Configuración de ASR9K TACACS con Cisco Identity Services Engine 2.4

Contenido

Introducción

Este documento describe la configuración de ASR 9000 Series Aggregation Services Router (ASR) para autenticar y autorizar a través de TACACS+ con el servidor Cisco Identity Services Engine 2.4.

Antecedentes

Muestra la implementación del modelo administrativo de autorización basada en tareas que se utiliza para controlar el acceso del usuario en el sistema de software Cisco IOS® XR. Las principales tareas necesarias para implementar la autorización basada en tareas incluyen cómo configurar grupos de usuarios y grupos de tareas. Los grupos de usuarios y los grupos de tareas se configuran mediante el conjunto de comandos de software Cisco IOS® XR utilizado para los servicios de autenticación, autorización y contabilidad (AAA). Los comandos de autenticación se utilizan para verificar la identidad de un usuario o entidad principal. Los comandos de autorización se utilizan para verificar que a un usuario (o entidad principal) autenticado se le concede permiso para realizar una tarea específica. Los comandos de contabilidad se utilizan para registrar sesiones y crear una pista de auditoría mediante la grabación de ciertas acciones generadas por el usuario o el sistema.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Implementación y configuración básica de ASR 9000
- Protocolo TACACS+
- Implementación y configuración de ISE 2.4

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASR 9000 con Cisco IOS® XR Software, versión 5.3.4
- Cisco ISE 2.4

La información de este documento se crea a partir de dispositivos en un entorno de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está activa, asegúrese de que se comprende completamente el impacto potencial de cualquier cambio de configuración.

Configurar

Componentes predefinidos en IOS® XR

Hay grupos de usuarios y grupos de tareas predefinidos en IOS® XR. El administrador puede utilizar estos grupos predefinidos o definir grupos personalizados según los requisitos.

Grupos de usuarios predefinidos

Estos grupos de usuarios están predefinidos en IOS® XR:

Grupo de usuarios	Privilegios
soporte de Cisco	Funciones de depuración y resolución de problemas (normalmente, utilizadas por el person de soporte técnico de Cisco).
netadmin	Configure los protocolos de red, como Open Shortest Path First (OSPF) (que suelen utiliza los administradores de red).
operador	Realice actividades de supervisión diarias y tenga derechos de configuración limitados.
root-lr	Muestra y ejecuta todos los comandos dentro de un solo RP.
sistema raíz	Muestra y ejecuta todos los comandos para todos los RPs del sistema.
sysadmin	Realice tareas de administración del sistema para el router, como el mantenimiento del lug donde se almacenan los vaciados de memoria o la configuración del reloj del protocolo de tiempo de red (NTP).
serviceadmin	Realice tareas de administración de servicios, como el controlador de límite de sesión (SB

Cada grupo de usuarios predefinido tiene determinados grupos de tareas asignados a ellos y no se pueden modificar. Utilice estos comandos para verificar los grupos de usuarios predefinidos:

```
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>
```

Grupos de tareas predefinidos

Estos grupos de tareas predefinidos están disponibles para que los administradores los utilicen, normalmente para la configuración inicial:

- Soporte de Cisco: Tareas del personal de soporte de Cisco
- netadmin: Tareas del administrador de red
- operador: Tareas diarias del operador (a efectos de demostración)
- root-lr: Tareas del administrador del router de dominio seguro
- sistema raíz: Tareas de administrador en todo el sistema
- sysadmin: Tareas del administrador del sistema
- serviceadmin: Tareas de administración de servicios

Utilice estos comandos para verificar los grupos de tareas predefinidos:

```
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>
```

Utilice este comando para verificar las tareas soportadas:

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

Esta es la lista de tareas admitidas:

AAA	Acl	Admin	Ancp	ATM	servicios básicos	Bcdl	Bfd
Reiniciar	Paquete	call-home	Cdp	CEF	Cgn	soporte de Cisco	config-mgmt
Criptografía	DIAG	No permitido	Factores	Dwdm	Eem	EIGRP	ethernet-service
Fabric	fail-mgr	Sistema	Firewall	FR	Hdlc	host-services	Hsrp

Inventario	ip-services	de archivos IPv4	Ipv6	Isis	L2vpn	Li	Lisp
Lpts	Monitor	mpls-ldp	mpls-static	mpls-te	Multicast (multidifusión)	Netflow	Red
OSPF	Ouni	Pbr	pkg-mgmt	pos-dpt	PPP	QoS	Rcmd
RIP	root-lr	sistema raíz	route-map	route-policy	Sbc	SNMP (Protocolo de administración de red simple)	sonet-sdh
Sysmgr	Sistema	Transporte	Acceso a tty	Túnel	Universal	Vlan	VPDN

Cada una de estas tareas mencionadas puede darse con cualquiera de estos o los cuatro permisos:

Leer	Especifica una designación que permite sólo una operación de lectura.
Escritura	Especifica una designación que permite una operación de cambio y permite implícitamente una operación de lectura.
Ejecutar	Especifica una designación que permite una operación de acceso; por ejemplo, ping y Telnet.
Depurar	Especifica una designación que permite una operación de depuración.

Grupos de tareas definidos por el usuario

Los administradores pueden configurar grupos de tareas personalizados para satisfacer necesidades específicas. Este es un ejemplo de configuración:

```
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
```

Describir puede utilizarse para encontrar el grupo de tareas y el permiso necesarios para un comando determinado.

Ejemplo 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#
```

Para permitir que un usuario ejecute el **comando show aaa usergroup**, el grupo de tareas: **tarea read aaa** se debe asignar al grupo de usuarios.

Ejemplo 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)#
```

Para permitir que un usuario ejecute el **comando authentication login default tacacs+**desde el modo de configuración, grupo de tareas: **tarea read write aaa** se debe asignar al grupo de usuarios.

Los administradores pueden definir el grupo de usuarios que puede heredar varios grupos de tareas. Este es el ejemplo de configuración:

```
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
```

Configuración AAA en el Router

Configure el servidor TACACS en el router ASR con la dirección IP y el secreto compartido que se utilizará.

```
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
!
```

Configure la autenticación y autorización para utilizar el servidor TACACS configurado.

