

Ejemplo de Configuración de Prime Infrastructure Integration con ACS 4.2 TACACS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuraciones](#)

[Agregar ACS como servidor TACACS en PI](#)

[Configuración del modo AAA en PI](#)

[Recuperar atributos de rol de usuario de PI](#)

[Configuración de ACS 4.2](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el ejemplo de configuración para Terminal Access Controller Access-Control System (TACACS+)

autenticación y autorización en la aplicación Cisco Prime Infrastructure (PI).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Definir PI como cliente en Access Control Server (ACS)
- Defina la dirección IP y una clave secreta compartida idéntica en ACS e PI

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ACS versión 4.2
- Prime Infrastructure versión 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.

Configurar

Configuraciones

Agregar ACS como servidor TACACS en PI

Complete estos pasos para agregar ACS como servidor TACACS:

Paso 1. Vaya a **Administración > Usuarios > Usuarios, funciones y AAA en PI**

Paso 2. En el menú de la barra lateral izquierda, seleccione **TACACS+ Servers**, en **Add TACACS+ servers** haga clic en **Go** y la página aparece como se muestra en la imagen:

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

- * IP Address: [Empty text box]
- * DNS Name: [Empty text box]
- * Port: [49]
- Shared Secret Format: [ASCII]
- * Shared Secret: [Empty text box with help icon]
- * Confirm Shared Secret: [Empty text box]
- * Retransmit Timeout: [5] (secs)
- * Retries: [1]
- Authentication Type: [PAP]
- Local Interface IP: [10.106.68.130]

At the bottom of the form are two buttons: 'Save' and 'Cancel'.

Paso 3. Agregue la dirección IP del servidor ACS.

Paso 4. Introduzca el secreto compartido TACACS+ configurado en el servidor ACS.

Paso 5. Vuelva a introducir el secreto compartido en el cuadro de **texto Confirmar secreto compartido**.

Paso 6. Deje el resto de los campos en su configuración predeterminada.

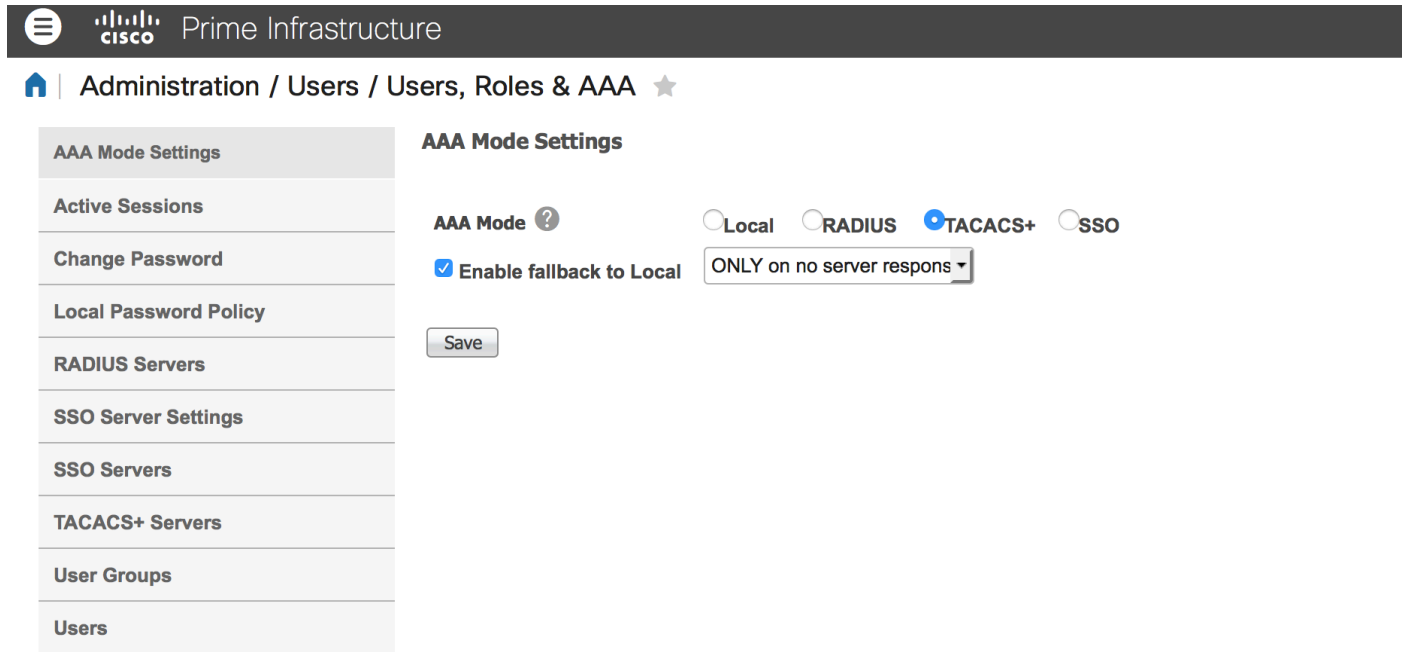
Paso 7. Haga clic en Submit (Enviar).

