Configuration de TACACS+ avec l'interface Gigabit Ethernet 1 ISE

Table des matières

Introduction

Ce document décrit la configuration ISE TACACS+ avec l'interface Gigabit Ethernet 1 où le routeur et le commutateur fonctionnent comme des périphériques réseau.

Informations générales

Cisco ISE prend en charge jusqu'à 6 interfaces Ethernet. Il ne peut avoir que trois liaisons, liaison 0, liaison 1 et liaison 2. Vous ne pouvez pas modifier les interfaces qui font partie d'une liaison ou

modifier le rôle de l'interface dans une liaison.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Connaissances de base en réseau
- Cisco Identity Service Engine.

Composants utilisés

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

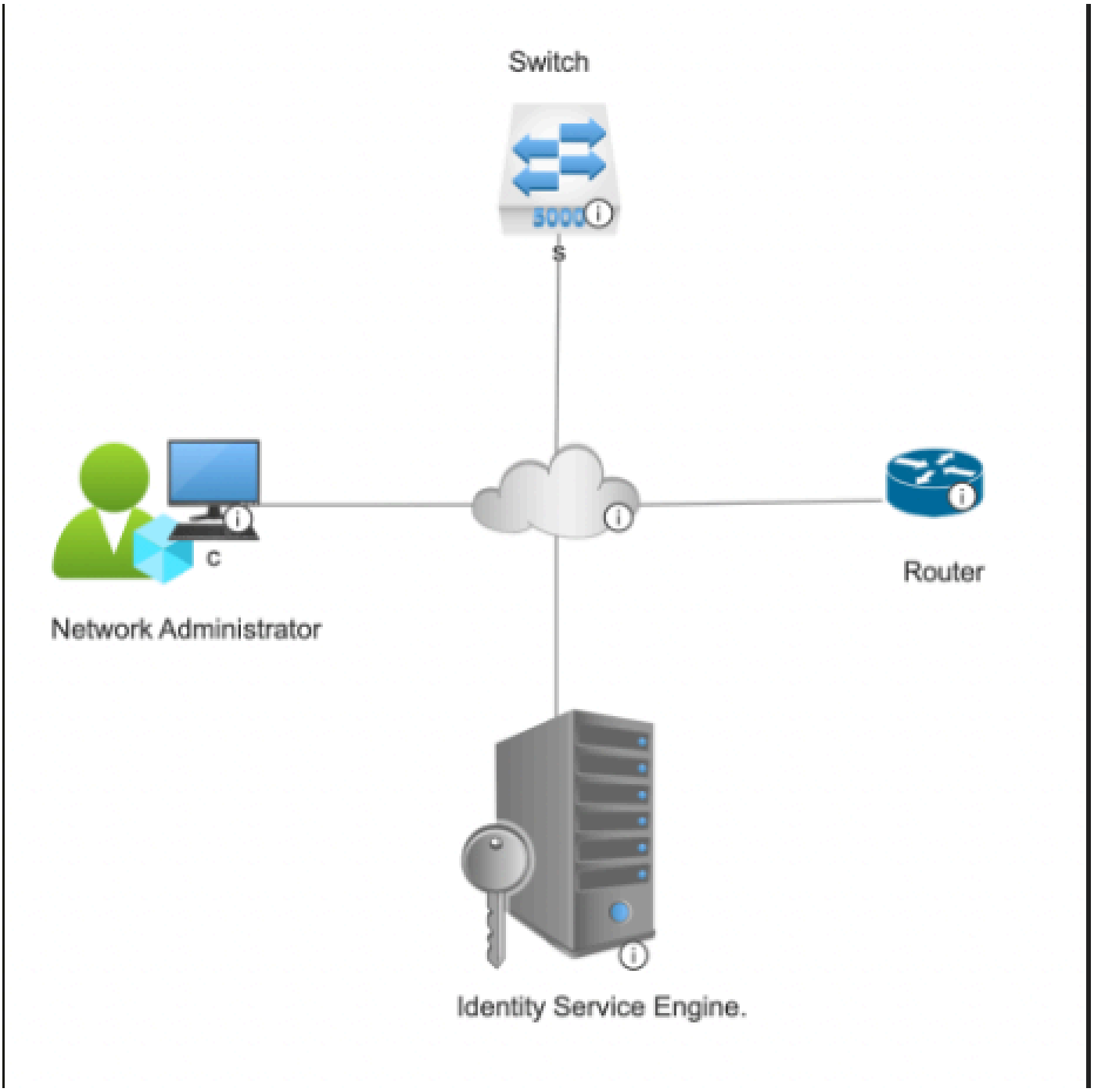
- Cisco Identity Service Engine v3.3
- Logiciel Cisco IOS® version 17.x
- Commutateur Cisco C9200

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.

Configurer

L'objectif de la configuration est de : Configurez Gigabit Ethernet 1 d'ISE pour TACACS+ et authentifiez le commutateur et le routeur avec TACACS+ avec ISE comme serveur d'authentification.

Diagramme du réseau

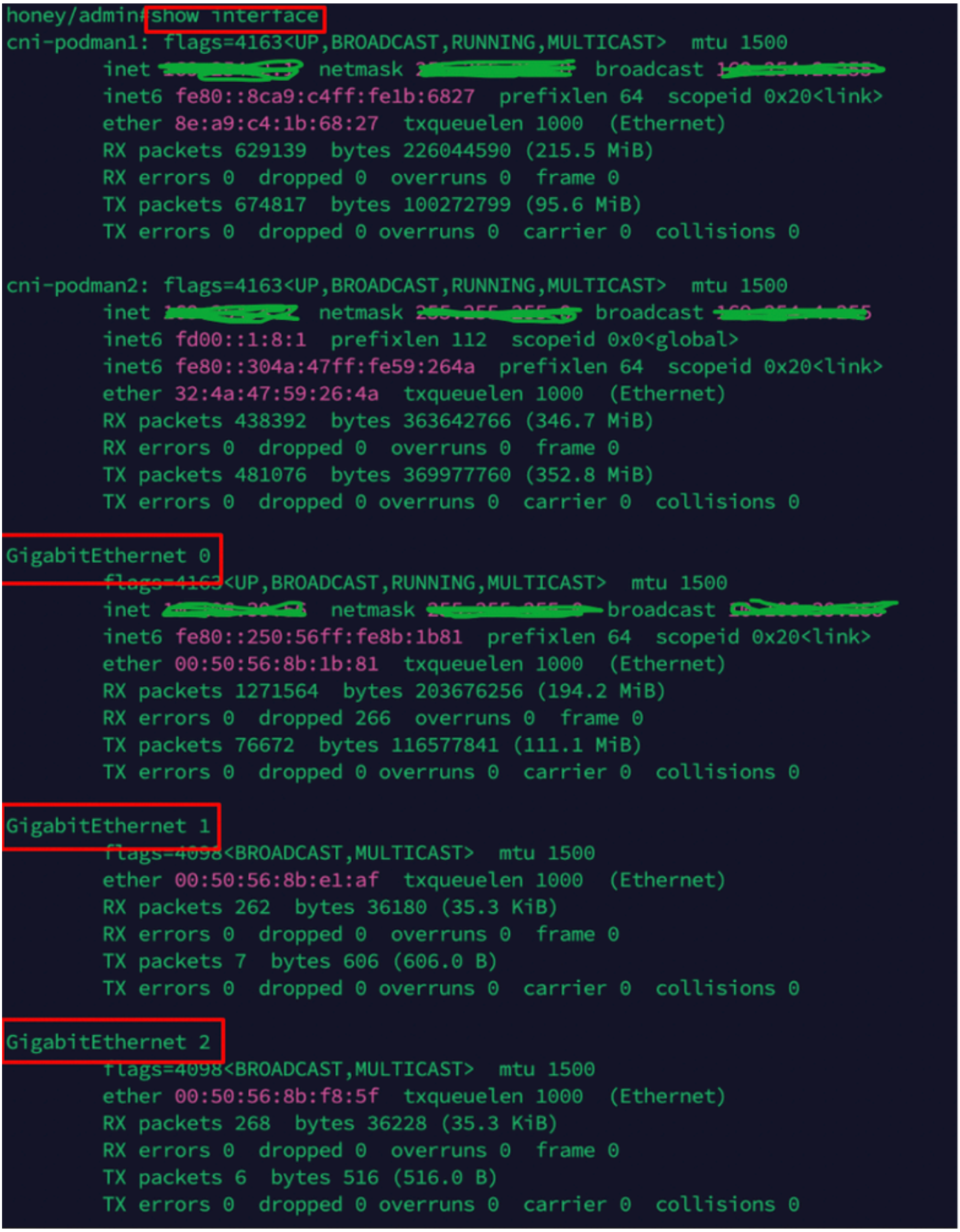


Topologie du réseau

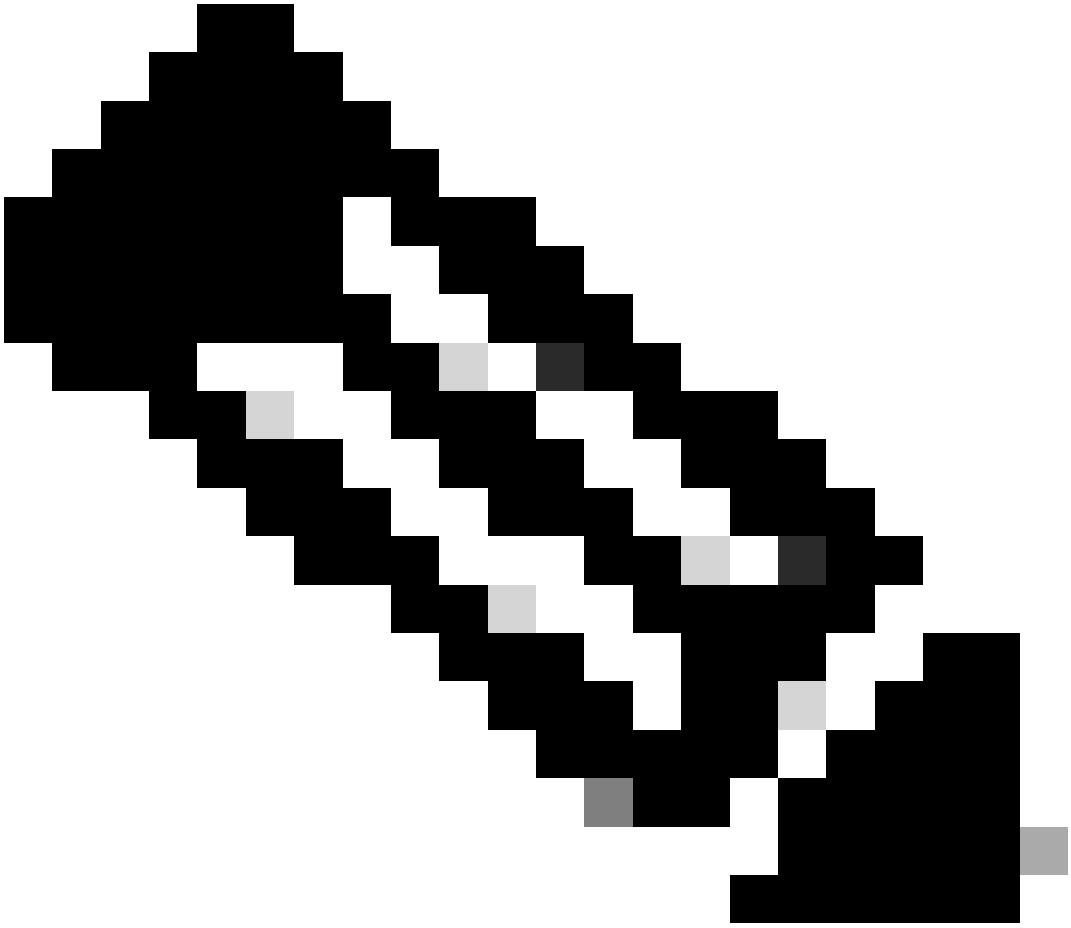
Configuration de Identity Services Engine pour TACACS+

Configuration de l'adresse IP pour l'interface Gigabit Ethernet 1 dans ISE

1. Connectez-vous à la CLI du noeud PSN ISE où Device admin est activé et vérifiez les interfaces disponibles à l'aide de la commande show interface :



Vérification des interfaces dans ISE



Remarque : Dans cette configuration, seules trois interfaces sont configurées dans ISE, avec un accent sur l'interface Gigabit Ethernet 1. La même procédure peut être appliquée pour configurer l’adresse IP de toutes les interfaces. Par défaut, ISE prend en charge jusqu'à six interfaces Gigabit Ethernet.

---

2. À partir de l’interface de ligne de commande du même noeud PSN, attribuez une adresse IP à l’interface Gigabit Ethernet 1 à l’aide des commandes suivantes :

nomhôte#configure t

nomhôteInse/admin(config)#interface Gigabit Ethernet 1

hostnameofise/admin(config-GigabitEthernet-1)# <adresse ip> <masque de réseau de sous-réseau> % La modification de l’adresse IP peut entraîner le redémarrage des services ise

Poursuivre le changement d'adresse IP ?

