Configurer l'autorisation de commande d'authentification TACACS+ ISE 2.0

Table des matières

- Introduction
- Informations générales
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - Diagramme du réseau
  - Configurations
    - Configurer ISE pour l'authentification et l'autorisation
    - Joindre ISE 2.0 à Active Directory
    - Ajouter un périphérique réseau
    - Activer le service d'administration des périphériques
    - Configurer les jeux de commandes TACACS
    - Configurer le profil TACACS
    - Configurer la stratégie d'autorisation TACACS
    - Configuration du routeur Cisco IOS pour l'authentification et l'autorisation
- Vérifier
  - Vérification du routeur Cisco IOS
  - Vérification ISE 2.0
- Dépannage
- Informations connexes

Introduction

Ce document décrit comment configurer l'authentification TACACS+ et l'autorisation de commande en fonction de l'appartenance au groupe Microsoft Active Directory (AD).

Informations générales

Pour configurer l'authentification TACACS+ et l'autorisation de commande en fonction de l'appartenance à un groupe Microsoft Active Directory (AD) d'un utilisateur avec Identity Service Engine (ISE) 2.0 et versions ultérieures, ISE utilise AD comme magasin d'identités externe pour stocker des ressources telles que des utilisateurs, des machines, des groupes et des attributs.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Le routeur Cisco IOS® est entièrement opérationnel
- Connectivité entre le routeur et ISE.
- Le serveur ISE est amorcé et dispose d'une connectivité à Microsoft AD

Composants utilisés

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

- Cisco Identity Service Engine 2.0
- Logiciel Cisco IOS® version 15.4(3)M3
- Microsoft Windows Server 2012 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

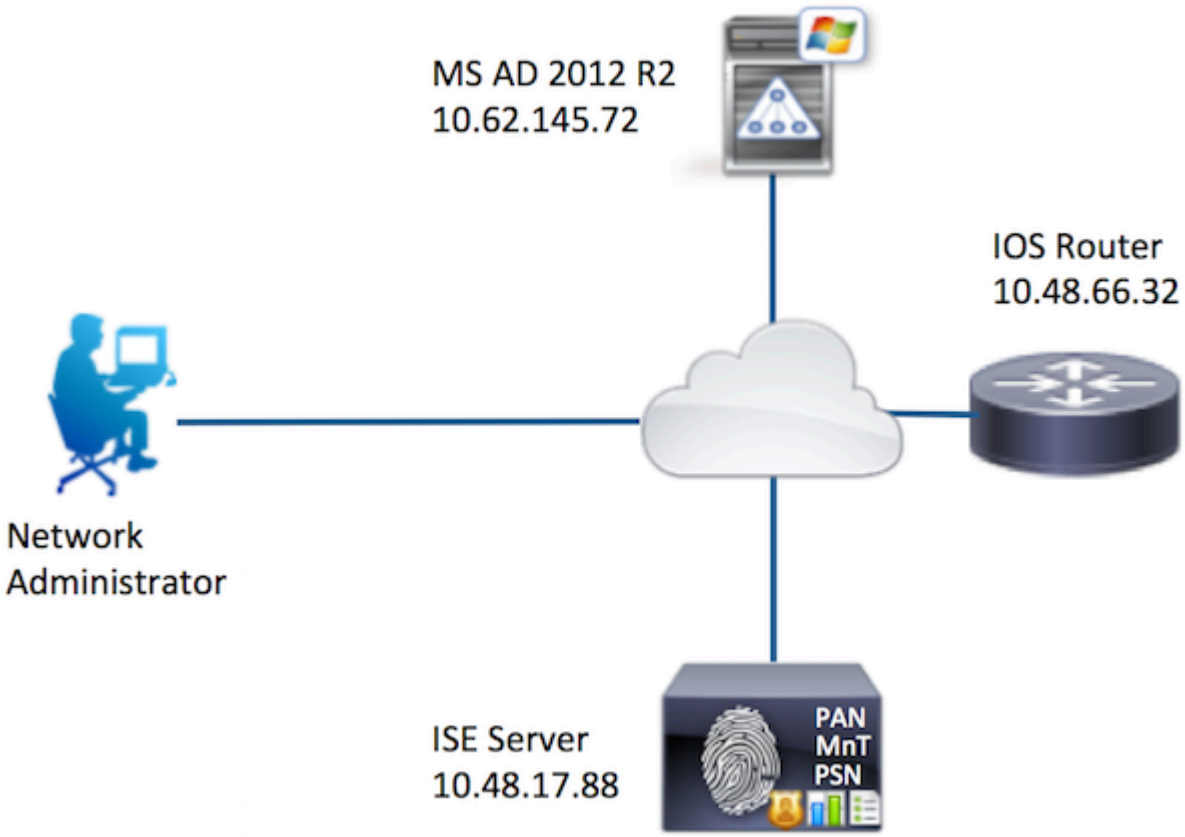
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurer

L'objectif de la configuration est de :

- Authentifier un utilisateur Telnet via AD
- Autoriser l’utilisateur Telnet à passer en mode d’exécution privilégié après la connexion
- Vérifier et envoyer chaque commande exécutée à ISE pour vérification

Diagramme du réseau

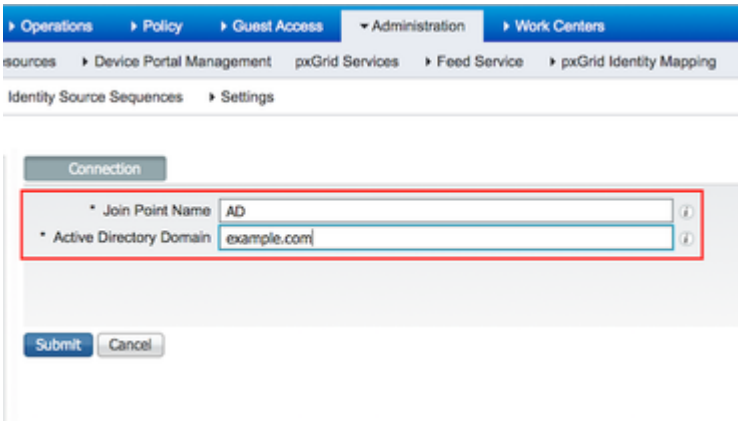


Configurations

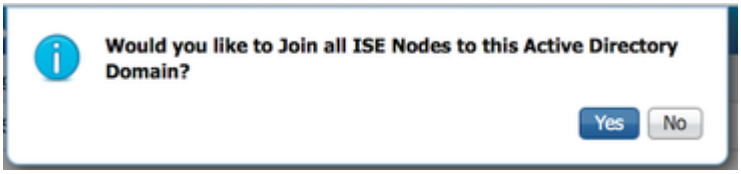
Configurer ISE pour l'authentification et l'autorisation

Joindre ISE 2.0 à Active Directory

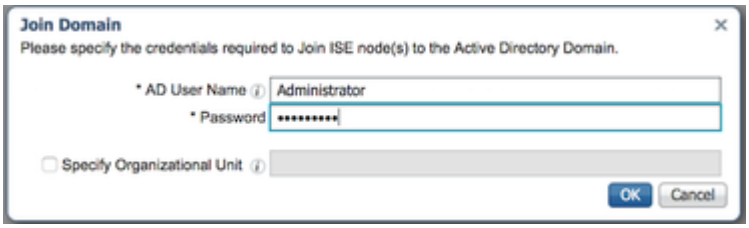
1. Accédez à Administration > Gestion des identités > Magasins d'identités externes > Active Directory > Ajouter. Fournissez le nom du point de jonction, le domaine Active Directory et cliquez sur Envoyer.



