Configurer ISE en tant qu'authentification externe pour l'interface utilisateur graphique SD-WAN de Catalyst

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Avant de commencer

Configuration - Utilisation de TACACS+

- Configuration du SD-WAN Catalyst à l'aide de TACACS+
- Configurer ISE pour TACACS+
- Vérification de la configuration TACACS+

Dépannage

Références

Introduction

Ce document décrit comment configurer Cisco Identity Services Engine(ISE) en tant qu'authentification externe pour l'administration de l'interface utilisateur graphique Cisco Catalyst SD-WAN.

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des sujets suivants :

- protocole TACACS+
- Administration des périphériques Cisco ISE
- Administration SD-WAN de Cisco Catalyst
- Évaluation de la politique Cisco ISE

Composants utilisés

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

- Correctif2 de Cisco Identity Services Engine (ISE) version 3.4

- Cisco Catalyst SD-WAN version 20.15.3

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.

Avant de commencer

À partir de la version 20.9.1 de Cisco vManage, de nouvelles balises sont utilisées dans l'authentification :

- Viptela-User-Group : pour les définitions de groupes d'utilisateurs au lieu de Viptela-Group-Name.
- Viptela-Resource-Group : pour les définitions de groupes de ressources.

Configuration - Utilisation de TACACS+

Configuration du SD-WAN Catalyst à l'aide de TACACS+

Procédure

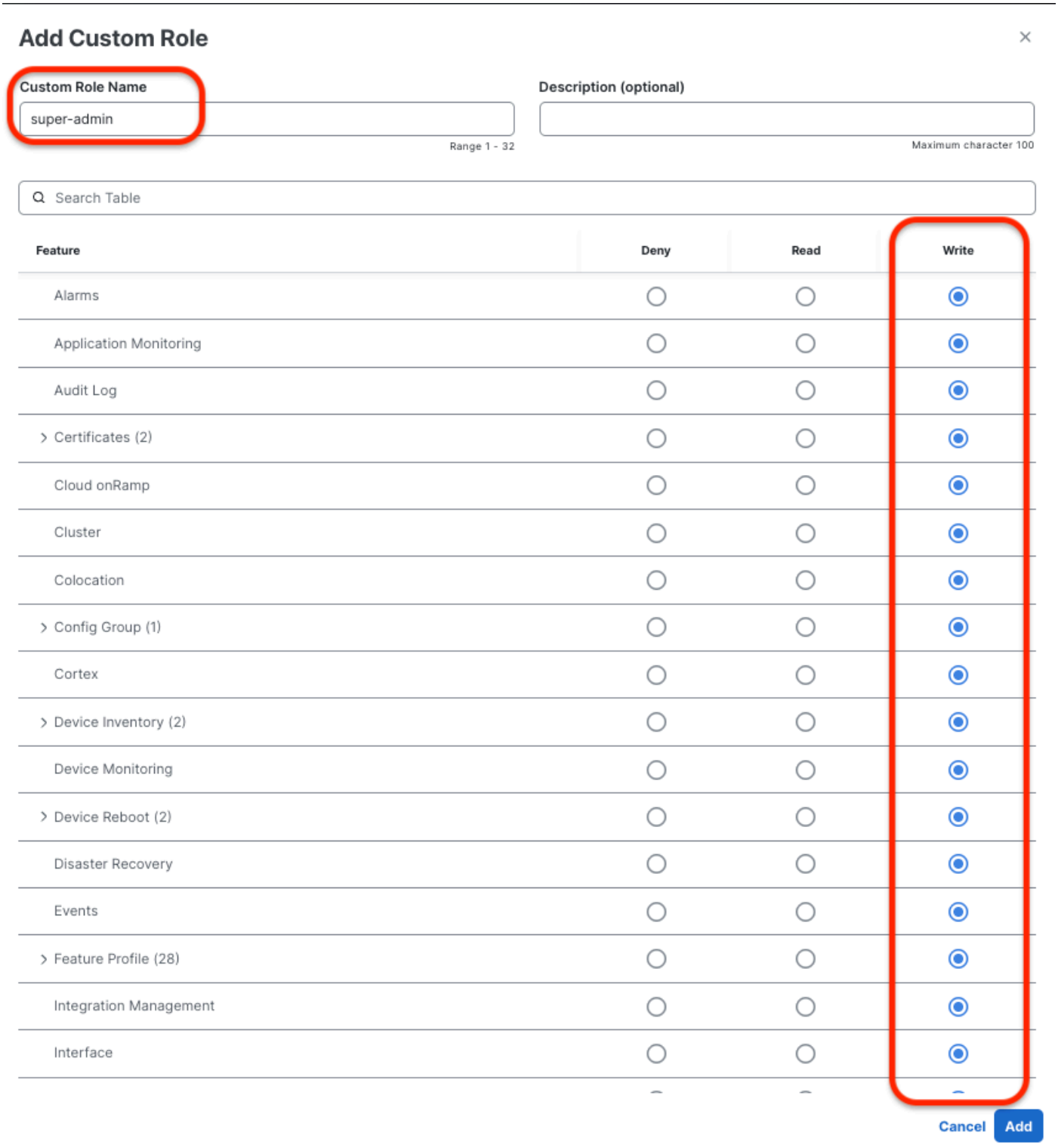
Étape 1. (Facultatif) Définissez des rôles personnalisés.

