el nivel de privilegio de 5760 interfaces Web basó el ejemplo de configuración del control de acceso con el Access Control Server de Cisco (el ACS)

Contenido

Introducción

Este documento explicará cómo crear Cisco ACS autenticación de TACACS+ y los perfiles de la autorización con diversos niveles de privilegio e integrarlo con 5760 para el acceso al WebUI. Esta característica se soporta a partir del 3.6.3 hacia adelante (pero no en 3.7.x en la época de esta escritura).

Prerequisites

Requisitos

Se asume que el lector es familiar con Cisco ACS y configuración de controlador convergida del acceso. Este documento se centra solamente en la interacción entre esos 2 componentes en el ámbito de autorización TACACS+.

Componentes Utilizados

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

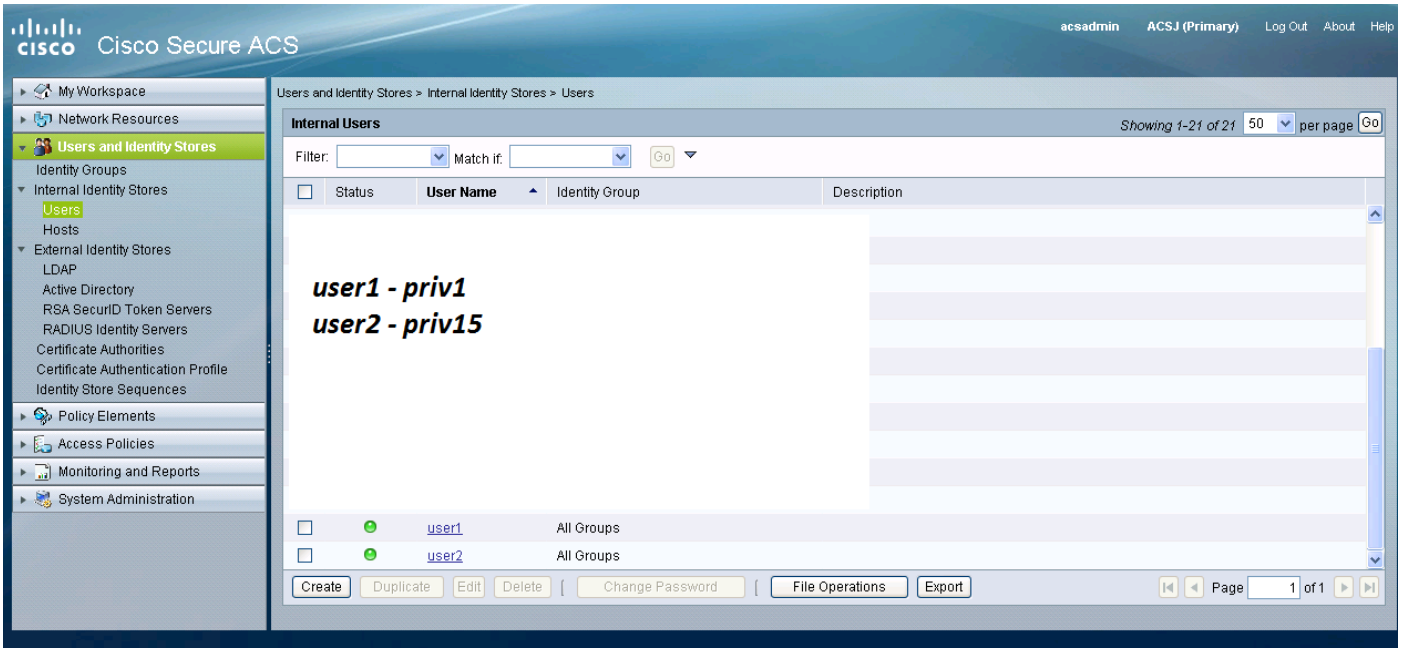
- Cisco convergió el acceso 5760, la versión 3.6.3
- Servidor de control de acceso de Cisco (ACS) 5.2

Configuración

Cree a algunos usuarios a prueba en el ACS

Haga clic en a los “usuarios y la identidad salva”, después selecciona a los “usuarios”.

Haga clic “crean” y configuran a algunos usuarios a prueba tales como ilustrado abajo.



