ACS与Motorola的版本5.4集成飞过5.X (AP)配置示例

目录

简介

本文提供配置示例思科安全访问控制服务器(ACS)版本5.4支持TACACS+认证、授权和核算(AAA)在Motorola无线控制器和接入点。在本文中， Motorola供应商专用属性和值分配到ACS的组为了确定每个用户角色和访问权限。属性和值分配到有用户定义的在每组启用的服务和协议的组。

先决条件

要求

应该连接ACS版本5.x到Motorola翼5.x。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ACS版本5.4
- 翼5.2

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。

配置

ACS配置

设备类型

这是示例如何定义翼5设备作为在Cisco Secure ACS版本5.x的设备类型。设备类型允许在Cisco Secure ACS版本5.x将分组的设备，使用，当您定义了设备授权策略时。

在ACS GUI，请导航对**网络资源>网络设备组>设备类型**，并且单击**创建**。

输入**名称**和**说明**，并且选择**帕伦特**。单击 **submit**。

这创建Motorola解决方案设备的一个**网络设备组**。

网络设备和AAA客户端

这如何是示例添加翼5设备作为Cisco Secure ACS版本5.x的一个AAA客户端。

在Cisco Secure ACS，请导航给**网络资源>网络设备和AAA客户端**，并且单击**创建**：

输入一**名称**对于无线控制器，并且选择**位置**。分配在前面部分创建的**设备类型**，并且检查**TACACS+**复选框。输入**共享塞克雷**，并且在适当的**IP地址选项旁边**单击单选按钮。在本例中，**由掩码的IP范围**选择，并且IPv4子网无线控制器连接对(**192.168.20.0/24**)定义。一旦输入所有信息，请单击**提交**。

这定义了无线控制器作为**网络设备和AAA客户端**：

标识组

在本例中，两组，已命名MotorolaRO和MotorolaRW，定义。而用户分配到MotorolaRW组分配到超级用户角色并且授权所有访问权限，用户分配到MotorolaRO组分配到箴言报角色和授权的Web访问访问权限。

导航给**用户，并且标识存储>标识Groups>创建**：

输入一**名称**和**说明**只读访问组的，并且单击**提交。**

创建第二组。输入一**名称**和**说明**读/写访问组的，并且单击**提交**。

您当前创建两**标识组**。

Shell配置文件

这是示例如何定义在Cisco Secure ACS版本5.x的shell配置文件。在本例中，两shell配置文件，已命名MOTO RO和MOTO RW，定义与确定角色和访问权限的属性每个管理用户分配。每shell配置文件名称必须匹配在TACACS+ AAA策略定义的TACACS+认证服务的名称。

导航到**策略元素>授权和权限>设备Administration > Shell配置文件**。单击**创建**。

在**常规选项卡**，请定义需要的TACACS+服务和协议添加。您能使用当前服务和协议或者创建您自己。此示例以MOTO RO名义定义了服务和协议为了提供只读访问飞过5个设备：

在**共同性任务**选中，设置**最大权限**为**静态**，并且选择值为**1。**

在**自定义属性**选项卡，在**属性**和**属性值**字段，请定义将分配的属性到用户。在本例中，只读用户分配到箴言报角色和授权的Web访问访问权限。单击 **submit**。

创建一新的**Shell配置文件**。在**常规选项卡**，请定义需要的TACACS+服务和协议添加。您能使用当前服务和协议或者创建您自己。此示例定义了服务和协议，已命名MOTO RW，为翼5设备提供读/写访问：

在**共同性任务**选中，设置**最大权限**为**静态**，并且选择值为**1。**

在**自定义属性**选项卡，在**属性**和**属性值**字段，请定义将分配的属性到用户。在本例中，读/写用户分配到超级用户角色并且授权所有访问权限。单击 **submit**。

您当前创建名为MOTO RO的**Shell配置文件**和MOTO RW。

设备授权配置文件

这是示例如何定义设备在Cisco Secure ACS版本5.x的授权策略。设备授权策略确定shell配置文件用户分配根据设备类型请求验证、位置和标识组成员的每管理。在本例中，两项设备授权策略，已命名MotorolaRO和MotorolaRW，定义。

在Cisco Secure ACS，请导航到**访问策略>默认设备Admin >授权>自定义**：

添加名为**Identity的**自定义条件**Group**， **NDG ：位置**， **NDG ：设备类型**和**协议**。在自定义结果下，请添加**Shell配置文件**，并且点击OK键：

单击**创建**。在**Name字段**，请输入**MotorolaRO**，并且选择**标识组**， **NDG ：位置**和**NDGevice类型**。设置协议为**TACACS**，并且选择名为**MOTO RO的**Shell配置文件。点击OK键：