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

Configure la autorización de comandos para utilizar el servidor TACACS configurado (opcional):

> **Nota:** Asegúrese de que la autenticación y la autorización funcionen como se espera, y asegúrese de que los conjuntos de comandos también estén configurados correctamente antes de habilitar la autorización de comandos. Si no se configura correctamente, es posible que los usuarios no puedan introducir ningún comando en el dispositivo.

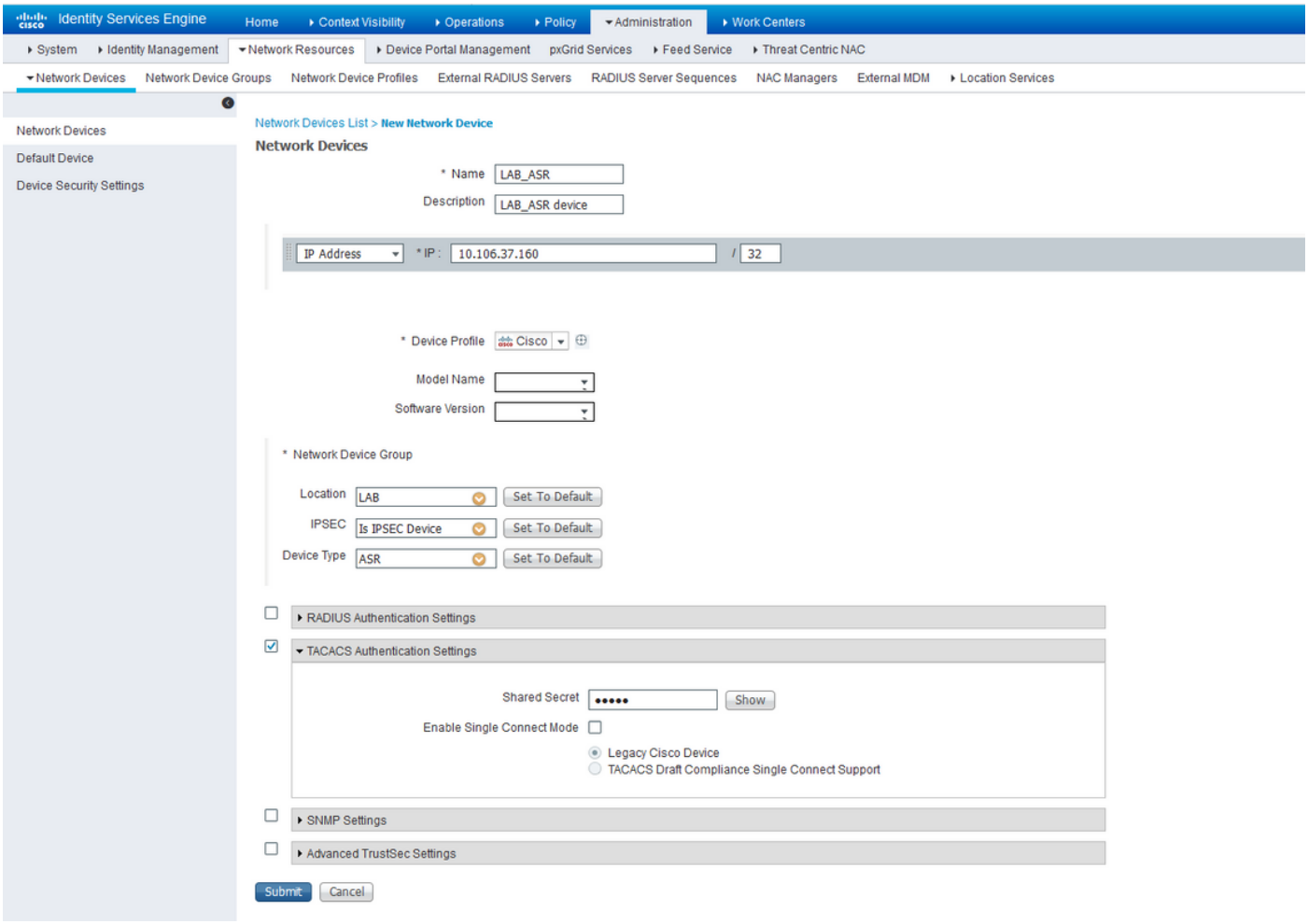
```
#aaa authorization commands default group tacacs+
```

Configure la contabilización de comandos para utilizar el servidor TACACS configurado (opcional).

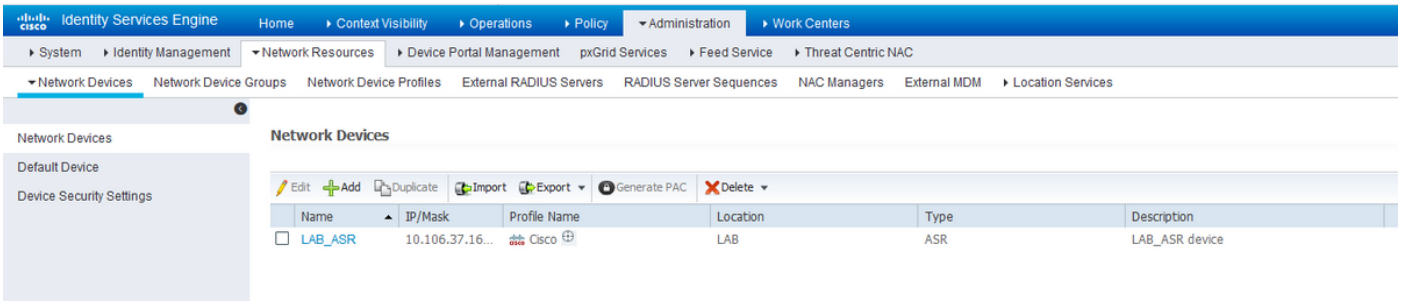
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

Configuración del servidor ISE

Paso 1. Para definir la IP del router en la lista de clientes AAA en el servidor ISE, navegue hasta **Administration > NRecursos de red > Dispositivos de red** como se muestra en la imagen. El secreto compartido debe ser el mismo que el configurado en el router ASR como se muestra en la imagen.



