

Integração principal da infraestrutura com exemplo da configuração de TACACS ACS 4.2

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurações](#)

[Adicionar o ACS como o servidor de TACACS no PI](#)

[Configurações de modo AAA no PI](#)

[Recupere o papel de usuário dos atributos do PI](#)

[Configurar ACS 4.2](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve o exemplo de configuração para o Terminal Access Controller Access Control System (o TACACS+)

authentication e autorização no aplicativo da infraestrutura da prima de Cisco (PI).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defina o PI como um cliente no Access Control Server (o ACS)
- Defina o endereço IP de Um ou Mais Servidores Cisco ICM NT e uma chave de segredo compartilhado idêntica no ACS e no PI

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de ACS 4.2
- 3.0 principal da liberação da infraestrutura

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Configurações

Adicionar o ACS como o servidor de TACACS no PI

Termine estas etapas a fim adicionar o ACS como um servidor de TACACS:

Etapa 1. Navegue à **administração > aos usuários > aos usuários, aos papéis & ao AAA no PI**

Etapa 2. Do menu esquerdo do sidebar, os **server** seletos **TACACS+**, **adicionam** abaixo **server** **que TACACS+** o clique **vai** e a página publica-se segundo as indicações da imagem:

The screenshot shows the Cisco Prime Infrastructure interface. The top navigation bar includes the Cisco logo and 'Prime Infrastructure'. Below it, the breadcrumb path is 'Administration / Users / Users, Roles & AAA'. A sidebar on the left lists various configuration options, with 'TACACS+ Servers' selected. The main content area is titled 'Add TACACS+ Server' and contains the following fields:

- * 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

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

Etapa 3. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor ACS.

Etapa 4. Incorpore o segredo compartilhado TACACS+ configurado ao servidor ACS.

Etapa 5. Reenter o segredo compartilhado na caixa de texto **secreta compartilhada confirmação**.

Etapa 6. Saa do resto dos campos em sua configuração padrão.

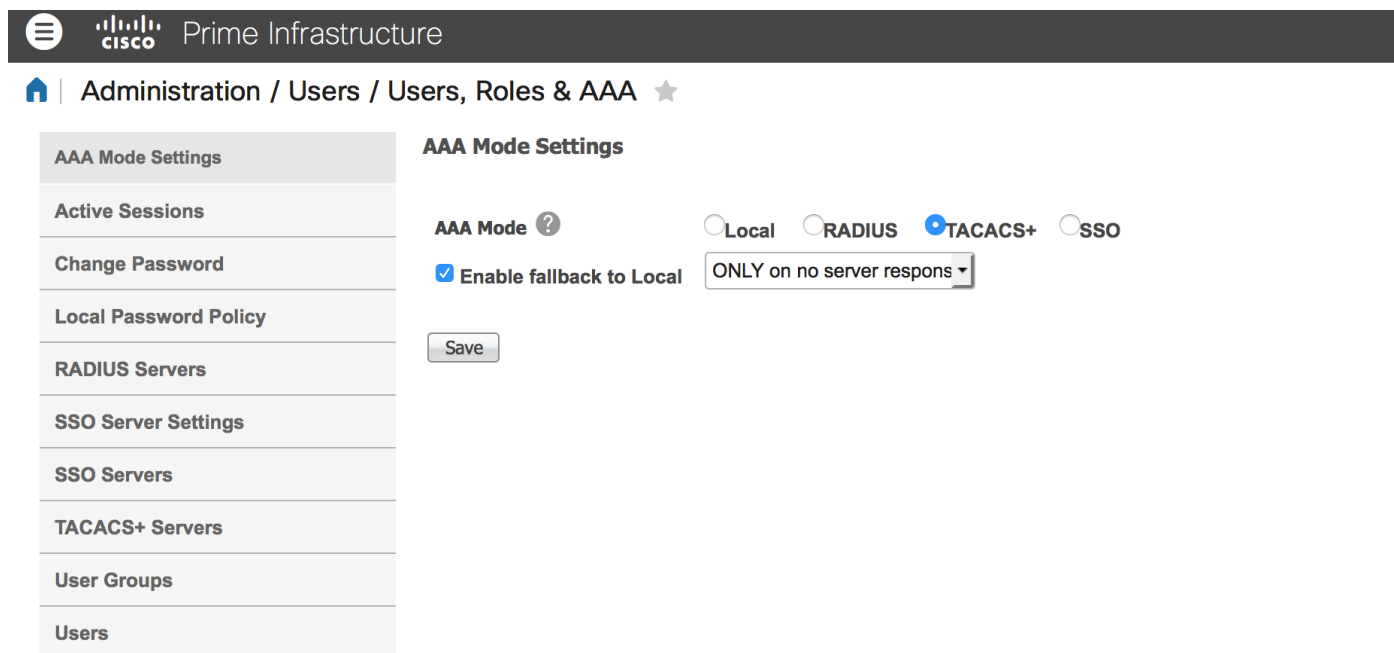
Etapa 7. O clique **submete-se**.

