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

目录

简介

本文描述如何配置在思科安全访问控制服务器(ACS)的shell授权集AAA客户端的，例如Cisco IOS路由器或交换机和Cisco安全伊莱克斯(ASA/PIX/FWSM)有TACACS+的作为授权协议。

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，请选择**Interface Configuration > Advanced Options**，并且保证**每用户TACACS+/RADIUS属性**复选框被检查。

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

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： 截至 PIX OS 版本 6.3，pixshell 服务尚未实施。

注意： Cisco安全设备(ASA/PIX)当前不允许将被放置的用户直接地到特权模式在登录期间。用户必须手工开始特权模式。

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

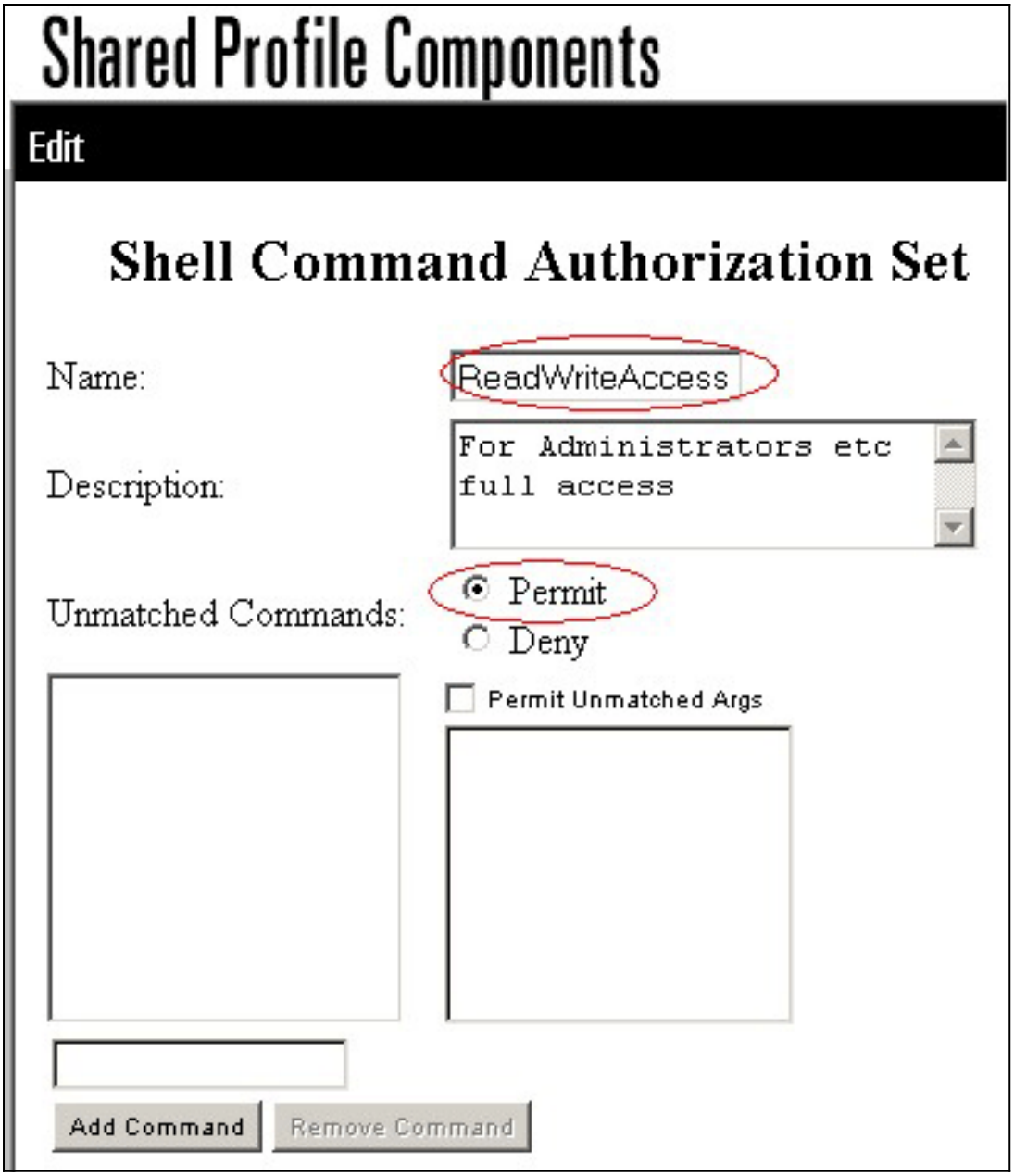
注意： 有关如何创建命令授权集的详细信息，请参阅 Cisco 安全访问控制服务器 4.1 用户指南的添加命令授权集部分。有关如何编辑和删除命令授权集的详细信息，请参阅编辑命令授权集和删除命令授权集。