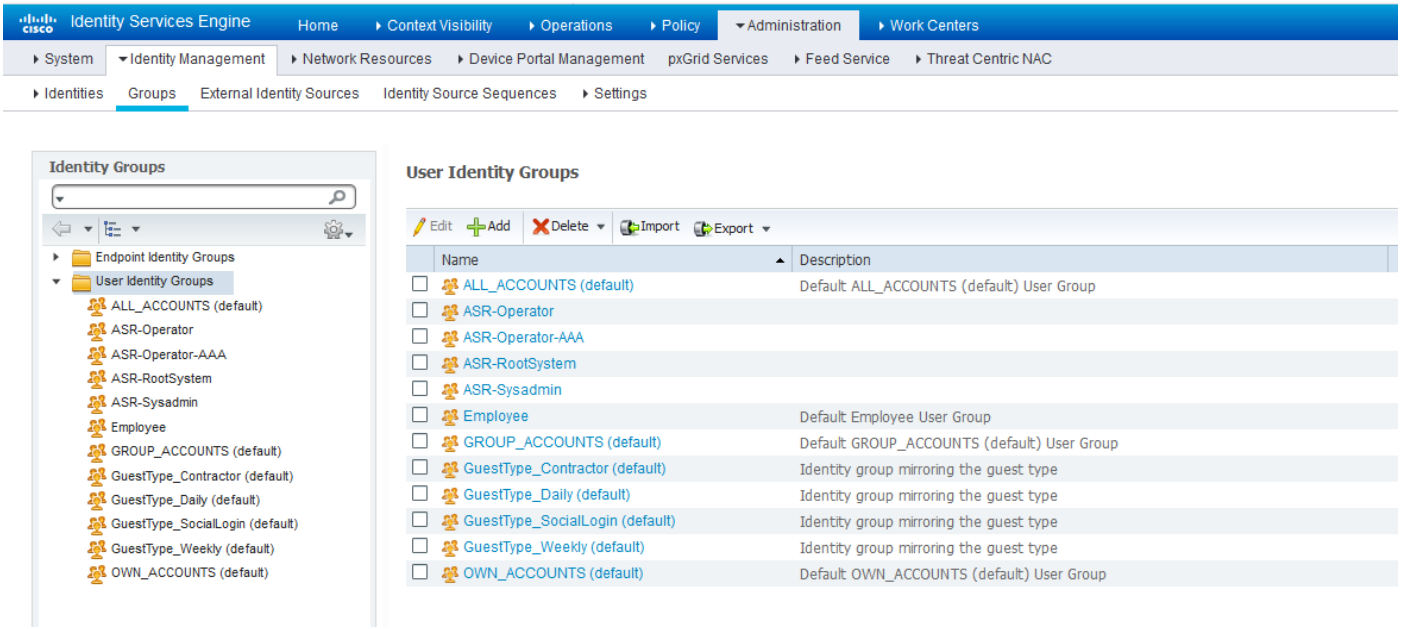
Configuración del dispositivo de red



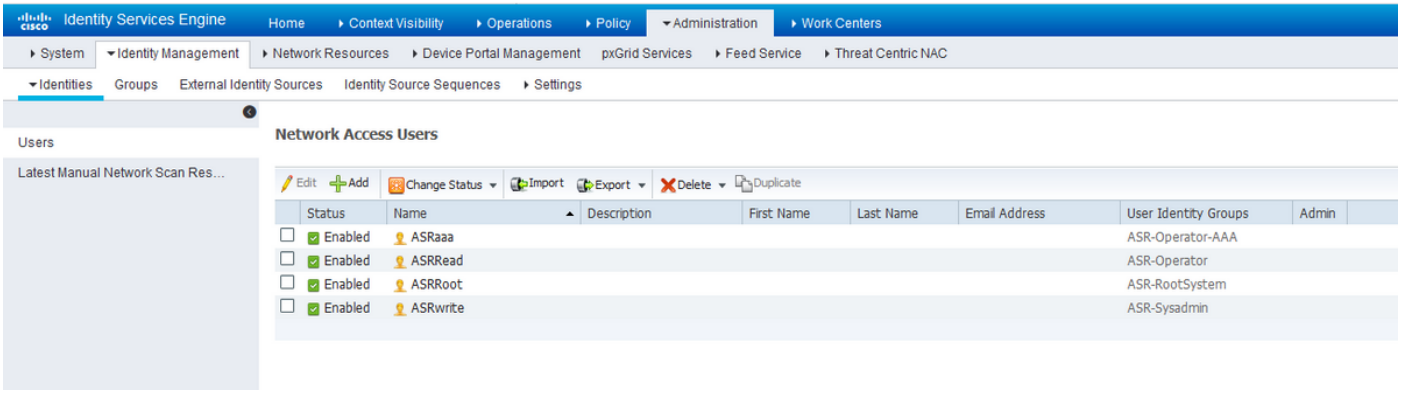
Configuración del dispositivo de red

Paso 2. Defina los grupos de usuarios según sus requisitos, en el ejemplo, como se muestra en esta imagen, puede utilizar cuatro grupos. Puede definir los grupos bajo **Administración > Administración de identidades > Grupos > Grupos de identidades de usuario**. Los grupos creados en este ejemplo son:

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



Grupos de identidadPaso 3. Como se muestra en la imagen, cree los usuarios y asígnelos al grupo de usuarios respectivo que se creó anteriormente.



Identidades/Usuarios

> **Nota:** En este ejemplo, los usuarios internos de ISE se utilizan para la autenticación y autorización. Las autenticaciones y autorizaciones con External Identity Source están fuera del alcance de este documento.

