使用RADIUS(FreeRADIUS)配置UCSM身份驗證

目錄

簡介

本文檔介紹使用RADIUS配置UCSM身份驗證。

必要條件

需求

- FreeRADIUS工作正常。
- UCS Manager、交換矩陣互聯和FreeRADIUS伺服器相互通訊。

目標受眾是對UCS功能有基本瞭解的UCS管理員。

思科建議您瞭解或熟悉以下主題：

- Linux配置檔案版本
- UCS管理器
- FreeRADIUS
- Ubuntu或任何其他Linux版本

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- UCS Manager(UCSM)4.3(3a)或更高版本。
- 光纖互連6464
- 烏班圖市22.04.4液晶
- FreeRADIUS版本3.0.26

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

適用於UCSM驗證的FreeRADIUS組態

這些步驟要求具有freeRADIUS伺服器的根訪問許可權。

步驟1.將UCSM域配置為客戶端。

導覽至/etc/freeradius/3.0目錄中的clients.conf檔案，然後使用您偏好的文字編輯器編輯該檔案。對於此示例，「vim」編輯器已被使用，並且建立了客戶端「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欄位只能包含主交換矩陣互聯的IP。在本示例中，IP 10.0.0.100/29 IP用於包括兩個FI的VIP + mgmt0 IP。

secret欄位包含在UCSM RADIUS配置中使用的密碼(步驟2。)

步驟2.配置允許向UCSM進行身份驗證的使用者清單。

在同一目錄/etc/freeradius/3.0 中，開啟users檔案並建立使用者。在本示例中，使用者「alerosa」的密碼「password」被定義為以管理員身份登入到UCSM域。

<#root>

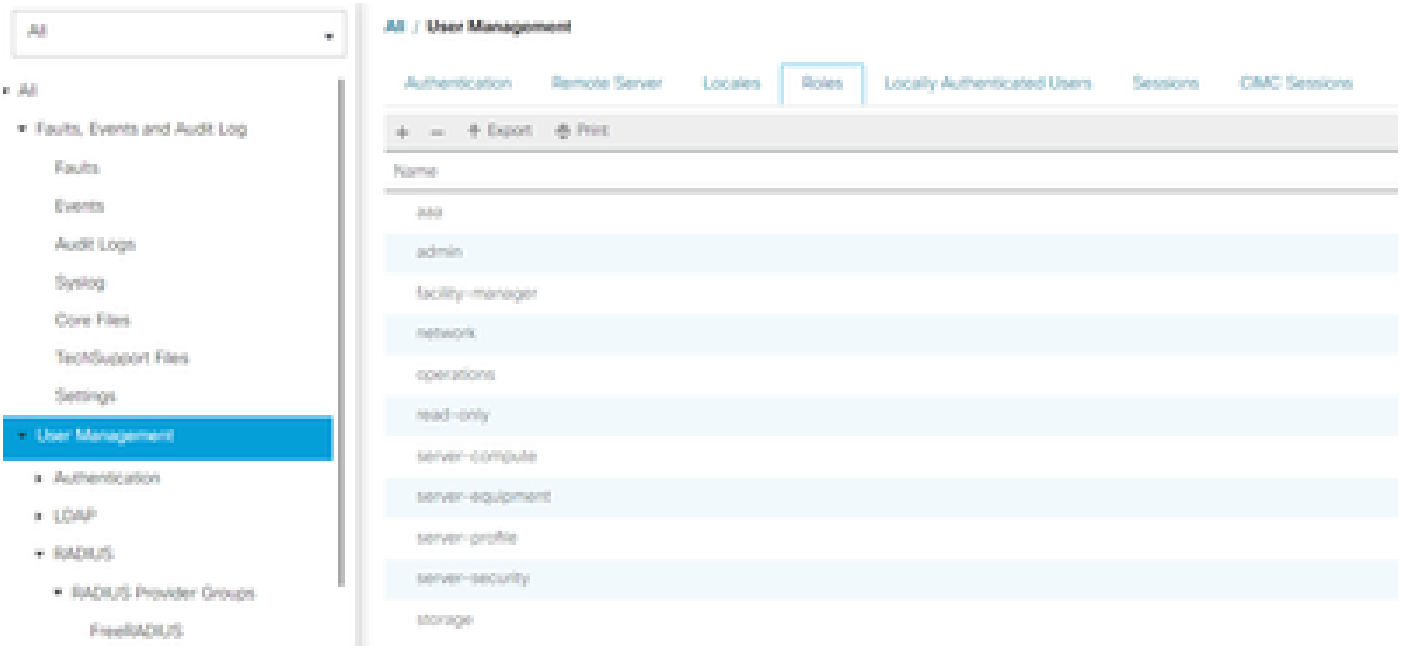
```
root@ubuntu:/etc/freeradius/3.0#
```

