Configurer ASR9K TACACS avec Cisco Identity Services Engine 2.4

Contenu

Introduction

Ce document décrit la configuration du routeur ASR 9000 afin d'authentifier et d'autoriser via TACACS+ avec le serveur Cisco Identity Services Engine 2.4.

Informations générales

Il illustre la mise en oeuvre du modèle administratif d'autorisation basée sur des tâches qui est utilisé pour contrôler l'accès utilisateur dans le système logiciel Cisco IOS® XR. Les principales tâches requises pour mettre en oeuvre l'autorisation basée sur les tâches consistent à configurer les groupes d'utilisateurs et les groupes de tâches. Les groupes d'utilisateurs et les groupes de tâches sont configurés via le jeu de commandes du logiciel Cisco IOS® XR utilisé pour les services AAA (Authentication, Authorization and Accounting). Les commandes d'authentification permettent de vérifier l'identité d'un utilisateur ou d'un principal. Les commandes d'autorisation permettent de vérifier qu'un utilisateur (ou principal) authentifié bénéficie d'une autorisation pour effectuer une tâche spécifique. Les commandes de comptabilité servent à consigner les sessions et à créer une piste d'audit en enregistrant certaines actions générées par l'utilisateur ou le système.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Déploiement et configuration de base de l'ASR 9000
- Protocole TACACS+
- Déploiement et configuration d'ISE 2.4

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASR 9000 avec le logiciel Cisco IOS® XR, version 5.3.4
- Cisco ISE 2.4

Les informations de ce document sont créées à partir de périphériques dans un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. Si le réseau est actif, assurez-vous que l'impact potentiel de toute modification de configuration est bien compris.

Configuration

Composants prédéfinis sur IOS® XR

Il existe des groupes d'utilisateurs et de tâches prédéfinis dans IOS® XR. L'administrateur peut utiliser ces groupes prédéfinis ou définir des groupes personnalisés selon les besoins.

Groupes d'utilisateurs prédéfinis

Ces groupes d'utilisateurs sont prédéfinis sur IOS® XR :

Groupe d'utilisateurs	Privilèges
assistance Cisco	Déboguer et dépanner les fonctionnalités (généralement utilisées par le personnel de l'assistance technique Cisco).
netadmin	Configurez des protocoles réseau tels que le protocole OSPF (Open Shortest Path First) (généralement utilisé par les administrateurs réseau).
opérateur	Effectuez des activités de surveillance quotidiennes et disposez de droits de configuration limités.
root-lr	Affichez et exécutez toutes les commandes dans un seul RP.
root-system	Affichez et exécutez toutes les commandes pour tous les RP du système.
sysadmin	Effectuez des tâches d'administration système pour le routeur, telles que la maintenance de l'emplacement de stockage des vidages principaux ou la configuration de l'horloge NTP (Network Time Protocol).
serviceadmin	Exécuter des tâches d'administration de services, telles que Session Border Controller (SBC).

Chaque groupe d'utilisateurs prédéfini est associé à certains groupes de tâches et ne peut pas être modifié. Utilisez ces commandes afin de vérifier les groupes d'utilisateurs prédéfinis :

```
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>
```

Groupes de tâches prédéfinis

Ces groupes de tâches prédéfinis peuvent être utilisés par les administrateurs, généralement pour la configuration initiale :

- support cisco : Tâches du personnel d'assistance Cisco
- netadmin : Tâches d'administrateur réseau
- opérateur : Tâches quotidiennes de l'opérateur (à des fins de démonstration)
- root-lr : Tâches administrateur du routeur de domaine sécurisé
- root-system : Tâches d'administrateur système
- sysadmin : Tâches de l'administrateur système
- serviceadmin : Tâches d'administration des services

Utilisez ces commandes afin de vérifier les groupes de tâches prédéfinis :

```
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>
```

Utilisez cette commande afin de vérifier les tâches prises en charge :

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

Voici la liste des tâches prises en charge :

AAA	Acl	Admin	Ancp	Atm	services de base	Bcdl	Bfd
Démarrage	Offre groupée	call-home	Cdp	Cef	Câble	assistance Cisco	config-mgmt
Crypto	Diag	Non autorisé	Pilotes	Dwdm	Eem	eigrp	ethernet-services
Fabric	pannes-mgr	Système	Pare-feu	Fr	Hdlc	host-services	Hsrp

		de fichiers					
Inventaire	ip-services	IPv4	Ipv6	isis	L2vpn	Li	Lister
Lpts	Monitor	mpls-ldp	mpls-static	mpls-te	Multidiffusion	Netflow	Réseau
ospf	Ouni	Pbr	pkg-mgmt	pos-dpt	Ppp	Qos	Rcmd
rip	root-lr	root-system	route-map	route-policy	Sbc	SNMP	sonet-sdh
Sysmgr	système	Transport	tty-access	Tunnel	Universel	Vlan	Vpdn

Chacune de ces tâches peut être attribuée avec l'une de ces autorisations ou les quatre autorisations suivantes :

Lire	Spécifie une désignation qui autorise uniquement une opération de lecture.
Écrire	Spécifie une désignation qui autorise une opération de modification et autorise implicitement u opération de lecture.
Exécuter	Spécifie une désignation qui autorise une opération d'accès ; par exemple, ping et Telnet.
Déboguer	Spécifie une désignation qui autorise une opération de débogage.

Groupes de tâches définis par l'utilisateur

Les administrateurs peuvent configurer des groupes de tâches personnalisés pour répondre à des besoins particuliers. Voici un exemple de configuration :

```
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
```

Décrire une commande peut être utilisée pour trouver le groupe de tâches et l'autorisation nécessaires pour une commande donnée.

Exemple 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#
```

Afin de permettre à un utilisateur d'exécuter le **groupe d'utilisateurs** de la **commande show aaa**, le groupe de tâches : **tâche read aaa** doit être affecté au groupe d'utilisateurs.

Exemple 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)#
```

Afin de permettre à un utilisateur d'exécuter la **commande authentication login default group tacacs+**à partir du mode de configuration, task group : **task read write aaa** doit être affecté au groupe utilisateur.

