

# ACS与WAAS配置示例的版本5.x集成

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[配置 ACS](#)

[在WAAS的配置](#)

[验证](#)

[故障排除](#)

## 简介

本文描述如何配置Cisco与Cisco访问控制服务器(ACS)版本5.x的广域应用服务(WAAS)集成。当配置每在本文的步骤，用户能验证到与TACACS+凭证的WAAS通过ACS。

## [先决条件](#)

### [要求](#)

本文档没有任何特定的要求。

### [使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- Cisco Secure ACS版本5.x
- Cisco WAAS

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

### 配置 ACS

1. 为了定义ACS版本5.x的一个AAA客户端，请导航给**网络资源>网络设备和AAA客户端**。配置AAA客户端用一描述性名称、单个IP地址和共享密钥TACACS+的。
2. 为了定义Shell配置文件，请导航到**策略元素>授权和权限>设备Administration > Shell配置文件**。在本例中，呼叫**WAAS\_Attribute**的一新的shell配置文件配置。此自定义属性发送对WAAS，允许它推断哪个用户组是管理员组。配置这些自定义属性：  
**属性是waas\_rbac\_groups。需求可选**，以便不干扰任何其它设备。**值是必须分配管理访问组的名称(实验小组)**。
3. 为了定义set命令允许所有命令，请导航对**策略元素>授权，并且权限>设备Administration >命令设置**。  
编辑**Permit\_All set命令**。如果检查**permit any命令**不在下表复选框，用户授权全双工权限。  
**Note:**因为此示例使用TACACS，选择的默认服务是**默认设备admin**。
4. 为了指向标识正确标识来源，请导航到**访问策略>Access Services>默认设备Admin >标识**。如果用户在本本地ACS数据库存在，请选择**内部用户**。如果用户在活动目录存在，请选择已配置的标识存储(在本例中的**AD1**)。
5. 为了创建授权规则，请导航到**访问策略>Access Services>默认设备Admin >授权**。创建呼叫**WAAS授权**的一项新的授权策略。这检查从WAAS的请求。在本例中，设备IP使用作为情况。然而，这可以更改根据部署需求。应用shell配置文件并且发出命令在此部分的步骤配置的集2和3。

## 在WAAS的配置

1. 为了定义TACACS+服务器，请导航到**设备> <Central管理器系统Name> >配置> Security >AAA > TACACS+**。配置ACS服务器IP地址和预先共享密钥。
2. 为了修改认证和授权方法，请导航到**设备> <Central管理器系统Name> >配置> Security >AAA >认证方法**。在此屏幕画面，主要的登录方法为与为TACACS+配置的第二的本地配置。
3. 导航给**霍姆> Admin >AAA >用户组**为了添加匹配自定义属性值的组名(请参阅在**配置ACS**部分的步骤2)在WAAS。
4. 分配在**霍姆> Admin >AAA**的此组(Test\_Group) **Admin级别>用户组角色管理**选项卡。预先配置在中央管理器的**admin**角色。

## 验证

尝试登录到与TACACS+凭证的WAAS。如果一切正确地配置，您是授权访问。

## 故障排除

目前没有针对此配置的故障排除信息。