

RADIUS(FreeRADIUS)를 사용하여 UCSM 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[UCSM 인증을 위한 FreeRADIUS 컨피그레이션](#)

[UCSM RADIUS 인증 컨피그레이션](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 RADIUS를 사용하여 UCSM 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

- FreeRADIUS가 작동 중입니다.
- UCS Manager, Fabric Interconnect 및 FreeRADIUS 서버는 서로 통신합니다.

대상 고객은 UCS 기능을 기본적으로 이해하고 있는 UCS 관리자입니다.

Cisco에서는 다음 항목에 대해 알고 있거나 숙지할 것을 권장합니다.

- Linux 구성 파일 버전
- UCS 관리자
- 자유반지름
- Ubuntu 또는 기타 Linux 버전

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- UCS Manager(UCSM) 4.3(3a) 이상
- Fabric Interconnect 6464
- 우분투 22.04.4 LTS.
- FreeRADIUS 버전 3.0.26

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

UCSM 인증을 위한 FreeRADIUS 컨피그레이션

이 단계에서는 freeRADIUS 서버에 대한 루트 액세스 권한이 필요합니다.

1단계. UCSM 도메인을 클라이언트로 구성합니다.

/etc/freeradius/3.0 디렉토리에 있는 clients.conf 파일로 이동하여 기본 설정의 텍스트 편집기를 사용하여 파일을 편집합니다. 이 예에서는 'vim' 편집기가 사용되고 'UCS-POD' 클라이언트가 생성되었습니다.

```
<#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 필드는 기본 Fabric Interconnect의 IP만 포함할 수 있습니다. 이 예에서는 IP 10.0.0.100/29 IP를 사용하여 두 FI의 VIP + mgmt0 IP를 포함했습니다.

Secret 필드는 UCSM RADIUS 컨피그레이션에 사용되는 비밀번호를 포함합니다(2단계).

2단계. UCSM에 인증할 수 있는 사용자 목록을 구성합니다.

동일한 디렉토리(/etc/freeradius/3.0)에서 users 파일을 열고 사용자를 생성합니다. 이 예에서는 비밀번호가 'password'인 사용자 'alerosa'가 UCSM 도메인에 관리자로 로그인하도록 정의되었습니다

```
<#root>
```

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

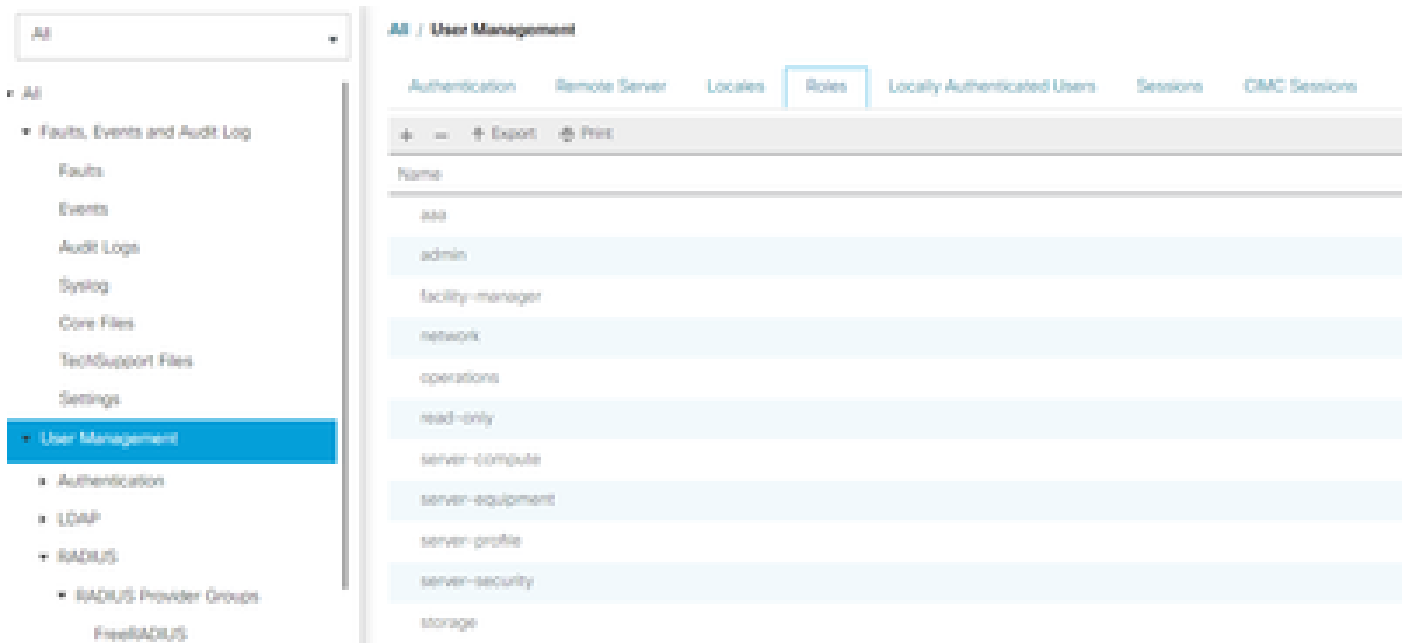
```
vim users
*Inside users file*
```

