Configuration de l'authentification UCSM avec RADIUS (FreeRADIUS)

Table des matières

Introduction

Ce document décrit la configuration de l'authentification UCSM à l'aide de RADIUS.

Conditions préalables

Exigences

- FreeRADIUS est opérationnel.
- UCS Manager, Fabric Interconnects et le serveur FreeRADIUS communiquent entre eux.

Les administrateurs UCS qui possèdent une compréhension de base des fonctions UCS constituent le public cible.

Cisco vous recommande d'avoir des connaissances ou de vous familiariser avec les sujets suivants :

- édition du fichier de configuration Linux
- UCS Manager
- FreeRADIUS
- Ubuntu ou toute autre version Linux

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- UCS Manager (UCSM) version 4.3(3a) ou ultérieure.

- Fabric Interconnect 6464
- Ubuntu 22.04.4 LTS
- FreeRADIUS version 3.0.26

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Configuration de FreeRADIUS pour l'authentification UCSM

Ces étapes nécessitent un privilège d'accès racine au serveur freeRADIUS.

Étape 1 : configuration du domaine UCSM en tant que client.

Accédez au fichier clients.conf situé dans le répertoire /etc/freeradius/3.0 et modifiez-le à l'aide d'un éditeur de texte de votre préférence. Pour cet exemple, l'éditeur « vim » a été utilisé et le client « UCS-POD » a été créé.

<#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
}
```

Le champ ipaddr ne peut contenir que l'adresse IP de l'interconnexion de fabric principale. Dans cet exemple, l'adresse IP 10.0.0.100/29 a été utilisée pour inclure l'adresse IP VIP + mgmt0 des deux interfaces de réseau.

Le champ secret contient le mot de passe utilisé dans la configuration UCSM RADIUS (étape 2).

Étape 2 : configuration de la liste des utilisateurs autorisés à s'authentifier auprès d'UCSM.

Dans le même répertoire - /etc/freeradius/3.0 - ouvrez le fichier users et créez un utilisateur. Dans cet exemple, l'utilisateur « alerosa » avec le mot de passe « password » a été défini pour se connecter en tant qu'administrateur au domaine UCSM.

<#root>

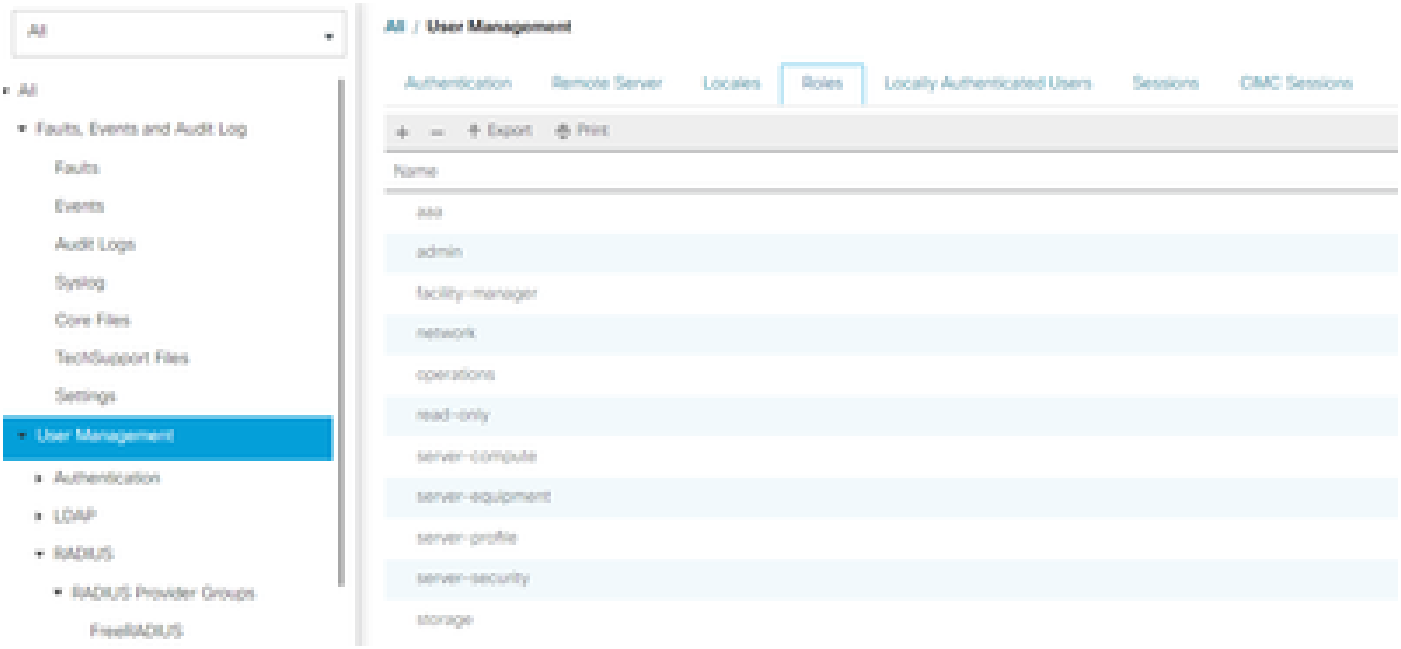
```
root@ubuntu:/etc/freeradius/3.0#
```

