ASR9k TACACS configureren met Cisco Secure ACS 5.x server

Inhoud

Inleiding

Dit document beschrijft de configuratie van ASR 9000 Series aggregation services router (ASR) om via TACACS+ en Cisco Secure Access Control Server (ACS) 5.x server te certificeren en te autoriseren.

Deze voorbeelden van de implementatie van het administratieve model van op taak gebaseerde vergunning die wordt gebruikt om de toegang van gebruikers in het Cisco IOS XR-softwaresysteem te controleren. De belangrijkste taken die vereist zijn om de op taken gebaseerde vergunning uit te voeren omvatten de manier waarop u gebruikersgroepen en taakgroepen kunt configureren. Gebruikersgroepen en taakgroepen worden ingesteld door de Cisco IOS XR-softwareset die wordt gebruikt voor verificatie, autorisatie en accounting (AAA) services. De verificatieopdrachten worden gebruikt om de identiteit van een gebruiker of hoofd te controleren. De opdrachten van de autorisatie worden gebruikt om te controleren of een geauthentiseerde gebruiker (of opdrachtgever) toestemming is verleend om een specifieke taak uit te voeren. Boekhoudopdrachten worden gebruikt voor het registreren van sessies en voor het maken van een controlespoor door het opnemen van bepaalde gebruikers- of systeemgenereerde acties.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ASR 9000-toepassing en basisconfiguratie
- ACS 5.x plaatsing en configuratie.
- TACACS+ protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASR 9000 met Cisco IOS XR-software, versie 4.3.4
- Cisco beveiligde ACS 5.7

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg ervoor dat u de potentiële impact van elke configuratie verandering begrijpt.

Configuratie

Vooraf gedefinieerde componenten op IOS XR

Er zijn vooraf gedefinieerde gebruikersgroepen en taakgroepen in IOS XR. De beheerder kan deze vooraf gedefinieerde groepen gebruiken of aangepaste groepen definiëren zoals vereist.

Vooraf gedefinieerde gebruikersgroepen

Deze gebruikersgroepen zijn vooraf gedefinieerd op IOS XR:

Gebruikersgroep	Privileges
Cisco-ondersteuning	Standaard en probleemoplossing functies (meestal gebruikt door het personeel van Technical Support).
netbeheerder	Configureer netwerkprotocollen zoals Open Shortest Path First (OSPF) (gewoonlijk gebruikt door netwerkbeheerders).
exploitant	De dagelijkse controleactiviteiten uitvoeren en beperkte configuratierechten hebben.
wortel-lr	Geef alle opdrachten binnen één RP weer en voer deze uit.
wortelsysteem	Geef alle opdrachten voor alle RP's in het systeem weer en voer deze uit.
sysadmin	Voer systeembeheertaken voor de router uit, zoals het onderhoud waar de kerndum zijn opgeslagen of het instellen van de NTP-kloktijd (Network Time Protocol).
onderhoud	Voer servicetaken uit, zoals Session border-controller (SBC).

De gebruikersgroep van het wortelsysteem heeft vooraf een vergunning verleend; Dat wil zeggen dat zij de volledige verantwoordelijkheid heeft voor de door de gebruiker beheerde middelen van het basissysteem en bepaalde verantwoordelijkheden voor andere diensten.

Gebruik deze opdracht om de vooraf gedefinieerde gebruikersgroepen te controleren:

```
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>
```

Vooraf gedefinieerde taakgroepen

Deze vooraf gedefinieerde taakgroepen zijn beschikbaar voor beheerders die deze kunnen gebruiken, doorgaans voor de initiële configuratie:

- Cisco-ondersteuning: Cisco-ondersteuningspersoneelstaken
- netadmin: Netwerkbeheertaken
- exploitant: Dagelijkse taken van de exploitant (voor demonstratiedoeleinden)
- wortel-lr: Secure-routerbeheertaken
- wortelsysteem: Beheertaken voor het hele systeem
- sysadmin: Systeembeheertaken
- ServiceAdmin: Dienstbeheerstaken, bijvoorbeeld SBC

Gebruik deze opdracht om de vooraf gedefinieerde taakgroepen te controleren:

```
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>
```

Gebruik deze opdracht om de ondersteunde taken te controleren:

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

Hier volgt een lijst met ondersteunde taken:

Aaa	Acl	Beheer	Ancp	ATM	basisdiensten	Bcdl	BD
Boot	bundelen	call-home	Cdp	Cef	Cgn	Cisco-ondersteuning	config
Crypto	diag	verworpen	Drivers	DWDM	Eem	Eigrp	Ether
Fabric	foutmarge	Filesysysteem	Firewall	Fr	HDLC	diensten van ontvangst	HSRP
inventaris	ip-diensten	IPv4	IPv6	ISIS	L2VPN	Li	Lisp
LAantal	monitor	MPLS-ldp	MPLS-statisch	mpls-te	Multicast	NetFlow	Netwo
Ospf	Ouni	pbr	pkg	PPT	Ppp	QoS	Rcmd
riem	wortel-lr	wortelsysteem	routekaart	routebeleid	SBC	slang	sdh

Sysmgr	Systeem	Vervoer	tty access	Tunnel	universeel	Vlan	VPDN

Elk van de bovengenoemde taken kan met één van deze of alle vier machtigingen worden gegeven.

