RADIUS(FreeRADIUS)を使用したUCSM認証の設定

内容

はじめに

このドキュメントでは、RADIUSを使用したUCSM認証の設定について説明します。

前提条件

要件

- FreeRADIUSは動作しています。
- UCS Manager、Fabric Interconnect、およびFreeRADIUSサーバは相互に通信します。

対象読書は、UCS 機能の基本的な知識がある UCS 管理者です。

次の項目に関する知識があるか、または精通しておくことをお勧めします。

- Linux構成ファイルエディション
- UCS マネージャ
- FreeRADIUS
- Ubuntuまたはその他のLinuxバージョン

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- UCS Manager(UCSM)4.3(3a)以降
- ファブリックインターコネクト6464
- Ubuntu 22.04.4 LTS。
- FreeRADIUSバージョン3.0.26

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

UCSM認証用のFreeRADIUS設定

これらの手順には、freeRADIUSサーバへのルートアクセス権限が必要です。

ステップ 1：UCSMドメインをクライアントとして設定する。

/etc/freeradius/3.0 ディレクトリにあるclients.confファイルに移動し、テキスト エディタを使用してファイルを編集します。この例では、「vim」エディタが使用され、クライアント「UCS-POD」が作成されました。

<#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フィールドには、プライマリFabric InterconnectのIPだけを入力できます。この例では、IP 10.0.0.100/29 IPが使用され、両方のFIのVIP + mgmt0 IPが含まれています。

secretフィールドには、UCSM RADIUS設定(ステップ2)で使用するパスワードが含まれています。

ステップ 2：UCSMへの認証を許可されるユーザのリストを設定します。

同じディレクトリ(/etc/freeradius/3.0)で、users ファイルを開き、ユーザを作成します。この例では、パスワード「password」のユーザ「alerosa」は、UCSMドメインに管理者としてログインするように定義されています。

<#root>

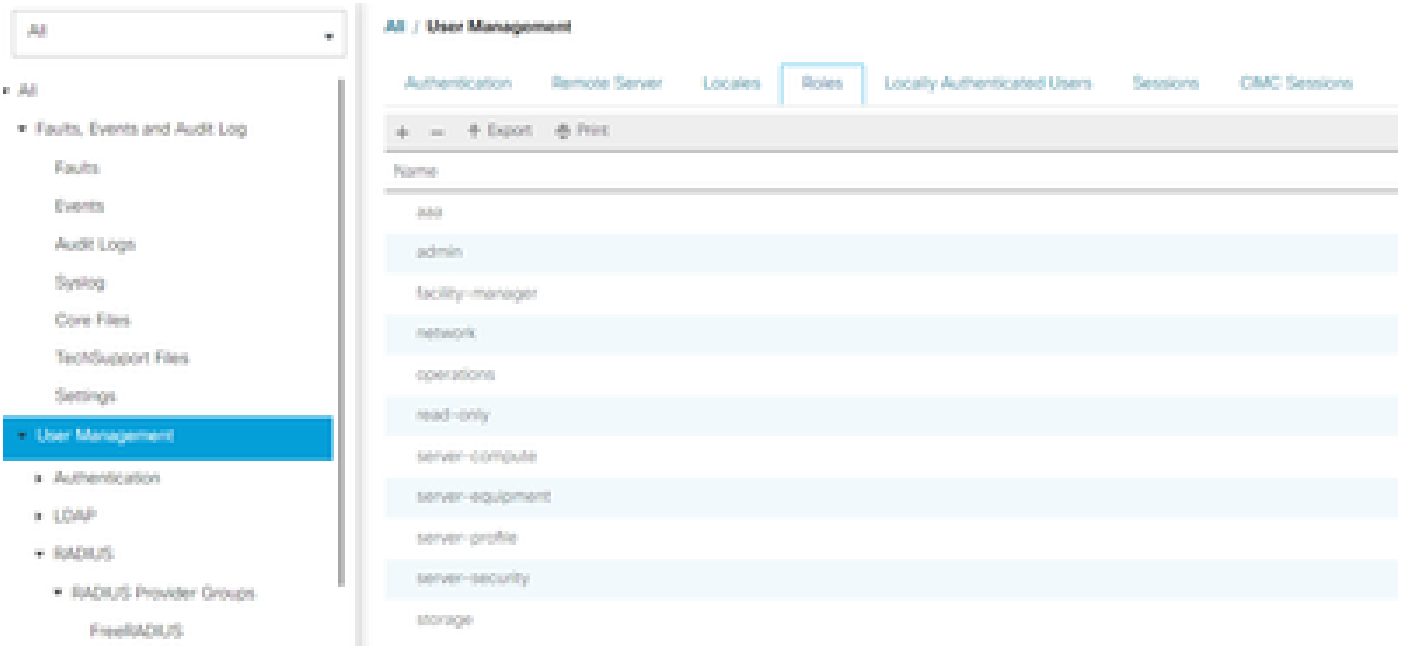
```
root@ubuntu:/etc/freeradius/3.0#

vim users
*Inside users file*
```

