Configurazione dell'autenticazione UCSM tramite RADIUS (FreeRADIUS)

Sommario

Introduzione

In questo documento viene descritta la configurazione dell'autenticazione UCSM con RADIUS.

Prerequisiti

Requisiti

- FreeRADIUS è operativo.
- UCS Manager, Fabric Interconnect e FreeRADIUS Server comunicano tra loro.

I destinatari sono gli amministratori UCS che hanno una conoscenza di base delle funzioni UCS.

Cisco raccomanda la conoscenza o la familiarità con i seguenti argomenti:

- Edizione file di configurazione Linux
- UCS Manager
- RaggioLibero
- Ubuntu o qualsiasi altra versione di Linux

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- UCS Manager (UCSM) 4.3(3a) o versione successiva.
- Fabric Interconnect 6464
- Ubuntu 22.04.4 LTS

- FreeRADIUS versione 3.0.26

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazione FreeRADIUS per autenticazione UCSM

Per eseguire questa procedura è necessario disporre del privilegio di accesso alla directory principale per il server freeRADIUS.

Passaggio 1. Configurare il dominio UCSM come client.

Passare al file clients.conf situato nella directory /etc/freeradius/3.0 e modificarlo utilizzando un editor di testo personalizzato. Per questo esempio è stato utilizzato l'editor 'vim' ed è stato creato il client '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
}
```