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。

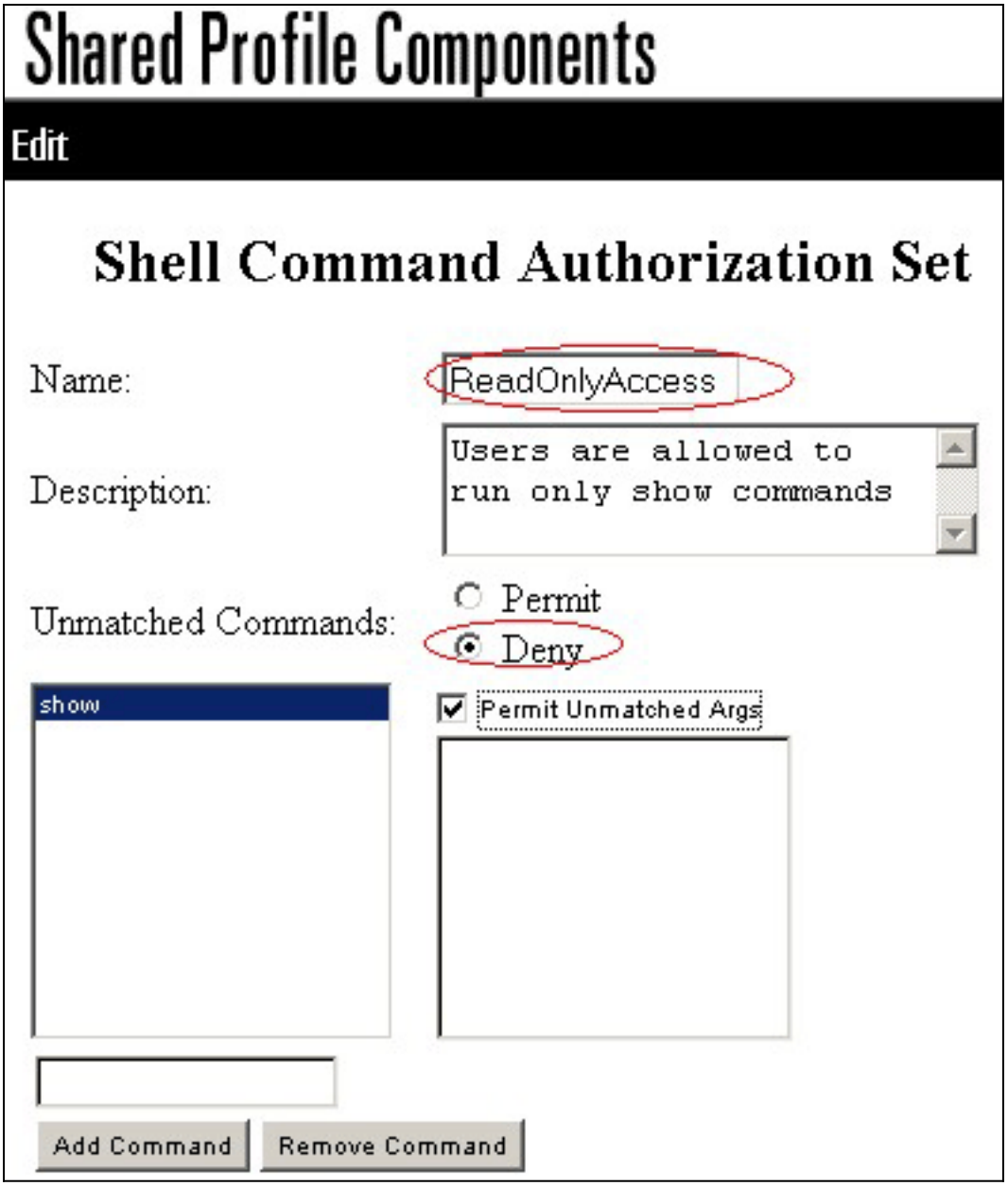


方案 2：只读访问权限

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

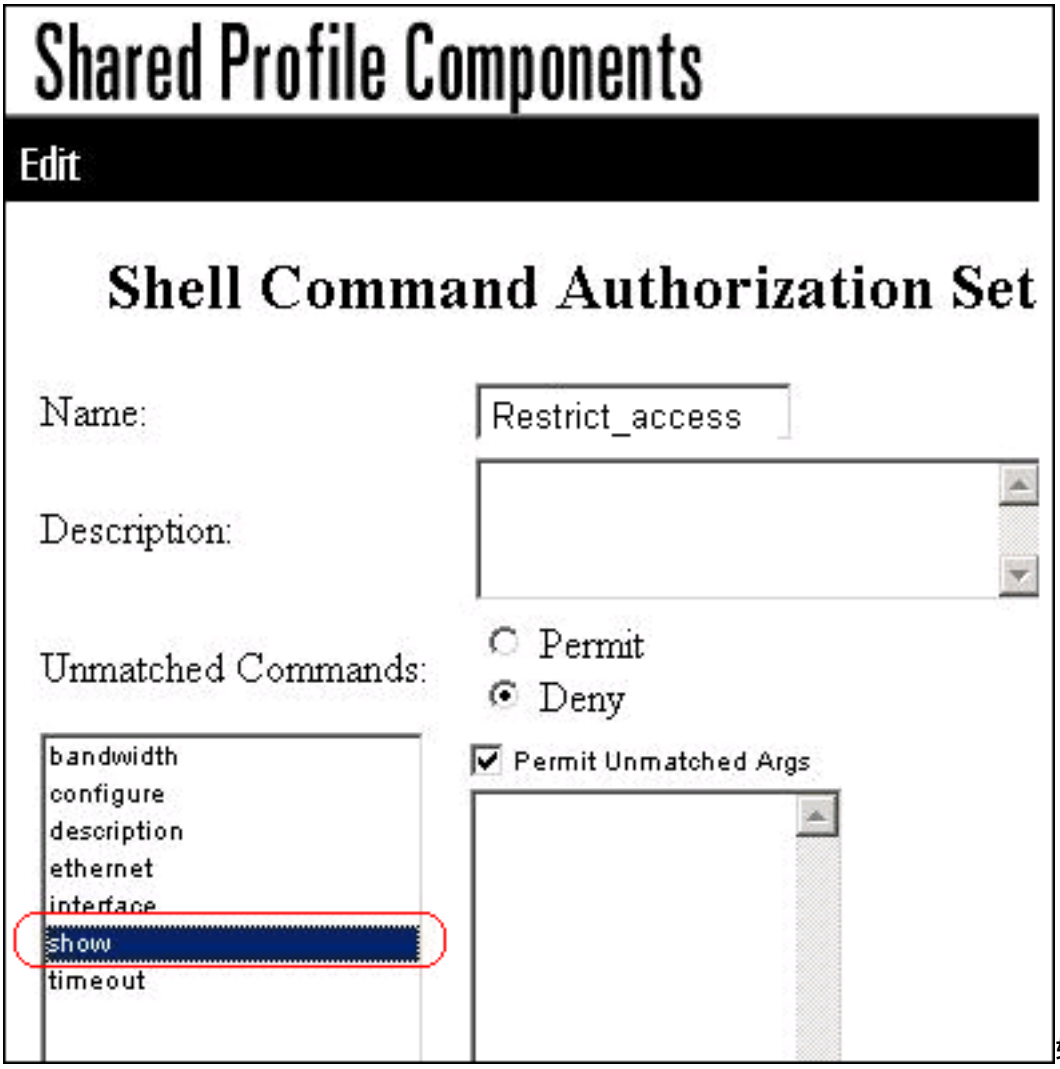


情形 3：受限访问权限

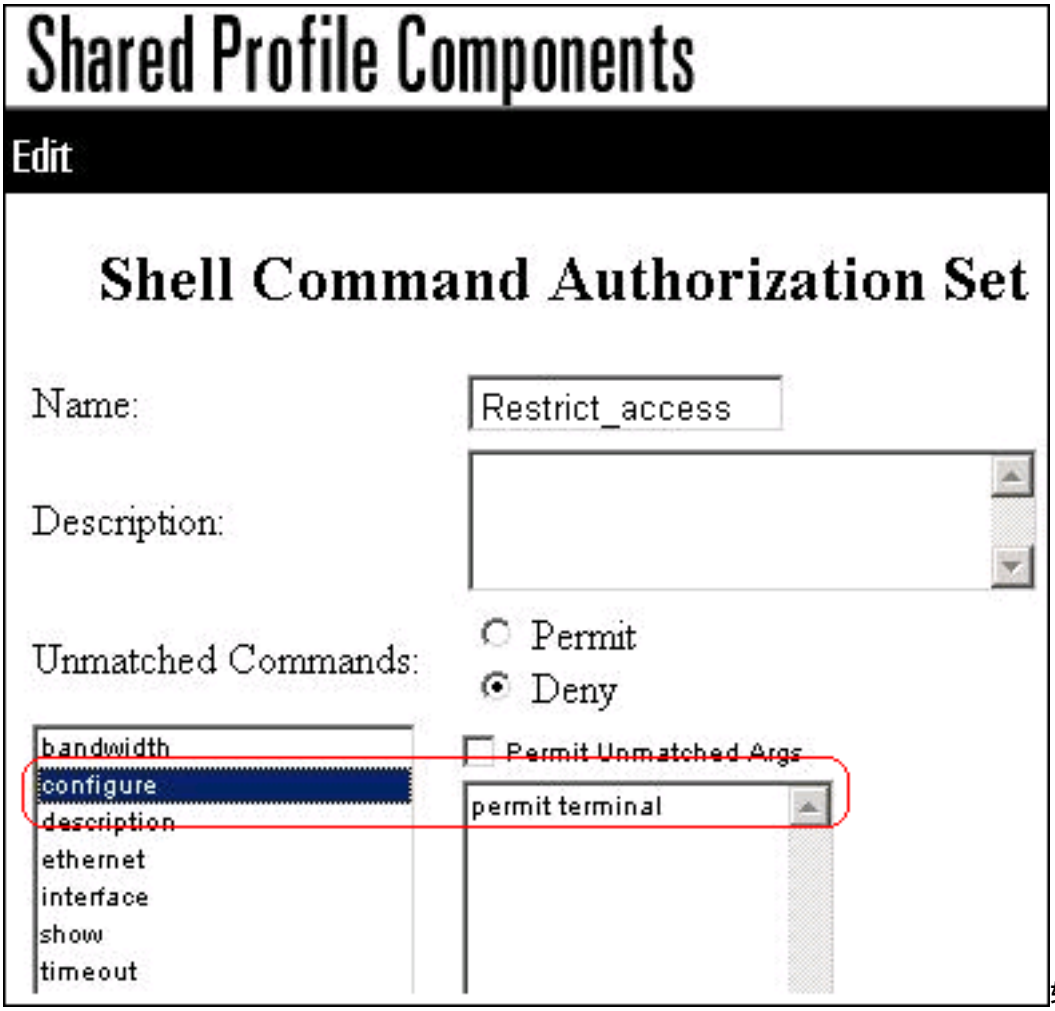
在此方案中，用户可以有选择性地使用一些命令。

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

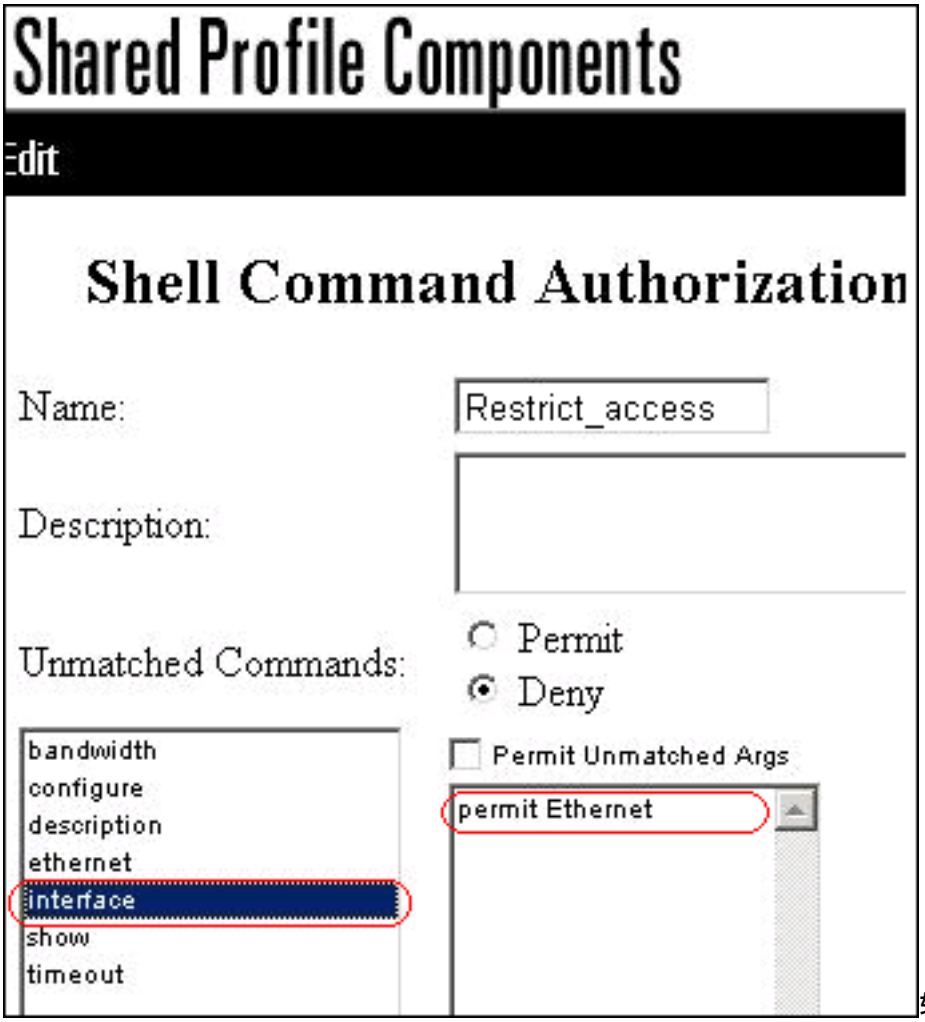