```
vim users
*Inside users file*


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

L'attribut cisco-avpair est obligatoire et doit suivre la même syntaxe.

Le rôle admin peut être modifié pour n'importe quel rôle configuré dans UCSM dans Admin > User Management > Roles. Dans cette configuration spécifique, ces rôles existent



Si un utilisateur doit avoir plusieurs rôles, une virgule peut être utilisée entre les rôles et la syntaxe doit ressembler à cisco-avpair = "shell : roles=aaa, facility-manager, read-only". Si un rôle qui n'est pas créé dans UCSM est défini dans l'utilisateur, l'authentification dans UCSM échoue.

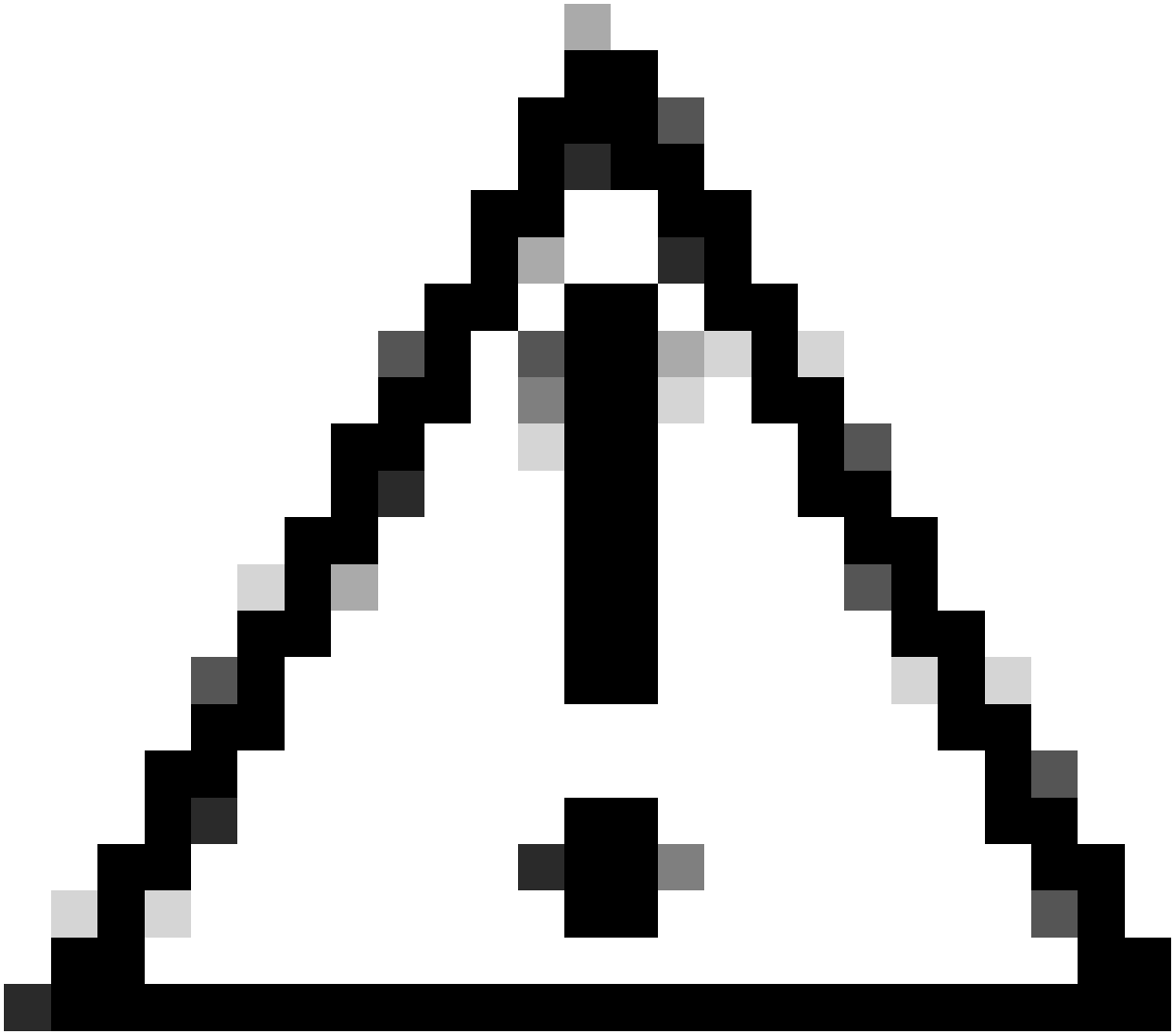
Étape 3 : activation/démarrage du démon FreeRADIUS.

