

# Verifique a Conectividade do servidor Radius com comando dos radius AAA do teste

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Como a característica trabalha](#)

[Sintaxe do comando](#)

[A encenação 1. passou a tentativa de autenticação](#)

[Cenário 2: Tentativa da autenticação falha](#)

[Cenário 3: Uma comunicação falhada entre o WLC e o servidor Radius](#)

[Encenação 4: Reserva do raio](#)

[Caveats](#)

## Introdução

Este documento descreve como o comando dos **radius AAA do teste em** Cisco WLC pode ser usado para identificar edições da Conectividade e da autenticação do cliente do servidor Radius sem o uso de um cliente Wireless.

## Pré-requisitos

### Requisitos

Cisco recomenda que você tem o conhecimento do código 8.2 do controlador do Wireless LAN (WLC) e acima.

### [Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

## Informações de Apoio

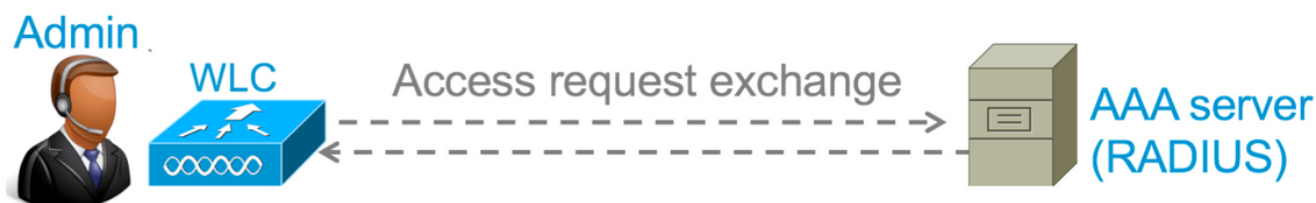
As edições da autenticação de cliente Wireless são um dos problemas os mais desafiantes que a rede Wireless projeta a cara. A fim de pesquisar defeitos isto, exige frequentemente para obter a posse do cliente problemático, trabalhar com os utilizadores finais que não podem ter o melhor conhecimento das redes Wireless e para recolher debug e captura. Em uma rede Wireless cada vez mais crítica, isto pode causar o tempo ocioso da máquina significativo.

Até aqui não havia nenhuma maneira fácil de identificar se uma falha de autenticação foi causada

pelo servidor Radius que rejeita o cliente, ou apenas simplesmente por uma edição da alcançabilidade. O comando dos **radius AAA do teste** deixa-o fazer apenas aquele. Você pode agora remotamente verificar se a comunicação do server do WLC-raio falha ou se as credenciais para o cliente conduzem a uma passada ou a uma autenticação falha.

## Como a característica trabalha

Este é uns trabalhos básicos quando você usa os **radius AAA do** comando test, segundo as indicações da imagem.



Etapa 1. O WLC envia um mensagem request do acesso ao servidor Radius junto com os parâmetros que é mencionado no comando dos **radius AAA do teste**.

Para ex: **teste o server-deslocamento predeterminado 2 do grupo padrão do apgroup WLAN-identificação 1 do cisco123 da senha do admin de nome de usuário dos radius AAA**

Etapa 2. O servidor Radius valida as credenciais fornecidas e fornece os resultados do pedido de autenticação.

## Sintaxe do comando

Estes parâmetros precisam de ser fornecidos para executar o comando:

(Controlador de Cisco) > **<server-index> do server-deslocamento predeterminado do <apgroup-name> do grupo AP do <wlan-id> WLAN-identificação do <password> da senha do name> do <user username dos radius AAA do teste**

<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.

## A encenação 1. passou a tentativa de autenticação

Deixe-nos ter um olhar em como o comando trabalha e as saídas são consideradas quando o comando dos **radius AAA do teste** conduz a uma autenticação passada. Quando o comando é executado, o WLC indica os parâmetros com que manda o pedido do acesso:

```
(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
```

A fim ver os resultados do pedido de autenticação, você precisa de executar o **raio da mostra aaa do comando test**. O comando pode tomar algum tempo para mostrar a saída se um servidor Radius é inacessível e o WLC precisa de experimentar de novo ou reserva a um servidor Radius diferente.

```
(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-acs5-6-0-22/230677882/20313
Session-Timeout     0x0000001e (30)
Termination-Action  0x00000000 (0)
Tunnel-Type         0x0000000d (13)
Tunnel-Medium-Type  0x00000006 (6)
Tunnel-Group-Id     0x00000051 (81)
```

O aspecto extremamente útil deste comando é que mostra aos atributos quais são retornados pelo servidor Radius. Isto pode ser reorienta URL e Access Control List (ACL). Por exemplo, no caso da autenticação da Web central (CWA) ou da informação de VLAN quando você usar a ultrapassagem VLAN.

**Caution:** O username/senha no pedido do acesso é enviado no texto claro ao servidor Radius, assim que você precisa de usá-lo com cuidado se fluxos de tráfego sobre uma rede não protegida.

## Cenário 2: Tentativa da autenticação falha

Deixe-nos ver como a saída aparece quando um username/entrada de senha conduz a uma autenticação falha.

```
(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
```

Neste caso, você pode ver que o teste de conectividade conduziu a um “sucesso”, porém o servidor Radius enviou uma rejeição de acesso para a combinação de nome de usuário/senha usada.

## Cenário 3: Uma comunicação falhada entre o WLC e o servidor Radius

```
(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
```

Você precisa de esperar o WLC para terminá-lo é novas tentativas antes que indique a saída. O tempo pode variar baseado nos pontos iniciais da nova tentativa configurados.

```
(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
```

Na saída acima você pode ver que o WLC tentou contactar os tempos do servidor Radius 6 e quando não havia nenhuma resposta marcou o servidor Radius como inacessível.

## Encenação 4: Reserva do raio

Quando você tem os servidores Radius múltiplos configurados sob o Service Set Identifier (SSID) e o servidor Radius preliminar não responde, a seguir o WLC tenta com o servidor radius secundário configurado. Isto é mostrado muito claramente na saída onde o primeiro servidor Radius não responde e o WLC a seguir tenta o segundo servidor Radius qual responde imediatamente.

```
(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
```

## Caveats

- Não há atualmente nenhum apoio GUI. É somente um comando que possa ser executado do WLC.
- A verificação é somente para o raio. Não pode ser usada para a autenticação TACACS.
- A autenticação local de Flexconnect não pode ser testada com este método.