使用TACACS+驗證配置思科路由器

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[驗證](#)
[新增授權](#)
[新增記帳](#)
[測試檔案](#)
[相關資訊](#)

簡介

本檔案介紹如何設定思科路由器，以使用在UNIX上執行的TACACS+進行驗證。TACACS+提供的功能不及商業上提供的Cisco Secure ACS for Windows或Cisco Secure ACS UNIX。

Cisco Systems先前提供的TACACS+軟體已停產，且Cisco Systems不再支援。

現在，您在您喜愛的網際網路搜尋引擎上搜尋「TACACS+免費軟體」時，可以找到許多可用的TACACS+免費軟體版本。思科並不特別建議實施任何特定的TACACS+免費軟體。

思科安全存取控制伺服器(ACS)可透過世界各地的定期思科銷售和分銷管道購買。Cisco Secure ACS for Windows包含在Microsoft Windows工作站上進行獨立安裝所需的所有必要元件。Cisco Secure ACS解決方案引擎附帶預裝的Cisco Secure ACS軟體許可證。訪問思科訂購首頁(僅限註冊客戶)下訂單。

注意：您需要具有相關服務合約的CCO帳戶才能獲得適用於Cisco Secure ACS for Windows的90天試用版。

本文中的路由器組態是在執行Cisco IOS®軟體版本11.3.3的路由器上開發的。Cisco IOS軟體版本12.0.5.T和更新版本使用**group tacacs+**而不是**tacacs+**，因此**aaa authentication login default tacacs+ enable**等陳述式顯示為**aaa authentication login default group tacacs+ enable**。

請參閱Cisco IOS軟體檔案以瞭解更多有關路由器命令的完整資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco IOS軟體版本11.3.3和Cisco IOS軟體版本12.0.5.T及更新版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

驗證

請完成以下步驟：

1. 請確保您已在UNIX伺服器上編譯TACACS+(TAC+)代碼。這裡的伺服器配置假定您使用Cisco TAC+伺服器代碼。無論伺服器程式碼是否為思科伺服器程式碼，路由器組態都應正常運作。TAC+必須作為根運行；如有必要，請轉到根目錄。
2. 複製本檔案結尾的test_file，將其放在TAC+伺服器上，並命名為**test_file**。檢查以確保**tac_plus_executable守護程**序以**test_file**啟動。在此命令中，**-P**選項將檢查編譯錯誤，但不啟動守護程式：
   ```
   tac_plus_executable -P -C test_file
   ```
   您可能會看到test_file的內容向下滾動視窗，但您不應該看到`cannot find file`、`cleartext expected - found cleartext`或`unexpected }`等消息。如果出現錯誤，請檢查test_file的路徑，重新檢查鍵入內容，然後重新測試，然後繼續。
3. 開始在路由器上配置TAC+。輸入**enable**模式，並在命令集之前鍵入**configure terminal**。此命令語法可確保您最初沒有鎖定在路由器之外，但前提是沒有**tac_plus_executable**:

   ```
   !--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
   authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are
   names of lists, and the methods !--- listed on the same lines are the methods !--- in the
   order to be tried. As used here, if !--- authentication fails due to the !---
   tac_plus_executable not being started, the !--- enable password is accepted because !--- it
   is in each list.

      !
      aaa authentication login linmethod tacacs+ enable
      aaa authentication login vtymethod tacacs+ enable
      aaa authentication login conmethod tacacs+ enable
      !
      !--- Point the router to the server, where #.#.#.# !--- is the server IP address. !
   tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being
   locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8
   login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400
   flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being
   locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
   ```
4. 繼續進行之前，請進行測試，確保您仍可以通過Telnet和控制檯埠訪問路由器。由於**tac_plus_executable**未運行，因此應該接受**enable**密碼。**注意：**保持控制檯埠會話處於活動狀態並保持啟用模式。此會話不應超時。此時對路由器的訪問受到限制，您需要能夠進行配置更改而不將自己鎖定。發出以下命令檢視路由器上的伺服器到路由器的互動：
   ```
   terminal monitor
     debug aaa authentication
   ```
5. 以根使用者身份在伺服器上啟動TAC+:

```
tac_plus_executable -C test_file -d 16
```

6. 檢查以確保TAC+已啟動：
   ```
   ps -aux | grep tac_plus_executable
   ```
   或
   ```
   ps -ef | grep tac_plus_executable
   ```
   如果TAC+沒有啟動，通常是test_file中的語法問題。返回步驟1以更正此問題。
7. 鍵入**tail -f /var/tmp/tac_plus.log**檢視伺服器上的路由器到伺服器互動。**注意：**步驟5-d 16選項將所有事務的輸出傳送到/var/tmp/tac_plus.log。
8. Telnet(VTY)使用者現在必須透過TAC+進行驗證。在路由器和伺服器上進行debug（步驟4和7）後，從網路的另一部分Telnet至路由器。路由器會產生使用者名稱和密碼提示，您會對此進行回覆：
   ```
   'authenuser'   (username from test_file)
   'admin'   (password from test_file)
   ```
   使用者`authenuser`位於`admin`組中，該組的密碼為`admin`。觀察伺服器和路由器，從中可以看到TAC+互動 — 傳送位置、響應、請求等。請更正所有問題，然後再繼續。
9. 如果您也希望使用者透過TAC+進行驗證以進入啟用模式，請確保您的主控台連線埠作業階段仍處於作用中狀態，並將以下命令新增到路由器中：
   ```
   !--- For enable mode, list 'default' looks to TAC+ !--- then enable password if TAC+ does
   not run. aaa authentication enable default tacacs+ enable
   ```
   使用者現在必須透過TAC+啟用。
10. 在路由器和伺服器上進行debug（步驟4和7）後，從網路的另一部分Telnet至路由器。路由器會產生使用者名稱和密碼提示，您會對此進行回覆：
    ```
    'authenuser'   (username from test_file)
    'admin'   (password from test_file)
    ```
    進入啟用模式時，路由器會要求您回覆的密碼：
    ```
    'cisco'  ($enable$ password from test_file)
    ```
    觀察伺服器和路由器，您應該從其中看到TAC+互動 — 傳送內容、響應、請求等。請更正所有問題，然後再繼續。
11. 在仍連線到主控台連線埠時，關閉伺服器上的TAC+程式，確保在TAC+關閉時，使用者仍可以存取路由器：
    ```
    ps -aux | grep tac_plus_executable
    ```
    或
    ```
    ps -ef | grep tac_plus_executable)
      kill -9 pid_of_tac_plus_executable
    ```
    重複上一步的Telnet和啟用。然後，路由器會意識到TAC+進程沒有響應，並允許使用者使用預設密碼登入和啟用。
12. 檢查您通過TAC+對控制檯埠使用者的身份驗證。若要執行此操作，請再次啟動TAC+伺服器（步驟5和6），並建立到路由器的Telnet會話（該會話應通過TAC+進行身份驗證）。在啟用模式下通過Telnet保持與路由器的連線，直到確定可以通過控制檯埠登入路由器。通過控制檯埠註銷與路由器的原始連線，然後重新連線到控制檯埠。使用使用者ID和密碼（如步驟10所示）登入和啟用的控制檯埠身份驗證現在應通過TAC+。
13. 當您通過Telnet會話或控制檯埠保持連線，並且在路由器和伺服器上進行調試時（步驟4和7），建立到線路1的數據機連線。線路使用者現在必須通過TAC+登入和啟用。路由器會產生使用者名稱和密碼提示，您會對此進行回覆：
    ```
    'authenuser'   (username from test_file)
    'admin'   (password from test_file)
    ```
    進入啟用模式時，路由器會要求密碼。回覆：
    ```
    'cisco'   ($enable$ password from test_file)
    ```
    觀察您看到TAC+互動的伺服器和路由器 — 傳送位置、響應、請求等。請更正所有問題，然後再繼續。使用者現在必須透過TAC+啟用。

新增授權

新增授權是可選的。

預設情況下，路由器上有三個命令等級：

- 許可權級別0，包括禁用、啟用、退出、幫助和註銷
- 許可權級別1 - Telnet上的正常級別 — 提示符為`router>`
- 許可權級別15 — 啟用級別 — 提示`router#`

由於可用命令取決於IOS功能集、Cisco IOS版本、路由器型號等，因此沒有第1級和第15級的所有命令的完整清單。例如，**show ipx route**不存在於僅IP功能集中，**show ip nat trans**不存在於Cisco IOS軟體版本10.2.x中，因為當時未引入NAT，並且沒有電源和溫度監控的路由器型號中沒有**show environment**。當您輸入**?**處於該許可權級別時，在路由器中提示符處。

實施思科錯誤ID CSCdi82030(僅限註冊客戶)之前，未將控制檯埠授權新增為功能。預設情況下，控制檯埠授權處於關閉狀態，以減少您意外被鎖定在路由器之外的可能性。如果使用者可以通過控制檯對路由器進行物理訪問，則控制檯埠授權不會非常有效。但是可以在以下命令中實作Cisco錯誤ID CSCdi82030(僅限註冊客戶)的映像中的`con 0`行下開啟主控台連線埠授權：

```
authorization exec default|WORD
```

1. 路由器可以配置為在所有或某些級別通過TAC+授權命令。此路由器配置允許所有使用者在伺服器上設定每個命令的授權。此處我們通過TAC+授權所有命令，但是如果伺服器關閉，則無需授權。
   ```
   aaa authorization commands 1 default tacacs+ none
     aaa authorization commands 15 default tacacs+ none
   ```
2. TAC+伺服器執行期間，使用userid **authenuser**Telnet連線至路由器。由於authenuser在test_file中具有預設服務= permit，因此該使用者應該能夠執行所有功能。在路由器中，進入**enable**模式，然後開啟授權調試：
   ```
   terminal monitor
     debug aaa authorization
   ```
3. 使用userid **authoruser**和password **operator**Telnet至路由器。此使用者無法執行兩種show命令**traceroute**和**logout**(請參見**test_file**)。觀察應看到TAC+互動的伺服器和路由器（傳送位置、響應、請求等）。 請更正所有問題，然後再繼續。
4. 如果要為autocommand配置使用者，請消除test_file中的已註釋掉的使用者瞬態，並放置有效的IP地址目標來代替#.#.#.#。停止並啟動TAC+伺服器。在路由器上：
   ```
   aaa authorization exec default tacacs+
   ```
   使用userid **transient**和**password** transientTelnet至路由器。**telnet #.#.#.#**將執行，並將使用者瞬態資訊傳送到另一個位置。

新增記帳

新增記帳是可選操作。

對記帳檔案的引用位於test_file - accounting file = /var/log/tac.log。但是，除非在路由器中配置（如果路由器運行的是高於11.0的Cisco IOS軟體版本），否則不會進行記帳。

1. 在路由器中啟用記帳：
   ```
   aaa accounting exec default start-stop tacacs+
     aaa accounting connection default start-stop tacacs+
     aaa accounting network default start-stop tacacs+
   ```

```
aaa accounting system default start-stop tacacs+
```

注意：在某些版本中，AAA記帳不執行按命令記帳。因應措施是使用每個命令的授權，並將發生的情況記錄在記帳檔案中。(請參閱Cisco錯誤ID CSCdi44140。) 如果您使用的映像使用了此固定版本[Cisco IOS軟體版本11.2(1.3)F、11.2(1.2)、11.1(6.3)、11.1(6.3)AA01、11.1(6.3)CA截至1997年9月24日]，您還可以啟用命令記帳。

2. TAC+在伺服器上執行時，請在伺服器上輸入以下命令，以便檢視進入記帳檔案的專案：

```
tail -f /var/log/tac.log
```

然後登入並退出路由器，Telnet退出路由器等等。如有必要，在路由器上輸入：

```
terminal monitor
  debug aaa accounting
```

測試檔案

```
- - - - - - - (cut here) - - - - - - -

# Set up accounting file if enabling accounting on NAS
accounting file = /var/log/tac.log

# Enable password setup for everyone:
user = $enable$ {
        login = cleartext "cisco"
        }

# Group listings must be first:
group = admin {
# Users in group 'admin' have cleartext password
        login = cleartext "admin"
        expires = "Dec 31 1999"
}

group = operators {
# Users in group 'operators' have cleartext password
        login = cleartext "operator"
        expires = "Dec 31 1999"
}

group = transients {
# Users in group 'transient' have cleartext password
        login = cleartext "transient"
        expires = "Dec 31 1999"
}

# This user is a member of group 'admin' & uses that group's password to log in.
#  The $enable$ password is used to enter enable mode.  The user can perform all commands.
 user = authenuser {
        default service = permit
        member = admin
        }

# This user is limitted in allowed commands when aaa authorization is enabled:
 user = telnet {
        login = cleartext "telnet"
        cmd = telnet {
        permit .*
        }
        cmd = logout {
        permit .*
        }
        }
```

```
# user = transient {
#       member = transients
#       service = exec {
        # When transient logs on to the NAS, he's immediately
        # zipped to another site
#       autocmd = "telnet #.#.#.#"
#       }
#       }

# This user is a member of group 'operators'
# & uses that group's password to log in
 user = authenuser {
        member = operators
# Since this user does not have 'default service = permit' when command
# authorization through TACACS+ is on at the router, this user's commands
# are limited to:
        cmd = show {
        permit ver
        permit ip
        }
        cmd = traceroute {
        permit .*
        }
        cmd = logout {
        permit .*
        }
}
- - - - (end cut here) - - - -
```

注意：如果TACACS伺服器無法訪問，則會生成以下錯誤消息：`%AAAA-3-DROPACCTSNDFAIL:system-start`。驗證TACACS+伺服器是否正常運行。

相關資訊

- 單使用者網路存取安全TACACS+
- 終端存取控制器存取控制系統(TACACS+)
- 思科安全存取控制伺服器（Windows專用）
- 技術支援與文件 - Cisco Systems