使用Cisco Secure ACS 5.x伺服器配置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，以通過TACACS+和思科安全存取控制伺服器(ACS)5.x伺服器進行驗證和授權。

以下範例說明在Cisco IOS XR軟體系統中用於控制使用者存取的基於任務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

- ACS 5.x部署和配置。
- TACACS+通訊協定

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4.3.4的ASR 9000
- Cisco安全ACS 5.7

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。如果您的網路正在作用，請確保您已瞭解任何組態變更的潛在影響。

組態

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)。

根系統使用者組具有預定義的授權；也就是說，它完全負責根系統使用者管理的資源，並在其他服務中承擔某些責任。

使用以下命令檢查預定義的使用者組：

```
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>
```

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，例如SBC

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>
```

使用以下命令檢查支援的任務：

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

以下是支援的任務清單：

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

上述每項任務都可以賦予上述或所有四種許可權。

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。

IOS XR上的使用者定義元件

使用者定義的使用者組

管理員可以配置自己的使用者組以滿足特定需求。以下是配置示例：

```
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
```

使用者定義的任務組

管理員可以配置自己的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
```

如果您不確定如何查詢特定命令所需的任務組和許可權，可以使用**describe**命令查詢該任務。下面是一個示例：

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**，您需要在任務組中允許以下行：

任務讀取aaa

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**aaa authentication login default group tacacs+**命令，您需要在任務組中允許以下行：

任務讀寫aaa

您可以定義可以匯入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

在路由器上定義TACACS伺服器：

在此將ACS伺服器IP地址定義為tacacs-server，金鑰為cisco

```
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
!
```

將驗證和授權指向外部TACACS伺服器。

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

命令授權（可選）：

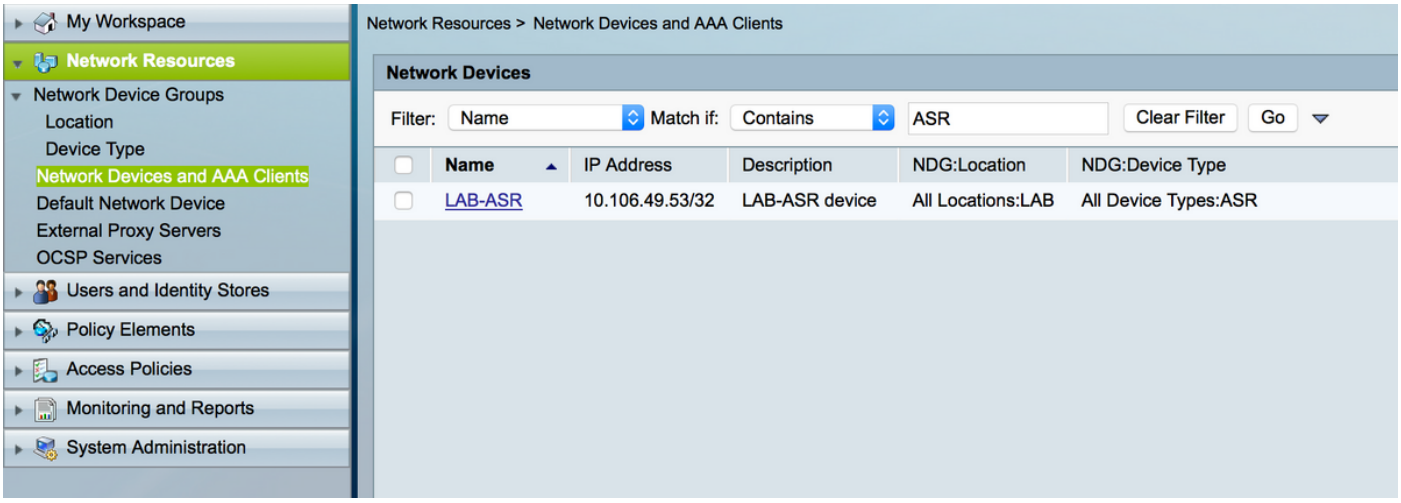
```
#aaa authorization commands default group tacacs+
```