Configurez vos rôles personnalisés en fonction de vos besoins. Vous pouvez utiliser les rôles d'utilisateurs par défaut. Vous pouvez effectuer cette opération à partir de l'onglet Catalyst SD-WAN : Administration > Utilisateurs et accès > Rôles.

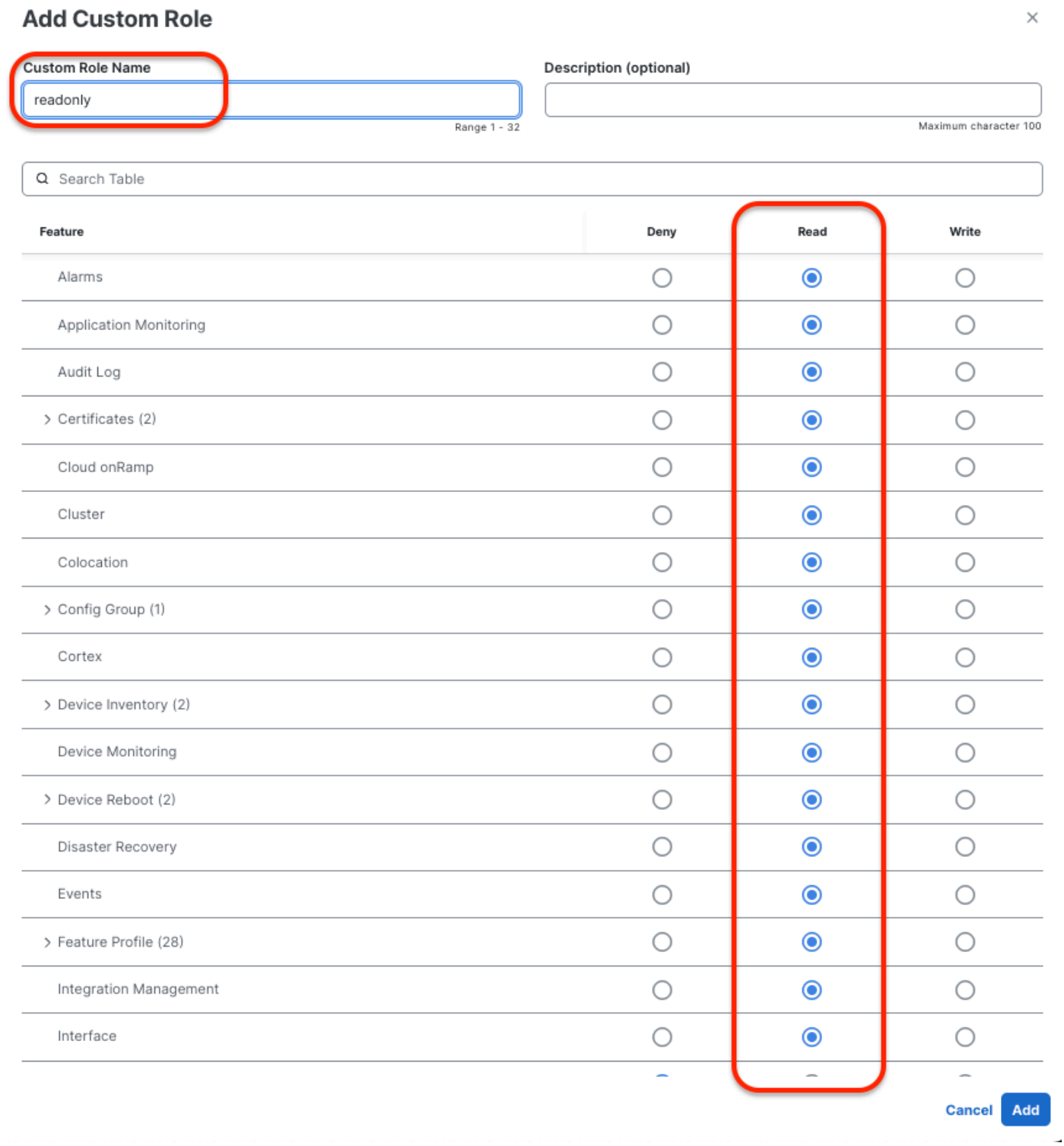
Créez deux rôles personnalisés :

