与ACS 4.2 TACACS配置示例的头等基础设施集成

目录

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

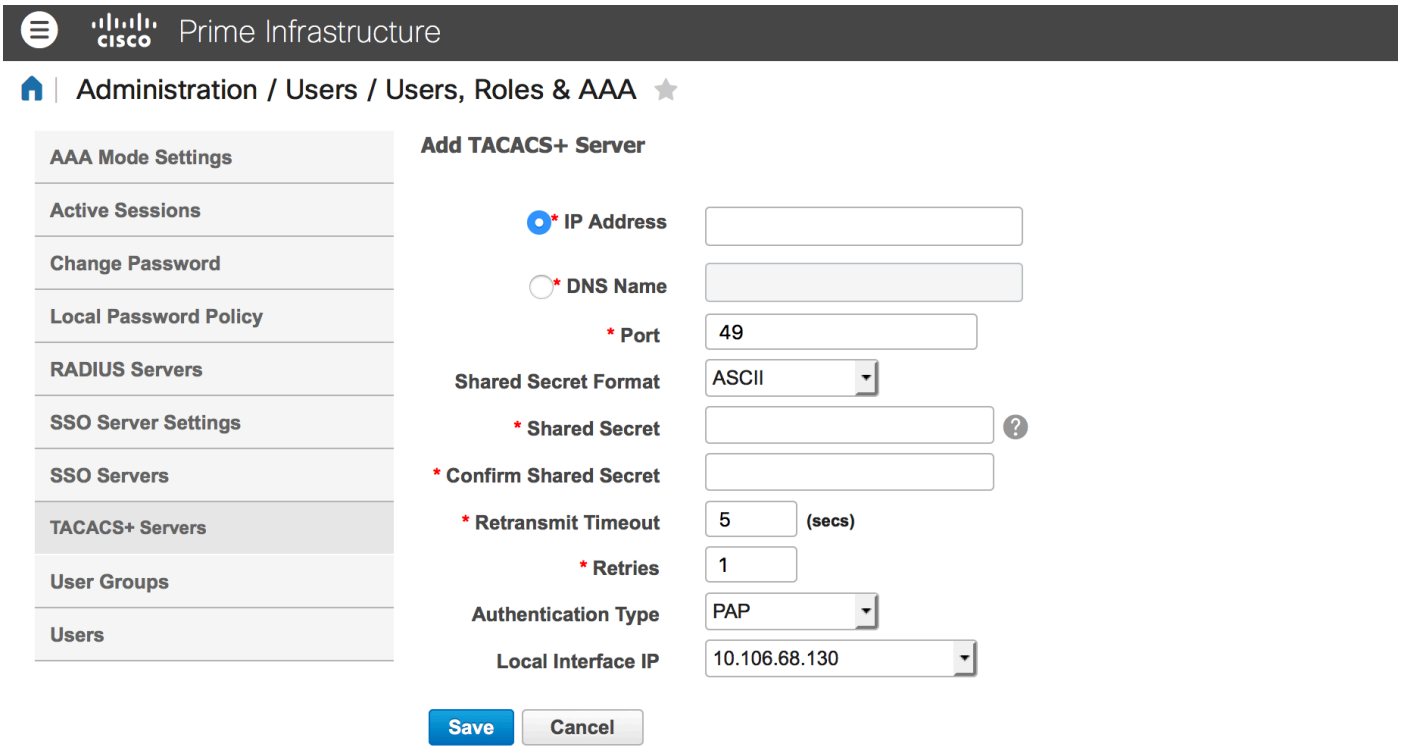
配置

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：



