使用RADIUS(FreeRADIUS)配置UCSM身份验证

目录

简介

本文档介绍使用RADIUS配置UCSM身份验证。

先决条件

要求

- FreeRADIUS运行正常。
- UCS Manager、交换矩阵互联和FreeRADIUS服务器相互通信。

目标受众是对UCS功能有基本了解的UCS管理员。

思科建议您了解或熟悉以下主题：

- Linux配置文件版本
- UCS 管理器
- FreeRADIUS
- Ubuntu或任何其他Linux版本

使用的组件

本文档中的信息基于以下软件和硬件版本：

- UCS Manager(UCSM)4.3(3a)或更高版本。
- 交换矩阵互联6464
- Ubuntu 22.04.4 LTS
- FreeRADIUS版本3.0.26

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

用于UCSM身份验证的FreeRADIUS配置

这些步骤要求具有freeRADIUS服务器的根访问权限。

步骤1.将UCSM域配置为客户端。

导航到/etc/freeradius/3.0 目录中的clients.conf文件，并使用首选文本编辑器编辑该文件。对于此示例，已使用“vim”编辑器，并创建了客户端“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
}
```

ipaddr字段只能包含主交换矩阵互联的IP。在本示例中，IP 10.0.0.100/29 IP用于包含两个FI的VIP + mgmt0 IP。