將記帳指向外部伺服器（可選）。

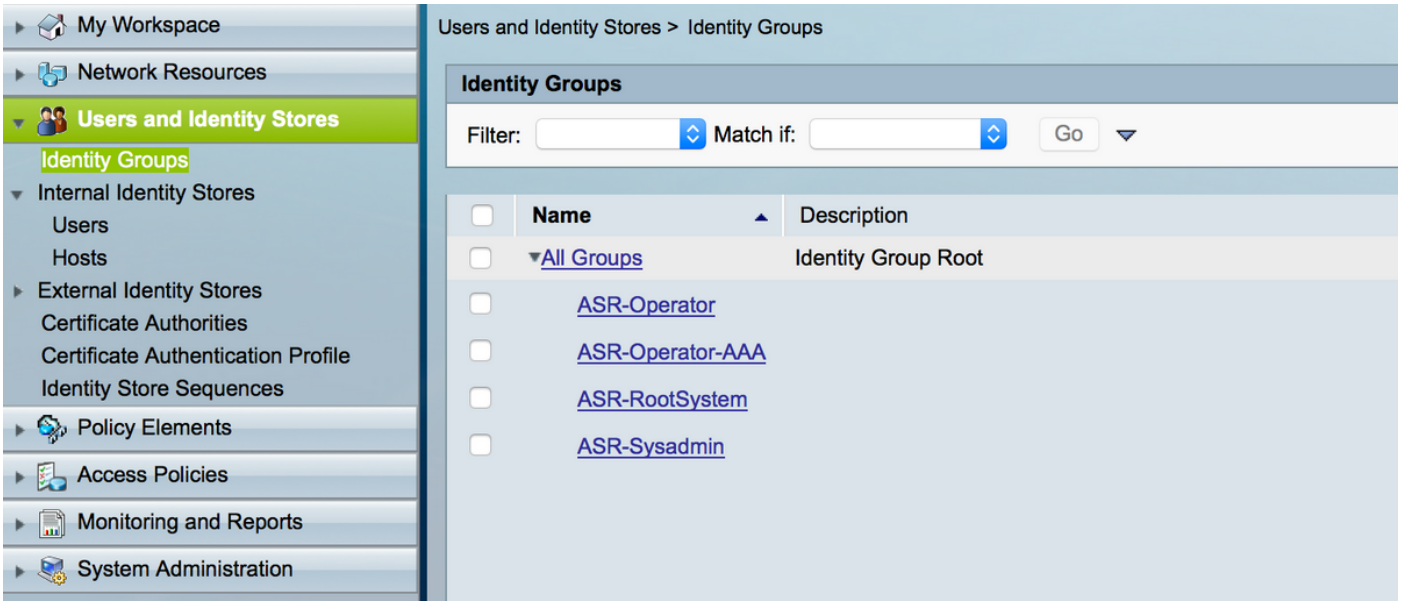
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ACS伺服器配置