1. Rôle Admin : super-administrateur
2. Rôle en lecture seule : en lecture seule

Vous pouvez effectuer cette opération à partir de l'onglet Catalyst SD-WAN : Administration > Utilisateurs et accès > Rôles > Cliquez sur > Ajouter un rôle.



Rôle admin (super-admin)



Rôle en lecture seule (lecture seule)

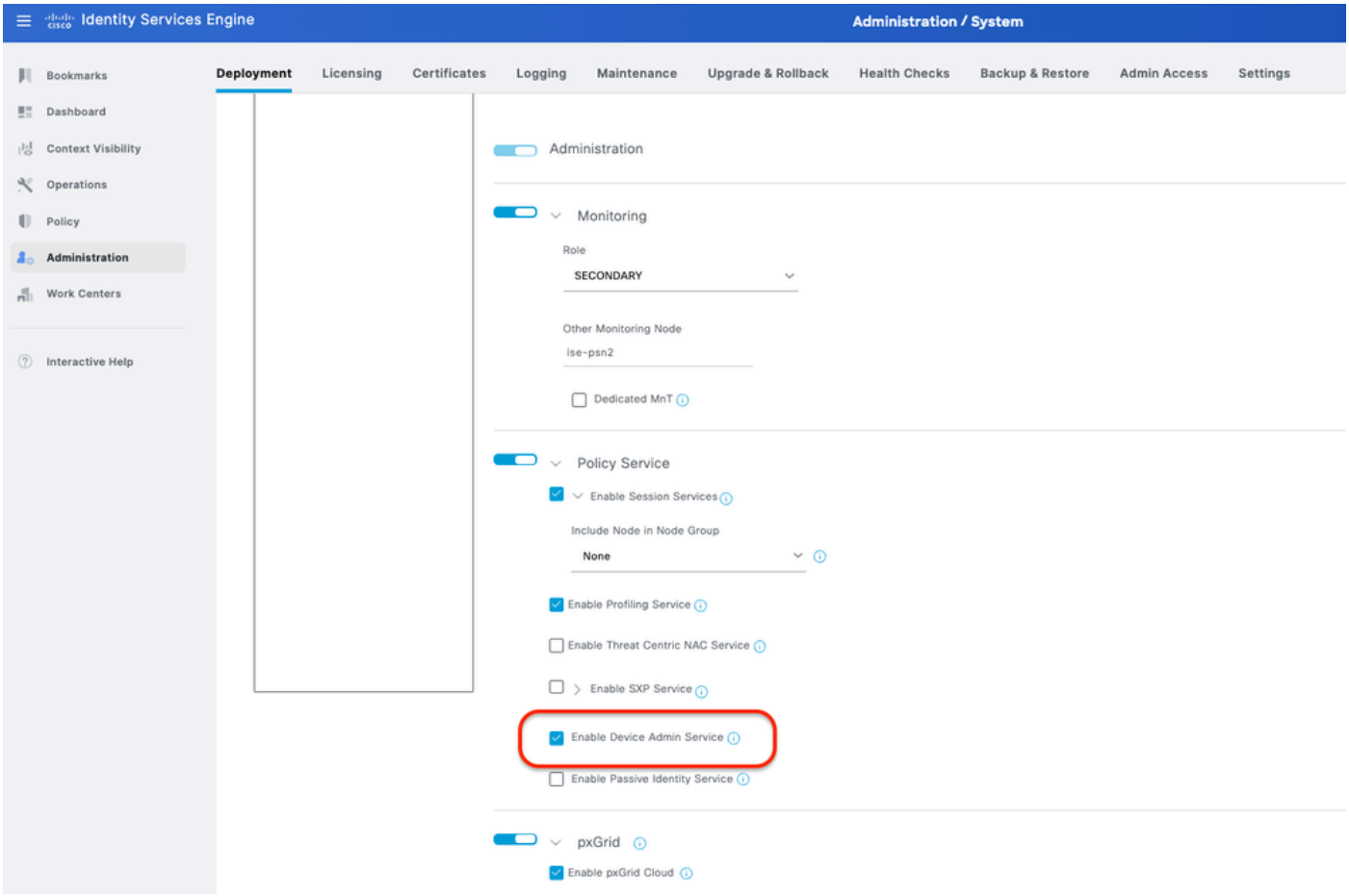
Étape 2 : configuration de l'authentification externe à l'aide de TACACS+ (CLI)

```
Entering configuration mode terminal
vmanage(config)#
vmanage(config)#
vmanage(config)# system
vmanage(config-system)# aaa
vmanage(config-aaa)# auth-order tacacs radius local
vmanage(config-aaa)# auth-fallback
vmanage(config-aaa)# commit and-quit
Commit complete.
```

CLI vManager - Configuration de TACACS+

Configurer ISE pour TACACS+

Étape 1 : activation du service d'administration des périphériques
Pour ce faire, accédez à l'onglet Administration > System > Deployment > Edit (ISE PSN Node)>Check Enable Device Admin Service.