vim users
Inside users file

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

cisco-avpair屬性是必需的，而且必須遵循相同的語法。

可在Admin > User Management > Roles中為UCSM中配置的任何角色更改管理員角色。在此特定設定中，存在這些角色



如果使用者需要多個角色，可以在角色之間使用逗號，並且語法必須類似cisco-avpair = "shell:roles=aaa，facility-manager，read-only"。如果使用者中定義了一個未在UCSM中建立的角色，則UCSM中的身份驗證將失敗。

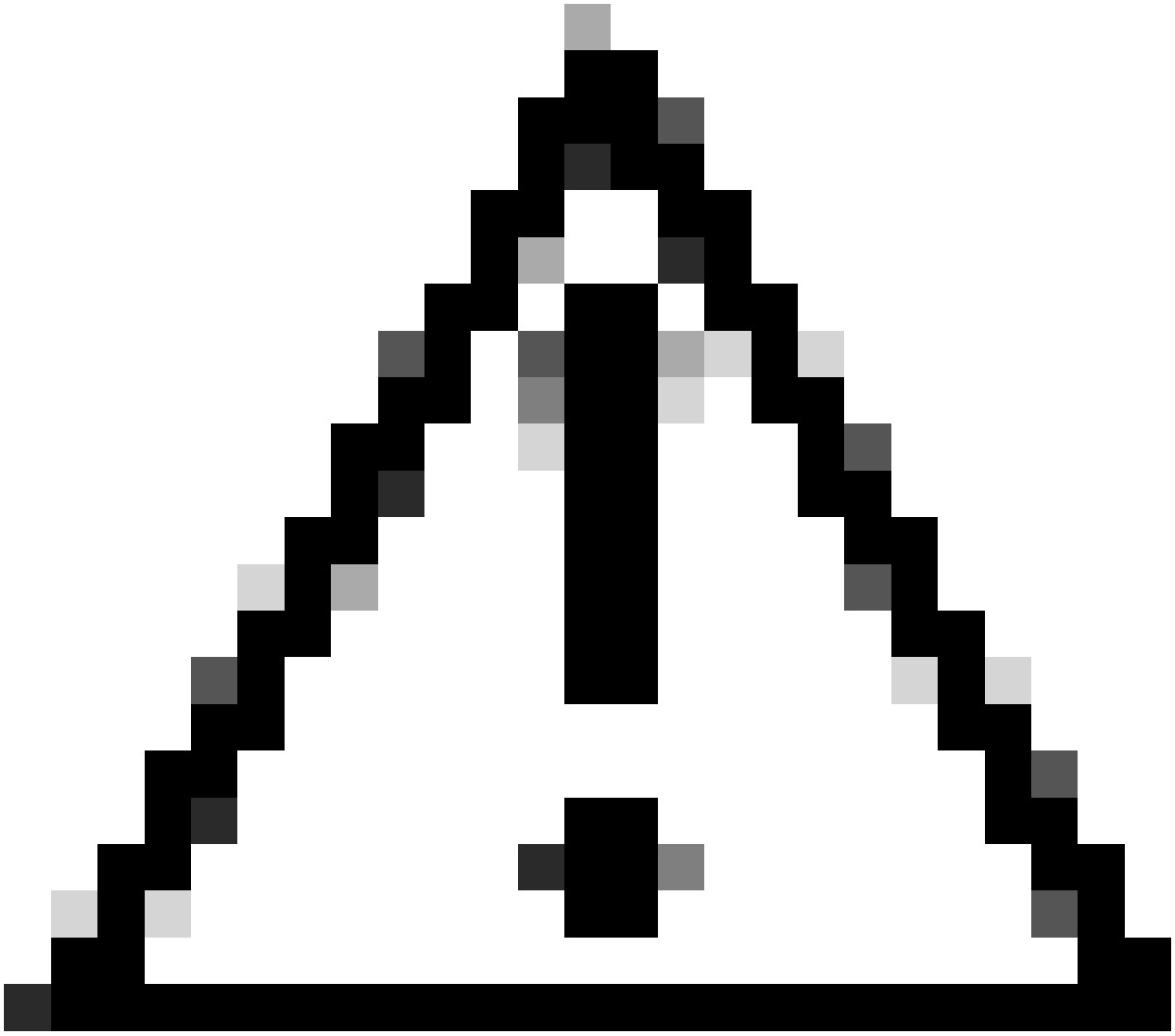
