使用思科身份服务引擎2.4配置ASR9K TACACS

目录

简介

本文档介绍ASR 9000系列聚合服务路由器(ASR)的配置，以便通过TACACS+与思科身份服务引擎2.4服务器进行身份验证和授权。

背景信息

它举例说明了在Cisco IOS® XR软件系统中用于控制用户访问的基于任务的授权管理模型的实施。实施基于任务的授权所需的主要任务涉及如何配置用户组和任务组。用户组和任务组通过Cisco IOS® XR软件命令集进行配置，该命令集用于身份验证、授权和记帐(AAA)服务。身份验证命令用于验证用户或主体的身份。授权命令用于验证已通过身份验证的用户（或主体）是否被授予执行特定任务的权限。记帐命令用于记录会话，并通过记录特定用户或系统生成的操作来创建审计跟踪。

先决条件

要求

Cisco 建议您了解以下主题：

- ASR 9000部署和基本配置
- TACACS+协议

- ISE 2.4部署和配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带Cisco IOS® XR软件的ASR 9000，版本5.3.4
- 思科ISE 2.4

本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果网络处于活动状态，请确保完全了解任何配置更改的潜在影响。

配置

IOS® XR上的预定义组件

IOS® XR中有预定义的用户组和任务组。管理员可以使用这些预定义组或根据要求定义自定义组。

预定义用户组

这些用户组在IOS® XR上预定义：

用户组	权限
思科支持	调试和故障排除功能（通常由思科技术支持人员使用）。
netadmin	配置网络协议，如开放最短路径优先(OSPF)（通常由网络管理员使用）。
操作员	执行日常监控活动，并具有有限的配置权限。
root-lr	在单个RP中显示并执行所有命令。
根系统	显示并执行系统中所有RP的所有命令。
sysadmin	执行路由器的系统管理任务，例如维护核心转储的存储位置或设置网络时间协议(NTP)时钟。
serviceadmin	执行服务管理任务，例如会话边界控制器(SBC)。

每个预定义用户组都映射了某些任务组，无法修改。使用以下命令检查预定义的用户组：

```
RP/0/RSP0/CPU0:ASR9k#sh aaa usergroup ?

 |              Output Modifiers
 root-lr        Name of the usergroup
 netadmin       Name of the usergroup
 operator       Name of the usergroup
 sysadmin       Name of the usergroup
 retrieval      Name of the usergroup
 maintenance    Name of the usergroup
 root-system    Name of the usergroup
 provisioning   Name of the usergroup
 read-only-tg   Name of the usergroup
 serviceadmin   Name of the usergroup
 cisco-support  Name of the usergroup
 WORD           Name of the usergroup
 <cr>
```

预定义任务组

这些预定义任务组可供管理员使用，通常用于初始配置：

- 思科支持：思科支持人员任务
- netadmin:网络管理员任务
- 运算符：操作员日常任务（用于演示目的）
- root-lr:保护域路由器管理员任务
- 根系统：系统级管理员任务
- sysadmin:系统管理员任务
- serviceadmin:服务管理任务

使用以下命令检查预定义的任务组：

```
RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup ?

|              Output Modifiers
root-lr        Name of the taskgroup
netadmin       Name of the taskgroup
operator       Name of the taskgroup
sysadmin       Name of the taskgroup
root-system    Name of the taskgroup
serviceadmin   Name of the taskgroup
cisco-support  Name of the taskgroup
WORD           Name of the taskgroup
<cr>
```

```
RP/0/RSP1/CPU0:ASR9k#show aaa task supported
```

AAA	ACL	管理员	Ancp	ATM	基本服务	BCDL	BFD	调试输出中显示“bgp
Boot	捆绑包	呼叫总部	CDP	CEF	CGN	思科支持	config-mgmt	config-services
加密	迪亚格	禁止	驱动程序	DWDM	埃姆	EIGRP	以太网服务	ext-access
交换矩阵	故障管理器	文件系统	防火墙	Fr	HDLC	主机服务	hsrp	接口
资产	IP服务	Ipv4	IPv6	ISIS	L2vpn	李	Lisp	日志记录
lpts	监控	mpls-ldp	mpls-static	mpls-te	组播	Netflow	网络	nps
OSPF	乌尼	PBR	pkg-mgmt	pos-dpt	PPP	QoS	rcmd	肋
安息	root-lr	根系统	route-map	路由策略	SBC	SNMP	SONET-SDH	静态
Sysmgr	system	传输	tty-access	隧道	通用	Vlan	VPDN	vrrp

上述每项任务都可以具有以下任意或全部四种权限：

阅读 指定仅允许读取操作的指定。
写入 指定允许更改操作并隐式允许读取操作的指定。
执行 指定允许访问操作的指定；例如，ping和Telnet。
调试 指定允许调试操作的指定。

用户定义的任务组

管理员可以配置自定义任务组以满足特定需求。以下是配置示例：

```
RP/0/RSP1/CPU0:ASR9k(config)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-tg)#task ?
  debug    Specify a debug-type task ID
  execute  Specify a execute-type task ID
```

```
  read     Specify a read-type task ID
  write    Specify a read-write-type task ID

RP/0/RSP1/CPU0:ASR9k(config-tg)#task read aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task debug aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task read acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#commit

RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup TAC-Defined-TASK
Task group 'TAC-Defined-TASK'

Task IDs included directly by this group:
Task:                   aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                   acl  : READ    WRITE    EXECUTE

Task group 'TAC-Defined-TASK' has the following combined set
  of task IDs (including all inherited groups):
Task:                   aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                   acl  : READ    WRITE    EXECUTE
```

Describe命令可用于查找特定命令需要什么任务组和权限。

示例 1.

```
RP/0/RSP1/CPU0:ASR9k#describe show aaa usergroup
Package:
.....
User needs ALL of the following taskids:

aaa (READ)
RP/0/RSP1/CPU0:ASR9k#
```

为了允许用户运行命令show aaa usergroup，应将**task group: task read aaa** 分配给**该用户**组。

示例 2.

```
RP/0/RSP1/CPU0:ASR9k(config)#describe aaa authentication login default group tacacs+
Package:
.....
User needs ALL of the following taskids:

aaa (READ WRITE)
RP/0/RSP1/CPU0:ASR9k(config)#
```

为了允许用户在配置模式下运行**commandaa authentication login default group tacacs+**，应将任务组: **task read write aaa** 分配给用户组。