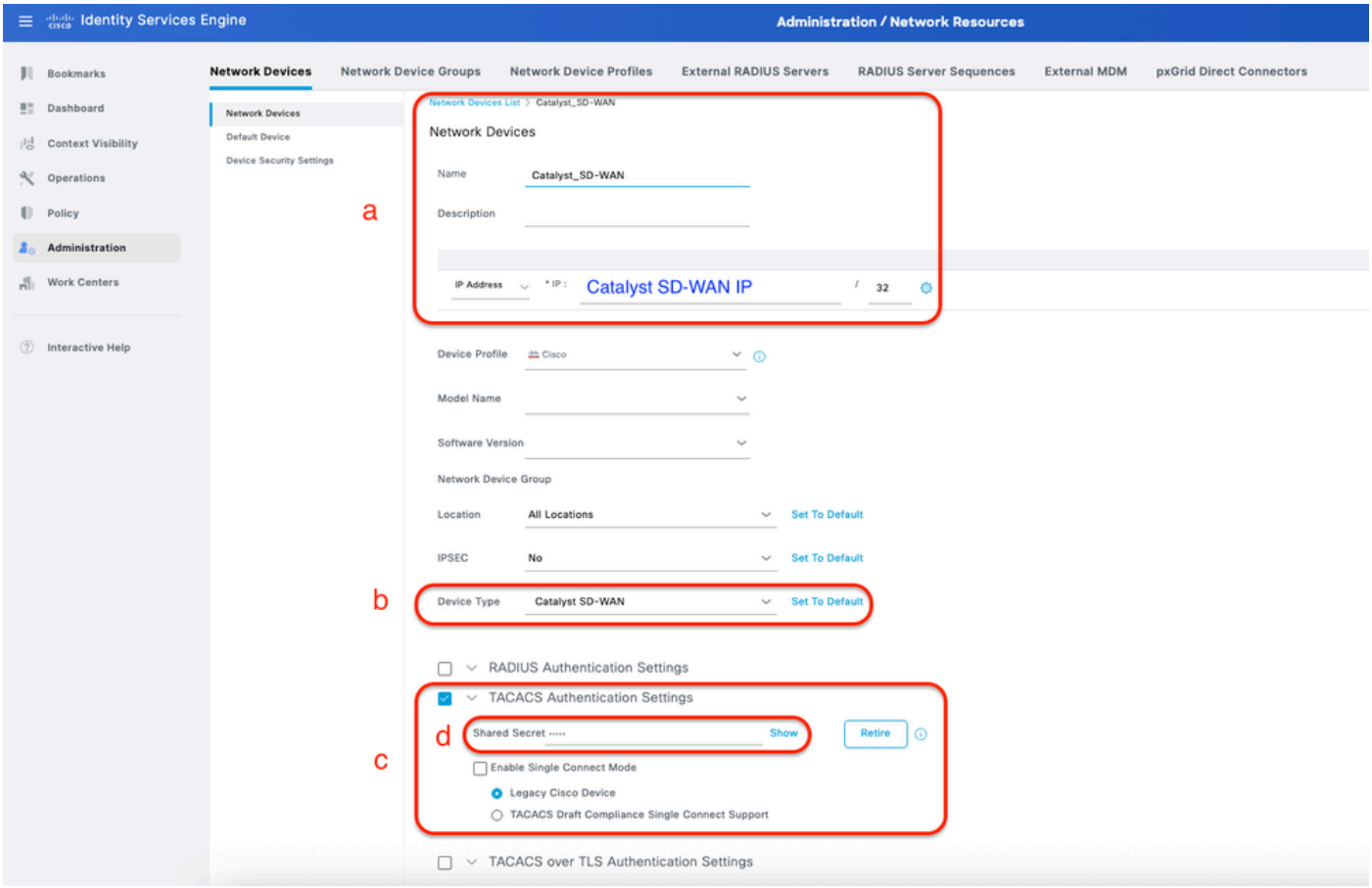
Activer le service d'administration des périphériques

Étape 2. Ajout du SD-WAN Catalyst en tant que périphérique réseau sur ISE

Pour ce faire, accédez à l'onglet Administration > Network Resources > Network Devices.

Procédure

a. Définissez le nom et l'IP du périphérique réseau (Catalyst SD-WAN).
b. (Facultatif) Classez le type de périphérique pour la condition Jeu de stratégies.
c. Activez les paramètres d'authentification TACACS+.
d. Définissez le secret partagé TACACS+.



