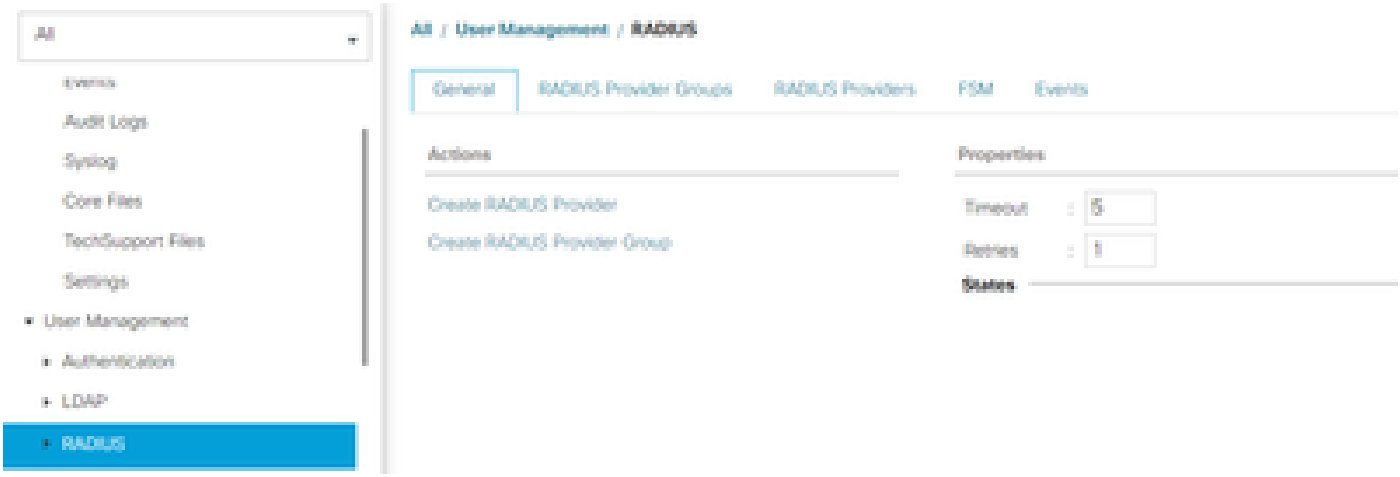
Precaución: Cuando se realizan cambios en los archivos 'clients.conf' o 'users', el demonio FreeRADIUS debe reiniciarse, de lo contrario los cambios no se aplican

Configuración de autenticación RADIUS de UCSM

La configuración de UCS Manager sigue las instrucciones de este documento: https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configura

Paso 1. Propiedades predeterminadas configuradas para proveedores RADIUS.

Vaya a Admin > User Management > RADIUS y utilice los valores predeterminados.



Paso 2. Crear un proveedor RADIUS.

En Admin > User Management, seleccione RADIUS y haga clic en Create RADIUS Provider.

Nombre de host/FQDN (o dirección IP) es la dirección IP o FQDN del servidor/máquina virtual.

Key es la clave/secreto definida en el servidor RADIUS en el archivo 'clients.conf' (Paso 1. de la configuración de FreeRADIUS).

Paso 3. Cree un Grupo de Proveedores RADIUS.