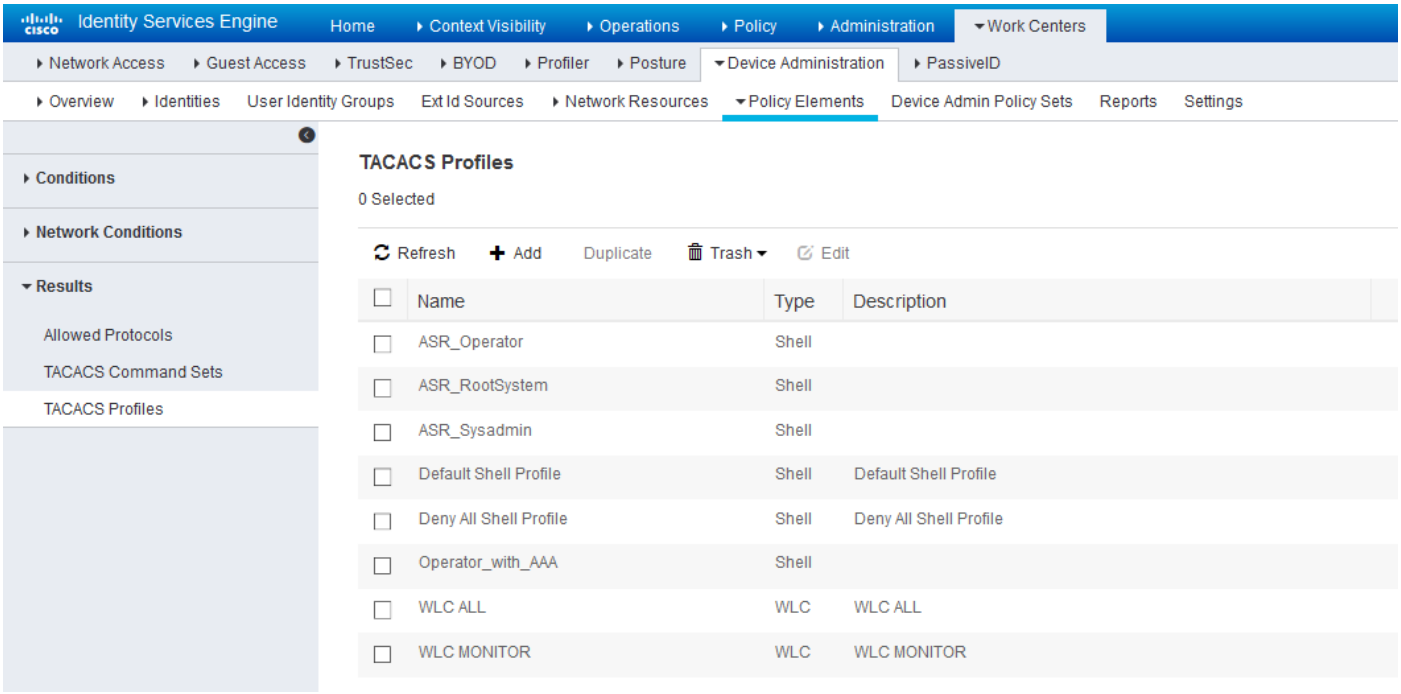
Paso 4. Defina el perfil de shell que se aplicará a los usuarios respectivos. Para hacerlo, navegue hasta **Centros de trabajo > Administración de dispositivos > Elementos de políticas > Resultados > Perfiles TACACS**. Se puede configurar un nuevo perfil de shell como se muestra en las imágenes, así como en las versiones anteriores de ISE. Los perfiles de shell definidos en este ejemplo son:

1. ASR_Operator

2. ASR_RootSystem

3. ASR_Sysadmin

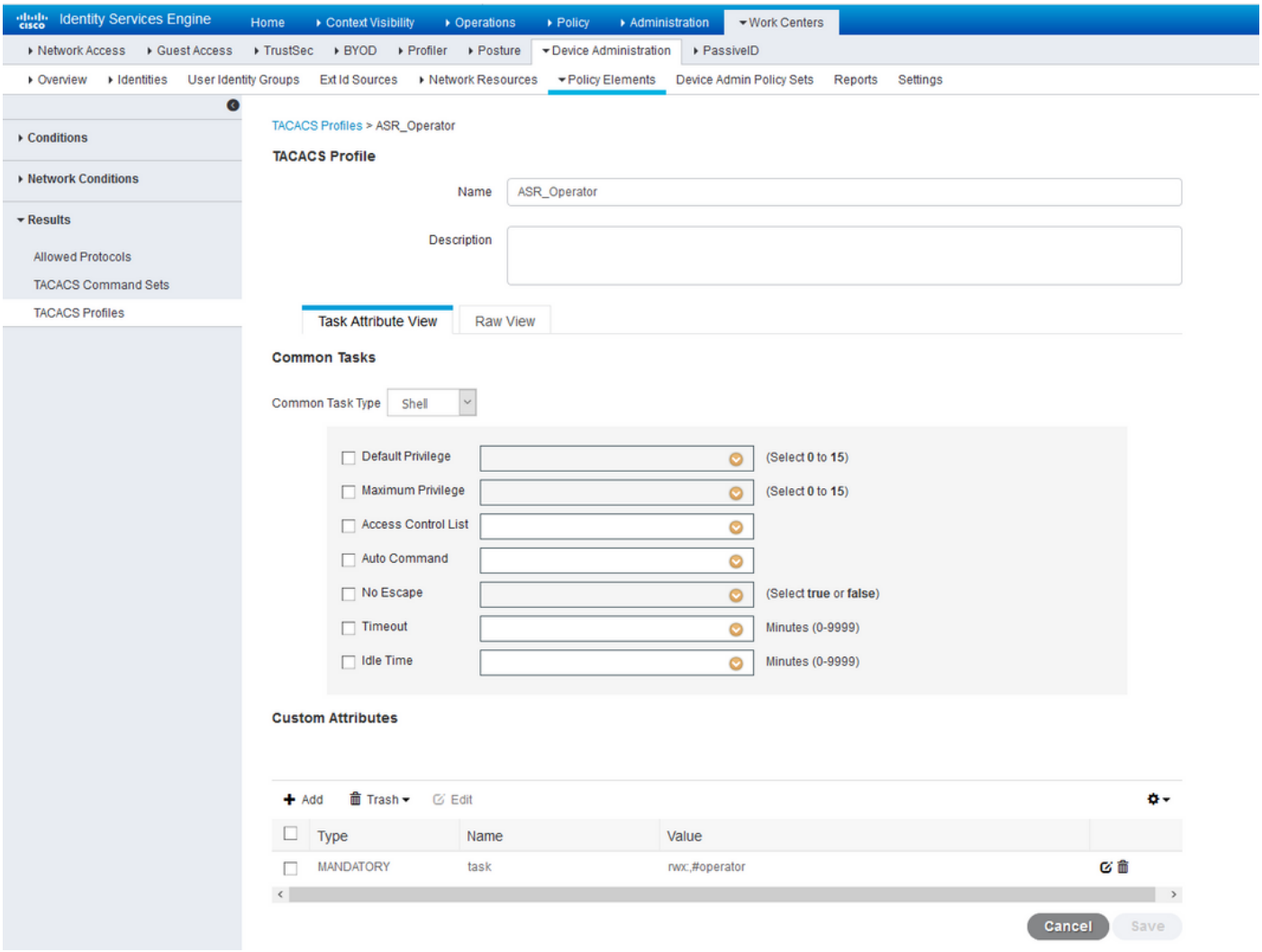
4. Operador_con_AAA



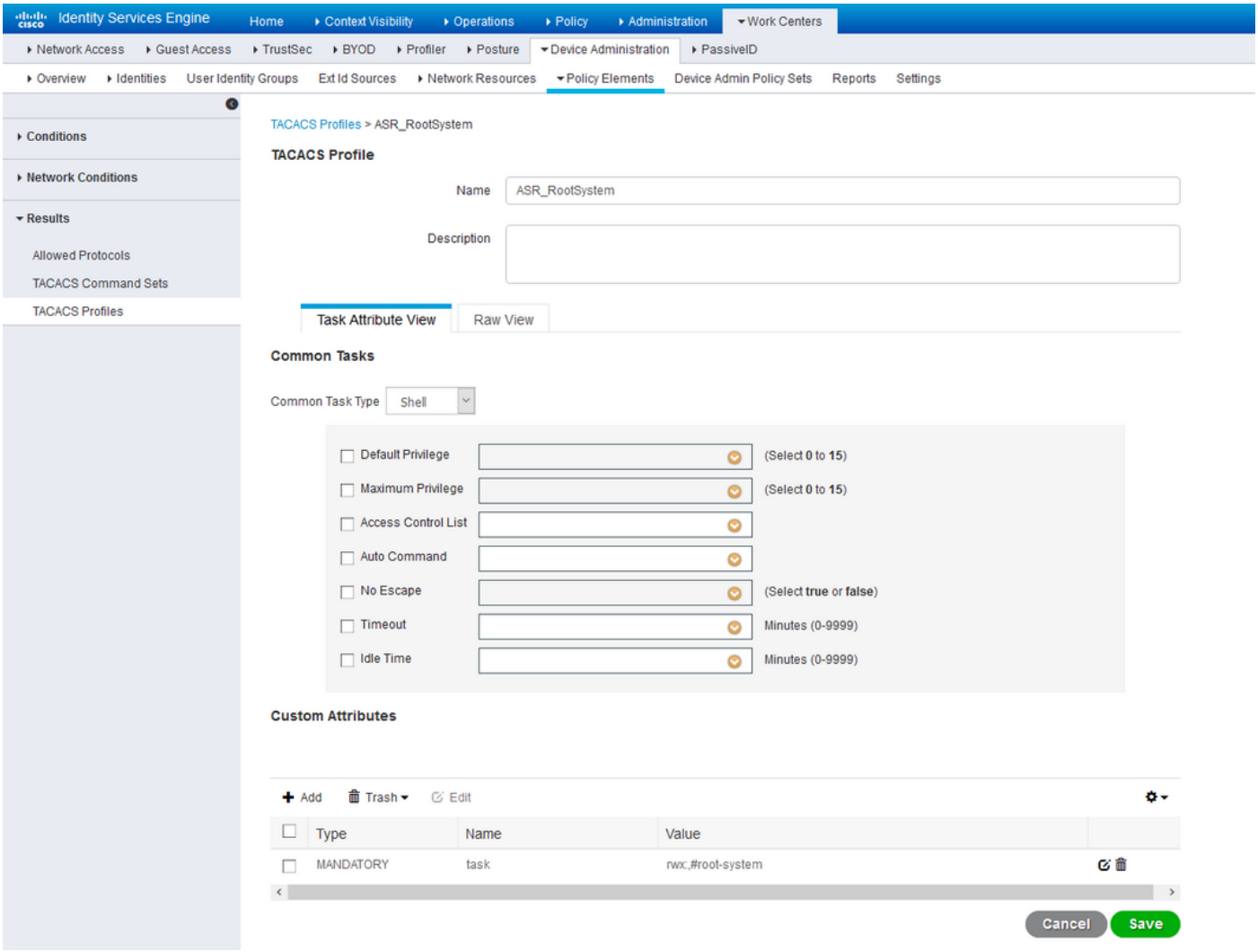
Perfiles de Shell para TACACS

Se puede hacer clic en el botón **Agregar** para introducir los campos Tipo, Nombre y Valor, como se muestra en las imágenes bajo la sección **Atributos personalizados**.