步驟3.啟用/啟動FreeRADIUS守護程式。

在系統啟動時啟用FreeRADIUS的自動啟動。

```
systemctl enable freeradius
```

啟動FreeRADIUS守護程式：

```
systemctl restart freeradius
```



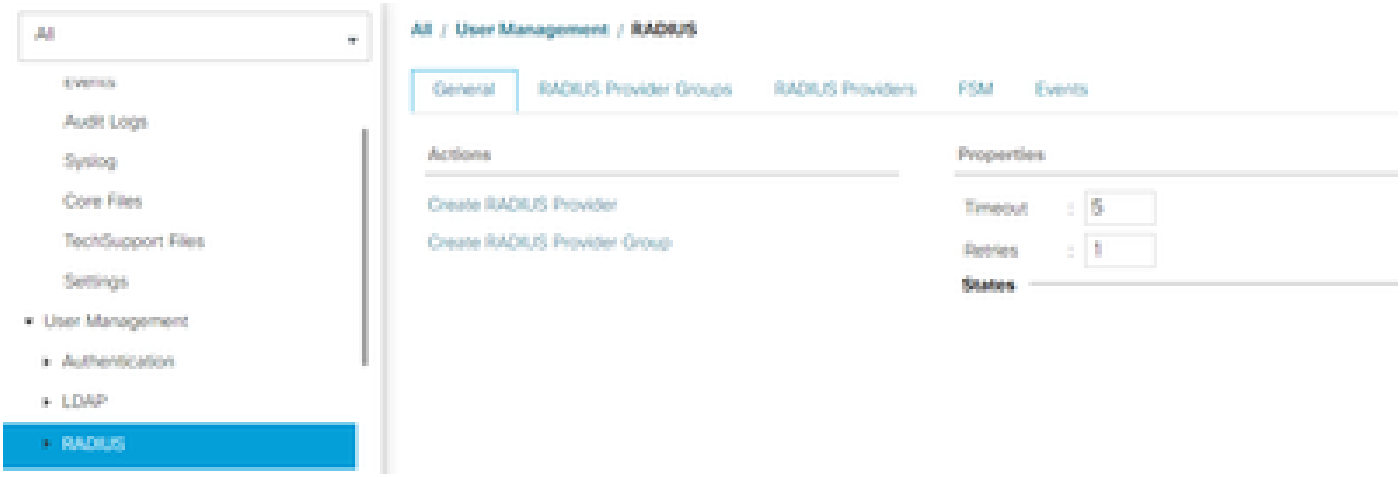
注意：在「clients.conf」或「users」檔案中進行更改時，需要重新啟動FreeRADIUS守護程式，否則不會應用更改

UCSM RADIUS身份驗證配置

UCS Manager配置遵循本文檔中的說明 — https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configura