Poursuivre ? [oui, non] oui

3. L’exécution de l’étape 2 entraîne le redémarrage des services de noeud ISE. Pour vérifier l'état des services ISE, exécutez la commande show application status ise et assurez-vous que l'état des services est en cours d'exécution selon cette capture d'écran :

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          1739169
Database Server                        running          102 PROCESSES
Application Server                     running          1755746
Profiler Database                      running          1746379
ISE Indexing Engine                    running          1757121
AD Connector                           running          1759148
M&T Session Database                   running          1752122
M&T Log Processor                      running          1755926
Certificate Authority Service          running          1759026
EST Service                            running          1786647
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          1743222
ISE API Gateway Database Service       running          1745409
ISE API Gateway Service                running          1750887
ISE pxGrid Direct Service              running          1874179
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          1760519
ISE Prometheus Service                 running          1762540
ISE Grafana Service                    running          1765779
ISE MNT LogAnalytics Elasticsearch     running          1768218
ISE Logstash Service                   running          1773207
ISE Kibana Service                     running          1774914
ISE Native IPSec Service               running          1779658
MFC Profiler                           running          1932013
```

Vérification de l'état du service ISE

4. Vérifiez l’adresse IP de l’interface Gig1 à l’aide de la commande show interface :

V

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 633876  bytes 228753800 (218.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 680052  bytes 102100762 (97.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 503576  bytes 516105026 (492.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 595701  bytes 383404526 (365.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1387052  bytes 213478717 (203.5 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 136494  bytes 261900250 (249.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:e1af  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 5165  bytes 1072036 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2260 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Vérification de l'adresse IP de l'interface ISE Gig2 à partir de CLI

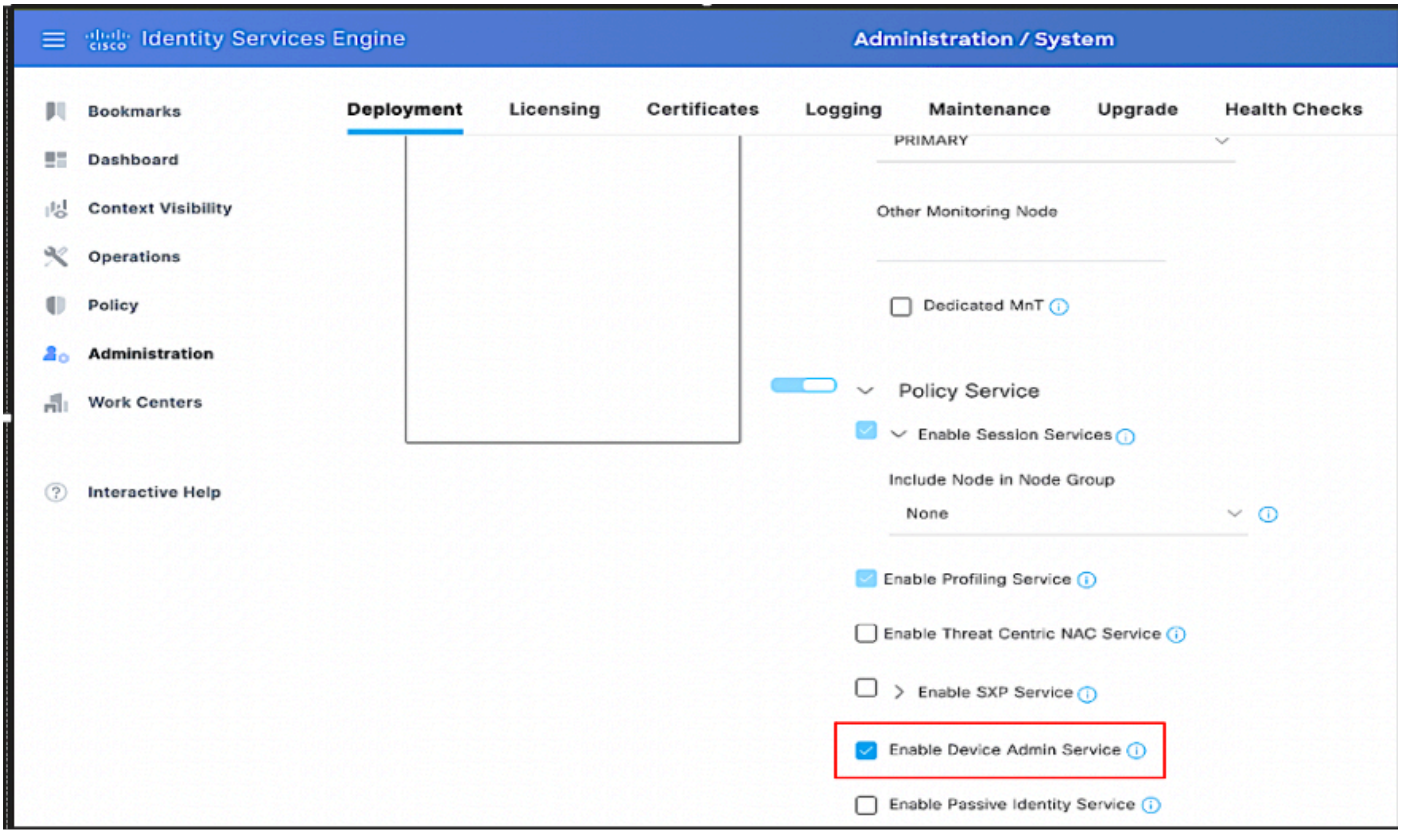
5. Vérifiez la tolérance du port 49 dans le noeud ISE en utilisant la commande show ports | inc 49, commande :