Configurar los elementos de la directiva y los perfiles del shell

Usted necesita crear 2 perfiles para los 2 diversos tipos de acceso. El privilegio 15 en el mundo de los tacacs de Cisco significa proporcionar al acceso total al dispositivo sin ninguna restricción. Privilegie 1 por otra parte permitirá que usted inicie sesión y que ejecute solamente las cantidades limitadas de comandos. Abajo está una descripción breve de los niveles de acceso proporcionados por Cisco.

nivel de privilegio 1 = sin privilegios (el prompt es router>), el nivel predeterminado para abrir una sesión

nivel de privilegio 15 = privilegiado (la solicitud es router#), el nivel luego de pasar al modo de activación

el nivel de privilegio 0 = utilizado raramente, pero incluye 5 comandos: **neutralización**, **permiso**, **salida**, **ayuda**, y **logout**

En 5760, los niveles 2-14 se consideran lo mismo que el nivel 1. Se dan el mismo privilegio que 1. **No configure los tacacs que los niveles de privilegio con certeza ordenan en los 5760**. El acceso UI por las lenguetas no se soporta en 5760. Usted puede tener el acceso total (priv15) o solamente acceso a la lengueta del monitor (priv1). También, los usuarios con el nivel de privilegio 0 no alowed para iniciar sesión.

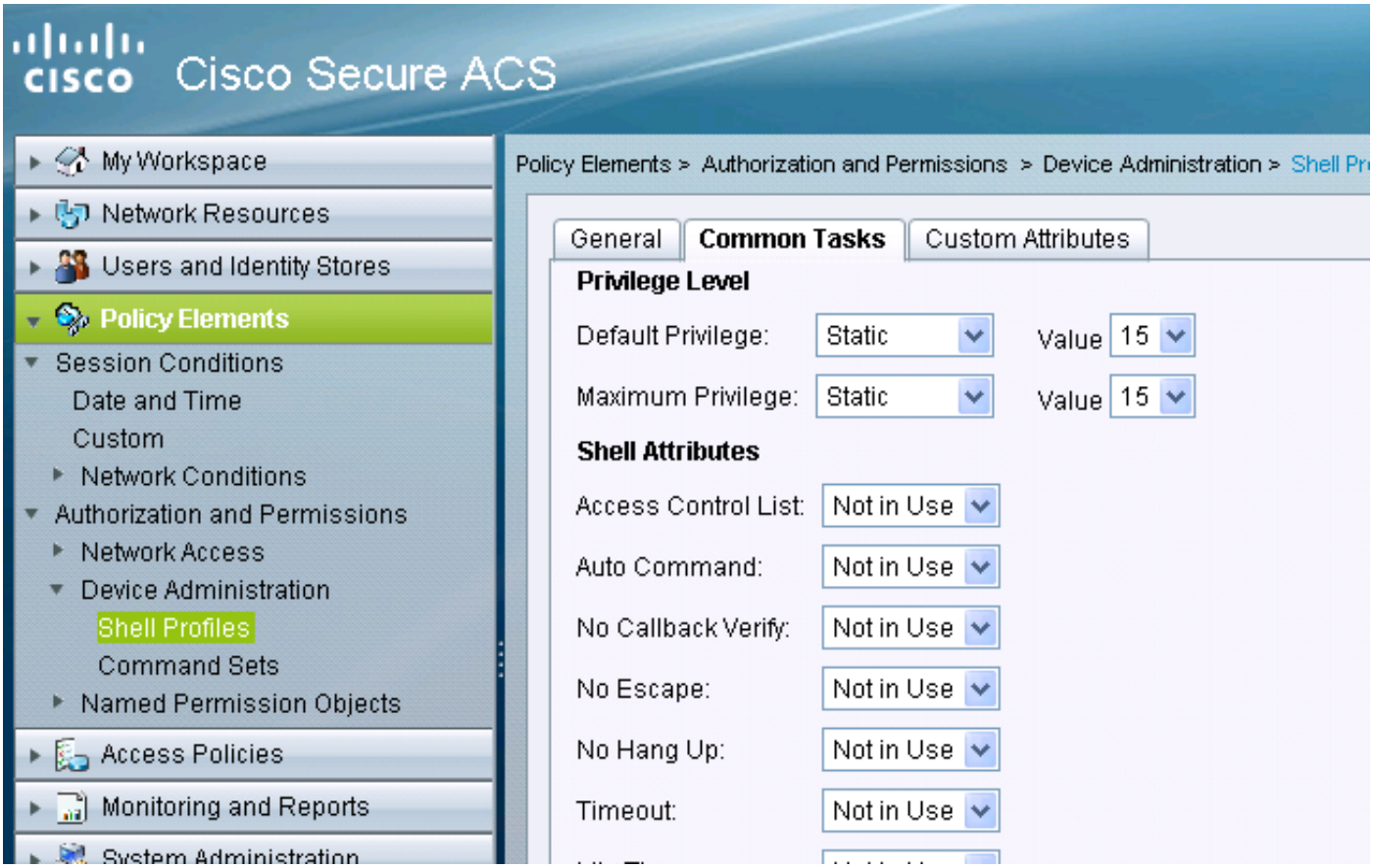
Crear el perfil llano del acceso del shell del privilegio 15

Usando la captura de pantalla abajo cree ese perfil:

Haga clic en los “elementos de la directiva”. Haga clic en el “shell perfila”.

