ISE 2.0 : Exemple de configuration d'autorisation d'authentification et de commande ASA CLI TACACS+

Contenu

Introduction

Ce document décrit comment configurer l'autorisation d'authentification et de commande TACACS+ sur l'appliance de sécurité adaptable Cisco (ASA) avec l'engine de gestion d'identité (ISE) 2.0 et plus tard. ISE emploie la mémoire locale d'identité pour enregistrer des ressources telles que des utilisateurs, des groupes, et des points finaux.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Le Pare-feu ASA est complètement opérationnel

- Connectivité entre l'ASA et l'ISE
- Le serveur ISE est amorcé

Composants utilisés

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

- Engine 2.0 de gestion d'identité de Cisco
- Version de logiciel 9.5(1) de Cisco ASA

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

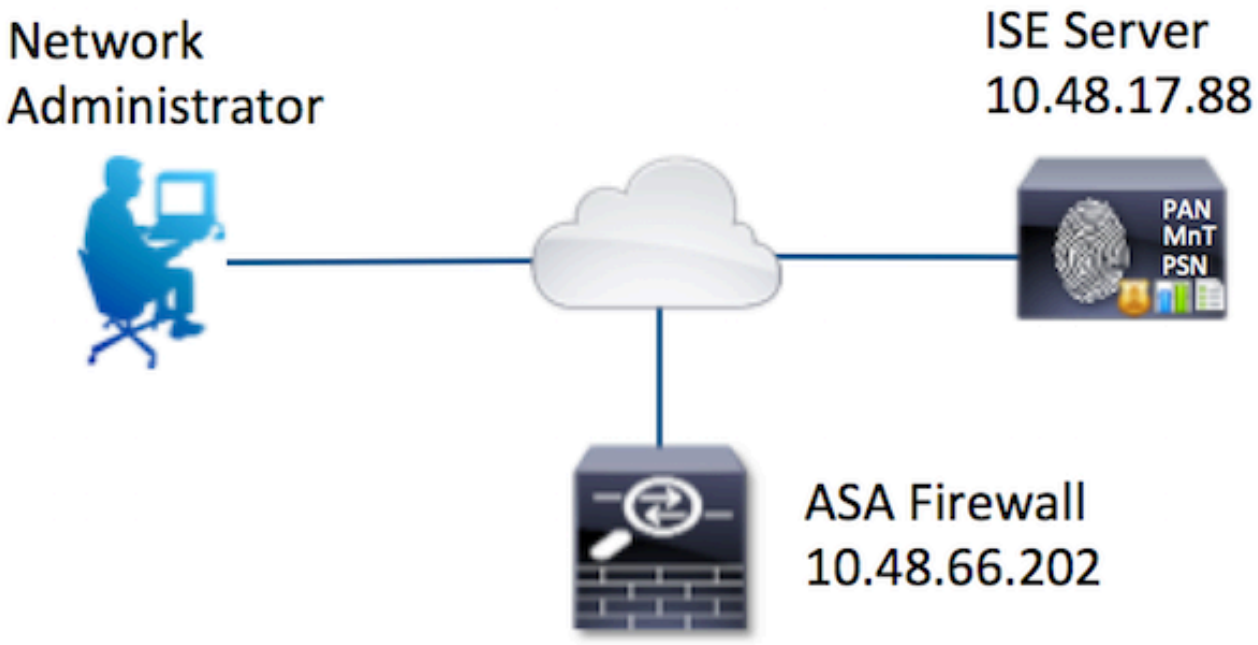
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurer

Le but de la configuration est à :

- Authentifiez l'utilisateur de ssh par l'intermédiaire de la mémoire interne d'identité
- Autorisez l'utilisateur de ssh ainsi il sera placé dans le mode d'exécution privilégié après la procédure de connexion
- Vérifiez et envoyez chaque commande exécutée à ISE pour la vérification

