Cisco Secure UNIX의 명령 권한 부여 및 권한 레벨

목차

소개

이 문서에서는 중앙 집중식 셸 및 명령 제어를 위해 AAA(authentication, authorization, and accounting)를 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.0(5)T 이상
- Cisco Secure for UNIX 2.3(6)

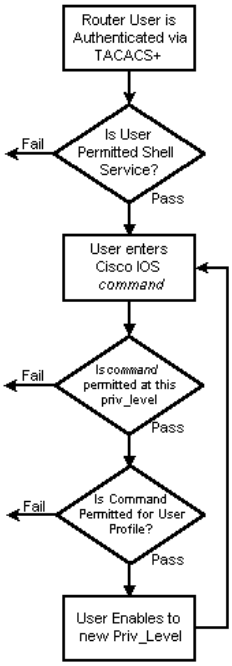
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

샘플 AAA 흐름

	Cisco IOS(AAA 클라이언트)	Cisco Secure(AAA 서버)
	`aaa authentication login default group tacacs+ local`	사용자=fred { password=des }
	`aaa authorization exec default group tacacs+ local`	service-shell { set priv level=x }
	`privilege exec level x` (아래 참고 참조).	
	`aaa authorization commands # default \ group tacacs none` `aaa authorization config-commands`	service=shell { default cmd=(허용/거부) prohibit cmd=x cmd=y{ }}
	`enable secretaaa authentication enable default \ group tacacs+ enable`	권한 = des "********" 15

권한 레벨

기본적으로 라우터에는 3가지 명령 레벨이 있습니다.

- privilege level 0 - disable, **enable**, **exit**, **help** 및 logout **명령을** 포함합니다.
- privilege level 1—`router>` 프롬프트에 모든 *사용자* 수준 명령 포함합니다.
- privilege level 15—`router>` 프롬프트에 모든 *enable*-level 명령 포함합니다.

다음 명령을 사용하여 권한 레벨 간에 명령을 이동할 수 있습니다.

`privilege exec level priv-lvl command`

콘솔 포트 인증

Cisco 버그 ID CSCdi82030을 구현할 때까지 콘솔 포트 권한 부여가 기능으로 추가되지 않았습니다(등록된 고객만 해당). 콘솔 포트 권한 부여는 라우터에서 잠길 가능성을 줄이기 위해 기본적으로 꺼져 있습니다.사용자가 콘솔을 통해 라우터에 물리적으로 액세스할 수 있는 경우 콘솔 포트 권한 부여는 매우 효과적이지 않습니다.그러나 Cisco 버그 ID CSCdi82030이 구현된 이미지의 경우 hidden 명령 aaa **authorization console**을 사용하여 행 con 0에서 콘솔 포트 권한 부여를 설정할 수 있습니다.

Cisco 보안 사용자 프로필

이 출력은 샘플 사용자 프로필을 보여줍니다.

```
# ./ViewProfile -p 9900 -u fred
User Profile Information
user = fred{
profile_id = 189
profile_cycle = 1
password = clear "********"
privilege = clear "********" 15
service=shell {
cmd=show {
permit "users"
}
}

}
```

라우터 컨피그레이션

```
Partial router configuration:

aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ none
aaa authorization exec default group tacacs+ none
aaa authorization commands 1 default group tacacs+ none
tacacs-server host 172.18.124.113
tacacs-server key cisco
```

샘플 출력

일부 출력은 공간 고려 사항으로 인해 두 줄로 래핑됩니다.

