Configurar a autenticação UCSM usando RADIUS (FreeRADIUS)

Contents

Introdução

Este documento descreve a configuração da autenticação UCSM usando o RADIUS.

Pré-requisitos

Requisitos

- FreeRADIUS está operacional.
- O UCS Manager, as interconexões em malha e o servidor FreeRADIUS se comunicam entre si.

O público-alvo são os administradores do UCS que têm uma compreensão básica das funções do UCS.

A Cisco recomenda que você tenha conhecimento ou esteja familiarizado com estes tópicos:

- Edição do arquivo de configuração do Linux
- UCS Manager
- FreeRADIUS
- Ubuntu ou qualquer outra versão do Linux

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- UCS Manager (UCSM) 4.3(3a) ou superior.
- Interconexão de estrutura 6464

- Ubuntu 22.04.4 LTS.
- FreeRADIUS versão 3.0.26

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Configuração FreeRADIUS para autenticação UCSM

Essas etapas exigem privilégio de acesso raiz para o servidor RADIUS livre.

Etapa 1. Configurar o domínio UCSM como um cliente.

Navegue até o arquivo clients.conf localizado no diretório /etc/freeradius/3.0 e edite o arquivo usando um editor de texto de sua preferência. Para este exemplo, foi usado o editor 'vim' e foi criado o 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
}
```

O campo ipaddr pode conter apenas o IP da interconexão de estrutura primária. Neste exemplo, o IP IP 10.0.0.100/29 foi usado para incluir o IP VIP + mgmt0 de ambos os FIs.

O campo secret contém a senha que é usada na configuração RADIUS UCSM (Etapa 2.)

Etapa 2. Configurar a lista de usuários com permissão para autenticar no UCSM.

No mesmo diretório - /etc/freeradius/3.0 - abra o arquivo users e crie um usuário. Para este exemplo, o usuário 'alerosa' com a senha 'password' foi definido para efetuar login como administrador do domínio UCSM.

<#root>

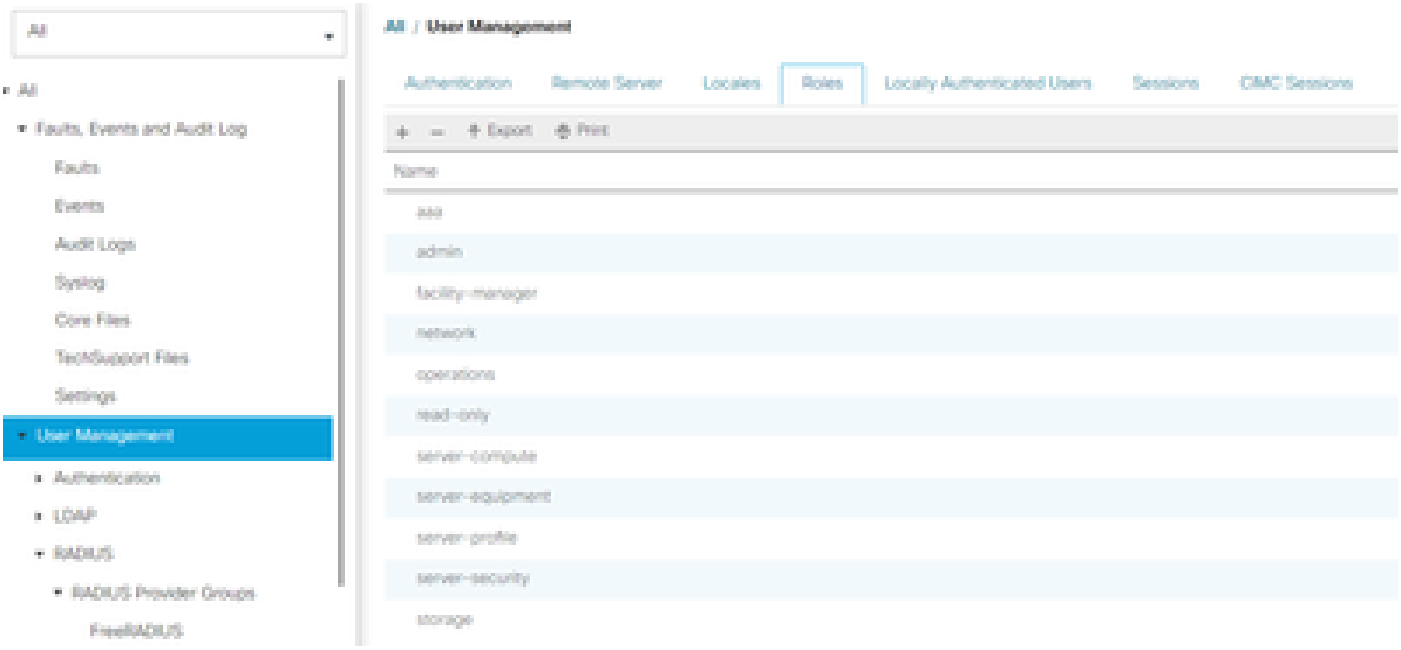
```
root@ubuntu:/etc/freeradius/3.0#

