

Cisco IOS 라우터: HTTP 연결 컨피그레이션의 로컬, TACACS+ 및 RADIUS 인증 예

목차

[소개](#)

[시작하기 전에](#)

[표기 규칙](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[배경 이론](#)

[구성](#)

[HTTP 서버 사용자에게 대한 로컬 인증 구성](#)

[HTTP 서버 사용자를 위한 TACACS+ 인증 구성](#)

[HTTP 서버 사용자에게 대한 RADIUS 인증 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[트러블슈팅 명령](#)

[관련 정보](#)

소개

이 문서에서는 HTTP 연결의 로컬, TACACS+ 및 RADIUS 인증을 구성하는 방법을 보여줍니다. 일부 관련 디버깅 명령도 제공됩니다.

시작하기 전에

표기 규칙

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

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 아래의 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® Software 릴리스 11.2 이상
- 이러한 소프트웨어 개정을 지원하는 하드웨어

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.

배경 이론

Cisco IOS® Software Release 11.2에는 HTTP를 통해 라우터를 관리하는 기능이 추가되었습니다. Cisco IOS Configuration Fundamentals Command Reference의 "[Cisco IOS Web Browser Commands](#)" 섹션에는 이 기능에 대한 다음 정보가 포함되어 있습니다.

"ip http authentication 명령을 사용하면 HTTP 서버 사용자에게 대해 특정 인증 방법을 지정할 수 있습니다. HTTP 서버는 enable password 메소드를 사용하여 권한 레벨 15에서 사용자를 인증합니다. ip http authentication 명령을 사용하면 enable, local, TACACS 또는 AAA(authentication, authorization, and accounting) HTTP 서버 사용자 인증을 지정할 수 있습니다."

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

이 문서에서는 아래에 표시된 컨피그레이션을 사용합니다.

- [HTTP 서버 사용자에게 대한 로컬 인증 구성](#)
- [HTTP 서버 사용자를 위한 TACACS+ 인증 구성](#)
- [HTTP 서버 사용자에게 대한 RADIUS 인증 구성](#)

참고: 이 문서에 사용된 명령에 대한 추가 정보를 보려면 [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용하십시오.

HTTP 서버 사용자에게 대한 로컬 인증 구성

- [라우터 컨피그레이션](#)
- [사용자 결과](#)

라우터 컨피그레이션

Cisco IOS Software 릴리스 11.2를 사용한 로컬 인증

```
!---- This is the part of the configuration related to local authentication.
!
aaa new-model
aaa authentication login default local
aaa authorization exec local
username one privilege 15 password one
username three password three
```

```
username four privilege 7 password four
ip http server
ip http authentication aaa
!
```

!--- Example of command moved from level 15 (enable) to level 7

```
!
privilege exec level 7 clear line
```

Cisco IOS Software 릴리스 11.3.3.T 이상을 사용한 로컬 인증

!--- This is the part of the configuration !--- related to local authentication.

```
!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username one privilege 15 password one
username three password three
username four privilege 7 password four
ip http server
ip http authentication local
!
```

!--- Example of command moved from level 15 (enable) to level 7

```
!
privilege exec level 7 clear line
```

사용자 결과

이러한 결과는 이전 라우터 컨피그레이션의 사용자에게 적용됩니다.

- 사용자 1
 - URL이 http://#.#.#.#으로 입력된 경우 사용자가 웹 권한 부여를 전달합니다.
 - 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.
 - 사용자가 로그인 후 활성화 모드에 있습니다(표시 권한은 15입니다).
 - 라우터에 명령 권한 부여가 추가되어도 사용자는 모든 명령에서 계속 성공합니다.
- 사용자 3
 - 권한 수준이 없기 때문에 사용자가 웹 권한 부여에 실패합니다.
 - 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.

- 사용자가 로그인 후 비 활성화 모드에 있습니다(show 권한은 1임).
- 라우터에 명령 권한 부여가 추가되어도 사용자는 모든 명령에서 계속 성공합니다.
- 사용자 4
 - URL이 http://#.#.#.#/level/7/exec로 입력된 경우 사용자가 웹 권한 부여를 전달합니다.
 - 레벨 1 명령과 레벨 7 clear line 명령이 나타납니다.
 - 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.
 - 로그인 후 사용자는 권한 레벨 7에 있게 됩니다(show privilege는 7이 됨).
 - 라우터에 명령 권한 부여가 추가되어도 사용자는 모든 명령에서 계속 성공합니다.

