

ACS Shell 命令授权集在IOS和ASA/PIX/FWSM上的配置示例的

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[命令授权集](#)

[添加 Shell 命令授权集](#)

[情形 1：读写访问权限或完全访问权限](#)

[方案 2：只读访问权限](#)

[情形 3：受限访问权限](#)

[将 Shell 命令授权集与用户组关联](#)

[将 Shell 命令授权集 \(ReadWrite Access\) 与用户组 \(Admin Group\) 关联](#)

[将 Shell 命令授权集 \(ReadOnly Access\) 与用户组 \(Read-Only Group\) 关联](#)

[将 Shell 命令授权集 \(Restrict access\) 与用户关联](#)

[IOS 路由器配置](#)

[ASA/PIX/FWSM 配置](#)

[故障排除](#)

[Error:命令授权失败](#)

[相关信息](#)

简介

本文档介绍如何在Cisco安全访问控制服务器(ACS)中为AAA客户端(例如Cisco IOS®路由器或交换机)和Cisco安全设备(ASA/PIX/FWSM)配置外壳授权集，并将TACACS+作为授权协议。

注意：ACS Express不支持命令授权。

先决条件

要求

本文档假设 AAA 客户端和 ACS 中均已设置基本配置。

在ACS中，选择Interface Configuration > Advanced Options，并确保选中Per-user TACACS+/RADIUS Attributes复选框。

使用的组件

本文档中的信息基于运行软件版本 3.3 及更高版本的 Cisco 安全访问控制服务器 (ACS)。

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

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

命令授权集

命令授权集提供了一种中央控制机制，用于控制在任意给定网络设备上发出的每个命令的授权。此功能极大地增强了设置授权限制所需要的可扩展性和可管理性。

在 ACS 中，默认的命令授权集包括 Shell 命令授权集和 PIX 命令授权集。Cisco 设备管理应用程序 (例如 CiscoWorks Management Center for Firewalls) 可以指示 ACS 支持其他命令授权集类型。

注意：PIX 命令授权集要求 TACACS+ 命令授权请求将服务标识为 *pixshell*。请验证您的防火墙所使用的 PIX OS 版本中是否已实施此服务；如果没有，请使用 Shell 命令授权集为 PIX 设备执行命令授权。有关详细信息，请参阅 [为用户组配置 Shell 命令授权集](#)。

注意：从 PIX OS 版本 6.3 开始，尚未实施 *pixshell* 服务。

注意：思科安全设备 (ASA/PIX) 当前不允许用户在登录期间直接进入启用模式。用户必须手动进入启用模式。

为了更好地控制设备托管的 Telnet 管理会话，使用 TACACS+ 的网络设备可以请求对每个命令行进行授权然后再执行。您可以定义一组命令，允许或拒绝由给定设备上的特定用户执行。ACS 通过以下特性进一步增强了此功能：

- **Reusable Named Command Authorization Sets** — 无需直接引用任何用户或用户组，就可以创建一组命名命令授权。您可以定义多个命令授权集，描述不同的访问配置文件。例如：*Help desk* 命令授权集可允许访问高级浏览命令 (例如 *show run*) 并拒绝所有配置命令。*All network engineers* 命令授权集可包含一个有限列表，其中列出企业中任何网络工程师被允许使用的命令。*Local network engineers* 命令授权集可允许使用所有命令 (包括 IP 地址配置命令)。
- **Fine Configuration Granularity** — 您可以在命名命令授权集和网络设备组 (NDG) 之间创建关联。因此，可以根据用户访问的网络设备为其定义不同的访问配置文件。您可以将相同的命名命令授权集与多个 NDG 关联并将其用于多个用户组。ACS 加强了数据完整性。命名命令授权集保存在 ACS 内部数据库中。您可以使用 ACS 备份和恢复功能对其进行备份和恢复。也可以将命令授权集与其他配置数据一起复制到辅助 ACS。

对于支持 Cisco 设备管理应用程序的命令授权集类型而言，使用命令授权集时的优点类似。您可以将命令授权集应用到包含设备管理应用程序用户的 ACS 组，以便在设备管理应用程序中强制实施各种权限的授权。ACS 组可以对应设备管理应用程序中的不同角色，您可以根据情况对每个组应用不同的命令授权集。

