TACACS+和RADIUS属性多种思科和非Cisco设备配置示例的

目录

简介

本文提供多种思科和非Cisco的产品期望从验证、授权和统计(AAA)服务器接收属性的编译;在这种情况下，AAA服务器是访问控制服务器(ACS)。ACS能与Access-Accept一起返回这些属性作为shell配置文件(TACACS+)或授权配置文件(RADIUS)的部分。

本文提供逐步指导关于怎样添加自定义属性给shell配置文件和授权配置文件。设备期望发现返回从AAA服务器的本文也包含设备列表和TACACS+和RADIUS属性。所有主题包括示例。

在本文提供的属性列表不详尽或授权，并且可能在任何时间变成没有更新本文。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据ACS版本5.2/5.3。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

创建Shell配置文件(TACACS+)

shell配置文件是TACACS+-based访问的一个基本权限容器。除Cisco® IOS权限级别、会话超时和其他参数之外， TACACS+属性和属性值应该返回与Access-Accept的您能指定。

完成这些步骤为了添加自定义属性到一新的shell配置文件：

1. 登陆对ACS接口。
2. 导航到**策略元素>授权和权限>设备Administration > Shell配置文件**。
3. 点击**创建按钮**。
4. 给出shell配置文件。
5. 点击**自定义属性**选项卡。
6. 在**属性**字段进入属性名称。
7. 选择需求是否从需求下拉列表是**必须**或**可选**。
8. 留下下拉式属性值的设置为**静态**。如果值是静态的，您能输入在下一个字段的值。如果值动态，您不能手工输入属性;反而归因于的在其中一被映射对一个属性标识存储中。
9. 在最后字段输入属性的值。
10. 点击**Add按钮**为了添加条目到表。
11. 重复配置您需要的所有属性。
12. 在底部的屏幕单击**SUBMIT按钮**。