2. Lorsque vous êtes invité à joindre tous les noeuds ISE à ce domaine Active Directory, cliquez sur Oui.



3. Fournissez un nom d'utilisateur et un mot de passe AD, puis cliquez sur OK.



Le compte AD requis pour l'accès au domaine dans ISE peut avoir l'un des éléments suivants :

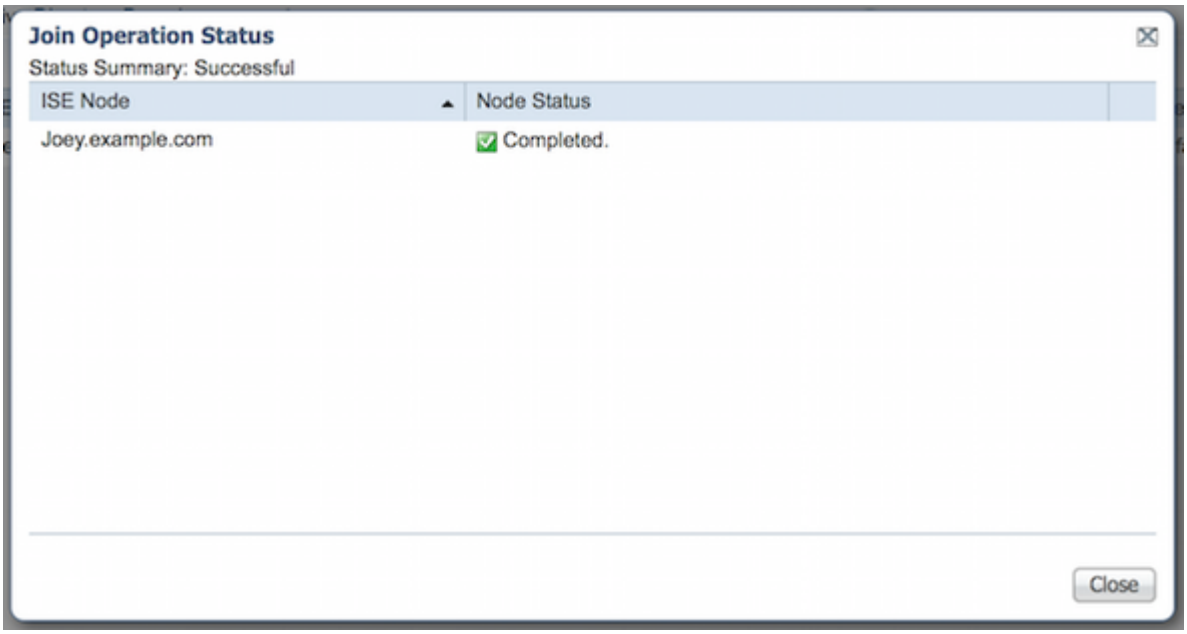
- Ajouter des stations de travail au droit utilisateur de domaine dans le domaine respectif
- Autorisation Créer des objets ordinateur ou Supprimer des objets ordinateur sur le conteneur d'ordinateurs respectif où le compte de l'ordinateur ISE est créé avant qu'il ne joigne l'ordinateur ISE au domaine

---

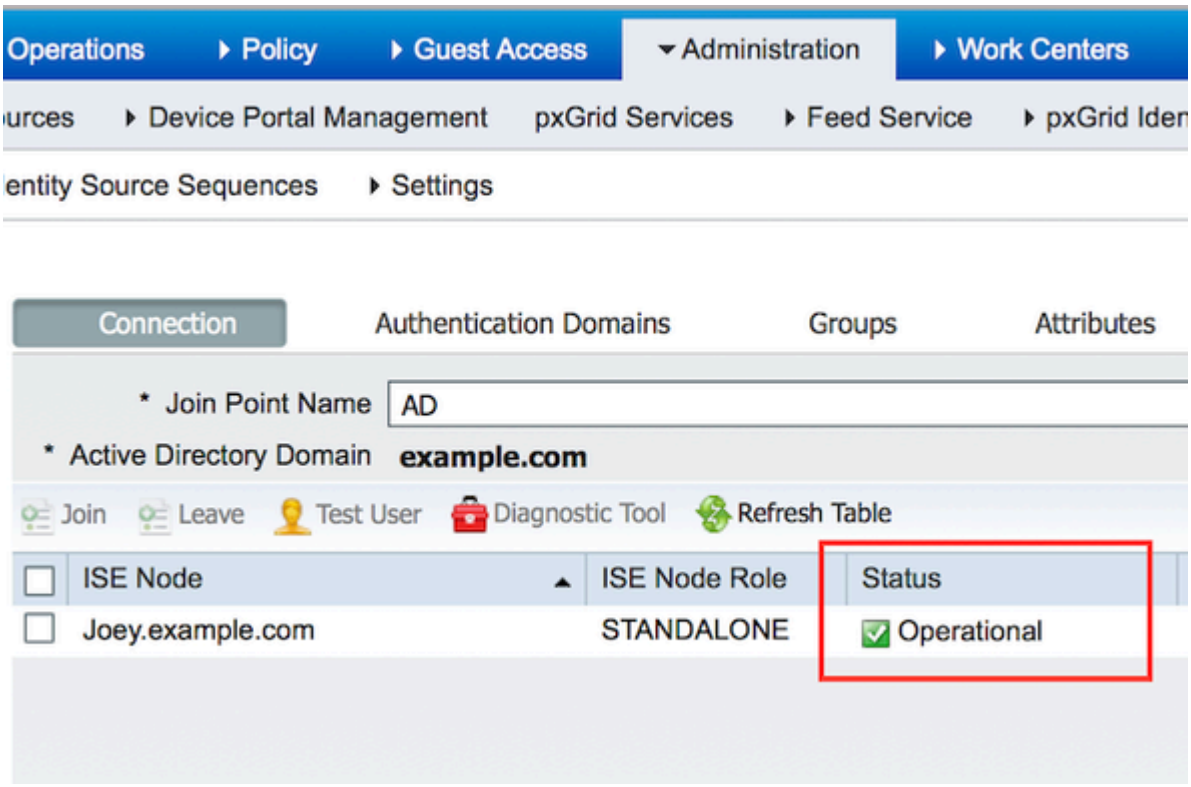
Remarque : Cisco recommande de désactiver la stratégie de verrouillage pour le compte ISE et de configurer l'infrastructure AD pour envoyer des alertes à l'administrateur si un mot de passe incorrect est utilisé pour ce compte. Lorsque le mauvais mot de passe est entré, ISE ne crée pas ou ne modifie pas son compte d'ordinateur lorsqu'il est nécessaire et peut donc refuser toutes les authentifications.

