Cisco Secure UNIX的命令授權和許可權級別

目錄

簡介

本文提供有關如何使用身份驗證、授權和記帳(AAA)進行集中外殼和命令控制的資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

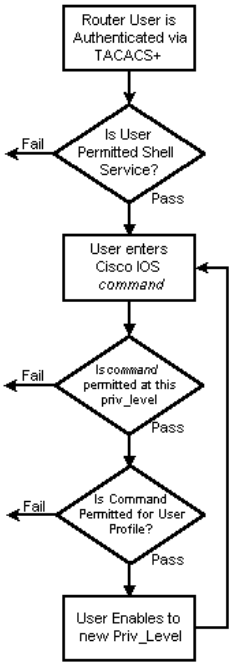
- Cisco IOS®軟體版本12.0(5)T及更新版本
- Cisco Secure for UNIX 2.3(6)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

AAA流示例

	Cisco IOS（AAA使用者端）	Cisco Secure（AAA伺服器）
	`aaa authentication login default group tacacs+ local`	user=fred { password=des }
	`aaa authorization exec default group tacacs+ local`	service-shell { set priv-level=x }
	`execx`（請參閱下面的說明。）	
	`aaa authorization commands # default \ group tacacs none` `aaa authorization config-commands`	service=shell { default cmd=(permit/deny)prohibit cmd=x cmd=y{ }}
	`enable secretaaa authentication enable default \ group tacacs+ enable`	privilege = des "********" 15

許可權級別

預設情況下，路由器上有三個命令層級：

- privilege level 0 — 包括disable、**enable**、exit、help和**logout**命令
- privilege level 1 — 在`router>`*提示*符下包含所有用令
- privilege level 15 — 在`router>`*提*示符中包括所有`enable-level`令

您可以使用以下命令在許可權級別之間移動命令：

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

控制檯埠身份驗證

實施思科錯誤ID CSCdi82030(僅限註冊客戶)之前，未將控制檯埠授權新增為功能。 預設情況下，控制檯埠授權關閉，以便減少意外鎖定到路由器之外的可能性。如果使用者可以通過控制檯對路由器進行物理訪問，則控制檯埠授權不會非常有效。但是對於已實作Cisco錯誤ID CSCdi82030的映像，可以使用**aaa authorization console** 隱藏命令在line con 0下啟用控制檯埠授權。

思科安全使用者設定檔

此輸出顯示了示例使用者配置檔案。

```
# ./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"
}
}

}
```

路由器配置

```
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
```

輸出示例

請注意，由於空間方面的考慮，某些輸出會換成兩行。

AAA作業階段 — 使用者擷取

```
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作業階段 — Cisco IOS偵錯

```
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作業階段 — Cisco Secure UNIX偵錯

```
!--- 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.

高級思科安全配置檔案示例

group LANadmins{
 	
service=shell {
 	
cmd=interface{
 	
permit "Ethernet *"
	此配置檔案允許屬於組「LAN管理員」的任何使用者登入到路由器並輸入大多數命令。不允許使用者更改串列介面配置或更改AAA配置（因此他們不能刪除命令授權或禁用TACACS伺服器）。

deny "Serial *" }
 	
cmd=aaa{
 	
deny ".*" }
 	
cmd=tacacs-server{
 	
deny ".*" }
 	
default cmd=permit }	

group Boston_Admins{
 	
service=shell {
 	
allow "10.28.17.1" ".*" ".*"
 	
allow bostonswitch ".*" ".*"
 	
allow "^boston
	此配置檔案為其組成員提供bostonswitch、*bostonrtr1 - bostonrtr9*裝置和10.28.17.1裝置上的**enable**許可權。這些裝置允許所有命令。對*NYrouterX*裝置的訪問僅限於使用者exec級別，如果請求授權，所有命令都會被拒絕。

rtr[0-9]+" ".*" ".*"
 	
set priv-lvl=15
 	
default cmd=permit
}
 	
service=shell {
 	
allow "^NYrouter[0-9]+" ".*" ".*"
 	
set priv-lvl=1
 	
default cmd=deny
}
}	

group NY_wan_admins{
 	
service=shell {
 	
allow "^NYrout
	該組擁有對所有NY路由器的完全訪問許可權，以及對Serial 0/x和Serial 1/x介面上的NY核心路由器的完全訪問許可權。請注意，使用者還可以在核心路由器上禁用AAA。

er[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]+"
}
}
}	

user	此使用者是「NY_wan_admins」組的成員，並繼承這些許可權。此使用者還指定了登入密碼和啟用密碼

bob{
 	
password =
des
"********"
 	
privilege =
des
"********"
15
 	
member =
NY_wan_admins
}
	。

group
LAN_support
{
 	
service=
shell {
 	
default
cmd =
deny
 	
cmd =
set{
 	
deny
"port
enable
3/10
"
 	
permit
"port
enable
	此設定檔專為Catalyst交換器設計。使用者只能使用某些**set**命令。不允許它們停用連線埠3/10（主干連線埠）。 允許使用者指定埠所分配的VLAN，但拒絕所有其他**set vlan**命令。

```
*"

deny
"por
t
disa
ble
3/10
"

perm
it
"por
t
disa
ble
*"

perm
it
"por
t
name
*"

perm
it
"por
t
spee
d *"

perm
it
"por
t
dupl
ex
*"

perm
it
"vla
n
[0-
9]+
[0-
9]+/
[0-
9]+"

deny
".*"
   }

cmd
=
show
{

perm
it
".*"
   }
```

```
cmd
=
enab
le{

perm
it
".*"
   }
 }
}
```

相關資訊

- Cisco Secure UNIX產品支援
- 技術支援與文件 - Cisco Systems