HTTP 서버 사용자를 위한 TACACS+ 인증 구성

- [라우터 컨피그레이션](#)
- [사용자 결과](#)
- [Freeware 데몬 서버 컨피그레이션](#)
- [UNIX 서버 컨피그레이션용 Cisco Secure ACS](#)
- [Windows Server용 Cisco Secure ACS 컨피그레이션](#)

라우터 컨피그레이션

Cisco IOS Software 릴리스 11.2를 통한 인증

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco

!--- Example of command moved from level 15 (enable) to level 7

privilege exec level 7 clear line
```

Cisco IOS Software 릴리스 11.3.3.T에서 12.0.5.T로 인증

```
aaa new-model
aaa authentication login default tacacs+
```

```
aaa authorization exec default tacacs
ip http server
ip http authentication aaa tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
```

!--- Example of command moved from level 15 (enable) to level 7

```
privilege exec level 7 clear line
```

Cisco IOS Software 릴리스 12.0.5.T 이상을 사용한 인증

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
```

!--- Example of command moved from level 15 (enable) to level 7

```
privilege exec level 7 clear line
```

사용자 결과

다음 결과는 아래 서버 컨피그레이션의 사용자에게 적용됩니다.

- 사용자 1

- URL이 http://#.#.#.#으로 입력된 경우 사용자가 웹 권한 부여를 전달합니다.
- 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.
- 사용자가 로그인 후 활성화 모드에 있습니다(표시 권한은 15입니다).
- 라우터에 명령 권한 부여가 추가되어도 사용자는 모든 명령에서 계속 성공합니다.

- 사용자 2

- URL이 http://#.#.#.#으로 입력된 경우 사용자가 웹 권한 부여를 전달합니다.
- 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.
- 사용자가 로그인 후 활성화 모드에 있습니다(표시 권한은 15입니다).
- 라우터에 명령 권한 부여가 추가되면 서버 컨피그레이션에서 권한을 부여하지 않으므로 사용자가 모든 명령을 실패합니다.

- 사용자 3

- 권한 수준이 없기 때문에 사용자가 웹 권한 부여에 실패합니다.
- 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.
- 사용자가 로그인 후 비 활성화 모드에 있습니다(show 권한은 1임).
- 라우터에 명령 권한 부여가 추가되어도 사용자는 모든 명령에서 계속 성공합니다.

- 사용자 4

- URL이 http://#.#.#.#/level/7/exec로 입력된 경우 사용자가 웹 권한 부여를 전달합니다.
- 레벨 1 명령과 레벨 7 clear line 명령이 나타납니다.
- 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.
- 로그인 후 사용자는 권한 레벨 7에 있게 됩니다(show privilege는 7이 됨).
- 라우터에 명령 권한 부여가 추가되어도 사용자는 모든 명령에서 계속 성공합니다.

Freeware 데몬 서버 컨피그레이션

```
user = one {  
  default service = permit  
  login = cleartext "one"  
  service = exec {  
    priv-lvl = 15  
  }  
}
```

```
user = two {  
  login = cleartext "two"  
  service = exec {  
    priv-lvl = 15  
  }  
}
```

```
user = three {  
  default service = permit  
  login = cleartext "three"  
}
```

```
user = four {  
  default service = permit  
  login = cleartext "four"  
  service = exec {  
    priv-lvl = 7  
  }  
}
```

UNIX 서버 컨피그레이션용 Cisco Secure ACS

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "*****"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "*****"
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "*****"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "*****"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

Windows Server용 Cisco Secure ACS 컨피그레이션

그룹 1의 사용자 1

- 그룹 설정
 - 셸(exec)을 확인합니다.
 - 권한 레벨=15를 선택합니다.
 - Default (Undefined) Services(기본(정의되지 않음) 서비스)를 선택합니다.

참고: 이 옵션이 나타나지 않으면 Interface Configuration(인터페이스 컨피그레이션)으로 이동하여 TACACS+를 선택한 다음 Advanced Configuration Options(고급 컨피그레이션 옵션)를 선택합니다. Display enable default (undefined) service configuration(기본(정의되지 않은) 서비스 컨피그레이션 표시)을 선택합니다.

- 사용자 설정
 - 어느 데이터베이스로부터의 비밀번호; 위쪽 영역에 비밀번호를 입력하고 확인합니다.

그룹 2의 사용자 2

- 그룹 설정
 - 셸(exec)을 확인합니다.
 - 권한 레벨=15를 선택합니다.
 - Default (Undefined) Services(기본(정의되지 않은) 서비스)를 선택하지 마십시오.
- 사용자 설정
 - 어느 데이터베이스로부터의 비밀번호; 위쪽 영역에 비밀번호를 입력하고 확인합니다.

그룹 3의 사용자 3

- 그룹 설정
 - 셸(exec)을 확인합니다.
 - 권한 수준을 비워 둡니다.
 - Default (Undefined) Services(기본(정의되지 않음) 서비스)를 선택합니다.
- 참고: 이 옵션이 나타나지 않으면 Interface Configuration(인터페이스 컨피그레이션)으로 이동하여 TACACS+를 선택한 다음 Advanced Configuration Options(고급 컨피그레이션 옵션)를 선택합니다. Display enable default (undefined) service configuration(기본(정의되지 않은) 서비스 컨피그레이션 표시)을 선택합니다.

