

Verificar a conectividade do servidor Radius com o comando Test AAA Radius

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Como O Recurso Funciona](#)

[Sintaxe do comando](#)

[Cenário 1. Tentativa de Autenticação Aprovada](#)

[Cenário 2: Falha na tentativa de autenticação](#)

[Cenário 3: Falha na comunicação entre a WLC e o servidor Radius](#)

[Cenário 4 : Fallback de raio](#)

[Caveats](#)

Introduction

Este documento descreve como o comando **test aaa radius** no Cisco WLC pode ser usado para identificar problemas de conectividade de servidor radius e de autenticação de cliente sem o uso de um cliente sem fio.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do código 8.2 da controladora Wireless LAN (WLC) e superior.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

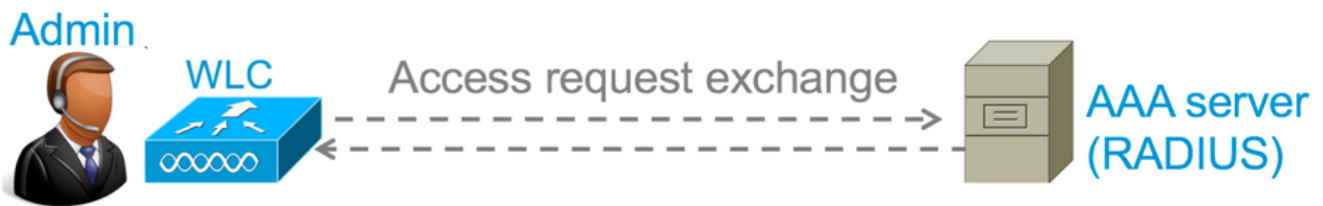
Os problemas de autenticação de cliente sem fio são um dos problemas mais difíceis que os engenheiros de rede sem fio enfrentam. Para solucionar problemas, geralmente é necessário ter o controle do cliente problemático, trabalhar com os usuários finais que não podem ter o melhor

conhecimento das redes sem fio e coletar depurações e capturas. Em uma rede sem fio cada vez mais crítica, isso pode causar um tempo de inatividade significativo.

Até agora não havia uma maneira fácil de identificar se uma falha de autenticação foi causada pelo servidor radius que rejeita o cliente, ou simplesmente um problema de acessibilidade. O comando **test aaa radius** permite fazer exatamente isso. Agora você pode verificar remotamente se a comunicação do servidor WLC-Radius falha ou se as credenciais do cliente resultam em uma autenticação aprovada ou com falha.

Como O Recurso Funciona

Este é um fluxo de trabalho básico quando você usa o comando **test aaa radius**, como mostrado na imagem.



Etapa 1. A WLC envia uma mensagem de solicitação de acesso ao servidor radius junto com os parâmetros mencionados no comando **test aaa radius**.

Por exemplo: **test aaa radius username admin password cisco123 wlan-id 1 apgroup default-group server-index 2**

Etapa 2. O servidor radius valida as credenciais fornecidas e fornece os resultados da solicitação de autenticação.

Sintaxe do comando

Estes parâmetros precisam ser fornecidos para executar o comando:

```
(Controlador Cisco) > test aaa radius username <user name> password <password> wlan-id <wlan-id> apgroup <apgroup-name> server-index <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.
```

Cenário 1. Tentativa de Autenticação Aprovada

Vejamos como o comando funciona e as saídas são vistas quando o comando **test aaa radius** resulta em uma autenticação aprovada. Quando o comando é executado, a WLC exibe os

parâmetros com os quais envia a solicitação de 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
```

Para visualizar os resultados da solicitação de autenticação, você precisa executar o comando **test aaa show radius**. O comando pode levar algum tempo para mostrar a saída se um servidor radius estiver inacessível e a WLC precisar repetir ou fazer fallback para 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-accs5-6-0-22/230677882/20313
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 desse comando é que ele mostra os atributos que são retornados pelo servidor radius. Pode ser o URL de redirecionamento e a Lista de Controle de Acesso (ACL). Por exemplo, no caso de Central Web Authentication (CWA) ou de informações de VLAN quando você usa VLAN override.

Caution: O nome de usuário/senha na solicitação de acesso é enviado em texto claro ao

servidor radius, portanto, você precisa usá-lo com cuidado se o tráfego fluir por uma rede não segura.

Cenário 2: Falha na tentativa de autenticação

Deixe-nos ver como a saída aparece quando uma entrada de nome de usuário/senha resulta em uma falha de autenticação.

```
(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
```

Nesse caso, você pode ver que o teste de conectividade resultou em um 'Sucesso', no entanto, o servidor radius enviou um access-reject para a combinação de nome de usuário/senha usada.

Cenário 3: Falha na comunicação entre a WLC e o servidor Radius

```
(Cisco Controller) >test aaa show radius
previous test command still not completed, try after some time
```

Você precisa esperar até que a WLC termine as novas tentativas antes de exibir a saída. O tempo pode variar com base nos limites de repetição configurados.

```
(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
```

Nesta saída, você pode ver que o WLC tentou entrar em contato com o servidor radius 6 vezes e, quando não houve resposta, ele marcou o servidor radius como inalcançável.

Cenário 4 : Fallback de raio

Quando você tem vários servidores radius configurados no Service Set Identifier (SSID) e o servidor radius primário não responde, a WLC tenta com o servidor radius secundário configurado. Isso é mostrado claramente na saída em que o primeiro servidor radius não responde e a WLC tenta o segundo servidor radius que responde imediatamente.

```
(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
```

Caveats

- Não há suporte para GUI no momento. É apenas um comando que pode ser executado da WLC.
- A verificação é somente para radius. Ele não pode ser usado para autenticação TACACS.
- A autenticação local do Flexconnect não pode ser testada com este método.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.