在接入伺服器上配置基本AAA

目錄

簡介

本檔案介紹如何在使用Radius或TACACS+通訊協定的思科路由器上設定驗證、授權和計量(AAA)。

必要條件

需求

本文件沒有特定需求。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

採用元件

本檔案中的資訊是根據Cisco IOS®軟體版本12主行。

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。

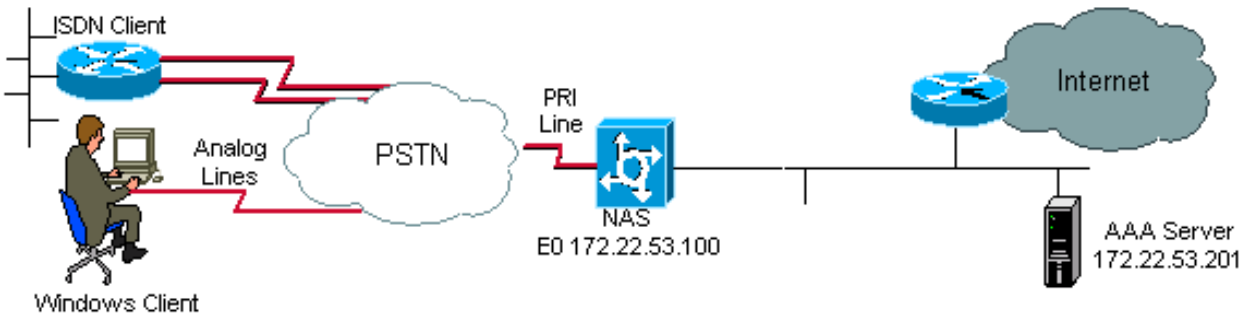
背景資訊

本檔案將說明如何在使用Radius或TACACS+通訊協定的思科路由器上設定驗證、授權和計量(AAA)。本文件的目標並非涵蓋所有 AAA 功能，而是說明主要指令，並提供範例和指南。

> **附註**：繼續進行Cisco IOS配置之前，請閱讀有關AAA常規配置的一節。否則可能會導致組態錯誤和後續封鎖。

有關詳細資訊，請參閱身份驗證、授權和記帳配置指南。

網路圖表



網路圖表

常規AAA配置

啟用AAA

要啟用AAA，需要在全域性配置中配置 **aaa new-model**命令。

附註：在啟用此命令之前，所有其他AAA命令都處於隱藏狀態。

警告： aaa new-model 命令立即將本地身份驗證應用於所有線路和介面(控制檯線路**line con 0除外**)。 如果啟用此命令（或如果連線超時且必須重新連線），則使用者必須通過路由器的本地資料庫進行身份驗證。建議在啟動AAA配置之前，在接入伺服器上定義使用者名稱和密碼，這樣就不會鎖定在路由器之外。請參見下一個代碼示例。

```
Router(config)#username xxx password yyy
```

提示：配置AAA命令之前， save 您的配置。您可以 save 僅在完成AAA配置後再次進行配置（並確信其運行正常）。 這樣您就可以從意外的鎖定中恢復，因為您可以重新載入路由器來回滾任何更改。

指定外部AAA伺服器

在全域組態中，定義與AAA一起使用的安全通訊協定(Radius、TACACS+)。 如果不想使用這兩種協定中的任一種，則可以使用路由器上的本地資料庫。

如果使用TACACS+，請使用 **tacacs-server host** <IP address of the AAA server> <key> 命令。

如果使用Radius，請使用 **radius-server host <IP address of the AAA server> <key>** 命令。

AAA伺服器組態

在AAA伺服器上，配置以下引數：

- 訪問伺服器的名稱。
- 訪問伺服器用於與AAA伺服器通訊的IP地址。**附註**：如果兩台裝置位於同一個乙太網路中，則預設情況下，訪問伺服器在傳送AAA資料包時使用乙太網介面上定義的IP地址。當路由器有多個介面（因此有多個地址）時，此問題非常重要。
- 與訪問伺服器中配置的**<key>**完全相同。**附註**：金鑰區分大小寫。
- 存取伺服器使用的通訊協定（TACACS+或Radius）。