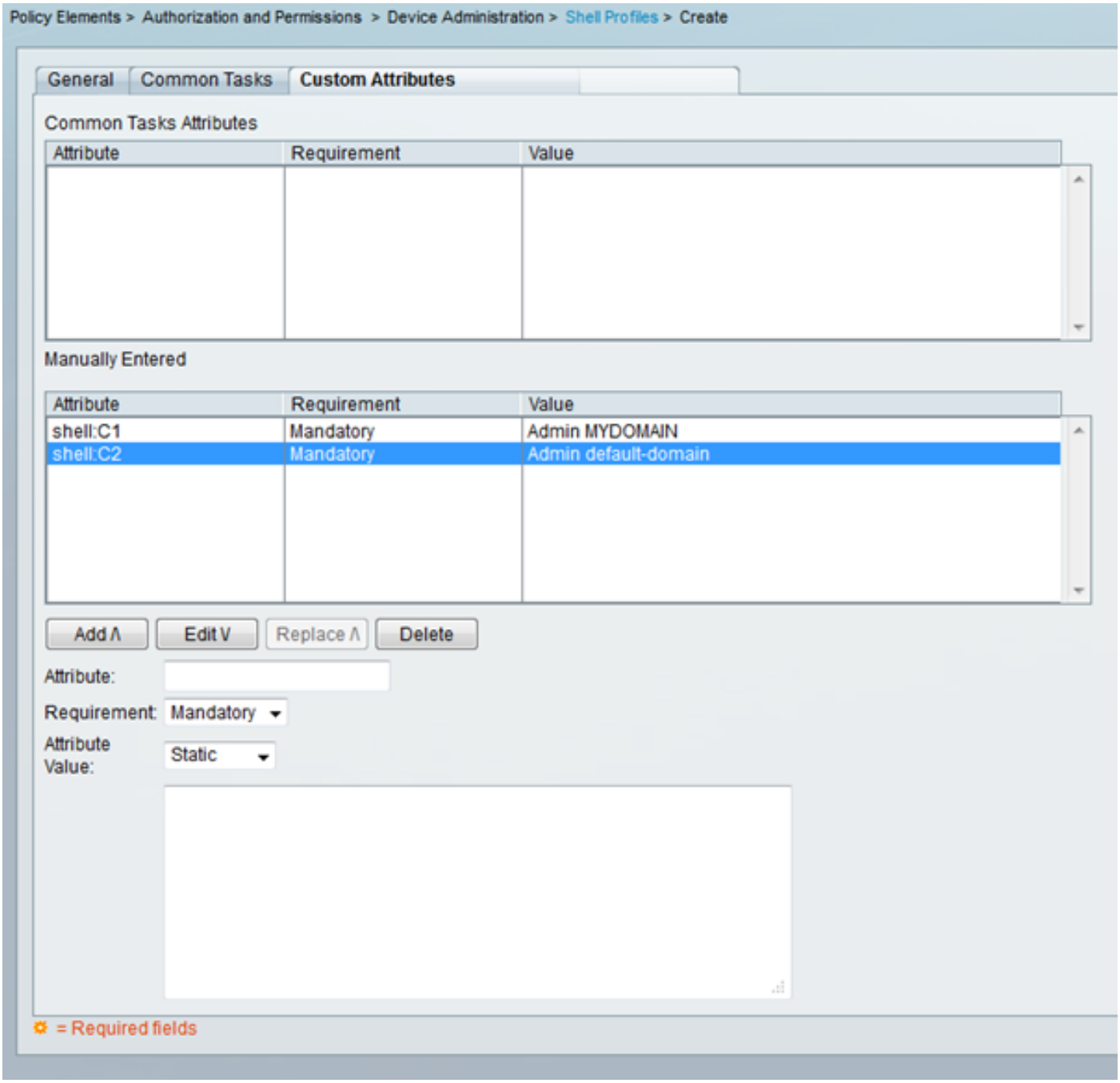
配置示例

设备：应用程序控制引擎 (ACE)

属性：`shell <context-name>`

值：`<Role-name> <domain-name1>`

使用情况：角色和域由空格符分离。您能配置(例如， USER1)将分配角色(例如， ADMIN)和域的用户(例如， MYDOMAIN)，当用户登录到上下文(例如， C1)。



创建授权配置文件(RADIUS)

授权配置文件是基于RADIUS的访问的一个基本权限容器。您能指定应该返回除VLAN、访问控制列表(ACL)和其他参数之外，哪些RADIUS属性和属性值与Access-Accept。

完成这些步骤为了添加自定义属性到一新的授权配置文件：

1. 登陆对ACS接口。
2. 导航对**策略元素>授权和权限>网络访问>授权配置文件**。
3. 点击**创建按钮**。
4. 给出授权配置文件。
5. 点击**RADIUS属性**选项卡。
6. 选择从**词典类型**下拉菜单的一个字典。
7. 为了设置精选RADIUS属性字段的属性，点击**下选择按钮**。新窗口出现。
8. 查看可用的属性，做您的选择，并且点击OK键。默认情况下**Attribute type**值根据您做的属性

选择设置。

9. 留下下拉式属性值的设置为**静态**。如果值是静态的，您能输入在下一个字段的值。如果值动态，您不能手工输入属性;反而归因于的在其中一被映射对一个属性标识存储中。
10. 在最后字段输入属性的值。
11. 点击**Add按钮**为了添加条目到表。
12. 重复配置您需要的所有属性。
13. 在底部的屏幕单击**SUBMIT按钮**。