vim users
```

Inside users file

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

O atributo cisco-avpair é obrigatório e deve seguir a mesma sintaxe.

A função de administrador pode ser alterada para qualquer função configurada no UCSM em Admin > Gerenciamento de usuário > Funções. Nessa configuração específica, essas funções existem



Se um usuário precisar ter várias funções, uma vírgula poderá ser usada entre as funções e a sintaxe deverá parecer algo como cisco-avpair = "shell:roles=aaa,facility-manager,read-only". Se uma função que não é criada no UCSM for definida no usuário, a autenticação no UCSM falhará.

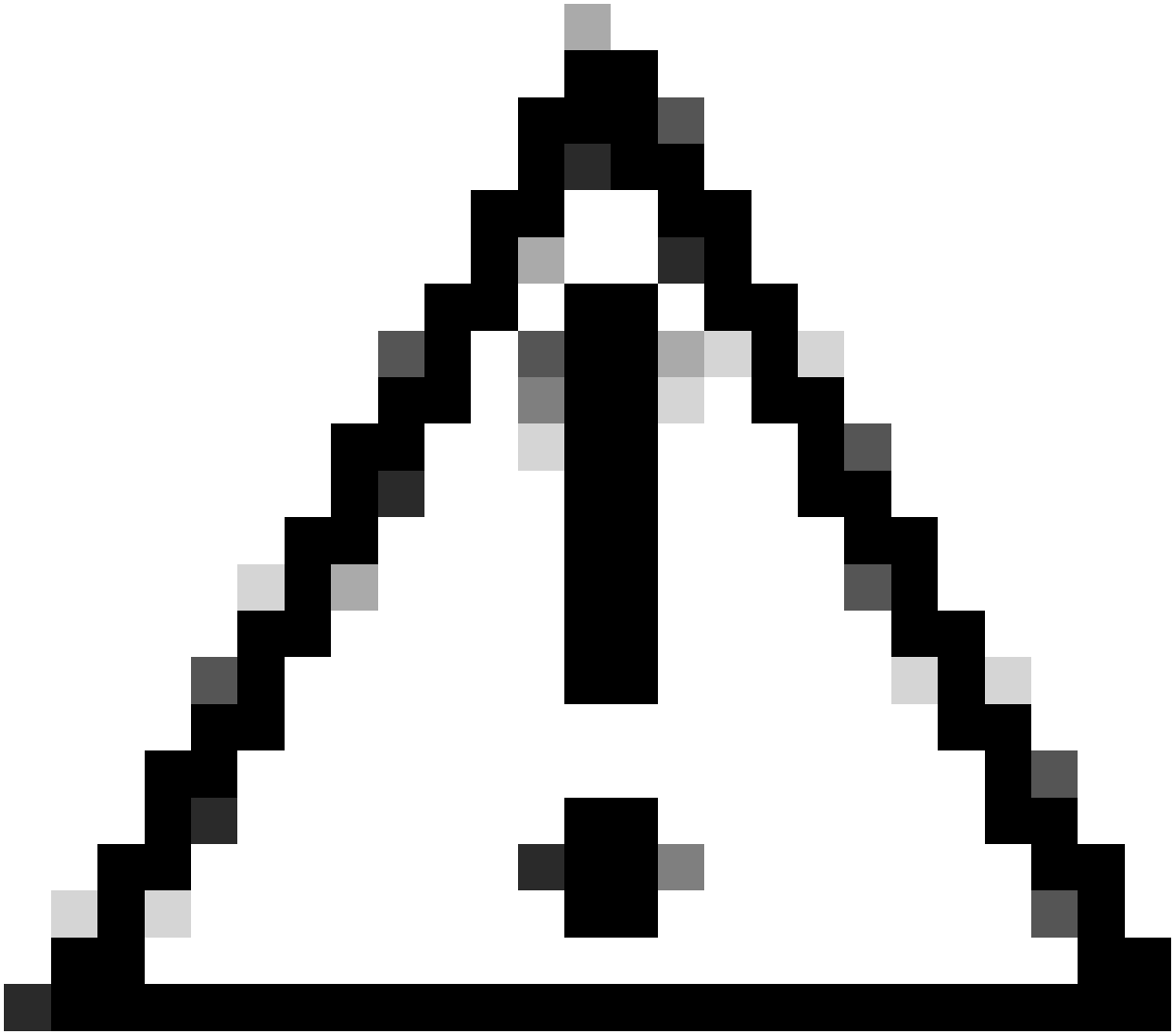
Etapa 3. Ativar/Iniciar o daemon FreeRADIUS.

Ative o início automático para FreeRADIUS na inicialização do sistema.

