NAC(CCA) ：在Clean Access Manager (CAM) with ACS上配置认证

目录

简介

本文描述如何配置在Clean Access管理器(CAM)的验证用思科安全访问控制服务器(ACS)。对于一相似的配置使用ACS 5.x和以后，参考NAC(CCA) ：配置在Clean Access管理器的验证有ACS的5.x和以后。

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的验证的步骤与ACS

完成这些步骤：

1. **添加新的角色 创建Admin角色**在CAM中，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**在CAM中，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**到目前为止在CAM中，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**—端口号RADIUS服务器侦听的**1812**。**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。

ACS配置

1. 选择**接口配置**为了确保， RADIUS (IETF)类别属性[025]启用。
2. **添加RADIUS客户端到ACS服务器**选择**网络配置**为了添加AAA客户端CAM如显示：单击**Submit+ Restart**。**注意：** 确保RADIUS密钥配比与AAA客户端并且使用RADIUS (IETF)。选择**网络配置**为了添加AAA客户端CAS如显示：单击 **Submit+ Restart**。**注意：** 对于认为VPN网关的RADIUS， CCA策略必须允许RADIUS认为的数据包(UDP 1646/1813)从CAS IP地址通过未经鉴定到ACS服务器IP地址。选择**网络配置**为了添加AAA客户端ASA如显示：用户左侧

PIX/ASA接口地址(典型地内部接口)对RADIUS (思科IOS/PIX)的Set type。

3. **添加ACS服务器的/Configure组创建Admin group**设置IETF RADIUS类别属性[025]合适组的值。值必须匹配在CAS映射配置的那。**创建用户组**添加/配置能将被映射的每个Clean Access用户角色的组。**添加/配置ACS服务器的用户**添加/配置ACS能将验证的每个Clean Access用户的ACS用户。设置ACS组成员。ACS也支持代理验证到其他外部服务器。

验证

使用本部分可确认配置能否正常运行。

在监控部分的ACS，您能看到关于合格认证的信息如显示：

同样地，您能为RADIUS核算看到屏幕画面：

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设备支持页面
- 技术支持和文档 - Cisco Systems