Configurez ASR9k TACACS avec le serveur du Cisco Secure ACS 5.x

Contenu

Introduction

Ce document décrit la configuration du routeur de services d'agrégation de gamme 9000 ASR (ASR) pour authentifier et autoriser par l'intermédiaire de TACACS+ avec le serveur 5.x du Cisco Secure Access Control Server (ACS).

Ce exemples l'implémentation du modèle administratif de l'autorisation basée sur tâche utilisé pour contrôler l'accès client dans le système de Logiciel Cisco IOS XR. Les tâches principales exigées pour implémenter l'autorisation basée sur tâche implique comment configurer des groupes d'utilisateurs et des groupes de travail. Des groupes d'utilisateurs et les groupes de travail sont configurés par le positionnement de commande de Logiciel Cisco IOS XR utilisé pour des services d'authentification, d'autorisation et de comptabilité (AAA). Des authentications command sont utilisées de vérifier l'identité d'un utilisateur ou d'un directeur. Des commandes d'autorisation sont utilisées de vérifier qu'on accorde un utilisateur authentifié (ou le directeur) l'autorisation d'effectuer une tâche spécifique. Des commandes de traçabilité sont utilisées pour se connecter des sessions et pour créer une vérification rétrospective en enregistrant certaines actions d'utilisateur ou générées par le système.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Déploiement et configuration de base ASR 9000
- Déploiement et configuration ACS 5.x.
- Protocole TACACS+

Composants utilisés

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 4.3.4
- Cisco Secure ACS 5.7

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle modification de configuration.

Configuration

Composants de prédéfinis sur IOS XR

Il y a des groupes d'utilisateurs de prédéfinis et des groupes de travail dans IOS XR. L'administrateur peut utiliser ces groupes de prédéfinis ou définir les groupes faits sur commande selon la condition requise.

Groupes d'utilisateurs de prédéfinis

Ces groupes d'utilisateurs sont prédéfinis sur IOS XR :

Groupe d'utilisateurs	Privilèges
Cisco-support	Débuggez et dépannez les caractéristiques (habituellement, utilisé par le personnel de support technique de Cisco).
netadmin	Protocoles de configure network tels que le Protocole OSPF (Open Shortest Path First) (habituellement utilisé par des administrateurs réseau).
opérateur	Exercez les activités de jour en jour de surveillance, et avez limité des droites de configuration.
la racine-LR	Affichez et exécutez toutes les commandes dans un RP simple.
racine-système	Affichez et exécutez toutes les commandes pour toute la RPS dans le système.
sysadmin	Effectuez les tâches d'administration système pour le routeur, tel que mettre à jour où les vidages de mémoire sont enregistrés ou installants l'horloge de Protocole NTP (Network Time Protocol).
serviceadmin	Effectuez les tâches de gestion de service, telles que la Session Border Controller (SBC).

Le groupe d'utilisateurs de racine-système a l'autorisation de prédéfinis ; c'est-à-dire, il a la responsabilité complète des ressources utilisateur-gérées parsystème et de certaines

responsabilités dans d'autres services.

Utilisez ces derniers commandent de vérifier les groupes d'utilisateurs de prédéfinis :

```
RP/0/RSP1/CPU0:ASR9k#show aaa usergroup ?
  |              Output Modifiers
  root-lr        Name of the usergroup
  netadmin       Name of the usergroup
  operator       Name of the usergroup
  sysadmin       Name of the usergroup
  root-system    Name of the usergroup
  serviceadmin   Name of the usergroup
  cisco-support  Name of the usergroup
  WORD           Name of the usergroup
  <cr>
```

Groupes de travail de prédéfinis

Ceux-ci ont prédéfini des groupes de travail sont disponibles pour que les administrateurs les utilisent, typiquement pour la configuration initiale :

- Cisco-support : Tâches de personnel d'assistance technique de Cisco
- netadmin : Tâches d'administrateur réseau
- opérateur : Tâches de jour en jour d'opérateur (pour la démonstration)
- la racine-LR : Tâches sécurisées d'administrateur de routeur de domaine
- racine-système : Au niveau système tâches d'administrateur
- sysadmin : Tâches d'administrateur système
- serviceadmin : Entretenez les tâches de gestion, par exemple, SBC

Utilisez ces derniers commandent de vérifier les groupes de travail de 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 de vérifier les tâches prises en charge :

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

Voici la liste de tâches prises en charge :

AAA	Acl	Admin	Ancp	Atmosphère	services de base	Bcdl
Démarrage	Paquet	Fonction Call Home	Cdp	Cef	Cgn	Cisco-sup

Crypto	Diag	Rejeté	Gestionnaires	Dwdm	Eem	Eigrp
Matrice	défaut-directeur	Système de fichiers	Pare-feu	Franc	HDLC	hôte-servi
Stocks	Services IP	Ipv4	IPv6	ISIS	L2vpn	Li
Lpts	Moniteur	MPLS-LDP	MPLS-statique	MPLS-te	Multidiffusion	NetFlow
OSPF	Ouni	Pbr	module-gestion	POS-DPT	Ppp	Qos
Déchirure	la racine-LR	racine-système	route-map	artère-stratégie	Sbc	SNMP
Sysmgr	Système	Transport	téléscripteur-Access	Tunnel	Universel	VLAN

Chacune des tâches mentionnées ci-dessus peut être donnée avec l'un de ces ou toutes les quatre autorisations.