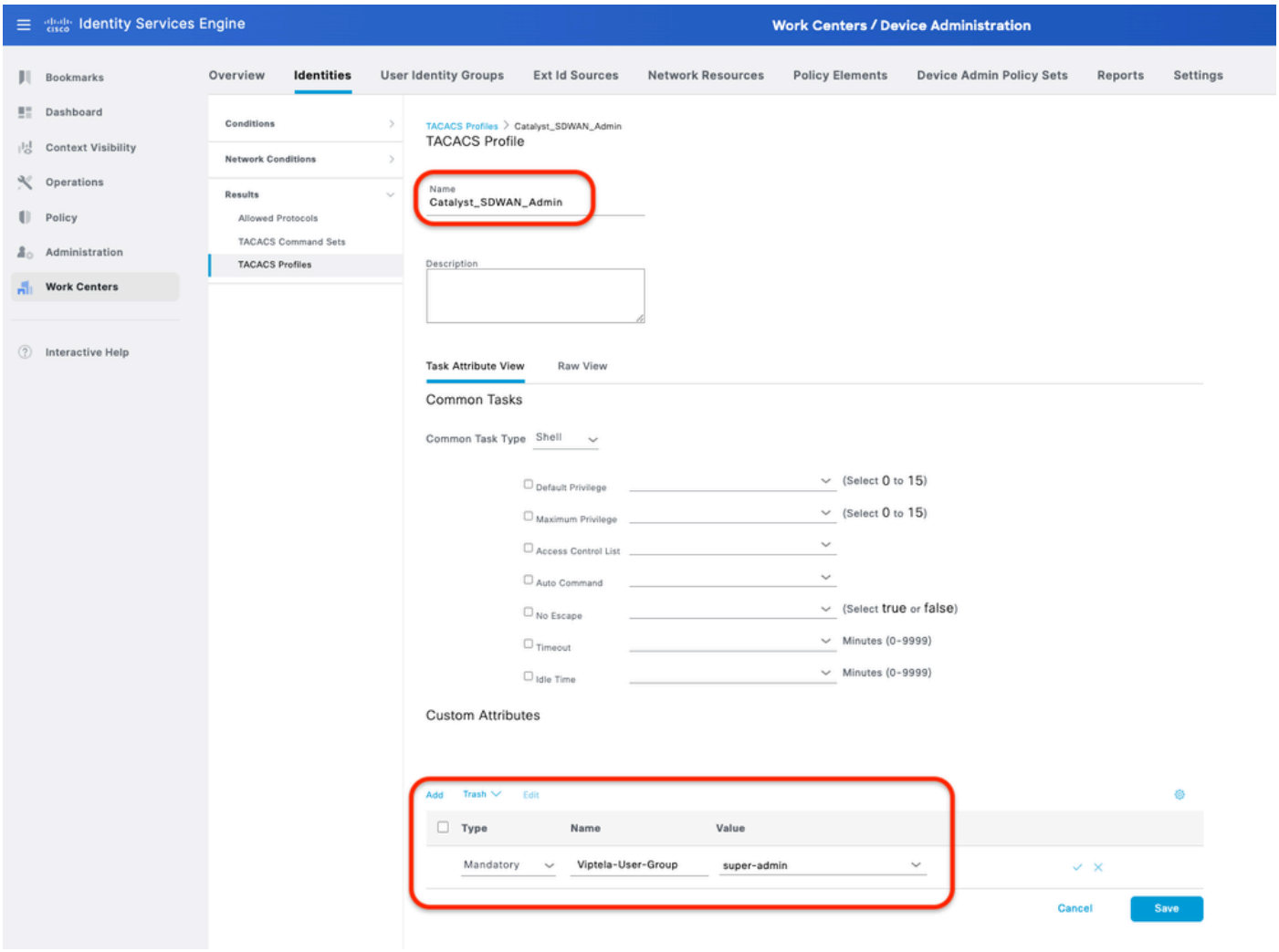
Périphérique réseau ISE (Catalyst SD-WAN) pour TACACS+