步驟1.為RADIUS提供程式配置預設屬性。

導覽至Admin > User Management > RADIUS，然後使用預設值。



步驟2.建立RADIUS提供程式。

在Admin > User Management中，選擇RADIUS，然後按一下Create RADIUS Provider。

主機名/FQDN(或IP地址)是伺服器/虛擬機器的IP或FQDN。

Key是在RADIUS伺服器的「clients.conf」檔案中定義的金鑰/密碼（FreeRADIUS組態的步驟1）。

步驟3.建立RADIUS提供程式組。

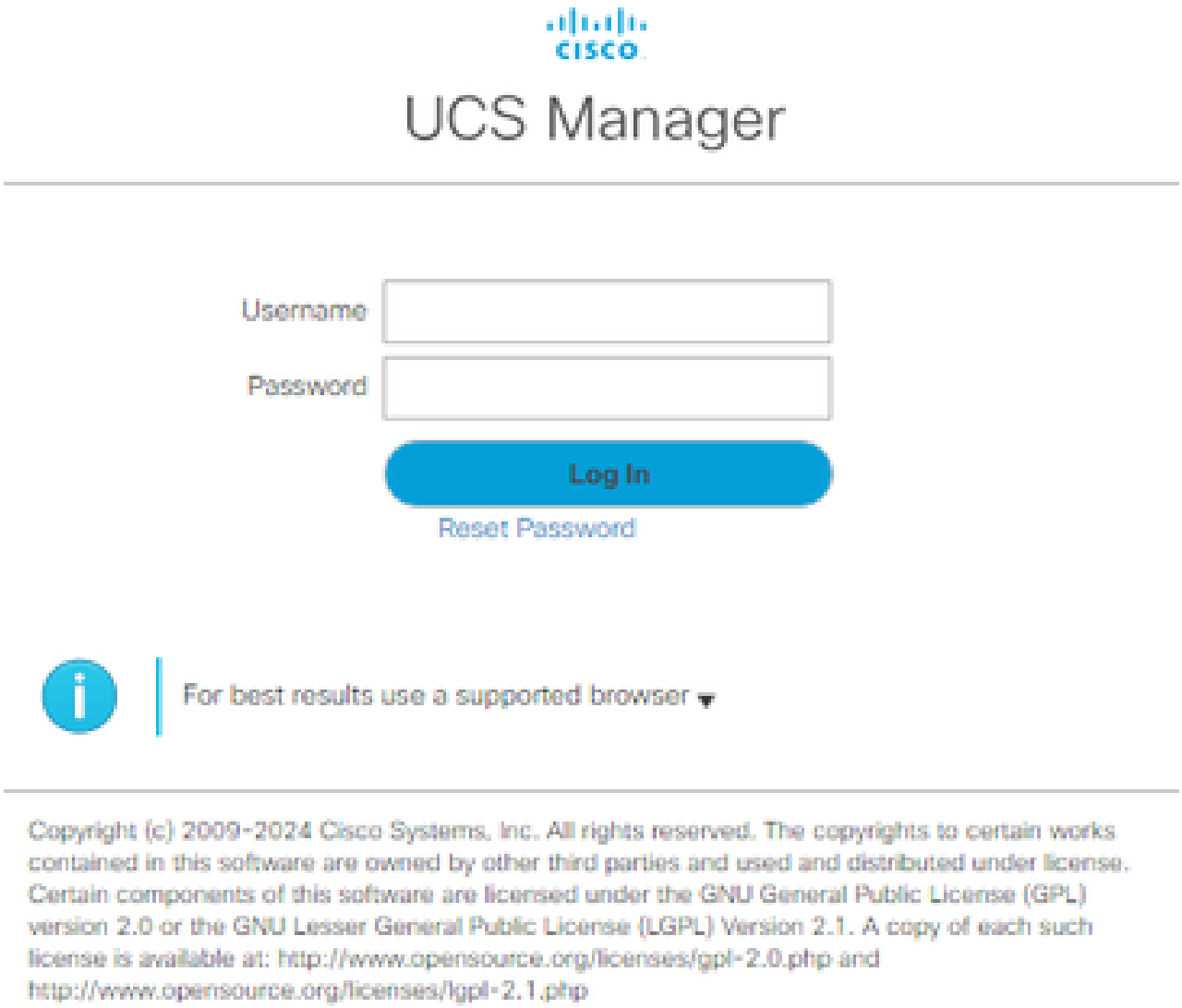
在Admin > User Management中，選擇RADIUS，然後按一下Create RADIUS Provider Group。

