Intégration NCS avec l'exemple de configuration ACS 5.4

Contenu

Introduction

Ce document fournit un exemple de configuration pour l'authentification TACACS+ et l'autorisation sur la version 1.1 du Cisco Prime Network Control System (NCS).

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Définissez NCS en tant que client dans le système de contrôle d'accès (ACS).
- Définissez l'adresse IP et une clé secrète partagée identique sur l'ACS et le NCS.

Composants utilisés

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

- Version 5.4 ACS
- Version 1.1 de perfection NCS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

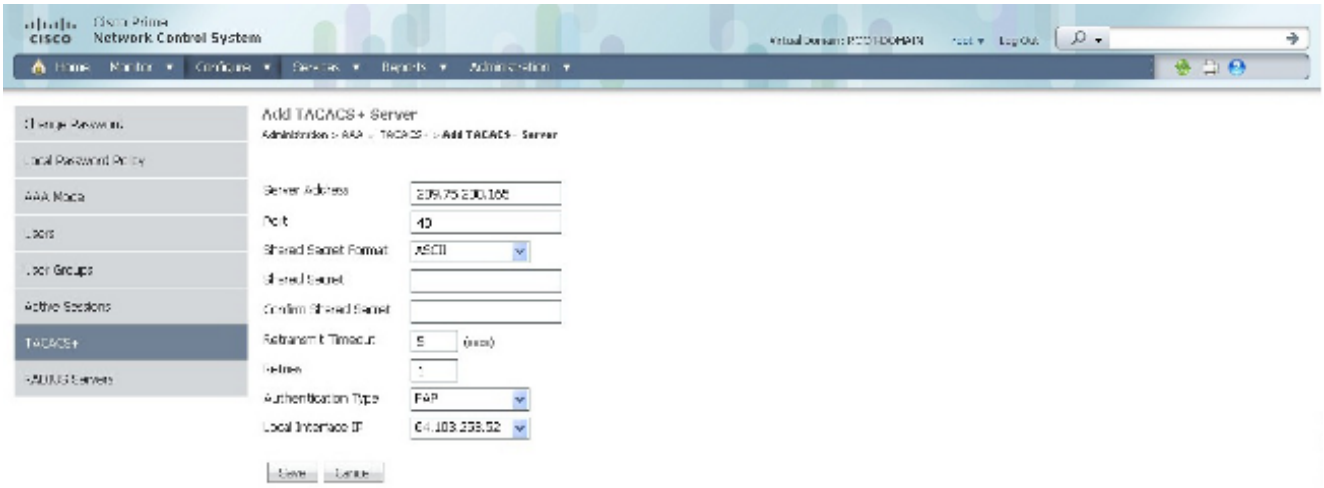
Dans cette section, vous êtes présenté avec les informations utilisées afin de configurer les caractéristiques décrites dans ce document.

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Ajoutez ACS en tant que serveur TACACS

Terminez-vous ces étapes afin d'ajouter ACS en tant que serveur TACACS :

1. Naviguez vers la **gestion > l'AAA**.
2. Du menu gauche de barre latérale, choisissez **TACACS+**, et affichages de la cette information :



La page TACACS+ affiche l'adresse IP, port, retransmet le débit, et le type d'authentification.

3. Ajoutez l'adresse IP du serveur ACS.
4. Écrivez le secret partagé par TACACS+ utilisé par le serveur ACS.
5. Ressaisissez le secret partagé dans la zone de texte **secrète partagée par confirmer**.
6. Quittez le reste des champs sur leur valeur par défaut.
7. Cliquez sur **Submit**.

Paramètres de mode d'AAA

Afin de choisir un mode d'Authentification, autorisation et comptabilité (AAA), terminez-vous ces étapes :

1. Naviguez vers la **gestion > l'AAA**.

2. Choisissez le **mode d'AAA du** menu gauche de barre latérale, et les affichages de la cette information :

3. Choisissez **TACACS+**.

4. Cochez le **retour d'enable dans la** case **locale** si vous voulez que l'administrateur utilise la base de données locale quand le serveur externe d'AAA (ACS) est en panne. Ceci est recommandé de sorte que l'authentification se produise toujours si le serveur TACACS+ échoue. Une fois que la configuration est vérifiée et des travaux, vous pouvez apporter des modifications, si désiré.