Lezen	Specificeert een aanduiding die alleen een gelezen handeling toestaat.
Schrijven	Specificeert een aanwijzing die een veranderingsverrichting toestaat en impliciet een gelezen verrichting toestaat.
uitvoeren	Specificeert een aanduiding die een toegangshandeling toestaat; Bijvoorbeeld, pingelen en tel
Debuggen	Specificeert een aanduiding die een debug handeling toestaat.

Door gebruiker gedefinieerde onderdelen op IOS XR

door de gebruiker gedefinieerde gebruikersgroepen

De beheerder kan zijn eigen gebruikersgroepen configureren om aan bepaalde behoeften te voldoen. Hier is het configuratievoorbeeld:

```
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
```

Door de gebruiker gedefinieerde taakgroepen

De beheerder kan hun eigen taakgroepen configureren om aan bepaalde behoeften te voldoen. Dit is het configuratievoorbeeld:

```
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
```

Als u niet zeker weet hoe u moet vinden welke taakgroep en toestemming voor bepaalde opdracht

nodig is, kunt u de opdracht **beschrijven** om deze te vinden. Hier is een voorbeeld:

Voorbeeld 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#
```

U kunt een gebruiker de opdracht **voor een gebruikersgroep** laten uitvoeren, dan moet u deze regel in de taakgroep toestaan:

lezen van taken

Voorbeeld 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)#
```

Om een gebruiker toe te staan om het commando te gebruiken **als authenticatie loginloggroep tacacs+** van de configuratiemodus, moet u deze regel in de taakgroep toestaan:

lezen van taken

U kunt de gebruikersgroep definiëren die meerdere taakgroepen kan importeren. Hier is het configuratievoorbeeld:

```
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
```

AAA-configuratie op de router

Defineert een TACACS server op de router:

Hier definieert u het ACS-server-IP-adres als de tacacs-server met 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
!
```

Wijs de authenticatie en autorisatie aan externe TACACS server aan.

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

Opdrachtvergunning (optioneel):

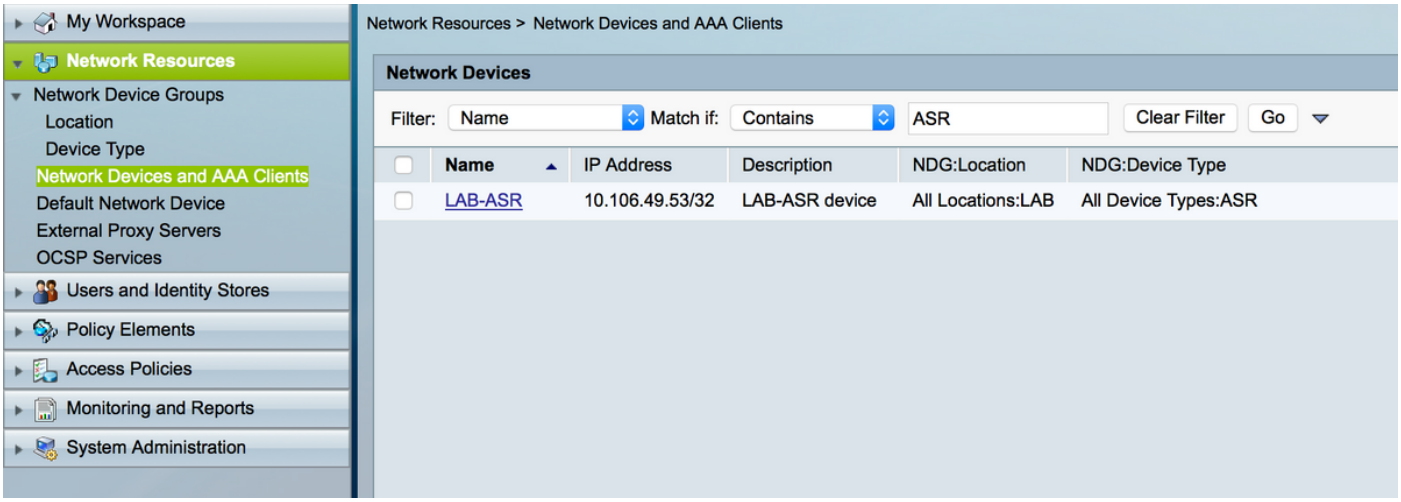
```
#aaa authorization commands default group tacacs+
```

Wijs de accounting naar externe server (optioneel).

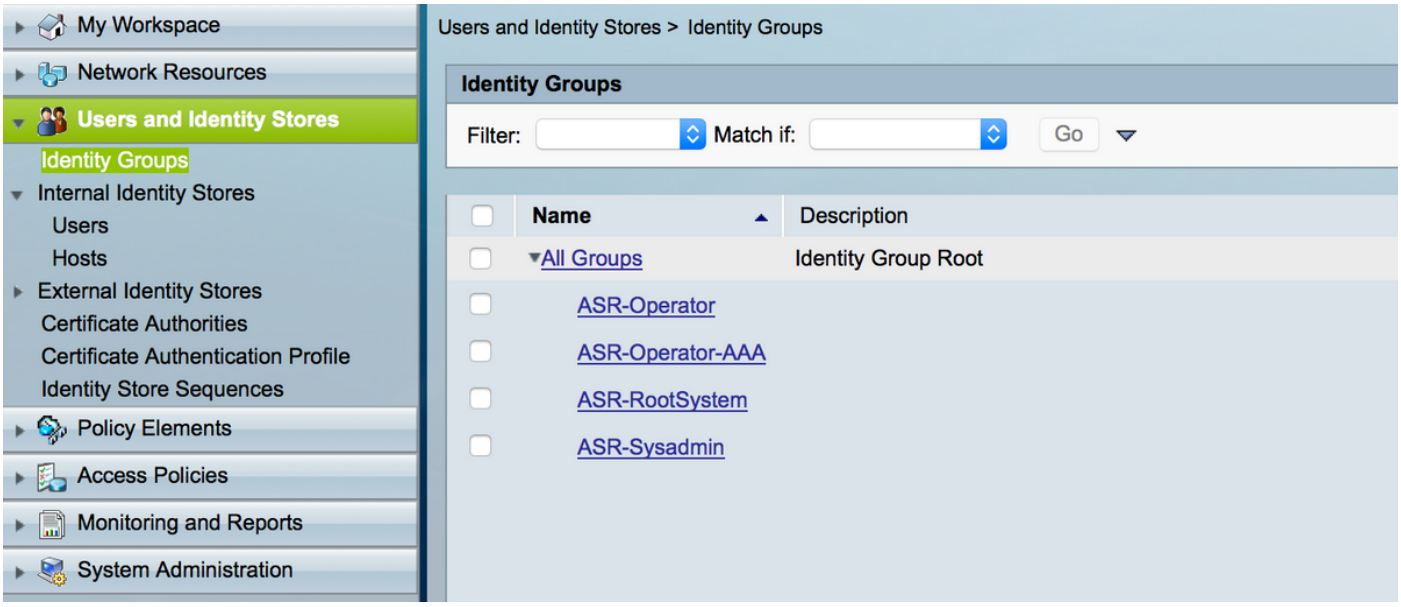
