Konfigurieren der UCSM-Authentifizierung mithilfe von RADIUS (FreeRADIUS)

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der UCSM-Authentifizierung mithilfe von RADIUS beschrieben.

Voraussetzungen

Anforderungen

- FreeRADIUS ist betriebsbereit.
- UCS Manager, Fabric Interconnects und FreeRADIUS-Server kommunizieren miteinander.

Zielgruppe sind UCS-Administratoren mit grundlegenden Kenntnissen über UCS-Funktionen.

Cisco empfiehlt, dass Sie mit diesen Themen vertraut sind bzw. über entsprechende Kenntnisse verfügen:

- Edition der Linux-Konfigurationsdatei
- UCS-Manager
- FreeRADIUS
- Ubuntu oder eine andere Linux-Version

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- UCS Manager (UCSM) 4.3(3a) oder höher

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

FreeRADIUS-Konfiguration für UCSM-Authentifizierung

Für diese Schritte ist eine Root-Zugriffsberechtigung für den freeRADIUS-Server erforderlich.

Schritt 1: Konfigurieren der UCSM-Domäne als Client.

Navigieren Sie zur Datei clients.conf im Verzeichnis /etc/freradius/3.0 und bearbeiten Sie die Datei mit einem Texteditor Ihrer Wahl. Für dieses Beispiel wurde der 'vim'-Editor verwendet, und der Client 'UCS-POD' wurde erstellt.

<#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
}
```

Das Feld ipaddr darf nur die IP-Adresse des primären Fabric Interconnects enthalten. In diesem Beispiel wurde die IP 10.0.0.100/29 IP verwendet, um die IP VIP + mgmt0 beider FIs einzuschließen.

Das geheime Feld enthält das Kennwort für die UCSM RADIUS-Konfiguration (Schritt 2).

Schritt 2: Konfigurieren Sie die Liste der Benutzer, die sich bei UCSM authentifizieren dürfen.

Im gleichen Verzeichnis - /etc/freradikus/3.0 - öffnen Sie die Benutzer-Datei und erstellen Sie einen Benutzer. Für dieses Beispiel wurde der Benutzer "alerosa" mit dem Kennwort "password" definiert, um sich als Administrator bei der UCSM-Domäne anzumelden.

<#root>

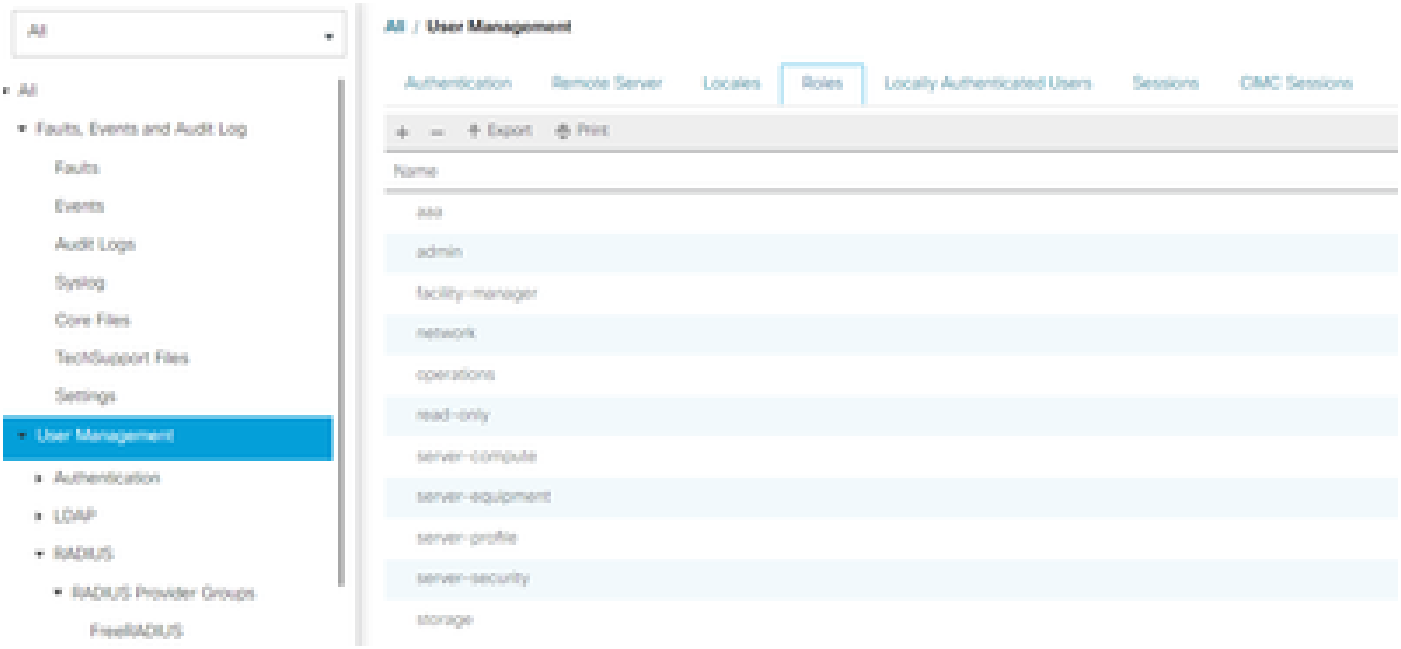
```
root@ubuntu:/etc/freeradius/3.0#

