

验证RADIUS服务器连接用测验AAA RADIUS命令

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[功能如何运作](#)

[命令语法](#)

[方案1.合格认证尝试](#)

[方案 2：失败的认证尝试](#)

[情形 3：通信失败在WLC和RADIUS服务器之间](#)

[场景 4：Radius Fallback](#)

[警告](#)

简介

本文描述**测验AAA RADIUS on命令Cisco WLC**如何可以用于识别RADIUS服务器连接，并且客户端验证发出，不用使用无线客户端。

先决条件

要求

思科建议您有知识无线局域网控制器(WLC)代码8.2以上。

使用的组件

本文档不限于特定的软件和硬件版本。

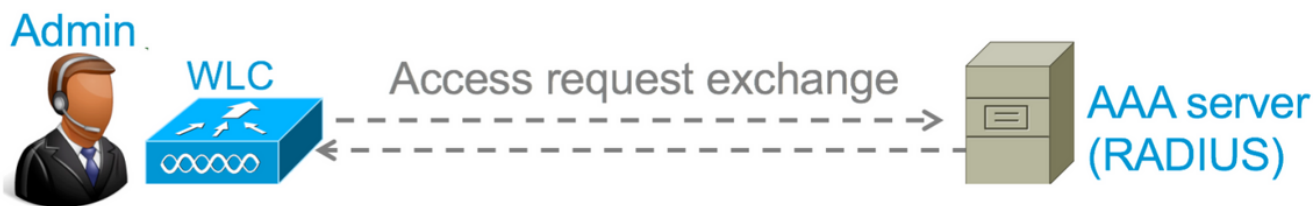
背景信息

无线客户端验证问题是其中最富挑战性的问题无线网络设计表面。为了排除故障此，它经常要求抓住有问题的客户端，工作与可能没有无线网络最好的知识和收集调试和捕获的最终用户。在一个越来越关键无线网络中，这能导致重大的停机时间。

直到现在没有识别的简单的方法，如果认证失败是由拒绝客户端的RADIUS服务器，或者连通性问题造成的。**测验AAA RADIUS命令**让您执行那。您能远程当前验证，如果WLC RADIUS服务器通信发生故障或，如果客户端的凭证导致合格或失败的认证。

功能如何运作

这是基本工作流程，当您使用test命令AAA RADIUS时，如镜像所显示。



步骤1:WLC发送一访问Request信息对在**测验AAA RADIUS**命令被提及的RADIUS服务器与参数一起。

前：**测试AAA RADIUS用户名管理员密码cisco123 wlan-id 1个apgroup默认组服务器索引2**

第二步：RADIUS服务器验证提供的凭证并且提供认证请求的结果。

命令语法

需要提供这些参数执行命令：

(思科控制器) >**测验AAA RADIUS用户名<user name>密码<password> wlan-id <wlan-id> ap-group <apgroup-name>服务器索引<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 configured.
<server-index> (optional)	---	The server index configured for the radius server that you are trying to test. This can be found under Security > Authentication tab.

方案1.合格认证尝试

请查看一下命令如何运作，并且输出被看到，当**测验AAA RADIUS**命令导致一合格验证时。当命令被执行时，WLC显示派出访问请求的参数：

```
(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                0x000000514 (1300)
Nas-Port-Type             0x000000013 (19)
Tunnel-Type               0x00000000d (13)
Tunnel-Medium-Type        0x000000006 (6)
Tunnel-Group-Id           0x000000051 (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

```

为了查看认证请求的结果，您需要执行test命令**aaa show radius**。命令能采取一些时间显示输出，如果RADIUS服务器是不可得到的和WLC需要重试或者fallback到一个不同的RADIUS服务器。

```

(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-accs5-6-0-22/230677882/20313
Session-Timeout           0x00000001e (30)
Termination-Action        0x000000000 (0)
Tunnel-Type               0x00000000d (13)
Tunnel-Medium-Type        0x000000006 (6)
Tunnel-Group-Id           0x000000051 (81)

```

此命令的非常有用的方面是显示属性哪些由RADIUS服务器返回。这可以是重定向URL和访问控制表(ACL)。例如，一旦中央Web验证(CWA)或VLAN信息，当您使用VLAN覆盖。

Caution:在访问请求的用户名/密码在明文发送到RADIUS服务器，因此您需要小心地使用它，如果在非安全网络的通信流。

方案 2：失败的认证尝试

请发现输出如何出现，当用户名/密码条目导致失败的认证。

```

(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 indicates that the user authentication will fail.
No AVPs in Response

```

在这种情况下，您能看到连通性测试导致‘成功的，然而RADIUS服务器发送使用的用户名/密码组合

的访问拒绝。

情形 3 : 通信失败在WLC和RADIUS服务器之间

```
(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 indicates that the user authentication will fail.
  No AVPs in Response
```

在显示输出前，您需要等待WLC完成它是重试次数。时间能变化基于配置的重试次数阈值。

```
(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 indicates that the user authentication will fail.
  No AVPs in Response
```

在上述输出中您能看到设法的WLC联系RADIUS服务器6次，并且，当没有无响应它指示了RADIUS服务器作为不可达的。

场景 4 : Radius Fallback

当您有多个RADIUS服务器配置在服务集标识(SSID)下，并且主要的RADIUS服务器不回应，然后WLC尝试用配置的附属RADIUS服务器。这在第一个RADIUS服务器不回应的输出中非常清楚显示，并且WLC然后尝试第二个RADIUS服务器哪些立即响应。

```
(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 indicates that the user authentication will fail.
  No AVPs in Response
```

警告

- 当前没有GUI支持。它是可以从WLC被执行仅的命令。
- 验证仅是为radius。它不可能用于TACACS认证。
- Flexconnect本地认证不可能用此方法测试。