```
honey/admin#show ports | include 49
        tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, [redacted]:49, [redacted]:49,
```

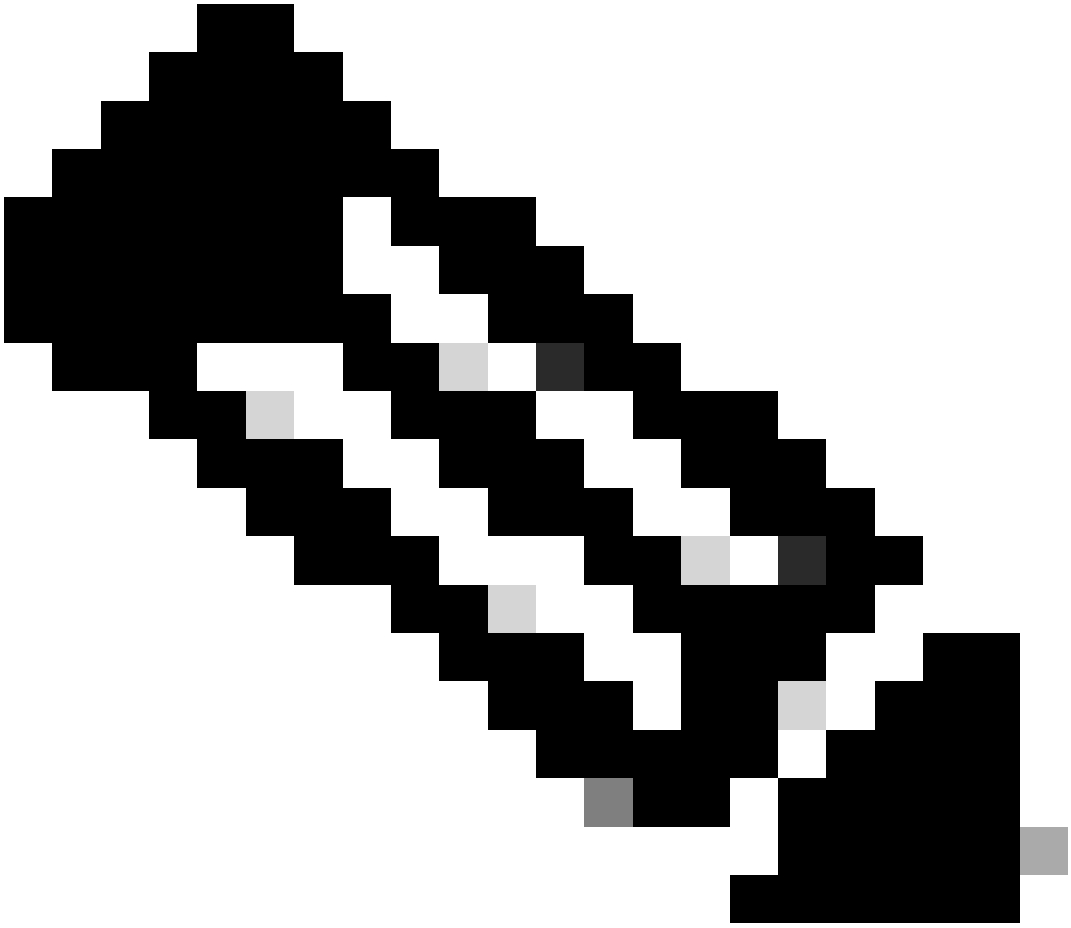
vérification de l'autorisation port 49 dans ISE

Activer l'administration des périphériques dans ISE

Accédez à GUI of ISE > Administration > Deployment > Sélectionnez le noeud PSN, puis cochez Enable Device admin service:



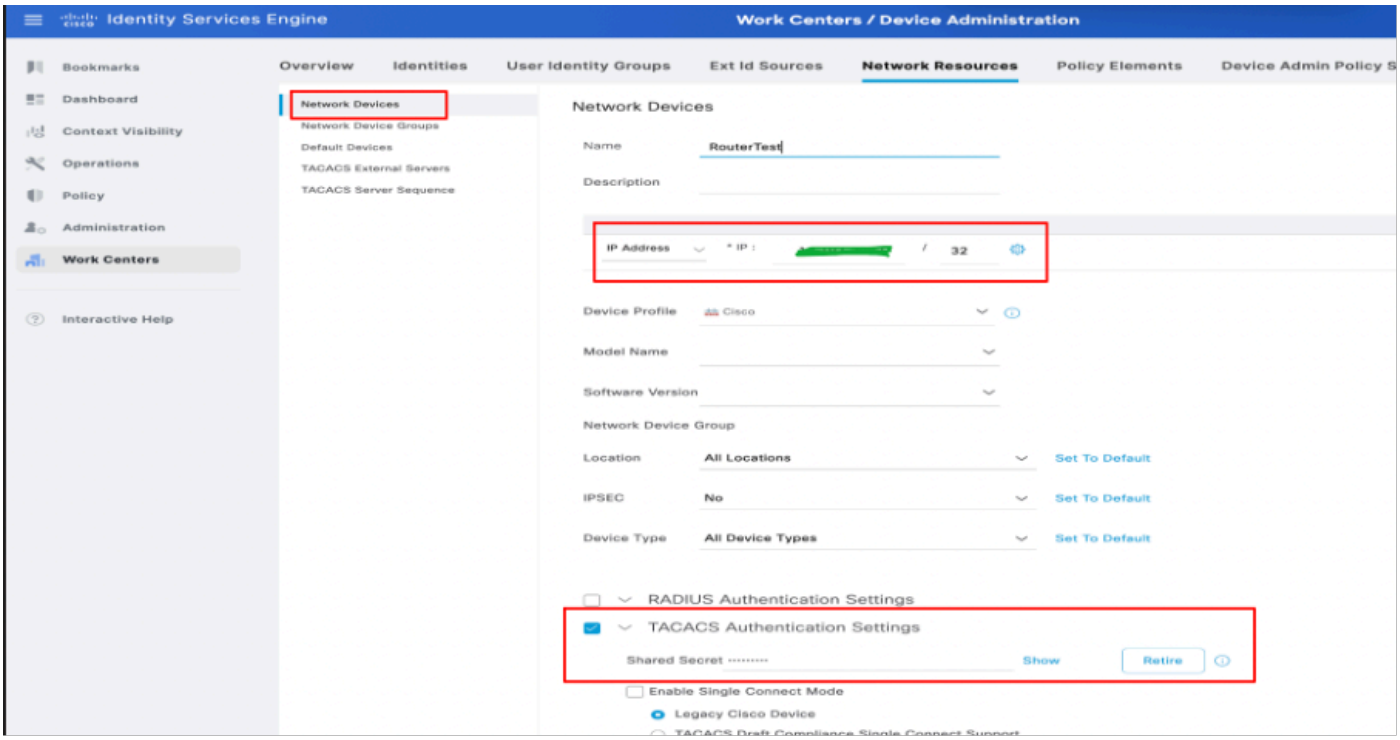
Activation du service d'administration des périphériques dans ISE



Remarque : Pour activer le service Device Admin, une licence Device Administration est requise.

Ajouter un périphérique réseau dans ISE

1. 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 fournissez la clé secrète partagée.



Configuration du périphérique réseau dans ISE

2. Suivez la procédure ci-dessus pour ajouter tous les périphériques réseau requis pour l'authentification TACACS.

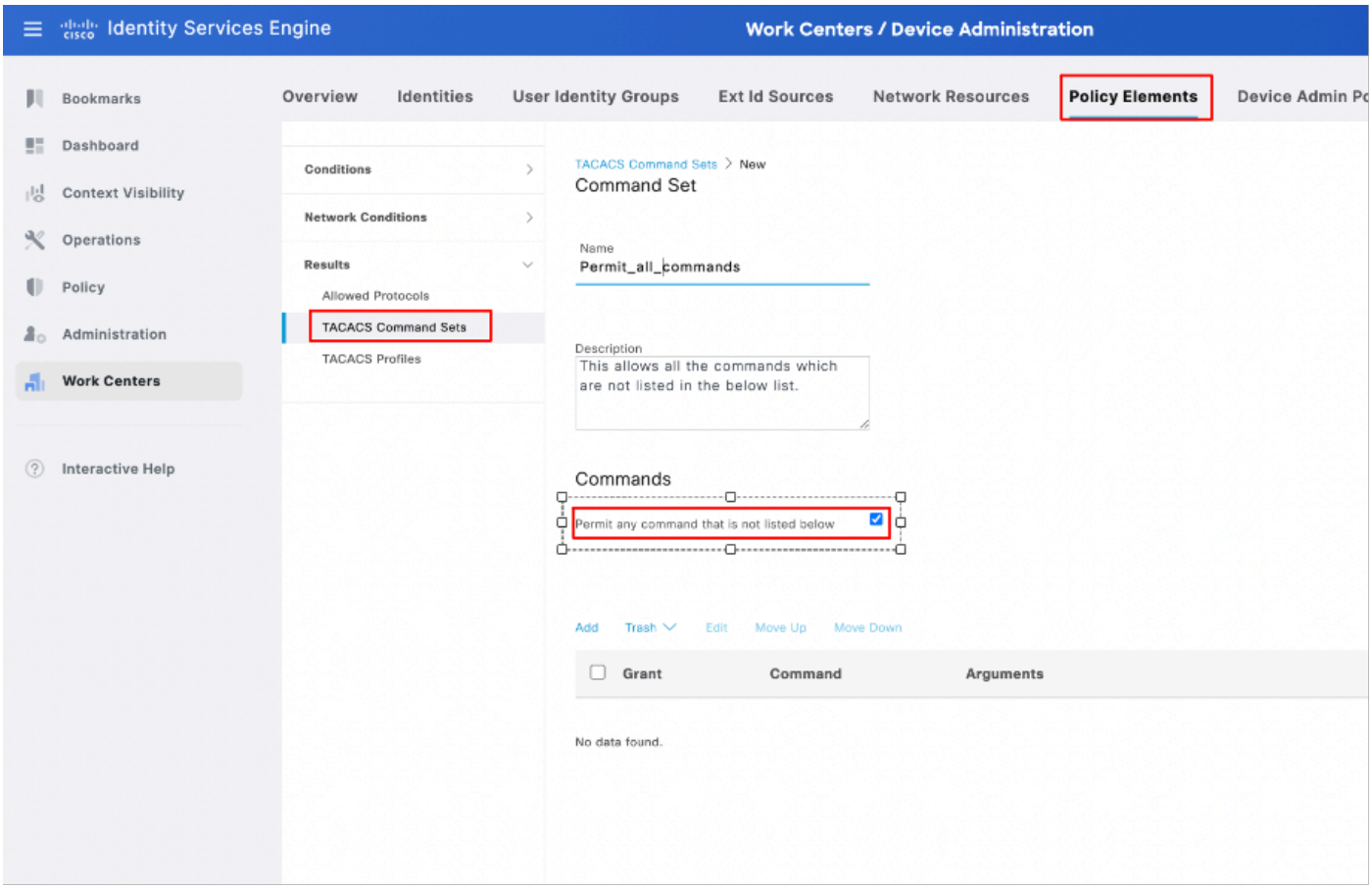
Configuration des jeux de commandes TACACS+

Deux jeux de commandes sont configurés pour cette démonstration :

Permit_all_commands, est attribué à l'utilisateur admin et autorise toutes les commandes sur le périphérique.

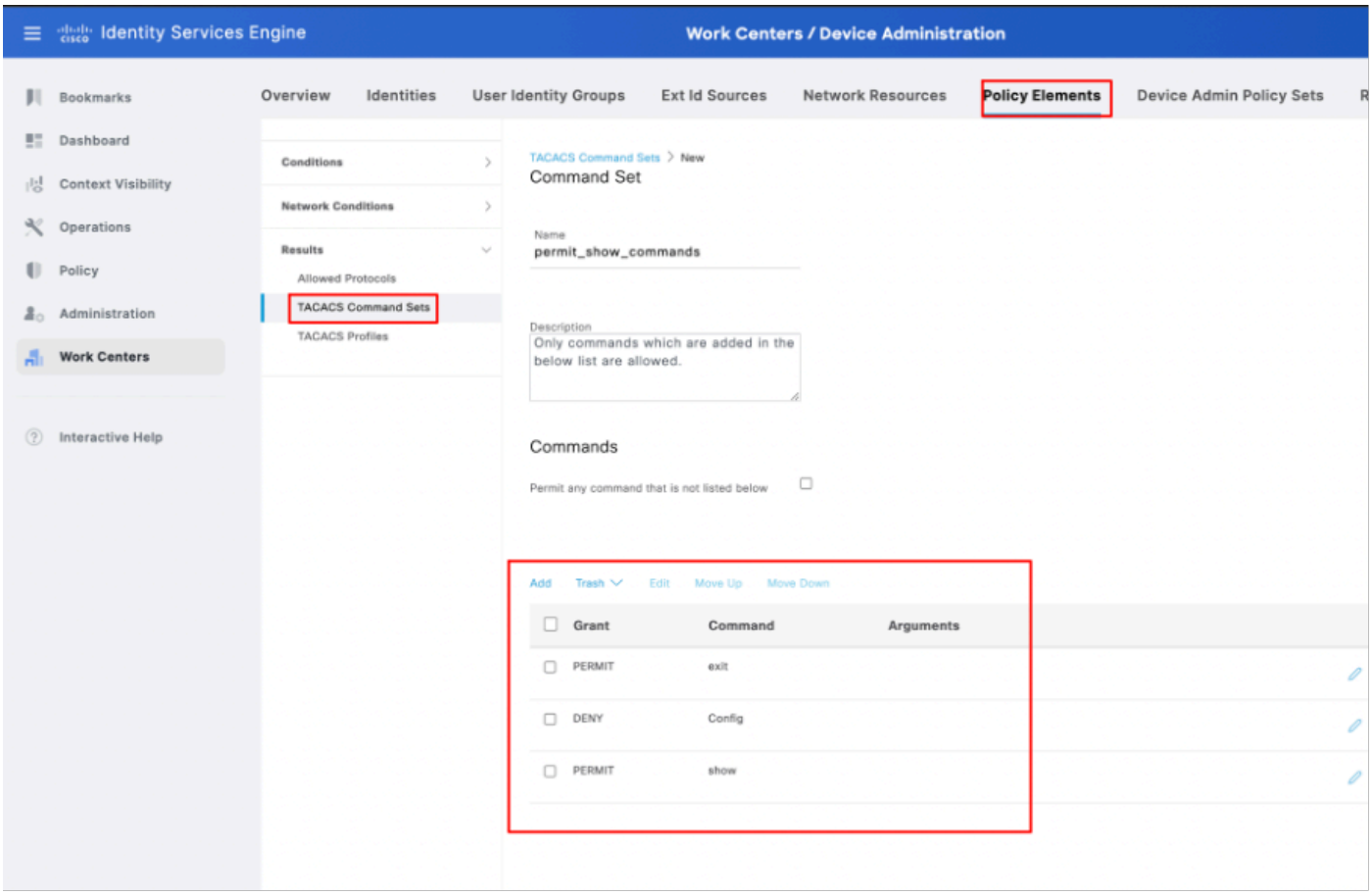
permit_show_commands, est attribué à un utilisateur et autorise uniquement les commandes show

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



Configuration des jeux de commandes dans ISE

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

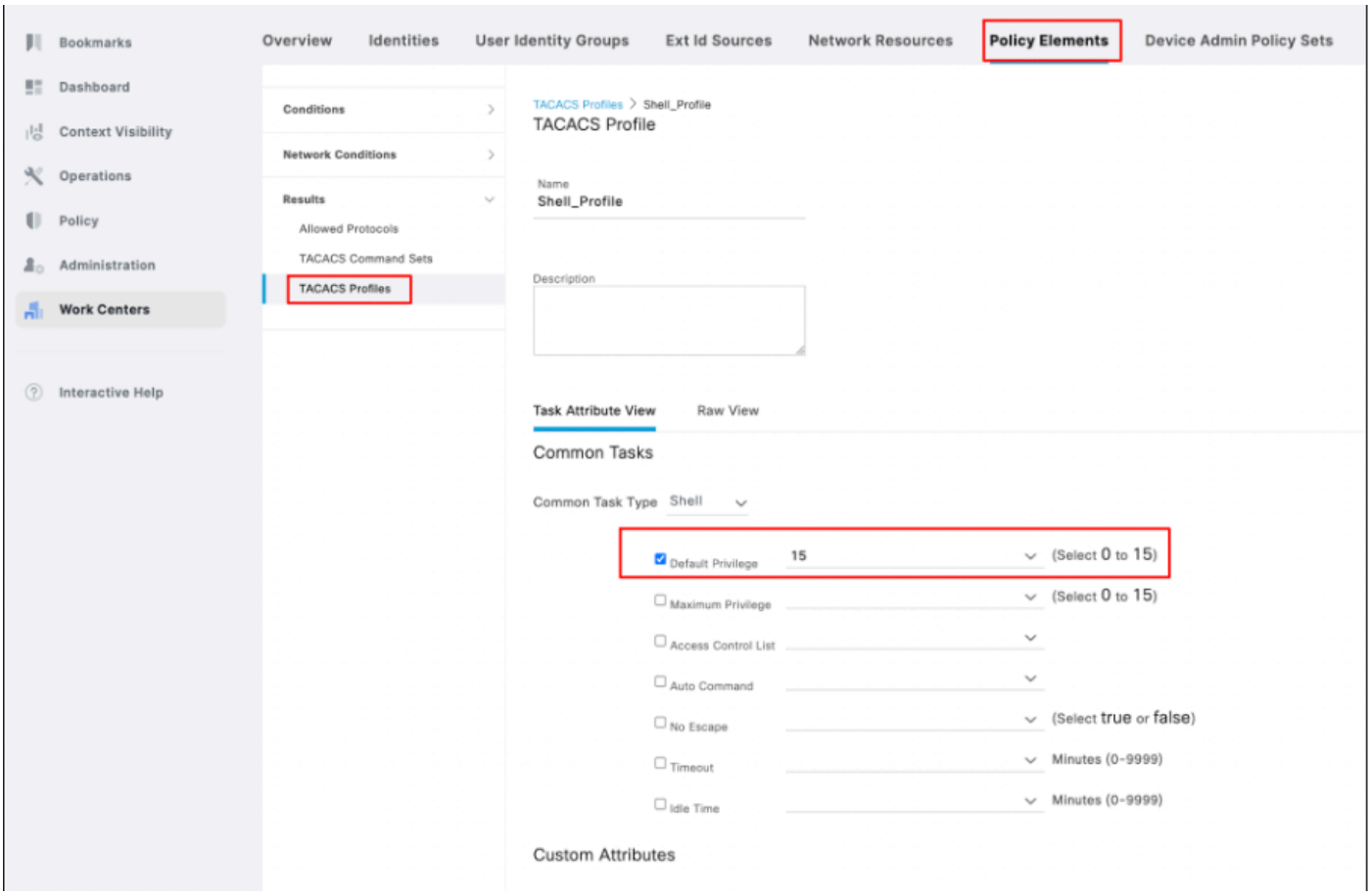


Configuration de permit_show_commands dans ISE

Configuration du profil TACACS+

Un seul profil TACACS+ est configuré et l'autorisation des commandes est effectuée via des jeux de commandes.

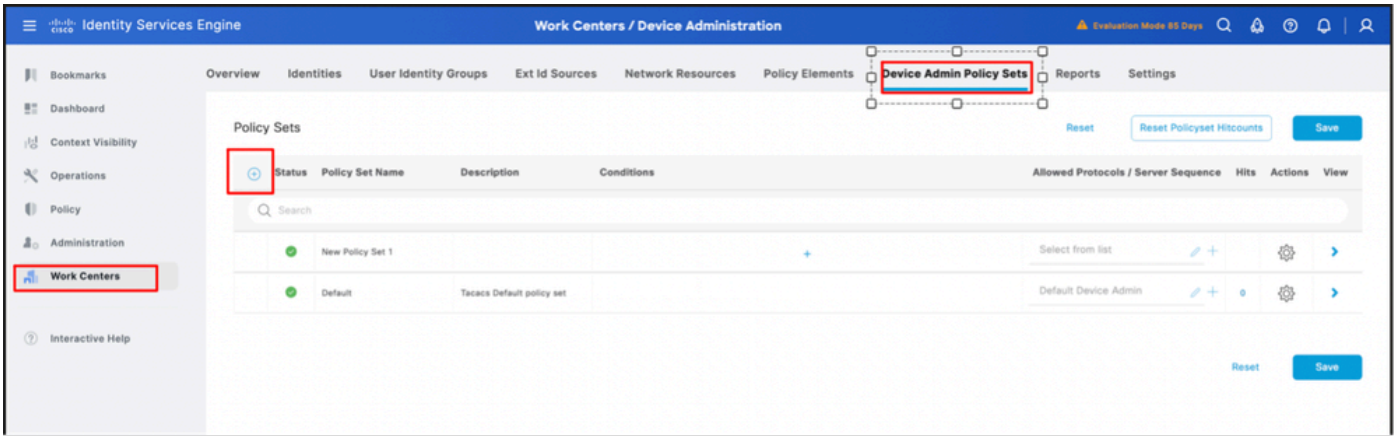