Diagramme du réseau



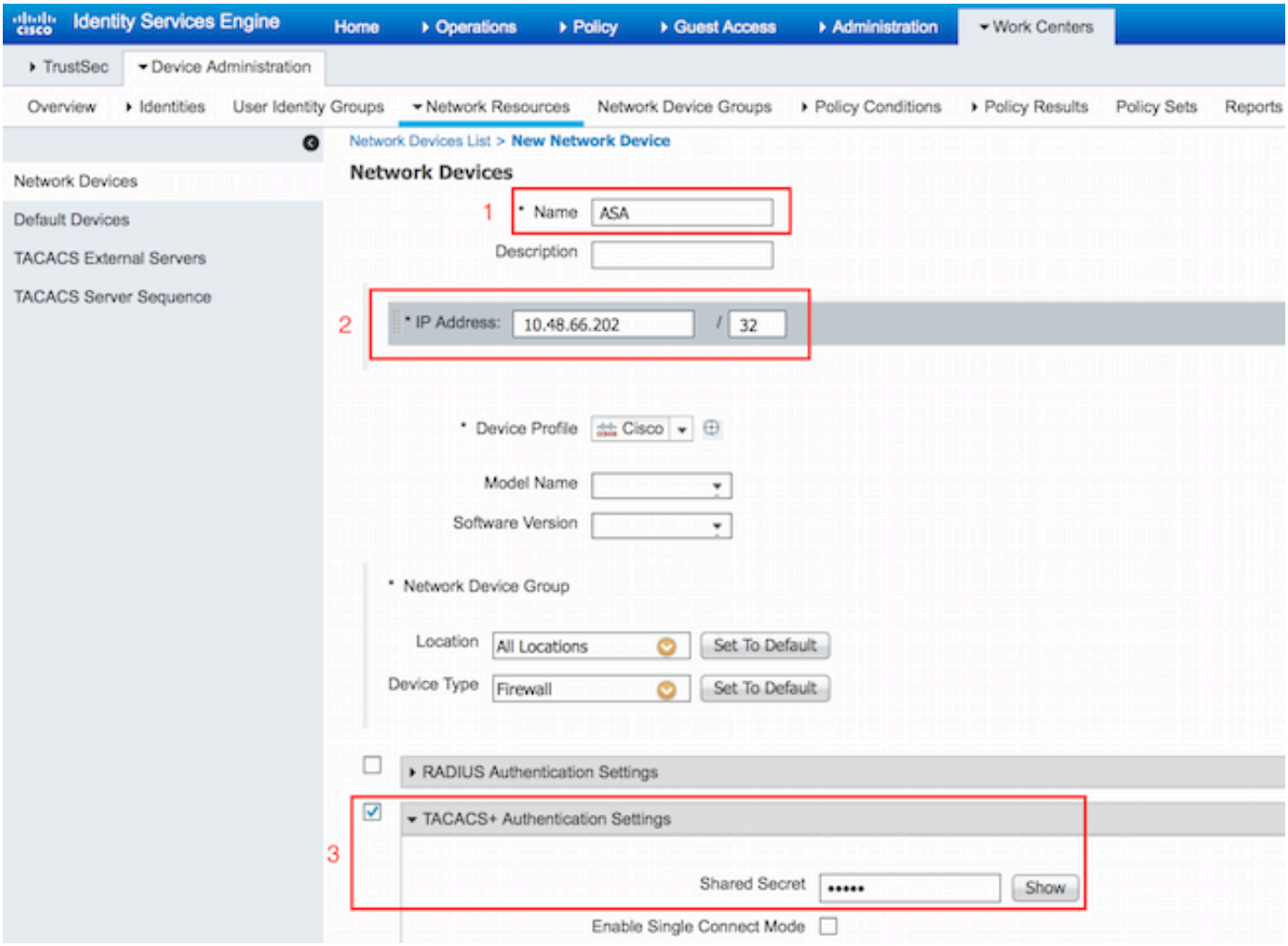
Configurations

Configurez ISE pour l'authentification et l'autorisation

Deux utilisateurs sont créés. **L'administrateur d'**utilisateur est une partie de groupe local d'identité d'**admins de réseau** sur ISE. Cet utilisateur a de pleins privilèges CLI. **L'utilisateur d'**utilisateur est une partie de groupe local d'identité d'**équipe de maintenance du réseau** sur ISE. On permet à cet utilisateur pour faire seulement des commandes show et le ping.

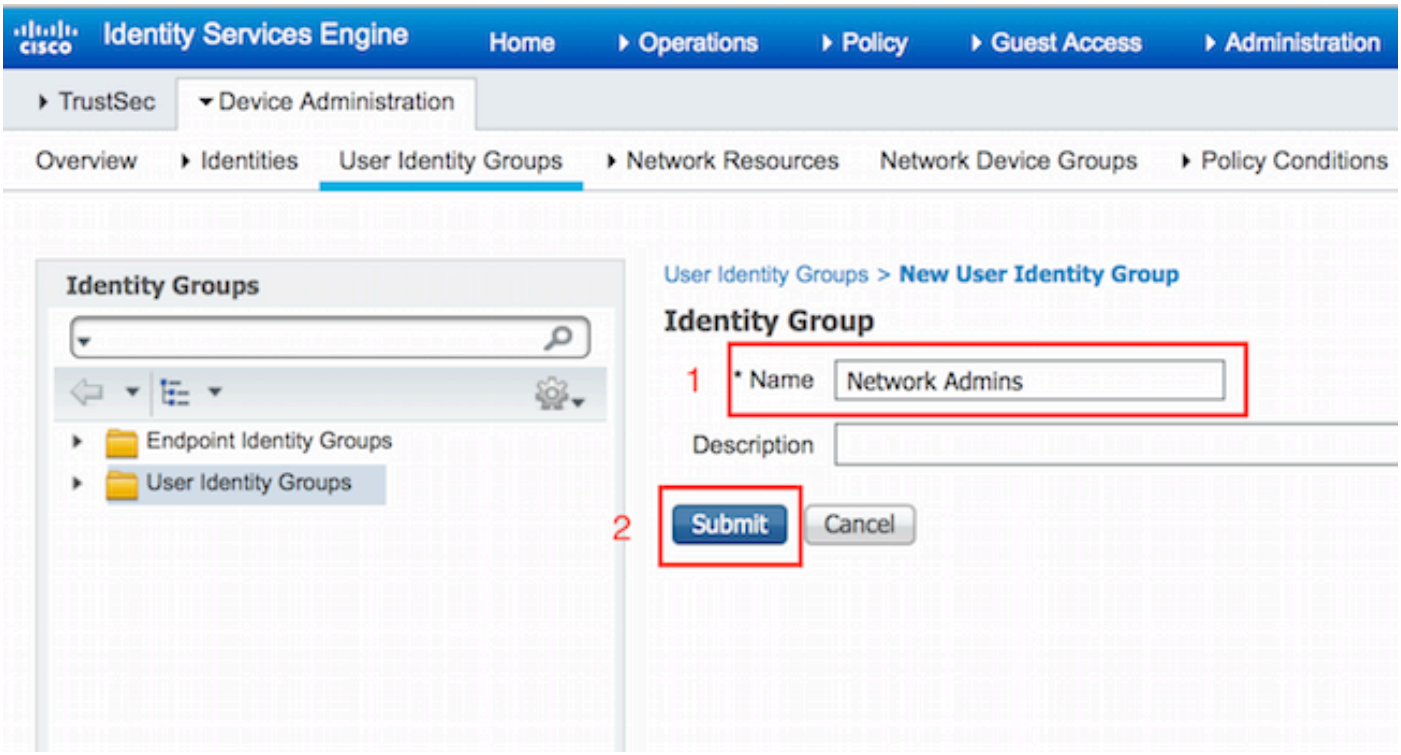
Ajoutez le périphérique de réseau

Naviguez vers les **centres de travail > la gestion de périphérique > les ressources de réseau > les périphériques de réseau.** Cliquez sur **Add**. Fournissez le nom, adresse IP, sélectionnez la case à cocher de **configurations d'authentification TACACS+** et fournissez la clé **secrète partagée**. Sur option le type de périphérique/emplacement peut être spécifié.



