

5760个Web接口权限级别根据与思科访问控制服务器(ACS)的访问控制配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[创建ACS的一些个测试用户](#)

[设置策略元素和shell配置文件](#)

[创建权限15级别shell访问配置文件](#)

[创建管理员用户的命令集](#)

[创建只读用户的shell配置文件](#)

[创建服务选择规则匹配TACACS协议](#)

[创建全双工管理访问的授权策略。](#)

[创建只读管理访问的授权策略。](#)

[配置5760 TACACS的](#)

[访问同样5760与2不同的配置文件](#)

[相关的思科支持社区讨论](#)

简介

本文将解释如何创建Cisco ACS TACACS+认证和授权配置文件用不同的权限级别和集成它与5760访问的对WebUI。此功能从3.6.3向前支持(但是不在此文字的时期的3.7.x)。

先决条件

要求

假设，读者熟悉Cisco ACS和聚合的访问控制器配置。在TACACS+授权的范围内，本文只着重那些2个组件之间的交互作用。

使用的组件

本文档中的信息基于以下软件和硬件版本：

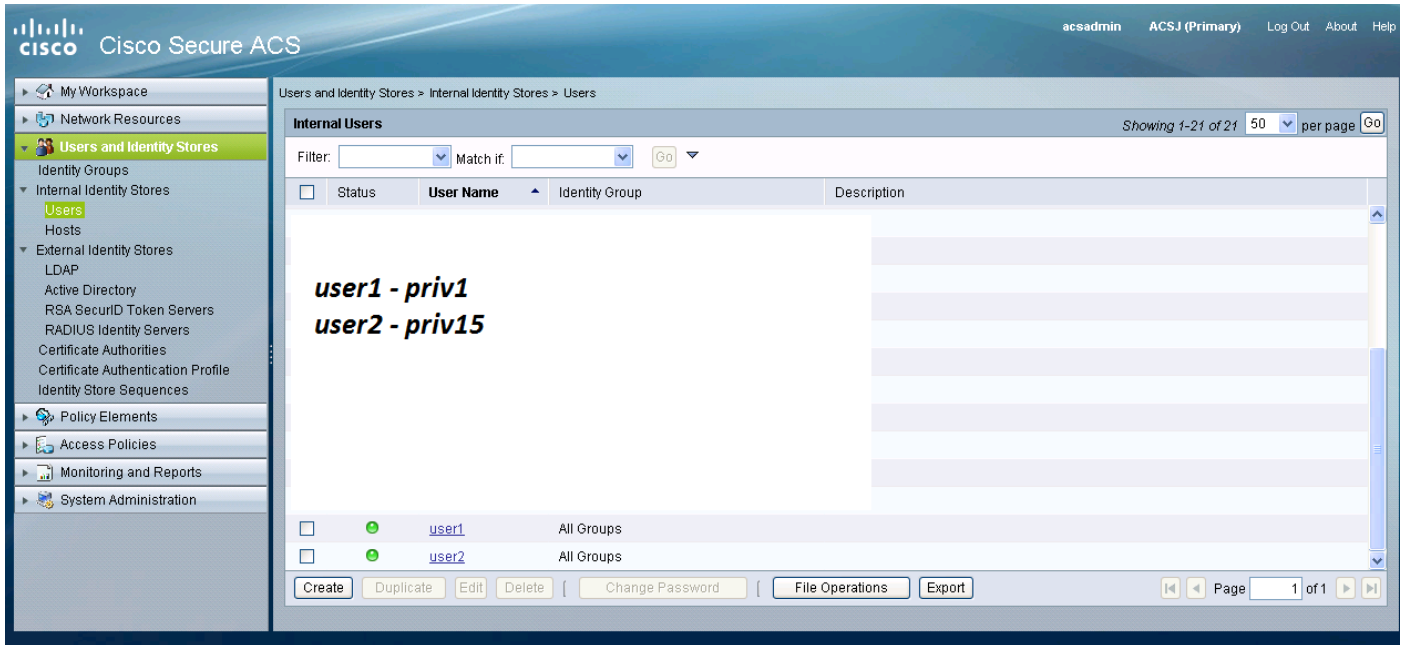
- 思科聚合访问5760，版本3.6.3
- 思科Access控制服务器(ACS) 5.2

