Configure UCSM Authentication Using RADIUS (FreeRADIUS)

Contents

Introduction

This document describes configuring UCSM authentication using RADIUS.

Prerequisites

Requirements

- FreeRADIUS is operational.
- UCS Manager, Fabric Interconnects and FreeRADIUS server have communication with each other.

The target audience is UCS administrators who have a basic understanding of UCS functions.

Cisco recommends that you have knowledge or be familiar with these topics:

- Linux configuration file edition
- UCS Manager
- FreeRADIUS
- Ubuntu or any other Linux version

Components Used

The information in this document is based on these software and hardware versions:

- UCS Manager (UCSM) 4.3(3a) or above.
- 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. If your network is live, ensure that you understand the potential impact of any command.

Configure

FreeRADIUS Configuration for UCSM Authentication

These steps require root access privilege to the freeRADIUS server.

Step 1. Configure the UCSM domain as a client.

Navigate to the **clients.conf** file located in the **/etc/freeradius/3.0** directory and edit the file using a text editor of your preference. For this example 'vim' editor has been used and client 'UCS-POD' was created.

<#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
}
```

The **ipaddr** field can contain only the IP of the primary Fabric Interconnect. In this example, the IP 10.0.0.100/29 IP was used to include the VIP + mgmt0 IP of both FIs.

The **secret** field contains the password that is used on the UCSM RADIUS configuration (**Step 2**.)

Step 2. Configure the list of users allowed to authenticate to UCSM.

In the same directory - **/etc/freeradius/3.0** - open the **users** file and create a user. For this example, user 'alerosa' with password 'password' was defined to login as administrator to the UCSM domain.

<#root>

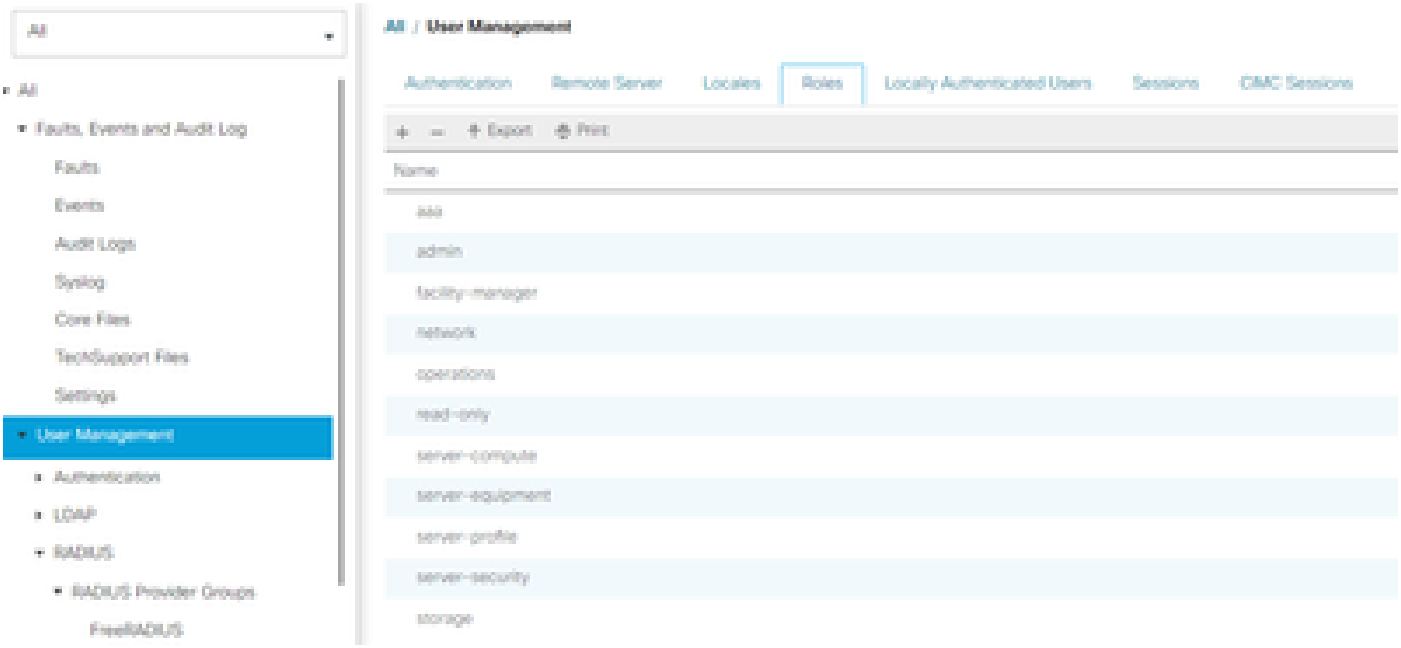
```
root@ubuntu:/etc/freeradius/3.0#
```

