Exemplo de configuração de controle de acesso baseado em privilégios de interface da Web 5760 com o Cisco Access Control Server (ACS)

Contents

Introduction

Este documento explicará como criar perfis de autenticação e autorização do Cisco ACS Tacs+ com diferentes níveis de privilégio e como integrá-lo ao 5760 para acesso à WebUI. Este recurso é suportado a partir de 3.6.3 (mas não em 3.7.x no momento da gravação).

Prerequisites

Requirements

Supõe-se que o leitor esteja familiarizado com o Cisco ACS e a configuração do controlador de acesso convergente. Este documento concentra-se apenas na interação entre esses 2 componentes no escopo da autorização TACACS+.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

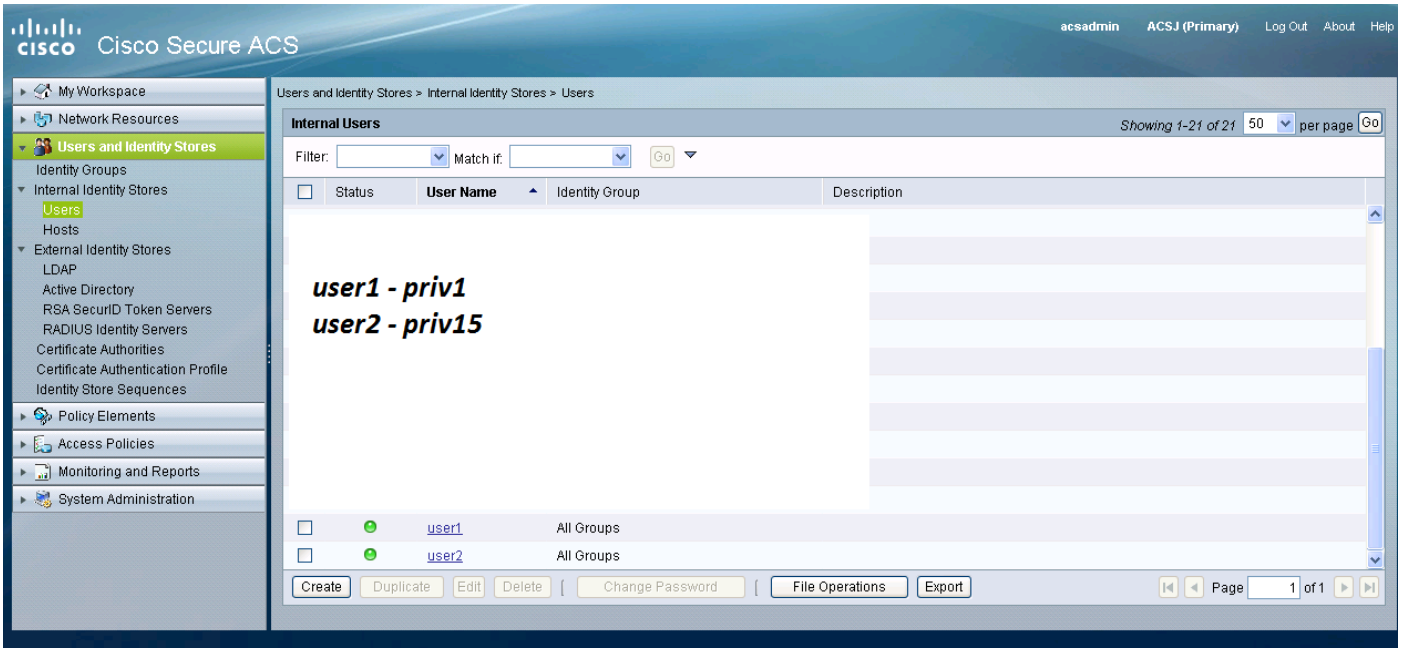
- Cisco Converged Access 5760, versão 3.6.3
- Cisco Access Control Server (ACS) 5.2

Configuração

Crie alguns usuários de teste no ACS

Clique em "Usuários e lojas de identidade" e selecione "Usuários".

Clique em "Criar" e configure alguns usuários de teste, como ilustrado abaixo.



Configurando elementos de política e perfis de shell

Você precisa criar 2 perfis para os 2 diferentes tipos de acesso .Privilege 15 no mundo dos cisco tacacs significa fornecer acesso total ao dispositivo sem nenhuma restrição. O privilégio 1, por outro lado, permitirá que você faça login e execute apenas uma quantidade limitada de comandos. Abaixo, há uma breve descrição dos níveis de acesso fornecidos pela cisco.

nível de privilégio 1 = não privilegiado (prompt é router>), o nível padrão para fazer logon

nível de privilégio 15 = privilegiado (o prompt é número de roteador), o nível depois que se entra no modo de ativação

nível de privilégio 0 = raramente usado, mas inclui 5 comandos: **desabilitar**, **habilitar**, **sair**, **ajudar** e **desconectar**

No 5760, os níveis 2-14 são considerados iguais ao nível 1. Eles recebem o mesmo privilégio que 1. **Não configure os níveis de privilégio de TACACS para determinados comandos no 5760**. O acesso à IU por guias não é suportado no 5760. Você pode ter acesso total (priv15) ou apenas acesso à guia Monitor (priv1). Além disso, os usuários com nível de privilégio 0 não têm permissão para fazer login.

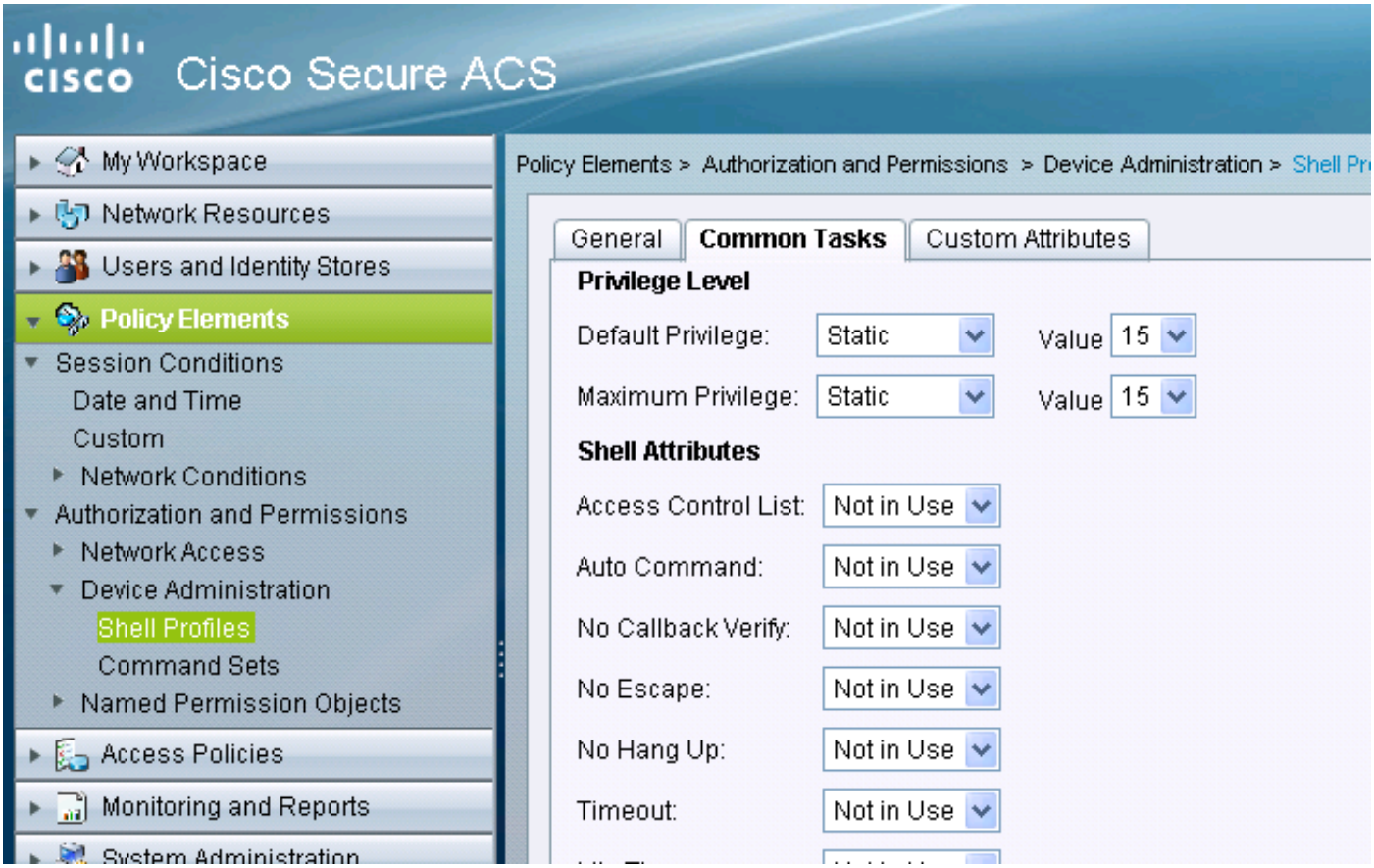
Criando um perfil de acesso de shell de 15 níveis de privilégio

Usando a tela de impressão abaixo, crie esse perfil:

Clique em "Elementos de política". Clique em "Shell Profiles" (Perfis da shell).

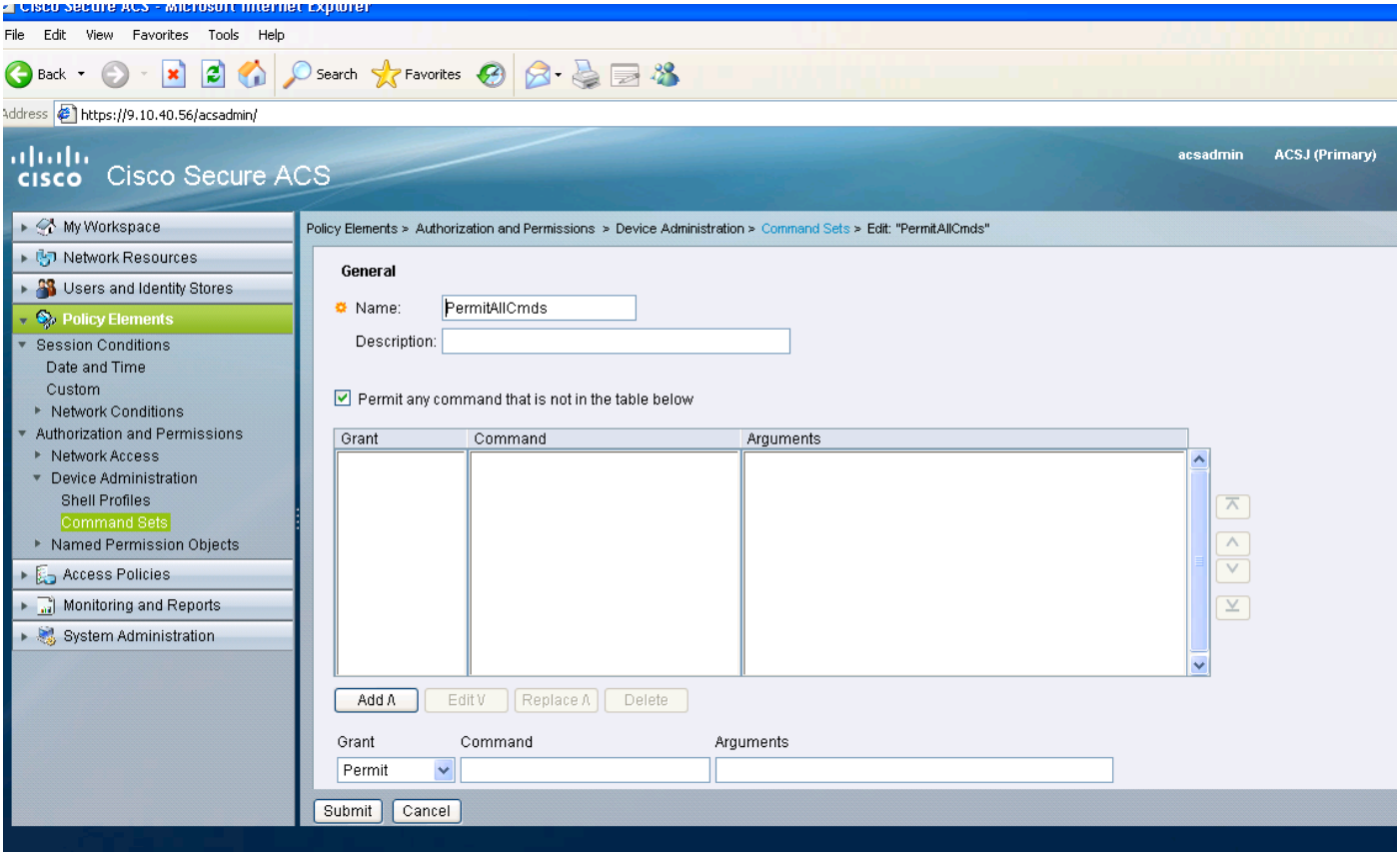
Crie um novo.

Acesse a guia "Tarefas comuns" e defina os níveis de privilégio padrão e máximo como 15.



