

与ACS 4.2 TACACS配置示例的头等基础设施集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[配置](#)

[添加ACS作为在PI的TACACS服务器](#)

[在PI的AAA模式设置](#)

[从PI的检索用户角色属性](#)

[配置ACS 4.2](#)

[验证](#)

[故障排除](#)

简介

本文描述终端访问控制器访问控制系统的(TACACS+)配置示例

在思科最初基础设施(PI)应用程序的认证和授权。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

- 定义PI作为访问控制服务器的(ACS)一个客户端
- 定义IP地址和相同的共享密钥在ACS和PI

[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
- 头等基础设施版本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

添加ACS作为在PI的TACACS服务器

完成这些步骤为了添加ACS作为TACACS服务器：

步骤1.导航对**管理> Users > Users、角色& AAA在PI**

第二步：从左侧侧边栏菜单，挑选**TACACS+服务器**，下**添加TACACS+服务器**单击去如镜像所显示，并且页出版：

The screenshot shows the Cisco Prime Infrastructure web interface. The breadcrumb navigation is Administration / Users / Users, Roles & AAA. 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, User Groups, and Users. The main content area is titled 'Add TACACS+ Server' and contains the following configuration fields:

- * IP Address (text input)
- * DNS Name (text input)
- * Port: 49 (text input)
- Shared Secret Format: ASCII (dropdown menu)
- * Shared Secret: (password input field with a help icon)
- * Confirm Shared Secret: (password input field)
- * Retransmit Timeout: 5 (secs) (text input)
- * Retries: 1 (text input)
- Authentication Type: PAP (dropdown menu)
- Local Interface IP: 10.106.68.130 (dropdown menu)

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

步骤3.添加ACS服务器的IP地址。

步骤4.输入在ACS服务器配置的TACACS+共享的机密。

步骤5.重新输入共享机密在**确认共享的秘密**文本框。

步骤6.留下字段的其余他们的默认设置的。

步骤7.单击**提交**。

在PI的AAA模式设置

为了选择验证、授权和统计(AAA)模式，请完成这些步骤：

步骤1.导航对**管理>AAA**。

步骤2.如镜像所显示，从左侧侧边栏菜单选择**AAA模式**，您能看到页：

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 ▼

步骤3.挑选TACACS+。

第四步：检查Enable (event) Fallback到本地方框，如果希望管理员使用本地数据库，当ACS服务器不可及的时。这是推荐的设置。

从PI的检索用户角色属性

步骤1.导航给管理>AAA >用户组。此示例显示管理员验证。如镜像所显示，寻找在列表的Admin group名称并且单击在右边的任务列表选项，：

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

一旦点击任务列表选项，如镜像所显示，窗口出现，：

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.复制这些属性并且保存它在记事本文件。

第三步：您在ACS服务器可能需要添加自定义虚拟域属性。自定义虚拟域属性在同样任务列表页底部是可用的。

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

步骤4.单击[点击此处](#)选项获得虚拟域属性页，如镜像所显示，并且您能看到页，：

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.登陆对ACS Admin GUI，并且导航对Interface Configuration > TACACS+页。

步骤2.创建最初的新的服务。此示例显示服务名称配置与命名NCS，如镜像所显示：

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.从在步骤创建的记事本添加所有属性2到用户或组配置。保证添加虚拟域属性。

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.点击OK键。

验证

登陆对与您创建的新用户用户名的最初并且确认您有Admin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。

查看从头等根CLI联机的usermgmt.log在/opt/CSColumos/logs目录。检查是否有任何错误消息。

```
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]
```

此示例显示错误消息，可能归结于多种原因类似防火墙拒绝的连接，或者所有中间设备等示例。