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

cisco-avpair属性は必須であり、同じ構文に従う必要があります。

管理者ロールは、UCSMのAdmin > User Management > Rolesで設定されたロールに対して変更できます。この特定の設定では、次のロールが存在します



ユーザが複数のロールを持つ必要がある場合は、ロール間にカンマを使用できます。構文はcisco-avpair = "shell:roles=aaa,facility-manager,read-only"のようになります。 UCSMで作成されていないロールがユーザで定義されている場合、UCSMでの認証は失敗します。

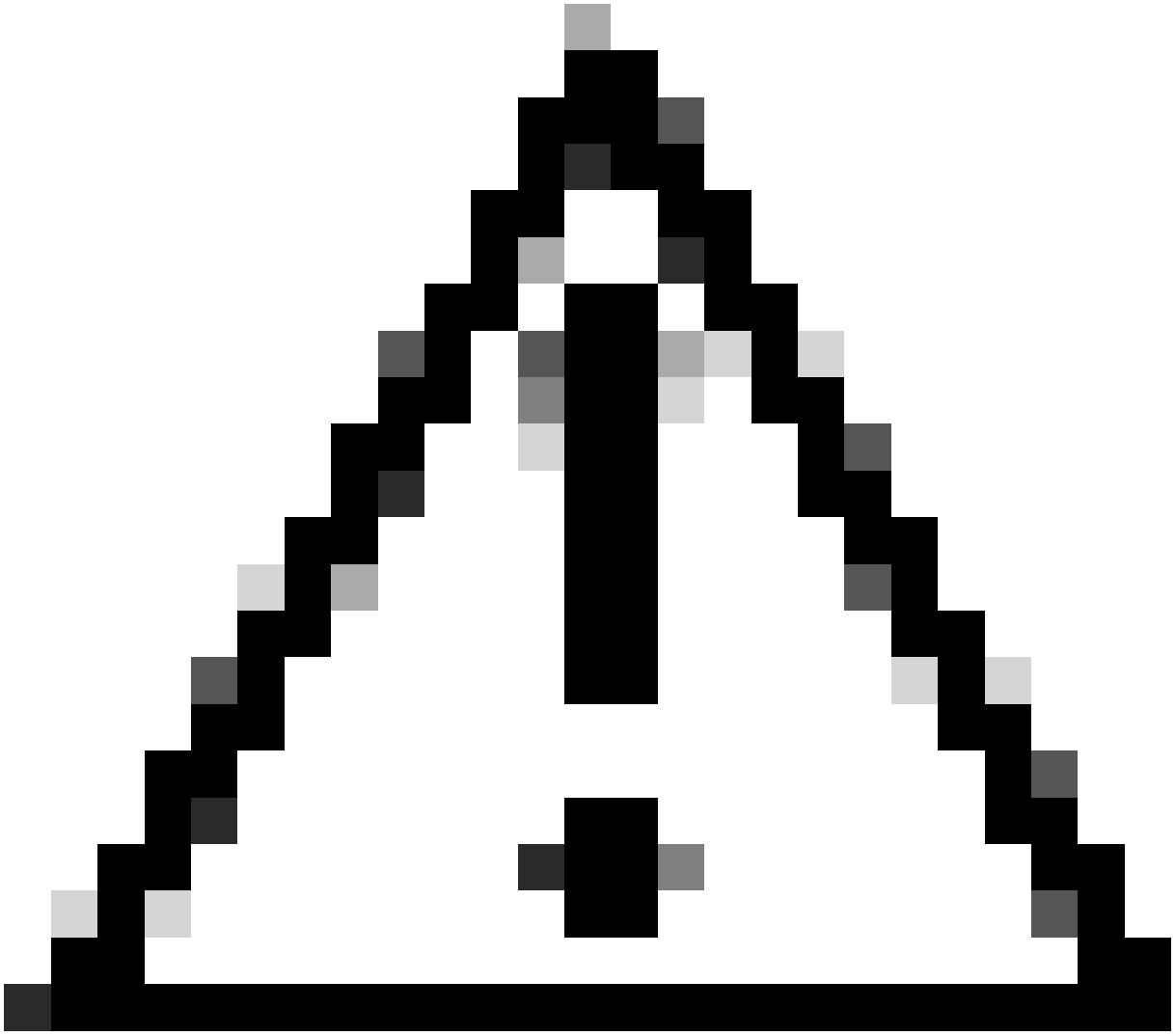
ステップ 3：FreeRADIUSデーモンを有効/開始します。

システムの起動時にFreeRADIUSの自動起動を有効にします。

```
systemctl enable freeradius
```

FreeRADIUSデーモンを起動します。

```
systemctl restart freeradius
```



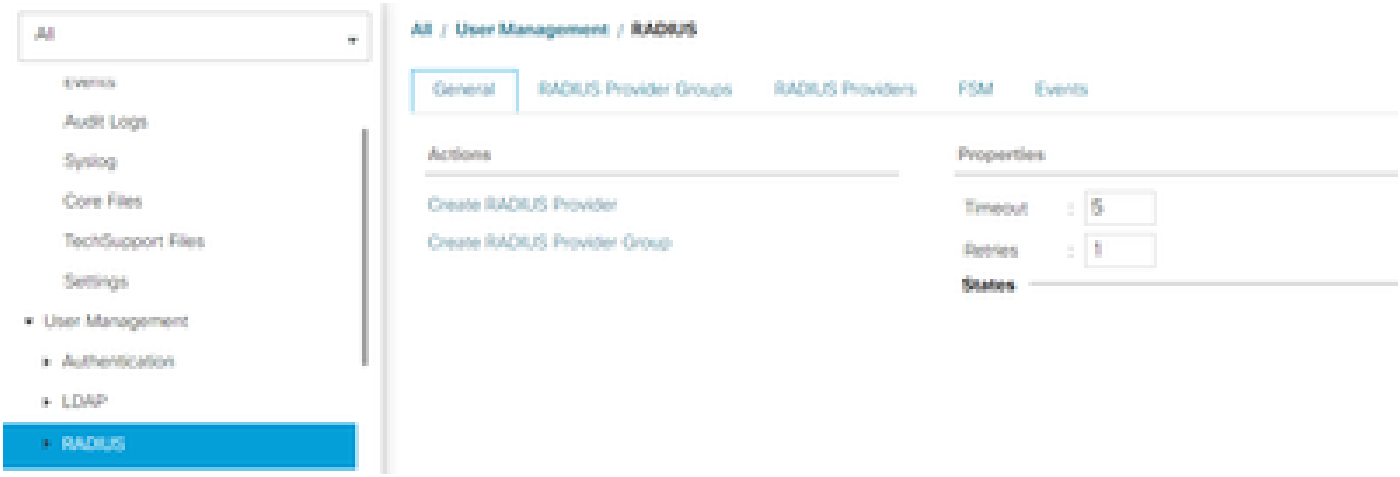
注意:「clients.conf」または「users」ファイルを変更した場合、FreeRADIUSデーモンを再起動する必要があります。再起動しない場合、変更は適用されません

