# 配置ASR9k TACACS用Cisco Secure ACS 5.x服务器

## 目录


[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[在IOS XP的预定义的组件](#)
[预定义的用户组](#)
[预定义的任务组](#)
[在IOS XP的用户定义的组件](#)
[用户定义的用户组](#)
[用户定义的任务组](#)
[在路由器的AAA配置](#)
[ACS服务器配置](#)
[验证](#)
[操作员](#)
[有AAA的操作员](#)
[Sysadmin](#)
[根系统](#)
[故障排除](#)


## 简介

本文描述ASR 9000系列聚合服务路由器(ASR)的配置通过TACACS+验证和授权用思科安全访问控制服务器(ACS) 5.x服务器。

此示例用于的基于任务的授权管理模型的实施控制在Cisco IOS XR软件系统的用户访问。要求的主要任务实现基于任务的授权介入如何配置用户组和任务组。用户组和任务组通过用于验证、授权和核算(AAA)服务的Cisco IOS XR软件set命令配置。认证命令用于验证用户或负责人的标识。授权命令用于验证已认证的用户(或负责人)授权权限执行一特定任务。记帐命令使用记录会话和创建审计追踪通过记录某些用户或系统生成的操作。

## 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

- ACS 5.x部署和配置。
- TACACS+协议

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 与Cisco IOS XR软件的ASR 9000，版本4.3.4
- Cisco Secure ACS 5.7

本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请确保您了解所有配置更改潜在影响。

# 配置

## 在IOS XP的预定义的组件

有预定义的用户组和任务组IOS XP的。管理员能使用这些预定义的组或根据需求定义自定义组。

### 预定义的用户组

这些用户组在IOS XP预定义：

| 用户组 | 权限 |
|---|---|
| cisco-support | 调试和排除功能故障(通常，使用由思科技术网络人员)。 |
| netadmin | Configure network协议例如开放最短路径优先(OSPF) (通常使用由网络管理员)。 |
| 操作员 | 执行每日监视活动，并且有受限的配置权利。 |
| 根LR | 显示并且执行在单个RP内的所有命令。 |
| 根系统 | 显示并且执行所有RP的所有命令在系统。 |
| sysadmin | 执行路由器的系统管理任务，例如维护core dump是存储或设置网络时间协议(NTP)时钟的地 |
| serviceadmin | 执行服务管理任务，例如会话博德控制器(SBC)。 |

根系统用户组预了定义授权;即它有对根系统用户托管型资源和某些责任的完整责任在其他服务中。

请使用这些命令检查预定义的用户组：

```
RP/0/RSP1/CPU0:ASR9k#show 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
  root-system    Name of the usergroup
  serviceadmin   Name of the usergroup
  cisco-support  Name of the usergroup
  WORD           Name of the usergroup
  <cr>
```

### 预定义的任务组

这些预定义的任务组是可用为了管理员能使用，典型地初始配置：

- cisco-support ：Cisco支持人员任务
- netadmin ：网络管理员任务
- 操作员：操作员每日任务(演示目的)
- 根LR ：安全域路由器管理员任务
- 根系统：全系统的管理员任务
- sysadmin ：系统管理员任务
- serviceadmin ：服务管理任务，例如， SBC

请使用这些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>
```

请使用此命令检查支持的任务：

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

这是支持的任务列表：

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Aaa | ACL | 管理员 | Ancp | Atm | 基本服务 | Bcdl | Bfd | bgp |
| 引导程序 | 套件 | 呼叫到家 | Cdp | CEF | Cgn | cisco-support | 设置mgmt | 设置服务 |
| crypto | Diag | 不允许 | 驱动程序 | Dwdm | Eem | Eigrp | 以太网服务 | ext访问 |
| 结构 | 故障Mgr | 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 | 口齿 | 记录 |
| Lpts | 箴言报 | MPLS LDP | MPLS静态 | MPLS TE | 组播 | Netflow | 网络 | NP |
| Ospf | Ouni | Pbr | PKG mgmt | POS DPT | Ppp | Qos | Rcmd | 肋骨 |
| RIP | 根LR | 根系统 | route-map | 路由策略 | Sbc | Snmp | SONET sdh | 静态 |
| 17-May-01 | 系统 | 传输 | TTY访问 | 通道 | 通用 | VLAN | VPDN | vrrp |

其中每一上述的任务可以给与其中每一个或所有四种权限。

| | |
|---|---|
| 读 | 指定允许仅读操作的指定。 |
| 写道 | 指定允许更改操作和隐含地允许读操作的指定。 |
| 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。 |

## 在IOS XP的用户定义的组件

### 用户定义的用户组

管理员能配置他自己的用户组适应特定的需要。 这是配置示例：

```
RP/0/RSP1/CPU0:ASR9k(config)#usergroup TAC-Defined
```

```
RP/0/RSP1/CPU0:ASR9k(config-ug)#taskgroup operator
RP/0/RSP1/CPU0:ASR9k(config-ug)#commit
```

**用户定义的任务组**

管理员能配置他们自己的任务组适应特定的需要。 这是配置示例：

```
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
```

如果不是肯定的如何查找什么任务组和权限为某一命令是需要的，您能使用**描述**命令查找它。 示例如下：

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show命令**aaa用户组**，您在任务组中需要允许此线路：

**任务读了aaa**

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)#
```

为了允许用户从配置模式运行aaa authentication login命令**默认组TACACS+**，您在任务组中需要允许此线路：

**任务读/写aaa**

您能定义能导入几个任务组的用户组。这是配置示例：

```
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
```

# 在路由器的AAA配置

定义在路由器的一个TACACS服务器：

您定义了ACS服务器IP地址作为与关键思科的tacacs-server

```
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 10.106.73.233 port 49
key 7 14141B180F0B
!
```

指向认证和授权外部TACACS服务器。

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

命令authorisation(optional) ：

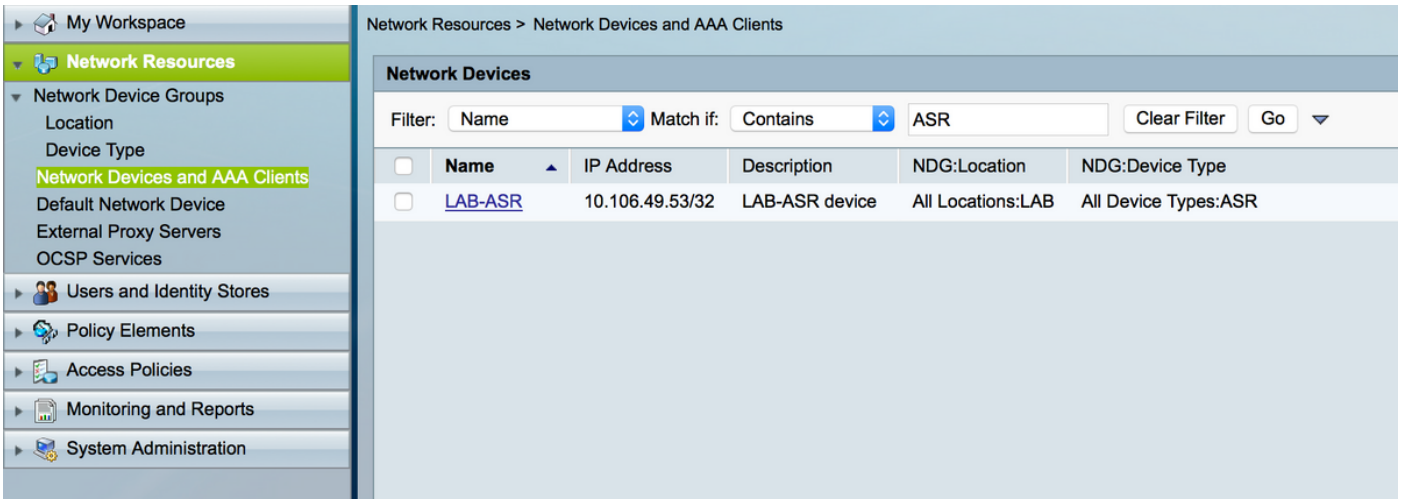
```
#aaa authorization commands default group tacacs+
```