Les administrateurs peuvent définir le groupe d'utilisateurs qui peut hériter de plusieurs groupes de tâches. Voici l'exemple de configuration :

```
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
```

Configuration AAA sur le routeur

Configurez le serveur TACACS sur le routeur ASR avec l'adresse IP et le secret partagé à utiliser.

```
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
!
```

Configurez l'authentification et l'autorisation afin d'utiliser le serveur TACACS configuré.

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

Configurez l'autorisation de commande pour utiliser le serveur TACACS configuré (facultatif) :

> **Note**: Assurez-vous que l'authentification et l'autorisation fonctionnent comme prévu et assurez-vous que les jeux de commandes sont également configurés correctement avant d'activer l'autorisation de commande. Si la configuration n'est pas correcte, les utilisateurs risquent de ne pas pouvoir entrer de commandes sur le périphérique.

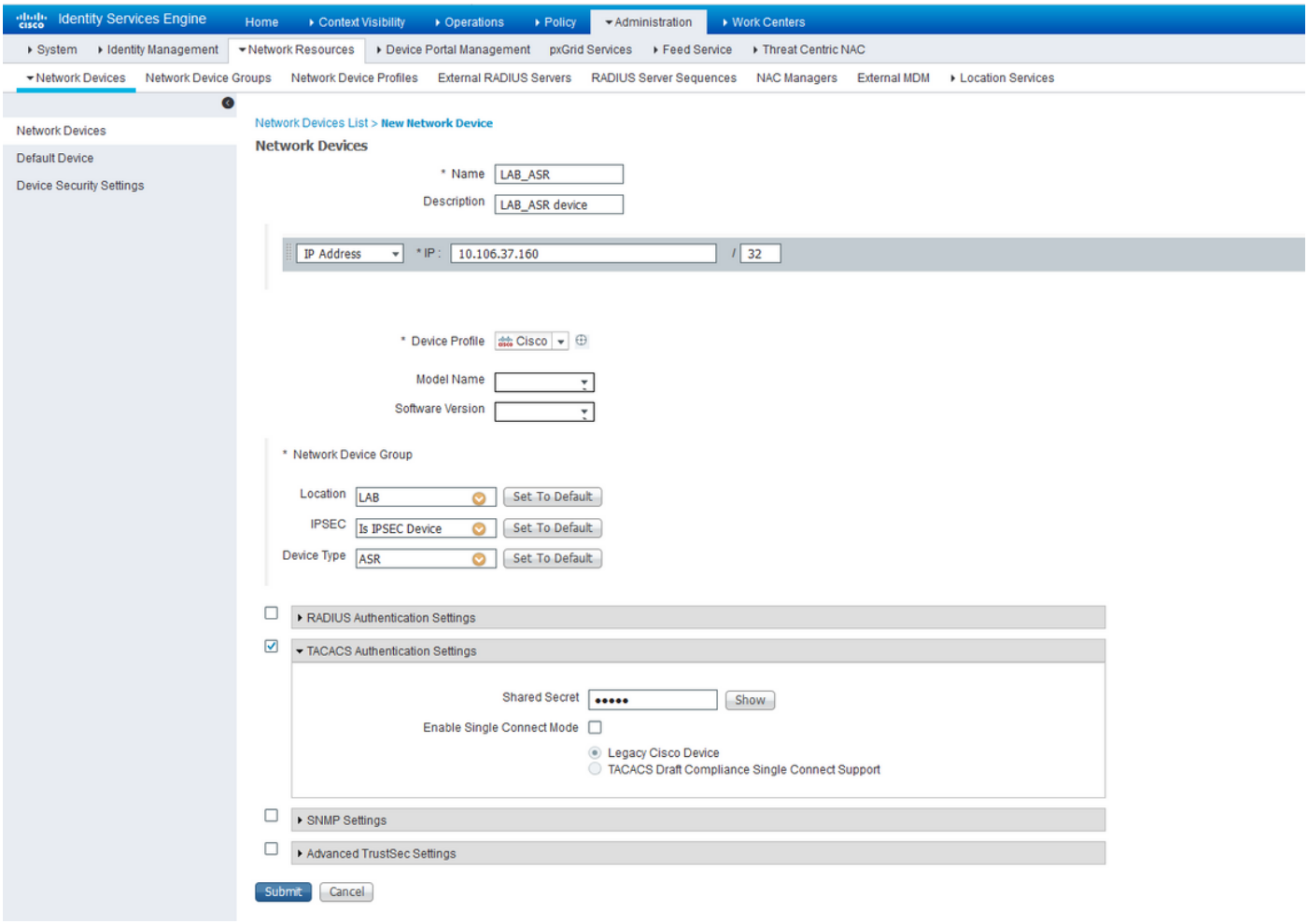
```
#aaa authorization commands default group tacacs+
```

Configurez la comptabilité de commande afin d'utiliser le serveur TACACS configuré (facultatif).

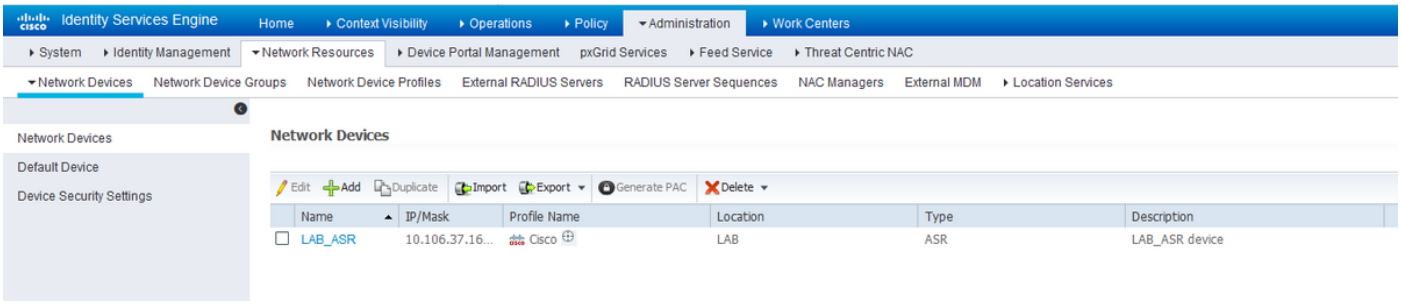
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

Configuration du serveur ISE

Étape 1. Afin de définir l'adresse IP du routeur dans la liste des clients AAA sur le serveur ISE, accédez à **Administration > NRessources réseau > Périphériques réseau** comme le montre l'image. Le secret partagé doit être identique à celui configuré sur le routeur ASR, comme illustré dans l’image.



