

与ACS 5.x配置示例的无线控制系统和网络控制系统管理

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[步骤1.添加WCS到ACS AAA客户端。](#)

[步骤2.添加Cisco Secure ACS作为在WCS的一个TACACS+服务器。](#)

[步骤3.配置在ACS的正确shell配置文件。](#)

[步骤4.配置Cisco Secure ACS返回属性。](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述如何使用思科安全访问控制服务器(ACS) 5.x为了配置思科无线控制系统(WCS)和思科头等网络控制系统(NCS)管理。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco 无线控制系统
- 思科最初网络控制系统
- 思科安全访问控制服务器

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科无线控制系统7.0.172.0
- Cisco Secure ACS 5.x

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。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

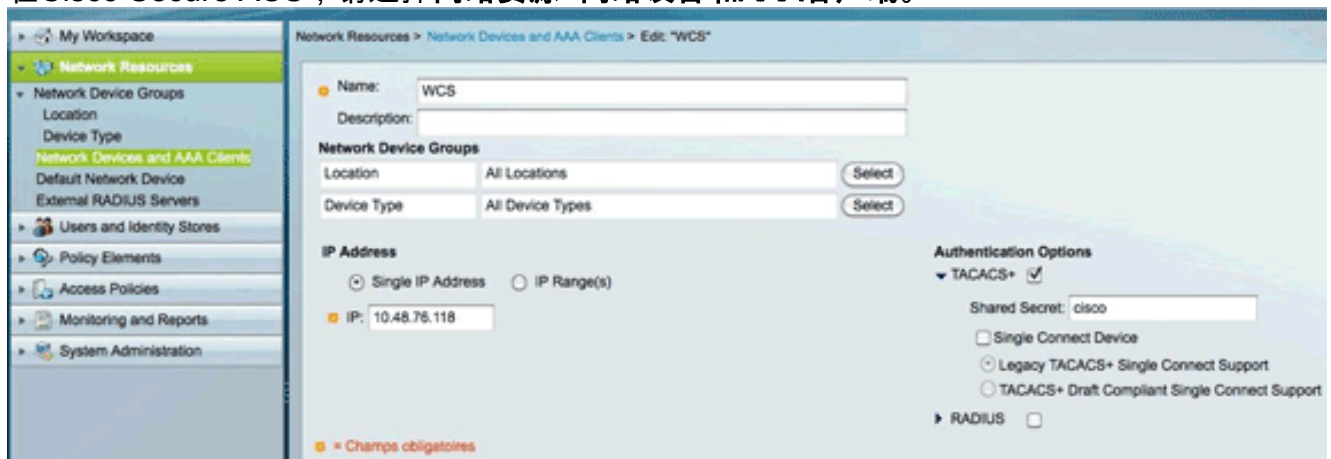
配置

此配置示例描述如何验证有TACACS+的一个用户。

注意：虽然多种选项和可能性存在，当您验证有Cisco Secure ACS的5.x WCS/NCS用户，不是所有的组合在本文描述。然而，此示例提供您必要的信息知道如何修改示例成您要达到的准确的配置。

步骤1.添加WCS到ACS AAA客户端。

1. 在Cisco Secure ACS，请选择**网络资源>网络设备和AAA客户端**。



2. 在 Name 字段中输入名称。
3. 输入在IP地址字段的WCS IP地址。
4. 在认证选项地区下，请点击**TACACS+**复选框为了启用TACACS+，然后输入作为一共享机密将使用的期限。**注意：**此示例使用cisco作为共享机密;然而，由于安全原因，您应该使用一个较不明显的用语。

步骤2.添加Cisco Secure ACS作为在WCS的TACACS+服务器。

1. 登陆对WCS，并且选择**管理>AAA**。
2. 点击**TACACS+**。

3. 输入您的在共享塞克雷的共享秘密期限并且确认共享秘密字段。
4. 从本地接口IP字段选择Cisco ACS IP地址。
5. 在左侧定位区域，请点击**AAA模式**。

6. 点击**TACACS+**单选按钮。**注意**：因安全上的原因，思科建议您在**验证失败或没有服务器响应**选择从Enable (event) fallback到本地下拉列表。选择此选项防止您锁定在问题的情况下。一切正确地一次工作的您能更改选项。

[步骤3.配置在ACS的正确shell配置文件。](#)

此步骤描述如何配置Cisco Secure ACS返回正确属性为了确定在WCS的用户权限。

1. 在左侧定位区域中，请点击**组**。用户类型列表发表。此示例验证从大厅大使用户类型的一个用户。
2. 在**LobbyAmbassador**组旁边单击**任务列表**链路。

Change Password
Local Password Policy
AAA Mode
Users
Groups
Active Sessions
TACACS+
RADIUS

Export Task List

Administration > AAA > Export Task List

Please cut and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=LobbyAmbassador
task0=Configure Guest Users
task1=Lobby Ambassador User Preferences
```

RADIUS Custom Attributes