Étape 3 : création du profil TACACS+ pour chaque rôle SD-WAN Catalyst

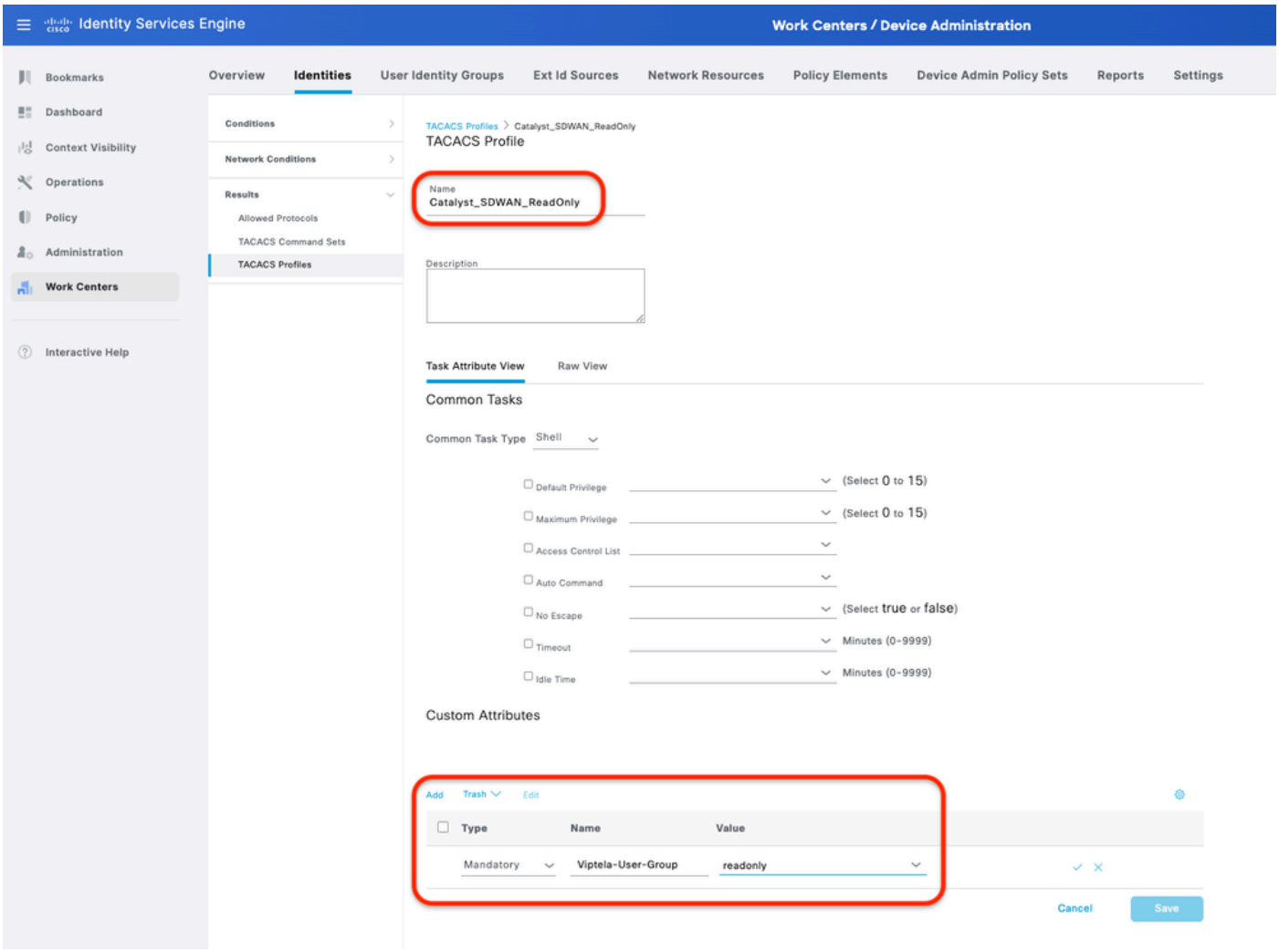
Créer des profils TACACS+ :

1. Catalyst_SDWAN_Admin : Pour les super administrateurs.
2. Catalyst_SDWAN_ReadOnly : Pour les utilisateurs en lecture seule.

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles > Add.



