

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Configurations](#)

[Ajoutez ACS comme serveur TACACS dans pi](#)

[Paramètres de mode d'AAA dans pi](#)

[Récupérez le rôle de l'utilisateur d'attributs de pi](#)

[Configurez ACS 4.2](#)

[Vérifiez](#)

[Dépannez](#)

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 :

The screenshot shows the 'Add TACACS+ Server' configuration page in Cisco Prime Infrastructure. On the left is a navigation menu with options like 'AAA Mode Settings', 'Active Sessions', 'Change Password', 'Local Password Policy', 'RADIUS Servers', 'SSO Server Settings', 'SSO Servers', 'TACACS+ Servers', 'User Groups', and 'Users'. The main area is titled 'Add TACACS+ Server' and contains the following fields:

- * IP Address (text input)
- * DNS Name (text input)
- * Port: 49 (text input)
- Shared Secret Format: ASCII (dropdown menu)
- * Shared Secret: (password input with a help icon)
- * Confirm Shared Secret: (password input)
- * Retransmit Timeout: 5 (secs) (text input)
- * Retries: 1 (text input)
- Authentication Type: PAP (dropdown menu)
- Local Interface IP: 10.106.68.130 (dropdown menu)

At the bottom are 'Save' and 'Cancel' buttons.

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.

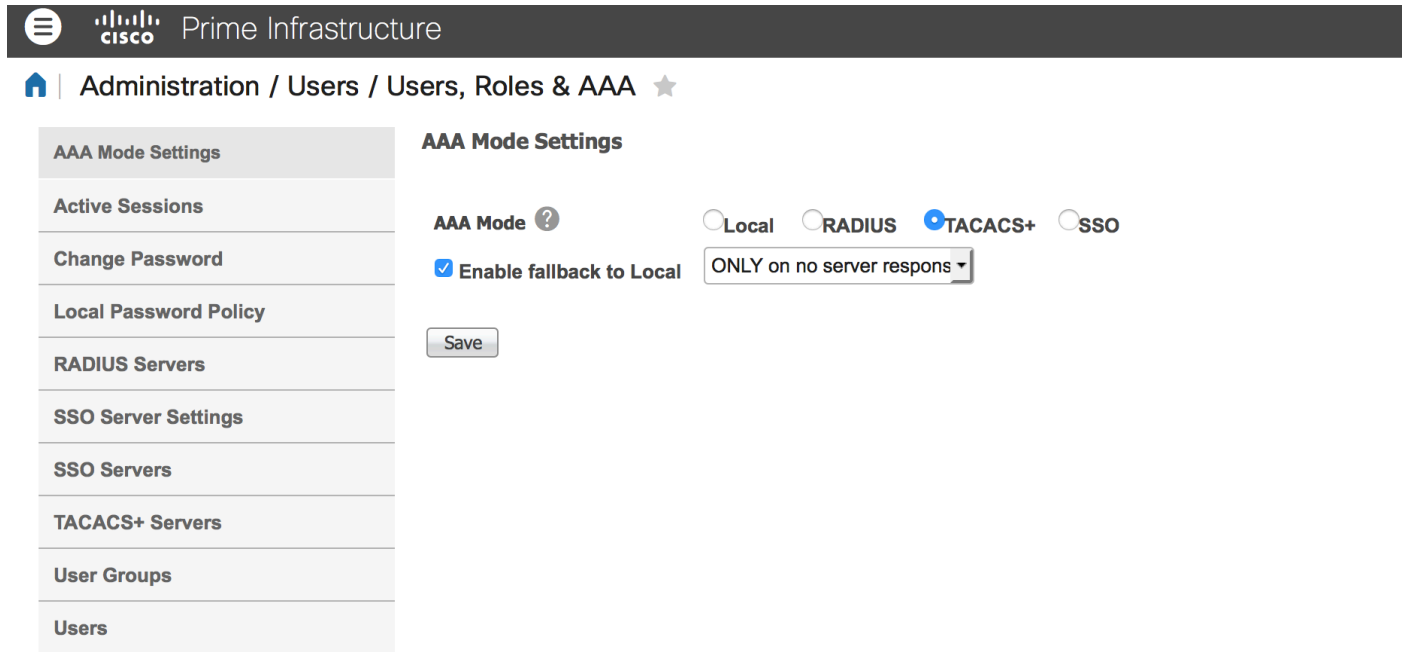
Étape 7. Cliquez sur Submit.

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 :

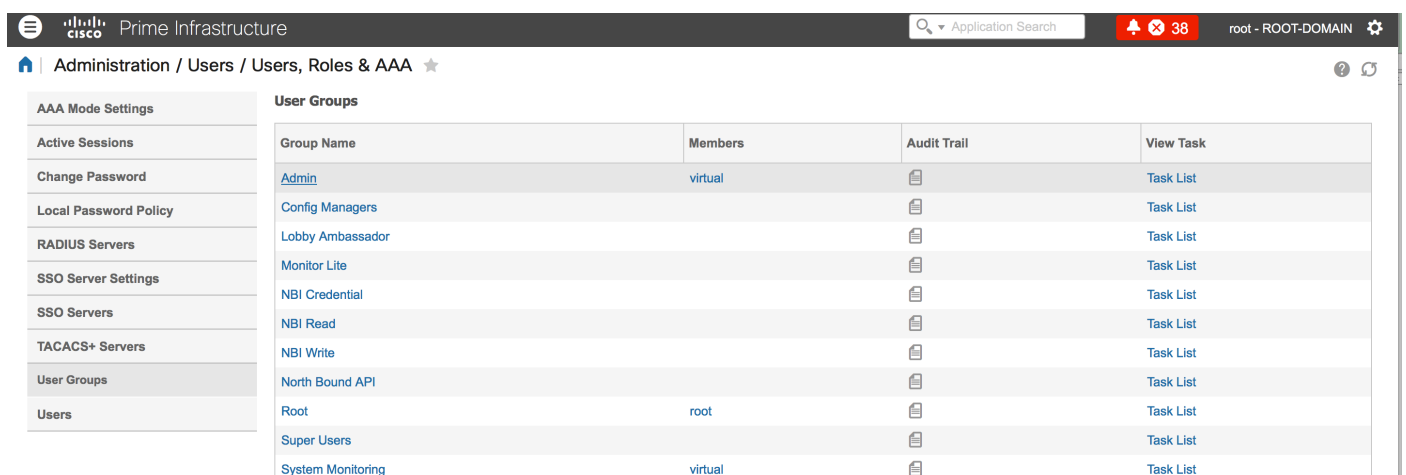


Étape 3. **TACACS+** choisi.

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 :

Task List

Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=View Alerts and Events
task1=Run Job
task2=Device Reports
task3=Alarm Stat Panel Access
task4=RADIUS Servers
task5=Raw NetFlow Reports
task6=Credential Profile Delete Access
task7=Compliance Audit Fix Access
task8=Network Summary Reports
task9=Discovery View Privilege
task10=Configure ACS View Servers
task11=Run Reports List
task12=View CAS Notifications Only
task13=Administration Menu Access
task14=Monitor Clients
task15=Configure Guest Users
task16=Monitor Media Streams
task17=Configure Lightweight Access Point
Templates
task18=Monitor Chokepoints
task19=Maps Read Write
task20=Administrative privileges under Manage and
```

RADIUS Custom Attributes

If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=View Alerts and Events
NCS:task1=Run Job
NCS:task2=Device Reports
NCS:task3=Alarm Stat Panel Access
NCS:task4=RADIUS Servers
NCS:task5=Raw NetFlow Reports
NCS:task6=Credential Profile Delete Access
NCS:task7=Compliance Audit Fix Access
NCS:task8=Network Summary Reports
NCS:task9=Discovery View Privilege
NCS:task10=Configure ACS View Servers
NCS:task11=Run Reports List
NCS:task12=View CAS Notifications Only
NCS:task13=Administration Menu Access
NCS:task14=Monitor Clients
NCS:task15=Configure Guest Users
NCS:task16=Monitor Media Streams
NCS:task17=Configure Lightweight Access Point
Templates
NCS:task18=Monitor Chokepoints
NCS:task19=Maps Read Write
NCS:task20=Administrative privileges under Manage
```

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.

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click [here](#).

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 :

TACACS+ Custom Attributes

```
virtual-domain0=ROOT-DOMAIN
virtual-domain1=test1
```

RADIUS Custom Attributes

```
NCS:virtual-domain0=ROOT-DOMAIN
NCS:virtual-domain1=test1
```

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 :

New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Wireless-WCS	HTTP
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

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.

NCS HTTP

Custom attributes

```
virtual-domain0=ROOT-DOMAIN
role0=Admin
task0=View Alerts and Events
task1=Device Reports
task2=RADIUS Servers
task3=Alarm Stat Panel Access
```

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.