Lu	Spécifie une désignation qui permet seulement une opération "lecture".
Écrivez	Spécifie une désignation qui permet une exécution de modification et permet implicitement une opération "lecture".
Exécutez	Spécifie une désignation qui permet une exécution d'accès ; par exemple, ping et telnet.
Debug	Spécifie une désignation qui permet une exécution de débogage.

Composants définis par l'utilisateur sur IOS XR

Groupes d'utilisateurs définis par l'utilisateur

L'administrateur peut configurer ses propres groupes d'utilisateurs pour répondre aux besoins particuliers. Voici l'exemple de configuration :

```
RP/0/RSP1/CPU0:ASR9k(config)#usergroup TAC-Defined
RP/0/RSP1/CPU0:ASR9k(config-ug)#taskgroup operator
RP/0/RSP1/CPU0:ASR9k(config-ug)#commit
```

Groupes de travail définis par l'utilisateur

L'administrateur peut configurer leurs propres groupes de travail pour répondre aux besoins particuliers. Voici l'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
```

Si vous n'êtes pas sûr comment trouver quels groupe et autorisation de travail est nécessaire pour certaine commande, vous pouvez utiliser **décrivez la** commande de la trouver. Voici un exemple :

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 pour exécuter l'**usergroup de show aaa de** commande, vous devez permettre cette ligne dans le groupe de travail :

la tâche a lu l'AAA

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 pour exécuter le **groupe tacacs+ d'aaa authentication login default de** commande du mode de config, vous devez permettre cette ligne dans le groupe de travail :

AAA lecture/écriture de tâche

Vous pouvez définir le groupe d'utilisateurs qui peut importe plusieurs groupes de travail. 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 d'AAA sur le routeur

Définissez un serveur TACACS sur le routeur :

Voici que vous définissez l'adresse IP de serveur ACS en tant que serveur TACACS avec Cisco principal

```
RP/0/RSP1/CPU0:ASR9k(config)#tacacs-server host 10.106.73.233 port 49
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#key 0 cisco
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#commit