```
alerosa Cleartext-Password := "password"
Reply-Message := "Hello, %{User-Name}",
```

```
cisco-avpair = "shell:roles=admin"
```

cisco-avpair 특성은 필수입니다. 동일한 구문을 따라야 합니다.

Admin(관리) > User Management(사용자 관리) > Roles(역할)에서 UCSM에 구성된 모든 역할에 대해 관리자 역할을 변경할 수 있습니다. 이 특정 설정에서는 이러한 역할이 존재합니다



사용자에게 여러 역할이 필요한 경우 역할 사이에 쉼표를 사용할 수 있으며 구문은 `cisco-avpair = "shell:roles=aaa,facility-manager,read-only"`와 같은 형태로 표시되어야 합니다. UCSM에서 생성되지 않은 역할이 사용자에게 정의된 경우 UCSM의 인증이 실패합니다.

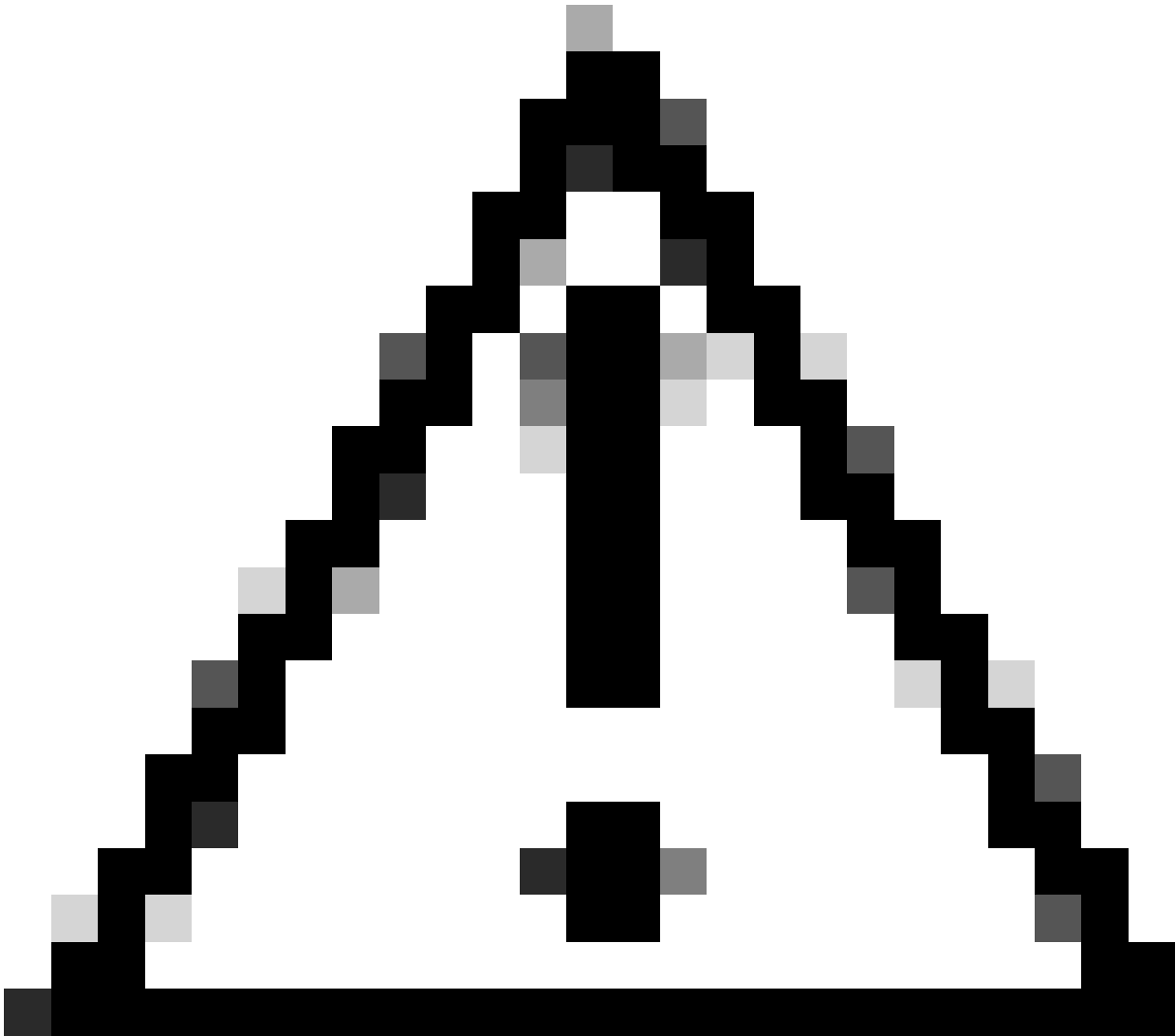
3단계. FreeRADIUS 데몬을 활성화/시작합니다.

시스템 부팅 시 FreeRADIUS에 대해 auto-start를 활성화합니다.

