ASR9K TACACS configureren met Cisco Identity Services Engine 2.4

Inhoud

Inleiding

Dit document beschrijft de configuratie van ASR 9000 Series aggregation services router (ASR) om verificatie en autorisatie via de TACACS+-server met Cisco Identity Services Engine 2.4 mogelijk te maken.

Achtergrondinformatie

Het geeft 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 nodig zijn om een op taken gebaseerde autorisatie uit te voeren, omvatten de manier waarop u gebruikersgroepen en taakgroepen kunt configureren. Gebruikersgroepen en taakgroepen worden geconfigureerd in de Cisco IOS XR-softwareopdrachtset die wordt gebruikt voor verificatie, autorisatie en accounting (AAA) services. De verificatieopdrachten worden gebruikt om de identiteit van een gebruiker of hoofd te controleren. autorisatie-opdrachten 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 de vastlegging van sessies en voor het maken van een audittraject door het opnemen van bepaalde door gebruiker of systeem gegenereerde acties.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ASR 9000 implementatie en basisconfiguratie
- TACACS+ protocol
- ISE 2.4 Installatie en configuratie

Gebruikte componenten

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

- ASR 9000 met Cisco IOS XR-software, versie 5.3.4
- Cisco ISE 2.4

De informatie in dit document wordt gemaakt van apparaten in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als het netwerk actief is, zorg er dan voor dat het potentiële effect van elke configuratieverandering volledig wordt begrepen.

Configureren

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 als een vereiste.

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).

Elke vooraf ingestelde gebruikersgroep heeft bepaalde taakgroepen die aan deze groepen zijn toegewezen en kan niet worden aangepast. Gebruik deze opdrachten om de vooraf gedefinieerde gebruikersgroepen te controleren:

```
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>
```

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: Dienstadministratieve taken

Gebruik deze opdrachten 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
```

Dit is de 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	Netwe

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 deze genoemde taken kan met één van deze of alle vier de 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 de gebruiker gedefinieerde taakgroepen

De beheerders kunnen aangepaste taakgroepen configureren om aan bepaalde behoeften te voldoen. Hier is een 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
```

Beschrijf opdracht kan worden gebruikt om te vinden welke taakgroep en toestemming nodig is voor een bepaalde opdracht.

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#
```

Om een gebruiker in staat te stellen de **commando** op **een gebruikersgroep** uit te voeren, moet de **taakgroep**: de **taak gelezen** moet aan de gebruikersgroep worden toegewezen.

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 in staat te stellen de **standaardstandaardinstellingsloggroep tacacs+** van de configuratiemodus uit te voeren, dient de taakgroep: **schrijf** a **van de taak** te worden toegewezen aan de gebruikersgroep.

De beheerders kunnen de gebruikersgroep definiëren die meerdere taakgroepen kan erven. 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

Configureer de TACACS-server op de ASR-router met het IP-adres en het gedeelde geheim dat moet worden gebruikt.