1. 在 Name 字段中输入 **Restrict_access** 作为命令授权集的名称。
2. 单击 **Deny** 单选按钮。
3. 输入您希望在 AAA 客户端上允许使用的命令。在 Add Command 按钮上方的字段中输入 **show** 命令，单击 Add Command。



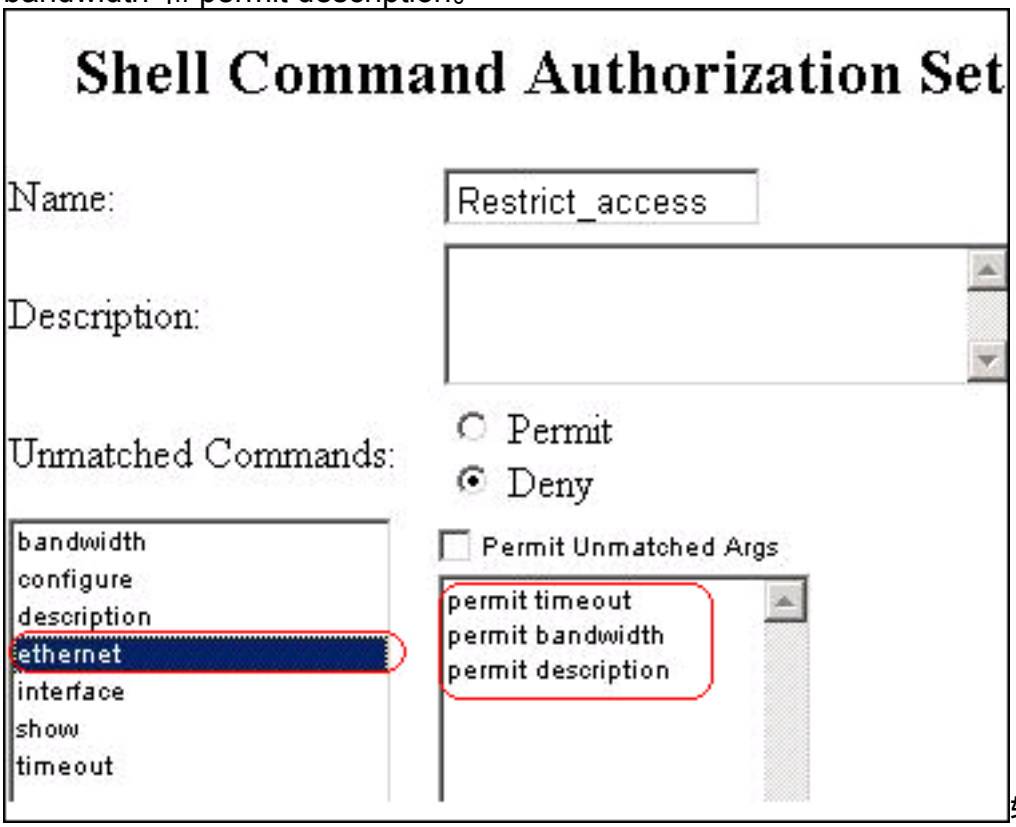
输入 **configure** 命令，单击 Add Command。选择 **configure** 命令，在右侧的字段中输入 permit terminal。



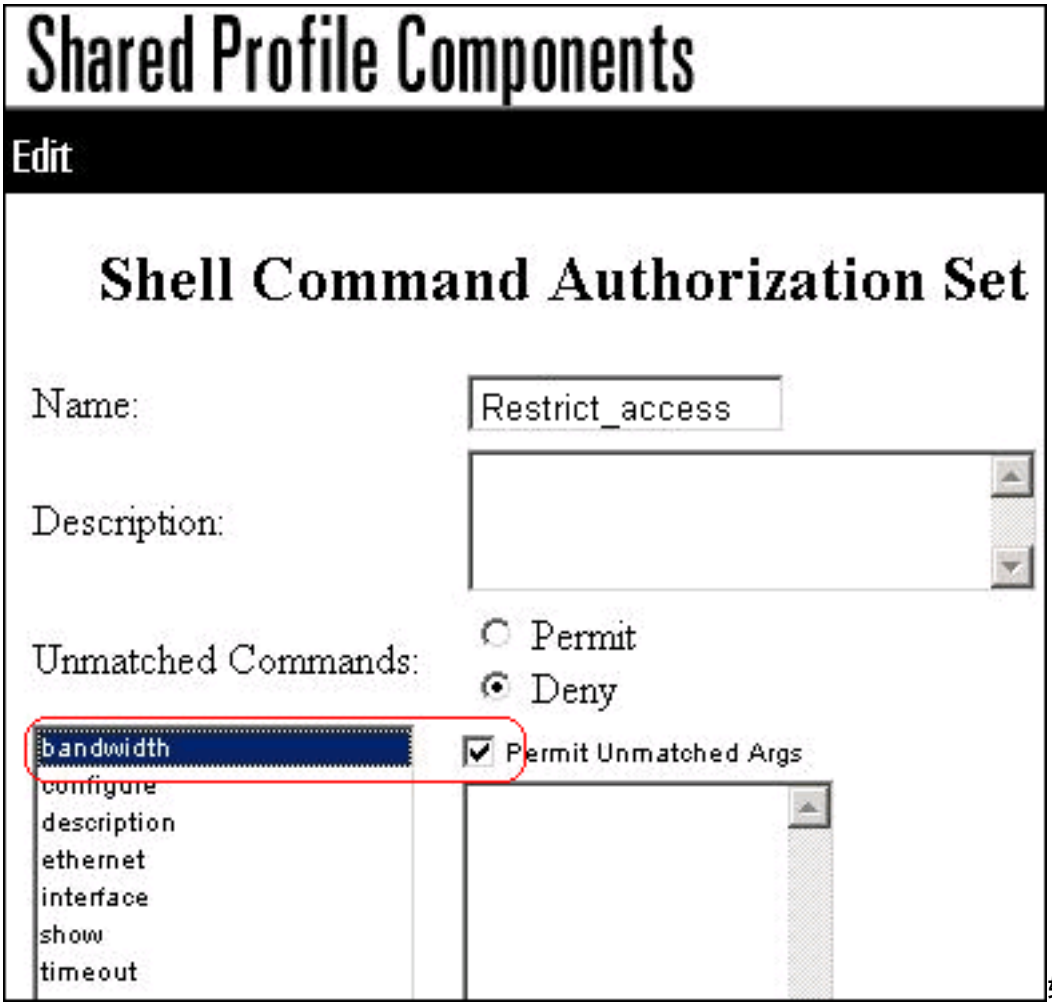
输入 **interface** 命令，单击 Add Command。选择 **interface** 命令，在右侧的字段中输入 permit Ethernet。