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。

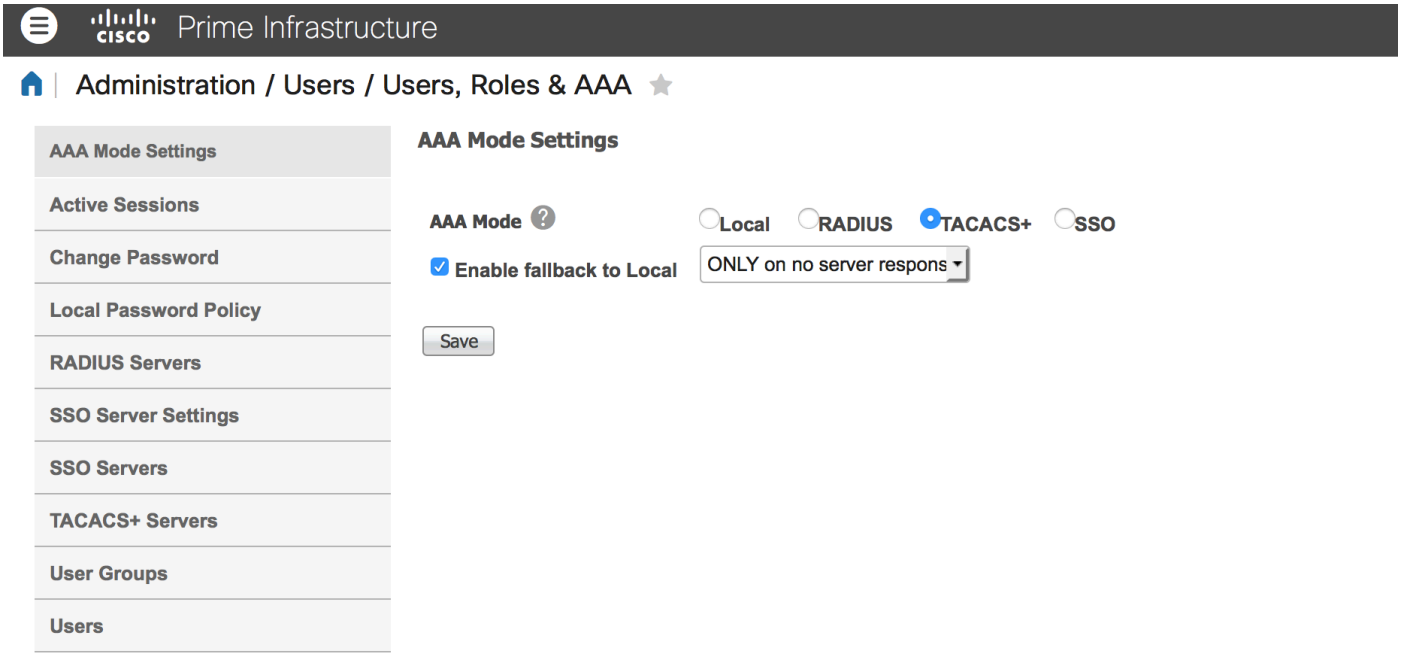
步骤7.单击**提交**。

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：