---

4. Vérifiez l'état des opérations. L'état du noeud doit apparaître comme Terminé. Cliquez sur Fermer.

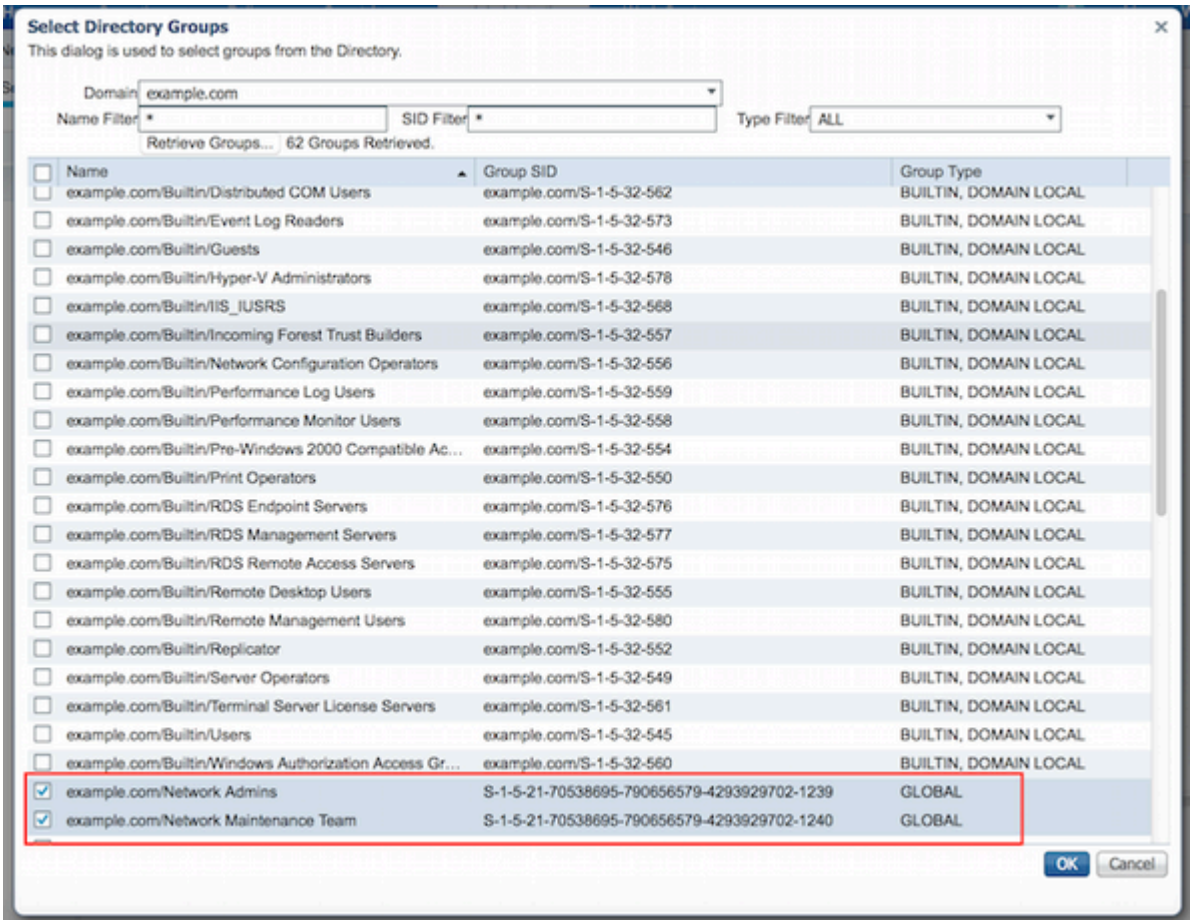


5. L'état d'AD est opérationnel.

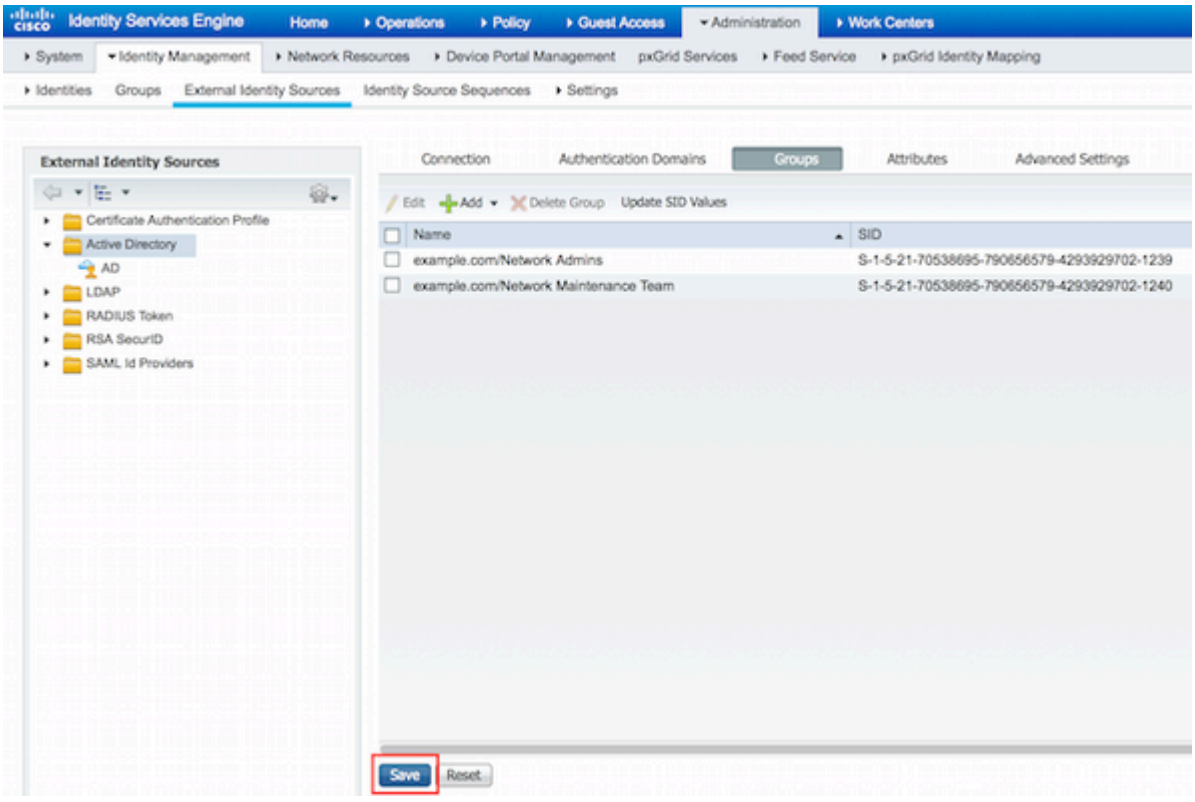


6. Accédez à Groups > Add > Select Groups From Directory > Retrieve Groups. Cochez les cases Administrateurs réseau Groupe AD et Équipe de maintenance réseau Groupe AD, comme illustré dans cette image.

