Cisco IOS路由器：HTTP連線的本地、TACACS+和RADIUS身份驗證配置示例

目錄

簡介

本檔案介紹如何設定HTTP連線的本地、TACACS+和RADIUS驗證。還提供了一些相關的調試命令。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

本文件沒有特定先決條件。

採用元件

本檔案中的資訊是根據以下軟體和硬體版本。

- Cisco IOS®軟體版本11.2或更高版本
- 支援這些軟體版本的硬體

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。

背景理論

在Cisco IOS®軟體版本11.2中，新增了一項透過HTTP管理路由器的功能。Cisco IOS配置基礎命令參考的「Cisco IOS Web瀏覽器命令」部分包含有關此功能的以下資訊。

"**ip http authentication**命**令使您能**夠為HTTP伺服器使用者指定特定的身份驗證方法。HTTP伺服器使用enable password方法對許可權級別15的使用者進行身份驗證。現在，**ip http authentication**命令允許您指定enable、local、TACACS或身份驗證、授權和記帳(AAA)HTTP伺服器使用者身份驗證。

設定

本節提供用於設定本文件中所述功能的資訊。

本文檔使用如下所示的配置。

- 為HTTP伺服器使用者配置本地身份驗證
- 為HTTP伺服器使用者配置TACACS+身份驗證
- 為HTTP伺服器使用者配置RADIUS身份驗證

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

為HTTP伺服器使用者配置本地身份驗證

- 路由器配置
- 使用者結果

路由器配置

使用Cisco IOS軟體版本11.2的本機驗證

```
!--- This is the part of the configuration related to
local authentication. ! aaa new-model aaa authentication
login default local aaa authorization exec local
username one privilege 15 password one username three
password three username four privilege 7 password four
ip http server ip http authentication aaa ! !--- Example
of command moved from level 15 (enable) to level 7 !
privilege exec level 7 clear line
```

使用Cisco IOS軟體版本11.3.3.T或更高版本的本地身份驗證

```
!--- This is the part of the configuration !--- related
to local authentication. ! aaa new-model aaa
authentication login default local aaa authorization
exec default local username one privilege 15 password
one username three password three username four
```

```
privilege 7 password four ip http server ip http
authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
7 clear line
```

使用者結果

這些結果適用於先前路由器配置中的使用者。

- **使用者1**如果輸入的URL為http://#.#.#.#，則使用者將通過Web授權。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於啟用模式(**show privilege**將為15)。如果將命令授權新增到路由器，使用者仍會成功執行所有命令。
- **使用者3**使用者由於沒有許可權級別，將無法進行Web授權。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於非啟用模式(**show privilege**將為1)。如果將命令授權新增到路由器，使用者仍會成功執行所有命令。
- **使用者4**如果輸入的URL為http://#.#.#.#/level/7/exec，使用者將通過Web授權。將顯示1級命令和7級**clear line**命令。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於許可權級別7(**show privilege**將為7)如果將命令授權新增到路由器，使用者仍會成功執行所有命令。

為HTTP伺服器使用者配置TACACS+身份驗證

路由器配置

使用Cisco IOS軟體版本11.2進行驗證

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

使用Cisco IOS軟體版本11.3.3.T到12.0.5.T進行身份驗證

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

使用Cisco IOS軟體版本12.0.5.T及更高版本進行身份驗證

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

使用者結果

以下結果適用於下面伺服器配置中的使用者。

- **使用者1**如果輸入的URL為http://#.#.#.#，則使用者將通過Web授權。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於啟用模式(**show privilege**將為15)。如果將命令授權新增到路由器，使用者仍會成功執行所有命令。
- **使用者2**如果輸入的URL為http://#.#.#.#，則使用者將通過Web授權。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於啟用模式(**show privilege**將為15)。如果向路由器新增了命令授權，則使用者將拒絕所有命令，因為伺服器配置未授權這些命令。
- **使用者3**使用者由於沒有許可權級別，將無法進行Web授權。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於非啟用模式(**show privilege**將為1)。如果將命令授權新增到路由器，使用者仍會成功執行所有命令。
- **使用者4**如果輸入的URL為http://#.#.#.#/level/7/exec，使用者將通過Web授權。將顯示1級命令和7級**clear line**命令。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於許可權級別7(**show privilege**將為7)如果將命令授權新增到路由器，使用者仍會成功執行所有命令。