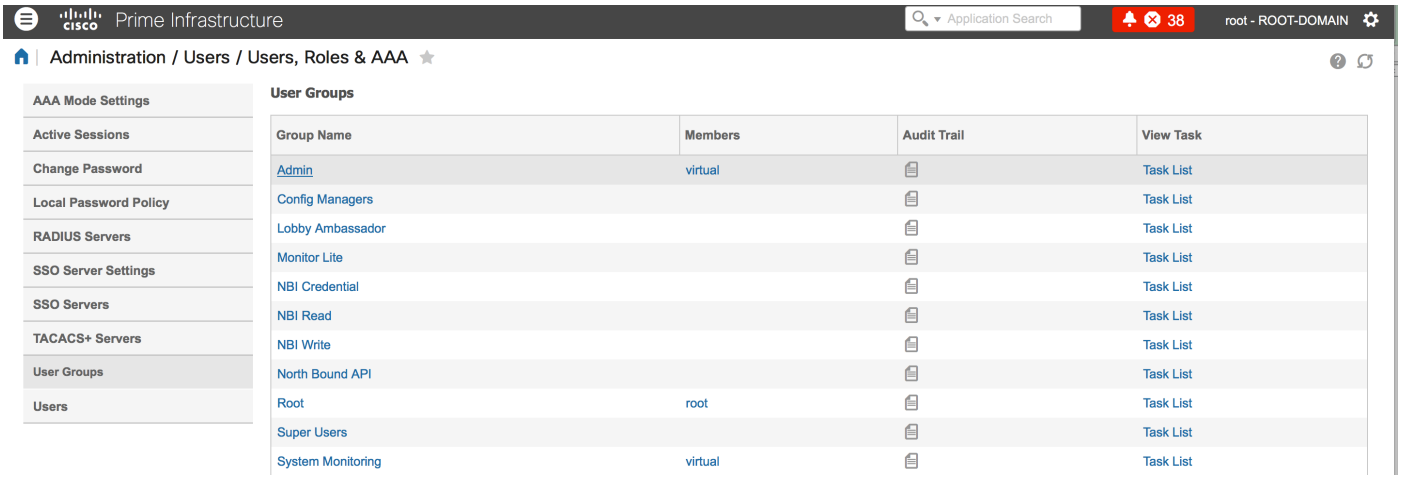


步骤3.挑选**TACACS+**。

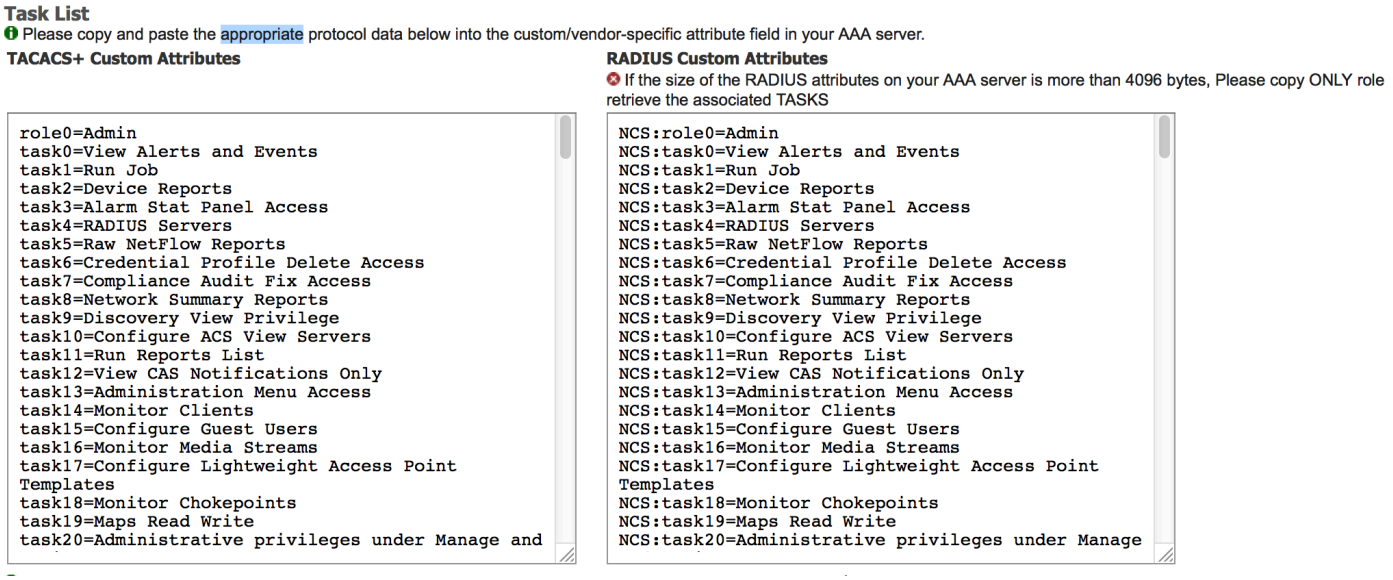
第四步：检查**Enable (event) Fallback到本地**方框，如果希望管理员使用本地数据库，当ACS服务器不可及的时。这是推荐的设置。

