使用思科身份服務引擎2.4配置ASR9K TACACS

目錄

簡介

本檔案將介紹ASR 9000系列聚合服務路由器(ASR)的配置，以便使用Cisco身份識別服務引擎2.4伺服器通過TACACS+進行身份驗證和授權。

背景資訊

其中範例說明在Cisco IOS® XR軟體系統中用於控制使用者存取的任務型授權管理模型的實作。實施基於任務的授權所需的主要任務包括如何配置使用者組和任務組。使用者組和任務組通過用於身份驗證、授權和記帳(AAA)服務的Cisco IOS® XR軟體命令集進行配置。身份驗證命令用於驗證使用者或主體的身份。授權命令用於驗證經過身份驗證的使用者（或主體）是否被授予執行特定任務的許可權。記帳命令用於記錄會話並通過記錄某些使用者或系統生成的操作來建立稽核跟蹤。

必要條件

需求

思科建議您瞭解以下主題：

- ASR 9000部署和基本配置
- TACACS+通訊協定

- ISE 2.4部署和配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用Cisco IOS® XR軟體版本5.3.4的ASR 9000
- Cisco ISE 2.4

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果網路處於活動狀態，請確保完全瞭解任何配置更改的潛在影響。

設定

IOS® XR上的預定義元件

IOS® XR中有預定義的使用者組和任務組。管理員可以使用這些預定義組，或根據需要定義自定義組。

預定義使用者組

這些使用者組是在IOS® XR上預定義的：

使用者組	許可權
思科支援	調試和故障排除功能（通常由思科技術支援人員使用）。
netadmin	配置網路協定，如開放最短路徑優先(OSPF)（通常由網路管理員使用）。
運算子	執行日常監視活動，並具有有限的配置許可權。
root-lr	顯示並執行單個RP中的所有命令。
根系統	顯示並執行系統中所有RP的所有命令。
sysadmin	執行路由器的系統管理任務，例如維護核心轉儲的儲存位置或設定網路時間協定(NTP)時鐘。
serviceadmin	執行服務管理任務，例如會話邊界控制器(SBC)。

每個預定義使用者組都有對映到的特定任務組，無法修改。使用以下命令檢查預定義使用者組：

```
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>
```

預定義任務組

管理員可以使用這些預定義任務組，通常用於初始配置：

- 思科支援：思科支援人員任務
- netadmin:網路管理員任務
- 操作員：操作員日常任務（用於演示）
- root-lr:安全域路由器管理員任務
- root-system:系統範圍的管理員任務
- sysadmin:系統管理員任務
- serviceadmin:服務管理任務

使用以下命令檢查預定義的任務組：

```
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	Admin	Ancp	Atm	基本服務	Bcdl	Bfd	bgp
開機	套件組合	call-home	Cdp	Cef	Cgn	思科支援	config-mgmt	config-servic
加密	diag	不允許	驅動因素	Dwdm	Eem	Eigrp	ethernet-services	ext-access
交換矩陣	fault-mgr	檔案系統	防火牆	Fr	Hdlc	主機服務	Hsrp	介面
庫存	ip-services	Ipv4	Ipv6	ISIS	L2vpn	李	Lisp	日誌記錄
Lpts	監視	mpls-ldp	mpls-static	mpls-te	多點傳播	Netflow	網路	nps
Ospf	烏尼	Pbr	pkg-mgmt	pos-dpt	Ppp	Qos	Rcmd	肋
RIP	root-lr	根系統	route-map	route-policy	Sbc	Snmp	sonet-sdh	靜態
Sysmgr	系統	傳輸	tty-access	通道	通用	VLAN	Vpdn	vrrp

可以賦予上述每項任務其中任意一項或全部四項許可權：

讀取 指定僅允許讀取操作的指定。
寫入 指定允許更改操作並隱式允許讀取操作的指定。
執行 指定允許訪問操作的指定；例如ping和Telnet。
調試 指定允許調試操作的指定。

使用者定義的任務組

管理員可以配置自定義任務組以滿足特定需求。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 命令可用於查詢特定命令所需的任務組和許可權。

範例 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#
```

為了允許使用者運行**命令show aaa usergroup**，應將**task group** read aaa分配給該使用者組。

範例 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)#
```

為了允許使用者在配置模式下運行**命令身份驗證登入預設組tacacs+**，應該將task group: task read write aaa 分配給使用者組。

管理員可以定義可以繼承多個任務組的使用者組。以下是組態範例：

```
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

使用要使用的IP地址和共用金鑰配置ASR路由器上的TACACS伺服器。

```
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
!
```