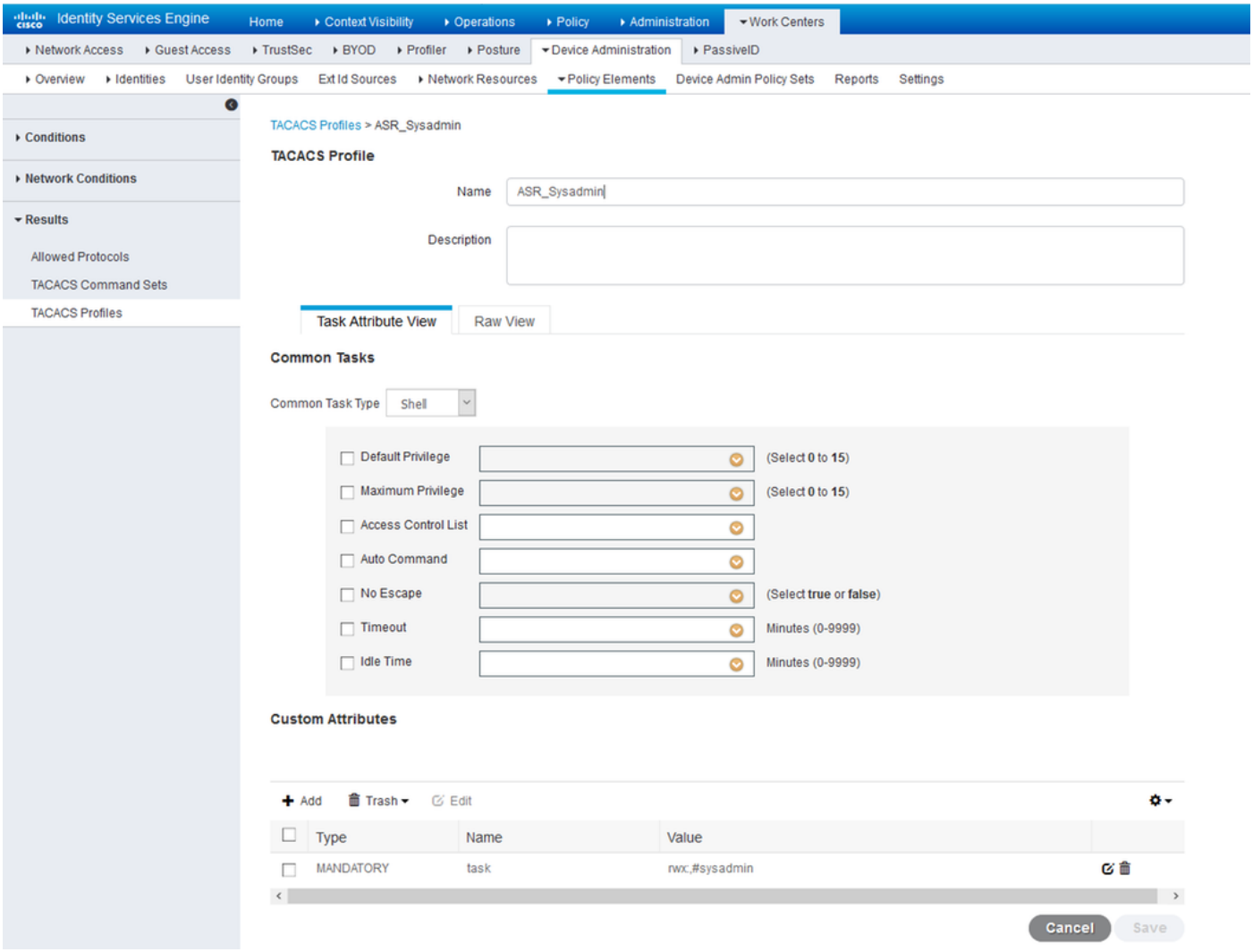
Para la función de operador:



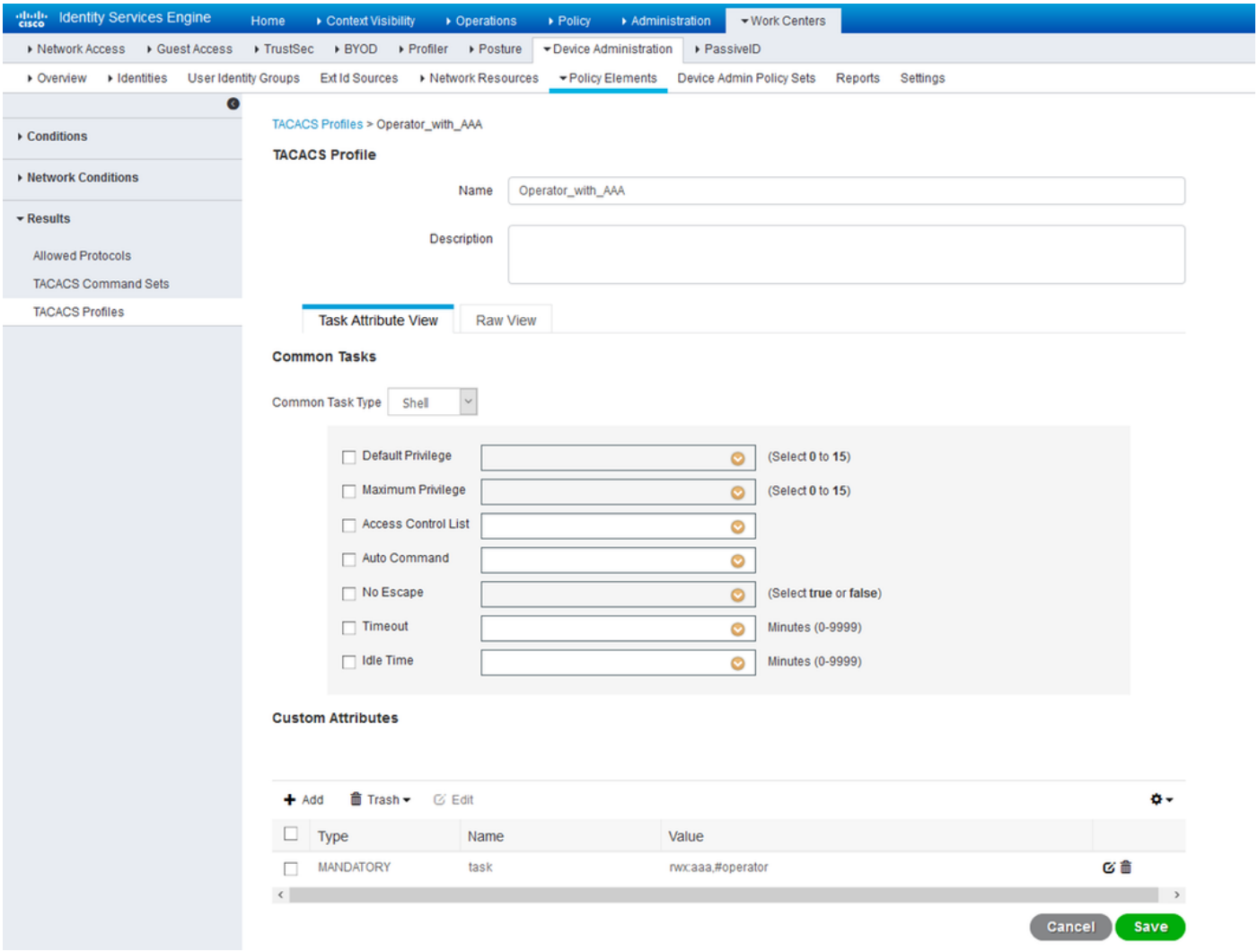
perfil del shell del operador ASRPara la función de sistema raíz:



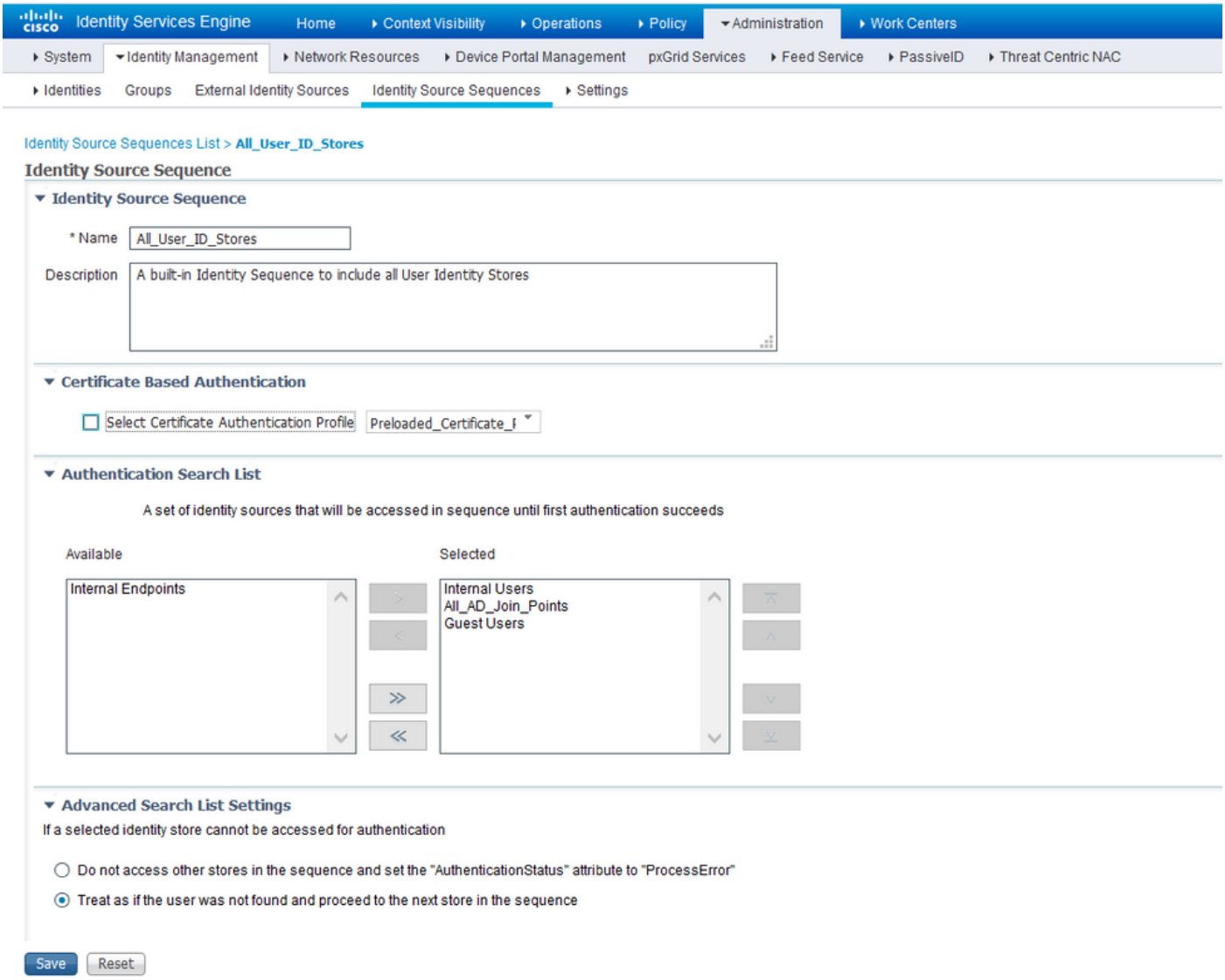
perfil del shell del sistema raíz ASRPara el rol de sysadmin:



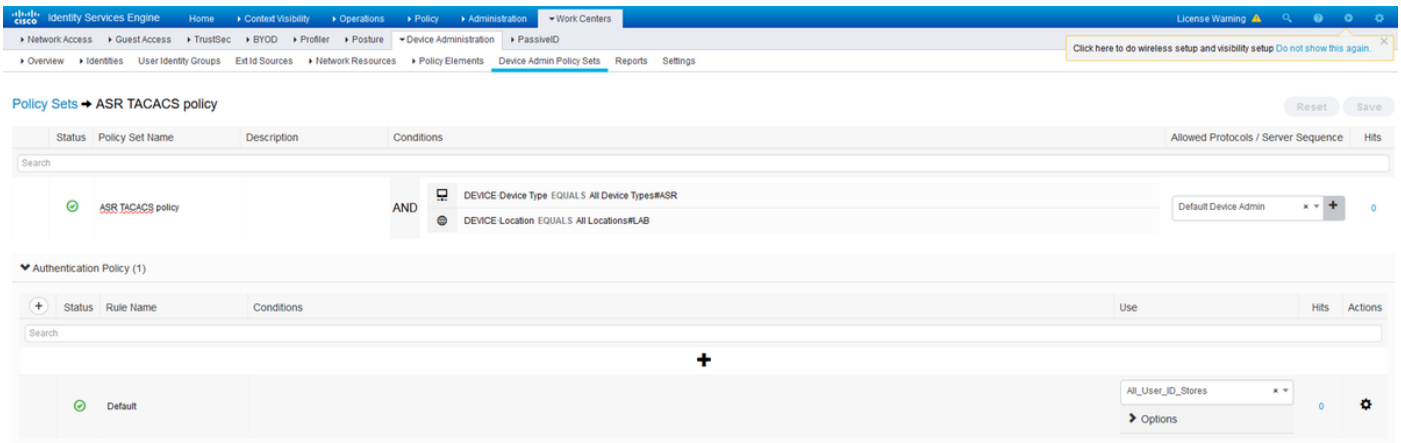
perfil del shell del sistema ASRPara la función de operador y AAA:



Operador con perfil de shell AAAPaso 5. Configure la Secuencia de Origen de Identidad para utilizar los Usuarios Internos en **Administration > Identity Management > Identity Source Sequences.** Se puede agregar una nueva secuencia de origen de identidad o editar las disponibles.