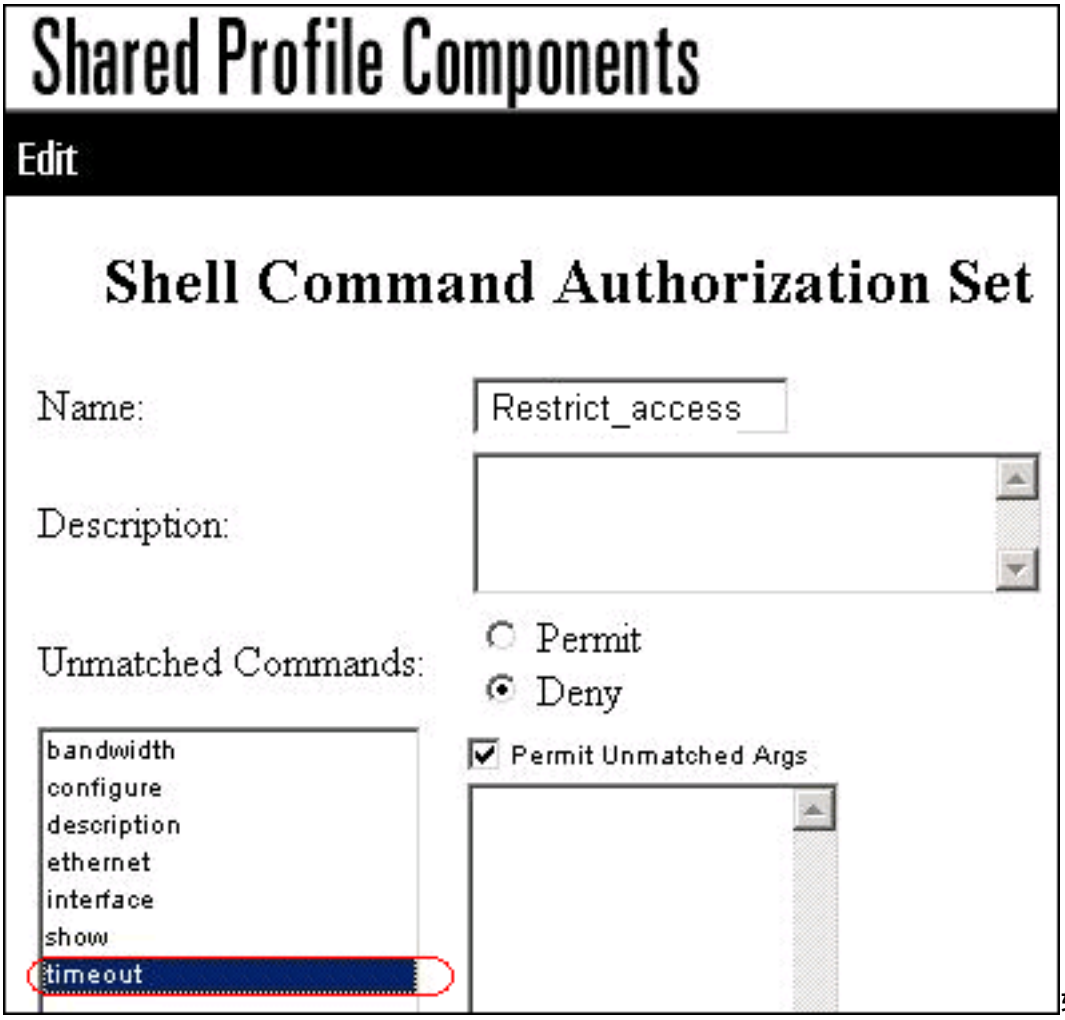
输入 **ethernet** 命令，单击 Add Command。选择 **interface** 命令，在右侧的字段中输入 permit timeout、permit bandwidth 和 permit description。