```
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
!
```

Verificatie en autorisatie configureren om een TACACS-server te gebruiken.

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

Configureer de opdrachttoestemming om een TACACS-server te gebruiken (optioneel):

> Opmerking: Zorg ervoor dat de verificatie en autorisatie naar verwachting werken en zorg ervoor dat de opdrachtsets ook goed zijn geconfigureerd voordat u toestemming voor de opdracht geeft. Indien niet goed ingesteld, kunnen gebruikers mogelijk geen opdrachten op het apparaat invoeren.

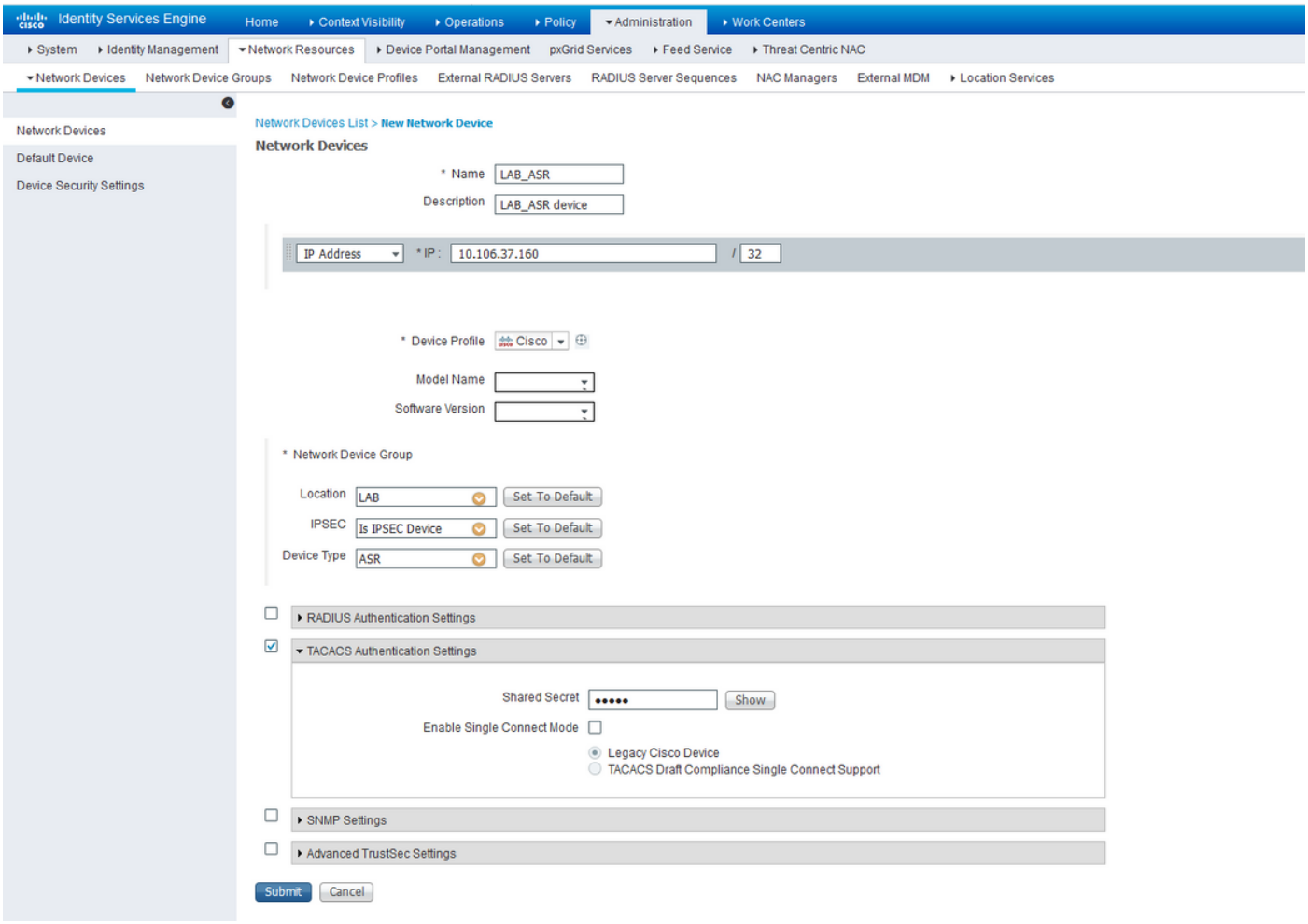
```
#aaa authorization commands default group tacacs+
```

Configuratie van opdrachtaccounting om TACACS server ingesteld (optioneel) te gebruiken.