請為其提供名稱，本例中使用的是「FreeRADIUS」。然後將在步驟2中建立的RADIUS提供程式新增到Included Providers清單中。

步驟4.建立新的身份驗證域（可選）。

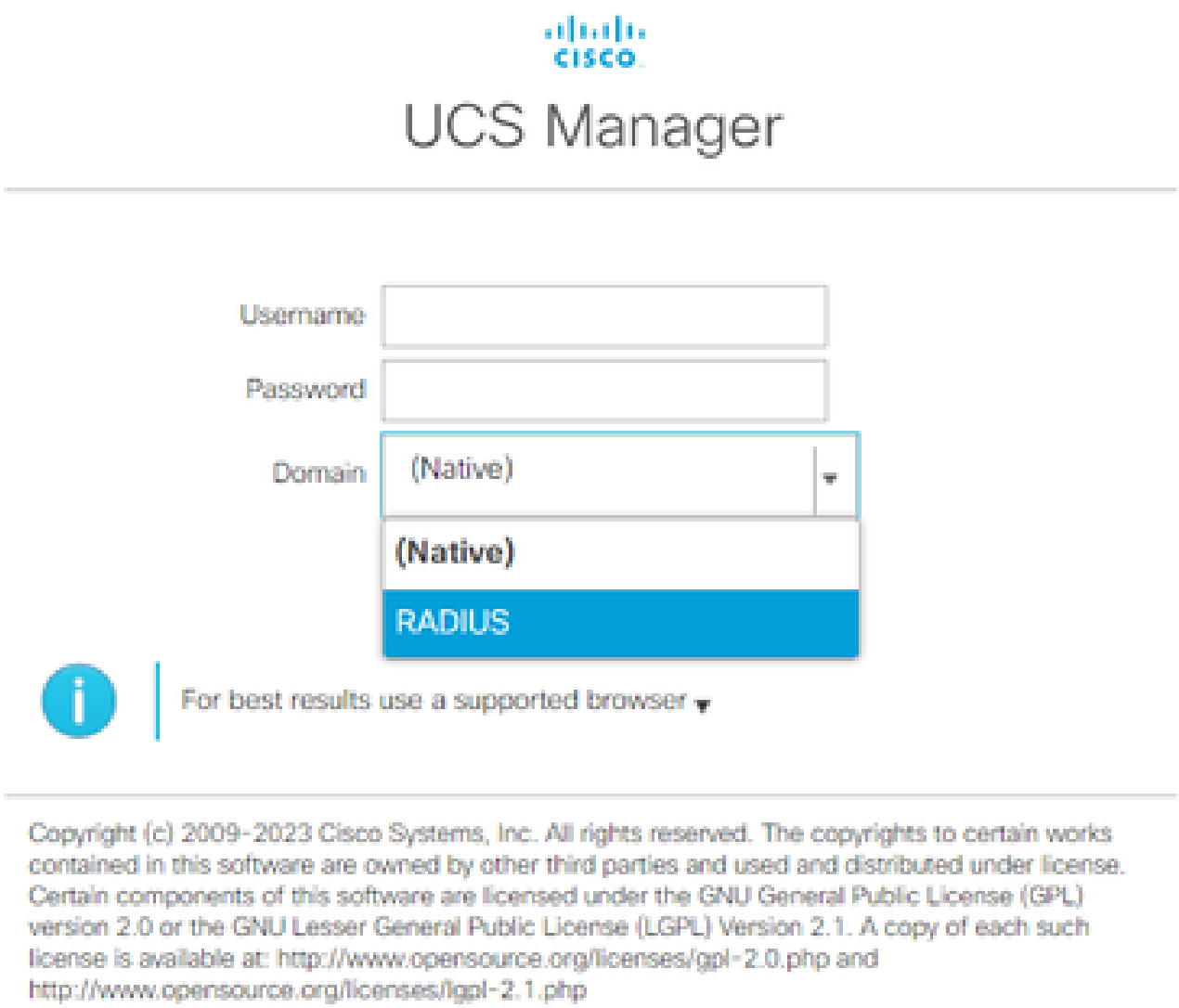
下一步並非強制性的。但是，執行此操作是為了使用與使用本地使用者的身份驗證域不同的身份驗證域，在UCS Manager初始登入螢幕中可以看到。

如果沒有單獨的身份驗證域，UCS Manager的登入螢幕如下所示：



沒有單獨身份驗證域的UCS Manager登入螢幕

使用單獨的身份驗證域時，這是UCS Manager的登入螢幕，其中新增了已建立的身份驗證域的清單。



帶有單獨身份驗證域的UCS Manager登入螢幕

如果您要將RADIUS身份驗證與UCS域中使用的其他身份驗證型別分開，這非常有用。

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

選擇新建立的身份驗證域的名稱，然後選擇RADIUS單選按鈕。在Provider Group中，選擇在本節的步驟3中建立的提供程式組。

驗證

FreeRADIUS有一些調試和故障排除工具，如下所述：

1. journalctl -u freeradius 命令提供有關freeRADIUS守護進程的一些有價值的資訊，例如錯誤配置和時間戳或初始化。在下面的示例中，我們可以看到users檔案修改錯誤。(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目錄包含一些日誌檔案，這些檔案包含為RADIUS伺服器記錄的所有日誌的清單。在此範例中：

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

3. systemctl status freeradius命令提供有關freeRADIUS服務的資訊：

```
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.
```

如需更多FreeRADIUS疑難排解/檢查，請參閱以下檔案 — https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf。

對於UCSM，可以使用以下命令在主FI中跟蹤使用RADIUS使用者的成功和不成功登入：

- connect nxos
- show logging logfile

成功的登入必須如下所示：

```
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
```

不成功的登入如下所示：

```
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是用於通過SSH連線到交換矩陣互聯的電腦的IP。

相關資訊

- 在UCSM中配置身份驗證
- FreeRADIUS伺服器設定
- FreeRADIUS Wiki

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。