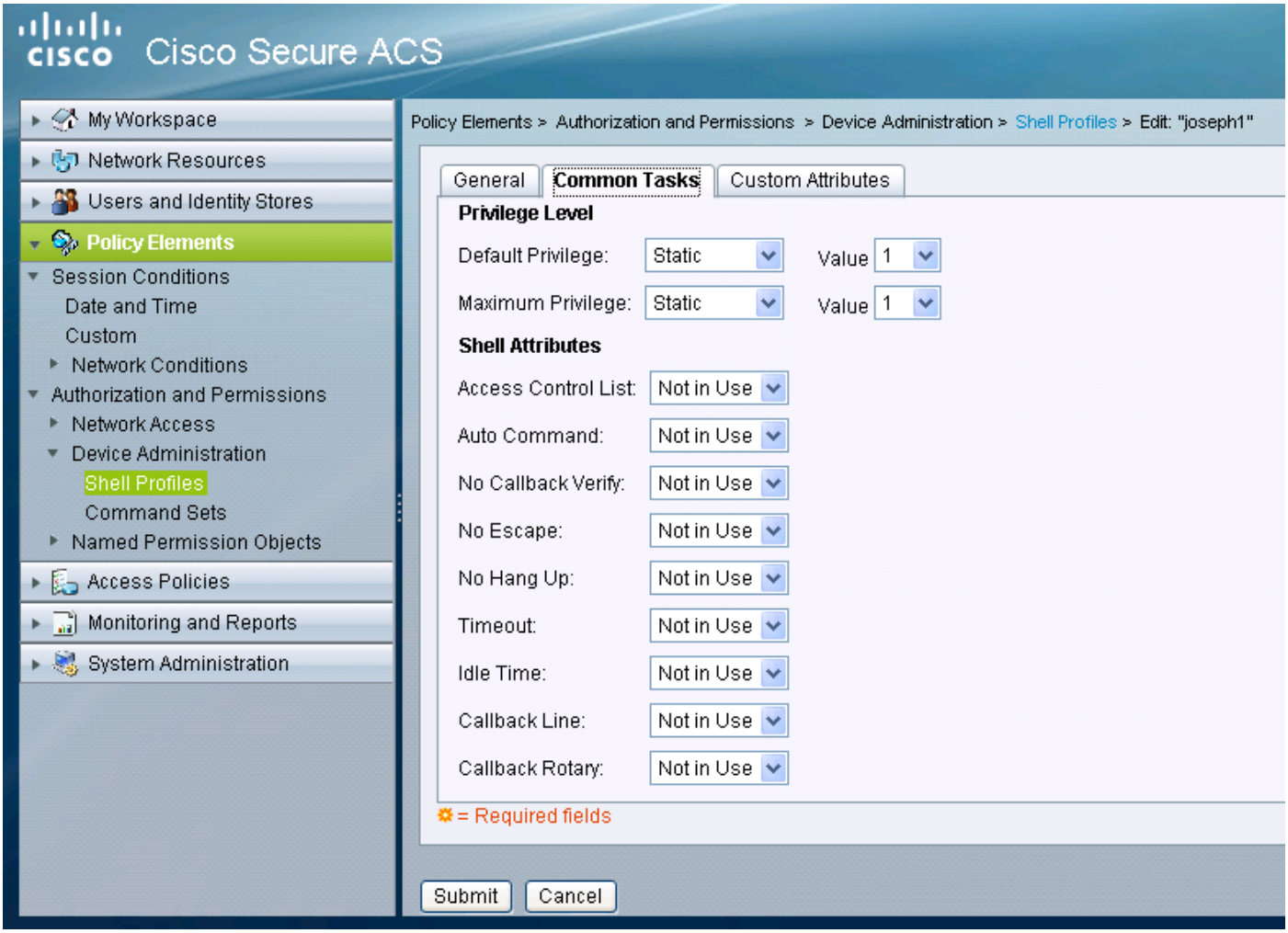
Criando conjuntos de comandos para o usuário administrador

Os conjuntos de comandos são conjuntos de comandos usados por todos os dispositivos tacacs.Eles podem ser usados para restringir os comandos que um usuário tem permissão para usar se for atribuído a esse perfil específico. Como no 5760, a restrição é feita no código Webui com base no nível de privilégio passado, os conjuntos de comandos para os níveis de privilégio 1 e 15 são os mesmos.



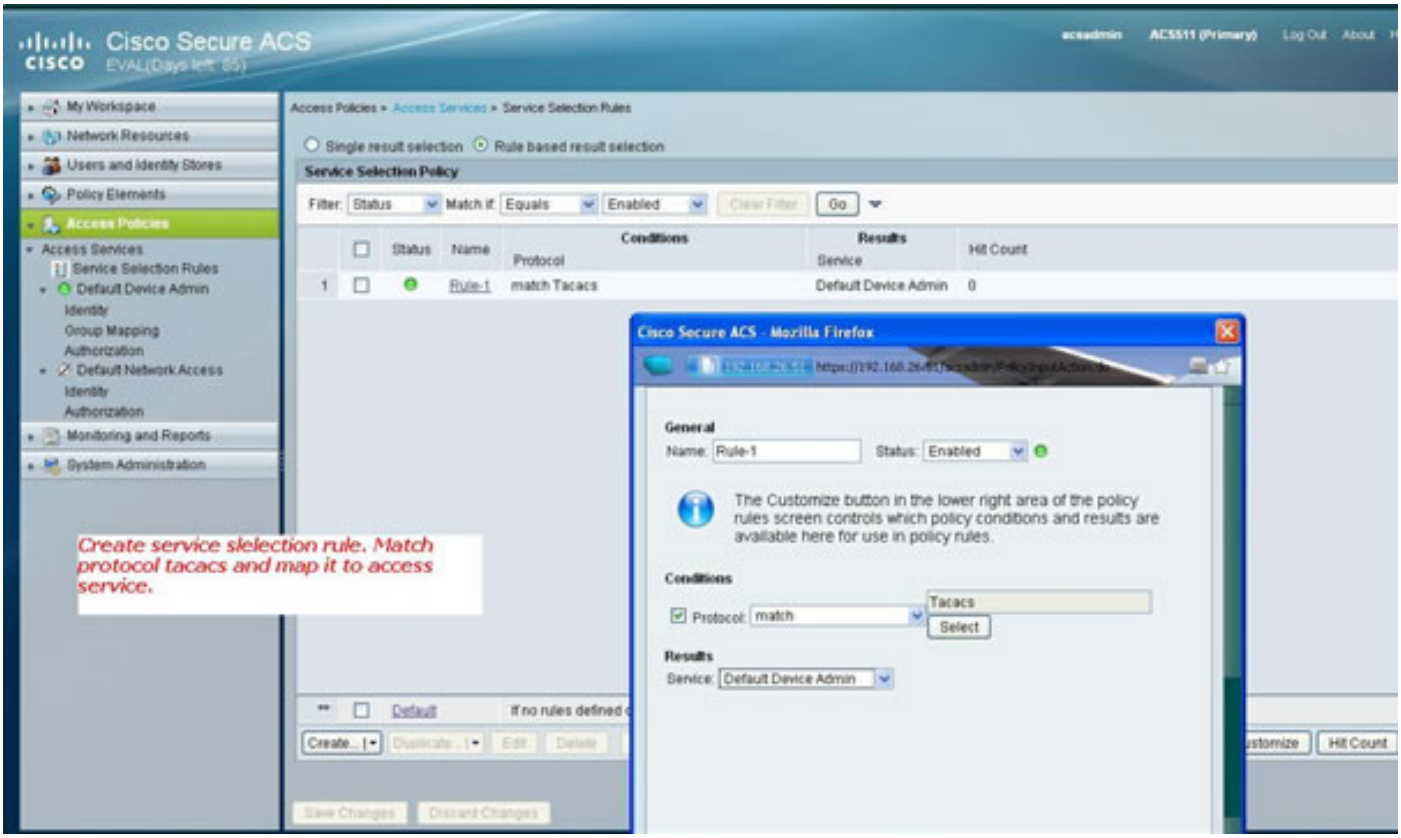
Criando perfil de shell para usuário somente leitura

Crie outro perfil de shell para usuários somente leitura. Esse perfil será diferente pelo fato de que os níveis de privilégio estão definidos como 1.



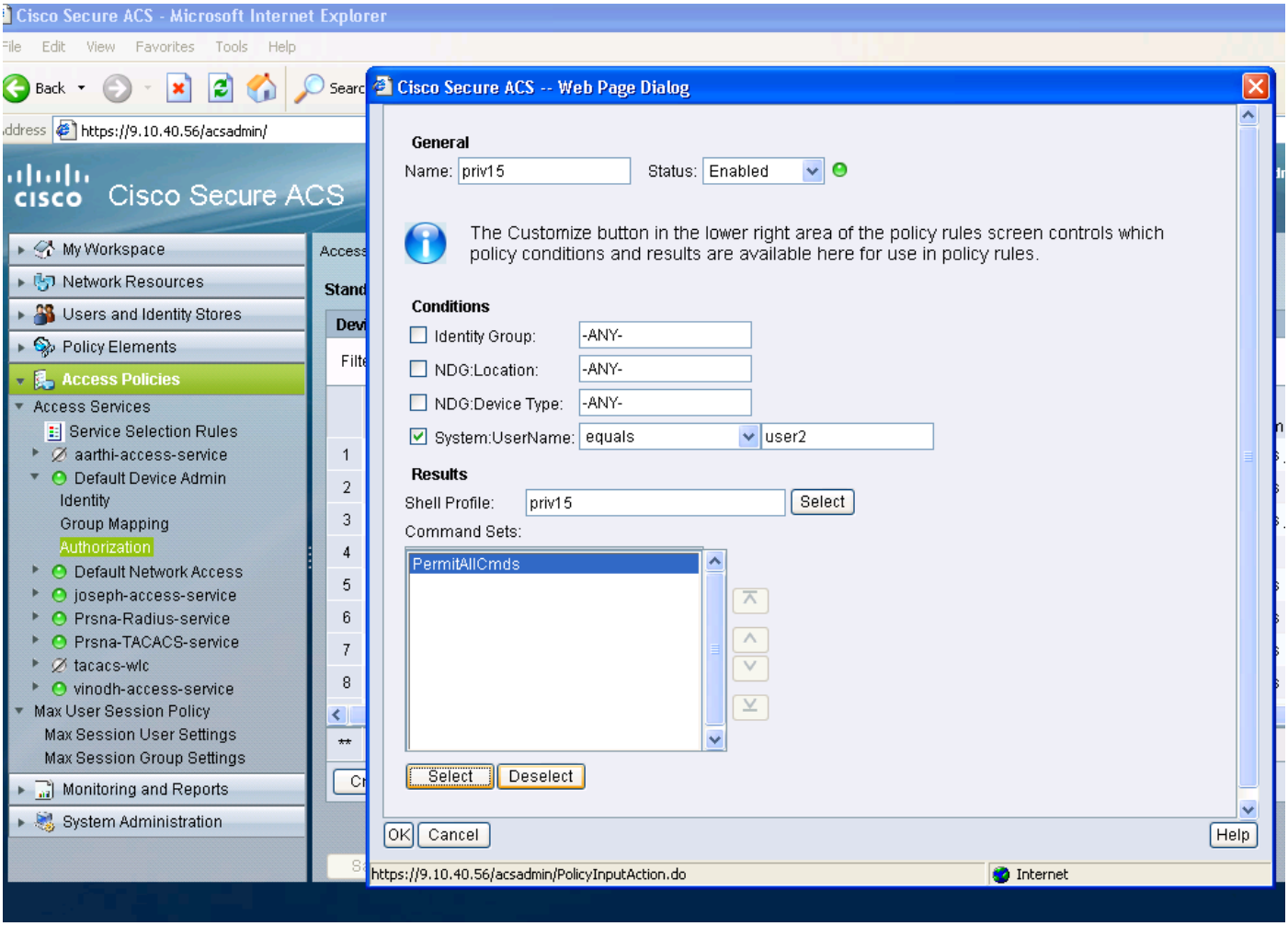
Criar uma regra de seleção de serviço para corresponder ao protocolo TACACS

Dependendo das suas políticas e configuração, certifique-se de que você tenha uma regra correspondente de tacacs vinda do 5760.



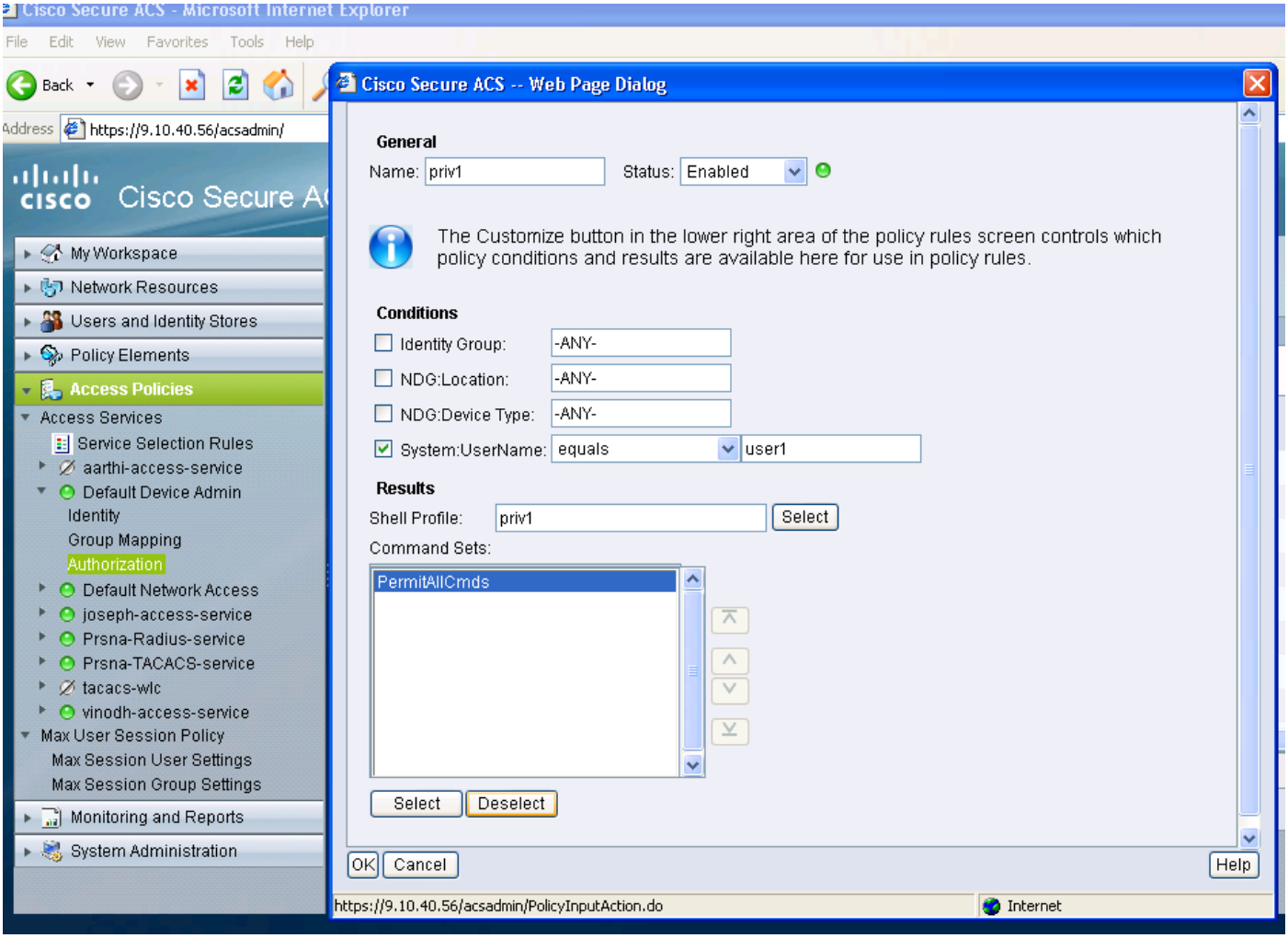
Crie uma política de autorização para acesso de administração completo.

A política Default Device Admin usada com a seleção do protocolo TACACS é selecionada como parte do processo de política de avaliação. Ao usar o protocolo TACACS para autenticar, a política de serviço selecionada é chamada de política de Administrador de dispositivo padrão. Essa política, em si mesma, compreende duas seções: Identificar significa quem é o usuário e a que grupo ele pertence (local ou externo) e o que ele pode fazer de acordo com o perfil de autorização configurado. Atribua o conjunto de comandos relacionado ao usuário que você está configurando.



Criar política de autorização para acesso de administração somente leitura.

O mesmo é feito para usuários somente leitura. Esses exemplos configuram o perfil de shell de nível de privilégio 1 para o usuário 1 e o privilégio 15 para o usuário 2.



Configurando o 5760 para TACACS

1. O servidor Radius/Tacacs precisa ser configurado.

tacacs server tac_acct

address ipv4 9.1.0.100

chave cisco

2. Configurar o grupo de servidores

aaa group server tacacs+ gtac

nome do servidor tac_acct

Não há pré-requisitos até a etapa acima.

3. configurar listas de métodos de autenticação e autorização

aaa authentication login <method-list> group <srv-grp>

aaa authorization exec <method-list> group srv-grp>

aaa authorization exec default group <srv-grp> — à workround para obter tacacs em http.

Os 3 comandos acima e todos os outros parâmetros de autenticação e autorização devem estar

usando o mesmo banco de dados, seja radius/tacacs ou local

Por exemplo, se a autorização de comando precisa ser habilitada, ela também precisa apontar para o mesmo banco de dados.

Por exemplo:

aaa authorization command 15 <method-list> group <srv-grp> —> o grupo de servidores que aponta para o banco de dados (tacacs/radius ou local) deve ser o mesmo.

4. configure http para usar as listas de métodos acima

ip http authentication aaa login-auth <method-list> —> a lista de métodos precisa ser especificada explicitamente aqui, mesmo que a lista de métodos seja "default"

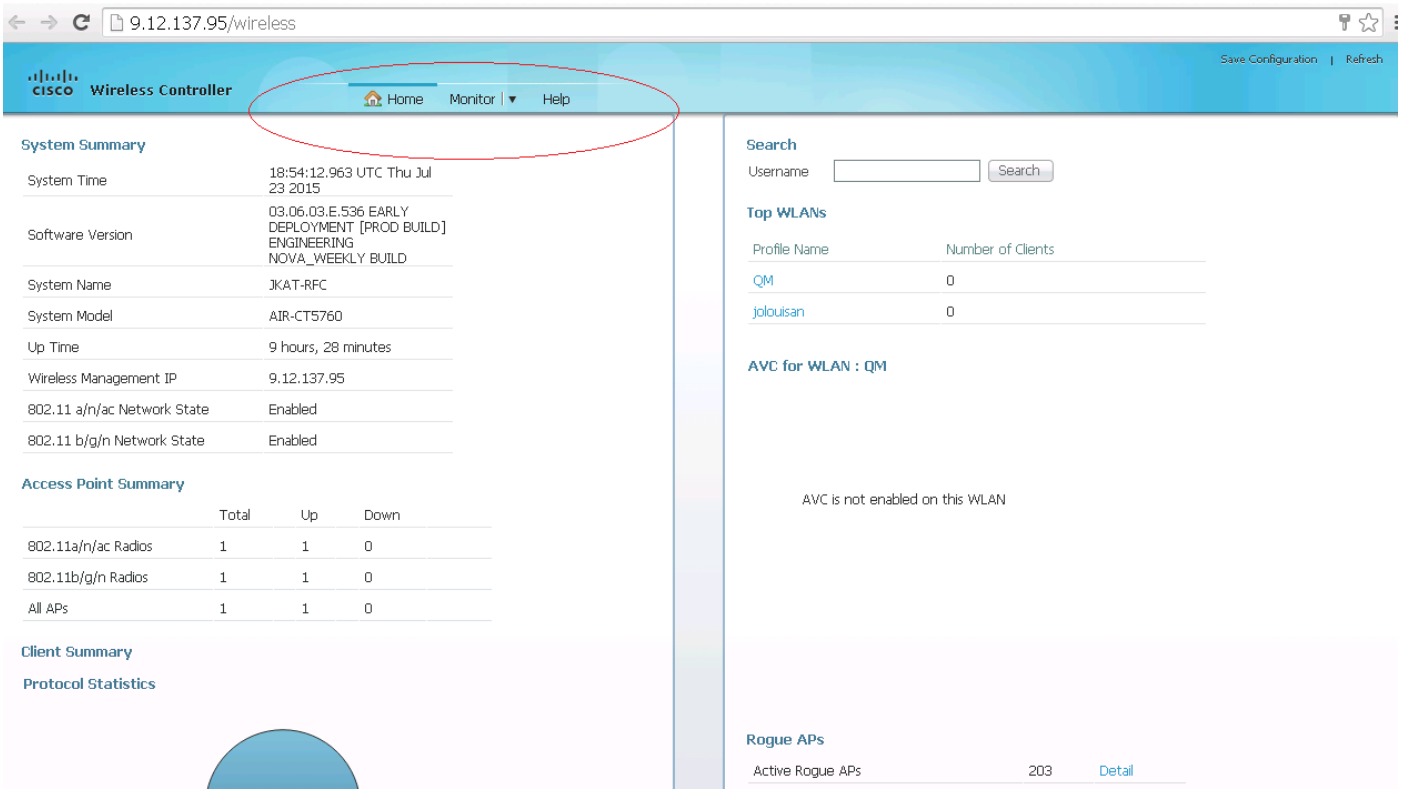
ip http authentication aaa exec-auth <method-list>

** Pontos a observar

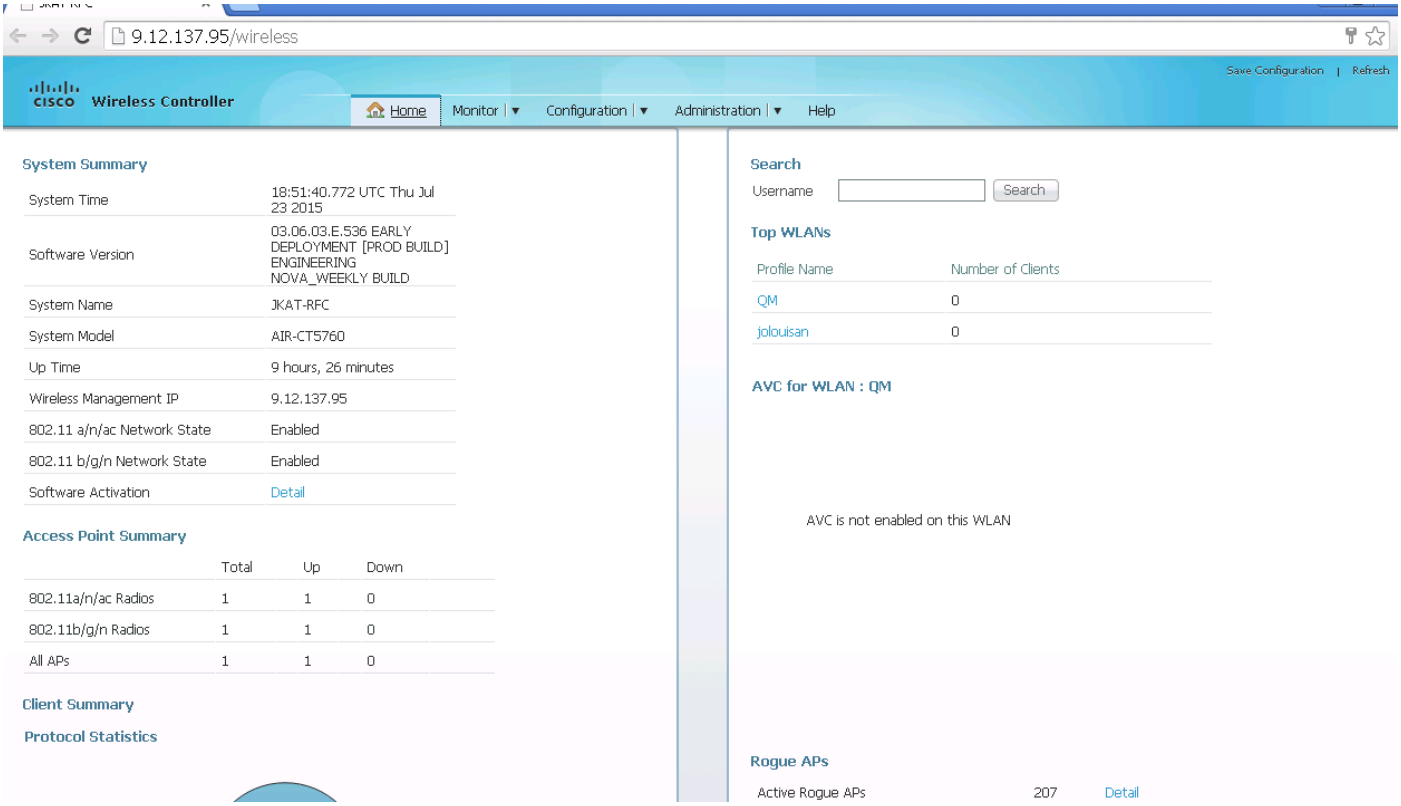
- Não configure nenhuma lista de métodos nos parâmetros de configuração "line vty". Se as etapas acima e a linha vty tiverem configurações diferentes, as configurações de linha vty terão precedência.
- O banco de dados deve ser o mesmo em todos os tipos de configuração de gerenciamento, como ssh/telnet e webui.
- A autenticação Http deve ter a lista de métodos definida explicitamente.

Acessando o mesmo 5760 com os dois perfis diferentes

A seguir está um acesso de um usuário de nível de privilégio 1 onde o acesso limitado é fornecido



A seguir está um acesso de um usuário de nível de privilégio 15 ao qual você tem acesso total


9.12.137.95/wireless
Wireless Controller
Save Configuration | Refresh
Home
Monitor
Configuration
Administration
Help
System Summary
System Time 18:51:40.772 UTC Thu Jul 23 2015
Software Version 03.06.03.E.536 EARLY DEPLOYMENT [PROD BUILD] ENGINEERING NOVA_WEEKLY BUILD
System Name JKAT-RFC
System Model AIR-CT5760
Up Time 9 hours, 26 minutes
Wireless Management IP 9.12.137.95
802.11 a/n/ac Network State Enabled
802.11 b/g/n Network State Enabled
Software Activation Detail
Access Point Summary
Total Up Down
802.11a/n/ac Radios 1 1 0
802.11b/g/n Radios 1 1 0
All APs 1 1 0
Client Summary
Protocol Statistics
Search
Username
Search
Top WLANs
Profile Name Number of Clients
QM 0
jolouisan 0
AVC for WLAN : QM
AVC is not enabled on this WLAN
Rogue APs
Active Rogue APs 207 Detail