vim users
*Inside users file*


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

Das Attribut cisco-avpair ist obligatorisch und muss der gleichen Syntax folgen.

Die Admin-Rolle kann für jede Rolle geändert werden, die in UCSM unter Admin > Benutzerverwaltung > Rollen konfiguriert ist. In dieser spezifischen Konfiguration gibt es diese Rollen.



Wenn ein Benutzer über mehrere Rollen verfügen muss, kann ein Komma zwischen den Rollen verwendet werden, und die Syntax muss etwa cisco-avpair = "shell:roles=aaa,facility-manager,read-only" lauten. Wenn eine nicht in UCSM erstellte Rolle im Benutzer definiert ist, schlägt die Authentifizierung in UCSM fehl.

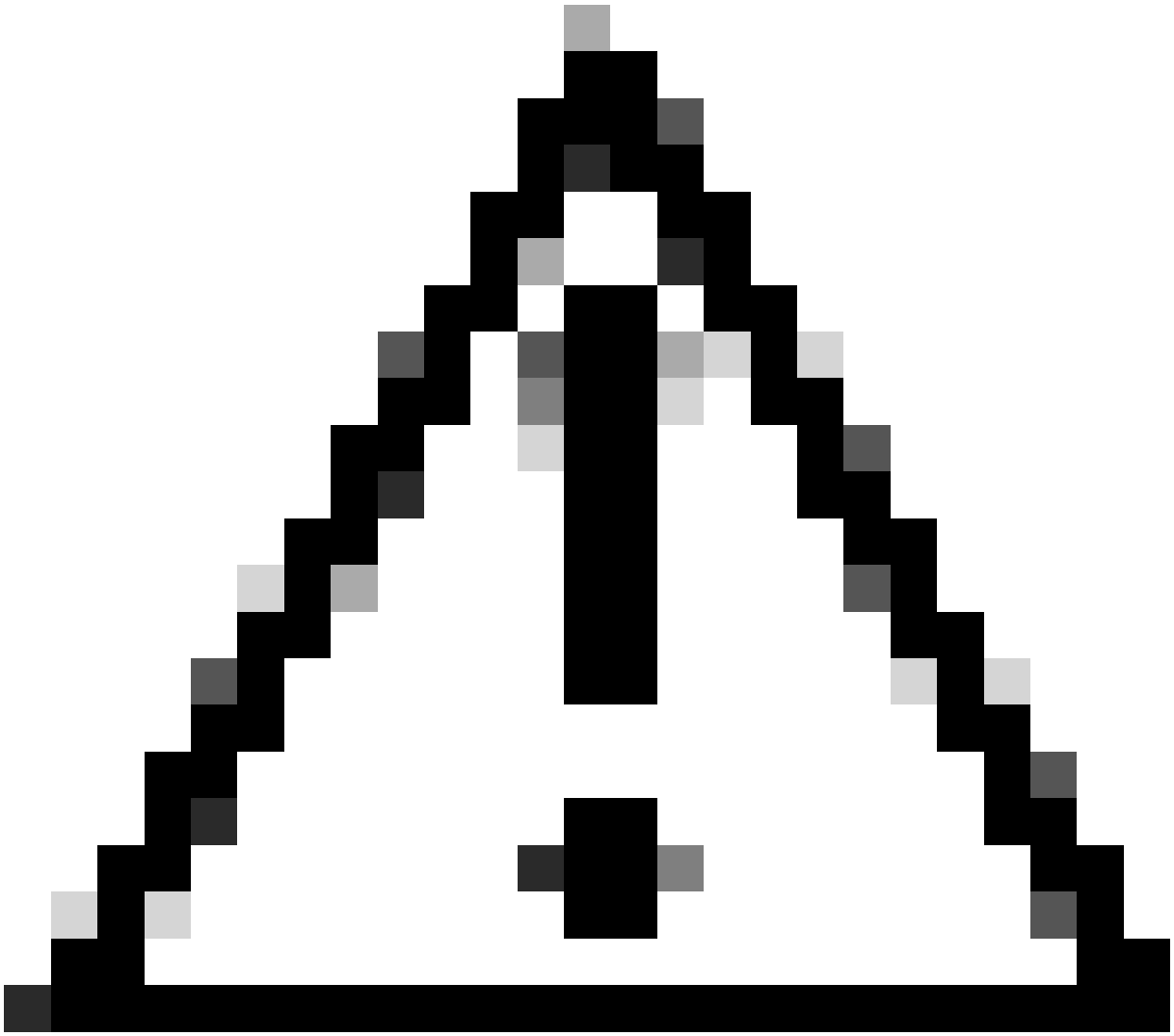
Schritt 3: Aktivieren/Starten des FreeRADIUS-Daemons.