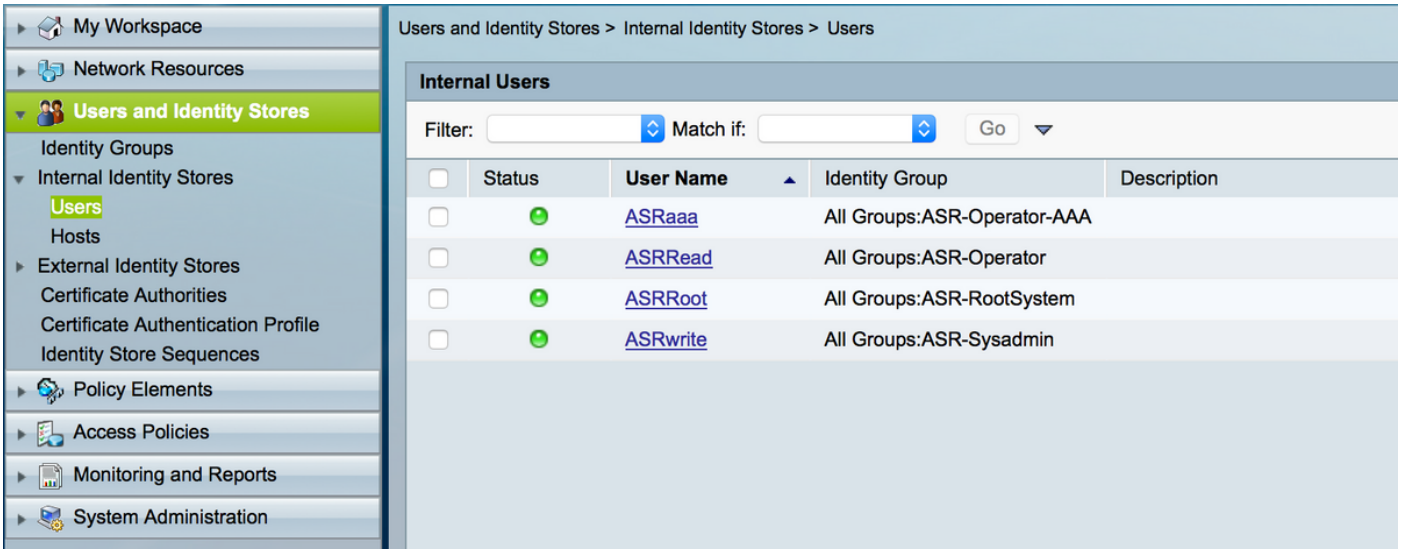
步驟1。若要定義ACS伺服器上AAA使用者端清單中的路由器IP，請導覽至**Network Resources > Network Devices and AAA Clients**，如下圖所示。在本示例中，您將**cisco**定義為ASR中配置的共用金鑰。