!
tacacs-server host 10.106.73.233 port 49
key 7 14141B180F0B
!
```

Indiquez l'authentification et l'autorisation le serveur TACACS externe.

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

Authorisation(optional) de commande :

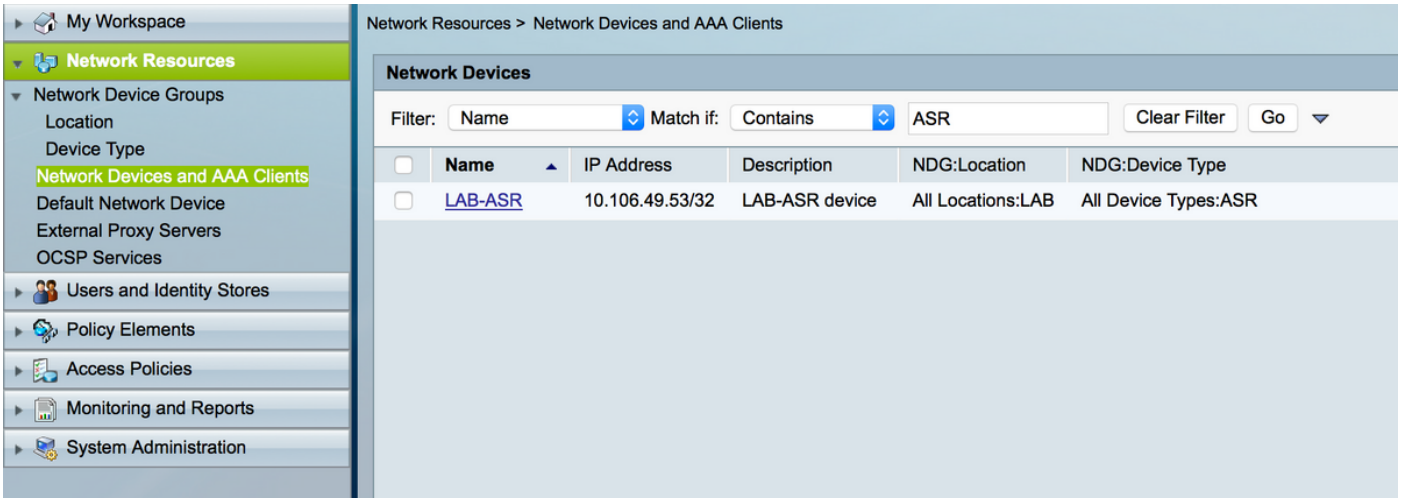
```
#aaa authorization commands default group tacacs+
```

Indiquez la comptabilité le serveur externe (facultatif).

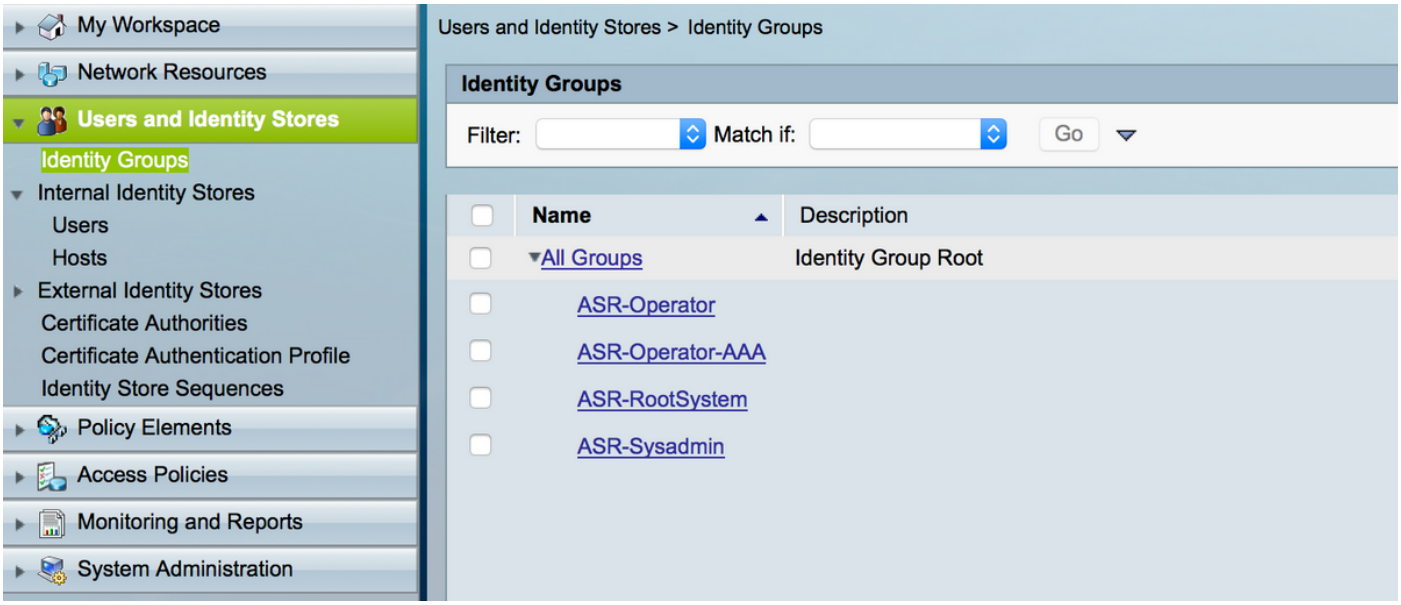
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

Configuration de serveur ACS

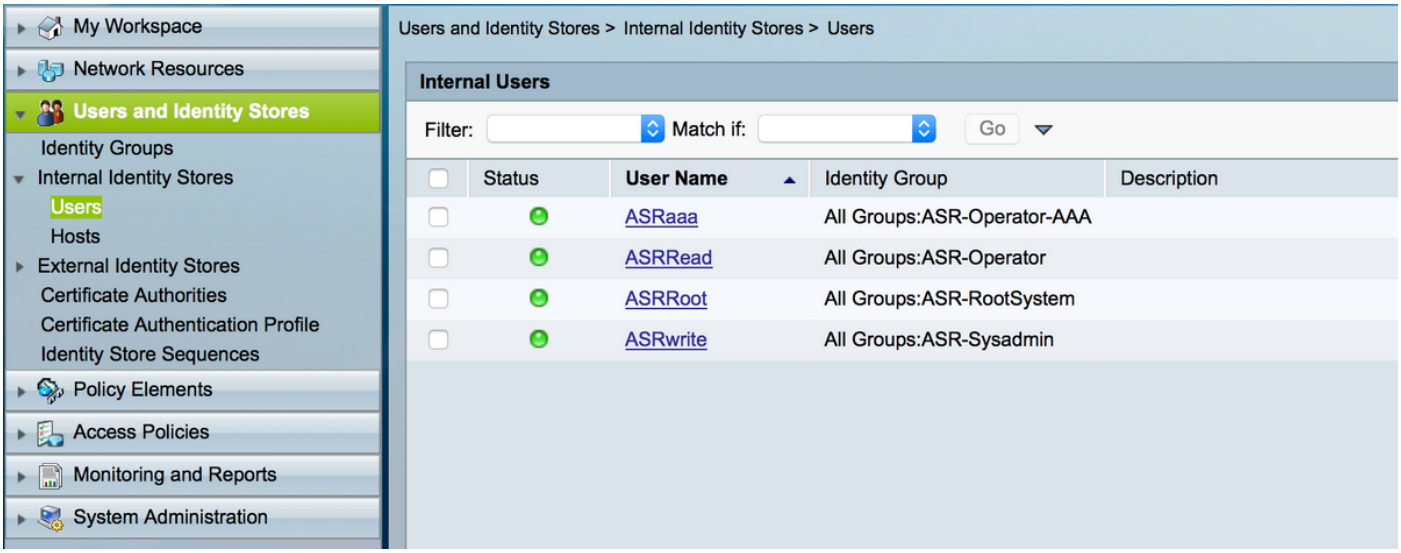
Étape 1. Afin de définir le routeur que l'IP dans les clients d'AAA les répertorient sur le serveur ACS, naviguent vers des **ressources de réseau > des périphériques de réseau et des clients d'AAA**, suivant les indications de l'image. Dans cet exemple, vous définissez **Cisco** en tant que secret partagé comme configuré dans l'ASR.



