Vérifier la connectivité du serveur Radius avec la commande de test d'AAA Radius

Contenu

Introduction

Ce document décrit comment la commande **test aaa radius** sur le WLC Cisco peut être utilisée pour identifier les problèmes de connectivité du serveur radius et d'authentification du client sans l'utilisation d'un client sans fil.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître le code 8.2 du contrôleur LAN sans fil (WLC) et les versions ultérieures.

Components Used

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

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

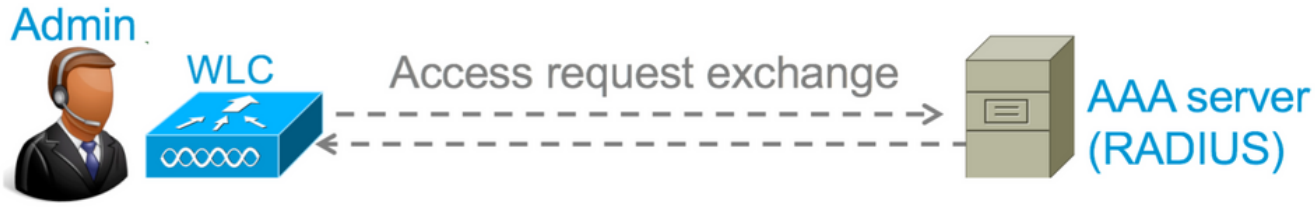
Les problèmes d'authentification des clients sans fil sont parmi les plus difficiles auxquels sont confrontés les ingénieurs réseau sans fil. Afin de dépanner, il faut souvent mettre la main sur le client problématique, travailler avec les utilisateurs finaux qui ne peuvent pas avoir la meilleure

connaissance des réseaux sans fil et collecter des débogages et des captures. Dans un réseau sans fil de plus en plus critique, cela peut entraîner des temps d'arrêt importants.

Jusqu'à présent, il n'y avait pas de moyen facile d'identifier si un échec d'authentification était causé par le serveur radius qui rejette le client, ou simplement un problème d'accessibilité. La commande **test aaa radius** vous permet de faire exactement cela. Vous pouvez maintenant vérifier à distance si la communication du serveur WLC-Radius échoue ou si les informations d'identification pour le client aboutissent à une authentification réussie ou échouée.

Fonctionnement De La Fonction

Il s'agit d'un workflow de base lorsque vous utilisez la commande **test aaa radius**, comme illustré dans l'image.



Étape 1. Le WLC envoie un message de demande d'accès au serveur radius avec les paramètres mentionnés dans la commande **test aaa radius**.

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

Étape 2. Le serveur RADIUS valide les informations d'identification fournies et fournit les résultats de la demande d'authentification.

Syntaxe de commande

Ces paramètres doivent être fournis pour exécuter la commande :

(Contrôleur Cisco) > **test aaa radius username <nom d'utilisateur> password <mot de passe> wlan-id <wlan-id> apgroup <nom-groupe> server-index <index-serveur>**

```
<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. Tentative d'authentification réussie

Examinons le fonctionnement de la commande et voyons les résultats lorsque la commande **test aaa radius** aboutit à une authentification réussie. Lorsque 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
```

Pour afficher les résultats de la demande d'authentification, vous devez exécuter la commande **test aaa show radius**. La commande peut prendre un certain temps pour afficher le résultat si un serveur radius est inaccessible et que le WLC doit réessayer ou revenir à un serveur radius différent.

```
(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'elle affiche les attributs qui sont retournés par le serveur radius. Il peut s'agir d'une URL de redirection et d'une liste de contrôle d'accès. Par exemple, dans le cas de l'authentification Web centrale (CWA) ou des informations VLAN lorsque vous utilisez le remplacement VLAN.

Attention : Le nom d'utilisateur/mot de passe de la demande d'accès est envoyé en texte

clair au serveur RADIUS. Vous devez donc l'utiliser avec précaution si le trafic circule sur un réseau non sécurisé.

Scénario 2 : Échec de la tentative d'authentification

Voyons comment le résultat apparaît lorsqu'une entrée de nom d'utilisateur/mot de passe entraîne un échec d'authentification.

```
(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 abouti à un « succès », mais le serveur RADIUS a envoyé un refus d'accès pour la combinaison nom d'utilisateur/mot de passe utilisée.

Scénario 3 : Échec de la communication entre le WLC et le serveur Radius

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

Vous devez attendre que le WLC termine ses nouvelles tentatives avant d'afficher le résultat. La durée peut varier en fonction des seuils de nouvelle tentative configurés.

```
(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
```

Dans ce résultat, vous pouvez voir que le WLC a essayé de contacter le serveur RADIUS 6 fois et quand il n'y avait pas de réponse, il a marqué le serveur RADIUS comme inaccessible.

Scénario 4 : Reprise Du Rayon

Lorsque plusieurs serveurs RADIUS sont configurés sous le SSID (Service Set Identifier) et que le serveur RADIUS principal ne répond pas, le WLC essaie avec le serveur RADIUS secondaire configuré. Ceci est montré très clairement dans la sortie où le premier serveur radius ne répond pas et le WLC essaie alors le second serveur radius qui répond immédiatement.

```
(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
```

Mises en garde

- Aucune interface graphique utilisateur n'est actuellement prise en charge. C'est seulement une commande qui peut être exécutée à partir du WLC.
- La vérification concerne uniquement le rayon. Il ne peut pas être utilisé pour l'authentification TACACS.
- L'authentification locale Flexconnect ne peut pas être testée avec cette méthode.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.