NAC(CCA) ：配置在Clean Access管理器的验证有ACS的5.x和以后

目录

简介

本文提供信息如何配置在Clean Access管理器(CAM)的验证用思科安全访问控制系统(ACS) 5.x和以后。对于一相似的配置使用版本早于ACS 5.x，参考NAC(CCA) ：配置在Clean Access管理器(CAM)的验证有ACS的。

先决条件

要求

此配置是可适用的对CAM版本3.5和以上。

使用的组件

本文档中的信息根据CAM版本4.1。

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

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置在CCA的验证与ACS 5.x

完成这些步骤：

1. **添加新的角色 创建Admin角色**从CAM，请选择**用户管理>用户角色>New角色**。输入唯一的名称， **admin**，在角色的作用的Name字段。输入**管理员用户角色**作为一个可选角色说明。选择**正常洛金角色**作为角色类型。配置**带外(OOB)**用户角色与适当的VLAN的VLAN。例如，请选择VLAN ID并且指定ID作为10。当完成，请单击**创建角色**。为了恢复在表的默认属性，请点击**“Reset”**。角色在角色列表当前出现选项卡如OOB基于任务的映射部分的标记VLAN所显示。**创建用户角色**从CAM，请选择**用户管理>用户角色>New角色**。输入唯一的名称，**用户**，在角色的作用的Name字段。输入**普通用户角色**作为一个可选角色说明。配置**带外(OOB)**用户角色与适当的VLAN的VLAN。例如，请选择VLAN ID并且指定ID作为20。当完成，请单击**创建角色**。为了恢复在表的默认属性，请点击**“Reset”**。角色在角色列表当前出现选项卡如OOB基于任务的映射部分的标记VLAN所显示。
2. **OOB基于任务的映射的标记VLAN**到目前为止从CAM，请选择**用户管理>角色用户角色>列表**为了看到角色列表。
3. **添加RADIUS认证服务器(ACS)**选择**用户管理>认证服务器>New**。从认证类型下拉菜单，请选择**Radius**。输入运营商名称作为**ACS**。输入服务器名作为**auth.cisco.com**。**服务器端口**— **1812**端口号在哪些RADIUS服务器侦听。**Radius类型**— RADIUS验证方法。支持的方法包括EAPMD5、PAP、CHAP、MSCHAP和MSCHAP2。使用**默认角色，**如果映射对ACS没有正确地定义也没有设置，或者，如果RADIUS属性在ACS没有正确地定义也没有设置。**共享塞克雷**— RADIUS共享秘密区域对指定的客户端IP地址。**nas-ip-address** —用所有RADIUS验证数据包将传送的此值。单击**添加服务器**。
4. **映射ACS用户对CCA用户角色**选择**用户管理>认证服务器>映射映射林克的规则>Add**为了映射ACS的管理员用户到CCA管理员用户角色。选择**用户管理>认证服务器>映射映射林克的规则>Add**为了映射在ACS的普通用户到CCA用户角色。这是用户角色映射摘要：
5. **在用户页的Enable (event)备选供应商**选择**Administration >用户页>登录页>Add >内容**为了启用在用户登录页的备选供应商。

ACS5.x配置

1. 选择**网络资源>网络设备和AAA客户端**，然后单击**创建**为了添加**CAM**作为**AAA客户端**。
2. 提供**名称， IP地址**并且选择**RADIUS**在认证选项下。然后，为**CAM请**提供**共享塞克雷**并且单击**提交**。
3. 选择**网络资源>网络设备和AAA客户端**，然后单击**创建**为了添加**CAS**作为**AAA客户端**。
4. 提供**名称， IP地址**并且选择**RADIUS**在认证选项下。然后，为**CAS请**提供**共享塞克雷**并且单击**提交**。
5. 选择**网络资源>网络设备和AAA客户端**并且单击**创建**为了添加**ASA**作为**AAA客户端**。
6. 提供**名称， IP地址**并且选择**RADIUS**在认证选项下。然后，为**ASA请**提供**共享塞克雷**并且单击**提交**。

7. 选择**用户，并且标识存储>标识组**并且单击**创建**为了创建一新的标识组。
8. 提供**组名**并且单击**提交**。
9. 选择**用户，并且标识存储>标识组**并且单击**创建**为了创建一新的标识组。
10. 提供**组名**并且单击**提交**。
11. 选择**用户，并且标识存储>内部标识存储>** Users并且单击**创建**为了创建新用户。
12. 提供用户的**名称**并且更改组成员对Admin group。然后，请提供**密码**并且证实密码。单击 submit。
13. 选择**用户，并且标识存储>内部标识存储>** Users并且单击**创建**为了创建新用户。
14. 提供用户的**名称**并且更改组成员对用户组。然后，请提供**密码**并且证实密码。单击 submit。
15. 选择**策略元素>授权和权限>网络访问>授权配置文件**并且单击**创建**为了创建一新的**授权配置文件**。
16. 提供**配置文件名称**并且点击RADIUS**属性**。
17. 从RADIUS**属性请**选中，选择RADIUS-IETF作为**词典类型**。然后，请在RADIUS**属性旁边**单击**精选**。
18. 选择**类别属性**并且点击OK键。
19. 保证**属性值**是**静态的**并且进入Admin作为值。单击**添加**，然后单击**提交**。
20. 选择**策略元素>授权和权限>网络访问>授权配置文件**并且单击**创建**为了创建一新的**授权配置文件**。
21. 提供**配置文件名称**并且点击RADIUS**属性**。
22. 从RADIUS**属性请**选中，选择RADIUS-IETF作为**词典类型**。然后，请在RADIUS**属性旁边**单击**精选**。
23. 选择**类别属性**并且点击OK键。
24. 保证**属性值**是**静态的**并且输入**用户**作为值。单击**添加**，然后单击**提交**。
25. 选择**访问策略>**Access Services>服务处理RADIUS**请求的服务选择规则**并且识别。在本例中，服务是**默认网络网络访问**。
26. 选择**访问策略>**Access Services>**默认网络网络访问**(服务在处理RADIUS请求)的上一步识别**>授权**。点击**自定义**。
27. 移动从**联机的标识组**向**选定**列。单击 Ok。
28. 单击**创建**为了创建新规则。
29. 保证**标识**Group**复选框**被检查，然后在**标识组旁边**单击**精选**。
30. 选择Admin group并且点击OK键。
31. 点击**精选**在**授权配置文件**部分。
32. 选择Admin授权配置文件并且点击OK键。
33. 单击**创建**为了创建新规则。
34. 保证**标识**Group**复选框**被检查并且在标识组旁边单击**精选**。
35. 选择用户组并且点击OK键。
36. 点击**精选**在**授权配置文件**部分。
37. 选择用户授权配置文件并且点击OK键。
38. 单击 Ok。
39. 点击Save Changes。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco NAC设备支持
- 思科安全访问控制系统
- 技术支持和文档 - Cisco Systems