Integración primera de la infraestructura con el ejemplo de la Configuración de TACACS ACS 4.2

Contenido

Introducción

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

autenticación y autorización en la aplicación de la infraestructura de la prima de Cisco (PI).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

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

- ACS versión 4.2
- 3.0 primero de la versión de la infraestructura

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

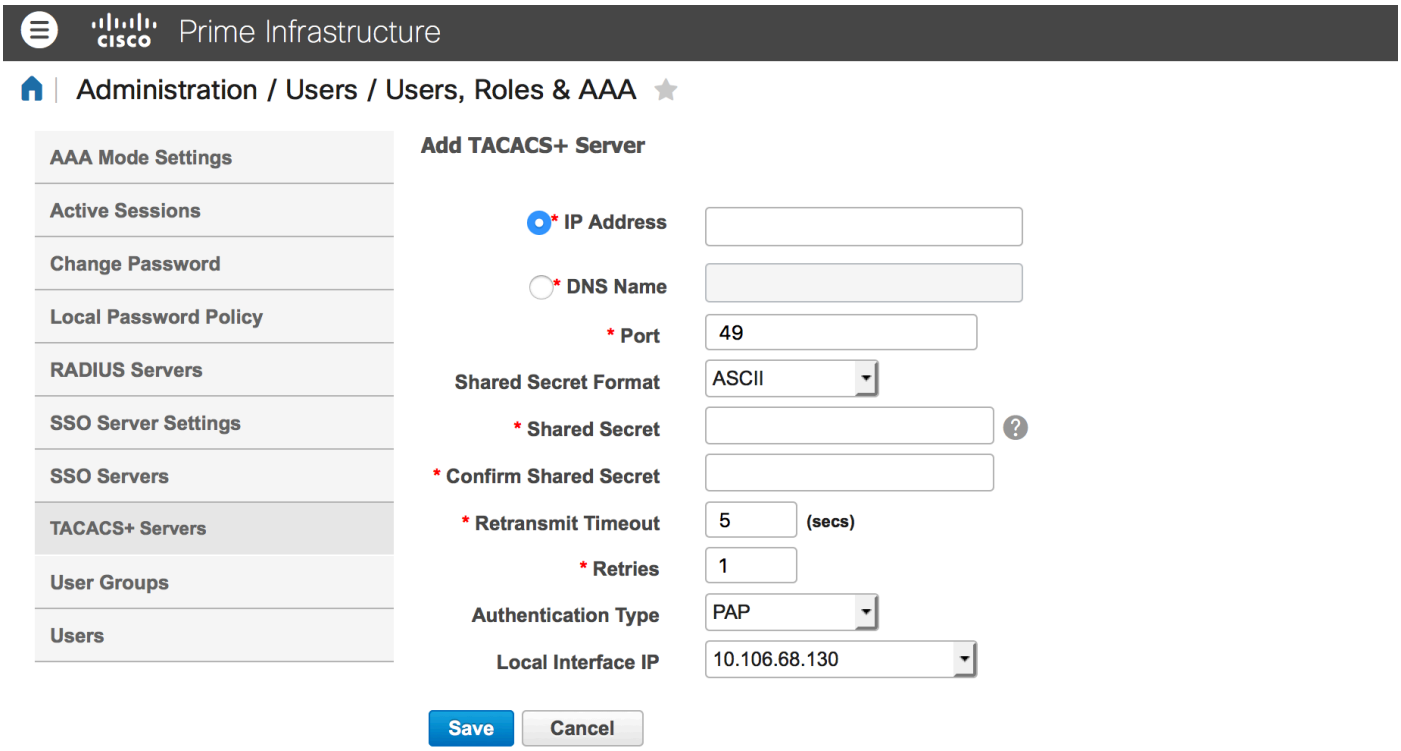
Configuraciones

Agregue el ACS como servidor TACACS en el PI

Complete estos pasos para agregar el ACS como servidor TACACS:

Paso 1. Navegue a la **administración > Users > Users, a los papeles y al AAA en el PI**

Paso 2. Del menú izquierdo de la barra lateral, los **servidores** selectos **TACACS+**, debajo **agregan los servidores TACACS+ que va el** tecleo y la página aparece tal y como se muestra en de la imagen:



Paso 3. Agregue la dirección IP del servidor ACS.

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

Paso 5. Entre el secreto compartido de nuevo en el cuadro de texto del **secreto compartido del confirmar**.

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

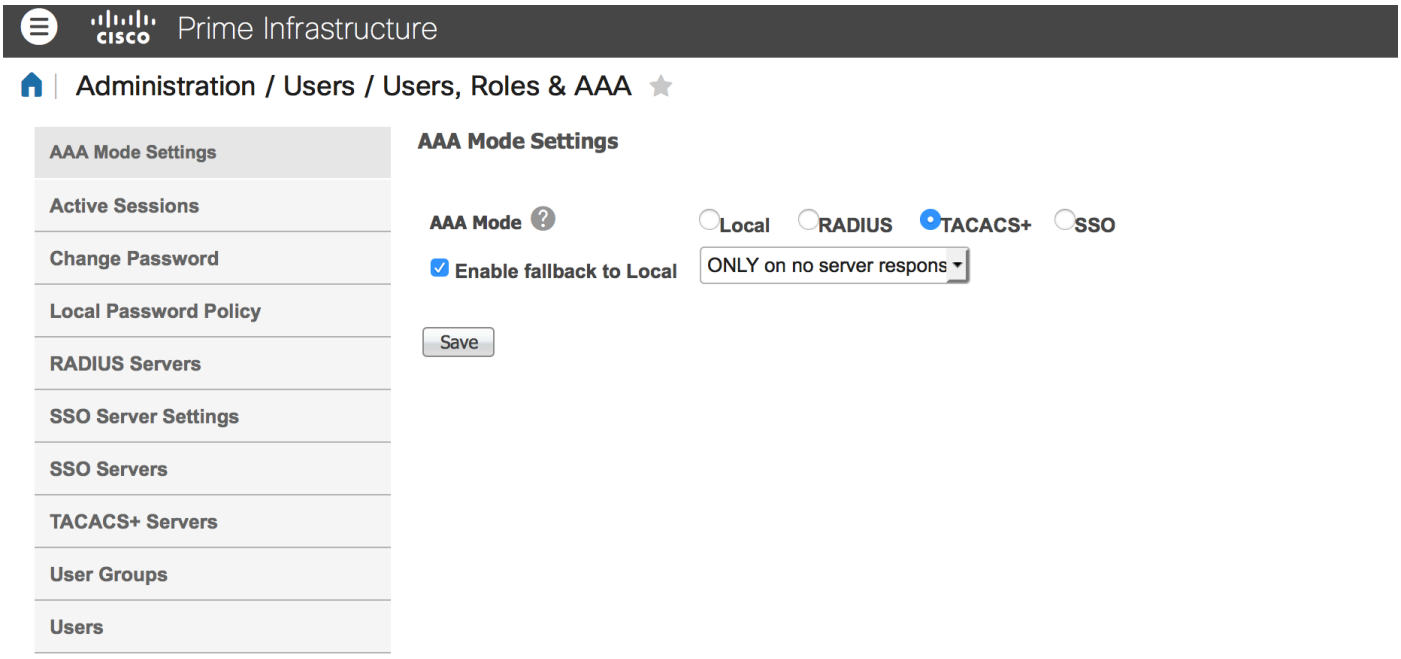
Paso 7. El tecleo **somete**.

Configuraciones de modo AAA en el PI

Para elegir un modo del Authentication, Authorization, and Accounting (AAA), complete estos pasos:

Paso 1. Navegue a la **administración >AAA**.