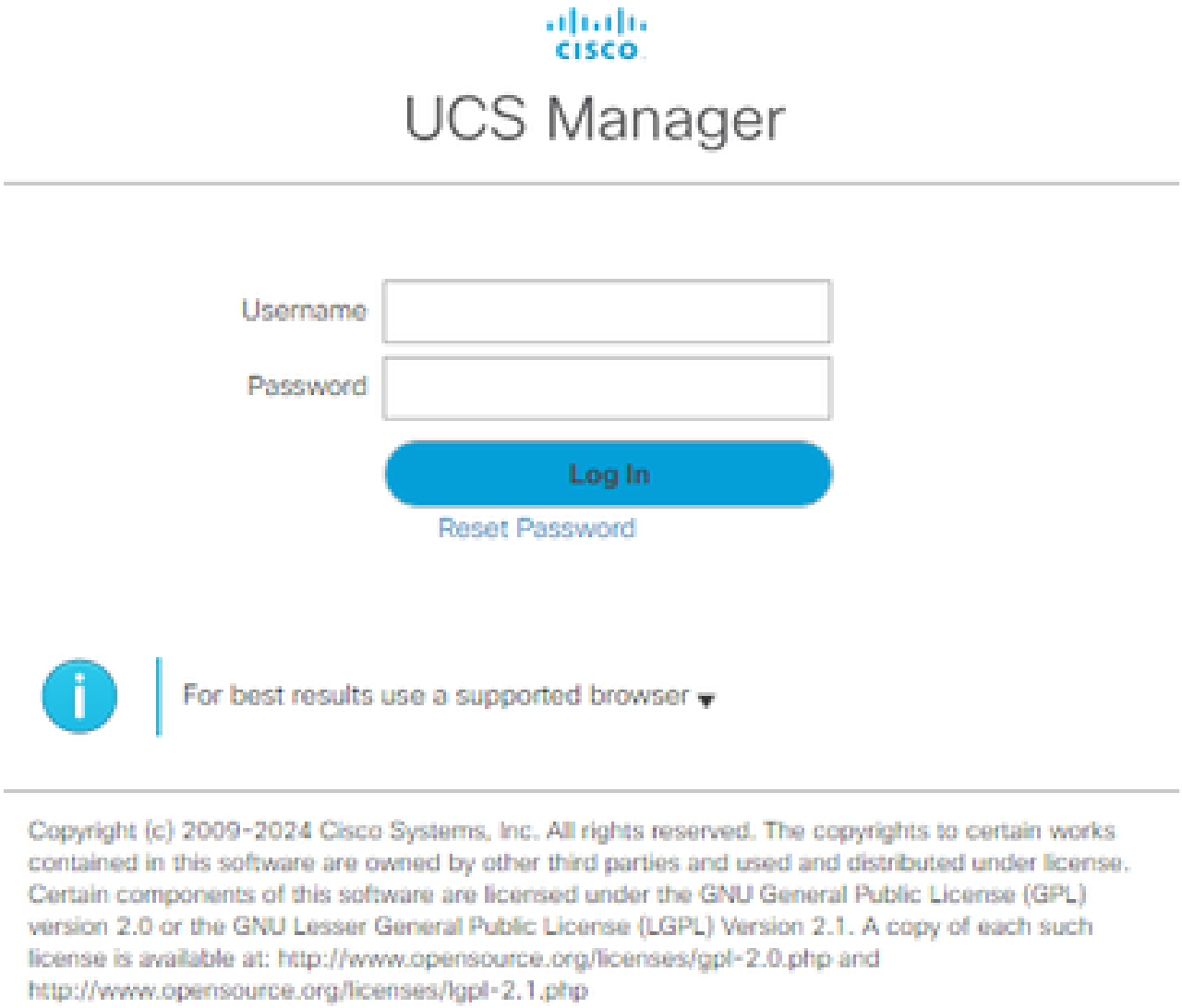
En Admin > User Management, seleccione RADIUS y haga clic en Create RADIUS Provider Group.

Proporciónele un nombre, en este caso se utilizó 'FreeRADIUS'. A continuación, agregue el proveedor RADIUS creado en el paso 2 a la lista de proveedores incluidos.

Paso 4. Cree un nuevo dominio de autenticación (opcional).

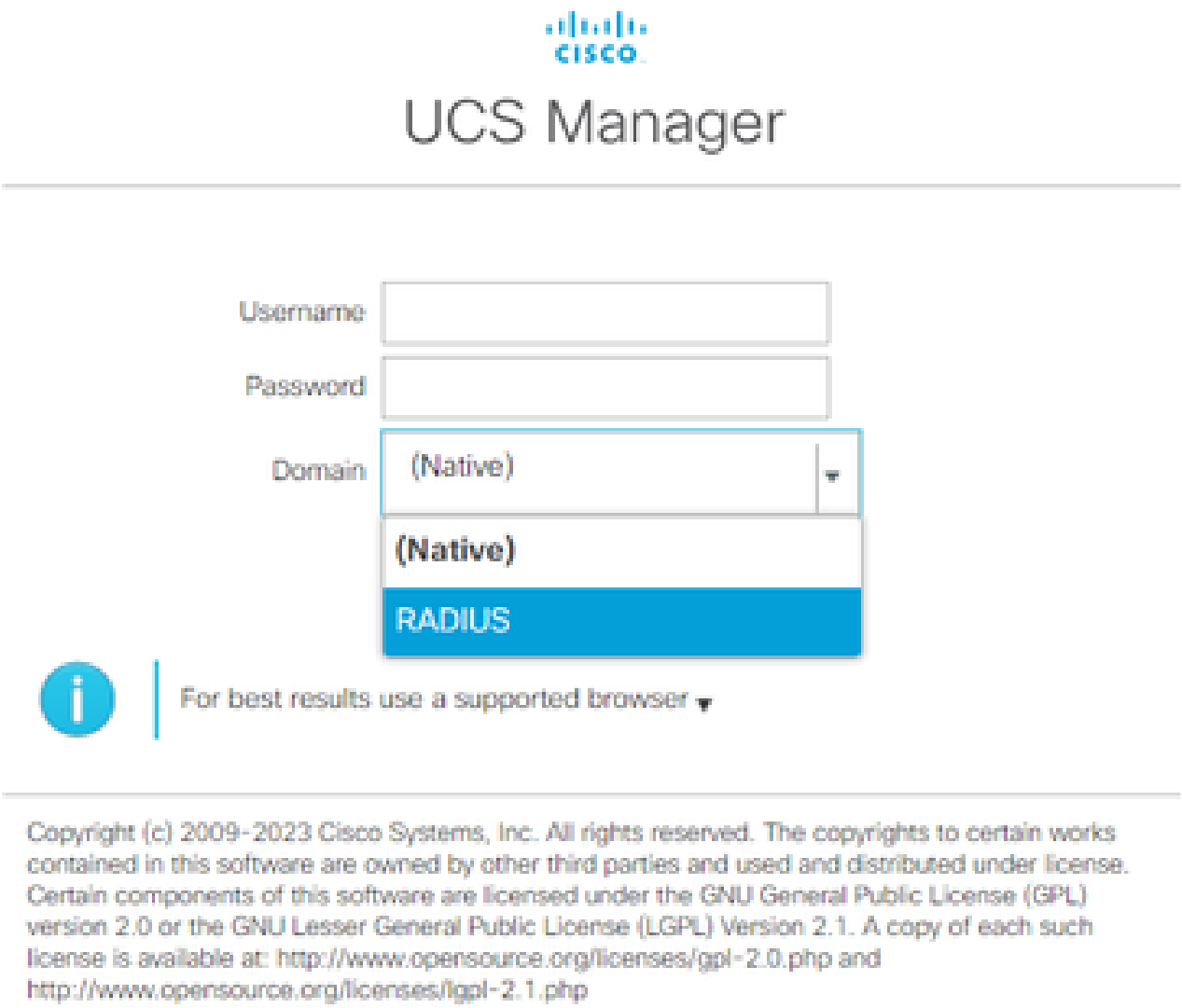
El siguiente paso no es obligatorio. Sin embargo, se llevó a cabo para tener un dominio de autenticación independiente, distinto del que utilizaban los usuarios locales, que está visible en la pantalla de inicio de sesión inicial de UCS Manager.

Sin un dominio de autenticación independiente, la pantalla de inicio de sesión de UCS Manager tiene el siguiente aspecto:



Pantalla de inicio de sesión de UCS Manager sin un dominio de autenticación independiente

Mientras que con un dominio de autenticación independiente, esta es la pantalla de inicio de sesión de UCS Manager que agrega una lista de los dominios de autenticación creados.