secret字段包含在UCSM RADIUS配置中使用的密码(步骤2)。

步骤2.配置允许向UCSM进行身份验证的用户列表。

在同一目录/etc/freeradius/3.0中，打开用户文件并创建用户。在本示例中，定义用户“alerosa”和密码“password”以管理员身份登录到UCSM域。

<#root>

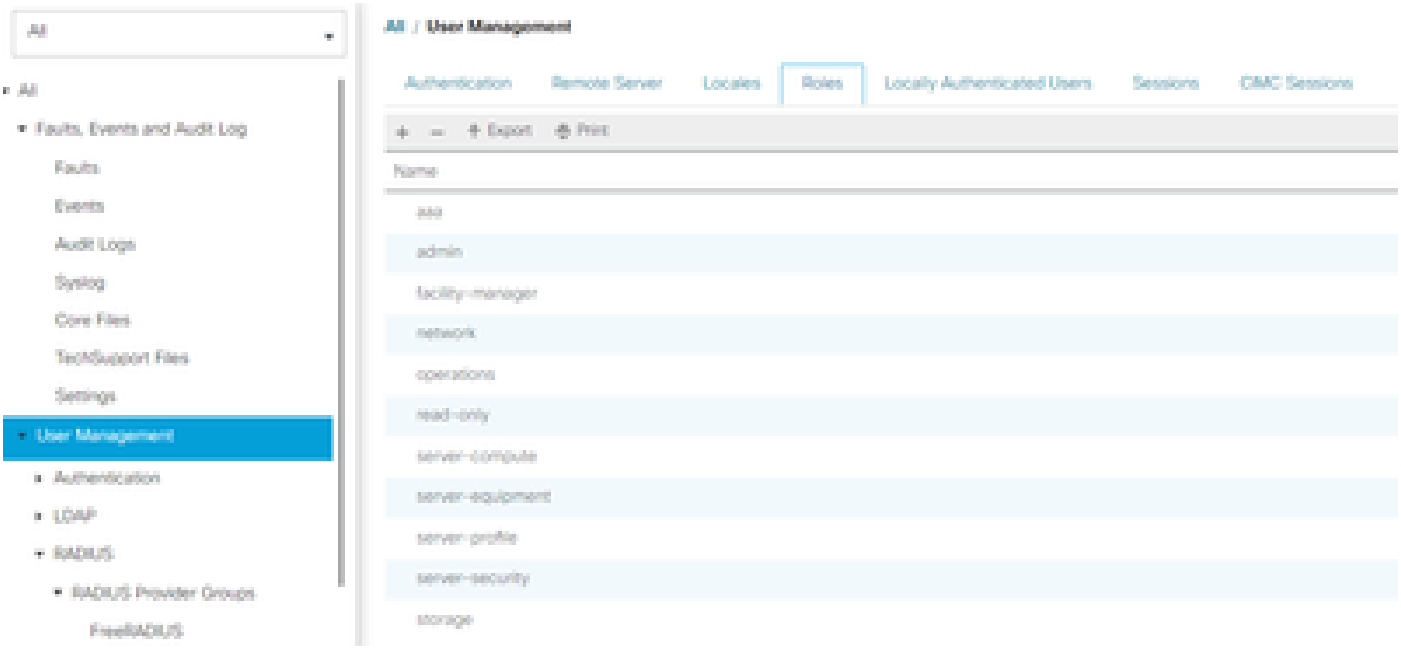
```
root@ubuntu:/etc/freeradius/3.0#
```

vim users
Inside users file

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

cisco-avpair属性是必需的，必须遵循相同的语法。

管理员角色可以在Admin > User Management > Roles中为UCSM中配置的任何角色进行更改。在此特定设置中，这些角色存在



如果用户需要具有多个角色，则可以在这些角色之间使用逗号，并且语法必须类似于cisco-avpair = "shell:roles=aaa，facility-manager，read-only"。如果用户中定义了未在UCSM中创建的角色，则UCSM中的身份验证将失败。

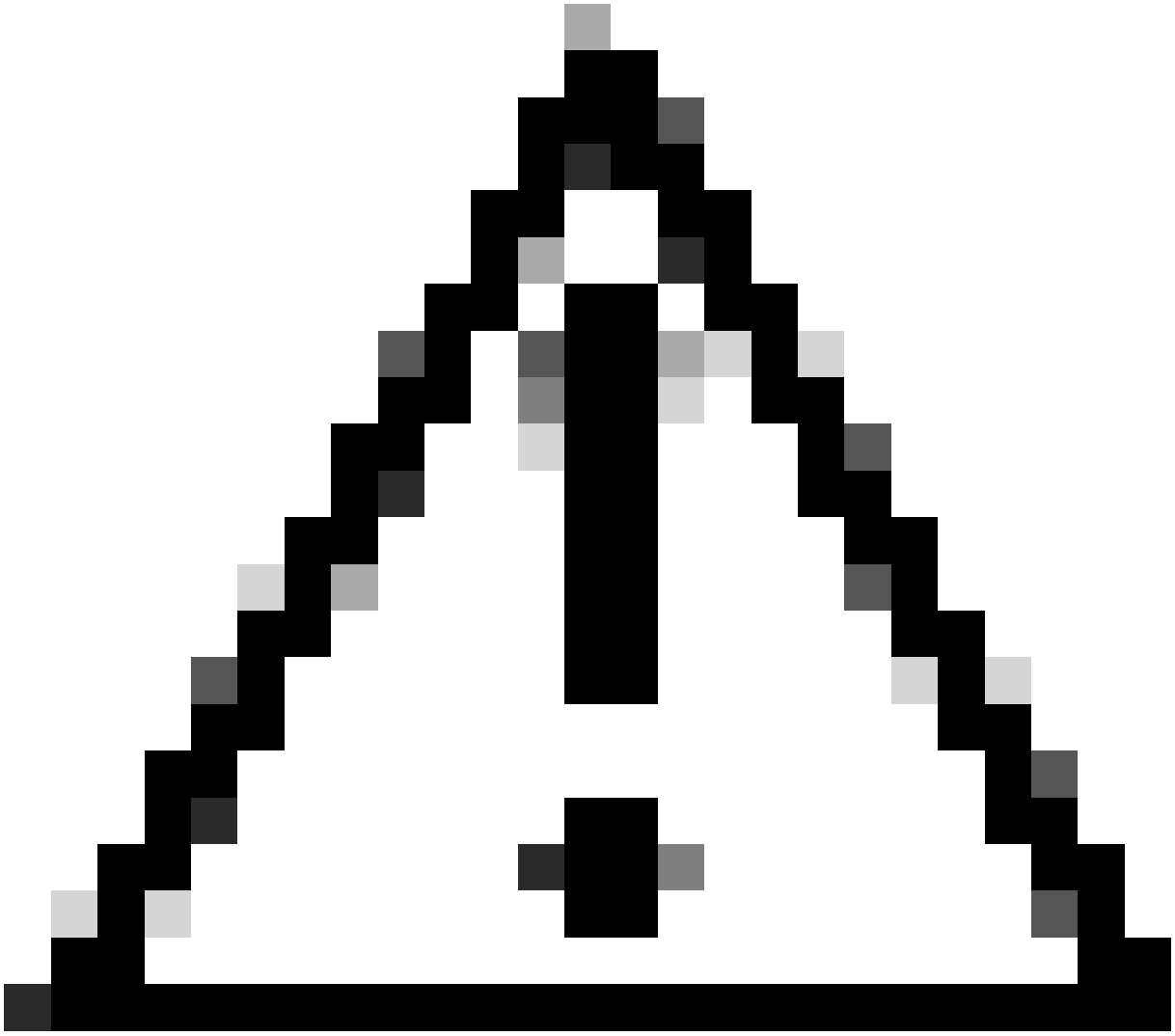
步骤3.启用/启动FreeRADIUS后台程序。

在系统启动时启用FreeRADIUS的自动启动。