单击**创建**。在**Name字段**，请输入**MotorolaRW**，并且选择**标识组**， **NDG ：位置**和**NDGevice类型**。设置协议为**TACACS**，并且选择名为**MOTO RW的**Shell配置文件。点击OK键：

您当前创建**设备**名为MotorolaRO和MotorolaRW的**授权策略**：

Motorola解决方案飞过5.2配置

AAA TACACS策略

AAA TACACS策略定义了在翼5设备的TACACS+客户端配置。每项AAA TACACS策略能包含两个TACACS+ AAA服务器条目除在Cisco Secure ACS和协议的定义的名称之外TACACS+认证服务。TACACS+ AAA策略也确定转发到记帐服务器的信息。

此AAA TACACS策略示例定义了TACACS+ AAA的Cisco Secure ACS，定义了名为MOTO RO的TACACS+服务和协议和MOTO RW，并且启用CLI命令和会话核算。

AAA TACACS策略示例

```
aaa-tacacs-policy CISCO-ACS-SERVER

authentication server 1 host 192.168.10.21 secret 0 hellomoto

authorization server 1 host 192.168.10.21 secret 0 hellomoto

accounting server 1 host 192.168.10.21 secret 0 hellomoto

authentication service MOTO protocol RO

authentication service MOTO protocol RW

accounting commands

accounting session

!
```

管理策略

一旦AAA TACACS+策略定义，必须分配到一个或更多管理策略，在使用前TACACS+。管理策略确定在每翼5设备、本地管理用户、角色和访问权限启用的管理接口和外部用于的RADIUS或TACACS+服务器为了验证管理用户。

默认情况下，每个翼5设备分配到管理策略，名为默认，分配与使用配置文件。TACACS+在默认管理策略或所有用户定义的管理策略可以启用。

多数典型的部署包括无线控制器和接入点的独立的管理策略。因为管理需求和接口每个设备的有所不同，推荐独立的管理策略。在这种情况下，在每管理策略必须启用TACACS+为了启用在无线控制器和接入点的TACACS+。

在下一部分的管理策略示例启用在分配到无线控制器和接入点的用户定义的管理策略的TACACS+ AAA。在翼5设备不能到达验证的情况下，任何定义TACACS+服务器对本地认证的TACACS+ fallback也启用。

管理策略示例

```
!
```

```
management-policy CONTROLLER-MANAGEMENT

no http server

https server

ssh

user admin password 0 hellomoto role superuser access all

snmp-server user snmptrap v3 encrypted des auth md5 0 hellomoto

snmp-server user snmpoperator v3 encrypted des auth md5 0 hellomoto

snmp-server user snmpmanager v3 encrypted des auth md5 0 hellomoto

aaa-login tacacs fallback

aaa-login tacacs authorization

aaa-login tacacs accounting

aaa-login tacacs policy CISCO-ACS-SERVER

!

!

management-policy AP-MANAGEMENT

ssh

user admin password 0 hellomoto role superuser access all

aaa-login tacacs fallback

aaa-login tacacs authorization

aaa-login tacacs accounting

aaa-login tacacs policy CISCO-ACS-SERVER

!
```

验证

此部分提供要求的必要的步骤为了验证TACACS+ AAA。在本例中，两个用户帐户在每Cisco Secure ACS定义并且分配到适合的组。用户的组成员确定角色和访问权限分配到管理用户。

```
Username           Role          Access Permissions
-----------------------------------------------------
monitor Monitor Web
super user Superuser all
```

角色分配

此部分提供要求的验证步骤为了验证验证和角色分配。

在Web UI，对无线控制器的登录有**监视器**用户名和密码的：

用户验证，授权，并且分配到箴言报角色，在无线控制器提供只读访问。选择**Configuration>设备**，并且尝试编辑设备。

注意：因为用户是允许的只读访问，没有请编辑功能是可用的。

在设备的访问：(只**View按钮**是可用的;**删除按钮**是已变成灰色。)

在Web UI，对无线控制器的登录有**超级用户**用户名和密码的：

用户验证，授权，并且分配到超级用户角色，在无线控制器提供完全权限。选择**Configuration>设备**，并且尝试编辑设备。

注意：因为用户是在设备的允许的完全权限**编辑按钮**当前是可用的。

故障排除

在Cisco Secure ACS版本5.X，请导航对**监控，并且报告>启动监听&报告查看器>选择报告>目录>AAA协议> TACACS认证>Run**。

这提交所有合格的用户的结果和失败的认证并且包括失败原因。点击**放大镜**(详细信息)按钮关于更详细的资料。