Exemple de configuration de contrôle d'accès basé sur les privilèges de l'interface Web du 5760 avec Cisco Access Control Server (ACS)

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Configuration](#)
[Créer quelques utilisateurs de test dans ACS](#)
[Configuration des éléments de stratégie et des profils de shell](#)
[Création d'un profil d'accès de shell de privilège de 15 niveaux](#)
[Création de jeux de commandes pour l'utilisateur admin](#)
[Création d'un profil shell pour l'utilisateur en lecture seule](#)
[Créer une règle de sélection de service correspondant au protocole tacacs](#)
[Créer une stratégie d'autorisation pour l'accès à l'administration complète.](#)
[Créer une stratégie d'autorisation pour l'accès en lecture seule à l'administration.](#)
[Configuration du 5760 pour tacacs](#)
[Accès au même 5760 avec les 2 profils différents](#)
[Discussions connexes de la communauté d'assistance Cisco](#)

Introduction

Ce document explique comment créer des profils d'authentification et d'autorisation Cisco ACS Tacacs+ avec différents niveaux de privilège et l'intégrer au 5760 pour l'accès à WebUI. Cette fonctionnalité est prise en charge à partir de la version 3.6.3 (mais pas à partir de la version 3.7.x au moment de l'écriture).

Conditions préalables

Conditions requises

Il est supposé que le lecteur connaît bien la configuration des contrôleurs Cisco ACS et d'accès convergé. Ce document se concentre uniquement sur l'interaction entre ces deux composants dans le champ d'application de l'autorisation tacacs+.

Components Used

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

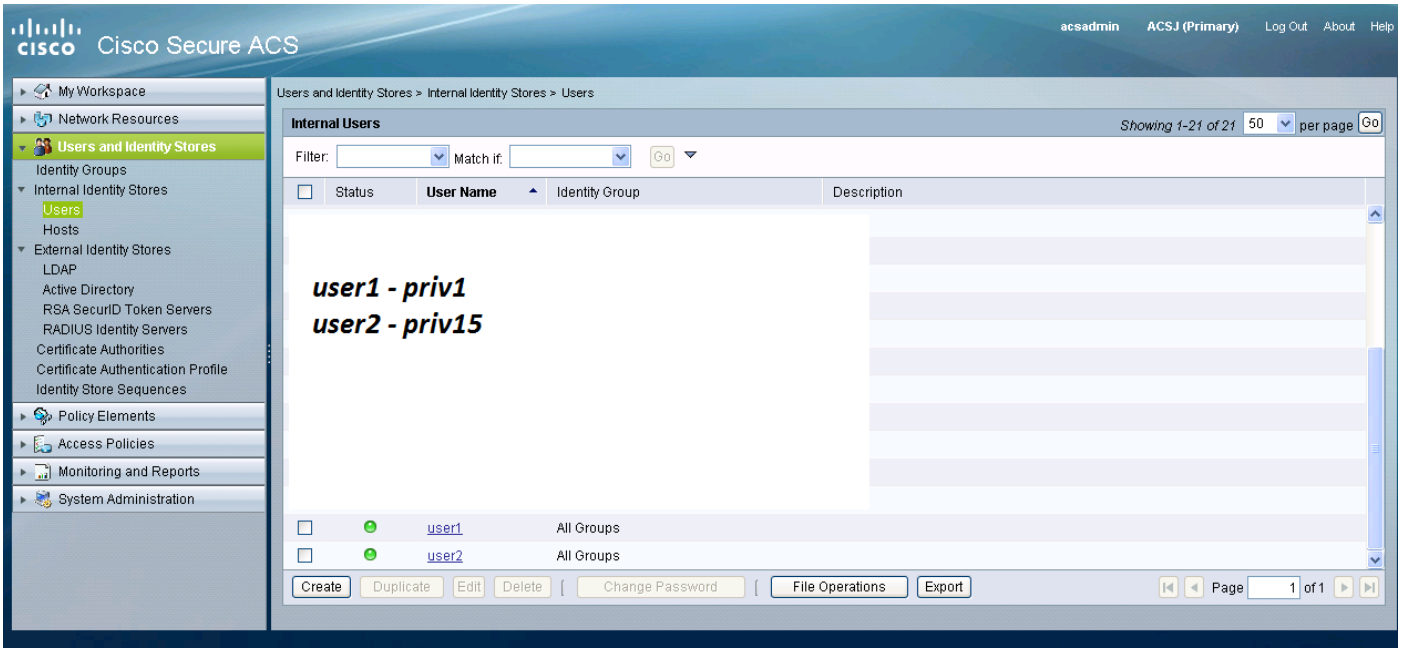
- Cisco Converged Access 5760, version 3.6.3
- Cisco Access Control Server (ACS) 5.2

Configuration

Créer quelques utilisateurs de test dans ACS

Cliquez sur « Utilisateurs et magasins d'identité », puis sélectionnez « Utilisateurs ».