Étape 2. Définissez les groupes d'utilisateurs selon votre condition requise, dans l'exemple, suivant les indications de cette image, vous utilisent quatre groupes.

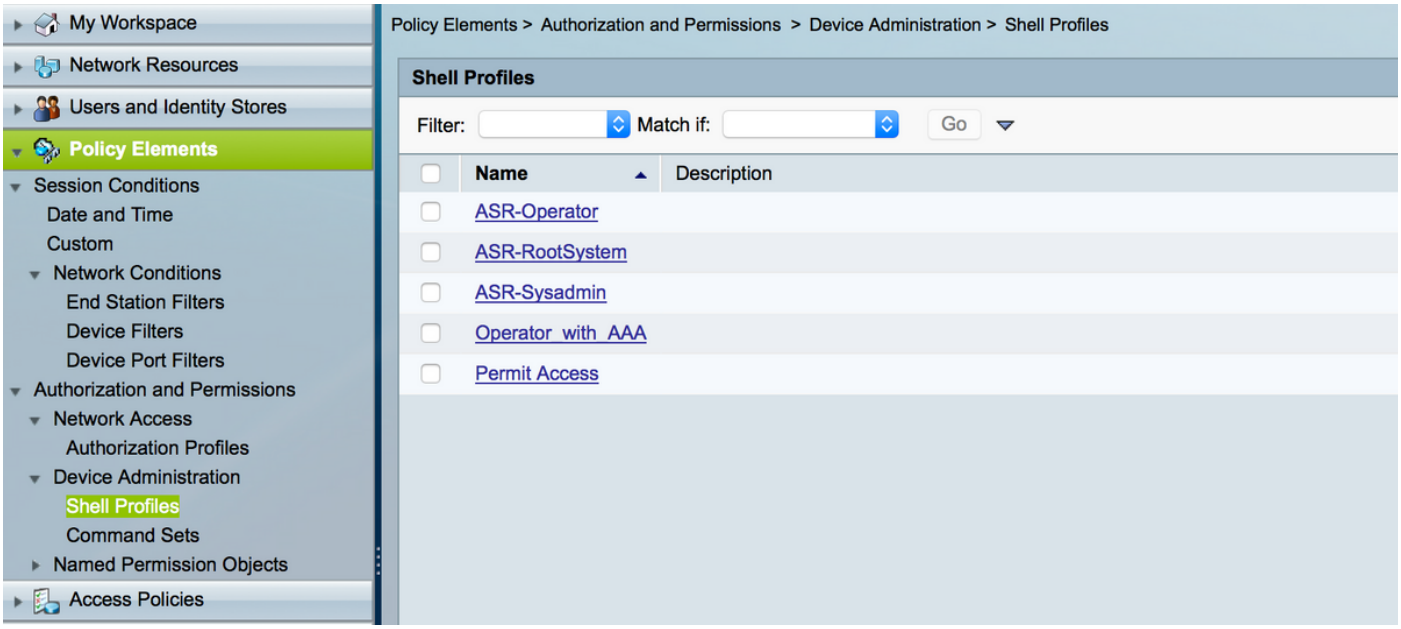


Étape 3. Suivant les indications de l'image, créez les utilisateurs et tracez-les au groupe d'utilisateurs respectif créé ci-dessus.

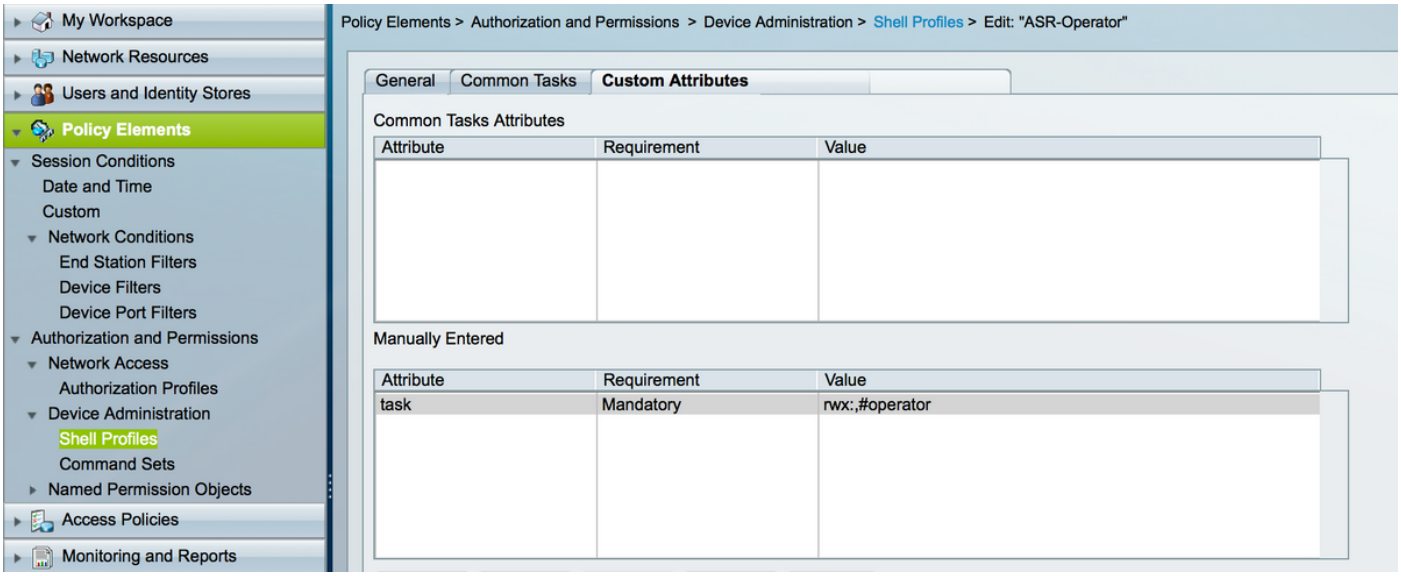


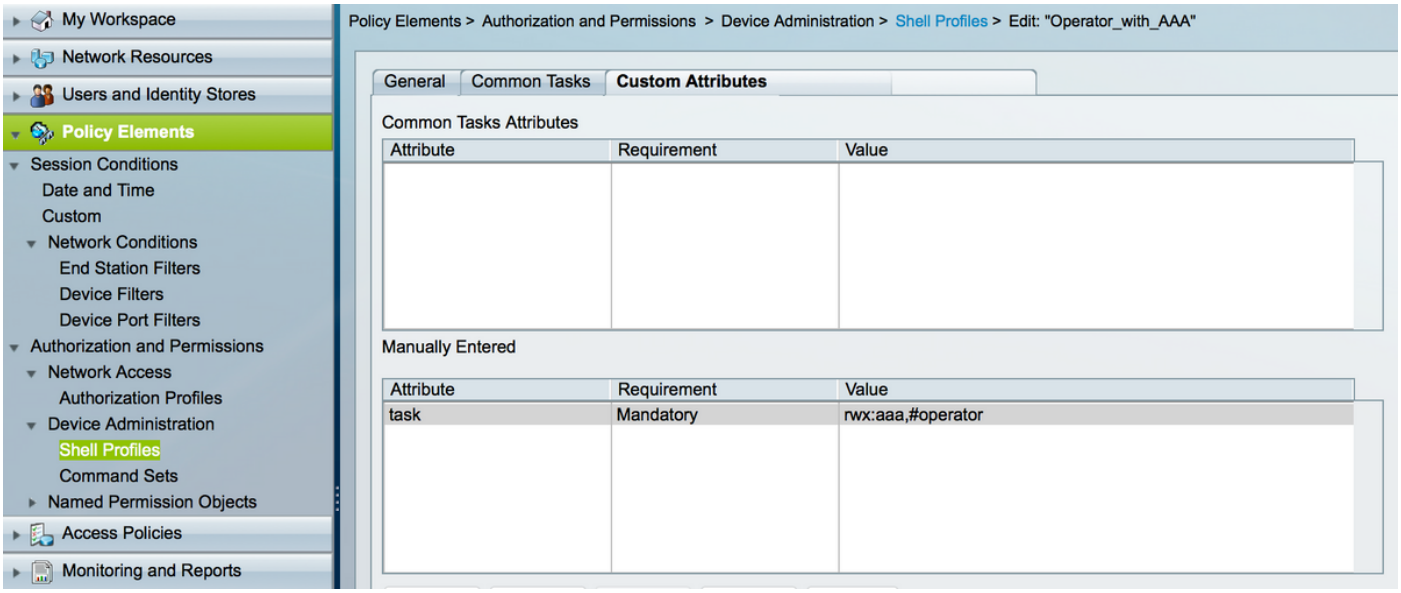
Note: Dans cet exemple, les utilisateurs internes ACS pour l'authentification est utilisés, si vous voulez utiliser les utilisateurs créés dans l'identité externe vous enregistre pouvez les utiliser aussi bien. Dans cet exemple, les utilisateurs externes de source d'identité n'est pas couverts.

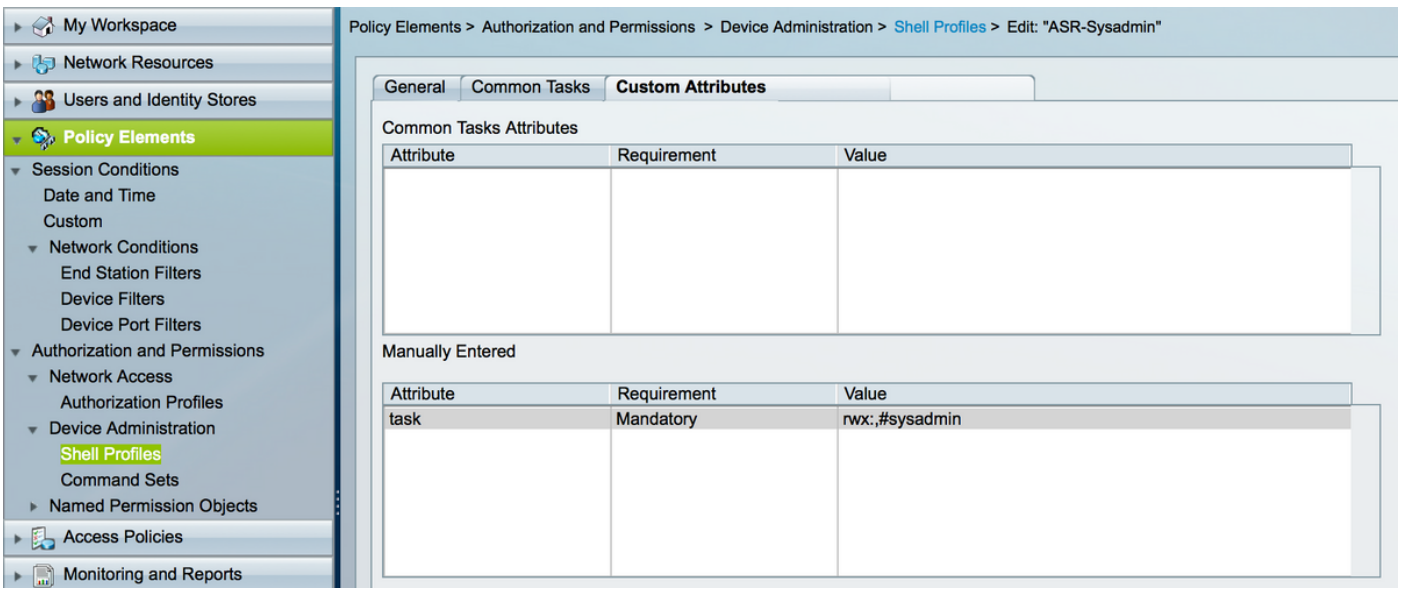
Étape 4. Définissez le profil de shell que vous voulez pousser les utilisateurs respectifs.