Pantalla de inicio de sesión de UCS Manager con un dominio de autenticación independiente

Esto resulta útil si desea separar la autenticación RADIUS de otros tipos de autenticación que también se utilizan en el dominio UCS.

Vaya a Admin > User Management > Authentication > Create a Domain.

Elija el nombre del dominio de autenticación recién creado y elija el botón de opción RADIUS. En el grupo de proveedores, seleccione el grupo de proveedores creado en el paso 3 de esta sección.

Verificación

FreeRADIUS tiene un par de herramientas de depuración y solución de problemas como las que se describen a continuación:

1. El comando journalctl -u freeradius proporciona información valiosa sobre el daemon freeRADIUS, como errores en la configuración y marcas de tiempo de errores o inicializaciones. En el siguiente ejemplo podemos ver que el archivo users fue modificado incorrectamente. (mods-

config/files/authorized es el enlace simbólico del archivo de usuarios):

```
Sep 14 12:18:50 ubuntu freeradius[340627]: /etc/freeradius/3.0/mods-config/files/authorize[90]: Entry d
Sep 14 12:18:50 ubuntu freeradius[340627]: Failed reading /etc/freeradius/3.0/mods-config/files/authori
```

2. El directorio /var/log/freeradius contiene algunos archivos log que contienen una lista de todos los logs registrados para el servidor RADIUS. En este ejemplo:

```
Tue Sep 24 05:48:58 2024 : Error: Ignoring request to auth address * port 1812 bound to server default
```

3. El comando systemctl status freeradius proporciona información sobre el servicio freeRADIUS:

```
root@ubuntu:/# systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
Active: active (running) since Mon 2024-09-16 11:43:38 UTC; 1 week 4 days ago
Docs: man:radiusd(8)
man:radiusd.conf(5)
http://wiki.freeradius.org/
http://networkradius.com/doc/
Main PID: 357166 (freeradius)
Status: "Processing requests"
Tasks: 6 (limit: 11786)
Memory: 79.1M (limit: 2.0G)
CPU: 7.966s
CGroup: /system.slice/freeradius.service
└─357166 /usr/sbin/freeradius -f

Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Auth-Type PAP for attr Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Auth-Type CHAP for attr Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Auth-Type MS-CHAP for attr Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Autz-Type New-TLS-Connection for attr Autz-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Post-Auth-Type REJECT for attr Post-Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Post-Auth-Type Challenge for attr Post-Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Post-Auth-Type Client-Lost for attr Post-Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: radiusd: #### Skipping IP addresses and Ports ####
Sep 16 11:43:38 ubuntu freeradius[357163]: Configuration appears to be OK
Sep 16 11:43:38 ubuntu systemd[1]: Started FreeRADIUS multi-protocol policy server.
```

Para obtener más información sobre la solución de problemas y las comprobaciones de FreeRADIUS, consulte este documento: https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf.

Para UCSM, los inicios de sesión correctos e incorrectos que utilizan usuarios RADIUS se pueden rastrear en el FI principal mediante los siguientes comandos:

- connect nxos
- show logging logfile

El inicio de sesión correcto debe tener el siguiente aspecto:

```
2024 Sep 16 09:56:19 UCS-POD %UCSM-6-AUDIT: [session][internal][creation][internal][2677332][sys/user-e
_8291_A, name:ucs-RADIUS\alerosa, policyOwner:local][] Web A: remote user ucs-RADIUS\alerosa logged in
```

Un inicio de sesión fallido se parece a:

```
2024 Sep 16 09:51:49 UCS-POD %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from X.X.X.X - svc_s
```

Donde X.X.X.X es la dirección IP de la máquina utilizada para conectar SSH a Fabric Interconnect.

Información Relacionada

- Configuración de la autenticación en UCSM
- Configuración del servidor FreeRADIUS
- Wiki de FreeRADIUS

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).