Configurar o ASR9K TACACS com o Cisco Identity Services Engine 2.4

Contents

Introduction

Este documento descreve a configuração do ASR 9000 Series Aggregation Services Router (ASR) para autenticar e autorizar via TACACS+ com o servidor Cisco Identity Services Engine 2.4.

Informações de Apoio

Ele exemplifica a implementação do modelo administrativo de autorização baseada em tarefas que é usado para controlar o acesso do usuário no sistema de software Cisco IOS® XR. As principais tarefas necessárias para implementar a autorização baseada em tarefas envolvem como configurar grupos de usuários e grupos de tarefas. Os grupos de usuários e grupos de tarefas são configurados por meio do conjunto de comandos do software Cisco IOS® XR usado para serviços de Autenticação, Autorização e Contabilidade (AAA). Os comandos de autenticação são usados para verificar a identidade de um usuário ou do principal. Os comandos de autorização são usados para verificar se um usuário autenticado (ou principal) recebe permissão para executar uma tarefa específica. Os comandos de contabilidade são usados para o registro de sessões e para criar uma trilha de auditoria por meio da gravação de determinadas ações geradas pelo sistema ou pelo usuário.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Implantação do ASR 9000 e configuração básica
- Protocolo TACACS+
- Implantação e configuração do ISE 2.4

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASR 9000 com Cisco IOS® XR Software, versão 5.3.4
- Cisco ISE 2.4

As informações neste documento são criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que o impacto potencial de qualquer alteração de configuração seja completamente compreendido.

Configurar

Componentes predefinidos no IOS® XR

Há grupos de usuários e grupos de tarefas predefinidos no IOS® XR. O administrador pode usar esses grupos predefinidos ou definir grupos personalizados de acordo com o requisito.

Grupos de usuários predefinidos

Esses grupos de usuários são predefinidos no IOS® XR:

Grupo de usuários	Privilégios
Cisco-Support	Depurar e solucionar problemas de recursos (geralmente usados pela equipe do Suporte Técnico da Cisco).
netadmin	Configurar protocolos de rede como o OSPF (Open Shortest Path First) (normalmente usa por administradores de rede).
operador	Realize atividades diárias de monitoramento e tenha direitos de configuração limitados.
root-lr	Exiba e execute todos os comandos em um único RP.
sistema raiz	Exiba e execute todos os comandos para todos os RPs no sistema.
sysadmin	Execute tarefas de administração do sistema para o roteador, como manter onde os dump do núcleo são armazenados ou configurar o relógio do Network Time Protocol (NTP).
serviceadmin	Execute tarefas de administração de serviços, como Session Border Controller (SBC).

Cada grupo de usuários predefinido tem determinados grupos de tarefas mapeados para eles e não podem ser modificados. Use estes comandos para verificar os grupos de usuários 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 tarefas predefinidos

Esses grupos de tarefas predefinidos estão disponíveis para que os administradores usem, normalmente para a configuração inicial:

- suporte da cisco: Tarefas do pessoal de suporte da Cisco
- netadmin: Tarefas do administrador de rede
- operador: Tarefas diárias do operador (para fins de demonstração)
- root-lr: Proteger tarefas do administrador do roteador do domínio
- sistema raiz: Tarefas do administrador em todo o sistema
- sysadmin: Tarefas do administrador do sistema
- serviceadmin: Tarefas de administração de serviços

Use estes comandos para verificar os grupos de tarefas 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>
```

Use este comando para verificar as tarefas suportadas:

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

Esta é a lista de tarefas suportadas:

AAA	Acl	Admin	Ancp	ATM	serviços básicos	Bcdl	Bfd	bgp
Inicialização	Pacote	call-home	Cdp	CEF	Cgn	Cisco-Support	config-mgmt	config-s
Crypto	DIAG	Não permitido	Drivers	Dwdm	Eem	EIGRP	serviços de Ethernet	ext-acce
Estrutura	mestre de falha	Sistema de	Firewall	FR	Hdlc	host-services	Hsrp	interfac

Inventário	ip-services	arquivos IPv4	IPv6	Isis	L2vpn	Li	Lisp	registro
Lpts	Monitor	mpls-ldp	mpls-static	mpls-te	Multicast	Netflow	Rede	nps
OSPF	Ouni	Pbr	pkg-mgmt	pos-dpt	PPP	Qos	Rcmd	costela
Rip	root-lr	sistema raiz	route-map	route-policy	Sbc	Snmp:	sonet-sdh	estático
Sysmgr	Sistema	Transporte	tty-access	Túnel	Universal	Vlan	VPDN	vrrp

Cada uma dessas tarefas mencionadas pode ser fornecida com qualquer uma dessas ou todas as quatro permissões:

Ler	Especifica uma designação que permite apenas uma operação de leitura.
Gravar	Especifica uma designação que permite uma operação de alteração e permite implicitamente u operação de leitura.
Executar	Especifica uma designação que permite uma operação de acesso; por exemplo, ping e Telnet.
Debug	Especifica uma designação que permite uma operação de depuração.

Grupos de tarefas definidos pelo usuário

Os administradores podem configurar grupos de tarefas personalizados para atender a necessidades específicas. Aqui está um exemplo de configuração:

```
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
```

Descrever comando pode ser usado para encontrar o grupo de tarefas e a permissão necessários para um determinado comando.

Exemplo 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 um usuário execute o **comando show aaa usergroup**, grupo de tarefas: **aaa de leitura de tarefas** deve ser atribuído ao grupo de usuários.

Exemplo 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 um usuário execute o **comando authentication login default group tacacs+**do modo de configuração, grupo de tarefas: **leitura de tarefas write aaa** deve ser atribuído ao grupo de usuários.

Os administradores podem definir o grupo de usuários que pode herdar vários grupos de tarefas. Aqui está o exemplo de configuração:

```
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
```

Configuração AAA no roteador

Configure o servidor TACACS no roteador ASR com o endereço IP e o segredo compartilhado a serem usados.

```
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 a autenticação e a autorização para usar o servidor TACACS configurado.