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ACS-serverconfiguratie

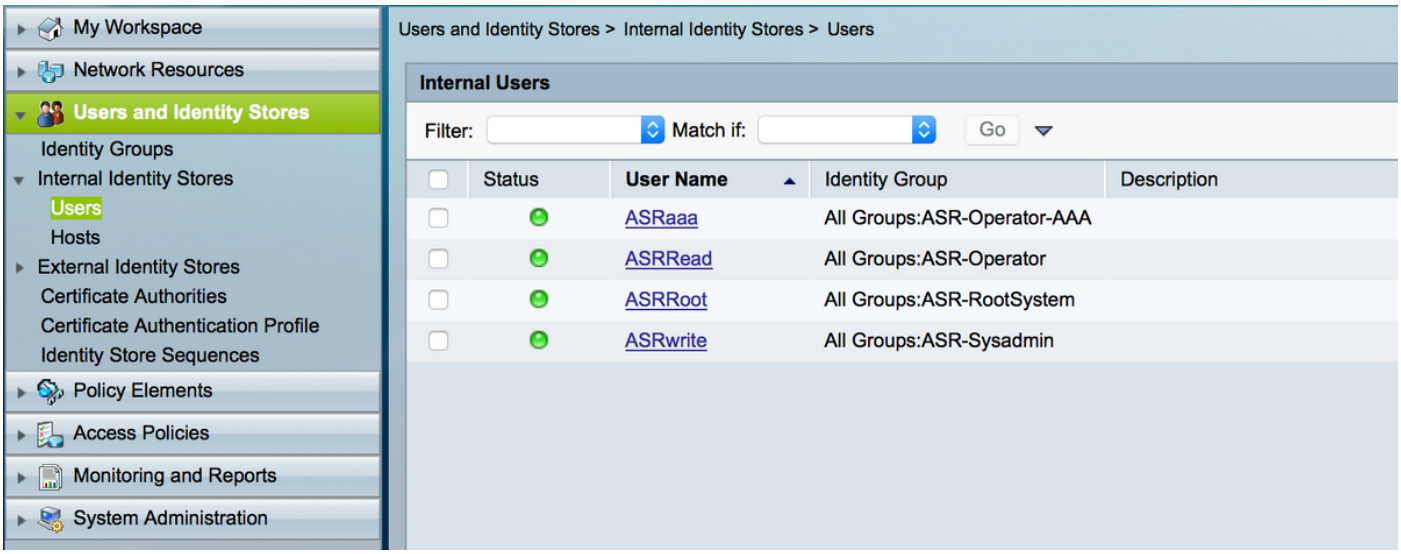
Stap 1. Om de router IP in de lijst met AAA-clients op de ACS-server te definiëren, navigeer naar **Network Resources > Network Devices en AAA-clients**, zoals in de afbeelding. In dit voorbeeld definieert u **cisco** als gedeeld geheim zoals ingesteld in de ASR.



Stap 2. Bepaal de gebruikersgroepen volgens uw behoefte. In het voorbeeld, zoals in deze afbeelding, gebruikt u vier groepen.