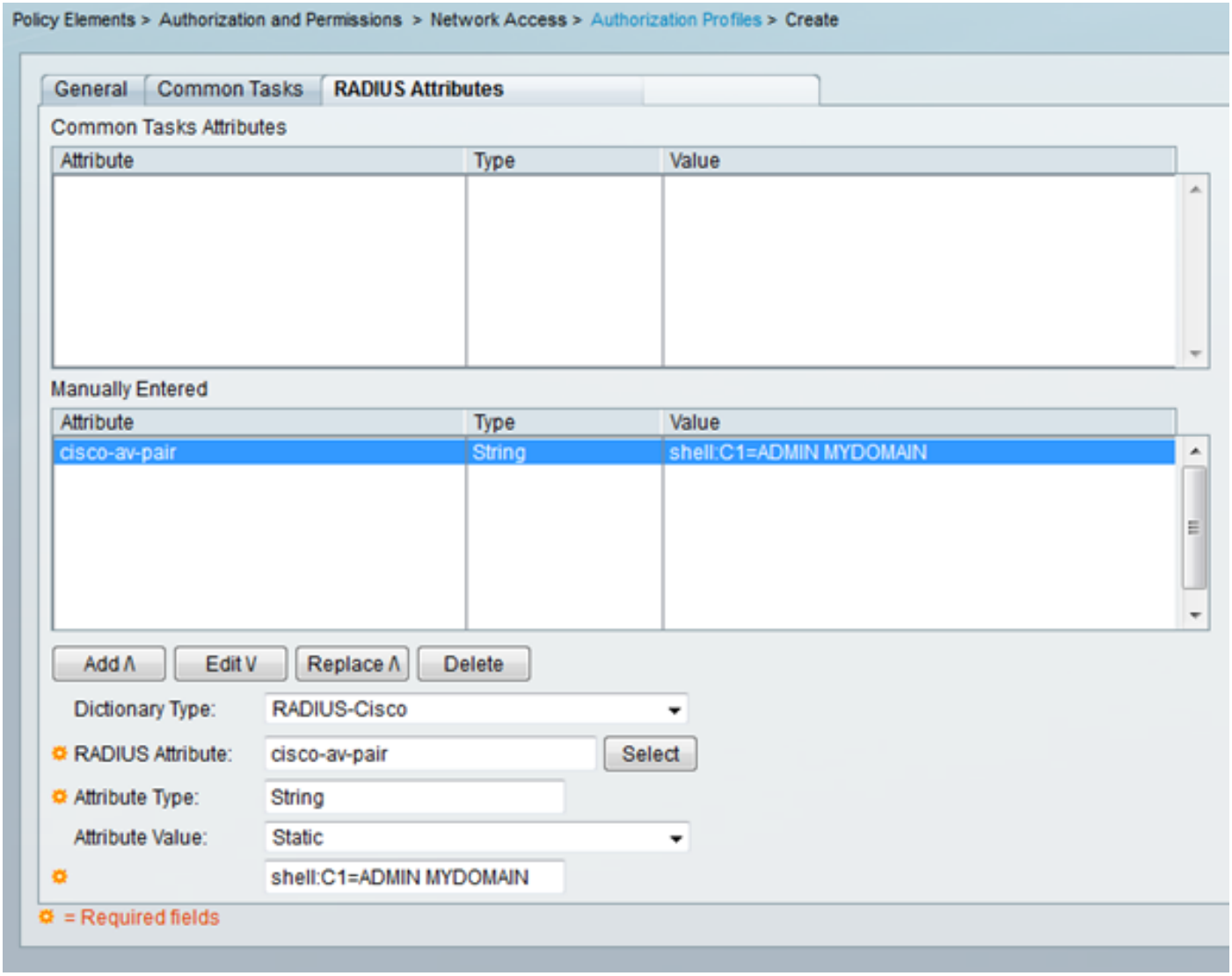
配置示例

设备：ACE

属性：`cisco-av-pair`

值：`shell <context-name>=<Role-name> <domain-name1> <domain-name2>`

使用情况：在等号以后的每个值由空格符分离。您能配置(例如， USER1)将分配角色(例如，ADMIN)和域的用户(例如， MYDOMAIN)，当用户登录到上下文(例如， C1)。



设备清单

聚合服务路由器(ASR)

RADIUS (授权配置文件)

属性：`cisco-av-pair`

值：`shell tasks= " #<role-name> <permission> <process>”`

使用情况：设置值`<role-name>`为在路由器本地定义的角色的名称。角色层级可以描述根据树，角色`#root`是在树顶部，并且角色`#leaf`添加其它命令。这两个角色可以被结合和通过的上一步，如果`：shell tasks= " #root #leaf”`。

权限可以也是根据单个进程基本类型的通过的上一步，因此用户能授权读，写入和执行某些进程的权限。例如，为了授权用户请读并且写入BGP进程的权限，设置值对：`shell tasks= " #root rw bgp”`。属性的命令不重要;结果是相同的值是否设置为`shell tasks= " #root rw bgp”`或ro `shell tasks= " rw bgp #root”`。

示例–添加属性到授权配置文件

词典类型	RADIUS 属性	Attribute type	属性值
RADIUS 思科	`cisco-av-pair`	字符串	`shell:tasks="#root,#leaf,rwx:bgp,r:ospf"`

应用程序控制引擎 (ACE)

TACACS+ (Shell配置文件)

属性：`shell <context-name>`

值：`<Role-name> <domain-name1>`

使用情况：角色和域由空格符分离。您能配置(例如， USER1)将分配角色(例如， ADMIN)和域的用户(例如， MYDOMAIN)，当用户登录到上下文(例如， C1)。

示例–添加属性到Shell配置文件

属性	需求	属性值
`shell:C1`	必须	`Admin MYDOMAIN`

如果USER1通过C1上下文登陆，该用户自动地分配ADMIN角色和MYDOMAIN域(在授权规则配置条件下的地方，一旦USER1登陆，他们分配此授权配置文件)。

如果USER1通过不同的上下文登陆，没有返回按属性的值ACS退还，用户自动地分配默认角色(网络监控器)和默认域(默认域)。

RADIUS (授权配置文件)