Il campo ipaddr può contenere solo l'indirizzo IP dell'interconnessione fabric principale. Nell'esempio, l'indirizzo IP 10.0.0.100/29 è stato usato per includere l'indirizzo IP VIP + mgmt0 di entrambi gli FI.

Il campo secret contiene la password utilizzata nella configurazione UCSM RADIUS (Passaggio 2).

Passaggio 2. Configurare l'elenco di utenti a cui è consentita l'autenticazione in UCSM.

Nella stessa directory - /etc/freeradius/3.0 - aprire il file users e creare un utente. Per questo esempio, è stato definito l'utente 'alerosa' con password 'password' per accedere come amministratore al dominio UCSM.

<#root>

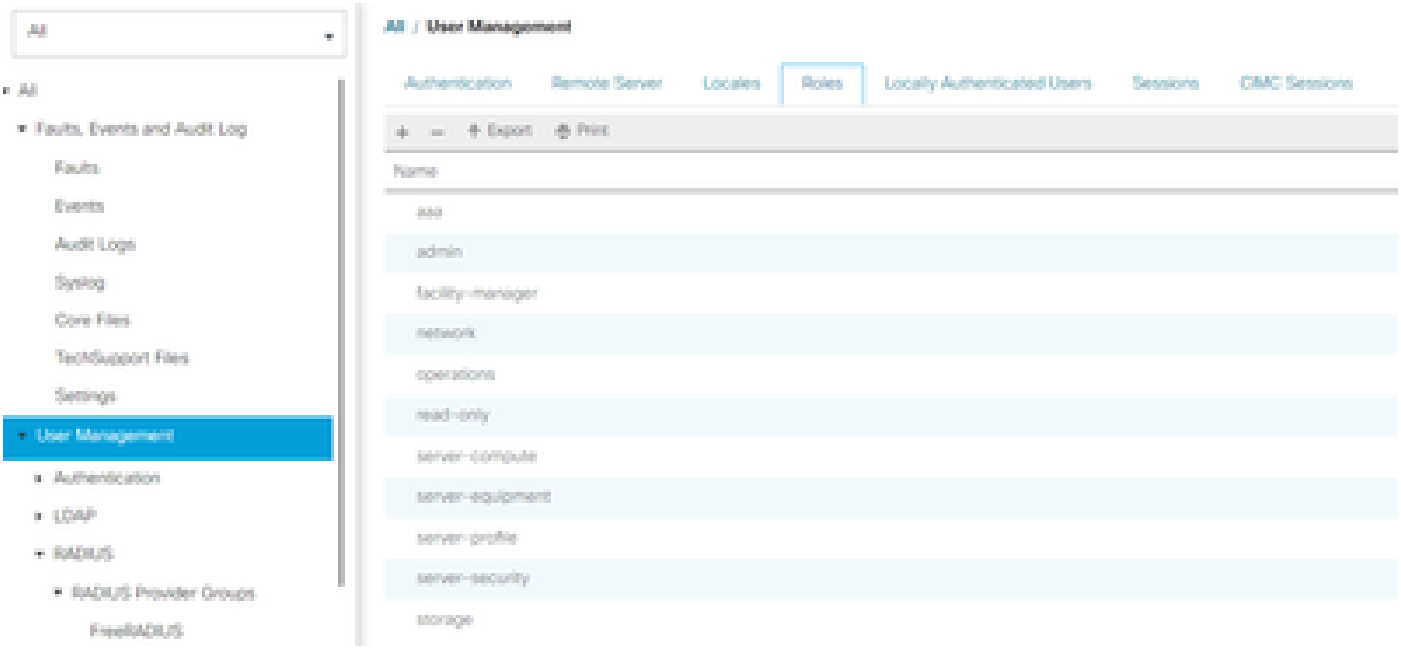
```
root@ubuntu:/etc/freeradius/3.0#
```

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

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

L'attributo cisco-avpair è obbligatorio e deve avere la stessa sintassi.

Il ruolo di amministratore può essere modificato per qualsiasi ruolo configurato in UCSM in Amministrazione > Gestione utente > Ruoli. In questa impostazione specifica, questi ruoli esistono



Se un utente deve avere più ruoli, è possibile utilizzare una virgola tra i ruoli e la sintassi deve essere simile a cisco-avpair = "shell:roles=aaa,facility-manager,read-only". Se un ruolo non creato in UCSM è definito nell'utente, l'autenticazione in UCSM non riesce.

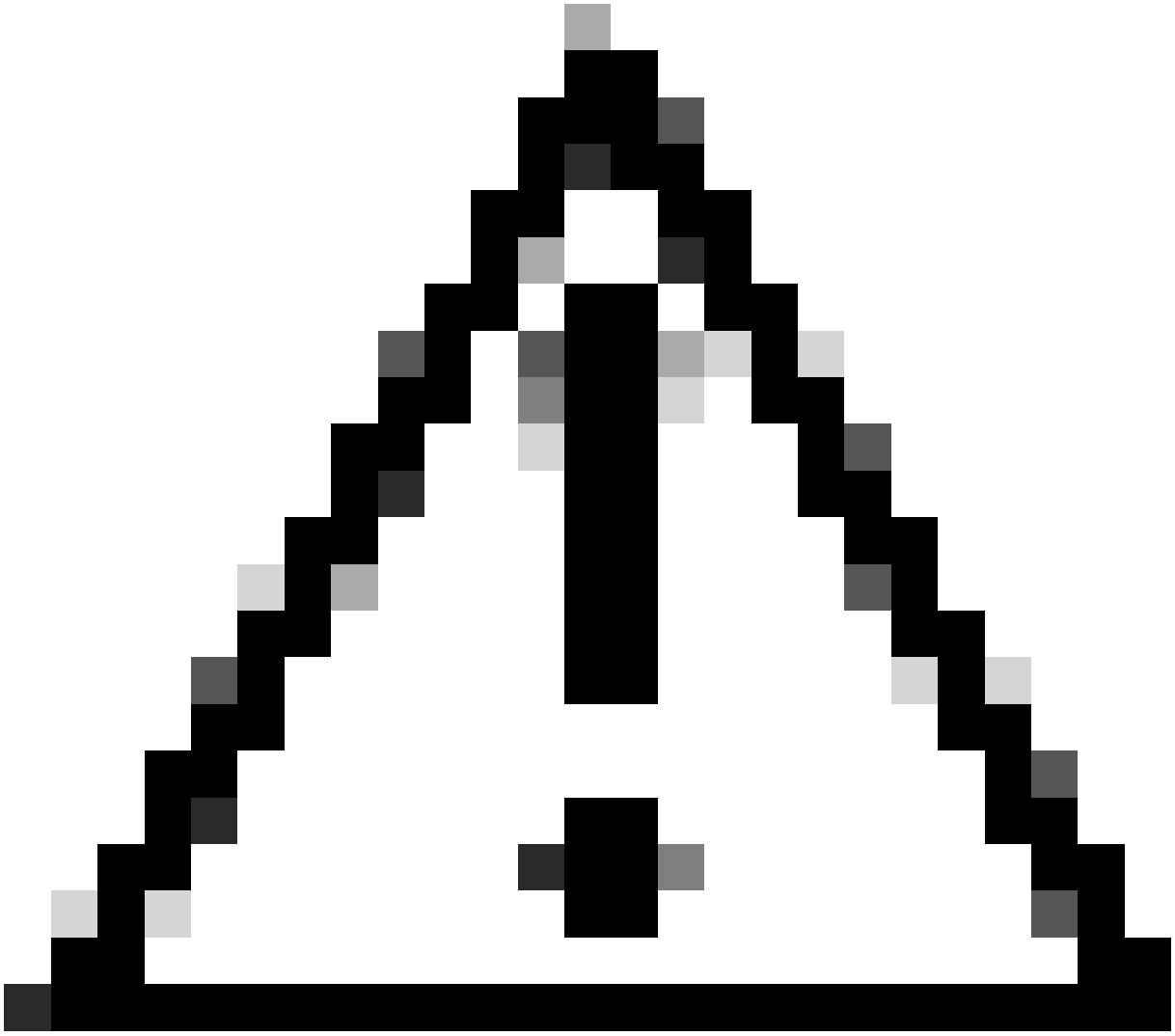
Passaggio 3. Abilitare/avviare il daemon FreeRADIUS.

Abilita avvio automatico per FreeRADIUS all'avvio del sistema.