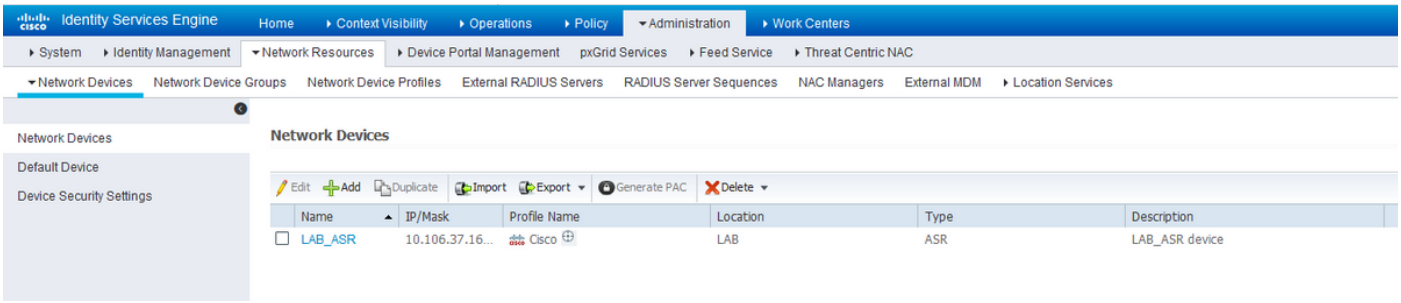
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ISE-serverconfiguratie

Stap 1. Om de router IP in de lijst van AAA-clients op ISE-server te definiëren, navigeer naar **Administratie > NNetwerkbronnen > Netwerkapparaten** zoals in de afbeelding wordt getoond. Gedeeld geheim moet hetzelfde zijn als de geheimen die zijn ingesteld op de ASR-router zoals in de afbeelding.



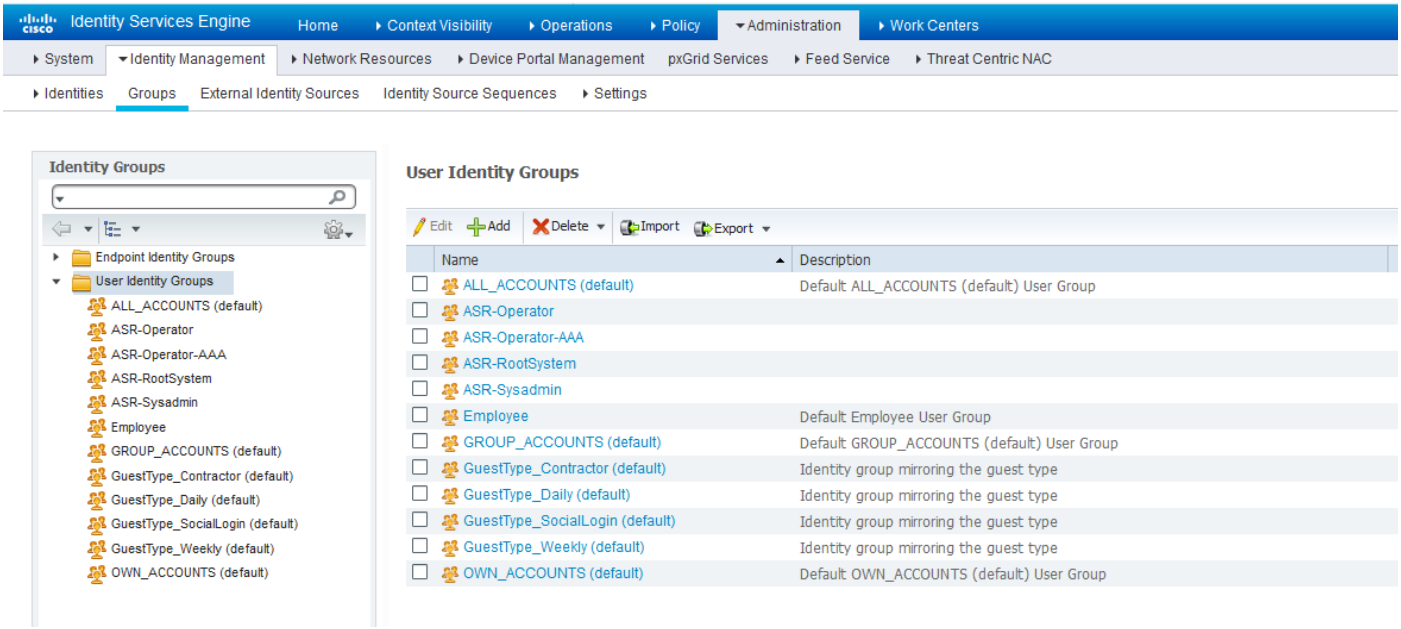
Configuratie van netwerkapparaten



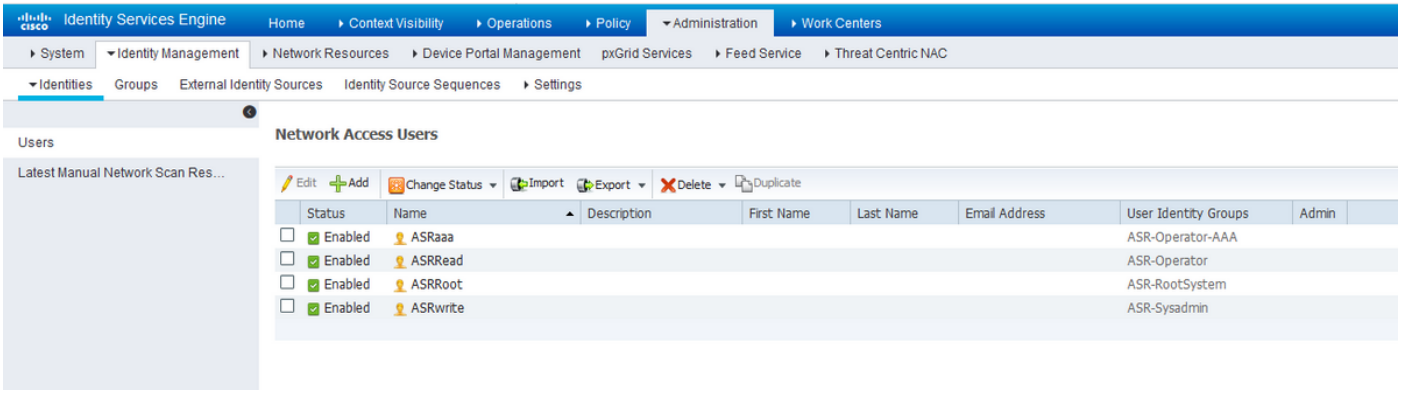
Configuratie van netwerkapparaten

Stap 2. Defineer de gebruikersgroepen volgens uw vereiste, in het voorbeeld, zoals in deze afbeelding, gebruikt u vier groepen. U kunt de groepen definiëren onder **Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen**. De groepen die in dit voorbeeld worden gemaakt zijn:

1. ASR-operator
2. ASR-operator-AAA
3. ASR-rootsysteem
4. ASR-SYsadmin



IdentiteitsgroepenStap 3. Zoals in de afbeelding, kunt u de gebruikers maken en ze in kaart brengen naar de respectievelijke gebruikersgroep die eerder is gemaakt.



Identiteiten/gebruikers

> Opmerking: In dit voorbeeld worden de interne gebruikers van ISE gebruikt voor echtheidscontrole en autorisatie. Verificaties en machtigingen met externe identiteitsbron vallen buiten het toepassingsgebied van dit document.

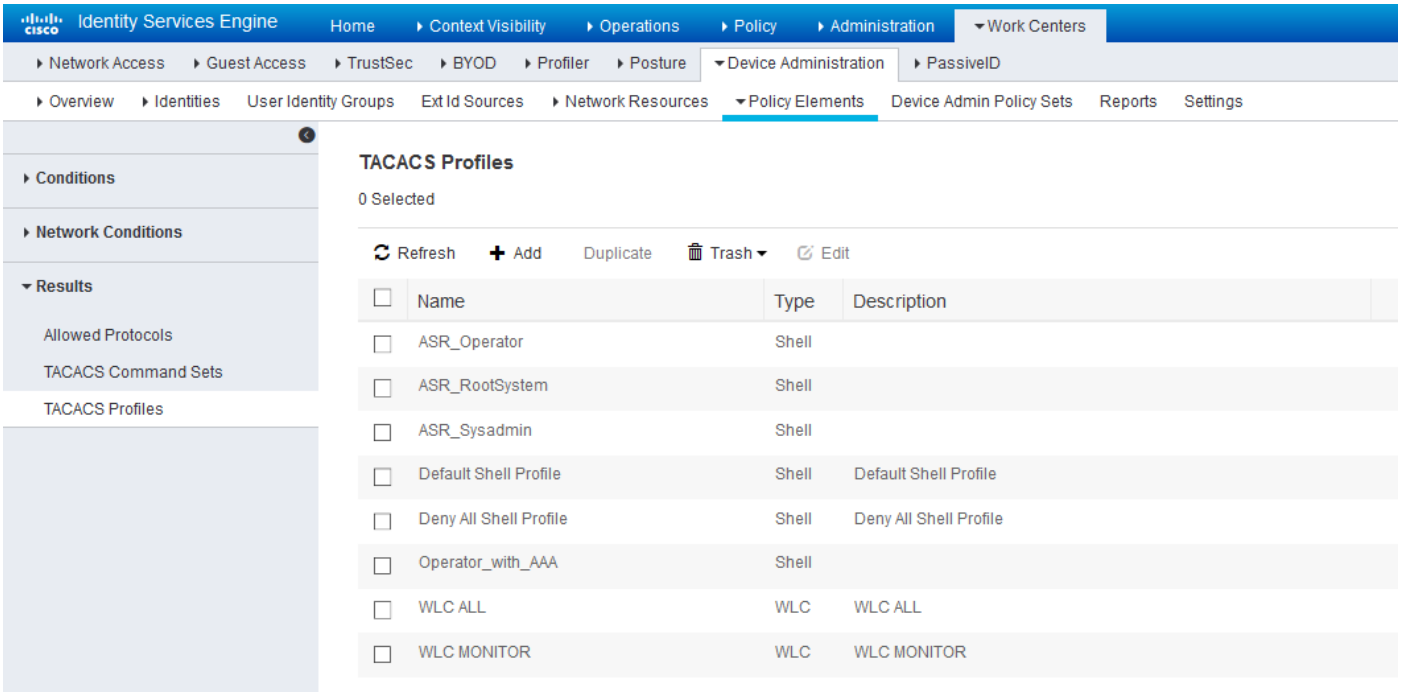
Stap 4. Defineer het Shell-profiel dat voor de respectieve gebruikers moet worden geduwd. Om dit te doen, navigeer naar **Werkcentra > Apparaatbeheer > Elementen beleid > Resultaten > TACACS profielen**. U kunt een nieuw shell-profiel configureren zoals in de beelden ook voor vorige versies van ISE wordt getoond. De in dit voorbeeld gedefinieerde shell profielen zijn:

1. ASR_operator

2. ASR_RootSystem

3. ASR_Sysadmin

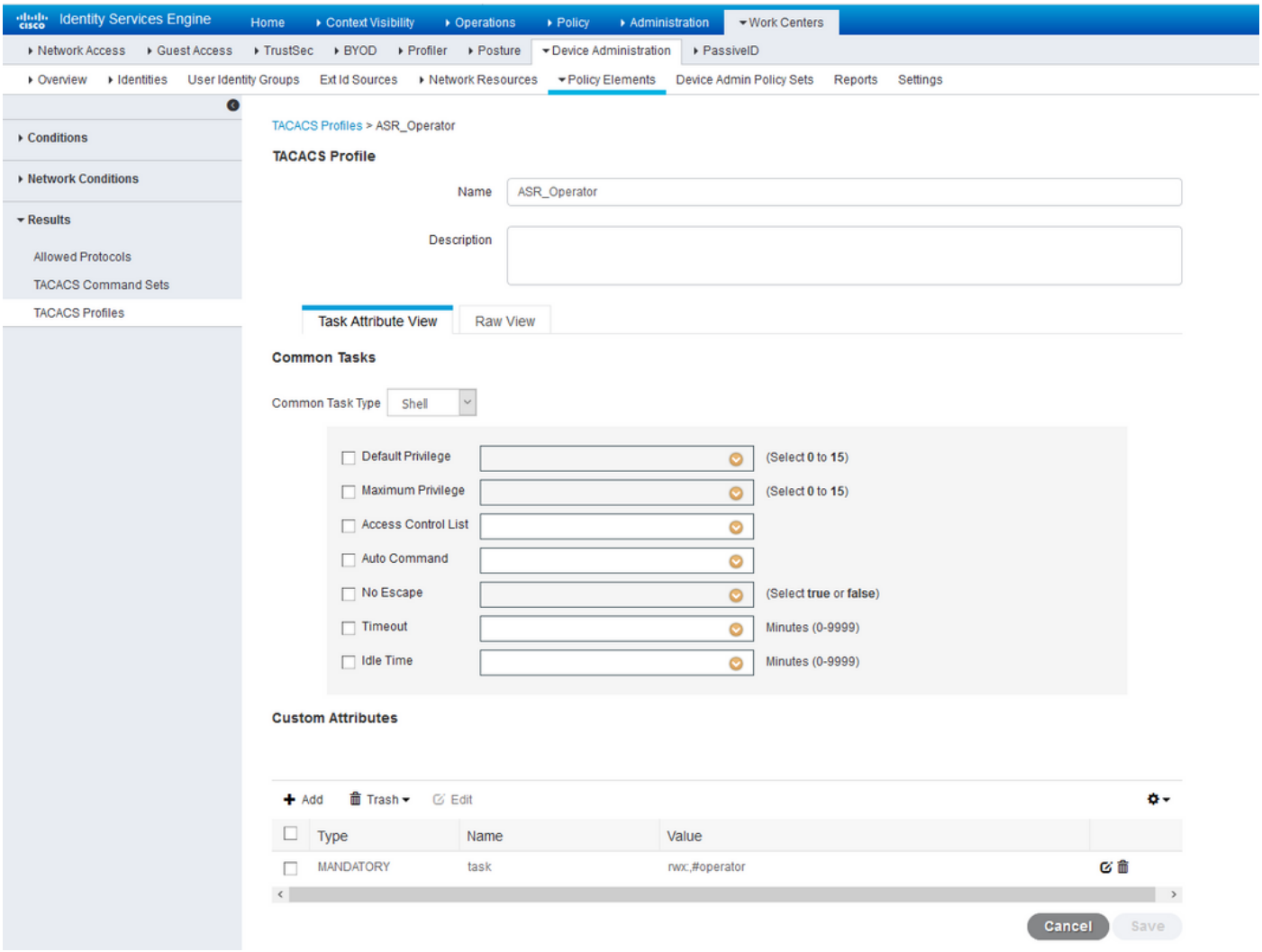
4. Exploitant_met_AAA



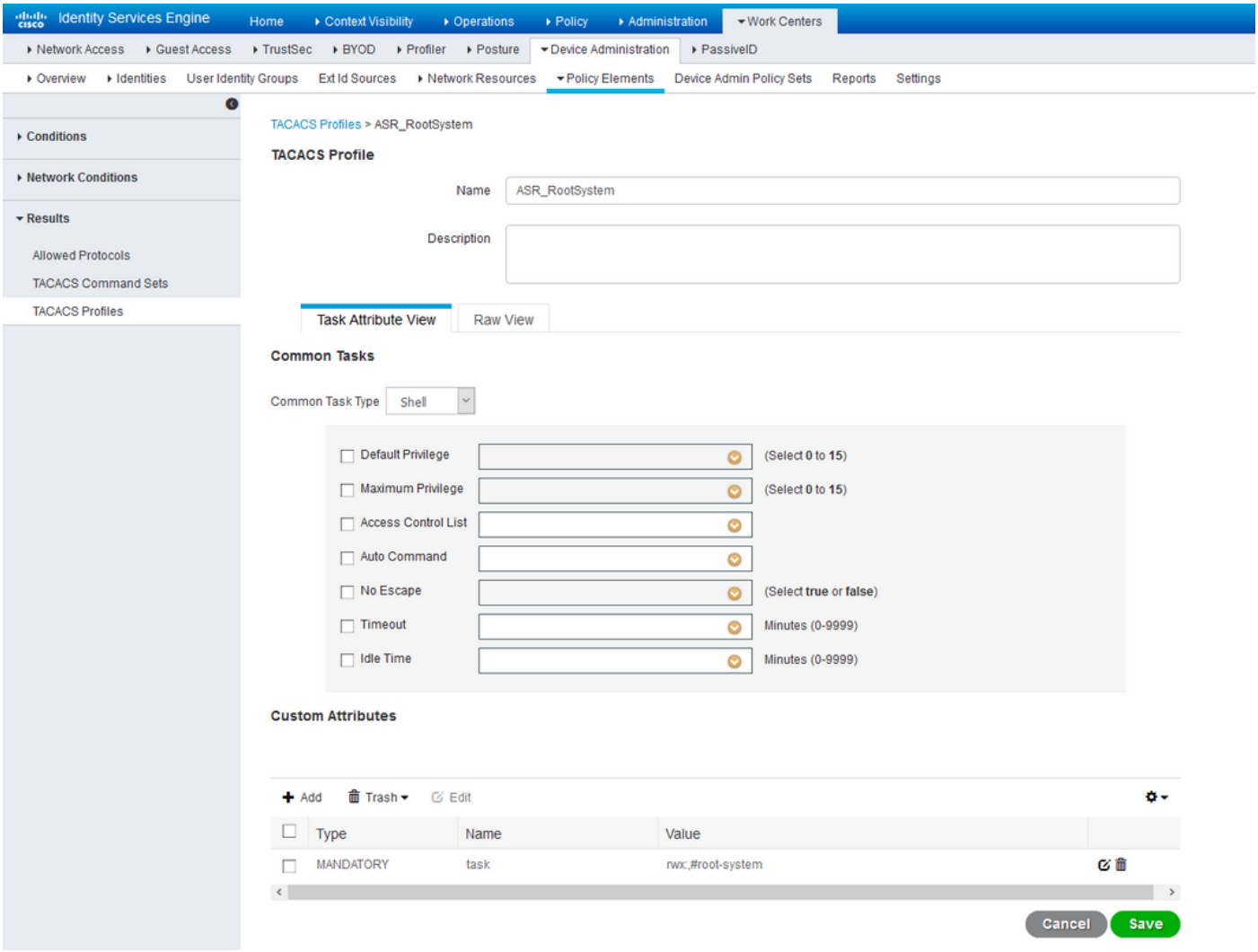
Shell-profielen voor TACACS

U kunt op de knop **Toevoegen** klikken om het veldtype, de naam en de waarde in te voeren zoals in de afbeeldingen onder de sectie **Aangepaste kenmerken wordt weergegeven**.

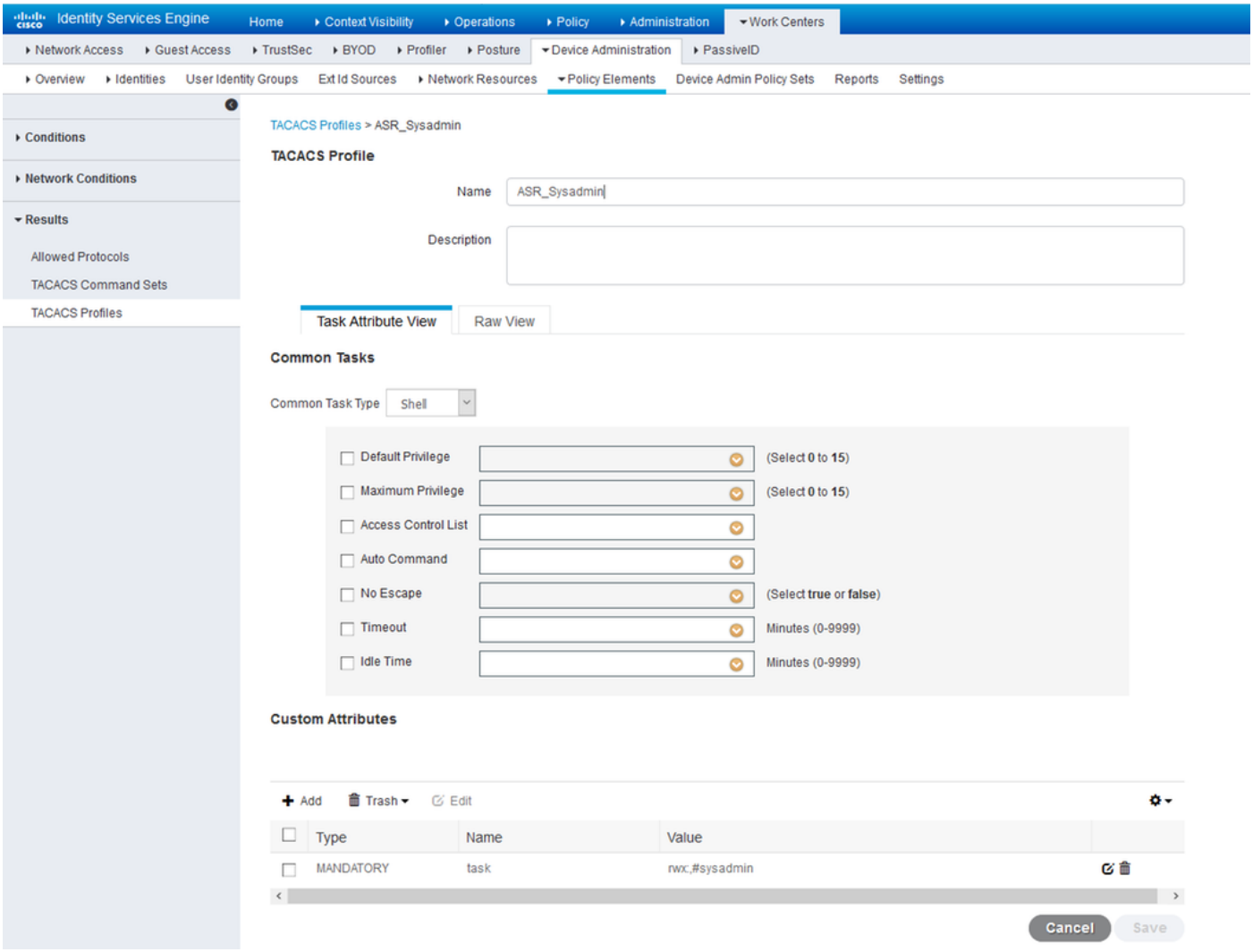
Voor de rol van exploitant:



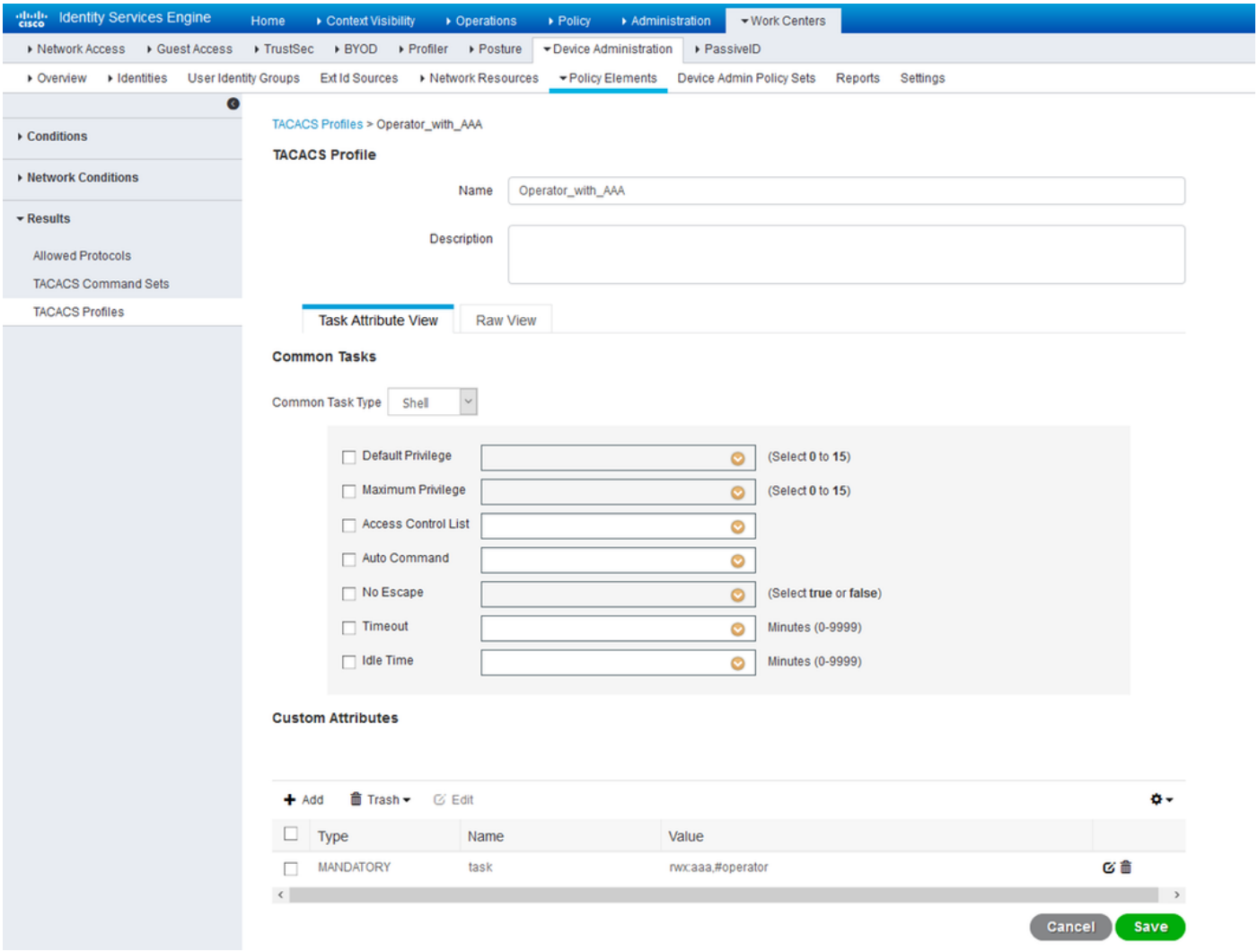
ASR-profiel van operatorVoor de rol van het wortelsysteem:



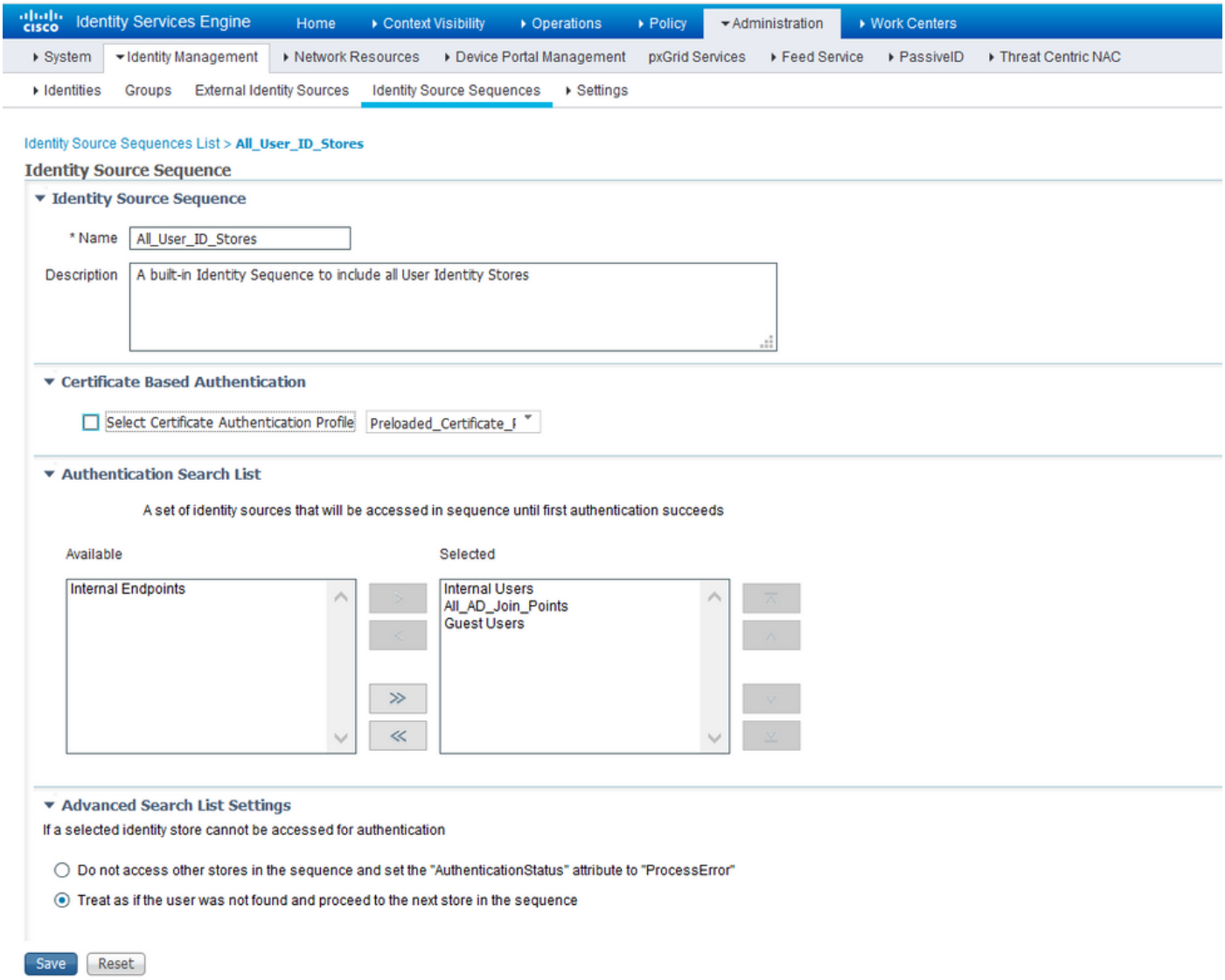
ASR-profiel voor wortelsysteemVoor sysadmin rol:



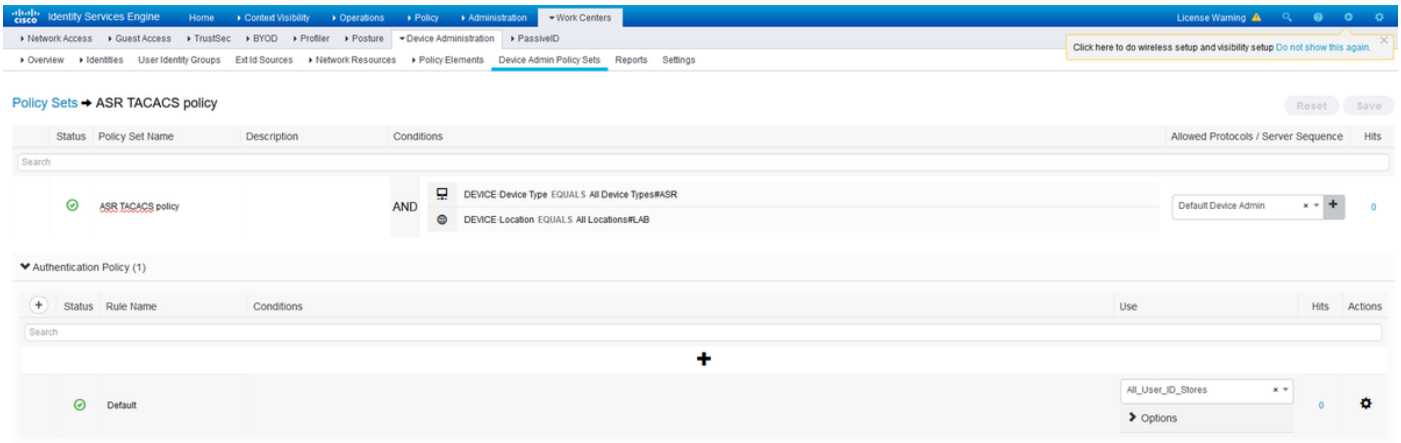
ASR Sysadmin shell-profielVoor de rol van exploitant en AAA:



Exploitant met AAA-shell-profielStap 5. Configureer de volgorde van de identiteitsbron om de interne gebruikers te gebruiken bij **Administratie > identiteitsbeheer > Vervolgingen van identiteitsbron.** U kunt een nieuwe reeks van Identity Bron toevoegen of de beschikbare reeks bewerken.



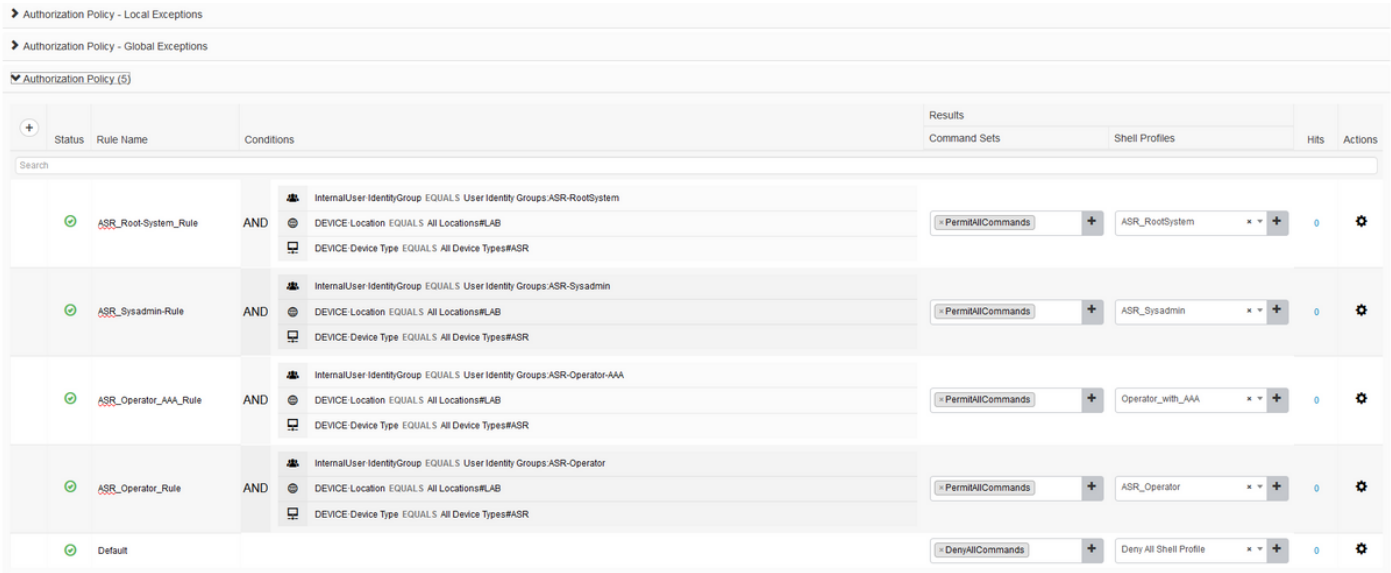
Stap 6. Configureer het verificatiebeleid in **Workcenters > Apparaatbeheer > ApparaatAdmin Policy Sets > [Policy Suite]** om gebruik te maken van de Identity Store Sequence die de interne gebruikers bevat. Configuratie de vergunning op basis van de vereiste met het gebruik van de eerder gemaakte gebruikersidentiteitsgroepen en kaart de respectieve Shell profielen in, zoals weergegeven in het beeld.



Verificatiebeleid

Het autorisatiebeleid kan op veel manieren worden geconfigureerd op basis van de vereiste. De regels die hier in de afbeelding worden weergegeven, zijn gebaseerd op de locatie, het type en de specifieke groep gebruikers met identiteit. De geselecteerde Shell-profielen worden op het

moment van de autorisatie samen met de Opdrachten geduwd.



machtigingsbeleid

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Exploitant

Controleer de gebruikersgroep en de taakgroepen die **worden** toegewezen **wanneer** de gebruiker zich in de router inlogt.