```
systemctl enable freeradius
```

FreeRADIUS 데몬을 시작합니다.

```
systemctl restart freeradius
```



주의: 'clients.conf' 또는 'users' 파일을 변경하면 FreeRADIUS 데몬을 다시 시작해야 합니다. 그렇지 않으면 변경 사항이 적용되지 않습니다

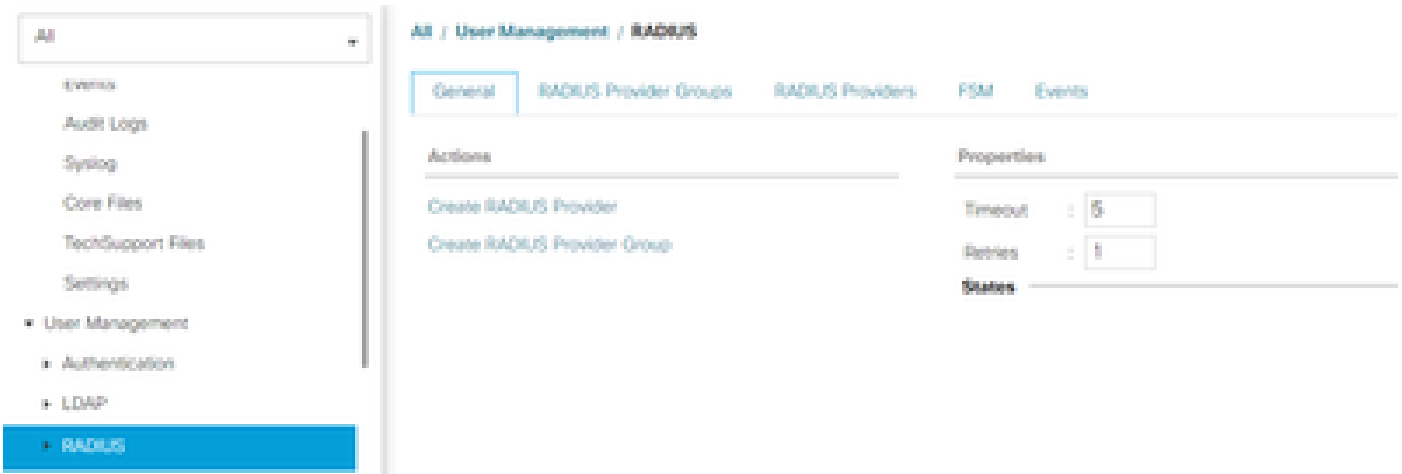
UCSM RADIUS 인증 컨피그레이션

UCS Manager 컨피그레이션은 이 문서의 지침을 따릅니다.

https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configuration.html

1단계. RADIUS 공급자에 대해 구성된 기본 속성입니다.

Admin(관리) > User Management(사용자 관리) > RADIUS로 이동하고 기본값을 사용합니다.



2단계. RADIUS 제공자를 생성합니다.

Admin(관리) > User Management(사용자 관리)에서 RADIUS를 선택하고 Create RADIUS Provider(RADIUS 제공자 생성)를 클릭합니다.

호스트 이름/FQDN(또는 IP 주소)은 서버/가상 머신의 IP 또는 FQDN입니다.

키는 'clients.conf' 파일의 RADIUS 서버에 정의된 키/암호입니다(FreeRADIUS 컨피그레이션의 1단계).

3단계. RADIUS 제공자 그룹을 생성합니다.

Admin(관리) > User Management(사용자 관리)에서 RADIUS를 선택하고 Create RADIUS Provider Group(RADIUS 제공자 그룹 생성)을 클릭합니다.

이름을 제공하십시오. 이 경우 'FreeRADIUS'가 사용되었습니다. 그런 다음 2단계에서 생성한 RADIUS 제공자를 포함된 제공자 목록에 추가합니다.

4단계. 새 인증 도메인을 생성합니다(선택 사항).

다음 단계는 필수가 아닙니다. 그러나 UCS Manager 초기 로그인 화면에서 볼 수 있는 로컬 사용자를 사용하는 인증 도메인과 다른 별도의 인증 도메인을 갖도록 수행되었습니다.

별도의 인증 도메인이 없으면 UCS Manager의 로그인 화면은 다음과 같습니다.



UCS Manager

Username

Password

Log In

[Reset Password](#)



For best results use a supported browser ▼

Copyright (c) 2009-2024 Cisco Systems, Inc. All rights reserved. The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at: <http://www.opensource.org/licenses/gpl-2.0.php> and <http://www.opensource.org/licenses/lgpl-2.1.php>

별도의 인증 도메인이 없는 UCS Manager 로그인 화면

별도의 인증 도메인을 사용하는 경우, UCS Manager의 로그인 화면에서 생성된 인증 도메인 목록을 추가합니다.



UCS Manager

Username

Password

Domain ▾

(Native)

RADIUS