Aktivieren Sie den automatischen Start für FreeRADIUS beim Systemstart.

```
systemctl enable freeradius
```

Starten Sie den FreeRADIUS-Daemon:

```
systemctl restart freeradius
```



Vorsicht: Wenn Änderungen in den 'clients.conf'- oder 'users'-Dateien vorgenommen werden, muss der FreeRADIUS-Daemon neu gestartet werden, andernfalls werden die Änderungen nicht angewendet

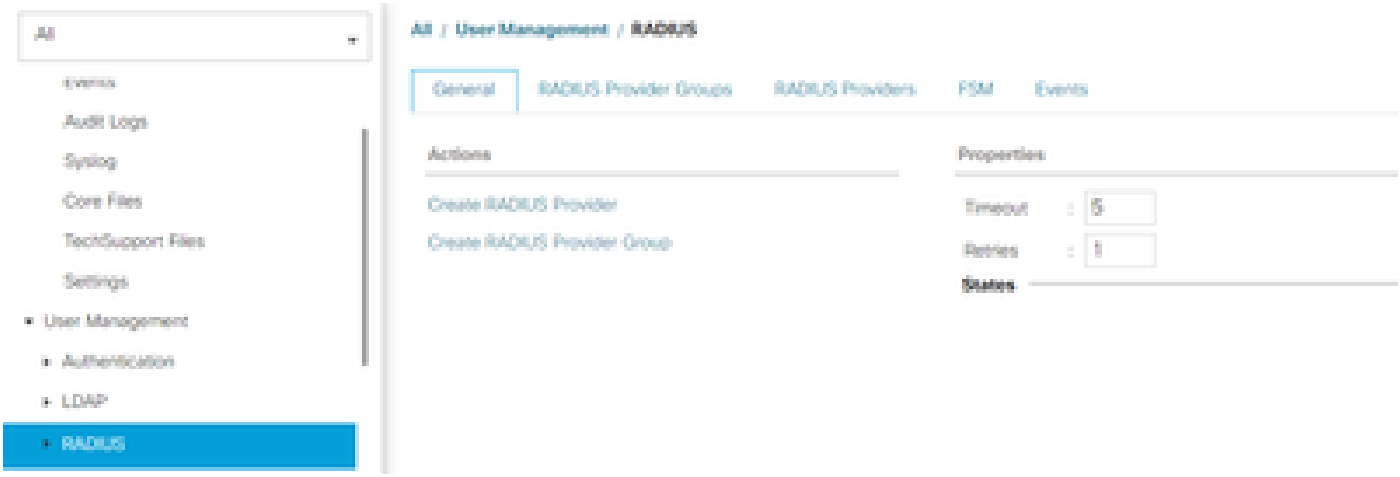
---

UCSM RADIUS-Authentifizierungskonfiguration

Die UCS Manager-Konfiguration folgt den Anweisungen in diesem Dokument: https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configura

Schritt 1: Konfigurierte Standardeigenschaften für RADIUS-Anbieter.