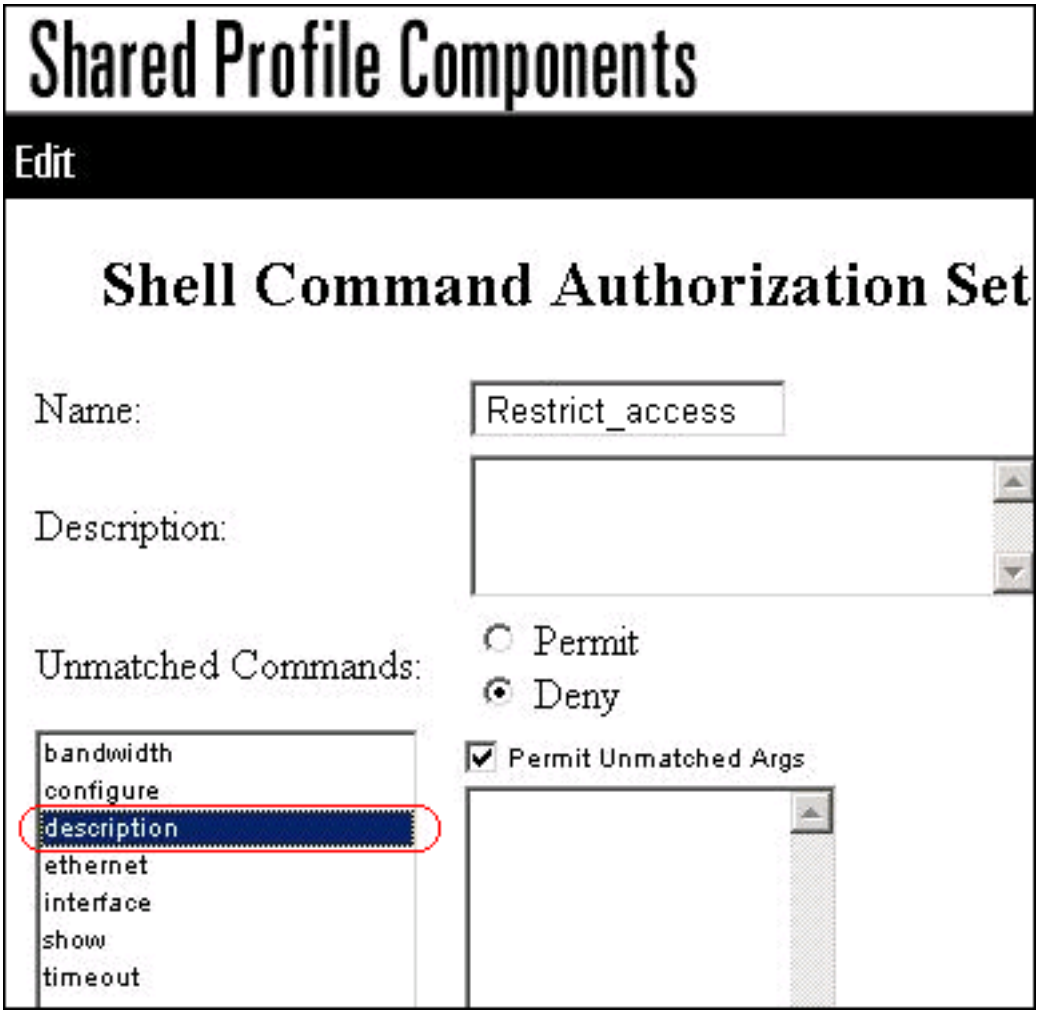
输入 **bandwidth** 命令，单击 Add Command。



输入 **timeout** 命令，单击 Add Command。



输入 **description** 命令，单击 Add Command。



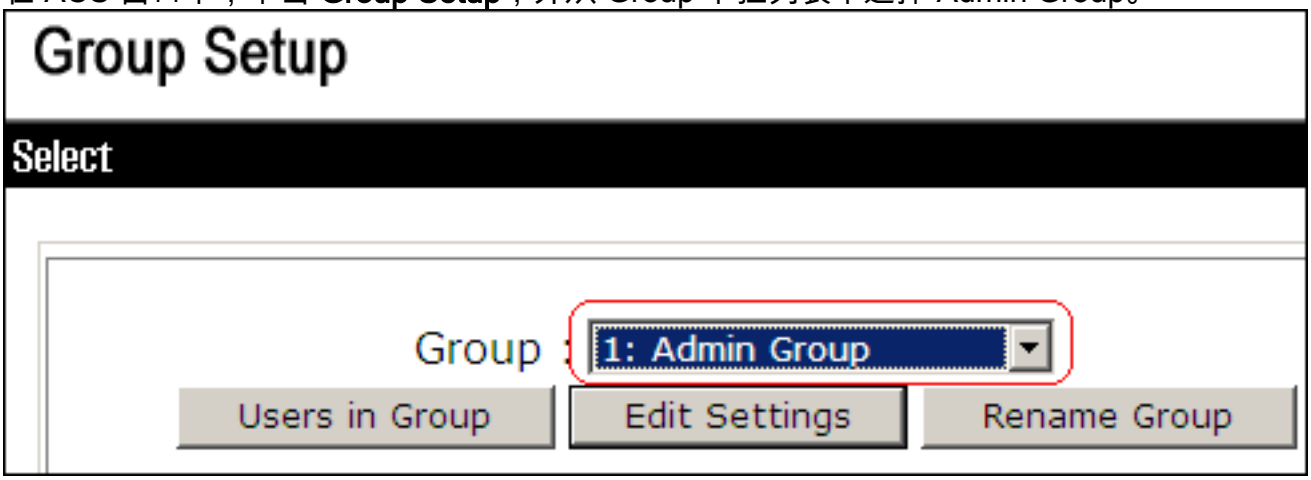
4. 单击 **submit**。

将 Shell 命令授权集与用户组关联

参考配置为用户指南的用户组部分设置的一个shell命令授权思科安全访问控制服务器的4.1关于如何配置用户组的shell命令授权集合配置的更多信息。

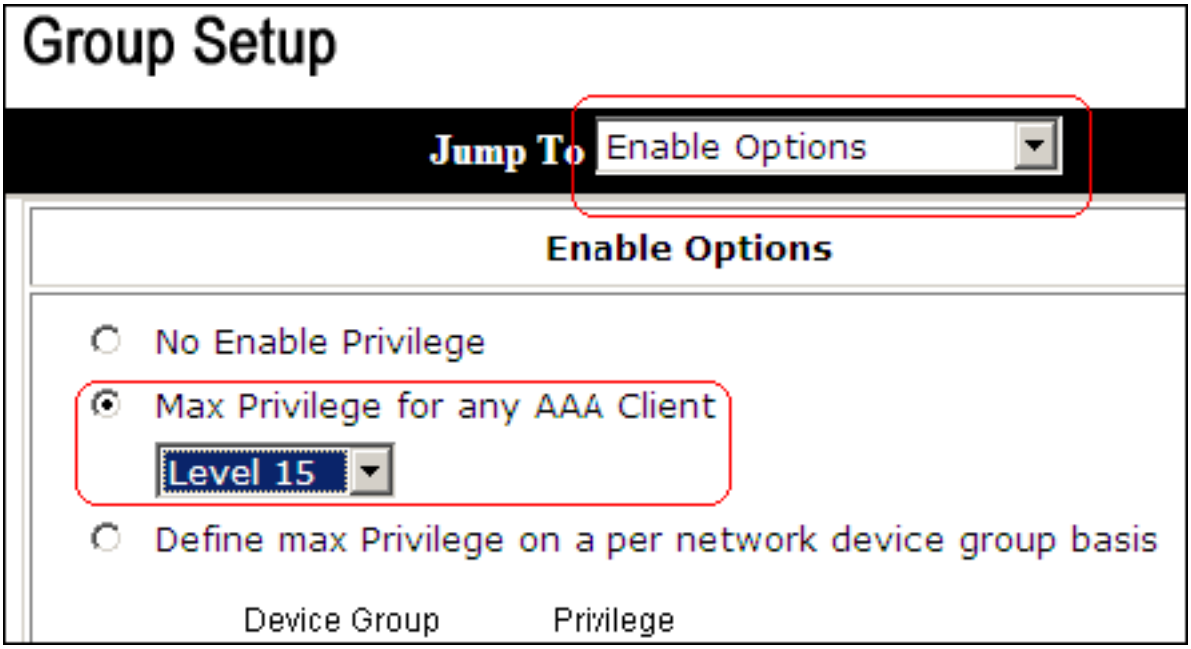
将 Shell 命令授权集 (ReadWrite Access) 与用户组 (Admin Group) 关联

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

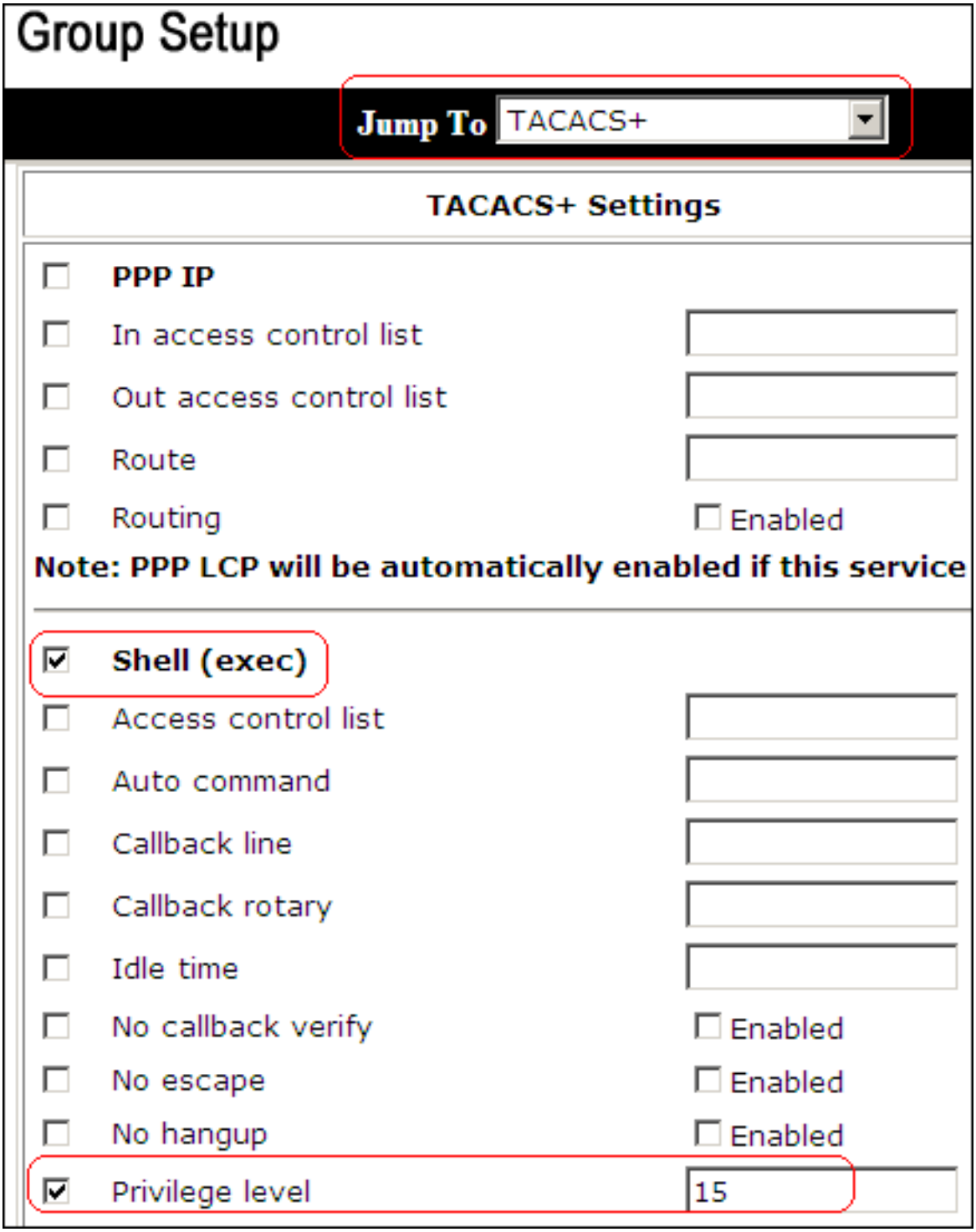


2. 单击 **Edit Settings**。
3. 从 Jump To 下拉列表中选择 **Enable Options**。

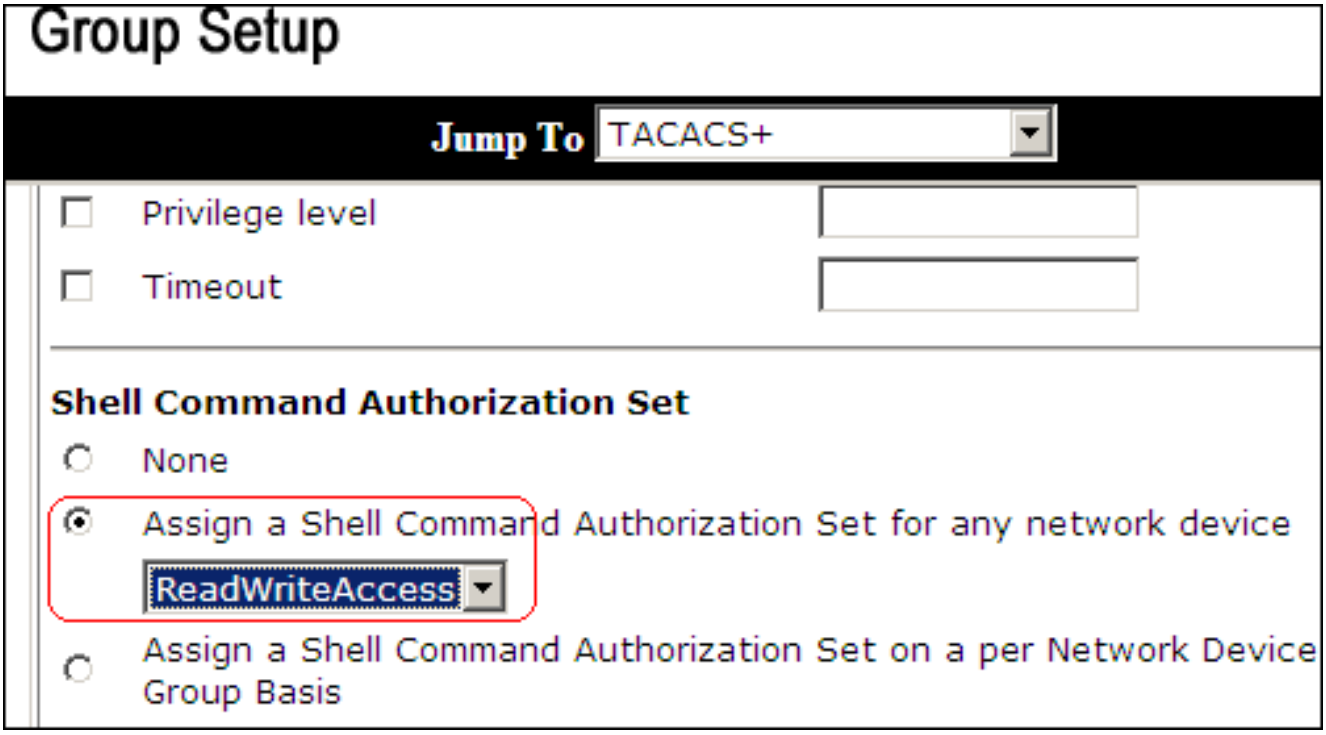
4. 在 Enable Options 区域中，单击 **Max Privilege for any AAA client** 单选按钮，并从下拉列表中选择 Level 15。



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。



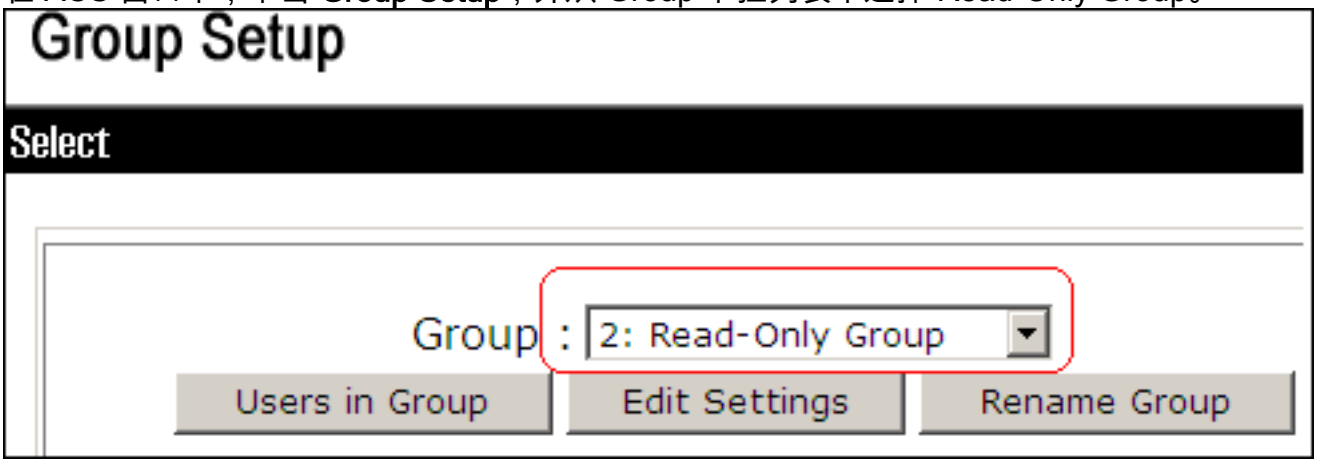
7. 在 Shell Command Authorization Set 区域中，单击 **Assign a Shell Command Authorization Set for any network device** 单选按钮，并从下拉列表中选择 ReadWriteAccess。



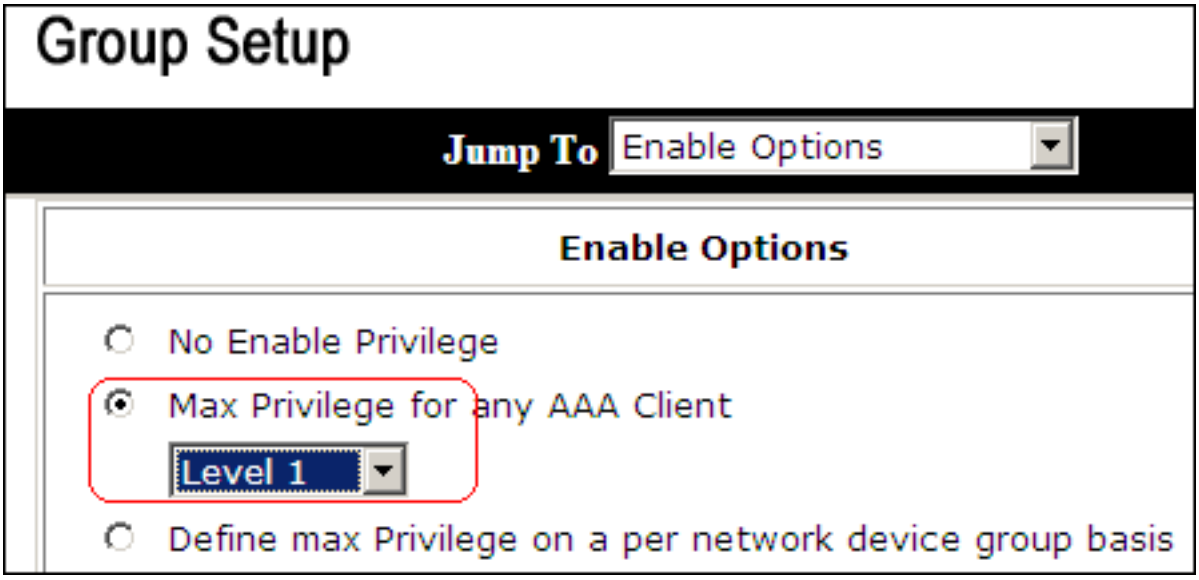
8. 单击 **Submit**

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

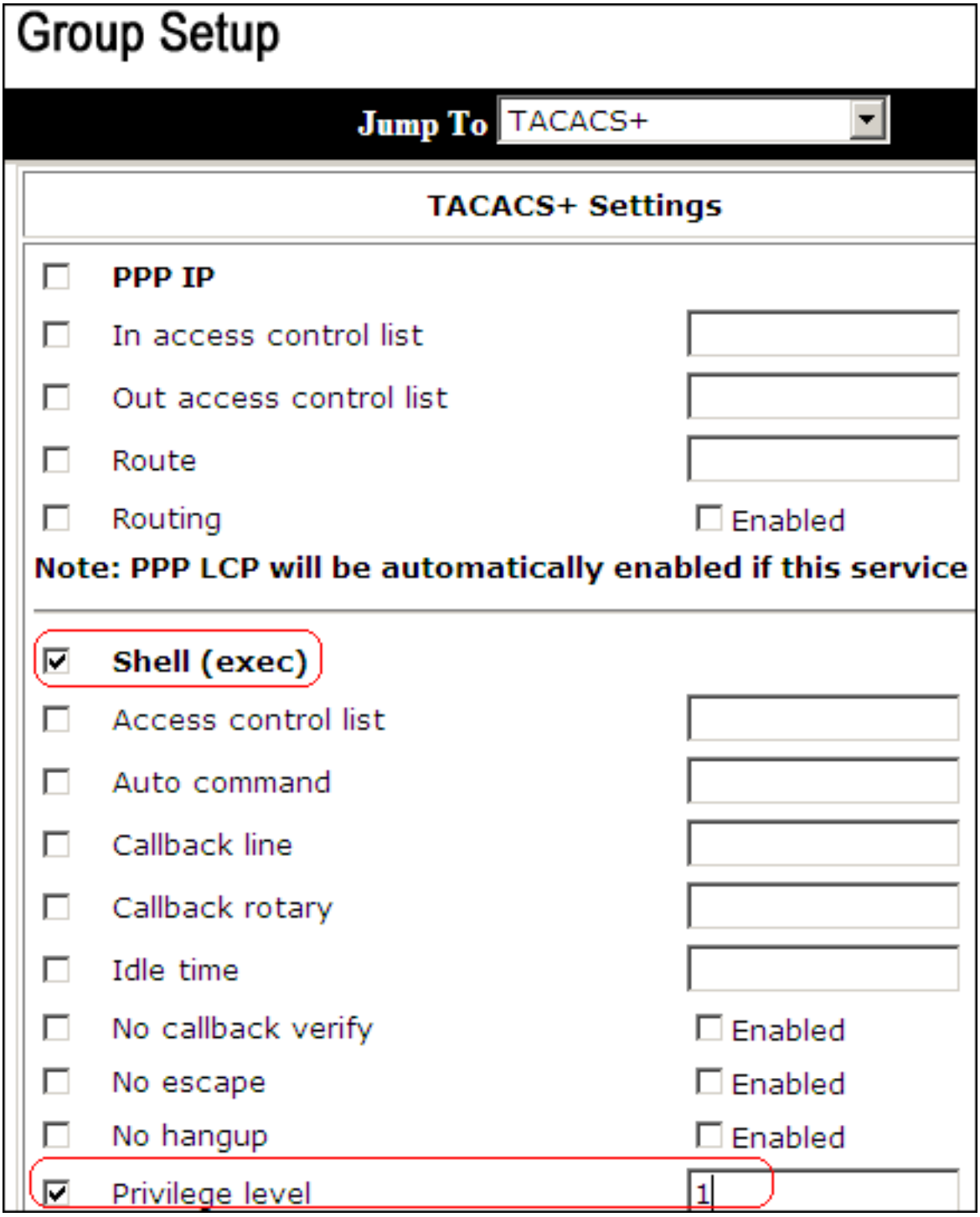
1. 在 ACS 窗口中，单击 **Group Setup**，并从 Group 下拉列表中选择 Read-Only Group。