```
Wireless-WCS:role0=LobbyAmbassador
Wireless-WCS:task0=Configure Guest Users
Wireless-WCS:task1=Lobby Ambassador User Preferences
```

注意： 您必须配置用户角色(此示例的大厅大使)和他们可执行和菜单项他们能访问任务的列表。如果使用WCS最近版本，您必须也配置虚拟域用户将属于。

- 选择Administration > 虚拟域。
- 点击出口。

Virtual Domain Custom Attributes

Please cut and paste the appropriate protocol specific data below into the custom/vendor-specific attribute field in access to.

TACACS+ Custom Attributes

```
virtual-domain0=root
virtual-domain1=w1
```

RADIUS Custom Attributes

```
Wireless-WCS:virtual-domain0=root
Wireless-WCS:virtual-domain1=w1
```

- 选择策略元素>授权和权限>设备Administration > Shell配置文件为了创建一新的shell配置文件。
- 输入一有意义的名称(例如WCS)，然后单击自定义属性选项卡。
- 配置属性，他们在WCS存在。

Manually Entered

Attribute	Requirement	Value
role0	Mandatory	LobbyAmbassador
task0	Mandatory	Configure Guest Users
task1	Mandatory	Lobby Ambassador User Preferences
virtual-domain0	Mandatory	root

注意： 在ACS中版本早于版本5.2补丁程序7，您也许面对问题，当您参与包含词“警报”的任务时。这在最新ACS版本修复。同一问题在身份服务引擎(ISE)版本存在早于1.2。这是示例如何手工输入属性：

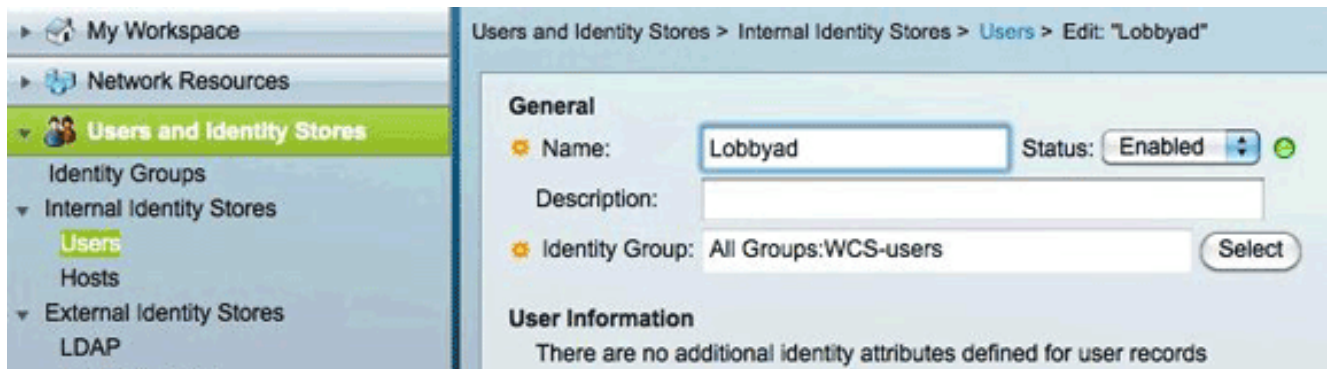
```
-type "role0" in the "Attribute" field
-type "LobbyAmbassador" in the Value field
-click the "add" button.
```

Etc... for the other attributes. **注意：** 在ACS 4，它是可能复制/粘贴属性列表从WCS GUI的到ACS 4 GUI。在ACS 5，必须逐个输入他们。在NCS和头等基础设施，按非常详细的顺序必须输入属性。命令是虚拟域、角色和任务列表。如果输入在错误的命令，NCS/Prime拒绝验证。

```
NCS:virtual-domain0=ROOT-DOMAIN
NCS:role0=Super Users
NCS:task0=View Alerts and Events
```

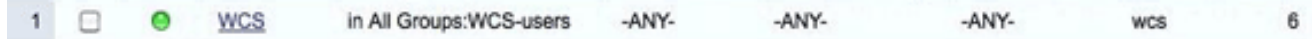
步骤4.配置Cisco Secure ACS返回属性。

- 配置用户(此示例使用Lobbyad)作为ACS的一个用户。



注意： 对于配置方便，此示例添加Lobbyad用户到WCS用户组。(此步骤可选。)

2. 在访问策略，在**默认设备Admin >授权**下，请配置规则匹配WCS验证。



3. 如果用户名属于WCS用户请分组，返回包含组属性)的wcs shell配置文件(。

4. 如果要配置用户的其他类型(例如管理员)，您必须配置另一shell配置文件返回不同的属性。从那时起，您在一不同的组中必须分组管理员为了区分和了解什么返回的shell配置文件。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [思科无线控制系统配置指南，版本7.0.172.0](#)
- [思科安全访问控制系统的5.2用户指南](#)
- [技术支持和文档 - Cisco Systems](#)