Navigieren Sie zu Admin > User Management > RADIUS, und verwenden Sie die Standardwerte.



Schritt 2: Erstellen eines RADIUS-Anbieters.

Wählen Sie in Admin > User Management (Verwaltung > Benutzerverwaltung) RADIUS aus, und klicken Sie auf Create RADIUS Provider (RADIUS-Anbieter erstellen).

Hostname/FQDN (oder IP-Adresse) ist die IP-Adresse oder der FQDN des Servers/virtuellen Systems.

Schlüssel ist der Schlüssel/Schlüssel, der im RADIUS-Server in der Datei "clients.conf" definiert ist (Schritt 1 der FreeRADIUS-Konfiguration).

Schritt 3: Erstellen einer RADIUS-Anbietergruppe.

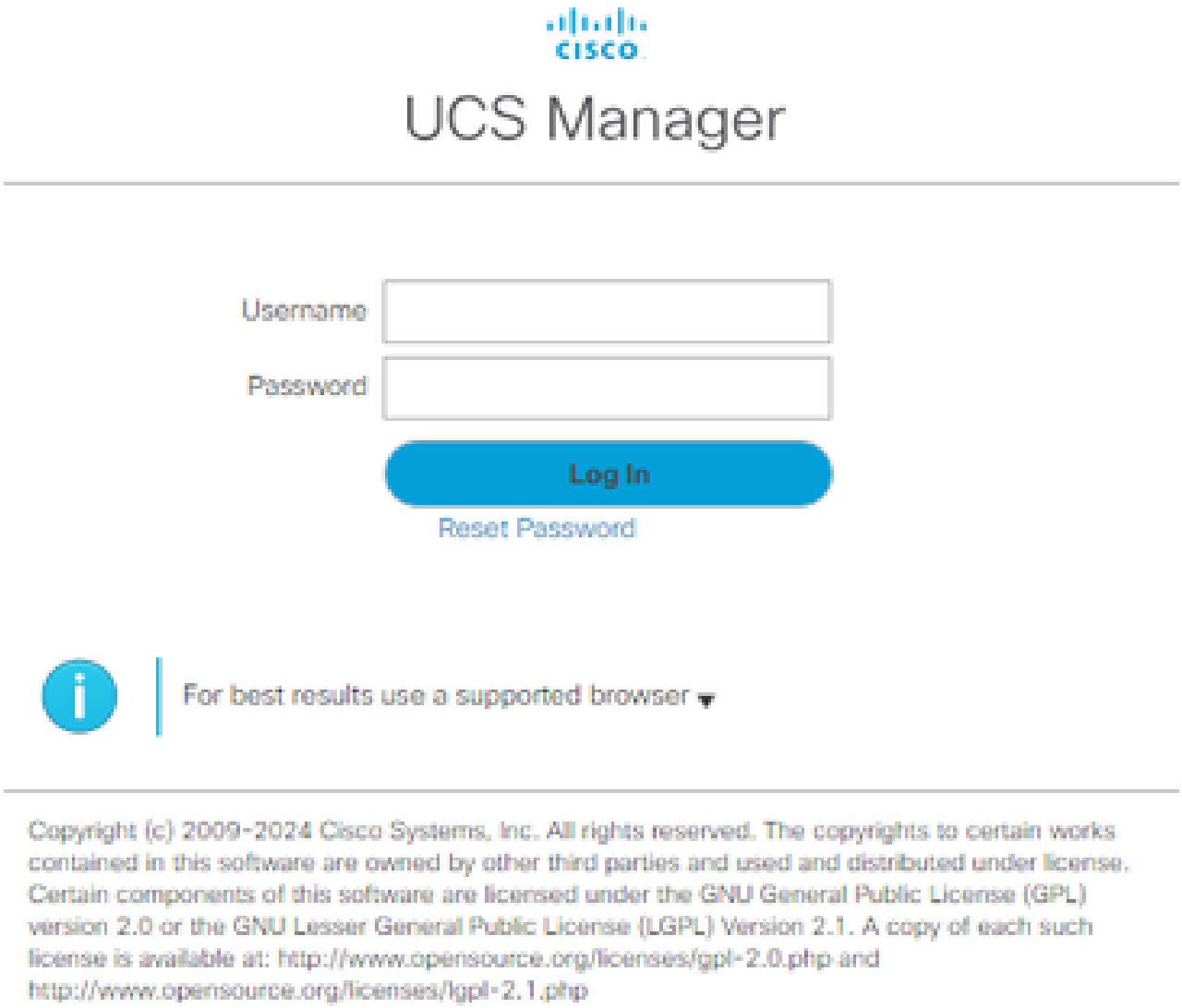
Wählen Sie in Admin > User Management (Verwaltung > Benutzerverwaltung) RADIUS aus, und klicken Sie auf Create RADIUS Provider Group (RADIUS-Anbietergruppe erstellen).