```
systemctl enable freeradius
```

Avviare il daemon FreeRADIUS:

```
systemctl restart freeradius
```



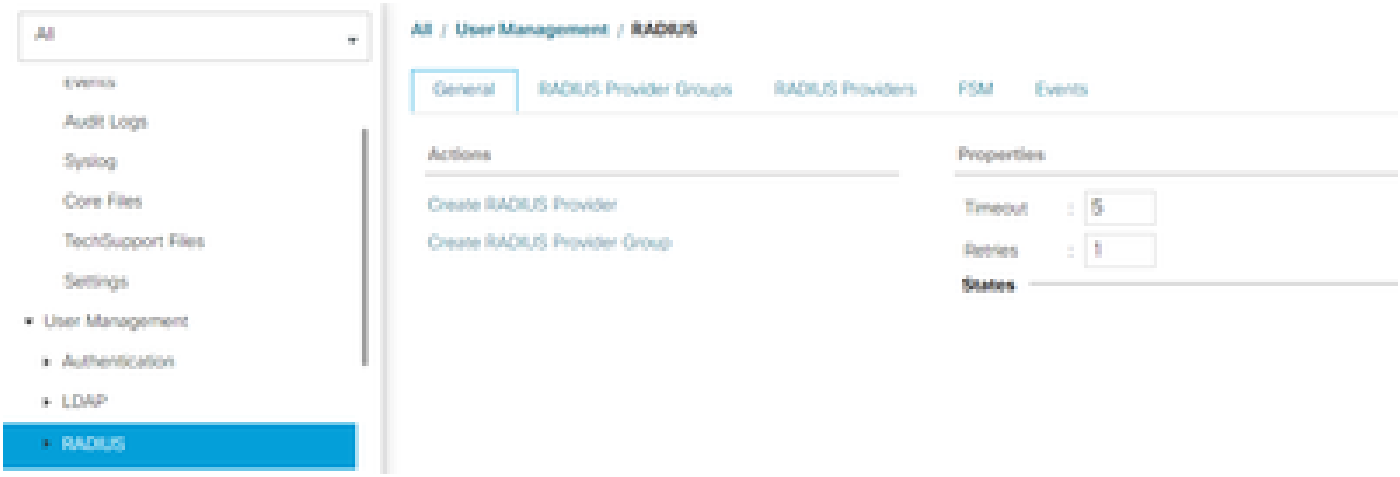
Attenzione: Quando vengono apportate modifiche nei file 'clients.conf' o 'users', è necessario riavviare il daemon FreeRADIUS, altrimenti le modifiche non vengono applicate

Configurazione autenticazione RADIUS UCSM

La configurazione di UCS Manager segue le istruzioni di questo documento - https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configura

Passaggio 1. Proprietà predefinite configurate per i provider RADIUS.

Selezionare Admin > User Management > RADIUS e sono stati utilizzati i valori predefiniti.



Passaggio 2. Creare un provider RADIUS.

In Amministrazione > Gestione utente, selezionare RADIUS e fare clic su Crea provider RADIUS.

Nome host/FQDN (o indirizzo IP) è l'indirizzo IP o FQDN del server/macchina virtuale.

Chiave è la chiave o il segreto definiti nel server RADIUS nel file 'clients.conf' (Passaggio 1. della configurazione FreeRADIUS).

Passaggio 3. Creare un gruppo di provider RADIUS.