```
systemctl enable freeradius
```

Inicie o daemon FreeRADIUS:

```
systemctl restart freeradius
```



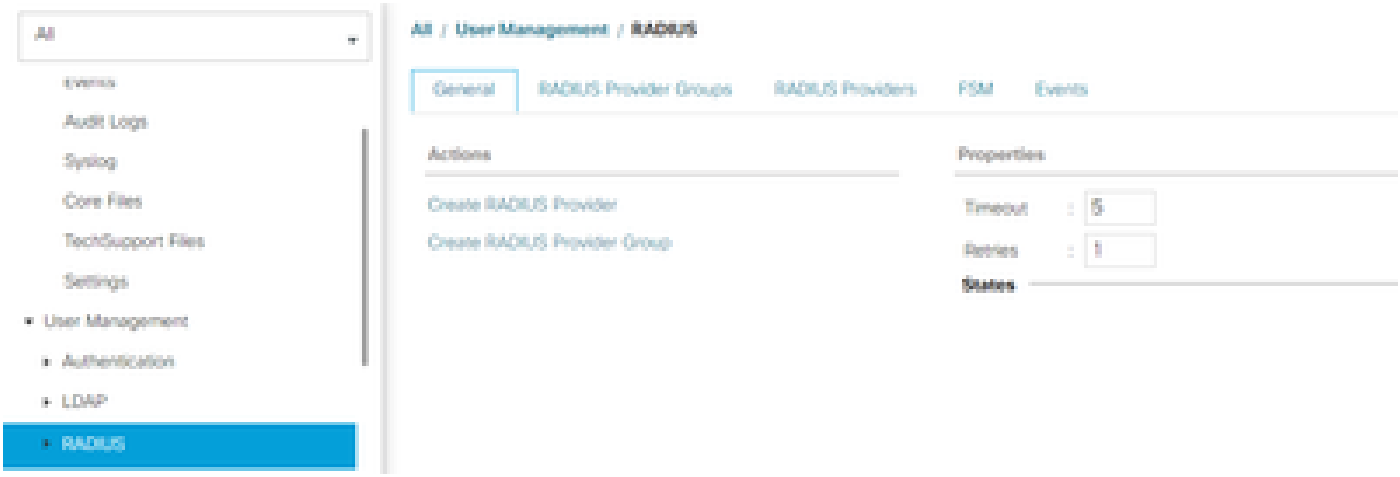
Caution: Quando são feitas alterações nos arquivos 'clients.conf' ou 'users', o daemon FreeRADIUS precisa ser reiniciado, caso contrário as alterações não serão aplicadas

Configuração de autenticação UCSM RADIUS

A configuração do UCS Manager segue as instruções deste documento - https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configura

Etapa 1. Propriedades Padrão Configuradas para Provedores de RADIUS.

Navegue até Admin > User Management > RADIUS e use os valores padrão.



Etapa 2. Criar um provedor RADIUS.

Em Admin > User Management, selecione RADIUS e clique em Create RADIUS Provider.

Nome de host/FQDN (ou Endereço IP) é o IP ou FQDN do servidor/Máquina Virtual.

A chave é a chave/segredo definido no servidor RADIUS no arquivo 'clients.conf' (Etapa 1 da configuração FreeRADIUS).

Etapa 3. Crie um Grupo de Provedores RADIUS.