AAA 세션 - 사용자 캡처

```
telnet 10.32.1.64
Trying 10.32.1.64...
Connected to 10.32.1.64.
Escape character is '^]'.


User Access Verification

Username: fred
Password:
```

```
vpn-2503>show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:51
*  2 vty 0     fred       idle                 00:00:00 rtp-cherry.cisco.com

  Interface      User        Mode                    Idle     Peer Address

vpn-2503>enable
Password:
vpn-2503#
```

AAA 세션 - Cisco IOS 디버그

```
vpn-2503#show debug
General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
vpn-2503#terminal monitor
vpn-2503#
!--- In this capture, AAA authentication first tries the TACACS+ !--- server (and goes to local
authentication only if the server is down), !--- as configured in aaa authentication login
default group tacacs+ local.

*Mar 15 18:21:25: AAA: parse name=tty3 idb type=-1 tty=-1
*Mar 15 18:21:25: AAA: name=tty3 flags=0x11 type=5 shelf=0 slot=0 adapter=0
   port=3 channel=0
*Mar 15 18:21:25: AAA/MEMORY: create_user (0x524528) user='' ruser='' port='tty3'
   rem_addr='172.18.124.113' authen_type=ASCII service=LOGIN priv=1
*Mar 15 18:21:25: AAA/AUTHEN/START (4191717920): port='tty3' list=''
   action=LOGIN service=LOGIN
*Mar 15 18:21:25: AAA/AUTHEN/START (4191717920): using "default" list
*Mar 15 18:21:25: AAA/AUTHEN/START (4191717920): Method=tacacs+ (tacacs+)
 !--- Test TACACS+ for user authentication. *Mar 15 18:21:25: TAC+: send AUTHEN/START packet
ver=192 id=4191717920 *Mar 15 18:21:25: TAC+: Using default tacacs server-group "tacacs+" list.
*Mar 15 18:21:25: TAC+: Opening TCP/IP to 172.18.124.113/49 timeout=5 *Mar 15 18:21:25: TAC+:
Opened TCP/IP handle 0x5475C8 to 172.18.124.113/49 *Mar 15 18:21:25: TAC+: 172.18.124.113
(4191717920) AUTHEN/START/LOGIN/ASCII queued *Mar 15 18:21:25: TAC+: (4191717920)
AUTHEN/START/LOGIN/ASCII processed *Mar 15 18:21:25: TAC+: ver=192 id=4191717920 received AUTHEN
status = GETUSER *Mar 15 18:21:25: AAA/AUTHEN (4191717920): status = GETUSER *Mar 15 18:21:27:
AAA/AUTHEN/CONT (4191717920): continue_login (user='(undef)') *Mar 15 18:21:27: AAA/AUTHEN
(4191717920): status = GETUSER *Mar 15 18:21:27: AAA/AUTHEN (4191717920): Method=tacacs+
(tacacs+) *Mar 15 18:21:27: TAC+: send AUTHEN/CONT packet id=4191717920 *Mar 15 18:21:27: TAC+:
172.18.124.113 (4191717920) AUTHEN/CONT queued *Mar 15 18:21:27: TAC+: (4191717920) AUTHEN/CONT
processed *Mar 15 18:21:27: TAC+: ver=192 id=4191717920 received AUTHEN status = GETPASS *Mar 15
18:21:27: AAA/AUTHEN (4191717920): status = GETPASS *Mar 15 18:21:29: AAA/AUTHEN/CONT
(4191717920): continue_login (user='fred') *Mar 15 18:21:29: AAA/AUTHEN (4191717920): status =
GETPASS *Mar 15 18:21:29: AAA/AUTHEN (4191717920): Method=tacacs+ (tacacs+) *Mar 15 18:21:29:
TAC+: send AUTHEN/CONT packet id=4191717920 *Mar 15 18:21:29: TAC+: 172.18.124.113 (4191717920)
AUTHEN/CONT queued *Mar 15 18:21:29: TAC+: (4191717920) AUTHEN/CONT processed *Mar 15 18:21:29:
TAC+: ver=192 id=4191717920 received AUTHEN status = PASS *Mar 15 18:21:29: AAA/AUTHEN
(4191717920): status = PASS !--- TACACS+ passes user authentication. There is a check !--- to
see if shell access is permitted for this user, as configured in !--- aaa authorization exec
default group tacacs+ local.

*Mar 15 18:21:29: TAC+: Closing TCP/IP 0x5475C8 connection to 172.18.124.113/49
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): Port='tty3' list='' service=EXEC
*Mar 15 18:21:29: AAA/AUTHOR/EXEC: tty3 (3409614729) user='fred'
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): send AV service=shell
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): send AV cmd*
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): found list "default"
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): Method=tacacs+ (tacacs+)
```

```
*Mar 15 18:21:29: AAA/AUTHOR/TAC+: (3409614729): user=fred
*Mar 15 18:21:29: AAA/AUTHOR/TAC+: (3409614729): send AV service=shell
*Mar 15 18:21:29: AAA/AUTHOR/TAC+: (3409614729): send AV cmd*
*Mar 15 18:21:29: TAC+: using previously set server 172.18.124.113 from group tacacs+
*Mar 15 18:21:29: TAC+: Opening TCP/IP to 172.18.124.113/49 timeout=5
*Mar 15 18:21:29: TAC+: Opened TCP/IP handle 0x547A10 to 172.18.124.113/49
*Mar 15 18:21:29: TAC+: Opened 172.18.124.113 index=1
*Mar 15 18:21:29: TAC+: 172.18.124.113 (3409614729) AUTHOR/START queued
*Mar 15 18:21:29: TAC+: (3409614729) AUTHOR/START processed
*Mar 15 18:21:29: TAC+: (3409614729): received author response status = PASS_ADD
*Mar 15 18:21:29: TAC+: Closing TCP/IP 0x547A10 connection to 172.18.124.113/49
*Mar 15 18:21:29: AAA/AUTHOR (3409614729): Post authorization status = PASS_ADD
*Mar 15 18:21:29: AAA/AUTHOR/EXEC: Authorization successful
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): Port='tty3' list='' service=CMD
```