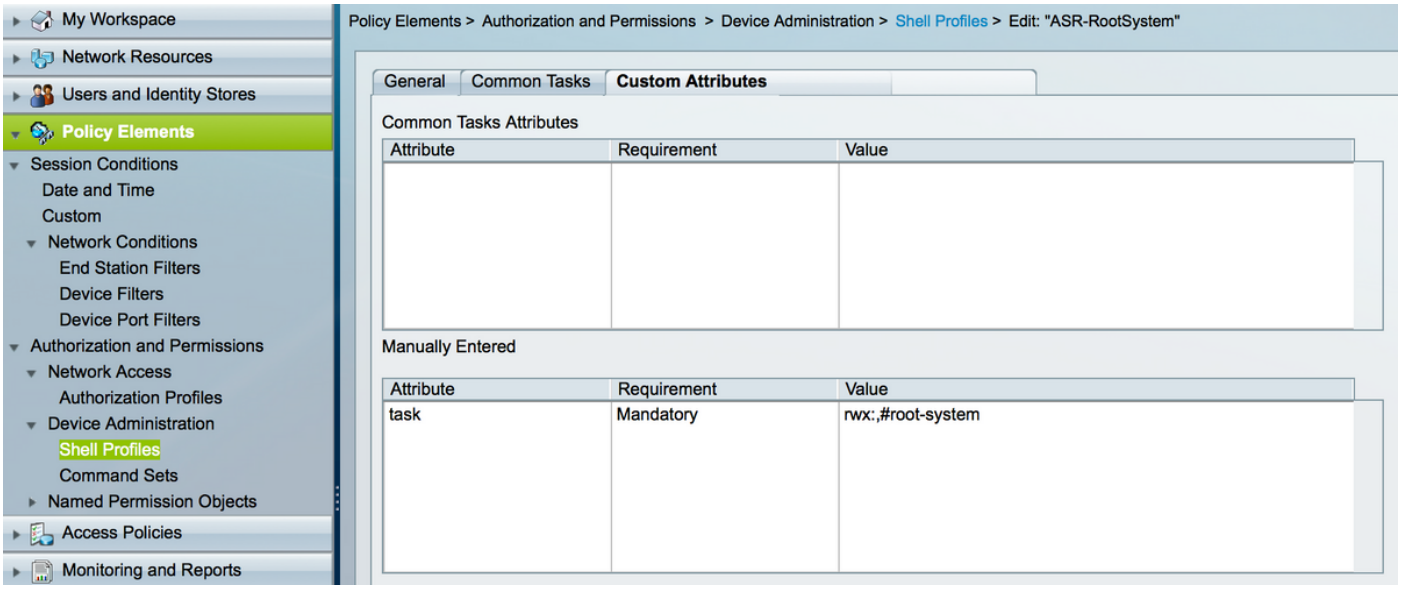


Dans le profil déjà créé de shell, vous configurez pour pousser les groupes de travail respectifs suivant les indications de l'image.

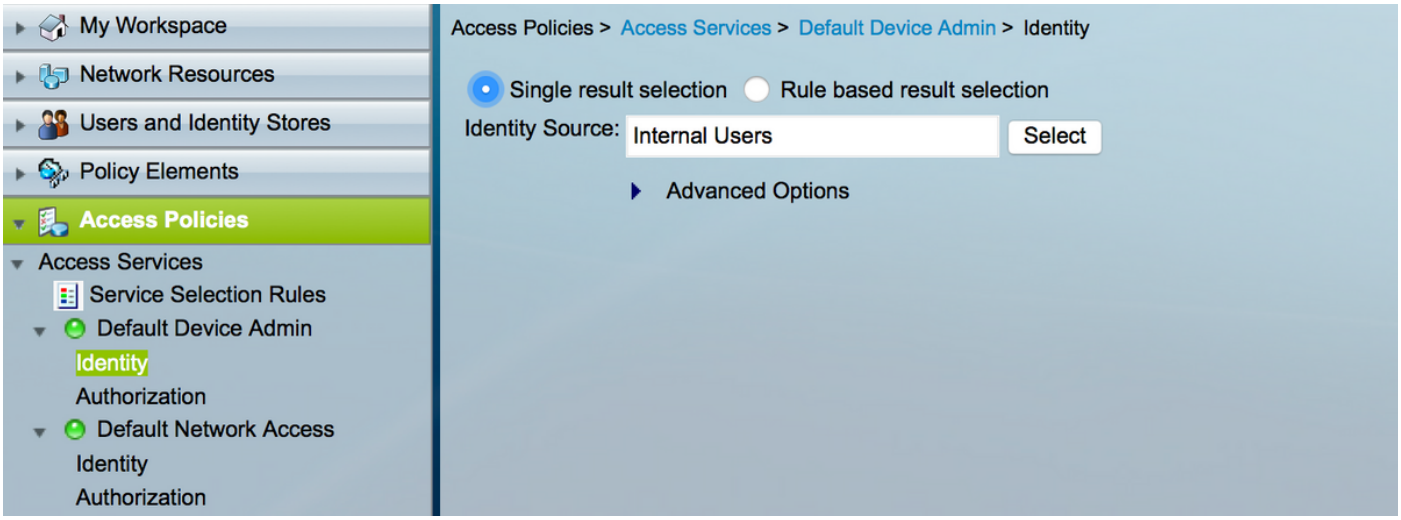

My Workspace
Network Resources
Users and Identity Stores
Policy Elements
Session Conditions
Date and Time
Custom
Network Conditions
End Station Filters
Device Filters
Device Port Filters
Authorization and Permissions
Network Access
Authorization Profiles
Device Administration
Shell Profiles
Command Sets
Named Permission Objects
Access Policies
Monitoring and Reports
Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "ASR-Operator"
General
Common Tasks
Custom Attributes
Common Tasks Attributes
Attribute
Requirement
Value
Manually Entered
Attribute
Requirement
Value
task
Mandatory
rwx:,#operator