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，：



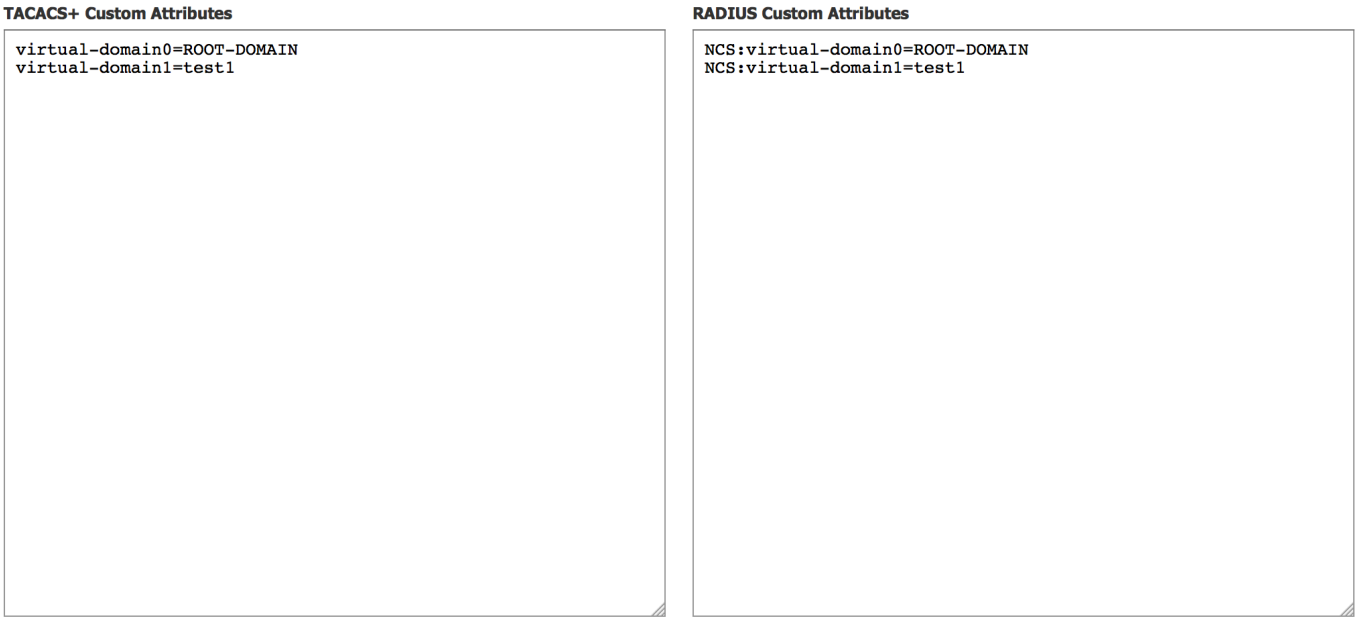
一旦点击**任务列表**选项，如镜像所显示，窗口出现，：



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。

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，：

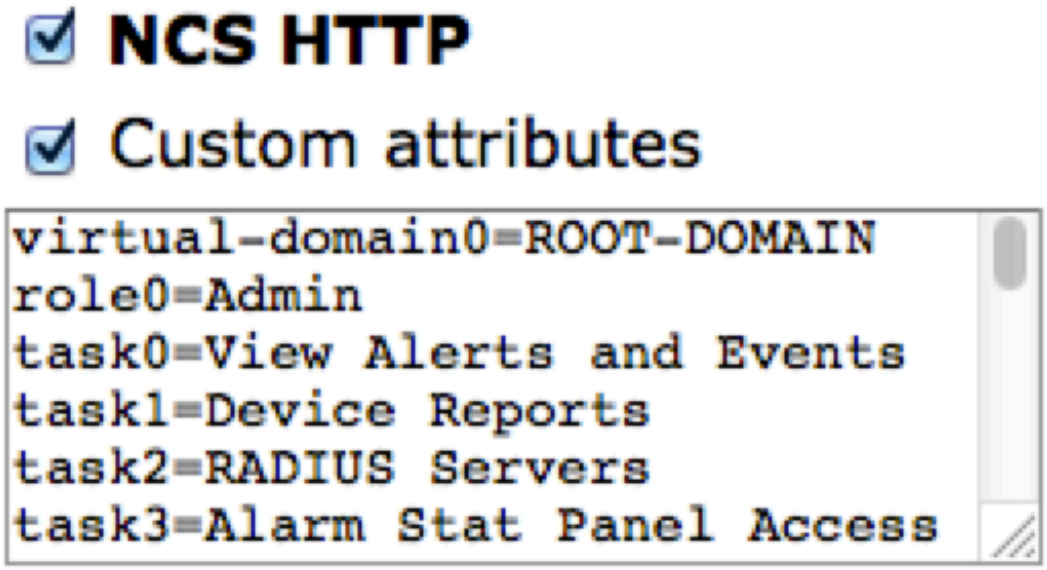


配置ACS 4.2

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：

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。



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。