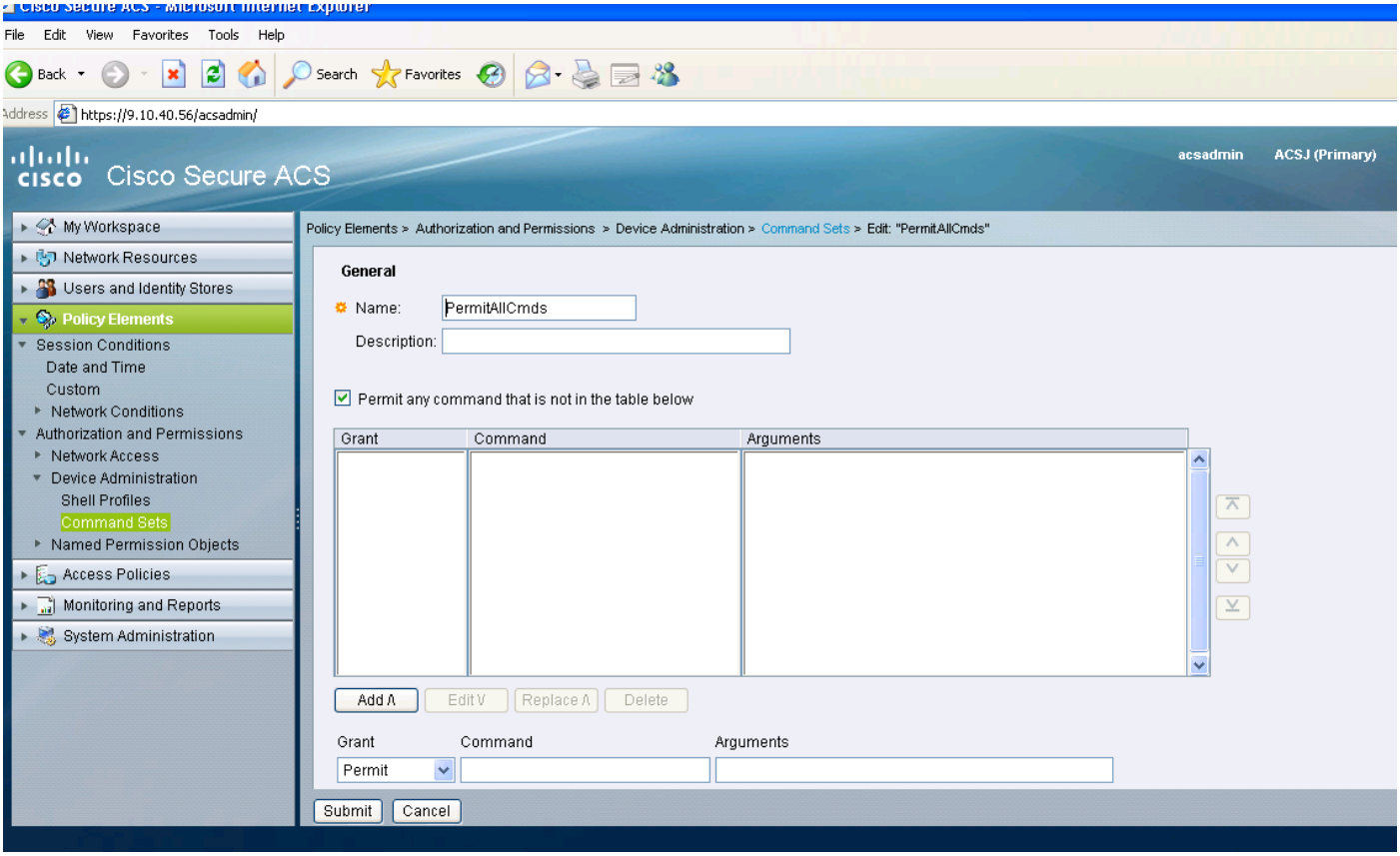
Cree un nuevo.

Entre en las “tareas comunes” lengueta y fije los niveles de privilegio predeterminados y máximos a 15.