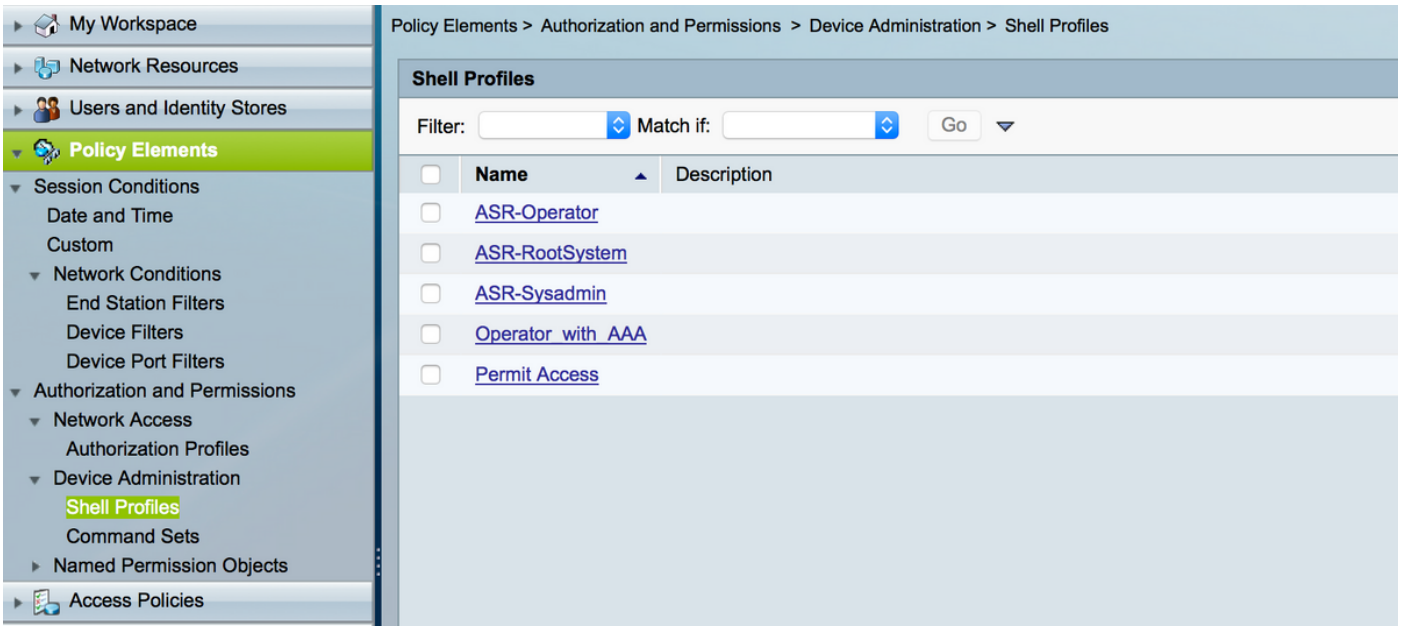
Stap 3. Zoals in de afbeelding, maakt u de gebruikers en stelt u deze in kaart met de respectievelijke gebruikersgroep die hierboven is gemaakt.



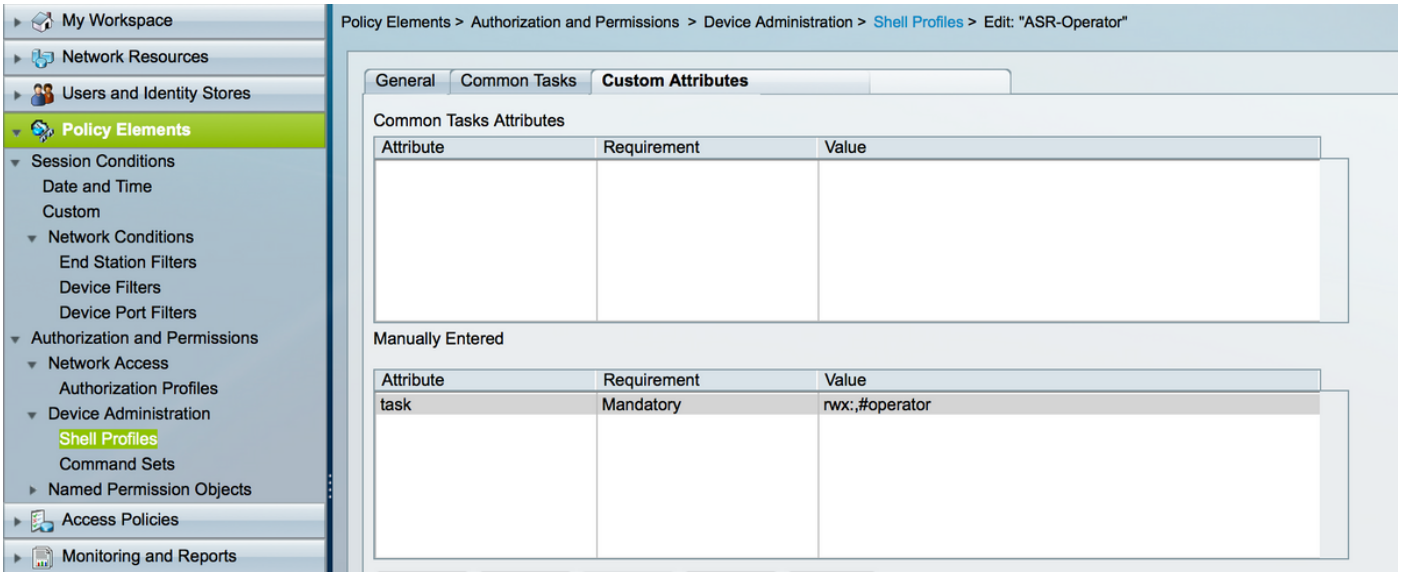
Opmerking: In dit voorbeeld worden de ACS interne gebruikers voor authenticatie gebruikt,

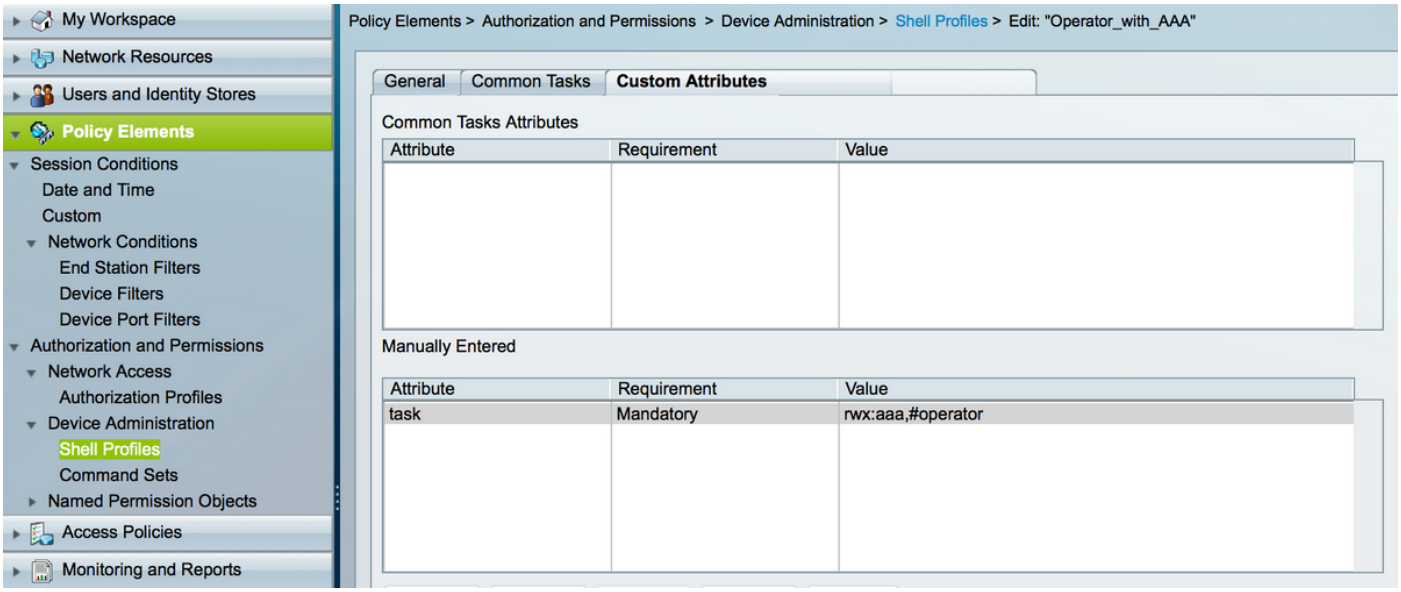
