Gestion de système de contrôle sans fil et de Système de contrôle de réseau avec l'exemple de configuration ACS 5.x

Contenu

Introduction

Ce document décrit comment utiliser le Cisco Secure Access Control Server (ACS) 5.x afin de configurer la gestion du Système de contrôle sans fil Cisco (WCS) et du Cisco Prime Network Control System (NCS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Système de contrôle sans fil Cisco
- Cisco Prime Network Control System
- Cisco Secure Access Control Server

Composants utilisés

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

- Système de contrôle sans fil Cisco 7.0.172.0
- Cisco Secure ACS 5.x

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

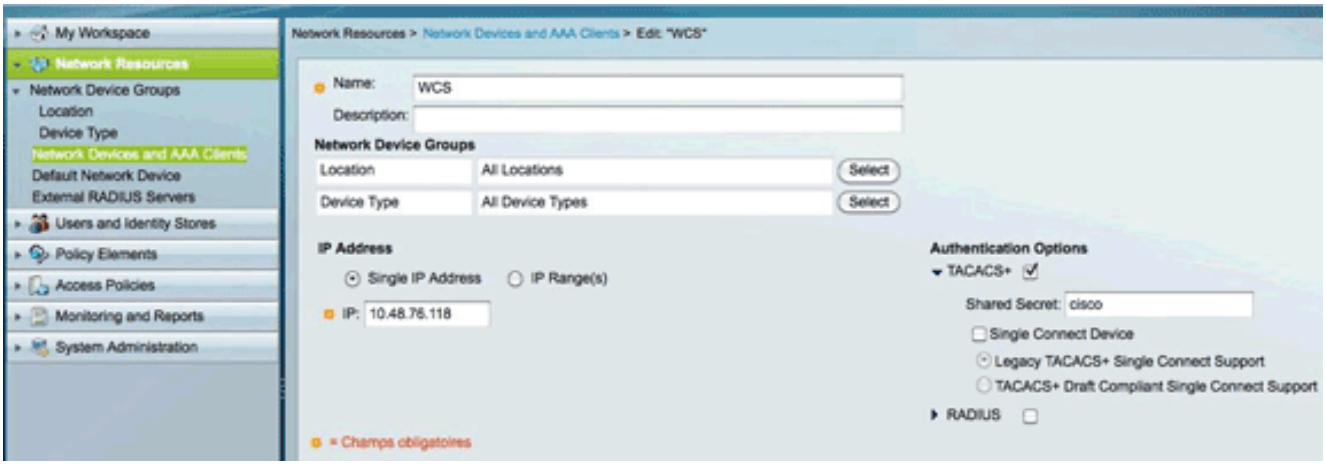
Configurez

Cette configuration d'échantillon décrit comment authentifier un utilisateur avec TACACS+.

Remarque: Bien que les diverses options et possibilités existent quand vous authentifiez des utilisateurs WCS/NCS avec le Cisco Secure ACS 5.x, non toutes les combinaisons sont décrites dans ce document. Cependant, cet exemple te fournit les informations nécessaires pour comprendre comment modifier l'exemple à la configuration précise que vous voulez réaliser.

Étape 1. Ajoutez le WCS aux clients d'AAA ACS.

