exemple basé niveau du privilège de configuration de contrôle d'accès de 5760 interfaces web avec le serveur de contrôle d'accès de Cisco (ACS)

Contenu

Introduction

Ce document expliquera comment créer des profils d'authentification et d'autorisation de Cisco ACS Tacacs+ avec différents niveaux de privilège et les intégrer avec 5760 pour l'accès à WebUI. Cette caractéristique est prise en charge à compter de 3.6.3 (mais pas sur 3.7.x à la période de cette écriture).

Conditions préalables

Conditions requises

On le suppose que le lecteur est familiarisé avec Cisco ACS et configuration convergée de contrôleur d'Access. Ce document se concentre seulement sur l'interaction entre ces 2 composants à portée de l'autorisation tacacs+.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

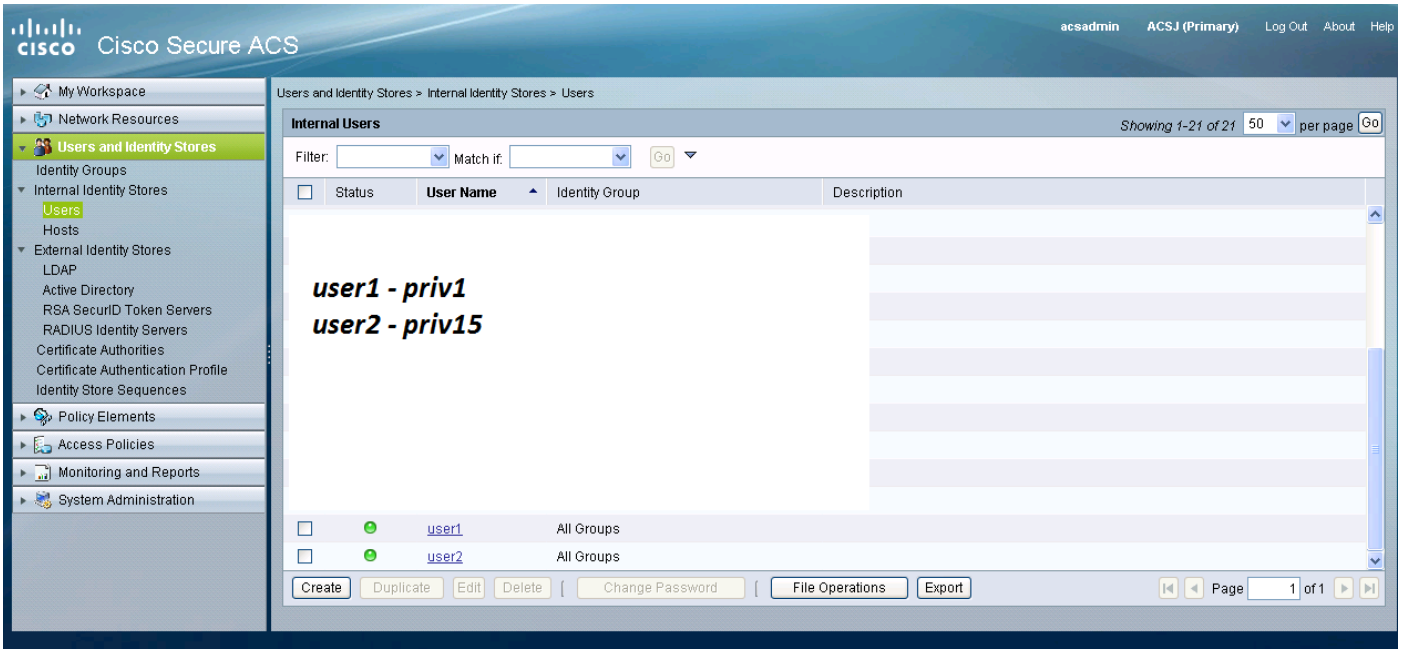
- Cisco a convergé Access 5760, la version 3.6.3
- Serveur de contrôle de Cisco Acess (ACS) 5.2

Configuration

Créez quelques utilisateurs de test dans ACS

Cliquez sur en fonction les « utilisateurs et l'identité enregistre », puis sélectionne des « utilisateurs ».

Cliquez sur « créent » et configurent quelques utilisateurs de test tels qu'illustré ci-dessous.



Installation des éléments de stratégie et des profils de shell

Vous devez créer 2 profils pour les 2 types différents d'accès. Le privilège 15 dans le monde de tacacs de Cisco signifie fournir l'accès complet au périphérique sans n'importe quelle restriction. Favorisez 1 d'autre part te permettra pour ouvrir une session et exécuter seulement une quantité limitée de commandes. Est ci-dessous une description courte des niveaux d'accès fournis par Cisco.

niveau de privilège 1 = non-privilégié (l'invite indique router>), niveau par défaut pour se connecter

le niveau de privilège 15 = a favorisé (l'invite indique router#), niveau après être entré en mode activer

le niveau de privilège 0 = rarement utilisé, mais inclut 5 commandes : **désactiver**, **activer**, **quitter**, **aide** et **déconnexion**

Sur 5760, des niveaux 2-14 sont considérés les mêmes que le niveau 1. Ils sont donnés le même privilège que 1. **Ne configurez pas les niveaux de privilège de tacacs pour certaines commandes sur les 5760**. L'accès UI par onglets n'est pas pris en charge en 5760. Vous pouvez avoir l'accès complet (priv15) ou seulement l'accès à l'onglet de moniteur (priv1). En outre, des utilisateurs avec le niveau de privilège 0 pas alowed pour ouvrir une session.

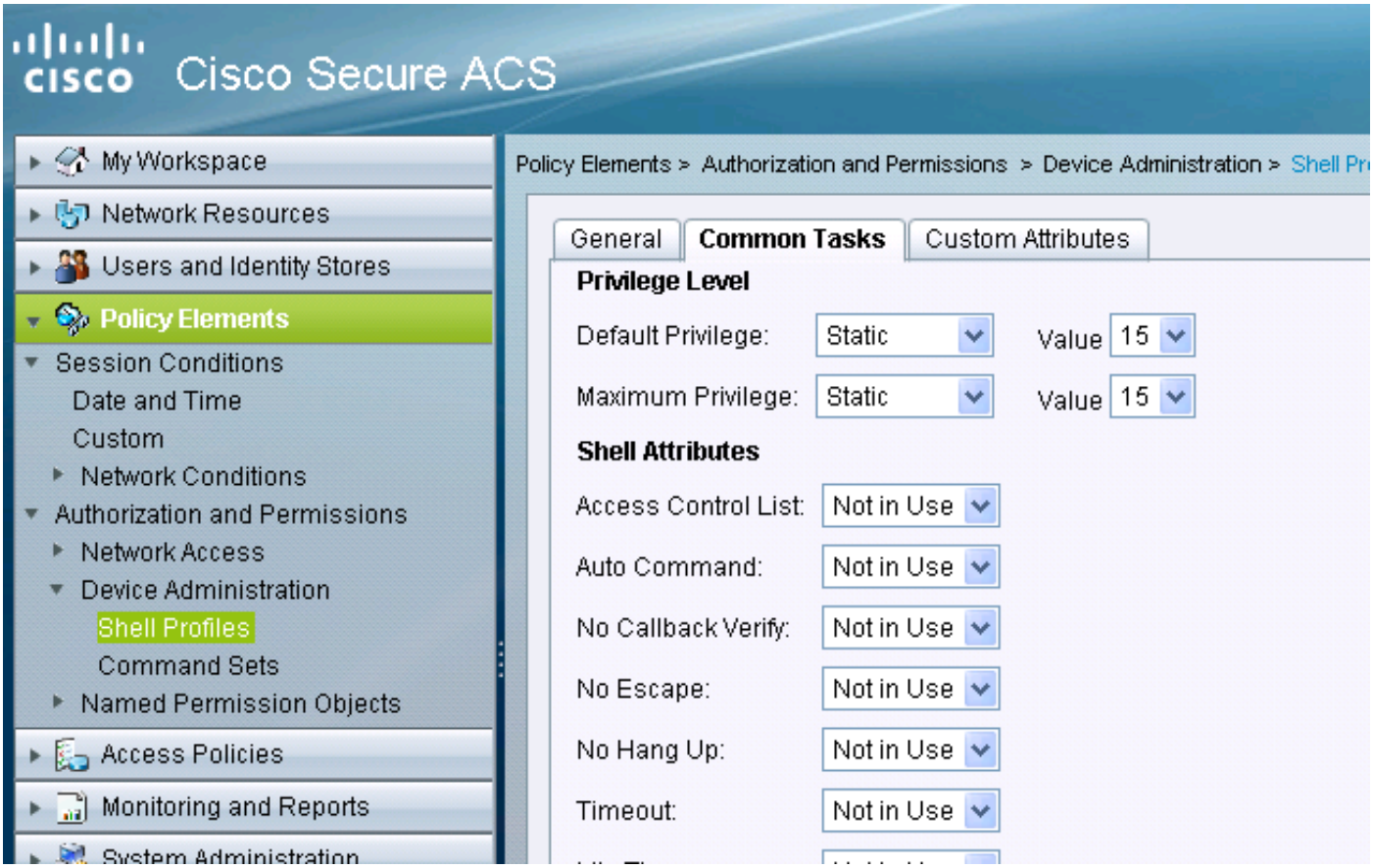
Création du profil de niveau d'accès de shell du privilège 15

Utilisant l'impression écran ci-dessous créez ce profil :

Cliquez sur en fonction les « éléments de stratégie ». Cliquez sur en fonction le « shell profile ».

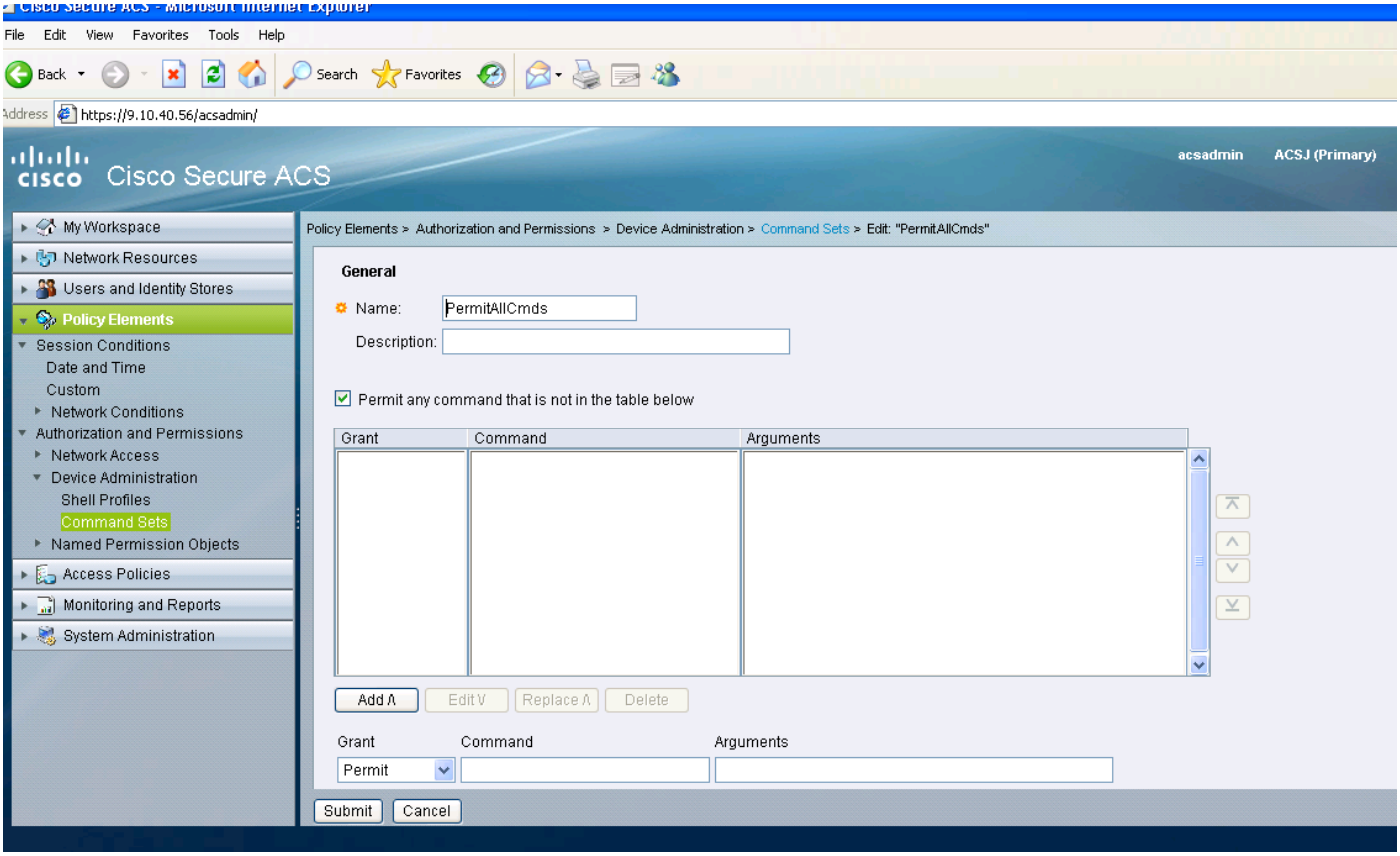
Créez un neuf.

Entrez dans les « fonctionnalités usuelles » onglet et placez les niveaux de privilège par défaut et maximum à 15.



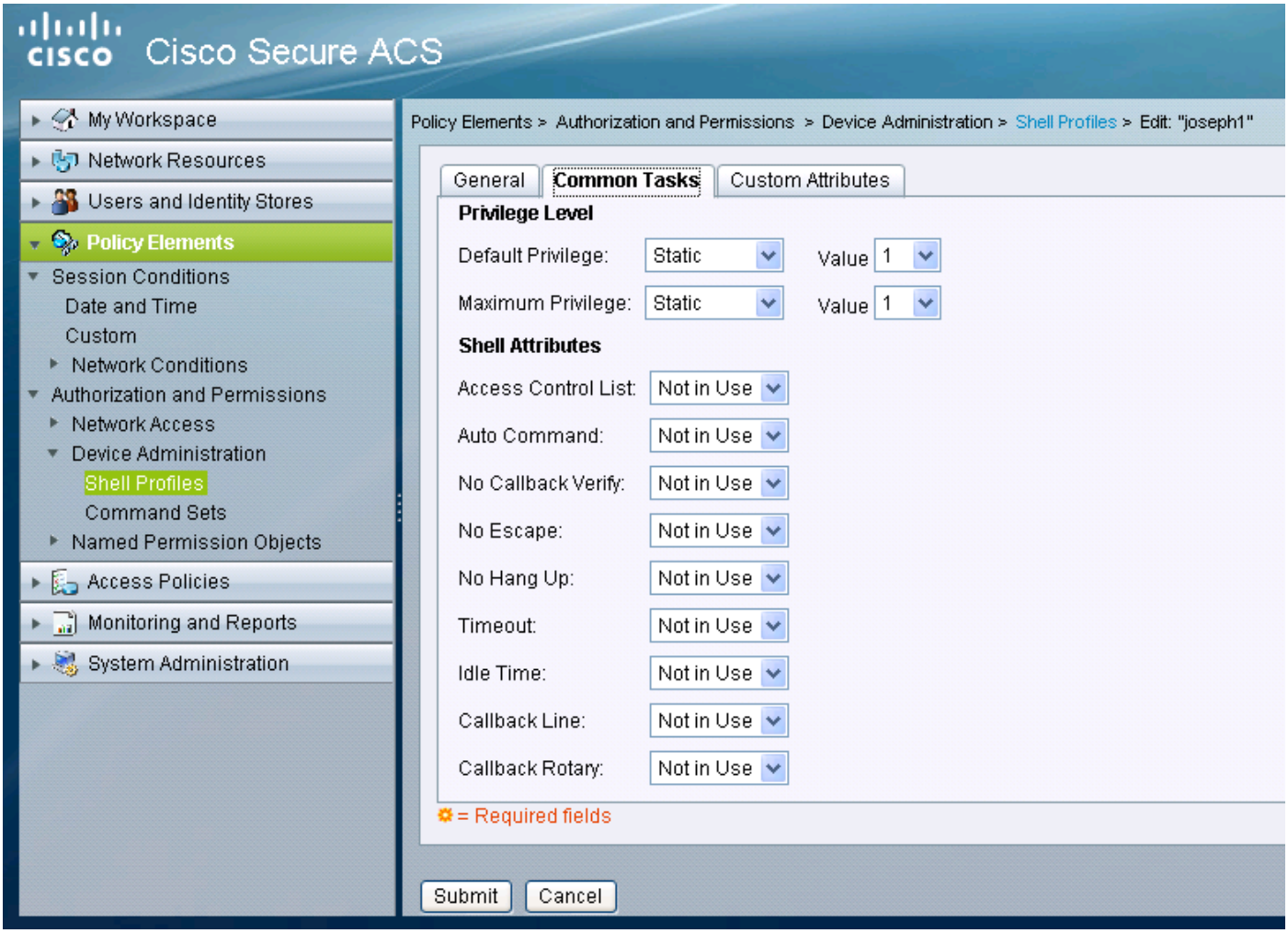
Création des positionnements de commande pour l'utilisateur d'admin

Les positionnements de commande sont des ensembles de commandes utilisées par tous les périphériques de tacacs. Ils peuvent être utilisés pour limiter les commandes qu'on permet à un un utilisateur pour utiliser si assigné ce profil spécifique. Puisque sur les 5760, la restriction est faite sur le code de Webui basé sur le niveau de privilège passé, la commande place pour le privilège level1 et 15 sont identiques.



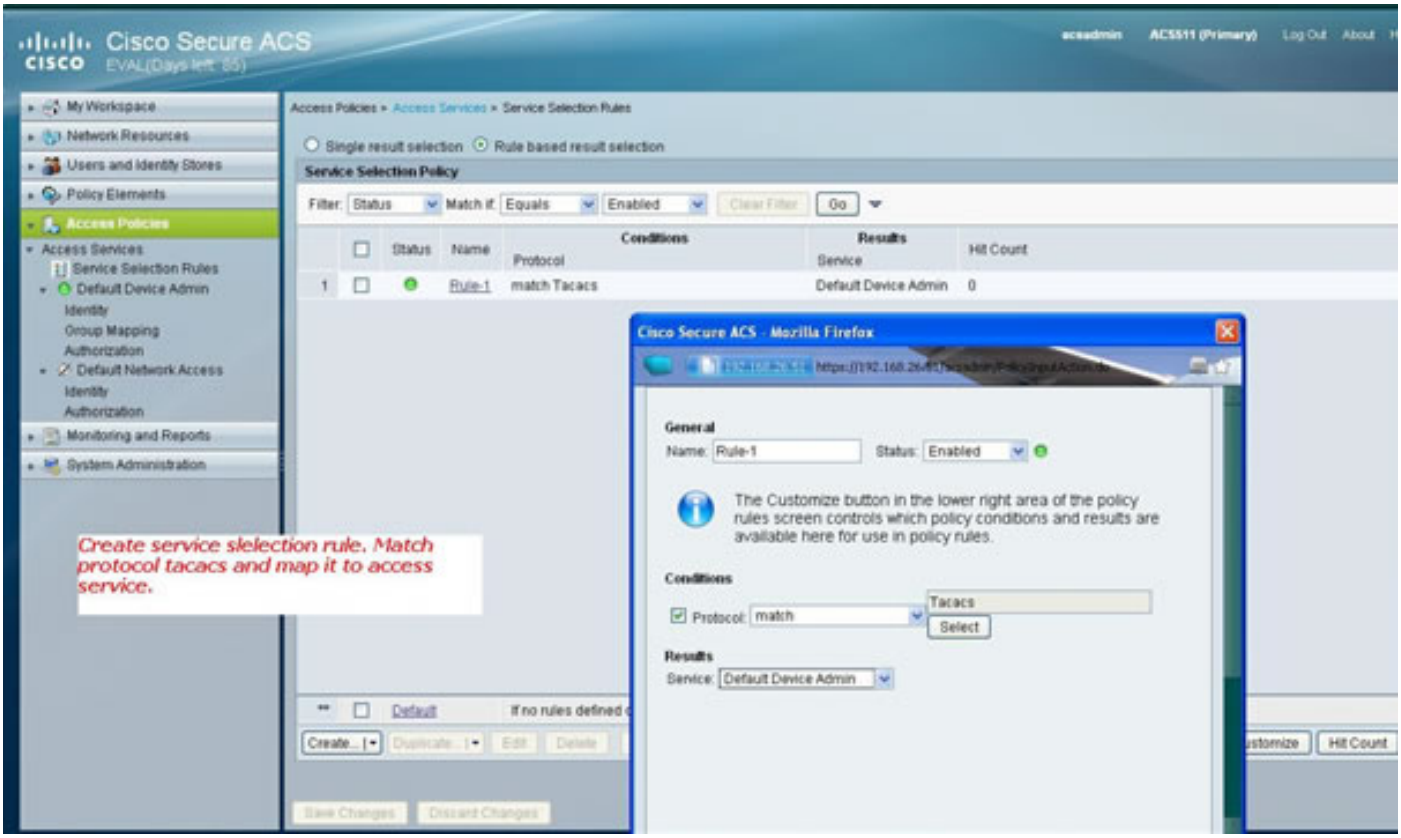
Création du profil de shell pour seulement l'utilisateur lu

Créez un autre profil de shell pour les utilisateurs en lecture seule. Ce profil différera par le fait que les niveaux de privilège sont placés à 1.



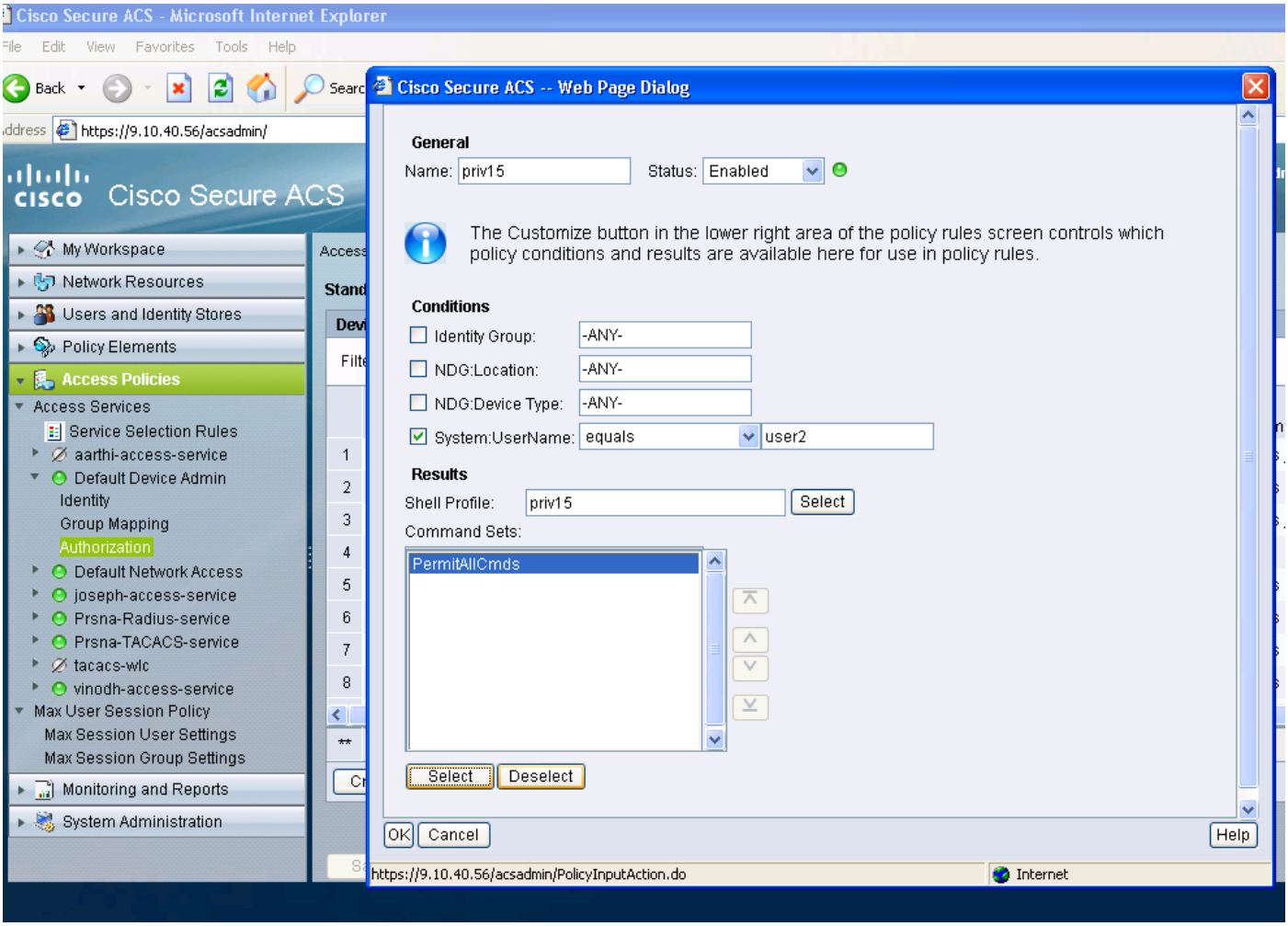
Créez une règle de sélection de service d'apparier le protocole de tacacs

Selon vos stratégies et configuration, assurez-vous que vous avez les tacacs assortis d'une règle provenant les 5760.



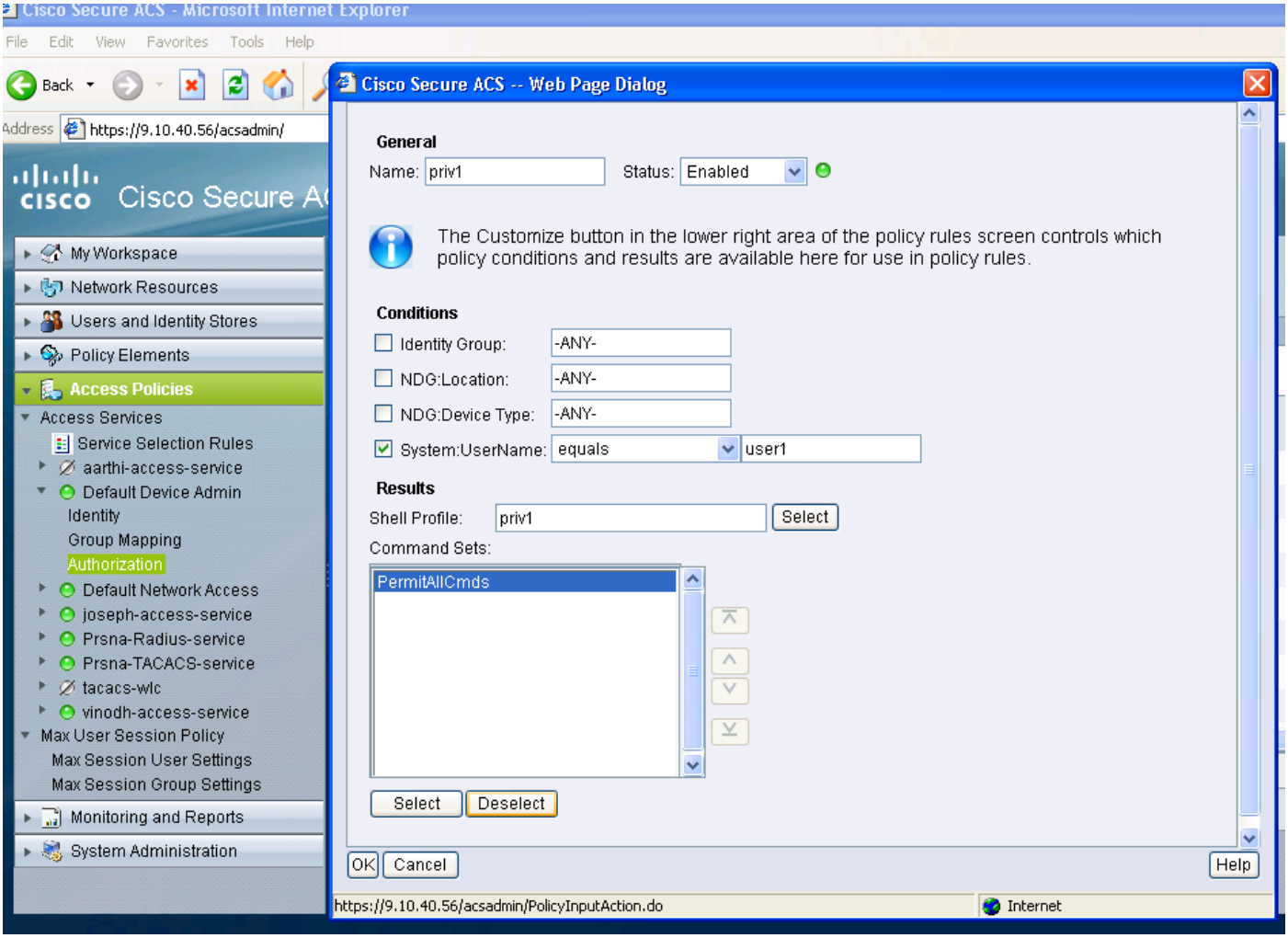
Créez la stratégie d'autorisation pour le plein accès de gestion.

La stratégie par défaut d'admin de périphérique utilisée avec la sélection de protocole de tacacs est sélectionnée en tant qu'élément du processus de stratégie d'évaluation. En employant le protocole de tacacs pour authentifier, la stratégie de service sélectionnée s'appelle la stratégie par défaut d'admin de périphérique. Que la stratégie comporte en soi 2 sections. Identiy veut dire qui l'utilisateur est et à quel groupe il appartient (local ou externe) et ce qu'il est permis pour faire selon le profil d'autorisation configuré. Assignez à la commande connexe réglé à l'utilisateur que vous configurez.



Créez la stratégie d'autorisation pour seulement l'accès lu de gestion.

Le même est fait pour les utilisateurs en lecture seule. Ce les exemples configurent le profil de shell du niveau de privilège 1 pour l'utilisateur 1 et le privilège 15 à l'utilisateur 2.



Configurer les 5760 pour des tacacs

1. Le rayon/serveur TACACS doit être configuré.
tac_acct de serveur TACACS

address ipv4 9.1.0.100

Cisco principal

2. Configurez le groupe de serveurs
gtac d'aaa group server tacacs+

tac_acct de nom du serveur

Il n'y a aucune condition préalable jusqu'à l'étape ci-dessus.

3. configurez les listes d'authentification et d'authorization method
<srv-grp> de groupe de <method-list> d'authentication login d'AAA

srv-grp> de groupe de <method-list> d'exécutif d'autorisation d'AAA

<srv-grp> de groupe d'exec default d'autorisation d'AAA ----contournement d'à pour obtenir des tacacs sur le HTTP.

Les 3 commandes ci-dessus et tous autres paramètres d'authentification et d'autorisation devraient utiliser la même base de données, rayon/tacacs ou gens du pays

Par exemple, si l'autorisation de commande a besoin activé, il doit également indiquer la même base de données.

Pour ex :

l'autorisation d'AAA commande le <srv-grp> de groupe de 15 <method-list> — — > le groupe de serveurs indiquant la base de données (tacacs/rayon ou gens du pays) devrait être identique.

4. configurez le HTTP pour utiliser les listes ci-dessus de méthode

le <method-list> de procédure de connexion-auth d'AAA d'ip http authentication — — — > la liste de méthode a besoin spécifié explicitement ici, même si la liste de méthode est « par défaut »

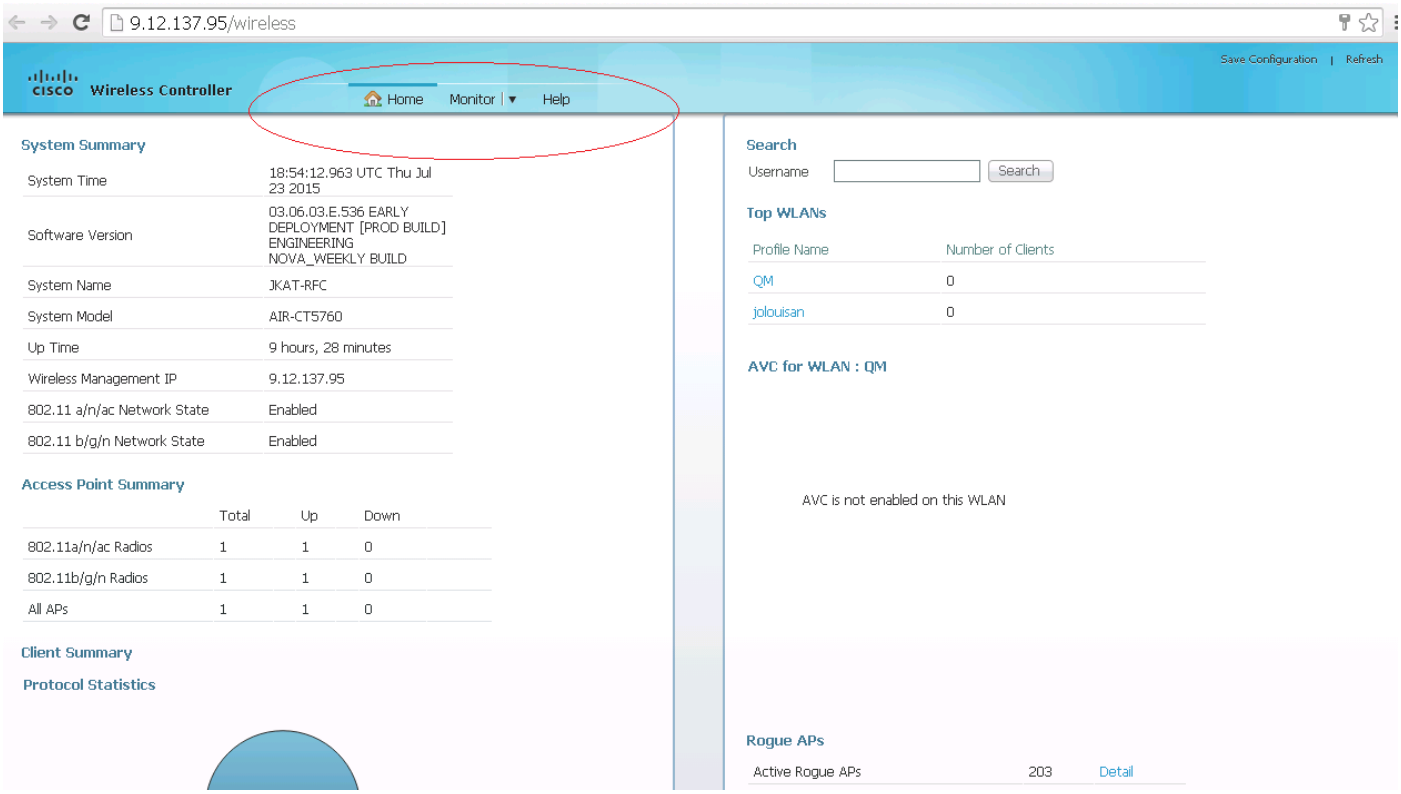
<method-list> d'exécutif-auth d'AAA d'ip http authentication

** Points à noter

- Ne configurez aucun method-list sur les paramètres de config de « line vty ». Si les étapes ci-dessus et le line vty ont différents configs, alors les configs de line vty auraient la priorité.
- La base de données devrait être identique à travers tous les types de configuration de gestion comme le ssh/telnet et le webui.
- L'authentification de HTTP devrait avoir la liste de méthode définie explicitement.

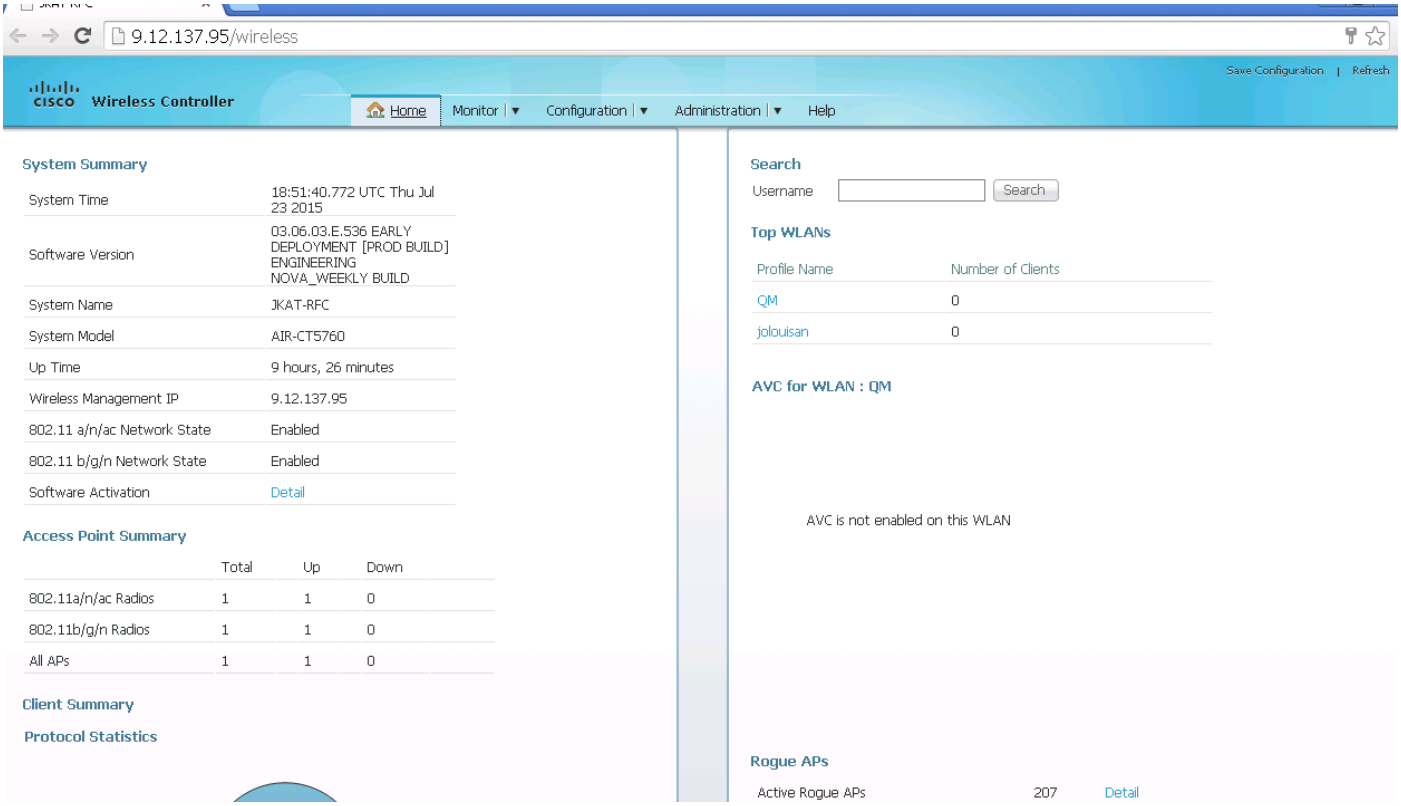
Accéder aux mêmes 5760 avec les 2 profils différents

Le ci-dessous est un accès d'un utilisateur du niveau de privilège 1 où l'accès limité est donné



Le ci-dessous est un accès d'un utilisateur du niveau de privilège 15 où vous êtes donné l'accès

complet


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