Befehlsautorisierung und Berechtigungsstufen für Cisco Secure UNIX

Inhalt

Einführung

Dieses Dokument enthält Informationen zur Verwendung von AAA (Authentication, Authorization, Accounting) für die zentralisierte Shell und Befehlssteuerung.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® Software-Versionen 12.0(5)T und höher
- Cisco Secure für UNIX 2.3(6)

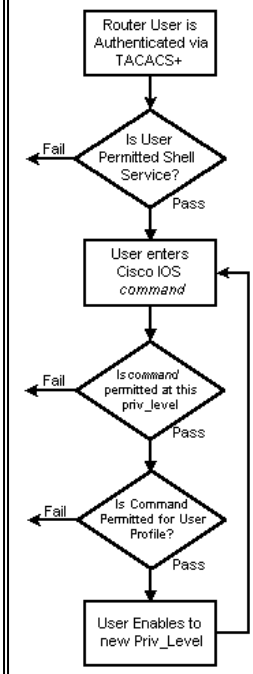
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Beispiel für AAA-Fluss

	Cisco IOS (AAA-Client)	Cisco Secure (AAA-Server)
	`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 command` (siehe Hinweise unten).	
	`aaa authorization commands # default \ group tacacs none aaa authorization config-commands`	service=shell { default cmd=(permit/deny) noch cmd=x cmd=y{ }}
	`enable secretaaa authentication enable default \ group tacacs+ enable`	privilege = des "*******" 15

Berechtigungsstufen

Standardmäßig gibt es drei Befehlsstufen auf dem Router:

- Berechtigungsstufe 0 - Enthält die **Befehle disable**, **enable**, **exit**, **help** und **logout.**
- Berechtigungsstufe 1 - Beinhaltet alle Befehle auf *Benutzerebene* an der `Router->`Eingabeaufforderung.
- Berechtigungsstufe 15 - Enthält alle Befehle auf *Aktivierungsebene* an der `Router->`Eingabeaufforderung.

Mit dem folgenden Befehl können Sie Befehle zwischen den Berechtigungsebenen verschieben:

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

Konsolenport-Authentifizierung

Die Konsolenport-Autorisierung wurde erst als Funktion hinzugefügt, wenn die Cisco Bug-ID CSCdi82030 implementiert wurde (nur registrierte Kunden). Die Konsolen-Port-Autorisierung ist standardmäßig deaktiviert, um die Wahrscheinlichkeit zu verringern, dass der Router versehentlich gesperrt wird. Wenn ein Benutzer über die Konsole physischen Zugriff auf den Router hat, ist die Konsolenport-Autorisierung nicht sehr effektiv. Bei Images, in denen die Cisco Bug-ID CSCdi82030 implementiert ist, können Sie die Konsolenport-Autorisierung unter Zeile con 0 mit dem ausgeblendeten Befehl **aaa authorized console aktivieren**.

Cisco Secure User Profile

Diese Ausgabe zeigt ein Beispielbenutzerprofil.

```
# ./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"
}
}

}
```

Routerkonfiguration

```
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
```

Beispielausgabe

Beachten Sie, dass einige Ausgaben aus räumlichen Gründen in zwei Zeilen eingewickelt sind.

AAA-Sitzung - Benutzererfassung

```
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-Sitzung - Cisco IOS-Fehlerbehebung

```
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-Sitzung - Cisco Secure UNIX Debug

```
!--- 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.
```

Beispiele für Cisco Secure Profile

`group LANadmins{`
` service=shell {`
` cmd=interface{`
`  permit "Ethernet *"`
`  deny "Serial *"`
	Dieses Profil ermöglicht es jedem Benutzer, der Mitglied der Gruppe "LAN-Administratoren" ist, sich bei einem Router anzumelden

}
cmd=aaa{
deny ".*"
}
cmd=tacacs-server{
deny ".*"
}
default cmd=permit
}
	und die meisten Befehle einzugeben. Benutzern ist es nicht gestattet, Änderungen an der Konfiguration der seriellen Schnittstelle vorzunehmen oder Änderungen an der AAA-Konfiguration vorzunehmen (sie können also die Befehlsautorisierung nicht entfernen oder den TACACS-Server deaktivieren).

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
}
}
	Dieses Profil gibt seinen Gruppenmitgliedern **die** Berechtigungen für die bostonswitch-Geräte, die *bostonrtr1-bostonrtr9*-Geräte und das 10.28.17.1-Gerät. Alle Befehle sind für diese Geräte zulässig. Der Zugriff auf die *NYrouterX*-Geräte ist auf die exec-Ebene des Benutzers beschränkt, und alle Befehle werden verweigert, wenn eine Autorisierung beantragt wird.

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]+"
}
}
}
	Diese Gruppe hat vollen Zugriff auf alle NY-Router sowie vollen Zugriff auf den NY-Core-Router an den Schnittstellen Serial 0/x & Serial 1/x. Beachten Sie, dass Benutzer auch die Möglichkeit haben, AAA auf dem Core-Router zu deaktivieren.

user bob{
password = des "********"
privilege = des
"********" 15
member = NY_wan_admins
}
	Dieser Benutzer ist Mitglied der Gruppe "NY_wan_admins" und erbt diese Berechtigungen. Dieser Benutzer verfügt außerdem über ein

	Anmeldungs-Kennwort und ein Aktivierungskennwort.

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 ".*"
}
}
}
	Dieses Profil ist für einen Catalyst Switch vorgesehen. Benutzern sind nur bestimmte **festgelegte** Befehle gestattet. Sie dürfen Port 3/10 (einen Trunk-Port) nicht deaktivieren. Benutzer können das VLAN angeben, dem ein Port zugewiesen ist, aber alle anderen **festgelegten VLAN-**Befehle werden abgelehnt.

Zugehörige Informationen

- Produktsupport für Cisco Secure UNIX
- Technischer Support und Dokumentation - Cisco Systems