Cliquez sur « Créer » et configurez quelques utilisateurs de test comme illustré ci-dessous.



Configuration des éléments de stratégie et des profils de shell

Vous devez créer 2 profils pour les 2 différents types d'accès .Privilège 15 dans le monde de cisco tacacs signifie fournir un accès complet au périphérique sans aucune restriction. Par contre, le privilège 1 vous permet de vous connecter et d'exécuter uniquement un nombre limité de commandes. Vous trouverez ci-dessous une brève description 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 le modèle 5760, les niveaux 2 à 14 sont considérés comme identiques aux niveaux 1. Ils ont le même privilège que 1. **Ne configurez pas les niveaux de privilège tacacs pour certaines commandes sur le 5760**. L'accès à l'interface utilisateur par onglet n'est pas pris en charge dans 5760. Vous pouvez disposer d'un accès complet (priv15) ou uniquement d'un accès à l'onglet Moniteur (priv1). En outre, les utilisateurs disposant du niveau de privilège 0 ne sont pas autorisés à se connecter.

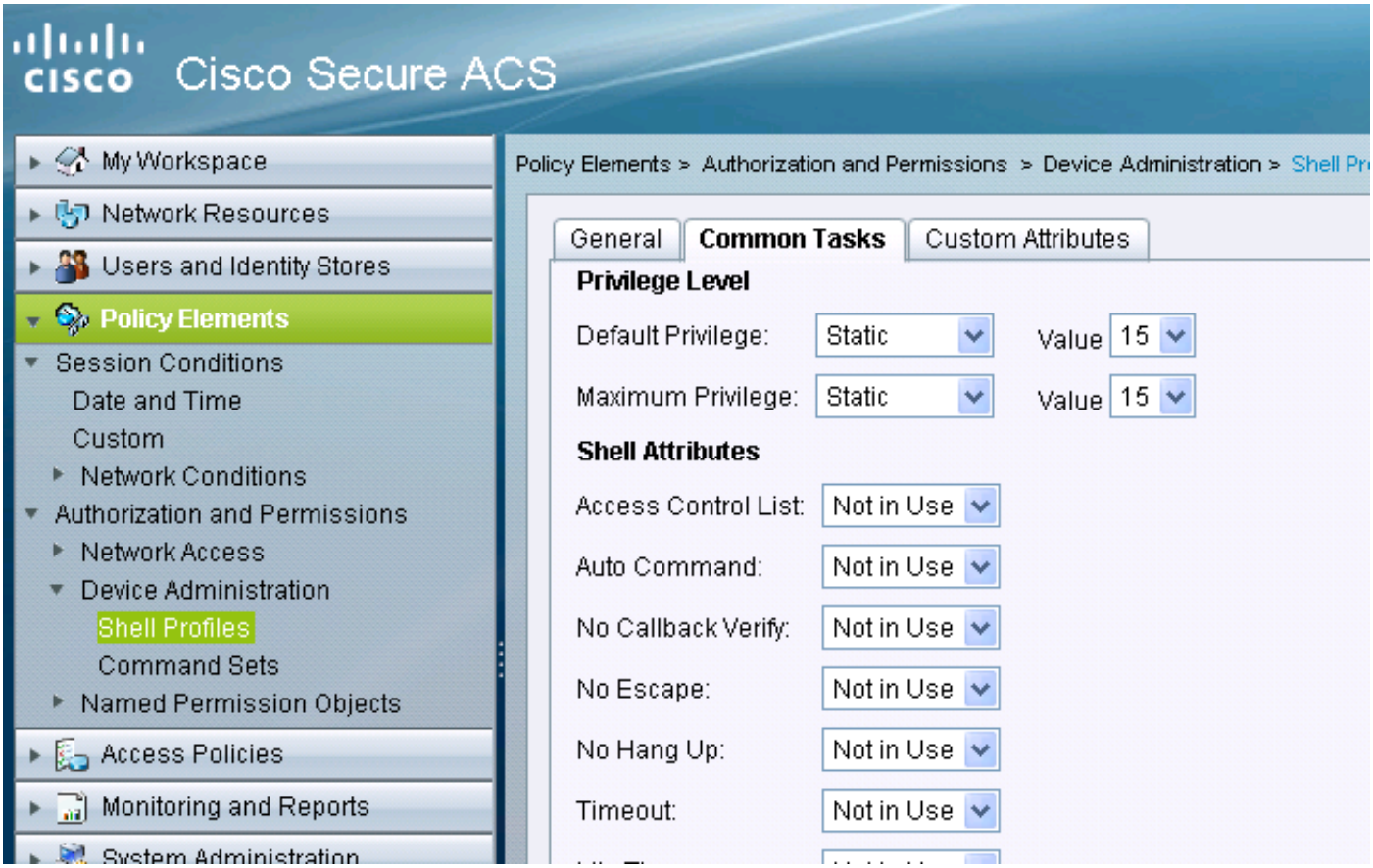
Création d'un profil d'accès de shell de privilège de 15 niveaux

