Verifique la conectividad de servidores Radius con el comando Test AAA Radius

Contenido

Introducción

Este documento describe cómo el comando **test aaa radius** en el WLC de Cisco se puede utilizar para identificar la conectividad del servidor radius y los problemas de autenticación del cliente sin el uso de un cliente inalámbrico.

Prerequisites

Requirements

Cisco recomienda que conozca el código 8.2 y superior del Wireless LAN Controller (WLC).

Componentes Utilizados

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

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

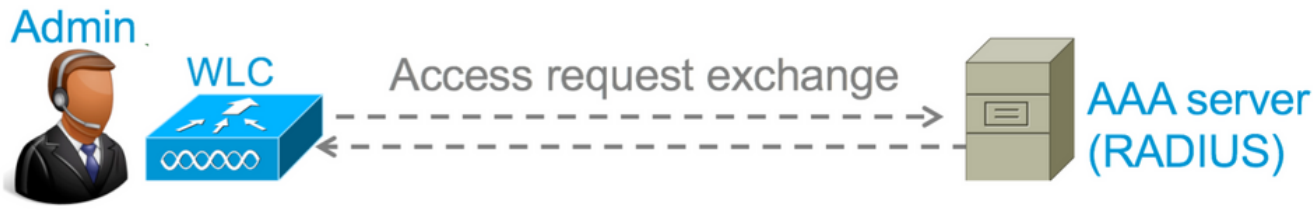
Los problemas de autenticación de clientes inalámbricos son uno de los problemas más difíciles a los que se enfrentan los ingenieros de redes inalámbricas. Para solucionar problemas, a menudo es necesario hacerse con el cliente problemático, trabajar con los usuarios finales que no pueden

tener el mejor conocimiento de las redes inalámbricas y recopilar depuraciones y capturas. En una red inalámbrica cada vez más importante, esto puede provocar un tiempo de inactividad considerable.

Hasta ahora no había una manera fácil de identificar si una falla de autenticación fue causada por el servidor RADIUS que rechaza al cliente, o simplemente un problema de alcance. El comando **test aaa radius** le permite hacer precisamente eso. Ahora puede verificar remotamente si la comunicación del servidor WLC-Radius falla o si las credenciales para el cliente resultan en una autenticación pasada o fallida.

Cómo Funciona la Función

Este es un flujo de trabajo básico cuando utiliza el comando **test aaa radius**, como se muestra en la imagen.



Paso 1. El WLC envía un mensaje de solicitud de acceso al servidor radius junto con los parámetros que se mencionan en el comando **test aaa radius**.

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

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

Sintaxis del comando

Se deben proporcionar estos parámetros para ejecutar el comando:

(Cisco Controller) > **test aaa radius username <user name> password <password> wlan-id <wlan-id> apgroup <apgroup-name> server-index <server-index>**

```
<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.
```

Situación 1. Intento de autenticación superado

Veamos cómo funciona el comando y los resultados se ven cuando el comando **test aaa radius** da

como resultado una autenticación pasada. Cuando se ejecuta el comando, el WLC muestra los parámetros con los que envía la solicitud de 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 de la solicitud de autenticación, debe ejecutar el comando **test aaa show radius**. El comando puede tomar algún tiempo para mostrar el resultado si un servidor radius es inalcanzable y el WLC necesita reintentar o fallback a un servidor radius diferente.

```
(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 los atributos que devuelve el servidor RADIUS. Puede ser una URL de redirección y una lista de control de acceso (ACL). Por ejemplo, en el caso de la autenticación web central (CWA) o la información de VLAN cuando se utiliza la invalidación de VLAN.

Precaución: El nombre de usuario/contraseña en la solicitud de acceso se envía en texto sin

formato al servidor RADIUS, por lo que debe utilizarlo con precaución si el tráfico fluye a través de una red no segura.

Escenario 2: Intento de autenticación fallido

Veamos cómo aparece la salida cuando una entrada de nombre de usuario/contraseña resulta en 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, puede ver que la prueba de conectividad resultó en un 'Éxito', sin embargo el servidor RADIUS envió un rechazo de acceso para la combinación de nombre de usuario/contraseña utilizada.

Escenario 3: Error de comunicación entre el WLC y el servidor Radius

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

Debe esperar a que el WLC termine los reintentos antes de que muestre la salida. El tiempo puede variar en función de los umbrales de reintento configurados.

```
(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
```

En esta salida puede ver que el WLC intentó contactar con el servidor de radio 6 veces y cuando no hubo respuesta marcó el servidor de radio como inalcanzable.

Escenario 4: Radius Fallback

Cuando tiene varios servidores RADIUS configurados bajo el identificador del conjunto de servicios (SSID) y el servidor RADIUS primario no responde, el WLC intenta con el servidor RADIUS secundario configurado. Esto se muestra muy claramente en la salida donde el primer servidor radius no responde y el WLC intenta entonces el segundo servidor radius que responde inmediatamente.

```
(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
```

Advertencias

- Actualmente no hay soporte para GUI. Es solamente un comando que se puede ejecutar desde el WLC.
- La verificación es solo para RADIUS. No se puede utilizar para la autenticación TACACS.
- La autenticación local de Flexconnect no se puede probar con este método.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).