1. Sur le Cisco Secure ACS, choisissez les **ressources de réseau > les périphériques de réseau et les clients d'AAA**.

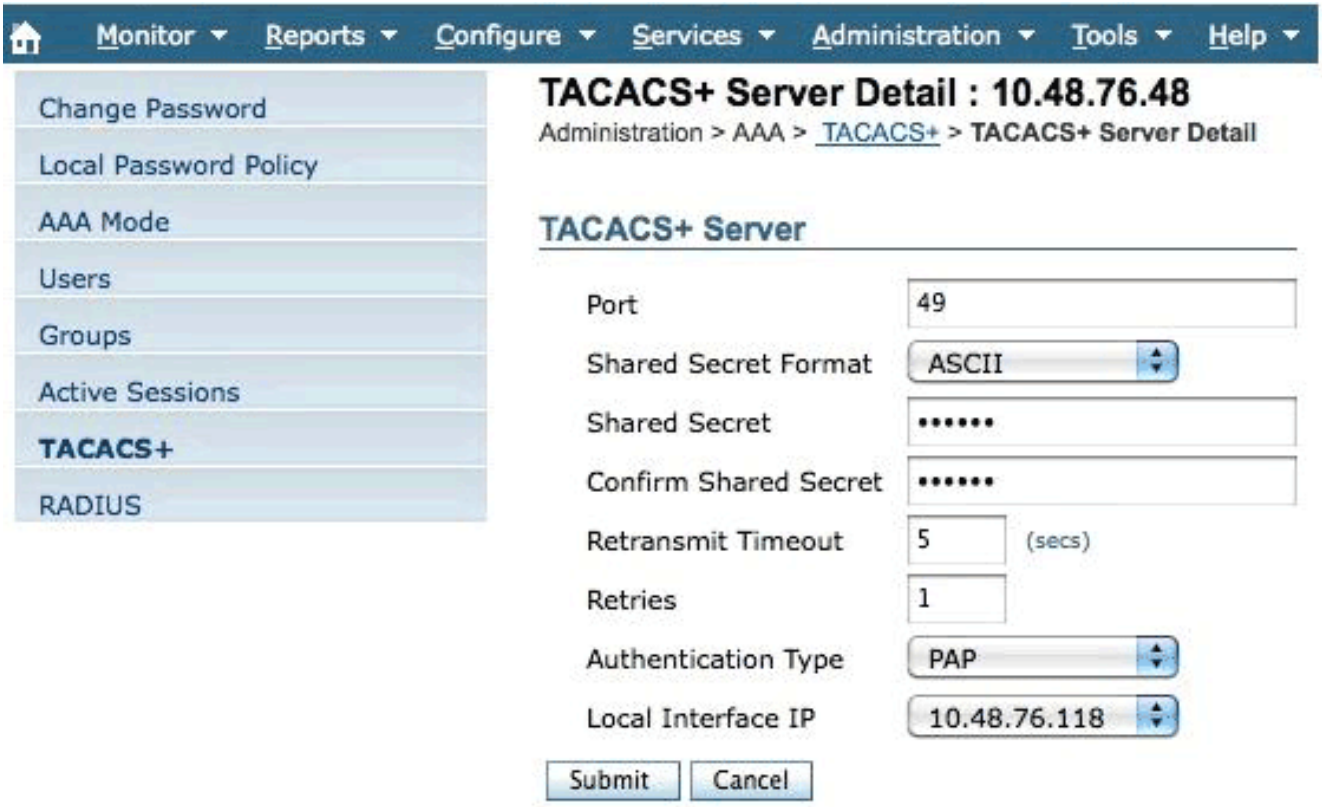


2. Écrivez un nom dans la zone d'identification.
3. Écrivez l'adresse IP WCS dans le domaine d'adresse IP.
4. Sous la région d'options d'authentification, cliquez sur la case **TACACS+** afin d'activer TACACS+, et puis écrivez un terme à utiliser comme secret partagé.**Remarque:** Cet exemple utilise *Cisco* comme secret partagé ; cependant, pour des raisons de sécurité, vous devriez utiliser un terme moins évident.

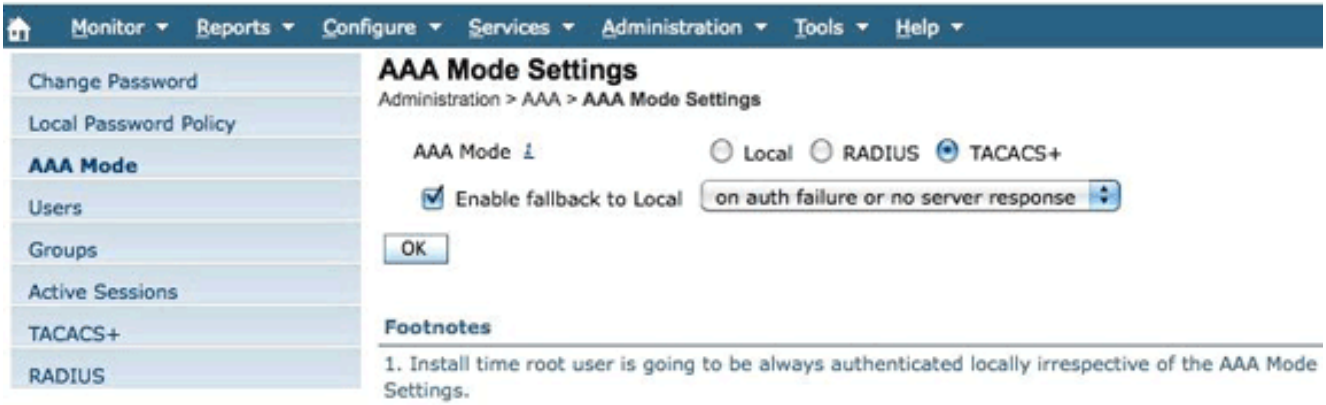
Étape 2. Ajoutez le Cisco Secure ACS en tant que serveur TACACS+ dans WCS.

1. Ouvrez une session à WCS, et choisissez la **gestion > l'AAA**.
2. Clic

TACACS+.



3. Écrivez votre terme secret partagé dans le secret partagé et confirmez les champs secrets partagés.
4. Choisissez l'adresse IP de Cisco ACS du champ IP d'interface locale.
5. Sur la zone gauche de navigation, **mode d'AAA de** clic.



6. Cliquez sur la case d'option **TACACS+**.**Remarque:** Pour des raisons de sécurité, Cisco recommande que vous choisissiez **sur la panne authentique ou aucune réponse de serveur du** retour d'enable à la liste déroulante locale. Choisir cette option vous empêche d'être verrouillé en cas de questions. Vous pouvez changer l'option une fois que tout travaille correctement.

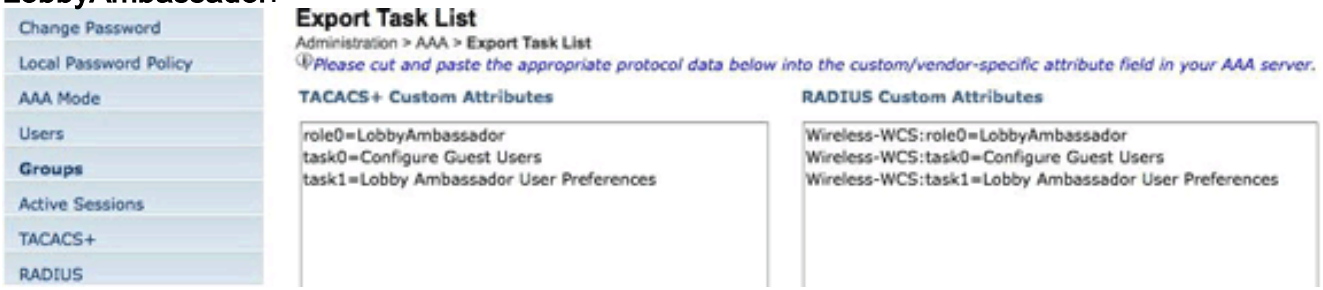
Étape 3. Configurez le profil correct de shell sur ACS.

Cette étape décrit comment configurer le Cisco Secure ACS pour renvoyer les attributs corrects afin de déterminer les privilèges des utilisateurs sur WCS.