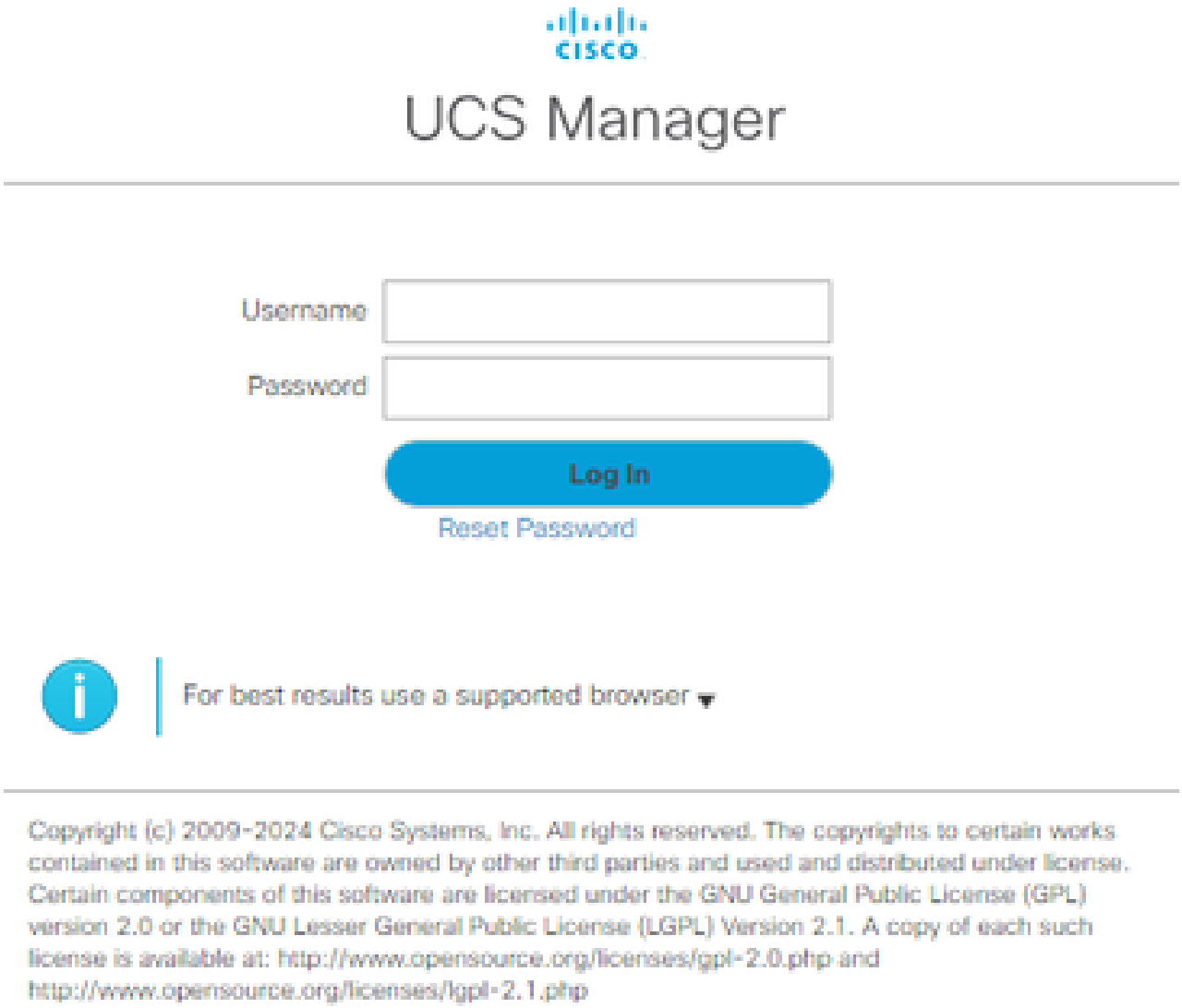
Em Admin > User Management, selecione RADIUS e clique em Create RADIUS Provider Group.

Forneça um nome, neste caso foi usado 'FreeRADIUS'. Em seguida, adicione o provedor RADIUS criado na Etapa 2 à lista de Provedores Incluídos.

Etapa 4. Criar um novo domínio de autenticação (opcional).

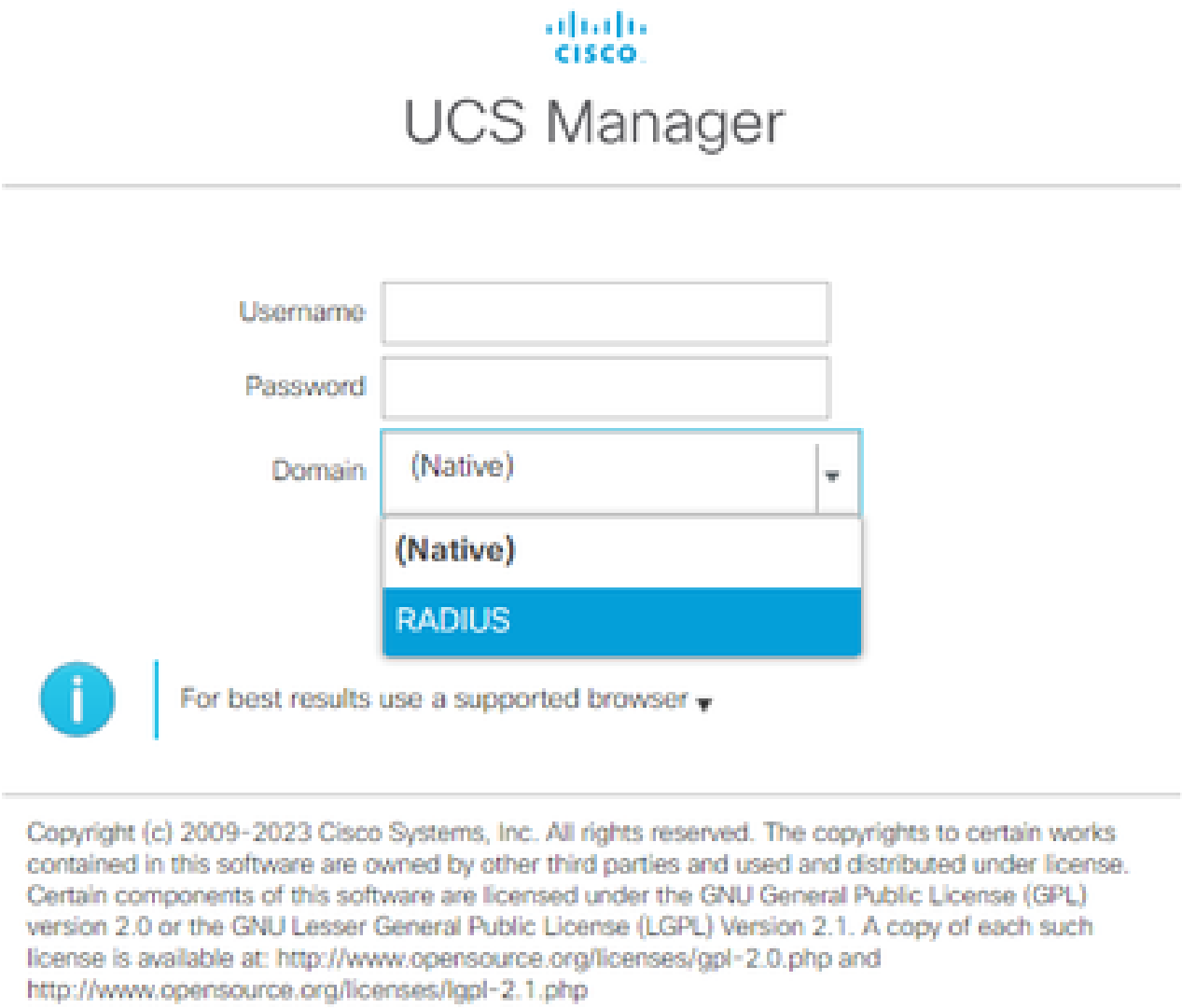
A próxima etapa não é obrigatória. No entanto, foi realizado para ter um Domínio de autenticação separado diferente daquele que usa usuários locais, que é visível na tela de login inicial do UCS Manager.

Sem um Domínio de autenticação separado, a tela de login do UCS Manager fica assim:



Tela de login do UCS Manager sem um domínio de autenticação separado

Embora com um domínio de autenticação separado, esta é a tela de login do UCS Manager adiciona uma lista dos domínios de autenticação criados.



Tela de login do UCS Manager com um domínio de autenticação separado

