

# ACS 5.x : 根据AD组成员配置示例和Authorization命令的TACACS+认证

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[配置认证和授权的ACS 5.x](#)

[配置认证和授权的Cisco IOS设备](#)

[验证](#)

[相关信息](#)

## 简介

本文提供配置根据用户的AD组成员和Authorization命令示例的TACACS+认证思科安全访问控制系统(ACS) 5.x和以后。ACS使用Microsoft Active Directory (AD)，外部标识存储资源例如用户、机器、组和属性。

## 先决条件

### 要求

尝试进行此配置之前，请确保满足以下要求：

- ACS 5.x充分地集成对希望的AD域。如果ACS没有集成与希望的AD域，参考[ACS 5.x和以后：与Microsoft Active Directory配置示例的集成](#)欲知更多信息为了执行集成任务。

### 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 5.3
- Cisco IOS软件版本12.2(44)SE6。注意：此配置在所有Cisco IOS设备可以被执行。
- Microsoft Windows服务器2003域

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

### 配置认证和授权的ACS 5.x

在您开始ACS 5.x的配置认证和授权的前，应该顺利地集成ACS与Microsoft AD。如果ACS没有集成与希望的AD域，参考[ACS 5.x和以后：与Microsoft Active Directory配置示例的集成](#)欲知更多信息为了执行集成任务。

在此部分，您映射两AD组对两不同命令集和两Shell配置文件，一与全部存取和其他与有限享用在Cisco IOS设备。

1. 使用Admin凭证，登录ACS GUI。
2. 选择用户，并且标识存储>外部标识存储>活动目录并且验证ACS加入希望的域并且连接状态显示如连接。点击目录组选项卡。
3. 单击选择。
4. 选择需要被映射到Shell配置文件并且发出命令集在配置的后部的组。单击 Ok。
5. 单击Save Changes。
6. 选择访问策略>Access Services>服务选择规则并且识别访问服务，处理TACACS+认证。在本例中，它是默认设备Admin。
7. 选择访问策略>Access Services>默认设备Admin >标识并且在标识来源旁边单击精选。
8. 选择AD1并且单击OK键。
9. 单击Save Changes。
10. 选择访问策略>Access Services>默认设备Admin >授权并且单击自定义。
11. 复制AD1:ExternalGroups从联机到自定义情况所选的部分然后移动Shell配置文件并且发出命令集从联机到自定义结果所选的部分。现在请单击 OK。
12. 单击创建为了创建新规则。
13. 单击精选在AD1:ExternalGroups情况。
14. 选择组您在Cisco IOS设备要提供完全权限。单击 Ok。
15. 在Shell配置文件字段单击精选。
16. 单击创建为了创建全部存取的用户的一新的Shell配置文件。
17. 提供名称和Description(optional)在常规选项卡并且单击普通的任务选项卡。
18. 更改默认权限和最大数量权限对与值15的静态。单击 submit。
19. 现在请选择新建立的全部存取的Shell配置文件(在本例中的FULL权限)并且单击OK键。
20. 在命令集字段单击精选。
21. 单击创建为了创建全部存取的用户的新命令集。
22. 提供一名称并且保证在permit any命令旁边的复选框不在下表的被检查。单击 submit。注意：  
：参考的[创建，复制和设备管理的editing命令集](#)关于命令集的更多信息。
23. 单击 Ok。
24. 单击 Ok。这完成Rule-1的配置。
25. 单击创建为了创建有限享用用户的一新规则。
26. 选择AD1:ExternalGroups并且单击精选。
27. 选择组(或)组您要提供有限访问对和单击OK键。
28. 在Shell配置文件字段单击精选。
29. 单击创建为了创建有限访问的一新的Shell配置文件。

30. 提供名称和Description(optional)在常规选项卡并且点击普通的任务选项卡。
31. 分别更改默认权限和最大数量权限对与值1和15的静态。单击 submit。
32. 单击 Ok。
33. 在命令集字段点击精选。
34. 单击创建创建有限享用组的新命令集。
35. 提供一名称并且保证在permit any命令旁边的复选框不在下表的没有选择。单击在键入以后添加显示在section命令提供的空间并且选择在授予部分的Permit，以便仅显示命令为用户在有限享用组中允许。
36. 同样请添加所有其他命令为用户允许在有使用的有限享用组中Add。单击 submit。注意：参考的[创建、复制和设备管理的editing命令集](#)关于命令集的更多信息。
37. 单击 Ok。
38. 单击 Ok。
39. 点击Save Changes。
40. 单击创建为了添加Cisco IOS设备作为ACS的一个AAA客户端。
41. 为TACACS+提供一名称，IP地址，共享塞克雷并且单击提交。

## 配置认证和授权的Cisco IOS设备

完成这些步骤为了配置Cisco IOS设备和ACS认证和授权的。

1. 创建一个本地用户有fallback的全双工权限用username命令如显示此处：  

```
username admin
privilege 15 password 0 cisco123!
```
2. 提供ACS的IP地址为了启用AAA和添加ACS 5.x作为TACACS服务器。aaa new-model  

```
tacacs-server host 192.168.26.51 key cisco123
```

**注意：** 密钥应该配比与在ACS提供的共享密钥为此Cisco IOS设备。
3. 测试与[测验的](#)TACACS服务器可接通性aaa命令如显示。  

```
test aaa group tacacs+ user1 xxxxx
legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

前面的命令的输出显示TACACS服务器可及的，并且用户顺利地验证。**注意：** User1和密码xxx属于AD。如果测试请失败请保证在上一步提供的共享密钥正确。
4. 配置登录并且启用认证然后请使用Exec和命令授权如显示此处：  

```
aaa authentication login
default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa authorization config-commands
```

**注意：** 如果TACACS服务器分别为不可得到的，本地和Enable (event)关键字使用对Cisco IOS本地用户和enable secret的fallback。

## 验证

为了验证认证和授权请登陆到Cisco IOS设备通过Telnet。

1. 远程登录到属于AD的全部存取的组的Cisco IOS设备作为user1。网络管理员组是被映射的FULL权限Shell配置文件和全部存取的Set命令在ACS AD的组。设法运行所有命令保证您有完全权限。
2. 远程登录到属于AD的有限享用组的Cisco IOS设备作为user2。(网络维护团队组是在ACS的被

映射的有限权限Shell配置文件和SHOW访问Set命令) AD的组。如果设法运行任何命令除在SHOW访问set命令提及的那个之外，您应该收到Authorization错误，显示该user2有有限访问。

3. 登陆对ACS GUI并且启动监听并且报告查看器。选择AAA协议> TACACS+Authorization为了验证user1和user2执行的活动。

## 相关信息

- [思科安全访问控制系统](#)
- [技术支持和文档 - Cisco Systems](#)