Pour configurer un profil TACACS+, accédez à Work Centers > Device Administration > Policy Results > TACACS Profiles. Cliquez sur Add, donnez un nom au profil Shell, activez la case à cocher Default Privilege et entrez la valeur 15. Enfin, cliquez sur Submit.



Configuration du profil TACACS dans ISE

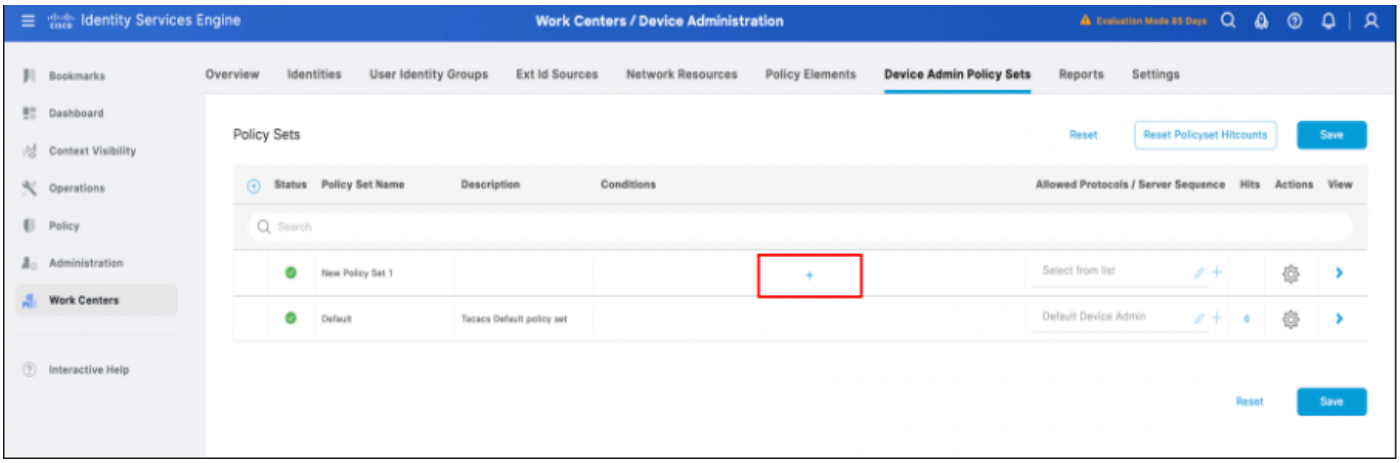
Configuration du profil d'authentification et d'autorisation TACACS+

1. Connectez-vous à l'interface utilisateur graphique du PAN ISE -> Administration -> Work Centers -> Device administration -> Device admin policy sets. Cliquez sur l'icône + (plus) pour créer une nouvelle stratégie. Dans ce cas, l'ensemble de stratégies est nommé New Policy set 1.



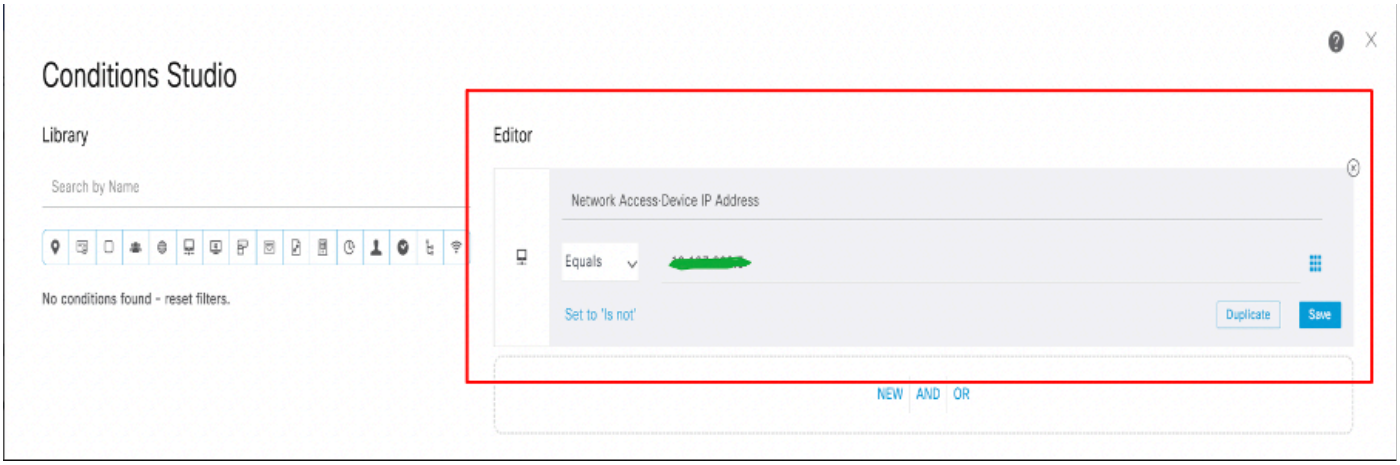
Configuration d'un ensemble de stratégies dans ISE

2. Avant d'enregistrer le jeu de stratégies, vous devez configurer les conditions, comme indiqué dans cette capture d'écran. Cliquez sur l'icône + (plus) pour configurer les conditions pour l'ensemble de stratégies.

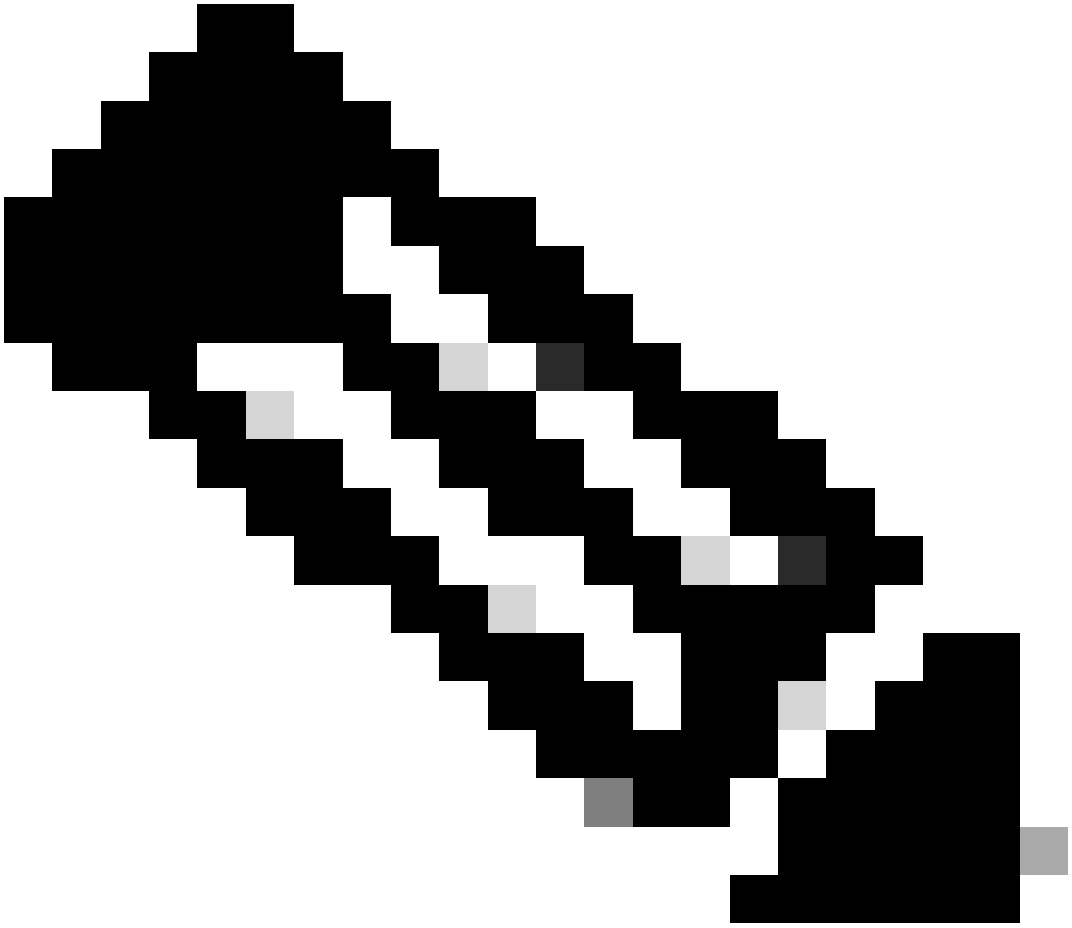


Configuration des conditions d'ensemble de stratégies dans ISE

3. Après avoir cliqué sur l'icône + (plus) comme mentionné à l'étape 2, la boîte de dialogue conditions studio s'ouvre. Configurez les conditions requises. Enregistrez la condition avec les conditions nouvelles ou existantes, faites défiler. Cliquez sur utiliser.

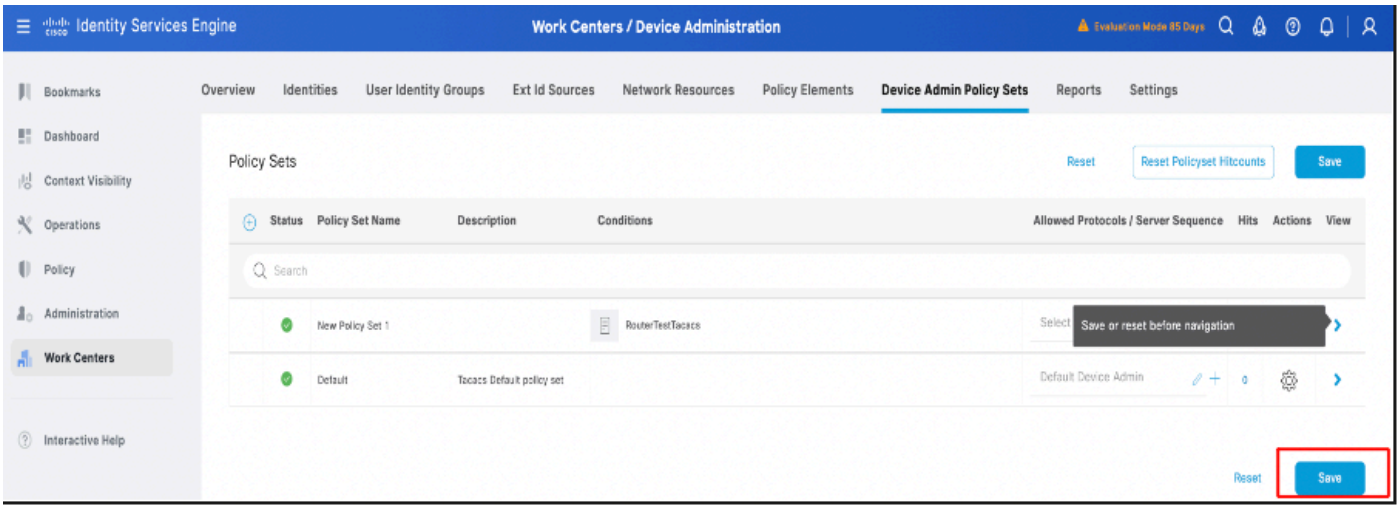


Configuration des conditions d'ensemble de stratégies dans ISE



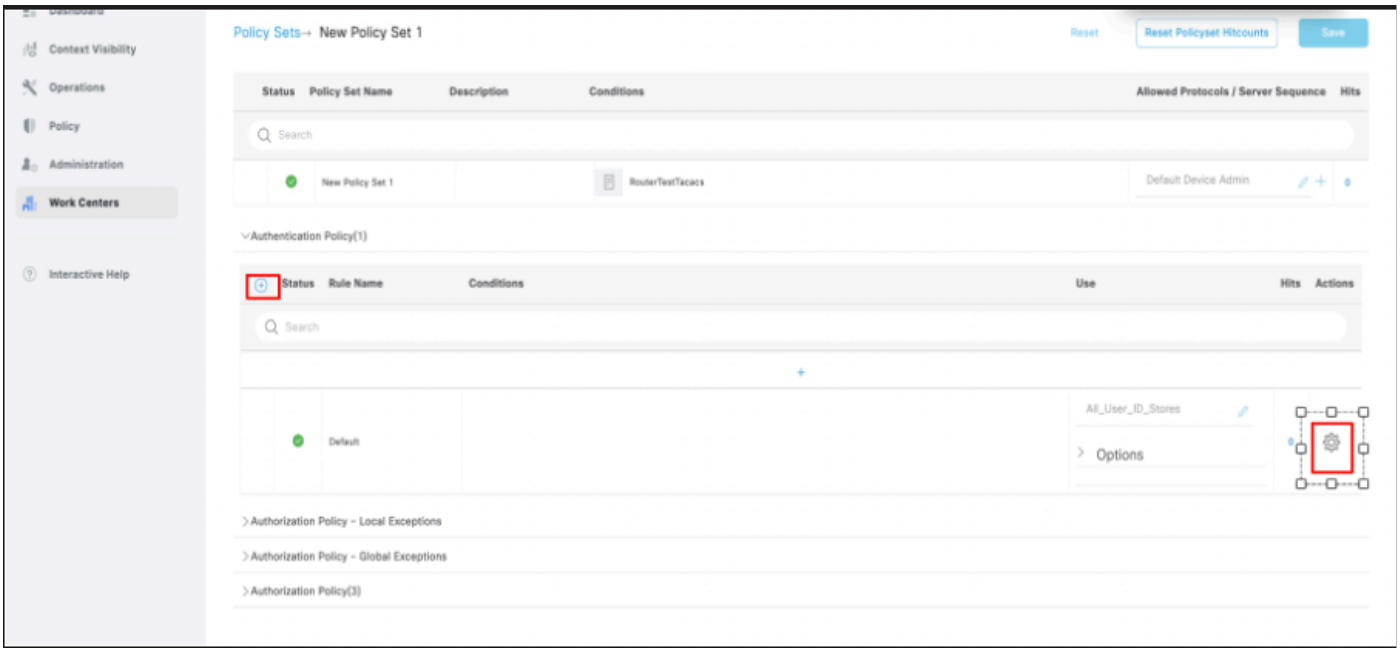
Remarque : Pour cette documentation, les conditions correspondent à l'adresse IP du périphérique réseau. Toutefois, les conditions peuvent varier en fonction des exigences de déploiement.

4. Une fois les conditions configurées et enregistrées, configurez les protocoles autorisés en tant qu'administrateur de périphérique par défaut. Enregistrez le jeu de stratégies créé en cliquant sur l'option Enregistrer .

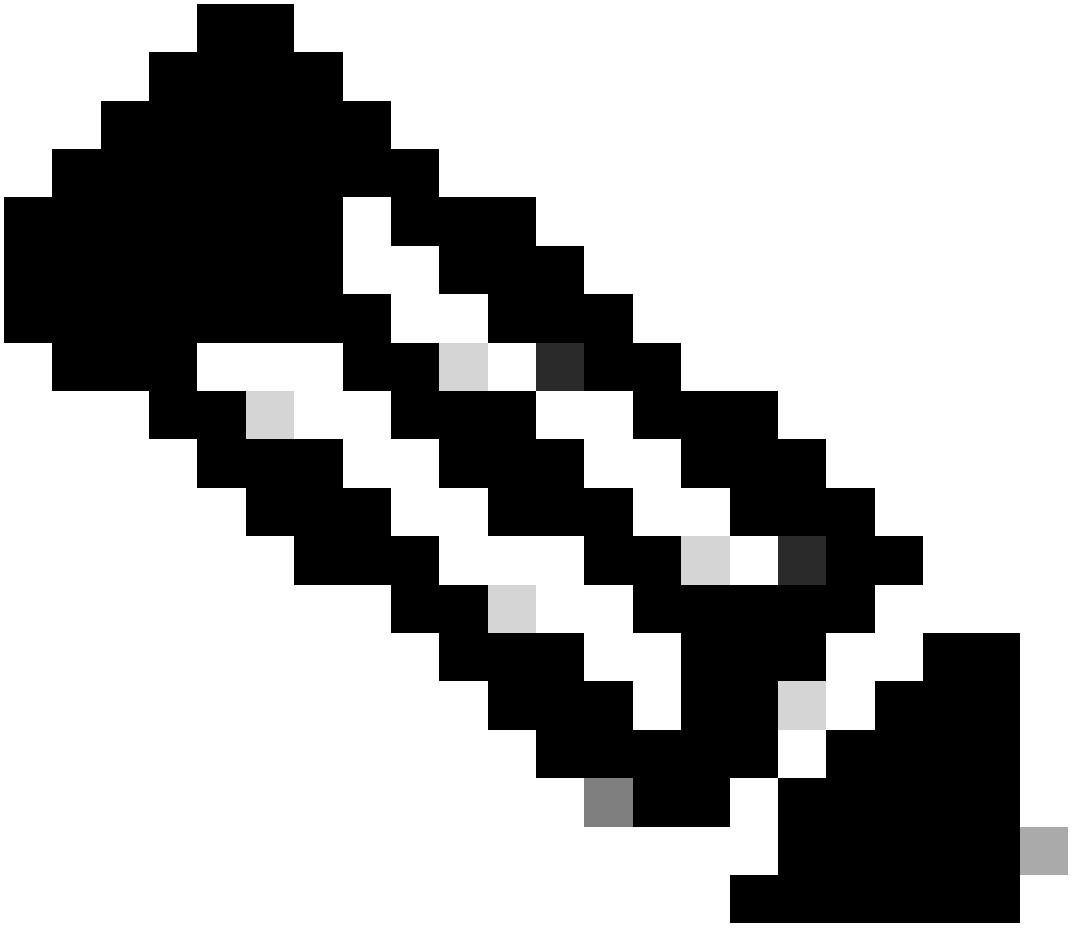


