在Catalyst交換器上設定TACACS+、RADIUS和Kerberos

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[背景資訊](#)
[配置步驟](#)
[步驟A - TACACS+驗證](#)
[步驟B - RADIUS驗證](#)
[步驟C — 本地使用者名稱身份驗證/授權](#)
[步驟D - TACACS+命令授權](#)
[步驟E - TACACS+ Exec授權](#)
[步驟F - RADIUS Exec授權](#)
[步驟G — 記帳 — TACACS+或RADIUS](#)
[步驟H - TACACS+啟用身份驗證](#)
[步驟I - RADIUS啟用身份驗證](#)
[步驟J - TACACS+啟用授權](#)
[步驟K - Kerberos驗證](#)
[Cisco出版書籍](#)
[增強安全的ip permit命令](#)
[在Catalyst上調試](#)
[相關資訊](#)

簡介

Cisco Catalyst系列交換機（運行CatOS的Catalyst 4000、Catalyst 5000和Catalyst 6000）已支援某種形式的身份驗證（以2.2代碼開頭）。在更高的版本中加入了增強功能。用於身份驗證、授權和記帳(AAA)的TACACS+ TCP埠49，而不是XTACACS使用者資料包協定(UDP)埠49)、RADIUS或Kerberos伺服器使用者設定與路由器使用者設定相同。本文包含啟用這些功能所需的最少命令的示例。相關版本的交換機文檔中提供了其他選項。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

由於較新版本的代碼支援其他選項，因此需要發出**show version**命令來確定交換機上的代碼版本。一旦確定了交換機上使用的代碼版本，請使用下表來確定您的裝置上可用的選項以及要配置的選項。

新增驗證和授權時，請始終保留在交換機中。在另一個視窗中測試配置，以避免被意外鎖定。

方法（最小）	**Cat版本2.2到5.1**	**Cat版本5.1到5.4.1**	**Cat版本5.4.1到7.5.1**	**Cat版本7.5.1及更高版本**
TACACS+驗證或	步驟A	步驟A	步驟A	步驟A
RADIUS驗證或	不適用	步驟B	步驟B	步驟B
Kerberos驗證或	不適用	不適用	步驟K	步驟K
本地使用者名稱身份驗證/授權	不適用	不適用	不適用	步驟C
Plus（選項）				
TACACS+命令授權	不適用	不適用	步驟D	步驟D
TACACS+ Exec授權	不適用	不適用	步驟E	步驟E
RADIUS Exec授權	不適用	不適用	步驟F	步驟F
計量 — TACACS+或RADIUS	不適用	不適用	步驟G	步驟G
TACACS+啟用授權	步驟H	步驟H	步驟H	步驟H
RADIUS啟用授權	不適用	步驟I	步驟I	步驟I
TACACS+啟用授權	不適用	不適用	步驟J	步驟J

配置步驟

步驟A - TACACS+驗證

在早期版本的代碼中，命令並不像某些較新版本那樣複雜。較新版本中的其他選項可在交換器上使用。

1. 發出**set authentication login local enable**命令，以確保在伺服器關閉時交換機有後門。
2. 發出**set authentication login tacacs enable**命令以啟用TACACS+身份驗證。
3. 發出**set tacacs server #.#.#.#**命令以定義伺服器。
4. 發出**set tacacs key *your_key*** 命令以定義伺服器金鑰（在TACACS+中是選用的），因為它會導致交換器到伺服器資料加密。如果使用，則必須與伺服器一致。**註：**Cisco Catalyst OS軟體**不**接受問號(?)**是**任何金鑰或密碼的一部分。問號明確用於有關命令語法的幫助。

步驟B - RADIUS驗證

在早期版本的代碼中，命令並不像某些較新版本那樣複雜。較新版本中的其他選項可在交換器上使用。

1. 發出**set authentication login local enable**命令，以確保在伺服器關閉時交換機有後門。
2. 發出**set authentication login radius enable**命令以啟用RADIUS身份驗證。
3. 定義伺服器。在所有其他思科裝置上，預設RADIUS埠為1645/1646（身份驗證/記帳）。在Catalyst上，預設埠是1812/1813。如果您使用Cisco Secure或與其他思科裝置通訊的伺服器，請使用1645/1646埠。發出**set radius server #.#.#.# auth-port 1645 acct-port 1646 primary**命令，將伺服器和在Cisco IOS中的對應命令定義為**radius-server source-ports 1645-1646**。
4. 定義伺服器金鑰。這是強制性的，因為它會按照RADIUS驗證/授權RFC 2865 和RADIUS計量RFC 286 中的說明加密交換器到伺服器的密碼。如果使用，則必須與伺服器一致。發出**set radius key *your_key*** 指令。

