

ISE 2.0 : ASA CLI TACACS+认证和Authorization命令配置示例

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[配置](#)

[配置认证和授权的ISE](#)

[添加网络设备](#)

[配置用户身份组](#)

[配置用户](#)

[以启用设备Admin服务](#)

[配置tacacs命令集](#)

[配置TACACS配置文件](#)

[配置TACACS授权策略](#)

[配置认证和授权的Cisco ASA防火墙](#)

[Verify](#)

[Cisco ASA防火墙验证](#)

[ISE 2.0验证](#)

[Troubleshoot](#)

[Related Information](#)

[相关的思科支持社区讨论](#)

Introduction

本文描述如何用身份服务引擎(ISE) 2.0配置TACACS+认证和Authorization命令在Cisco可适应的安全工具(ASA)上及以后。ISE使用本地身份存储存储资源例如用户、组和终端。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- ASA防火墙是完全能操作的
- ASA和ISE之间的连接
- ISE服务器被引导

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco 身份服务引擎2.0
- Cisco ASA Software Release 9.5(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

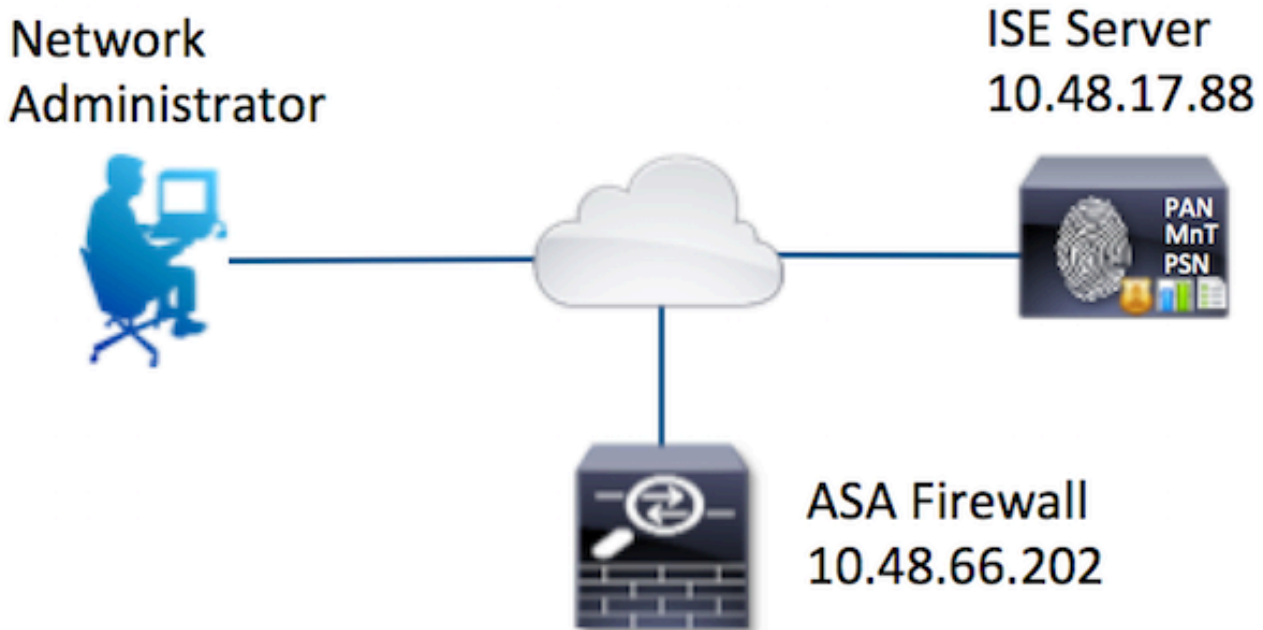
Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

Configure

配置的AIM对：

- 通过内部身份存储验证SSH用户
- 认证SSH用户，因此它将被放置到privileged EXEC模式在登录以后
- 检查并且发送每个被执行命令到验证的ISE

Network Diagram



配置

配置认证和授权的ISE

两个用户被创建。用户**管理员**是**网络管理员**本地身份组的部分在ISE的。此用户有充分的CLI权限。用户**用户**是**网络维护小组**本地身份组的部分在ISE的。此用户允许执行只显示命令和ping。

