Intégration principale d'infrastructure avec l'exemple de configuration ACS 4.2 TACACS

Contenu

Introduction

Ce document décrit l'exemple de configuration pour le Terminal Access Controller Access Control System (TACACS+)

authentification et autorisation sur l'application de l'infrastructure de perfection de Cisco (pi).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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

- Version 4.2 ACS
- Version 3.0 principale d'infrastructure

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

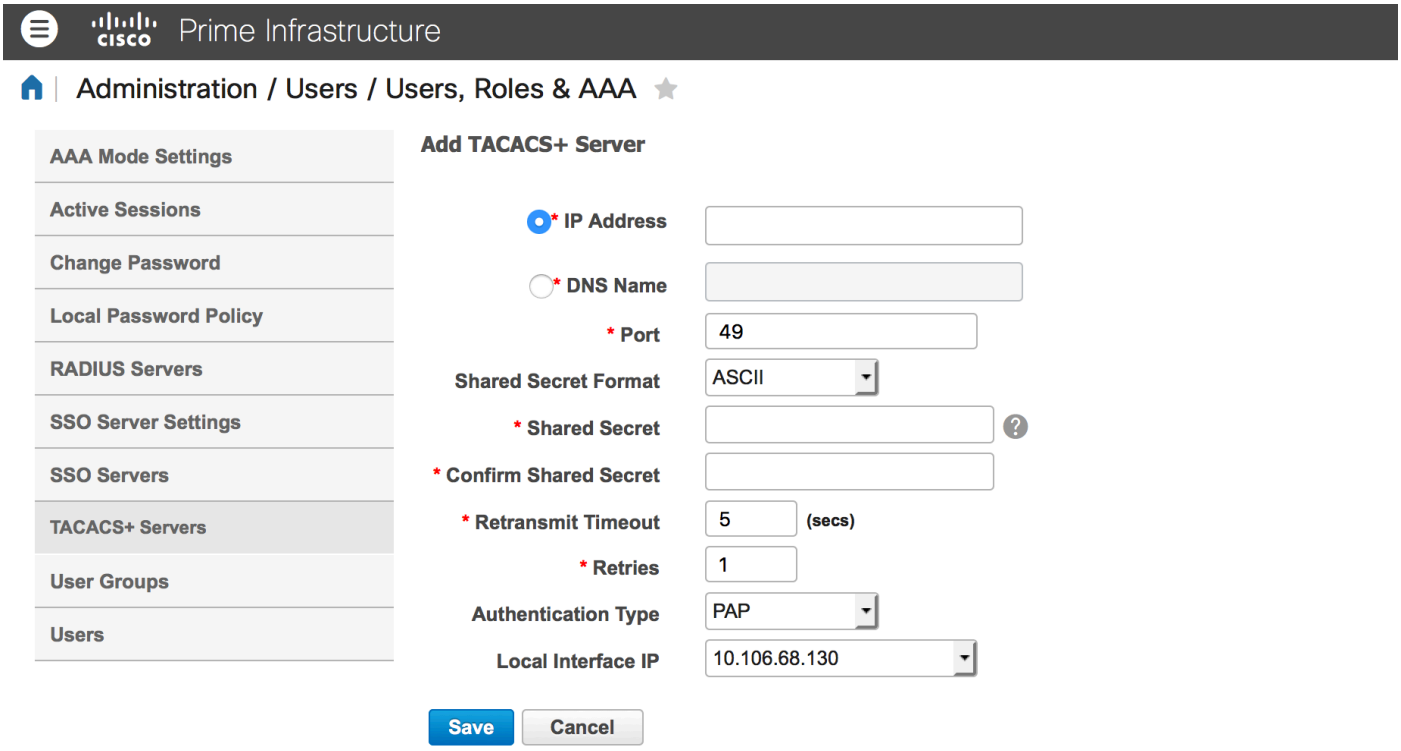
Configurations

Ajoutez ACS comme serveur TACACS dans pi

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

Étape 1. Naviguez vers la **gestion > les utilisateurs > les utilisateurs, les rôles et l'AAA dans pi**

Étape 2. Du menu gauche de barre latérale, les **serveurs** choisis **TACACS+**, **ajoutent** dessous des **serveurs TACACS+** cliquent sur Go et la page paraît suivant les indications de l'image :



Étape 3. Ajoutez l'adresse IP du serveur ACS.