指向核算外部服务器(可选)。

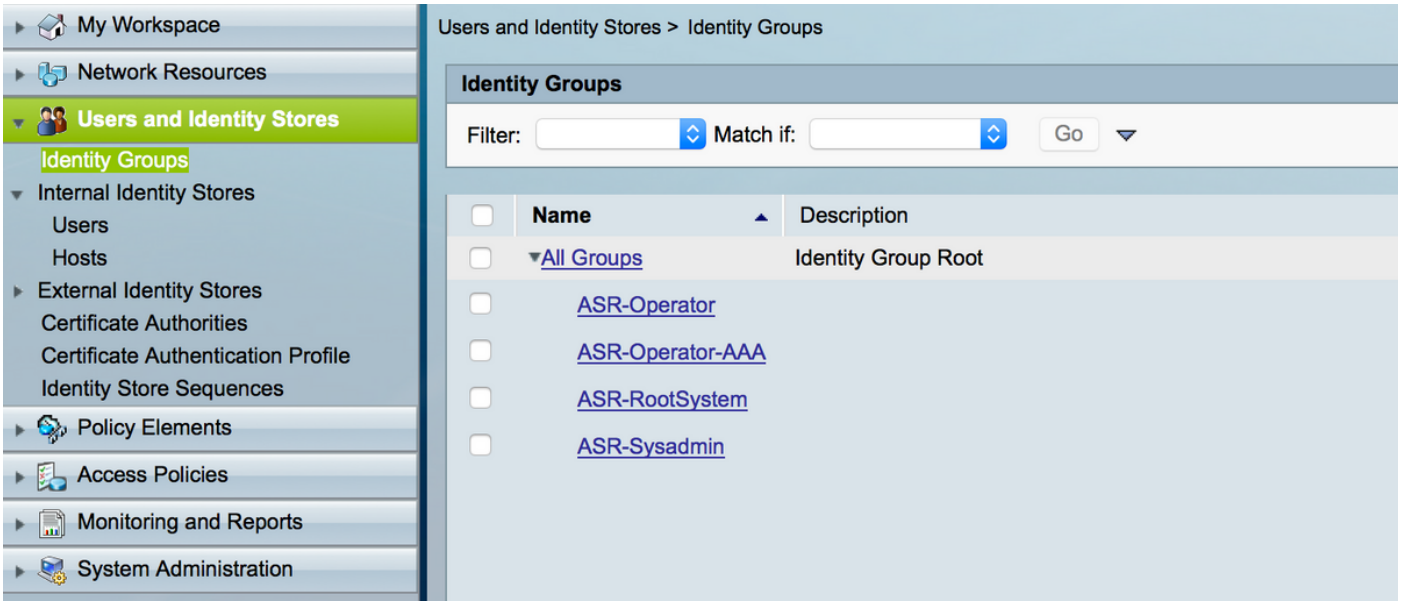
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

# ACS服务器配置

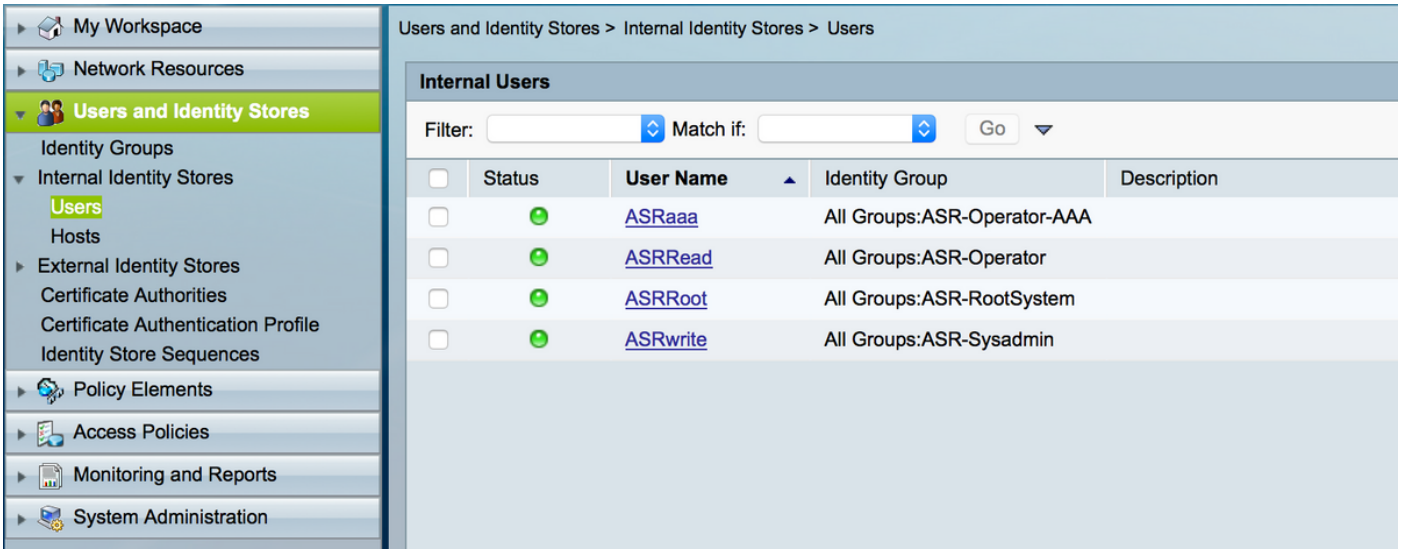
步骤1.如镜像所显示，为了定义在AAA客户端的路由器IP请列出在ACS服务器，导航给**网络资源>网络设备和AAA客户端**。在本例中，您定义了**cisco**作为共享塞克雷如ASR所配置的一样。