属性：`cisco-av-pair`

值：`shell <context-name>=<Role-name> <domain-name1> <domain-name2>`

使用情况：在等号以后的每个值由空格符分离。您能配置(例如， USER1)将分配角色(例如， ADMIN)和域的用户(例如， MYDOMAIN)，当用户登录到上下文(例如， C1)。

示例–添加属性到授权配置文件

词典类型	RADIUS属性	Attribute type	属性值
RADIUS思科	`cisco-av-pair`	字符串	`shell:C1=ADMIN MYDOMAIN`

如果USER1通过C1上下文登陆，该用户自动地分配ADMIN角色和MYDOMAIN域(在授权规则配置条件下的地方，一旦USER1登陆，他们分配此授权配置文件)。

如果USER1通过不同的上下文登陆，没有返回按属性的值ACS退还，用户自动地分配默认角色(网络监控器)和默认域(默认域)。

Bluecoat数据包成型机

RADIUS (授权配置文件)

属性：`Packeteer AVPair`

值：`access=<level>`

使用情况：`<level>`是授权的级别访问。而查看访问与只读，是等同的联系访问与读写是等同的。

默认情况下Bluecoat VSA在ACS字典不存在。为了使用Bluecoat属性在授权配置文件，您必须创建Bluecoat字典和添加Bluecoat属性到该字典。

创建字典：

1. 导航对**系统管理> Configuration>字典>协议> RADIUS> RADIUS VSA**。
2. 单击**创建**。
3. 输入字典的详细信息：名称：Bluecoat厂商ID ：2334属性前缀：Packeteer-
4. 单击 **submit**。

创建在新的字典的一个属性：

1. 导航对**系统管理> Configuration>字典>协议> RADIU** S **> RADIUS VSA > Bluecoat**。
2. 单击**创建**。
3. 输入属性的详细信息：属性：`Packeteer AVPair`说明：用于为了指定访问级别供应商属性ID ：1方向：出站允许的多个：错误包括属性在日志：已勾选Attribute type ：字符串
4. 单击 **submit**。

示例–添加属性到授权配置文件(只读访问)

词典类型	RADIUS属性	Attribute type	属性值
RADIUS Bluecoat	`Packeteer-AVPair`	字符串	`access=look`

示例–添加属性到授权配置文件(读写访问)

词典类型	RADIUS属性	Attribute type	属性值

RADIUS Bluecoat	Packeteer-AVPair	字符串	access=touch

Brocade交换机

RADIUS (授权配置文件)

属性：ID

值：U:<VLAN1>;T:<VLAN2>

使用情况：设置<VLAN1>为数据VLAN的值。设置<VLAN2>为语音VLAN的值。在本例中，数据VLAN是VLAN10，并且语音VLAN是VLAN21。

示例–添加属性到授权配置文件

词典类型	RADIUS属性	Attribute type	属性值
RADIUS-IETF	Tunnel-Private-Group-ID	标记为的字符串	U:10;T:21

Cisco Unity Express (CUE)

RADIUS (授权配置文件)

属性：cisco-av-pair

值：fndn groups=<group name>

使用情况：<group name>是组的名称有您要授权对用户的权限。此组在Cisco Unity Express (CUE)必须配置。

示例–添加属性到授权配置文件

词典类型	RADIUS属性	Attribute type	属性值
RADIUS思科	cisco-av-pair	字符串	fndn:groups=Administrators

Infoblox

RADIUS (授权配置文件)

属性：InfobloxINFO

值：<group name>

使用情况：<group name>是组的名称有您要授权对用户的权限。此组在Infoblox设备必须配置。在本例中配置示例，组名是MyGroup。

默认情况下Infoblox VSA在ACS字典不存在。为了使用Infoblox属性在授权配置文件，您必须创建Infoblox字典和添加Infoblox属性到该字典。

创建字典：

1. 导航对**系统管理> Configuration>字典>协议> RADIUS> RADIUS VSA**。
2. 单击**创建**。
3. 在**使用提前的供应商选项旁边**单击小箭头。
4. 输入字典的详细信息：名称：Infoblox厂商ID ：7779供应商Length字段大小：1供应商类型字段长度：1
5. 单击 **submit**。

创建在新的字典的一个属性：

1. 导航对**系统管理> Configuration>字典>协议> RADIUS> RADIUS VSA > Infoblox**。
2. 单击**创建**。
3. 输入属性的详细信息：属性：`InfobloxINFO`供应商属性ID ：009方向：出站允许的多个：错误包括属性在日志：已勾选Attribute type ：字符串
4. 单击 **submit**。

示例–添加属性到授权配置文件

词典类型	RADIUS属性	Attribute type	属性值
RADIUSInfoblox	`Infoblox-Group-Info`	字符串	`MyGroup`