```
vim users
*Inside users file*
```

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

The **cisco-avpair** attribute is mandatory and must follow the same syntax.

The admin role can be changed for any role that is configured in UCSM in **Admin > User Management > Roles.** In this specific setup, these roles exist



If a user needs to have multiple roles, a comma can be used between the roles and the syntax must look something like **cisco-avpair = "shell:roles=aaa,facility-manager,read-only".** If a role that is not created in UCSM is defined in the user, the authentication in UCSM fails.

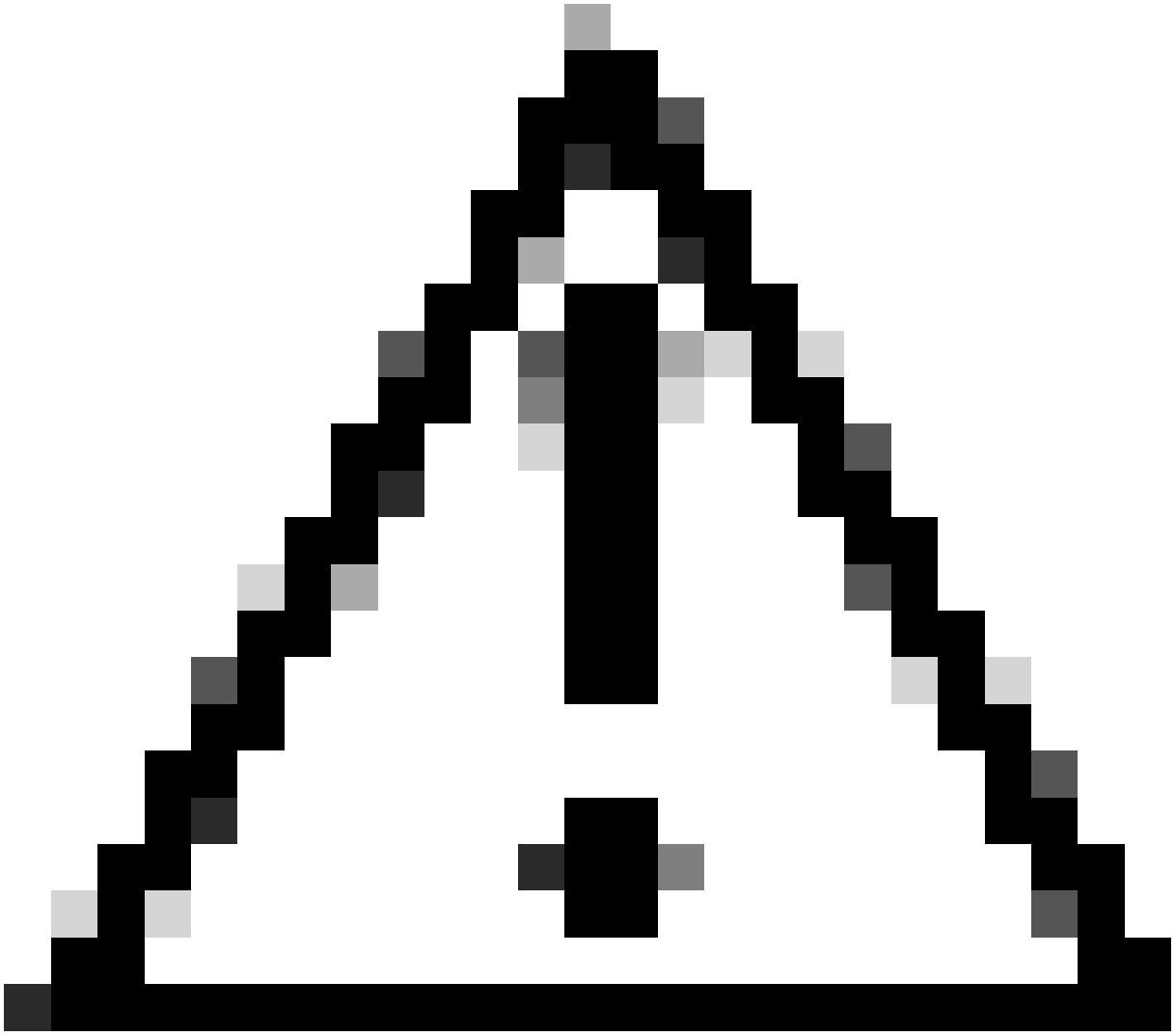
Step 3. Enable/Start FreeRADIUS daemon.

Enable auto-starrt for FreeRADIUS on system boot up.