Confirmation de configuration du jeu de stratégies.

5. Développez le nouvel ensemble de stratégies -> Stratégie d'authentification (1) -> Créez une nouvelle stratégie d'authentification en cliquant sur l'icône + (plus) ou en cliquant sur l'icône de l'engrenage, puis insérez une nouvelle ligne au-dessus.



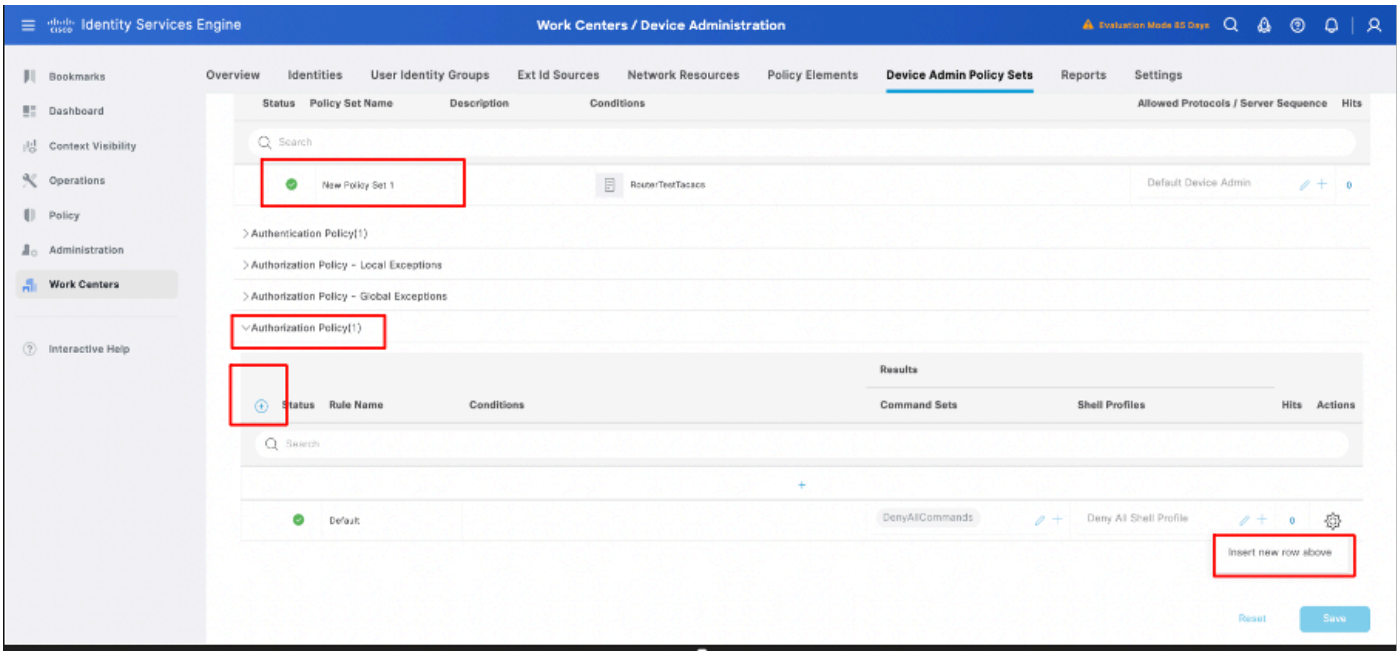
Configuration de la stratégie d'authentification dans l'ensemble de stratégies.



Remarque : Pour cette démonstration, la stratégie d'authentification par défaut définie avec All_User_ID_Stores est utilisée. Cependant, l'utilisation des magasins d'identités est personnalisable selon les exigences de déploiement.

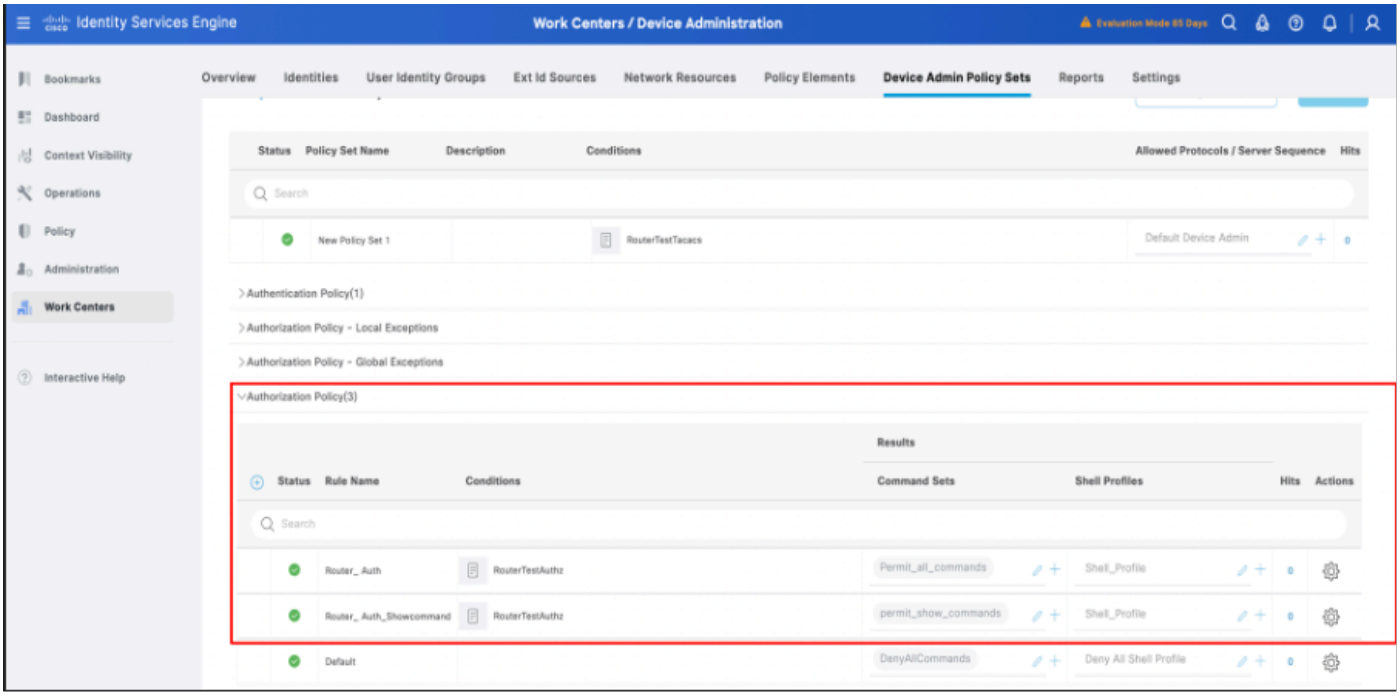
---

6. Développez le nouvel ensemble de stratégies -> Stratégie d'autorisation (1). Cliquez sur l'icône + (plus) ou sur l'icône de l'engrenage. Ensuite, insérez une nouvelle ligne ci-dessus pour créer une stratégie d'autorisation.

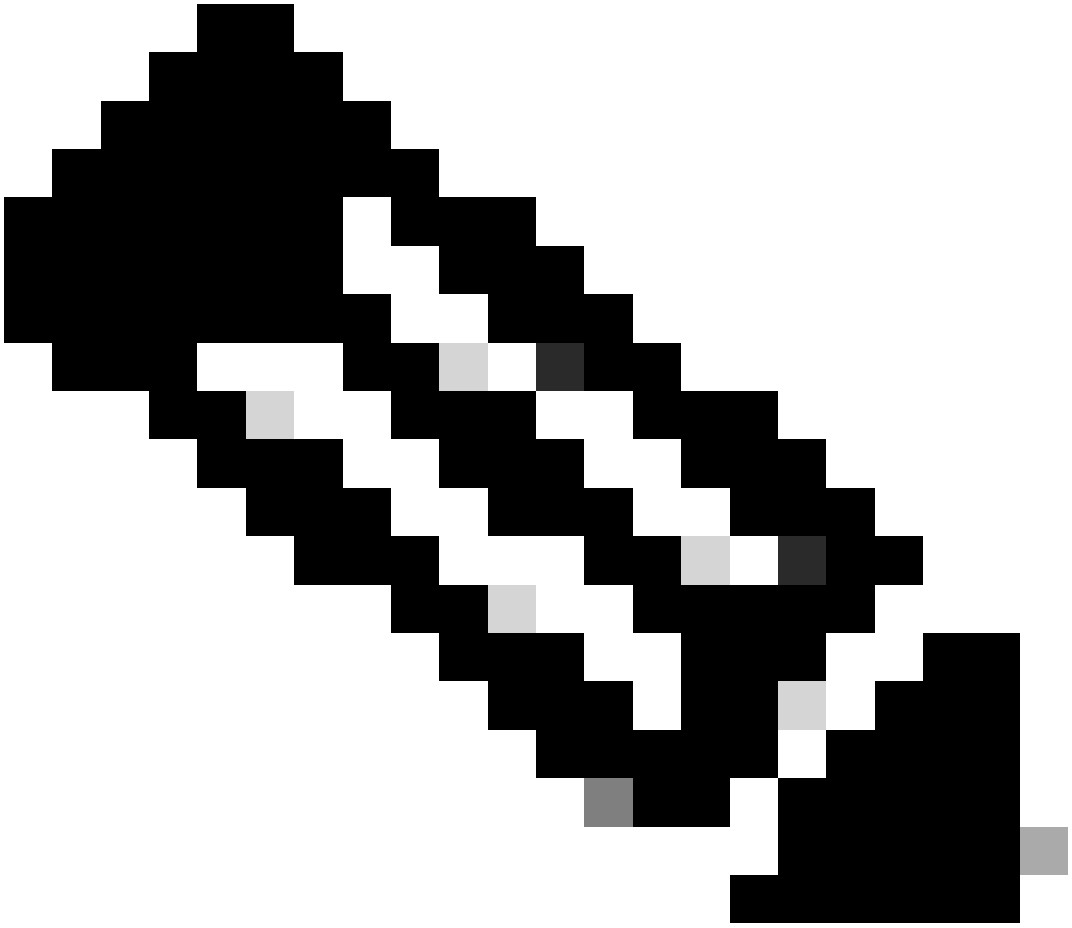


Configuration de la stratégie d'autorisation

7. Configurez la stratégie d'autorisation avec des conditions, des jeux de commandes et un profil d'environnement mappés aux stratégies d'autorisation.



Configuration complète de la stratégie d'autorisation dans ISE

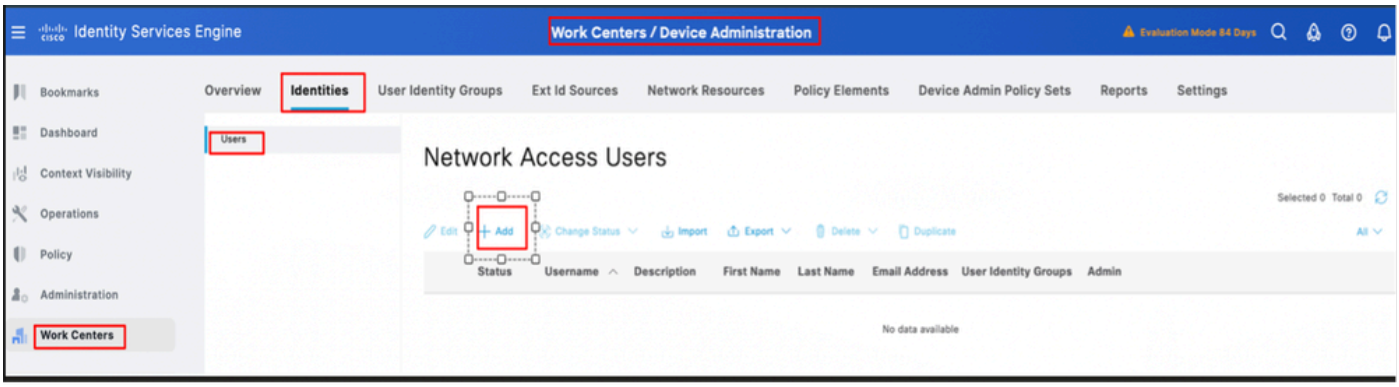


Remarque : Les conditions configurées sont conformes à l’environnement des travaux pratiques et peuvent être configurées conformément aux exigences de déploiement.

8. Suivez les 6 premières étapes pour configurer les ensembles de stratégies pour le commutateur ou tout autre périphérique réseau utilisé pour TACACS+.

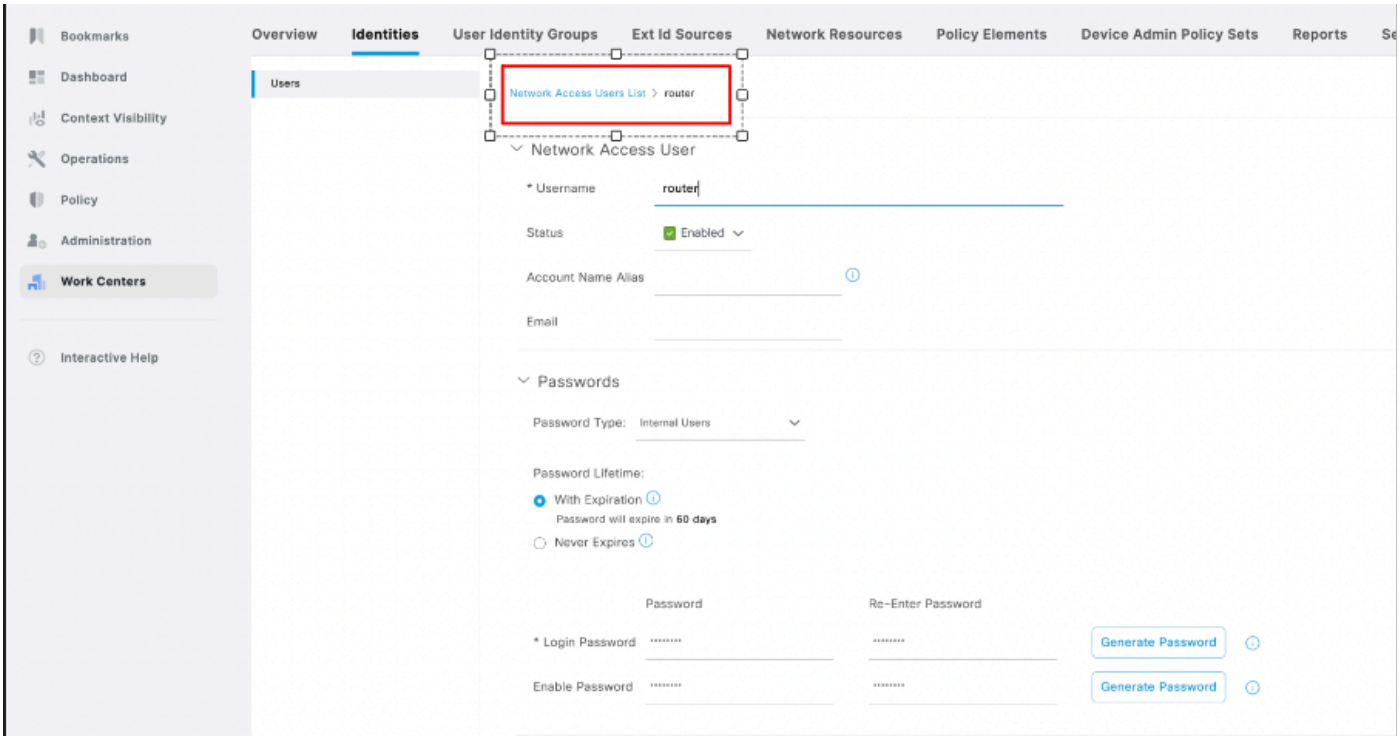
Configuration des utilisateurs d'accès réseau pour l'authentification TACACS de NAD dans ISE

1. Accédez à Workcenters -> Device Administration -> Identities -> Users. Cliquez sur l'icône +(plus) pour créer un nouvel utilisateur.