Remarque : L'utilisateur admin est membre du groupe AD Administrateurs réseau. Cet utilisateur dispose de privilèges d'accès complets. Cet utilisateur est membre du groupe AD de l'équipe de maintenance du réseau. Cet utilisateur ne peut exécuter que des commandes show.

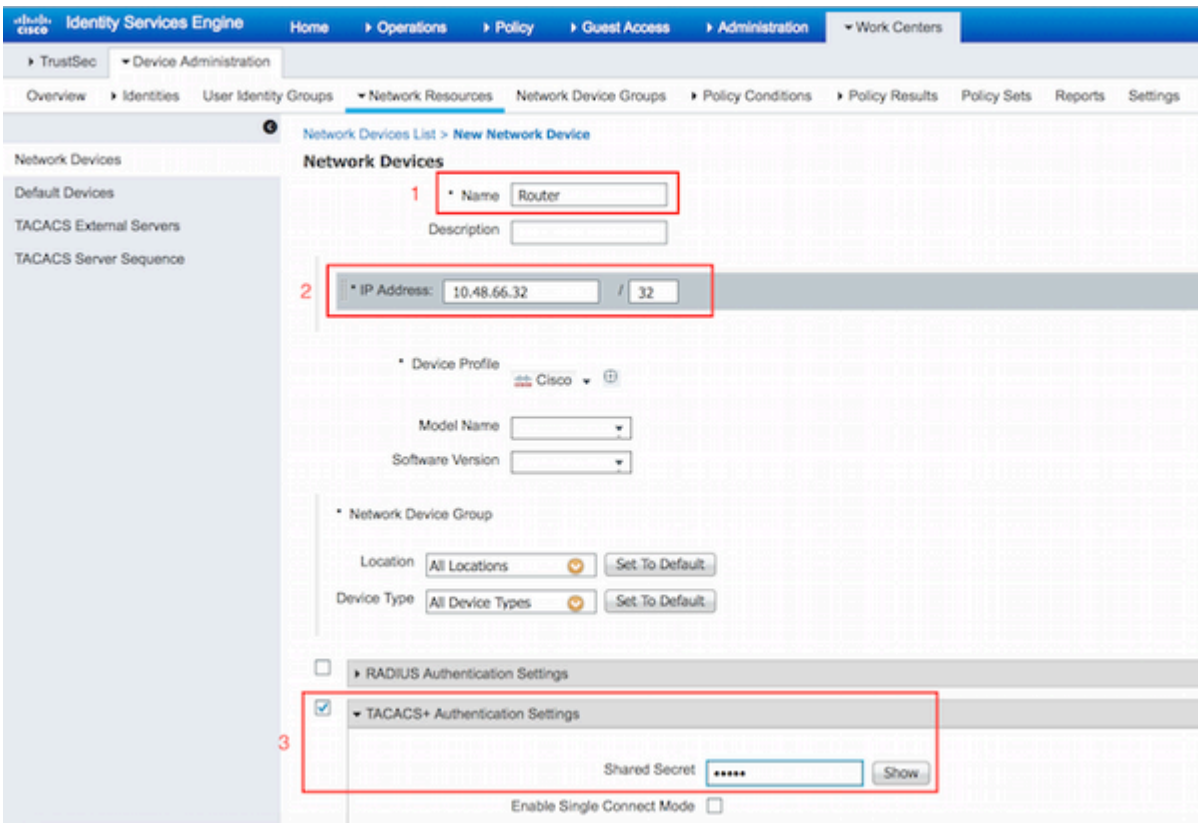


7. Cliquez sur Enregistrer pour enregistrer les groupes AD récupérés.



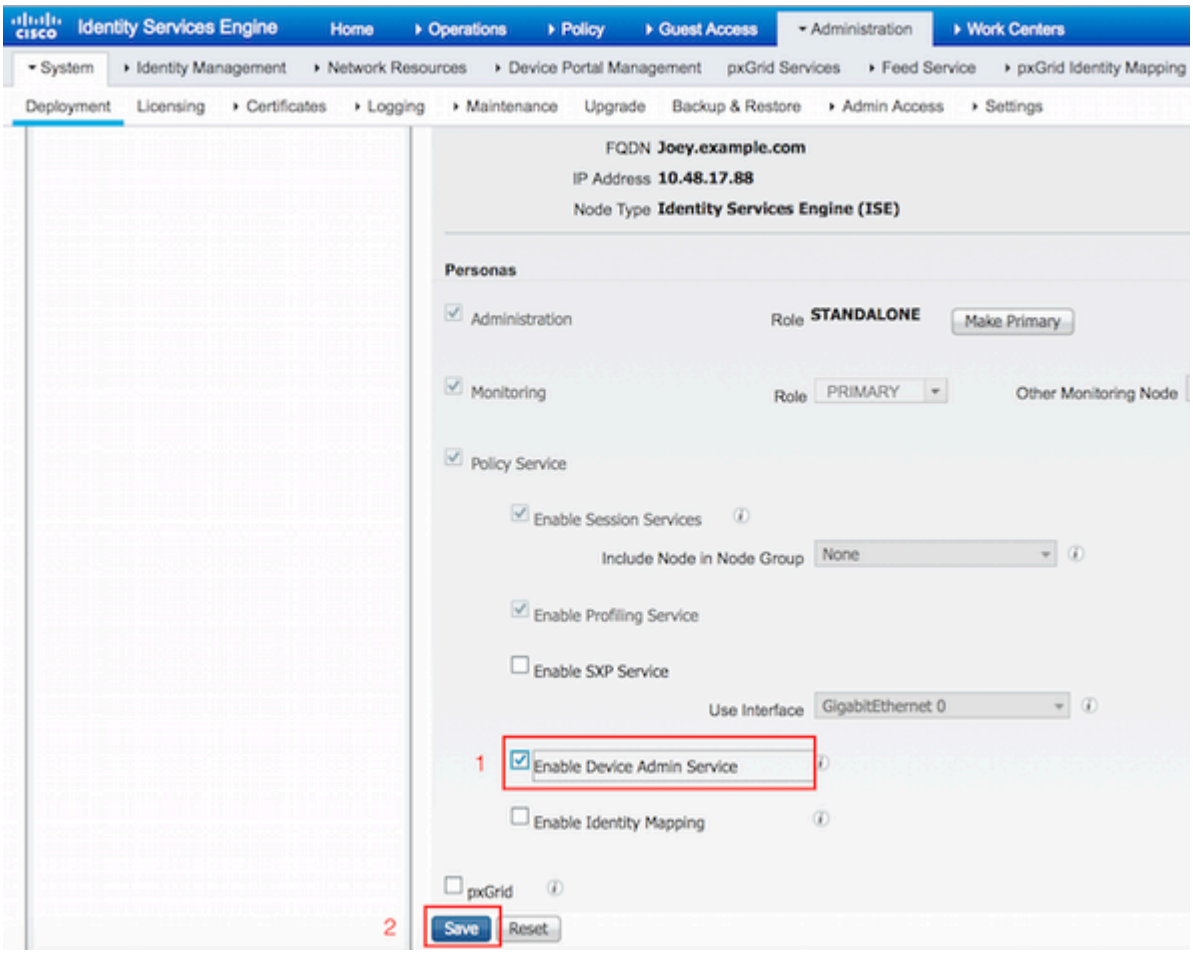
Ajouter un périphérique réseau

Accédez à Work Centers > Device Administration > Network Resources > Network Devices. Cliquez sur Add. Indiquez le nom et l'adresse IP, cochez la case TACACS+ Authentication Settings et indiquez la clé secrète partagée.



Activer le service d'administration des périphériques

Accédez à Administration > System > Deployment. Choisissez required Node. Cochez la case Enable Device Admin Service et cliquez sur Save.

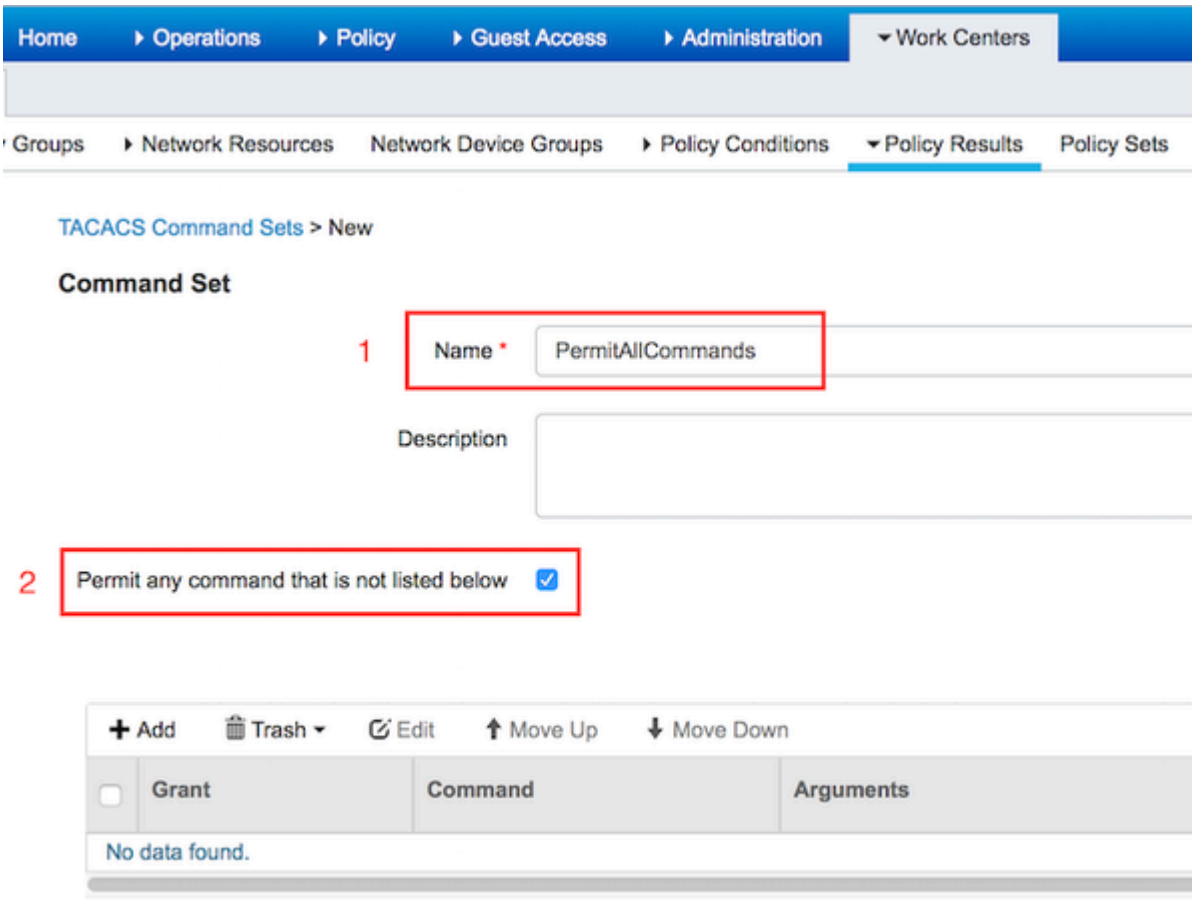


Remarque : Pour TACACS, vous devez avoir installé des licences distinctes.

