

# TACACS身份驗證問題故障排除

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[TACACS的運作方式](#)

[TACACS問題故障排除](#)

[相關資訊](#)

---

## 簡介

本文檔介紹對Cisco IOS®/Cisco IOS® XE路由器和交換機上的TACACS身份驗證問題進行故障排除的步驟。

## 必要條件

### 需求

思科建議您瞭解以下主題的基本知識：

- 思科裝置上的驗證、授權和記帳(AAA)組態
- TACACS配置

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## TACACS的運作方式

TACACS+通訊協定使用傳輸控制通訊協定(TCP)作為傳輸通訊協定，且目的地連線埠號碼為49。當路由器收到登入請求時，它會與TACACS伺服器建立TCP連線，並向使用者發佈顯示的使用者名稱提示。使用者輸入使用者名稱後，路由器再次與TACACS伺服器進行通訊以提示密碼。使用者輸入口令後，路由器會再次將此資訊傳送到TACACS伺服器。TACACS伺服器驗證使用者憑證並將響應傳送迴路由器。AAA會話的結果可以是以下任何一種：

**透過：**經過身份驗證後，僅當路由器上配置了AAA授權時服務才會開始。此時開始授權階段。

**失敗：**當您驗證失敗時，系統可能會拒絕您進一步存取，或提示您依序重試記錄。這取決於

TACACS+後台程式。如果從伺服器收到FAIL，則在此示例中，您可以檢查為TACACS伺服器中的使用者配置的策略。

錯誤：表示在驗證期間發生錯誤。這可以是在守護程式中，也可以是在守護程式和路由器之間的網路連線中。如果收到ERROR響應，路由器通常會嘗試使用另一種方法對使用者進行身份驗證。

以下是Cisco路由器上AAA和TACACS的基本配置。

```
aaa new-model
aaa authentication log in default group tacacs+ local
aaa authorization exec default group tacacs+ local
!
tacacs server prod
address ipv4 10.106.60.182
key cisco123
!
ip tacacs source-interface Gig 0/0
```

## TACACS問題故障排除

### 步驟 1.

在埠49上使用telnet從具有相應源介面的路由器驗證與TACACS伺服器的連線。如果路由器無法連線到埠49上的TACACS伺服器，則可能存在一些防火牆或訪問清單來阻止流量。

```
Router#telnet 10.106.60.182 49
Trying 10.106.60.182, 49 ... Open
```

### 步驟 2.

驗證已在TACACS伺服器上使用正確的IP地址和共用金鑰正確配置了AAA客戶端。如果路由器有多個傳出介面，建議使用此命令配置TACACS源介面。可以將其IP地址配置為TACACS伺服器上的客戶端IP地址的介面配置為路由器上的TACACS源介面

```
Router(config)#ip tacacs source-interface Gig 0/0
```

### 步驟 3.

驗證TACACS源介面是否位於虛擬路由和轉發(VRF)上。如果介面位於VRF上，您可以在AAA伺服器組下配置VRF資訊。有關VRF感知TACACS的配置資訊，請參閱[TACACS配置指南](#)。

### 步驟 4.

執行test aaa並驗證您是否從伺服器收到正確的響應。

```
Router#test aaa group tacacs+ cisco cisco legacy
Sending password
User successfully authenticated
```

### 步驟 5.

如果測試aaa失敗，請同時啟用這些調試，以便分析路由器和TACACS伺服器之間的事務以確定根本原因。

```
debug aaa authentication
debug aaa authorization
debug tacacs
debug ip tcp transaction
```

這是工作情境中的偵錯輸出範例：

```
*Apr 6 13:32:50.462: AAA/BIND(00000054): Bind i/f
*Apr 6 13:32:50.462: AAA/AUTHEN/LOGIN (00000054): Pick method list 'default'
*Apr 6 13:32:50.462: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr 6 13:32:50.462: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:50.462: TPLUS: processing authentication start request id 84
*Apr 6 13:32:50.462: TPLUS: Authentication start packet created for 84()
*Apr 6 13:32:50.462: TPLUS: Using server 10.106.60.182
*Apr 6 13:32:50.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr 6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr 6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: wrote entire 38 bytes request
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: Would block while reading
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 43 bytes data)
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 55 bytes response
*Apr 6 13:32:50.466: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr 6 13:32:50.466: TPLUS: Received authen response status GET_USER (7)
*Apr 6 13:32:53.242: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr 6 13:32:53.242: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:53.242: TPLUS: processing authentication continue request id 84
```

```

*Apr 6 13:32:53.242: TPLUS: Authentication continue packet generated for 84
*Apr 6 13:32:53.242: TPLUS(00000054)/0/WRITE/10882BBC: Started 5 sec timeout
*Apr 6 13:32:53.242: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 16 bytes data)
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 28 bytes response
*Apr 6 13:32:53.246: TPLUS(00000054)/0/10882BBC: Processing the reply packet
*Apr 6 13:32:53.246: TPLUS: Received authen response status GET_PASSWORD (8)
*Apr 6 13:32:54.454: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr 6 13:32:54.454: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:54.454: TPLUS: processing authentication continue request id 84
*Apr 6 13:32:54.454: TPLUS: Authentication continue packet generated for 84
*Apr 6 13:32:54.454: TPLUS(00000054)/0/WRITE/2432818: Started 5 sec timeout
*Apr 6 13:32:54.454: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 18 bytes response
*Apr 6 13:32:54.458: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr 6 13:32:54.458: TPLUS: Received authen response status PASS (2)
*Apr 6 13:32:54.462: AAA/AUTHOR (0x54): Pick method list 'default'
*Apr 6 13:32:54.462: TPLUS: Queuing AAA Authorization request 84 for processing
*Apr 6 13:32:54.462: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:54.462: TPLUS: processing authorization request id 84
*Apr 6 13:32:54.462: TPLUS: Protocol set to None .....Skipping
*Apr 6 13:32:54.462: TPLUS: Sending AV service=shell
*Apr 6 13:32:54.462: TPLUS: Sending AV cmd*
*Apr 6 13:32:54.462: TPLUS: Authorization request created for 84(cisco)
*Apr 6 13:32:54.462: TPLUS: using previously set server 10.106.60.182 from group tacacs+
*Apr 6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr 6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr 6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: wrote entire 62 bytes request
*Apr 6 13:32:54.462: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.462: TPLUS(00000054)/0/READ: Would block while reading
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 18 bytes data)
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 30 bytes response
*Apr 6 13:32:54.470: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr 6 13:32:54.470: TPLUS: Processed AV priv-lvl=15
*Apr 6 13:32:54.470: TPLUS: received authorization response for 84: PASS
*Apr 6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV cmd=
*Apr 6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV priv-lvl=15
*Apr 6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): Authorization successful

```

這是當TACACS伺服器配置了錯誤的預共用金鑰時，來自路由器的調試輸出示例。

```

*Apr 6 13:35:07.826: AAA/BIND(00000055): Bind i/f
*Apr 6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr 6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr 6 13:35:07.826: TPLUS(00000055) log in timer started 1020 sec timeout
*Apr 6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr 6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr 6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr 6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request

```

```
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr 6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr 6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr 6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

## 相關資訊

- [Cisco IOS上的TACACS配置](#)
- [技術支援與文件 - Cisco Systems](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。