免費軟體守護程式伺服器配置

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
```

```
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

Cisco Secure ACS for UNIX伺服器配置

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "********"
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "********"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

Cisco Secure ACS for Windows Server配置

第一組中的使用者1

- 組設定檢查**shell(exec)**。檢查**privilege level=15**。選中**Default(Undefined)Services**。**注意：如果未顯示此選項，請轉到Interface Configuration，然後選擇TACACS+**，然後選擇**Advanced Configuration Options**。選擇**Display enable default(undefined)service** configuration。
- 使用者設定來自任何資料庫的密碼；在頂部區域輸入密碼並確認。

第二組中的使用者2

- 組設定檢查**shell(exec)**。檢查**privilege level=15**。請勿選中**Default(Undefined)Services**。
- 使用者設定來自任何資料庫的密碼；在頂部區域輸入密碼並確認。

第三組使用者

- 組設定檢查**shell(exec)**。將**許可權級別**留空。選中**Default(Undefined)Services**。**注意：如**果未顯示此選項，請轉到**Interface Configuration，然後選擇TACACS+**，然後選擇**Advanced Configuration Options**。選擇**Display enable default(undefined)service** configuration。
- 使用者設定來自任何資料庫的密碼；在頂部區域輸入密碼並確認。

組四中的使用者4

- 組設定檢查**shell(exec)**。檢查**privilege level=7**。選中**Default(Undefined)Services**。**注意：如**果未顯示此選項，請轉到**Interface Configuration，然後選擇TACACS+**，然後選擇**Advanced Configuration Options**。選擇**Display enable default(undefined)service** configuration。
- 使用者設定來自任何資料庫的密碼；在頂部區域輸入密碼並確認。

為HTTP伺服器使用者配置RADIUS身份驗證

路由器配置

使用Cisco IOS軟體版本11.2進行驗證

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to
level 7 ! privilege exec level 7 clear line radius-
server host 171.68.118.101 radius-server key cisco
```

使用Cisco IOS軟體版本11.3.3.T到12.0.5.T進行身份驗證

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

使用Cisco IOS軟體版本12.0.5.T及更高版本進行身份驗證

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
```

```
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

使用者結果

以下結果適用於下面伺服器配置中的使用者。

- **使用者1**如果輸入的URL為http://#.#.#.#，則使用者將通過Web授權。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於啟用模式(**show privilege**將為15)。
- **使用者3**使用者由於沒有許可權級別，將無法進行Web授權。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於非啟用模式(**show privilege**將為1)。
- **使用者4**如果輸入的URL為http://#.#.#.#/level/7/exec，使用者將通過Web授權。將顯示1級命令和7級**clear line**命令。通過Telnet連線到路由器後，使用者可以在登入身份驗證後執行所有命令。登入後，使用者將處於許可權級別7(**show privilege**將為7)

支援Cisco AV配對的伺服器上的RADIUS配置

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"

three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

Cisco Secure ACS for UNIX伺服器配置

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
```

```
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

Cisco Secure ACS for Windows Server配置

- 使用者=一，服務型別（屬性6）=管理
- 使用者=三，服務型別（屬性6）=登入
- 使用者= 4，服務型別（屬性6）=登入，選中Cisco AV配對框並輸入shell:priv-lvl=7

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

以下命令可用於調試HTTP身份驗證。路由器上會發出這些命令。

注意：發出debug指令之前，請先參閱有關Debug指令的重要資訊。

- **terminal monitor** — 顯示debug命令輸出以及目前終端和作業階段的系統錯誤訊息。
- **debug aaa authentication** — 顯示有關AAA/TACACS+身份驗證的資訊。
- **debug aaa authorization** — 顯示有關AAA/TACACS+授權的資訊。
- **debug radius** — 顯示與RADIUS關聯的詳細調試資訊。
- **debug tacacs** — 顯示與TACACS關聯的資訊。
- **debug ip http authentication** — 使用此命令排除HTTP身份驗證問題。顯示路由器嘗試的身份驗證方法和身份驗證特定的狀態消息。

相關資訊

- Cisco TACACS+存取軟體支援頁面
- RADIUS 支援頁面
- Cisco Secure ACS for Windows支援頁
- Cisco Secure ACS for UNIX支援頁
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems