

Exemple de configuration de Prime Infrastructure Integration avec ACS 4.2 TACACS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configurations](#)

[Ajouter ACS en tant que serveur TACACS dans PI](#)

[Paramètres du mode AAA dans PI](#)

[Récupérer les attributs de rôle d'utilisateur à partir de PI](#)

[Configurer ACS 4.2](#)

[Vérification](#)

[Dépannage](#)

Introduction

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

authentification et autorisation sur l'application Cisco Prime Infrastructure (PI).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Définir PI comme client dans Access Control Server (ACS)
- Définissez l'adresse IP et une clé secrète partagée identique sur ACS et PI.

Components Used

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

- ACS version 4.2
- Prime Infrastructure version 3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Configurations

Ajouter ACS en tant que serveur TACACS dans PI

Complétez ces étapes afin d'ajouter ACS en tant que serveur TACACS :

Étape 1. Accéder à **Gestion > Utilisateurs > Utilisateurs, rôles et AAA en PI**

Étape 2. Dans le menu latéral gauche, sélectionnez **Serveurs TACACS+** , sous **Ajouter des serveurs TACACS+**, cliquez sur **Aller** et la page apparaît comme illustré dans l'image :

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Add TACACS+ Server

* IP Address

* DNS Name

* Port: 49

Shared Secret Format: ASCII

* Shared Secret

* Confirm Shared Secret

* Retransmit Timeout: 5 (secs)

* Retries: 1

Authentication Type: PAP

Local Interface IP: 10.106.68.130

Save Cancel

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

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

Étape 5. Entrez à nouveau le secret partagé dans la zone de texte **Confirmer le secret partagé**.

Étape 6. Laissez les autres champs sur leur paramètre par défaut.

Étape 7. Cliquez sur Submit.

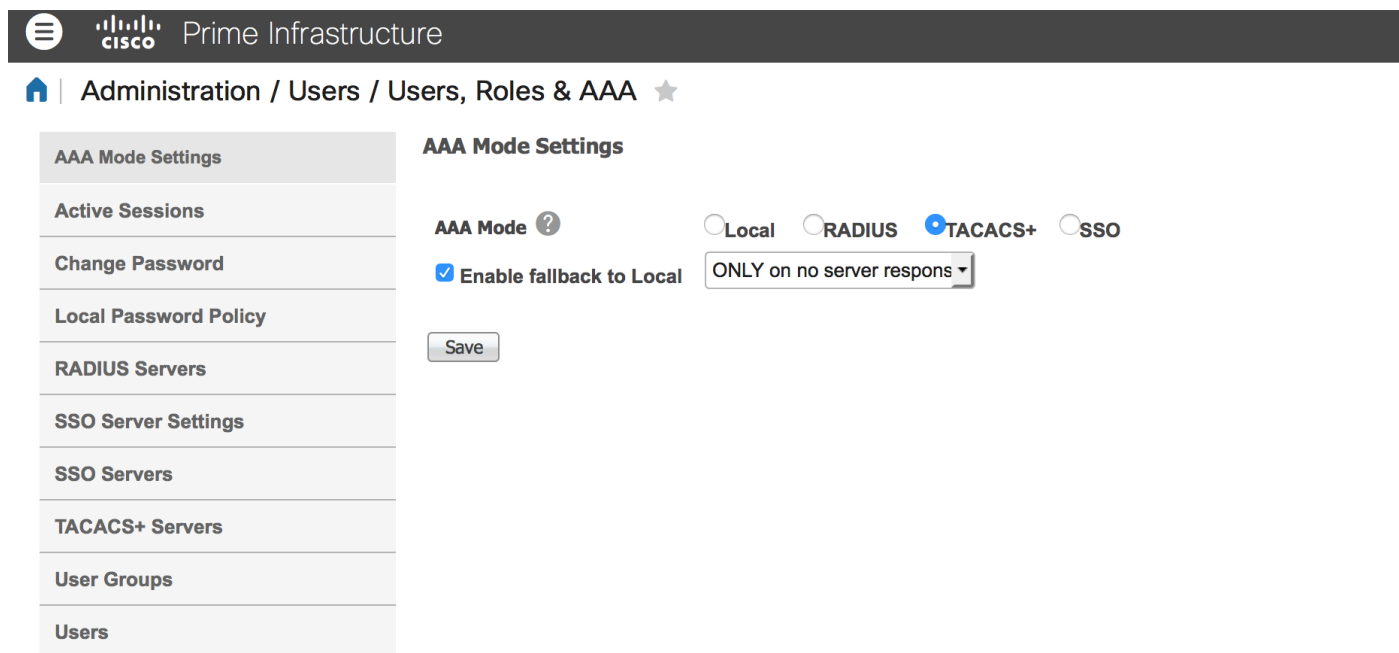
Paramètres du mode AAA dans PI

Pour choisir un mode AAA (Authentication, Authorization, and Accounting), procédez comme suit :

Étape 1. Accédez à **Administration > AAA**.

Étape 2. Choisissez **AAA Mode** dans le menu latéral gauche, vous pouvez voir la page comme

indiqué dans l'image :

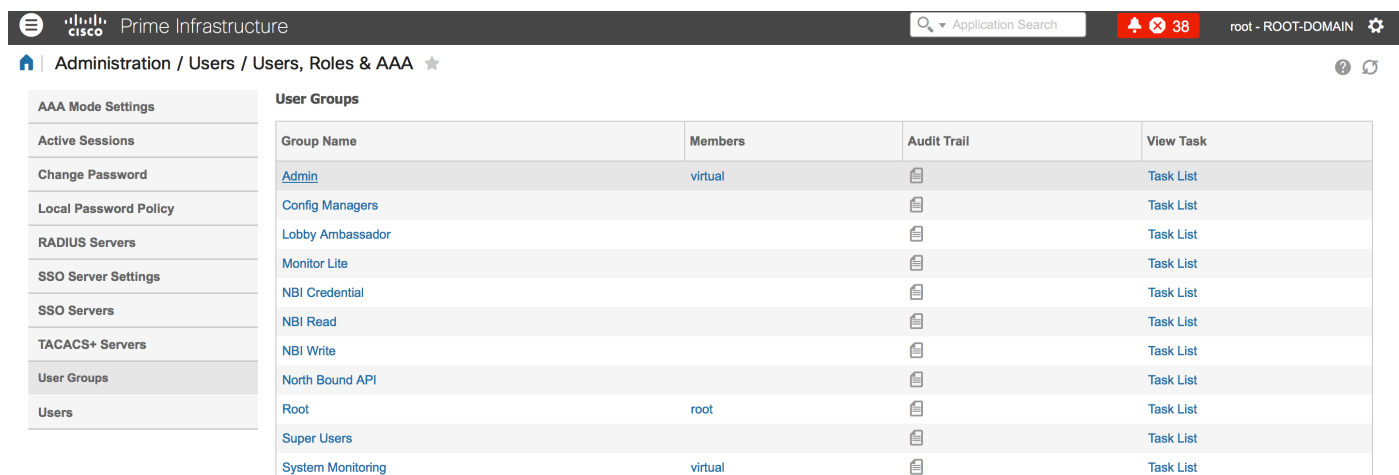


Étape 3. Sélectionnez **TACACS+**.

Étape 4. Cochez la case **Enable Fallback to Local**, si vous voulez que l'administrateur utilise la base de données locale lorsque le serveur ACS n'est pas accessible. Ce paramètre est recommandé.

Récupérer les attributs de rôle d'utilisateur à partir de PI

Étape 1. Accédez à **Administration > AAA > Groupes d'utilisateurs**. Cet exemple montre l'authentification de l'administrateur. Recherchez le **nom du groupe d'administrateurs** dans la liste et cliquez sur l'option **Liste des tâches** sur la droite, comme illustré dans l'image :



Lorsque vous cliquez sur l'option **Liste des tâches**, la fenêtre s'affiche, comme illustré dans 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 enregistrez-les dans un fichier bloc-notes.

Étape 3. Vous devrez peut-être ajouter des attributs de domaine virtuel personnalisés dans le serveur ACS. Les attributs de domaine virtuel personnalisés sont disponibles en bas 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 l'option **cliquez ici** pour obtenir la page d'attribut de domaine virtuel, et vous pouvez voir la page, comme illustré dans l'image :

TACACS+ Custom Attributes

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

RADIUS Custom Attributes

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

Configurer ACS 4.2

Étape 1. Connectez-vous à l'interface utilisateur graphique d'ACS Admin, puis accédez à Configuration d'interface > TACACS+ page.

Étape 2. Créer un nouveau service pour Prime. Cet exemple montre un nom de service configuré avec le nom **NCS**, comme illustré dans 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 bloc-notes créé à l'étape 2 à la configuration utilisateur ou groupe. Assurez-vous d'ajouter des attributs de domaine virtuel.

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. Cliquez sur OK.

Vérification

Connectez-vous au premier avec le nouveau nom d'utilisateur que vous avez créé et confirmez que vous avez le rôle **Admin**.

Dépannage

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

Consultez le fichier `usermgmt.log` de l'interface CLI racine principale disponible dans le répertoire `/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 montre un exemple de message d'erreur, qui peut être dû à différentes raisons, comme la connexion refusée par un pare-feu, ou tout périphérique intermédiaire, etc.