如何使用TACACS+和RADIUS分配許可權級別

目錄

簡介

本檔案將說明如何變更特定命令的許可權等級，並提供路由器和TACACS+及RADIUS伺服器部分範例組態的範例。

必要條件

需求

本文的讀者應該知道路由器上的許可權級別。

預設情況下，路由器上有三個許可權等級。

- privilege level 1 = non-privileged(prompt is `router>`)，登入的預設級別
- 特權級別15 =特權(提示為`router#`)，進入啟用模式後的級別
- 許可權級別0 =很少使用，但包括5個命令：**disable**、**enable**、**exit**、**help**和**logout**

級別2-14不在預設配置中使用，但通常位於級別15的命令可以移動到這些級別之一，而通常位於級別1的命令可以移動到這些級別之一。顯然，此安全模式涉及對路由器的某些管理。

要以登入使用者的身份確定許可權級別，請鍵入**show privilege**命令。要確定您正在使用的Cisco IOS®軟體版本在特定許可權級別上可用的命令，請鍵入**?**以該許可權級別登入時位於命令列上。

注意：如果身份驗證伺服器支援TACACS+，則您可以執行命令授權，而不是分配許可權級別。RADIUS通訊協定不支援指令授權。

採用元件

本檔案中的資訊是根據Cisco IOS軟體版本11.2和更新版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

範例

在本例中，**snmp-server**命令從許可權級別15（預設值）下移到許可權級別7。**ping**命令從許可權級別1上移到許可權級別7。當使用者7通過身份驗證時，伺服器為該使用者分配了許可權級別7，並且**show privilege**命令顯示「當前許可權級別為7」。 使用者可以在配置模式下執行ping和snmp-server配置。其他配置命令不可用。

配置 — 路由器

路由器 — 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

路由器 — 11.3.3.T及更高版本（直到12.0.5.T）

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

路由器 — 12.0.5.T及更高版本

```
aaa new-model
aaa authentication login default group tacacs+|radius local
```

```
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

配置 — 伺服器

Cisco安全NT TACACS+

按照以下步驟配置伺服器。

1. 填寫使用者名稱和密碼。
2. 在「組設定」中，確保已選中shell/exec並在許可權級別框中輸入了7。

TACACS+ — 免費軟體伺服器中的Stanza

```
Stanza in TACACS+ freeware:
user = seven {
login = cleartext seven
service = exec {
priv-lvl = 7
}
}
```

Cisco安全UNIX TACACS+

```
user = seven {
password = clear "seven"
service = shell {
set priv-lvl = 7
}
}
```

Cisco安全NT RADIUS

按照以下步驟配置伺服器。

1. 輸入使用者名稱和密碼。
2. 在IETF的組設定中，Service-type(attribute 6)= **Nas-Prompt**
3. 在CiscoRADIUS區域中，選中**AV-Pair**，並在下面的矩形框中輸入**shell:priv-lvl=7**。

Cisco安全UNIX RADIUS

```
user = seven{
radius=Cisco {
check_items= {
```

```
2="seven"
}
reply_attributes= {
6=7
9,1="shell:priv-lvl=7"
}
}
}
```

這是使用者名稱「seven」的使用者檔案。

注意：伺服器必須支援Cisco av配對。

- 七個密碼= **passwdxyz**
- Service-Type = **Shell-User**
- cisco-avpair =**shell:priv-lvl=7**

相關資訊

- RADIUS 支援頁面
- 要求建議 (RFC)
- IOS 文件中的 TACACS+
- TACACS+支援頁面
- Cisco Secure UNIX支援頁
- Cisco Secure ACS for Windows支援頁
- 技術支援 - Cisco Systems