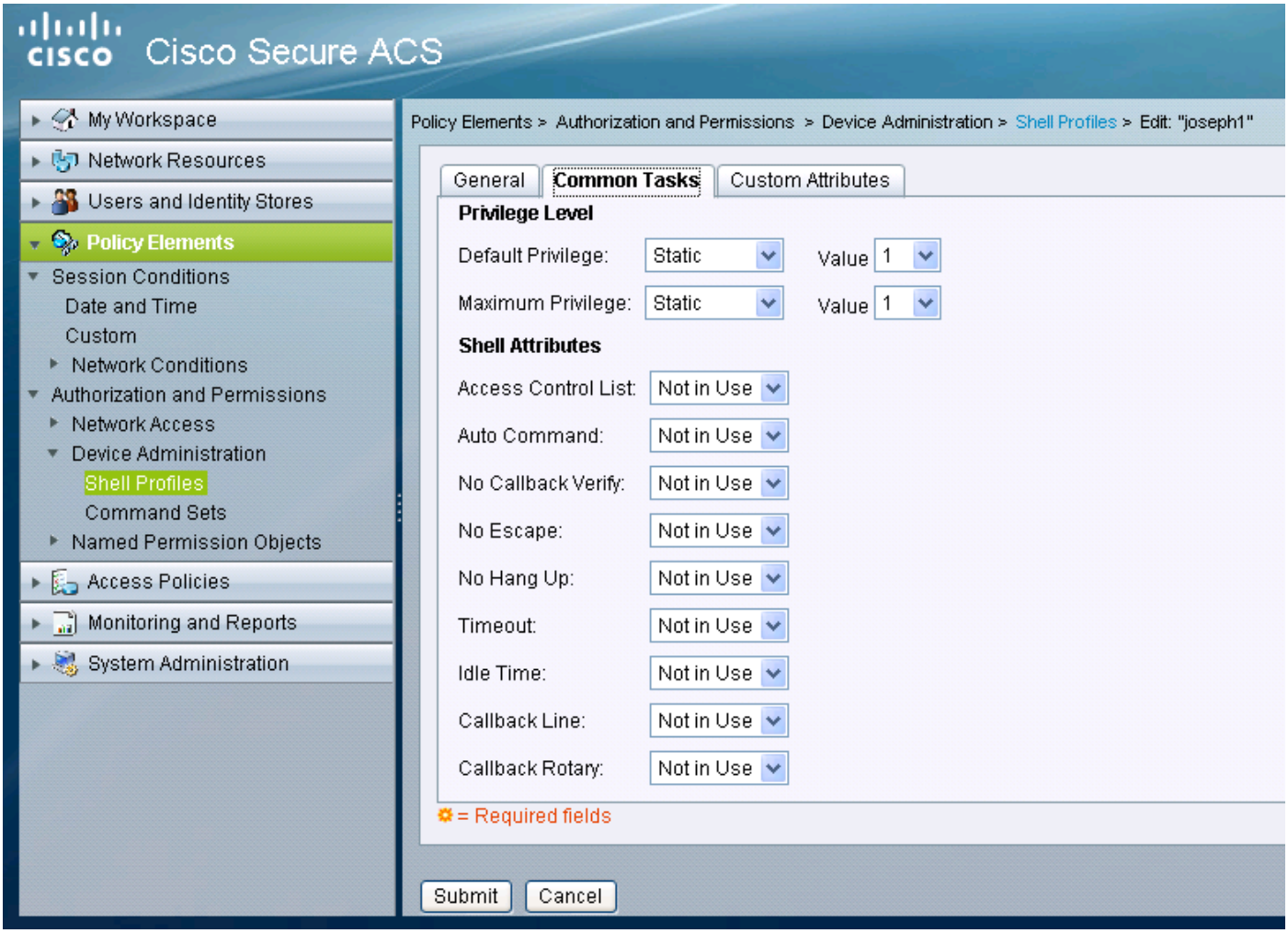
Crear a los comandos estableces para el Usuario administrador

Los comandos estableces son conjuntos de comandos usados por todos los dispositivos de los tacacs. Pueden ser utilizados para restringir los comandos que se permite a un usuario utilizar si está asignado ese perfil específico. Puesto que en los 5760, la restricción se hace en el código de Webui basado en el nivel de privilegio pasajero, los comandos estableces para el privilegio level1 y 15 son lo mismo.



