

Cisco IOS 컨피그레이션에서 관리 액세스에 사용되는 FreeRADIUS 컨피그레이션 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[인증 및 권한 부여를 위한 스위치 구성](#)

[FreeRADIUS 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 서드파티 RADIUS 서버(FreeRADIUS)를 사용하는 Cisco IOS® 스위치에서 RADIUS 인증을 구성하는 방법에 대해 설명합니다. 이 예에서는 인증 시 권한 15 모드로 사용자를 직접 배치하는 것을 다룹니다.

사전 요구 사항

요구 사항

Cisco 스위치가 FreeRADIUS에 클라이언트로 정의되어 있고 IP 주소와 FreeRADIUS 및 스위치에 동일한 공유 비밀 키가 정의되어 있는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 자유반지름
- Cisco IOS 버전 12.2

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

구성

인증 및 권한 부여를 위한 스위치 구성

1. 예비(fallback) 액세스를 위한 전체 권한이 있는 스위치에서 로컬 사용자를 생성하려면 다음을 입력합니다.

```
Switch(config)#username admin privilege 15 password 0 cisco123!
```

2. AAA를 활성화하려면 다음을 입력합니다.

```
switch(config)# aaa new-model
```

3. RADIUS 서버의 IP 주소와 키를 제공하려면 다음을 입력합니다.

```
switch# configure terminal
switch(config)#radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
switch(config)#radius-server key hello123
```

참고: 키는 스위치에 대해 RADIUS 서버에 구성된 공유 암호와 일치해야 합니다.

4. RADIUS 서버 가용성을 테스트하려면 `test aaa` 명령을 입력합니다.

```
switch# test aaa server Radius 172.16.71.146 user1 Ur2Gd2BH
```

테스트 인증은 아직 구성되지 않았으므로 서버에서 거부됨으로 인해 실패하지만, 서버 자체에 연결할 수 있는지 확인합니다.

5. RADIUS에 연결할 수 없는 경우 로컬 사용자에게 다시 돌아가도록 로그인 인증을 구성하려면 다음을 입력합니다.

```
switch(config)#aaa authentication login default group radius local
```

6. 권한 레벨 15에 대한 권한 부여를 구성하려면 사용자가 인증되는 한 다음을 입력합니다.

```
switch(config)#aaa authorization exec default group radius if-authenticated
```

FreeRADIUS 구성

FreeRADIUS 서버에서 클라이언트 정의

1. 구성 디렉토리로 이동하려면 다음을 입력합니다.

```
# cd /etc/freeradius
```

2. `clients.conf` 파일을 편집하려면 다음을 입력합니다.

```
# sudo nano clients.conf
```

3. 호스트 이름으로 식별된 각 디바이스(라우터/스위치)를 추가하고 올바른 공유 암호를 포함하려면 다음을 입력합니다.

```
client 192.168.1.1 {
secret = secretkey
nastype = cisco
shortname = switch
}
```

4. 사용자 파일을 편집하려면 다음을 입력합니다.

```
# sudo nano users
```

5. 디바이스에 액세스할 수 있는 각 사용자를 추가합니다. 이 예에서는 "cisco" 사용자의 Cisco IOS 권한 레벨을 15로 설정하는 방법을 보여 줍니다.

```
cisco Cleartext-Password := "password"  
Service-Type = NAS-Prompt-User,  
Cisco-AVPair = "shell:priv-lvl=15"
```

6. FreeRADIUS를 다시 시작 하려면 다음을 입력 합니다.

```
# sudo /etc/init.d/freeradius restart
```

7. 사용자 파일에서 DEFAULT 사용자 그룹을 변경하여 cisco-rw의 멤버인 모든 사용자에게 권한 레벨 15를 부여하려면 다음을 입력합니다.

```
DEFAULT Group == cisco-rw, Auth-Type = System  
Service-Type = NAS-Prompt-User,  
cisco-avpair := "shell:priv-lvl=15"
```

8. FreeRADIUS 사용자 파일에서 필요에 따라 다른 권한 레벨의 다른 사용자를 추가할 수 있습니다. 예를 들어, 이 사용자(life)에게 레벨 3(시스템 유지보수)이 주어집니다.

```
sudo nano/etc/freeradius/users
```

```
life Cleartext-Password := "testing"  
Service-Type = NAS-Prompt-User,  
Cisco-AVPair = "shell:priv-lvl=3"
```

```
Restart the FreeRADIUS service:  
sudo /etc/init.d/freeradius restart
```

참고: 이 문서의 컨피그레이션은 Ubuntu 12.04 LTE 및 13.04에서 실행되는 FreeRADIUS를 기반으로 합니다.

다음을 확인합니다.

스위치의 컨피그레이션을 확인하려면 다음 명령을 사용합니다.

```
switch# show run | in radius (Show the radius configuration)  
switch# show run | in aaa (Show the running AAA configuration)  
switch# show startup-config Radius (Show the startup AAA configuration in  
start-up configuration)
```

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- [자유반지름](#)

- [기술 지원 및 문서 - Cisco Systems](#)

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.