

Prime基础设施与ACS 4.2 TACACS集成配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[配置](#)

[在PI中将ACS添加为TACACS服务器](#)

[PI中的AAA模式设置](#)

[从PI检索用户角色属性](#)

[配置ACS 4.2](#)

[验证](#)

[故障排除](#)

简介

本文档介绍终端访问控制器访问控制系统(TACACS+)的配置示例

对Cisco Prime基础设施(PI)应用的身份验证和授权。

先决条件

要求

Cisco 建议您了解以下主题：

- 在访问控制服务器(ACS)中将PI定义为客户端
- 在ACS和PI上定义IP地址和相同的共享密钥

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ACS版本4.2
- Prime基础设施版本3.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

配置

在PI中将ACS添加为TACACS服务器

要将ACS添加为TACACS服务器，请完成以下步骤：

步骤1. 导航至 **管理 > 用户 > 用户、角色和AAA** 在PI中

步骤2. 从左侧栏菜单中，选择**TACACS+ Servers**，在**Add TACACS+ servers** 下单击**Go**，然后显示页面，如图所示：

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

步骤3. 添加ACS服务器的IP地址。

步骤4. 输入在ACS服务器中配置的TACACS+共享密钥。

步骤5. 在“确认共享密钥”文本框中**重新输入**共享密钥。

步骤6. 将其余字段保留为默认设置。

步骤7. 单击“提交”。

PI中的AAA模式设置

要选择身份验证、授权和记帐(AAA)模式，请完成以下步骤：

步骤1. 导航至**Administration > AAA**。

步骤2. 从左侧**栏菜单**中选择AAA模式，您可以看到该页面，如图所示：

- AAA Mode Settings
- Active Sessions
- Change Password
- Local Password Policy
- RADIUS Servers
- SSO Server Settings
- SSO Servers
- TACACS+ Servers
- User Groups
- Users

AAA Mode Settings

AAA Mode ? Local RADIUS TACACS+ SSO

Enable fallback to Local ONLY on no server respons

步骤3.选择TACACS+。

步骤4.如果希望管理员在ACS服务器无法访问时使用本地数据库，请选中启用回退到本地方框。这是建议的设置。

从PI检索用户角色属性

步骤1.导航至Administration > AAA > User Groups。此示例显示管理员身份验证。在列表中查找Admin Group Name，然后单击右侧的Task List选项，如图所示：

Group Name	Members	Audit Trail	View Task
Admin	virtual		Task List
Config Managers			Task List
Lobby Ambassador			Task List
Monitor Lite			Task List
NBI Credential			Task List
NBI Read			Task List
NBI Write			Task List
North Bound API			Task List
Root	root		Task List
Super Users			Task List
System Monitoring	virtual		Task List

单击“任务列表”选项后，将出现窗口，如图所示：

Task List

① 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

② 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
```

步骤2.复制这些属性并将其保存在记事本文件中。

步骤3.您可能需要在ACS服务器中添加自定义虚拟域属性。自定义虚拟域属性位于同一任务列表页面的底部。

① Virtual Domain custom attributes are mandatory.To add custom attributes related to Virtual Domains, please click [here](#).

步骤4.单击[此处](#)选项可获取“虚拟域”属性页，您可以看到该页，如图所示：

TACACS+ Custom Attributes

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

RADIUS Custom Attributes

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

配置ACS 4.2

步骤1.登录ACS Admin GUI，然后导航至Interface Configuration > TACACS+页面。

步骤2.为prime创建新服务。此示例显示了使用名称NCS配置的服务名称，如图所示：

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"/>		

步骤3.将步骤2中创建的记事本中的所有属性添加到用户或组配置。确保添加虚拟域属性。

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
```

步骤4.单击“确定”。

验证

使用您创建的新用户名登录到Prime，并确认您具有管理角色。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

从/opt/CSCOlumos/logs目录中提供的prime root CLI查看usermgmt.log。检查是否存在任何错误消息。

```
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]
```

此示例显示错误消息的示例，可能是由于各种原因（如防火墙或任何中间设备拒绝连接等）。