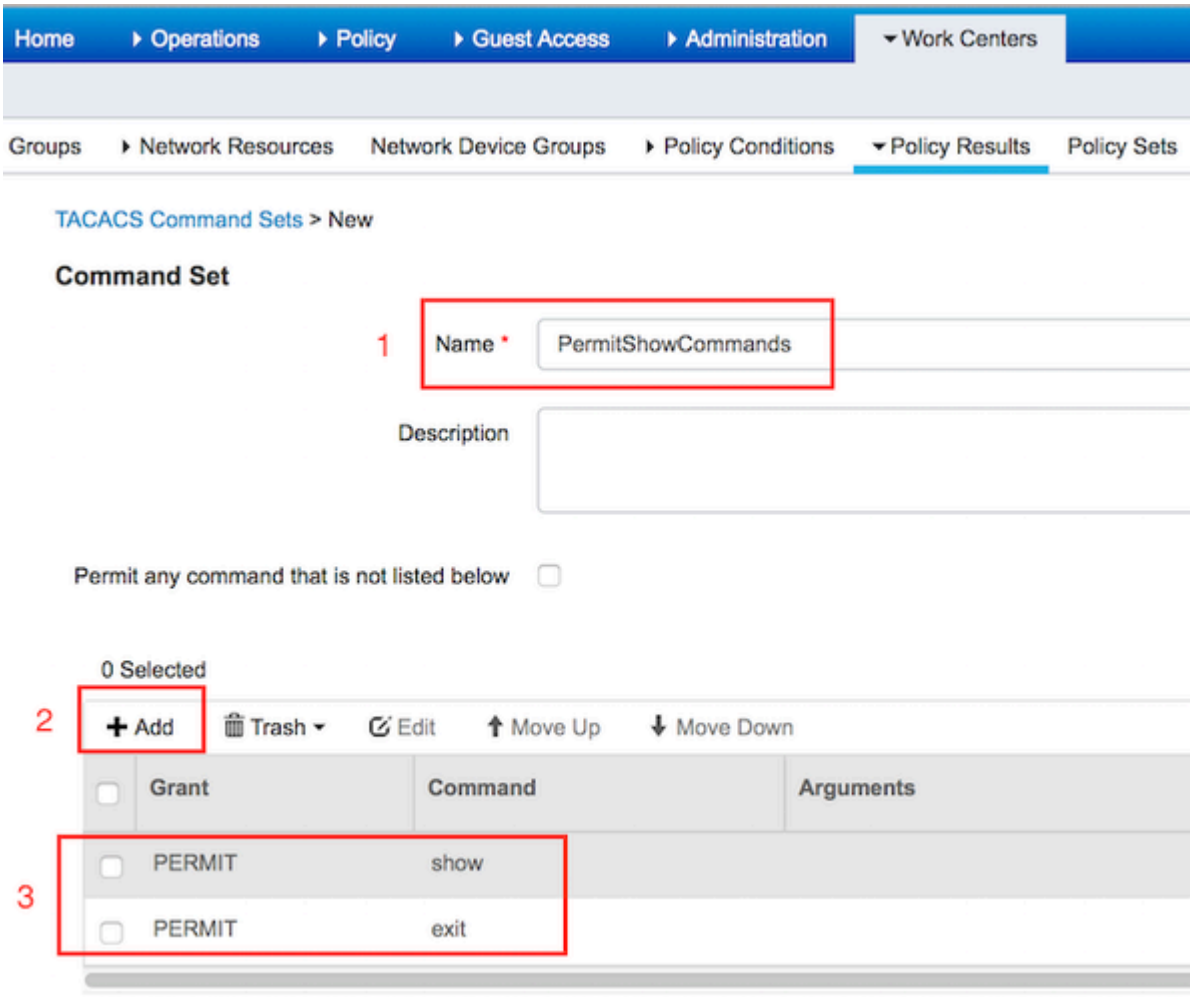
Configurer les jeux de commandes TACACS

Deux jeux de commandes sont configurés. First PermitAllCommands pour l'utilisateur admin qui autorise toutes les commandes sur le périphérique. Deuxième PermitShowCommands pour l'utilisateur qui autorise uniquement les commandes show.

1. Accédez à Work Centers > Device Administration > Policy Results > TACACS Command Sets. Cliquez sur Add. Fournissez le nom PermitAllCommands, sélectionnez la case à cocher Permit any command qui n'est pas répertoriée et cliquez sur Submit.

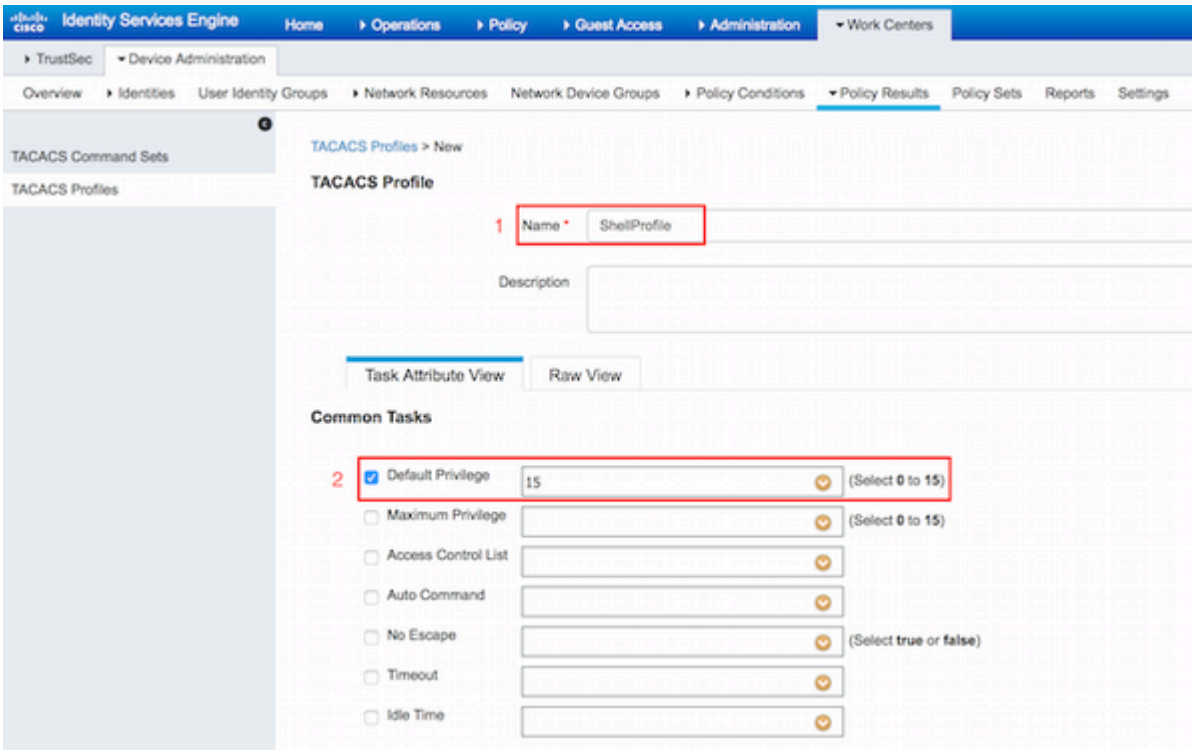


2. Accédez à Work Centers > Device Administration > Policy Results > TACACS Command Sets. Cliquez sur Add. Fournissez le nom PermitShowCommands, cliquez sur Add et autorisez les commandes show et exit. Par défaut, si Arguments est laissé vide, tous les arguments sont inclus. Cliquez sur Submit.



Configurer le profil TACACS

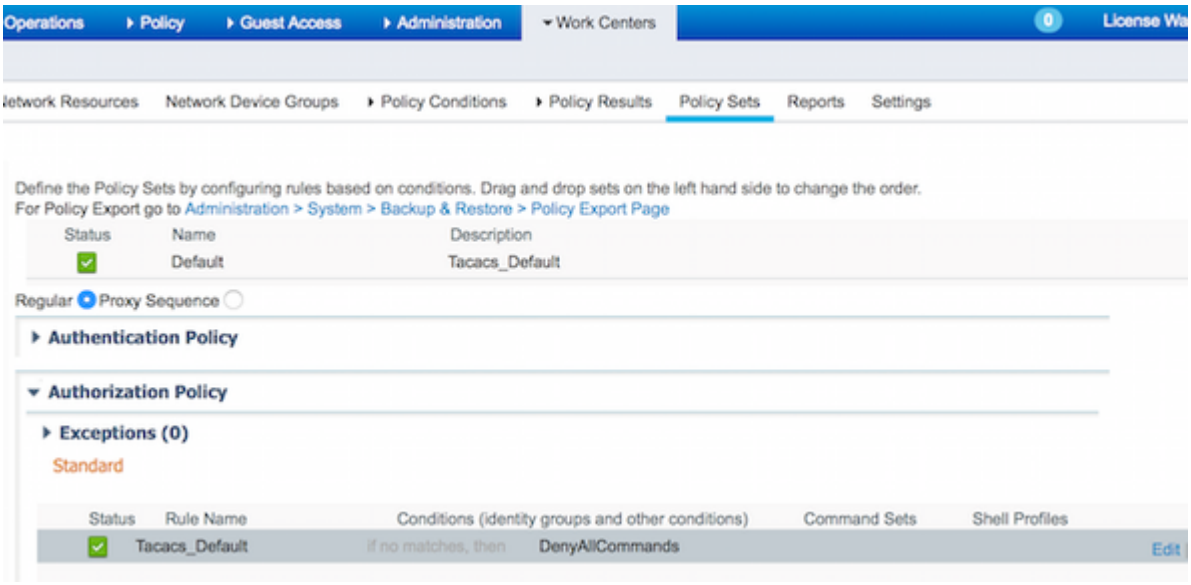
Un seul profil TACACS est configuré. Le profil TACACS est le même concept que le profil Shell sur ACS. L'application effective des commandes se fait via des jeux de commandes. Accédez à Work Centers > Device Administration > Policy Results > TACACS Profiles. Cliquez sur Add. Fournissez Name ShellProfile, cochez la case Default Privilege et entrez la valeur 15. Cliquez sur Submit.



