

Проверьте подключение сервера RADIUS с тестовым AAA Radius

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Как работает функция](#)

[Синтаксис команды](#)

[Сценарий 1. Переданная попытка аутентификации](#)

[Сценарий 2: Неудачная попытка аутентификации](#)

[Ситуация 3: Связь, отказавшая между WLC и сервером RADIUS](#)

[Сценарий 4: нейтрализация радиуса](#)

[Предупреждения](#)

Введение

Этот документ описывает, как **тестовый AAA Radius** на WLC Cisco может использоваться для определения подключения сервера RADIUS и проблем аутентификации клиента без использования беспроводного клиента.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с кодом 8.2 Контроллера беспроводной локальной сети (WLC) и выше.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

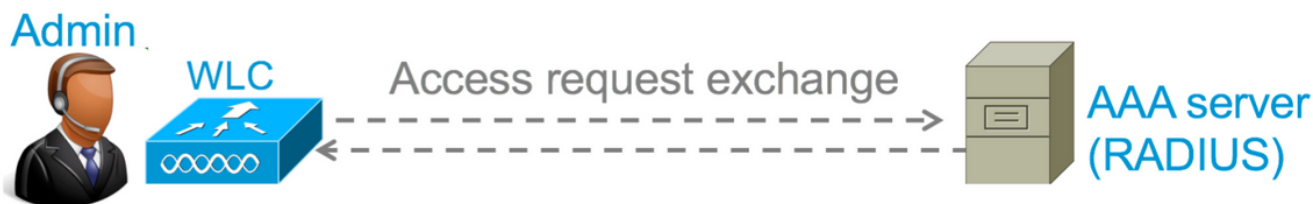
Общие сведения

Проблемы аутентификации беспроводного клиента являются одной из самых стимулирующих проблем та беспроводная сеть, с которой сталкиваются инженеры. Для устранения проблем этого это часто требует, чтобы овладеть проблематичным клиентом, работать с конечными пользователями, у которых может не быть лучшего знания беспроводных сетей и собирать отладки и перехваты. Во все более и более важной беспроводной сети это может вызвать значительное время простоя.

Вплоть до сих пор не было никакого простого способа, чтобы определить, если ошибка проверки подлинности была вызвана сервером RADIUS, который отклоняет клиента, или просто проблему достижимости. **Тестовый AAA Radius** позволяет вам сделать просто это. Можно теперь удаленно проверить, отказывает ли связь сервера RADIUS WLC или если учетные данные для клиента приводят к переданному или ошибке проверки подлинности.

Как работает функция

Это - основной поток операций при использовании радиуса команды `test aaa`, как показано в образе.



Шаг 1. WLC передает сообщение запроса доступа к серверу RADIUS наряду с параметрами, который упомянут в тестовом AAA Radius.

Поскольку исключая: тестовый wlan-идентификатор пароля администратора cisco123 имени пользователя RADIUS aaa 1 apgroup индекс сервера 2 группы по умолчанию

Шаг 2. Сервер RADIUS проверяет предоставленные учетные данные и предоставляет результаты запроса аутентификации.

Синтаксис команды

Эти параметры должны быть предоставлены для выполнения команды:

(Cisco Controller)> тестирует имя пользователя RADIUS aaa <имя пользователя> wlan-идентификатор <password> пароля <wlan-идентификатор> ap-group <индекс сервера apgroup-name-> <индекс сервера>

```
<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.
```

Сценарий 1. Переданная попытка аутентификации

Давайте взглянем на то, как команда работает, и выходные данные замечены, когда тестовый AAA Radius приводит к переданной аутентификации. Когда команда выполняется, WLC отображает параметры, с которыми это отсылает запрос доступа:

```

(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-Identifler                           WLC_5508
Airespace / WLAN-Identifler              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

```

Для просмотра результатов запроса аутентификации необходимо выполнить **show radius** команды **test aaa**. Команда может занять время для показа выходных данных, если сервер RADIUS недостижим, и WLC должен повторить или нейтрализация к другому серверу 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: 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)

```

Чрезвычайно полезный аспект этой команды - то, что она показывает атрибуты, которые возвращены сервером RADIUS. Это может быть URL перенаправления и Списком контроля доступа (ACL). Например, в случае Центральной веб-аутентификации (CWA) или информации VLAN, когда вы используете замену VLAN.

Внимание. : Имя пользователя/пароль в запросе доступа передается в открытом тексте серверу RADIUS, таким образом, необходимо использовать его с осторожностью если трафики по незащищенной сети.

Сценарий 2: Неудачная попытка аутентификации

Давайте посмотрим, как выходные данные появляются, когда имя пользователя/ввод пароля приводит к ошибке проверки подлинности.

```
(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
```

В этом случае вы видите, что тест подключения привел к 'Успеху', однако сервер RADIUS передал отклонение доступа за используемым сочетанием имени пользователя и пароля.

Ситуация 3: Связь, отказавшая между WLC и сервером 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
```

Необходимо ждать WLC для завершения, это - повторные попытки, прежде чем это отобразит выходные данные. Время может варьироваться на основе настроенных порогов повторной попытки.

```
(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

В вышеупомянутых выходных данных вы видите, что WLC пытался связаться с сервером RADIUS 6 раз и когда не было никакого ответа, это отметило сервер RADIUS как недостижимый.

Сценарий 4: нейтрализация радиуса

Когда вам настроили множественные серверы RADIUS под идентификаторами наборов сервисов (SSID), и основной сервер RADIUS не отвечает, тогда WLC пробует настроенным дополнительным сервером RADIUS. Это показывают очень ясно в выходных данных, где первый сервер RADIUS не отвечает, и WLC тогда пробует второй сервер RADIUS, который сразу отвечает.

```
(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
```

Предупреждения

- В настоящее время нет никакой поддержки GUI. Это - только команда, которая может быть выполнена от WLC.
- Проверка только для радиуса. Это не может использоваться для Аутентификации TACACS.
- Локальная проверка подлинности Flexconnect не может быть протестирована с этим методом.