Niveaux d'autorisation et de privilège des commandes pour Cisco Secure UNIX

Contenu

Introduction

Ce document fournit les informations sur la façon dont utiliser l'Authentification, autorisation et comptabilité (AAA) pour le contrôle centralisé de shell et de commande.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Versions de logiciel 12.0(5)T et ultérieures de Cisco IOS®
- Cisco Secure pour l'UNIX 2.3(6)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Écoulement d'AAA d'échantillon

Cisco IOS (client d'AAA)	Cisco Secure (serveur d'AAA)
`aaa authentication login default group tacacs+ local`	user=fred {password=des}
`aaa authorization exec default group tacacs+ local`	service-shell {placez le priv-level=x}
`commande du niveau X d'exec privilégié` (voir les notes ci-dessous.)	
`aaa authorization commands # default \ group tacacs none aaa authorization config-commands`	service=shell {le cmd= par défaut (l'autorisation/refusent) interdisent le cmd=x cmd=y {}}
`enable secretaaa authentication enable default \ group tacacs+ enable`	privilège = DES « ******** » 15

Niveaux de privilège

Par défaut, il y a trois niveaux commande sur le routeur :

- niveau de privilège 0 — Inclut le **débronchement**, l'**enable**, la **sortie**, l'**aide**, et les commandes de **déconnexion**
- niveau de privilège 1 — Inclut toutes les commandes de *niveau utilisateur à la* demande de `router>`
- niveau de privilège 15 — Inclut toutes les commandes *niveau de l'enable à la* demande de `router>`

Vous pouvez déplacer des commandes autour entre les niveaux de privilège avec cette commande :

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

Authentification de port de console

L'autorisation sur le port de console n'a pas été ajoutée comme caractéristique jusqu'à ce que l'implémentation de l'ID de bogue Cisco CSCdi82030 (clients enregistrés seulement).

L'autorisation sur le port de console est éteinte par défaut afin de diminuer la probabilité accidentellement d'être verrouillée hors du routeur. Si un utilisateur a accès physique au routeur par l'intermédiaire de la console, l'autorisation sur le port de console n'est pas extrêmement efficace. Cependant, pour les images dans lesquelles l'ID de bogue Cisco CSCdi82030 est mis en application, vous pouvez activer l'autorisation sur le port de console sous la ligne l'escroquerie 0 avec l'**aaa authorization console de** commande masquée.

Profil utilisateur Cisco Secure

Cette sortie affiche un profil utilisateur d'échantillon.

```
# ./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"
}
}

}
```

Configuration du routeur

```
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
```

Exemple de sortie

Notez qu'une certaine sortie est enveloppée sur deux lignes en raison des considérations spatiales.

Session d'AAA - Capture d'utilisateur

```
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#

Session d'AAA - Debug de 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.*

Session d'AAA - Debug de Cisco Secure 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.*

Exemples Cisco Secures avancés de profil

group LANadmins{
service=shell {
cmd=interface{
	Ce profil permet n'importe quel utilisateur qui est un

permit "Ethernet *"
deny "Serial *"
}
cmd=aaa{
deny ".*"
}
cmd=tacacs-server{
deny ".*"
}
default cmd=permit
}
	membre de groupe « LANadmins » à se connecter dans un routeur et pour sélectionner la plupart des commandes. On ne permet pas à des des utilisateurs pour apporter des modifications à la configuration de l'interface série, ou pour apporter des modifications à l'AAA le config (ainsi eux ne peut pas enlever l'autorisation de commande ou désactiver le serveur 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
}
}
	Ce profil donne à ses membres du groupe des privilèges d'**enable** sur le bostonswitch, le *bostonrtr1 - les* périphériques *bostonrtr9*, et le périphérique de 10.28.17.1. On permet toutes les commandes pour ces périphériques. Access aux périphériques de *NYrouterX* est limité au niveau d'Exec de l'utilisateur seulement, et toutes les commandes sont refusées si demandé l'autorisation.

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]+"
}
}
}
	Ce groupe a l'accès complet à tous les Routeurs NY, aussi bien que l'accès complet au routeur de noyau NY sur le 0/x séquentiel et les interfaces 1/x séquentielles. Notez que les utilisateurs ont également la capacité de désactiver l'AAA sur le principal routeur.

user bob{
password = des "********"
privilege = des
"********" 15
member = NY_wan_admins
}
	Cet utilisateur est un membre du groupe de « NY_wan_admins » et hérite de ces privilèges. Cet utilisateur fait également spécifier un mot de passe de

	connexion aussi bien qu'un mot de passe d'enable.

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 ".*"
  }
 }
}
	Ce profil est conçu pour un commutateur de Catalyst. On permet à des utilisateurs seulement certaines **commandes set**. On ne leur permet pas pour désactiver le port 3/10 (un port de joncteur réseau). On permet à des des utilisateurs pour spécifier le VLAN qu'un port est assigné à, mais toutes autres commandes de **set vlan** sont refusées.

Informations connexes

- Support produit de Cisco Secure UNIX
- Support et documentation techniques - Cisco Systems