My Workspace
Network Resources
Users and Identity Stores
Policy Elements
Session Conditions
Date and Time
Custom
Network Conditions
End Station Filters
Device Filters
Device Port Filters
Authorization and Permissions
Network Access
Authorization Profiles
Device Administration
Shell Profiles
Command Sets
Named Permission Objects
Access Policies
Monitoring and Reports
Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "Operator_with_AAA"
General
Common Tasks
Custom Attributes
Common Tasks Attributes
Attribute
Requirement
Value
Manually Entered
Attribute
Requirement
Value
task
Mandatory
rwx:aaa,#operator

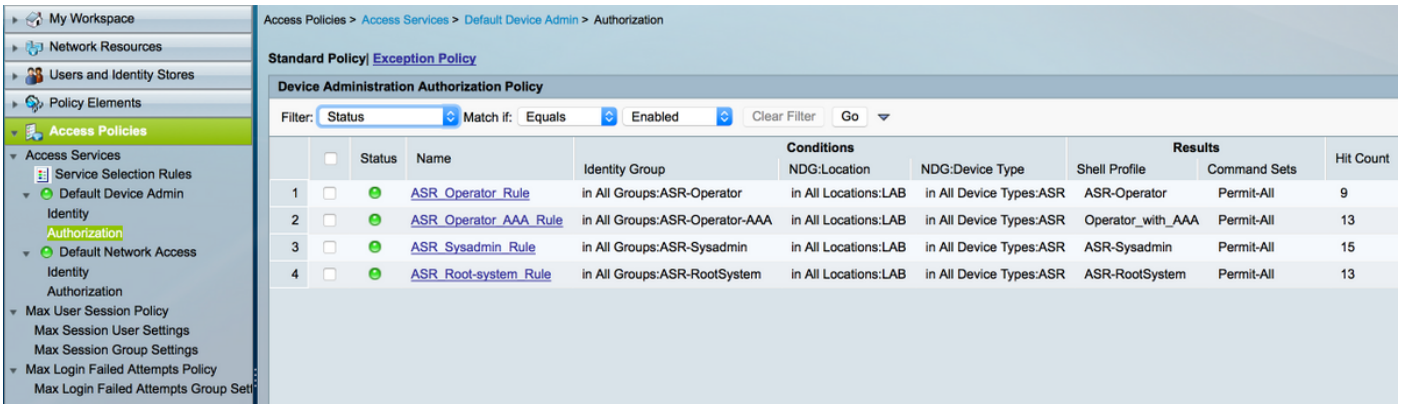

My Workspace
Network Resources
Users and Identity Stores
Policy Elements
Session Conditions
Date and Time
Custom
Network Conditions
End Station Filters
Device Filters
Device Port Filters
Authorization and Permissions
Network Access
Authorization Profiles
Device Administration
Shell Profiles
Command Sets
Named Permission Objects
Access Policies
Monitoring and Reports
Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "ASR-Sysadmin"
General
Common Tasks
Custom Attributes
Common Tasks Attributes
Attribute
Requirement
Value
Manually Entered
Attribute
Requirement
Value
task
Mandatory
rwx:,#sysadmin



Étape 5. Définissez la stratégie d'accès. L'authentification est faite contre les utilisateurs internes.



Étape 6. Configurez l'autorisation basée sur la condition requise utilisant les groupes précédemment créés d'identité de l'utilisateur et tracez les profils respectifs de shell, suivant les indications de l'image.



Vérifiez

Opérateur

Afin d'ouvrir une session, l'**asrread de** nom d'utilisateur est utilisé. Ce sont les commandes de vérification.

