NAC(CCA) 4.x ：使用IDAP的某些角色的映射用户配置示例

目录

简介

本文描述映射功能的轻量级目录访问协议(LDAP)为了映射用户到在网络准入控制(NAC)设备或思科Clean Access (CCA)的某些角色。

Cisco NAC设备(以前思科Clean Access)是使用网络基础设施强制执行在所有设备的安全策略标准寻求访问网络计算资源的一种容易地配置的美洲台产品。使用NAC设备，网络管理员能验证，授权，评估和在网络访问前配线的，无线和远程用户和他们的机器修正。它识别网络设备例如膝上型计算机、IP电话或者游戏控制台是否与您的网络的安全策略是兼容的并且在允许对网络的访问前修改所有漏洞。

先决条件

要求

本文假设， CCA管理器、CCA服务器和LDAP服务器适当地安装并且工作。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 3300系列的Cisco NAC设备- Clean Access管理器4.0
- 3300系列的Cisco NAC设备- Clean Access服务器4.0

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

后端活动目录的验证

验证供应商的几种类型在Clean Access管理器的可以用于利用激活目录(AD)服务器验证用户，Microsoft的所有权目录服务。这些包括Windows NT(NTLM)、Kerberos和LDAP (首选)。

如果使用LDAP连接到AD， Search(Admin)全双工特有名(DN)必须典型地设置为一个帐户的DN与管理权限或基本用户权限的。第一个共同名称(CN)条目应该是AD的管理员或者一个用户有读的权限。注意搜索过滤器， SamAccountName，是在默认AD模式的用户登录名。

AD/LDAP配置示例

这说明一配置示例使用LDAP与后端活动目录联络：

1. 创建在激活目录用户和计算机内的一个域管理员用户。放置此用户到用户文件夹。
2. 在激活目录用户和计算机内，请选择从Actions菜单的**查找**。确保您的结果显示已创建用户的组成员列。您的搜索结果应该显示**用户**和相关的**组成员**在活动目录内。这是您将需要转接到Clean Access管理器的信息。
3. 从Clean Access管理器Web控制台，去**用户管理>认证服务器>New服务器**表。
4. 选择**LDAP**作为服务器类型。
5. 对于**Search(Admin)全双工DN**和**搜索库上下文字段**，请输入从查找的结果在激活目录用户和计算机内。
6. 这些字段是必要适当地设置在CAM内的此认证服务器的非常：**ServerURL**：ldap://192.168.137.10:389 -这是域控制器IP地址和LDAP监听端口。**Search(Admin)全双工DN** ：CN=sheldon muir， Cn=users， DC=domainname， Dc=com**搜索库上下文**：DC=domainname， Dc=com**默认角色**：选择用户将被放到一次已验证的默认角色。**说明**：使用供参考。**运营商名称**：这是用于用户页的LDAP服务器的名称设置在CAM。**搜索密码**：sheldon muir的域密码**搜索过滤器**：SAMAccountName=$user$
7. 单击**添加服务器**。这时，您的验证测验应该工作。
8. 为了测试验证：从**用户管理> Test选项认证服务器>的验证**，请选择您要测试在**供应商**列表的凭证的供应商。如果供应商没出现，请确保它正确地配置在**服务器**选项卡**列表**。若需要输入用户和VLAN ID值的用户名和密码。单击 **Authenticate**。测试结果在窗口的底部出现。**成功的验证：**任何供应商类型，结果：当验证测验成功时，成功用户的验证和角色显示。对于LDAP/RADIUS服务器，当验证是成功的时，并且映射规则配置，在映射规则指定的属性/值也显示，如果认证服务器(LDAP/RADIUS)返回那些值。例如：`Result: Authentication successful`
`Role: <role name>`
`Attributes for Mapping:`
`<Attribute Name>=<Attribute value>` **验证失败：**当验证发生故障时，与验证失败一起的信息显示结果如显示。

角色的地图用户使用属性或VLAN ID

映射规则表可以用于映射用户到根据这些参数的用户角色：

- 于CAS起源用户数据流的VLAN ID (所有认证服务器类型)的不信任侧
- 从LDAP和RADIUS认证服务器通过的验证从Cisco VPN集中器通过的属性(和RADIUS属性)

例如，如果有两套用户同样IP子网的，但是用不同的网络访问访问权限，例如无线员工和学员，您能使用从LDAP服务器的一个属性映射一套用户到特定用户角色。您能然后创建数据流策略允许对一个角色的网络访问和拒绝对其他角色的网络访问。

Cisco NAC设备执行映射顺序如显示：

Cisco NAC设备允许管理员指定复杂布尔表示式，当定义映射时为Kerberos规定， LDAP和RADIUS验证服务器。映射规则是被分解为的情况，并且您能使用布尔表示式结合多个用户属性和多个VLAN ID为了映射用户到用户角色。映射规则可以为范围VLAN ID创建，并且属性匹配可以被做不区分大小写。这允许为映射规则灵活地配置的多个情况。