!--- TACACS+ passes exec authorization and wants to perform the !--- **show users** command, as configured in !--- **aaa authorization commands 1 default group tacacs+ none**.

```
*Mar 15 18:21:32: AAA/AUTHOR/CMD: tty3 (4185871454) user='fred'
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): send AV service=shell
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): send AV cmd=show
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): send AV cmd-arg=users
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): send AV cmd-arg=
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): found list "default"
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): Method=tacacs+ (tacacs+)
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): user=fred
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): send AV service=shell
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): send AV cmd=show
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): send AV cmd-arg=users
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): send AV cmd-arg=
*Mar 15 18:21:32: TAC+: using previously set server 172.18.124.113 from group tacacs+
*Mar 15 18:21:32: TAC+: Opening TCP/IP to 172.18.124.113/49 timeout=5
*Mar 15 18:21:32: TAC+: Opened TCP/IP handle 0x54F26C to 172.18.124.113/49
*Mar 15 18:21:32: TAC+: Opened 172.18.124.113 index=1
*Mar 15 18:21:32: TAC+: 172.18.124.113 (4185871454) AUTHOR/START queued
*Mar 15 18:21:33: TAC+: (4185871454) AUTHOR/START processed
*Mar 15 18:21:33: TAC+: (4185871454): received author response status = PASS_ADD
*Mar 15 18:21:33: TAC+: Closing TCP/IP 0x54F26C connection to 172.18.124.113/49
*Mar 15 18:21:33: AAA/AUTHOR (4185871454): Post authorization status = PASS_ADD
```