管理员可以定义可以继承多个任务组的用户组。以下是配置示例：

```
RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:50:56.799 UTC
```

```
User group 'TAC-Defined'
  Inherits from task group 'operator'

User group 'TAC-Defined' has the following combined set
  of task IDs (including all inherited groups):
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ

RP/0/RSP1/CPU0:ASR9k#conf t
RP/0/RSP1/CPU0:ASR9k(config)#usergroup TAC-Defined
RP/0/RSP1/CPU0:ASR9k(config-ug)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-ug)#commit

RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:51:31.494 UTC
User group 'TAC-Defined'
  Inherits from task group 'operator'
  Inherits from task group 'TAC-Defined-TASK'

User group 'TAC-Defined' has the following combined set
  of task IDs (including all inherited groups):
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

路由器上的AAA配置

在ASR路由器上配置TACACS服务器，使用IP地址和共享密钥。

```
RP/0/RSP1/CPU0:ASR9k(config)#tacacs-server host 10.106.73.233 port 49
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#key 0 cisco
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#commit

!
tacacs-server host 10.127.196.160 port 49
key 7 14141B180F0B
!
```

配置身份验证和授权以使用已配置的TACACS服务器。

```
#aaa authentication login default group tacacs+ local
#aaa authorization exec default group tacacs+ local
```

配置命令授权以使用已配置的TACACS服务器（可选）：

> **注意：**确保身份验证和授权按预期工作，并确保在启用命令授权之前也正确配置命令集。如果配置不正确，用户可能无法在设备上输入任何命令。

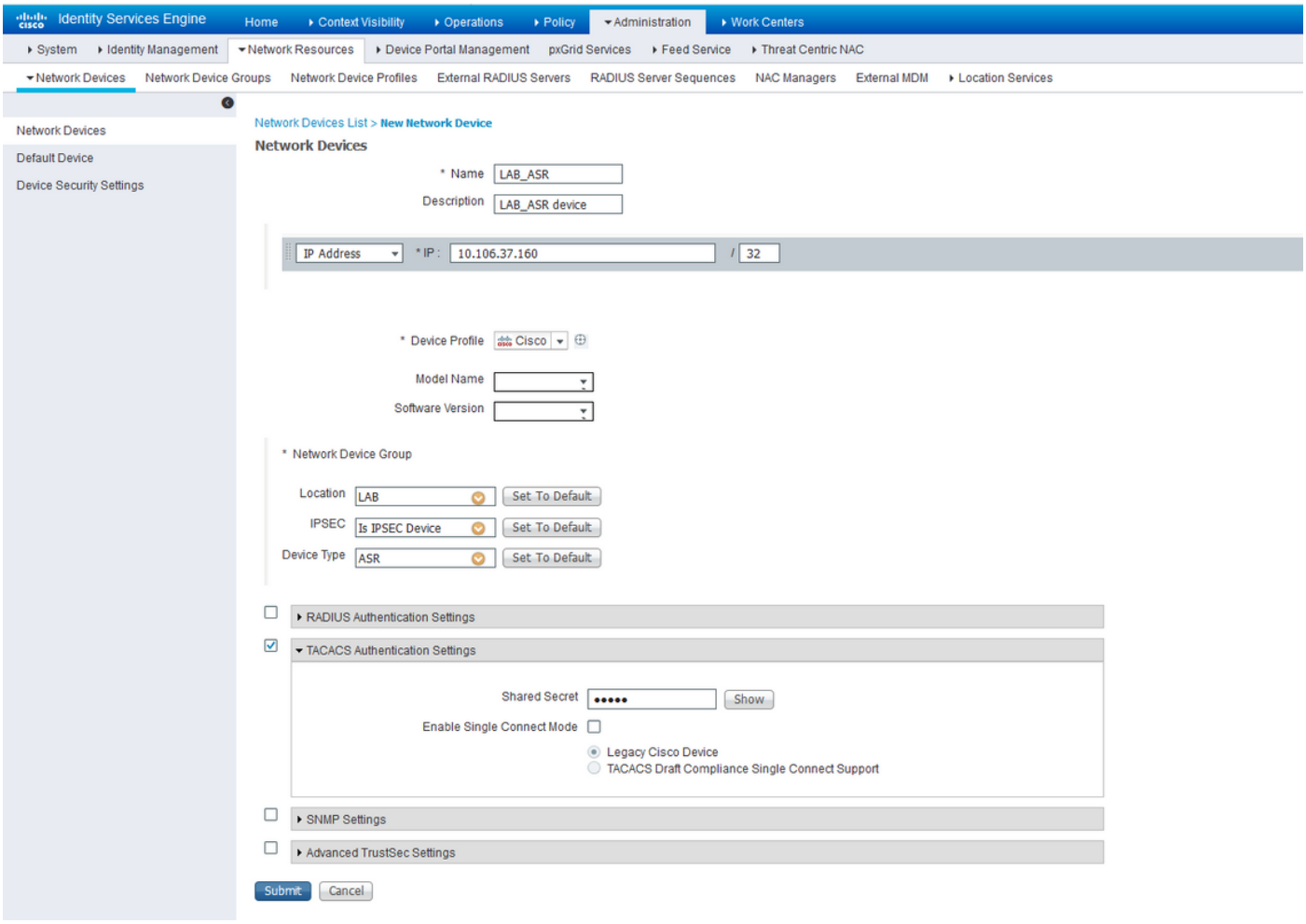
```
#aaa authorization commands default group tacacs+
```

配置命令记帐以使用已配置的TACACS服务器（可选）。

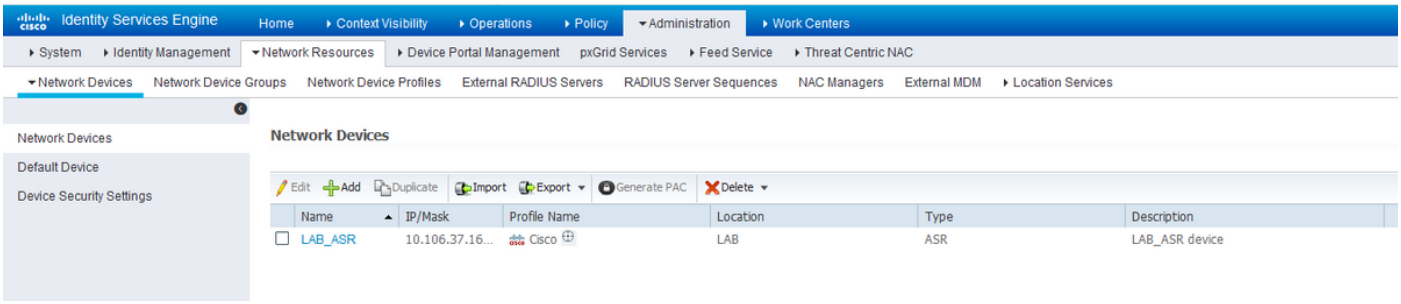
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ISE服务器配置

步骤1.要在ISE服务器上的AAA客户端列表中定义路由器IP，请导航至**Administration > N网络资源>网络设备** 如图所示。共享密钥应与在ASR路由器上配置的密钥相同，如图所示。



网络设备配置

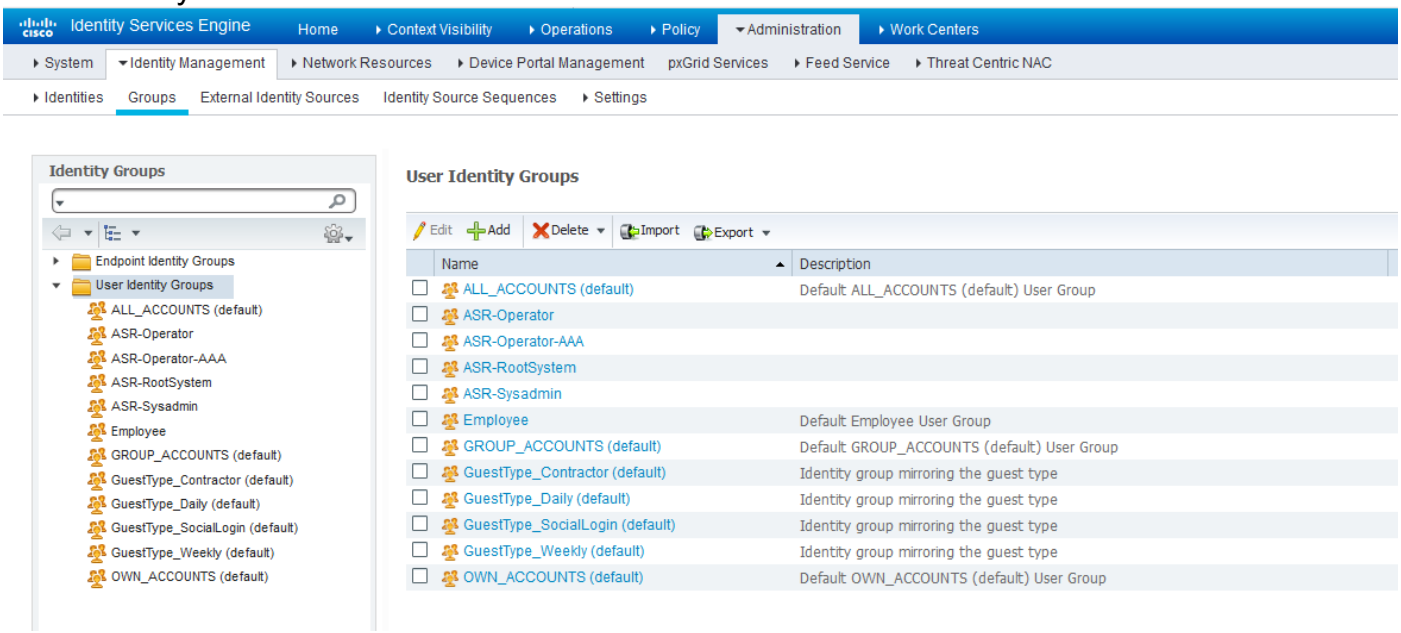


网络设备配置

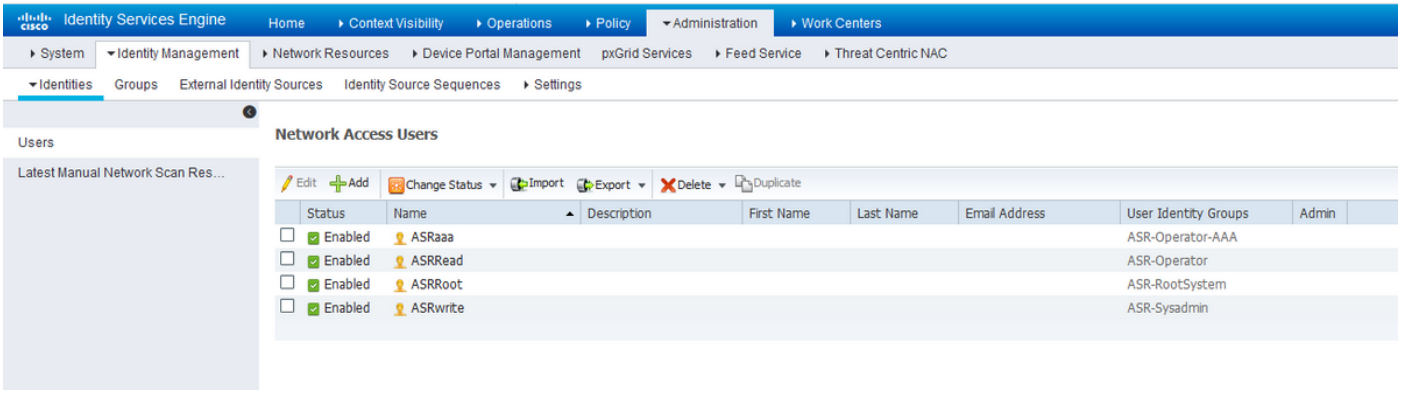
步骤2.根据您的要求定义用户组，在示例中，如本图所示，您使用四个组。可以在“管理”>“身份**管理**”>“**组**”>“**用户身份组**”下定义组。本示例中创建的组包括：

1. ASR操作员
2. ASR-Operator-AAA

3. ASR根系统
4. ASR-Sysadmin



身份组步骤3.如图所示，创建用户并将其映射到之前创建的相应用户组。



身份/用户

注意：在本例中，ISE内部用户用于身份验证和授权。使用外部身份源进行身份验证和授权不在本文档的范围内。

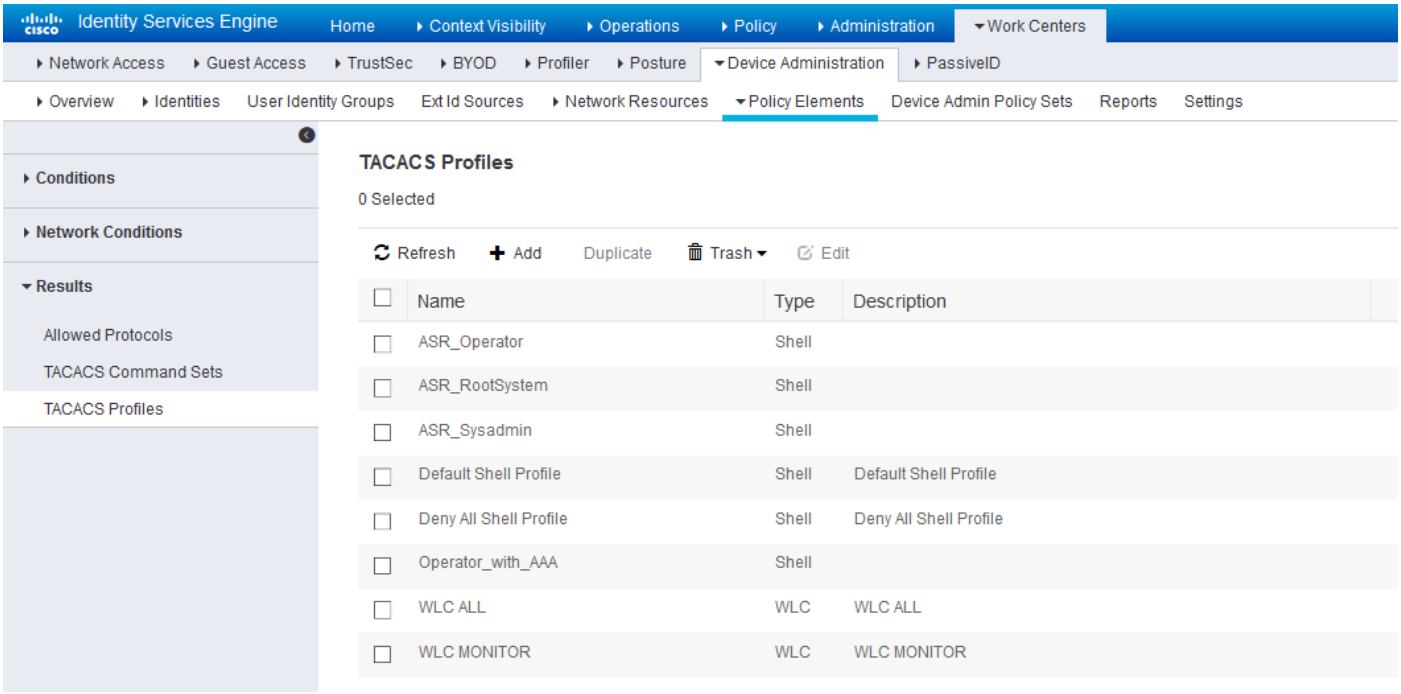
步骤4.定义要为各个用户推送的外壳配置文件。为此，请导航至工作中心(**Work Centers)>设备管理(Device Administration)>策略元素(Policy Elements)>结果(Results)> TACACS配置文件(TACACS Profiles)**。您可以配置新的外壳配置文件，如图所示，也可以配置ISE的早期版本。本示例中定义的外壳配置文件如下：

1. ASR_Operator

2. ASR_RootSystem

3. ASR_Sysadmin

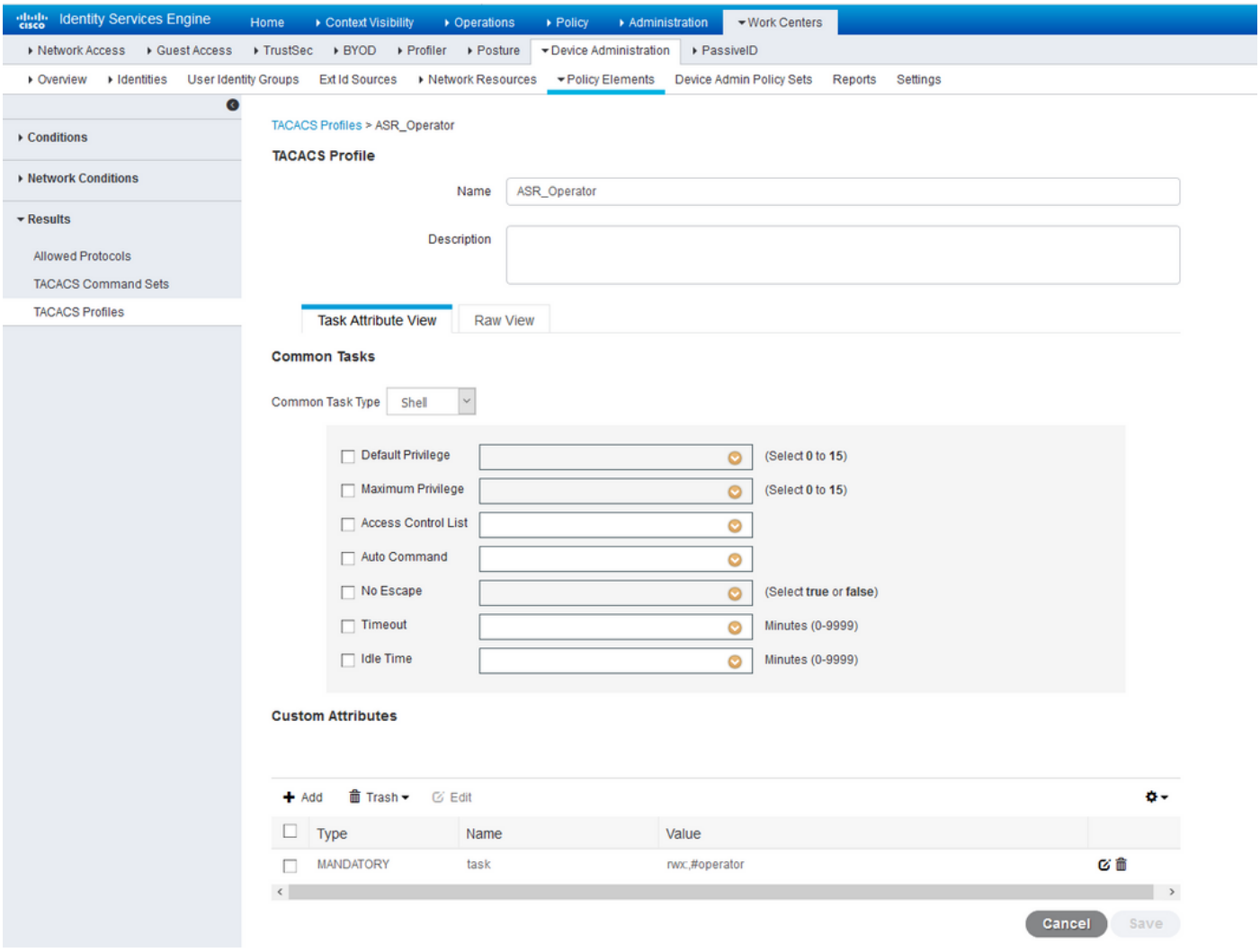
4. Operator_with_AAA



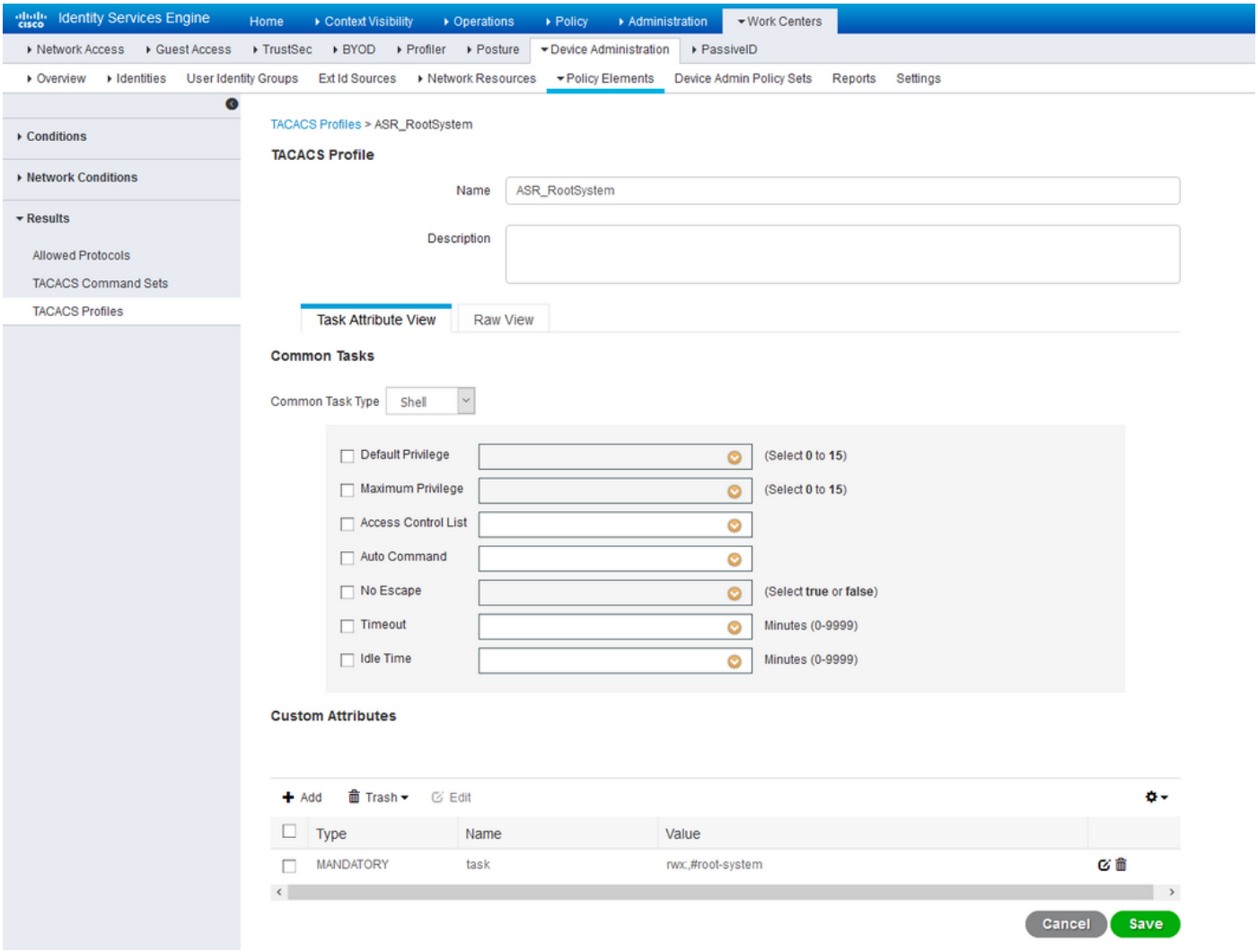
TACACS的外壳配置文件

单击“添加”**按钮**可输入“类型”、“名称”和“值”字段，如“自定义属性”部分下**的图**像所示。

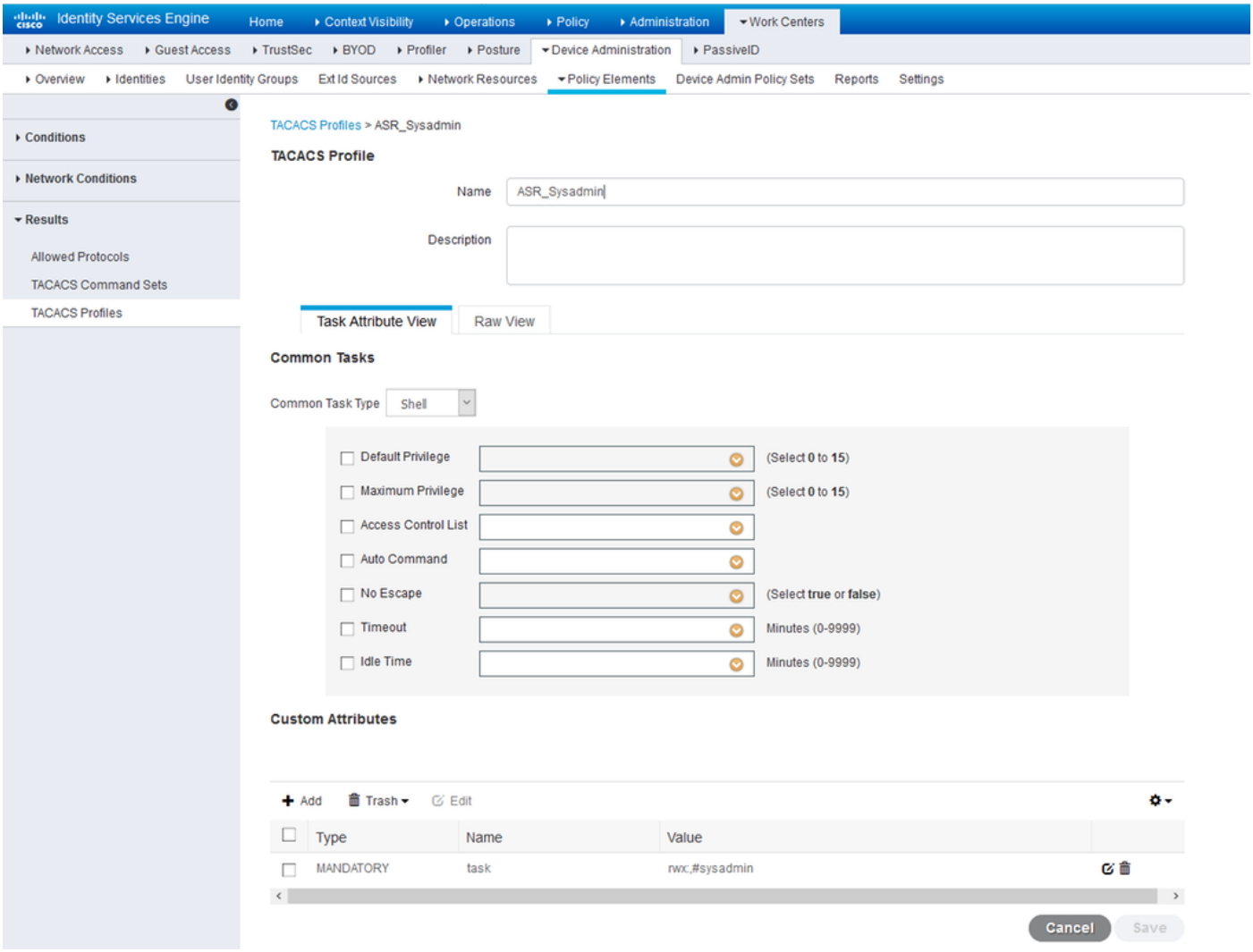
对于操作员角色：



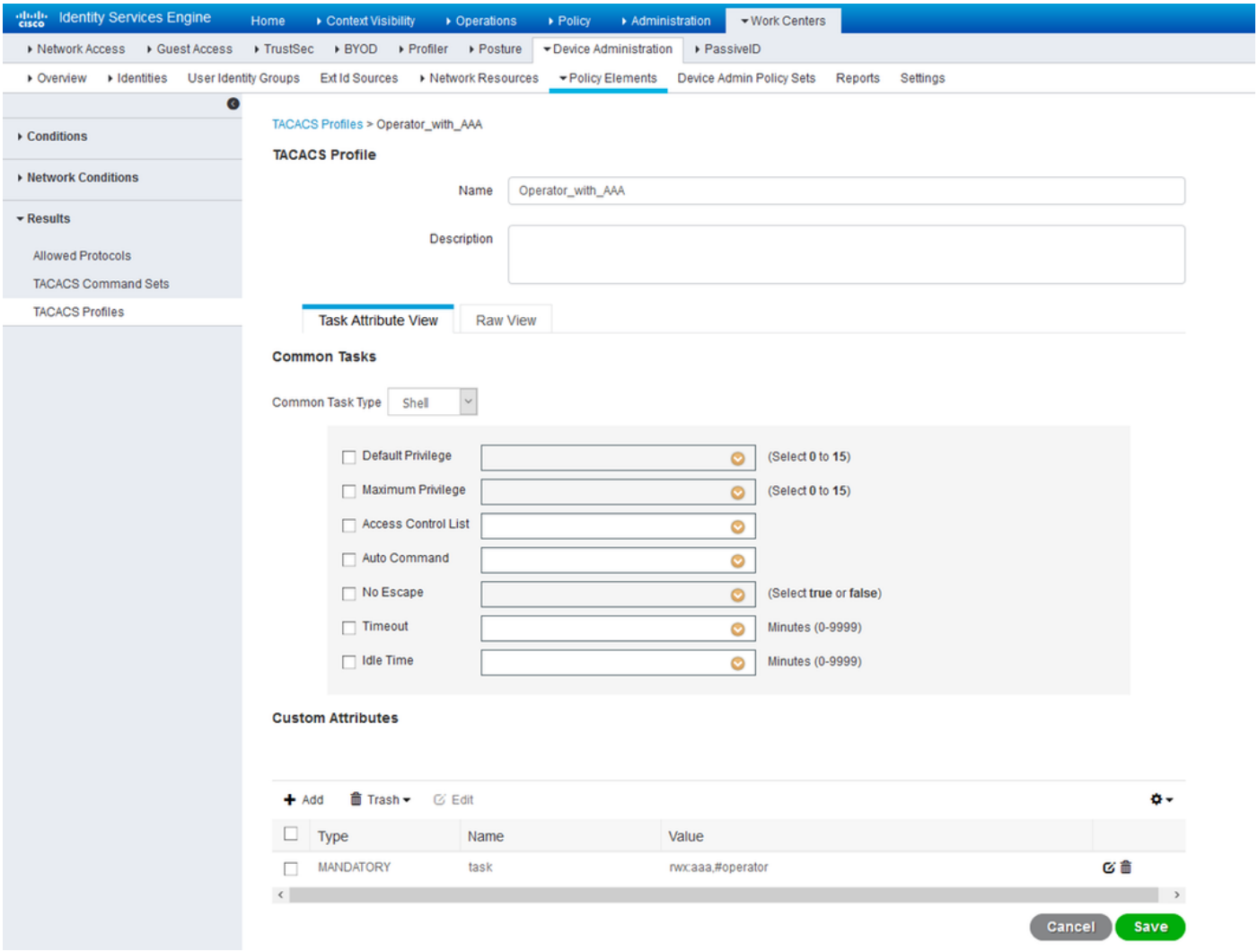
ASR操作员外壳配置文件对于根系统角色：



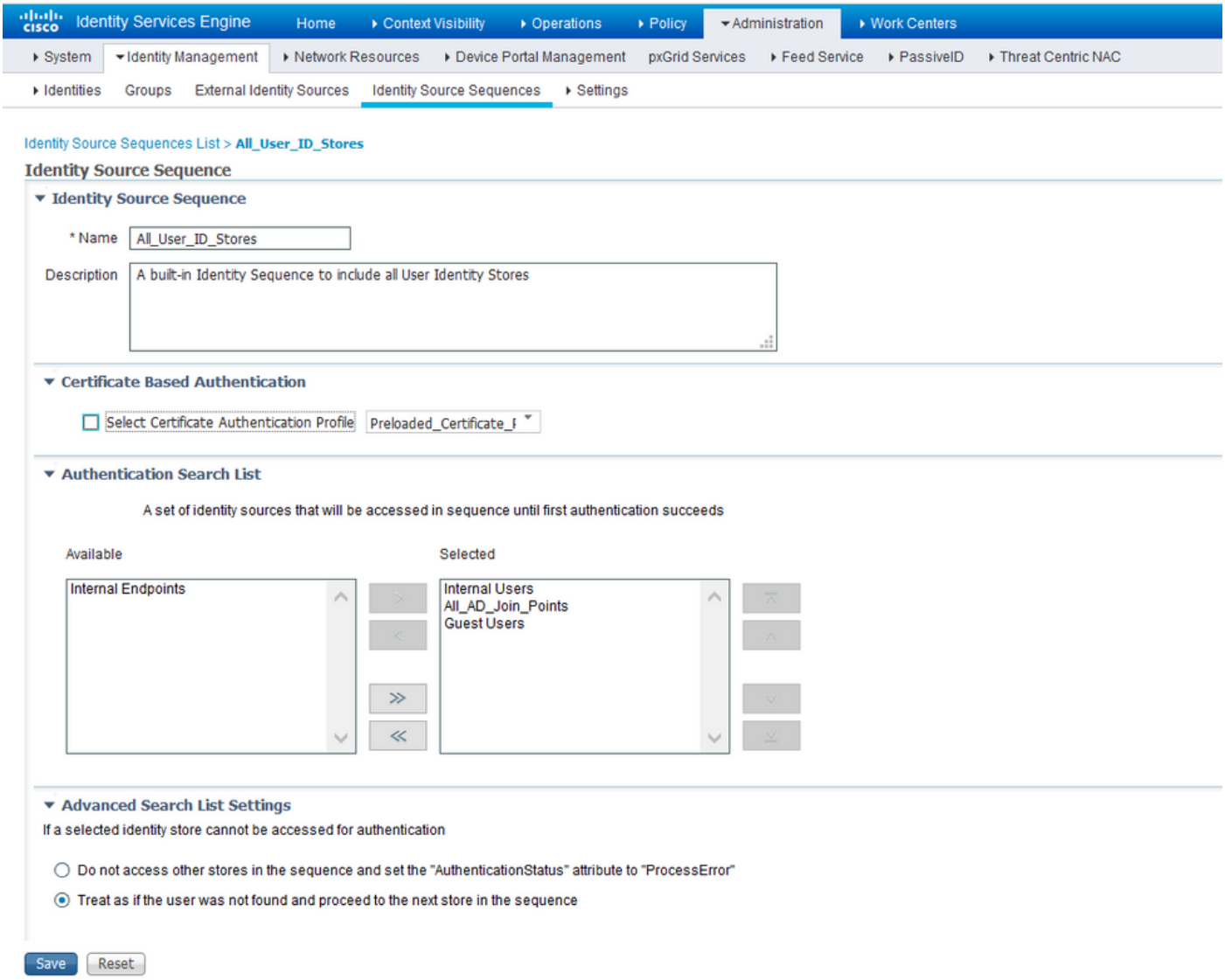
ASR根系统外壳配置文件对于sysadmin角色：



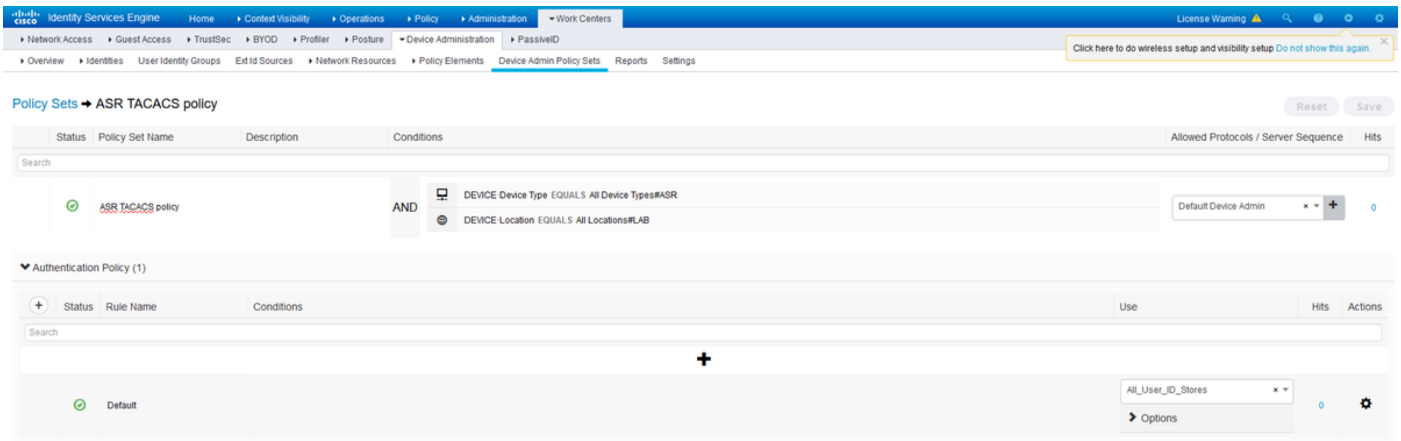
ASR Sysadmin外壳配置文件对于操作员和AAA角色：



具有AAA外壳配置文件的操作符步骤5.配置身份源序列，使用“管理”>“身份管理”>“身份源序列”中的“内**部用户”。您可以**添加新的身份源序列或编辑可用的身份源序列。

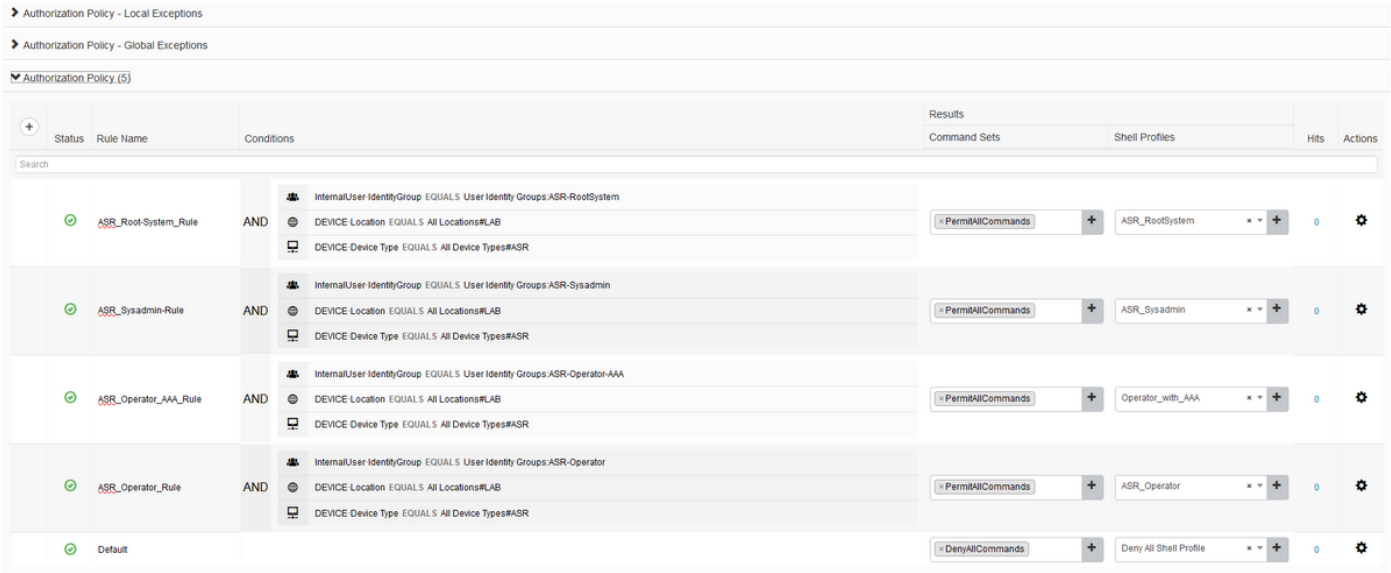


步骤6.在工作中心(Work Centers)>设备管理(Device Administration)>设备管理策略集(Device Admin Policy Sets)> [选择策略集]中配置身份验证策略，以便使用包含内部用户的身份库序列。使用之前创建的用户身份组根据要求配置授权并映射相应的外壳配置文件，如图所示。



验证策略

可根据要求以多种方式配置授权策略。此图中显示的规则基于设备位置、类型和特定内部用户身份组。所选的外壳配置文件将在授权时与命令集一起推送。



授权策略

验证

使用本部分可确认配置能否正常运行。

运算符

验证用户登录路由器时分配**的用**户组和任务组。