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

Configure a autorização do comando para usar o servidor TACACS configurado (opcional):

> **Note**: Assegure-se de que a autenticação e a autorização funcionem conforme esperado e assegure-se de que os conjuntos de comandos também estejam configurados corretamente antes de habilitar a autorização do comando. Se não estiver configurado corretamente, os usuários talvez não consigam inserir nenhum comando no dispositivo.

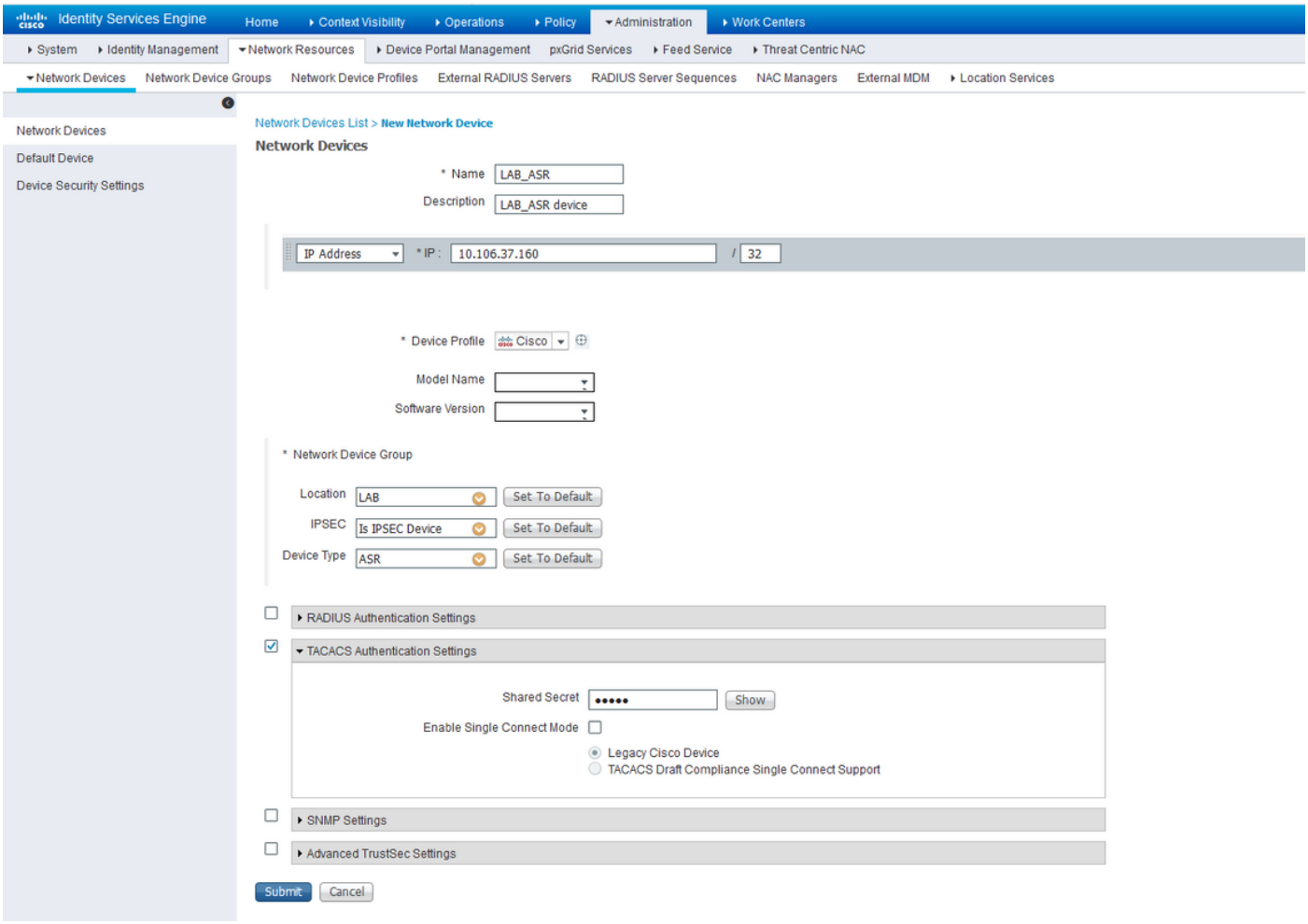
```
#aaa authorization commands default group tacacs+
```

Configure a contabilização de comandos para usar o servidor TACACS configurado (opcional).

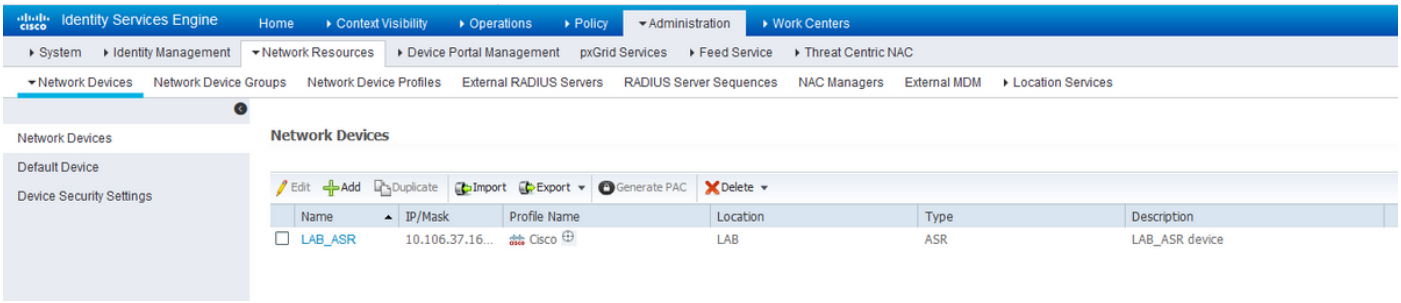
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

Configuração do servidor ISE

Etapa 1. Para definir o IP do roteador na lista de clientes AAA no servidor ISE, navegue até **Administration > NRecursos de rede > Dispositivos de rede** conforme mostrado na imagem. O segredo compartilhado deve ser o mesmo que o configurado no roteador ASR, como mostrado na imagem.