步骤2.如此镜像所显示，根据您的需求定义用户组，在示例，您使用四组。

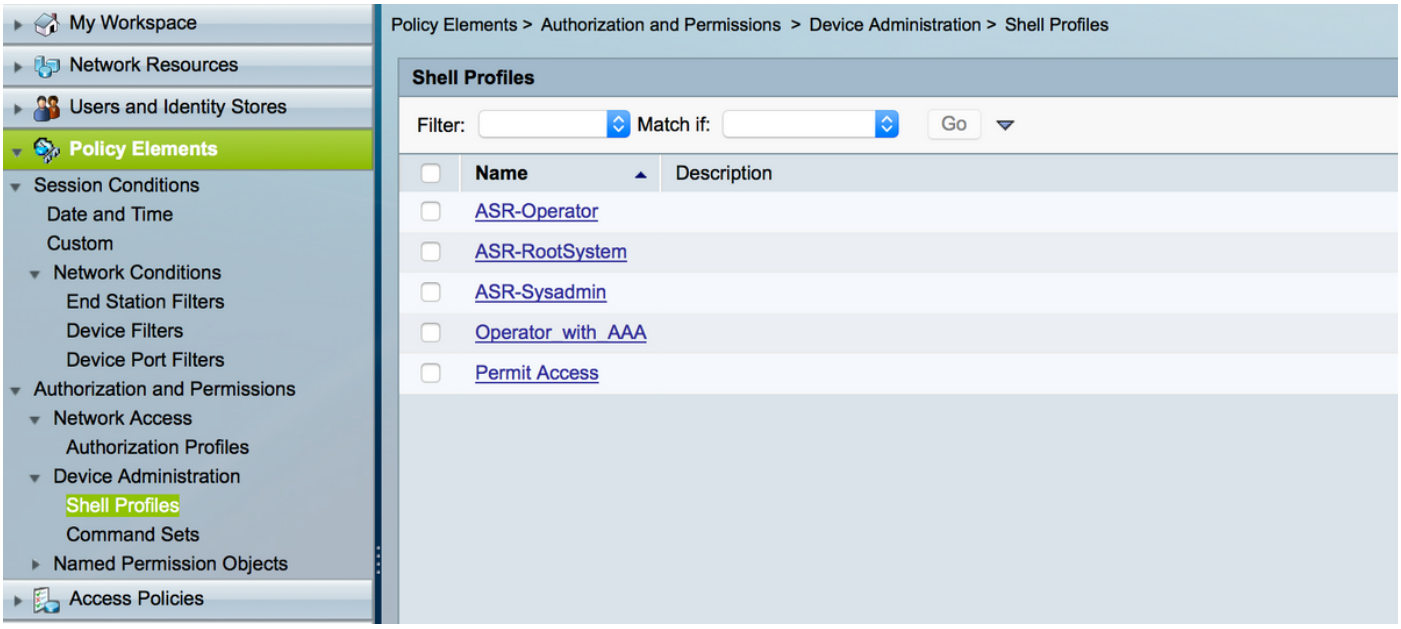



步骤3.如镜像所显示，请创建用户并且映射他们给各自用户组创建以上。

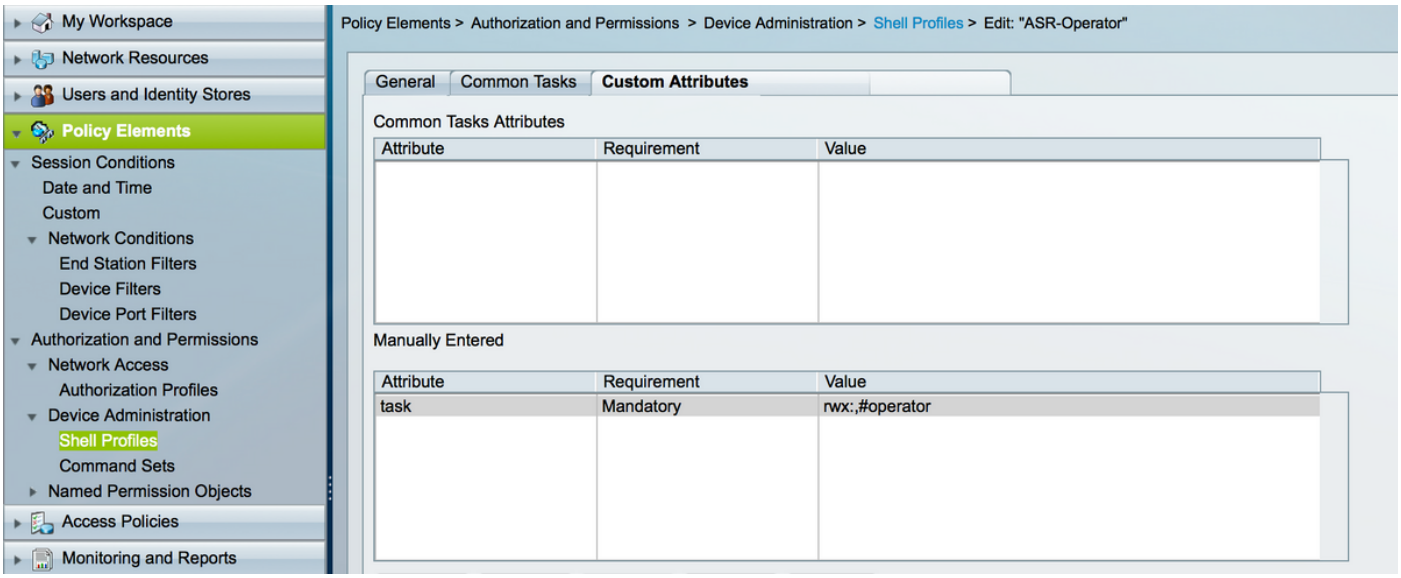


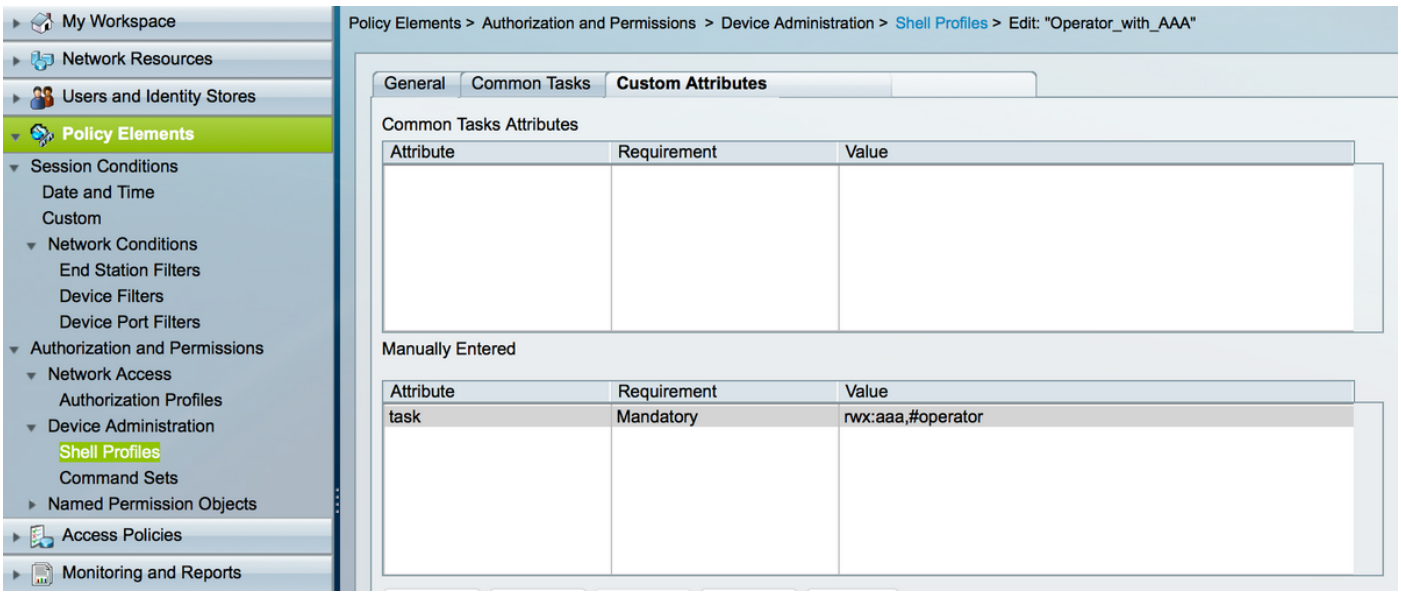

Note:在本例中，如果在外部标识要使用用户创建存储您能使用他们，使用验证的ACS内部用户。在本例中，外部标识来源用户没有被覆盖。

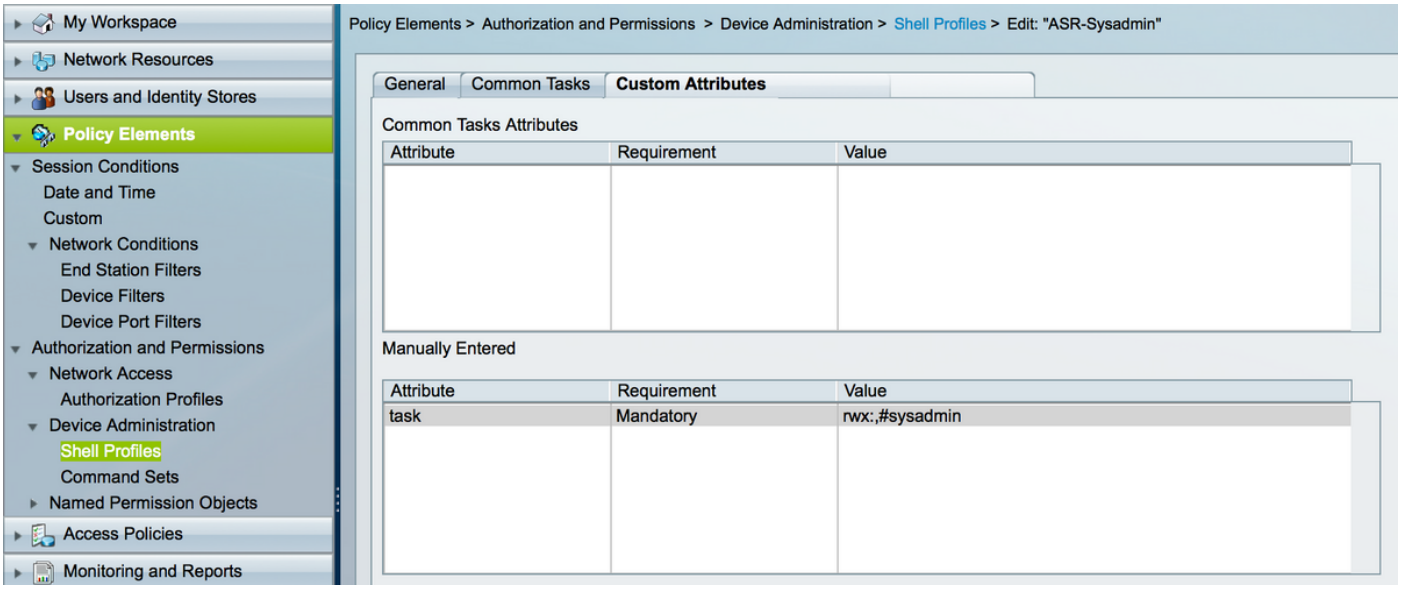
步骤4.定义您要争取各自用户的Shell配置文件。

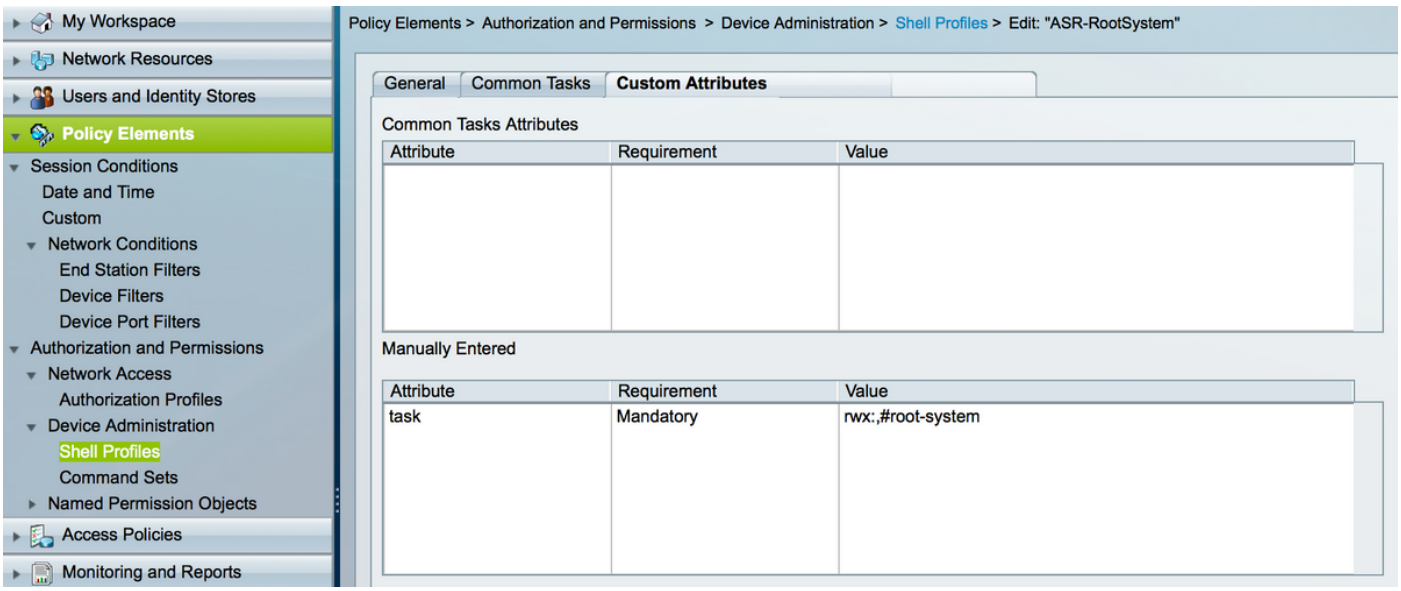



如镜像所显示，在已经已创建shell配置文件，您配置推送各自任务组。

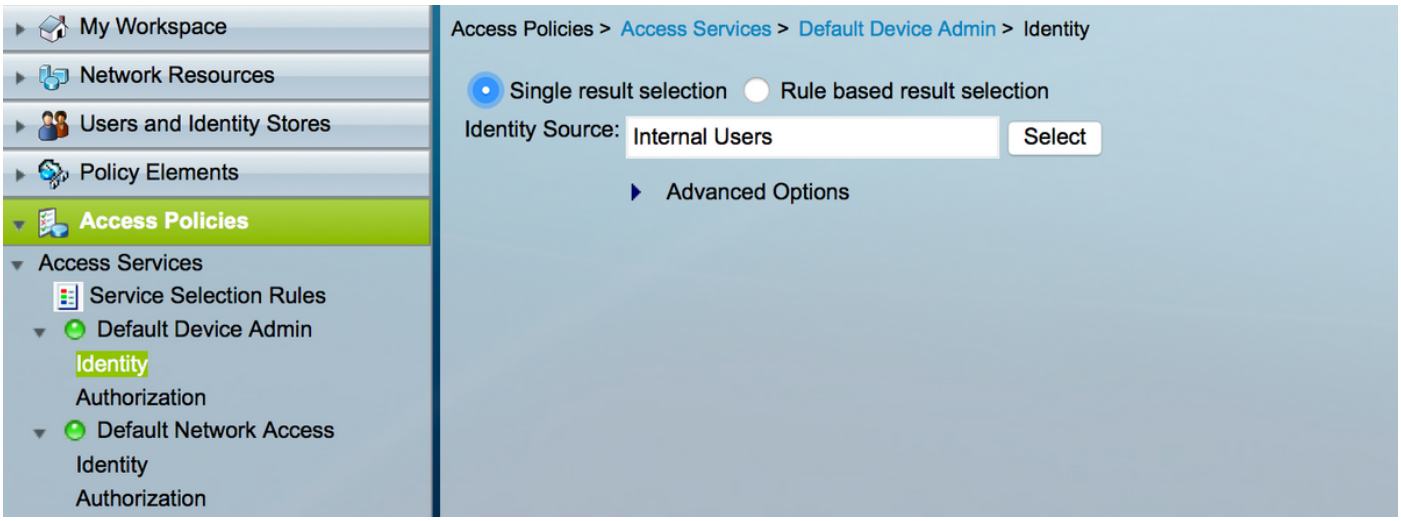


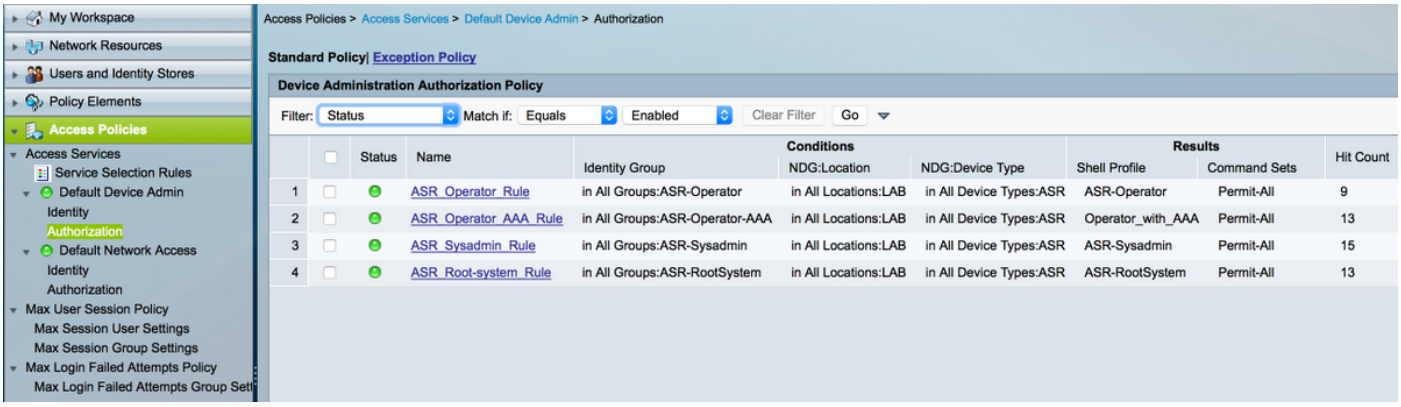