Isso é útil se você quiser separar a autenticação RADIUS de outros tipos de autenticação também usados no domínio UCS.

Navegue até Admin > User Management > Authentication > Create a Domain.

Escolha o nome do Domínio de autenticação recém-criado e escolha o botão de opção RADIUS. No Grupo de Provedores, selecione o Grupo de Provedores criado na Etapa 3 desta seção.

Verificar

O FreeRADIUS tem algumas ferramentas de depuração e solução de problemas, como as descritas abaixo:

1. O comando journalctl -u freeradius fornece algumas informações valiosas sobre o daemon freeRADIUS tais como erros na configuração e timestamps de erros ou inicializações. No exemplo abaixo, podemos ver que o arquivo users foi modificado incorretamente. (mods-config/files/authorized é o link simbólico do arquivo users):

```
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. O diretório /var/log/freeradius contém alguns arquivos de log que contêm uma lista de todos os logs registrados para o servidor RADIUS. Neste exemplo:

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

3. O comando systemctl status freeradius fornece informações sobre o serviço 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 obter mais troubleshooting/verificações de FreeRADIUS, consulte este documento - https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf.

Para o UCSM, logons bem-sucedidos e malsucedidos usando usuários RADIUS podem ser rastreados no FI primário usando os seguintes comandos:

- connect nxos
- show logging logfile

Um login bem-sucedido deve ter a seguinte aparência:

```
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
```

Um login malsucedido se parece com:

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

Onde X.X.X.X é o IP da máquina usada para SSH para interconexão de estrutura.

Informações Relacionadas

- Configurando a autenticação no UCSM
- Configuração do servidor FreeRADIUS
- wiki FreeRADIUS

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.