Configurer des groupes d'identité de l'utilisateur

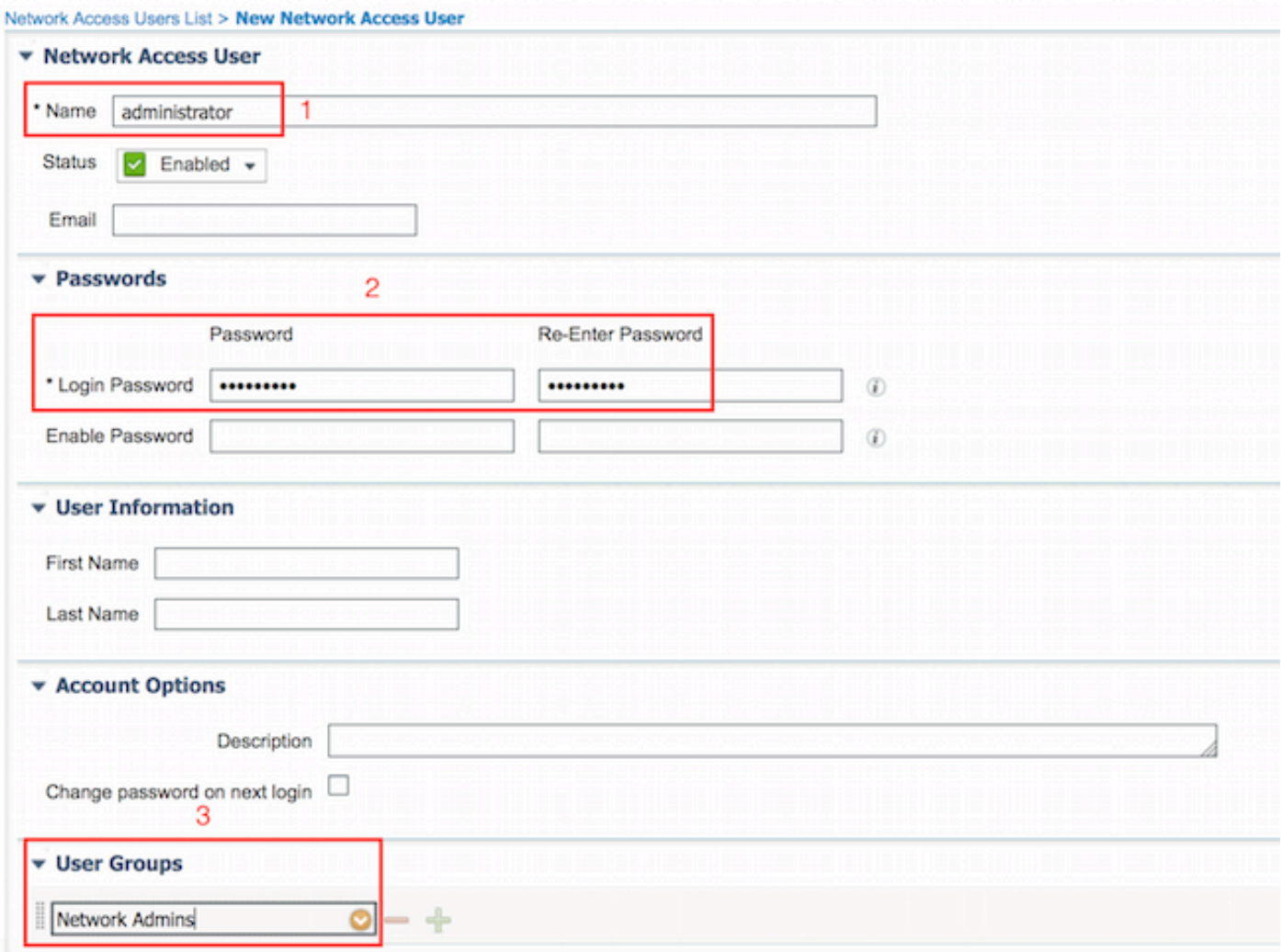
Naviguez vers des **groupes de centres de travail > de gestion > d'identité de l'utilisateur de périphérique.** Cliquez sur **Add**. Fournissez le nom et cliquez sur Submit.



Répétez la même étape au groupe d'identité de l'utilisateur d'**équipe de maintenance de** configure network.

Configurer des utilisateurs

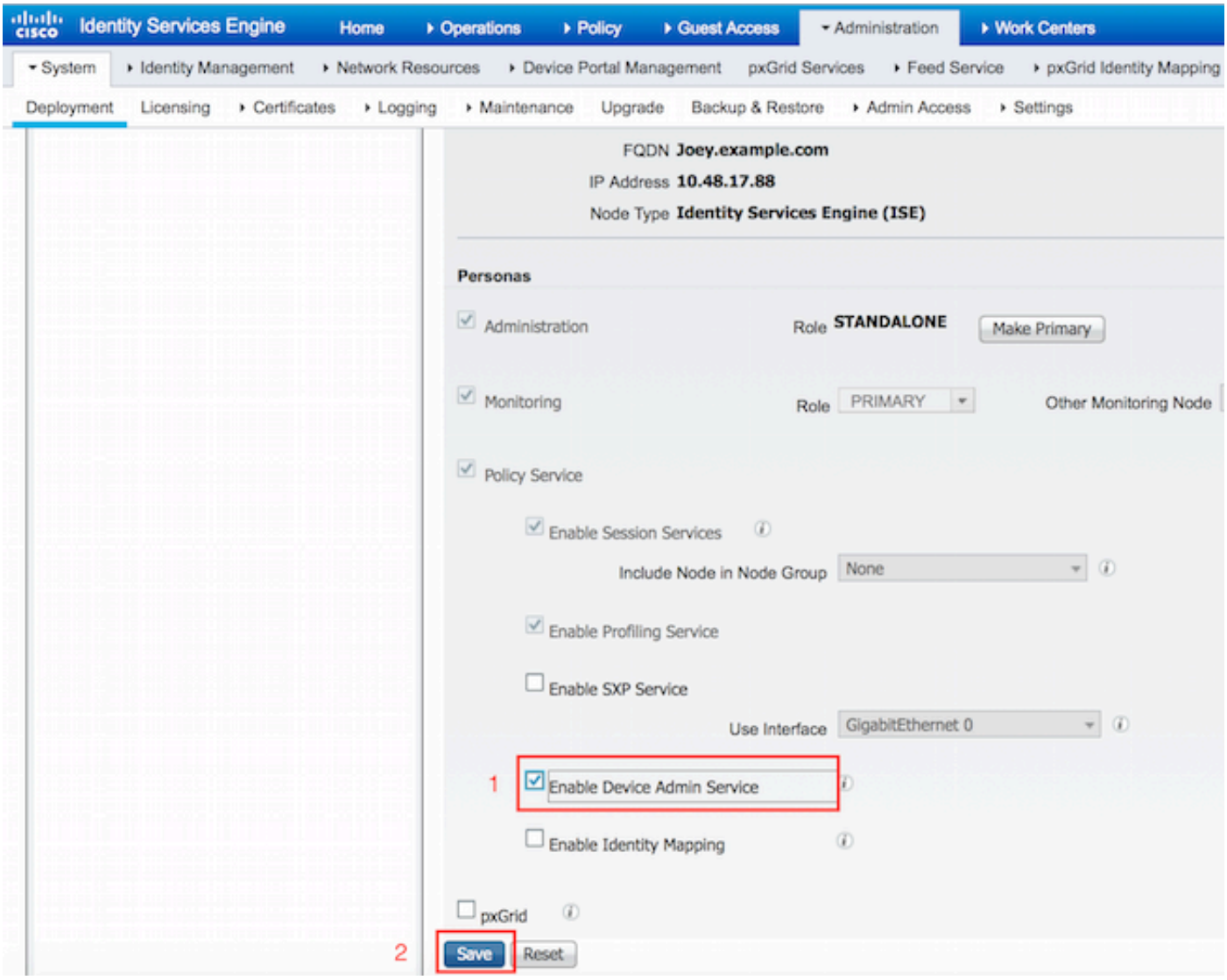
Naviguez vers les **centres de travail > la gestion > les identités > les utilisateurs de périphérique.** Cliquez sur **Add**. Fournissez le nom, le mot de passe de connexion spécifient le groupe d'utilisateurs et cliquent sur Submit.



