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

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Informations générales](#)

[Fonctionnement De La Fonction](#)

[Syntaxe de commande](#)

[Scénario 1 : Tentative d'authentification réussie](#)

[Scénario 2 : Échec de la tentative d'authentification](#)

[Scénario 3 : Échec de la communication entre le WLC et le serveur Radius](#)

[Scénario 4 : Reprise Du Rayon](#)

[Mises en garde](#)

[Informations connexes](#)

Introduction

Ce document décrit comment la commande test aaa radius identifie les problèmes de connectivité serveur radius et d'authentification client.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance du code 8.2 du contrôleur LAN sans fil (WLC) AireOS et des versions ultérieures.

Composants utilisés

Ce document et les commandes mentionnées sont spécifiques aux WLC Cisco AireOS.

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.

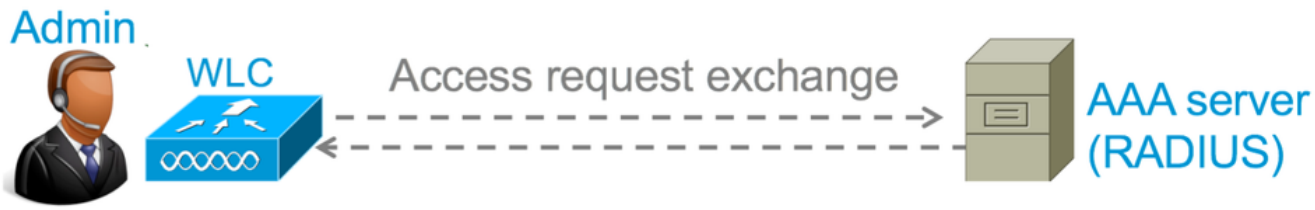
Informations générales

Les problèmes d'authentification des clients sans fil peuvent être un domaine où les ingénieurs réseau sans fil rencontrent des difficultés. Pour résoudre ce problème, il est souvent nécessaire de travailler avec les utilisateurs finaux pour collecter des informations supplémentaires telles que les journaux de débogage et les captures. Dans un réseau sans fil de plus en plus critique, cela peut entraîner des temps d'arrêt importants.

Jusqu'à présent, identifier si un échec d'authentification a été causé par le serveur radius qui rejette le client, ou s'il s'agissait simplement d'un problème d'accessibilité n'était pas une tâche facile. 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 lors de l'exécution de la commande test aaa radius :



---

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

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

Exemple

<#root>

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

---

2. Le serveur RADIUS valide les informations d'identification 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 co
<server-index>  (optional)  ---> The server index configured for the radius server that you are tryin
```

Scénario 1 : Tentative d'authentification réussie

Lorsque la commande test aaa radius aboutit à une authentification réussie. Lorsque la commande est exécutée, le WLC affiche les paramètres qu'il envoie avec la demande d'accès :

<#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-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, exécutez la commande test aaa show radius. Cette commande peut prendre quelques minutes pour afficher le résultat si un serveur radius est inaccessible et que le WLC doit réessayer ou revenir à un serveur radius différent :

<#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-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)
```

Cette commande montre que les attributs sont retournés par le serveur RADIUS, il peut s'agir d'une URL de redirection et d'une liste de contrôle d'accès (ACL). Par exemple, dans le cas de l'authentification Web centrale (CWA) ou des informations VLAN lorsque vous utilisez le remplacement VLAN.

⚠ Mise en garde : 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

Dans cet exemple, voici comment un résultat apparaît lorsqu'une entrée de nom d'utilisateur/mot de passe entraîne un échec d'authentification :

<#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
```

Dans ce cas, le test de connectivité aboutit à Success, cependant, 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

<#root>

```
(Cisco Controller) >

test aaa show radius


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

Attendez que le WLC termine toutes les nouvelles tentatives avant d'afficher le résultat. La durée peut varier en fonction des seuils de nouvelle tentative configurés :

<#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
```

Dans ce résultat, 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 dans le résultat où le premier serveur radius ne répond pas et le WLC essaie le second serveur radius qui répond immédiatement.

```
<#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
```

Mises en garde

- Aucune interface graphique utilisateur n'est actuellement prise en charge. Il s'agit seulement d'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.
- Impossible de tester l'authentification locale Flexconnect avec cette méthode.

Informations connexes

- Assistance technique de Cisco et téléchargements

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.