```
systemctl enable freeradius
```

启动FreeRADIUS后台程序：

```
systemctl restart freeradius
```



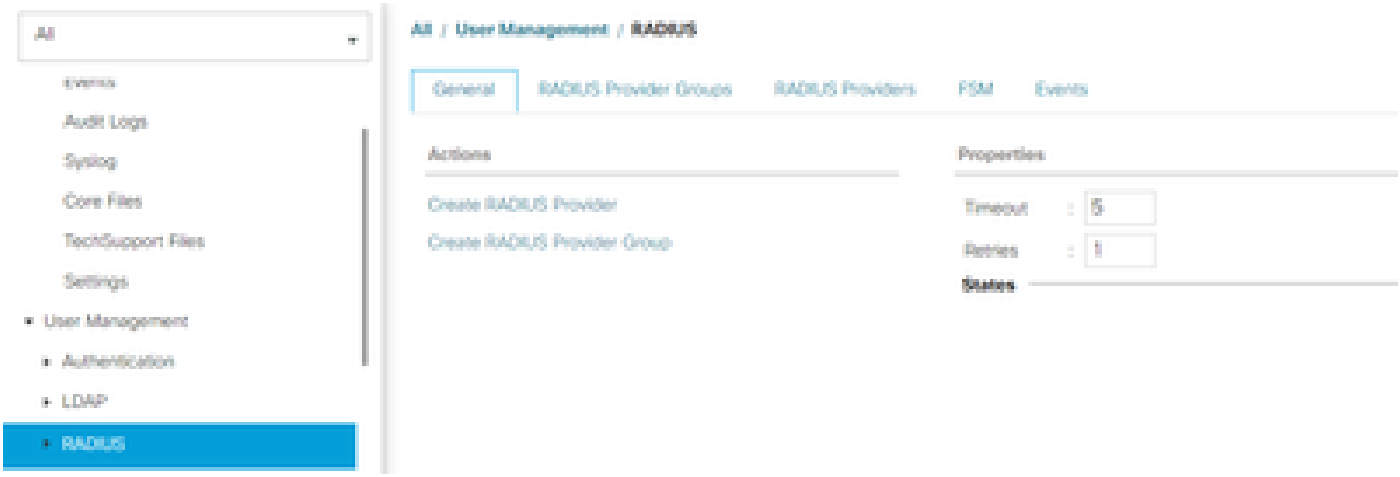
警告：在“clients.conf”或“users”文件中进行更改时，需要重新启动FreeRADIUS后台程序，否则不会应用更改

UCSM RADIUS身份验证配置

UCS Manager配置遵循本文档中的说明 — https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configura

步骤1.为RADIUS提供程序配置默认属性。

导航到Admin > User Management > RADIUS并使用默认值。



步骤2.创建RADIUS提供程序。

在Admin > User Management中，选择RADIUS，然后单击Create RADIUS Provider。

主机名/FQDN(或IP地址)是服务器/虚拟机的IP或FQDN。

Key是在“clients.conf”文件中的RADIUS服务器中定义的密钥/密钥（FreeRADIUS配置的第1步）。

步骤3.创建RADIUS提供程序组。

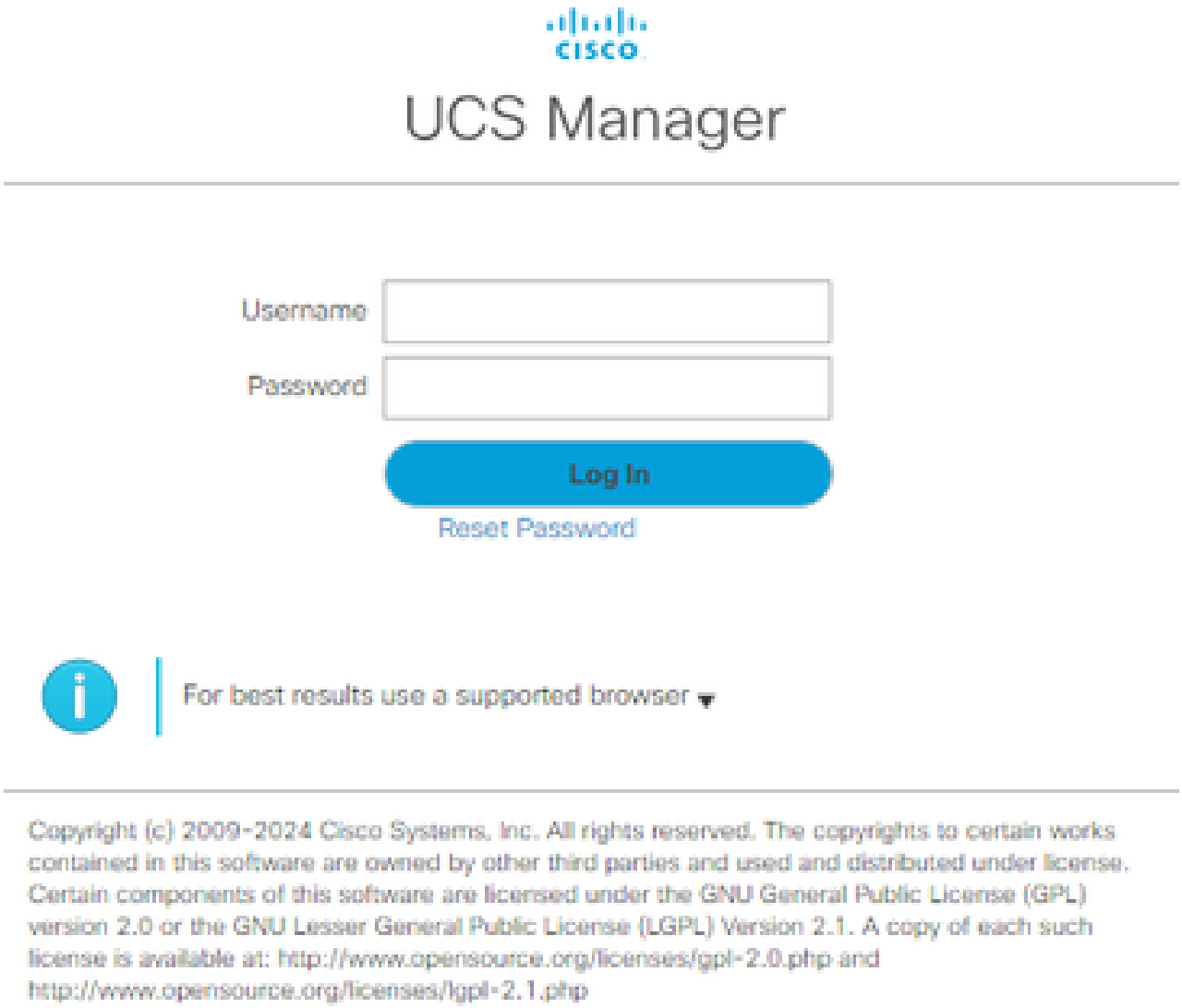
在Admin > User Management中，选择RADIUS，然后单击Create RADIUS Provider Group。