Répétez les étapes pour configurer l'**utilisateur d'**utilisateur et pour assigner le groupe d'identité de l'utilisateur d'**équipe de maintenance du réseau**.

Service d'admin de périphérique d'enable

Naviguez vers la **gestion > le système > le déploiement.** Select a exigé le noeud. Sélectionnez la case à cocher de **service d'admin de périphérique d'enable** et cliquez sur la **sauvegarde.**

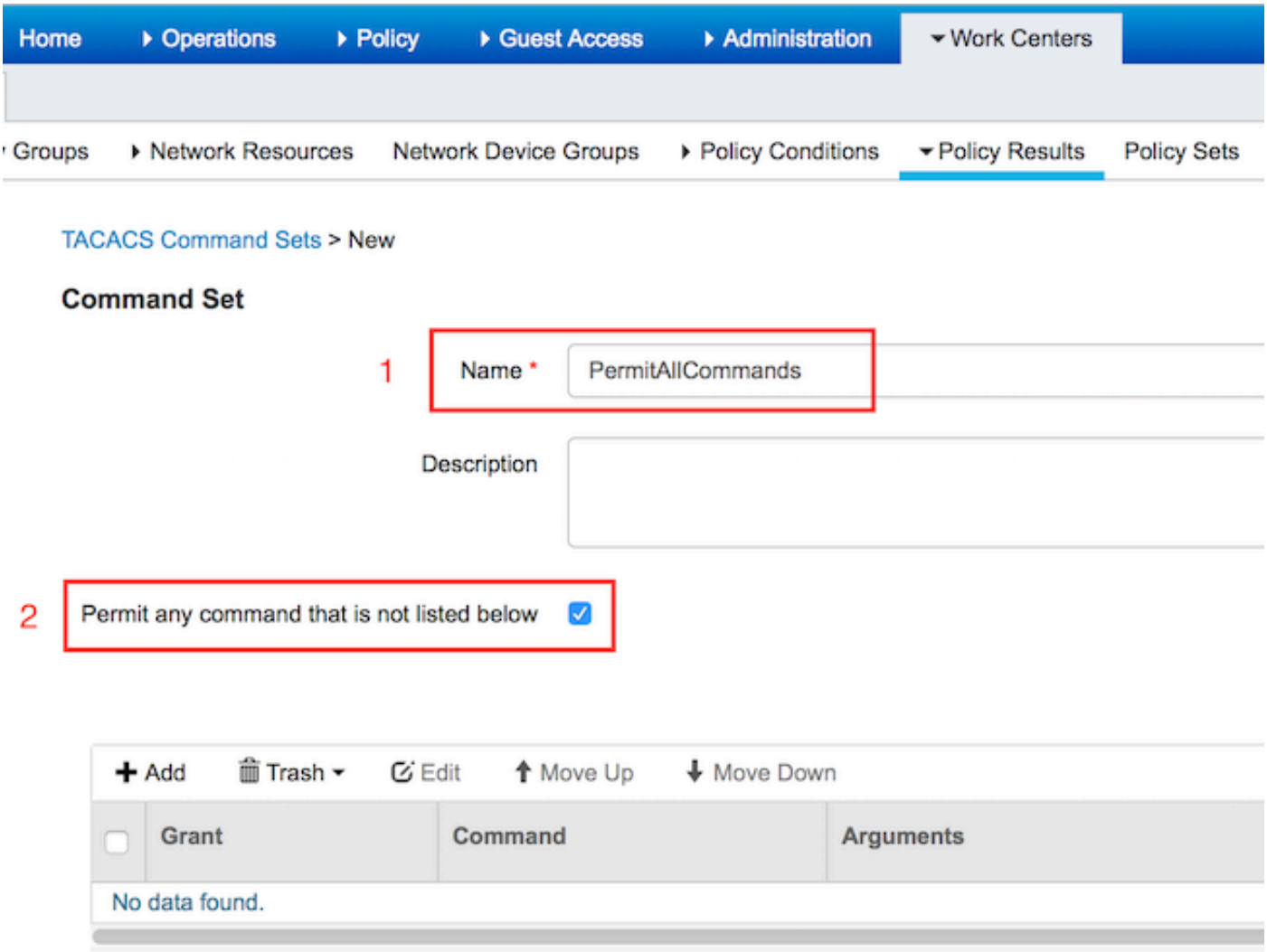


Note: Pour TACACS vous devez faire installer la licence indépendante.