步驟2.根據您的要求定義使用者組，在此示例中，如本圖所示，您將使用四個組。

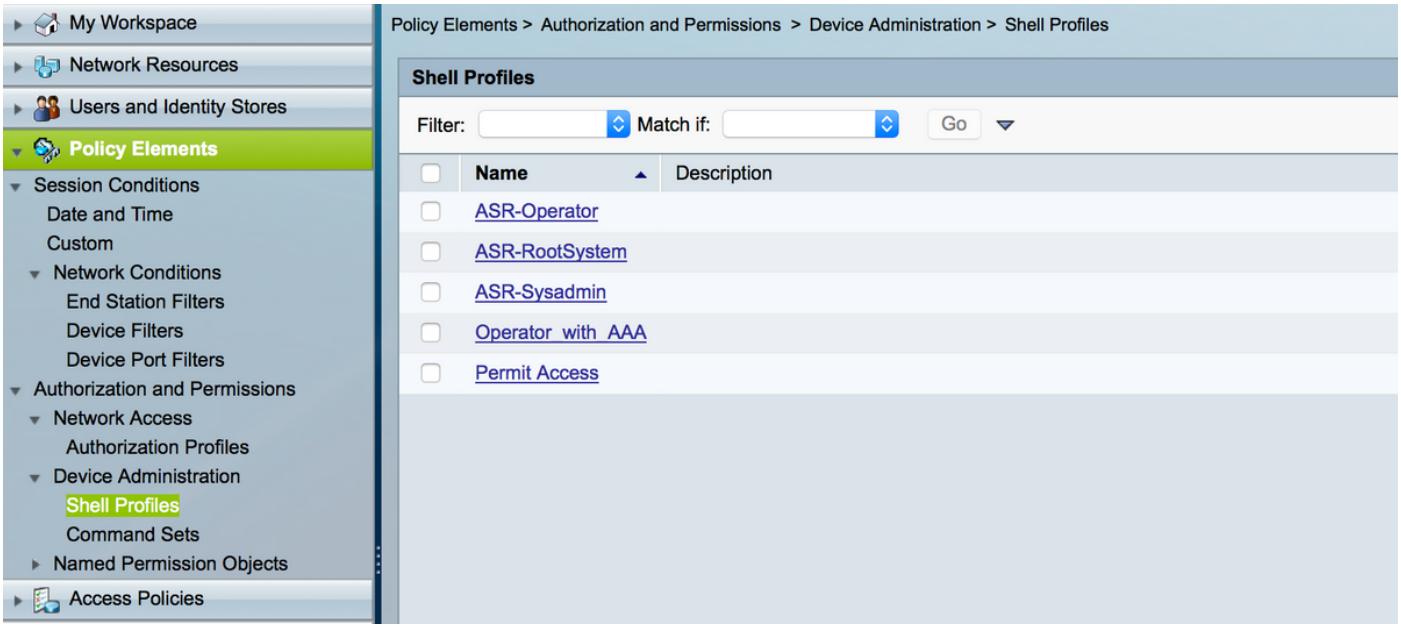


步驟3.如圖所示，建立使用者並將其對映到上面建立的各個使用者組。

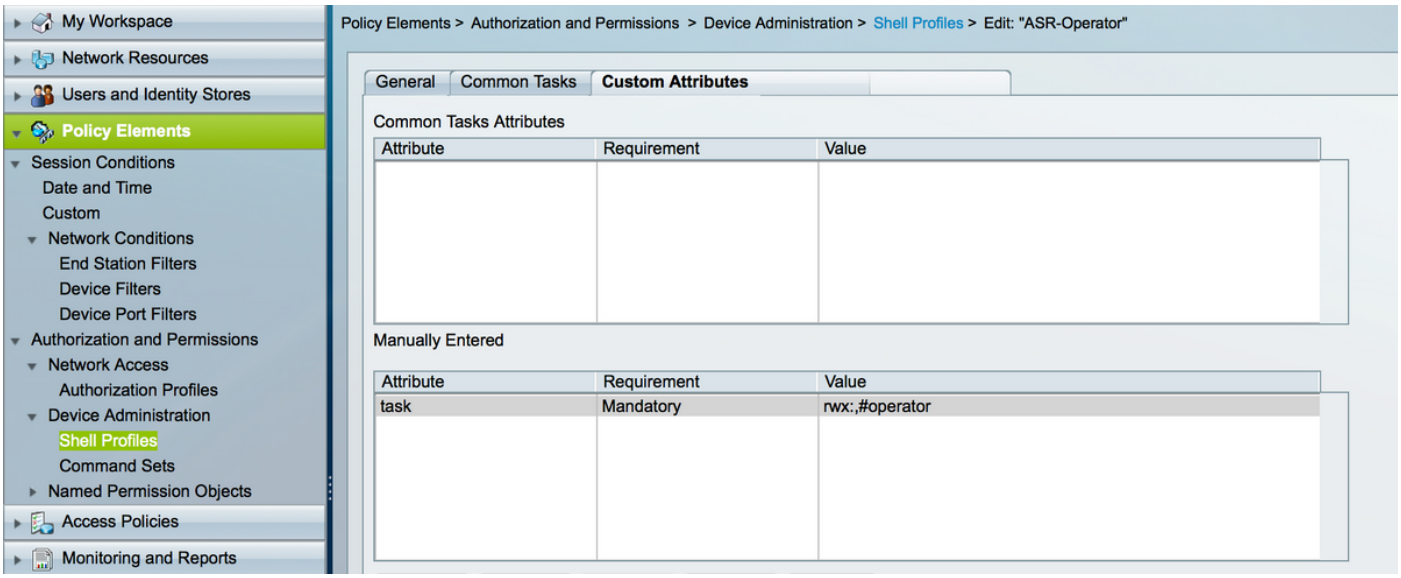