```
systemctl enable freeradius
```

Start the FreeRADIUS daemon:

```
systemctl restart freeradius
```



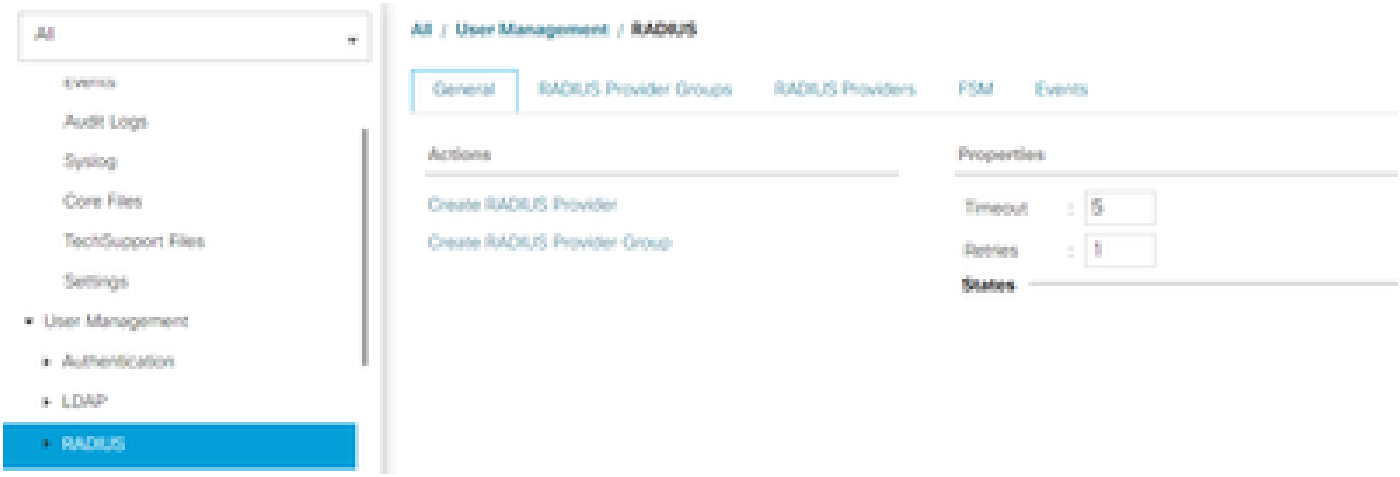
Caution: When changes are made in the 'clients.conf' or 'users' files, the FreeRADIUS daemon needs to be restarted, otherwise the changes are not applied

UCSM RADIUS Authentication Configuration

The UCS Manager configuration follows the instructions from this document - https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configuration_G

Step 1. Configured Default Properties for RADIUS Providers.

Navigate to **Admin > User Management > RADIUS** and used the default values.



Step 2. Create a RADIUS Provider.

In **Admin > User Management**, select RADIUS and click on **Create RADIUS Provider**.

Hostname/FQDN (or IP Address) is the IP or FQDN of the server/Virtual Machine.

Key is the key/secret defined in the RADIUS server in the 'clients.conf' file (Step 1. of the FreeRADIUS configuration).

Step 3. Create a RADIUS Provider Group.

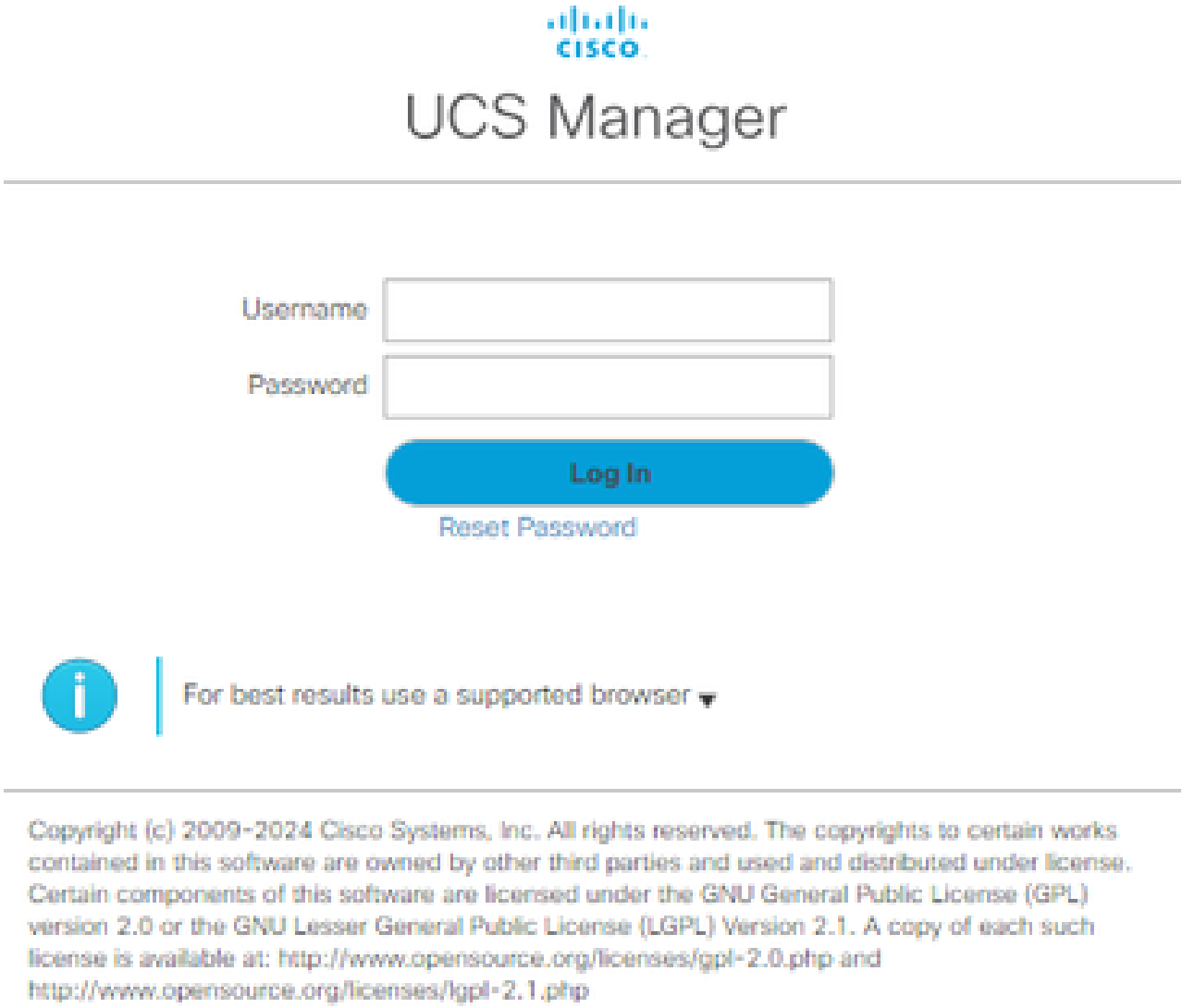
In **Admin > User Management**, select RADIUS and click on **Create RADIUS Provider Group.**

Provide it a name, in this case 'FreeRADIUS' was used. Then add the RADIUS provider created in Step 2 to the list of **Included Providers**.