als u de gebruikers wilt gebruiken die gemaakt zijn in de externe identiteitszaken die u ook kunt gebruiken. In dit voorbeeld vallen de externe gebruikers van de identiteitsbron niet. .

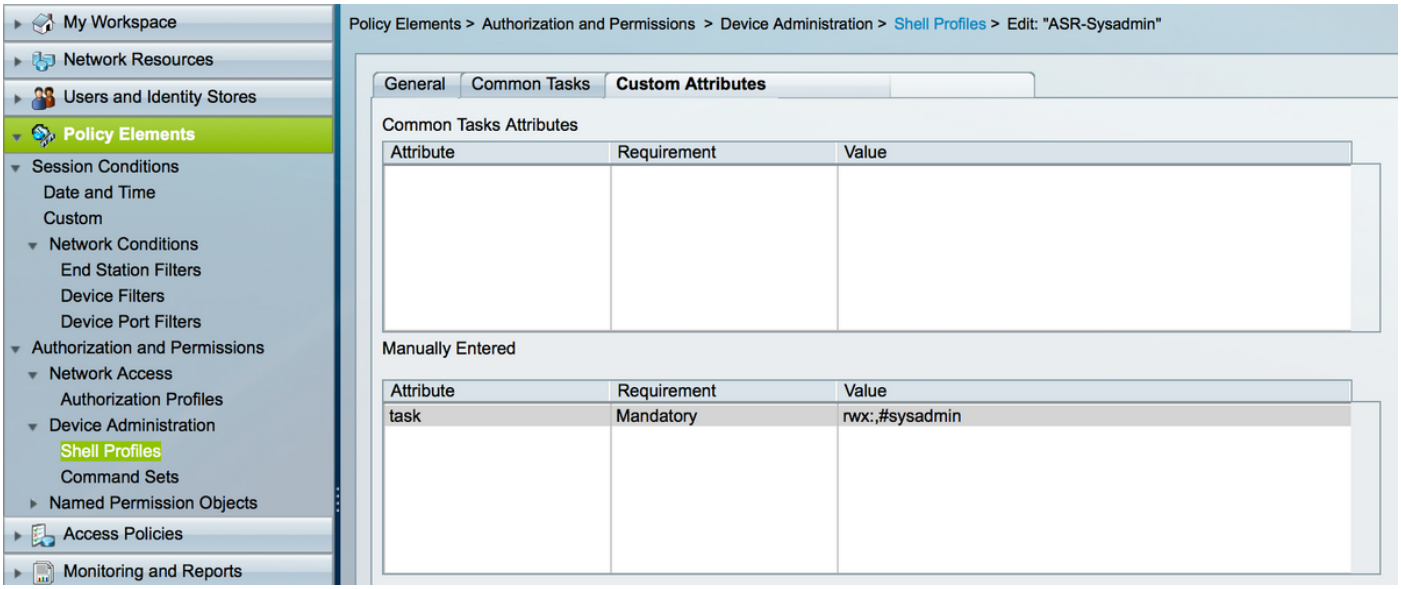
Stap 4. Bepaal het Shell-profiel dat u voor de respectieve gebruikers wilt instellen.

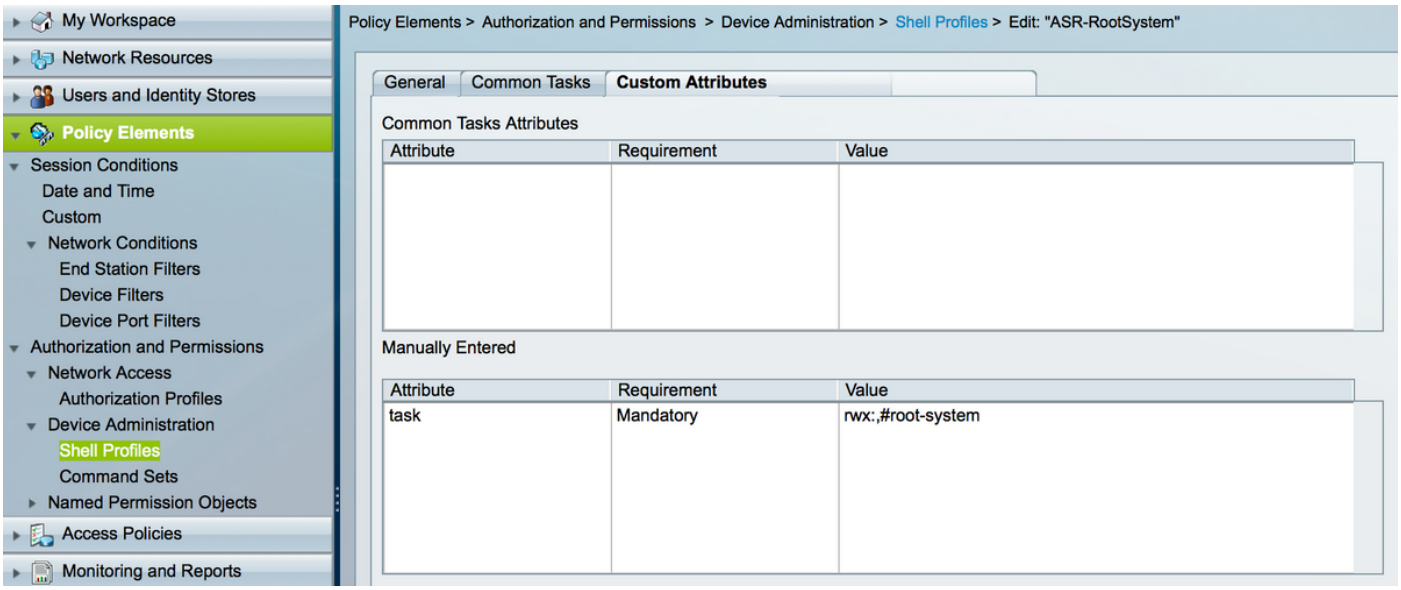


In het reeds gemaakte shell profiel, vormt u configuratie om de respectieve taakgroepen zoals weergegeven in de afbeelding te duwen.

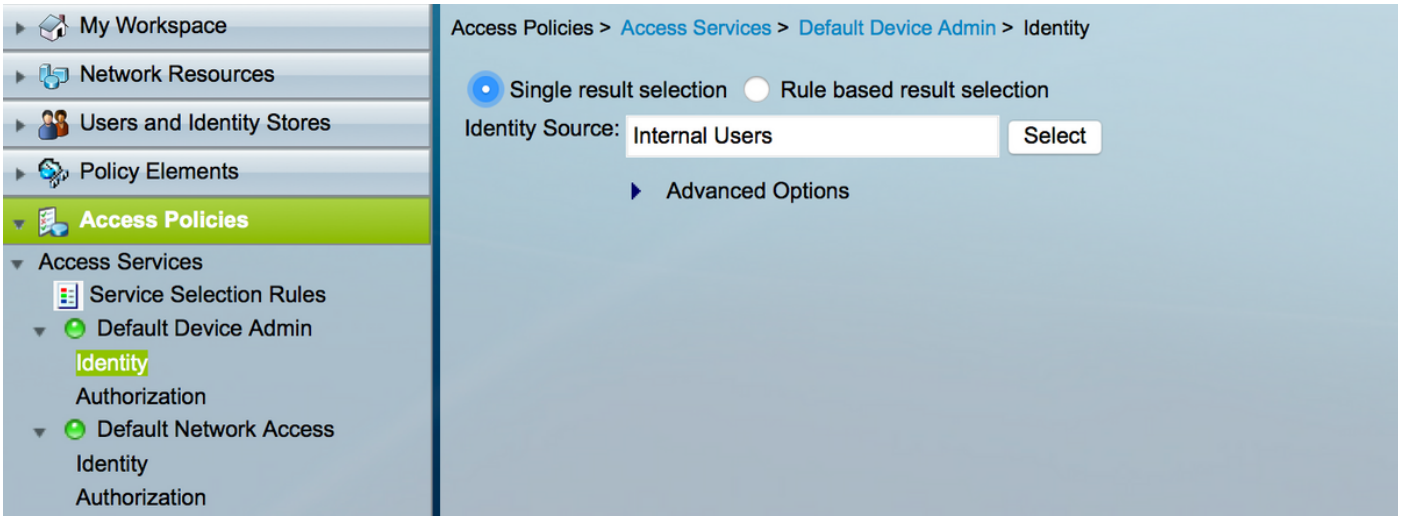




