Cisco Secure UNIX的命令授权和权限级别

目录

简介
先决条件
要求
使用的组件
规则
示例AAA流
权限级别
控制台端口认证
Cisco安全用户配置文件
路由器配置
示例输出
AAA会话-用户访问
AAA会话- Cisco IOS调试
AAA会话- Cisco Secure UNIX调试
先进的Cisco Secure配置文件示例
相关信息

简介

本文提供关于如何的信息使用验证、授权和统计(AAA)集中化shell和命令控制。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

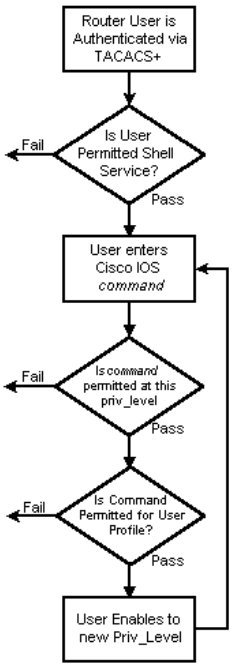
- Cisco IOS软件版本12.0(5)T和以后
- UNIX的Cisco Secure 2.3(6)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

示例AAA流

	Cisco IOS (AAA客户端)	Cisco Secure (AAA服务器)
	`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`(请参阅下面的笔记。)	
	`aaa authorization commands # default \ group tacacs none aaa authorization config-commands`	service=shell {默认cmd= (permit/拒绝)禁止cmd=x cmd=y {}}
	`enable secretaaa authentication enable default \ group tacacs+ enable`	权限= des “********” 15

权限级别

默认情况下，路由器上有三个命令级别：

- 权限级别0 —包括**禁用**、**enable (event)**、**退出**、**帮助**和**注销**命令
- 权限级别1 —包括所有*用户级*at命令`router>`提示符
- 权限级别15 —包括所有*启用级*at命令`router>`提示符

您能移动命令在权限级别之间用此命令：

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

控制台端口认证

控制台端口授权未被添加作为直到Cisco Bug ID CSCdi82030 (仅限注册用户)的实施的一个功能。默认情况下控制台端口授权关闭为了偶然减轻可能性锁定在路由器外面。如果用户访问物理访问路由器通过控制台，控制台端口授权不是十分有效的。然而，为Cisco Bug ID CSCdi82030实现的镜像，您能打开控制台端口授权在line con 0下用隐藏命令**AAA授权控制台**。

Cisco安全用户配置文件

此输出显示用户配置文件。

```
# ./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
```

示例输出

注意若干输出包裹在两条线路上由于空间的考虑事项。

AAA会话-用户访问

```
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会话- Cisco IOS调试

```
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会话- Cisco Secure UNIX调试

!--- 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.*

先进的Cisco Secure配置文件示例

group LANadmins{
 	
service=shell {
 	
cmd=interface{
 	
per
	此配置文件允许是组“”成员登录路由器和输入多数命令的LANadmins的所有用户。用户没有允许做对串行接口配置的变动，或者做对AAA的更改配置(因此他们不能取消authorization命令或禁用TACACS服务器)。

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

group Boston_Admins{
 	
service=shell {
 	
allow "10
	此配置文件给其组成员在bostonswitch、*bostonrtr1 - bostonrtr9*设备和10.28.17.1设备的**enable (event)**权限。所有命令为这些设备允许。对*NYrouterX*设备的访问只限制对级用户的exec，并且所有命令拒绝，如果询问为授权。

```
.28
.17
.1"
".*
"
".*
"

allow boston switch ".*
"
".*
"

allow "^bostonrtr[0-9]+
"
".*
"
".*
"

set priv-lvl=15

default cmd=permit
 }

service=shell {

allow "^NYrouter[0-9]+
"
".*
```

" ".* " set priv- lvl =1 def aul t cmd =de ny } }	

gro
up
NY_
wan
_ad
min
s{
 	
ser
vic
e=s
hel
l {
 	
all
ow
"^N
Yro
ute
r[0
-
9]+
"
".*
"
".*
"
 	
set
pri
v-
lvl
=15
 	
def
aul
t
cmd
=pe
rmi
t
}
 	
ser
vic
	此组有对所有NY路由器的对NY核心路由器的完全权限，以及完全权限序列0/x &序列1/x接口的。注意用户也有能力禁用在核心路由器的AAA。

e=shell {
 	
allow "^NYcore$" ".*" ".*"
 	
default cmd=permit
 	
cmd=interface{
 	
permit "Serial 0/[0-9]+"
 	
permit "Serial 1/[0-9]+"
  }
 }
}	

user bob { password= des "****** 	此用户是“NY_wan_admins”组的成员并且继承那些权限。此用户也安排一个登录密码以及一特权密码指定。

*** " pri vil ege = des "** *** *** " 15 mem ber = NY_ wan _ad min s }	

gro
up
LAN
_su
ppo
rt
{
 	
ser
vic
e=s
hel
l {
 	
def
aul
t
cmd
=
den
y
 	
cmd
=
set
{
 	
den
y
"po
rt
ena
ble
3/1
0"
 	
per
mit
"po
rt
	此配置文件为Catalyst交换机设计。用户允许仅某些**集合**命令。他们没有允许使端口3/10 (中继端口)无效。用户允许指定VLAN端口分配对，但是其他**set vlan**命令拒绝。

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
=
sho
w{

per
mit
".*
"

}

cmd
=
ena
ble
{

per
mit
".*
"

}
 }
}
```

相关信息

- Cisco Secure UNIX产品支持
- 技术支持和文档 - Cisco Systems