Asignación del VLAN dinámico con el WLCs basado en el ACS al ejemplo de configuración de la asignación del grupo del Active Directory

Contenido

Introducción

Este documento explica cómo autenticar al cliente de red inalámbrica que usa la base de datos del Active Directory de Windows del Microsoft® (AD), cómo configurar la asignación del grupo entre el grupo AD y el grupo del Cisco Secure Access Control Server (ACS), y cómo asignar al cliente autenticado dinámicamente a un VLA N configurado en el grupo asociado ACS. Este documento se centra en el grupo AD que asocia solamente con el producto del software ACS y no

con el motor de solución ACS.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Tenga conocimiento básico de los reguladores del Wireless LAN (WLCs) y de los Puntos de acceso ligeros (los revestimientos)
- Tenga conocimiento funcional del Cisco Secure ACS
- Tenga conocimiento completo de las redes inalámbricas y de los problemas de seguridad de red inalámbrica
- Tenga conocimiento funcional y configurable en la asignación del VLAN dinámicoRefiera a la asignación del VLAN dinámico para más información.
- Tenga comprensión básica de los servicios de Microsoft Windows AD, así como del controlador de dominio y de los conceptos DNS
- Tenga conocimiento básico del protocolo ligero AP (el LWAPP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de las Cisco 2000 Series que funciona con la versión de firmware 4.0.217.0
- REVESTIMIENTO Cisco 802.11a/b/g de las Cisco 1000 Series
- Adaptador de red inalámbrica de cliente que funciona con la versión de firmware 3.6
- Utilidad de escritorio del Cisco Aironet (ADU) esa versión 3.6 de los funcionamientos
- Cisco Secure ACS que funciona con la versión 4.1
- Servidor de Microsoft Windows 2003 configurado como controlador de dominio
- Cisco 2950 Series Switch que funciona con la versión 12.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

La versión 4.1 del Cisco Secure ACS para Windows autentica a los usuarios de red inalámbrica contra una de varias bases de datos posibles, que incluye su base de datos interna. Usted puede configurar el ACS para autenticar a los usuarios con más de un tipo de base de datos. Usted puede configurar el ACS para remitir la autenticación de los usuarios a una o más Bases de datos de usuarios externas. El soporte para las Bases de datos de usuarios externas significa que el

ACS no le requiere crear las entradas de usuario duplicados en la base de datos de usuarios.

Los usuarios de red inalámbrica pueden ser autenticados usando varias bases de datos externas por ejemplo:

- Base de datos de Windows
- Servicios de directorio del Novell Netware (NDS)
- Lightweight Directory Access Protocol (LDAP) genérico
- Conectividad abierta de base de datos (ODBC) - bases de datos relacionales obedientes
- Servidores del Remote Access Dial-In User Service del proxy del SALTO (RADIUS)
- Rivest, Shamir, y servidores Token del SecurID del Adelman (RSA)
- servidores Token RADIUS-obedientes

Las tablas de compatibilidad de la autenticación ACS y de la base de datos de usuarios enumeran los diversos Protocolos de autenticación soportados por el ACS interno y las bases de datos externas.

Este documento se centra en los usuarios de red inalámbrica de autenticidad que utilizan la base de datos externa de Windows.

Usted puede configurar el ACS para autenticar a los usuarios con la Base de datos de usuarios externa en una de dos maneras:

- Por la asignación específica del usuario — Usted puede configurar el ACS para autenticar a los usuarios específicos con una Base de datos de usuarios externa. Para hacer esto, el usuario debe existir en la base de datos interna ACS y usted debe fijar la lista de la autenticación de contraseña en configuración de usuario a la Base de datos de usuarios externa que el ACS debe utilizar para autenticar al usuario.
- Por la Política de usuario desconocido — Usted puede configurar el ACS para intentar la autenticación de los usuarios que no están en la base de datos interna ACS usando una Base de datos de usuarios externa. Usted no necesita definir a los usuarios nuevos en la base de datos interna ACS para este método.

Este documento se centra en los usuarios de red inalámbrica de autenticidad que usan el método de la Política de usuario desconocido.

Cuando el ACS intenta autenticar al usuario contra la base de datos de Windows, ACS los credenciales de usuario adelante a la base de datos de Windows. La base de datos de Windows valida los credenciales de usuario, y sobre la autenticación satisfactoria, informa al ACS.

Después de la autenticación satisfactoria, el ACS recopila la información del grupo de este usuario de la base de datos de Windows. Después de recibir esta información del grupo, el ACS asocia a los usuarios de la información recopilada del grupo de la base de datos de Windows al grupo asociado correspondiente ACS con el fin de asignar los VLAN dinámicos al cliente de red inalámbrica. En fin, el ACS se puede configurar para asociar la base de datos de Windows a un grupo ACS y para asignar al usuario autenticado dinámicamente a un VLA N configurado en el grupo asociado ACS.

También, después de la primera autenticación satisfactoria, crean al usuario dinámicamente en el ACS. Una vez que autentican al usuario con éxito por primera vez, ocultan al usuario en el ACS con un puntero a su base de datos. Esto evita el ACS de buscar la lista entera de la base de datos durante las tentativas de la autenticación subsiguiente.

Restricciones ACS en la asignación del grupo con la base de datos de usuario de Windows

El ACS tiene estos límites en la asignación del grupo para los usuarios que son autenticados por una base de datos de usuario de Windows:

- El ACS puede solamente asignación del grupo de soporte para los usuarios que pertenecen a 500 o menos grupos de Windows.
- El ACS puede realizar solamente la asignación del grupo usando el local y los grupos globales a quienes un usuario pertenece en el dominio que autenticó al usuario.

Configurar

En este ejemplo, le configuran en el Winodws AD y se asocian a un grupo determinado AD. El Cisco Secure ACS se configura para utilizar la base de datos externa en Windows AD para los clientes de red inalámbrica de autenticidad. Entonces, el AD entonces se asocia al grupo ACS para los usuarios autenticados de tal modo que asignan al usuario de ese grupo determinado AD a un VLA N especificado en el grupo asociado correspondiente ACS.

La siguiente sección explica cómo configurar los dispositivos para esto.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuración de la configuración

En este documento, se utilizan estas configuraciones:

- Domain Name de Microsoft Windows: **lab.wireless**
- Usuarios AD: **wireless123**
- Usuario AD: **wireless123** asignado al grupo AD: **VLAN 20**
- Grupo AD: **VLAN 20** asociado al grupo ACS: **Grupo 20** donde configuran al grupo 20 para asignar a los usuarios autenticados de este grupo en la interfaz **vlan20** en el WLC.
- Aquí configuran al *controlador de dominio* y al *servidor ACS* en la misma máquina.

Se hacen estas suposiciones antes de que usted realice esta configuración:

- El REVESTIMIENTO se registra ya con el WLC.
- Usted es consciente de cómo configurar un servidor DHCP interno o a un servidor DHCP externo en el regulador para asignar la dirección IP al cliente de red inalámbrica. Refiera a configurar el DHCP para configurar a un servidor DHCP interno en el regulador.
- El documento discute la configuración requerida en el lado inalámbrico y asume que la red alámbrica exista.

Para lograr la asignación del VLAN dinámico con el WLCs basado en el ACS a la asignación del grupo AD, estos pasos deben ser realizados:

1. Active Directory de la configuración y base de datos de usuario de Windows
2. Configure el Cisco Secure ACS

3. Configure el regulador del Wireless LAN

Configure la base de datos del Active Directory y de usuario de Windows

Para configurar el AD y la base de datos de usuario de Windows que se utilizarán para autenticar a los clientes de red inalámbrica, estos pasos deben ser realizados:

1. Configure el servidor en su red como el controlador de dominio
2. Cree los usuarios y a los grupos de Active Directory en el dominio
3. Agregue al servidor ACS como el miembro del dominio

Configure el servidor en su red como el controlador de dominio

La configuración de un controlador de dominio implica la creación de una nueva estructura AD, y la instalación y la configuración del servicio DNS en el servidor.

Este documento crea un dominio **lab.wireless en el** servidor de Windows 2003 configurado como controlador de dominio.

Como parte de este proceso de la creación AD, usted instala al servidor DNS en el servidor de Windows 2003 para resolver lab.wireless a su propia dirección IP y a otros procesos de la resolución de nombre en el dominio. Usted puede también configurar a un servidor DNS externo para conectar con Internet.

Note: Aseegurese le tener el CD de Windows 2003 para instalar al servidor DNS en la máquina servidor.

Refiera a instalar y a configurar Windows 2003 como controlador de dominio para un procedimiento de configuración detallada.

Cree los usuarios y a los grupos de Active Directory en el dominio

El siguiente paso es crear los usuarios y a los grupos en el dominio lab.wireless. Refiera a los pasos 1 y 2 del AddingUsers y de las Computadoras a la sección del dominio de Active Directory de este documento de MicrosoftSupport para crear los usuarios y a los grupos AD.

Según lo mencionado ya en la sección de configuración de la configuración de este documento, crean y se asocian a un usuario **wireless123 al** grupo **vlan20** AD.

Agregue al servidor ACS como el miembro del dominio

Refiera a los pasos 1 y 2 de los usuarios y de las Computadoras que agregan a la sección del dominio de Active Directory de este documento de soporte de Microsoft para agregar al servidor ACS al dominio lab.wireless.

Note: Menciones de esta sección solamente cómo agregar la máquina de Windows que funciona con el software ACS al dominio. Este procedimiento es no corresponde para agregar el motor de solución ACS como miembro del dominio.

Configure el Cisco Secure ACS

Para configurar el ACS para esta configuración, estos pasos deben ser realizados:

1. Configure el ACS para la autenticación de la base de datos de usuario de Windows y la asignación del grupo
2. Configure el ACS para la asignación del VLAN dinámico

Configure el ACS para la autenticación de la base de datos de usuario de Windows y la asignación del grupo

Ahora que el servidor ACS se une a al dominio lab.wireless, el siguiente paso es configurar el ACS para la autenticación de la base de datos de usuario de Windows y asociar la base de datos externa de Windows AD al grupo ACS. Los usuarios desconocidos que autentican usando la base de datos especificada automáticamente pertenecen a, y heredan las autorizaciones del grupo.

Según lo mencionado anterior, este ejemplo asocia el VLAN 20 del grupo AD, con el grupo 20 del grupo ACS.

Note: Antes de que usted configure al servidor ACS, realice las tareas como se explica en el capítulo de configuración de la autenticación de Windows para la autenticación de usuario y la asignación confiables del grupo.

Configure la Base de datos de usuarios externa de Windows en el servidor ACS

Del ACS GUI, complete estos pasos:

1. En la barra de navegación, haga clic en External User Databases.
2. En las Bases de datos de usuarios externas pagine, haga clic la **configuración de la base de datos**.El ACS visualiza una lista de todos los tipos posibles de la Base de datos de usuarios externa.
3. Haga clic en base de datos de Windows.Si existe ninguna configuración de base de datos de Windows, la tabla de la creación de la configuración de la base de datos aparece. Si no, la página de la Configuración de base de datos de usuarios externa aparece.
4. Haga clic en Configure (Configurar).La página de la configuración de la base de datos del usuario de Windows aparece con varias opciones.
5. Configure las opciones obligatorias. Todas las configuraciones en la página de la **configuración de la base de datos del usuario de Windows** son opcionales y no necesitan ser habilitadas a menos que usted quiera permitir y configurar las características del específico que soportan.**Note**: Este documento no configura ninguno de estos opciones manualmente pues no son necesarias para este ejemplo de configuración.Refiera a las opciones de configuración de la base de datos del usuario de Windows para más información.
6. El tecleo **somete** para acabar esta configuración.El ACS guarda la configuración de la base de datos del usuario de Windows que usted creó. Usted puede ahora agregarlo a su Política de usuario desconocido o asignar las cuentas de usuario específicas para utilizar esta base de datos para la autenticación. Este documento agrega esta configuración a la Política de usuario desconocido.

Política de usuario desconocido de la configuración con la base de datos de Windows

La Política de usuario desconocido es una expedición de la forma de autenticación. Esencialmente, esta característica es un paso adicional en el proceso de autenticación. Si un nombre de usuario no existe en la base de datos interna ACS, el ACS adelante el pedido de autenticación de un nombre de usuario y contraseña entrante a las bases de datos externas con las cuales se configura para comunicar. La base de datos externa debe soportar el protocolo de autenticación usado en el pedido de autenticación.

Refiera a la Política de usuario desconocido para más información.

En este ejemplo, el ACS debe remitir el pedido de autenticación que viene con el WLC de un cliente de red inalámbrica a la base de datos de Windows configurada en la sección anterior. Para alcanzar esto, el grupo de usuario desconocido debe ser asociado a la base de datos de Windows externa (lab.wireless) usando estos pasos:

1. En la barra de navegación, haga clic en External User Databases. Entonces, **Política de usuario desconocido del** tecleo.
2. Para permitir la autenticación de usuario desconocido, habilite la Política de usuario desconocido:Seleccione el **control la** opción **siguiente de las Bases de datos de usuarios externas**.Seleccione la **base de datos de Windows en la** lista de las **bases de datos externas** y haga clic **-->** (botón de la flecha correcta) moverlo desde las bases de datos externas a las bases de datos seleccionadas enumere. Para quitar una base de datos de las bases de datos seleccionadas enumere, seleccione la base de datos, y después haga clic **<--** (botón de la flecha izquierda) para moverlo de nuevo a las bases de datos externas enumere.
3. Haga clic en Submit (Enviar).El ACS guarda y implementa la configuración de la Política de usuario desconocido que usted creó.

Cree la asignación del grupo ACS con el grupo de Windows

Complete estos pasos del ACS GUI:

1. En la barra de navegación, haga clic en External User Databases. Entonces, **Mapeo de grupo de base de datos del** tecleo.
2. Haga clic el nombre de Base de datos de usuarios externa para el cual usted quiere configurar una asignación del grupo.En este ejemplo, es base de datos de Windows.
3. En el dominio del resultado las configuraciones paginan, hacen clic la **nueva configuración**.**Note**: Por abandono usted ve solamente el dominio \ el VALOR POR DEFECTO en esta página.La nueva Domain Configuration (Configuración del dominio) página de la definición aparece.
4. En el cuadro detectado de los dominios de esta página, usted debe poder ver el **LABORATORIO de la** base de datos de usuario de Windows. Haga clic en Submit (Enviar).**El LABORATORIO del** dominio de las nuevas ventanas aparece en la lista de dominios en la página de las configuraciones del dominio.
5. Haga clic el dominio del **LABORATORIO**.Las asignaciones del grupo para el dominio: La tabla del LABORATORIO aparece.
6. El tecleo **agrega la asignación**.La nueva asignación del grupo del crear para el dominio: La página del LABORATORIO se abre. La lista del grupo visualiza los nombres del grupo que se derivan de la base de datos del LABORATORIO. En este conjunto del grupo, usted debe

poder ver el grupo vlan20 creado en el AD de este dominio del laboratorio.
7. Elija **vlan20 de la** lista del grupo, después haga clic **agregan a seleccionado**.
8. En la casilla desplegable del grupo ACS, elija **Group20 al** cual usted quiera asociar a los usuarios que pertenecen al grupo AD: VLAN 20.
9. Haga clic en Submit (Enviar).El grupo asociado a la lista ACS aparece en la parte inferior de la columna de los grupos de la base de datos tal y como se muestra en del ejemplo. El asterisco (*) en el extremo de cada conjunto de los grupos indica que los usuarios que se autentican con la Base de datos de usuarios externa pueden pertenecer a otros grupos además de ésos en el conjunto.

Configuración ACS para la asignación del VLAN dinámico

La asignación del VLAN dinámico es una característica que coloca a un usuario de red inalámbrica en un VLA N específico basado en las credenciales suministradas por el usuario. Esta tarea de asignar a los usuarios a un VLA N específico es manejada por un servidor de autenticación de RADIUS, tal como Cisco Secure ACS. Esto se puede utilizar, por ejemplo, para permitir que el host inalámbrico permanezca en el mismo VLA N que mueve dentro de una red de oficinas centrales.

Note: Este documento utiliza el [VSA (Vendor-Specific)] del Airespace de Cisco Atributo para asignar con éxito a un usuario autenticado con un nombre de la interfaz VLAN (no el VLAN ID) según la configuración de grupo en el ACS.

Para configurar el ACS para la asignación del VLAN dinámico, estos pasos deben ser realizados:

1. Agregue el WLC como cliente AAA al ACS
2. Configure al grupo ACS con la opción del atributo del Airespace VSA de Cisco

Agregue el WLC como cliente AAA al ACS

Para configurar el ACS para la asignación del VLAN dinámico, usted necesita configurar al cliente AAA para el WLC en el servidor de RADIUS. Este documento asume que el WLC está agregado ya al ACS como cliente AAA. Refiera a agregar a los clientes AAA a un ACS para la información sobre cómo agregar al cliente AAA al ACS.

Note: En el ejemplo de este documento, la opción **RADIUS (Airespace)** bajo autenticidad usando tira hacia abajo el menú del cliente AAA del agregar que la página debe ser configurada, mientras que el WLC como el cliente AAA al ACS se configura.

Configure al grupo ACS con la opción del atributo del Airespace VSA de Cisco

Complete estos pasos:

1. Del ACS GUI en la barra de navegación, haga clic la **configuración de grupo del** lado izquierdo para configurar a un nuevo grupo.
2. En la casilla desplegable del grupo, elija el **grupo 20** (según este ejemplo) y el tecleo **edita las configuraciones**.
3. En el grupo 20 edite la página de las configuraciones, haga clic el **salto a la** casilla desplegable y elija **RADIUS (Airespace de Cisco)** para configurar la configuración del

atributo del Airespace VSA.**Note**: Si este atributo no se visualiza bajo configuración de grupo, edite las configuraciones **RADIUS (Airespace)** para incluir el nombre de la interfaz bajo la pantalla de la configuración de la interfaz del ACS.
4. En el Airespace de Cisco los atributos de RADIUS seccionan, habilitan el Aire-Interfaz-**nombre** y ingresan **vlan20** como el nombre de la interfaz que se volverá por este grupo ACS sobre la autenticación satisfactoria.
5. Tecleo **Submit + Restart**.

Configure el regulador del Wireless LAN

Para configurar el WLC para esta configuración, estos pasos deben ser realizados:

1. Configure el WLC con los detalles del servidor de autenticación
2. Configure las interfaces dinámicas (VLA N) en el WLC
3. Configure los WLAN (el SSID)

Configure el WLC con los detalles del servidor de autenticación

Complete estos pasos para configurar el WLC para esta configuración:

1. Del regulador GUI, haga clic la **Seguridad**.
2. Haga clic en **New**.
3. En la página de configuración del servidor de autenticación del RADIO (ACS), ingrese el IP Address del servidor de RADIUS y de la clave secreta compartida usados entre el servidor de RADIUS y el WLC.Esta clave secreta compartida debe ser lo mismo que la que está configurada en el ACS bajo **entrada de los clientes AAA de la Configuración de la red > Add**. Este documento utiliza al servidor ACS con la dirección IP de 10.77.244.196/27.
4. Aseegurese que habilitan al estado del servidor. Marque el cuadro del **usuario de la red**. Esto se asegura de que autentiquen a los usuarios de la red contra este servidor.

Configure las interfaces dinámicas (VLA N) en el WLC

Este procedimiento explica cómo configurar las interfaces dinámicas en el WLC. Para una asignación acertada del VLAN dinámico, el nombre de la interfaz VLAN especificado bajo configuración del atributo VSA del servidor ACS se debe también configurar en el WLC.

Este documento configura la interfaz VLAN con el nombre el "vlan20" y VLAN ID = 20, y la interfaz VLAN con el nombre en el WLC.

Complete estos pasos:

1. Del regulador GUI, bajo la ventana del **regulador > de las interfaces**, se configuran las interfaces dinámicas.
2. Haga clic en **New**.
3. En las **interfaces > la nueva ventana**, teclee el nombre de la interfaz como *vlan20*, que es lo mismo que el parámetro de la Airespace-interfaz configurado en el ACS y el VLAN ID como *20* para asignarlo al VLAN20.
4. Haga clic en Apply (Aplicar).

5. En las **interfaces > edite la** página, configure la información VLAN ID, de la dirección IP, del netmask y de dirección del gateway de la subred VLAN20 tal y como se muestra en de esta ventana.**Note**: Se recomienda siempre para utilizar a un servidor DHCP para asignar la dirección IP a los clientes. En ese caso, el campo de dirección primario del servidor DHCP se debe llenar de la dirección IP del servidor DHCP.
6. Haga clic en Apply (Aplicar).

Configure los WLAN (el SSID)

En el WLC, usted configura el *wirelesslab* SSID y elige un método de autentificación, que indica para el nombre de usuario y contraseña del cliente. En este ejemplo, usted utiliza el **SALTO** como el método de autentificación para autenticar al usuario. Complete estos pasos:

1. En el WLC GUI, haga clic los **WLAN**. Haga clic en **New**.
2. Elija un nombre del perfil y ingrese el *wirelesslab* WLAN SSID.
3. Haga clic en Apply (Aplicar).
4. Elija los WLAN > editan, y conforme a la ficha general, habilitan la red inalámbrica (WLAN) y eligen la interfaz como *Administración* para asignar los IP Addresses de la subred de administración.
5. Haga clic la **Seguridad**. Bajo lengueta de la capa 2, elija **WPA+WPA2** como **Seguridad de la capa 2**. Usted puede elegir la directiva WPA o WPA2. En este ejemplo usted elige el **WPA2** con el cifrado **TKIP** y el **802.1x** como el método de autentificación.
6. Haga clic a los **servidores de AAA** y elija **10.77.244.196** como el servidor de autenticación para autenticar a los usuarios de esta red inalámbrica (WLAN) contra este servidor.
7. Asignan los usuarios de red inalámbrica a la interfaz de administración. Para asignar al usuario a una interfaz suministrada por el servidor de RADIUS, elija **avanzado > permiten la invalidación AAA**.

Configure al cliente de red inalámbrica

Esta sección explica cómo configurar al cliente de red inalámbrica. Complete estos pasos:

1. Haga clic la **utilidad de escritorio del Cisco Aironet**.
2. Elija la **Administración del perfil**.
3. Resalte el perfil existente y elija **se modifican** tal y como se muestra en del cuadro 1.**Figura 1**
4. En la **ficha general**, elija un **nombre del perfil**. Este ejemplo utiliza el *LABORATORIO del* nombre. Ingrese el *wirelesslab* SSID usado en el WLC. Cuadro 2 demostraciones cómo hacer esto.**Figura 2**
5. **Seguridad del** tecleo. El método de autenticación configurado en el cliente debe ser idéntico al del WLC. Elija **WPA/WPA2/CCKM** y elija el **tipo EAP** como *SALTO* tal y como se muestra en del cuadro 3.**Figura 3**
6. Haga clic la **configuración** y elija el **manualmente pronto para el Nombre de usuario y la contraseña**. El cuadro 4 muestra esto.**'Figura 4'**
7. Click OK. Una ventana que le indica para el nombre de usuario y contraseña como se muestra aparece. Ingrese el Nombre de usuario y la contraseña que usted configuró en la base de datos de Windows. En este ejemplo, el Nombre de usuario es *wireless123*, la contraseña es *cisco123*. En el inicio a colocar, teclee adentro el dominio que usted configuró

en la **AUTORIZACIÓN del** Active Directory y del tecleo. En este ejemplo, es *LABORATORIO*. demuestra estos pasos.

Verificación

Active el perfil del usuario del **LABORATORIO que** usted ha configurado en el ADU. Según su configuración, indican al cliente para el nombre de usuario y contraseña.

Este ejemplo utiliza este nombre de usuario y contraseña del lado del cliente para recibir la autenticación y para ser asignado a un VLA N por el servidor de RADIUS:

- Nombre de usuario = **wireless123**
- Contraseña = **cisco123**

Además, especifique **lab.wireless en la** conexión a la comunicación para colocar del cuadro de diálogo de la contraseña de red inalámbrica del ingresar.

Una vez que el cliente de red inalámbrica autentica con éxito, encuentra el controlador de dominio, se une al dominio y se asocia a la red WLAN a través del wirelesslab SSID, usted necesitan verificar que asignen su cliente al VLA N apropiado según los atributos VSA enviados por las configuraciones de grupo del servidor de RADIUS.

Complete estos pasos para lograr esto:

1. Del regulador GUI, elija el **monitor**. Haga clic a los **clientes** que aparece a la izquierda de la ventana del (APS) de los Puntos de acceso.Las estadísticas del cliente se visualizan con el estatus según lo asociado.
2. Usted ve una lista de clientes de red inalámbrica que se asocien a este WLC. Haga clic en al cliente que autenticó con el ACS.Sobre los detalles pagine, observe que el **usuario: wireless123** se autentica y se asocia a través del *wirelesslab* SSID. Observe que la dirección IP es *20.0.0.4* y la interfaz es *vlan20*.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. Refiera a la información del debug AAA para el Cisco Secure ACS for Windows para más información sobre cómo cómo registrar y obtener la información del debug AAA en el ACS.

Comandos para resolución de problemas

Note: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **haga el debug del permiso de los eventos aaa** — Este comando se puede utilizar para asegurar la transferencia acertada de los atributos de RADIUS al cliente vía el regulador. Esta porción de la salida de los debugs asegura una transmisión exitosa de los atributos de RADIUS.Aquí está la salida de este comando basado en el ejemplo de configuración de este documento:

```
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Successful trans
```

```
mission of Authentication Packet (id 131) to 10.77.244.196:1812, proxy state 00:
40:96:af:3e:93-96:af
Fri Oct  5 15:47:38 2007: ****Enter processIncomingMessages: response code=11
Fri Oct  5 15:47:38 2007: ****Enter processRadiusResponse: response code=11
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Access-Challenge received from
RADIUS server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Successful transmission of Authentic
ation Packet (id 132) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-96:af

Fri Oct  5 15:47:38 2007: ****Enter processIncomingMessages: response code=11
Fri Oct  5 15:47:38 2007: ****Enter processRadiusResponse: response code=11
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Access-Challenge received from RADIUS
server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Successful transmission of Authentic
ation Packet (id 133) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-96:af

Fri Oct  5 15:47:38 2007: ****Enter processIncomingMessages: response code=2
Fri Oct  5 15:47:38 2007: ****Enter processRadiusResponse: response code=2
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Access-Accept received from RADIUS
server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Applying new AAA override for
station 00:40:96:af:3e:93
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Override values for station 00:40:96
:af:3e:93
                source: 4, valid bits: 0x200
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                                        vlanIfNa
me: vlan20, acl
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Inserting new RADIUS override into
chain for station 00:40:96:af:3e:93
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Override values for station 00:40:96
:af:3e:93
                source: 4, valid bits: 0x200
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                                        vlanIfNa
me: 'sales', acl
Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Applying override policy from source
 Override Summation:

Fri Oct  5 15:47:38 2007: 00:40:96:af:3e:93 Override values for station 00:40:96
:af:3e:93
                source: 256, valid bits: 0x200
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                                        vlanIfNa
me: 'sales', a
Fri Oct  5 15:47:39 2007: 00:40:96:af:3e:93 Sending Accounting request (0) for
station 00:40:96:af:3e:93
```

Según lo visto de esta salida de los debugs, del WLC pasajero en los pedidos de autenticación y de las respuestas entre el cliente de red inalámbrica y el servidor de RADIUS 10.77.244.196. El servidor ha autenticado con éxito al cliente de red inalámbrica (esto se puede verificar usando el mensaje del **access-accept**). Sobre la autenticación satisfactoria, usted puede también ver al servidor de RADIUS el transmitir de la **interfaz VLAN name:vlan20**, por lo tanto dinámicamente asignando al cliente de red inalámbrica en el VLAN20.

- **permiso aaa del dot1x del debug** — Se utiliza este comando de hacer el debug de la

autenticación entera del dot1x que ocurre entre el cliente de red inalámbrica y el servidor de autenticación (ACS).

- **el debug aaa todo habilita** — Debug de las configuraciones de todos los mensajes AAA.Aquí está la salida de este comando basado en el ejemplo de configuración de este documento:

```
(Cisco Controller) >Fri Oct  5 16:17:18 2007: AuthenticationRequest: 0xac4be5c
Fri Oct  5 16:17:18 2007:       Callback.....................................0x8
29a960
Fri Oct  5 16:17:18 2007:       protocolType.................................0x0
0040001
Fri Oct  5 16:17:18 2007:       proxyState...................................00:
40:96:AF:3E:93-07:00
Fri Oct  5 16:17:18 2007:       Packet contains 12 AVPs (not shown)
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Successful transmission of
Authentication Packet (id 137) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-96:af
.....................................................................
.....................................................................
.....................................................................

Fri Oct  5 16:17:18 2007: ****Enter processIncomingMessages: response code=11
Fri Oct  5 16:17:18 2007: ****Enter processRadiusResponse: response code=11
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Access-Challenge received from RADIUS
server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 7
Fri Oct  5 16:17:18 2007: AuthorizationResponse: 0x9845500
Fri Oct  5 16:17:18 2007:       structureSize...............................130

Fri Oct  5 16:17:18 2007:       resultCode..................................255

Fri Oct  5 16:17:18 2007:       protocolUsed................................0x0
0000001
Fri Oct  5 16:17:18 2007:       proxyState...................................00:
40:96:AF:3E:93-07:00
Fri Oct  5 16:17:18 2007:       Packet contains 3 AVPs (not shown)
.....................................................................
.....................................................................
.....................................................................
.....................................................................

Fri Oct  5 16:17:18 2007: ****Enter processIncomingMessages: response code=11
Fri Oct  5 16:17:18 2007: ****Enter processRadiusResponse: response code=11
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Access-Challenge received from
RADIUS server 10.77.244.196 for mobi)
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Successful transmission of
Authentication Packet (id 139) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-96:af

Fri Oct  5 16:17:18 2007: 00000000: 01 8b 00 bb 54 4c 75 3a  e5 b9 d2 c0 28 f2 9
3 b3  ....TLu:....(...
Fri Oct  5 16:17:18 2007: 00000010: f2 81 50 65 01 10 77 69  72 65 6c 65 73 73 5
c 75  ..Pe..lab\wireless123
Fri Oct  5 16:17:18 2007: 00000020: 73 65 72 31 1f 13 30 30  2d 34 30 2d 39 36 2
d 41  ser1..00-40-96-A
Fri Oct  5 16:17:18 2007: 00000030: 46 2d 33 45 2d 39 33 1e  18 30 30 2d 30 42 2
d 38  F-3E-93..00-0B-8
Fri Oct  5 16:17:18 2007: 00000040: 35 2d 35 42 2d 46 42 2d  44 30 3a 41 44 53 3
1 05  5-5B-FB-D0:wirelessl23.
Fri Oct  5 16:17:18 2007: 00000050: 06 00 00 00 01 04 06 0a  4d f4 d4 20 06 57 4
c 43  ........M....WLC
Fri Oct  5 16:17:18 2007: 00000060: 31 1a 0c 00 00 37 63 01  06 00 00 00 02 06 0
6 00  1....7c.........
Fri Oct  5 16:17:18 2007: 00000070: 00 00 02 0c 06 00 00 05  14 3d 06 00 00 00 1
3 4f  .........=.....O
```

```
Fri Oct  5 16:17:18 2007: 00000080: 20 01 05 00 1e 11 01 00  08 85 8e 81 b0 7d b
f ee  .............}..
Fri Oct  5 16:17:18 2007: 00000090: b1 77 69 72 65 6c 65 73  73 5c 75 73 65 72 3
1 18  .lab\wireless123
.....................................................................
.....................................................................
.....................................................................
Fri Oct  5 16:17:18 2007: 00000050: 31 1a 3b 00 00 00 09 01  35 6c 65 61 70 3a 7
3 65  1.;.....5leap:se
Fri Oct  5 16:17:18 2007: 00000060: 73 73 69 6f 6e 2d 6b 65  79 3d 84 e7 c5 3c 3
3 bd  ssion-key=...<3.
Fri Oct  5 16:17:18 2007: 00000070: a8 bf 7a 43 9d 6e bb c8  a8 2c 5d c6 91 d6 f
3 21  ..zC.n...,]....!
Fri Oct  5 16:17:18 2007: 00000080: df 1e 0e 28 c1 ef a5 31  a7 cd 62 da 1a 1f 0
0 00  ...(...1..b.....
Fri Oct  5 16:17:18 2007: 00000090: 00 09 01 19 61 75 74 68  2d 61 6c 67 6f 2d 7
4 79  ....auth-algo-ty
Fri Oct  5 16:17:18 2007: 000000a0: 70 65 3d 65 61 70 2d 6c  65 61 70 19 17 43 4
1 43  pe=eap-leap..CAC

      ....
Fri Oct  5 16:17:18 2007: ****Enter processIncomingMessages: response code=2
Fri Oct  5 16:17:18 2007: ****Enter processRadiusResponse: response code=2
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Access-Accept received from RADIUS
server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 7
Fri Oct  5 16:17:18 2007: AuthorizationResponse: 0x9845500
Fri Oct  5 16:17:18 2007:       structureSize.............................228

Fri Oct  5 16:17:18 2007:       resultCode.................................0
Fri Oct  5 16:17:18 2007:       protocolUsed...............................0x0
0000001
Fri Oct  5 16:17:18 2007:       proxyState.................................00:
40:96:AF:3E:93-07:02
Fri Oct  5 16:17:18 2007:       Packet contains 5 AVPs:
Fri Oct  5 16:17:18 2007:           AVP[01] Airespace / Interface-Name.........
.....vlan20 (5 bytes)
Fri Oct  5 16:17:18 2007:           AVP[02] EAP-Message.......................
.....DATA (46 bytes)
Fri Oct  5 16:17:18 2007:           AVP[03] Cisco / LEAP-Session-Key...........
.....DATA (16 bytes)
Fri Oct  5 16:17:18 2007:           AVP[04] Class..............................
.....CACS:0/5943/a4df4d4/1 (21 bytes)
Fri Oct  5 16:17:18 2007:           AVP[05] Message-Authenticator..............
.....DATA (16 bytes)
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Applying new AAA override for
station 00:40:96:af:3e:93
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Override values for station 00:40:96
:af:3e:93
                source: 4, valid bits: 0x200
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                                        vlanIfNa
me: 'sales', acl
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Inserting new RADIUS override into
chain for station 00:40:96:af:3e:93
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Override values for station 00:40:96
:af:3e:93
                source: 4, valid bits: 0x200
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                                        vlanIfNa
me: 'sales', acl
```

```
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Applying override policy from source
 Override Summation:

Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Override values for station 00:40:96
:af:3e:93
                source: 256, valid bits: 0x200
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                                        vlanIfNa
me: 'sales', a
Fri Oct  5 16:17:18 2007: 00:40:96:af:3e:93 Sending Accounting request (0) for
station 00:40:96:af:3e:93
Fri Oct  5 16:17:18 2007: AccountingMessage Accounting Interim: 0xac4b1f0
Fri Oct  5 16:17:18 2007:       Packet contains 20 AVPs:
Fri Oct  5 16:17:18 2007:           AVP[01] User-Name.........................
.....lab\wireless123 (14 bytes)
Fri Oct  5 16:17:18 2007:           AVP[02] Nas-Port..........................
.....0x00000001 (1) (4 bytes)
Fri Oct  5 16:17:18 2007:           AVP[03] Nas-Ip-Address....................
.....0x0a4df4d4 (172881108) (4 bytes)
Fri Oct  5 16:17:18 2007:           AVP[04] Class.............................
.....CACS:0/5943/a4df4d4/1 (21 bytes)
Fri Oct  5 16:17:18 2007:           AVP[05] NAS-Identifier....................
.....0x574c4331 (1464615729) (4 bytes)
Fri Oct  5 16:17:18 2007:           AVP[06] Airespace / WLAN-Identifier.........
.....0x00000002 (2) (4 bytes)
................................................................................
................................................................................
................................................................................
```

Información Relacionada

- Autenticación EAP con el servidor de RADIUS
- Diagnósticos 2003, troubleshooting, y recuperación del Active Directory del Servidor Windows
- Resolver problemas las operaciones del Active Directory
- Cisco LEAP
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Airespace VSA de Cisco en el ejemplo de configuración del servidor del Cisco Secure ACS
- Registro de AP Ligero (LAP) a un Controlador de LAN Inalámbrica (WLC)
- Guía del usuario para el Cisco Secure Access Control Server 4.1
- Soporte Técnico y Documentación - Cisco Systems