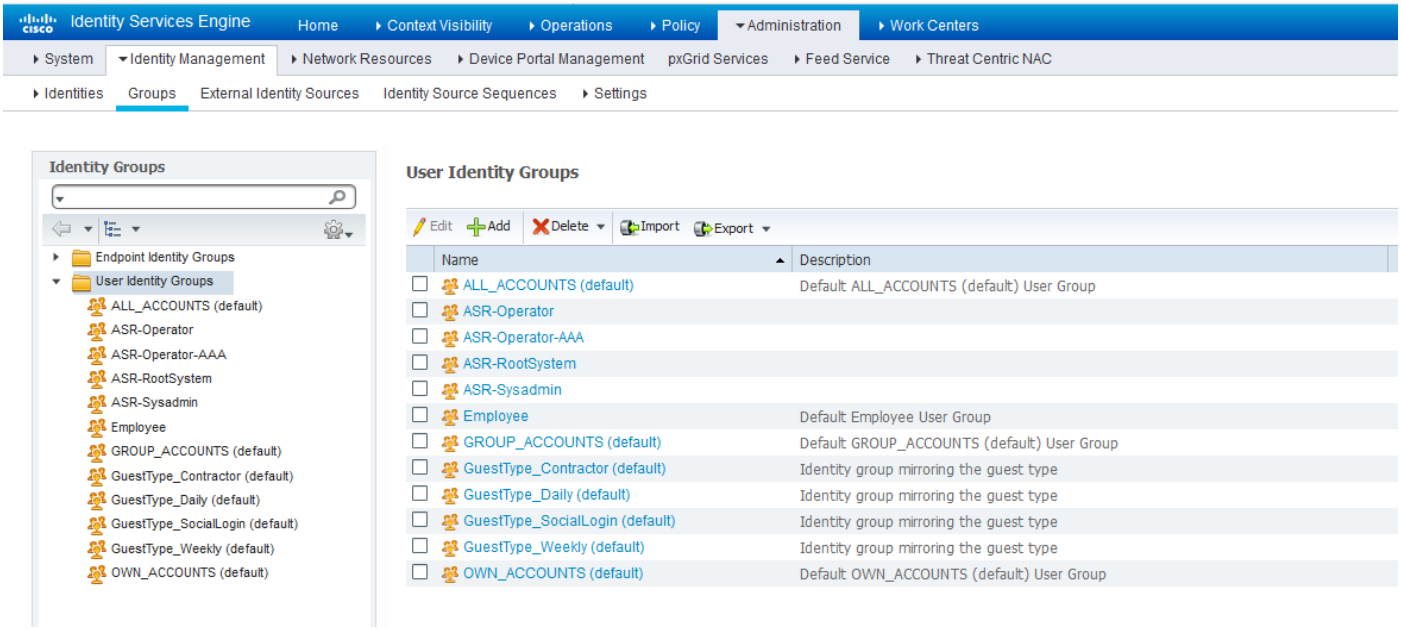
Configuration des périphériques réseau



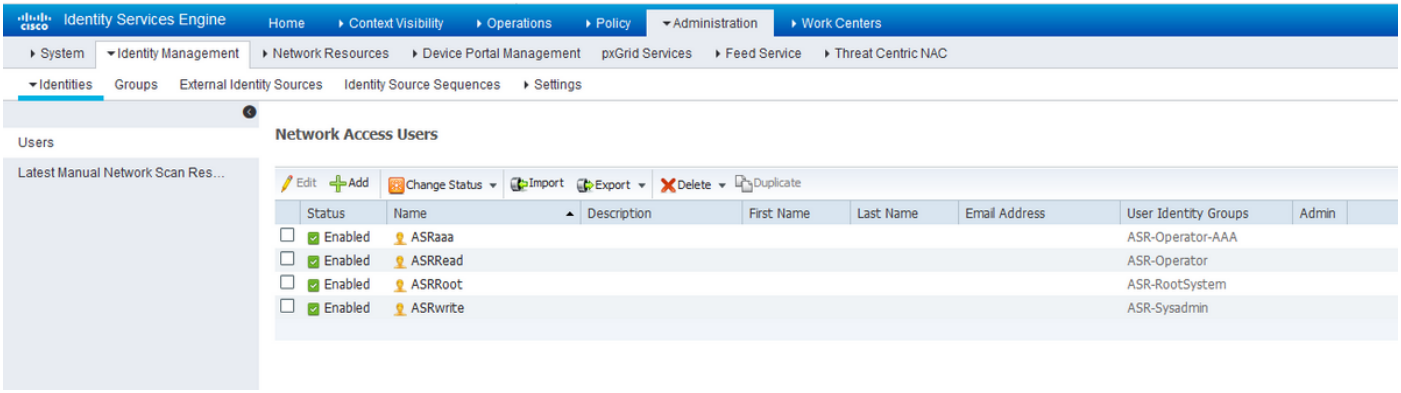
Configuration des périphériques réseau

Étape 2. Définissez les groupes d'utilisateurs en fonction de vos besoins, dans l'exemple, comme illustré dans cette image, vous utilisez quatre groupes. Vous pouvez définir les groupes sous **Administration > Identity Management > Groups > User Identity Groups**. Les groupes créés dans cet exemple sont les suivants :

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



Groupes d'identitésÉtape 3. Comme l'illustre l'image, créez les utilisateurs et associez-les au groupe d'utilisateurs correspondant créé précédemment.



Identités/Utilisateurs

> **Note**: Dans cet exemple, les utilisateurs internes ISE sont utilisés pour l'authentification et l'autorisation. Les authentifications et autorisations avec une source d'identité externe ne sont pas comprises dans ce document.