Configuración del modo AAA en PI

Para elegir un modo de autenticación, autorización y contabilidad (AAA), realice estos pasos:

Paso 1. Vaya a **Administration > AAA**.

Paso 2. Elija **AAA Mode** en el menú de la barra lateral izquierda, puede ver la página como se muestra en la imagen:

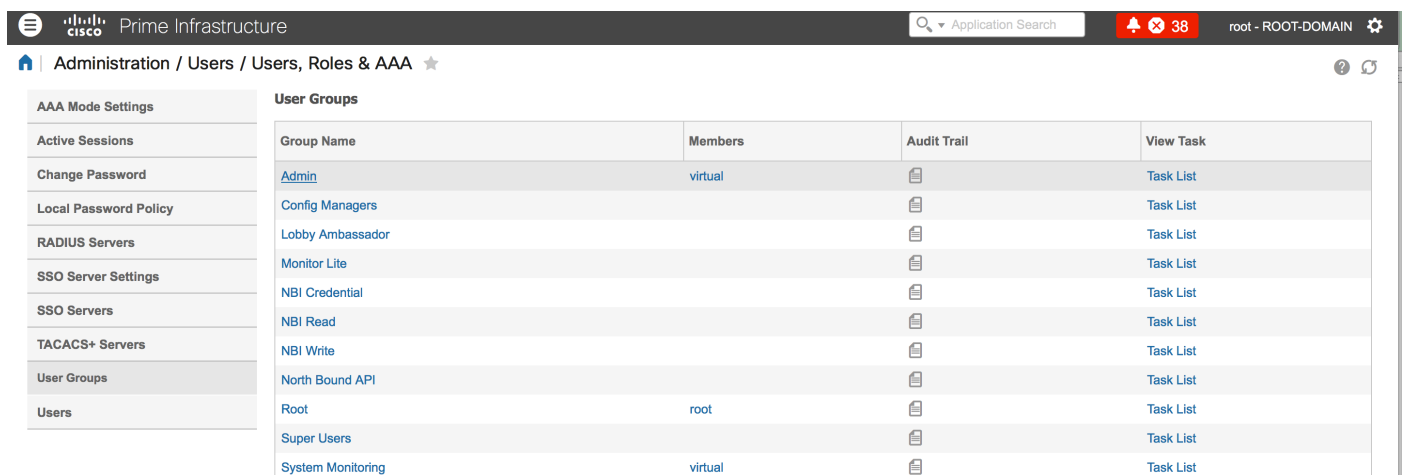


Paso 3. Seleccione **TACACS+**.

Paso 4. Marque la casilla **Enable Fallback to Local**, si desea que el administrador utilice la base de datos local cuando el servidor ACS no sea accesible. Esta es una configuración recomendada.

Recuperar atributos de rol de usuario de PI

Paso 1. Vaya a **Administration > AAA > User Groups**. Este ejemplo muestra la autenticación del administrador. Busque el nombre del grupo de administradores en la lista y haga clic en la opción **Lista de tareas** de la derecha, como se muestra en la imagen:



Una vez que haga clic en la opción **Lista de tareas**, aparecerá la ventana, como se muestra en la imagen:

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
```

Paso 2. Copie estos atributos y guárdelos en un archivo de bloc de notas.

Paso 3. Es posible que deba agregar atributos de dominio virtual personalizados en el servidor ACS. Los atributos de dominio virtual personalizados están disponibles en la parte inferior de la misma página de lista de tareas.

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

Paso 4. Haga clic en la opción **Click here** para obtener la página del atributo del dominio virtual, y puede ver la página, como se muestra en la imagen:

TACACS+ Custom Attributes

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

RADIUS Custom Attributes

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

Configuración de ACS 4.2

Paso 1. Inicie sesión en la GUI de ACS Admin y navegue hasta la configuración de la interfaz > la página TACACS+.

Paso 2. Cree un nuevo servicio para prime. Este ejemplo muestra un nombre de servicio configurado con el nombre NCS, como se muestra en la imagen:

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"/>		

Paso 3. Agregue todos los atributos del bloc de notas creado en el paso 2 a la configuración de usuario o grupo. Asegúrese de agregar atributos de dominio virtual.

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
```

Paso 4. Click OK.

Verificación

Inicie sesión en prime con el nuevo nombre de usuario que creó y confirme que tiene la función Admin.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Revise usermgmt.log desde la CLI de la raíz principal disponible en el directorio /opt/CSColumos/logs. Verifique si hay algún mensaje de error.

```
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]
```

Este ejemplo muestra un ejemplo de mensaje de error, que podría deberse a varias razones, como la conexión rechazada por un firewall, o cualquier dispositivo intermedio, etc.