映射规则包括一个验证供应商类型，规则表达式和映射用户的用户角色。规则表达式包括一或用户参数必须匹配被映射到指定的用户角色情况的组合。情况特定的属性匹配的包括情况类型、来源属性名称、操作员和属性值。

为了创建映射规则，您首先添加(保存)情况配置规则表达式。然后，规则表达式一次创建，您能增加映射规则到指定的用户角色的认证服务器。

映射规则可以是层叠。如果来源有超过一个映射的规则，规则按他们在映射规则列表出现的顺序被评估。使用第一个正映射规则的角色。一旦规则满足，其他规则没有测试。如果规则不是真的，使用该验证来源的默认角色。

配置映射规则

完成这些步骤：

1. 去**用户管理>认证服务器>映射规则**并且点击认证服务器的**添加映射规则**链路。**添加映射规则**表出现。
2. 配置映射的规则(a)条件：**运营商名称**—运营商名称设置映射规则表的字段该认证服务器类型的。例如，表只允许VLAN ID映射规则配置Kerberos、Windows NT、Windows NetBIOS SSO和S/Ident认证服务器类型。表允许VLAN ID或属性映射规则配置RADIUS、LDAP和思科VPN SSO认证类型。**情况类型**—在增加映射规则前首先配置并且添加情况(跨步在图的**A**)。从下拉菜单选择这些中的一个为了设置情况表的字段：**属性**— LDAP， RADIUS，思科VPN SSO仅验证供应商。**VLAN ID** —所有认证服务器类型。对于VLAN ID的情况类型(请参见图)，此字段呼叫**特性名称**。默认情况下，这带有“VLAN ID” (和禁用为编辑)。**属性名称**—对于LDAP服务器(请参见图)，**属性名称**是您输入来源属性您要测试的文本字段。名称一定是相同的(区分大小写)与验证来源通过的属性的名称，除非选择**等于忽略案件**操作员创造条件。**属性值**—输入将测试的值来源**属性名称**。**操作员(属性)** —选择定义了来源属性字符串的测验的操作员：**等于**—真，如果**属性名称的**值匹配**属性值**。**不是等于**—真，如果**属性名称的**值不匹配**属性值**。**包含**—真，如果**属性名称的**值包含**属性值**。**开始时**—真，如果**属性名称的**值开始与**属性值**。**末端与**—真，如果**属性名称的**值以**属性值**结束。**等于忽略案件**—真，如果**属性名称的**值匹配**属性值**字符串。不重要字符串是否大写或小写。**操作员(VLAN ID)** —如果选择VLAN ID，当**情况类型**，选择这些操作员之一定义情况该测验VLAN ID整数：**等于**—真，如果VLAN ID在**属性值**字段匹配VLAN ID。**不是等于**—真，如果VLAN ID不在**属性值**字段匹配VLAN ID。**属于对**—真，如果VLAN ID属于为**属性值**字段配置的范围值。值应该是一个或更多逗号被分离的VLAN ID。范围VLAN ID可以由连字符指定(-)，例如， [2,5,7,100-128,556-520]。仅整数可以被输入，不是字符串。注意托架可选。**示例：添加情况(保存情况)** —确保配置情况，然后单击**添加情况**为了添加情况到规则表达式(否则您的配置没有保存)。

3. 增加映射规则到角色(b) ：增加映射规则(在图的步骤B)，在您配置并且添加了条件后。**角色名称**—在您添加了至少一个情况后，请选择您将应用从下拉菜单的映射的用户角色。**优先级**—选择从下拉式的优先级确定映射规则测试的命令。评估对真的第一个规则是使用的分配用户角色。**规则表达式**—为了帮助在配置映射规则的条件语句，此字段显示将被添加的最后情况的内容。在添加条件以后，您必须单击**增加映射规则**为了保存所有条件到规则。**说明**—映射规则的可选说明。**添加映射(保存映射)** —点击此按钮，当完成添加的情况创建角色的映射规则。您必须添加或保存一个指定的角色的映射，否则您的配置和您的情况不会保存。

编辑映射规则

- **优先级**—为了更改后映射的规则的优先级，请在**服务器用户管理>认证服务器>列表的**条目旁边单击up/down箭头。优先级确定规则测试的命令。评估对真的第一个规则是使用的分配用户对角色。
- **编辑**—在规则修改映射规则旁边单击编辑按钮或者删除从规则的条件。请注意，当编辑一个复合条件，条件(已创建以后)时在底下没有显示。这是为了避免环路。
- **删除**—在认证服务器的映射规则条目旁边单击删除按钮删除单个映射规则。在编辑映射规则表的一个条件旁边单击删除按钮从映射规则删除条件。注意您不能删除依靠另一个规则于一个复合语句的情况。为了删除一个单个情况，您必须首先删除复合条件。

故障排除

如果映射CCA用户角色的AD用户不工作，则请确保您映射用户对根据与属性Names= memberof、Operator=contains和属性Value= (组名)的属性的角色。

相关信息

- Cisco NAC设备支持页面
- 技术支持和文档 - Cisco Systems