步骤5.定义访问策略。验证执行内部用户。




步骤6.如镜像所显示，配置根据需求的授权使用以前已创建用户标识组并且映射各自shell配置文件。




# 验证

## 操作员

为了登陆，使用用户名**asrread**。 这些是验证命令。

```
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
```

## 有AAA的操作员

为了登陆，使用用户名**asraaa**。这些是验证命令。

Note:asraaa是从TACACS服务器推送的操作员任务与读/写aaa的任务和执行权限一起。

```
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
```

## Sysadmin

为了登陆，使用用户名**asrwrite**。 这些是验证命令。

```
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

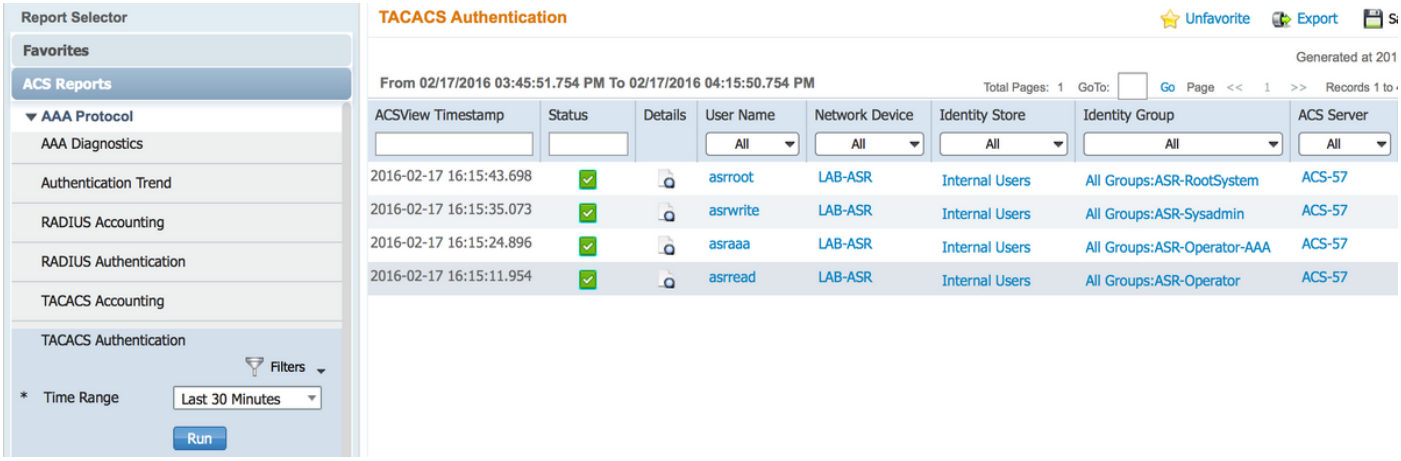
为了登陆，使用用户名**asrroot**。这些是验证命令。

```
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

您能验证从监听的ACS报告和报告页。 如镜像所显示，您可以点击放大镜sumbol发现详细的报告。




这些是一些个有用的命令排除故障在ASR ：

- **show users**
- **show users组**
- **show users任务**
- **show users全部**