Geben Sie einen Namen an, in diesem Fall wurde 'FreeRADIUS' verwendet. Fügen Sie dann den in Schritt 2 erstellten RADIUS-Anbieter zur Liste der enthaltenen Anbieter hinzu.

Schritt 4: Erstellen einer neuen Authentifizierungsdomäne (optional)

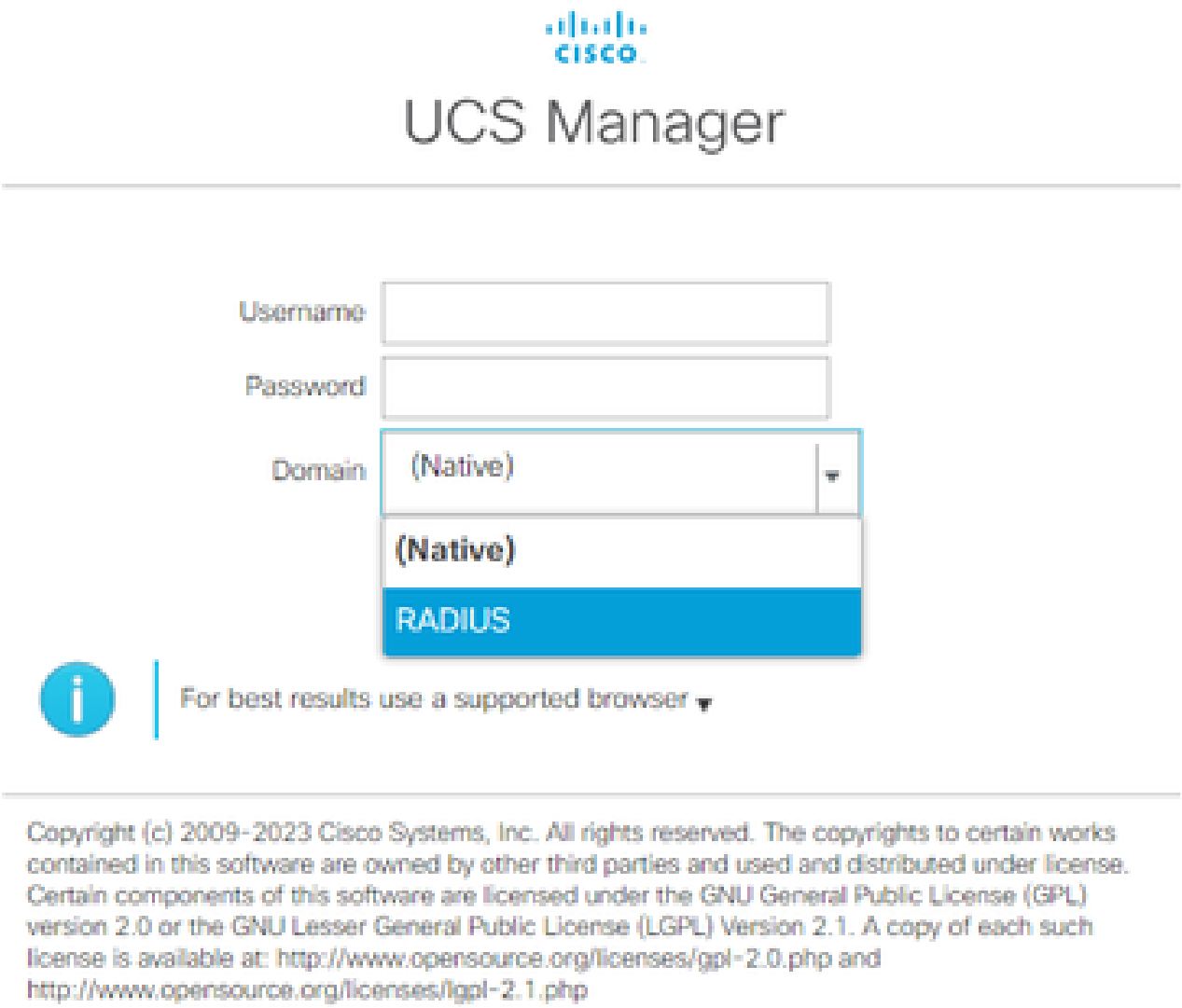
Der nächste Schritt ist nicht obligatorisch. Es wurde jedoch eine separate Authentifizierungsdomäne erstellt, die sich von der Domäne unterscheidet, die lokale Benutzer verwendet. Diese wird im UCS Manager-Anmeldebildschirm angezeigt.