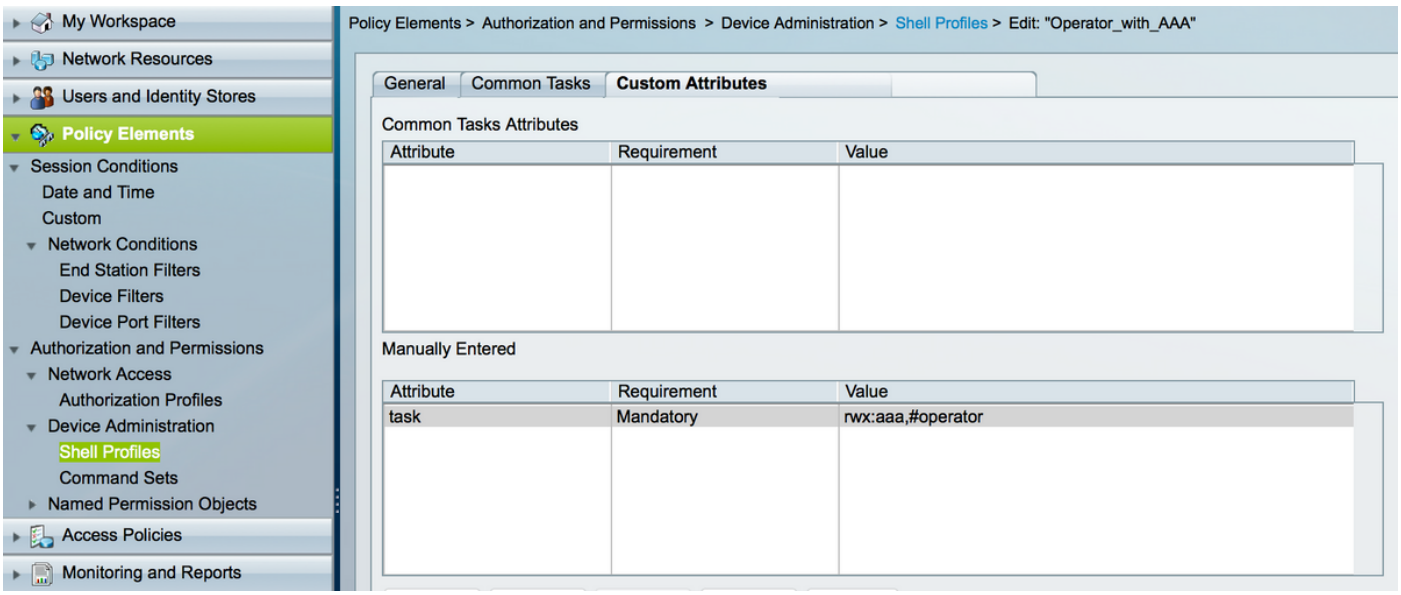
附註：在本示例中，使用用於身份驗證的ACS內部使用者，如果您要使用在外部身份儲存庫中建立的使用者，也可以使用它們。在此示例中，不涵蓋外部身份源使用者。.