Activez le démarrage automatique de FreeRADIUS au démarrage du système.

```
systemctl enable freeradius
```

Démarrez le démon FreeRADIUS :

```
systemctl restart freeradius
```



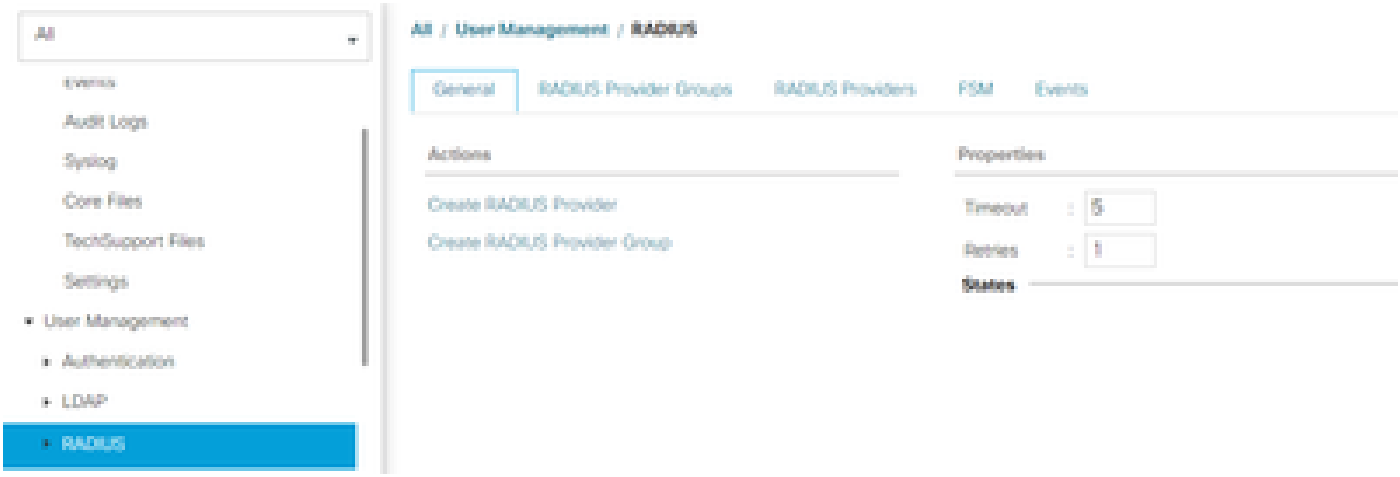
Mise en garde : Lorsque des modifications sont effectuées dans les fichiers 'clients.conf' ou 'users', le démon FreeRADIUS doit être redémarré, sinon les modifications ne sont pas appliquées