1. Dans la zone gauche de navigation, **groupes de** clic.Une liste de types d'utilisateur apparaît.

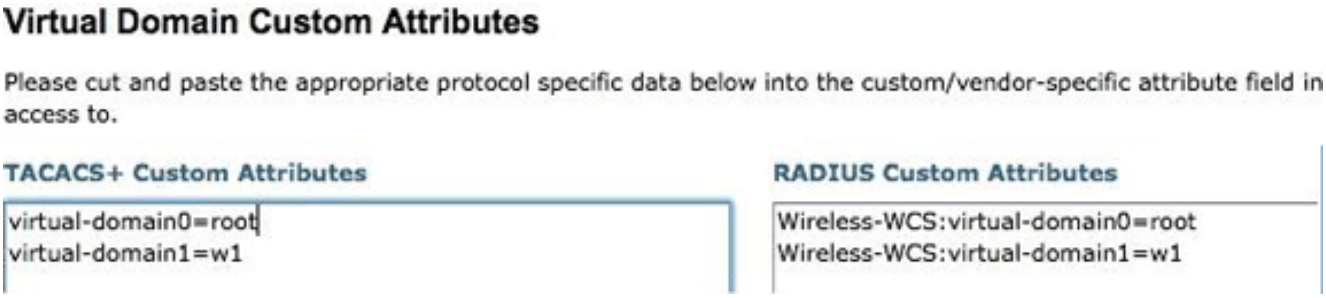
Cet exemple authentifie un utilisateur du type d'utilisateur d'ambassadeur de lobby.

2. Cliquez sur le lien de **liste des tâches** à côté du groupe de **LobbyAmbassador**.

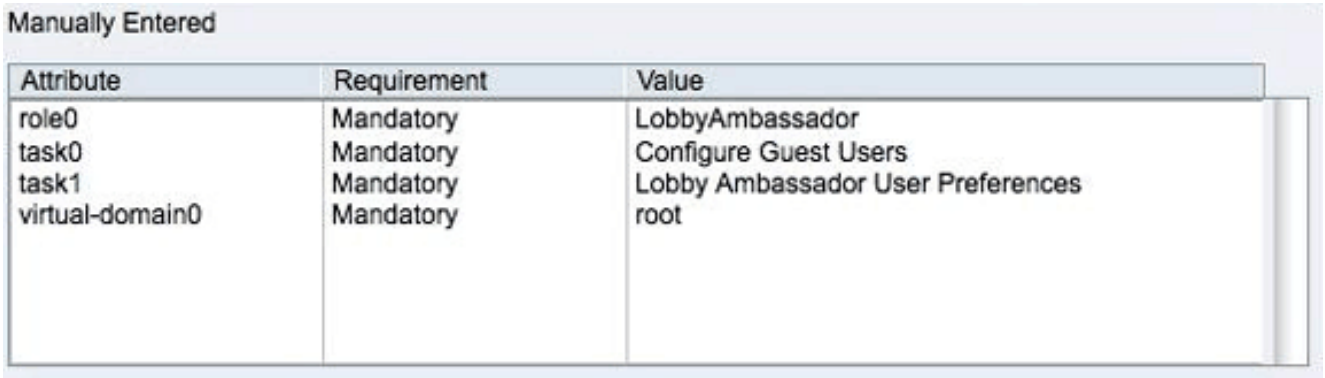


Remarque: Vous devez configurer le rôle de l'utilisateur (ambassadeur de lobby pour cet exemple) et une liste de tâches qu'ils peuvent effectuer et des commandes de menu ils peuvent accéder à. Si vous utilisez une version récente de WCS, vous devez également configurer le domaine virtuel que l'utilisateur appartiendra à.

3. Choisissez la **gestion > les domaines virtuels**.
4. **Exportation de** clic.



5. **Des profils** choisissez les **éléments de stratégie > l'autorisation et les autorisations > de périphérique gestion > shell** afin de créer un nouveau profil de shell.
6. Écrivez un nom signicatif (tel que *WCS*), et puis cliquez sur l'onglet d'**attributs personnalisés**.
7. Configurez les attributs comme ils existent sur WCS.

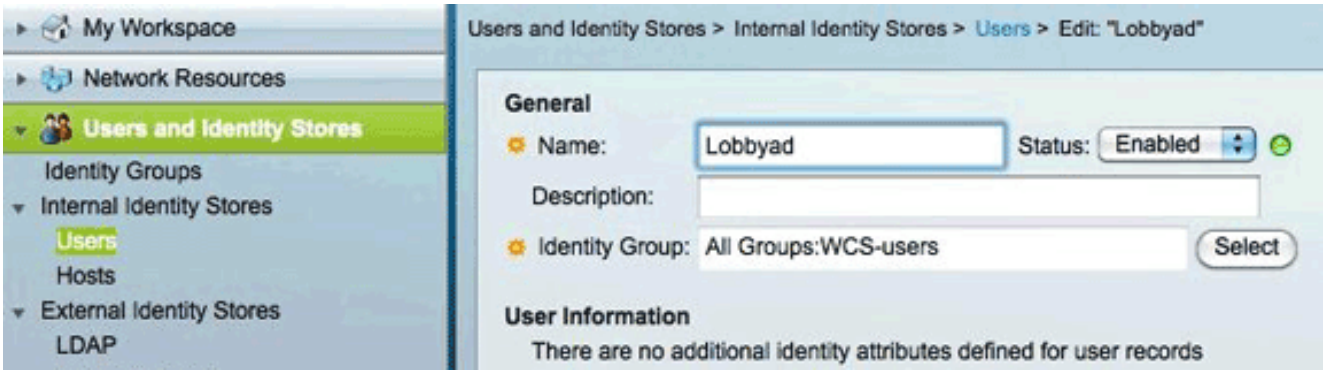


Remarque: Dans les versions d'ACS plus tôt que le correctif 7 de version 5.2, vous pourriez faire face à des questions quand vous écrivez une tâche qui contient le mot « alerte ». Ceci est réparé dans des versions postérieures ACS. Le même problème existe dans des versions du Cisco Identity Services Engine (ISE) plus tôt que 1.2.Voici un exemple de la façon écrire manuellement les attributs :`-type “role0” in the “Attribute” field`
`-type “LobbyAmbassador” in the Value field`
`-click the “add” button.`
`Etc… for the other attributes.`**Remarque:** Dans ACS 4, il était de copier possible/pâte la liste d'attributs du GUI WCS sur le GUI ACS 4. Dans ACS 5, ils doivent être entrés un.En NCS et infrastructure principale, l'attribut doit être écrit dans une commande très spécifique. La commande est domaine virtuel, rôle, et la liste de tâches. Si entré dans la commande fausse,

NCS/Prime refuse l'authentification.`NCS:virtual-domain0=ROOT-DOMAIN`
`NCS:role0=Super Users`
`NCS:task0=View Alerts and Events`

Étape 4. Configurez le Cisco Secure ACS pour renvoyer les attributs.

1. Configurez un utilisateur (cet exemple utilise *Lobbyad*) en tant qu'utilisateur sur ACS.



Remarque: Pour la facilité de la configuration, cet exemple ajoute l'utilisateur de Lobbyad au groupe de WCS-*utilisateurs*. (Cette étape est facultative.)

2. Dans des stratégies d'Access, sous l'**admin par défaut > l'autorisation de périphérique**, configurez une règle d'apparier l'authentification WCS.

3. Si le nom d'utilisateur appartient aux WCS-*utilisateurs* groupez, renvoyez le profil de shell de *wcs* (qui contient les attributs de groupe).
4. Si vous voulez configurer d'autres types d'utilisateurs (tels que des administrateurs), vous devez configurer un autre profil de shell pour renvoyer différents attributs. Dès lors, vous devez grouper des administrateurs dans un groupe différent afin de différencier et savoir quel profil de shell à retourner.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide de configuration de Système de contrôle sans fil Cisco, release 7.0.172.0
- Guide utilisateur pour le Système de contrôle d'accès sécurisé Cisco 5.2
- Support et documentation techniques - Cisco Systems