Überprüfen der RADIUS-Serververbindung mit dem AAA-RADIUS-Testbefehl

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Funktionsweise der Funktion
Befehlssyntax
Szenario 1. Authentifizierungsversuch erfolgreich
Szenario 2: Fehlgeschlagener Authentifizierungsversuch
Szenario 3: Kommunikation zwischen WLC und Radius-Server fehlgeschlagen
Szenario 4: Radius-Fallback
Hinweise

Einleitung

In diesem Dokument wird beschrieben, wie der Befehl **test aaa radius** auf dem Cisco WLC verwendet werden kann, um Probleme mit der RADIUS-Serververbindung und der Client-Authentifizierung ohne die Verwendung eines Wireless-Clients zu identifizieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie den Wireless LAN Controller (WLC)-Code 8.2 und höher kennen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

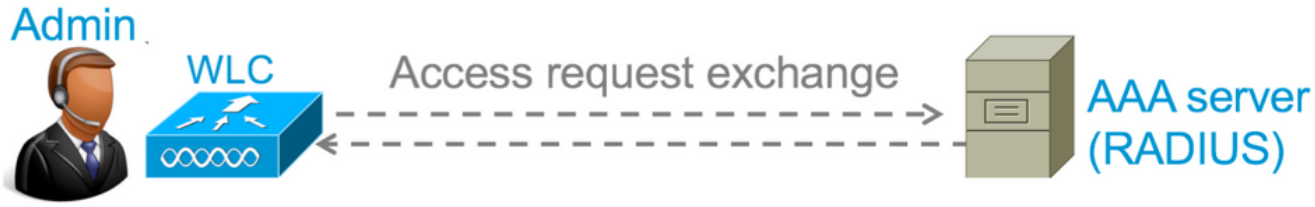
Die Authentifizierungsprobleme von Wireless-Clients gehören zu den schwierigsten Problemen, denen sich Wireless-Netzwerktechniker gegenübersehen. Für die Fehlerbehebung ist es oft erforderlich, den problematischen Client in den Griff zu bekommen, mit den Endbenutzern zu

arbeiten, die nicht über die besten Kenntnisse von Wireless-Netzwerken verfügen können, und Debug- und Erfassungen zu sammeln. In einem zunehmend kritischen Wireless-Netzwerk kann dies zu erheblichen Ausfallzeiten führen.

Bisher gab es keine einfache Möglichkeit festzustellen, ob ein Authentifizierungsfehler durch den Radius-Server verursacht wurde, der den Client zurückweist, oder einfach nur ein Erreichbarkeitsproblem. Mit dem Befehl **test aaa radius** können Sie genau das tun. Sie können jetzt per Fernzugriff überprüfen, ob die WLC-Radius-Serverkommunikation fehlschlägt oder ob die Anmeldeinformationen für den Client zu einer erfolgreichen oder fehlgeschlagenen Authentifizierung führen.

Funktionsweise der Funktion

Dies ist ein grundlegender Workflow, wenn Sie den Befehl **test aaa radius** verwenden, wie im Bild dargestellt.



Schritt 1: Der WLC sendet eine Zugriffsanforderungsnachricht an den Radius-Server zusammen mit den Parametern, die im Befehl **test aaa radius** angegeben sind.

Beispiel: **test aaa radius benutzername admin password cisco123 wlan-id 1 apgroup default-group server-index 2**

Schritt 2: Der Radius-Server validiert die bereitgestellten Anmeldeinformationen und stellt die Ergebnisse der Authentifizierungsanforderung bereit.

Befehlssyntax

Diese Parameter müssen angegeben werden, um den Befehl auszuführen:

(Cisco Controller) > **test aaa radius username <Benutzername> password <Kennwort> wlan-id <WLAN-ID> apgroup <apgroup-Name> server-index <Serverindex>**

```
<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.
```

Szenario 1. Authentifizierungsversuch erfolgreich

Sehen wir uns nun an, wie der Befehl funktioniert und welche Ausgaben ausgegeben werden, wenn der Befehl **test aaa radius** zu einer bestanden Authentifizierung führt. Wenn der Befehl ausgeführt wird, zeigt WLC die Parameter an, mit denen die Zugriffsanforderung gesendet wird:

```
(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
```

Um die Ergebnisse der Authentifizierungsanforderung anzuzeigen, müssen Sie den Befehl **test aaa show radius** ausführen. Der Befehl kann einige Zeit in Anspruch nehmen, um die Ausgabe anzuzeigen, wenn ein Radius-Server nicht erreichbar ist und der WLC einen Wiederholungsversuch durchführen oder auf einen anderen Radius-Server zurückgreifen muss.

```
(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)
```

Der äußerst nützliche Aspekt dieses Befehls ist, dass er die Attribute anzeigt, die vom Radius-Server zurückgegeben werden. Dies können Umleitungs-URLs und Zugriffskontrolllisten (ACLs) sein. Beispielsweise bei der zentralen Webauthentifizierung (CWA) oder VLAN-Informationen, wenn Sie VLAN override verwenden.

Vorsicht: Benutzername/Passwort in der Zugriffsanfrage werden unverschlüsselt an den Radius-Server gesendet. Sie müssen diesen daher mit Vorsicht verwenden, wenn der Datenverkehr über ein ungesichertes Netzwerk fließt.

Szenario 2: Fehlgeschlagener Authentifizierungsversuch

Lassen Sie uns sehen, wie die Ausgabe erscheint, wenn eine Eingabe von Benutzername/Kennwort zu einer fehlgeschlagenen Authentifizierung führt.

```
(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
```

In diesem Fall können Sie sehen, dass der Verbindungstest zu einem 'Success' geführt hat. Der Radius-Server hat jedoch eine Zugriffsablehnung für die verwendete Kombination aus Benutzername und Kennwort gesendet.

Szenario 3: Kommunikation zwischen WLC und Radius-Server fehlgeschlagen

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

Sie müssen warten, bis der WLC die Wiederholungsversuche abgeschlossen hat, bevor die Ausgabe angezeigt wird. Die Dauer kann je nach konfigurierten Schwellenwerten für erneute Versuche variieren.

```
(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
```

In dieser Ausgabe können Sie sehen, dass der WLC 6 Mal versucht hat, den Radius-Server zu kontaktieren, und wenn es keine Antwort gab, markierte er den Radius-Server als nicht erreichbar.

Szenario 4: Radius-Fallback

Wenn mehrere Radius-Server unter der Service Set Identifier (SSID) konfiguriert sind und der primäre Radius-Server nicht reagiert, versucht der WLC, den sekundären Radius-Server zu konfigurieren. Dies wird in der Ausgabe sehr deutlich, wo der erste Radius-Server nicht reagiert und der WLC dann den zweiten Radius-Server ausprobiert, der sofort antwortet.

```
(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
```

Hinweise

- Derzeit wird keine GUI unterstützt. Hierbei handelt es sich lediglich um einen Befehl, der vom WLC ausgeführt werden kann.
- Die Überprüfung bezieht sich nur auf den Radius. Sie kann nicht für die TACACS-Authentifizierung verwendet werden.
- Die lokale Flexconnect-Authentifizierung kann mit dieser Methode nicht getestet werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.