Étape 4. Écrivez le secret partagé par TACACS+ configuré dans le serveur ACS.

Étape 5. Ressaisissez le secret partagé dans la zone de texte **secrète partagée par confirmer**.

Étape 6. Quittez le reste des champs sur leur valeur par défaut.

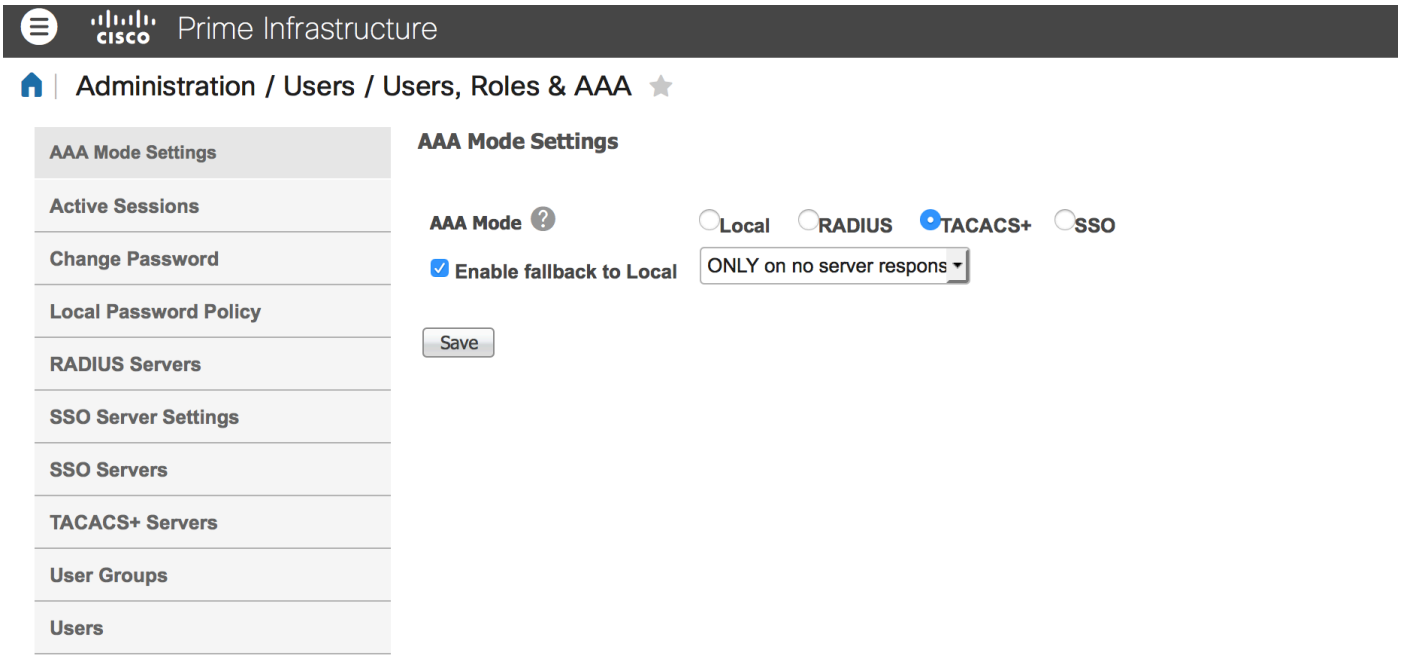
Étape 7. Cliquez sur Submit.

Paramètres de mode d'AAA dans pi

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

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

Étape 2. Choisissez le **mode d'AAA du** menu gauche de barre latérale, vous peut voir la page suivant les indications de l'image :

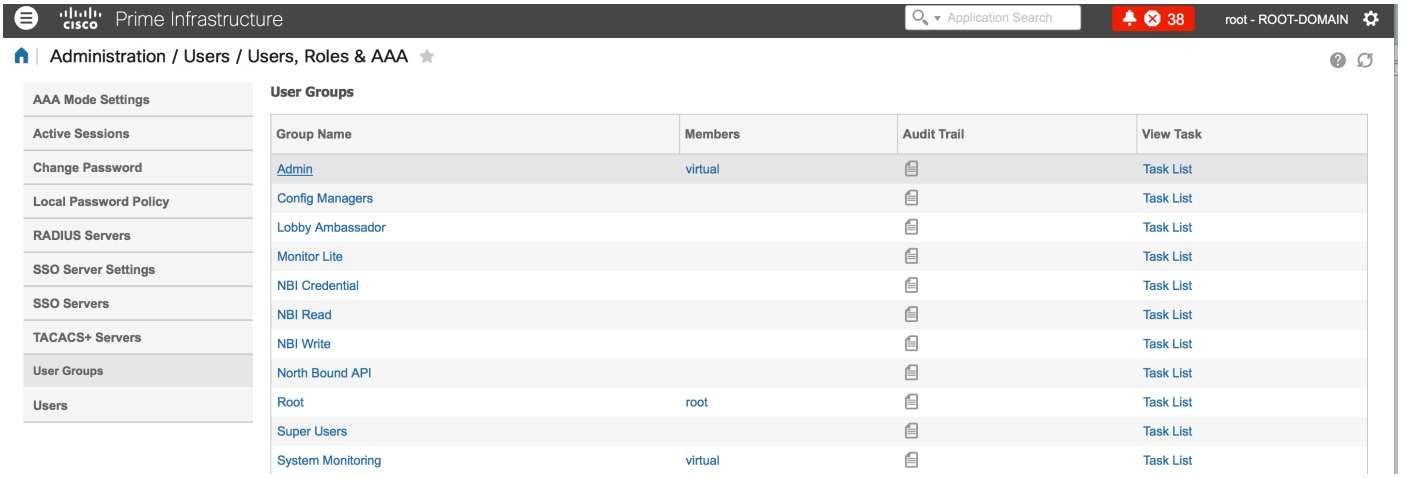


Étape 3. **TACACS+** choisi.

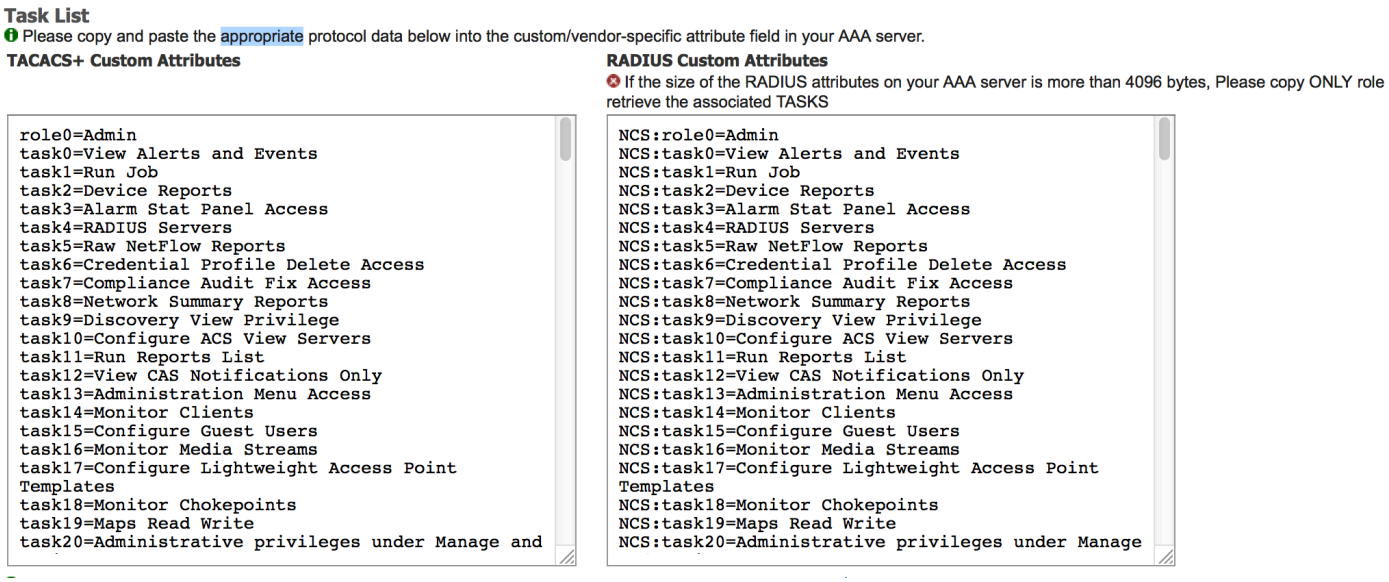
Étape 4. Cochez le **retour d'enable dans la** case **locale**, si vous voulez que l'administrateur utilise la base de données locale quand le serveur ACS n'est pas accessible. C'est une configuration recommandée.

Récupérez le rôle de l'utilisateur d'attributs de pi

Étape 1. 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, suivant les indications de l'image :



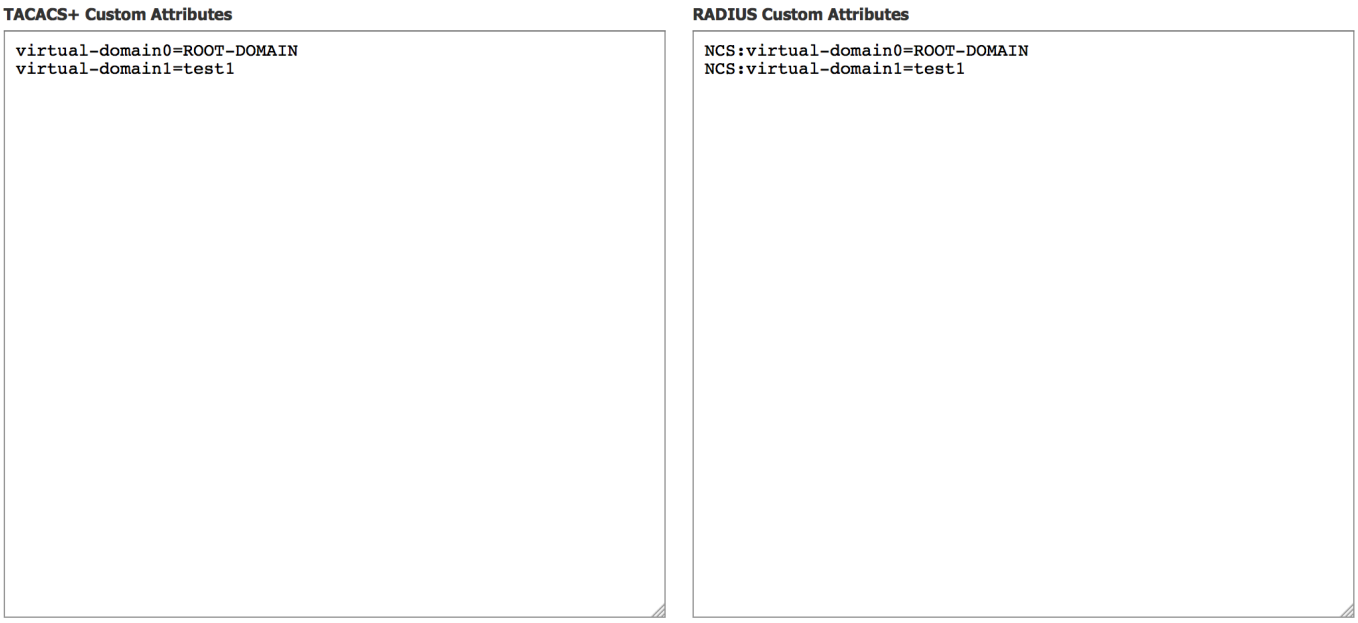
Une fois que vous cliquez sur l'option de **liste des tâches**, la fenêtre apparaît, suivant les indications de l'image :



Étape 2. Copiez ces attributs et sauvegardez-les sur un fichier de Notepad.

Étape 3. Vous pouvez devoir ajouter des attributs virtuels faits sur commande de domaine dans le serveur ACS. Les attributs virtuels faits sur commande de domaine sont disponibles en dessous de la même page de liste des tâches.

Étape 4. Cliquez sur **a en fonction cliquez ici l'**option d'obtenir la page virtuelle d'attribut de domaine, et vous pouvez voir la page, suivant les indications de l'image :

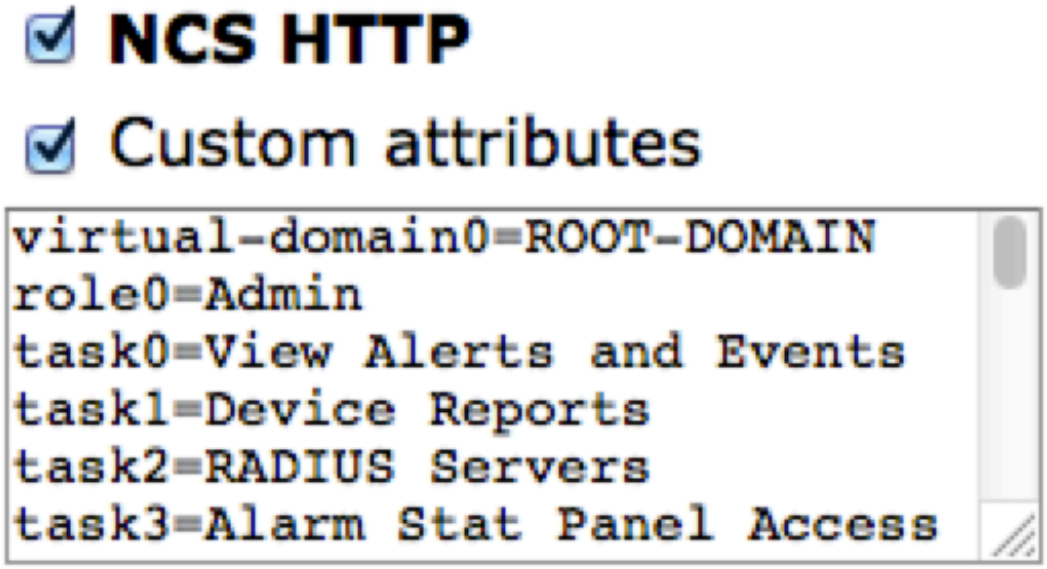


Configurez ACS 4.2

Étape 1. Ouvrez une session au **GUI d'admin ACS**, et naviguez vers la **configuration d'interface** > la page **TACACS+**.

Étape 2. Créez le nouveau service pour la perfection. Cet exemple affiche un nom de service configuré avec le nom **NCS**, suivant les indications de l'image :

Étape 3. Ajoutez tous les attributs du Notepad créé dans l'étape 2 à l'utilisateur ou groupez la configuration. Assurez pour ajouter des attributs de virtuel-domaine.



Étape 4. **Ok de** clic.

Vérifiez

Ouvrez une session à la perfection avec le nouveau nom d'utilisateur que vous avez créé et confirmez que vous avez le rôle d'**admin**.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Passez en revue usermgmt.log de la racine principale CLI disponible dans le répertoire de **/opt/CSCOlumos/logs**. Vérifiez s'il y a des messages d'erreur.

```
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - [        [TacacsLoginModule]
user entered username: 138527]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - [        [TacacsLoginModule]
Primary server=172.18.70.243:49]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.TacacsLoginClient].
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.SecondaryTacacsLoginClient].
2016-05-12 15:24:18,518 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[prepare to ping TACACS+ server (> 0):/172.18.70.243 (-1)].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Num of ACS is  3].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[Tacacs:activeACSIndex is  0].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Unable to connect to Server 2: /172.18.70.243 Reason: Connection refused].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] DEBUG usermgmt - [        [Thu May 12 15:24:18
EST 2016] [TacacsLoginModule] exception in client.login( primaryServer, primaryPort,seconda..:
com.cisco.xmp.jaas.XmpAuthenticationServerException: Server Not Reachable: Connection refused]
```

Cet exemple affiche un échantillon de message d'erreur, qui pourrait être dû à de diverses raisons comme la connexion refusée par un Pare-feu, ou de n'importe quel périphérique intermédiaire etc.