添加网络设备

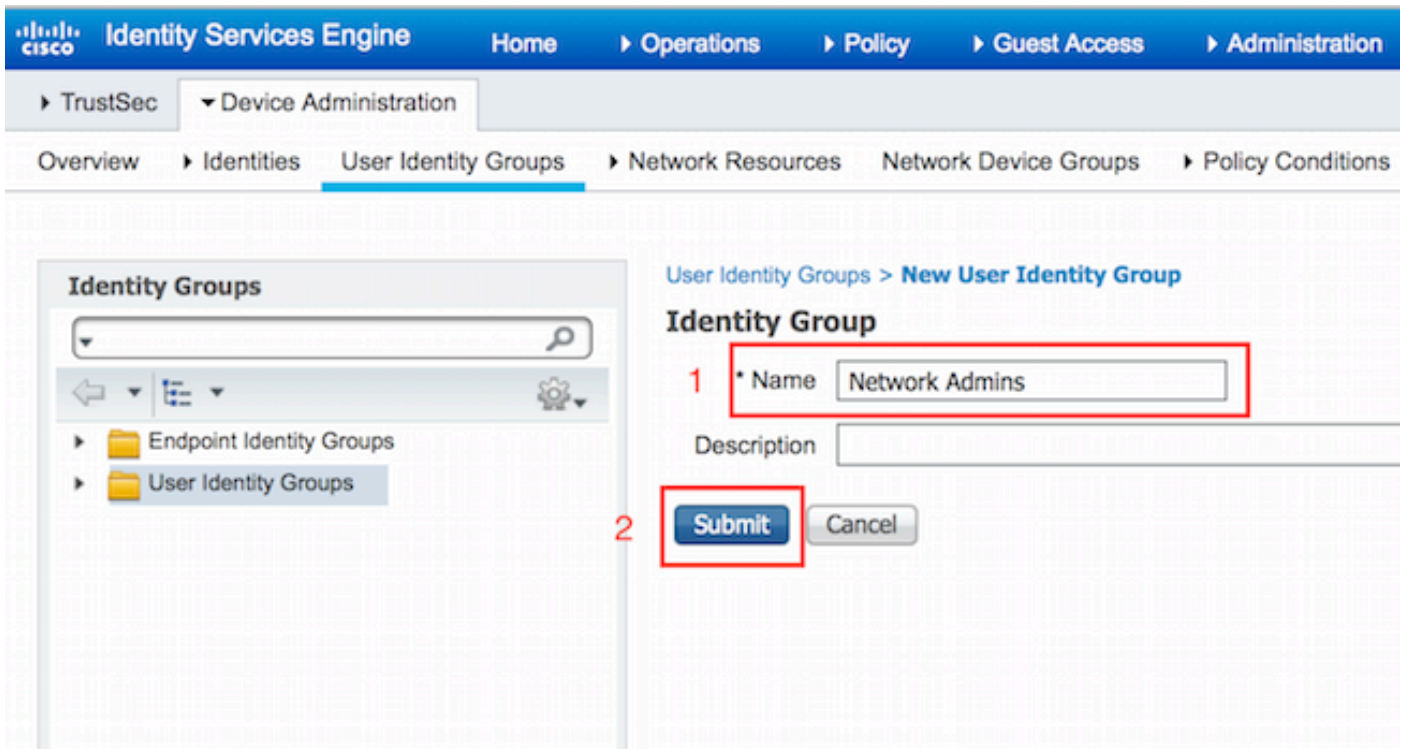
连接到**工作区>设备Administration >网络资源>网络设备**。单击 **Add**。提供名字，IP地址，选择**Settings**复选框的TACACS+认证并且提供被共享的密钥。随意地设备类型/位置可以指定。

The screenshot displays the 'New Network Device' configuration page in the Cisco Identity Services Engine (ISE) interface. The page is titled 'Network Devices' and includes a sidebar with navigation options like 'Default Devices', 'TACACS External Servers', and 'TACACS Server Sequence'. The main content area contains several sections for configuring a new device:

- Name:** A text input field containing 'ASA', highlighted with a red box and labeled '1'.
- Description:** An empty text input field.
- IP Address:** A text input field containing '10.48.66.202 / 32', highlighted with a red box and labeled '2'.
- Device Profile:** A dropdown menu set to 'Cisco'.
- Model Name:** An empty dropdown menu.
- Software Version:** An empty dropdown menu.
- Network Device Group:** A section with two dropdown menus: 'Location' set to 'All Locations' and 'Device Type' set to 'Firewall', each with a 'Set To Default' button.
- Authentication Settings:** A section with two checkboxes: 'RADIUS Authentication Settings' (unchecked) and 'TACACS+ Authentication Settings' (checked, highlighted with a red box and labeled '3'). Below the 'TACACS+ Authentication Settings' checkbox is a 'Shared Secret' field with a 'Show' button and a masked password '*****'.
- Enable Single Connect Mode:** An unchecked checkbox at the bottom.

配置用户身份组

连接到**工作区>设备Administration >用户身份组**。单击 **Add**。提供名字并且点击**提交**。



重复同一个步骤对configure network维护小组用户身份组。

配置用户

连接对工作区>设备Administration >身份> Users。单击 Add。提供名字，登录密码指定用户组并且点击提交。

Network Access User

* Name 1

Status Enabled

Email

Passwords 2

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

User Information

First Name

Last Name

Account Options

Description

Change password on next login

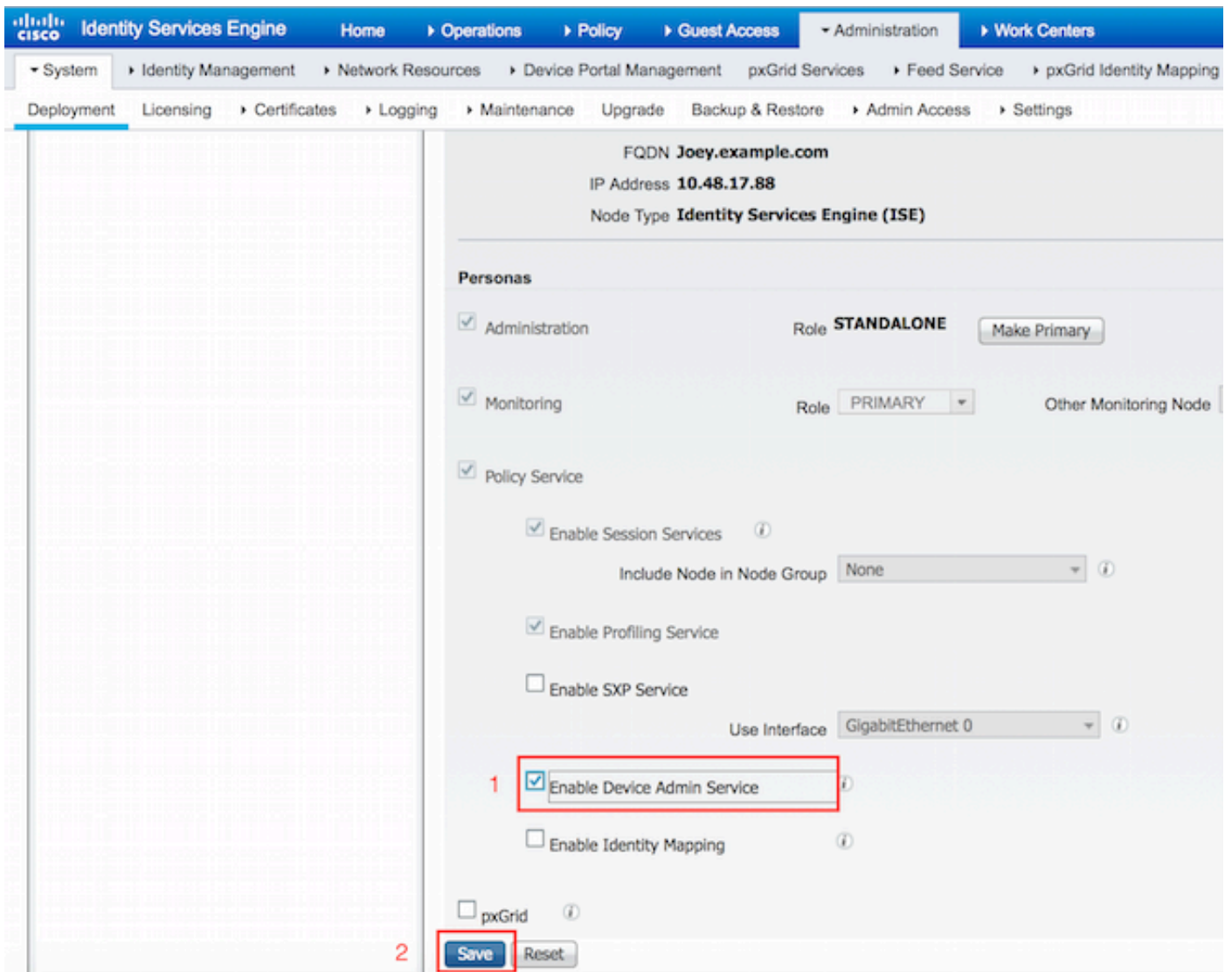
User Groups 3

ⓘ - +

重复步骤配置用户用户和分配网络维护小组用户身份组。

以启用设备Admin服务

连接对**管理>System >配置**。select要求了节点。选择以启用设备Admin服务复选框并且点击“Save”。



Note:对于TACACS您需要安排分开的许可证安装。

配置tacacs命令集

配置两命令集。提供所有on命令设备的**管理员用户**的第一**PermitAllCommands**。允许的用户用户的第二**PermitPingShowCommands**只显示和查验命令。

1. 连接对工作区>设备管理>Policy结果> tacacs命令集。单击 **Add**。提供名字 **PermitAllCommands** , 选择**permit any**命令不是列出的下面的复选框并且点击**提交**。

TACACS Command Sets > New

Command Set

1

Name * PermitAllCommands

Description

2

Permit any command that is not listed below