Configurações de modo AAA no PI

A fim escolher um modo do Authentication, Authorization, and Accounting (AAA), termine estas etapas:

Etapa 1. Navegue à **administração > ao AAA**.

Etapa 2. Escolha o **modo AAA** do menu esquerdo do sidebar, você pode ver a página segundo as indicações da imagem:

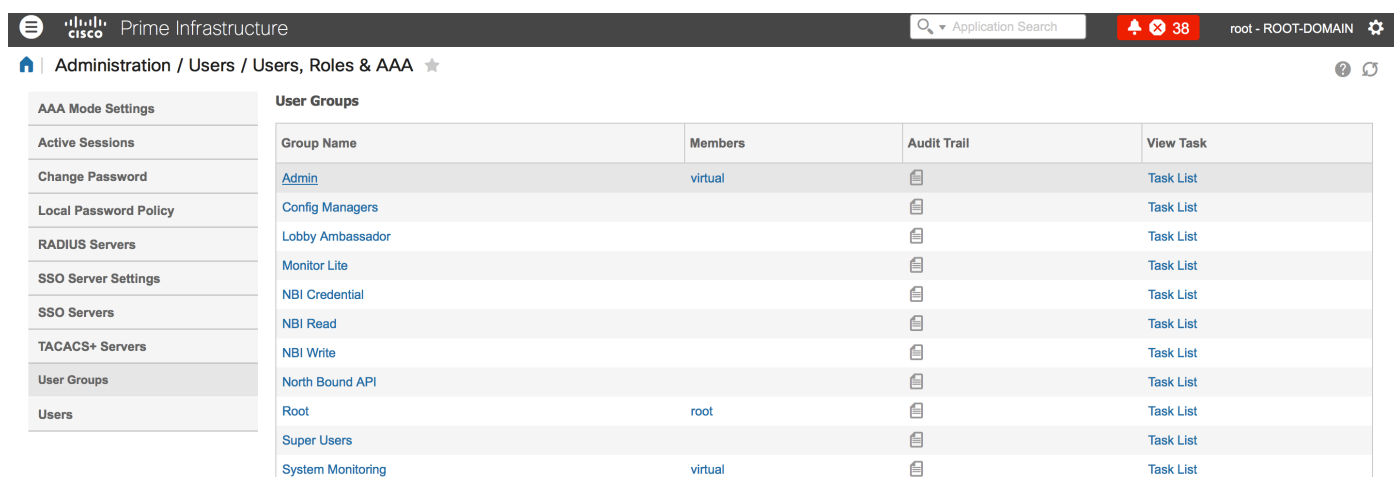


Etapa 3. Selecione o **TACACS+**.

Etapa 4. Verifique a **reserva da possibilidade à caixa local**, se você quer o administrador usar o base de dados local quando o servidor ACS não é alcançável. Esta é uma configuração recomendada.

Recupere o papel de usuário dos atributos do PI

Etapa 1. Navegue à **administração** > ao **AAA** > aos **grupos de usuário**. Este exemplo mostra a Autenticação do Administrador. Procure o **nome do admin group** na lista e clique a opção da **lista de tarefas** à direita, segundo as indicações da imagem:



Uma vez que você clica a opção da **lista de tarefas**, o indicador aparece, segundo as indicações da imagem:

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
```

Etapa 2. Copie estes atributos e salvar os em um arquivo do bloco de notas.

Etapa 3. Você pode precisar de adicionar atributos virtuais feitos sob encomenda do domínio no servidor ACS. Os atributos virtuais feitos sob encomenda do domínio estão disponíveis no fundo da mesma página da lista de tarefas.

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

Etapa 4. Clique **clícam** sobre **aquí a** opção para obter a página do atributo do Domínio Virtual, e você pode ver a página, segundo as indicações da imagem:

TACACS+ Custom Attributes

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

RADIUS Custom Attributes

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

Configurar ACS 4.2

Etapa 1. Entre ao ACS Admin GUI, e navegue **Interface Configuration > Tacacs+** para paginar.

Etapa 2. Crie o serviço novo para a prima. Este exemplo mostra um nome do serviço configurado com nome **NC**, segundo as indicações da imagem:

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"/>		

Etapa 3. Adicionar todos os atributos do bloco de notas criado em etapa 2 ao usuário ou à configuração de grupo. Assegure para adicionar atributos do virtual-domínio.

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
```

Etapa 4. Aprovação do clique.

Verificar

Entre à prima com o nome que de novo usuário você criou e confirme que você tem o papel Admin.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Reveja usermgmt.log da raiz principal CLI disponível no diretório de `/opt/CSCOlumos/logs`. Verifique se há algum Mensagem de Erro.

```
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 exemplo mostra uma amostra de Mensagem de Erro, que poderia ser devido às várias razões como a conexão recusada por um Firewall, ou de todo o dispositivo intermediário etc.