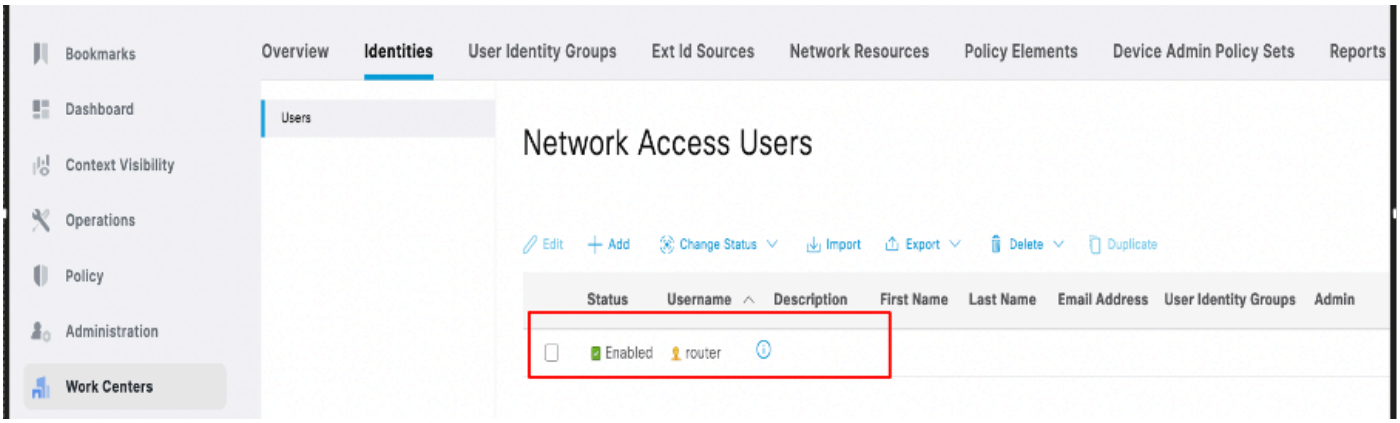
Configurer les utilisateurs d'accès réseau dans ISE

2. Fournissez des informations pour développer les détails du nom d'utilisateur et du mot de passe, mappez l'utilisateur à un groupe d'identités d'utilisateur (facultatif), puis cliquez sur Envoyer.



Configurer les utilisateurs d'accès réseau - Continuer

3. Après avoir soumis la configuration du nom d'utilisateur dans Centres de travail -> Identités -> Utilisateurs -> Utilisateurs d'accès au réseau, l'utilisateur est configuré et activé de manière visible.



Confirmation de la configuration utilisateur d'accès réseau.

Configuration du routeur pour TACACS+

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

1. Connectez-vous à l'interface de ligne de commande du routeur et exécutez ces commandes pour configurer TACACS dans le routeur.

ASR1001-X(config)#aaa new-model — commande requise pour activer aaa dans NAD

ASR1001-X(config)#aaa id_session commun. : commande requise pour activer aaa dans NAD.

ASR1001-X(config)#aaa authentication login default group tacacs+ local

ASR1001-X(config)#aaa authorization exec groupe par défaut tacacs+

ASR1001-X(config)#aaa authorization network list1 groupe tacacs+

ASR1001-X(config)#tacacs server ise1

ASR1001-X(config-server-tacacs)#address ipv4 <adresse IP du serveur TACACS > . — adresse IP G1 de l'interface ISE.

ASR1001-X(config-server-tacacs)# key XXXXX

ASR1001-X(config)# aaa group server tacacs+ isegroup

ASR1001-X(config-sg-tacacs+)#server name ise1

ASR1001-X(config-sg-tacacs+)#ip vrf forwarding Mgmt-intf

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet0

ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet1

ASR1001-X(config)#exit

2. Après avoir enregistré les configurations TACACS+ du routeur, vérifiez la configuration

TACACS+ à l’aide de la commande show run aaa.

```
ASR1001-X#show run aaa
!
aaa authentication login default group isegroup local
aaa authorization exec default group isegroup
aaa authorization network list1 group isegroup
username admin password 0 XXXXXXX
!
serveur tacacs ise1
 address ipv4 <adresse IP du serveur TACACS>
 clé XXXXX
!
!
serveur de groupe aaa tacacs+ isegroup
 nom du serveur ise1
 ip vrf forwarding Mgmt-intf
 ip tacacs source-interface GigabitEthernet1
!
!
!
aaa new-model
aaa session-id common
!
!
```

Configuration du commutateur pour TACACS+

Configuration du commutateur pour l'authentification et l'autorisation TACACS+

1. Connectez-vous à l'interface de ligne de commande du commutateur et exécutez ces commandes pour configurer TACACS dans le commutateur.

C9200L-48P-4X#configure t

Entrez les commandes de configuration, une par ligne. Terminez par CNTL/Z.

C9200L-48P-4X(config)#aaa nouveau modèle. — commande requise pour activer aaa dans NAD

C9200L-48P-4X(config)#aaa id-session commun. — commande requise pour activer aaa dans NAD.

C9200L-48P-4X(config)#aaa authentication login default group isegroup local

C9200L-48P-4X(config)#aaa authorization exec default group isegroup

C9200L-48P-4X(config)#aaa authorization network list1 group isegroup

C9200L-48P-4X(config)#tacacs server ise1

C9200L-48P-4X(config-server-tacacs)#address ipv4 <adresse IP du serveur TACACS> — Adresse IP G1 de l'interface ISE.

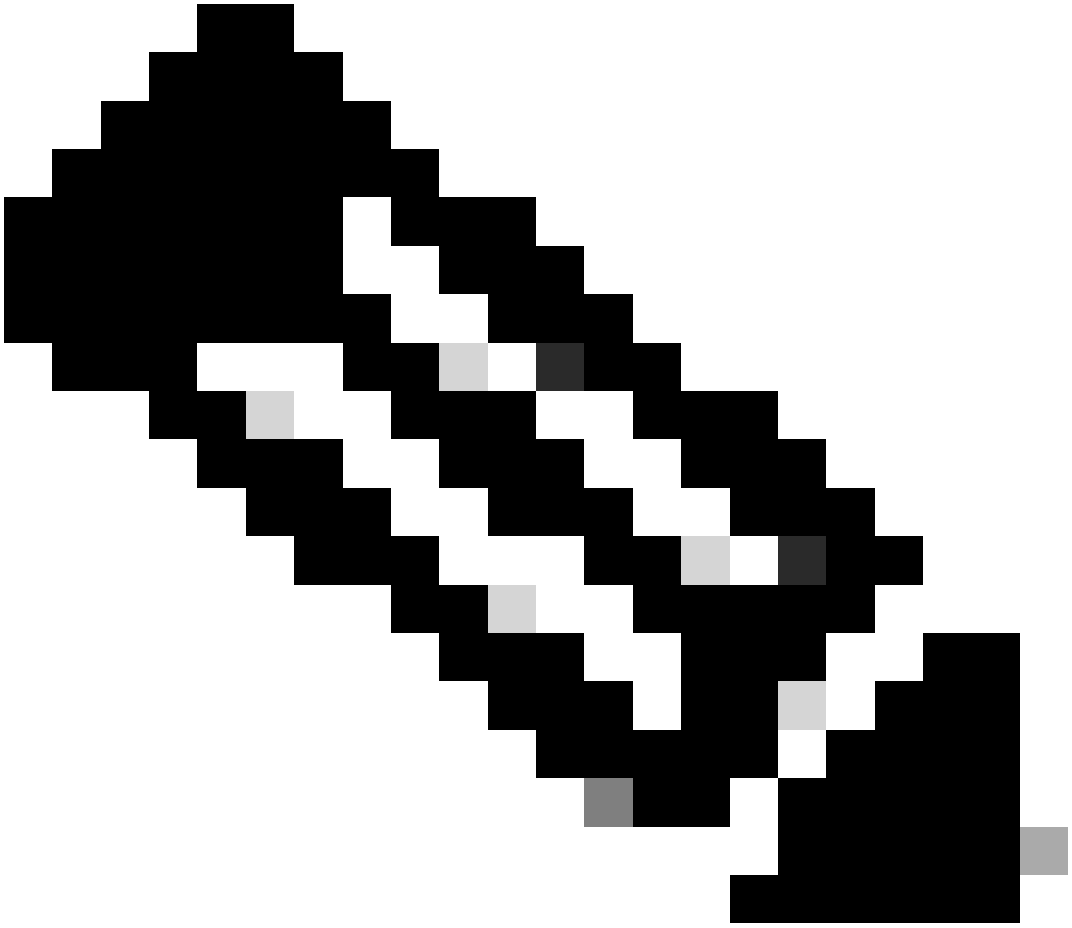
C9200L-48P-4X(config-server-tacacs)#key XXXXX

C9200L-48P(config)#aaa group server tacacs+ isegroup

C9200L-48P(config-sg-tacacs+)#server name ise1

C9200L-48P-4X(config)#exit

C9200L-48P-4X#wr mem



Remarque : Dans la configuration NAD TACACS+, tacacs+ est le groupe qui peut être personnalisé selon les exigences de déploiement.

---

2. Après avoir enregistré les configurations TACACS+ du commutateur, vérifiez la configuration TACACS+ à l'aide de la commande show run aaa.

C9200L-48P#show run aaa

!

aaa authentication login default group isegroup local

aaa authorization exec default group isegroup

aaa authorization network list1 group isegroup

username admin password 0 XXXXX

!

!

serveur tacacs ise1

address ipv4 <adresse IP du serveur TACACS>

clé XXXXX

!

!

serveur de groupe aaa tacacs+ isegroup

nom du serveur ise1

!

!

!

aaa new-model

aaa session-id common

!

!

Vérification

Vérification à partir du routeur

À partir de l'interface de ligne de commande du routeur, authentifiez l'authentification de TACACS+ par rapport à ISE avec l'interface Gigabit Ethernet 1 en utilisant la commande test aaa group tacacsgroupname username password new.

Voici l'exemple de résultat de Router & ISE :

Vérification du port 49 du routeur :

ASR1001-X#telnet ISE Gig 1 interface IP 49

Tentative d'adressage IP de l'interface ISE GIg 1, 49... Open (ouvert)

ASR1001-X#test aaa group isegroup router XXXX nouveau

Envoi du mot de passe

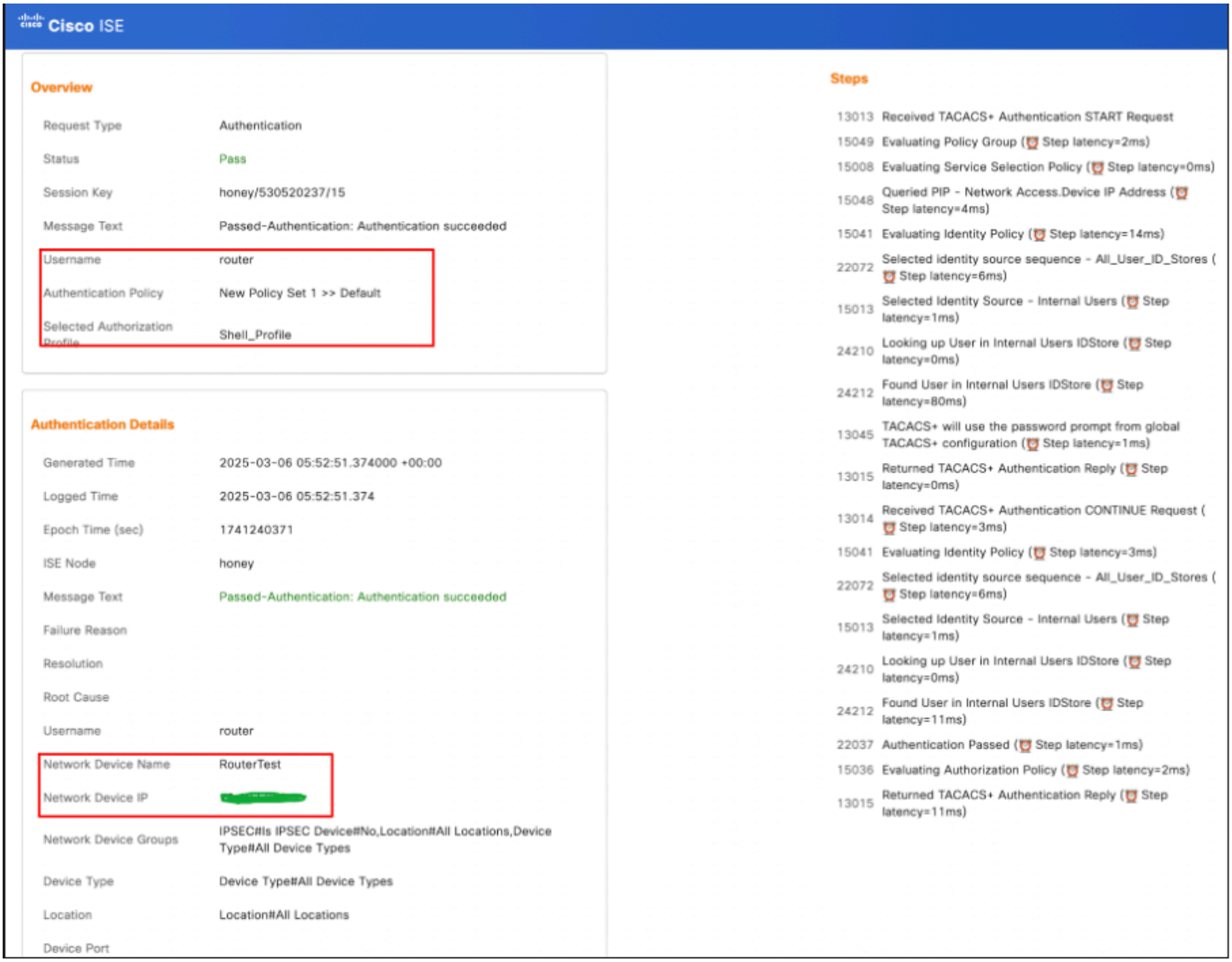
Utilisateur authentifié avec succès

ATTRIBUTS UTILISATEUR

username 0 "router"

reply-message 0 "Mot de passe :"

Pour la vérification à partir d'ISE, connectez-vous à l'interface utilisateur graphique -> Opérations -> Journaux TACACS en direct, puis filtrez avec l'adresse IP du routeur dans le champ Détails du périphérique réseau.



Journaux TACACS en direct d'ISE - Vérification du routeur.

Vérification du commutateur

À partir de l'interface de ligne de commande du commutateur, vérifiez l'authentification de TACACS+ par rapport à ISE avec l'interface Gigabit Ethernet 1 en utilisant la commande test aaa group tacacsgroupname username password new :

Voici un exemple de sortie du commutateur et de l'ISE.

Vérification du port 49 du commutateur :

C9200L-48P# telnet Interface ISE Gig1 IP 49

Tentative d'adressage IP de l'interface ISE Gig1, 49... Open (ouvert)

C9200L-48P#test aaa group isegroup switch XXXX nouveau

Envoi du mot de passe

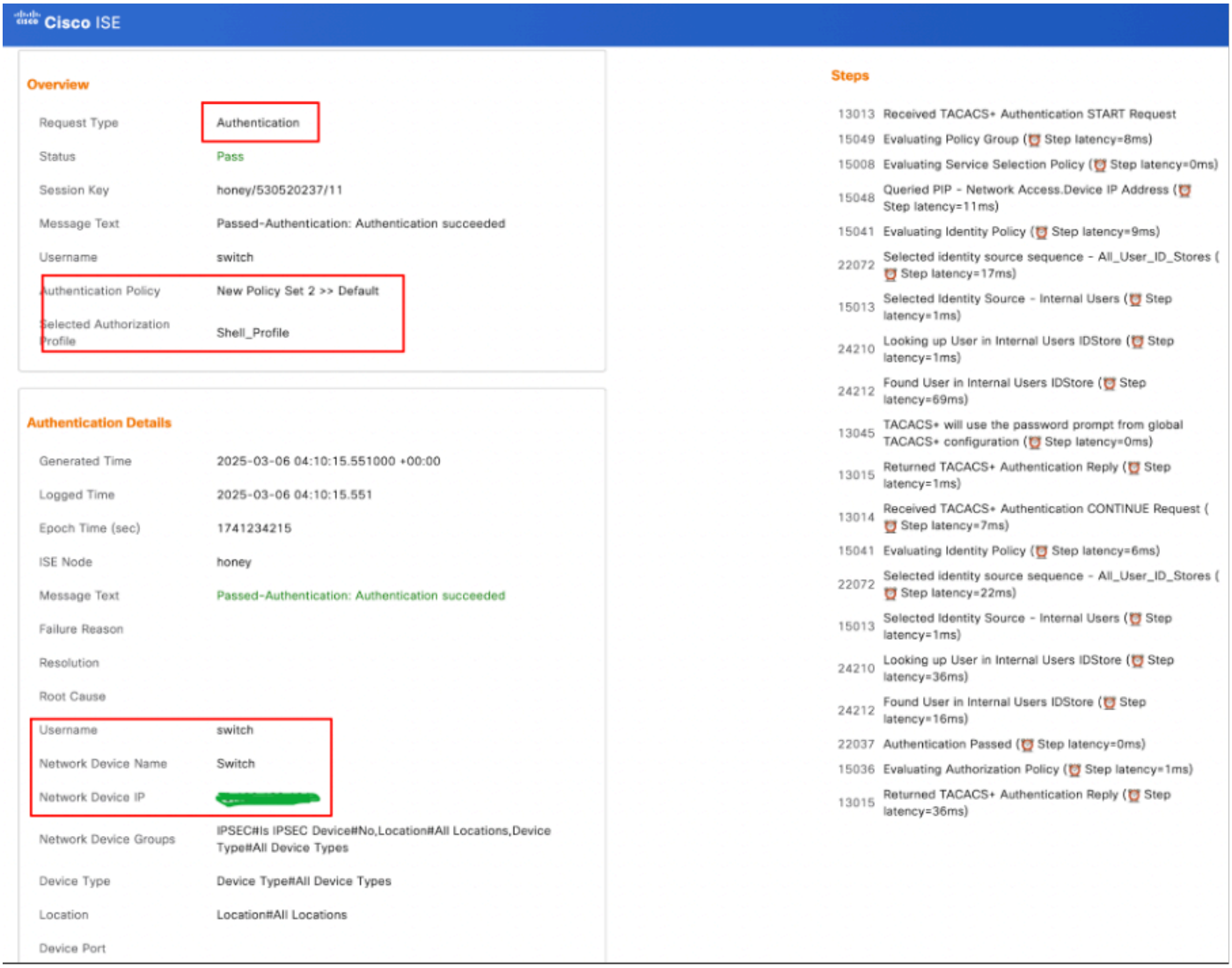
Utilisateur authentifié avec succès

ATTRIBUTS UTILISATEUR

username 0 "switch"

reply-message 0 "Mot de passe :"

Pour la vérification à partir d'ISE, connectez-vous à l'interface utilisateur graphique -> Opérations -> Journaux TACACS en direct, puis filtrez avec l'adresse IP du commutateur dans le champ Détails du périphérique réseau.

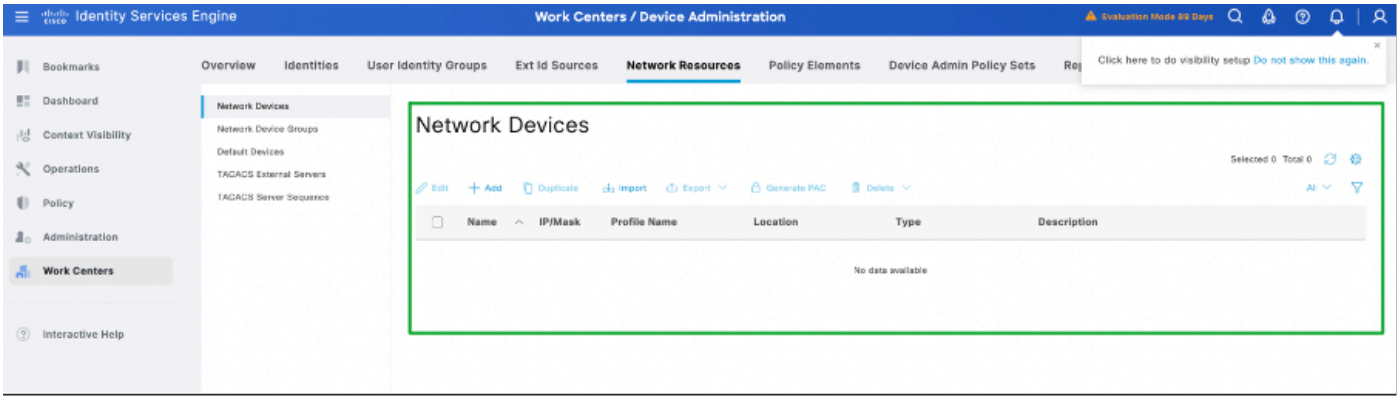


Dépannage

Cette section présente certains des problèmes courants rencontrés avec les authentifications TACACS+.

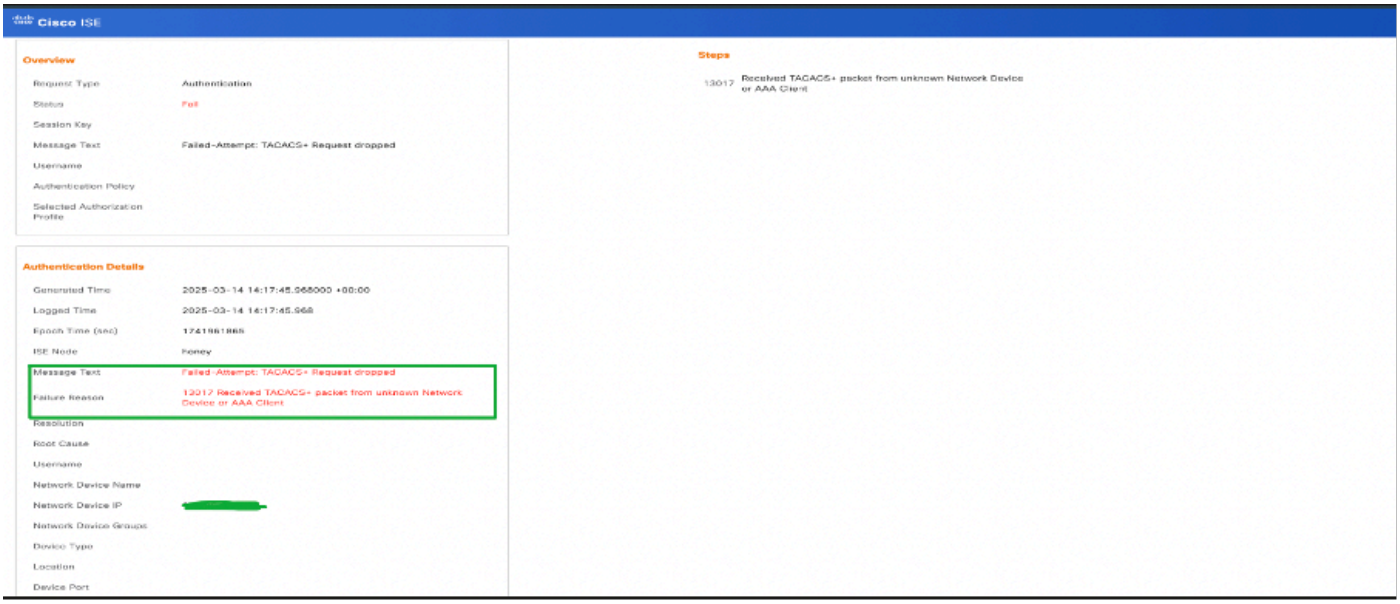
Scénario 1 : L'authentification TACACS+ échoue avec "Erreur : 13017 Paquet TACACS+ reçu d'un périphérique réseau inconnu ou d'un client AAA".

Ce scénario se produit lorsque le périphérique réseau n'est pas ajouté en tant que ressources réseau dans ISE. Comme l'illustre cette capture d'écran, le commutateur n'est pas ajouté aux ressources réseau d'ISE.



Scénario de dépannage : les périphériques réseau ne sont pas ajoutés dans ISE.

À présent, lorsque vous testez l'authentification à partir du commutateur/périphérique réseau, le paquet atteint ISE comme prévu. Cependant, l'authentification échoue avec l'erreur "Erreur : 13017 Received TACACS+ packet from unknown Network Device or AAA Client" comme indiqué dans cette capture d'écran :



Journaux TACACS en direct : échec lorsque le périphérique réseau n'est pas ajouté à ISE.

Vérification à partir du périphérique réseau (commutateur)

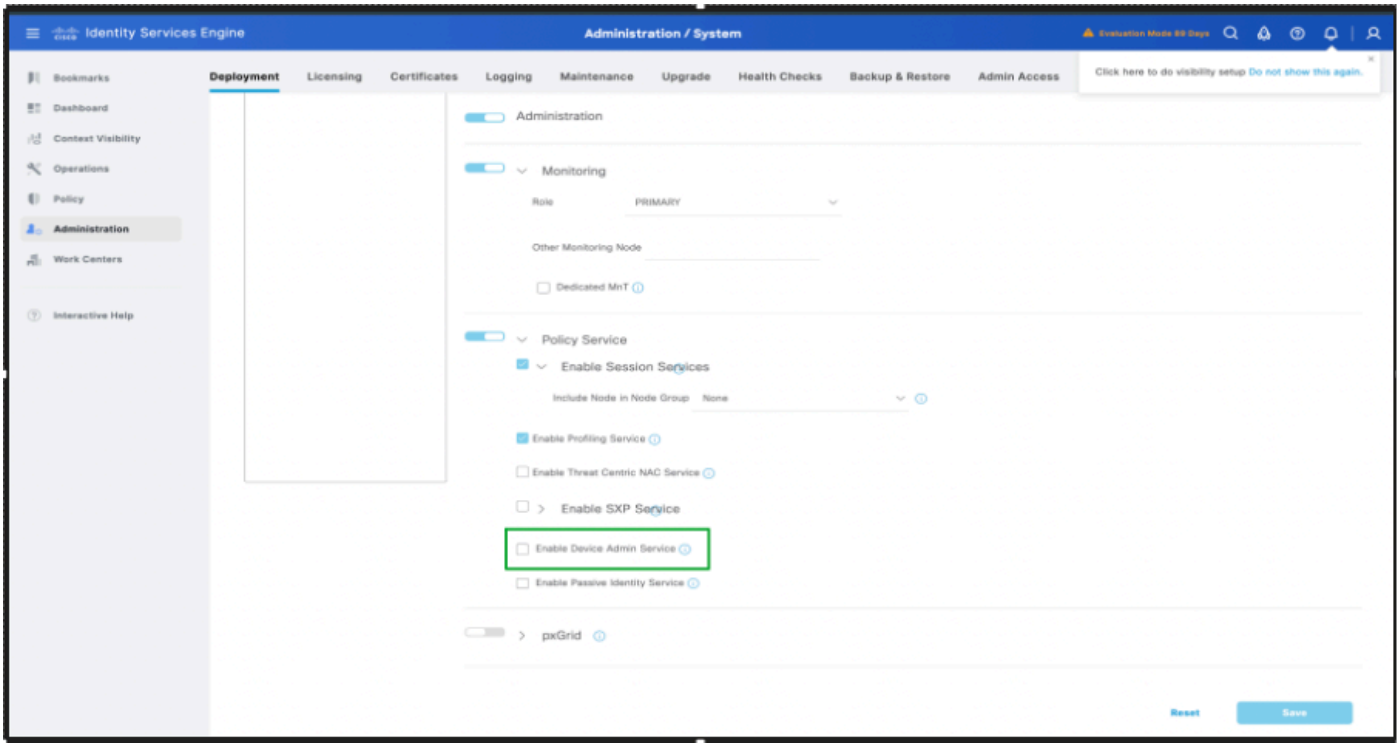
Switch#test aaa group isegroup switch XXXXXX nouveau
Utilisateur rejeté

Solution : Vérifiez si le commutateur / routeur / périphérique réseau est ajouté en tant que périphérique réseau dans ISE. Si le périphérique n'est pas ajouté, ajoutez-le à la liste des périphériques réseau d'ISE.

Scénario 2 : ISE abandonne le paquet TACACS+ en silence sans aucune information.

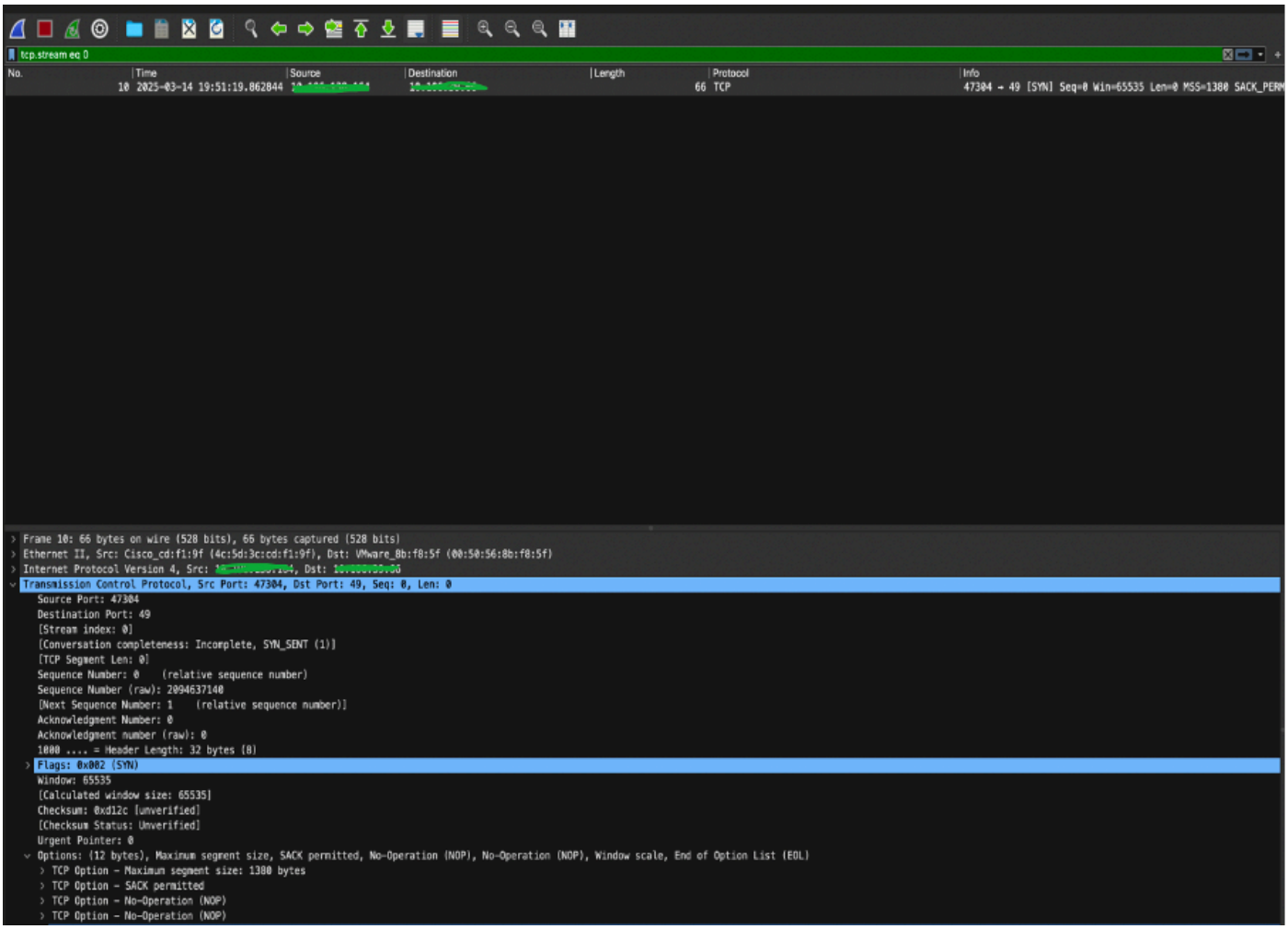
Ce scénario se produit lorsque le service d'administration des périphériques est désactivé dans ISE. Dans ce scénario, ISE abandonne le paquet et aucun journal en direct n'est vu même si l'authentification est lancée à partir du périphérique réseau qui est ajouté aux ressources réseau d'ISE.

Comme l'illustre cette capture d'écran, l'administration des périphériques est désactivée dans ISE.



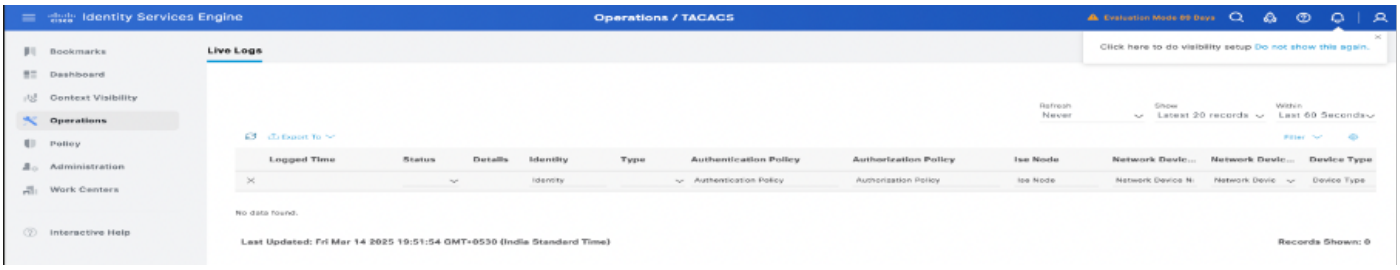
Scénario où l'administration des périphériques n'est pas activée dans ISE.

Lorsqu'un utilisateur lance l'authentification à partir du périphérique réseau, ISE abandonne silencieusement les paquets sans aucune information dans les journaux actifs et ISE ne répond pas au paquet Syn envoyé par le périphérique réseau pour terminer le processus d'authentification TACACS. Reportez-vous à cette capture d'écran :



ISE supprime les paquets en silence pendant TACACS

ISE n'affiche aucun journal actif pendant l'authentification.



Aucun journal TACACS en direct - Vérification par ISE

Vérification à partir du périphérique réseau (commutateur)

Commutateur#
Switch#test aaa group isegroup switch XXXX nouveau
Utilisateur rejeté
Commutateur#
*Mar 14 13:54:28.144: T+ : Version 192 (0xC0), type 1, seq 1, encryption 1, SC 0
*Mar 14 13:54:28.144: T+ : session_id 10158877 (0x9B031D), dlen 14 (0xE)
*Mar 14 13:54:28.144: T+ : type:AUTHEN/START, priv_lvl:15 action:LOGIN ascii
*Mar 14 13:54:28.144: T+ : svc:LOGIN_user_len:6 port_len:0 (0x0) raddr_len:0 (0x0) data_len:0
*Mar 14 13:54:28.144: T+ : utilisateur : aiguillage
*Mar 14 13:54:28.144: T+ : port :
*Mar 14 13:54:28.144: T+ : rem_addr :
*Mar 14 13:54:28.144: T+ : données :
*Mar 14 13:54:28.144: T+ : Paquet final

Solution : Activez l'administration des périphériques dans ISE.

Référence

- Dépannage des problèmes d'authentification TACACS
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.3
- VRF pour serveurs TACACS

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.