配置

创建ACS的一些个测试用户

点击“用户，并且标识存储”，然后选择"Users"。

下面点击"Create"并且配置一些个测试用户例如图示。



设置策略元素和shell配置文件

您需要创建2不同种类的2配置文件的访问。在Cisco TACACS世界的权限15含义提供对设备的完全权限，不用任何限制。另一方面权限1将允许您登陆和执行仅有限的命令。下面cisco访问提供的级别的简短的说明。

权限级别 1 = 无特权（提示符是 router>），这是登录的默认级别

权限级别 15 = 有特权（提示符是 router#），这是进入启用模式后的级别

权限级别 0 = 很少使用，但包括 5 个命令：**disable**、**enable**、**exit**、**help** 和 **logout**

在5760，级别2-14被认为同1级一样。他们给权限和1.一样。**请勿配置某些on命令的TACACS权限级别5760**。5760年不支持每选项卡的UI访问。您能得以进入对箴言报选项卡(priv1)的仅完全权限(priv15)或。并且，有权限级别的0用户没有alowed登录。

创建权限15级别shell访问配置文件

使用下面的打印屏幕请创建该配置文件：

点击“策略元素”。点击“Shell配置文件”。

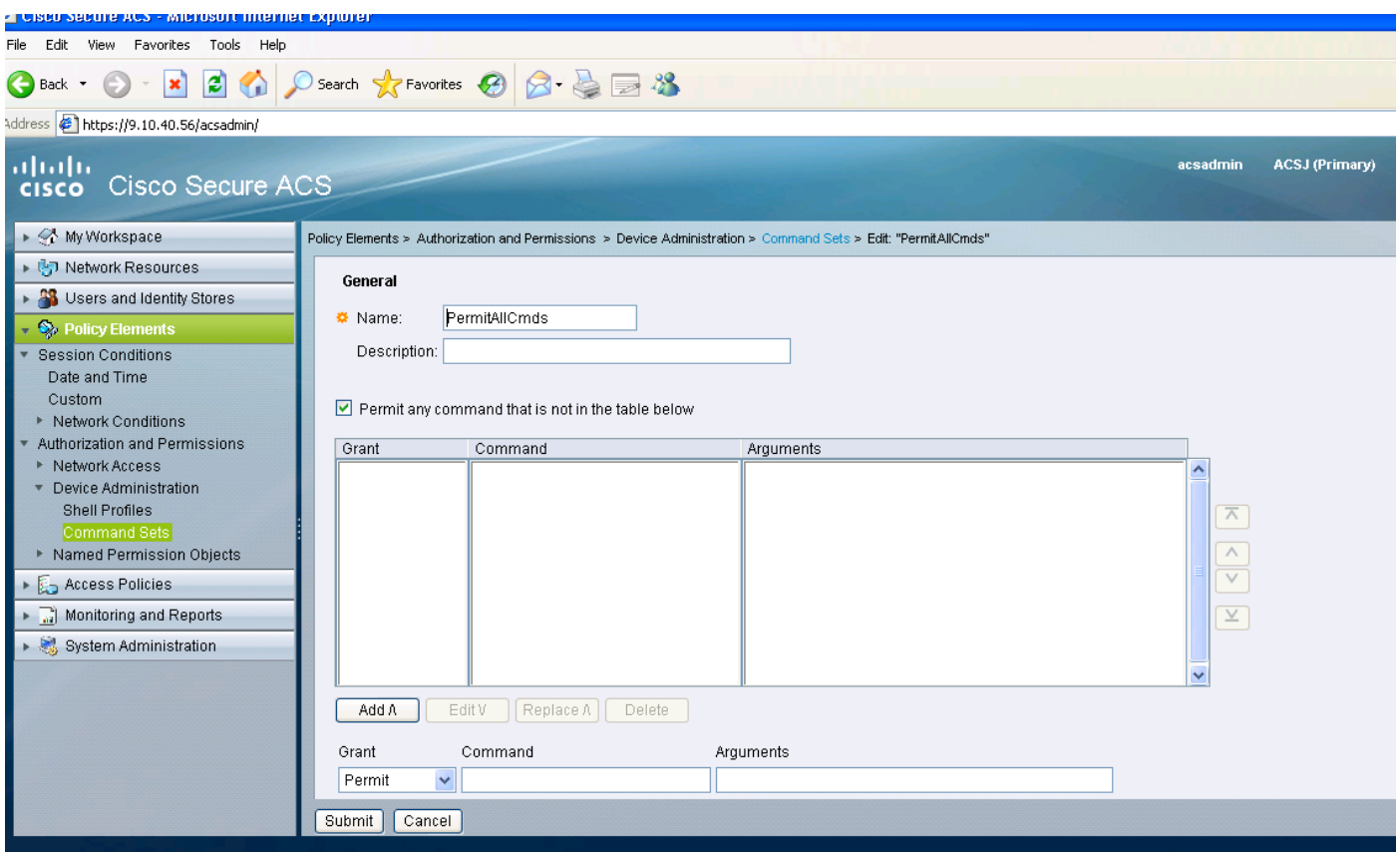
创建新的。

进来在“普通的任务”选项卡并且设置默认和最大值权限级别到15。



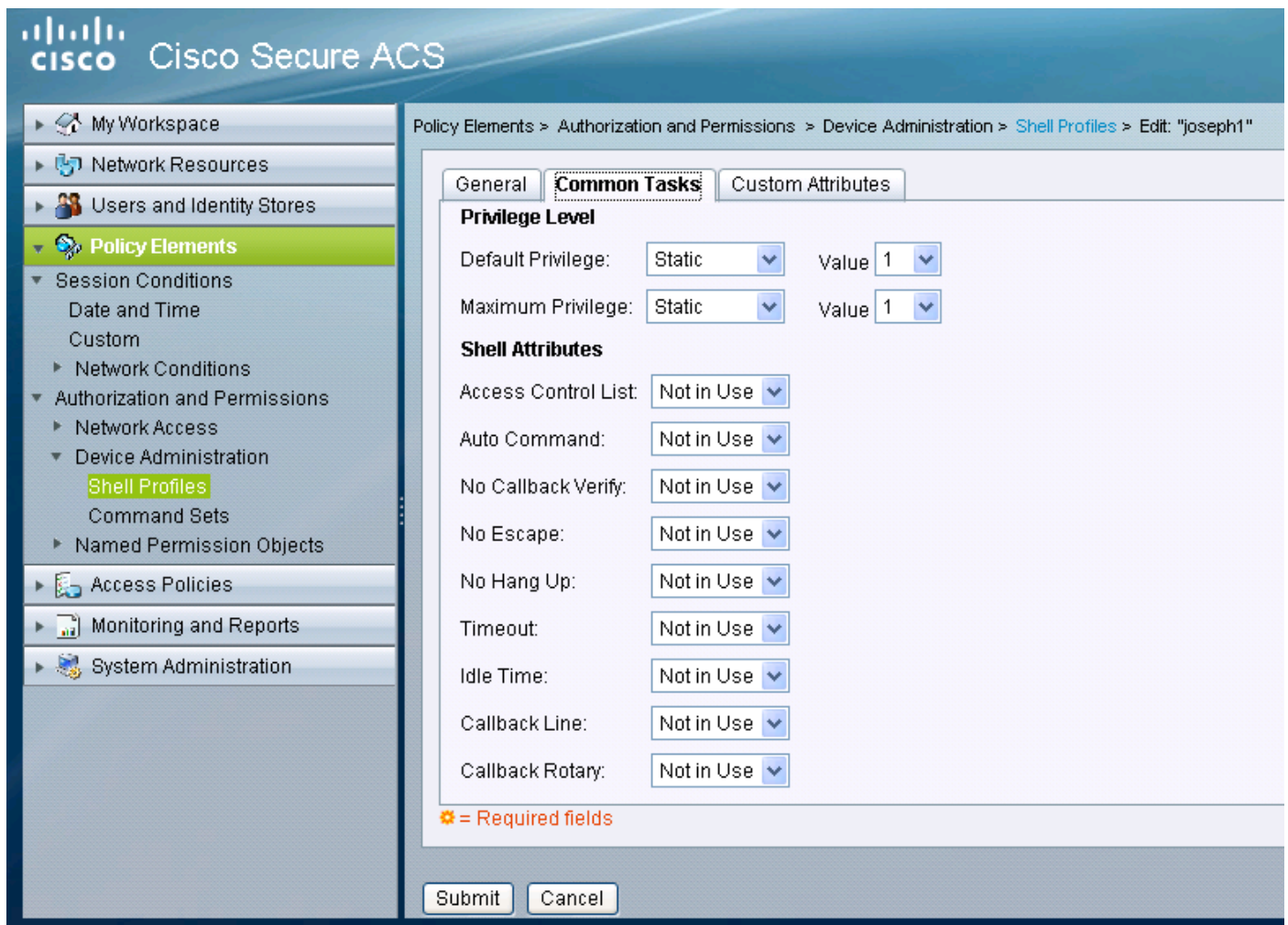
创建管理员用户的命令集

命令集是所有TACACS设备使用的一组命令。他们可以用于限制用户允许使用，如果已分配特定配置文件的命令。因为在5760，限制在根据权限级别的Webui代码完成通过，命令为两权限1级设置，并且15是相同的。



创建只读用户的shell配置文件

创建只读用户的另一shell配置文件。此配置文件将由权限级别设置到1的事实有所不同。

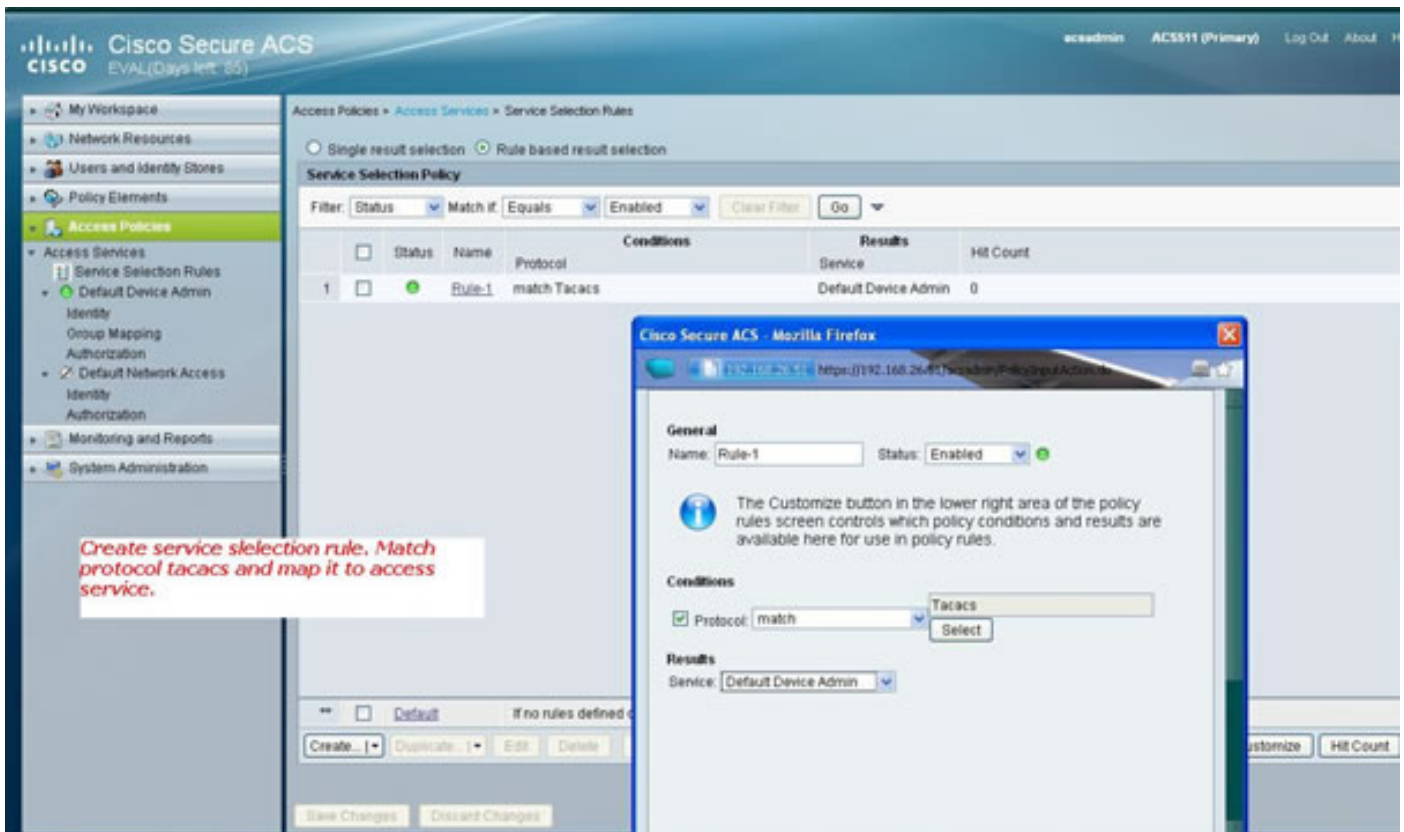


The screenshot displays the Cisco Secure ACS web interface. The left sidebar shows a navigation tree with 'Policy Elements' expanded to 'Shell Profiles'. The main content area is titled 'Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "joseph1"'. It features three tabs: 'General', 'Common Tasks', and 'Custom Attributes'. The 'Common Tasks' tab is active, showing configuration options for 'Privilege Level' and 'Shell Attributes'. Under 'Privilege Level', 'Default Privilege' and 'Maximum Privilege' are both set to 'Static' with a 'Value' of '1'. Under 'Shell Attributes', all fields are set to 'Not in Use'. A legend at the bottom indicates that a gear icon represents required fields. 'Submit' and 'Cancel' buttons are located at the bottom of the form.

Field	Value
Default Privilege	Static
Maximum Privilege	Static
Value (for Default Privilege)	1
Value (for Maximum Privilege)	1
Access Control List	Not in Use
Auto Command	Not in Use
No Callback Verify	Not in Use
No Escape	Not in Use
No Hang Up	Not in Use
Timeout	Not in Use
Idle Time	Not in Use
Callback Line	Not in Use
Callback Rotary	Not in Use

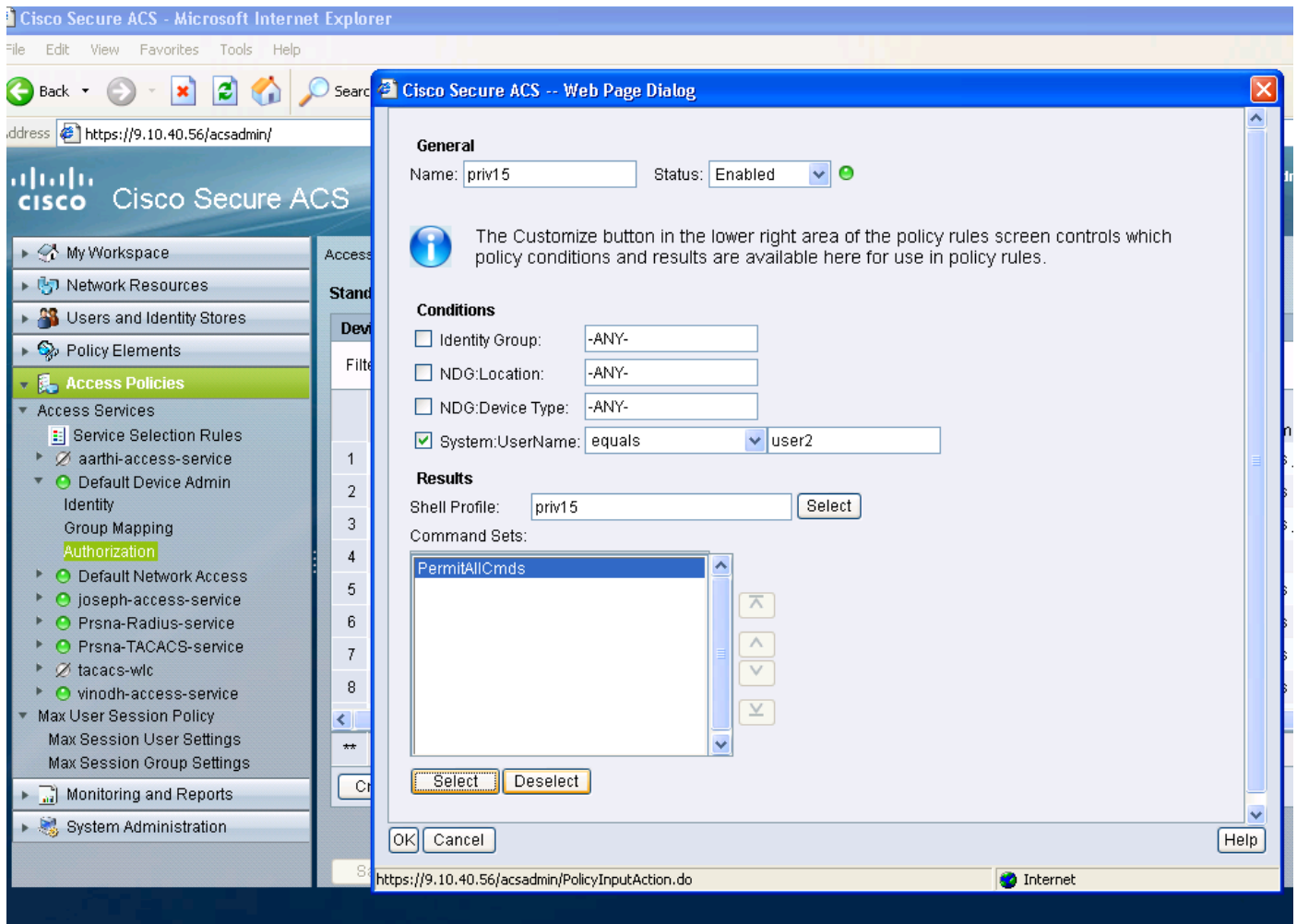
创建服务选择规则匹配TACACS协议

根据您的策略和配置，请确保有一个规则匹配TACACS的您来自5760。



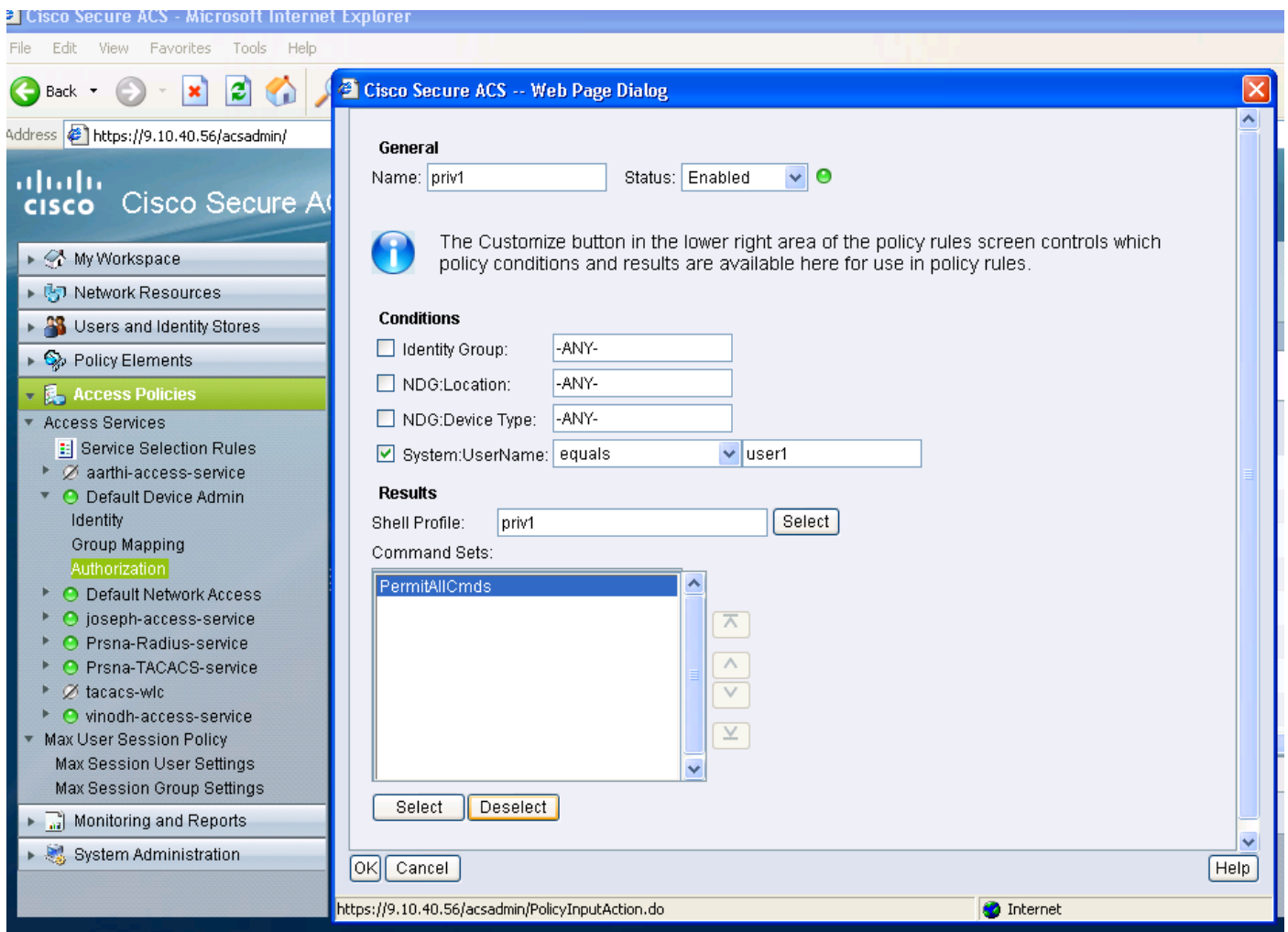
创建全双工管理访问的授权策略。

作为评估策略进程一部分，默认设备Admin策略与TACACS协议选择一起使用选择。当使用TACACS协议验证时，选择的服务策略呼叫默认设备Admin策略。策略本身包括2个部分。Identity含义谁用户是，并且什么组他属于(本地或外部)，并且什么他允许根据配置的授权配置文件执行。分配与您配置的用户涉及的set命令。