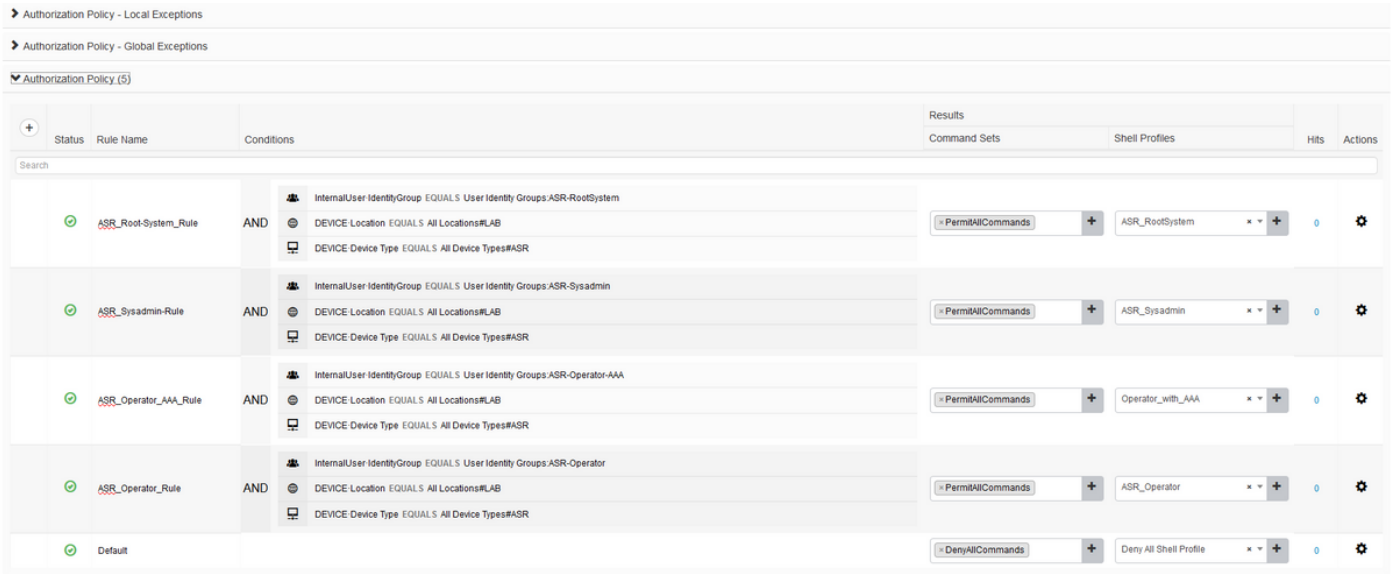
Paso 6. Configure la política de autenticación en **Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos > [Elegir conjunto de políticas]** para hacer uso de la secuencia de almacenamiento de identidad que contiene los usuarios internos. Configure la autorización en función del requisito con el uso de los grupos de identidad de usuario previamente creados y mapee los perfiles de shell respectivos, como se muestra en la imagen.



Política de autenticación

Las políticas de autorización se pueden configurar de muchas maneras según el requisito. Las reglas que se muestran aquí en la imagen se basan en la ubicación del dispositivo, el tipo y el

grupo de identidad de usuario interno específico. Los perfiles de shell seleccionados se enviarán en el momento de la autorización junto con los conjuntos de comandos.



Política de autorización

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Operador

Verifique el grupo de usuarios y los grupos de tareas asignados **cuando** el usuario inicie sesión en el router.

```
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
```

Operador con AAA

Verificar el grupo de usuarios y los grupos de tareas asignados cuando**asraaa** el usuario inicia sesión en el router.

> **Nota**: muestra la tarea de operador enviada desde el servidor TACACS junto con los permisos de lectura, escritura y ejecución de la tarea AAA.

```
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

Verificar el grupo de usuarios y los grupos de tareas asignados cuando**asrwrite** el usuario inicia sesión en el 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 )
```

Sistema raíz

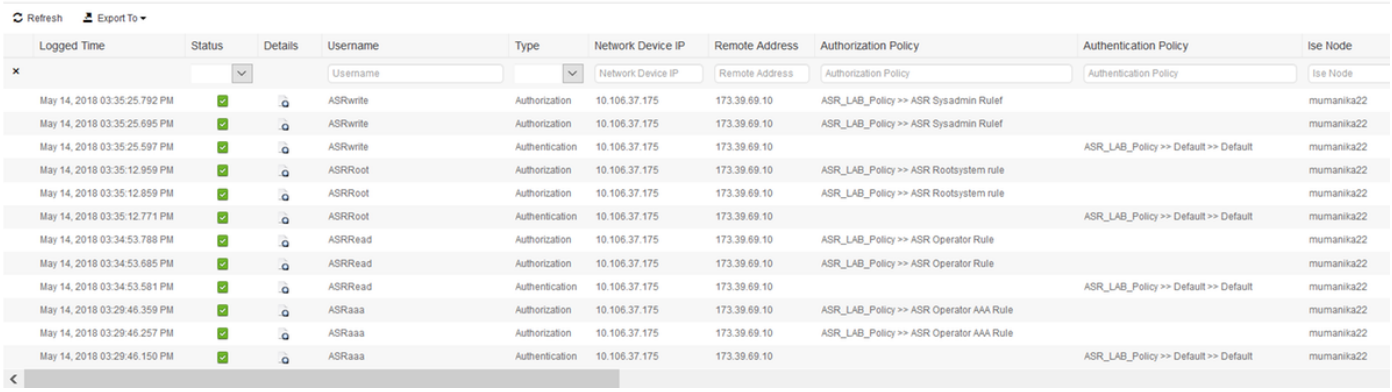
Verificar el grupo de usuarios y los grupos de tareas asignados cuando**asrroot** el usuario inicia sesión en el router.

```
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 )
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Verifique el informe ISE desde **Operations > TACACS > Live Logs**. Haga clic en el símbolo de la lupa para ver el informe detallado.



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

Estos son algunos comandos útiles para resolver problemas en ASR:

- show user
- show user group
- show user Tasks
- show user all