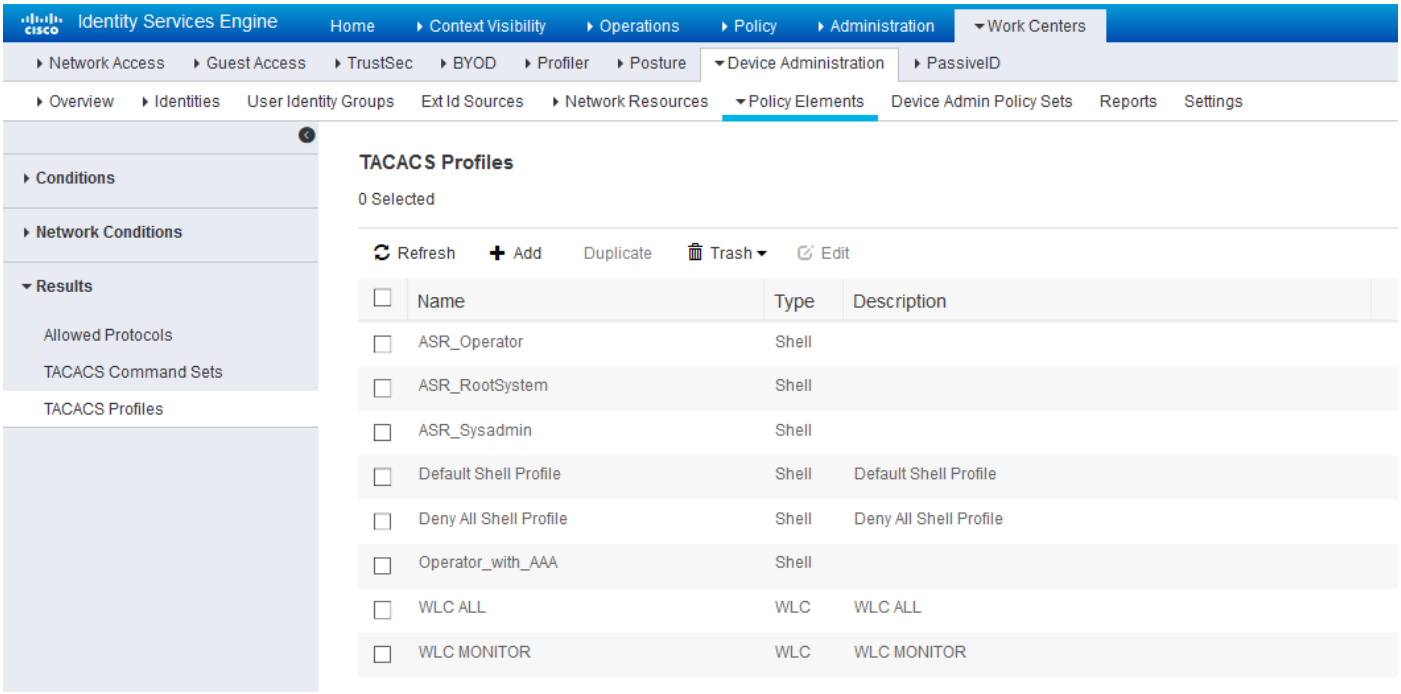
Étape 4. Définissez le profil Shell à pousser pour les utilisateurs respectifs. Pour ce faire, accédez à **Centres de travail > Administration des périphériques > Éléments de stratégie > Résultats > Profils TACACS**. On peut configurer un nouveau profil de shell comme indiqué dans les images aussi pour les versions précédentes d'ISE. Les profils de shell définis dans cet exemple sont les suivants :