UCSM RADIUS認証設定

UCS Managerの設定は、このドキュメント(https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configura
順に従います。

ステップ 1：RADIUSプロバイダーの設定済みデフォルトプロパティ』を参照してください。

Admin > User Management > RADIUSの順に移動し、デフォルト値を使用しました。



ステップ 2：RADIUSプロバイダーの作成

Admin > User Managementで、RADIUSを選択して、Create RADIUS Providerをクリックします。

Hostname/FQDN（またはIP Address）は、サーバ/仮想マシンのIPまたはFQDNです。

Keyは、「clients.conf」ファイル（FreeRADIUS設定のステップ1）のRADIUSサーバで定義されているキー/シークレットです。

ステップ 3：RADIUSプロバイダーグループを作成します。

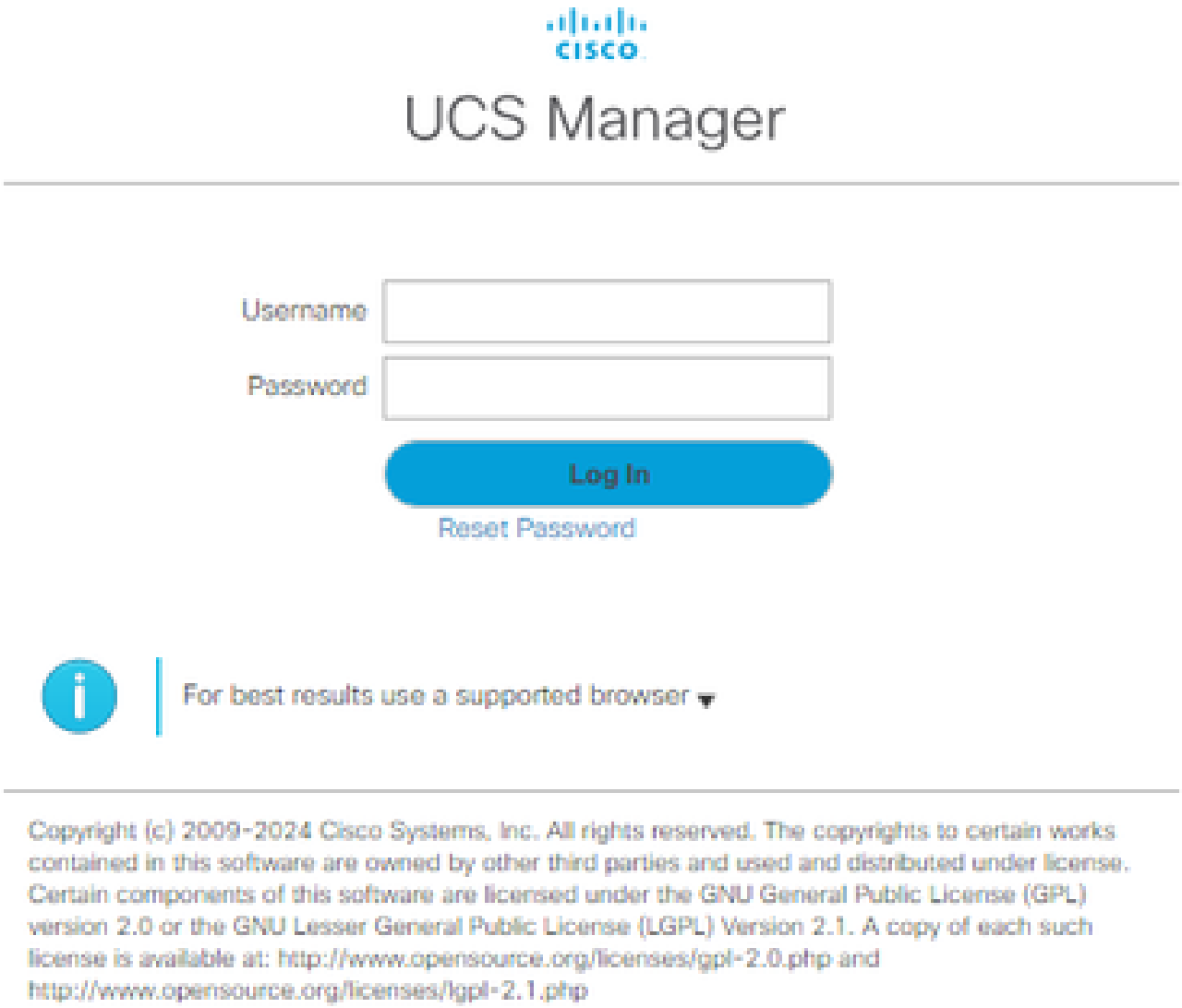
Admin > User Managementで、RADIUSを選択して、Create RADIUS Provider Groupをクリックします。

