配置ISE 2.0 TACACS+身份验证命令授权

目录

简介

背景信息

先决条件

- 要求
- 使用的组件

配置

- 网络图
- 配置
  - 配置ISE进行身份验证和授权
  - 加入ISE 2.0到Active Directory
  - 添加网络设备
  - 启用设备管理服务
  - 配置TACACS命令集
  - 配置TACACS配置文件
  - 配置TACACS授权策略
  - 配置Cisco IOS路由器以进行身份验证和授权

验证

- Cisco IOS路由器验证
- ISE 2.0验证

故障排除

相关信息

简介

本文档介绍如何基于Microsoft Active Directory(AD)组成员身份配置TACACS+身份验证和命令授权。

背景信息

要根据具有身份服务引擎(ISE)2.0及更高版本的用户的Microsoft Active Directory(AD)组成员身份配置TACACS+身份验证和命令授权，ISE使用AD作为外部身份库来存储资源，例如用户、计算机、组和属性。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS®路由器完全正常运行

- 路由器和ISE之间的连接。
- ISE服务器已引导并且与Microsoft AD连接

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎2.0
- 思科IOS®软件版本15.4(3)M3
- Microsoft Windows Server 2012 R2

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

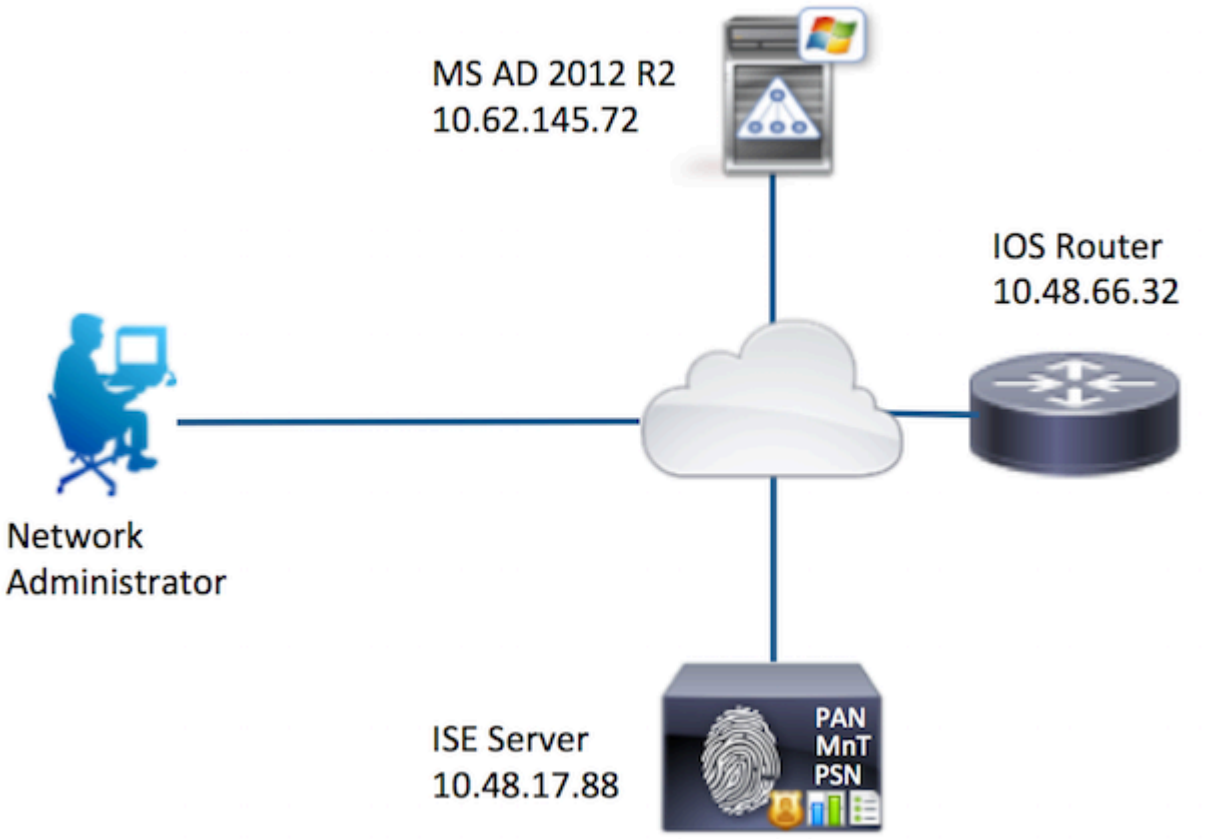
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

配置的目的是：

- 通过AD对Telnet用户进行身份验证
- 授权telnet用户，使其在登录后进入特权执行模式
- 检查并将每个执行的命令发送到ISE进行验证

网络图

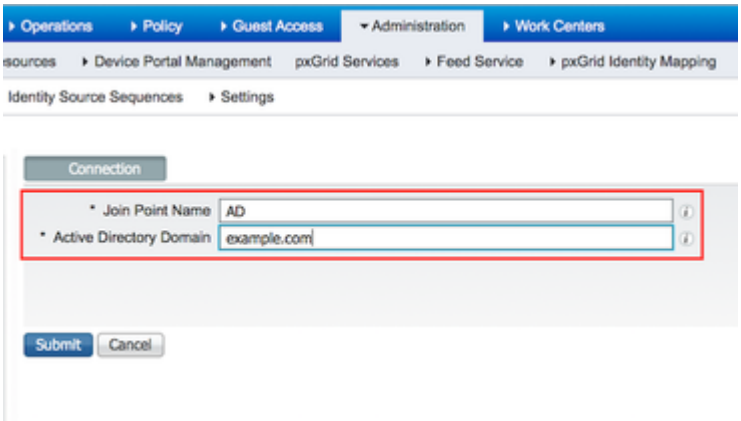


配置

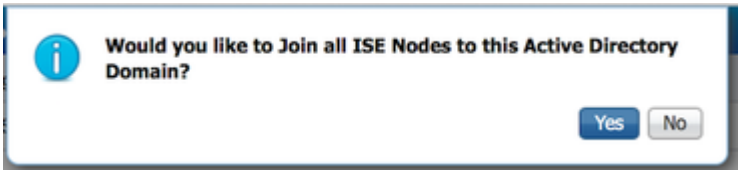
配置ISE进行身份验证和授权

加入ISE 2.0到Active Directory

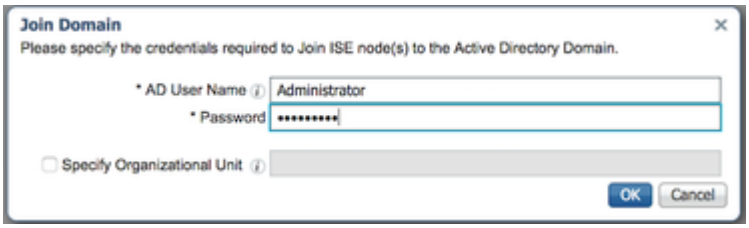
1.导航到管理>身份管理>外部身份库> Active Directory >添加。提供加入点名称、Active Directory域并点击提交。



2.当系统提示将所有ISE节点加入此Active Directory域时，点击是。



3.提供AD用户名和密码，然后点击确定。

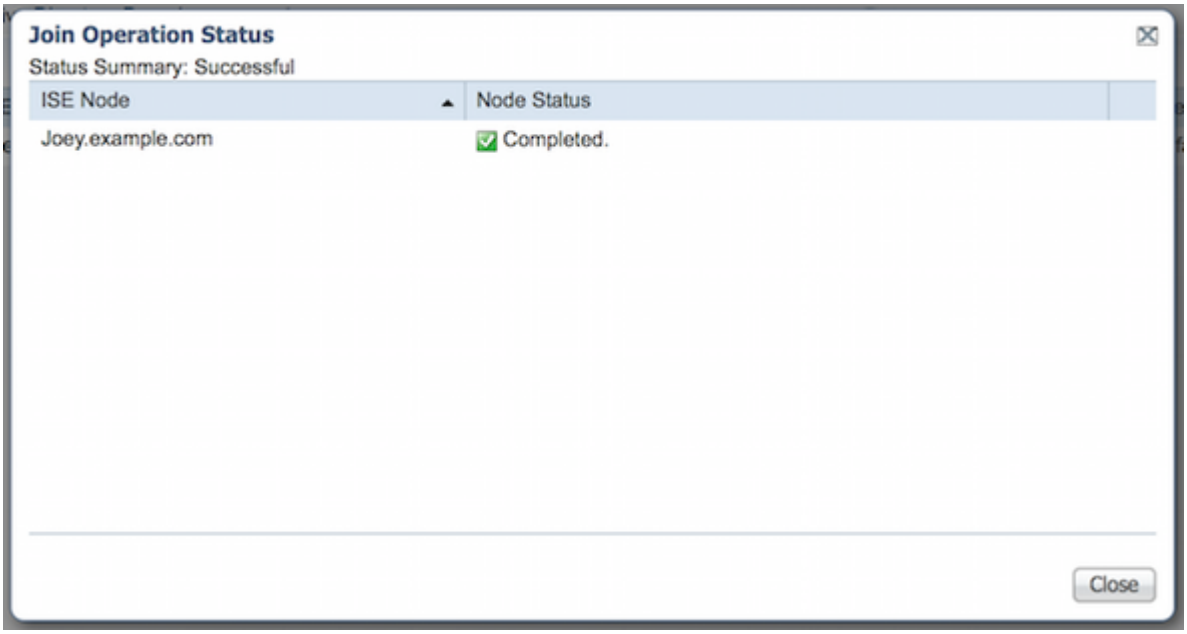


在ISE中访问域所需的AD帐户可以具有下列任一项：

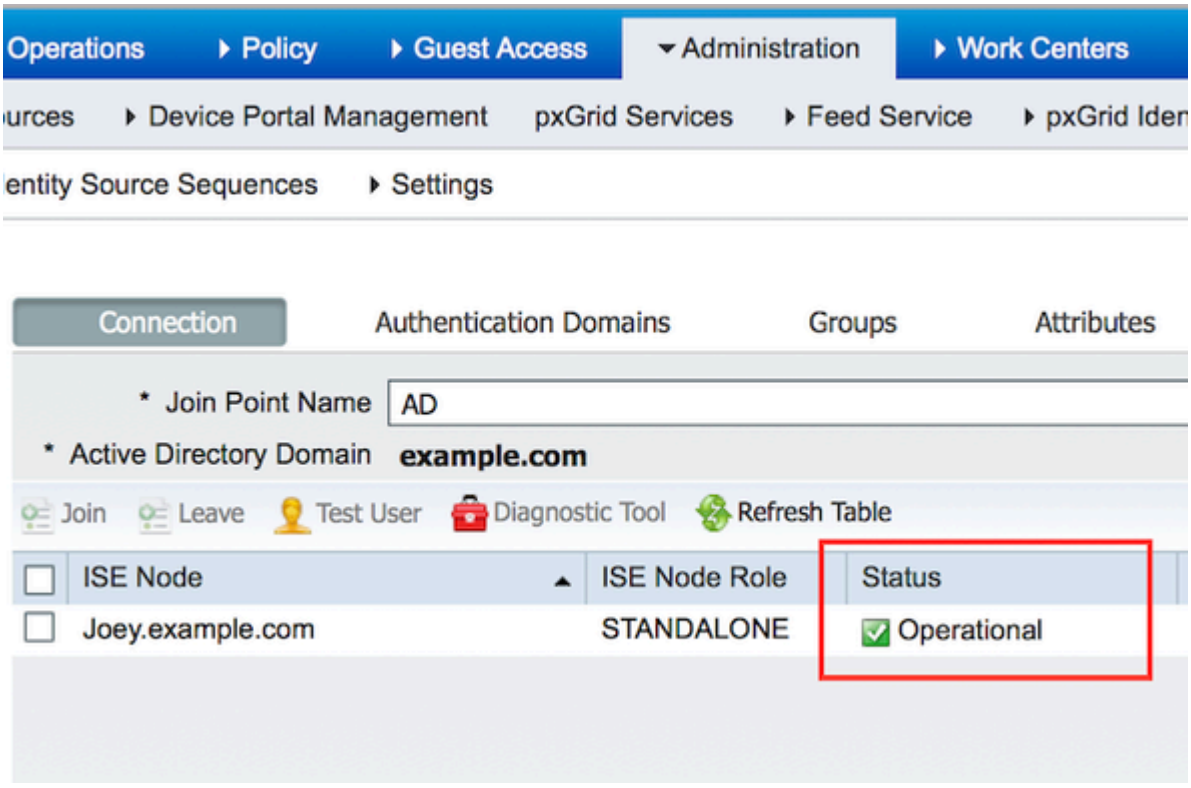
- 将工作站添加到相应域中的域用户权限
- 在创建ISE计算机的帐户后将ISE计算机加入域之前，在相应计算机容器上创建计算机对象或删除计算机对象权限

注意：思科建议禁用ISE帐户的锁定策略，并配置AD基础设施，以便在为该帐户使用错误密码时向管理员发送警报。输入错误密码时，ISE不会在必要时创建或修改其计算机帐户，因此可能会拒绝所有身份验证。

4.复查工序状态。节点状态必须显示为“已完成”。单击 Close。

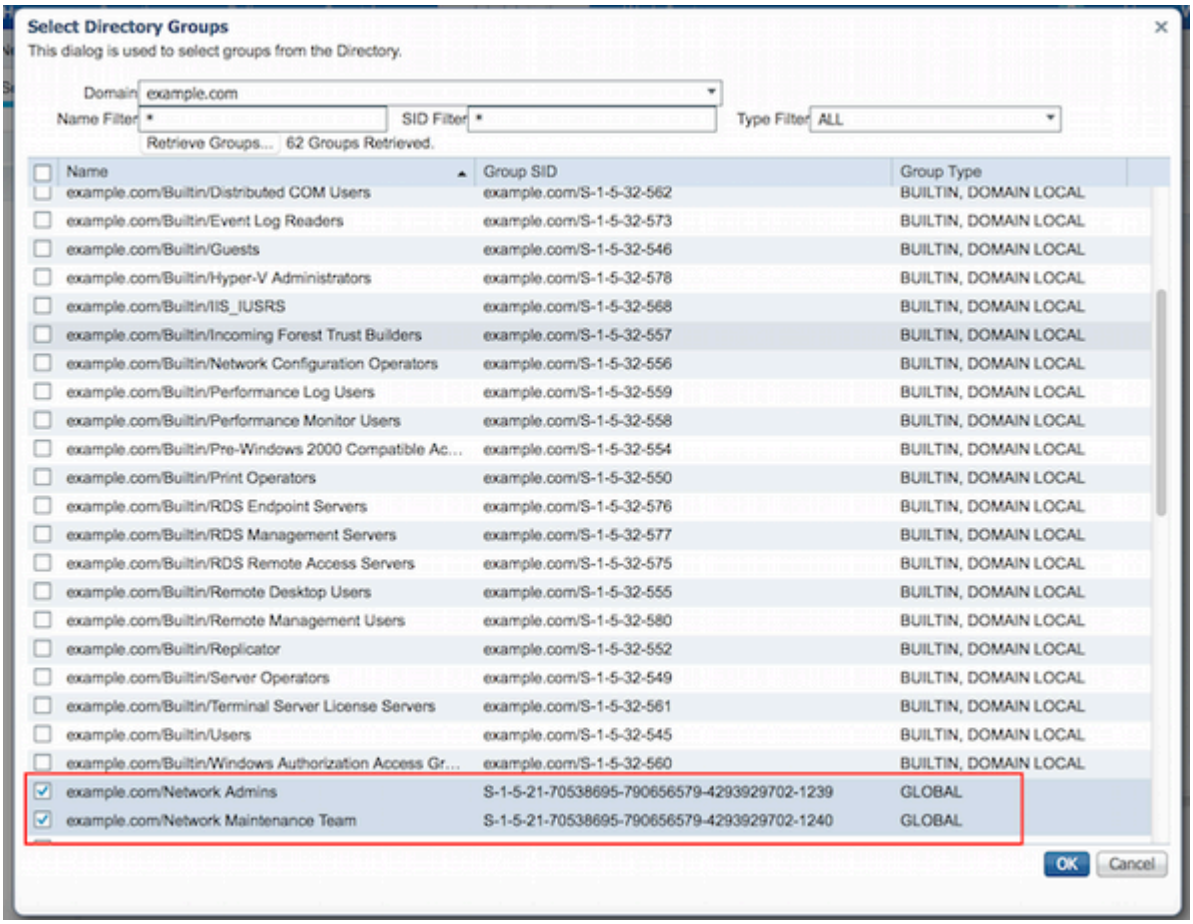


5. AD状态为运行状态。

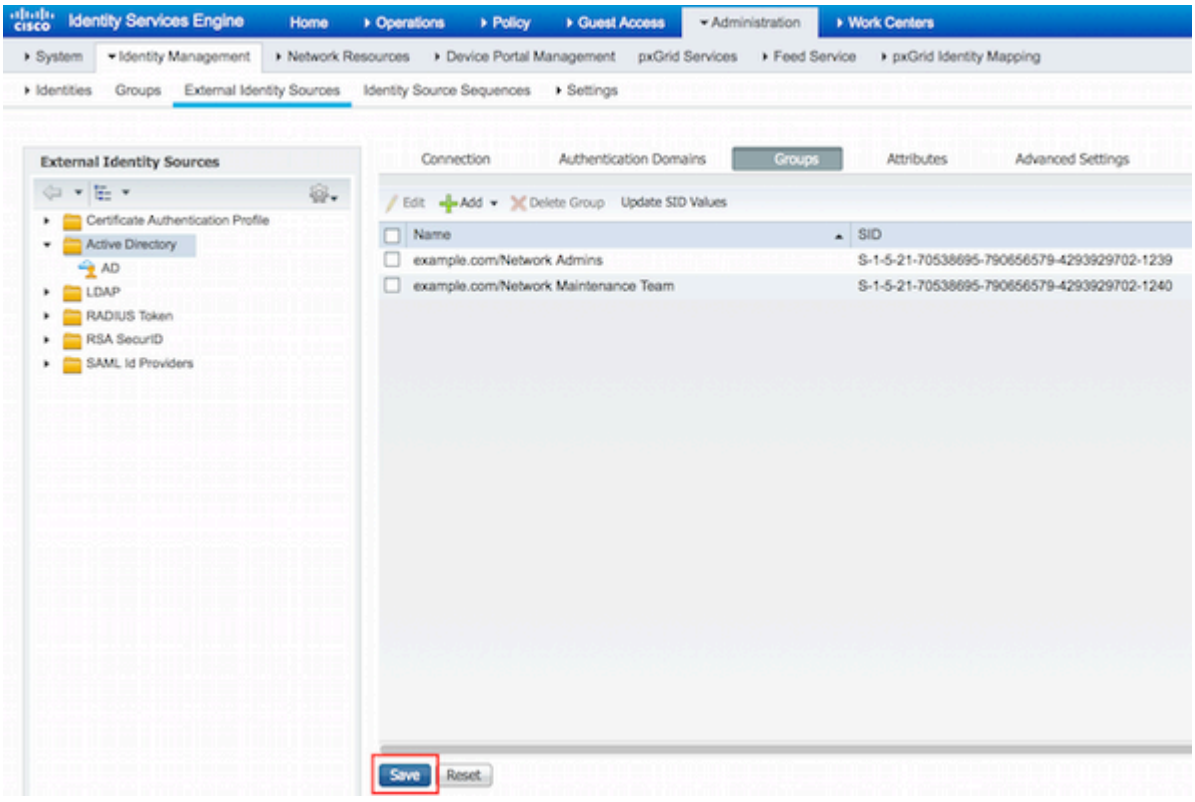


6.定位至“组”>“添加”>“从目录选择组”>“检索组”。选中Network Admins AD Group和Network Maintenance Team AD Group复选框，如下图所示。

注意：用户admin是网络管理员AD组的成员。此用户具有完全访问权限。此用户是网络维护团队AD组的成员。此用户只能执行show命令。

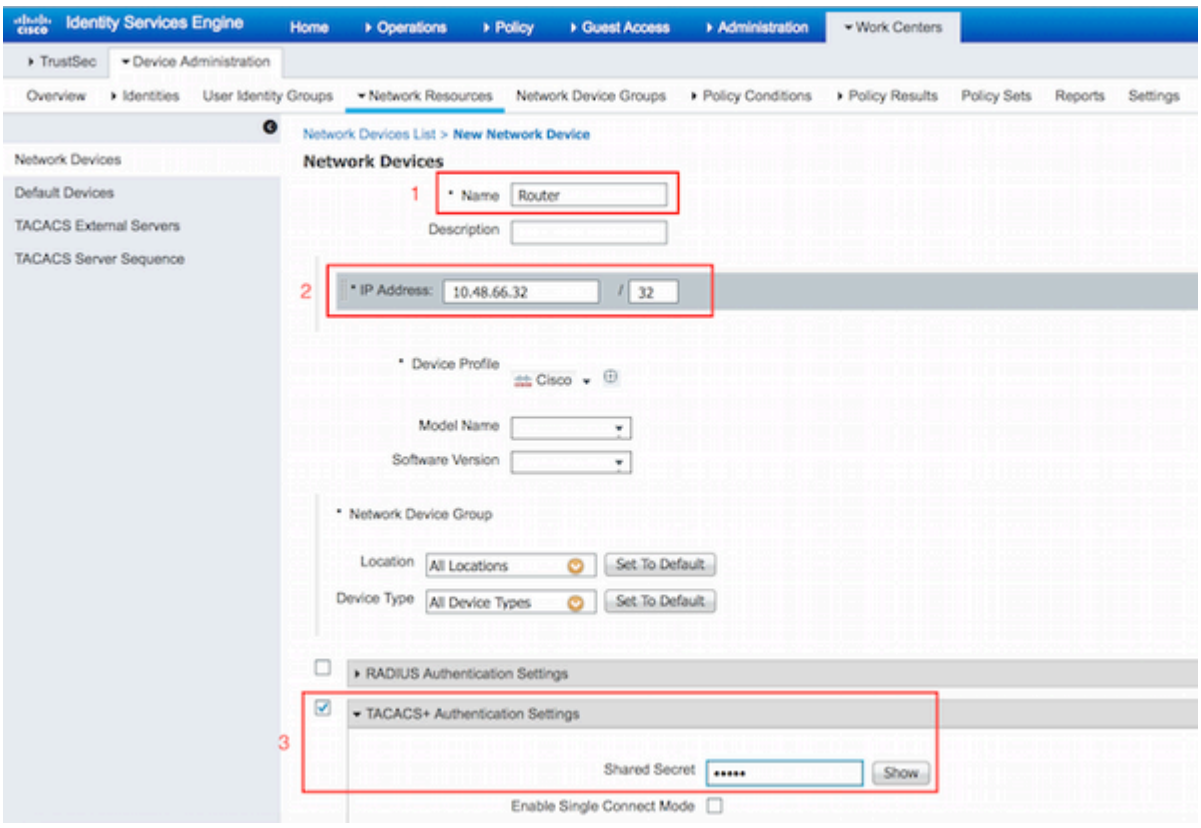


7.单击保存以保存检索到的AD组。



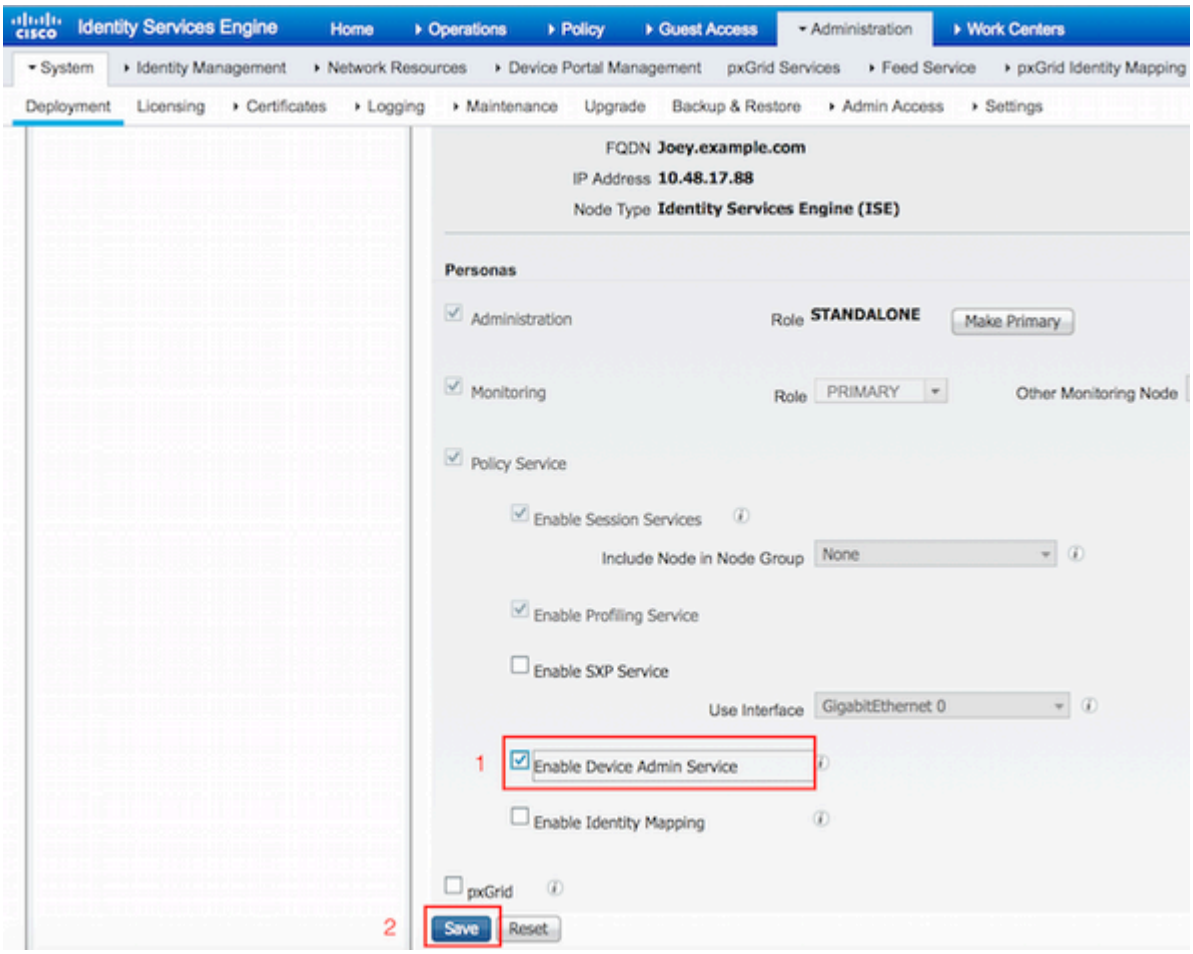
添加网络设备

导航至工作中心(Work Centers)>设备管理(Device Administration)>网络资源(Network Resources)>网络设备(Network Devices)。单击 Add。提供名称、IP地址，选中TACACS+身份验证设置复选框并提供共享密钥。



启用设备管理服务

导航到管理>系统>部署。选择所需的节点。选中Enable Device Admin Service复选框，然后单击 Save。

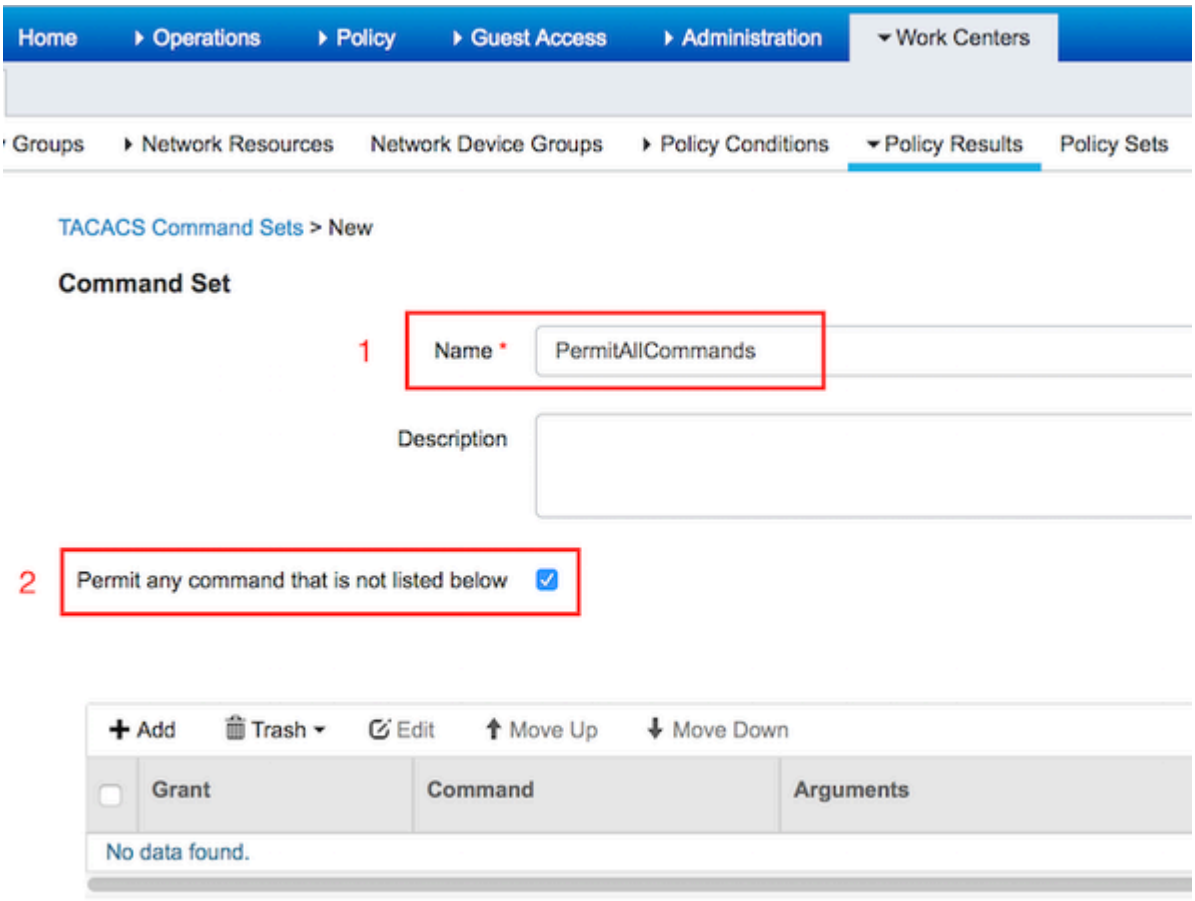


注意：对于TACACS，您需要安装单独的许可证。

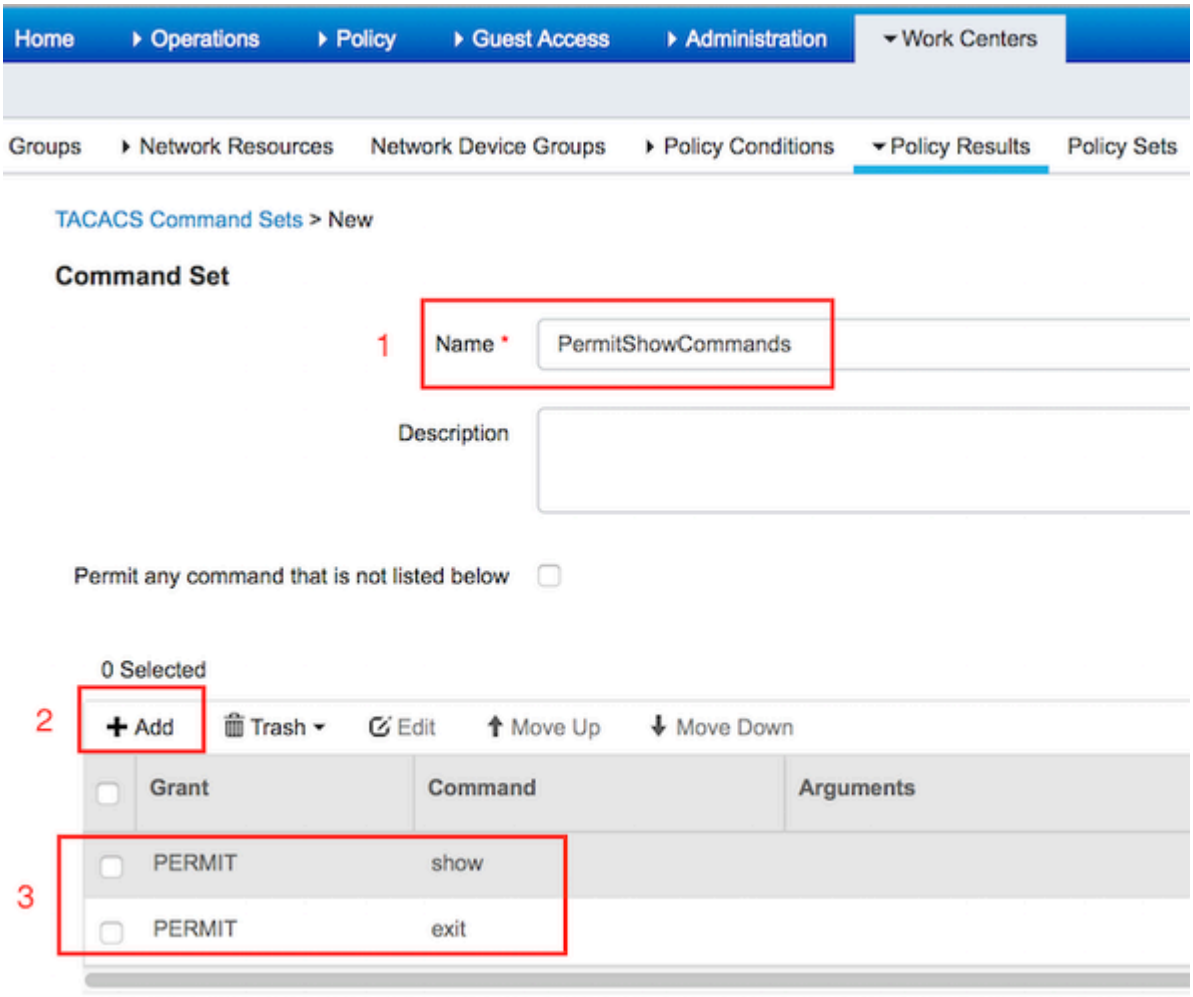
配置TACACS命令集

配置了两个命令集。用户admin的第一个PermitAllCommands，它允许设备上的所有命令。第二个PermitShowCommands用于仅允许show命令的用户用户。

1.导航到工作中心>设备管理>策略结果> TACACS命令集。单击 Add。提供名称PermitAllCommands，选中Permit any command复选框（未列出），然后单击Submit。

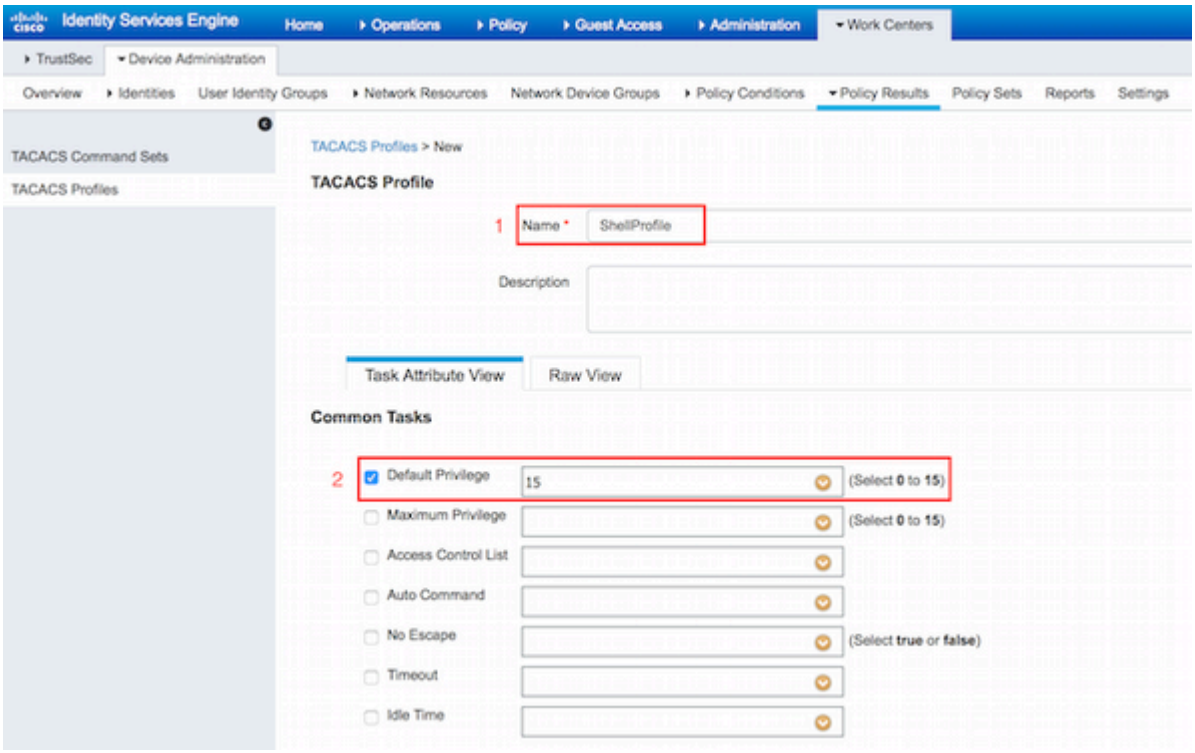


2.导航到工作中心>设备管理>策略结果> TACACS命令集。单击 Add。提供名称 PermitShowCommands，单击Add并允许show和exit命令。默认情况下，如果Arguments留空，则包括所有参数。单击 submit。



配置TACACS配置文件

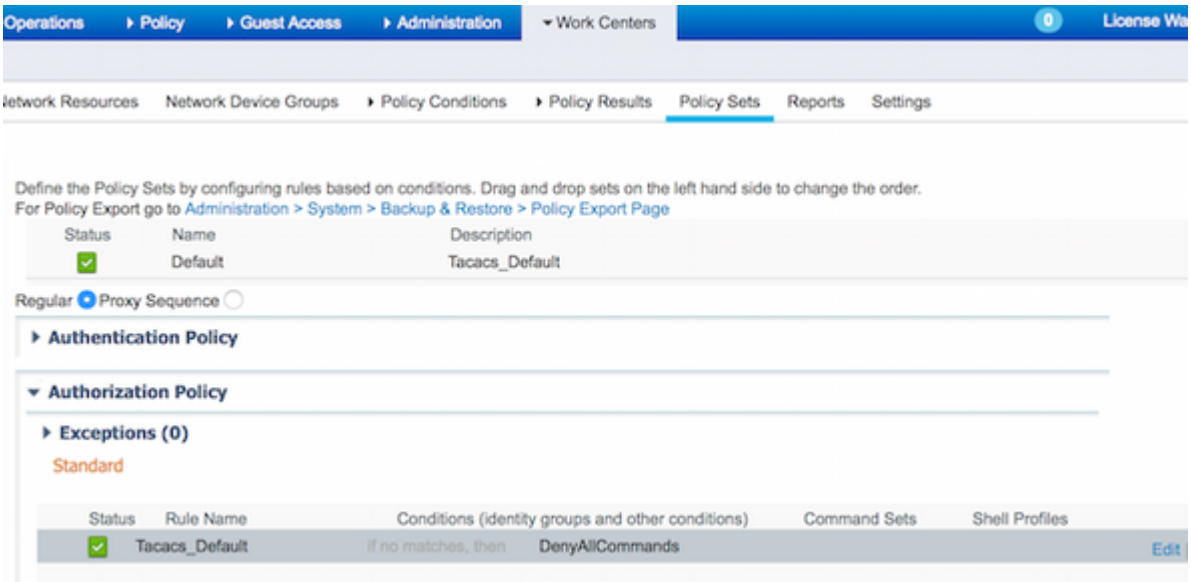
配置单个TACACS配置文件。TACACS配置文件与ACS上的外壳配置文件概念相同。实际的命令实施通过命令集完成。导航到工作中心(Work Centers)>设备管理(Device Administration)>策略结果(Policy Results)> TACACS配置文件(TACACS Profiles)。单击 Add。提供名称ShellProfile，选中Default Privilege复选框，然后输入值15。单击Submit。



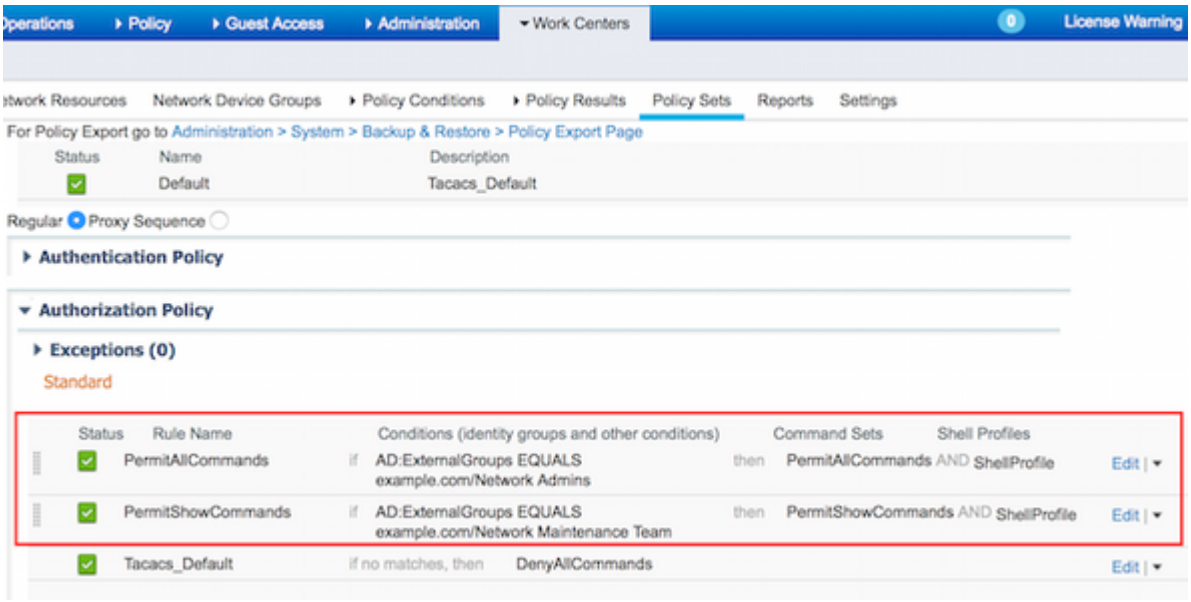
配置TACACS授权策略

默认情况下，“身份验证策略”(Authentication Policy)指向All_User_ID_Stores（包括AD），因此它保持不变。

导航至工作中心(Work Centers)>设备管理(Device Administration)>策略集(Policy Sets)>默认(Default)>授权策略(Authorization Policy)>编辑(Edit)>在上述位置插入新规则(Insert New Rule Above)。



配置两个授权规则；第一条 规则根据Network Admins AD Group membership分配TACACS配置文件ShellProfile和命令Set PermitAllCommands。第二条 规则根据网络维护团队AD组成员资格分配TACACS配置文件ShellProfile和命令Set PermitShowCommands。



配置Cisco IOS路由器以进行身份验证和授权

完成以下步骤以配置Cisco IOS路由器以进行身份验证和授权。

1.使用username命令创建具有完全回退权限的本地用户，如下所示。

```
username cisco privilege 15 password cisco
```

2.启用aaa new-model。定义TACACS服务器ISE，并将其放置在ISE_GROUP组中。

```
aaa new-model



tacacs server ISE
 address ipv4 10.48.17.88
 key cisco
aaa group server tacacs+ ISE_GROUP
 server name ISE
```

注意：服务器密钥与之前在ISE服务器上定义的密钥匹配。

3.使用test aaa命令测试TACACS服务器的可达性，如下所示。

<#root>

```
Router#
```

```
test aaa group tacacs+ admin Krakow123 legacy

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

上一个命令的输出显示TACACS服务器可访问，且用户已成功通过身份验证。

4.配置登录并启用身份验证，然后使用exec和命令授权，如下所示。

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

 注意：创建的方法列表名为AAA，稍后在将其分配至线路vty时使用。

5.将方法列表分配给行vty 0 4。

```
line vty 0 4
 authorization commands 0 AAA
 authorization commands 1 AAA
 authorization commands 15 AAA
 authorization exec AAA
 login authentication AAA
```

验证

Cisco IOS路由器验证

1. Telnet至Cisco IOS路由器，作为属于AD中完全访问组的admin。Network Admins group是AD中映射到ISE上的ShellProfile和PermitAllCommands命令集的组。尝试运行任何命令以确保完全访问。

```
<#root>

Username:

admin

Password:
```

```
Router#
conf t

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
crypto isakmp policy 10

Router(config-isakmp)#
encryption aes

Router(config-isakmp)#
exit

Router(config)#
exit

Router#
```

2.以属于AD中有限访问组的用户Telnet至Cisco IOS路由器。网络维护团队组是AD中映射到ISE上设置的ShellProfile和PermitShowCommands命令的组。尝试运行任何命令以确保只能发出show命令。

```
<#root>
Username:
user

Password:
Router#
show ip interface brief | exclude unassigned

Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.48.66.32     YES NVRAM  up                    up

