Cisco Secure for UNIX のコマンド権限と権限レベル

目次

概要

このドキュメントでは、認証、許可、アカウンティング（AAA）を使用して、シェルとコマンドの中央集中型の制御を行う方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® ソフトウェアリリース 12.0(5)T およびそれ以降
- UNIX 用の Cisco Secure 2.3(6)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始して

います。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

AAA フローを見本抽出して下さい

Cisco IOS（AAA クライアント）	Cisco Secure（AAAサーバ）
`aaa authentication login default group tacacs+ local`	user=fred {password=des}
`aaa authorization exec default group tacacs+ local`	サービス シェル{set priv-level=x}
`exec x`（下記の注記を参照して下さい。）	
`aaa authorization commands # default \ group tacacs none aaa authorization config-commands`	service=shell {デフォルト cmd=（割り当て/拒否は）cmd=x を cmd=y 禁止します{}}
`enable secretaaa authentication enable default \ group tacacs+ enable`	特権 = DES 「********」 15

権限レベル

デフォルトでは、ルータには次の 3 つのコマンド レベルがあります。

- 特権レベル 0 —**ディセーブル**、**イネーブル**、**終了**、**ヘルプ**および**ログアウト** コマンドが含まれています
- 特権レベル 1 — `router>` プロンプトですべての*ユーザー レベル* コマンドが含まれています
- 特権レベル 15 — `router>` プロンプトですべての*イネーブル レベル* コマンドが含まれています

このコマンドで特権レベルの間でコマンドを動かすことができます:

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

コンソール ポート認証

コンソールポート許可は Cisco バグ ID CSCdi82030（登録ユーザのみ）の実装までの機能として追加されません。 コンソールポート許可はデフォルトでルータからロックアウトされる確率を偶然減すこと消えています。 ユーザはコンソールによってルータに物理アクセスをアクセスできる場合、コンソールポート許可は非常に効果がありません。 ただし、Cisco バグ ID CSCdi82030 が設定されているイメージのために、隠しコマンド **AAA認証 コンソール**と line con 0 の下でコンソールポート許可をつけることができます。

Cisco Secure ユーザ プロファイル

この出力はサンプル ユーザ プロファイルを示したものです。

```
# ./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"
}
}

}
```

ルータの設定

```
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
```

サンプル出力

出力が空間的な考慮事項が理由で 2 つの行にラップされることに注目して下さい。

AAA セッション-ユーザ キャプチャ

```
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 セッション- Cisco IOS デバッグ

```
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 セッション- Cisco Secure UNIX デバッグ

!--- 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.*

高度 Cisco Secure プロファイル例

group LANadmins{
 	
service=shell {
 	
cmd=interface{
 	
permit "Ethern
	このプロファイルはルータにログイン し、ほとんどのコマンドを入力するグループ「 LANadmins」のメンバーであるユーザを可能にします。 ユーザはシリアルインターフェイス設定への変更を行なうか、または AAA 構成への変更できません（従ってコマンド許可を取除くか、または TACACSサーバをディセーブルにすることができません）作ることが。

et *"
  deny
"Serial
*"
}
 	
cmd=aaa
{
  deny
".*"
}
 	
cmd=tac
acs-
server{
  deny
".*"
}
 	
default
cmd=per
mit
}	

group
Boston_
Admins{
 	
service
=shell
{
  allow
"10.28.
17.1"
".*"
".*"
  allow
bostons
witch
".*"
".*"
  allow
"^bosto
nrtr[0-
9]+"
".*"
".*"
  set
priv-
lvl=15
 	
default
cmd=per
mit
}
 	
service
=shell
{
  allow
"^NYrou
ter[0-
9]+"
".*"
	このプロファイルはグループ メンバーに bostonswitch、*bostonrtr1 - bostonrtr9* デバイス、および 10.28.17.1 デバイスの**イネーブル**特権を与えます。 これらのデバイスにすべてのコマンドが割り当てられます。 *NYrouterX* デバイスへのアクセスはユーザ exec レベルだけに制限され、許可を頼まれた場合すべてのコマンドは否定されます。

".*" set priv- lvl=1 default cmd=den y } }	

group
NY_wan_
admins{
 	
service
=shell
{
  allow
"^NYrou
ter[0-
9]+"
".*"
".*"
  set
priv-
lvl=15
 	
default
cmd=per
mit
 }
 	
service
=shell
{
  allow
"^NYcor
e$"
".*"
".*"
 	
default
cmd=per
mit
 	
cmd=int
erface{
 	
permit
"Serial
0/[0-
9]+"
 	
permit
"Serial
1/[0-
9]+"
  }
 }
}
	このグループにすべての NY ルータにフルアクセス、またシリアル 0/x 及びシリアル 1/x インターフェイスの NY コア ルータにフルアクセスがあります。 ユーザにまたコア ルータの AAA をディセーブルにする機能があることに注目して下さい。

user bob{	このユーザは「NY_wan_admins」グループのメンバーで、それらの特権を受継ぎます。 このユーザはまたログインパスワード、またイネー

password = des "********" privilege = des "********" 15 member = NY_wan_admins }	ブルパスワードを規定 してもらいます。

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 *"
	このプロファイルは Catalyst スイッチのために設計されています。 ユーザはある特定の **set コマンドだけ**与えられます。 彼らはポート 3/10（トランク ポート）を無効にすることができません。 ユーザはポートがに割り当てられるが、他の **set vlan コマンドは**すべて否定されます VLAN を規定 することができます。

```
permit
"vlan
[0-9]+
[0-
9]+/[0-
9]+"

deny
".*"
   }
   cmd
= show{

permit
".*"
   }
   cmd
=
enable{

permit
".*"
   }
 }
}
```

関連情報

- Cisco Secure UNIX 製品サポート
- テクニカルサポートとドキュメント - Cisco Systems