À l'aide de l'écran d'impression ci-dessous, créez ce profil :

Cliquez sur « Eléments de politique ». Cliquez sur « Profiles Shell ».

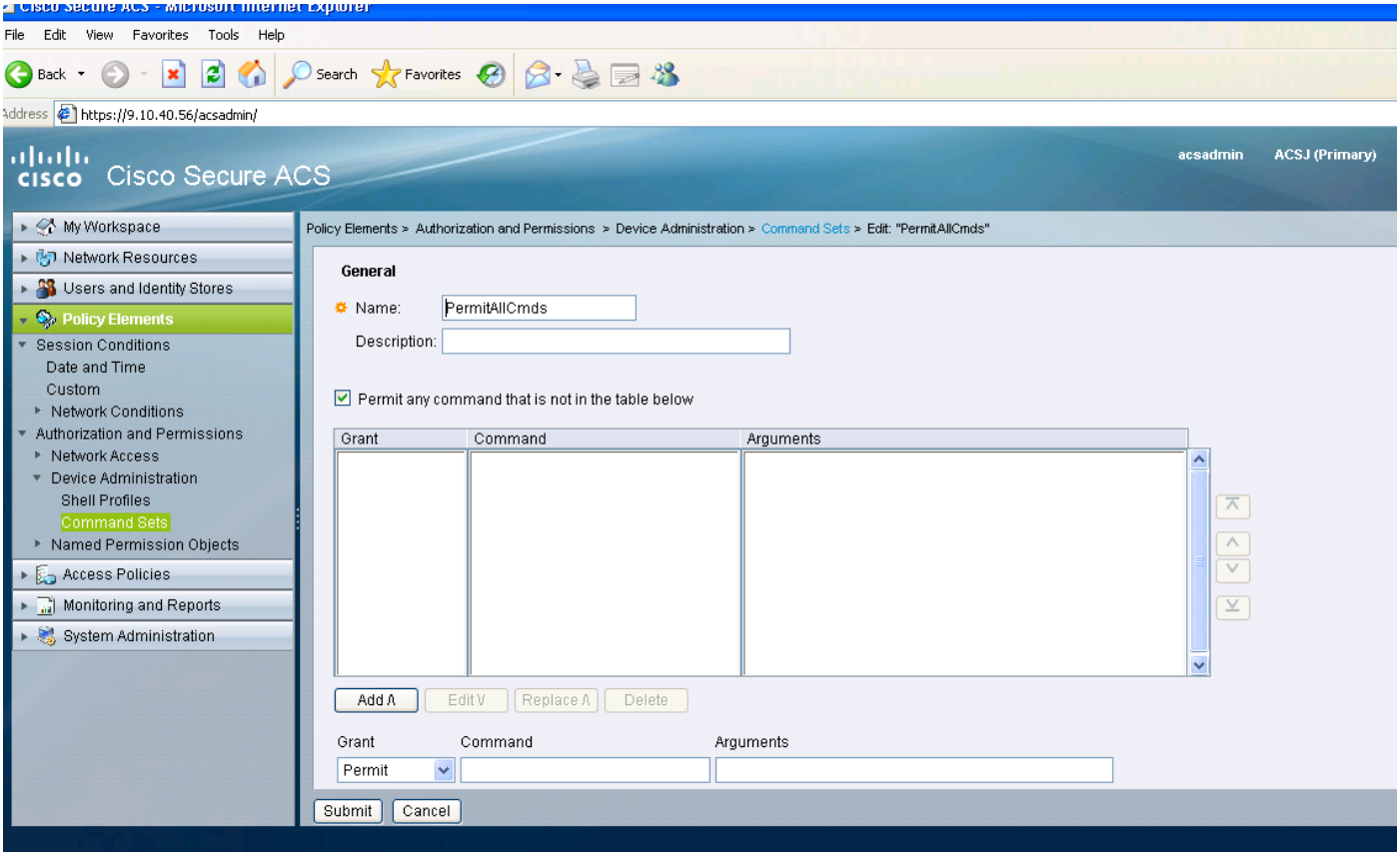
En créer un nouveau.

Allez dans l'onglet « Tâches courantes » et définissez les niveaux de privilège par défaut et maximum sur 15.



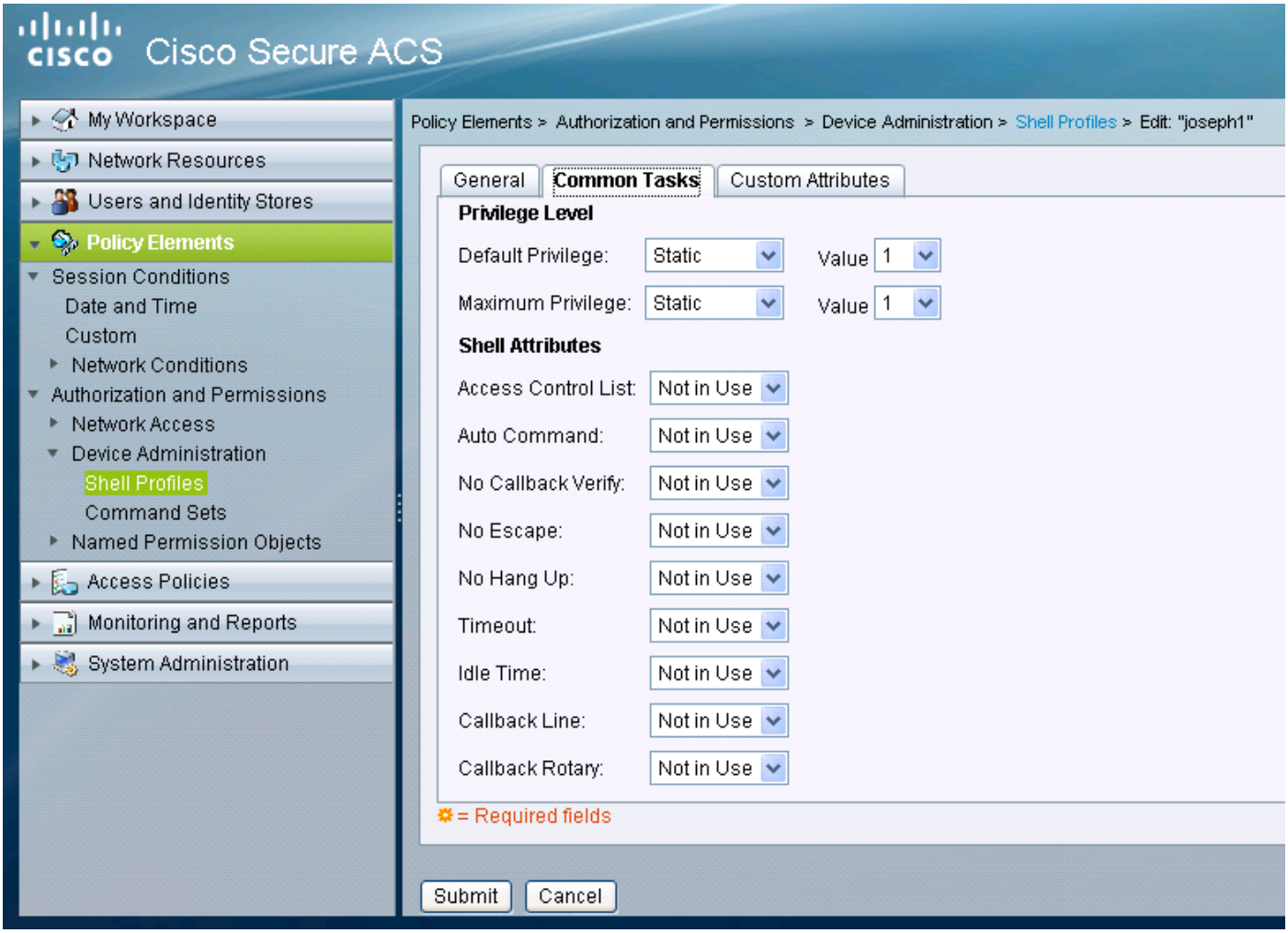
Création de jeux de commandes pour l'utilisateur admin

Les jeux de commandes sont des ensembles de commandes utilisés par tous les périphériques tacacs.Ils peuvent être utilisés pour restreindre les commandes qu'un utilisateur est autorisé à utiliser s'il reçoit ce profil spécifique. Depuis le 5760, la restriction est effectuée sur le code Webui en fonction du niveau de privilège passé, les jeux de commandes pour les niveaux de privilège 1 et 15 sont identiques.



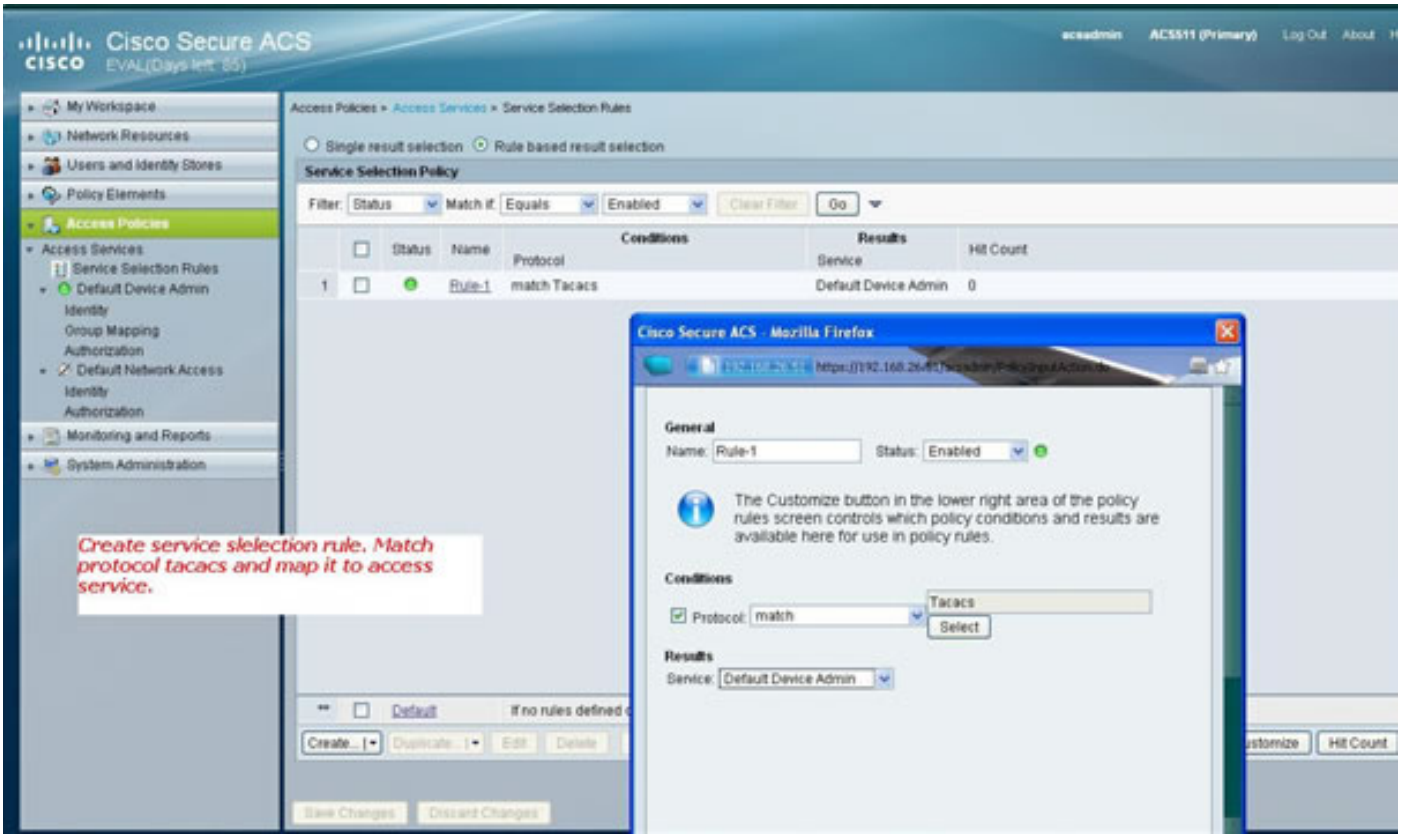
Création d'un profil shell pour l'utilisateur en lecture seule

Créez un autre profil shell pour les utilisateurs en lecture seule. Ce profil diffère par le fait que les niveaux de privilège sont définis sur 1.



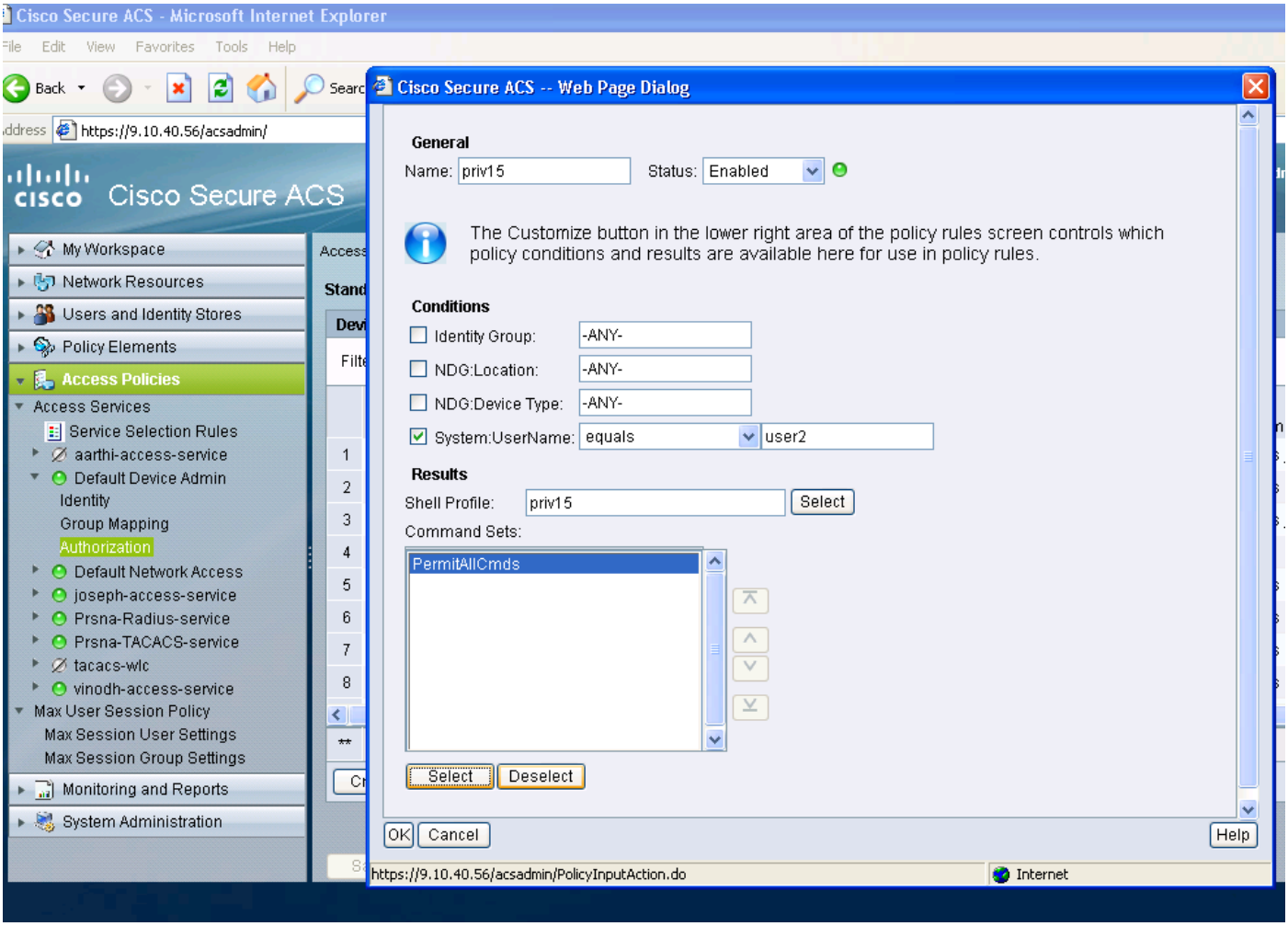
Créer une règle de sélection de service correspondant au protocole tacacs

En fonction de vos stratégies et de votre configuration, assurez-vous que vous avez une règle correspondant aux tacacs provenant du 5760.



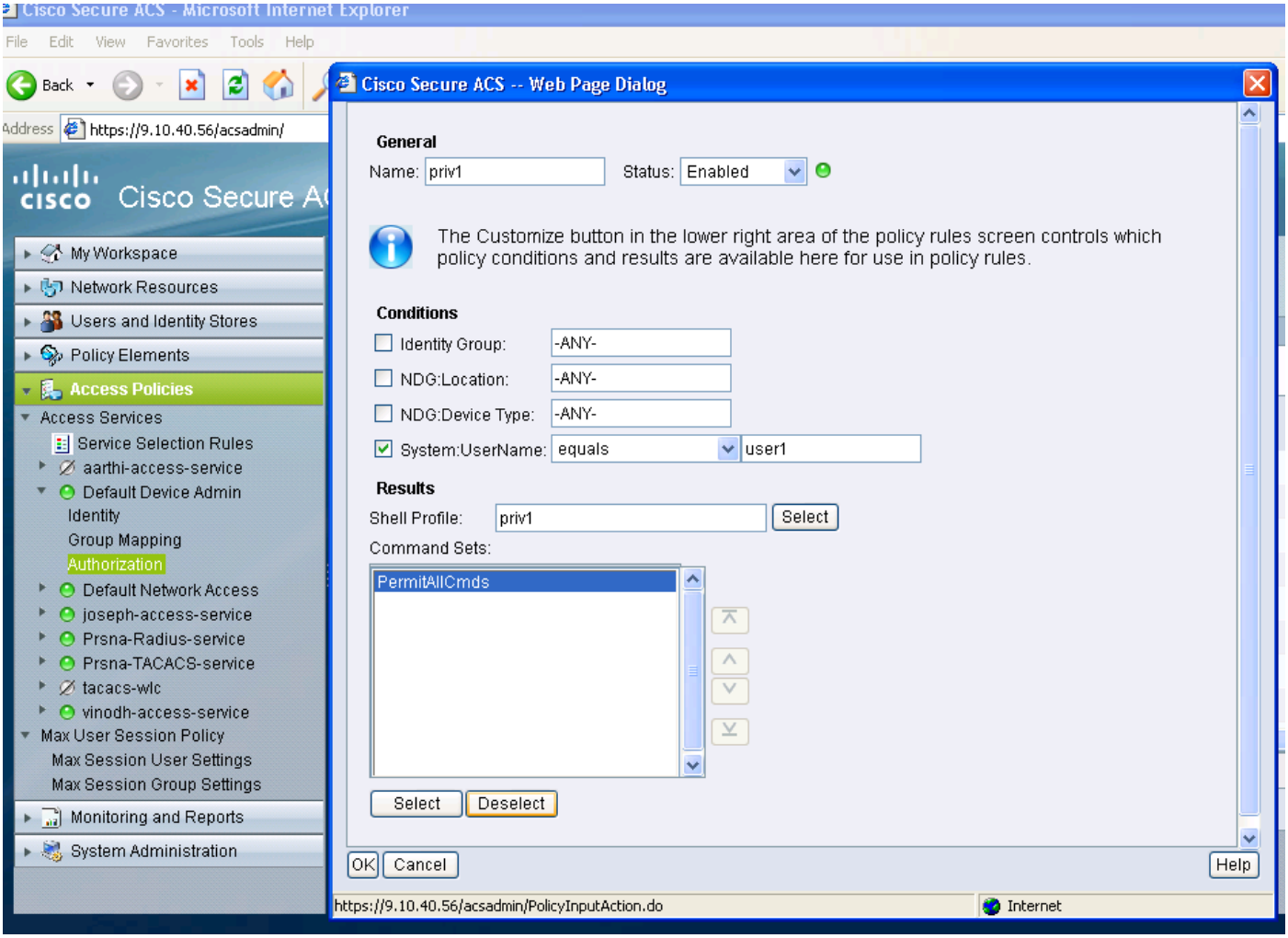
Créer une stratégie d'autorisation pour l'accès à l'administration complète.

La stratégie d'administration de périphérique par défaut utilisée avec la sélection du protocole tacacs est sélectionnée dans le cadre du processus de stratégie d'évaluation. Lorsque vous utilisez le protocole tacacs pour vous authentifier, la stratégie de service sélectionnée s'appelle Stratégie d'administration de périphérique par défaut. Cette politique comporte en elle-même 2 sections. Identité signifie qui est l'utilisateur et à quel groupe appartient-il (local ou externe) et ce qu'il est autorisé à faire selon le profil d'autorisation configuré. Attribuez le jeu de commandes associé à l'utilisateur que vous configurez.



Créer une stratégie d'autorisation pour l'accès en lecture seule à l'administration.

Il en va de même pour les utilisateurs en lecture seule. Cet exemple montre comment configurer le profil de shell de niveau de privilège 1 pour l'utilisateur 1 et le privilège 15 pour l'utilisateur 2.



Configuration du 5760 pour tacacs

1. Le serveur Radius/Tacacs doit être configuré.

tacacs server tac_acct

adresse ipv4 9.1.0.100

clé cisco

2. Configurer le groupe de serveurs

aaa group server tacacs+ gtac

nom du serveur tac_acct

Il n'y a pas de prérequis avant l'étape ci-dessus.

3. configurer les listes de méthodes d'authentification et d'autorisation

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

aaa authentication exec <liste de méthodes> group srv-grp>

aaa Authorization exec default group <srv-grp> —à contourner pour obtenir tacacs sur http.

Les 3 commandes ci-dessus et tous les autres paramètres d'authentification et d'autorisation

doivent utiliser la même base de données, soit radius/tacacs, soit local

Par exemple, si l'autorisation de commande doit être activée, elle doit également pointer vers la même base de données.

Par exemple :

les commandes aaa authentication 15 <method-list> group <srv-grp> —> le groupe de serveurs pointant vers la base de données (tacacs/radius ou local) doivent être identiques.

4. configurer http pour utiliser les listes de méthodes ci-dessus

ip http authentication aaa login-auth <method-list> —> la liste des méthodes doit être spécifiée explicitement ici, même si la liste des méthodes est “ liste par défaut ”

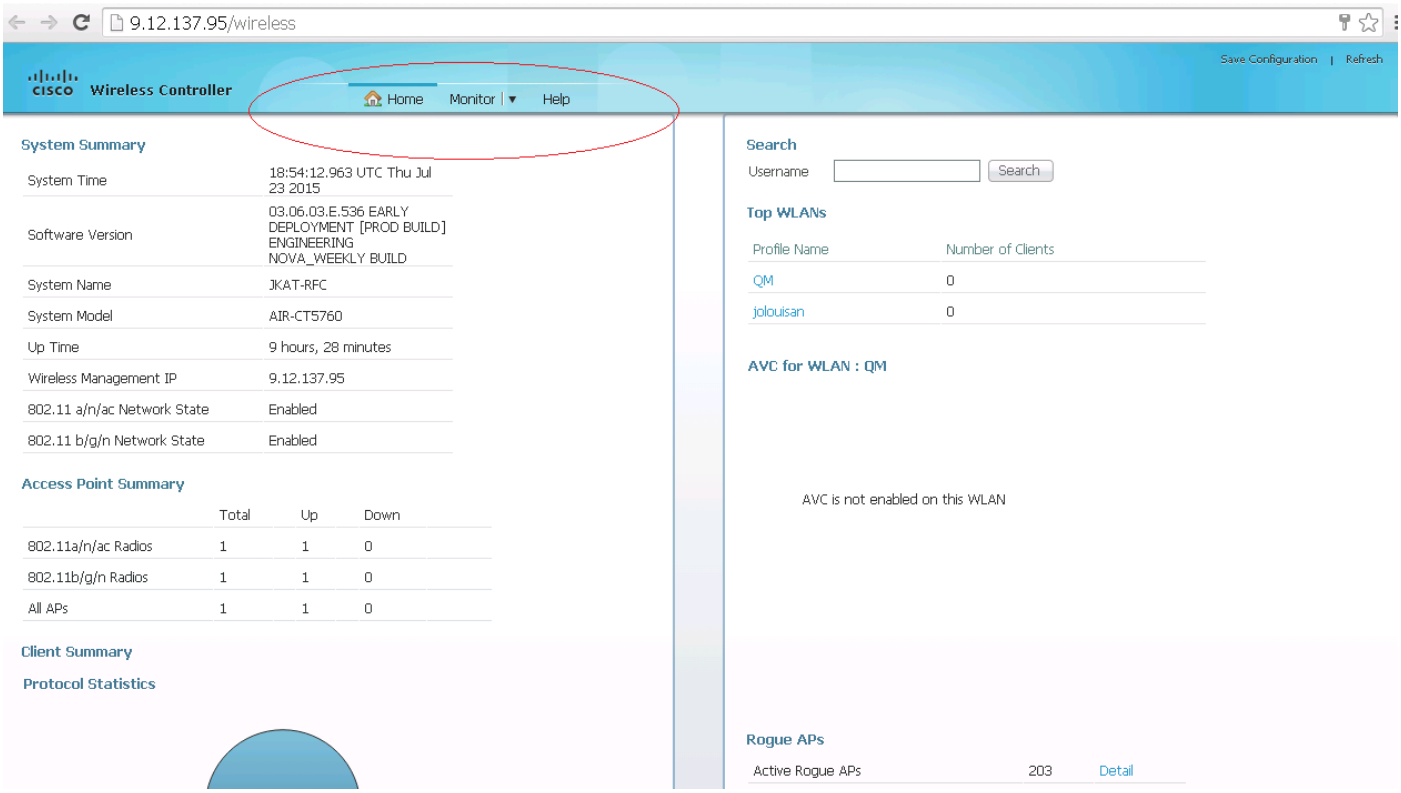
ip http authentication aaa exec-auth <method-list>

** Points à noter

- Ne configurez aucune liste de méthodes sur les paramètres de configuration ” vty de la ligne “. Si les étapes ci-dessus et la ligne vty ont des configurations différentes, les configurations de ligne vty ont la priorité.
- La base de données doit être identique pour tous les types de configuration de gestion tels que ssh/telnet et webui.
- La liste des méthodes de l'authentification HTTP doit être définie explicitement.

Accès au même 5760 avec les 2 profils différents

L'accès ci-dessous est un accès à partir d'un utilisateur de niveau de privilège 1 auquel un accès limité est accordé



L'accès ci-dessous est un accès à partir d'un utilisateur de niveau de privilège 15 auquel vous pouvez accéder en totalité