

TACACS+ 및 RADIUS로 권한 수준을 할당하는 방법

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[예](#)

[컨피그레이션 - 라우터](#)

[구성 - 서버](#)

[관련 정보](#)

소개

이 문서에서는 특정 명령의 권한 레벨을 변경하는 방법에 대해 설명하고, 라우터 및 TACACS+ 및 RADIUS 서버의 샘플 컨피그레이션 일부에 대한 예를 제공합니다.

사전 요구 사항

요구 사항

이 문서의 독자는 라우터의 권한 수준에 대해 알고 있어야 합니다.

기본적으로 라우터에는 세 가지 권한 레벨이 있습니다.

- 권한 레벨 1 = 권한 없음(prompt is router>), 기본 로그인 레벨
- 권한 레벨 15 = 권한(프롬프트는 router#), 활성화 모드로 전환된 후 레벨
- 권한 레벨 0 = 거의 사용되지 않지만 다음 5개의 명령이 포함됩니다. disable, enable, exit, help 및 logout을 선택합니다.

레벨 2-14는 기본 컨피그레이션에서 사용되지 않지만, 일반적으로 레벨 15에 있는 명령은 해당 레벨 중 하나로, 일반적으로 레벨 1에 있는 명령은 해당 레벨 중 하나로 이동할 수 있습니다. 물론 이 보안 모델에는 라우터에 대한 일부 관리가 포함됩니다.

권한 수준을 로그인한 사용자로 확인하려면 show privilege 명령을 입력합니다. 사용 중인 Cisco IOS® 소프트웨어 버전에 대해 특정 권한 수준에서 사용할 수 있는 명령을 확인하려면 a를 입력합니다. 해당 권한 레벨에서 로그인할 때 명령줄에 표시됩니다.

참고: 인증 서버가 TACACS+를 지원하는 경우 권한 레벨을 할당하는 대신 명령 권한 부여를 수행할 수 있습니다. RADIUS 프로토콜은 명령 권한 부여를 지원하지 않습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS Software 릴리스 11.2 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업 중인 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

예

이 예에서 snmp-server 명령은 권한 레벨 15(기본값)에서 권한 레벨 7로 내려갑니다. ping 명령은 권한 레벨 1에서 권한 레벨 7로 올라갑니다. 사용자 7이 인증되면 서버에 의해 해당 사용자에게 권한 레벨 7이 할당되며 show privilege 명령은 "현재 권한 레벨이 7입니다"를 표시합니다. 사용자는 컨피그레이션 모드에서 ping을 수행하고 snmp-server 컨피그레이션을 수행할 수 있습니다. 다른 컨피그레이션 명령은 사용할 수 없습니다.

컨피그레이션 - 라우터

라우터 - 11.2

```
<#root>
```

```
aaa new-model
```

```
aaa authentication login default tacacs+|radius local
```

```
aaa authorization exec tacacs+|radius local
```

```
username backup privilege 7 password 0 backup
```

```
tacacs-server host 171.68.118.101
```

```
tacacs-server key cisco
```

```
radius-server host 171.68.118.101
```

```
radius-server key cisco
```

```
privilege configure level 7 snmp-server host
```

```
privilege configure level 7 snmp-server enable
```

```
privilege configure level 7 snmp-server
```

```
privilege exec level 7 ping
```

```
privilege exec level 7 configure terminal
```

```
privilege exec level 7 configure
```

라우터 - 11.3.3.T 이상(12.0.5.T까지)

<#root>

aaa new-model

aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local

username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure

라우터 - 12.0.5.T 이상

<#root>

aaa new-model

aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local

username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure

구성 - 서버

Cisco Secure NT TACACS+

서버를 구성하려면 다음 단계를 수행합니다.

1. 사용자 이름과 비밀번호를 입력합니다.
2. Group Settings(그룹 설정)에서 shell/exec이 선택되어 있는지, 그리고 7이 privilege level(권한 레벨) 상자에 입력되었는지 확인합니다.

TACACS+ - Freeware 서버의 Stanza

Stanza in TACACS+ freeware:

```
user = seven {  
login = cleartext seven  
service = exec {  
priv-lvl = 7  
}  
}
```

Cisco Secure UNIX TACACS+

```
user = seven {  
password = clear "seven"  
service = shell {  
set priv-lvl = 7  
}  
}
```

Cisco Secure NT RADIUS

서버를 구성하려면 다음 단계를 수행합니다.

1. 사용자 이름 및 비밀번호를 입력합니다.
2. IETF에 대한 Group Settings(그룹 설정)에서 Service-type(특성 6) = Nas-Prompt
3. CiscoRADIUS 영역에서 AV-Pair를 선택하고 아래의 사각형 상자에 shell:priv-lvl=7을 입력합니다.

Cisco Secure UNIX RADIUS

```
user = seven{  
radius=Cisco {  
check_items= {  
2="seven"  
}  
reply_attributes= {  
6=7  
9,1="shell:priv-lvl=7"  
}  
}  
}
```

사용자 이름 "seven"에 대한 사용자 파일입니다.

참고: 서버는 Cisco av 쌍을 지원해야 합니다.

- 7개의 비밀번호 = passwdxyz
- Service-Type = 셸 사용자
- cisco-avpair =shell:priv-lvl=7

관련 정보

- [RADIUS 지원 페이지](#)
- [RFC\(설명 요청\)](#)
- [IOS의 TACACS+ 문서](#)
- [TACACS+ 지원 페이지](#)
- [Cisco Secure UNIX 지원 페이지](#)
- [Windows용 Cisco Secure ACS 지원 페이지](#)
- [Technical Support - 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.