```
username: ASRread
password:

RP/0/RSP1/CPU0:ASR9k#show user
ASRread

RP/0/RSP1/CPU0:ASR9k#show user group
operator

RP/0/RSP1/CPU0:ASR9k#show user tasks
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

具有AAA的操作员

验证在以下情况下分配的用户组和任务组：**asraa** 用户登录路由器。

> 注意: **asraaai从TACACS服务器推送的操作员任务以及AAA任务读、写和执行权限。**

```
username: asraaa
password:

RP/0/RSP1/CPU0:ASR9k#sh user
asraaa
```

```
RP/0/RSP1/CPU0:ASR9k#sh user group
operator

RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:                  aaa  : READ    WRITE    EXECUTE
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

西萨德明

验证在以下情况下分配的用户组和任务组：**aswrite** 用户登录路由器。

```
username: asrwrite
password:

RP/0/RSP1/CPU0:ASR9k#sh user
asrwrite

RP/0/RSP1/CPU0:ASR9k#sh user group
sysadmin

RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:                  aaa  : READ
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ
Task:                 ancp  : READ
Task:                  atm  : READ
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ
Task:                  bfd  : READ
Task:                  bgp  : READ
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ
Task:            call-home  : READ
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ
Task:                  cgn  : READ
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ
Task:                 dwdm  : READ
Task:                  eem  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ
Task:    ethernet-services  : READ
--More--
(output omitted )
```

根系统

验证在以下情况下分配的用户组和任务组：**asroot** 用户登录路由器。

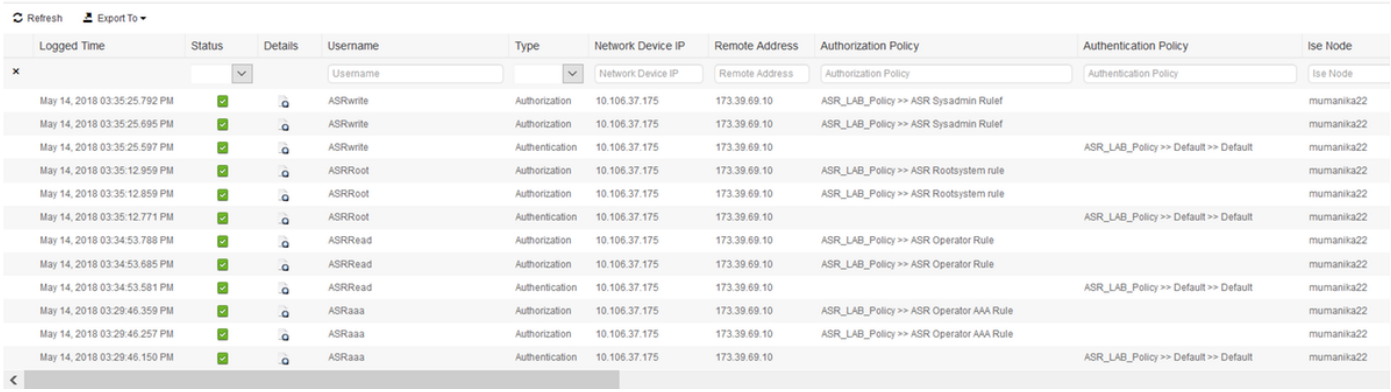
```
username: asrroot
```

```
password:

RP/0/RSP1/CPU0:ASR9k#show user
asrroot

RP/0/RSP1/CPU0:ASR9k#show user group
root-system

RP/0/RSP1/CPU0:ios#show user tasks
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ    WRITE    EXECUTE    DEBUG
Task:                ancp  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                 bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                 bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                boot  : READ    WRITE    EXECUTE    DEBUG
Task:              bundle  : READ    WRITE    EXECUTE    DEBUG
Task:           call-home  : READ    WRITE    EXECUTE    DEBUG
Task:                 cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                 cef  : READ    WRITE    EXECUTE    DEBUG
Task:                 cgn  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:              crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                diag  : READ    WRITE    EXECUTE    DEBUG
Task:             drivers  : READ    WRITE    EXECUTE    DEBUG
Task:                dwdm  : READ    WRITE    EXECUTE    DEBUG
Task:                 eem  : READ    WRITE    EXECUTE    DEBUG
Task:               eigrp  : READ    WRITE    EXECUTE    DEBUG
--More--
(output omitted )
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

从Operations > TACACS > Live Logs**验证ISE报告**。单击放大镜符号以查看详细报告。



以下是一些有助于排除ASR故障的命令：

- **show users**
- **show user group**
- **显示用户任务**
- **show user all**