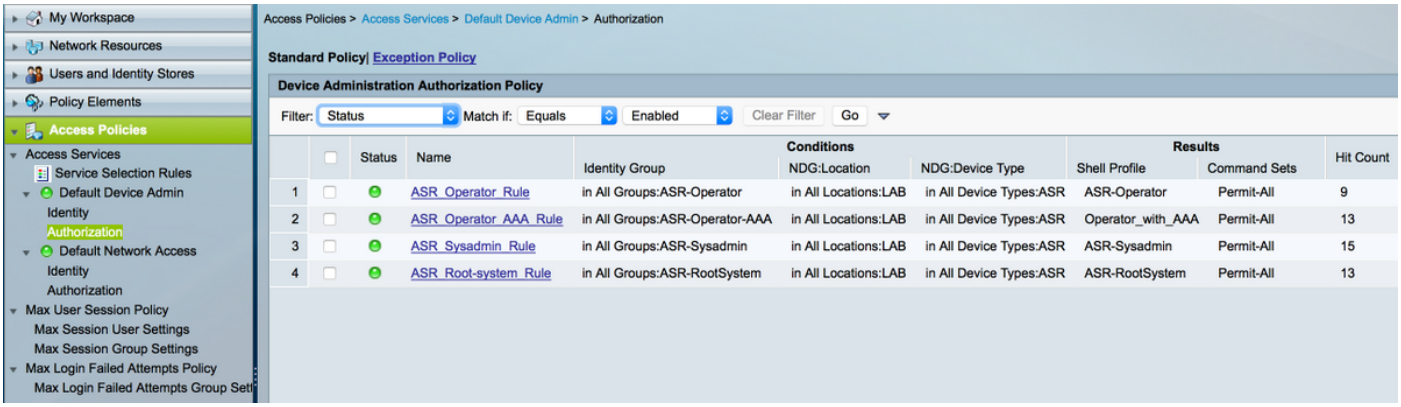




Stap 5. Bepaal het toegangsbeleid. Verificatie vindt plaats tegen de interne gebruikers.



Stap 6. Het configureren van de autorisatie op basis van de vereiste met de eerder gemaakte gebruikersidentiteitsgroepen en het in kaart brengen van de respectievelijke shell profielen, zoals in de afbeelding weergegeven.



Verifiëren

Exploitant

Om in te loggen, **wordt** de gebruikersnaam gebruikt. Dit zijn de verificatieopdrachten.

```
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
```

Exploitant met AAA

Om in te loggen, **wordt** de gebruikersnaam gebruikt. Dit zijn de verificatieopdrachten.

> Opmerking: **asraa** is de exploitanttaak die van de TACACS-server wordt geduwd samen met de aaa taak die wordt gelezen schrijfrecht en uitvoerrechten.

```
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

Om in te loggen, wordt de gebruikersnaam gebruikt. Dit zijn de verificatieopdrachten.

```
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 )
```

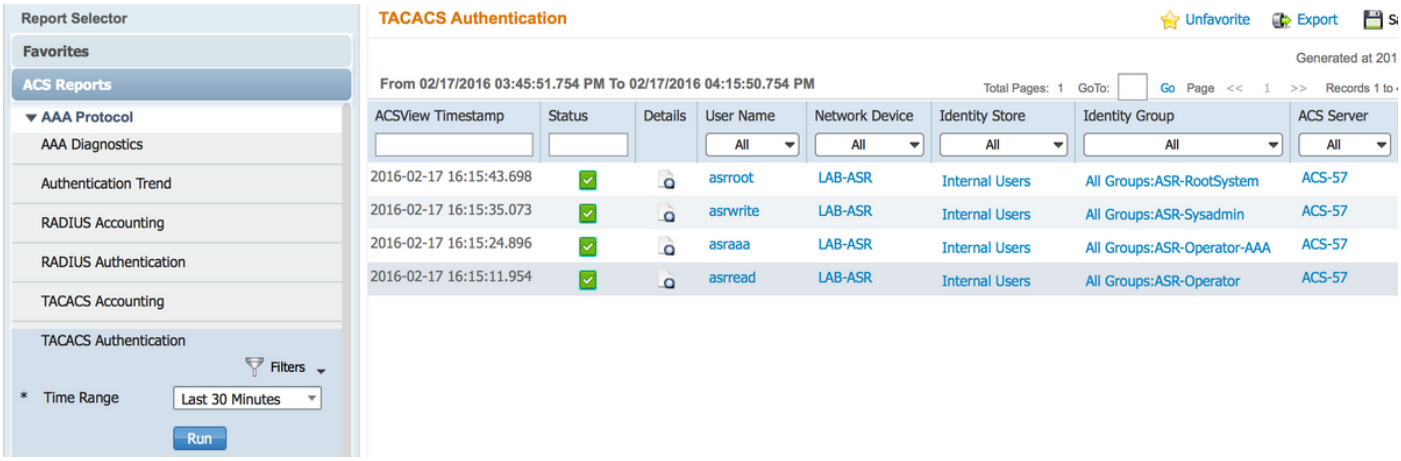
wortelsysteem

Om in te loggen, **wordt** de gebruikersnaam gebruikt. Dit zijn de verificatieopdrachten.

```
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 )
```

Problemen oplossen

U kunt het ACS-rapport van de toezichts- en rapportagepagina controleren. Zoals in de afbeelding wordt getoond, kunt u op het glazen bol van het vergrootglas klikken om het gedetailleerde rapport te zien.



Dit zijn een paar behulpzame opdrachten voor het oplossen van problemen bij ASR:

- show user
- gebruikersgroep tonen
- gebruikerstaken tonen
- alle gebruikers tonen