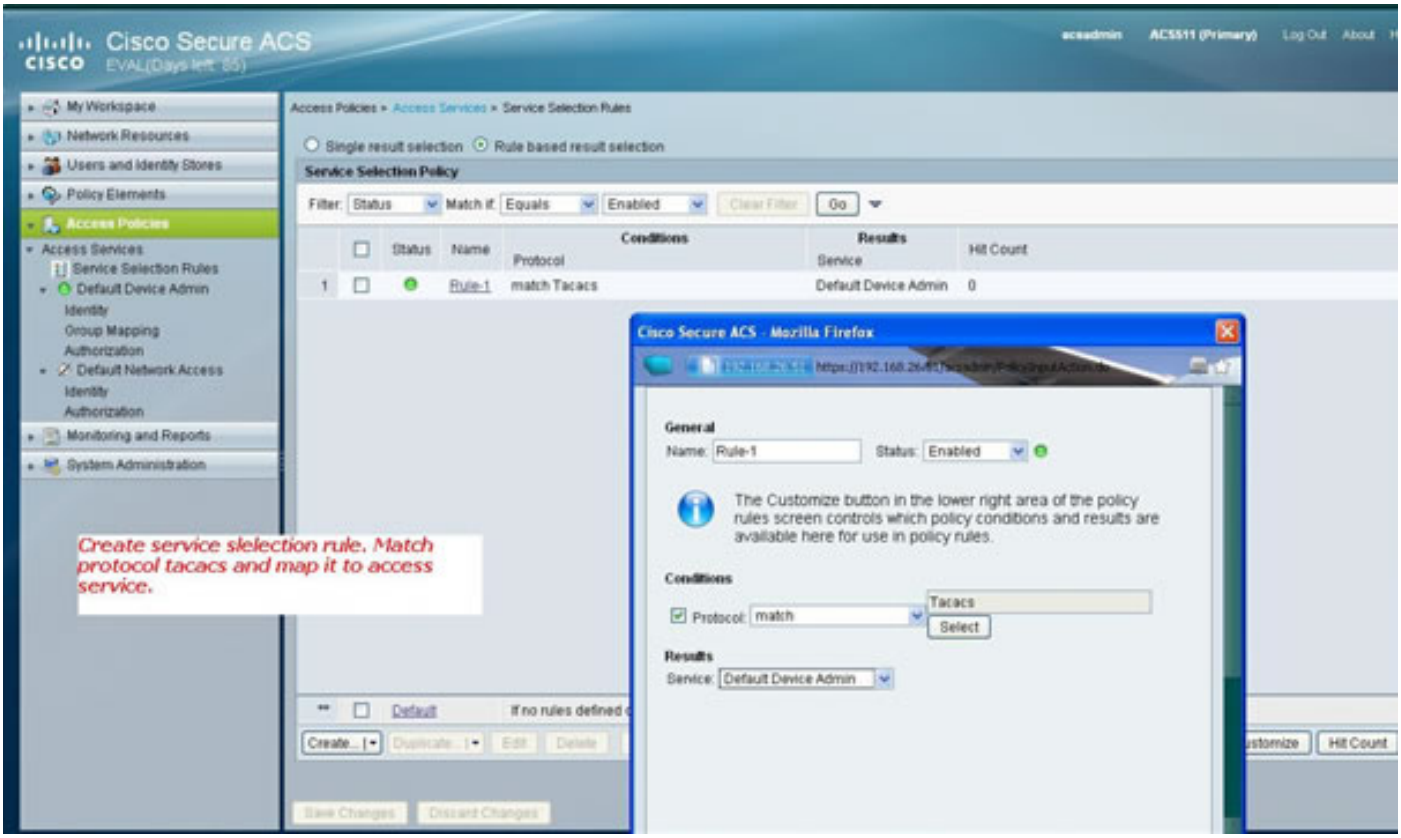
Crear el perfil del shell para el usuario del read only

Cree otro perfil del shell para los usuarios solo lecturas. Este perfil diferenciará por el hecho que los niveles de privilegio se fijan a 1.



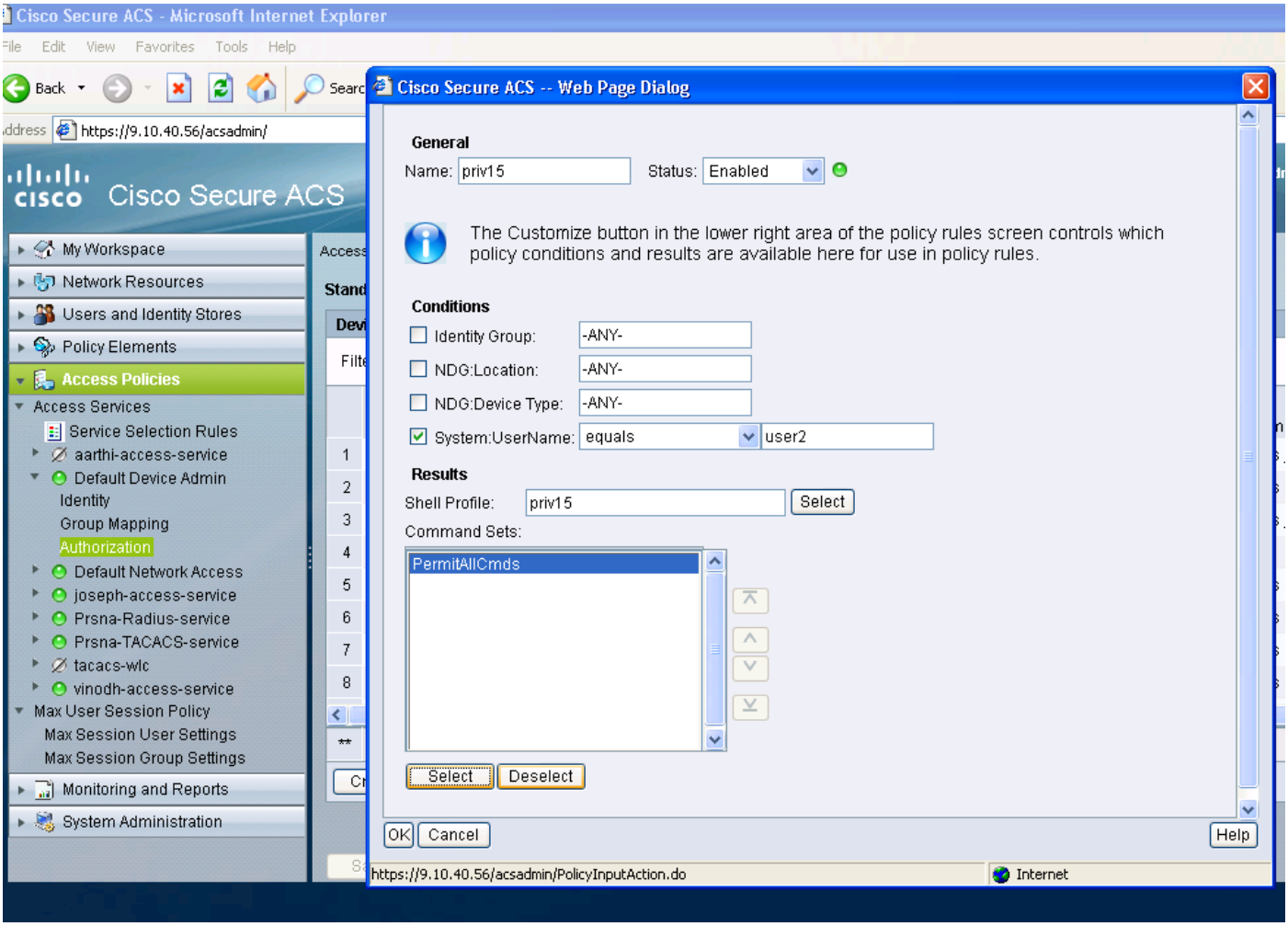
Cree una regla de selección del servicio para hacer juego el protocolo de los tacacs

Dependiendo de sus directivas y configuración, aseegurese que usted tiene tacacs que corresponden con de una regla que vienen de los 5760.