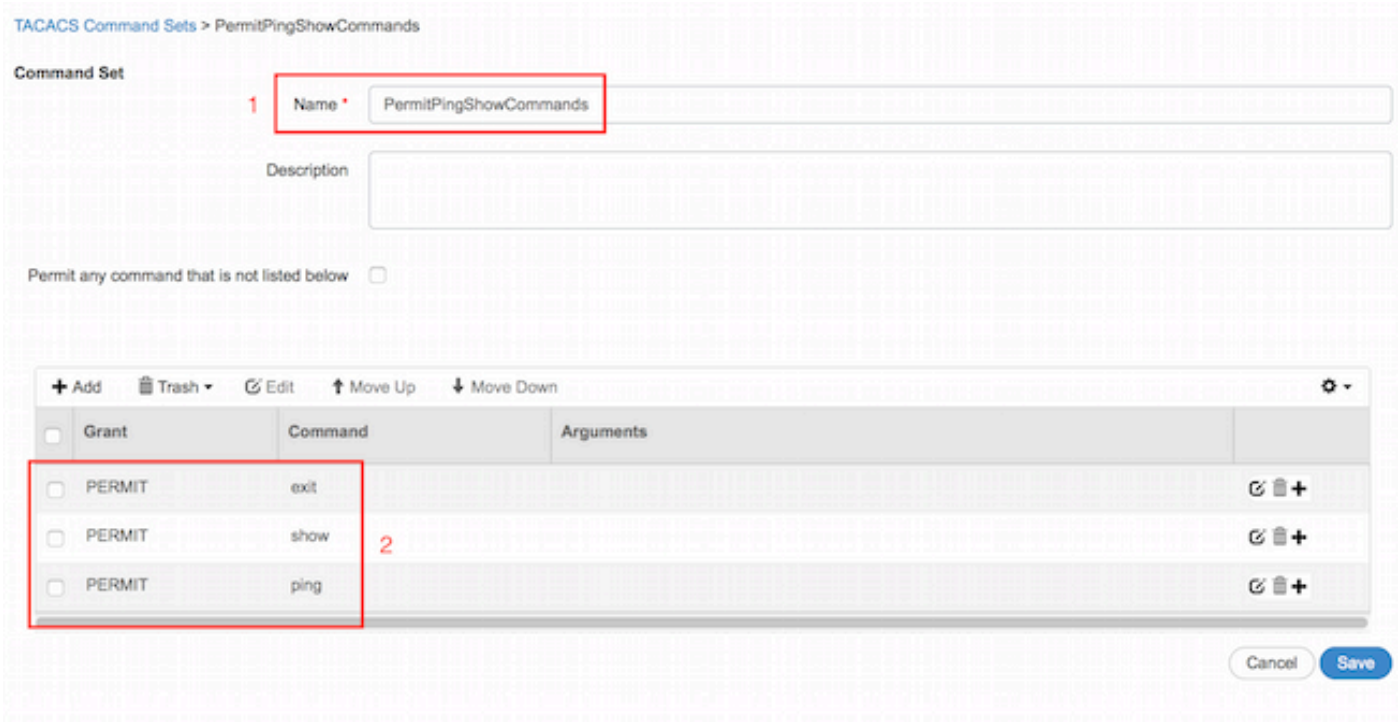
Configurer des positionnements de commande TACACS

Deux positionnements de commande sont configurés. Premier **PermitAllCommands** pour l'utilisateur d'**administrateur** qui permettent toutes les commandes sur le périphérique. En second lieu **PermitPingShowCommands** pour l'utilisateur d'**utilisateur** qui permettent seulement l'exposition et les commandes pings.

1. Naviguez vers les **centres de travail > la gestion > la stratégie de périphérique résulte > des positionnements de commande TACACS.** Cliquez sur **Add**. Fournissez le nom **PermitAllCommands,** sélectionnez l'**autorisation n'importe quelle commande qui n'est pas répertoriée au-dessous de la** case à cocher et cliquez sur Submit**.**