名前を入力します。この例では、「FreeRADIUS」が使用されています。次に、ステップ2で作成したRADIUSプロバイダーを含めるプロバイダーのリストに追加します。

ステップ 4：新しい認証ドメインを作成します（オプション）。

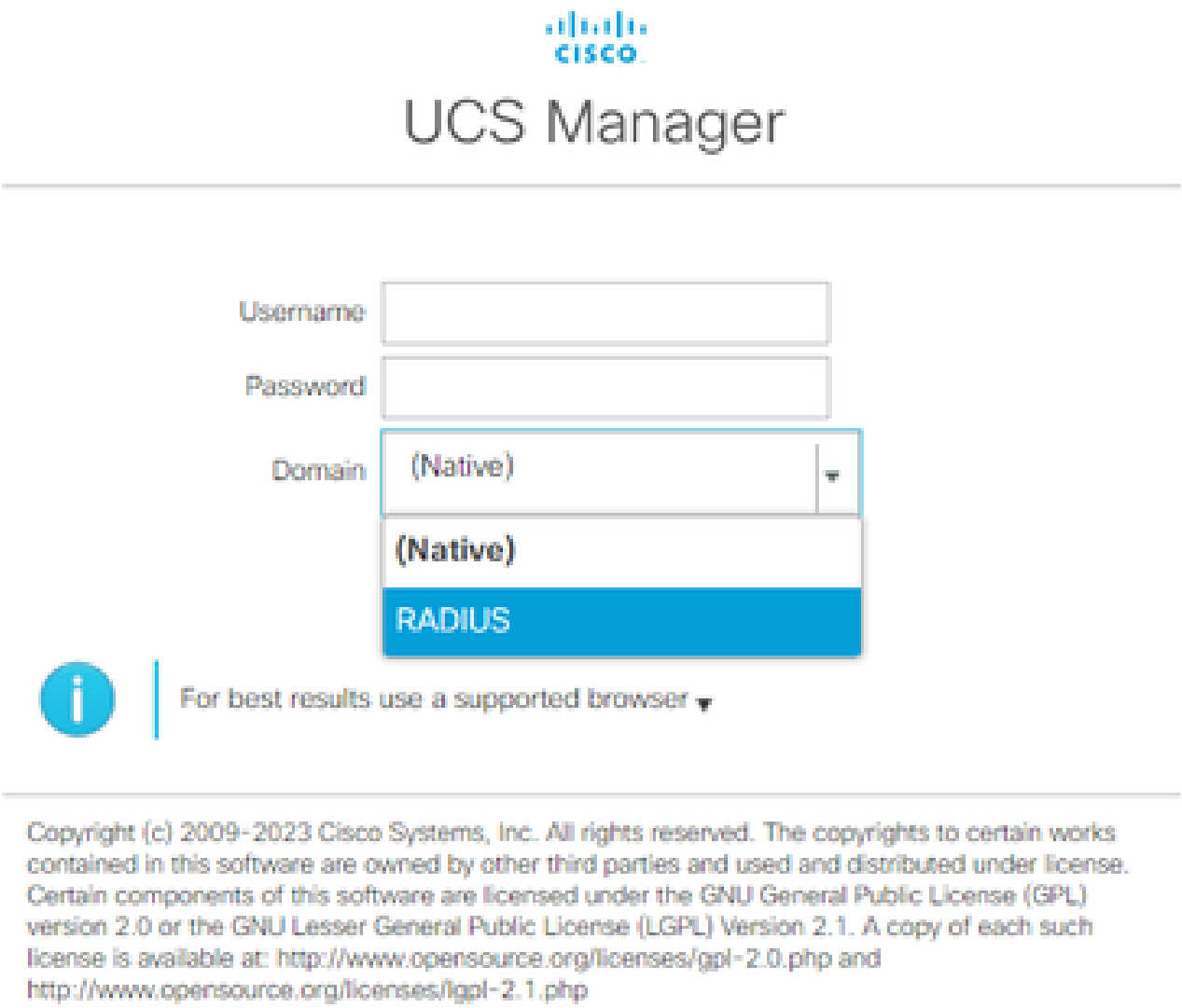
次の手順は必須ではありません。ただし、UCS Managerの初期ログイン画面に表示される、ローカルユーザを使用する認証ドメインとは異なる認証ドメインを設定するために実行されました。