```
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

Controleer de gebruikersgroep en de toegewezen taakgroepen wanneer**asraaa** De gebruiker logt in op de router.

> **Opmerking**:asrais de uitvoertaak die van de TACACS-server is geduwd samen met de AAA-taak die wordt gelezen, geschreven en uitgevoerd permissies.

```
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

Controleer de gebruikersgroep en de toegewezen taakgroepen wanneer**verbreden** De gebruiker logt in op de router.

```
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

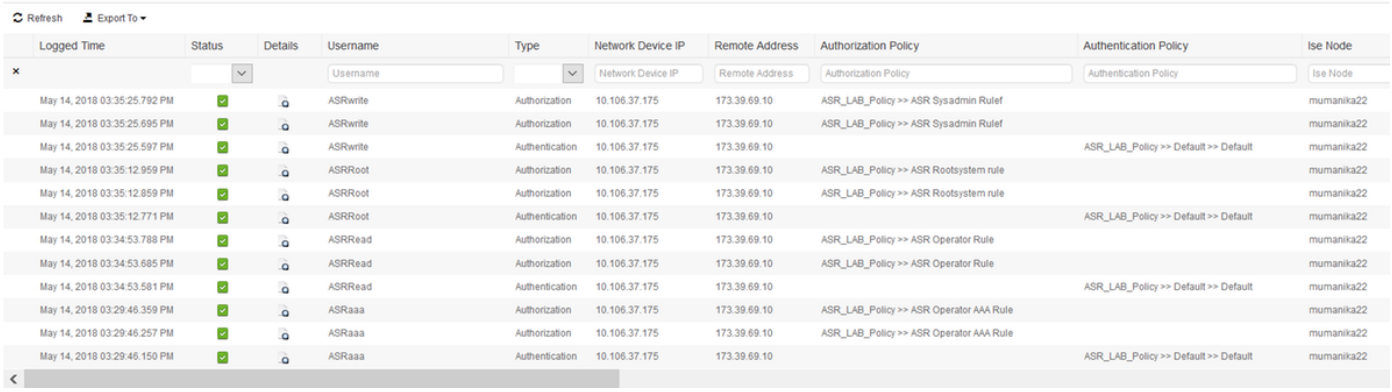
Controleer de gebruikersgroep en de toegewezen taakgroepen wanneer**wortel** De gebruiker logt in op de router.

```
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

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Controleer het ISE-rapport van de **bewerkingen > TACACS > Live Logs**. Klik op het symbool van het vergrootglas om het gedetailleerde rapport te zien.



Refresh Export To

Logged Time	Status	Details	Username	Type	Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
			Username		Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
May 14, 2018 03:35:25.792 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Sysadmin Rulef		mumanika22
May 14, 2018 03:35:25.695 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Sysadmin Rulef		mumanika22
May 14, 2018 03:35:25.597 PM	✓		ASRwrite	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
May 14, 2018 03:35:12.959 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Rootsystem rule		mumanika22
May 14, 2018 03:35:12.859 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Rootsystem rule		mumanika22
May 14, 2018 03:35:12.771 PM	✓		ASRRoot	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
May 14, 2018 03:34:53.788 PM	✓		ASRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator Rule		mumanika22
May 14, 2018 03:34:53.685 PM	✓		ASRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator Rule		mumanika22
May 14, 2018 03:34:53.581 PM	✓		ASRRead	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
May 14, 2018 03:29:46.359 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator AAA Rule		mumanika22
May 14, 2018 03:29:46.257 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator AAA Rule		mumanika22
May 14, 2018 03:29:46.150 PM	✓		ASRaaa	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22

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

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