1. Opérateur_ASR

2. ASR_RootSystem

3. ASR_Sysadmin

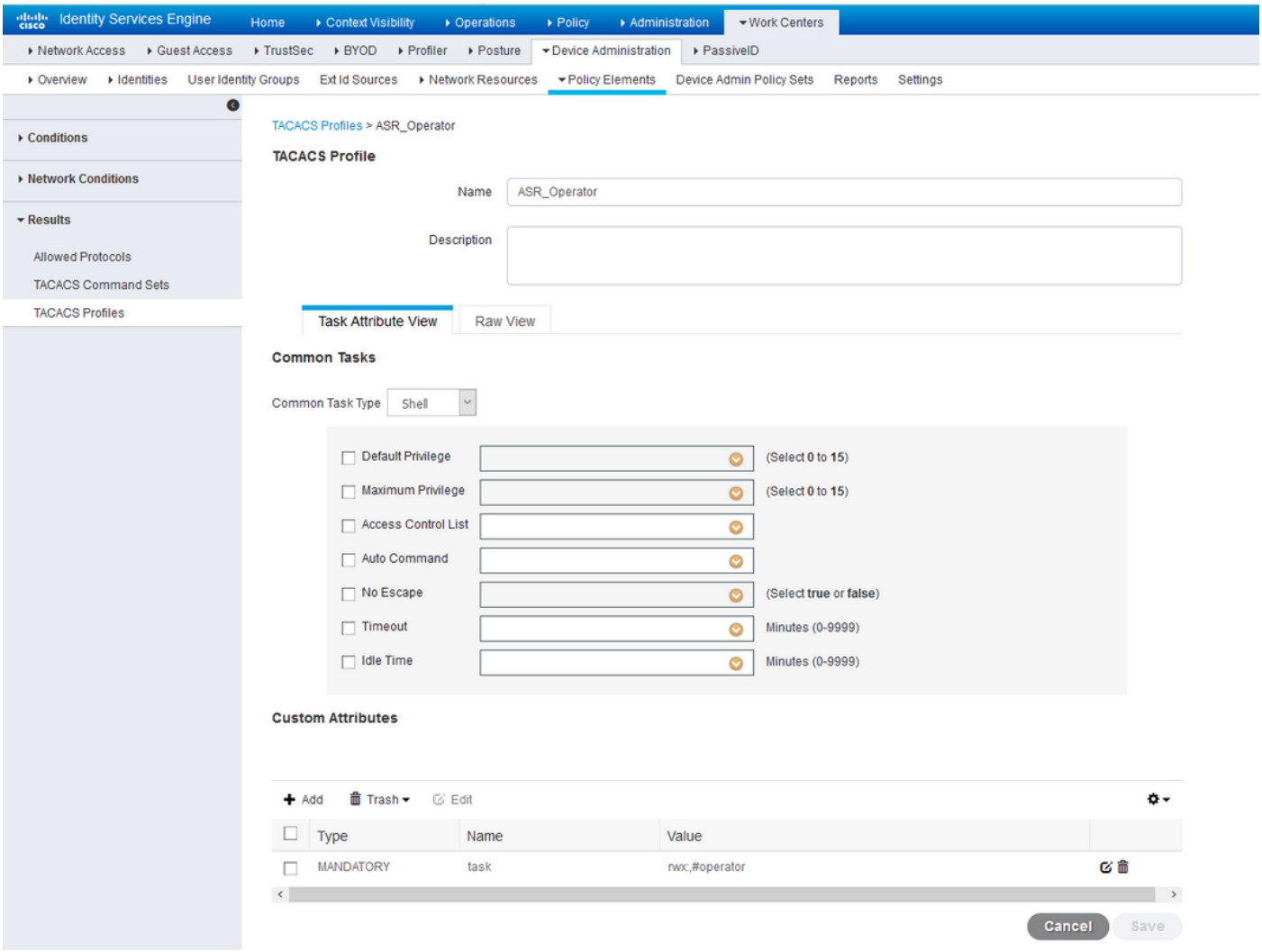
4. Opérateur_avec_AAA



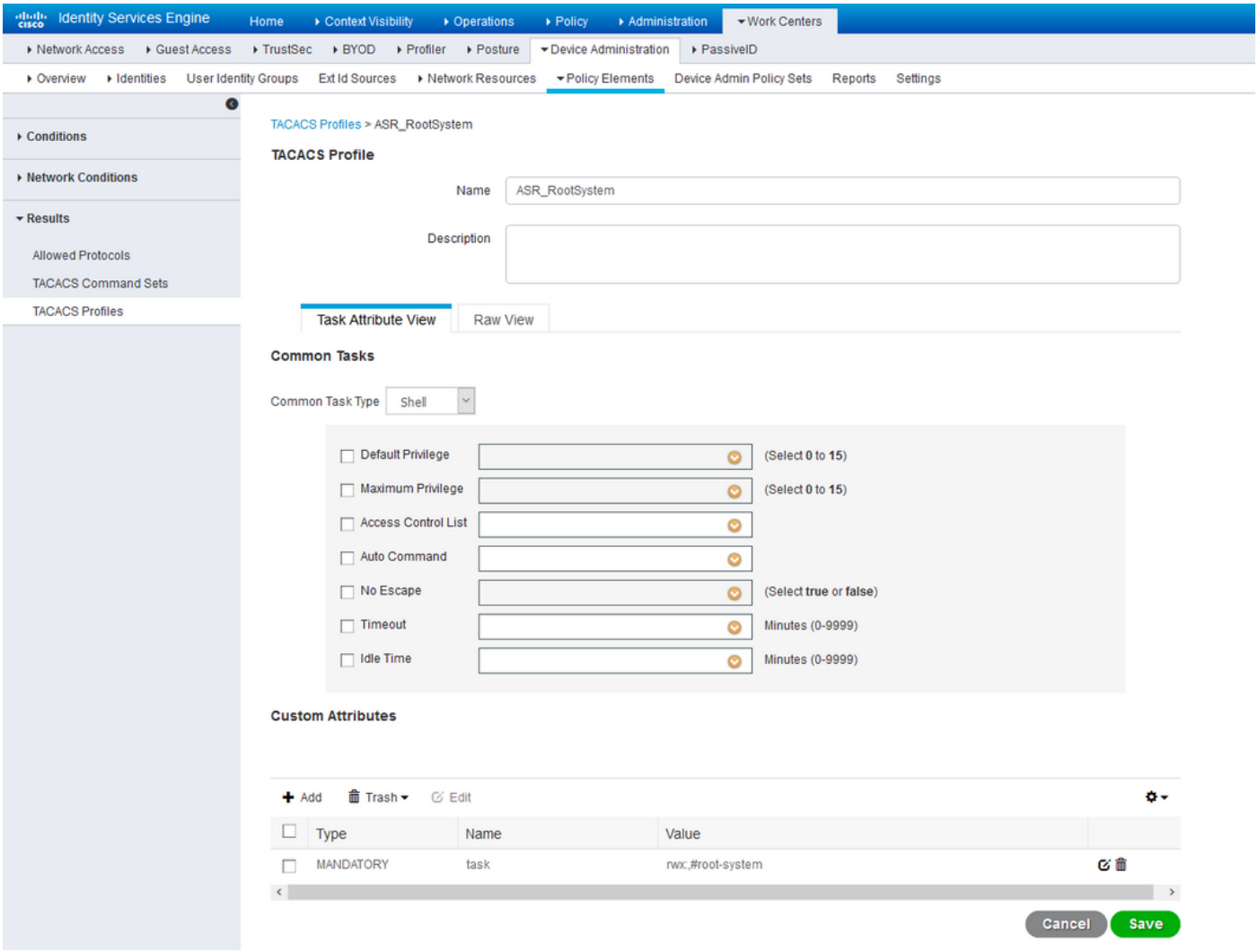
Profils Shell pour TACACS

Vous pouvez cliquer sur le bouton **Ajouter** pour entrer les champs Type, Name et Value comme indiqué dans les images de la section **Attributs personnalisés**.

