

# O comando authorization e os níveis de privilégio para Cisco fixam UNIX

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Fluxo da amostra AAA](#)

[Níveis de privilégio](#)

[Autenticação da Porta do Console](#)

[Perfil de usuário seguro de Cisco](#)

[Configuração do roteador](#)

[Saída de exemplo](#)

[Sessão de AAA - Captura de usuário](#)

[Sessão de AAA - O Cisco IOS debuga](#)

[Sessão de AAA - Cisco UNIX seguro debuga](#)

[Exemplos de perfil seguro avançados de Cisco](#)

[Informações Relacionadas](#)

## Introdução

Este documento dá a informação em como usar o Authentication, Authorization, and Accounting (AAA) para o shell e o controle de comando centralizados.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Release 12.0(5)T e Mais Recente de Cisco IOS®
- Cisco seguro para UNIX 2.3(6)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## [Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## [Prove o fluxo AAA](#)

Cisco IOS (cliente de AAA)	Cisco seguro (servidor AAA)
<pre>aaa authentication login default   group tacacs+ local</pre>	<pre>user=fred {password=des}</pre>
<pre>aaa authorization exec default   group tacacs+ local</pre>	<pre>serviço-shell {set priv- level=x}</pre>
comando x do nível do executivo do privilégio (veja as notas abaixo.)	
<pre>aaa authorization commands # default \   group tacacs none aaa authorization config- commands</pre>	<pre>service=shell {o cmd= do padrão (a licença/nega) proibe o cmd=x cmd=y {}}</pre>
<pre>enable secretaaa authentication enable default \   group tacacs+ enable</pre>	<pre>privilégio = DES "*****" 15</pre>

## [Níveis de privilégio](#)

À revelia, há três níveis de comando no roteador:

- nível de privilégio 0 — Inclui o **desabilitação, permitem-no, comandos exit, help, e logout**
- nível de privilégio 1 — Inclui todos os comandos do *nível de usuário na* alerta do `Roteador>`
- nível de privilégio 15 — Inclui todos os comandos do *permitir-nível na* alerta do `Roteador>`

Você pode mover comandos ao redor entre níveis de privilégio com este comando:

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

## [Autenticação da Porta do Console](#)

A autorização da porta de Console não foi adicionada como uma característica até a aplicação da identificação de bug Cisco [CSCdi82030](#) ([clientes registrados somente](#)). A autorização da porta de Console está fora à revelia a fim diminuir acidentalmente a probabilidade do travamento fora do roteador. Se um usuário tem o acesso físico ao roteador através do console, a autorização da porta de Console não é extremamente eficaz. Contudo, para as imagens em que a identificação de bug Cisco [CSCdi82030](#) é executada, você pode girar sobre a autorização da porta de Console sob a linha engodo 0 com o **console da autorização aaa do** comando oculto.

## Perfil de usuário seguro de Cisco

Esta saída mostra um perfil de usuário da amostra.

```
# ./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"
}
}
}
```

## Configuração do roteador

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
```

## Saída de exemplo

Note que alguma saída está envolvida em duas linhas devido às considerações espaciais.

## Sessão de AAA - Captura de usuário

```
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#
```

## Sessão de AAA - O Cisco IOS debuga

```
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.

```

## Sessão de AAA - Cisco UNIX seguro debuga

```

!--- 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 (bacelfbf) 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 (bacelfbf) Sep 7 07:22:33 rtp-cherry CiscoSecure: DEBUG - Password: Sep 7
07:22:35 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION CONTINUE request (bacelfbf) 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.

```

## Exemplos de perfil seguro avançados 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 todo o usuário que for um membro do grupo "LANadmins" a registrar em um roteador e para incorporar a maioria de comandos. Não são permitidos aos usuários fazer mudanças à configuração de interface serial, ou fazê-las

<pre> }</pre>	<p>mudanças à configuração AAA (assim que não pode remover o comando <code>authorization</code> ou desabilitar o servidor de TACACS).</p>
<pre> 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   } }</pre>	<p>Este perfil dá seu grupo que os membros <b>permitem</b> privilégios no <code>bostonswitch</code>, o <code>bostonrtr1</code> - os dispositivos <code>bostonrtr9</code>, e o dispositivo de 10.28.17.1. Os comandos <code>all</code> são permitidos para estes dispositivos. O acesso aos dispositivos de <code>NYrouterX</code> é restringido ao nível do executivo do usuário somente, e os comandos <code>all</code> são negados se pedido a autorização.</p>
<pre> 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]+"     }   } }</pre>	<p>Este grupo tem o acesso direto a todo o Roteadores NY, assim como o acesso direto ao roteador central NY no 0/x de série &amp; nas relações 1/x de série. Note que os usuários igualmente têm a capacidade para desabilitar o AAA no roteador central.</p>
<pre> user bob{   password = des "*****"   privilege = des "*****"   15   member = NY_wan_admins }</pre>	<p>Este usuário é um membro do grupo de "NY_wan_admins" e herda aqueles privilégios. Este usuário igualmente tem uma senha de login assim como uma senha da possibilidade especificadas.</p>
<pre> 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 *"     }   } }</pre>	<p>Este perfil é projetado para um Catalyst Switch. Determinados <b>comandos set</b> são permitidos aos usuários somente. Não são permitidos desabilitar a porta 3/10 (uma porta de tronco). São permitidos</p>

```
permit "port speed *"
permit "port duplex *"
permit "vlan [0-9]+ [0-
9]+/[0-9]+"
```

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

aos usuários especificar o VLAN que uma porta é atribuída a, mas todos **comandos set vlan** restantes são negados.

## [Informações Relacionadas](#)

- [Sustentação do produto segura de Cisco UNIX](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)