個別の認証ドメインがない場合、UCS Managerのログイン画面は次のようになります。



個別の認証ドメインを持たないUCS Managerログイン画面

別の認証ドメインがある場合、UCS Managerのログイン画面に作成された認証ドメインのリストが追加されます。



個別の認証ドメインを持つUCS Managerログイン画面

これは、RADIUS認証を、UCSドメインでも使用されている他の認証タイプと区別する場合に便利です。

Admin > User Management > Authentication > Create a Domainの順に移動します。

新しく作成した認証ドメインの名前を選択し、RADIUSオプションボタンを選択します。Provider Groupで、このセクションのステップ3で作成したProvider Groupを選択します。

確認

FreeRADIUSには、次に説明するようなデバッグおよびトラブルシューティングツールがいくつかあります。

1. journalctl -u freeradius コマンドは、設定のエラーや、エラーまたは初期化のタイムスタンプなど、freeRADIUSデーモンに関する有用な情報を提供します。次の例では、usersファイルが誤って変更されたことが分かります。(mods-config/files/authorizeは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ディレクトリには、RADIUSサーバに関して記録されたすべてのログのリストを含むログファイルが格納されています。この例では、

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

3. systemctl status freeradiusコマンドは、freeRADIUSサービスに関する情報を提供します。

```
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.
```

FreeRADIUSのトラブルシューティングとチェックの詳細については、https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdfを参照してください。

UCSMでは、RADIUSユーザを使用した成功および失敗のログインは、次のコマンドを使用してプライマリFIで追跡できます。

- NXOSの接続
- show logging logfile

正常なログインは次のようになります。

```
2024 Sep 16 09:56:19 UCS-POD %UCSM-6-AUDIT: [session][internal][creation][internal][2677332][sys/user-ex
_8291_A, name:ucs-RADIUS\alerosa, policyOwner:local][] Web A: remote user ucs-RADIUS\alerosa logged in
```

ログインに失敗した場合は、次のように表示されます。

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

X.X.X.Xは、ファブリックインターコネクトへのSSHに使用されるマシンのIPです。

関連情報

- UCSMでの認証の設定
- FreeRADIUSサーバセットアップ
- FreeRADIUSのWiki

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。