配置身份驗證和授權，以便使用已配置的TACACS伺服器。

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

配置命令授權以使用配置的TACACS伺服器（可選）：

> **附註**：確保身份驗證和授權按預期工作，並確保在啟用命令授權之前正確配置命令集。如果未正確配置，使用者可能無法輸入裝置上的任何命令。

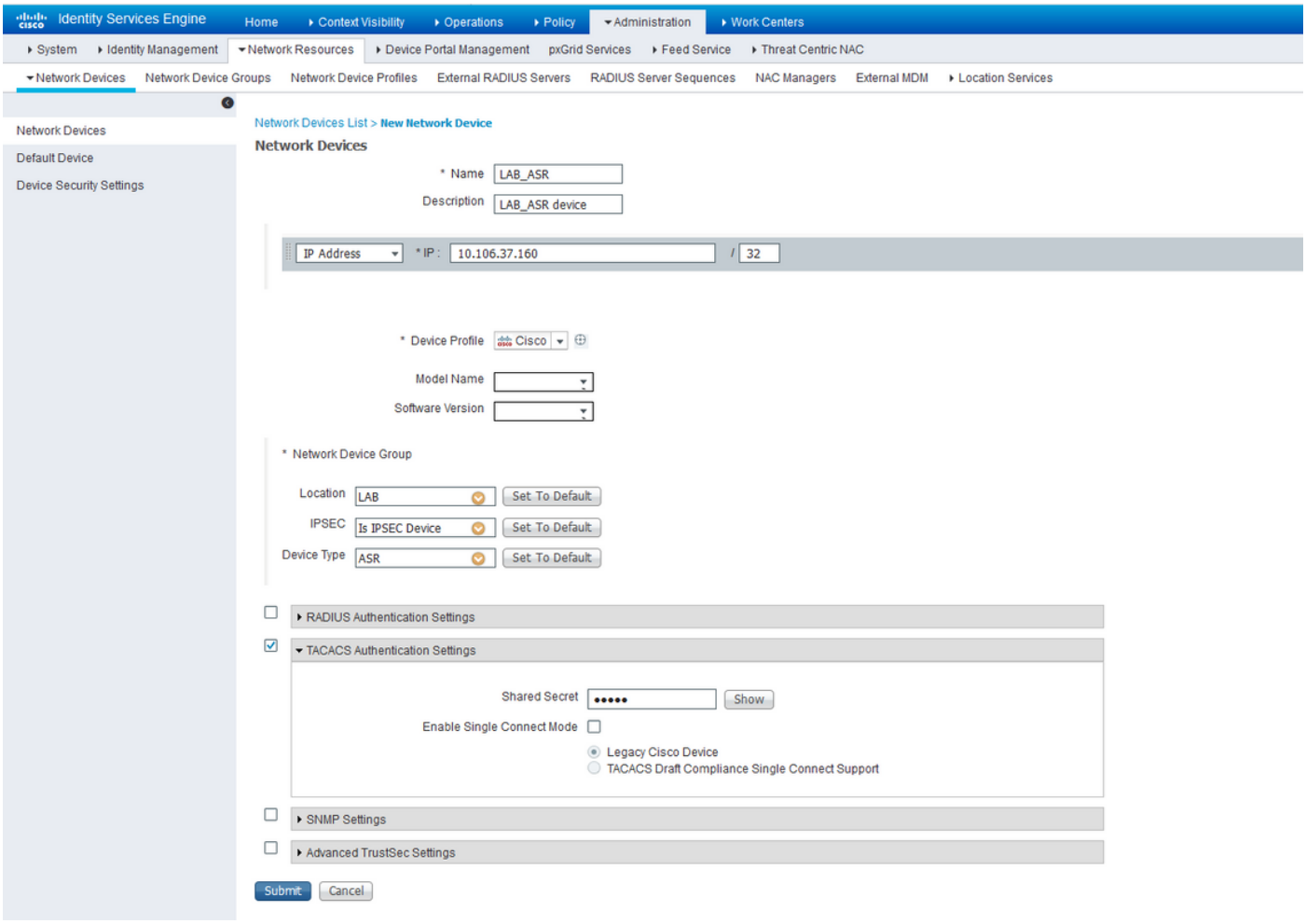
```
#aaa authorization commands default group tacacs+
```

配置命令記賬以使用已配置的TACACS伺服器（可選）。

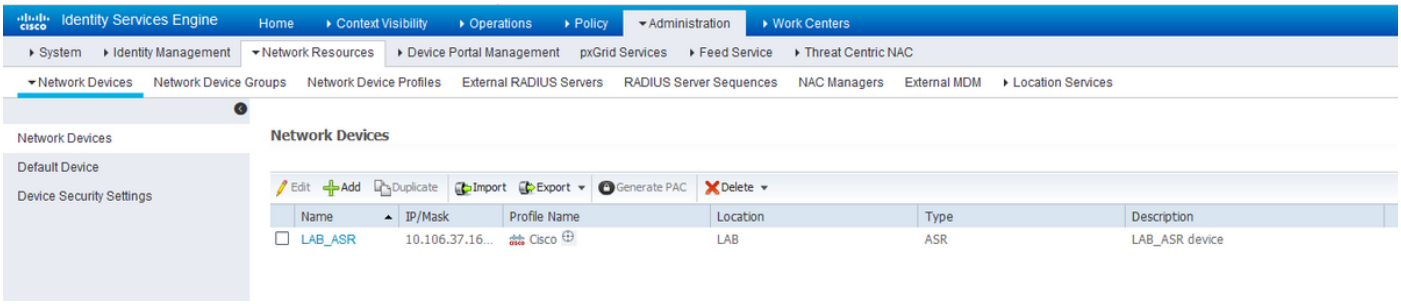
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ISE伺服器配置

步驟1。若要在ISE伺服器的AAA客戶端清單中定義路由器IP，請導航至**Administration > N網路資源>網路裝置** 如圖所示。共用金鑰應與ASR路由器上配置的共用金鑰相同，如圖所示。



