Verifique la Conectividad del servidor de RADIUS con el comando de la prueba RADIUS AAA

Contenido

Introducción

Este documento describe cómo el comando de la **prueba RADIUS AAA** en el WLC de Cisco se puede utilizar para identificar los problemas de la Conectividad y de la autenticación de cliente del servidor de RADIUS sin el uso de un cliente de red inalámbrica.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento del código 8.2 del regulador del Wireless LAN (WLC) y arriba.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Antecedentes

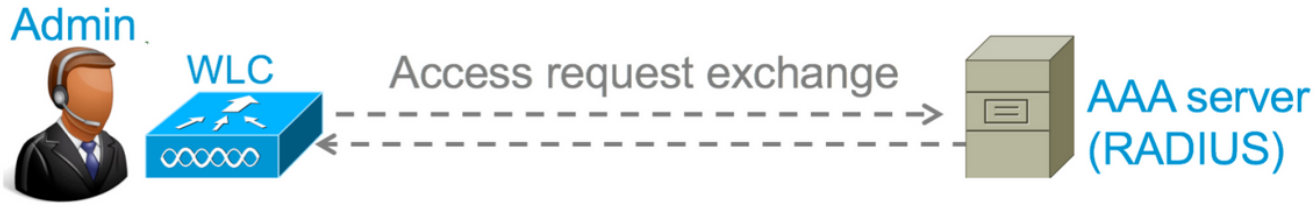
Los problemas de la autenticación de cliente de red inalámbrica son uno de los problemas más desafiadores que la red inalámbrica dirige la cara. Para resolver problemas esto, requiere a menudo para conseguir el control del cliente problemático, trabaja con los usuarios finales que pueden tener el mejor conocimiento de las redes inalámbricas y no recoger los debugs y las

capturas. En una red inalámbrica cada vez más crítica, esto puede causar el tiempo muerto significativo.

No había hasta ahora forma sencilla de identificar si un problema del accesibilidad causó una falla de autenticación el servidor de RADIUS que rechaza al cliente, o apenas simplemente. El comando de la **prueba RADIUS AAA** le deja hacer apenas eso. Usted puede ahora verificar remotamente si la comunicación del servidor del WLC-radio falla o si las credenciales para el cliente dan lugar a un haber pasado o a una autenticación fallida.

Cómo Funciona la Función

Esto es un flujo de trabajo básico cuando usted utiliza el comando test **RADIUS AAA**, tal y como se muestra en de la imagen.



Paso 1. El WLC envía un mensaje request del acceso al servidor de RADIUS junto con los parámetros que se menciona en el comando de la **prueba RADIUS AAA**.

Para ex: **pruebe RADIUS AAA el servidor-índice 2 del grupo predeterminado del apgroup WLAN-identificación 1 del cisco123 de la contraseña del nombre del usuario administrador**

Paso 2. El servidor de RADIUS valida las credenciales proporcionadas y proporciona los resultados del pedido de autenticación.

Sintaxis del comando

Estos parámetros necesitan ser proporcionados para ejecutar el comando:

(Regulador de Cisco) > **<server-index> del servidor-índice del <apgroup-name> del grupo ap del <wlan-id> WLAN-identificación del <password> de la contraseña del name> del <user del nombre de usuario de la prueba RADIUS AAA**

```
<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.
```

El escenario 1. pasó el intento de autenticación

Tengamos una mirada en cómo el comando trabaja y se consideran las salidas cuando el

comando de la **prueba RADIUS AAA** da lugar a una autenticación pasajera. Cuando se ejecuta el comando, el WLC visualiza los parámetros con los cuales envía la petición del acceso:

```
(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
```

Para ver los resultados del pedido de autenticación, usted necesita ejecutar el **radio de la demostración aaa del** comando test. El comando puede tardar un cierto tiempo para mostrar la salida si un servidor de RADIUS es inalcanzable y las necesidades del WLC de revisar o retraso a un diverso servidor de RADIUS.

```
(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)
```

El aspecto extremadamente útil de este comando es que muestra a atributos cuáles son vueltos por el servidor de RADIUS. Esto puede ser reorienta el URL y la lista de control de acceso (ACL). Por ejemplo, en el caso de la autenticación Web central (CWA) o de la información de VLAN cuando usted utiliza la invalidación del VLA N.

Caution: El nombre de usuario/la contraseña en la petición del acceso se envía en el texto claro al servidor de RADIUS, así que usted necesita utilizarlo con cautela si los flujos de tráfico sobre una red insegura.

Escenario 2: Tentativa de la autenticación fallida

Veamos cómo aparece la salida cuando un nombre de usuario/una entrada de contraseña da lugar a una autenticación fallida.

```
(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
```

En este caso, usted puede ver que la prueba de conectividad dio lugar a un “éxito”, no obstante el servidor de RADIUS envió un rechazo de acceso para la Combinación de nombre de usuario/contraseña usada.

Escenario 3: Comunicación fallada entre el WLC y el servidor de RADIUS

```
(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
```

Usted necesita esperar el WLC para acabarlo es recomprobaciones antes de que visualice la salida. El tiempo puede variar basado en los umbrales de la recomprobación configurados.

```
(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
```

En la salida antedicha usted puede ver que el WLC intentó entrar en contacto al servidor de RADIUS 6 veces y cuando no había respuesta marcó al servidor de RADIUS como inalcanzable.

Escenario 4: Retraso del radio

Cuando usted tiene los servidores de RADIUS múltiples configurados bajo el Service Set Identifier (SSID) y no responde el servidor de RADIUS primario, después el WLC intenta con el servidor RADIUS secundario configurado. Esto se muestra muy claramente en la salida donde no responde el primer servidor de RADIUS y el WLC después intenta al segundo servidor de RADIUS cuál responde inmediatamente.

```
(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
```

Advertencias

- No hay actualmente soporte GUI. Es solamente un comando que se puede ejecutar del WLC.
- La verificación está solamente para el radio. No puede ser utilizada para la autenticación de TACACS.
- La autenticación local de Flexconnect no se puede probar con este método.