Autorizzazione dei comandi e livelli di privilegi per Cisco Secure UNIX

Sommario

Introduzione

In questo documento viene illustrato come utilizzare l'autenticazione, l'autorizzazione e l'accounting (AAA) per il controllo centralizzato della shell e dei comandi.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS® versione 12.0(5)T e successive
- Cisco Secure per UNIX 2.3(6)

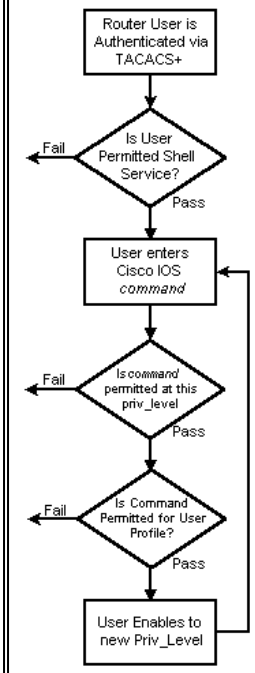
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Flusso AAA di esempio

	Cisco IOS (client AAA)	Cisco Secure (server AAA)
	`aaa authentication login default group tacacs+ local`	user=fred { password=des }
	`aaa authorization exec default group tacacs+ local`	service-shell { set priv-level=x }
	`privilege exec level x` (vedere le note di seguito).	
	`aaa authorization commands # default \ group tacacs none aaa authorization config-commands`	service=shell { default cmd=(consenti/nega) hibit cmd=x cmd=y{ }}
	`enable secretaaa authentication enable default \ group tacacs+ enable`	privilegio = des "********" 15

Livelli di privilegio

Per impostazione predefinita, sul router sono disponibili tre livelli di comando:

- livello di privilegio 0: include i comandi disable, **enable**, **exit**, **help** e **logout**
- privilegio livello 1: include tutti i comandi a livello *utente* al prompt `router`
- Privilege level 15 - Include tutti i comandi di *abilitazione* al prompt `router`

Èpossibile spostare i comandi tra i livelli di privilegio con questo comando:

```
privilege exec level priv-lvl command
```

Autenticazione porta console

L'autorizzazione della porta console non è stata aggiunta come funzionalità fino all'implementazione dell'ID bug Cisco CSCdi82030 (solo utenti registrati). Per impostazione predefinita, l'autorizzazione della porta console è disattivata per ridurre la probabilità di essere bloccata accidentalmente dal router. Se un utente ha accesso fisico al router tramite la console, l'autorizzazione della porta della console non è molto efficace. Tuttavia, per le immagini in cui è implementato l'ID bug Cisco CSCdi82030, è possibile attivare l'autorizzazione della porta della console alla riga con 0 con il comando nascosto **aaa authorization console**.

Cisco Secure User Profile

Questo output mostra un profilo utente di esempio.

```
# ./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"
}
}

}
```

Configurazione router

```
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
```

Output di esempio

Notare che per problemi di spazio alcuni output vengono riportati su due righe.

Sessione AAA - Acquisizione utente

```
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#
```

Sessione AAA - Debug Cisco IOS

```
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.
```

Sessione AAA - Debug Cisco Secure UNIX

```
!--- 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.
```

Esempi avanzati di profili sicuri Cisco

`group LANadmins{`
` service=shell {`
` cmd=interface{`
`  permit "Ethernet *"`
`  deny "Serial *"`
` }`
` cmd=aaa{`
	Questo profilo consente a qualsiasi utente membro del gruppo "LANadmins" di accedere a un router e immettere la maggior parte dei comandi. Gli

deny ".*"
}
cmd=tacacs-server{
deny ".*"
}
default cmd=permit
}
	utenti non sono autorizzati a modificare la configurazione dell'interfaccia seriale o la configurazione del server AAA (quindi non possono rimuovere l'autorizzazione del comando o disabilitare il server TACACS).

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
}
}
	Questo profilo fornisce ai membri del gruppo i privilegi di **abilitazione** sul dispositivo bostonswitch, sui dispositivi *bostonrtr1 - bostonrtr9* e sul dispositivo 10.28.17.1. Per questi dispositivi sono consentiti tutti i comandi. L'accesso ai dispositivi *NYrouterX* è limitato solo al livello di esecuzione utente e tutti i comandi sono negati se viene richiesta l'autorizzazione.

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]+"
}
}
}
	Questo gruppo dispone di accesso completo a tutti i router NY, nonché di accesso completo al router principale NY sulle interfacce Serial 0/x e Serial 1/x. Notare che gli utenti possono disabilitare il server AAA anche sul router principale.

user bob{
password = des "********"
privilege = des "********"
15
member = NY_wan_admins
}
	Questo utente è membro del gruppo "NY_wan_admins" ed eredita tali privilegi. L'utente dispone inoltre di una password di accesso e di una password di abilitazione specificate.

group LAN_support {
service=shell {
default cmd = deny
cmd = set{
deny "port enable 3/10"
	Questo profilo è progettato per uno switch Catalyst. Agli utenti sono consentiti solo alcuni comandi **set**. Non è

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 ".*"
}
cmd = show{
permit ".*"
}
cmd = enable{
permit ".*"
}
}
}
	consentito disabilitare la porta 3/10 (una porta trunk). Gli utenti possono specificare la VLAN a cui è assegnata una porta, ma tutti gli altri comandi **set vlan** sono rifiutati.

Informazioni correlate

- Cisco Secure UNIX - Supporto dei prodotti
- Documentazione e supporto tecnico – Cisco Systems