El comando authorization y los niveles de privilegio para Cisco aseguran UNIX

Contenido

Introducción

Este documento aporta información sobre cómo utilizar la autenticación, la autorización y la contabilización (AAA) para el shell y el control de comandos centralizados.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Release 12.0(5)T y Posterior de Cisco IOS®
- Cisco seguro para UNIX 2.3(6)

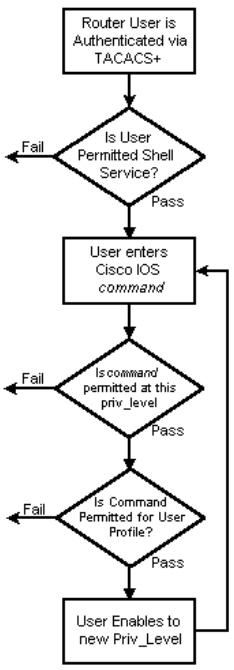
La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Muestree el flujo AAA

	Cisco IOS (cliente AAA)	Cisco seguro (servidor de AAA)
	`aaa authentication login default group tacacs+ local`	user=fred {password=des}
	`aaa authorization exec default group tacacs+ local`	servicio-shell {set priv-level=x}
	`comando x del nivel del ejecutivo del privilegio` (véase las notas abajo.)	
	`aaa authorization commands # default \ group tacacs none aaa authorization config-commands`	service=shell {el cmd= predeterminado (el permiso/niega) prohíbe el cmd=x cmd=y {}}
	`enable secretaaa authentication enable default \ group tacacs+ enable`	privilegio = DES “********” 15

Niveles de privilegio

Por abandono, hay tres niveles del comando en el router:

- nivel de privilegio 0 — Incluye la **neutralización**, **permiso**, los **comandos exit, help, y logout**
- nivel de privilegio 1 — Incluye todos los comandos del *nivel de usuario* en el prompt del `router>`
- nivel de privilegio 15 — Incluye todos los comandos del permiso-*nivel* en el prompt del `router>`

Usted puede mover los comandos alrededor entre los niveles de privilegio con este comando:

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

Autenticación del puerto de consola

La autorización de puerto de la consola no fue agregada como característica hasta la implementación del Id. de bug Cisco CSCdi82030 (clientes registrados solamente). La autorización de puerto de la consola es apagado por abandono para aminorar la probabilidad accidentalmente de ser router bloqueado de los. Si un usuario tiene acceso físico al router vía la consola, la autorización de puerto de la consola no es extremadamente eficaz. Sin embargo, para las imágenes en las cuales se implementa el Id. de bug Cisco CSCdi82030, usted puede girar la autorización de puerto de la consola bajo línea con 0 con la **consola de la autorización aaa del** comando oculto.

Perfil del usuario de Secure de Cisco

Esta salida muestra un perfil del usuario de la muestra.

```
# ./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"
}
}

}
```

Configuración del 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
```

Ejemplo de Salida

Observe que una cierta salida está envuelta sobre dos líneas debido a las consideraciones espaciales.

Sesión AAA - Captura de usuario

```
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#
```

Sesión AAA - Debug del 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.
```

Sesión AAA - Debug seguro de Cisco 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.
```

Ejemplos de perfil seguro avanzados de Cisco

`group LANadmins{`
`  service=shell {`
`  cmd=interface{`
`  permit "Ethernet *"`
`  deny "Serial *"`
`  }`
`  cmd=aaa{`
`  deny ".*"`
`  }`
`  cmd=tacacs-server{`
`  deny ".*"`
`  }`
`  default cmd=permit`
`}`
	Este perfil permite a cualquier usuario que sea un miembro del grupo “LANadmins” a registrar en un router y para ingresar la mayoría de los comandos. No se permite a los usuarios realizar los cambios a la configuración de la interfaz serial, o realizar los cambios a los config AAA (así que a los ellos no puede quitar el comando authorization o inhabilitar al servidor 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`
`  }`
`}`
	Este perfil da a su grupo los miembros los privilegios del **permiso** en el bostonswitch, el *bostonrtr1 - los* dispositivos *bostonrtr9*, y el dispositivo de 10.28.17.1. Permiten a los comandos all para estos dispositivos. El acceso a los dispositivos de *NYrouterX* se restringe al nivel del ejecutivo del usuario solamente, y niegan los comandos all si están pedidos la autorización.

`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]+"`
`  }`
`  }`
`}`
	Este grupo tiene el acceso total a todo el Routers NY, así como acceso total al router del núcleo NY en el 0/x serial y las interfaces seriales 1/x. Observe que los usuarios también tienen la capacidad de inhabilitar el AAA en el router del núcleo.

	Este usuario es un

`user bob{`
` password = des "********"`
` privilege = des "********" 15`
` member = NY_wan_admins`
`}`
	miembro del grupo de “NY_wan_admins” y hereda esos privilegios. Este usuario también hace una contraseña de inicio de sesión así como una contraseña habilitada especificar.

`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 ".*"`
`  }`
`  cmd = show{`
`  permit ".*"`
`  }`
`  cmd = enable{`
`  permit ".*"`
`  }`
` }`
`}`
	Este perfil se diseña para un switch de Catalyst. No prohiben los usuarios solamente ciertos **comandos set**. A les no se permite inhabilitar el puerto 3/10 (un puerto troncal). Se permite a los usuarios especificar el VLA N que un puerto se asigna a, pero niegan el resto de los **comandos set vlan**.

Información Relacionada

- Soporte de productos seguro de Cisco UNIX
- Soporte Técnico y Documentación - Cisco Systems