Step 4. Create a new Authentication domain (optional).

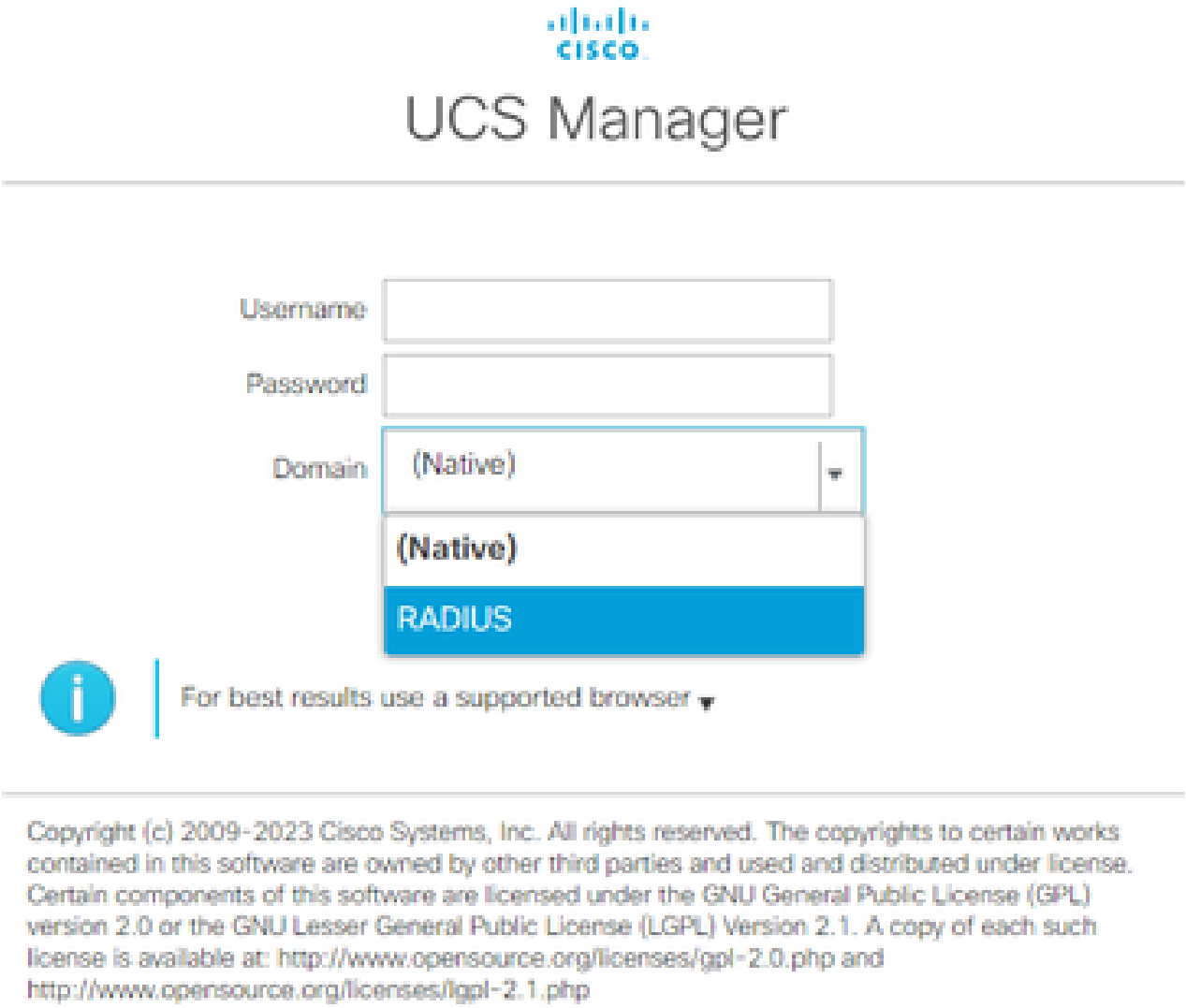
The next step is not mandatory. However, it was performed to have a separate Authentication Domain different from the one using local users, which is visible in the UCS Manager initial login screen.

Without a separate Authentication Domain, the login screen of UCS Manager looks like this:



UCS Manager login screen without a separate Authentication Domain

While with a separate Authentication Domain, this is the login screen of UCS Manager adds a list of the created Authentication Domains.



UCS Manager login screen with a separate Authentication Domain

This is useful if you want to separate the RADIUS authentication from other types of authentication also used in the UCS domain.

Navigate to **Admin > User Management > Authentication > Create a Domain**.

Choose the name of the newly created Authentication Domain and choose the RADIUS radio button. In the **Provider Group**, select the Provider Group created in **Step 3**. of this section.

Verify

FreeRADIUS has a couple of debugging and troubleshooting tools such as the ones described below:

1. The **journalctl -u freeradius** command provides some valuable information about the freeRADIUS daemon such as errors in the configuration and timestamps of errors or initializations. In the example below we can see that the **users** file was wrongly modified. (**mods-config/files/authorize** 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. The **/var/log/freeradius** directory contains some log files that contain a list of all the logs recorded for the RADIUS server. In this example:

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

3. The **systemctl status freeradius** command provides information about the freeRADIUS service:

```
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.
```

For further FreeRADIUS troubleshooting/checks, please refer to this document - https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf.

For UCSM, successful and unsuccessful logins using RADIUS users can be tracked in the primary FI using the following commands:

- **connect nxos**
- **show logging logfile**

A successful login must look like:

```
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
```

An unsuccessful login looks something like:

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

Where X.X.X.X is the IP of the machine used to SSH to Fabric Interconnect.

Related Information

- Configuring Authentication in UCSM
- FreeRADIUS server setup
- FreeRADIUS wiki