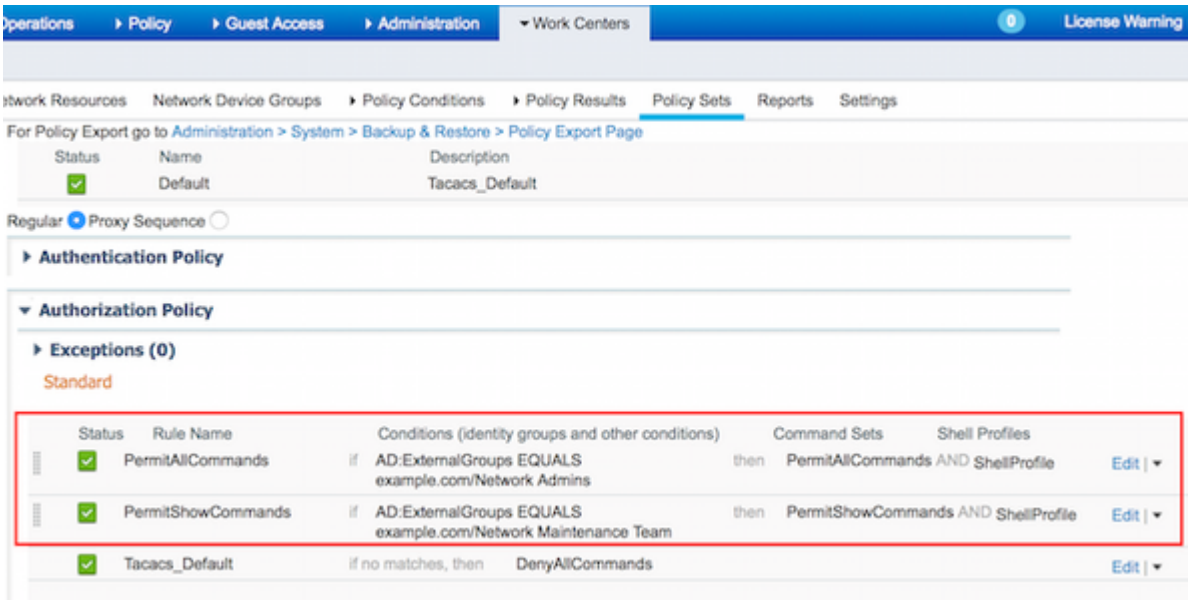
Configurer la stratégie d'autorisation TACACS

Par défaut, la stratégie d'authentification pointe vers All_User_ID_Stores, qui inclut Active Directory. Elle reste donc inchangée.

Accédez à Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule Above.



Deux règles d'autorisation sont configurées ; La première règle attribue le profil TACACS ShellProfile et la commande Set PermitAllCommands en fonction de l'appartenance au groupe AD des administrateurs réseau. La deuxième règle attribue le profil TACACS ShellProfile et la commande Set PermitShowCommands en fonction de l'appartenance au groupe AD de l'équipe de maintenance du réseau.



Configuration du routeur Cisco IOS pour l'authentification et l'autorisation

Complétez ces étapes afin de configurer le routeur Cisco IOS pour l'authentification et l'autorisation.

1. Créez un utilisateur local avec des privilèges complets pour le secours avec la commande username comme indiqué ici.

```
username cisco privilege 15 password cisco
```

2. Activez un nouveau modèle. Définissez le serveur TACACS ISE et placez-le dans le groupe ISE_GROUP.

```
aaa new-model



tacacs server ISE
 address ipv4 10.48.17.88
 key cisco
aaa group server tacacs+ ISE_GROUP
 server name ISE
```

Remarque : La clé du serveur correspond à celle définie sur le serveur ISE précédemment.

---

3. Testez l'accessibilité du serveur TACACS à l'aide de la commande test aaa, comme indiqué.

```
<#root>

Router#

test aaa group tacacs+ admin Krakow123 legacy


Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

Le résultat de la commande précédente indique que le serveur TACACS est accessible et que l'utilisateur a été authentifié avec succès.

4. Configurez la connexion et activez les authentifications, puis utilisez les autorisations d’exécution et de commande comme indiqué.

```
aaa authentication login AAA group ISE_GROUP local
aaa authentication enable default group ISE_GROUP enable
aaa authorization exec AAA group ISE_GROUP local
aaa authorization commands 0 AAA group ISE_GROUP local
aaa authorization commands 1 AAA group ISE_GROUP local
aaa authorization commands 15 AAA group ISE_GROUP local
aaa authorization config-commands
```

Remarque : La liste de méthodes créée est nommée AAA, qui est utilisée ultérieurement, lorsqu'elle est attribuée à la ligne vty.

---

5. Affectez des listes de méthodes à la ligne vty 0 4.

```
line vty 0 4
 authorization commands 0 AAA
 authorization commands 1 AAA
 authorization commands 15 AAA
 authorization exec AAA
 login authentication AAA
```

Vérifier

Vérification du routeur Cisco IOS

1. Établissez une connexion Telnet avec le routeur Cisco IOS en tant qu’administrateur appartenant au groupe d’accès complet dans Active Directory. Le groupe Admins réseau est le groupe dans Active Directory qui est mappé aux commandes ShellProfile et PermitAllCommands définies sur l'ISE. Essayez d'exécuter n'importe quelle commande pour garantir un accès complet.

```
<#root>

Username:

admin


Password:

Router#

conf t


Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#

crypto isakmp policy 10


Router(config-isakmp)#

encryption aes


Router(config-isakmp)#

exit


Router(config)#

exit


Router#
```

2. Établissez une connexion Telnet avec le routeur Cisco IOS en tant qu'utilisateur appartenant au groupe d'accès limité dans Active Directory. Le groupe d'équipe de maintenance réseau est le groupe dans AD qui est mappé à ShellProfile et PermitShowCommands définis sur l'ISE. Essayez d'exécuter n'importe quelle commande pour vous assurer que seules les commandes show peuvent être exécutées.