!--- TACACS+ passes command authorization and wants to !--- get into **enable** mode, as configured in !--- **aaa authentication enable default group tacacs+ enable**.

```
*Mar 15 18:21:34: AAA/MEMORY: dup_user (0x523E58) user='fred' ruser=''
   port='tty3' rem_addr='172.18.124.113' authen_type=ASCII service=ENABLE
   priv=15 source='AAA dup enable'
*Mar 15 18:21:34: AAA/AUTHEN/START (125091438): port='tty3' list=''
   action=LOGIN service=ENABLE
*Mar 15 18:21:34: AAA/AUTHEN/START (125091438): using "default" list
*Mar 15 18:21:34: AAA/AUTHEN/START (125091438): Method=tacacs+ (tacacs+)
*Mar 15 18:21:34: TAC+: send AUTHEN/START packet ver=192 id=125091438
*Mar 15 18:21:34: TAC+: Opening TCP/IP to 172.18.124.113/49 timeout=5
*Mar 15 18:21:34: TAC+: Opened TCP/IP handle 0x54D080 to 172.18.124.113/49
*Mar 15 18:21:34: TAC+: Opened 172.18.124.113 index=1
*Mar 15 18:21:34: TAC+: 172.18.124.113 (125091438) AUTHEN/START/LOGIN/ASCII queued
*Mar 15 18:21:34: TAC+: (125091438) AUTHEN/START/LOGIN/ASCII processed
*Mar 15 18:21:34: TAC+: ver=192 id=125091438 received AUTHEN status = GETPASS
*Mar 15 18:21:34: AAA/AUTHEN (125091438): status = GETPASS
*Mar 15 18:21:37: AAA/AUTHEN/CONT (125091438): continue_login (user='fred')
*Mar 15 18:21:37: AAA/AUTHEN (125091438): status = GETPASS
*Mar 15 18:21:37: AAA/AUTHEN (125091438): Method=tacacs+ (tacacs+)
*Mar 15 18:21:37: TAC+: send AUTHEN/CONT packet id=125091438
*Mar 15 18:21:37: TAC+: 172.18.124.113 (125091438) AUTHEN/CONT queued
*Mar 15 18:21:37: TAC+: (125091438) AUTHEN/CONT processed
*Mar 15 18:21:37: TAC+: ver=192 id=125091438 received AUTHEN status = PASS
*Mar 15 18:21:37: AAA/AUTHEN (125091438): status = PASS
```

```
*Mar 15 18:21:37: TAC+: Closing TCP/IP 0x54D080 connection to 172.18.124.113/49
*Mar 15 18:21:37: AAA/MEMORY: free_user (0x523E58) user='fred' ruser=''
   port='tty3' rem_addr='172.18.124.113' authen_type=ASCII service=ENABLE priv=15
 !--- TACACS+ passes enable authentication.
```

AAA 세션 - Cisco Secure UNIX 디버그

```
!--- In this capture, AAA authentication first tries the TACACS+ !--- server (and goes to local
authentication only if the server is down), !--- as configured in aaa authentication login
default group tacacs+ local.

Sep  7 07:22:32 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION
   START request (bace1fbf)
Sep  7 07:22:32 rtp-cherry CiscoSecure: DEBUG -
Sep  7 07:22:32 rtp-cherry User Access Verification
!--- Test TACACS+ for user authentication: Sep 7 07:22:32 rtp-cherry CiscoSecure: DEBUG -
Username: Sep 7 07:22:33 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION CONTINUE request
(bace1fbf) Sep 7 07:22:33 rtp-cherry CiscoSecure: DEBUG - Password: Sep 7 07:22:35 rtp-cherry
CiscoSecure: DEBUG - AUTHENTICATION CONTINUE request (bace1fbf) Sep 7 07:22:35 rtp-cherry
CiscoSecure: DEBUG - Authentication - LOGIN successful; [NAS=10.32.1.64, Port=tty2, User=fred,
Priv=1] !--- TACACS+ passes user authentication. There is a check !--- to see if shell access is
permitted for this user, as configured in !--- aaa authorization exec default group tacacs+
local.

Sep  7 07:22:35 rtp-cherry CiscoSecure: DEBUG -
Sep  7 07:22:36 rtp-cherry CiscoSecure: DEBUG - AUTHORIZATION request (9ad05c71)
Sep  7 07:22:36 rtp-cherry CiscoSecure: DEBUG - Authorization - Request authorized;
   [NAS = 10.32.1.64, user = fred, port = tty2, input: service=shell cmd* output: ]
!--- TACACS+ passes exec authorization and wants to perform the !--- show users command, as
configured in !--- aaa authorization commands 1 default group tacacs+ none.

Sep  7 07:22:38 rtp-cherry CiscoSecure: DEBUG - AUTHORIZATION request (563ba541)
Sep  7 07:22:38 rtp-cherry CiscoSecure: DEBUG - Authorization - Request authorized;
   [NAS = 10.32.1.64, user = fred, port = tty2, input: service=shell cmd=show
   cmd-arg=users cmd-arg= output: ]
!--- TACACS+ passes command authorization and wants to !--- get into enable mode, as configured
in !--- aaa authentication enable default group tacacs+ enable.

Sep  7 07:22:40 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION
   START request (f7e86ad4)
Sep  7 07:22:40 rtp-cherry CiscoSecure: DEBUG - Password:
Sep  7 07:22:41 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION
   CONTINUE request (f7e86ad4)
Sep  7 07:22:41 rtp-cherry CiscoSecure: DEBUG - Authentication - ENABLE successful;
   [NAS=10.32.1.64, Port=tty2, User=fred, Priv=15]
!--- TACACS+ passes enable authentication.
```