有關用於配置先前引數的確切過程，請參閱AAA伺服器文檔。如果AAA伺服器配置不正確，則AAA伺服器可以忽略來自NAS的AAA請求，並且連線可能會失敗。

AAA伺服器必須可從存取伺服器以IP方式連線(執行**ping**測試以驗證連線)。

驗證設定

身份驗證會在使用者被允許訪問網路和網路服務之前對其進行驗證（通過授權進行驗證）。

配置AAA身份驗證：

1. 首先定義身份驗證方法的命名清單（在全域性配置模式下）。
2. 將該清單應用到一個或多個介面（在介面配置模式下）。

唯一的例外是預設方法清單(名為**default**)。 預設方法清單會自動應用於所有介面，但顯式定義了命名方法清單的介面除外。定義的方法清單會覆蓋預設的方法清單。

這些驗證範例使用Radius、登入和點對點通訊協定(PPP)驗證來解釋概念，例如方法和命名清單。在所有範例中，TACACS+都可以替代Radius或本機驗證。

Cisco IOS軟體使用所列的第一種方法對使用者進行驗證。如果該方法無法響應（以ERROR表示），Cisco IOS軟體將選擇方法清單中列出的下一個身份驗證方法。此過程會一直持續，直到與列出的身份驗證方法成功通訊，或者方法清單中定義的所有方法都已用盡。

必須注意的是，只有在沒有來自前一方法的響應時，Cisco IOS軟體才會嘗試使用列出的下一個身份驗證方法進行身份驗證。如果身份驗證在此循環中的任何時刻失敗，即如果AAA伺服器或本地使用者名稱資料庫響應拒絕使用者訪問（由FAIL指示），則身份驗證過程將停止，並且不會嘗試任何其他身份驗證方法。

要允許使用者身份驗證，必須在AAA伺服器上配置使用者名稱和密碼。

登入驗證

您可以使用 aaa authentication login命令對想要exec訪問訪問訪問伺服器（tty、vty、控制檯和aux）的使用者進行身份驗證。

範例 1：使用Radius然後使用本地EXEC訪問

```
Router(config)#aaa authentication login default group radius local
```

在上面的命令中：

- 命名清單是預設清單（預設）。
- 有兩種驗證方法（群組radius和本地）。

所有使用者都使用Radius伺服器（第一種方法）進行驗證。 如果Radius伺服器沒有響應，則使用路由器本地資料庫（第二種方法）。 對於本地身份驗證，請定義使用者名稱名稱和密碼：

```
Router(config)#username xxx password yyy
```

由於使用了 aaa authentication login 命令中的預設清單，因此所有登入連線（如tty、vty、控制檯和aux）將自動應用登入身份驗證。

> **附註**：如果沒有IP連線，或者在AAA伺服器上沒有正確定義訪問伺服器或在訪問伺服器上沒有正確定義AAA伺服器，則伺服器（Radius或TACACS+）無法回覆訪問伺服器傳送的**aaa身份驗證**請求。

> **附註**：如果使用上一個示例(不帶**local**關鍵字)，則結果為：

```
Router(config)#aaa authentication login default group radius
```

> **附註**：如果AAA伺服器沒有回覆身份驗證請求，則身份驗證失敗（因為路由器沒有備用方法可嘗試）。

> **附註**： group關鍵字提供了一種將當前伺服器主機分組的方法。該功能允許使用者選擇已配置

的伺服器主機的子集並將其用於特定服務。

範例 2：控制檯訪問與線路口令一起使用

從示例1展開配置，以便控制檯登入僅通過線路con 0上設定的口令進行身份驗證。

將定義清單CONSOLE，然後將其應用於line con 0。

組態:

```
Router(config)#aaa authentication login CONSOLE line
```

在上面的命令中：

- 命名清單為CONSOLE。
- 只有一個身份驗證方法（線路）。

建立命名清單（在本例中為CONSOLE）時，必須在行或介面上應用該清單，然後才能執行該清單。這是通過 login authentication 指令:

```
Router(config)#line con 0
Router(config-line)#exec-timeout 0 0
Router(config-line)#password cisco
Router(config-line)#login authentication CONSOLE
```

CONSOLE清單會覆蓋第0行上的預設方法清單**預設值**。在第0行上進行此配置後，您需要輸入口令**cisco**來獲取控制檯訪問許可權。預設清單仍用於tty、vty和aux。

附註：要通過本地使用者名稱和密碼驗證控制檯訪問，請使用下一個代碼示例：

```
Router(config)#aaa authentication login CONSOLE local
```