入侵防御系统 (IPS)

RADIUS (授权配置文件)

属性：`IPS`

值：`<role name>`

使用情况：值`<role name>`可以是任何一个四个入侵防御系统(IPS)用户角色：查看器、操作员、管理员或者服务。参考IPS您的版本的配置指南关于授权的权限的详细信息对每个用户角色类型。

- 思科入侵防御系统IPS的7.0设备管理器配置指南
- 思科入侵防御系统IPS的7.1设备管理器配置指南

示例–添加属性到授权配置文件

词典类型	RADIUS属性	Attribute type	属性值
RADIUS思科	`cisco-av-pair`	字符串	`ips-role:administrator`

Juniper

TACACS+ (Shell配置文件)

属性：;;;;;

值：`<allow-commands-regex>;<allow-configuration-regex>;<local-username>;<deny-commands-regex>;<deny-configuration-regex>`

使用情况：设置值<local-username> (即值名字属性)为在Juniper设备存在本地的用户名。例如，您能配置和在Juniper设备存在本地的用户一样(例如， USER1)将分配的用户模板用户(例如， JUSER)，当您设置名字属性的值为JUSER时。允许命令、允许配置、拒绝命令和拒绝配置属性的值在REGEX格式可以被输入。值这些属性设置对是除用户登录类权限位授权的可操作/配置模式命令之外。

示例–添加属性到Shell配置文件1

属性	需求	属性值
allow-commands	可选	"(request system) | (show rip neighbor)"
allow-configuration	可选	
local-user-name	可选	sales
deny-commands	可选	"<^clear"
deny-configuration	可选	

示例–添加属性到Shell配置文件2

属性	需求	属性值
allow-commands	可选	"monitor | help | show | ping | traceroute"
allow-configuration	可选	
local-user-name	可选	engineering
deny-commands	可选	"configure"
deny-configuration	可选	

连结交换机

RADIUS (授权配置文件)

属性：cisco-av-pair

值：shell:roles="<role1> <role2>"

使用情况：设置值<role1>和<role2>为在交换机本地定义的角色名称。当您添加多个角色时，请分离他们与空格符。当多个角色是从AAA服务器的通过的上一步到连结交换机时，结果是用户访问所有三个角色联盟定义的命令。

内置的作用定义在配置用户帐户和RBAC。

示例–添加属性到授权配置文件

词典类型	RADIUS属性	Attribute type	属性值
RADIUS思科	cisco-av-pair	字符串	shell:roles="network-admin vdc-admin vdc-operator"

Riverbed

TACACS+ (Shell配置文件)

属性：;

值：`RBT exec;<username>`

使用情况：为了准许用户只读访问，必须设置`<username>`值监控。为了准许用户读写访问，必须设置`<username>`值为admin。如果有另一个帐户定义除admin和监视器之外，请配置将返回的该名称。

示例–添加属性到Shell配置文件(只读访问)

属性	需求	属性值
service	必须	rbt-exec
local-user-name	必须	monitor

示例–添加属性到Shell配置文件(读写访问)

属性	需求	属性值
service	必须	rbt-exec
local-user-name	必须	admin

无线局域网控制器(WLC)

RADIUS (授权配置文件)

属性：

值：`(6)/Nas(7)`

使用情况：为了准许用户对无线局域网控制器(WLC)的读/写访问，值一定是管理的;对于只读访问，值必须是Nas提示。

关于详细信息，请参阅管理用户的RADIUS服务器验证无线局域网控制器(WLC)配置示例的

示例–添加属性到授权配置文件(只读访问)

词典类型	RADIUS属性	Attribute type	属性值
RADIUS-IETF	Service-Type	列举	NAS-Prompt

示例–添加属性到授权配置文件(读写访问)

词典类型	RADIUS属性	Attribute type	属性值
RADIUS-IETF	Service-Type	列举	Administrative

数据中心网络管理器(DCNM)

DCNM，在认证方法更改后，必须重新启动。否则，它可能分配网络操作员权限而不是网络Admin。

DCNM角色	cisco-av-pair RADIUS	cisco-av-pair TACACS
用户	shell:roles = "network-operator"	cisco-av-pair=shell:roles="network-operator"
管理员	shell:roles =	cisco-av-

	"network-admin"	pair=shell:roles="network-admin"

相关信息

- 技术支持和文档 - Cisco Systems
- 终端访问控制器访问控制系统 (TACACS+)
- 远程用户拨入认证系统(RADIUS)
- 请求注解 (RFC)