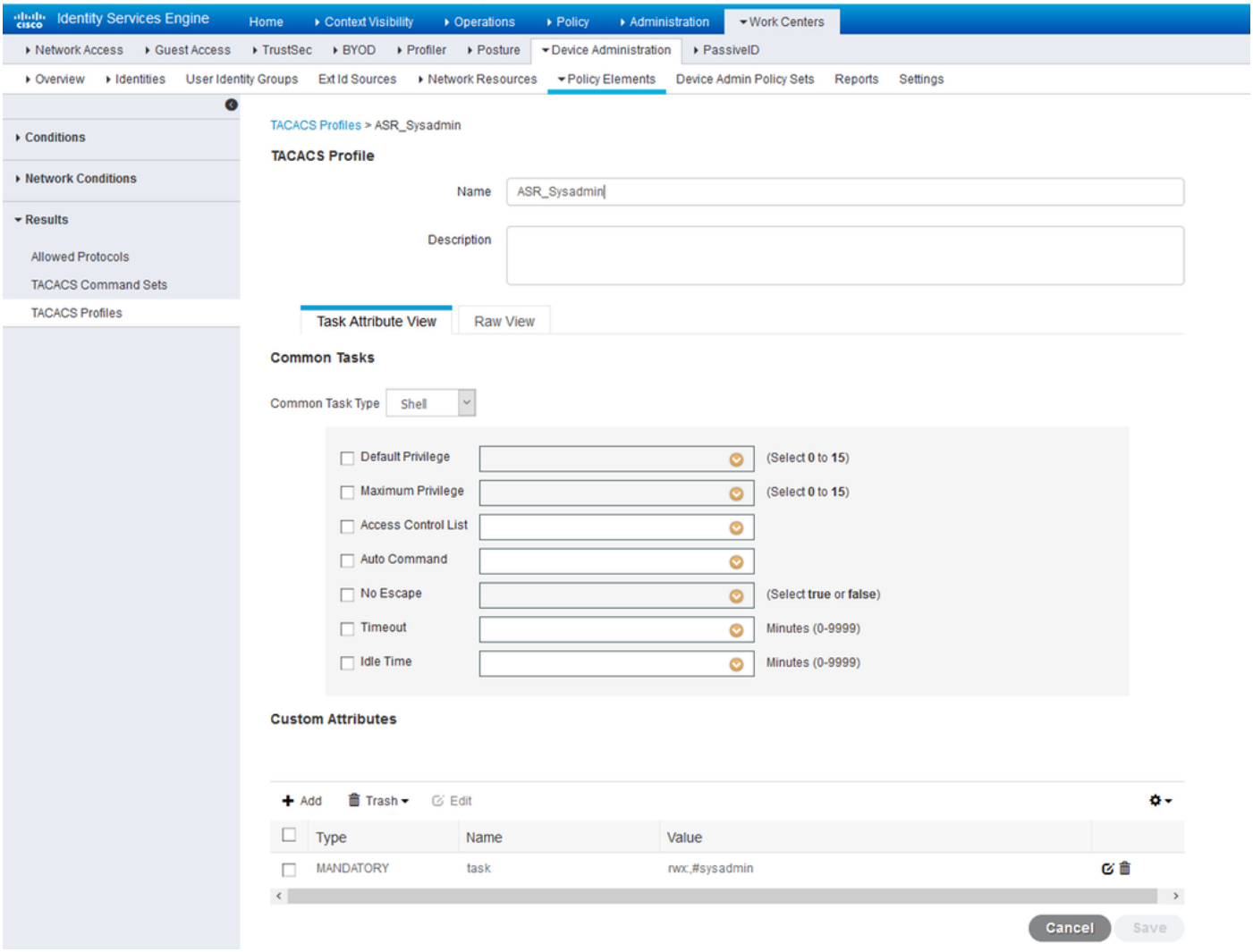
Pour le rôle Opérateur :



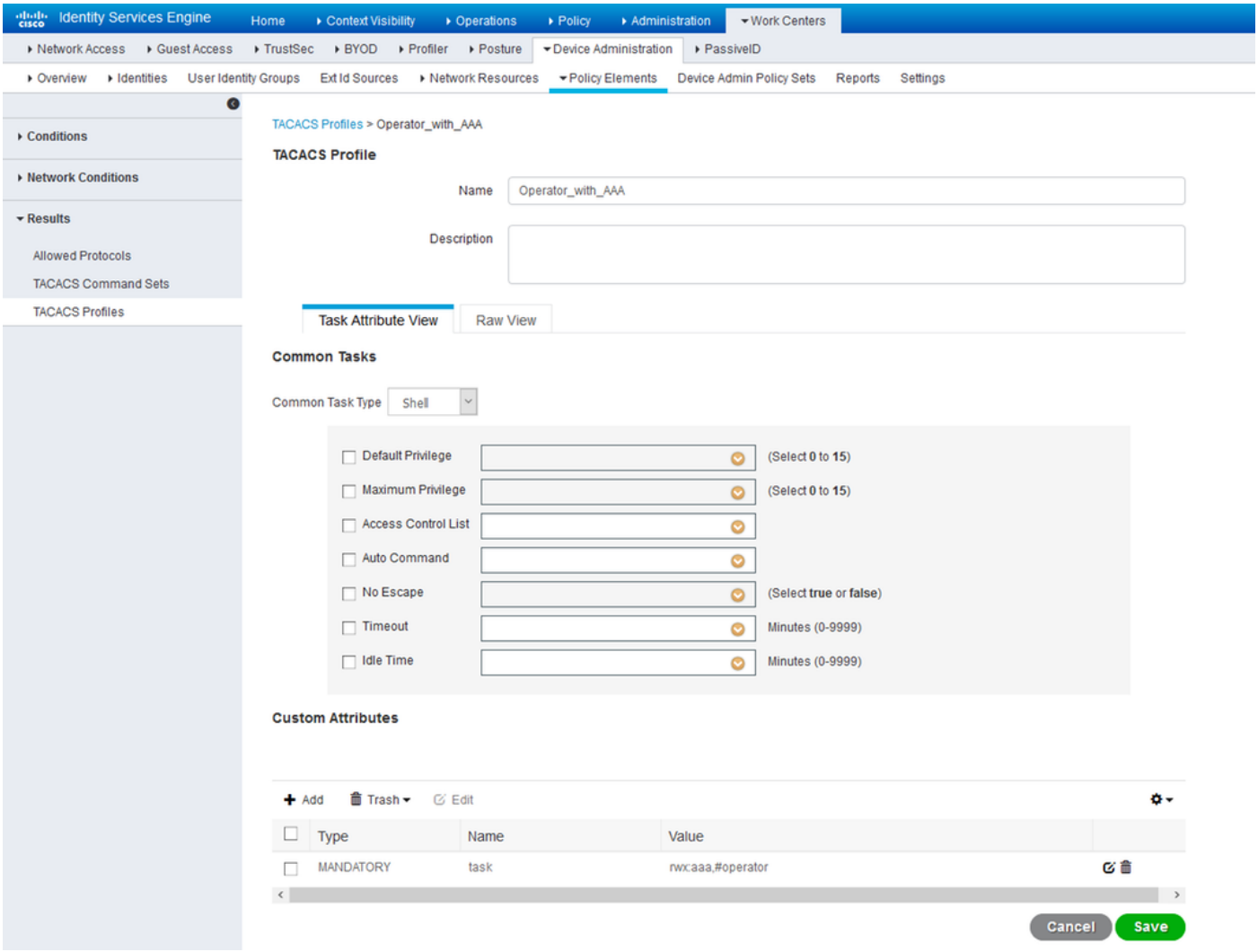
Profil de shell de l'opérateur ASRPour le rôle du système racine :