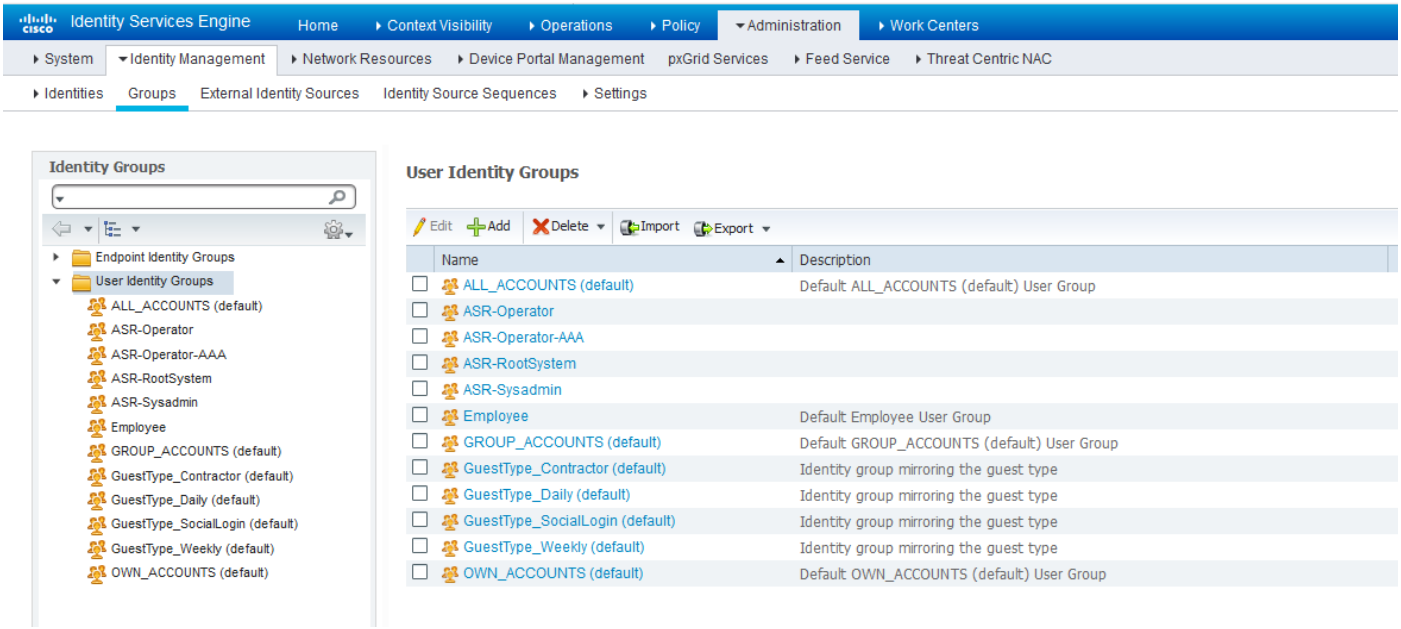
Configuração do dispositivo de rede



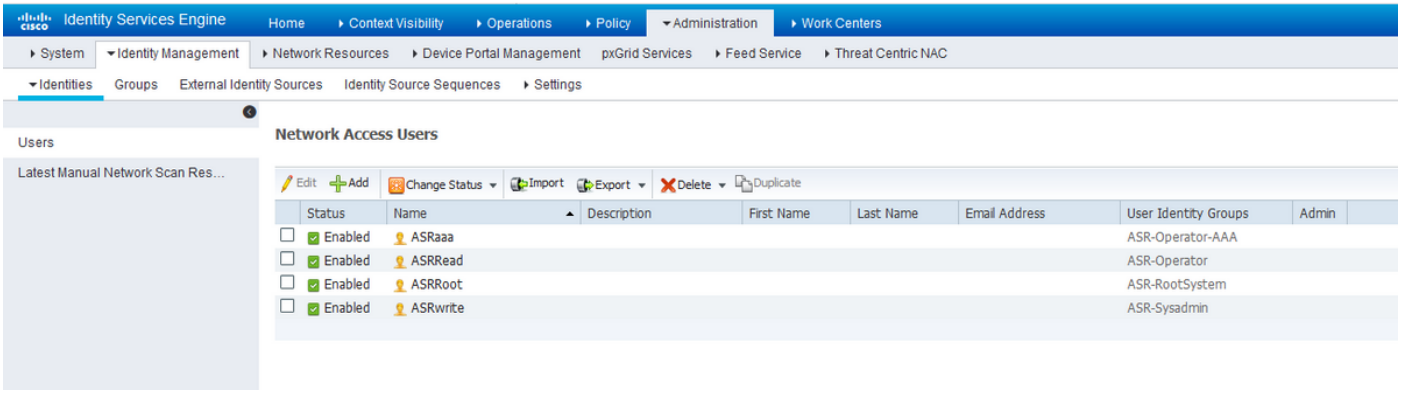
Configuração do dispositivo de rede

Etapa 2. Defina os grupos de usuários de acordo com seu requisito, no exemplo, como mostrado nesta imagem, você usa quatro grupos. Você pode definir os grupos em **Administration > Identity Management > Groups > User Identity Groups**. Os grupos criados neste exemplo são:

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



Grupos de identidadesEtapa 3. Como mostrado na imagem, crie os usuários e mapeie-os para o respectivo grupo de usuários criado antes.



Identidades/usuários

> **Note**: Neste exemplo, os usuários internos do ISE são usados para autenticação e autorização. As autenticações e autorizações com a fonte de identidade externa estão fora do escopo deste documento.

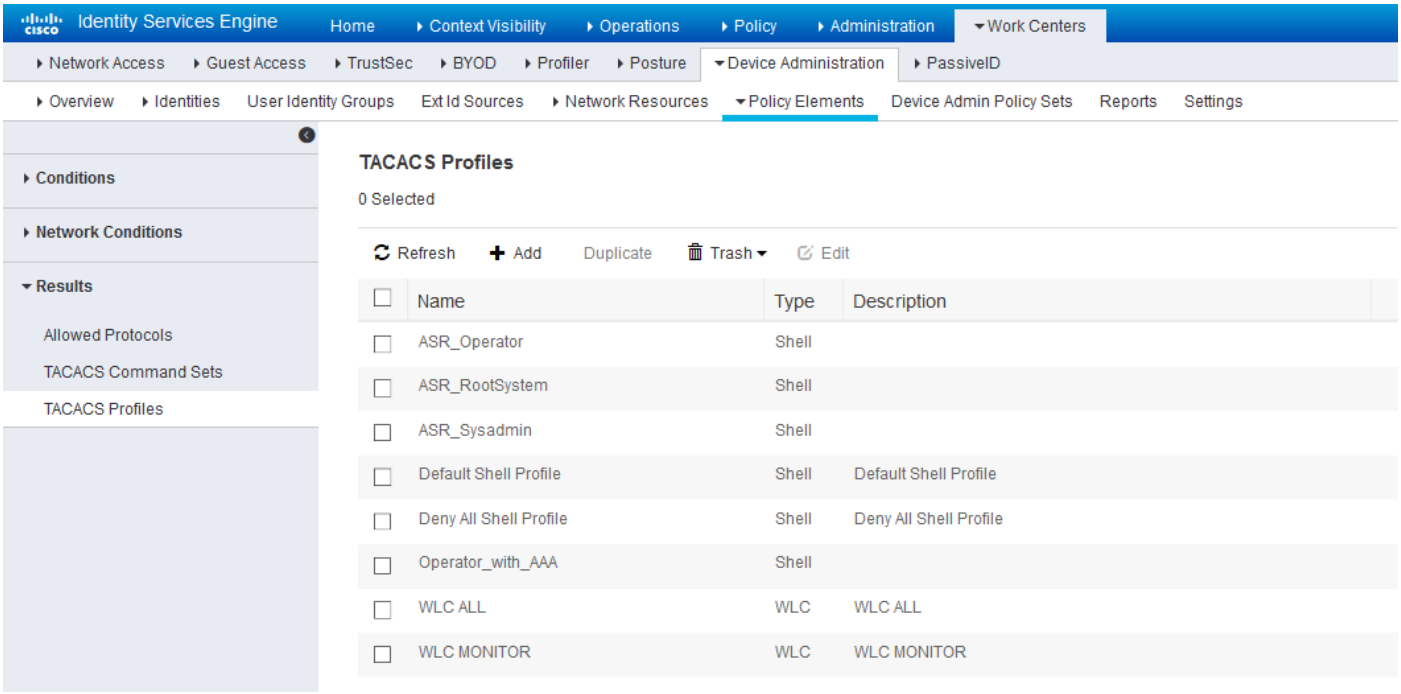
Etapa 4. Defina o Perfil do Shell a ser enviado para os respectivos usuários. Para fazer isso, navegue para **Centros de trabalho > Administração de dispositivos > Elementos de política > Resultados > Perfis TACACS**. É possível configurar um novo perfil de shell como mostrado nas imagens, bem como para versões anteriores do ISE. Os perfis de shell definidos neste exemplo são:

1. ASR_Operator

2. ASR_RootSystem

3. ASR_Sysadmin

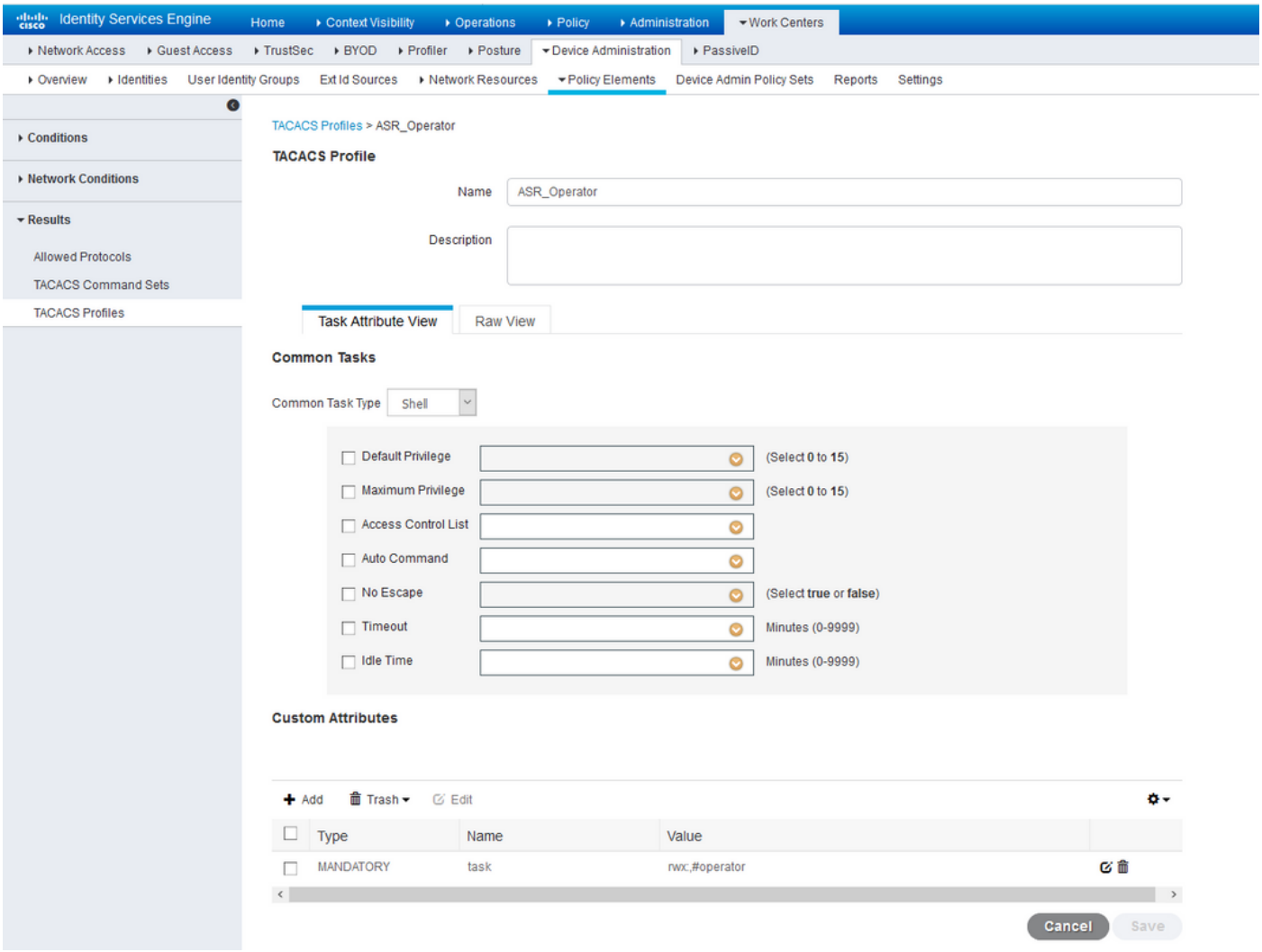
4. Operador_com_AAA



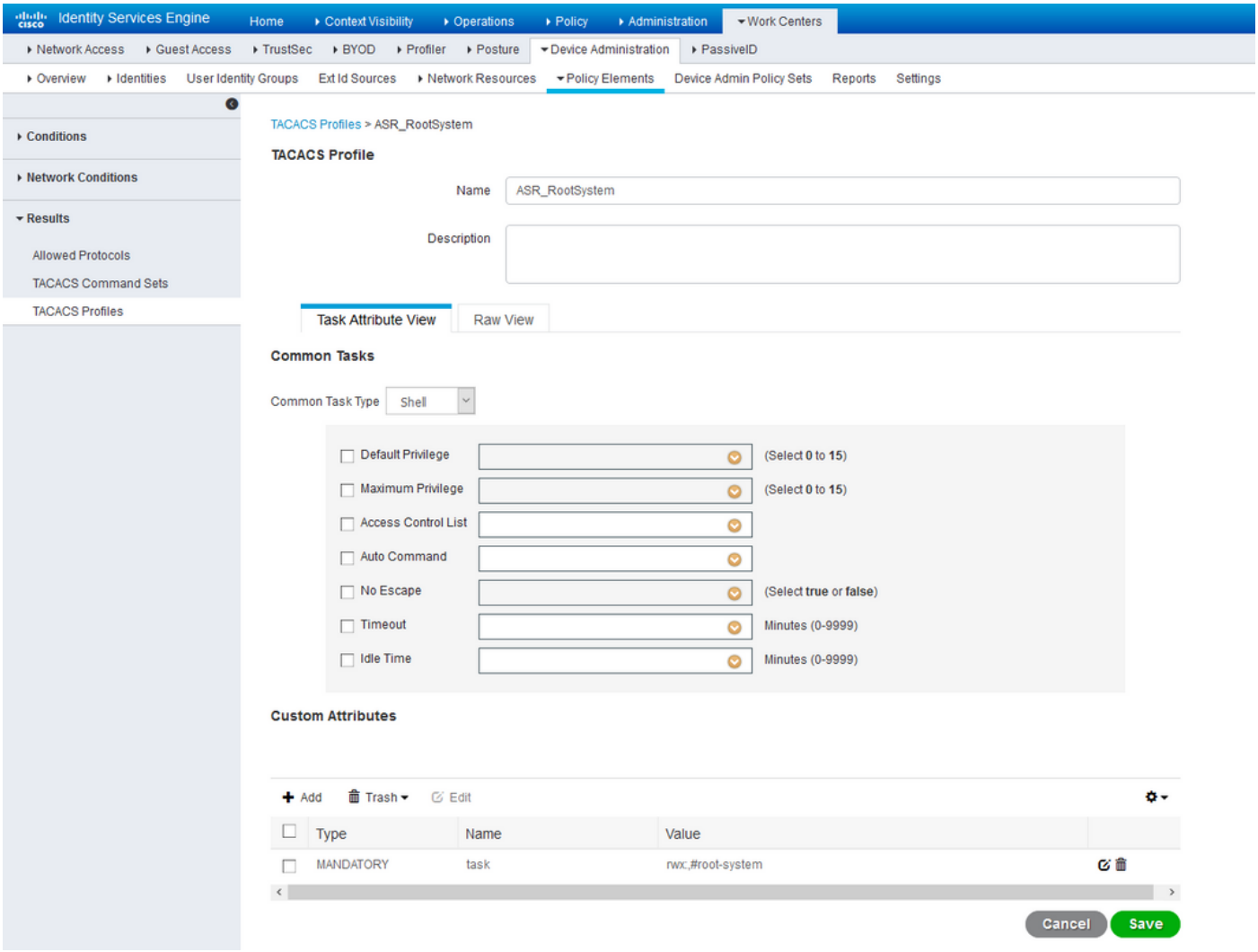
Perfis de shell para TACACS

Você pode clicar no botão **Adicionar** para inserir os campos Tipo, Nome e Valor, conforme mostrado nas imagens na seção **Atributos personalizados**.