Configuration de l'authentification UCSM RADIUS

La configuration d'UCS Manager suit les instructions de ce document : https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configura

Étape 1 : configuration des propriétés par défaut pour les fournisseurs RADIUS.

Accédez à Admin > User Management > RADIUS et utilisez les valeurs par défaut.



Étape 2 : création d’un fournisseur RADIUS.

Dans Admin > User Management, sélectionnez RADIUS et cliquez sur Create RADIUS Provider.

Le nom d'hôte/nom de domaine complet (ou adresse IP) est l'adresse IP ou le nom de domaine complet du serveur/de la machine virtuelle.

Key est la clé/secret définie dans le serveur RADIUS dans le fichier 'clients.conf' (Étape 1. de la configuration FreeRADIUS).

Étape 3 : création d’un groupe de fournisseurs RADIUS.

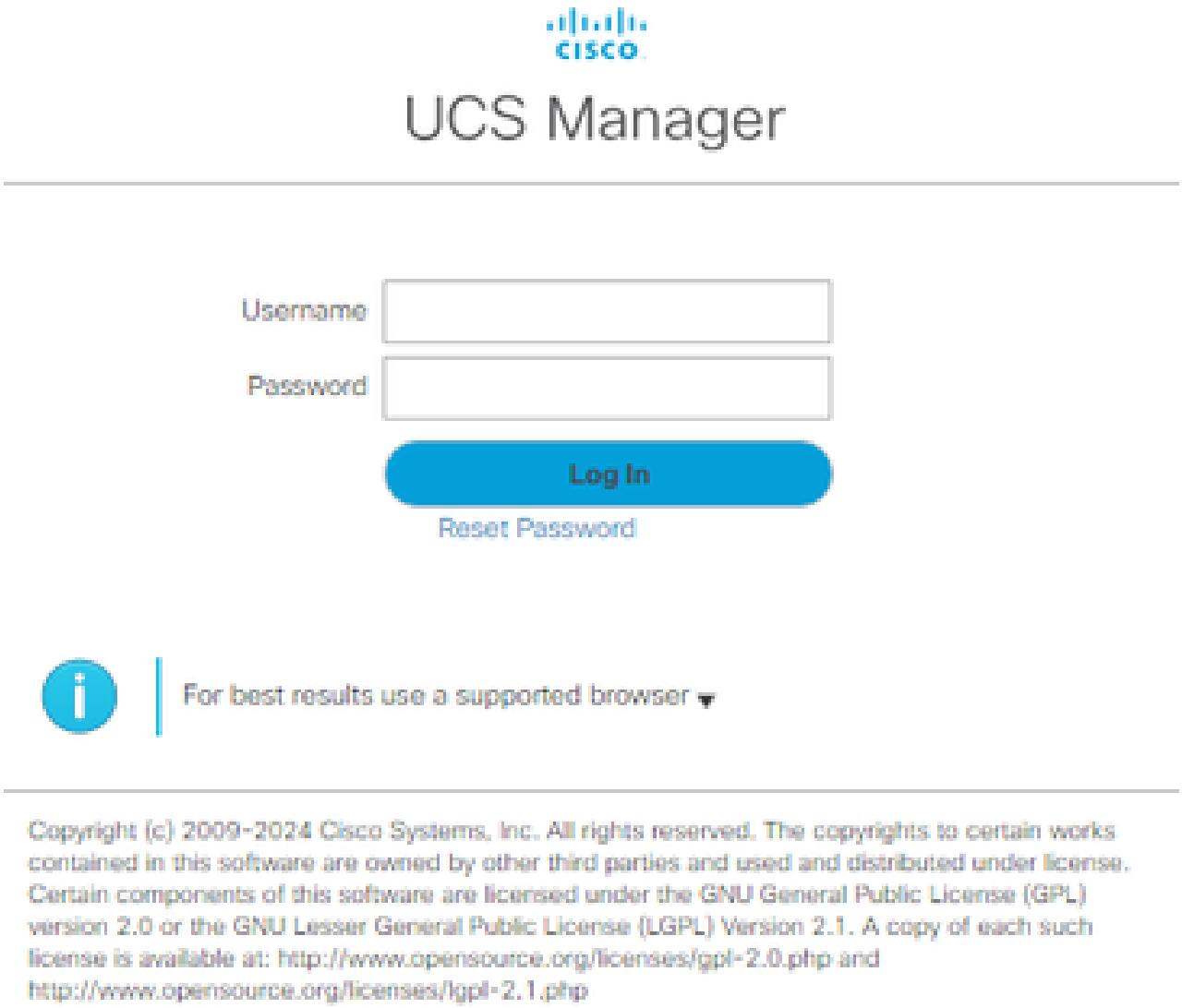
Dans Admin > User Management, sélectionnez RADIUS et cliquez sur Create RADIUS Provider Group.

