Vérifiez la Connectivité de serveur de rayon avec la commande d'AAA RADIUS de test

Contenu

Introduction

Ce document décrit comment la commande de **rayon d'AAA de test** sur le Cisco WLC peut être utilisée pour identifier des questions de Connectivité et d'authentification client de serveur de rayon sans utilisation d'un client sans fil.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du code Sans fil 8.2 du contrôleur LAN (WLC) et en haut.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

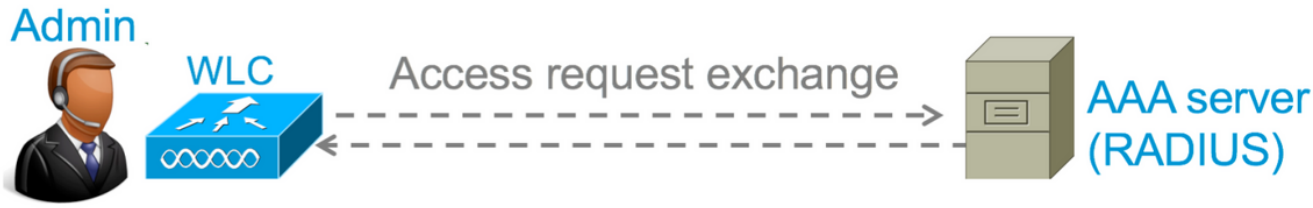
Informations générales

Les questions d'authentification de client sans fil sont l'un des problèmes les plus provocants aux lesquels les ingénieurs réseau Sans fil font face. Afin de dépanner ceci, cela exige souvent de mettre la main sur le client problématique, fonctionnent avec les utilisateurs finaux qui peuvent ne pas avoir la meilleure connaissance des réseaux Sans fil et pour collecter met au point et le capture. Dans un réseau Sans fil de plus en plus essentiel, ceci peut entraîner le temps d'arrêt significatif.

Jusqu'à présent il n'y avait aucune méthode facile de l'identifier si un échec d'authentification était provoqué par par le serveur de rayon qui rejette le client, ou juste simplement une question d'accessibilité. La commande de **rayon d'AAA de test** vous permet de faire juste cela. Vous pouvez maintenant à distance vérifier si la transmission de serveur de WLC-rayon échoue ou si les qualifications pour le client a comme conséquence passé ou une authentification défaillante.

Comment la caractéristique fonctionne

C'est un processus de base quand vous utilisez le **rayon d'AAA de test de** commande, suivant les indications de l'image.



Étape 1. Le WLC envoie un message de demande d'accès au serveur de rayon avec les paramètres qui est mentionné dans la commande de **rayon d'AAA de test**.

Pour ex : **testez le WLAN-id du mot de passe administrateur cisco123 de nom d'utilisateur RADIUS d'AAA 1 serveur-index 2 de groupe par défaut d'apgroup**

Étape 2. Le serveur de rayon valide les qualifications fournies et fournit les résultats de la demande d'authentification.

Syntaxe de commande

Ces paramètres doivent être fournis pour exécuter la commande :

(Contrôleur de Cisco) > **<server-index> de serveur-index de <apgroup-name> d'AP-groupe de <wlan-id> de WLAN-id de <password> de mot de passe de name> de <user de nom d'utilisateur RADIUS d'AAA de test**

```
<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.
```

Scénario 1. passé tentative d'authentification

Allons voir un regarder comment la commande fonctionne et les sorties sont vues quand la commande de **rayon d'AAA de test** a comme conséquence une authentification passée. Quand la commande est exécutée, WLC affiche les paramètres avec lesquels il envoie la demande d'accès :

```
(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
```

Afin de visualiser les résultats de la demande d'authentification, vous devez exécuter le **show radius d'AAA de test de** commande. La commande peut prendre un certain temps d'afficher la sortie si un serveur de rayon est inaccessible et le WLC doit relancer ou retour à un serveur différent de rayon.

```
(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)
```

L'aspect extrêmement utile de cette commande est qu'il affiche aux attributs ce qui sont retournés par le serveur de rayon. Ceci peut être réorientent URL et liste de contrôle d'accès (ACL). Par exemple, dans le cas de l'authentification Web centrale (CWA) ou des informations VLAN quand vous utilisez le dépassement VLAN.

> **Attention** : Le nom d'utilisateur/mot de passe dans la demande d'accès sont introduits le texte clair au serveur de rayon, ainsi vous devez l'utiliser avec prudence si la circulation au-dessus d'un réseau non sécurisé.

Scénario 2 : Tentative d'authentification défaillante

Voyons comment la sortie apparaît quand une entrée de nom d'utilisateur/mot de passe a comme conséquence une authentification défaillante.

```
(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
```

Dans ce cas, vous pouvez voir que le test de Connectivité a eu comme conséquence des « succès, toutefois le serveur de rayon a envoyé une Access-anomalie pour la combinaison de nom d'utilisateur/mot de passe utilisée.

Scénario 3 : La transmission a manqué entre WLC et serveur de rayon

```
(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
```

Vous devez attendre le WLC pour le terminer est des relances avant qu'il affiche la sortie. Le temps peut varier basé sur les seuils de relance configurés.

```
(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
```

Dans la sortie ci-dessus vous pouvez voir que le WLC essayé pour contacter le serveur de rayon 6 fois et quand il n'y avait aucune réponse il a marqué le serveur de rayon comme inaccessible.

Scénario 4 : Retour de rayon

Quand vous avez de plusieurs serveurs de rayon configurés sous l'Identifiant SSID (Service Set Identifier) et le serveur primaire de rayon ne répond pas, alors les essais WLC avec le serveur secondaire de rayon configuré. Ceci est affiché très clair dans la sortie où le premier serveur de rayon ne répond pas et le WLC puis juge le deuxième serveur de rayon ce qui répond immédiatement.

```
(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
```

Mises en garde

- Il n'y a actuellement aucun support GUI. C'est seulement une commande qui peut être exécutée du WLC.
- La vérification est seulement pour le rayon. Il ne peut pas être utilisé pour l'authentification TACACS.
- L'authentification locale de Flexconnect ne peut pas être testée avec cette méthode.