

使用Test AAA Radius命令驗證Radius伺服器連線

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[功能運作方式](#)

[指令語法](#)

[場景1：身份驗證嘗試通過](#)

[場景2：身份驗證嘗試失敗](#)

[案例3: WLC和Radius伺服器之間的通訊失敗](#)

[案例4: Radius後援](#)

[注意事項](#)

[相關資訊](#)

簡介

本檔案將介紹 `test aaa radius` 命令可識別radius伺服器連線和客戶端身份驗證問題。

必要條件

需求

思科建議您瞭解無線LAN控制器(WLC)代碼8.2及更新版本。

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。

背景資訊

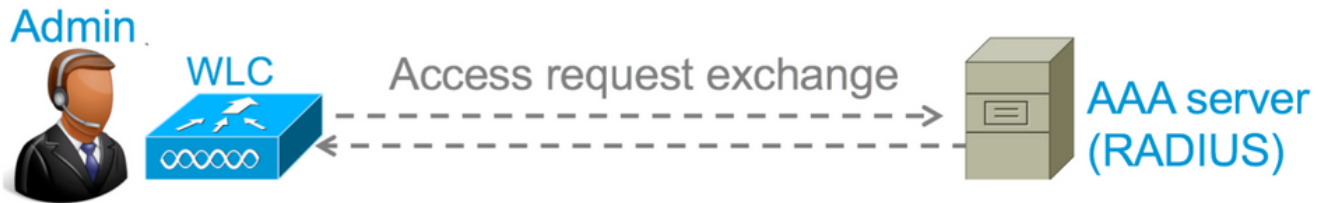
無線客戶端身份驗證問題是無線網路工程師所面臨的最困難的問題之一。為了進行故障排除，通常需要找到有問題的客戶端，與對無線網路一無所知的終端使用者合作，並收集調試和捕獲。在日益重要的無線網路中，這可能導致大量停機。

到目前為止，沒有簡單的方法可以識別身份驗證失敗是由拒絕客戶端的radius伺服器造成的，還是僅僅是因為可達性問題造成的。其 `test aaa radius` 命令允許您執行上述操作。現在，您可以遠端驗證

WLC-RADIUS伺服器通訊是否失敗，或者客戶端的憑證是否導致身份驗證通過或失敗。

功能運作方式

這是使用命令時的基本工作流程 `test aaa radius` 中，如圖所示。



步驟 1. WLC會向radius伺服器傳送存取要求訊息，並連同介面清單中提到的引數 `test aaa radius` 指令：

```
( 思科控制器 ) > test aaa radius username
```

```
password
```

```
wlan-id
```

```
apgroup
```

```
server-index
```

範例

```
<#root>
```

```
test aaa radius username admin password cisco123 wlan-id 1 apgroup default-group server-index 2
```

步驟 2. Radius伺服器會驗證提供的憑證並提供驗證要求的結果。

指令語法

需要提供以下引數才能執行命令：

```
( 思科控制器 ) > test aaa radius username
```

```
password
```

wlan-id

apgroup

server-index

<username> ---> Username that you are testing.
<password> ---> Password that you are testing
<wlan-id> ---> WLAN ID of the SSID that you are testing.
<apgroup-name> (optional) ---> AP group name. This will be default-group if there is no AP group co
<server-index> (optional) ---> The server index configured for the radius server that you are tryin

場景1：身份驗證嘗試通過

現在來看看命令如何運作，以及當命令執行時 `test aaa radius` 命令會導致通過身份驗證。執行命令時，WLC顯示其傳送存取要求所使用的引數：

<#root>

(Cisco Controller) >

```
test aaa radius username admin password cisco123 wlan-id 1 apgroup default-group server-index 2
```

Radius Test Request

Wlan-id.....	1
ApGroup Name.....	default-group
Attributes	Values
-----	-----
User-Name	admin
Called-Station-Id	00:00:00:00:00:00:WLC5508
Calling-Station-Id	00:11:22:33:44:55
Nas-Port	0x0000000d (13)
Nas-IP-Address	10.20.227.39
NAS-Identifier	WLC_5508
Airespace / WLAN-Identifier	0x00000001 (1)
User-Password	cisco123
Service-Type	0x00000008 (8)
Framed-MTU	0x00000514 (1300)
Nas-Port-Type	0x00000013 (19)
Tunnel-Type	0x0000000d (13)
Tunnel-Medium-Type	0x00000006 (6)
Tunnel-Group-Id	0x00000051 (81)
Cisco / Audit-Session-Id	ad14e327000000c466191e23
Acct-Session-Id	56131b33/00:11:22:33:44:55/210

test radius auth request successfully sent. Execute 'test aaa show radius' for response