请为其提供一个名称，在本例中使用了“FreeRADIUS”。然后将在步骤2中创建的RADIUS提供程序添加到Included Providers列表。

步骤4.创建新的身份验证域（可选）。

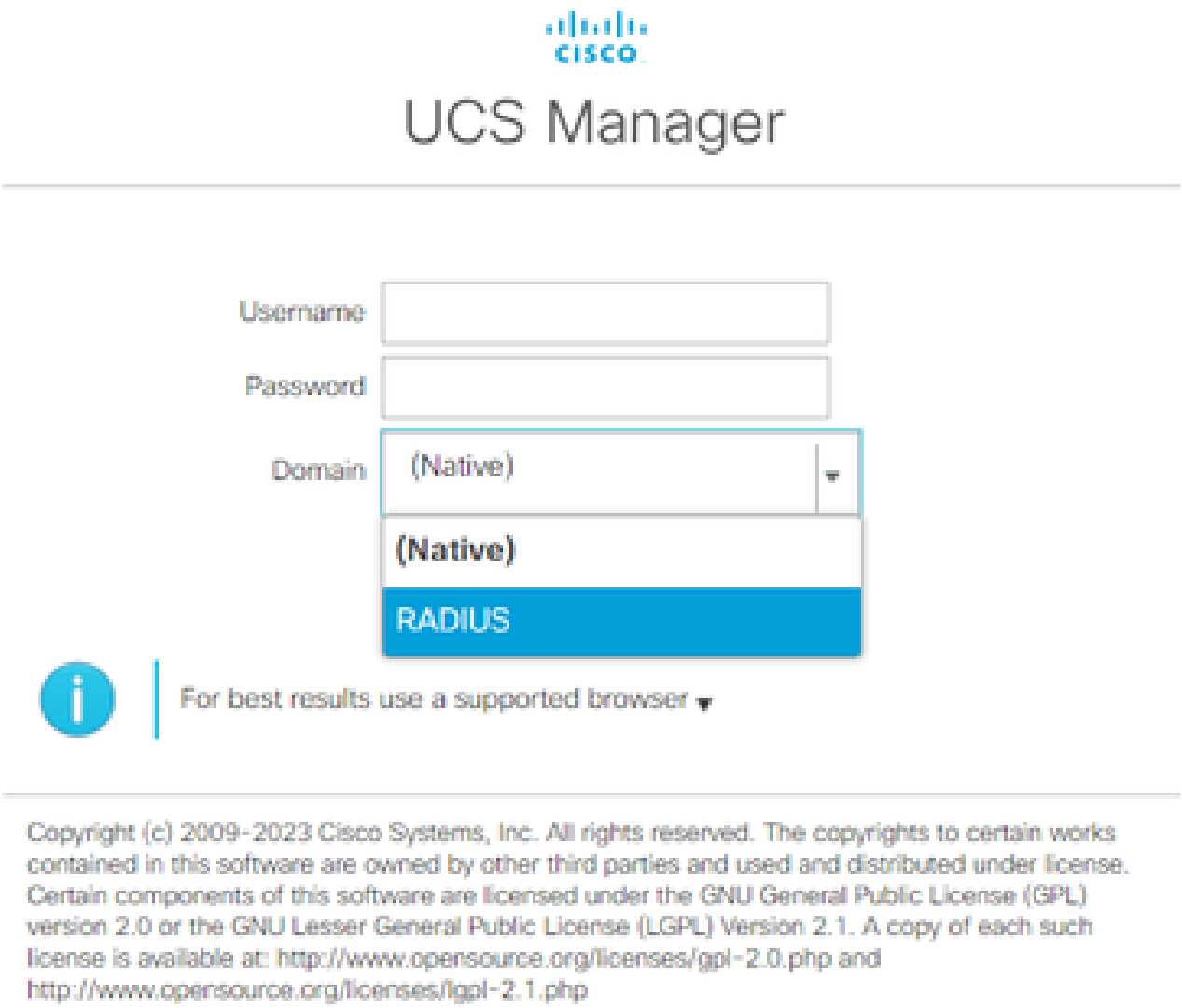
下一步不是强制性的。但是，执行此操作是为了使身份验证域与使用本地用户的身份验证域不同，在UCS Manager初始登录屏幕中可见身份验证域。

如果没有单独的身份验证域，UCS Manager的登录屏幕如下所示：



UCS Manager登录屏幕，无单独的身份验证域

当使用单独的身份验证域时，这是UCS Manager的登录屏幕，其中添加了已创建的身份验证域的列表。



UCS Manager登录屏幕具有单独的身份验证域

如果要将RADIUS身份验证与UCS域中使用的其他身份验证类型分开，这很有用。

导航到Admin > User Management > Authentication > Create a Domain。

选择新创建的身份验证域的名称，然后选择RADIUS单选按钮。在Provider Group中，选择在此部分的步骤3中创建的Provider Group。

验证

FreeRADIUS有一些调试和故障排除工具，如下所述：

1. journalctl -u freeradius命令提供一些有关freeRADIUS后台守护程序的重要信息，例如配置中的错误和错误的时间戳或初始化。在下面的示例中，我们可以看到users文件修改错误。(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. /var/log/freeradius目录包含一些日志文件，这些文件包含为RADIUS服务器记录的所有日志的列表。在本例中：

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

3. systemctl status freeradius命令提供有关freeRADIUS服务的信息：

```
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.
```

有关FreeRADIUS故障排除/检查的详细信息，请参阅本文档 — https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf。

对于UCSM，可以使用以下命令在主FI中跟踪使用RADIUS用户的成功和不成功登录：

- connect nxos
- show logging logfile

成功的登录必须如下所示：

```
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
```

不成功的登录如下所示：

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

其中，X.X.X.X是用于通过SSH连接到交换矩阵互联的计算机的IP。

相关信息

- 在UCSM中配置身份验证
- FreeRADIUS服务器设置
- FreeRADIUS维基

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。