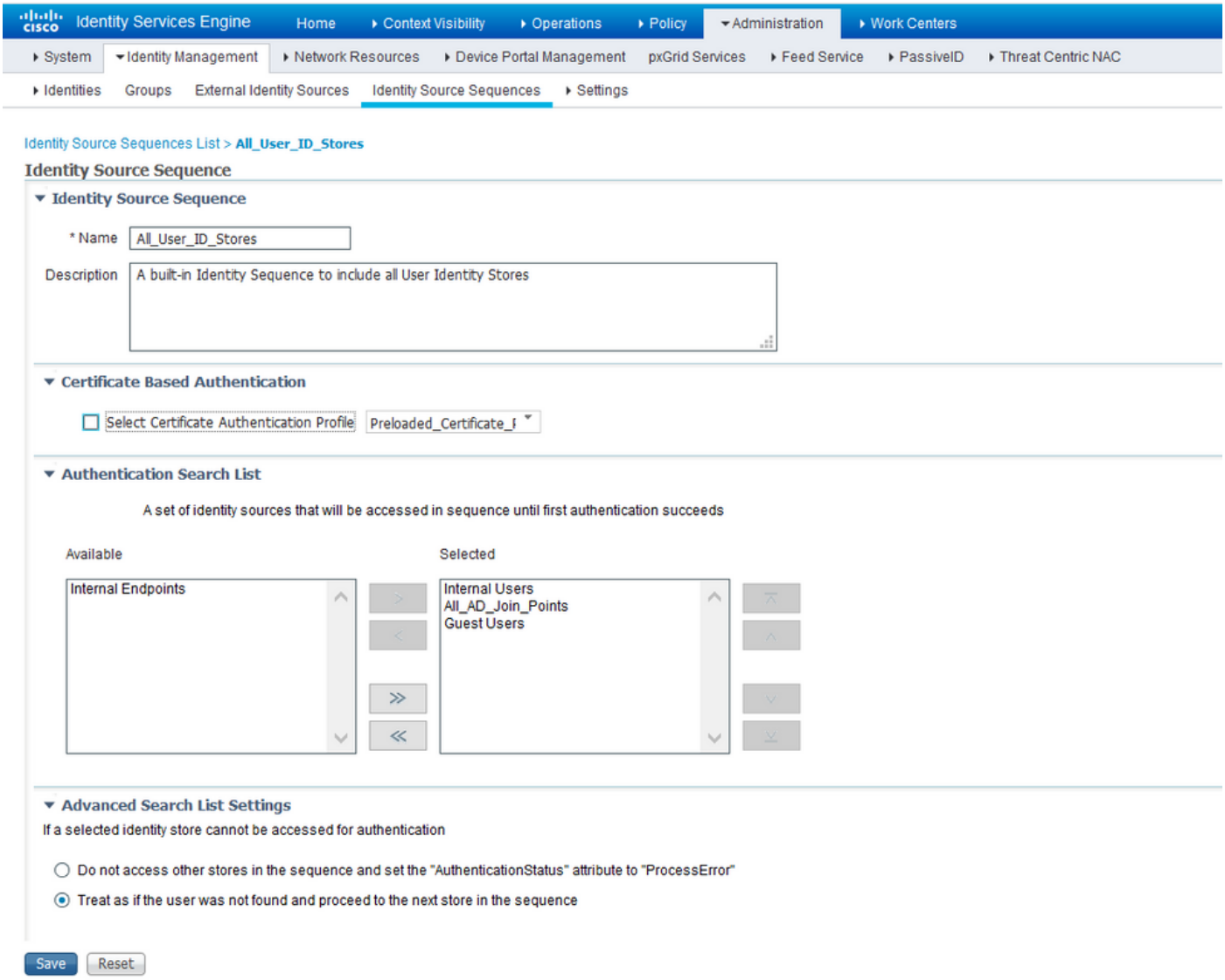
Profil du shell du système racine ASRPour le rôle sysadmin :



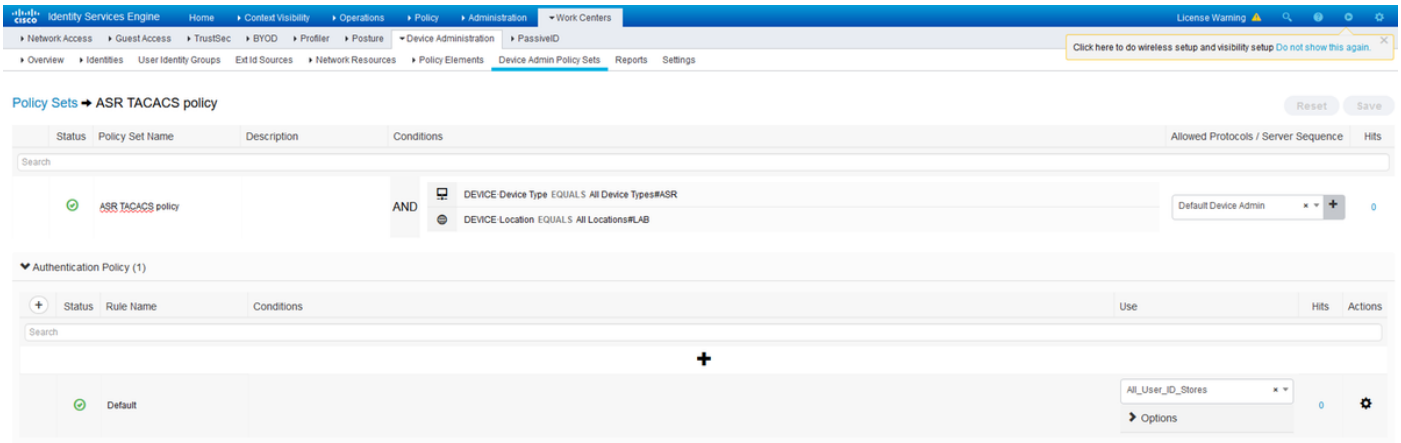
Profil ASR Sysadmin ShellPour le rôle opérateur et AAA :



Opérateur avec profil de shell AAAÉtape 5. Configurez la séquence de source d'identité pour utiliser les utilisateurs internes à **Administration > Identity Management > Identity Source Sequences.** Vous pouvez ajouter une nouvelle séquence de source d'identité ou modifier les séquences disponibles.