For best results use a supported browser ▾

Copyright (c) 2009-2023 Cisco Systems, Inc. All rights reserved. The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at: <http://www.opensource.org/licenses/gpl-2.0.php> and <http://www.opensource.org/licenses/lgpl-2.1.php>

별도의 인증 도메인이 있는 UCS Manager 로그인 화면

이는 UCS 도메인에서 사용되는 다른 인증 유형과 RADIUS 인증을 분리하려는 경우에 유용합니다.

Admin(관리) > User Management(사용자 관리) > Authentication(인증) > Create a Domain(도메인 생성)으로 이동합니다.

새로 생성된 인증 도메인의 이름을 선택하고 RADIUS 라디오 버튼을 선택합니다. 제공 기관 그룹에서 이 섹션의 3단계.에서 생성한 제공 기관 그룹을 선택합니다.

다음을 확인합니다.

FreeRADIUS에는 아래에 설명된 것과 같은 몇 가지 디버깅 및 문제 해결 툴이 있습니다.

1. `journalctl -u freeradius` 명령은 구성의 오류 및 오류 또는 초기화 타임스탬프와 같은 freeRADIUS 데몬에 대한 몇 가지 중요한 정보를 제공합니다. 아래 예에서 사용자 파일이 잘못 수정된 것을 확인할 수 있습니다. (`mods-config/files/authorize`는 사용자 파일 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 디렉토리는 RADIUS 서버에 대해 기록된 모든 로그 목록을 포함하는 일부 로그 파일을 포함합니다. 이 예에서는 다음을 수행합니다.

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

3. `systemctl status freeradius` 명령은 freeRADIUS 서비스에 대한 정보를 제공합니다.

```
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 문제 해결/확인에 대한 자세한 내용은 https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf을 [참조하십시오](#).

UCSM의 경우 다음 명령을 사용하여 기본 FI에서 RADIUS 사용자를 사용한 성공 및 실패 로그인을 추적할 수 있습니다.

- nxos 연결
- 로깅 로그 파일 표시

로그인에 성공하려면 다음과 같아야 합니다.

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

로그인 실패 시 다음과 같이 표시됩니다.

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

여기서 X.X.X.X는 Fabric Interconnect에 대한 SSH에 사용되는 시스템의 IP입니다.

관련 정보

- [UCSM에서 인증 구성](#)
- [FreeRADIUS 서버 설정](#)
- [FreeRADIUS 위키](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.