

Test AAA Radius コマンドによる Radius サーバ接続の確認

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[機能の仕組み](#)

[コマンド構文](#)

[シナリオ1: 認証の試行に合格した場合](#)

[シナリオ2: 認証の試行の失敗](#)

[シナリオ3:WLCとRADIUSサーバ間の通信の失敗](#)

[シナリオ4:Radiusフォールバック](#)

[警告](#)

[関連情報](#)

はじめに

このドキュメントでは、 `test aaa radius` コマンドは、radiusサーバの接続とクライアント認証の問題を特定します。

前提条件

要件

Wireless LAN Controller(WLC)コード8.2以降に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

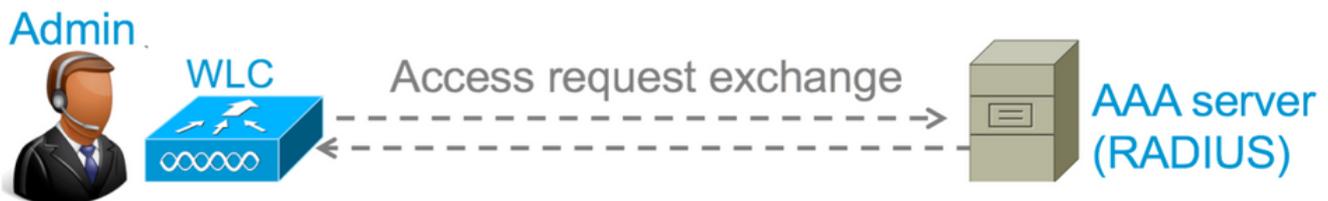
背景説明

ワイヤレスクライアントの認証の問題は、ワイヤレスネットワークエンジニアが直面する最も困難な問題の1つです。トラブルシューティングを行うには、問題のあるクライアントを把握し、ワイヤレスネットワークに関する最も適切な知識を持たないエンドユーザと協力して、デバッグとキャプチャを収集することが必要になる場合があります。重要性が増しているワイヤレスネットワークでは、これが重大なダウンタイムの原因となる可能性があります。

これまでは、認証の失敗の原因が、クライアントを拒否するRADIUSサーバにあるのか、あるいは単なる到達可能性の問題なのかを簡単に特定する方法がありませんでした。「`test aaa radius`」コマンドを使用すると、この操作を実行できます。WLC-RADIUSサーバの通信が失敗するかどうか、またはクライアントのクレデンシャルの結果として認証に成功または失敗するかどうかをリモートで確認できるようになりました。

機能の仕組み

これは、次のコマンドを使用するときの基本的なワークフローです `test aaa radius` を参照してください。



ステップ 1 : WLCは、RADIUSサーバにアクセス要求メッセージを、`test aaa radius` コマンドにより、WLC CLI で明確に示されます。

(シスココントローラ) `>test aaa radius username`

`password`

`wlan-id`

`apgroup`

`server-index`

例

`<#root>`

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

ステップ 2 : RADIUSサーバは提供されたクレデンシャルを検証し、認証要求の結果を提供します。

コマンド構文

コマンドを実行するには、次のパラメータを指定する必要があります。

```
( シスココントローラ ) > 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
```

シナリオ1 : 認証の試行に合格した場合

このコマンドがどのように動作し、出力が表示されるかを見てみましょう。 `test aaa radius` コマンドの結果、認証に成功します。このコマンドを実行すると、WLCはアクセス要求の送信に使用するパラメータを表示します。

```
<#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-Identifer             WLC_5508
Airespace / WLAN-Identifer 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

```

認証要求の結果を表示するには、コマンドを実行する必要があります `test aaa show radius` を参照。
RADIUSサーバに到達できず、WLCが別のRADIUSサーバに再試行またはフォールバックする必要がある場合、コマンドの出力が表示されるまでに時間がかかることがあります。

<#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)

```

このコマンドの非常に便利な点は、RADIUSサーバによって返される属性を表示することです。

リダイレクトURLとアクセスコントロールリスト(ACL)を指定できます。たとえば、中央Web認証(CWA)の場合や、VLANオーバーライドを使用する場合のVLAN情報などです。

 **注意**：アクセス要求のユーザ名/パスワードはRADIUSサーバにクリアテキストで送信されるため、トラフィックがセキュリティで保護されていないネットワークを通過する場合は注意して使用する必要があります。

シナリオ2：認証の試行の失敗

ユーザ名とパスワードを入力した結果、認証に失敗した場合の出力を見てみましょう。

```
<#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
```

この例では、接続テストの結果としてSuccess (成功) が返されましたが、RADIUSサーバが使用されたユーザ名とパスワードの組み合わせに対してアクセス拒否を送信したことがわかります。

シナリオ3:WLCとRADIUSサーバ間の通信の失敗

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

previous test command still not completed, try after some time
```

出力を表示する前に、WLCの再試行が完了するのを待つ必要があります。この時間は、設定されている再試行しきい値によって異なります。

```
<#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
```

この出力では、WLCがRADIUSサーバへの接続を6回試行し、応答がない場合はRADIUSサーバが到達不能としてマークされたことがわかります。

シナリオ4:Radiusフォールバック

Service Set Identifier(SSID)で複数のRADIUSサーバが設定されていて、プライマリRADIUSサーバが応答しない場合、WLCはセカンダリRADIUSサーバを設定して試行します。これは、最初のRADIUSサーバが応答せず、WLCが2番目のRADIUSサーバを試みてすぐに応答する場合の出力で非常に明確に示されています。

```
<#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

警告

- 現在、GUIはサポートされていません。これは、WLCから実行できるコマンドに過ぎません。
- この検証はRADIUSに対してのみ行われます。TACACS認証には使用できません。
- Flexconnectローカル認証は、この方式ではテストできません。

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。