Paso 2. Elija el **modo AAA del** menú izquierdo de la barra lateral, usted puede ver la página tal y como se muestra en de la imagen:

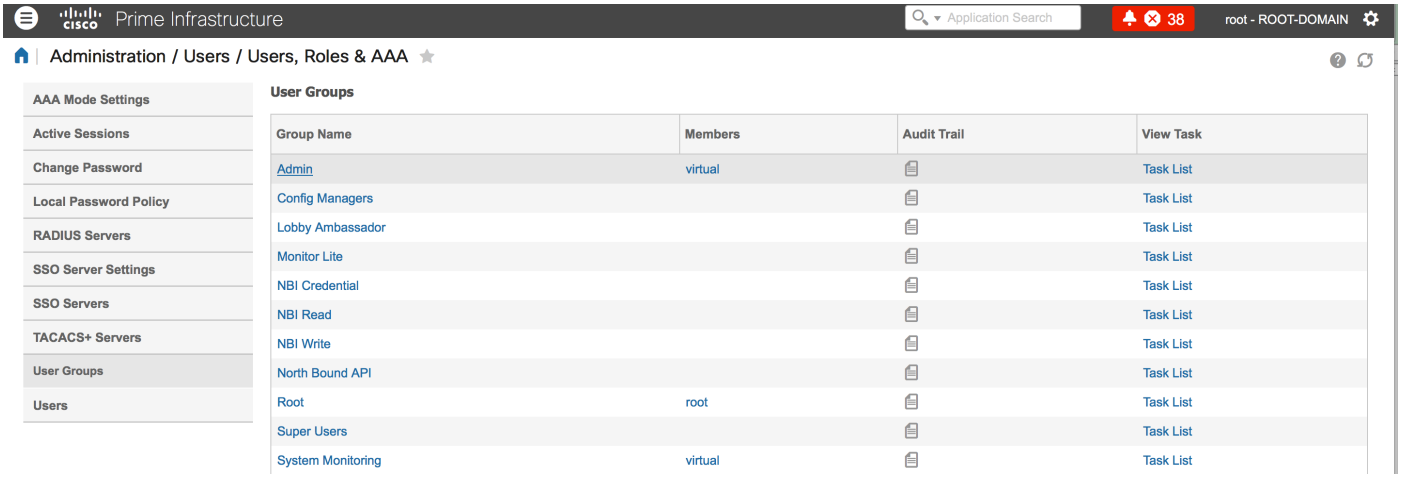


Paso 3. Seleccione el **TACACS+**.

Paso 4. Marque el **retraso del permiso al** cuadro **local**, si usted quisiera que el administrador utilizara la base de datos local cuando el servidor ACS no es accesible. Esto es una configuración recomendada.

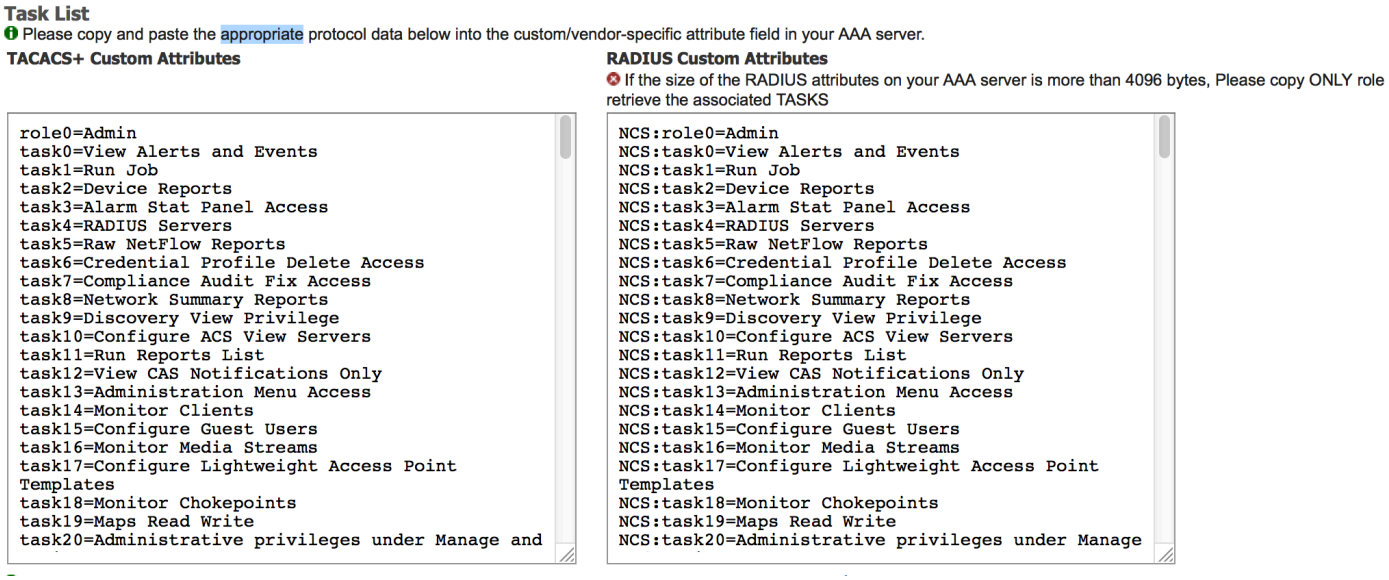
Extraiga el rol del usuario de los atributos del PI

Paso 1. Navegue a la **administración** >AAA > los **grupos de usuarios**. Este ejemplo muestra la autenticación de administrador. Busque el **nombre del admin group** en la lista y haga clic la opción de la **lista de tareas** a la derecha, tal y como se muestra en de la imagen:



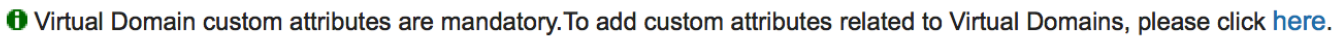
Una vez que usted hace clic la opción de la **lista de tareas**, la ventana aparece, tal y como se

muestra en de la imagen:

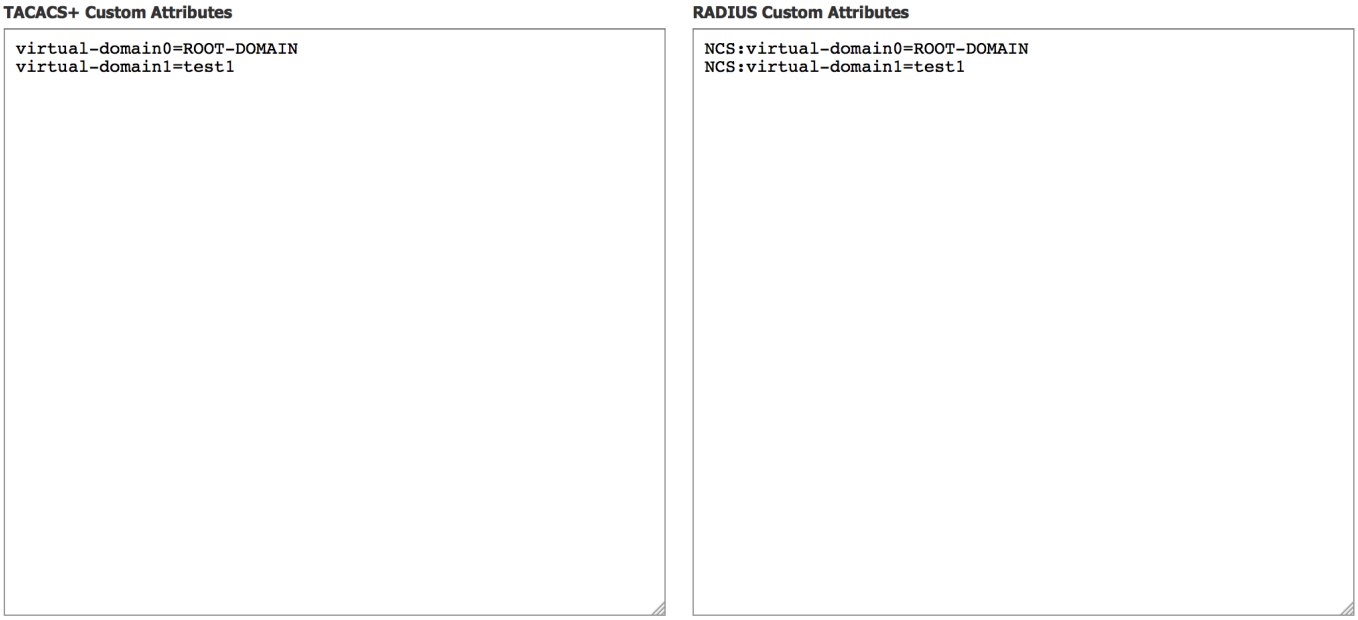


Paso 2. Copie estos atributos y sálvelos en un archivo de la libreta.

Paso 3. Usted puede necesitar agregar los atributos virtuales de encargo del dominio en el servidor ACS. Los atributos virtuales de encargo del dominio están disponibles al fondo de la misma página de la lista de tareas.



Paso 4. Haga clic en **hacen clic aquí la** opción para conseguir la página del atributo del dominio virtual, y usted puede ver la página, tal y como se muestra en de la imagen:

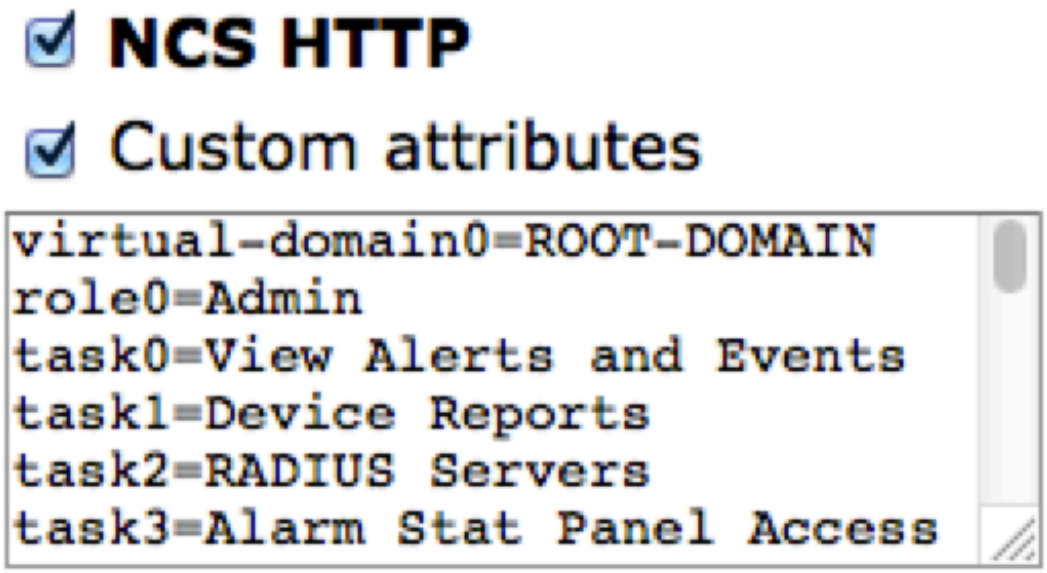


Configuración ACS 4.2

Paso 1. Inicie sesión al **ACS Admin GUI**, y navegue **Interface Configuration > Tacacs+** para paginar.

Paso 2. Cree el nuevo servicio para la prima. Este ejemplo muestra un nombre del servicio configurado con el nombre **NC**, tal y como se muestra en de la imagen:

Paso 3. Agregue todos los atributos de la libreta creada en el paso 2 al usuario o a la configuración de grupo. Asegure para agregar los atributos del virtual-dominio.



Paso 4. **Autorización del** tecleo.

Verificación

Inicie sesión a la prima con el nombre de usuario nuevo que usted creó y confirme que usted tiene el papel **Admin**.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Revise usermgmt.log de la raíz primera CLI disponible en el directorio de **/opt/CSCOlumos/logs**. Marque si hay algunos mensajes 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 una muestra de mensaje de error, que podría ser debido a las diversas razones como la conexión rechazada por un Firewall, o de cualquier dispositivo intermedio etc.