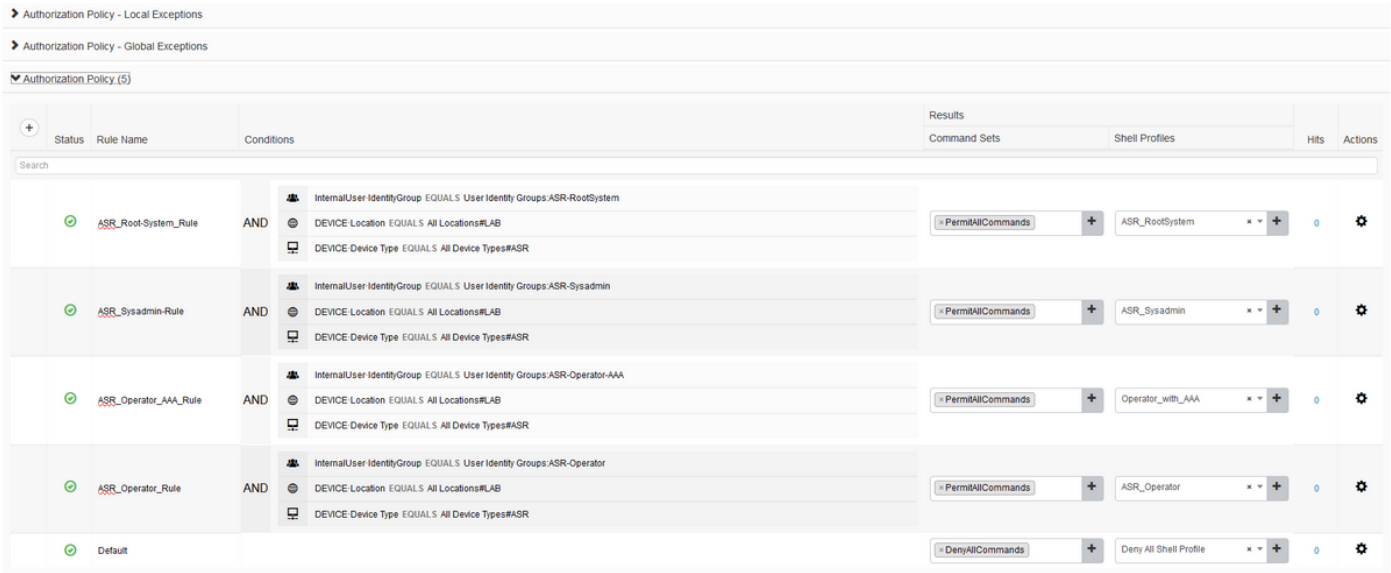
Étape 6. Configurez la stratégie d'authentification dans **Work Centers > Device Administration > Device Admin Policy Sets > [Choose Policy Set]** afin d'utiliser la séquence de magasin d'identités qui contient les utilisateurs internes. Configurez l'autorisation en fonction de la condition requise à l'aide des groupes d'identité utilisateur précédemment créés et mappez les profils Shell respectifs, comme illustré dans l'image.



Stratégie d'authentification

Les stratégies d'autorisation peuvent être configurées de plusieurs façons en fonction des besoins. Les règles affichées ici dans l'image sont basées sur l'emplacement, le type et le groupe d'identité utilisateur interne spécifique du périphérique. Les profils de coque sélectionnés seront

repoussés au moment de l'autorisation avec les jeux de commandes.



Stratégie d'autorisation

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Opérateur

Vérifiez le groupe d'utilisateurs et les groupes de tâches attribués **lorsque l'**utilisateur se connecte au routeur.

```
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
```

Opérateur avec AAA

Vérifier le groupe d'utilisateurs et les groupes de tâches affectés lorsque**asraa** l'utilisateur se connecte au routeur.

> **Remarque** : asraaais la tâche opérateur poussée du serveur TACACS avec les autorisations AAA lecture, écriture et exécution de la tâche.

```
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

Vérifier le groupe d'utilisateurs et les groupes de tâches affectés lorsque**réécrire** l'utilisateur se connecte au routeur.

```
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 )
```

Système racine

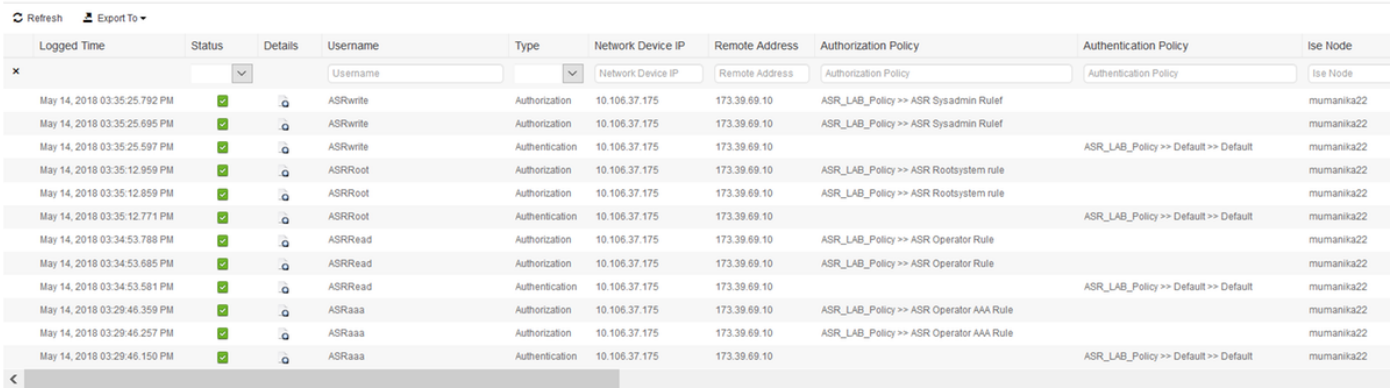
Vérifier le groupe d'utilisateurs et les groupes de tâches affectés lorsque**asrroot** l'utilisateur se connecte au routeur.

```
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 )
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Vérifiez le rapport ISE à partir de **Operations > TACACS > Live Logs**. Cliquez sur le symbole de la loupe afin de voir le rapport détaillé.



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

Voici quelques commandes utiles afin de dépanner sur ASR :

- show user
- show user group
- afficher les tâches utilisateur
- show user all