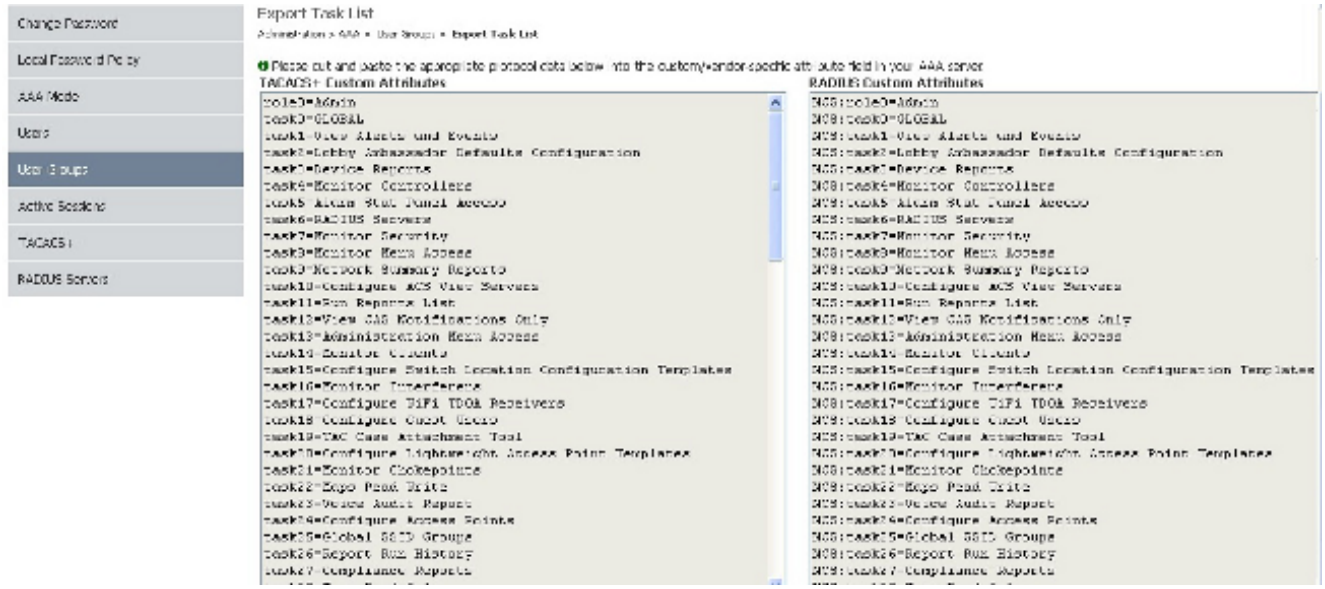
Configuration de version 5.4 ACS

Pour la configuration de version 5.4 ACS, vous devez se terminer ces étapes afin d'envoyer des attributs de l'ACS au NCS :

1. Récupérez les attributs :

   Naviguez vers la **gestion** > l'**AAA** > les **groupes d'utilisateurs**.

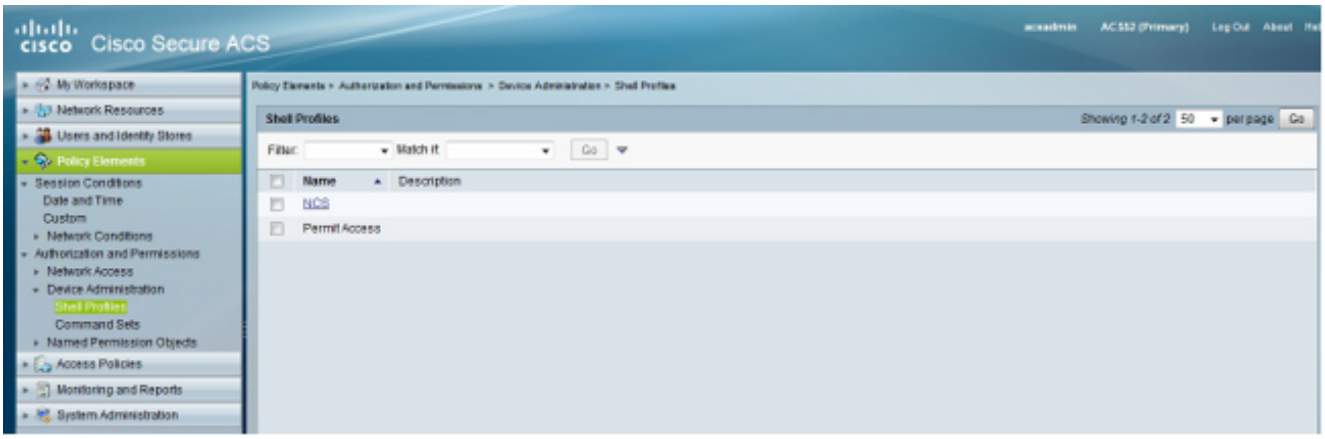
   Cet exemple affiche l'authentification d'administrateur. Recherchez le **nom de groupe d'admin** dans la liste, et cliquez sur l'option de **liste des tâches** du côté droit.



2. Exportez et sauvegardez les attributs à l'appareil de bureau.

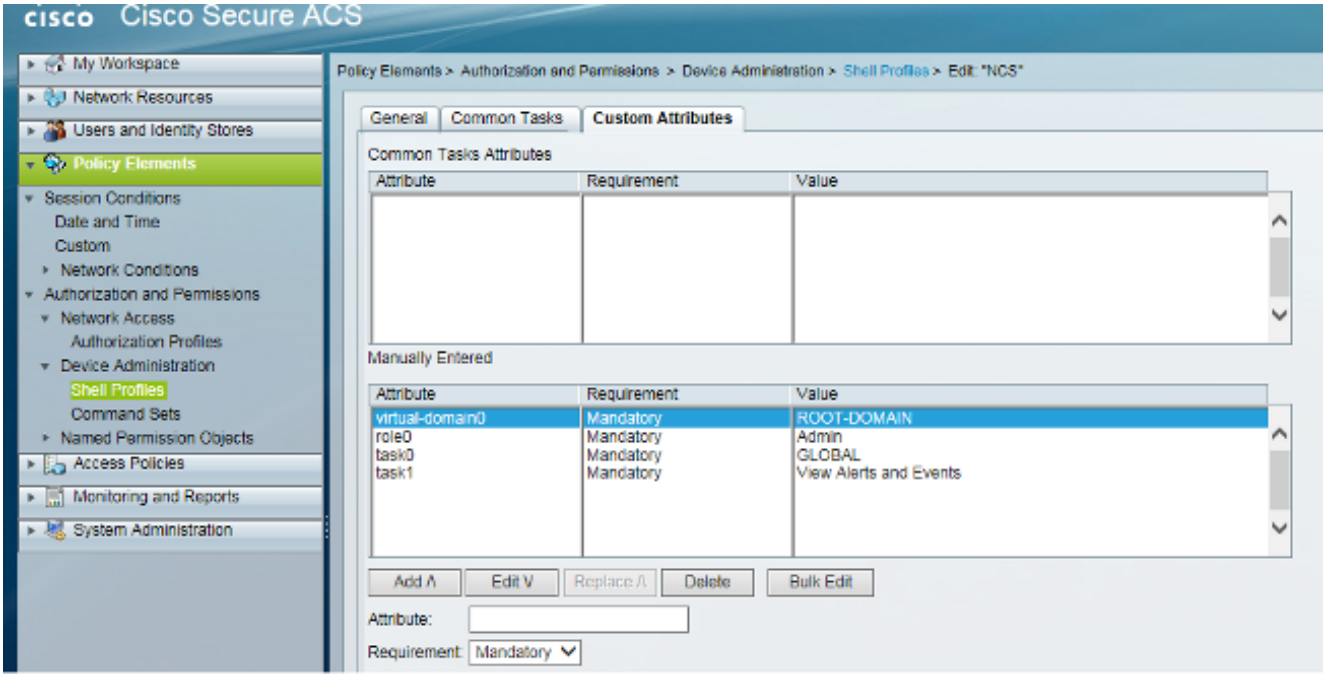
3. Ouvrez une session au **GUI d'admin ACS**, et naviguez des **profils** vers des **éléments de stratégie > l'authentification et des autorisations > de périphérique gestion > shell** afin de créer un profil de shell.

4. Nommez le profil **NCS**.



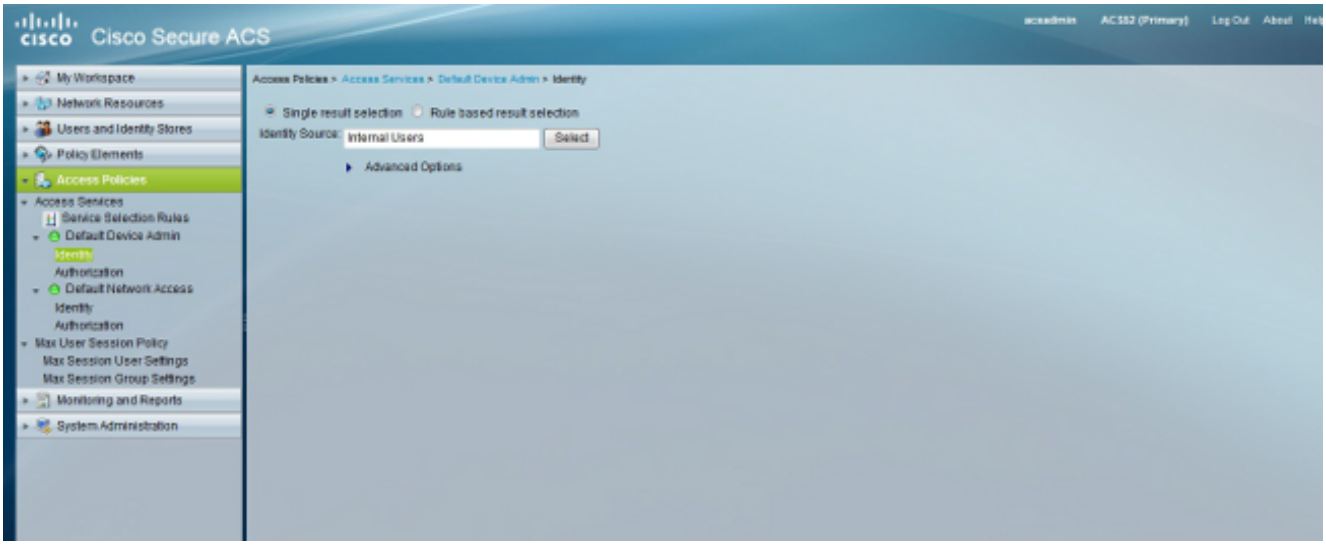
5. **Des attributs personnalisés** tabulez, écrivez ces valeurs :

Attribute	Requirement	Value
role0	Mandatory	Admin
task0	Mandatory	GLOBAL
task1	Mandatory	View Alerts and Events
Virtual-domain0	Mandatory	ROOT-DOMAINRemarque: le Virtuel-domaine est inclus dans la liste au cas où vous utiliseriez une version récente de NCS. Vous devez définir le domaine virtuel d'utilisateur.

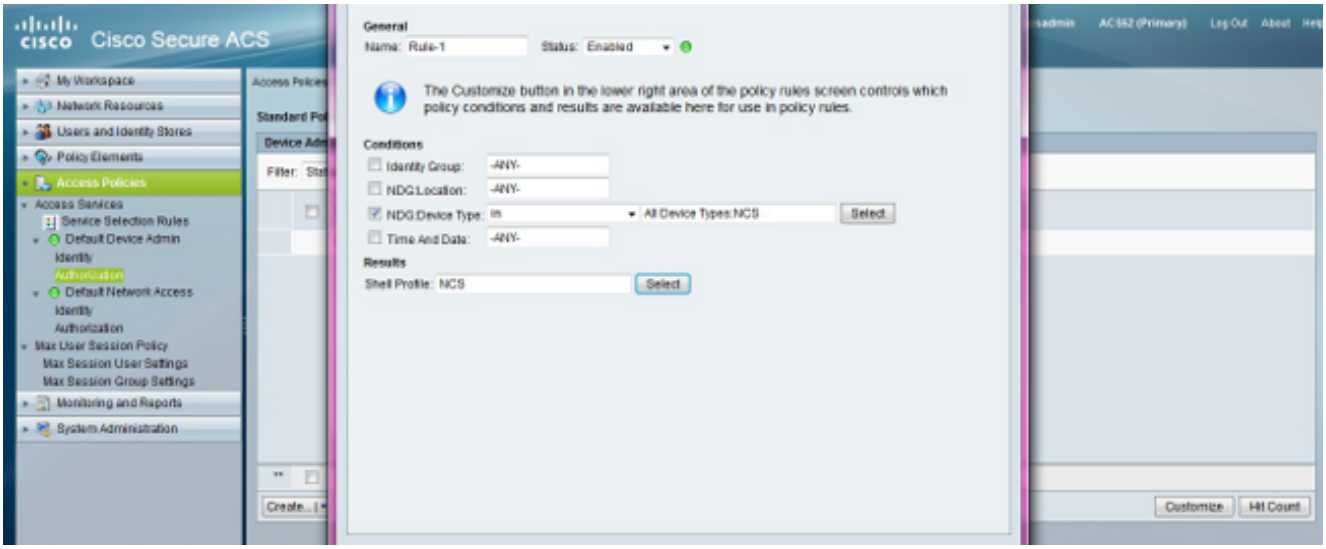


6. Soumettez les modifications afin de créer un rôle basé sur attribut pour le NCS.

7. Naviguez **pour accéder à des stratégies** > des **services d'accès** > l'**admin** > l'**identité de périphérique de par défaut**, et choisissez les **utilisateurs internes** pour la source d'identité.



8. Créez une nouvelle règle d'autorisation ou éditez une règle qui existe déjà dans la stratégie correcte d'accès. Par défaut, des demandes TACACS+ sont traitées par la stratégie **par défaut d'**accès d'**admin de périphérique**.



9. Dans la région de **conditions**, choisissez les conditions appropriées. Dans la région de **résultats**, choisissez **NCS** pour le profil de shell.

10. Cliquez sur **OK**.

Vérifiez

Connectez-vous dans le NCS et confirmez que vous avez le rôle d'**admin**.

Dépannez

Si vous ne pouvez pas se connecter dans le NCS, se connecter dans le GUI ACS et naviguer vers la **surveillance et les états** > le **catalogue** > les **protocoles AAA** > l'**authentification TACACS+**. Sélectionnez l'authentification défaillante, et choisissez les **détails** afin de voir pourquoi l'échec de l'authentification ou avez été rejeté.