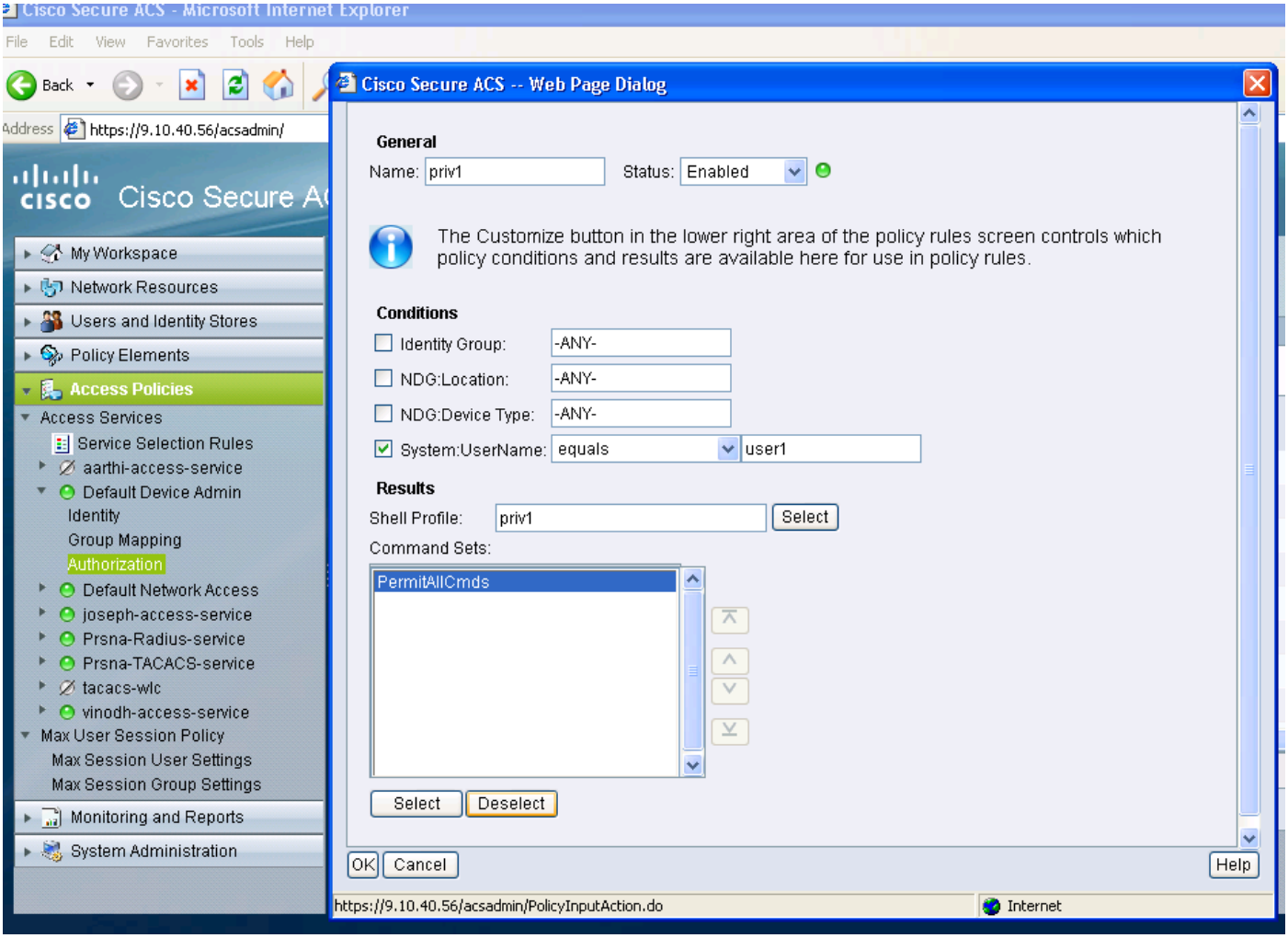
Cree la directiva de la autorización para el acceso completo de la administración.

La directiva predeterminada Admin del dispositivo usada con la selección de protocolo de los tacacs se selecciona como parte del proceso de la directiva de la evaluación. Al usar el protocolo de los tacacs para autenticar, la política de servicio seleccionada se llama directiva predeterminada Admin del dispositivo. Que la directiva en sí mismo comprende 2 secciones. Identiy significa quién es el usuario y qué grupo él pertenece (local o externo) y qué a le se permite hacer según el perfil de la autorización configurado. Asigne el comando set relacionado con el usuario que usted está configurando.



Cree la directiva de la autorización para el acceso de la administración del read only.

Lo mismo se hace para los usuarios solo lecturas. Este los ejemplos configuran el perfil del shell del nivel de privilegio 1 para el user1 y el privilegio 15 al usuario 2.



Configurar los 5760 para los tacacs

1. El radio/servidor TACACS necesita ser configurado.
tac_acct del servidor TACACS

direccionamiento ipv4 9.1.0.100

Cisco dominante

2. Configure al grupo de servidores
gtac del servidor tacacs+ del grupo aaa

Nombre del servidor tac_acct

No hay requisito previó hasta el paso antedicho.

3. listas de métodos de la autenticación y autorización de la configuración
<srv-grp> del grupo del <method-list> de la conexión con el sistema de autenticación aaa

srv-grp> del grupo del <method-list> del exec de autorización aaa

<srv-grp> del grupo predeterminado del exec de autorización aaa ----solución alternativa del à para conseguir los tacacs en el HTTP.

Los comandos 3 antedichos y el resto de los parámetros de la autenticación y autorización deben utilizar la misma base de datos, radio/los tacacs o local

Por ejemplo, si el comando authorization necesita habilitó, él también necesita señalar a la misma base de datos.

Para ex:

la autorización aaa ordena el <srv-grp> del grupo de 15 <method-list> — — > el grupo de servidores que señala a la base de datos (tacacs/radio o local) debe ser lo mismo.