網路裝置配置

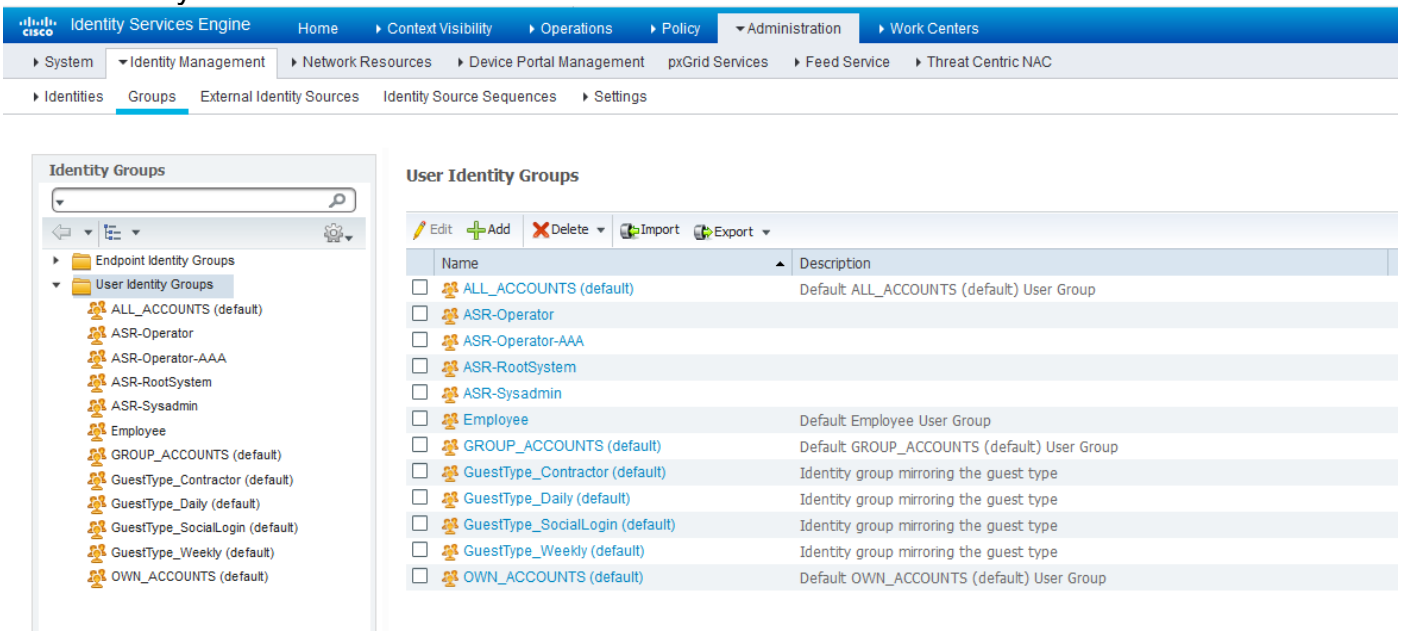


網路裝置配置

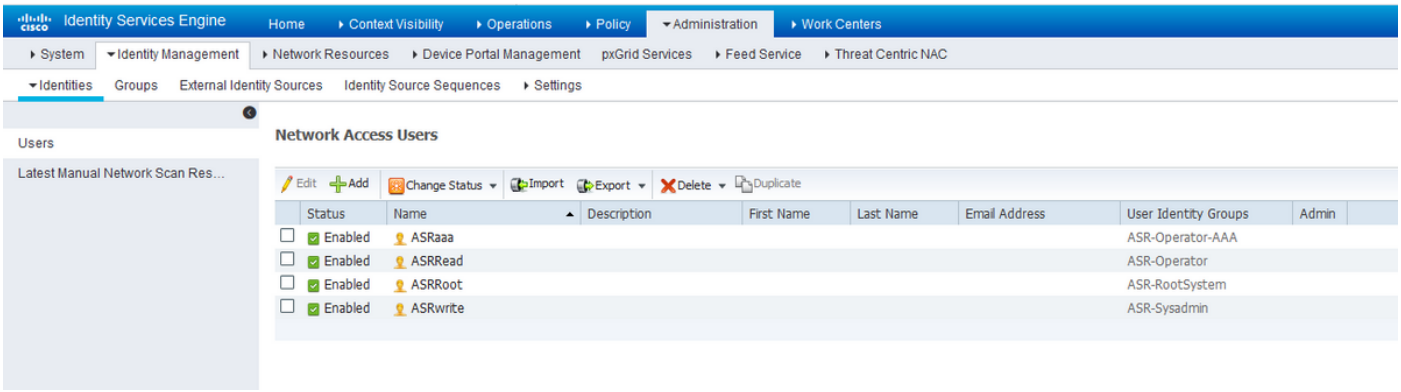
步驟2.根據您的需求定義使用者組，在示例中，如本圖所示，您將使用四個組。您可以在**Administration > Identity Management > Groups > User Identity Groups**下定義組。在此示例中建立的組包括：

1. ASR-Operator

2. ASR-Operator-AAA
3. ASR-RootSystem
4. ASR-Sysadmin



身份組步驟3.如圖所示，建立使用者並將其對映到之前建立的相應使用者組。



身份/使用者

附註：在本示例中，ISE內部使用者用於身份驗證和授權。使用外部身份源的身份驗證和授權不在本文檔的討論範圍之內。

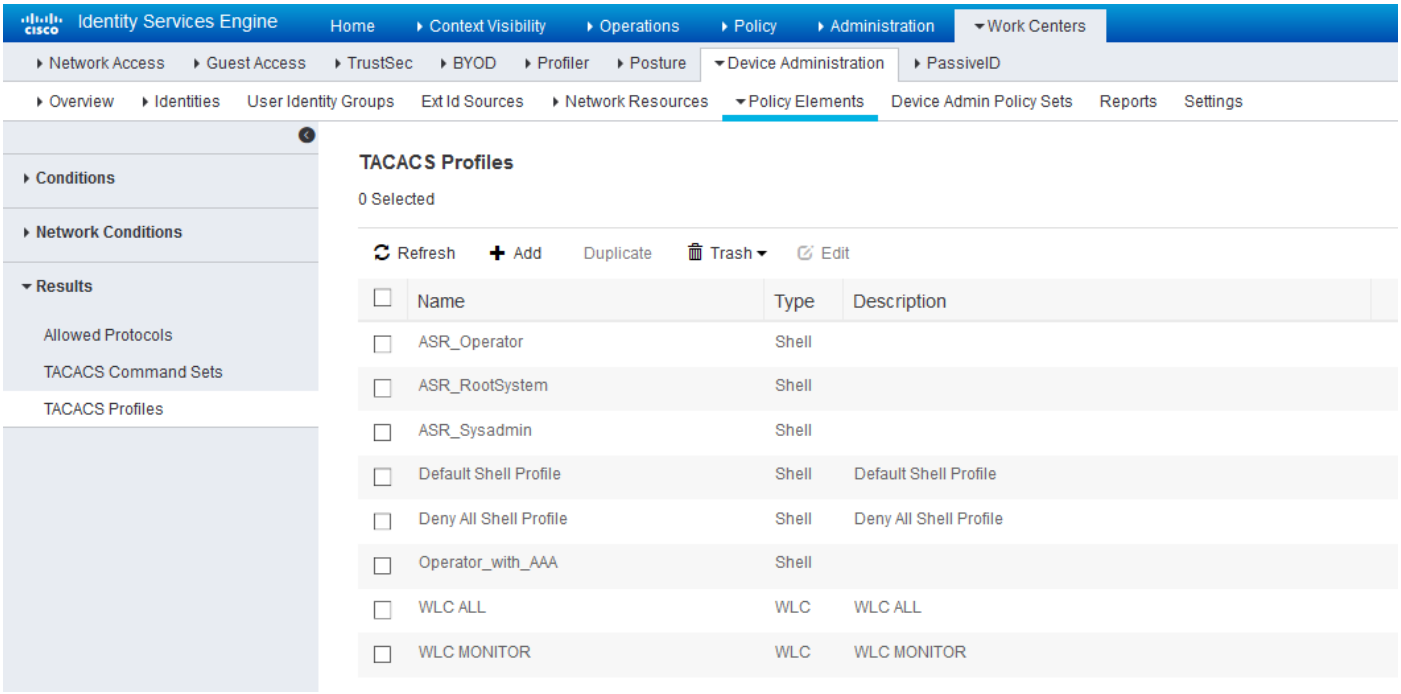
步驟4.定義要為每個使用者推送的殼配置檔案。為此，請導航至**工作中心>裝置管理>策略元素>結果> TACACS配置檔案**。您可以配置新的外殼配置檔案，如圖所示，也可以配置以前版本的ISE。在此示例中定義的殼配置檔案包括：