步驟C — 本地使用者名稱身份驗證/授權

從CatOS版本7.5.1開始，可以進行本地使用者身份驗證。例如，您可以使用儲存在Catalyst上的使用者名稱和密碼來實現身份驗證/授權，而不是使用本地密碼進行身份驗證。

本地使用者身份驗證只有兩個許可權級別：0或15。0級是非特權exec級別。Level 15是特權啟用級別。

如果您在此範例中新增這些命令，則使用者`poweruser`會到達交換器的Telnet或主控台上的啟用模式，而使用者`nonenable`會到達交換器的Telnet或主控台上的exec模式。

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

注意：如果使用者`nonenable`知道**set enable** password，則該使用者可以繼續啟用模式。

設定完成後，密碼會以加密方式儲存。

本地使用者名稱身份驗證可以與遠端TACACS+ exec、命令記帳或遠端RADIUS exec記帳結合使用。它還可以與遠端TACACS+ exec或命令授權結合使用，但以這種方式使用它沒有意義，因為使用

者名稱既需要儲存在TACACS+伺服器上，也需要儲存在本地交換機上。

步驟D - TACACS+命令授權

在本範例中，交換器被告知僅需要使用TACACS+的組態指令進行授權。在TACACS+伺服器關閉的情況下，身份驗證為無。這同時適用於主控台連線埠和Telnet作業階段。發出以下命令：

set authorization commands enable config tacacs none both

在此範例中，您可以設定以下引數時，將TACACS+伺服器設定為允許：

```
command=set
arguments (permit)=port 2/12
```

set port enable 2/12命令會傳送到TACACS+伺服器進行驗證。

注意：啟用命令授權後，與路由器中不會將enable視為命令的情況不同，交換機在嘗試啟用時將命令**enable**傳送到伺服器。確保伺服器也配置為允許**enable**命令。

步驟E - TACACS+ Exec授權

在本範例中，交換器被告知需要使用TACACS+的exec作業階段進行授權。當TACACS+伺服器關閉時，授權為無。這同時適用於主控台連線埠和Telnet作業階段。發出**set authorization exec enable tacacs+ none both**命令

除了驗證要求外，這也會從交換器向TACACS+伺服器傳送獨立的授權要求。如果在TACACS+伺服器上將使用者配置檔案配置為shell/exec，則該使用者能夠訪問交換機。

這樣可防止伺服器上未配置shell/exec服務的使用者（例如PPP使用者）登入到交換機。您會收到一條消息，顯示`Exec mode authorization failed`。除了允許/拒絕使用者的執行模式外，當您使用伺服器上分配的許可權級別15進入時，還可以強制進入啟用模式。必須執行已修正Cisco錯誤ID CSCdr51314(僅限註冊客戶)的代碼。

步驟F - RADIUS Exec授權

沒有命令可啟用RADIUS exec授權。另一種方法是在RADIUS伺服器中將Service-Type（RADIUS屬性6）設定為Administrative（值6），以便在RADIUS伺服器中將使用者啟動到啟用模式。如果服務型別設定為除6管理模式以外的其他型別（例如1登入、7外殼或2框架），則使用者會到達交換機exec提示，但不到達啟用提示。

在交換器中新增以下命令以進行驗證和授權：

```
aaa authorization exec TEST group radius
 line vty 0 4
 authorization exec TEST
 login authentication TEST
```

步驟G — 記帳 — TACACS+或RADIUS

若要對以下專案啟用TACACS+計量：

1. 如果收到交換器提示，請發出**set accounting exec enable start-stop tacacs+**指令。

2. 通過Telnet離開交換機的使用者發出**set accounting connect enable start-stop tacacs+**命令。
3. 如果重新啟動交換器，請發出**set accounting system enable start-stop tacacs+**指令。
4. 執行命令的使用者發出**set accounting commands enable all start-stop tacacs+**命令。
5. 提醒伺服器，例如，每分鐘更新一次記錄以顯示使用者仍登入，請發出**set accounting update periodic 1** 命令。