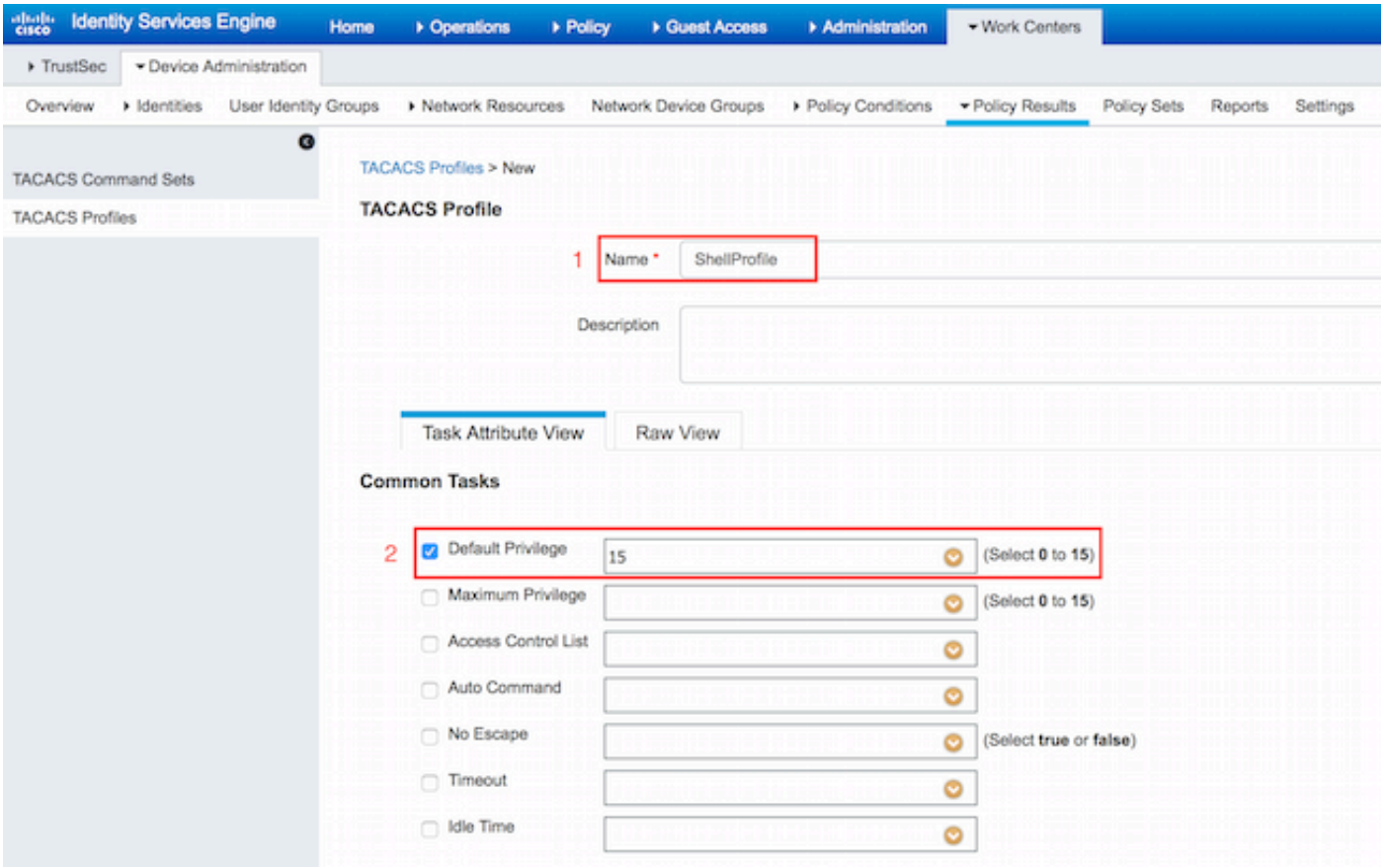


2. Naviguez vers les **centres de travail > la gestion > la stratégie de périphérique résulte > des positionnements de commande TACACS.** Cliquez sur **Add**. Fournissez le nom **PermitPingShowCommands,** cliquez sur Add et permettez l'**exposition, le ping** et les **commandes exit**. Par défaut si les arguments sont blanc de gauche, tous les arguments sont inclus. Cliquez sur **Submit**.



Configurer le profil TACACS

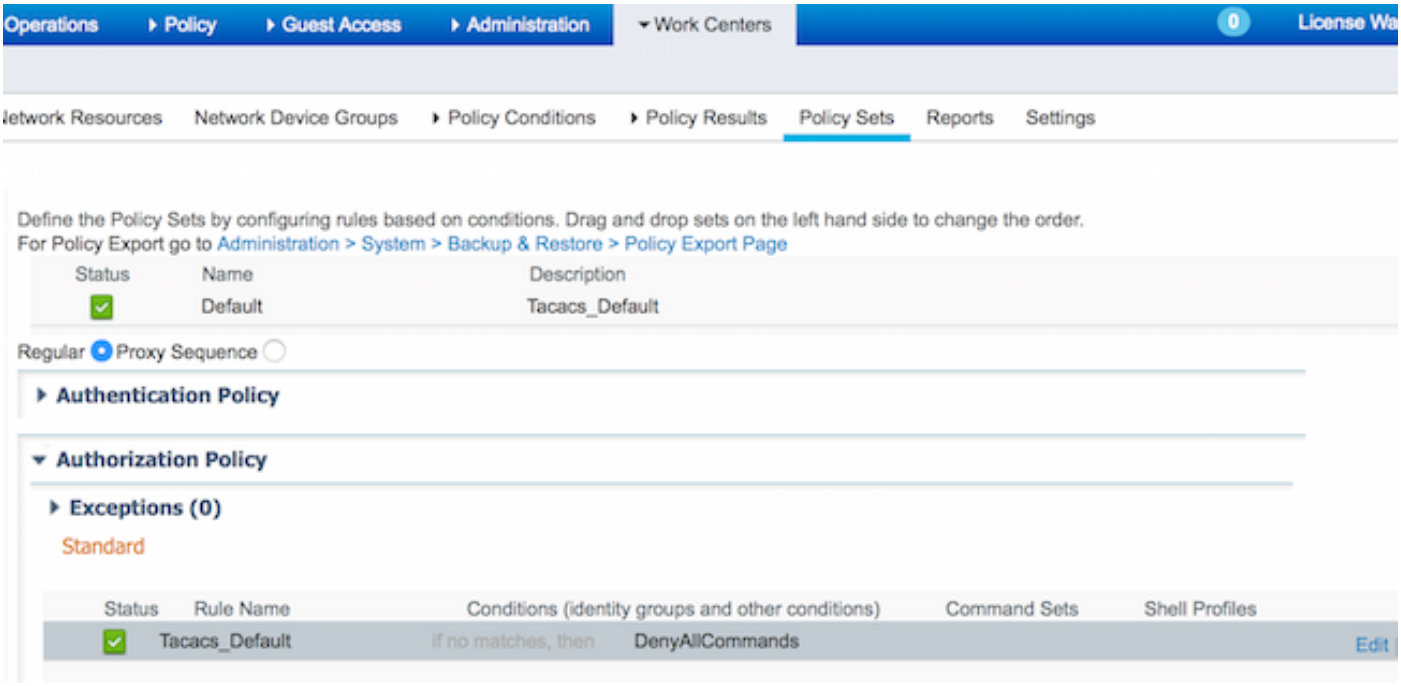
Le profil simple TACACS sera configuré. L'application réelle de commande sera faite par l'intermédiaire des positionnements de commande. Naviguez vers les **centres de travail > la gestion > la stratégie de périphérique résulte > des profils TACACS.** Cliquez sur **Add**. Fournissez le nom **ShellProfile,** sélectionnez la case à cocher de **privilège par défaut** et écrivez la valeur de 15. Cliquez sur **Submit**.