Ohne separate Authentifizierungsdomäne sieht der Anmeldebildschirm von UCS Manager wie folgt aus:



UCS Manager-Anmeldebildschirm ohne separate Authentifizierungsdomäne

Bei einer separaten Authentifizierungsdomäne handelt es sich um den Anmeldebildschirm von UCS Manager, auf dem eine Liste der erstellten Authentifizierungsdomänen hinzugefügt wird.



UCS Manager-Anmeldebildschirm mit separater Authentifizierungsdomäne

Dies ist nützlich, wenn Sie die RADIUS-Authentifizierung von anderen Authentifizierungstypen trennen möchten, die auch in der UCS-Domäne verwendet werden.

Navigieren Sie zu Admin > User Management > Authentication > Create a Domain.

Wählen Sie den Namen der neu erstellten Authentifizierungsdomäne und anschließend das Optionsfeld RADIUS aus. Wählen Sie in der Anbietergruppe die Anbietergruppe aus, die in Schritt 3 dieses Abschnitts erstellt wurde.

Überprüfung

FreeRADIUS bietet eine Reihe von Tools zur Fehlerbehebung, wie die unten beschriebenen:

1. Der Befehl journalctl -u freradius liefert einige wertvolle Informationen über den freeRADIUS-Daemon, wie Fehler in der Konfiguration und Zeitstempel von Fehlern oder Initialisierungen. Im Beispiel unten sehen wir, dass die Datei users falsch modifiziert wurde. (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. Das Verzeichnis /var/log/freradikus enthält einige Protokolldateien, die eine Liste aller Protokolle enthalten, die für den RADIUS-Server aufgezeichnet wurden. In diesem Beispiel:

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

3. Der Befehl systemctl status freradius liefert Informationen über den Dienst 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.
```

Weitere FreeRADIUS-Fehlerbehebungen/-Prüfungen finden Sie in diesem Dokument unter: https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf.

Für UCSM können erfolgreiche und erfolglose Anmeldungen mit RADIUS-Benutzern mithilfe der folgenden Befehle im primären FI nachverfolgt werden:

- Anschließen von NX
- Protokolldatei anzeigen

Eine erfolgreiche Anmeldung muss wie folgt aussehen:

```
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
```

Eine fehlgeschlagene Anmeldung sieht in etwa so aus:

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

wobei X.X.X.X die IP-Adresse des Systems ist, das für SSH-to-Fabric Interconnects verwendet wird.

Zugehörige Informationen

- Konfigurieren der Authentifizierung in UCSM
- FreeRADIUS Server-Setup
- FreeRADIUS-Wiki

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.