在這種情況下，必須在路由器的本地資料庫中配置使用者名稱和口令。該清單還必須應用於線路或介面。

附註：要無身份驗證，請使用下一個代碼示例：

```
Router(config)#aaa authentication login CONSOLE none
```

在這種情況下，沒有身份驗證可訪問控制檯。該清單還必須應用於線路或介面。

範例 3:與外部AAA伺服器一起使用的啟用模式訪問

您可以發出身份驗證以進入啟用模式（特權15）。

組態:

```
Router(config)#aaa authentication enable default group radius enable
```

只能請求密碼，使用者名稱是$enab15$。因此，必須在AAA伺服器上定義使用者名稱$enab15$。

如果Radius伺服器沒有回應，則可能必須輸入路由器上本地設定的啟用密碼。

PPP驗證

aaa authentication ppp 命令用於驗證PPP連線。它通常用於對希望通過訪問伺服器訪問Internet或中央辦公室的ISDN或模擬遠端使用者進行身份驗證。

範例 1：適用於所有使用者的單一PPP身份驗證方法

接入伺服器具有配置為接受PPP撥入客戶端的ISDN介面。我們使用dialer rotary-group 0，但配置可以在主介面或撥號程式配置檔案介面上完成。

組態:

```
Router(config)#aaa authentication ppp default group radius local
```

此命令使用Radius驗證所有PPP使用者。如果Radius伺服器沒有應答，則使用本地資料庫。

範例 2：與特定清單一起使用的PPP身份驗證

要使用命名清單而不是預設清單，請配置以下命令：

```
Router(config)#aaa authentication ppp ISDN_USER group radius

Router(config)#interface dialer 0
Router(config-if)#ppp authentication chap ISDN_USER
```

在本示例中，清單為ISDN_USER，方法為Radius。

範例 3:在字元模式會話中啟動PPP

接入伺服器具有內建數據機卡（Mica、Microcom或下一埠）。 假設已配置aaa authentication login和aaa authentication ppp命令。

如果數據機使用者首先使用字元模式exec會話訪問路由器（例如，撥號後使用終端視窗），則使用者在tty線路上進行身份驗證。要啟動資料包模式會話，使用者必須鍵入ppp default 或ppp。由於已明確配置PPP身份驗證(使用aaa authentication ppp)，因此使用者再次在PPP級別進行身份驗證。

要避免此第二次身份驗證，請使用if-needed關鍵字：

```
Router(config)#aaa authentication login default group radius local
Router(config)#aaa authentication ppp default group radius local if-needed
```

附註：如果客戶端直接啟動PPP會話，則直接執行PPP身份驗證，因為無法訪問訪問伺服器。

配置授權

授權是您可以用來控制使用者可執行的操作的過程。

AAA授權具有與身份驗證相同的規則：

1. 首先定義授權方法的命名清單。
2. 然後將該清單應用到一個或多個介面（預設方法清單除外）。
3. 使用列出的第一種方法。如果它沒有響應，則使用第二個響應，以此類推。

方法清單特定於請求的授權型別。本文檔重點介紹Exec和網路授權型別。

有關其他授權型別的詳細資訊，請參閱Cisco IOS安全配置指南。

Exec授權

aaa authorization exec 命令確定是否允許使用者運行EXEC shell。此工具可以返回使用者配置檔案資訊，如自動命令資訊、空閒超時、會話超時、訪問清單和許可權以及其他按使用者因素。

執行授權僅通過vty和tty線路執行。

下一個示例使用Radius。

範例 1：所有使用者使用相同的Exec身份驗證方法

使用驗證時：

```
Router(config)#aaa authentication login default group radius local
```

要登入到訪問伺服器的所有使用者必須使用Radius（第一種方法）或本地資料庫（第二種方法）進行授權。

組態:

```
Router(config)#aaa authorization exec default group radius local
```

附註：在AAA伺服器上，必須選擇Service-Type=1（登入）。

附註：在本例中，如果未包括**local**關鍵字，且AAA伺服器未響應，則無法進行授權，連線可能會失敗。

附註：在下一個示例2和3中，您無需在路由器上新增任何命令。您只需在訪問伺服器上配置配置檔案。

範例 2：從AAA伺服器分配Exec許可權級別

根據示例1，在AAA伺服器上配置下一個思科AV配對，以便使用者可以登入訪問伺服器並直接進入啟用模式：

```
shell:priv-lvl=15
```

使用者現在可以直接前往啟用模式。

> **附註**：如果第一種方法無法響應，則使用本地資料庫。但是，使用者無法直接前往啟用模式，但必須輸入enable命令並提供**enable** 密碼。

範例 3:從AAA伺服器分配空閒超時

要配置空閒超時（以便會話在空閒超時後沒有流量時斷開），請使用IETF Radius屬性28:使用者配置檔案下的Idle-Timeout。

網路授權

其 **aaa authorization network** 命令對所有與網路相關的服務請求（如PPP、SLIP和ARAP）運行授權。本節重點介紹最常用的PPP。