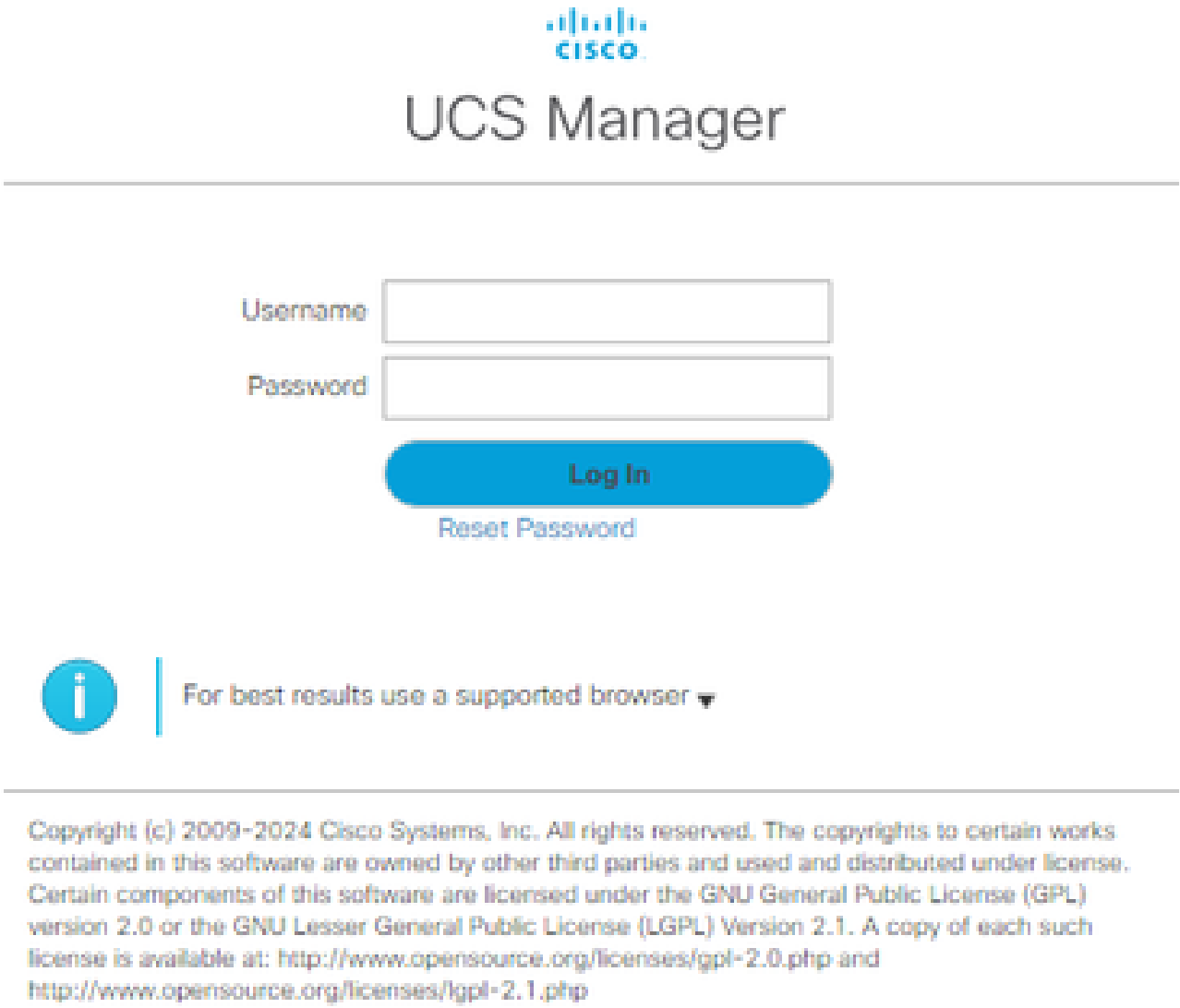
In Amministrazione > Gestione utente, selezionare RADIUS e fare clic su Crea gruppo di provider RADIUS.

Fornire un nome, in questo caso è stato utilizzato 'FreeRADIUS'. Aggiungere quindi il provider RADIUS creato nel passaggio 2 all'elenco dei provider inclusi.

Passaggio 4. Creare un nuovo dominio di autenticazione (facoltativo).

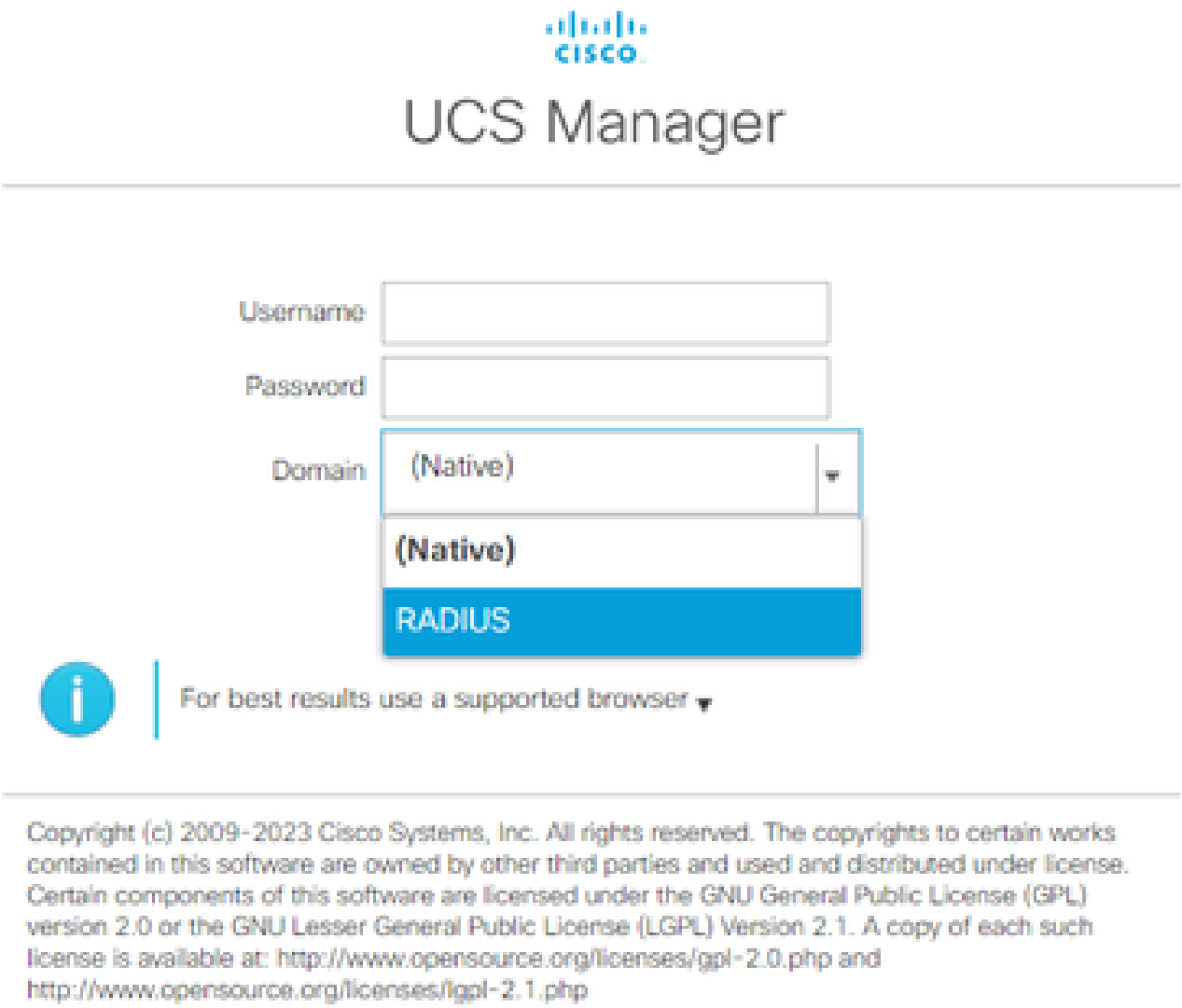
La fase successiva non è obbligatoria. Tuttavia, è stato eseguito per avere un dominio di autenticazione separato diverso da quello che utilizza gli utenti locali, che è visibile nella schermata di accesso iniziale di UCS Manager.

Senza un dominio di autenticazione separato, la schermata di accesso di UCS Manager ha il seguente aspetto:



Schermata di accesso a UCS Manager senza un dominio di autenticazione separato

Mentre con un dominio di autenticazione separato, questa è la schermata di accesso di UCS Manager aggiunge un elenco dei domini di autenticazione creati.



Schermata di accesso a UCS Manager con un dominio di autenticazione separato