创建只读管理访问的授权策略。

同样为只读用户执行。此示例配置user1的权限级别1 shell配置文件和权限15对user2。



配置5760 TACACS的

1. Radius/TACACS服务器需要配置。

TACACS服务器tac_acct

地址ipv4 9.1.0.100

关键思科

2. 配置服务器组

aaa组服务器TACACS+ gtac

服务器名tac_acct

没有直到上述步骤的前提。

3. 配置认证和授权方法列表

AAA认证登录<method-list>组<srv-grp>

AAA认证exec <method-list>组srv-grp>

AAA认证exec默认组<srv-grp> ----获得在http的TACACS的à应急方案。

上述3命令和其他认证和授权参数应该使用同一个数据库， radius/TACACS或本地

例如，如果authorization命令需要启用，它也需要指向同一个数据库。

例如：

AAA授权命令15 <method-list>组<srv-grp> ——>指向数据库(TACACS/radius或本地)的服务器组应该是相同的。

4. 配置http使用上述方法列表

IP HTTP验证aaa洛金验证<method-list> ——>方法列表需要明确地指定此处，即使方法列表是“默认”

IP HTTP验证aaa exec验证<method-list>

**注释的点

- 请勿配置在“线路VTY”设置参数的任何method-list。如果上述步骤和线路VTY有不同的配置，则线路VTY配置将获得优先权。
- 数据库应该是相同的在所有管理配置类型间类似SSH/telnet和webui。
- HTTP验证应该有明确地定义的方法列表。

访问同样5760与2不同的配置文件

下面是从有限访问给的权限级别1用户的一访问

The screenshot shows the Cisco Wireless Controller web interface. The browser address bar displays '9.12.137.95/wireless'. The interface includes a navigation menu with 'Home', 'Monitor', and 'Help' options. The main content area is divided into several sections:

- System Summary:** A table with the following data:

System Time	18:54:12.963 UTC Thu Jul 23 2015
Software Version	03.06.03.E.536 EARLY DEPLOYMENT [PROD BUILD] ENGINEERING NOVA_WEEKLY BUILD
System Name	JKAT-RFC
System Model	AIR-CT5760
Up Time	9 hours, 28 minutes
Wireless Management IP	9.12.137.95
802.11 a/n/ac Network State	Enabled
802.11 b/g/n Network State	Enabled
- Access Point Summary:** A table with the following data:

	Total	Up	Down
802.11a/n/ac Radios	1	1	0
802.11b/g/n Radios	1	1	0
All APs	1	1	0
- Client Summary:** A section with a blue semi-circle graphic.
- Protocol Statistics:** A section with a blue semi-circle graphic.
- Search:** A search bar with a 'Search' button.
- Top WLANs:** A table with the following data:

Profile Name	Number of Clients
QM	0
jalousian	0
- AVC for WLAN : QM:** A section stating 'AVC is not enabled on this WLAN'.
- Rogue APs:** A section showing 'Active Rogue APs' with a count of 203 and a 'Detail' link.

下面是从您给完全权限的权限级别15用户的访问

System Summary

System Time	18:51:40.772 UTC Thu Jul 23 2015
Software Version	03.06.03.E.536 EARLY DEPLOYMENT [PROD BUILD] ENGINEERING NOVA_WEEKLY BUILD
System Name	JKAT-RFC
System Model	AIR-CTS760
Up Time	9 hours, 26 minutes
Wireless Management IP	9.12.137.95
802.11 a/n/ac Network State	Enabled
802.11 b/g/n Network State	Enabled
Software Activation	Detail

Access Point Summary

	Total	Up	Down
802.11a/n/ac Radios	1	1	0
802.11b/g/n Radios	1	1	0
All APs	1	1	0

Client Summary

Protocol Statistics

Search

Username

Top WLANs

Profile Name	Number of Clients
QM	0
jolouisan	0

AVC for WLAN : QM

AVC is not enabled on this WLAN

Rogue APs

Active Rogue APs 207 [Detail](#)