```
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 l'AAA

Afin d'ouvrir une session, l'**asraaa de** nom d'utilisateur est utilisé. Ce sont les commandes de vérification.

> **Note**: **l'asraaa** est la tâche d'opérateur poussée du serveur TACACS avec la tâche d'AAA lecture/écriture et exécute des autorisations.

```
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

Afin d'ouvrir une session, l'**asrwrite de** nom d'utilisateur est utilisé. Ce sont les commandes de vérification.

```
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 )
```

Racine-système

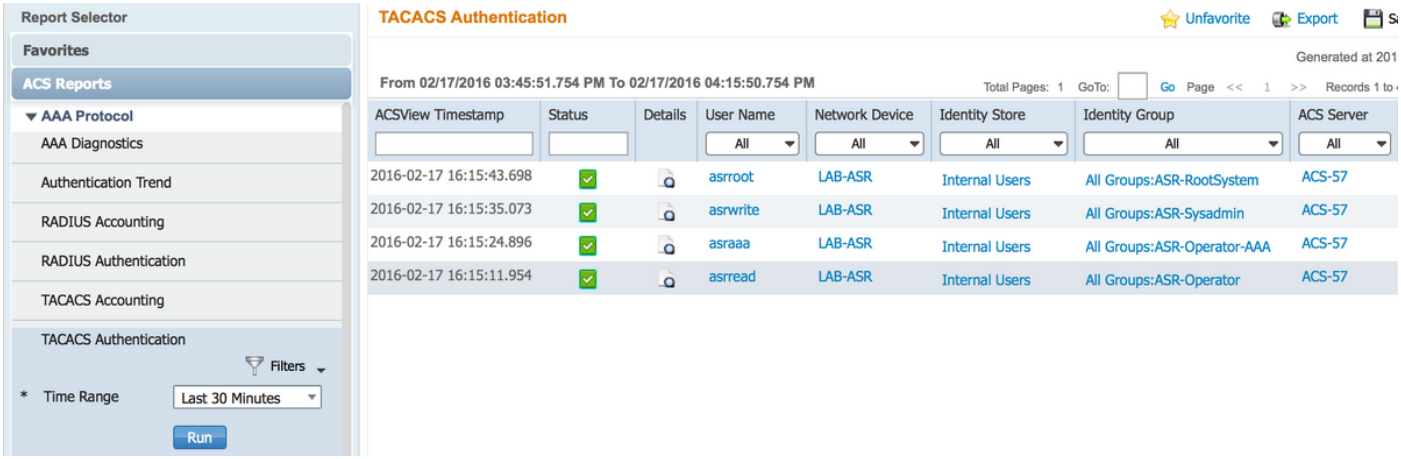
Afin d'ouvrir une session, l'**asrroot de** nom d'utilisateur est utilisé. Ce sont les commandes de vérification.

```
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 )
```

Dépannez

Vous pouvez vérifier l'état ACS de la page de surveillance et d'enregistrement. Suivant les indications de l'image, vous pouvez cliquer sur en fonction le sumbol de loupe pour voir le rapport détaillé.



Ce sont quelques commandes utiles de dépanner sur l'ASR :

- **affichez l'utilisateur**
- **affichez le groupe d'utilisateurs**
- **affichez les tâches d'utilisateur**
- **affichez l'utilisateur tout**