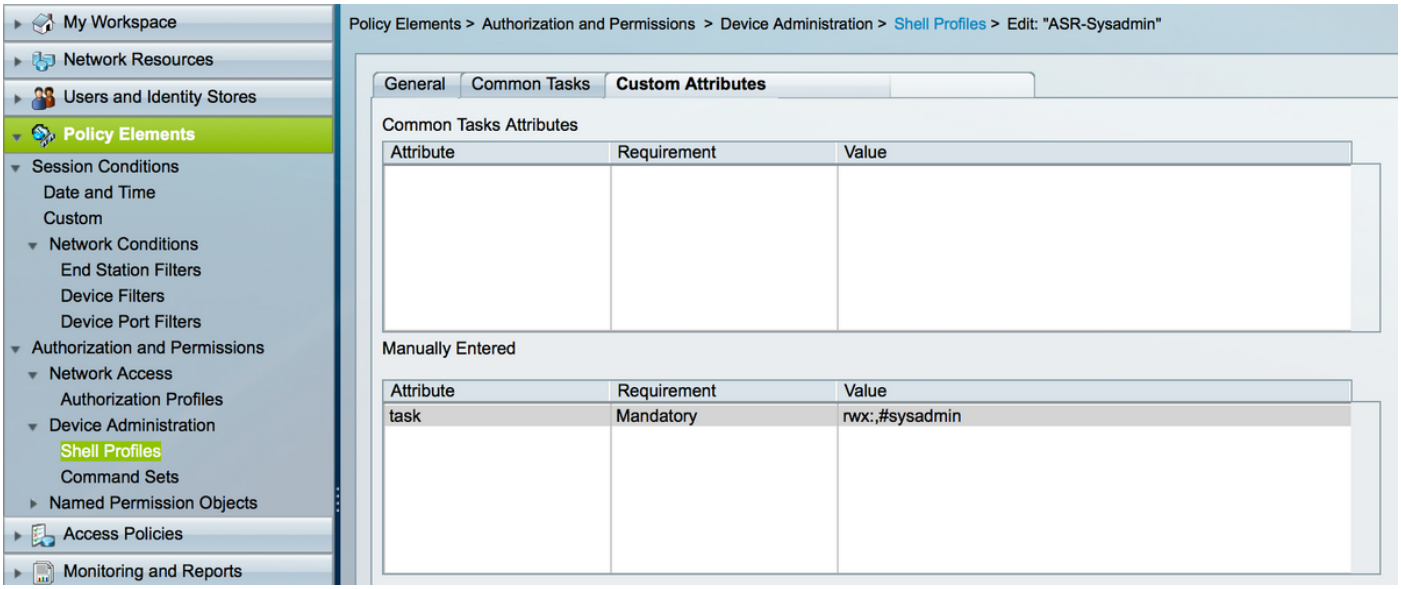
步驟4.定義要為各自使用者推送的殼配置檔案。

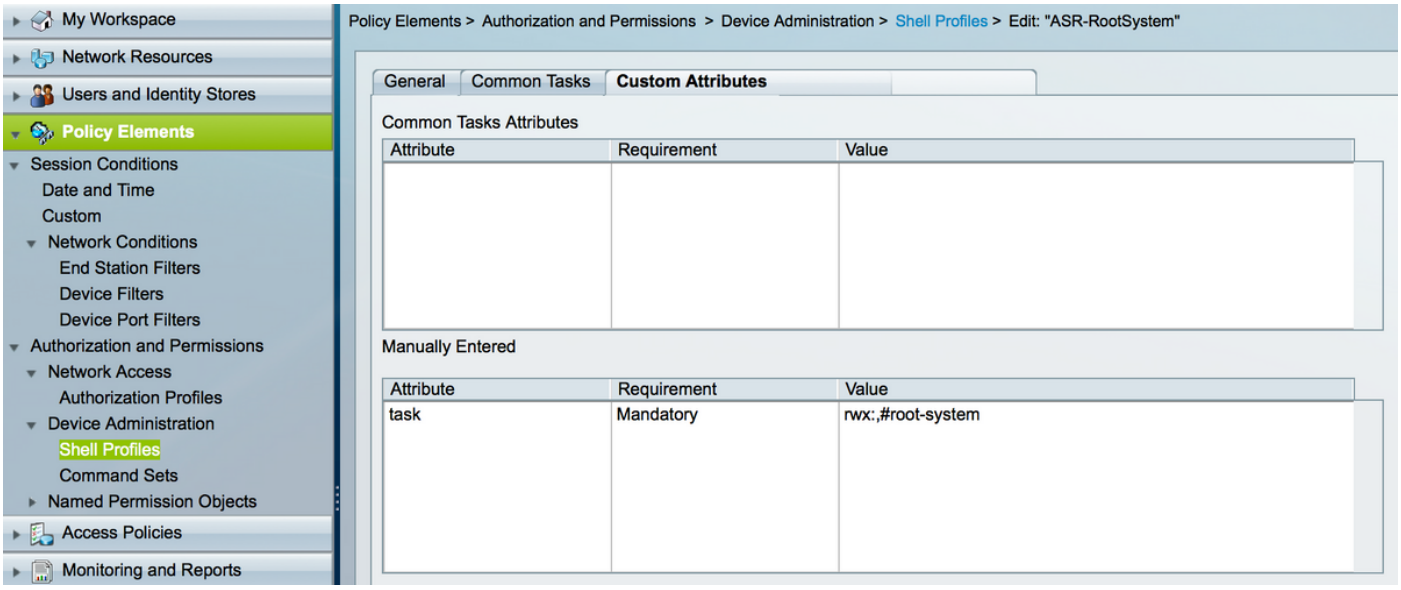


在已建立的外殼配置檔案中，配置以推送各自的任務組，如下圖所示。

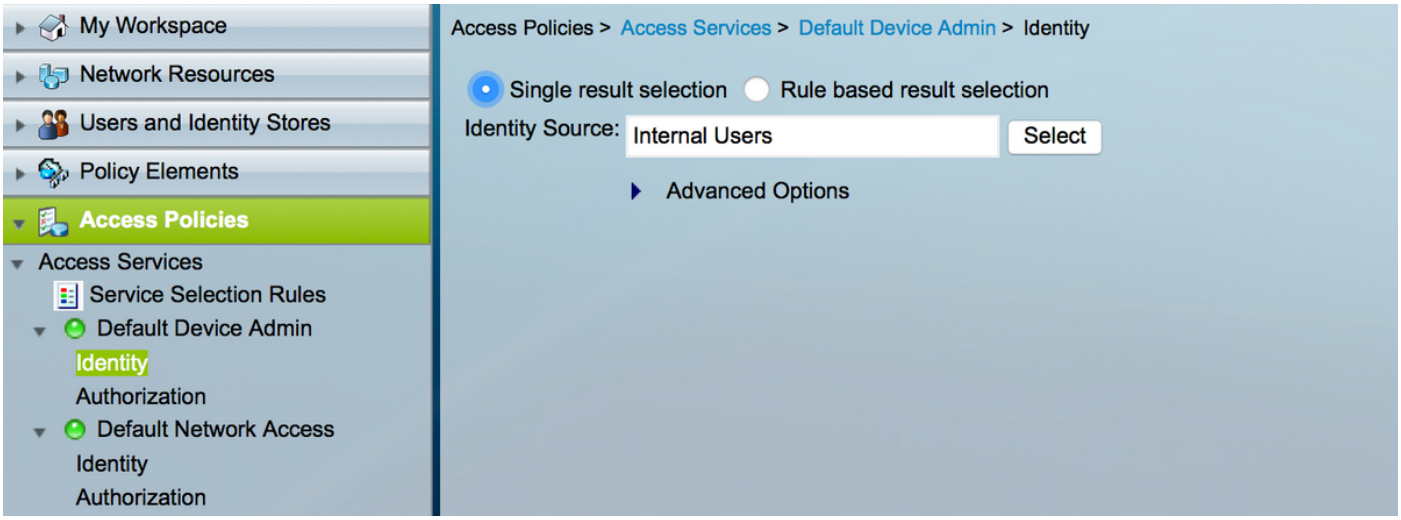




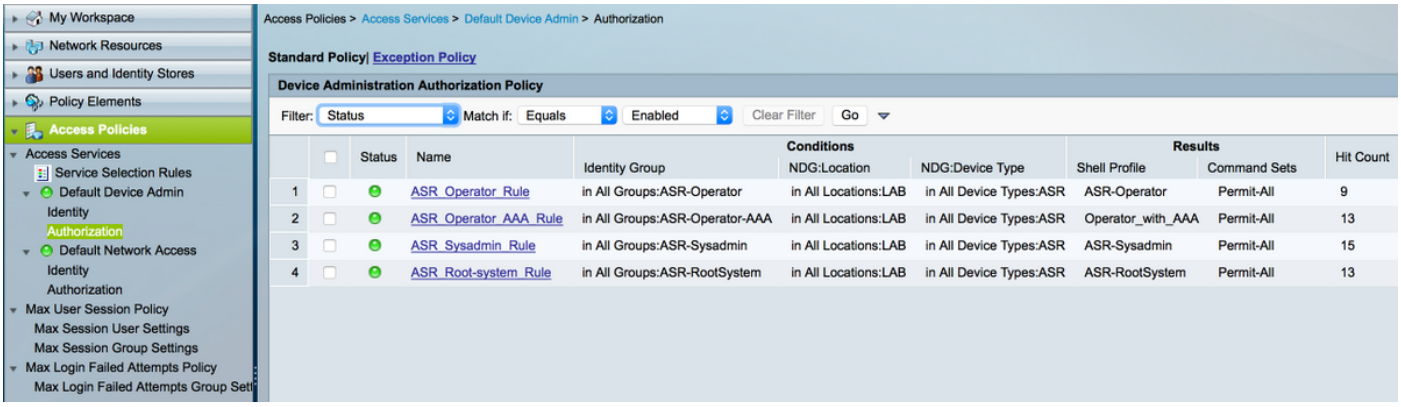




步驟5.定義訪問策略。對內部使用者進行身份驗證。



步驟6.使用以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。