Donnez-lui un nom, dans ce cas 'FreeRADIUS' a été utilisé. Ajoutez ensuite le fournisseur RADIUS créé à l'étape 2 à la liste des fournisseurs inclus.

Étape 4 : création d’un nouveau domaine d’authentification (facultatif)

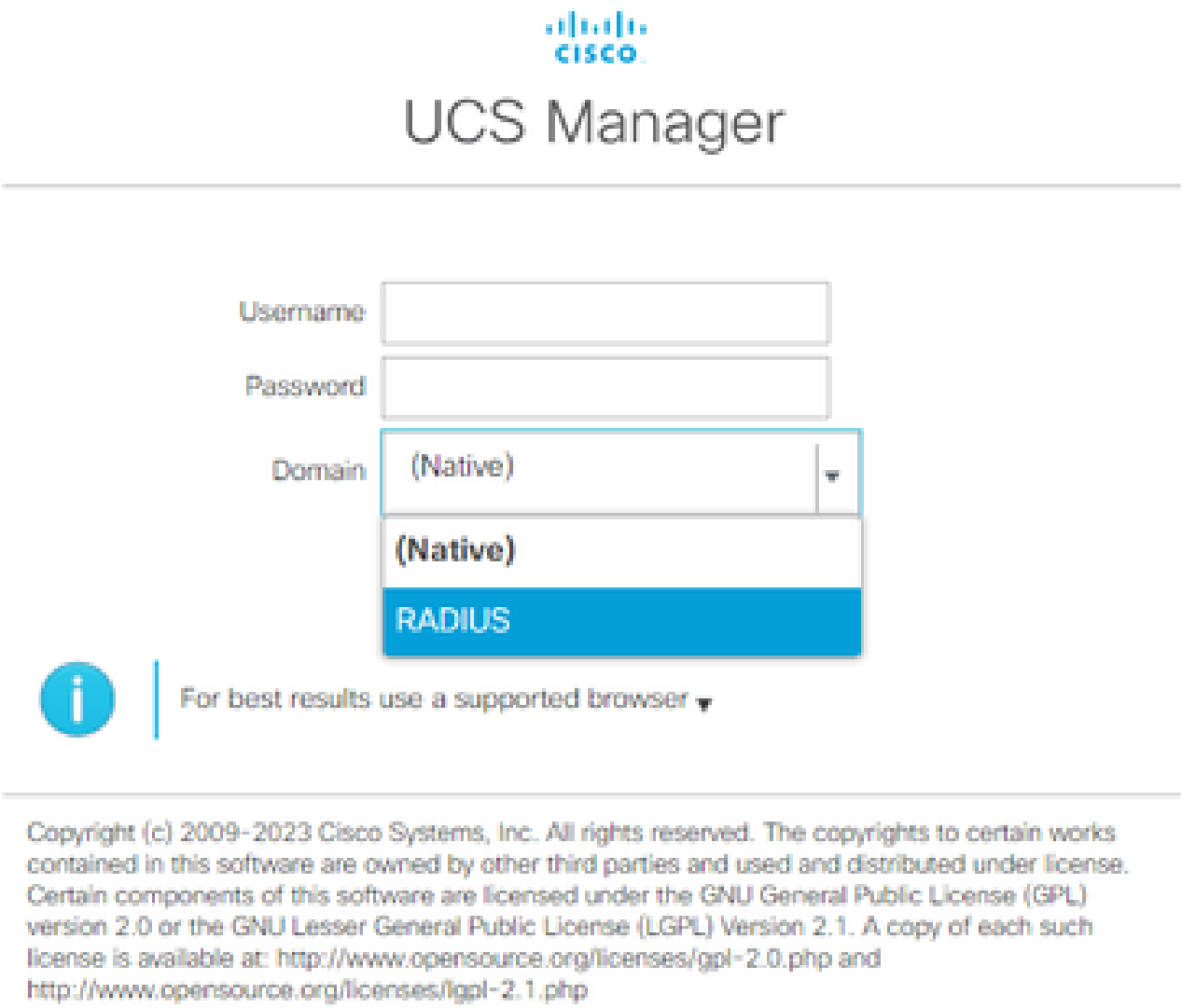
L'étape suivante n'est pas obligatoire. Cependant, il a été effectué pour avoir un domaine d'authentification distinct de celui utilisant des utilisateurs locaux, qui est visible dans l'écran de connexion initiale d'UCS Manager.