```
<#root>

Username:

user


Password:

Router#

show ip interface brief | exclude unassigned


Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.48.66.32     YES NVRAM  up                    up

Router#
```

```
ping 8.8.8.8

Command authorization failed.

Router#
configure terminal

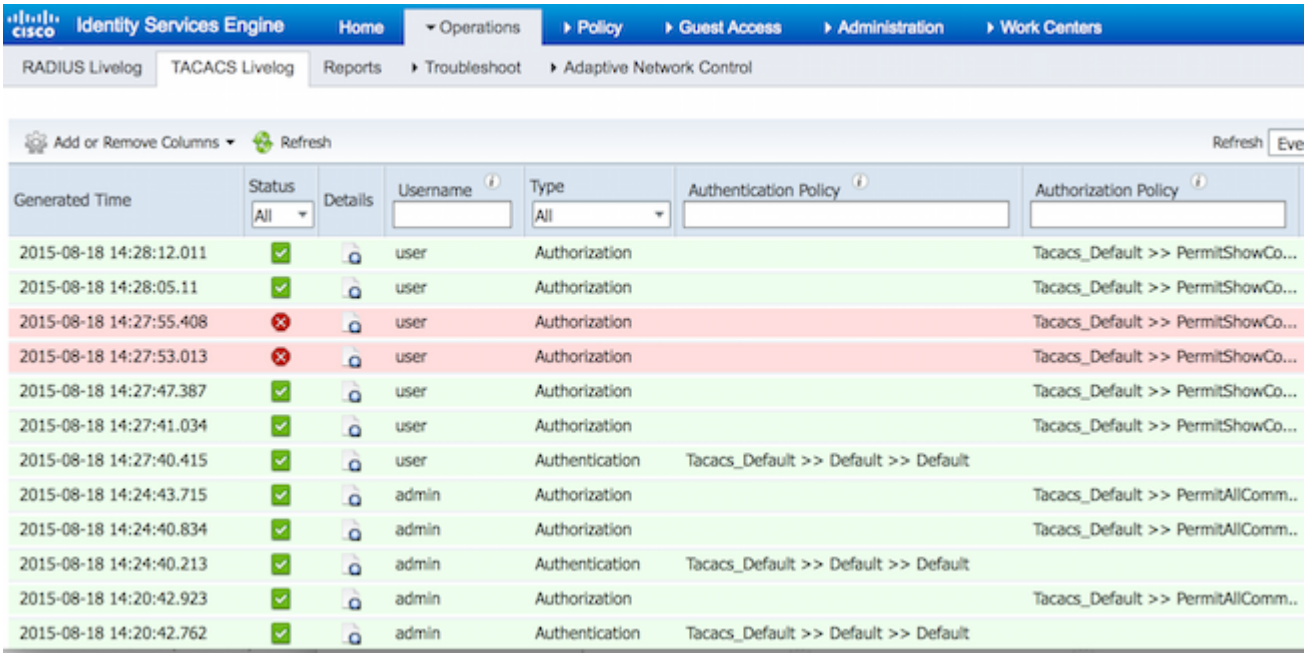
Command authorization failed.

Router#
show running-config | include hostname

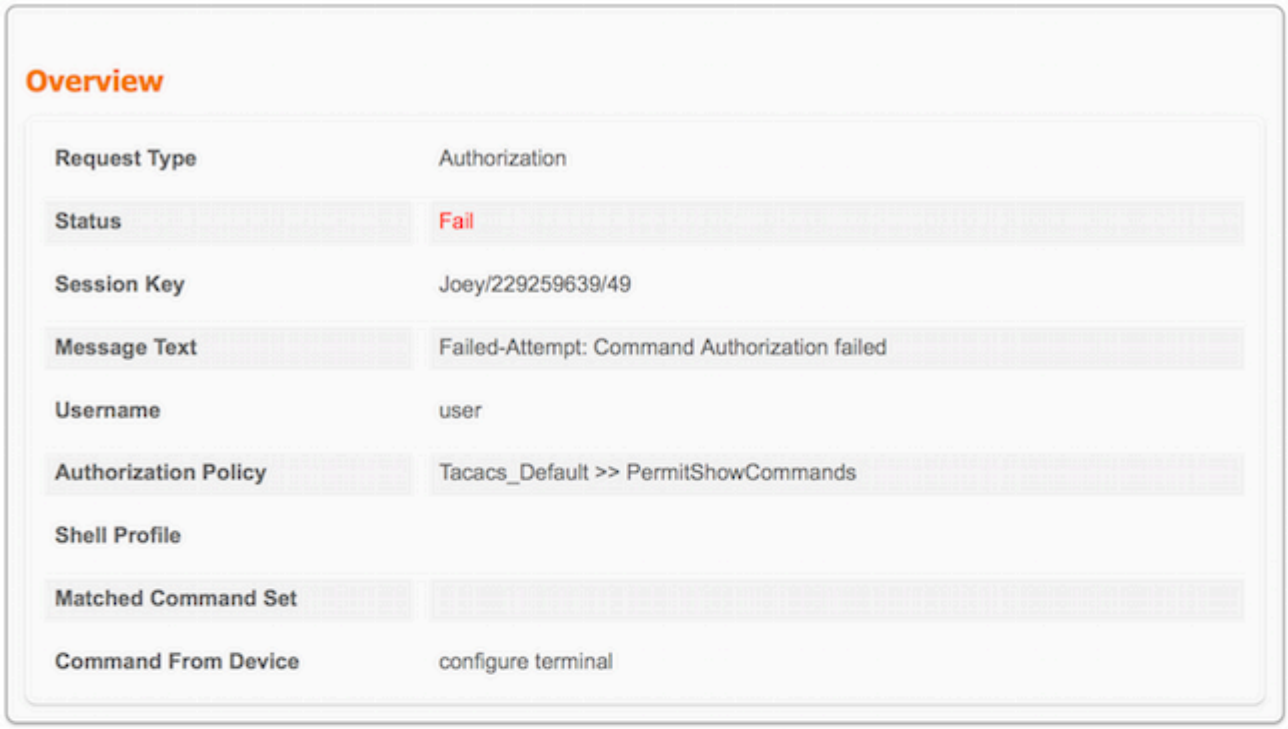
hostname Router
Router#
```

Vérification ISE 2.0

1. Accédez à Operations > TACACS Livellog. Assurez-vous que les tentatives effectuées sont visibles.



2. Cliquez sur les détails de l'un des rapports rouges. La commande ayant échoué exécutée précédemment est visible.





Dépannage

Erreur : La commande 13025 ne correspond pas à une règle d'autorisation

Vérifiez les attributs SelectedCommandSet pour vous assurer que les jeux de commandes attendus ont été sélectionnés par la stratégie d'autorisation.

Informations connexes

Assistance et documentation techniques - Cisco Systems

Notes de version ISE 2.0

Guide d'installation matérielle d'ISE 2.0

Guide de mise à niveau ISE 2.0

Guide de l'outil de migration ACS vers ISE

Guide d'intégration d'ISE 2.0 Active Directory

Guide d'administration du moteur ISE 2.0

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.