驗證

操作員

若要登入，需使用username **asrread**。以下是驗證指令。

```
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
```

具有AAA的運算子

若要登入，請使用使用者名稱**asraaa**。以下是驗證命令。

附註：**asraaa**是從TACACS伺服器推送的運營商任務以及aaa任務讀寫和執行許可權。

```
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

若要登入，需使用**username asrwrite**。以下是驗證指令。

```
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 )
```

根系統

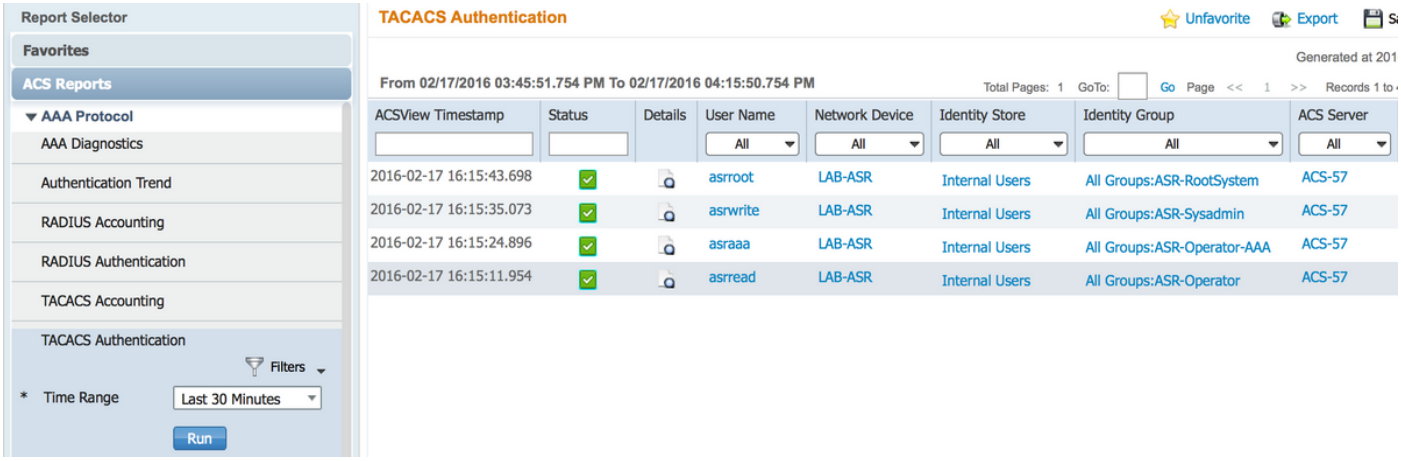
若要登入，請使用使用者名稱**asrroot**。以下是驗證命令。

```
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 )
```

疑難排解

您可以從監視和報告頁驗證ACS報告。如圖所示，您可以按一下放大鏡子以檢視詳細報告。



以下是在ASR上排除故障的一些有用命令：

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