ACS 的命令授权筛选有三个连续阶段。每个命令授权请求都将按照以下列出的顺序进行评估：

1. **命令匹配** — ACS 确定所处理的命令是否与命令授权集中列出的命令匹配。如果命令不匹配

，命令授权将由 Unmatched Commands 设置决定：*permit* 或 *deny*。否则，如果命令匹配，则评估继续。

2. **参数匹配** — ACS 确定显示的命令参数是否与命令授权集中列出的命令参数匹配。如果有任何参数不匹配，命令授权将根据 Permit Unmatched Args 选项是否启用来确定。如果允许存在不匹配的参数，则命令得到授权且评估结束；否则，命令将得不到授权且评估结束。如果所有参数都匹配，则评估继续。
3. **参数策略** — ACS 确定命令中的参数与命令授权集中的参数匹配后，ACS 将确定每个命令参数是否得到明确允许。如果所有参数都得到了明确允许，则 ACS 将予以命令授权。如果有任何参数未得到允许，ACS 将拒绝命令授权。

[添加 Shell 命令授权集](#)

本部分包括以下方案，介绍如何添加命令授权集：

- [情形 1：读写访问权限或完全访问权限](#)
- [方案 2：只读访问权限](#)
- [情形 3：受限访问权限](#)

注意：有关如何创建命令授权集的详细信息，请参阅[Cisco安全访问控制服务器4.1用户指南](#)的[添加命令授权集](#)部分。有关如何编辑和删除命令授权集的详细信息，请参阅[编辑命令授权集和删除命令授权集](#)。

[情形 1：读写访问权限或完全访问权限](#)

在本方案中，将授予用户读写（或完全）访问权限。

在 Shared Profile Components 窗口的 Shell Command Authorization Set 区域中，配置以下设置：

1. 在 Name 字段中输入 **ReadWriteAccess** 作为命令授权集的名称。
2. 在 Description 字段中输入对该命令授权集的说明。
3. 单击 **Permit** 单选按钮，然后单击 **Submit**。

Shared Profile Components

Edit

Shell Command Authorization Set

Name:

ReadWriteAccess

Description:

For Administrators etc
full access

Unmatched Commands:

Permit

Deny

Permit Unmatched Args

Add Command

Remove Command

[方案 2：只读访问权限](#)

在本方案中，用户仅可以使用 **show** 命令。

在 Shared Profile Components 窗口的 Shell Command Authorization Set 区域中，配置以下设置：

1. 在 Name 字段中输入 **ReadOnlyAccess** 作为命令授权集的名称。
2. 在 Description 字段中输入对该命令授权集的说明。
3. 单击 **Deny** 单选按钮。
4. 在 Add Command 按钮上方的字段中输入 **show** 命令，然后单击 Add Command。
5. 选中 **Permit Unmatched Args** 复选框，单击 Submit

Shared Profile Components

Edit

Shell Command Authorization Set

Name:

ReadOnlyAccess

Description:

Users are allowed to
run only show commands

Unmatched Commands:

Permit
 Deny

show

Permit Unmatched Args

Add Command

Remove Command

情形 3：受限访问权限

在此方案中，用户可以有选择性地使用一些命令。

在 Shared Profile Components 窗口的 Shell Command Authorization Set 区域中，配置以下设置：

1. 在 Name 字段中输入 **Restrict_access** 作为命令授权集的名称。
2. 单击 **Deny** 单选按钮。
3. 输入您希望在 AAA 客户端上允许使用的命令。在 Add Command 按钮上方的字段中输入 **show** 命令，单击 **Add Command**。

Shared Profile Components

Edit

Shell Command Authorization Set

Name:

Description:

Unmatched Commands:

Permit

Deny

Permit Unmatched Args

输入 configure 命令，单击 Add Command。选择 configure 命令，在右侧的字段中输入 permit terminal。

Shared Profile Components

Edit

Shell Command Authorization Set

Name:

Description:

Unmatched Commands: Permit
 Deny

Permit Unmatched Args

bandwidth	
configure	<input type="text" value="permit terminal"/>
description	
ethernet	
interface	
show	
timeout	

输入 interface 命令

, 单击 Add Command。选择 interface 命令，在右侧的字段中输入 permit Ethernet。

Shared Profile Components

Edit

Shell Command Authorization

Name:

Description:

Unmatched Commands: Permit Deny

Permit Unmatched Args

bandwidth
configure
description
ethernet
interface
show
timeout

输入 ethernet 命令，单击

Add Command。选择 interface 命令，在右侧的字段中输入 permit timeout、permit bandwidth 和 permit description。

Shell Command Authorization Set

Name:

Description:

Unmatched Commands: Permit Deny

Permit Unmatched Args

bandwidth
configure
description
ethernet
interface
show
timeout

输入 bandwidth 命令

，单击 Add Command。

Shared Profile Components

Edit

Shell Command Authorization Set

Name:

Description:

Unmatched Commands: Permit
 Deny

Permit Unmatched Args

bandwidth	
configure	
description	
ethernet	
interface	
show	
timeout	

输入 timeout 命令

, 单击 Add Command。

Shared Profile Components

Edit

Shell Command Authorization Set

Name:

Description:

Unmatched Commands:
 Permit
 Deny

Permit Unmatched Args

- bandwidth
- configure
- description
- ethernet
- interface
- show
- timeout**

输入 description

命令，单击 Add Command。

Shared Profile Components

Edit

Shell Command Authorization Set

Name:

Description:

Unmatched Commands:

Permit
 Deny

Permit Unmatched Args

4. 单击“Submit”。

将 Shell 命令授权集与用户组关联

有关如何为用户组配置shell命令授权集配置的详细信息，请参阅[Cisco安全访问控制服务器4.1用户指南](#)的[为用户组配置shell命令授权集](#)部分。

将 Shell 命令授权集 (ReadWrite Access) 与用户组 (Admin Group) 关联

1. 在 ACS 窗口中，单击 **Group Setup**，并从 Group 下拉列表中选择 Admin Group。

Group Setup

Select

Group:

2. 单击 **Edit Settings**。

3. 从 Jump To 下拉列表中选择 **Enable Options**。

4. 在 Enable Options 区域中，单击 Max Privilege for any AAA client 单选按钮，并从下拉列表中选择 Level 15。



The screenshot shows the 'Group Setup' configuration page. At the top, there is a 'Jump To' dropdown menu with 'Enable Options' selected. Below this, the 'Enable Options' section is visible, containing three radio button options: 'No Enable Privilege', 'Max Privilege for any AAA Client', and 'Define max Privilege on a per network device group basis'. The 'Max Privilege for any AAA Client' option is selected and highlighted with a red box. Below this option, there is a dropdown menu showing 'Level 15'. At the bottom of the page, there are two columns labeled 'Device Group' and 'Privilege'.

5. 从 Jump To 下拉列表中选择 TACACS+。
6. 在 TACACS+ Settings 区域中，选中 Shell (exec) 复选框和 Privilege level 复选框，并在 Privilege level 字段中输入 15。

Group Setup

Jump To TACACS+

TACACS+ Settings

PPP IP

In access control list

Out access control list

Route

Routing

Enabled

Note: PPP LCP will be automatically enabled if this service

Shell (exec)

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify

Enabled

No escape

Enabled

No hangup

Enabled

Privilege level

15

7. 在 Shell Command Authorization Set 区域中，单击 **Assign a Shell Command Authorization Set for any network device** 单选按钮，并从下拉列表中选择 **ReadWriteAccess**。

Group Setup

Jump To TACACS+ ▼

Privilege level

Timeout

Shell Command Authorization Set

None

Assign a Shell Command Authorization Set for any network device
 ▼

Assign a Shell Command Authorization Set on a per Network Device Group Basis

8. 单击 **Submit**

[将 Shell 命令授权集 \(ReadOnly Access\) 与用户组 \(Read-Only Group\) 关联](#)

1. 在 ACS 窗口中，单击 **Group Setup**，并从 Group 下拉列表中选择 Read-Only Group。

Group Setup

Select

Group : ▼

2. 单击 **Edit Settings**。

3. 从 Jump To 下拉列表中选择 **Enable Options**。

4. 在 Enable Options 区域中，单击 **Max Privilege for any AAA client** 单选按钮，并从下拉列表中选择 **Level 1**。

Group Setup

Jump To

Enable Options

No Enable Privilege

Max Privilege for any AAA Client

Define max Privilege on a per network device group basis

5. 在 TACACS+ Settings 区域中，选中 Shell (exec) 复选框和 Privilege level 复选框，并在 Privilege level 字段中输入 1。

