

瞭解AAA Authentication Login Default Local Group TACACS+命令

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹Cisco IOS®設備上aaa authentication login default local group tacacs+命令的行為。

必要條件

需求

思科建議：

- 裝置上啟用了aaa new-model。

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。

設定

注意：使用Cisco Tool Catalog中的[Cisco CLI Analyzer](#)，獲得本節所用命令的詳細資訊。只有註冊思科使用者才能訪問內部思科工具和資訊。

在全域性配置模式下在裝置上配置以下命令：

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

僅使用 aaa new model 配置後，本地身份驗證將應用於所有線路和介面(控制檯線路line con 0除外)。

在這裡，AAA方法清單應用於裝置的所有線路上的所有登入嘗試，其中首先檢查本地資料庫，然後如果需要，嘗試使用終端訪問控制器訪問控制系統(TACACS)伺服器。

```
username cisco privilege 15 password 0 cisco
```

本地使用者資料庫：

```
tacacs-server host 10.20.220.141
```

```
tacacs-server key cisco
```

TACACS伺服器現已配置。

驗證

使用本節內容，確認您的組態是否正常運作。

1. 在測試的裝置上啟用Debug TACACS和Debug AAA Authentication。

```
RUT#show debug
```

```
General OS:
```

```
  TACACS access control debugging is on
```

```
  AAA Authentication debugging is on
```

2. 在裝置上執行telnet:

```
RUT#show ip interface brief | exclude unassigned
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	10.197.235.96	YES	DHCP	up	up
Loopback0	192.168.1.2	YES	manual	up	up

```
RUT#telnet 192.168.1.2
```

```
Trying 192.168.1.2 ... Open
```

```
User Access Verification
```

```
Username: cisco
```

```
*Jul 23 09:34:37.023: AAA/BIND(0000001E): Bind i/f
```

```
*Jul 23 09:34:37.023: AAA/AUTHEN/LOGIN (0000001E): Pick method list 'default'
```

```
Password:
```

```
RUT>
```

您注意到它沒有嘗試連線TACACS伺服器，因為已在本地找到使用者名稱cisco。

現在，如果您嘗試使用未在本機配置的憑據：

```
RUT#telnet 192.168.1.2
```

```
Trying 192.168.1.2 ... Open
```

```
User Access Verification
```

```
Username:
```

```
*Jul 23 09:36:01.099: AAA/BIND(0000001F): Bind i/f
```

```
*Jul 23 09:36:01.099: AAA/AUTHEN/LOGIN (0000001F): Pick method list 'default'
```

```
Username: cisco1
```

```
*Jul 23 09:36:11.095: TPLUS: Queuing AAA Authentication request 31 for processing
```

```
*Jul 23 09:36:11.095: TPLUS: processing authentication start request id 31
*Jul 23 09:36:11.095: TPLUS: Authentication start packet created for 31(cisco1)
*Jul 23 09:36:11.095: TPLUS: Using server 10.20.220.141
*Jul 23 09:36:11.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: Started 5 sec timeout
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out, clean up
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/47A14C34: Processing the reply packet
% Authentication failed
```

您可以看到它嘗試連線到TACACS伺服器10.20.220.141。這是一種預期的預設行為。TACACS伺服器上未配置使用者名稱cisco1，因此顯示Authentication failed。

如果裝置在配置中的預設組tacacs+本地具有AAA身份驗證日誌，則其第一個首選項為TACACS。如果TACACS可訪問，但使用者未在其上配置，則它不會回退並嘗試在本地資料庫中搜尋。顯示消息「Authentication failed(身份驗證失敗)」。

疑難排解

目前尚無特定資訊可用於排解此組態的疑難問題。

相關資訊

- [在接入伺服器上配置基本AAA](#)
- [思科技術支援與下載](#)

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）。