4. HTTP de la configuración para utilizar las listas de métodos antedichas

ip http el <method-list> del login-auth aaa de la autenticación — — — > la lista de métodos necesita especificado explícitamente aquí, incluso si la lista de métodos es “predeterminada”

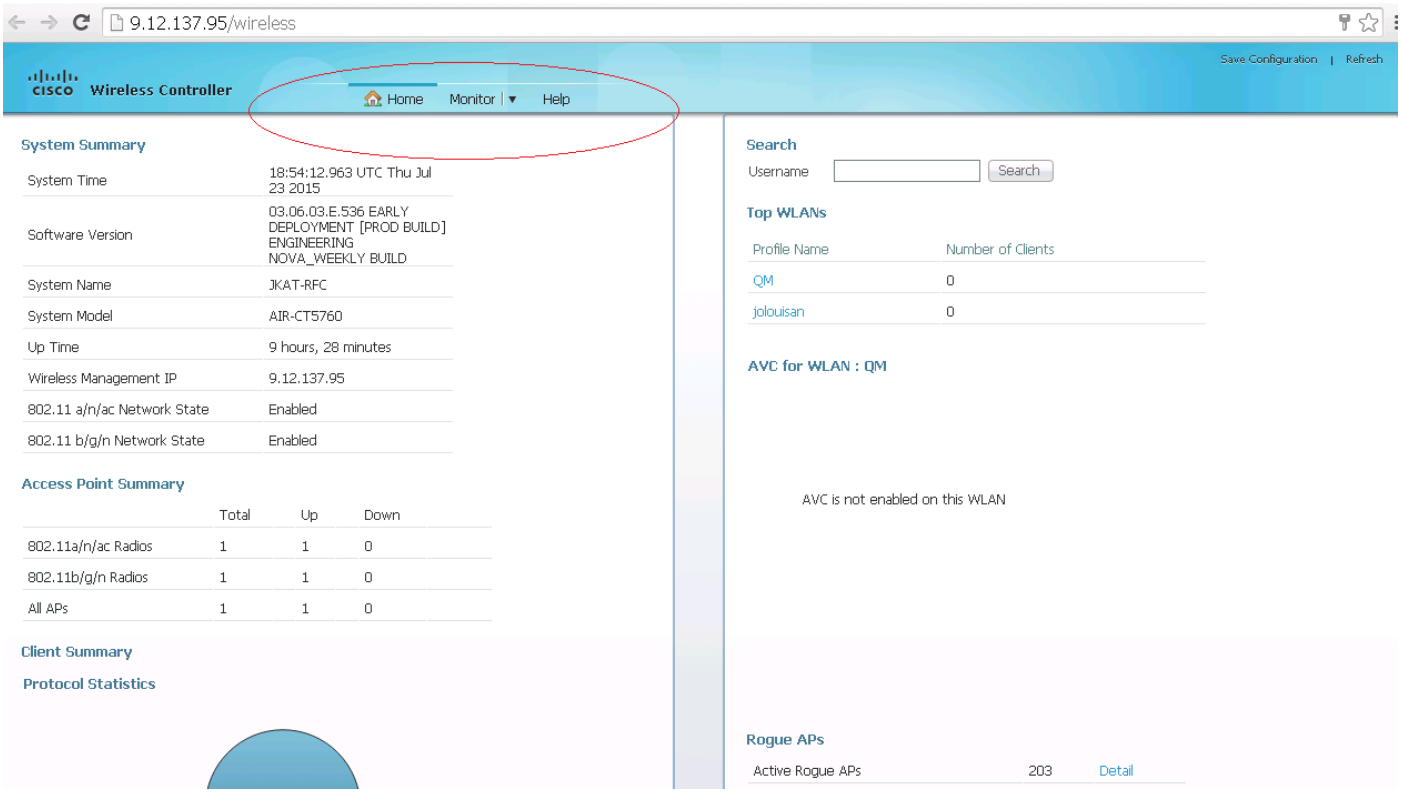
ip http <method-list> del EXEC-auth aaa de la autenticación

** Puntas a observar

- No configure ninguna listas de métodos en los Parámetros CONFIG de la “línea vty”. Si los pasos antedichos y la línea vty tienen diverso configs, después la línea configs del vty tomaría la precedencia.
- La base de datos debe ser lo mismo a través de todos los tipos de la configuración de la administración como el ssh/telnet y el webui.
- La autenticación HTTP debe tener la lista de métodos definida explícitamente.

Acceder los mismos 5760 con los 2 diversos perfiles

El abajo es un acceso de un usuario del nivel de privilegio 1 donde se da el acceso limitado



El abajo es un acceso de un usuario del nivel de privilegio 15 donde le dan el acceso total