- 사용자 설정
 - 어느 데이터베이스로부터의 비밀번호; 위쪽 영역에 비밀번호를 입력하고 확인합니다.

그룹 4의 사용자 4

- 그룹 설정
 - 셸(exec)을 확인합니다.
 - 권한 레벨=7을 선택합니다.
 - Default (Undefined) Services(기본(정의되지 않음) 서비스)를 선택합니다.

참고: 이 옵션이 나타나지 않으면 Interface Configuration(인터페이스 컨피그레이션)으로 이동하여 TACACS+를 선택한 다음 Advanced Configuration Options(고급 컨피그레이션 옵션)를 선택합니다. Display enable default (undefined) service configuration(기본(정의되지 않은) 서비스 컨피그레이션 표시)을 선택합니다.

- 사용자 설정
 - 어느 데이터베이스로부터의 비밀번호; 위쪽 영역에 비밀번호를 입력하고 확인합니다.

HTTP 서버 사용자에게 대한 RADIUS 인증 구성

- [라우터 컨피그레이션](#)
- [사용자 결과](#)
- [Cisco AV 쌍을 지원하는 서버의 RADIUS 컨피그레이션](#)
- [UNIX 서버 컨피그레이션용 Cisco Secure ACS](#)
- [Windows Server용 Cisco Secure ACS 컨피그레이션](#)

라우터 컨피그레이션

Cisco IOS Software 릴리스 11.2를 통한 인증

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!

!--- Example of command moved from level 15 (enable) to level 7

!
privilege exec level 7 clear line
radius-server host 171.68.118.101
radius-server key cisco
```

Cisco IOS Software 릴리스 11.3.3.T에서 12.0.5.T로 인증

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Cisco IOS Software 릴리스 12.0.5.T 이상을 사용한 인증

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-port 1646
radius-server key cisco
privilege exec level 7 clear line
```

사용자 결과

다음 결과는 아래 서버 컨피그레이션의 사용자에게 적용됩니다.

- 사용자 1
 - URL이 http://#.#.#.#으로 입력된 경우 사용자가 웹 권한 부여를 전달합니다.
 - 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.
 - 사용자가 로그인 후 활성화 모드에 있습니다(표시 권한은 15입니다).
- 사용자 3
 - 권한 수준이 없기 때문에 사용자가 웹 권한 부여에 실패합니다.
 - 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.
 - 사용자가 로그인 후 비 활성화 모드에 있습니다(show 권한은 1임).
- 사용자 4
 - URL이 http://#.#.#.#/level/7/exec로 입력된 경우 사용자가 웹 권한 부여를 전달합니다.
 - 레벨 1 명령과 레벨 7 clear line 명령이 나타납니다.
 - 라우터에 텔넷한 후 사용자는 로그인 인증 후 모든 명령을 수행할 수 있습니다.
 - 로그인 후 사용자는 권한 레벨 7에 있게 됩니다(show privilege는 7이 됨).

Cisco AV 쌍을 지원하는 서버의 RADIUS 컨피그레이션

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"
```

```
three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

UNIX 서버 컨피그레이션용 Cisco Secure ACS

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

Windows Server용 Cisco Secure ACS 컨피그레이션

- 사용자 = 1, 서비스 유형(속성 6) = 관리자
- 사용자 = 3, 서비스 유형(속성 6) = 로그인
- User = 4, service type (attribute 6) = login(사용자 = 4, 서비스 유형(특성 6) = 로그인), Cisco AV-pairs 상자를 선택하고 shell:priv-lvl=7을 입력합니다.

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

트러블슈팅 명령

다음 명령은 HTTP 인증을 디버깅하는 데 유용합니다. 라우터에서 발급됩니다.

참고: debug 명령을 실행하기 전에 Debug 명령 [에 대한 중요 정보를 참조하십시오](#).

- terminal monitor - 현재 터미널과 세션에 대한 디버그 명령 출력 및 시스템 오류 메시지를 표시합니다.
- debug aaa authentication - AAA/TACACS+ 인증에 대한 정보를 표시합니다.
- debug aaa authorization - AAA/TACACS+ 권한 부여에 대한 정보를 표시합니다.
- debug radius - RADIUS와 관련된 자세한 디버깅 정보를 표시합니다.
- debug tacacs - TACACS와 관련된 정보를 표시합니다.
- debug ip http authentication - HTTP 인증 문제를 해결하려면 이 명령을 사용합니다. 라우터가 시도한 인증 방법 및 인증별 상태 메시지를 표시합니다.

관련 정보

- [Cisco TACACS+ 액세스 소프트웨어 지원 페이지](#)
- [RADIUS 지원 페이지](#)
- [Windows용 Cisco Secure ACS 지원 페이지](#)
- [UNIX용 Cisco Secure ACS 지원 페이지](#)
- [RFC\(설명 요청\)](#)
- [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.