고급 Cisco 보안 프로파일 예

group LANadmins{
service=shell {
cmd=interface{
permit "Ethernet *"
deny "Serial *"
}
cmd=aaa{
deny ".*"
}
cmd=tacacs-server{
deny ".*"
}
	이 프로필은 "LANadmins" 그룹의 구성원인 모든 사용자가 라우터에 로그인하고 대부분의 명령을 입력할 수 있도록 합니다.사용자는 Serial 인터페이스 컨피그레이션을 변경하거나 AAA 컨피그레이션을 변경할 수 없으므로 명령 권한 부

default cmd=permit }	여를 제거하거나 TACACS 서버를 비활성화할 수 없습니다.

group Boston_Admins{
service=shell {
allow "10.28.17.1" ".*" ".*"
allow bostonswitch ".*" ".*"
allow "^bostonrtr[0-9]+" ".*"
".*"
set priv-lvl=15
default cmd=permit
}
service=shell {
allow "^NYrouter[0-9]+" ".*"
".*"
set priv-lvl=1
default cmd=deny
}
}
	이 프로필은 그룹 구성원**에게** 보스톤스위치, *보스톤tr1 - bostrtr9* 장치 및 10.28.17.1 장치에 대한 사용 권한을 제공합니다.이러한 디바이스에는 모든 명령이 허용됩니다.NYrouterX 디바이스에 대한 액세스는 사용자 EXEC 레벨로만 제한되며 권한 부여를 요청하는 경우 모든 명령이 거부됩니다.

group NY_wan_admins{
service=shell {
allow "^NYrouter[0-9]+" ".*"
".*"
set priv-lvl=15
default cmd=permit
}
service=shell {
allow "^NYcore$" ".*" ".*"
default cmd=permit
cmd=interface{
permit "Serial 0/[0-9]+"
permit "Serial 1/[0-9]+"
}
}
}
	이 그룹은 모든 NY 라우터에 대한 전체 액세스 권한을 가지며 Serial 0/x 및 Serial 1/x 인터페이스의 NY 코어 라우터에 대한 전체 액세스 권한을 가집니다.사용자는 코어 라우터에서 AAA를 비활성화할 수도 있습니다.

user bob{
password = des "********"
privilege = des "********" 15
member = NY_wan_admins
}
	이 사용자는 "NY_wan_admins" 그룹의 구성원이며 이러한 권한을 상속합니다.이 사용자는 로그인 비밀번호와 enable 비밀번호가 지정되어 있습니다.

group LAN_support {
service=shell {
default cmd = deny
cmd = set{
deny "port enable 3/10"
permit "port enable *"
deny "port disable 3/10"
permit "port disable *"
permit "port name *"
permit "port speed *"
permit "port duplex *"
permit "vlan [0-9]+ [0-
9]+/[0-9]+"
deny ".*"
	이 프로파일은 Catalyst 스위치용으로 설계되었습니다.사용자는 특정 **set** 명령만 허용됩니다.포트 3/10(트렁크 포트)을 비활성화할 수 없습니다. 사용자는 포트가 할당된 VLAN을 지정할 수 있지만 다른 모든 **set vlan** 명령은 거부됩니다.

```
    }
    cmd = show{
      permit ".*"
    }
    cmd = enable{
      permit ".*"
    }
  }
}
```

관련 정보

- Cisco Secure UNIX 제품 지원
- 기술 지원 및 문서 – Cisco Systems