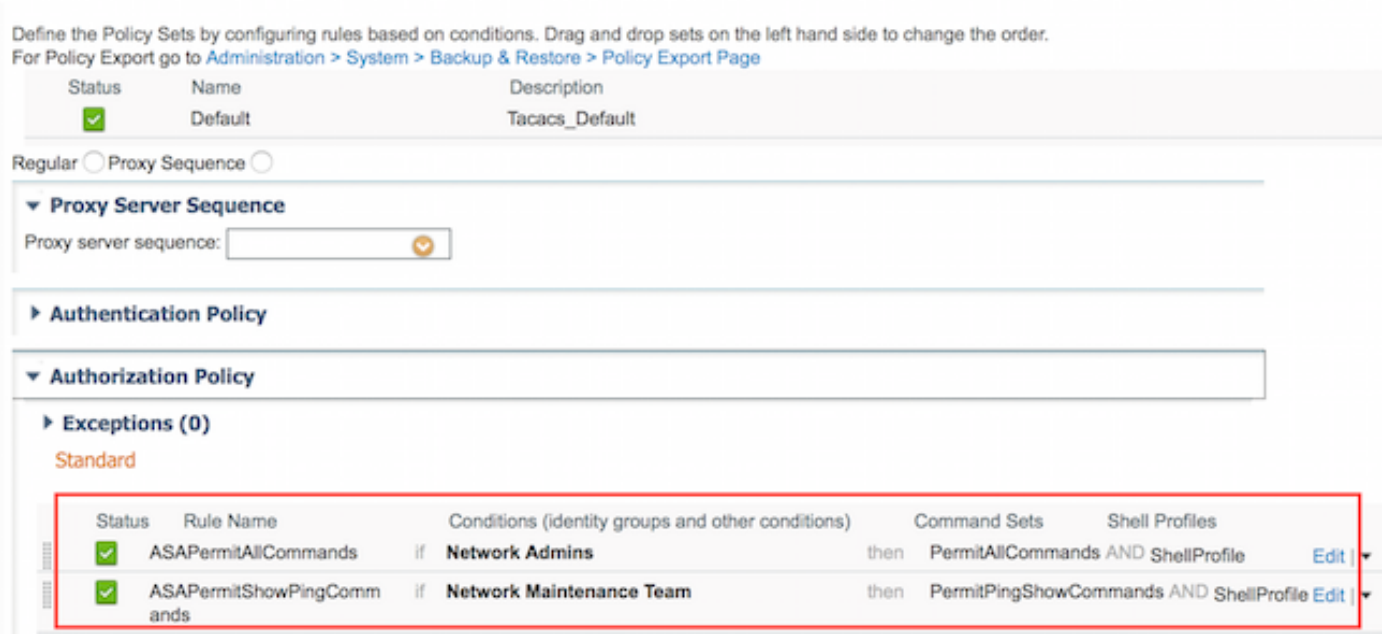
Configurer la stratégie d'autorisation TACACS

La stratégie d'authentification par les points par défaut à All_User_ID_Stores, qui inclut la mémoire locale aussi bien, ainsi à elle est laissée inchangée.

Naviguez vers des **positionnements de centres de travail > de gestion > de stratégie de périphérique > la stratégie de par défaut > d'autorisation > éditent > nouvelle règle d'insertion ci-dessus.**



Le rulesare de deux autorisations configuré, la première règle assigne le profil **ShellProfile** TACACS et la commande **PermitAllCommands** réglé basé sur l'adhésion à des associations d'identité de l'utilisateur d'**admins de réseau**. En second lieu la règle assigne le profil **ShellProfile** TACACS et la commande **PermitPingShowCommands** réglé basé sur l'adhésion à des associations d'identité de l'utilisateur d'**équipe de maintenance du réseau**.



Configurez le Pare-feu de Cisco ASA pour l'authentification et l'autorisation

1. Créez un utilisateur local avec le plein privilège pour le retour avec la commande de **nom**

d'utilisateur comme affiché ici

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. Définissez le serveur TACACS ISE, spécifiez l'interface, l'IP address de protocole, et la clé de **tacacs**.

```
ciscoasa(config)# username cisco password cisco privilege 15
```

> **Note**: La clé de serveur devrait apparier celui définissent sur le serveur ISE plus tôt.

3. Testez l'accessibilité de serveur TACACS avec la commande d'**AAA de** test comme affichée.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

La sortie de la commande précédente prouve que le serveur TACACS est accessible et l'utilisateur a été avec succès authentifié.

4. Configurez l'authentification pour des autorisations de ssh, d'autorisation EXEC et de commande comme affiché ci-dessous. Avec l'automatique-**enable d'authentification-serveur d'exécutif d'autorisation d'AAA** vous serez placé dans le mode d'exécution privilégié automatiquement.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

> **Note**: Avec les commandes ci-dessus, l'authentification est faite sur ISE, utilisateur est placée directement dans le mode privilège et l'autorisation de commande a lieu.