要檢視身份驗證請求的結果，您需要執行命令 `test aaa show radius`。如果RADIUS伺服器無法連線且WLC需要重試或回退到其他RADIUS伺服器，則此命令可能需要一段時間才能顯示輸出。


```
<#root>
(Cisco Controller) >
test aaa show radius

Radius Test Request
  Wlan-id..... 1
  ApGroup Name..... default-group
  Server Index..... 2
Radius Test Response
Radius Server      Retry Status
-----
10.20.227.52      1

Success

Authentication Response:
  Result Code: Success
  Attributes          Values
  -----
  User-Name           admin
  Class                CACS:rs-ac5-6-0-22/230677882/20313
  Session-Timeout     0x0000001e (30)
  Termination-Action  0x00000000 (0)
  Tunnel-Type         0x0000000d (13)
  Tunnel-Medium-Type  0x00000006 (6)
  Tunnel-Group-Id     0x00000051 (81)
```

此命令極為有用的方面是顯示radius伺服器傳回的屬性。可以是重新導向URL和存取控制清單(ACL)。例如，使用中央Web驗證(CWA)或VLAN資訊時，會使用VLAN覆寫。

 **注意：**訪問請求中的使用者名稱/密碼以明文形式傳送到radius伺服器，因此如果流量流經不安全的網路，您需要謹慎使用它。

場景2：身份驗證嘗試失敗

讓我們看看當使用者名稱/密碼輸入導致身份驗證失敗時，輸出是如何顯示的。

```
<#root>
(Cisco Controller) >
test aaa show radius
```

```

Radius Test Request
  Wlan-id..... 1
  ApGroup Name..... default-group
  Server Index..... 2
Radius Test Response
Radius Server          Retry Status
-----
10.20.227.52          1      Success
Authentication Response:
  Result Code:

Authentication failed

-----> This result indicates that the user authentication will fail.
No AVPs in Response

```

在這種情況下，您可以看到連線測試產生了Success，但radius伺服器針對所使用的使用者名稱/密碼組合傳送了access-reject指令。

案例3: WLC和Radius伺服器之間的通訊失敗

```

<#root>

(Cisco Controller) >
test aaa show radius

previous test command still not completed, try after some time

```

您需要等待WLC完成重試，才能顯示輸出。時間可能因配置的重試閾值而異。

```

<#root>

(Cisco Controller) >
test aaa show radius

Radius Test Request
  Wlan-id..... 1
  ApGroup Name..... default-group
  Server Index..... 3
Radius Test Response
Radius Server          Retry Status
-----
10.20.227.72          6      No response received from server
Authentication Response:
  Result Code:

No response received from server

No AVPs in Response

```

在此輸出中，您可以看到WLC已嘗試連線radius伺服器6次，而且如果沒有回應，WLC就會將radius伺服器標籤為無法連線。

案例4: Radius後援

如果您在服務組識別碼(SSID)下設定了多個RADIUS伺服器，但主RADIUS伺服器沒有回應，則WLC會嘗試設定輔助RADIUS伺服器。這會在輸出中非常清楚的顯示，第一個radius伺服器沒有回應，然後WLC嘗試立即回應的第二個radius伺服器。

```
<#root>
(Cisco Controller) >
test aaa show radius

Radius Test Request
  Wlan-id..... 1
  ApGroup Name..... default-group
Radius Test Response
Radius Server          Retry Status
-----
10.20.227.62          6
No response received from server
10.20.227.52          1

Success

Authentication Response:
  Result Code: Success
  Attributes          Values
-----
  User-Name           admin
```

注意事項

- 目前沒有GUI支援。它只是一個命令，只能從WLC執行。
- 驗證僅適用於radius。不能用於TACACS身份驗證。
- 無法使用此方法測試Flexconnect本地身份驗證。

相關資訊

- [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）。