<input type="checkbox"/>	Grant	Command	Arguments
No data found.			

2. 连接对工作区>设备管理>Policy结果> tacacs命令集。单击 Add。提供名字 PermitPingShowCommands，点击添加，并且许可证显示，连接并且退出命令。默认情况下，如果参数被留下空白，所有参数是包括的。单击 submit。

TACACS Command Sets > PermitPingShowCommands

Command Set

1

Name * PermitPingShowCommands

Description

Permit any command that is not listed below

<input type="checkbox"/>	Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	exit	
<input type="checkbox"/>	PERMIT	show	
<input type="checkbox"/>	PERMIT	ping	

2

Cancel Save

配置TACACS配置文件

将配置单个TACACS配置文件。实际命令实施通过命令集将完成。连接对**工作区>设备管理>Policy结果> TACACS配置文件**。单击 **Add**。提供命名**ShellProfile**，选择**默认权限**复选框并且输入值为15。单击 **submit**。

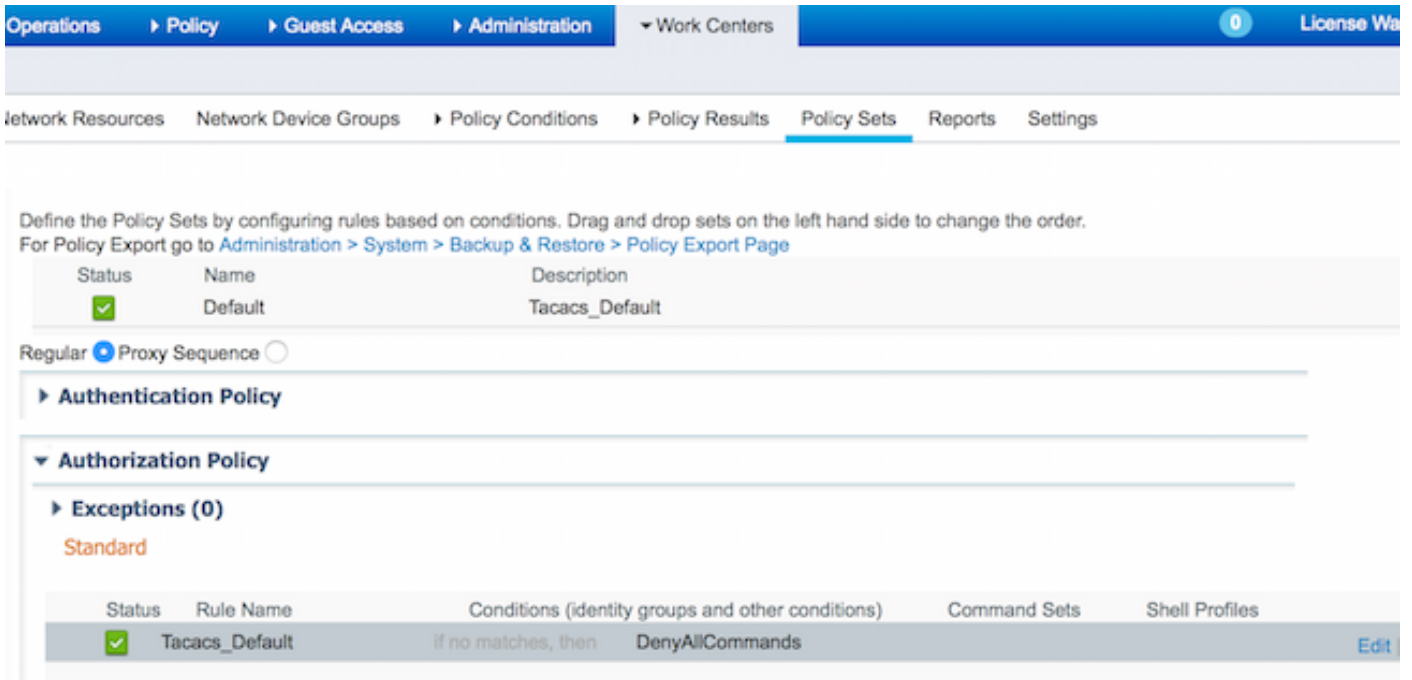
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for a new TACACS Profile. The page is titled "TACACS Profiles > New" and "TACACS Profile". The "Name" field is set to "ShellProfile". The "Description" field is empty. The "Common Tasks" section includes the following options:

- Default Privilege: 15 (Select 0 to 15)
- Maximum Privilege: (Select 0 to 15)
- Access Control List: (Select 0 to 15)
- Auto Command: (Select 0 to 15)
- No Escape: (Select true or false)
- Timeout: (Select 0 to 15)
- Idle Time: (Select 0 to 15)

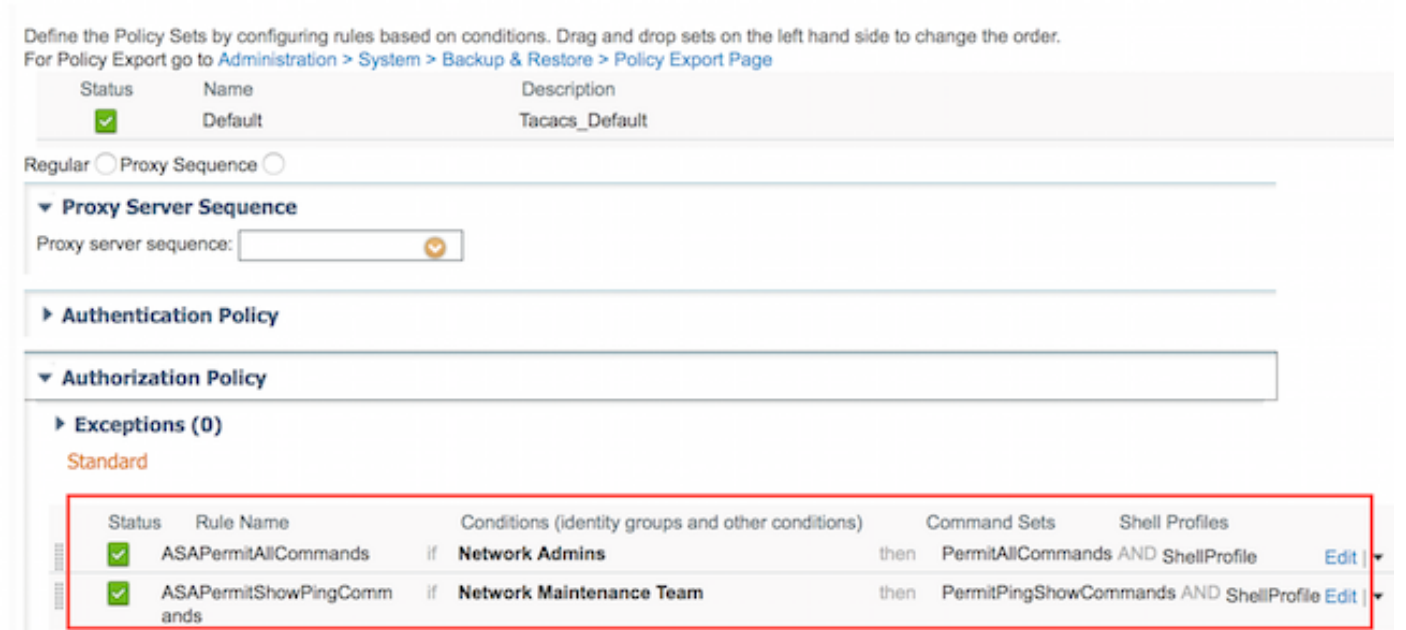
配置TACACS授权策略

默认情况下认证策略指向All_User_ID_Stores，包括本地存储，因此保持不变。

连接对**工作区>设备管理>Policy集>默认>授权策略> Edit >上面插入新规则**。



被配置的两个授权rulesare，第一个规则分配TACACS配置文件ShellProfile和set命令根据网络管理员用户身份组成员的PermitAllCommands。第二个规则分配TACACS配置文件ShellProfile和set命令根据网络维护小组用户身份组成员的PermitPingShowCommands。



配置认证和授权的Cisco ASA防火墙

1. 用退路的充分的权限创建一个本地用户用username命令如显示这里

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. 定义TACACS服务器ISE，指定接口、协议IP地址和TACACS键。

```
ciscoasa(config)# username cisco password cisco privilege 15
```

Note:服务器密钥在ISE服务器应该匹配那个定义了前。

3. 测试与测试的TACACS服务器可到达性aaa命令如显示。

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

前面的命令的输出表示，TACACS服务器可及的，并且用户成功验证。

4. 配置SSH、exec授权和命令授权的认证如下所示。使用AAA认证exec认证服务器自动enable(event)您在privileged EXEC模式将自动地安置。

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

Note:用以上的命令，认证在ISE完成，用户被放置直接地到特权模式，并且authorization命令发生。

5. 允许嘘在mgmt接口。

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

Verify

Cisco ASA防火墙验证

1. 对ASA防火墙的SSH作为属于全部存取的用户身份组的管理员。网络管理员组被映射对ShellProfile和PermitAllCommands Set命令在ISE。设法运行所有命令保证全部存取。

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
ciscoasa#
```

2. 对ASA防火墙的SSH作为属于有限享用用户身份组的用户。网络维护组被映射对ShellProfile和PermitPingShowCommands Set命令在ISE。设法运行所有命令保证只显示，并且可以发出查验命令。

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
```

```

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed

```

ISE 2.0验证

1. 连接对操作> TACACS Livelog。保证完成的尝试以上被看到。

Generated Time	Status	Username	Type	Authentication Policy	Authorization Policy	ISE N
2015-08-19 13:47:24.135	❌	user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:47:15.139	❌	user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:47:07.452	✅	user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:46:56.816	✅	user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:46:49.961	✅	user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:46:35.595	✅	user	Authorization		Tacacs_Default >> ASAPermitShowPingComma...	Joey
2015-08-19 13:46:35.581	✅	user	Authentication	Tacacs_Default >> Default >> Default		Joey
2015-08-19 13:46:20.209	✅	administrator	Authorization		Tacacs_Default >> ASAPermitAllCommands	Joey
2015-08-19 13:42:05.838	✅	administrator	Authorization		Tacacs_Default >> ASAPermitAllCommands	Joey
2015-08-19 13:42:04.886	✅	administrator	Authorization		Tacacs_Default >> ASAPermitAllCommands	Joey
2015-08-19 13:42:02.575	✅	administrator	Authorization		Tacacs_Default >> ASAPermitAllCommands	Joey

2. 点击详细资料其中一个红色报告，及早就执行的失败的命令能被看到。

Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229297775/274
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> ASAPermitShowPingCommands
Shell Profile	
Matched Command Set	
Command From Device	traceroute 8.8.8.8

Troubleshoot

Error:失败尝试：出故障的Authorization命令

检查SelectedCommandSet属性验证期望的命令集由授权策略选择

Related Information

[Technical Support & Documentation - Cisco Systems](#)

[ISE 2.0版本注释](#)

[ISE 2.0硬件安装指南](#)

[ISE 2.0升级指南](#)

[对ISE迁移工具指南的ACS](#)

[ISE 2.0激活目录集中指南](#)

[ISE 2.0引擎管理员指南](#)