5. Autorisez chut sur l'interface de mgmt.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

Vérifiez

Vérification de Pare-feu de Cisco ASA

1. Ssh au Pare-feu ASA comme **administrateur** qui appartient au groupe d'identité de l'utilisateur d'accès complet. Le groupe d'**admins de réseau** est tracé à la commande de **ShellProfile** et de **PermitAllCommands** réglée sur l'ISE. Essayez d'exécuter n'importe quelle commande d'assurer l'accès complet.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
```

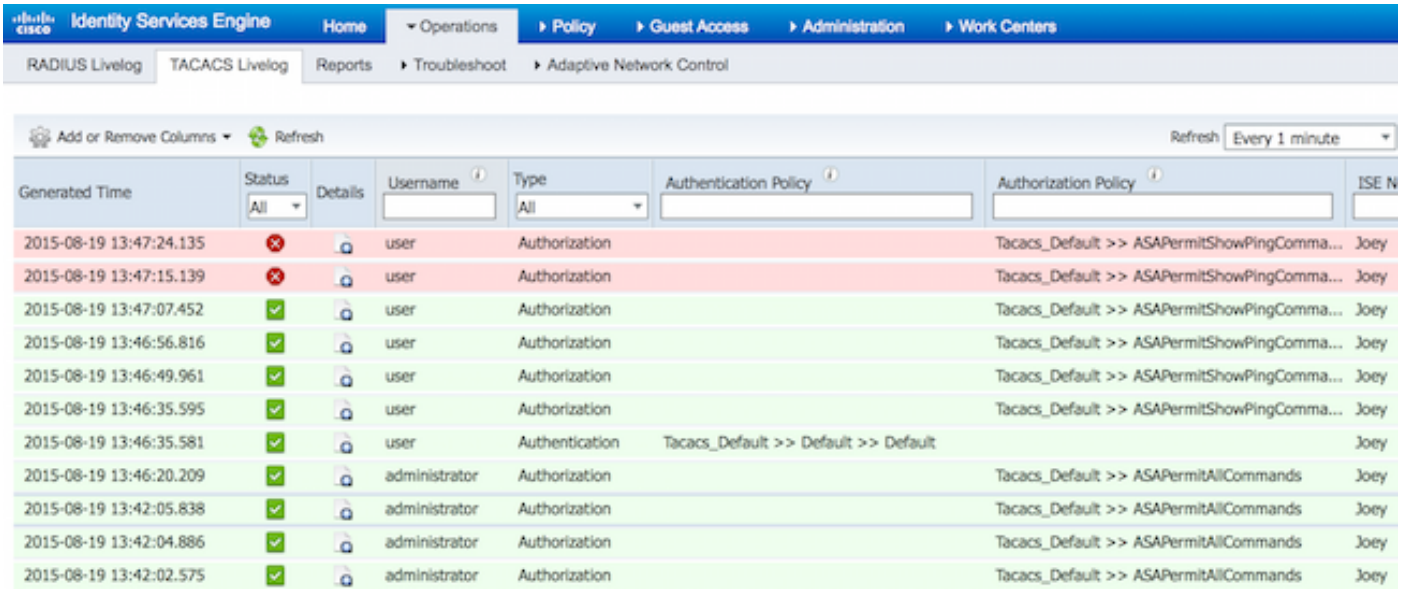
```
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
ciscoasa#
```

2. Ssh au Pare-feu ASA comme **utilisateur** qui appartient au groupe limité d'identité de l'utilisateur d'accès. Le groupe de **maintenance du réseau** est tracé à la commande de **ShellProfile** et de **PermitPingShowCommands** réglée sur l'ISE. Essayez d'exécuter n'importe quelle commande de s'assurer que seulement l'exposition et les commandes pings peuvent être émises.

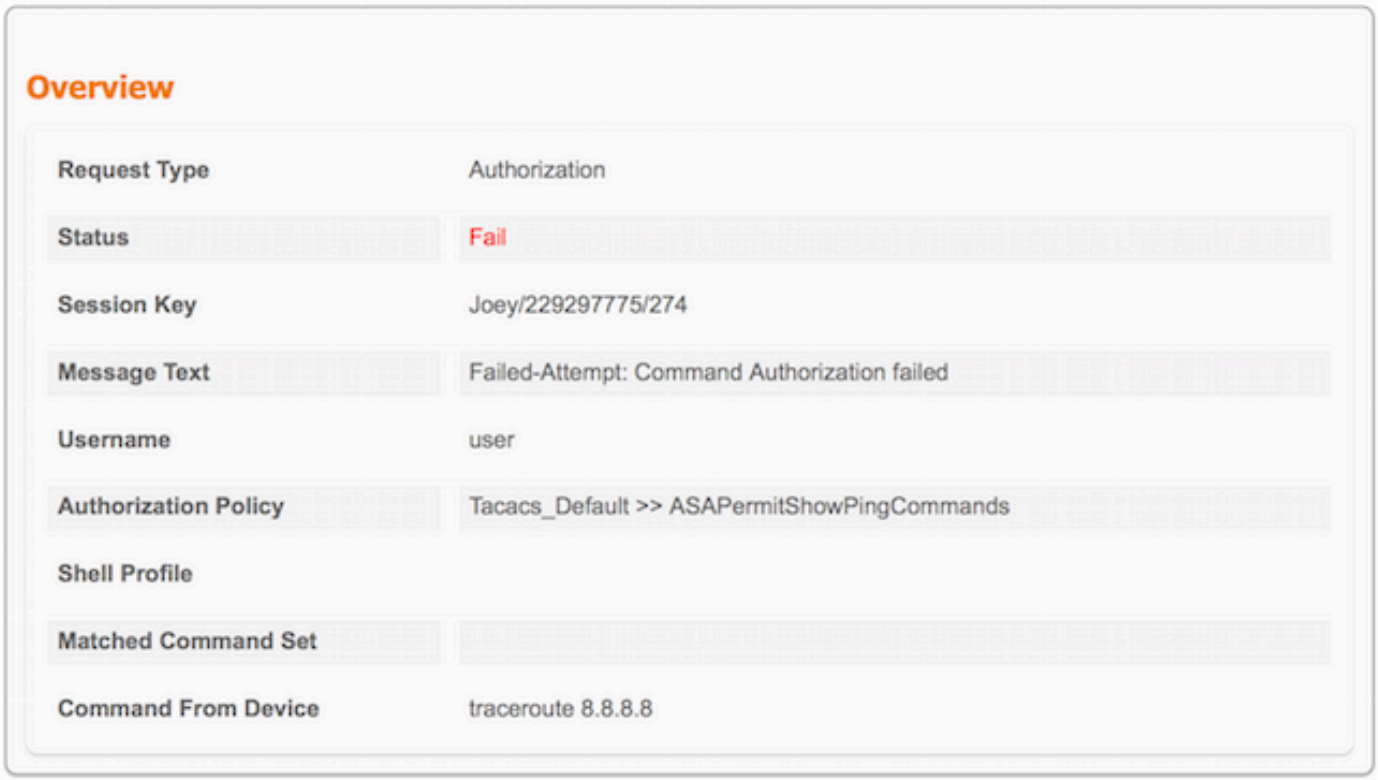
```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

Vérification ISE 2.0

1. Naviguez vers des **exécutions > TACACS Livelog.** Assurez-vous que des tentatives faites ci-dessus sont vues.



2. Cliquez sur en fonction les détails d'un des états rouges, plus tôt exécuté par commande défectueux peut être vu.



Dépanner

Erreur : Essai raté : L'autorisation de commande a manqué

Vérifiez les attributs de SelectedCommandSet pour vérifier que les positionnements prévus de commande ont été sélectionnés par la stratégie d'autorisation

Informations connexes

Support et documentation techniques - Cisco Systems

Notes de mise à jour ISE 2.0

Guide d'installation du matériel ISE 2.0

Guide de mise à jour ISE 2.0

ACS au guide d'outil de transfert ISE

Guide d'intégration de Répertoire actif ISE 2.0

Guide de l'administrateur d'engine ISE 2.0