Group Setup

Jump To TACACS+

TACACS+ Settings

PPP IP

In access control list

Out access control list

Route

Routing

Enabled

Note: PPP LCP will be automatically enabled if this service

Shell (exec)

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify

Enabled

No escape

Enabled

No hangup

Enabled

Privilege level

1

6. 在 Shell Command Authorization Set 区域中，单击 Assign a Shell Command Authorization Set for any network device 单选按钮，并从下拉列表中选择 ReadOnlyAccess。

The screenshot shows the 'Group Setup' configuration page. At the top, there is a 'Jump To' dropdown menu set to 'TACACS+'. Below this, the 'Shell Command Authorization Set' section is visible. It contains two radio button options: 'None' and 'Assign a Shell Command Authorization Set for any network'. The second option is selected and highlighted with a red box. Below this option is a dropdown menu with 'ReadOnlyAccess' selected.

7. 单击 **Submit**

将 Shell 命令授权集 (Restrict access) 与用户关联

有关如何为用户配置shell命令授权集配置的详细信息，请参阅[Cisco安全访问控制服务器4.1用户指南](#)的[为用户配置shell命令授权集](#)部分。

注意：用户级设置会覆盖ACS中的组级设置，这意味着如果用户在用户级设置中设置了shell命令授权，则它会覆盖组级设置。

1. 单击 **User Setup > Add/Edit**，创建一个名为 *Admin_user* 的新用户作为 *Admin* 组的一部分。

User Setup

Edit

User: Admin_user (New User)

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

2. 从 group to which the user is assigned 下拉列表中选择 **Admin Group**。

User Setup

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

3. 在 Shell Command Authorization Set 区域中，单击 **Assign a Shell Command Authorization Set for any network device** 单选按钮，并从下拉列表中选择 **Restrict_access**。注意：在此场景中，此用户是管理员组的一部分。*Restrict_access Shell* 授权集可应用；*ReadWrite Access Shell* 授权集不可应用。

User Setup

Idle time
 No callback verify Enabled
 No escape Enabled
 No hangup Enabled
 Privilege level
 Timeout

Shell Command Authorization Set

None
 As Group
 Assign a Shell Command Authorization Set for any network device
 Assign a Shell Command Authorization Set on a per Network Device Group Basis

注意：在Interface Configuration区域的TACACS+(Cisco)部分，确保在User列中选择了Shell(exec)选项。

IOS 路由器配置

除了预设的配置之外，还需要在 IOS 路由器或交换机上使用以下命令才能通过 ACS 服务器实施命令授权：

```

aaa new-model
aaa authorization config-commands
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
tacacs-server host 10.1.1.1
tacacs-server key cisco123

```

ASA/PIX/FWSM 配置

除了预设的配置之外，还需要在 ASA/PIX/FWSM 上使用以下命令才能通过 ACS 服务器实施命令授权：

```

aaa-server authserver protocol tacacs+
aaa-server authserver host 10.1.1.1
aaa authorization command authserver

```

注意：无法使用RADIUS协议来限制用户访问ASDM以只读目的。由于RADIUS数据包同时包含身份验证和授权，因此在RADIUS服务器中身份验证的所有用户都具有15级权限。您可以通过执行命令

授权集通过TACACS实现此功能。

注意：即使ACS无法执行命令授权，ASA/PIX/FWSM也会花费很长时间来执行键入的每个命令。如果ACS不可用且ASA配置了命令授权，ASA仍会为每个命令请求命令授权。

[故障排除](#)

[Error:命令授权失败](#)

问题

通过TACACS日志记录登录到防火墙后，命令不起作用。当您输入命令时，会收到以下错误：

解决方案

要解决此问题，请执行以下步骤：

1. 确保使用了正确的用户名，且所有所需权限都已分配给用户。
2. 如果用户名和权限正确，请验证ASA与ACS具有连接并且ACS处于活动状态。

注意：如果管理员错误地为本地和TACACS用户配置了命令授权，也会发生此错误。在这种情况下，请执行密码恢复以解决问题。

[相关信息](#)

- [Cisco PIX 防火墙软件](#)
- [Cisco Secure PIX 防火墙命令参考](#)
- [安全产品 Field Notices \(包括 PIX \)](#)
- [请求注解 \(RFC\)](#)
- [Cisco 安全控制访问控制服务器支持页](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。