若要對以下專案啟用RADIUS計量：

1. 獲得交換機提示的使用者發出**set accounting exec enable start-stop radius**命令。
2. 通過Telnet從交換機發出的使用者發出**set accounting connect enable start-stop radius**命令。
3. 重新啟動交換器時，發出**set accounting system enable start-stop radius**指令。
4. 提醒伺服器，例如，每分鐘更新一次記錄以顯示使用者仍然登入，請發出**set accounting update periodic 1** 命令。

TACACS+免費軟體記錄

以下輸出是記錄如何在伺服器上顯示的示例：

```
Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=5 start_time=953936729 timezone=UTC
service=shell disc-cause=2 elapsed_time=236
Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=15 start_time=953936975 timezone=UTC
service=shell priv-lvl=0 cmd=enable
Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=16 start_time=953936979 timezone=UTC
service=shell priv-lvl=15 cmd=write terminal
Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=17 start_time=953936984 timezone=UTC
service=shell priv-lvl=15 cmd=show version
Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
171.68.118.100 update task_id=14 start_time=953936974 timezone=UTC
service=shell
```

UNIX上的RADIUS記錄輸出

以下輸出是記錄如何在伺服器上顯示的示例：

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Start
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
```

```
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Stop
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Session-Time = 9
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Received unknown attribute 49
Acct-Session-Time = 30
Acct-Delay-Time = 0
```

步驟H - TACACS+啟用身份驗證

請完成以下步驟：

1. 發出**set authentication enable local enable**命令，以確保在伺服器關閉時存在後門。
2. 發出**set authentication enable tacacs enable**命令，以告知交換器將啟用要求傳送到伺服器。

步驟I - RADIUS啟用身份驗證

新增以下命令可讓交換器將使用者名稱$enab15$傳送到RADIUS伺服器。並非所有RADIUS伺服器都支援這種使用者名稱。有關另一個替代方法，請參閱步驟E，例如，如果將服務型別[RADIUS屬性6 — 設定為管理]，則會將單個使用者啟動到啟用模式。

1. 發出**set authentication enable local enable**命令，以確保在伺服器關閉時存在後門。
2. 如果您的RADIUS伺服器支援$enab15$使用者名稱，發出**set authentication enable radius enable**命令，以告知交換器將啟用要求傳送到伺服器。

步驟J - TACACS+啟用授權

新增此命令會導致交換機在使用者嘗試啟用時向伺服器傳送enable。伺服器需要允許**enable**命令。在本示例中，如果伺服器發生故障，則故障切換到none:

set auth enable enable tacacs+ none both

步驟K - Kerberos驗證

有關如何對交換機設定Kerberos的詳細資訊，請參閱使用身份驗證、授權和記帳控制和監視對交換機的訪問。

Cisco出版書籍

如需密碼復原程式的詳細資訊，請參閱密碼復原程式。

此頁是思科產品的密碼復原程式索引。

增強安全的ip permit命令

為了增強安全性，可以將Catalyst配置為通過**ip permit**命令控制Telnet訪問：

set ip permit enable telnet

set ip permit *range mask*|*host*

這僅允許指定通過Telnet連線到交換機的範圍。

在Catalyst上調試

在Catalyst上啟用調試之前，請檢查伺服器日誌以瞭解失敗的原因。這樣更容易，對交換機的干擾更少。在較早的交換器版本上，**debug**是在工程模式中執行的。在更高版本的代碼中，無需訪問工程模式即可執行**debug**命令：

set trace tacacs|radius|kerberos 4

注意：set trace tacacs|radius|kerberos 0命令將Catalyst返回到無跟蹤模式。

如需多層LAN交換器的詳細資訊，請參閱交換器產品支援頁面。

相關資訊

- TACACS+ 和 RADIUS 比較
- Cisco IOS檔案中的RADIUS、TACACS+和Kerberos
- RADIUS 支援頁面
- TACACS/TACACS+ 支援頁面
- Kerberos支援頁面
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems