Configuración de la red TACACS+ del Cisco Unified Wireless

Contenido

Introducción

Este documento proporciona un ejemplo de configuración de Terminal Access Controller Access Control System Plus (TACACS+) en un Controlador de LAN inalámbrico Cisco (WLC) y un Cisco

Wireless Control System (WCS) para una red inalámbrica unificada de Cisco. Este documento también proporciona algunos consejos de Troubleshooting básico.

El TACACS+ es un protocolo cliente/servidor que proporciona la Seguridad centralizada para los usuarios que intentan tener el Acceso de administración a un router o a un servidor de acceso a la red. El TACACS+ proporciona estos servicios AAA:

- Autenticación de los usuarios que intentan iniciar sesión al equipo de red
- Autorización de determinar qué nivel de usuarios del acceso debe tener
- El considerar para no perder de vista todos los cambios el usuario hace

Refiera a configurar el TACACS+ para más información sobre los servicios AAA y las funciones TACACS+.

Refiera a la Comparación entre TACACS+ y RADIUS para una comparación del TACACS+ y del RADIUS.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar el WLCs y los Puntos de acceso ligeros (revestimientos) para la operación básica
- Conocimiento de los métodos del protocolo (LWAPP) y de la seguridad de red inalámbrica del Lightweight Access Point
- Conocimiento básico RADIUS y TACACS+
- Conocimiento básico de la configuración de ACS de Cisco

Componentes Utilizados

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

- Versión 4.0 del Cisco Secure ACS for Windows
- Controlador LAN de la tecnología inalámbrica de Cisco que funciona con la versión 4.1.171.0. Las funciones TACACS+ en el WLCs se soportan en versión de software 4.1.171.0 o más adelante.
- Cisco Wireless Control System que funciona con la versión 4.1.83.0. Las funciones TACACS+ en el WCS se soportan en versión de software 4.1.83.0 o más adelante.

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.

Implementación TACACS+ en el regulador

Autenticación

La autenticación se puede realizar usando una base de datos local, el servidor RADIUS, o TACACS+ que utiliza un nombre de usuario y una contraseña. La implementación no es completamente modular. Atan a los servicios de autenticación y autorización el uno al otro. Por ejemplo, si la autenticación se realiza usando la base de datos RADIUS/local, después la autorización no se realiza con el TACACS+. Utilizaría los permisos asociados para el usuario en el local o base de datos RADIUS, tal como solo lectura o de lectura/grabación, mientras que cuando la autenticación se realiza con el TACACS+, la autorización se ata al TACACS+.

En caso de que se configuren las varias bases de datos, un CLI se proporciona para dictar la secuencia en la cual la base de datos backend debe ser referida.

Autorización

La autorización es tarea basada bastante que una autorización basada por-comando real. Las tareas se asocian a las diversas lenguetas que corresponden a los siete elementos de la barra de menú que están actualmente en la red GUI. Éstos son los elementos de la barra de menú:

- MONITOR
- WLAN
- REGULADOR
- TECNOLOGÍA INALÁMBRICA
- SEGURIDAD
- ADMINISTRACIÓN
- COMANDO

La razón de esta asignación se basa en el hecho de que la mayoría de los clientes utilizan la interfaz Web para configurar el regulador en vez del CLI.

Un papel adicional de la Administración admin del pasillo (PASILLO) está disponible para los usuarios que necesitan tener privilegios admin del pasillo solamente.

La tarea que dan derecho un usuario se configura en el servidor TACACS+ (ACS) usando los pares de encargo del valor de atributo (AV). El usuario puede ser autorizado para uno o las tareas del múltiplo. La autorización mínima es MONITOR solamente y el máximo es TODO (autorizado para realizar las siete lenguetas). Si no dan derecho un usuario para una tarea determinada, todavía se permite al usuario acceder esa tarea en el modo de sólo lectura. Si se habilita la autenticación y el servidor de autenticación hace inalcanzable o incapaz de autorizar, el usuario no puede iniciar sesión al regulador.

Nota: Para que la autenticación de la administración básica vía el TACACS+ a tener éxito, usted debe configurar los servidores de la autenticación y autorización en el WLC. La configuración que considera es opcional.

Contabilidad

Las estadísticas ocurren siempre que una acción usuario-iniciada detalle se realice con éxito. Los atributos cambiados se abren una sesión el servidor de contabilidad TACACS+ junto con éstos:

- La identificación del usuario del individuo que realizó el cambio
- El host remoto de donde abren una sesión al usuario
- La fecha y hora en que el comando fue realizado
- Autorización llana del usuario
- Una cadena que proporciona la información en cuanto a qué acción fue realizada y los valores proporcionados

Si el servidor de contabilidad hace inalcanzable, el usuario puede todavía continuar la sesión.

Nota: Los registros de contabilidad no se generan del WCS en el Software Release 4.1 o Anterior.

Configuración TACACS+ en el WLC

La versión de software WLC 4.1.171.0 y posterior introduce nuevos CLI y la red GUI cambia para habilitar las funciones TACACS+ en el WLC. Los CLI introducidos se enumeran en esta sección para la referencia. Los cambios correspondientes para la red GUI se agregan conforme a la ficha de seguridad.

Este documento asume que la configuración básica del WLC está completada ya.

Para configurar el TACACS+ en el regulador del WLC, usted necesita completar estos pasos:

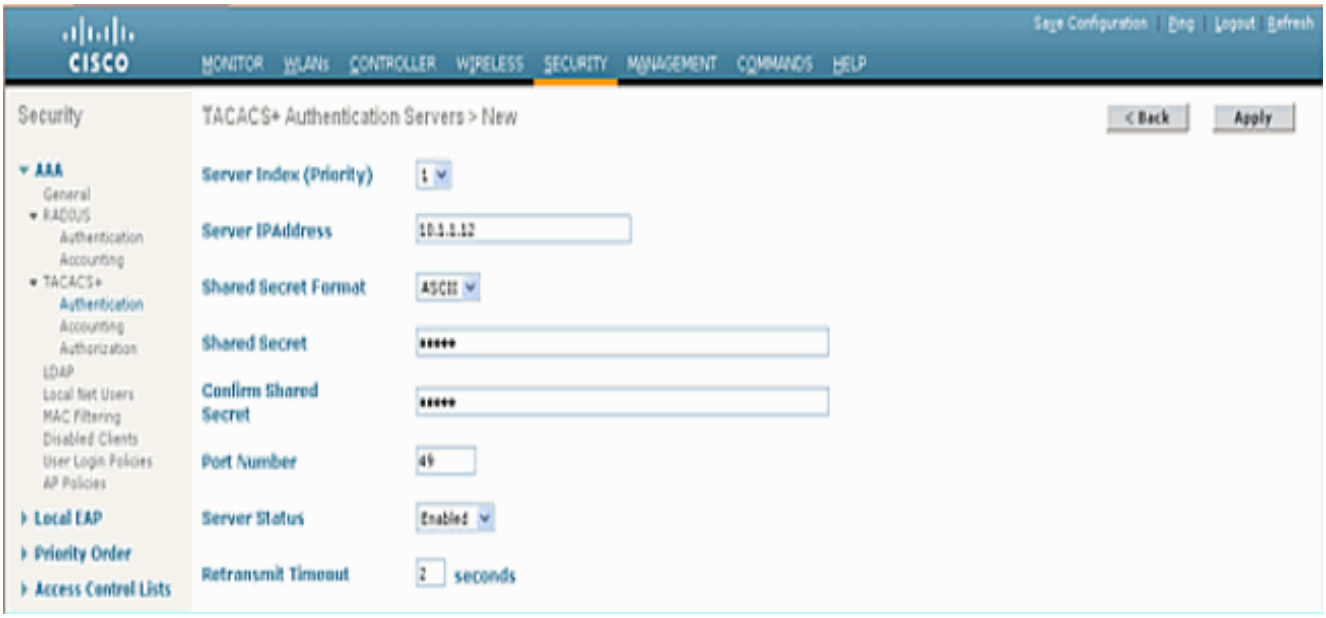
1. Agregue autenticación de TACACS+ un servidor
2. Agregue autorización TACACS+ un servidor
3. Agregue a un servidor de contabilidad TACACS+
4. Configure la orden de la autenticación

Agregue autenticación de TACACS+ un servidor

Complete estos pasos para agregar autenticación de TACACS+ un servidor:

1. Utilice el GUI, y vaya a la **Seguridad > al TACACS+ > a la autenticación**.

2. Agregue el IP Address del servidor TACACS+ y ingrese la clave secreta compartida. Si procede, cambie el puerto predeterminado de TCP/49.

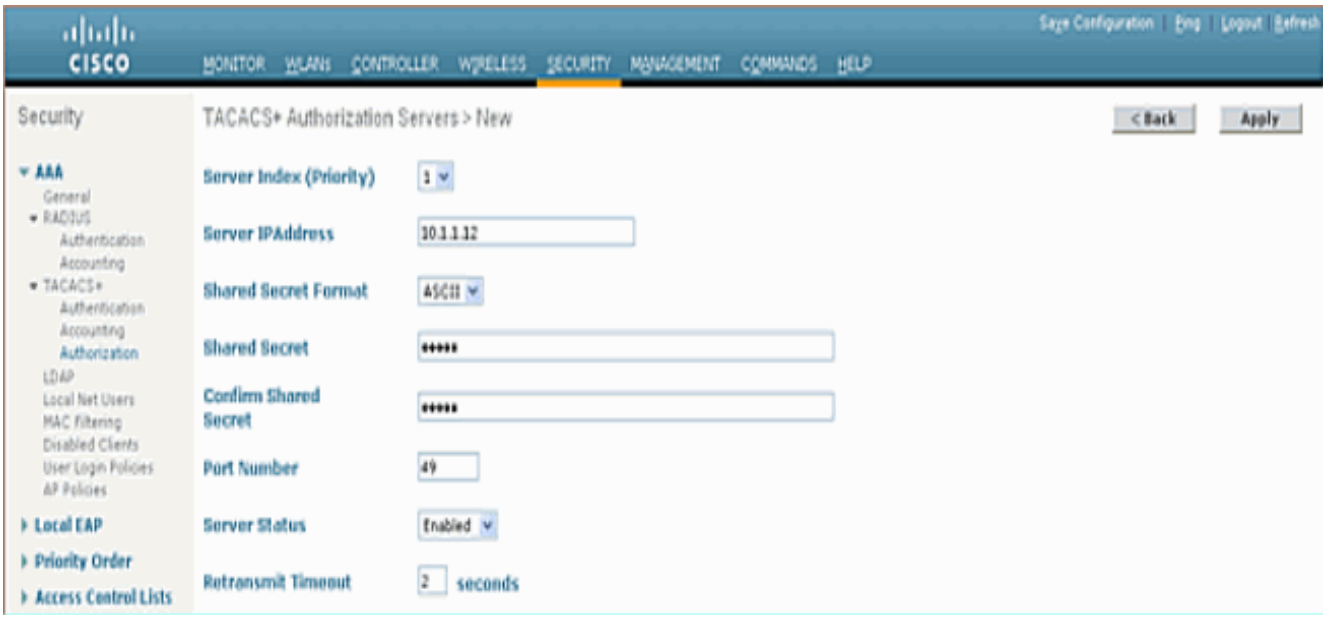


3. Haga clic en Apply (Aplicar).Usted puede lograr esto del CLI usando los **tacacs de los config que el auth agrega el** comando del **<secret> del** *[ascii/hex] del <port> del addr> de Index> <IP del <Server*:`(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123`

Agregue autorización TACACS+ un servidor

Complete estos pasos para agregar autorización TACACS+ un servidor:

1. Del GUI, vaya a la **Seguridad > al TACACS+ > a la autorización**.
2. Agregue el IP Address del servidor TACACS+ y ingrese la clave secreta compartida. Si procede, cambie el puerto predeterminado de TCP/49.



3. Haga clic en Apply (Aplicar).Usted puede lograr esto del CLI usando los **tacacs de los config que el athr agrega el** comando del **<secret> del** *[ascii/hex] del <port> del addr> de Index> <IP del <Server*:`(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123`

Agregue a un servidor de contabilidad TACACS+

Complete estos pasos para agregar a un servidor de contabilidad TACACS+:

1. Utilice el GUI, y vaya a la **Seguridad > al TACACS+ > a las estadísticas**.
2. Agregue el IP Address del servidor y ingrese la clave secreta compartida. Si procede, cambie el puerto predeterminado de TCP/49.

3. Haga clic en Apply (Aplicar).Usted puede lograr esto del CLI usando los **tacacs de los config que el acct agrega el** comando del **<secret> del** *[ascii/hex] del <port> del addr> de Index> <IP del <Server*:`(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123`

Configure la orden de la autenticación

Este paso explica cómo configurar la orden AAA de la autenticación cuando hay varias bases de datos configuradas. La orden de la autenticación puede ser **local y RADIUS**, o **local y TACACS**. La configuración de controlador predeterminada para la orden de la autenticación es *local y RADIUS*.

Complete estos pasos para configurar la orden de la autenticación:

1. Del GUI, vaya a la **Seguridad > a la orden > al usuario de administración de la prioridad**.
2. Seleccione la prioridad de la autenticación.En este ejemplo, se ha seleccionado el TACACS+.
3. El tecleo **se aplica** para que la selección ocurra.

Usted puede lograr esto del CLI usando el comando del **mgmt** *<server1> <server2> del* **auth aaa de los config**:`(Cisco Controller) >config aaa auth mgmt tacacs local`

Verifique la configuración

Esta sección describe los comandos usados para verificar la configuración TACACS+ en el WLC. Éstos son algunos comandos show útiles que ayudan a determinar si la configuración está correcta:

- **muestre el auth aaa** — Provee información por orden de la autenticación.`(Cisco Controller) >`**`show aaa auth`** `Management authentication server order:`
  `1..... local`
  `2..... Tacacs`
- **muestre el resumen de los tacacs** — Visualiza un resumen de servicios y de estadísticas TACACS+.`(Cisco Controller) >`**`show tacacs summary`** `Authentication Servers Idx Server Address Port State Tout --- --------------- ------ -------- ---- 1 10.1.1.12 49 Enabled 2 Authorization Servers Idx Server Address Port State Tout --- --------------- ------ ------- - ---- 1 10.1.1.12 49 Enabled 2 Accounting Servers Idx Server Address Port State Tout --- -- ------------- ------ -------- ---- 1 10.1.1.12 49 Enabled 2`
- **muestre el stats del auth de los tacacs** — Estadísticas del servidor de las visualizaciones autenticación de TACACS+.`(Cisco Controller) >`**`show tacacs auth statistics`** `Authentication Servers: Server Index..... 1` **`Server Address..... 10.1.1.12`** `Msg Round Trip Time..... 0 (1/100 second) First Requests..... 7 Retry Requests..... 3 Accept Responses..... 3 Reject Responses..... 0 Error Responses..... 0 Restart Responses..... 0 Follow Responses..... 0 GetData Responses..... 0 Encrypt no secret Responses..... 0 Challenge Responses..... 0 Malformed Msgs..... 0 Bad Authenticator Msgs..... 0 Timeout Requests..... 12 Unknowntype Msgs..... 0 Other Drops..... 0`
- **muestre el stats del athr de los tacacs** — Estadísticas del servidor de las visualizaciones autorización TACACS+.`(Cisco Controller) >`**`show tacacs athr statistics`** `Authorization Servers: Server Index..... 1` **`Server Address..... 10.1.1.12`** `Msg Round Trip Time..... 0 (1/100 second) First Requests..... 3 Retry Requests..... 3 Received Responses..... 3 Authorization Success..... 3 Authorization Failure..... 0 Challenge Responses..... 0 Malformed Msgs..... 0 Bad Athrenticator Msgs..... 0 Timeout Requests..... 0 Unknowntype Msgs..... 0 Other Drops..... 0`
- **muestre el stats del acct de los tacacs** — Estadísticas del servidor de contabilidad de las visualizaciones TACACS+.`(Cisco Controller) >`**`show tacacs acct statistics`** `Accounting Servers: Server Index..... 1` **`Server Address..... 10.1.1.12`** `Msg Round Trip Time..... 0 (1/100 second) First Requests..... 133 Retry Requests..... 0 Accounting Response..... 0 Accounting Request Success..... 0`

```
Accounting Request Failure..................... 0 Malformed
Msgs.................................. 0 Bad Authenticator Msgs.....................
0 Timeout Requests............................... 399 Unknowntype
Msgs................................ 0 Other Drops.................................... 0
```

Servidor del Cisco Secure ACS de la configuración

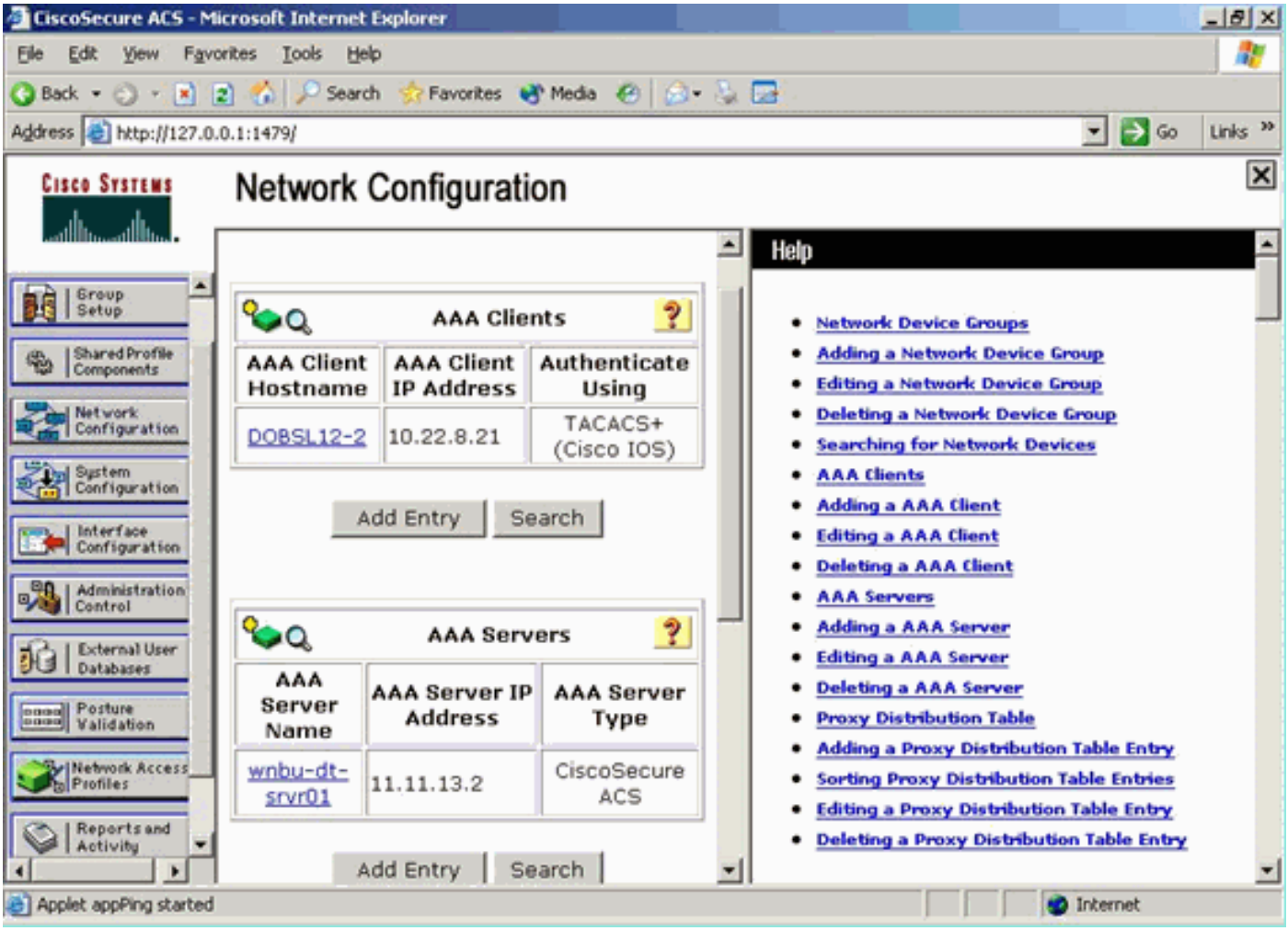
Esta sección proporciona los pasos implicados en el servidor ACS TACACS+ para crear los servicios y los atributos personalizados, y asigna los papeles a los usuarios o a los grupos.

La creación de los usuarios y del grupo no se explica en esta sección. Se asume que crean a los usuarios y a los grupos según las necesidades. Refiera al guía del usuario para el servidor 4.0 del Cisco Secure ACS for Windows para la información sobre cómo crear los usuarios y a los grupos de usuarios.

Configuración de red

Siga este paso:

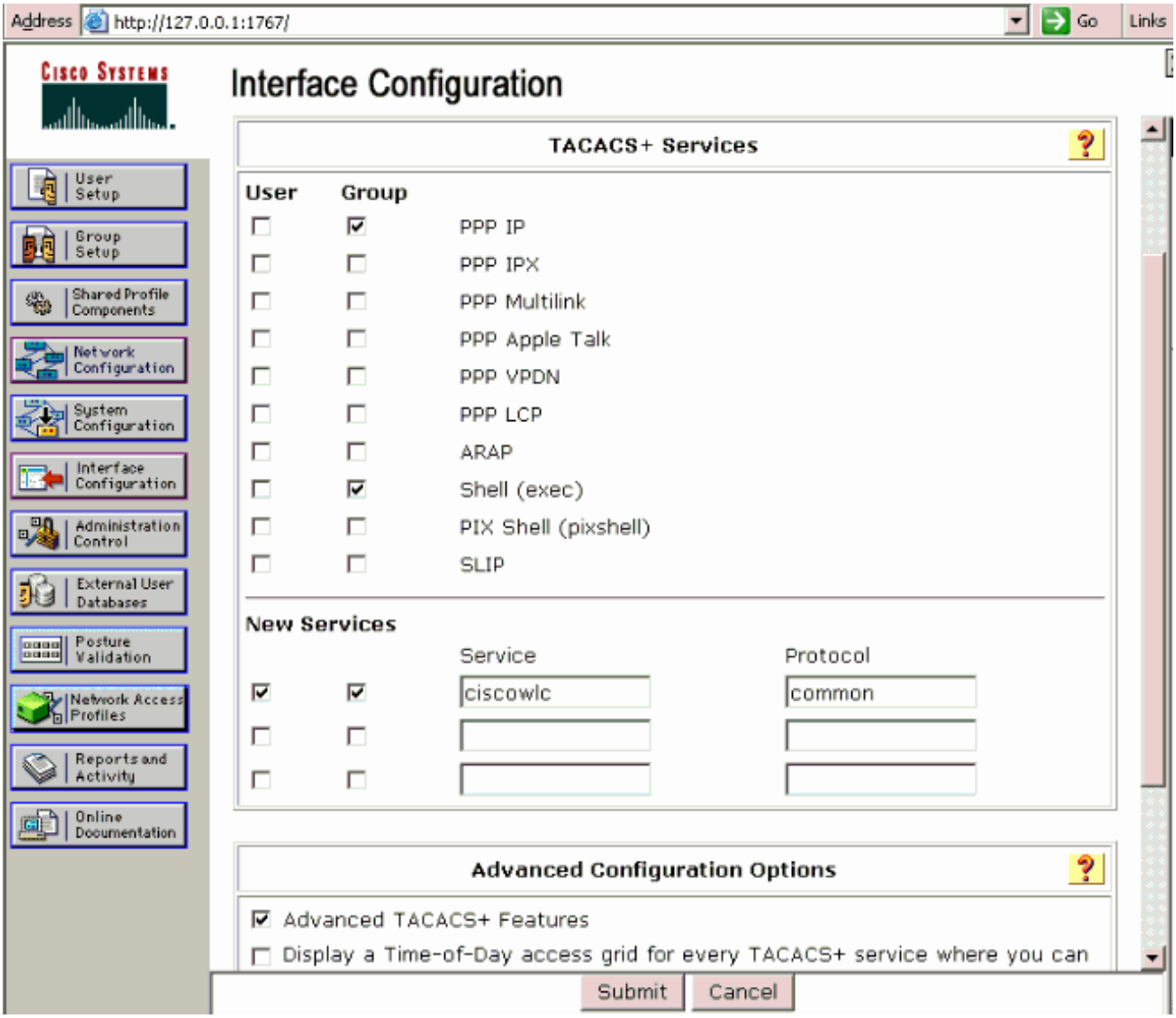
Agregue el IP Address de administración del regulador como cliente AAA con el mecanismo de autenticación como TACACS+ (Cisco IOS).



Configuración de la Interfaz

Complete estos pasos:

1. En el menú de la configuración de la interfaz, seleccione el link **TACACS+** (Cisco IOS).
2. Habilite los **nuevos servicios**.
3. Marque los cuadros del **usuario** y de **casilla del grupo**.
4. Ingrese el **ciscowlc** para el servicio y el **campo común** para el protocolo.
5. Habilite las **características del TACACS+ avanzado**.

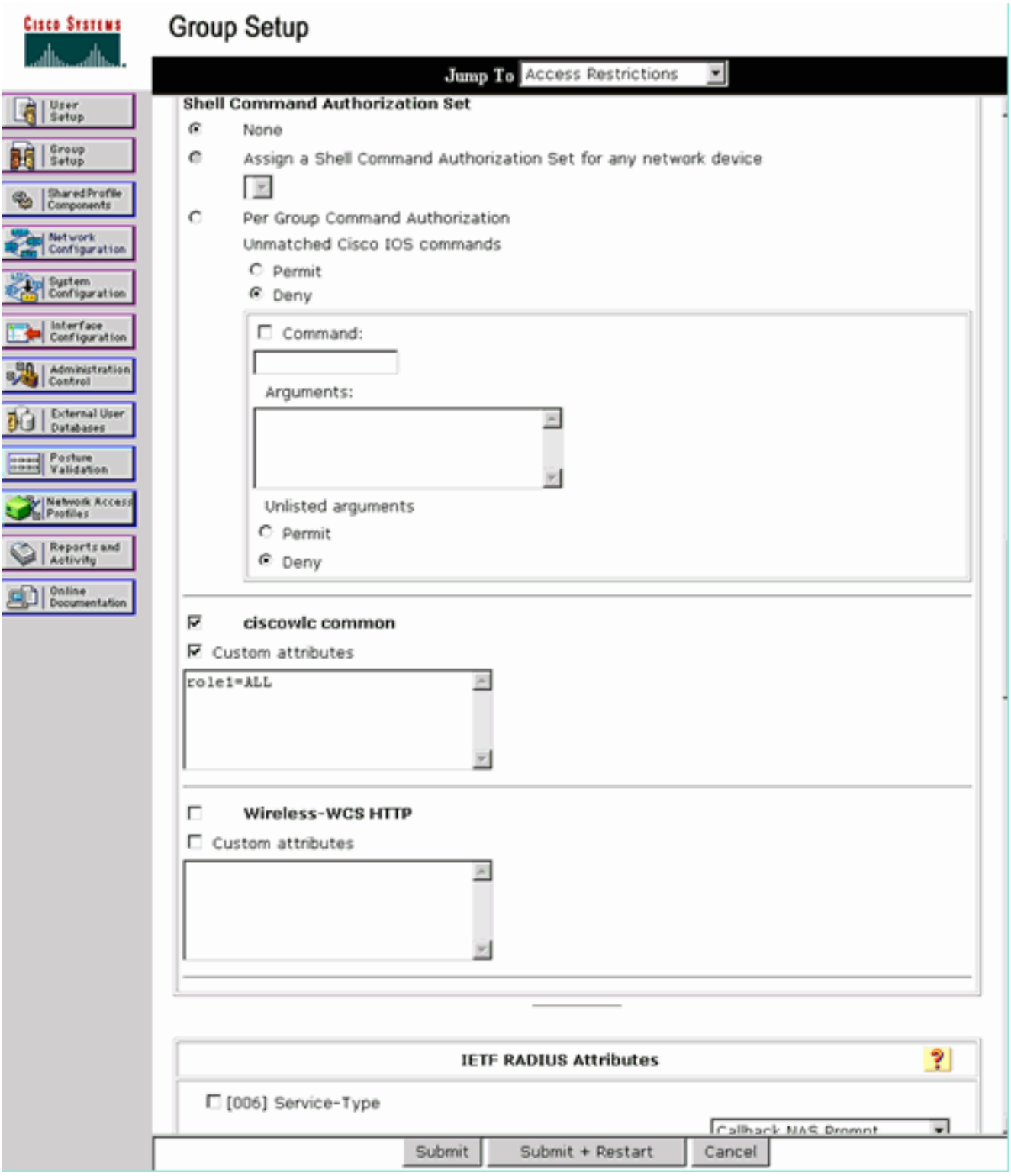


6. El tecleo **somete** para aplicar los cambios.

Usuario/configuración de grupo

Complete estos pasos:

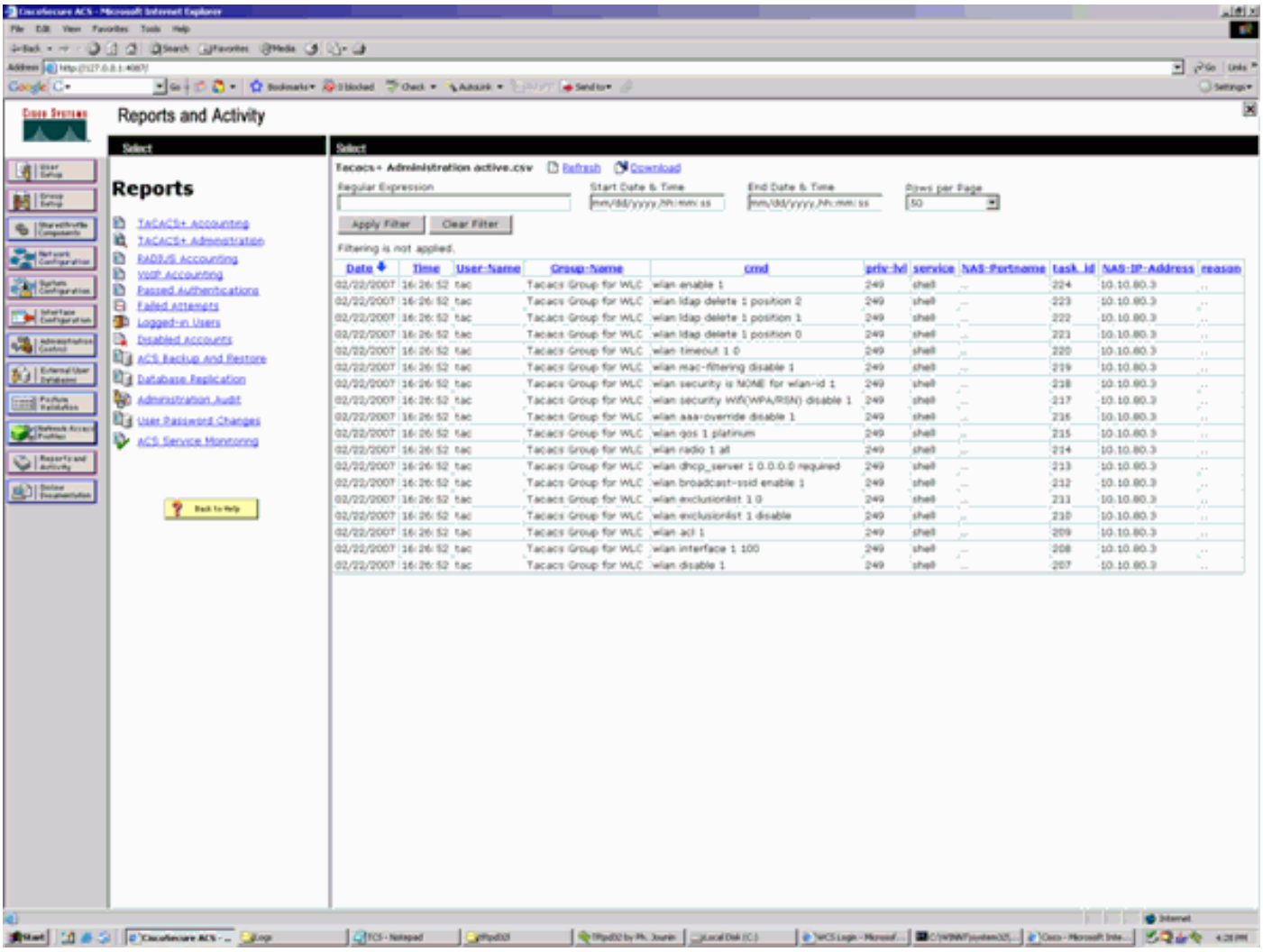
1. Seleccione un usuario/a un grupo previamente creados.
2. Vaya a las **configuraciones TACACS+**.
3. Marque la casilla de verificación que corresponde al servicio del *ciscowlc* que fue creado en la sección de configuración de la interfaz.
4. Marque la casilla de verificación de los **atributos personalizados**.



5. En el cuadro de texto debajo de los atributos personalizados, ingrese este texto si las necesidades creadas por el usuario acceden solamente al WLAN, a la SEGURIDAD y al REGULADOR: **role1=WLAN role2=SECURITY role3=CONTROLLER**.Si las necesidades de usuario acceden solamente a la ficha de seguridad, ingrese este texto: **role1=SECURITY**.El papel corresponde a los siete elementos de la barra de menú en la red GUI del regulador. Los elementos de la barra de menú son MONITOR, red inalámbrica (WLAN), REGULADOR, TECNOLOGÍA INALÁMBRICA, SEGURIDAD, ADMINISTRACIÓN y COMANDO.
6. Ingrese el papel que las necesidades de un usuario de role1, role2 etc. Si las necesidades de un usuario todos los papeles, entonces la palabra clave **TODA** se utilizan. Para el papel admin del pasillo, el **PASILLO de la** palabra clave debe ser utilizado.

Registros de contabilidad en el Cisco Secure ACS

Los registros de contabilidad TACACS+ del WLC están disponibles en el Cisco Secure ACS en la administración TACACS+ de los informes y de la actividad:



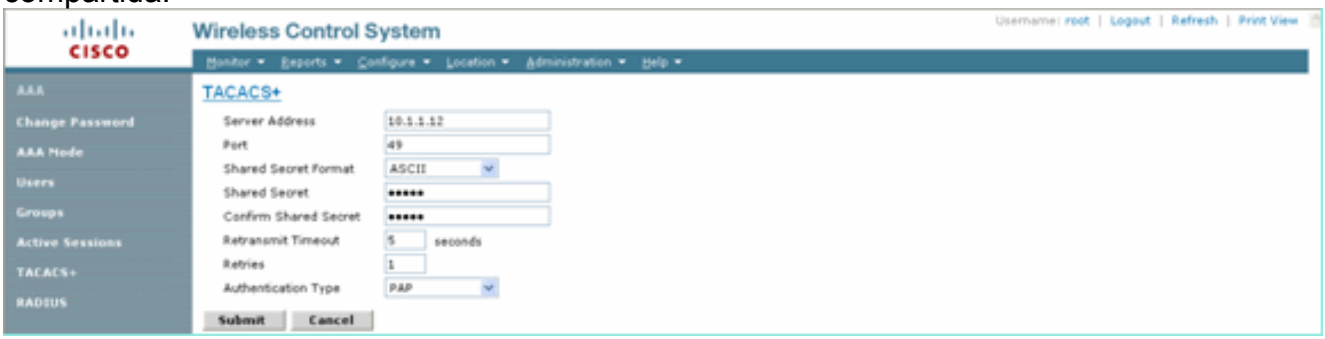
Configuración TACACS+ en el WCS

Complete estos pasos:

1. Del GUI, inicie sesión al WCS con la cuenta raíz.
2. Agregue el servidor TACACS+. Va a la **administración >AAA > el servidor TACACS+ > Add TACACS+**.

3. Agregue los detalles del servidor TACACS+, tales como dirección IP, número del puerto (49 es predeterminados), y clave secreta

compartida.



4. Habilite autenticación de TACACS+ para la administración en el WCS. Va al **modo de la administración >AAA >AAA > el TACACS+ selecto**.

WCS usando los dominios virtuales

El dominio virtual es una nueva función introducida con la versión 5.1 WCS. Un dominio virtual WCS consiste en un conjunto de dispositivos y las correspondencias y restringe una opinión de usuario a la información relevante a estos dispositivos y correspondencias. Con un dominio virtual, un administrador puede asegurarse de que los usuarios puedan ver solamente los dispositivos y las correspondencias de los cuales son responsables. Además, debido a los filtros del dominio virtual, los usuarios pueden configurar, ver las alarmas, y generar los informes por solamente su parte de asignada la red. El administrador especifica un conjunto de los dominios virtuales permitidos para cada usuario. Solamente uno de éstos puede ser activo para ese usuario en el login. El usuario puede cambiar el dominio virtual actual seleccionando un diverso dominio virtual permitido del menú desplegable del dominio virtual en la cima de la pantalla. Todos los informes, las alarmas, y otras funciones ahora son filtrados por ese dominio virtual.

Si hay solamente un dominio virtual definido (raíz) en el sistema y el usuario no tiene ninguna dominios virtual en los atributos personalizados coloca en el servidor TACACS+/RADIUS, asignan el usuario el dominio virtual de la raíz por abandono.

Si hay más de un dominio virtual, y el usuario no tiene ninguna atributos especificada, después bloquean al usuario de la apertura de sesión. Para permitir que el usuario inicie sesión, los atributos personalizados del dominio virtual se deben exportar al servidor Radius/TACACS+.

La ventana de los atributos personalizados del dominio virtual permite que usted indique los datos apropiados del protocol específico para cada dominio virtual. El botón de la exportación en la barra lateral de la jerarquía del dominio virtual preformatea los atributos RADIUS y TACACS+ del dominio virtual. Usted puede copiar y pegar estos atributos en el servidor ACS. Esto permite que usted copie solamente los dominios virtuales aplicables a la pantalla del servidor ACS y se asegura de que los usuarios tienen solamente acceso a estos dominios virtuales.

Para aplicar los atributos preformateados RADIUS y TACACS+ al servidor ACS, complete los

pasos explicados en el dominio virtual RADIUS y TACACS+ atribuye la sección.

Configure el Cisco Secure ACS para utilizar el WCS

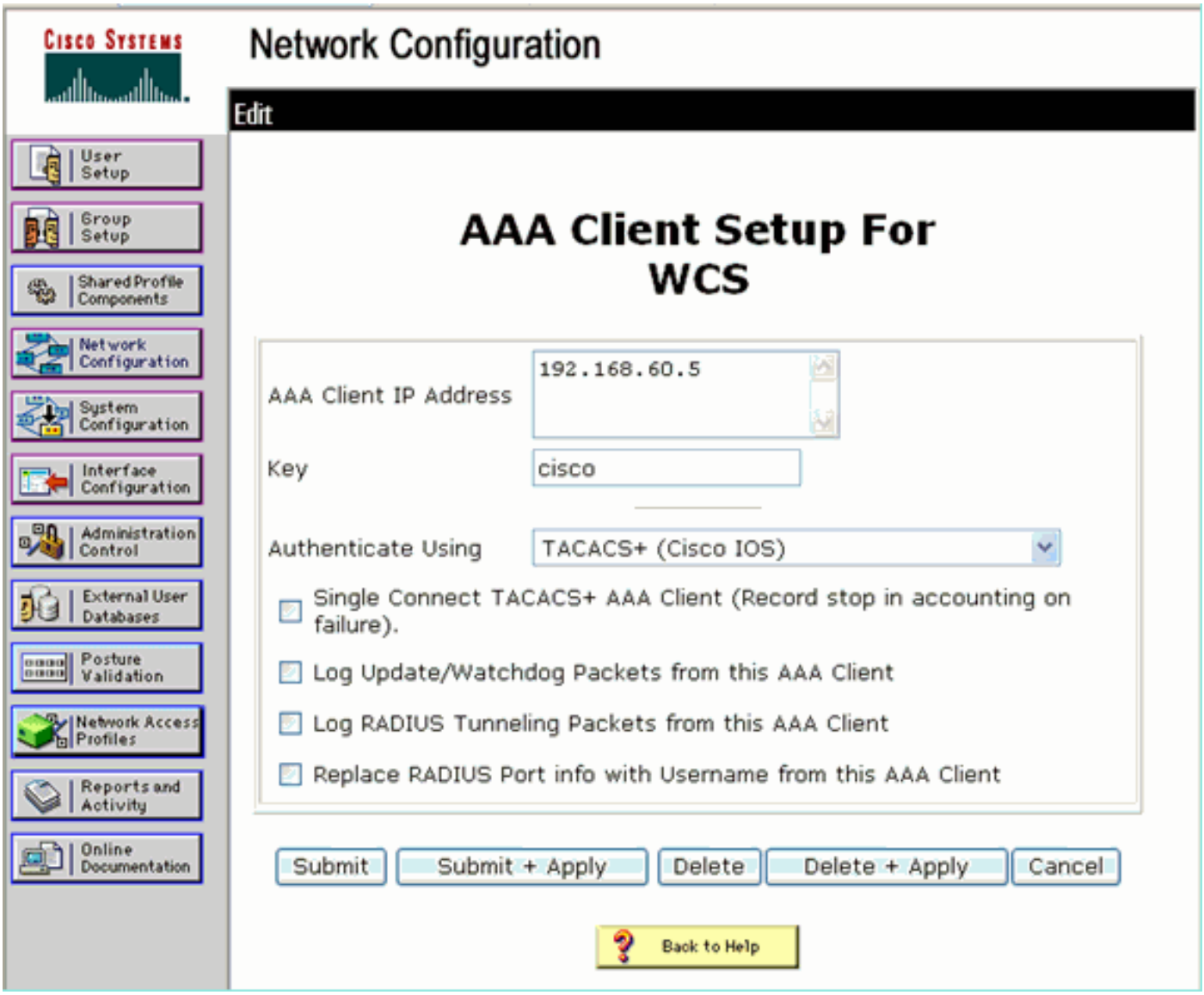
La sección proporciona los pasos implicados en el servidor ACS TACACS+ para crear los servicios y los atributos personalizados, y asigna los papeles a los usuarios o a los grupos.

La creación de los usuarios y del grupo no se explica en esta sección. Se asume que crean a los usuarios y a los grupos según las necesidades.

Configuración de red

Siga este paso:

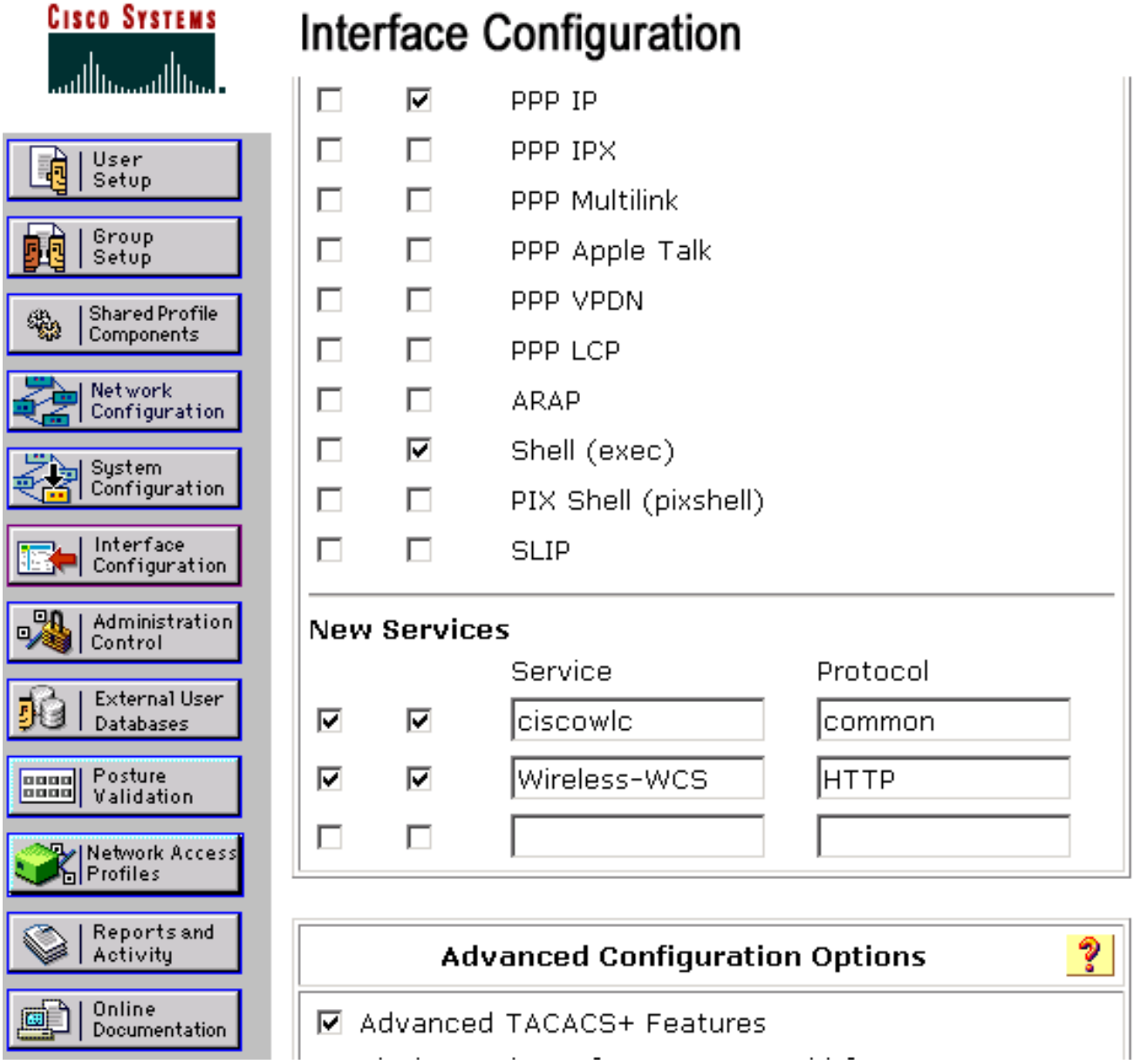
Agregue la dirección IP WCS como cliente AAA con el mecanismo de autenticación como TACACS+ (Cisco IOS).



Configuración de la Interfaz

Complete estos pasos:

1. En el menú de la configuración de la interfaz, seleccione el link **TACACS+** (Cisco IOS).
2. Habilite los **nuevos servicios**.
3. Marque los cuadros del **usuario** y de **casilla del grupo**.
4. Ingrese el Tecnología inalámbrica-**WCS** para el servicio y el **HTTP** para el protocolo.**Nota:** El HTTP debe estar en los CASQUILLOS.
5. Habilite las **características del TACACS+ avanzado**.

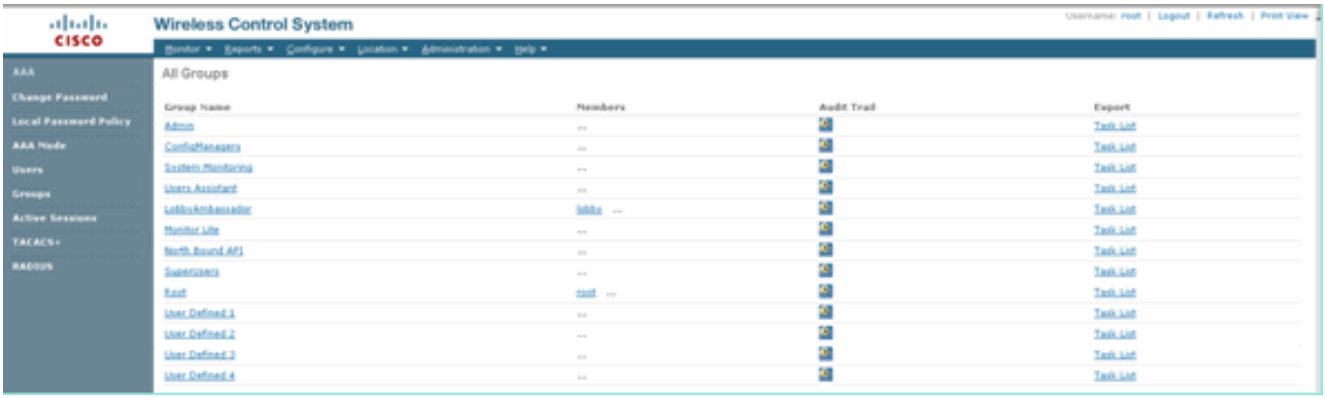


6. El tecleo **somete** para aplicar los cambios.

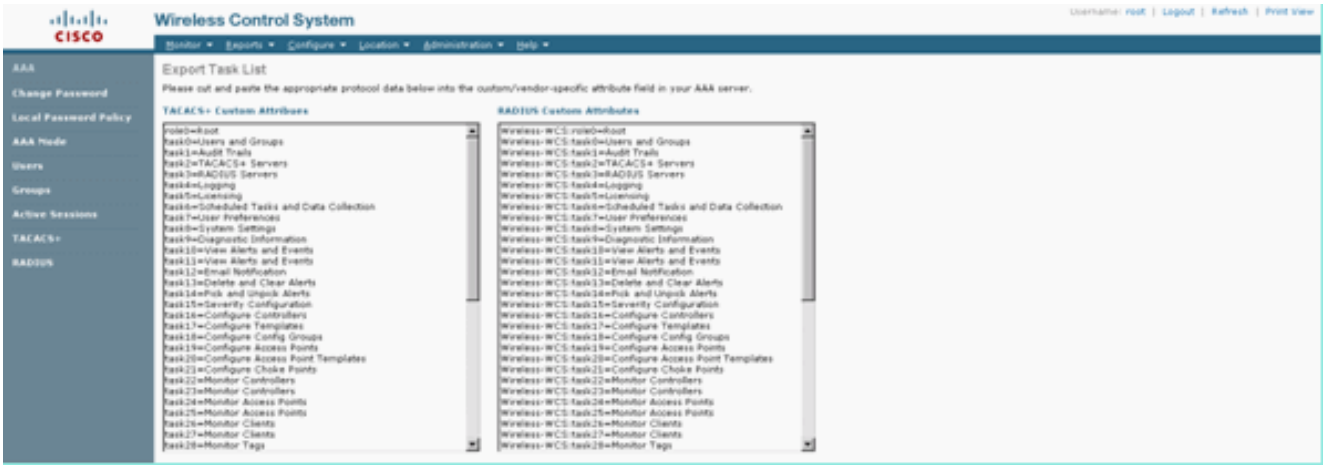
Usuario/configuración de grupo

Complete estos pasos:

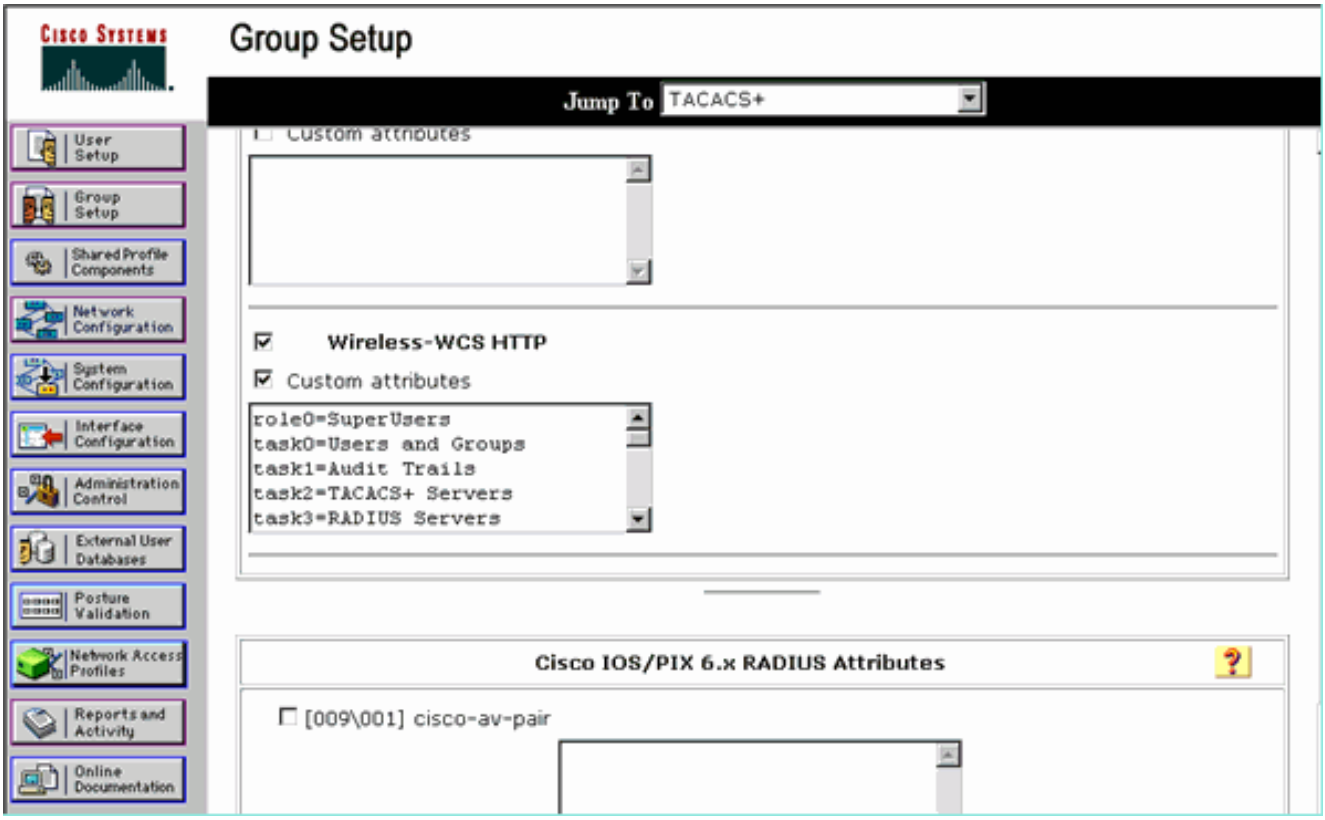
1. En el WCS GUI, navegue a la **administración >AAA > Groups** para seleccionar a los grupos de usuarios preconfigurados uces de los, tales como superusuarios en el WCS.



2. Seleccione la lista de tareas para los grupos de usuarios y la goma preconfigurados de la copia al
ACS.



3. Seleccione un usuario/a un grupo previamente creados y vaya a las **configuraciones TACACS+**.
4. En ACS GUI, seleccione la casilla de verificación que corresponde al servicio Tecnología inalámbrica-WCS que fue creado anterior.
5. En ACS GUI, marque el cuadro de los **atributos personalizados**.
6. En el cuadro de texto debajo de los atributos personalizados, ingrese este papel y encargue la información copiada del WCS. Por ejemplo, ingrese la lista de tareas permitidas por los SuperUsers.



7. Entonces, login al WCS con el nombre de usuario/la contraseña creados recientemente en el ACS.

Depuraciones

Debugs del WLC para role1=ALL

```
(Cisco Controller) >debug aaa tacacs enable (Cisco Controller) >Wed Feb 28 17:36:37 2007:
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:36:37 2007: tplus response: type=1
seq_no=2 session_id=5eaa857e length=16 encrypted=0 Wed Feb 28 17:36:37 2007:
TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction Wed Feb 28
17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e length=6 encrypted=0 Wed Feb
28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28
17:36:37 2007: Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:36:37 2007: author response
body: status=1 arg_cnt=1 msg_len=0 data_len=0 Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole fffffff8
```

Debugs del WLC para los papeles múltiples

```
(Cisco Controller) >debug aaa tacacs enable Wed Feb 28 17:59:33 2007: Forwarding request to
10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2 session_id=b561ad88
length=16 encrypted=0 Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:59:34
2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:59:34 2007:
processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:59:34 2007: tplus response:
type=1 seq_no=4 session_id=b561ad88 length=6 encrypted=0 Wed Feb 28 17:59:34 2007:
tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:59:34 2007:
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: author response body: status=1
arg_cnt=4 msg_len=0 data_len=0 Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN] Wed Feb 28
17:59:34 2007: arg[1] = [16][role2=CONTROLLER] Wed Feb 28 17:59:34 2007: arg[2] =
[14][role3=SECURITY] Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS] Wed Feb 28 17:59:34
2007: User has the following mgmtRole 150
```

Debugs de un WLC para la falla de autorización

```
(Cisco Controller) >debug aaa tacacs enable Wed Feb 28 17:53:04 2007: Forwarding request to
10.1.1.12 port=49 Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0 Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:53:04
2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:53:04 2007:
processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:53:04 2007: tplus response:
type=1 seq_no=4 session_id=89c553a1 length=6 encrypted=0 Wed Feb 28 17:53:04 2007:
tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:53:04 2007:
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:53:04 2007: author response body:
status=16 arg_cnt=0 msg_len=0 data_len=0 Wed Feb 28 17:53:04 2007:User has the following
mgmtRole 0 Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

Información Relacionada

- Controlador LAN de la tecnología inalámbrica de Cisco (WLC) y ejemplo de configuración de Cisco ACS 5.x (TACACS+) para la autenticación Web
- Configuración de TACACS+
- Cómo configurar la autenticación de TACACS y la autorización para los usuarios Admin y NON-Admin en ACS 5.1
- Comparación de TACACS+ y RADIUS
- Soporte Técnico y Documentación - Cisco Systems