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。



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。



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。

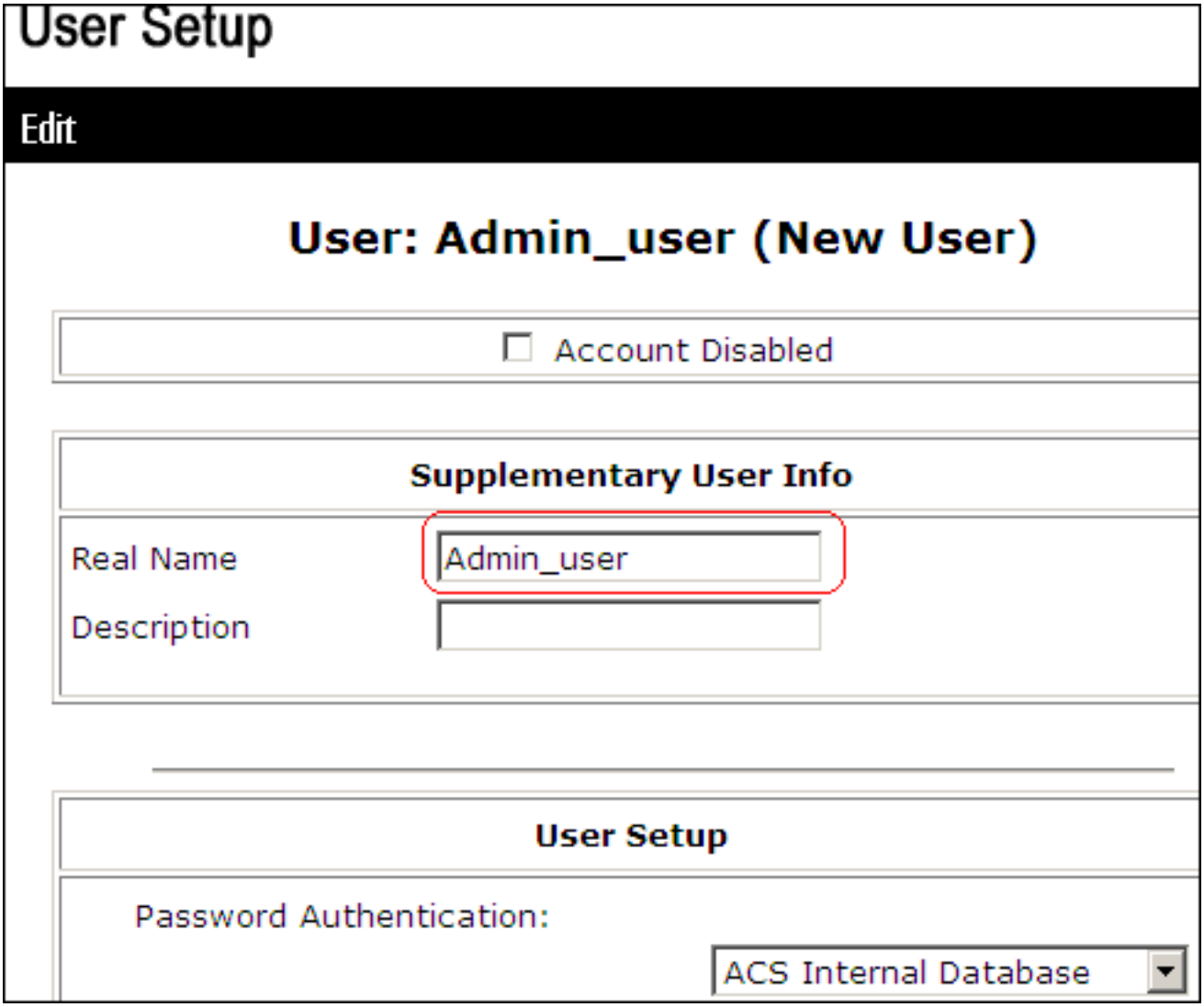
7. 单击 **Submit**

将 Shell 命令授权集 (Restrict_access) 与用户关联

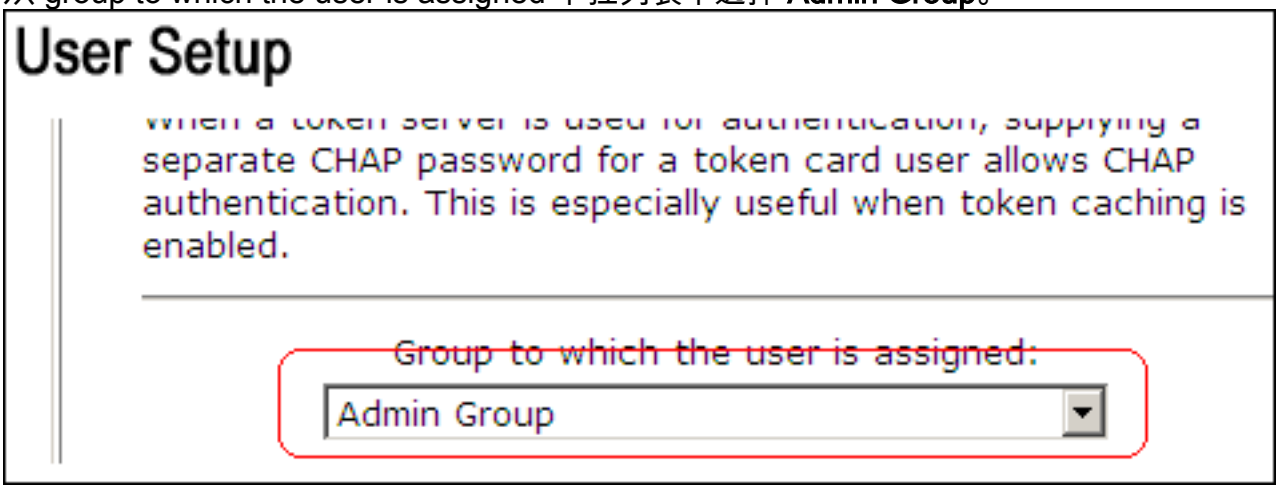
参考配置为用户指南的用户部分设置的一个shell命令授权思科安全访问控制服务器的4.1关于如何配置用户的shell命令授权集合配置的更多信息。

注意： ACS 中的用户级设置将覆盖组级设置，也就是说，如果用户在用户级设置中有 Shell 命令授权集，则它将覆盖组级设置。

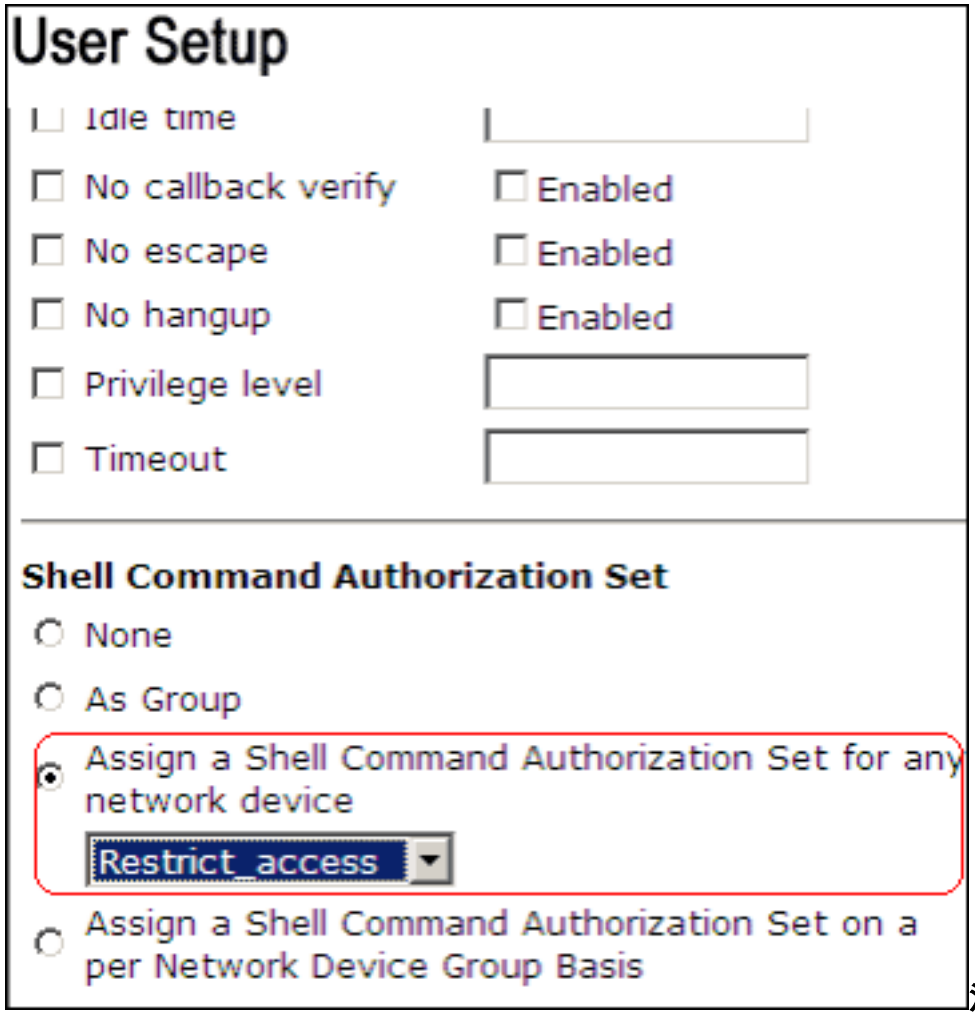
1. 单击 **User Setup > Add/Edit**，创建一个名为 *Admin_user* 的新用户作为 Admin 组的一部分。



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



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：** 在此方案中，该用户属于 Admin Group。*Restrict_access* Shell 授权集可应用；*ReadWrite Access* Shell 授权集不可应用。



注意： 在 Interface Configuration 区域的 TACACS+ (Cisco) 部分中，请确保 User 列中的 **Shell (exec)** 选项已选中。

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： 使用RADIUS协议为了限制对ASDM的用户访问只读目的是不可能的。因为RADIUS信息包同时包含认证和授权，在RADIUS服务器验证的所有用户有权限级别15。您能通过与authorization命令集的实施的TACACS达到此。

注意： ASA/PIX/FWSM需要很长时间执行被键入的每命令，即使ACS是不可用执行authorization命令。如果ACS不可用，并且ASA有配置的authorization命令， ASA将请求每命令的authorization命令。

故障排除

Error:失败的authorization命令

问题

在您登陆对防火墙通过记录后的TACACS，命令不运作。当您输入命令时，此错误接收：
`authorization。`

解决方案

要解决此问题，请执行以下步骤：

1. 保证正确用户名使用，并且全部必需权限分配到用户。
2. 如果用户名和权限正确，请验证ASA有与ACS的连接，并且ACS是活跃的。

注意： 此错误能也出现，如果本地的管理员错误地配置命令授权，以及TACACS，用户。在这种情况下，请执行密码恢复为了解决问题。

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