Sans domaine d'authentification distinct, l'écran de connexion d'UCS Manager ressemble à ceci :



Écran de connexion UCS Manager sans domaine d'authentification distinct

Avec un domaine d'authentification distinct, l'écran de connexion d'UCS Manager ajoute une liste des domaines d'authentification créés.



Écran de connexion d'UCS Manager avec un domaine d'authentification distinct

Cela est utile si vous souhaitez séparer l'authentification RADIUS des autres types d'authentification également utilisés dans le domaine UCS.

Accédez à Admin > User Management > Authentication > Create a Domain.

Choisissez le nom du domaine d'authentification nouvellement créé et sélectionnez la case d'option RADIUS. Dans le groupe de fournisseurs, sélectionnez le groupe de fournisseurs créé à l'étape 3. de cette section.

Vérifier

FreeRADIUS dispose de quelques outils de débogage et de dépannage tels que ceux décrits ci-dessous :

1. La commande journalctl -u freeradius fournit des informations précieuses sur le démon freeRADIUS telles que des erreurs dans la configuration et des horodatages d'erreurs ou d'initialisations. Dans l'exemple ci-dessous, nous pouvons voir que le fichier users a été modifié à

tort. (mods-config/files/authorized is users file symlink) :

```
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. Le répertoire /var/log/freeradius contient des fichiers journaux contenant la liste de tous les journaux enregistrés pour le serveur RADIUS. Dans cet exemple :

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

3. La commande systemctl status freeradius fournit des informations sur le service 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.
```

Pour plus d'informations sur le dépannage/les vérifications FreeRADIUS, veuillez vous reporter à ce document - https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf.

Pour UCSM, les connexions réussies et infructueuses à l'aide d'utilisateurs RADIUS peuvent être suivies dans l'IF principal à l'aide des commandes suivantes :

- connecter nxos
- show logging logfile

Une connexion réussie doit ressembler à ceci :

```
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
```

Une connexion infructueuse ressemble à ceci :

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

X.X.X.X est l'adresse IP de la machine utilisée pour établir une connexion SSH à Fabric Interconnect.

Informations connexes

- Configuration de l'authentification dans UCSM
- Configuration du serveur FreeRADIUS
- Wiki FreeRADIUS

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.