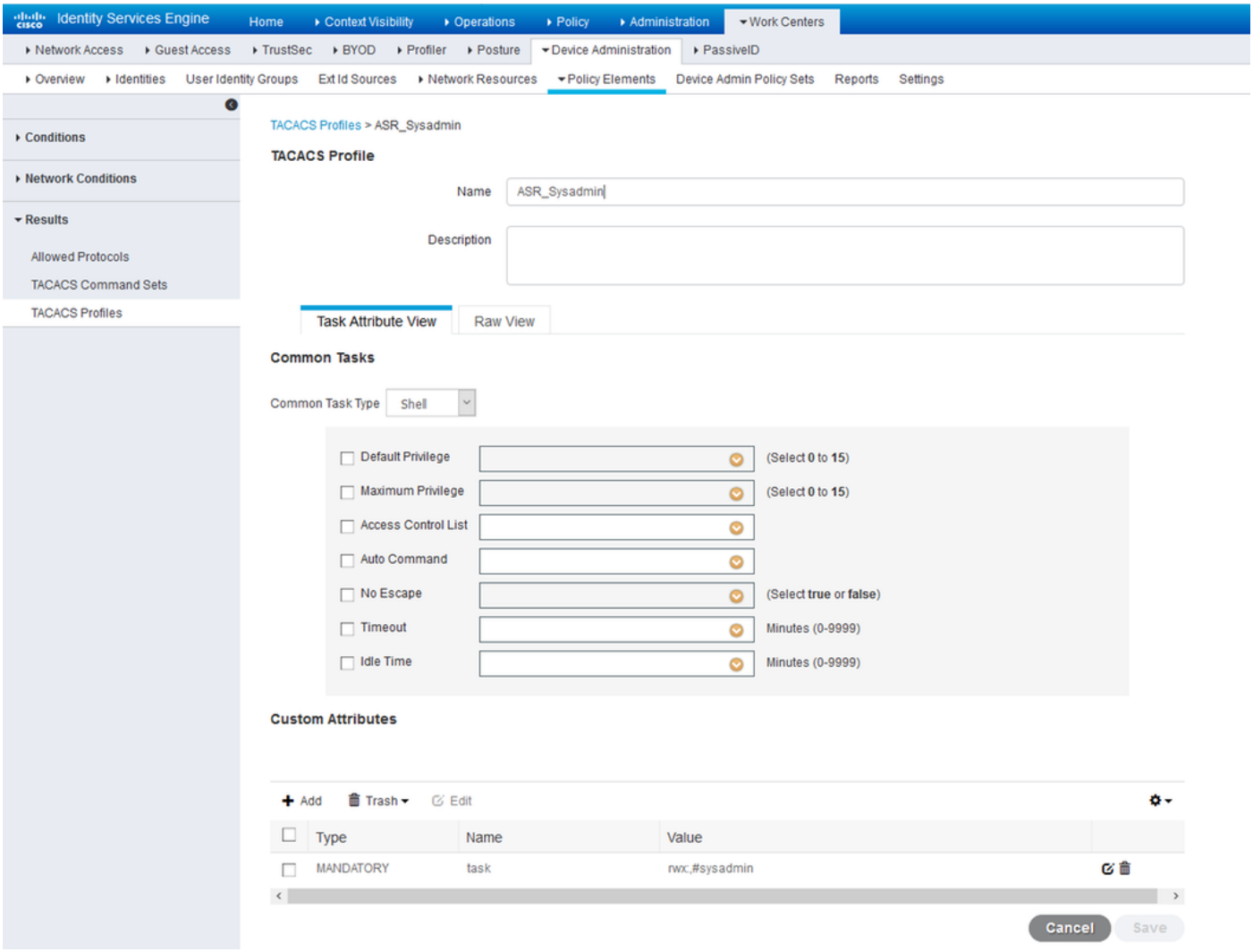
Para a função Operador:



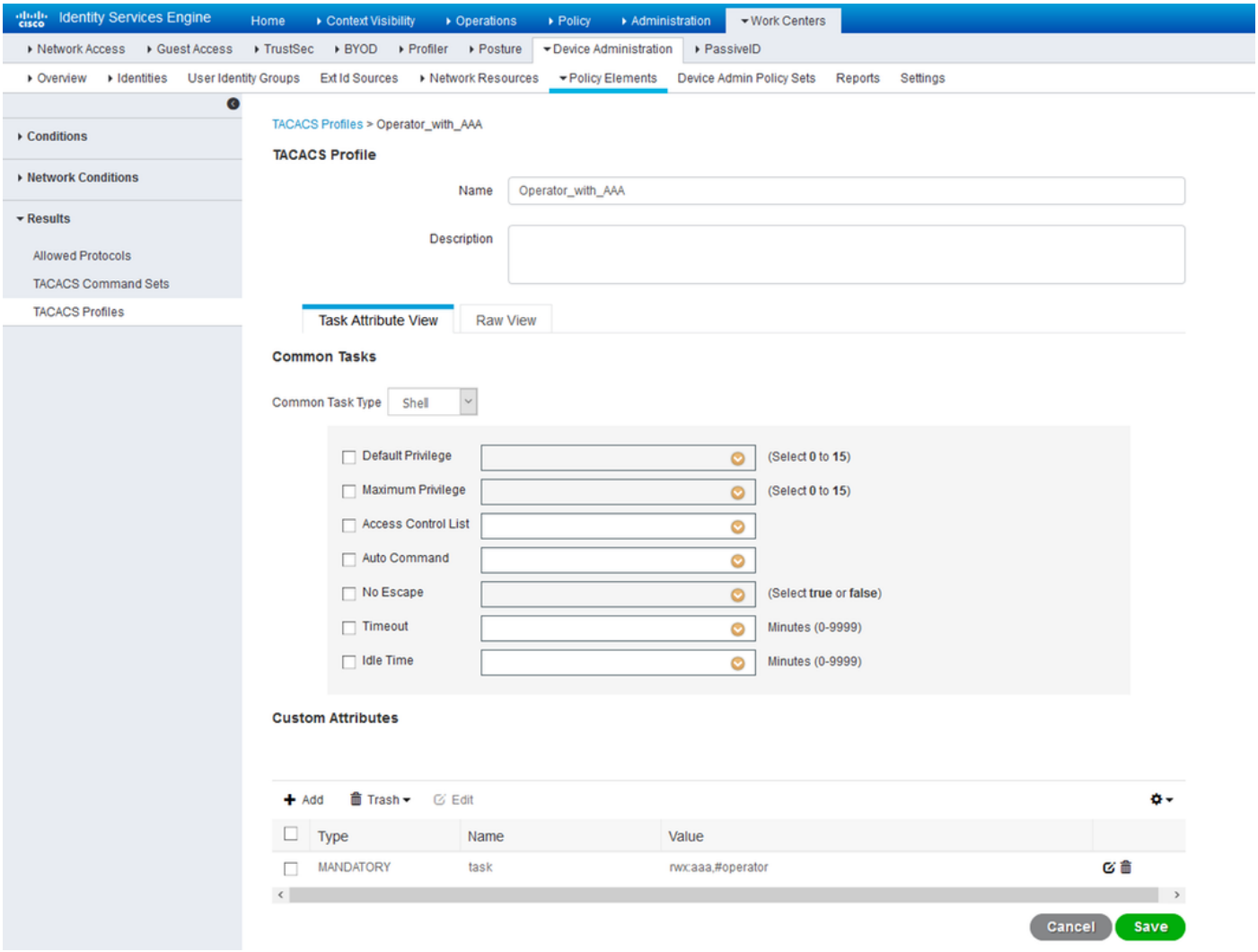
perfil de shell do operador ASRPara função de sistema raiz:



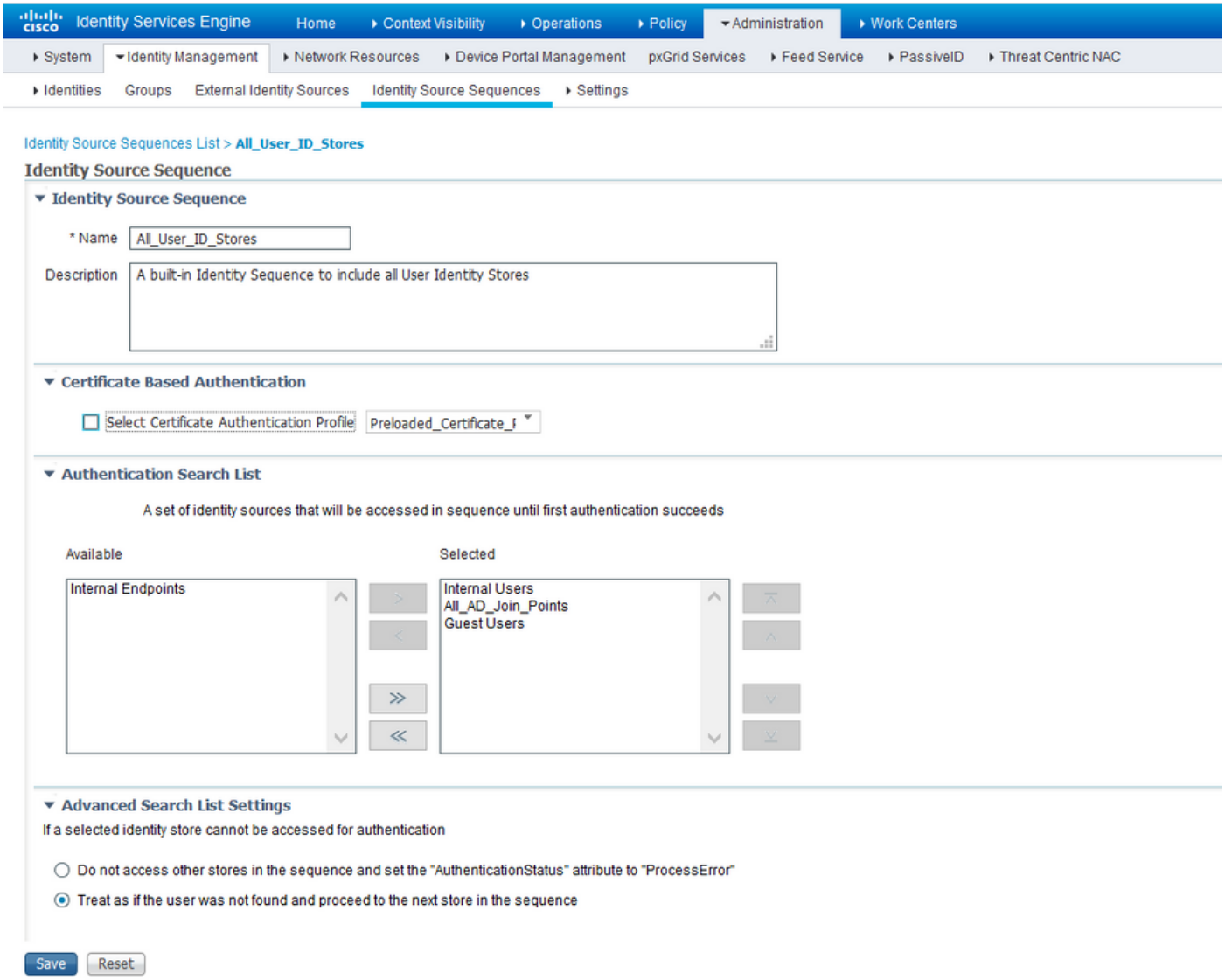
perfil de shell do ASR Root SystemPara a função sysadmin:



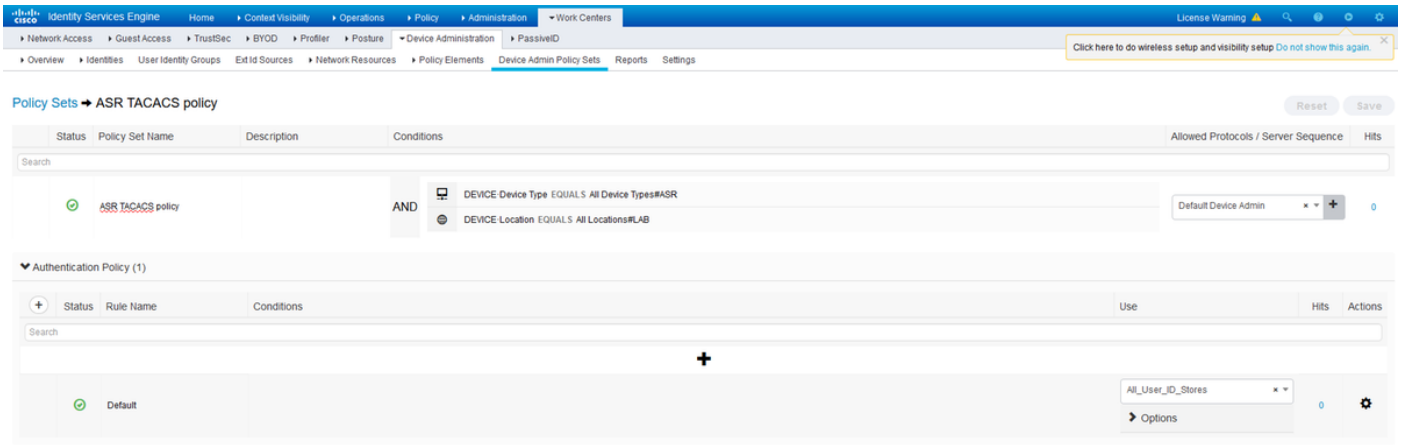
perfil de shell ASR SysadminPara a função de operador e AAA:



Operador com perfil de shell AAAEtapa 5. Configure a Sequência de Origem da Identidade para usar os Usuários Internos em **Administração > Gerenciamento de Identidade > Sequências de Origem da Identidade.** É possível adicionar uma nova Sequência de Origem de Identidade ou editar as disponíveis.



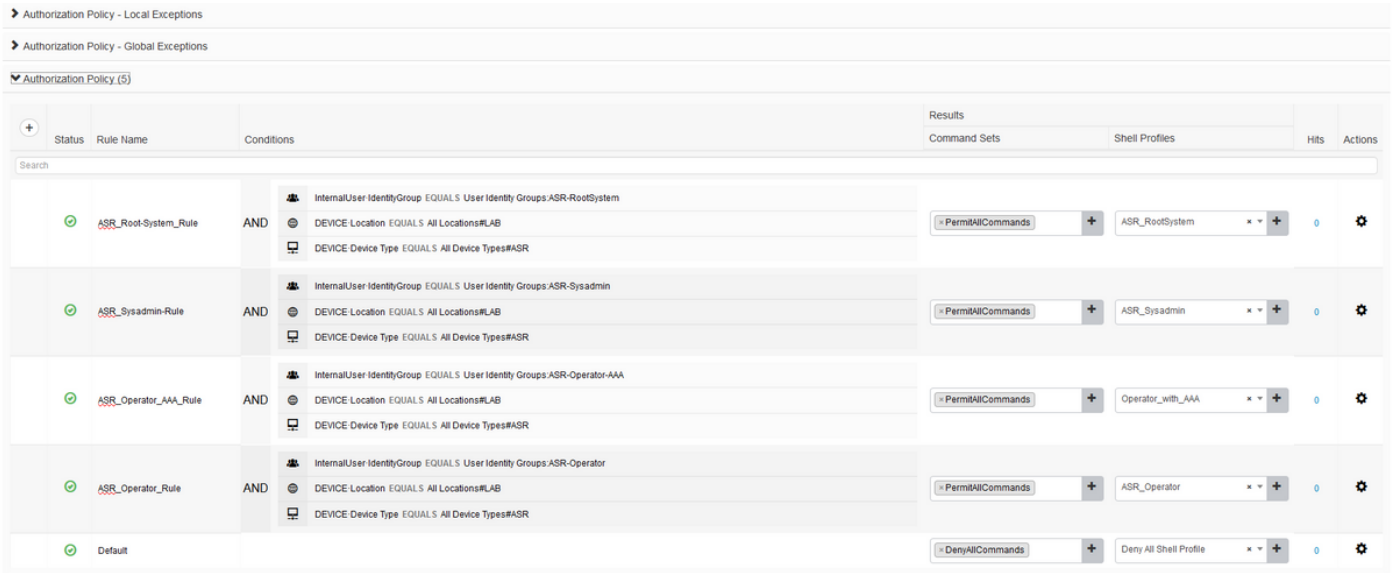
Etapa 6. Configure a política de autenticação em **Centros de Trabalho > Administração de Dispositivos > Conjuntos de Políticas de Administração de Dispositivos > [Escolher Conjunto de Políticas]** para usar a Sequência do Repositório de Identidades que contém os usuários internos. Configure a autorização com base no requisito com o uso dos grupos de identidade de usuário criados anteriormente e mapeie os respectivos Perfis de Shell, como mostrado na imagem.



Política de autenticação

As políticas de autorização podem ser configuradas de várias maneiras com base no requisito. As regras mostradas aqui na imagem se baseiam no local do dispositivo, no tipo e no grupo de identidade do usuário interno específico. Os perfis de shell selecionados serão enviados no

momento da autorização, juntamente com os conjuntos de comandos.



Política de autorização

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Operador

Verifique o grupo de usuários e os grupos de tarefas atribuídos **ao ler** o usuário no roteador.

```
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 com AAA

Verificar o grupo de usuários e os grupos de tarefas atribuídos quando**asara** o usuário faz login no roteador.

> **Nota**:o **pacote** corresponde à tarefa do operador enviada do servidor TACACS juntamente com as permissões de leitura, gravação e execução da tarefa 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 o grupo de usuários e os grupos de tarefas atribuídos quando**asrwrite** o usuário faz login no roteador.

```
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 raiz

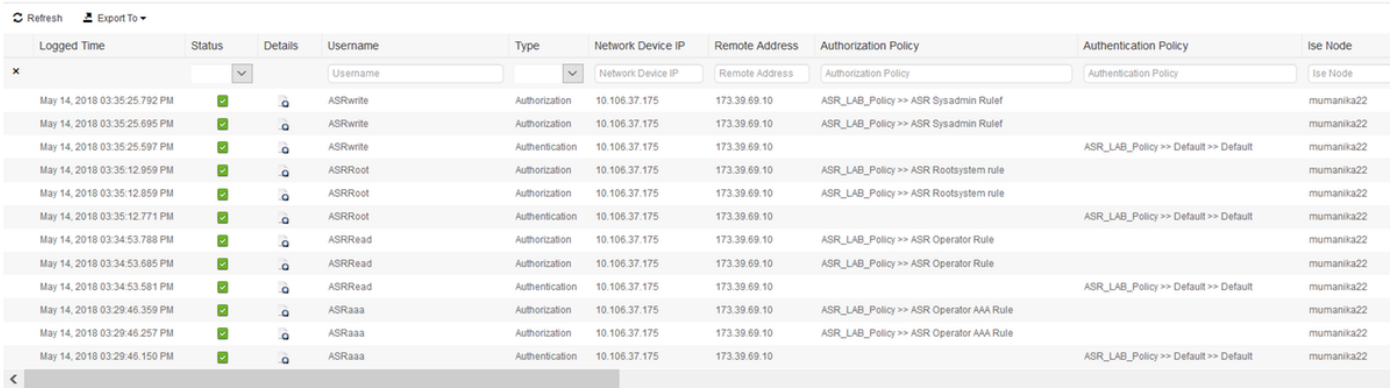
Verificar o grupo de usuários e os grupos de tarefas atribuídos quando**raiz** o usuário faz login no roteador.

```
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

Esta seção disponibiliza informações para a solução de problemas de configuração.

Verifique o relatório do ISE em **Operations > TACACS > Live Logs**. Clique no símbolo de lupa para ver o relatório detalhado.



Estes são alguns comandos úteis para solucionar problemas no ASR:

- show user
- show user group
- mostrar tarefas do usuário
- show user all