1. ASR_Operator

2. ASR_RootSystem

3. ASR_Sysadmin

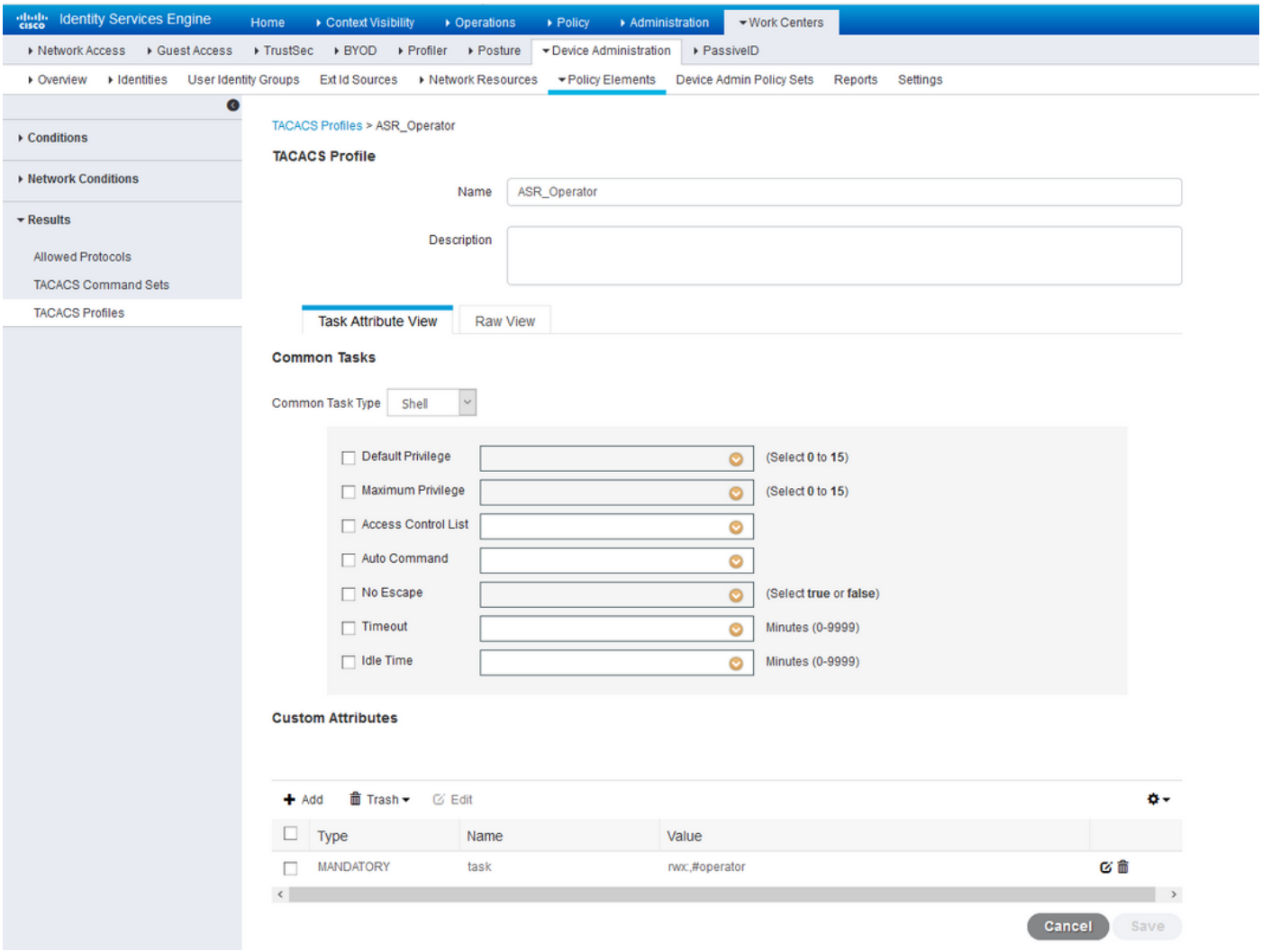
4. Operator_with_AAA



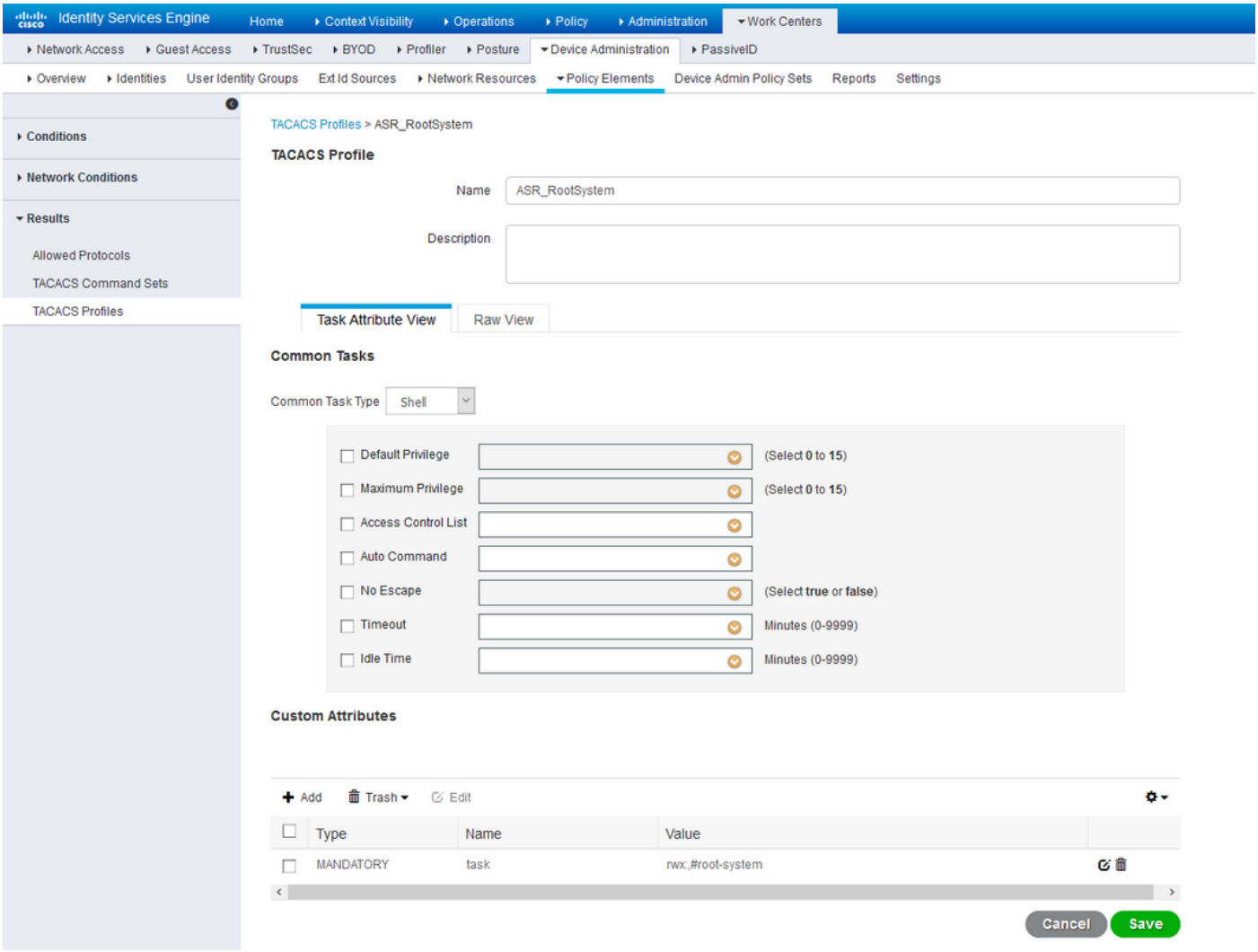
TACACS的外殼配置檔案

您可以按一下**Add**按鈕以輸入欄位Type、Name和Value，如**Custom Attributes**部分下的影象中所示。

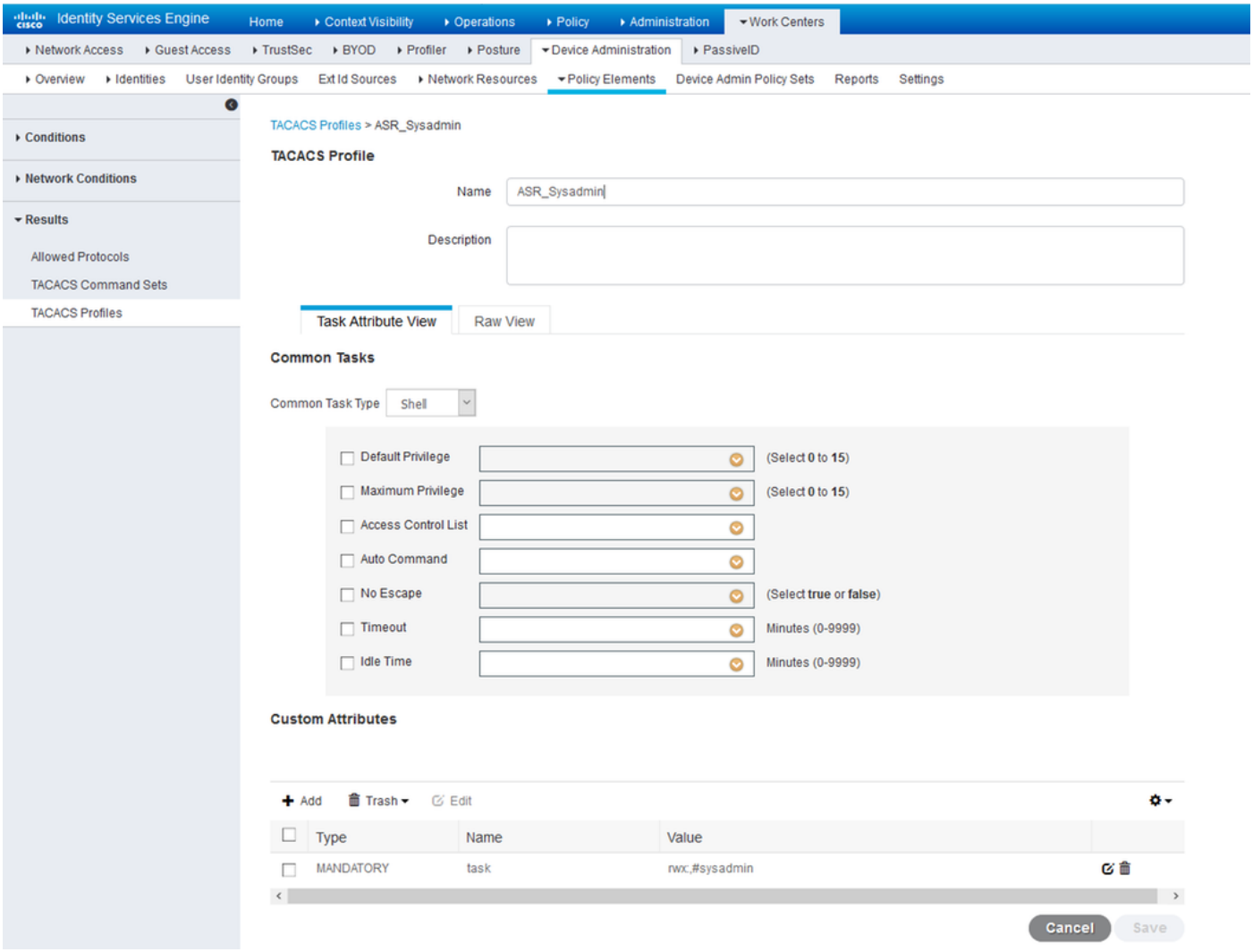
對於操作員角色：



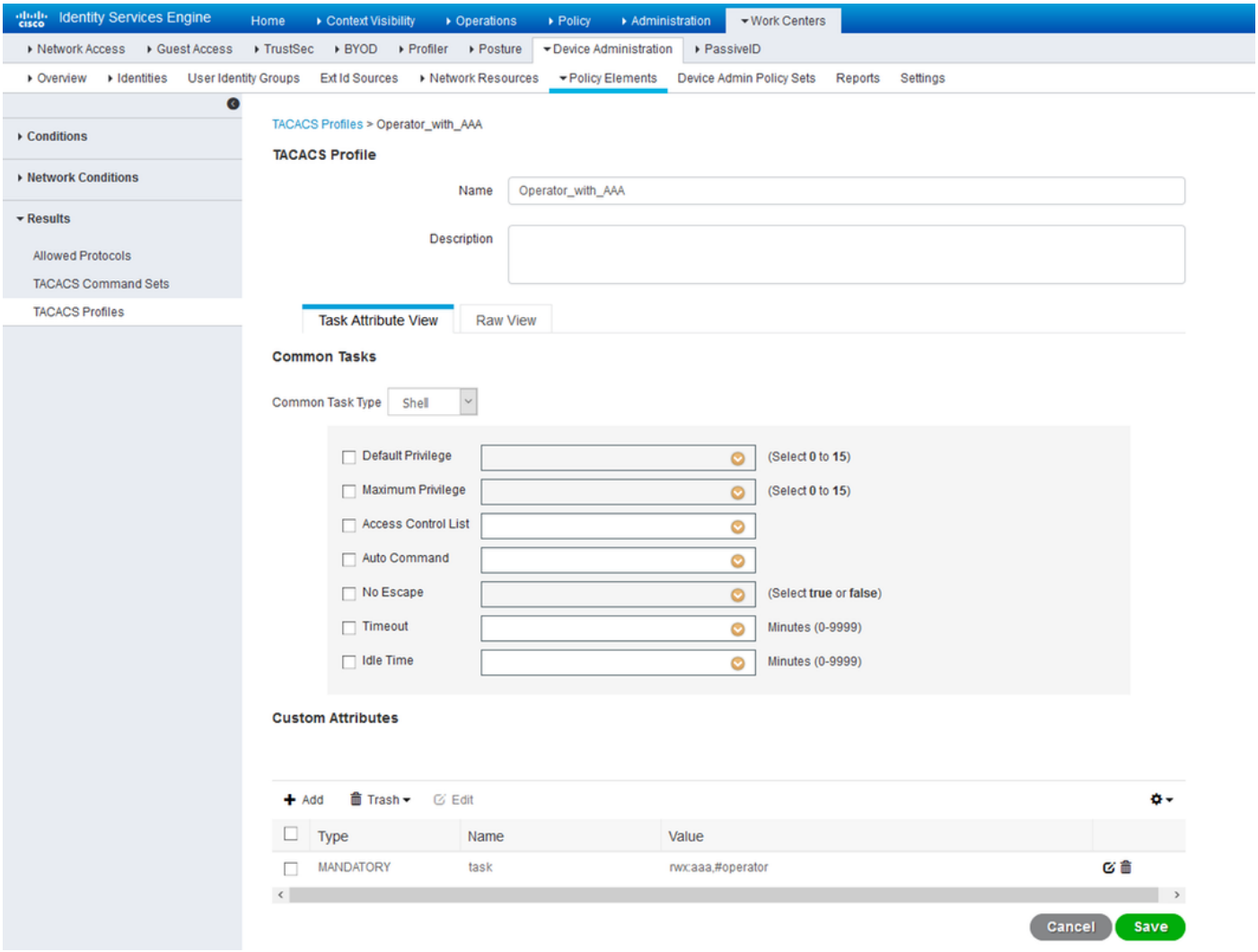
ASR操作員外殼配置檔案對於根系統角色：



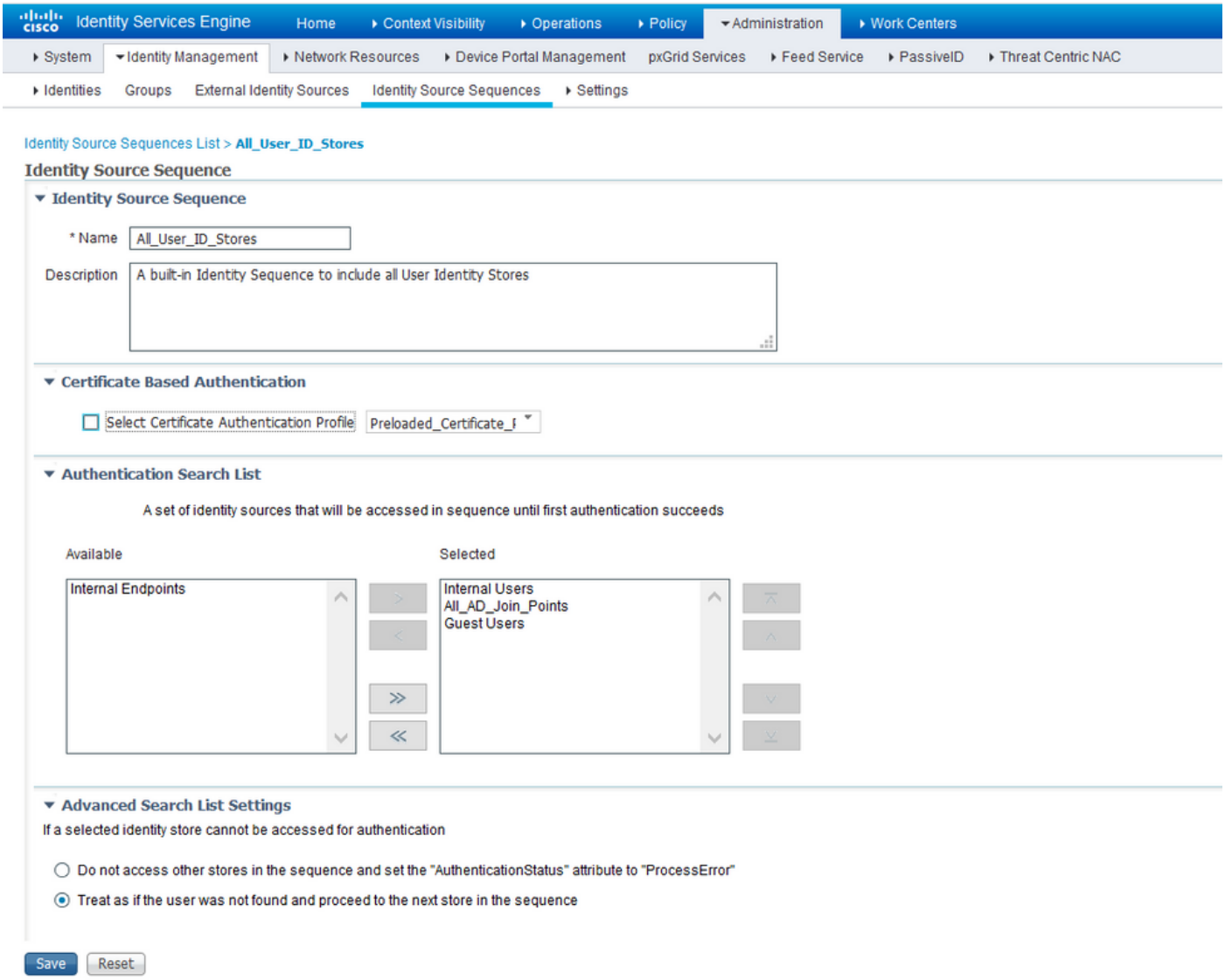
ASR根系統外殼配置檔案對於sysadmin角色：



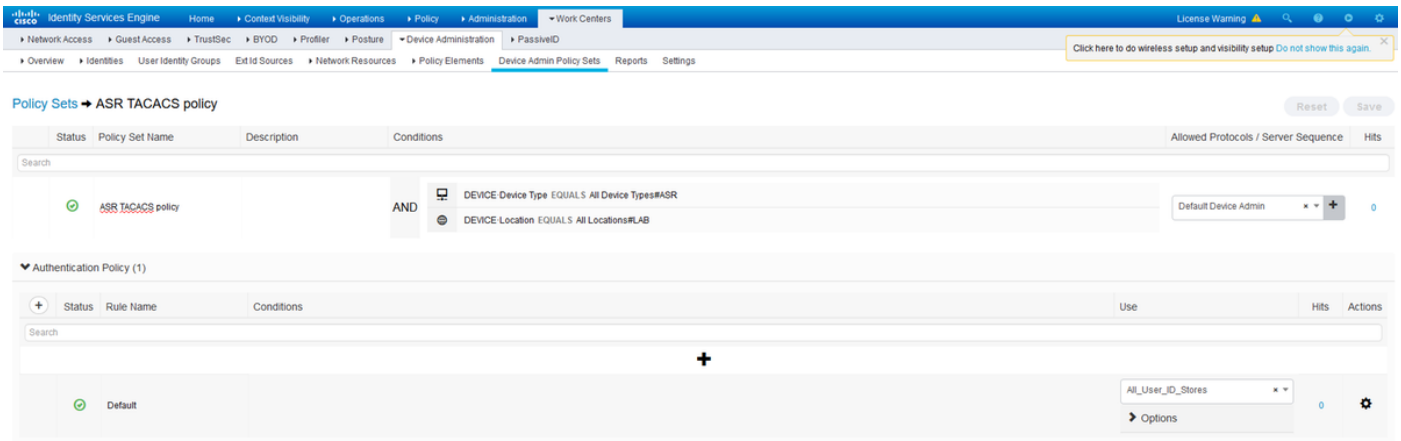
ASR Sysadmin外殼配置檔案對於操作員和AAA角色：



具有AAA外殼配置檔案的運算子步驟5.配置身份源序列，以使用Administration > Identity Management > Identity Source Sequences中的Internal Users。您可以新增新的身份源序列，也可以編輯可用的序列。