AAA伺服器會檢查使用者端是否允許PPP作業階段。此外，客戶端可以請求PPP選項：回撥、壓縮、IP地址等。必須在AAA伺服器上的使用者配置檔案中配置這些選項。此外，對於特定客戶端，AAA配置檔案可以包含閒置超時、訪問清單和其他每使用者屬性，這些屬性可以通過Cisco IOS軟體下載並應用於該客戶端。

下一個範例顯示使用Radius的授權。

範例 1：所有使用者使用相同的網路授權方法

接入伺服器用於接受PPP撥入連線。

使用者會透過以下方式進行驗證（如先前所設定）：

```
Router(config)#aaa authentication ppp default group radius local
```

使用下一個命令授權使用者：

```
Router(config)#aaa authorization network default group radius local
```

> **附註**：在AAA伺服器上，設定： **Service-Type=7(**framed)和**Framed-Protocol=PPP**。

範例 2：應用使用者特定屬性

您可以使用AAA伺服器分配每使用者屬性，例如IP地址、回撥號碼、撥號器空閒超時值或訪問清單

等。在這種實施中，NAS從AAA伺服器使用者配置檔案中下載適當的屬性。

範例 3:使用特定清單的PPP授權

與驗證類似，請設定清單名稱，而不是預設名稱：

```
Router(config)#aaa authorization network ISDN_USER group radius local
```

然後將此清單套用至介面：

```
Router(config)#interface dialer 0
Router(config-if)#ppp authorization ISDN_USER
```

記帳配置

AAA記帳功能使您能夠跟蹤使用者訪問的服務及其使用的網路資源數量。

AAA記帳的規則與身份驗證和授權相同：

1. 必須首先定義會計方法的命名清單。
2. 然後將該清單應用到一個或多個介面（預設方法清單除外）。
3. 使用列出的第一個方法，如果它沒有響應，則使用第二個方法等。

- 網路記帳提供所有PPP、Slip和AppleTalk遠端存取通訊協定(ARAP)作業階段的相關資訊：資料包計數、八位計數、會話時間、開始和停止時間。
- Exec記帳提供有關網路訪問伺服器的使用者EXEC終端會話（例如telnet會話）的資訊：會話時間、開始和停止時間。

接下來的示例重點介紹如何將資訊傳送到AAA伺服器。

記帳配置示例

範例 1：生成開始和停止記帳記錄

對於每個撥入PPP會話，一旦客戶端通過身份驗證，並在斷開連線後使用關鍵字start-stop將記帳資訊傳送到AAA伺服器。

```
Router(config)#aaa accounting network default start-stop group radius local
```

範例 2：僅生成停止記帳記錄

如果必須在客戶端斷開連線後傳送記帳資訊，請使用關鍵字 stop並配置下一行：

```
Router(config)#aaa accounting network default stop group radius local
```

示例3：生成身份驗證和協商失敗的資源記錄

在此之前，AAA記帳為已通過使用者身份驗證的呼叫提供啟動和停止記錄支援。

如果身份驗證或PPP協商失敗，則沒有身份驗證記錄。

解決方案是使用AAA資源故障停止記帳：

```
Router(config)#aaa accounting send stop-record authentication failure
```

停止記錄被傳送到AAA伺服器。

範例 4:啟用完整資源記帳

要啟用在呼叫建立時生成開始記錄和在呼叫終止時生成停止記錄的完整資源記帳，請配置：

```
Router(config)#aaa accounting resource start-stop
```

此命令是在Cisco IOS軟體版本12.1(3)T中匯入。

使用此命令，呼叫建立和呼叫斷開開始 — 停止記帳記錄將跟蹤與裝置的資源連線的進度。單獨的使用者身份驗證開始 — 停止記帳記錄跟蹤使用者管理進度。這兩組記帳記錄與呼叫的唯一會話ID相互關聯。

相關資訊

- 技術支援 - 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）。