Ciò è utile se si desidera separare l'autenticazione RADIUS da altri tipi di autenticazione utilizzati anche nel dominio UCS.

Selezionare Amministrazione > Gestione utenti > Autenticazione > Crea dominio.

Scegliere il nome del dominio di autenticazione appena creato e scegliere il pulsante di opzione RADIUS. Nel gruppo di provider, selezionare il gruppo di provider creato nel passo 3 di questa sezione.

Verifica

FreeRADIUS dispone di un paio di strumenti di debug e risoluzione dei problemi, come quelli descritti di seguito:

1. Il comando journalctl -u freeradius fornisce alcune informazioni importanti sul daemon freeRADIUS, ad esempio gli errori nella configurazione e i timestamp degli errori o delle inizializzazioni. Nell'esempio seguente è possibile notare che il file users è stato modificato in

modo errato. (mods-config/files/authorization è il collegamento simbolico del file degli utenti):

```
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. La directory /var/log/freeradius contiene alcuni file di log contenenti un elenco di tutti i log registrati per il server RADIUS. In questo esempio:

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

3. Il comando systemctl status freeradius fornisce informazioni sul servizio 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.
```

Per ulteriori procedure di risoluzione dei problemi/controllo di FreeRADIUS, fare riferimento a questo documento - https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf.

Per UCSM, gli accessi riusciti e non riusciti tramite utenti RADIUS possono essere rilevati nell'infrastruttura primaria utilizzando i comandi seguenti:

- connetti nxos
- mostra file registro

Un accesso riuscito deve avere il seguente aspetto:

```
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
```

Un accesso non riuscito ha il seguente aspetto:

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

Dove X.X.X.X è l'indirizzo IP del computer utilizzato per collegare il protocollo SSH all'interconnessione fabric.

Informazioni correlate

- Configurazione dell'autenticazione in UCSM
- Installazione del server FreeRADIUS
- Wiki FreeRADIUS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).