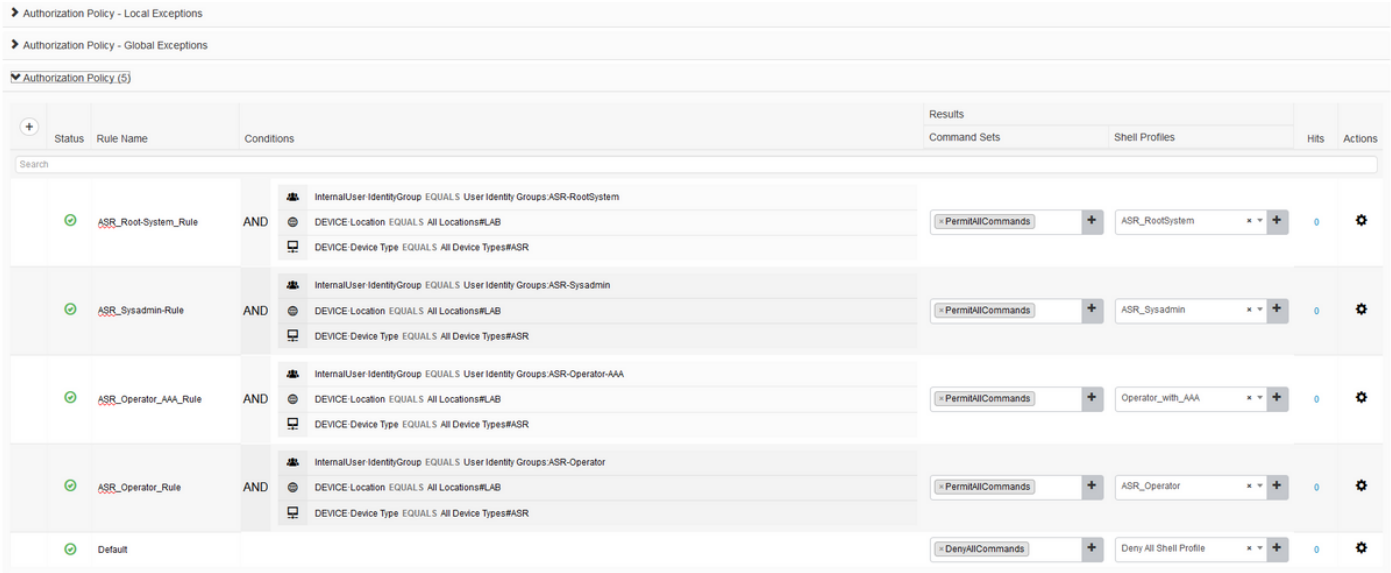


步驟6.在**Work Centers > Device Administration > Device Admin Policy Sets > [Choose Policy Set]處配置身份驗證策略，以便使用包含內部使用者的身份儲存序列。**使用之前建立的使用者身份組根據要求配置授權，並對映各自的Shell配置檔案，如下圖所示。



身份驗證策略

可根據要求以多種方式配置授權策略。圖中顯示的規則基於裝置位置、型別和特定的內部使用者身份組。所選的Shell配置檔案將在授權時與命令集一起推送。



授權策略

驗證

使用本節內容，確認您的組態是否正常運作。

操作員

驗證使用者登入到路由器時分配的**用**戶組和任務組。

```
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的運算子

驗證以下情況下分配的使用者組和任務組：**阿斯拉阿** 使用者登入路由器。

> **注意**:從TACACS伺服器推送操作員任務以及AAA任務讀取、寫入和執行許可權。

```
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

驗證以下情況下分配的使用者組和任務組：**asrwrite** 使用者登入路由器。

```
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 )
```

根系統

驗證以下情況下分配的使用者組和任務組：**asrroot** 使用者登入路由器。

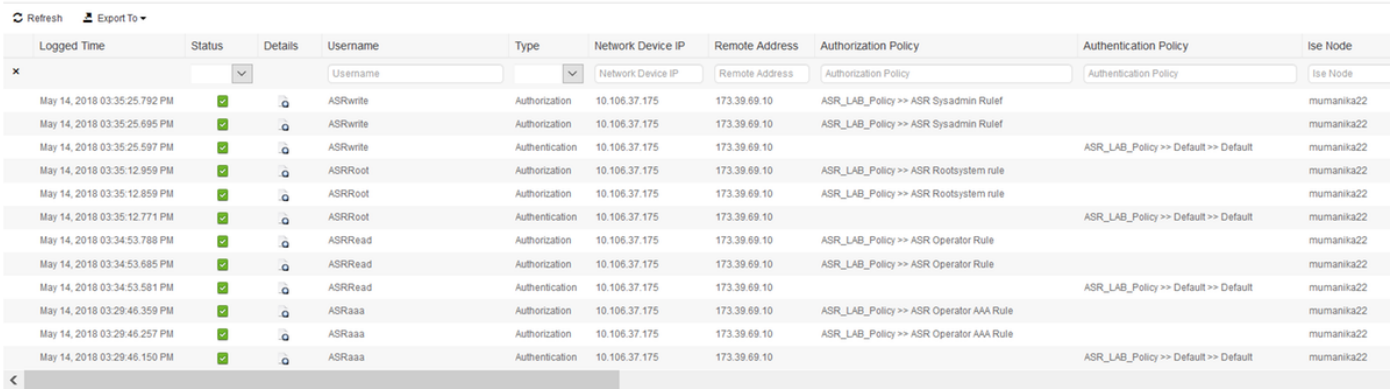
```
username: asrroot
```

```
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 )
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

從Operations > TACACS > Live Logs驗證ISE報告。按一下放大鏡符號以檢視詳細報告。



以下是一些用於對ASR進行故障排除的實用命令：

- **顯示使用者**
- **顯示使用者組**
- **顯示使用者任務**
- show user all