Router#
ping 8.8.8.8

Command authorization failed.
Router#
configure terminal

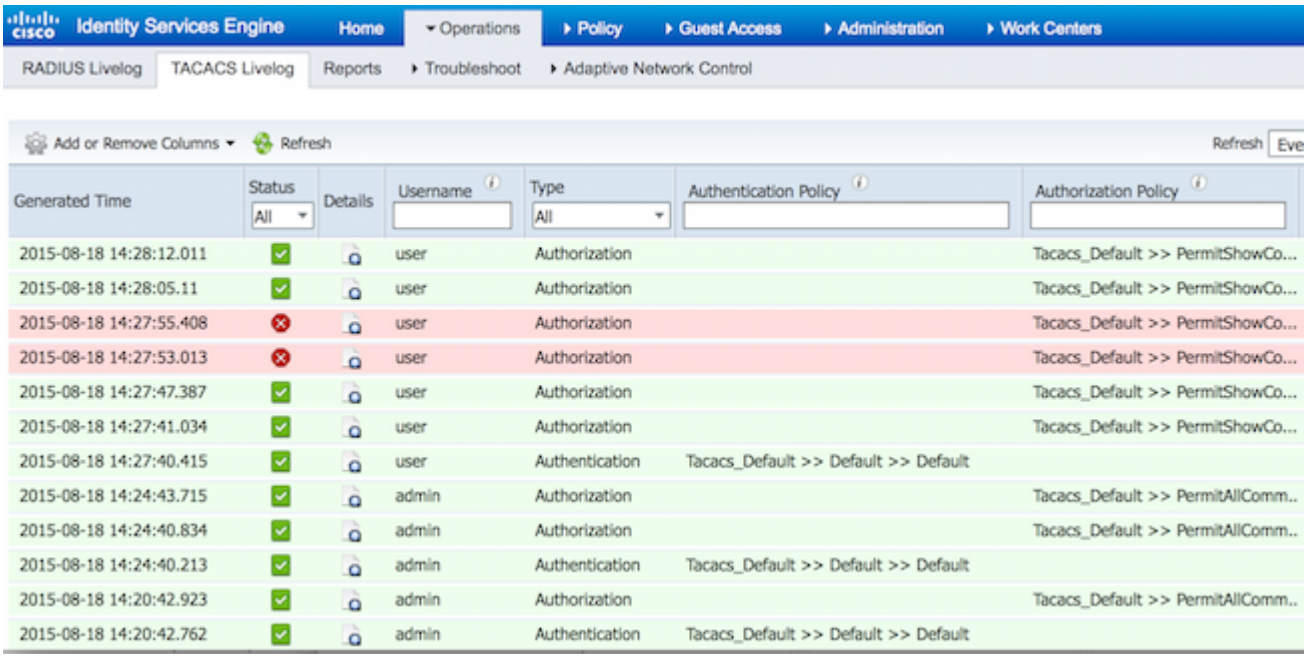
Command authorization failed.
```

```
Router#
show running-config | include hostname

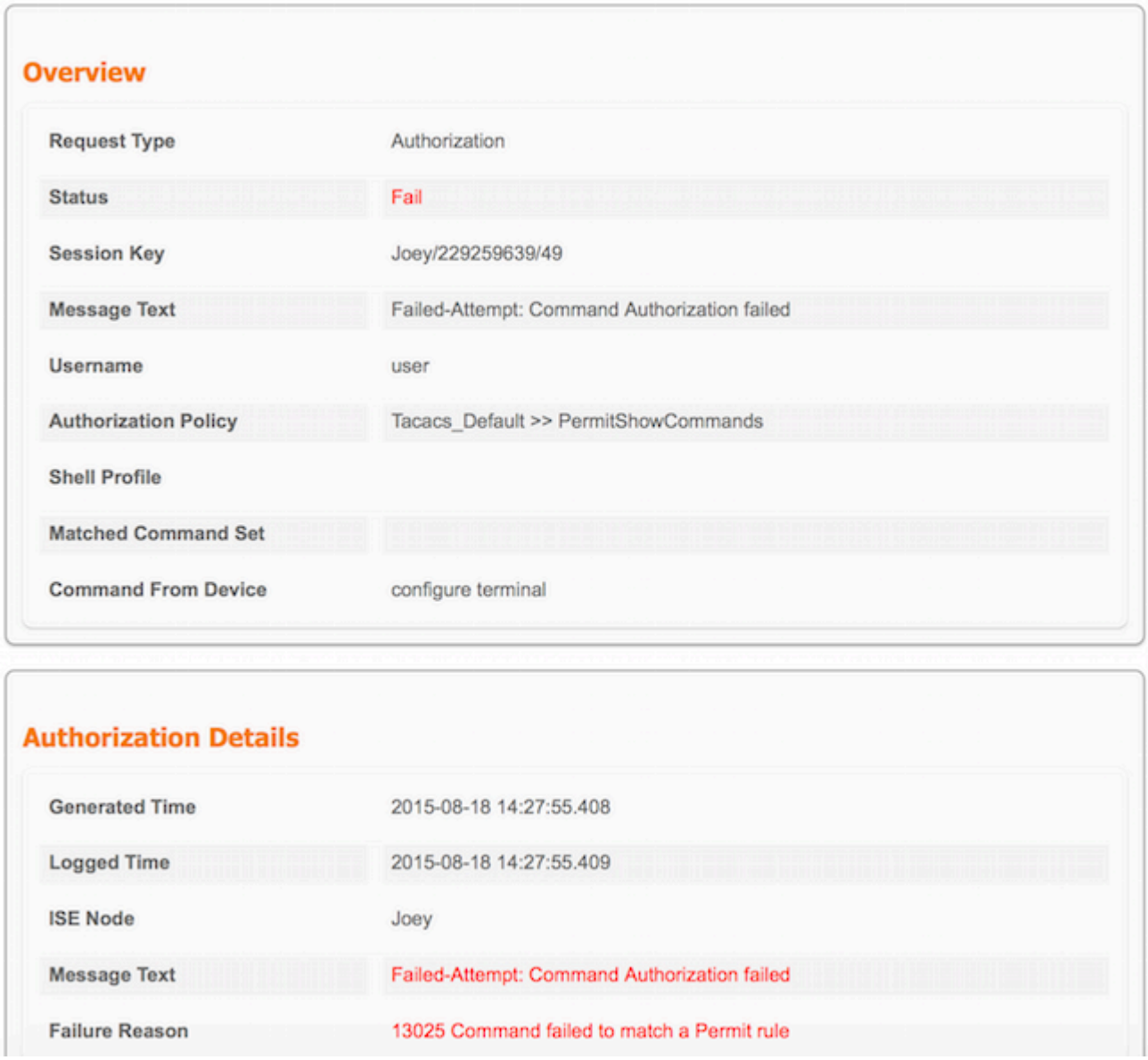
hostname Router
Router#
```

ISE 2.0验证

1.导航到操作> TACACS Livelog。确保看到已完成的尝试。



2.单击其中一个红色报表的详细信息。以前执行的失败命令可见。



Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Matched Command Set	
Command From Device	configure terminal

Authorization Details

Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

故障排除

Error:13025命令无法匹配Permit规则

检查SelectedCommandSet属性以验证预期命令集是否已由授权策略选择。

相关信息

[技术支持和文档 - Cisco Systems]

[ISE 2.0版本说明]

[ISE 2.0硬件安装指南]

[ISE 2.0升级指南]

[ACS至ISE迁移工具指南]

ISE 2.0 Active Directory集成指南

ISE 2.0引擎管理员指南

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）。