Profil TACACS+ - (Catalyst_SDWAN_Admin)



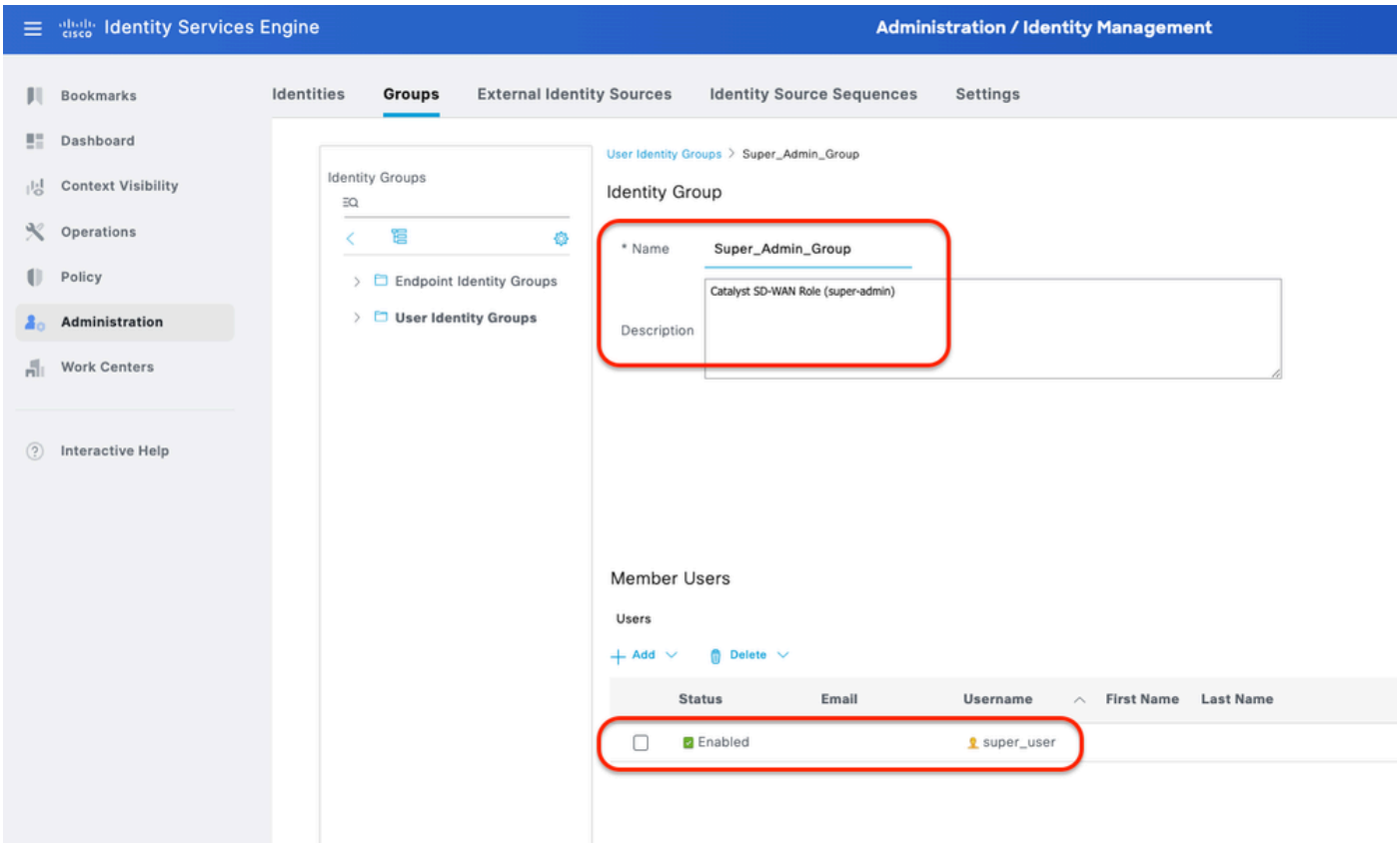
Profil TACACS+ - (Catalyst_SDWAN_ReadOnly)

Étape 4. Créer un groupe d'utilisateurs ajouter des utilisateurs locaux en tant que membre

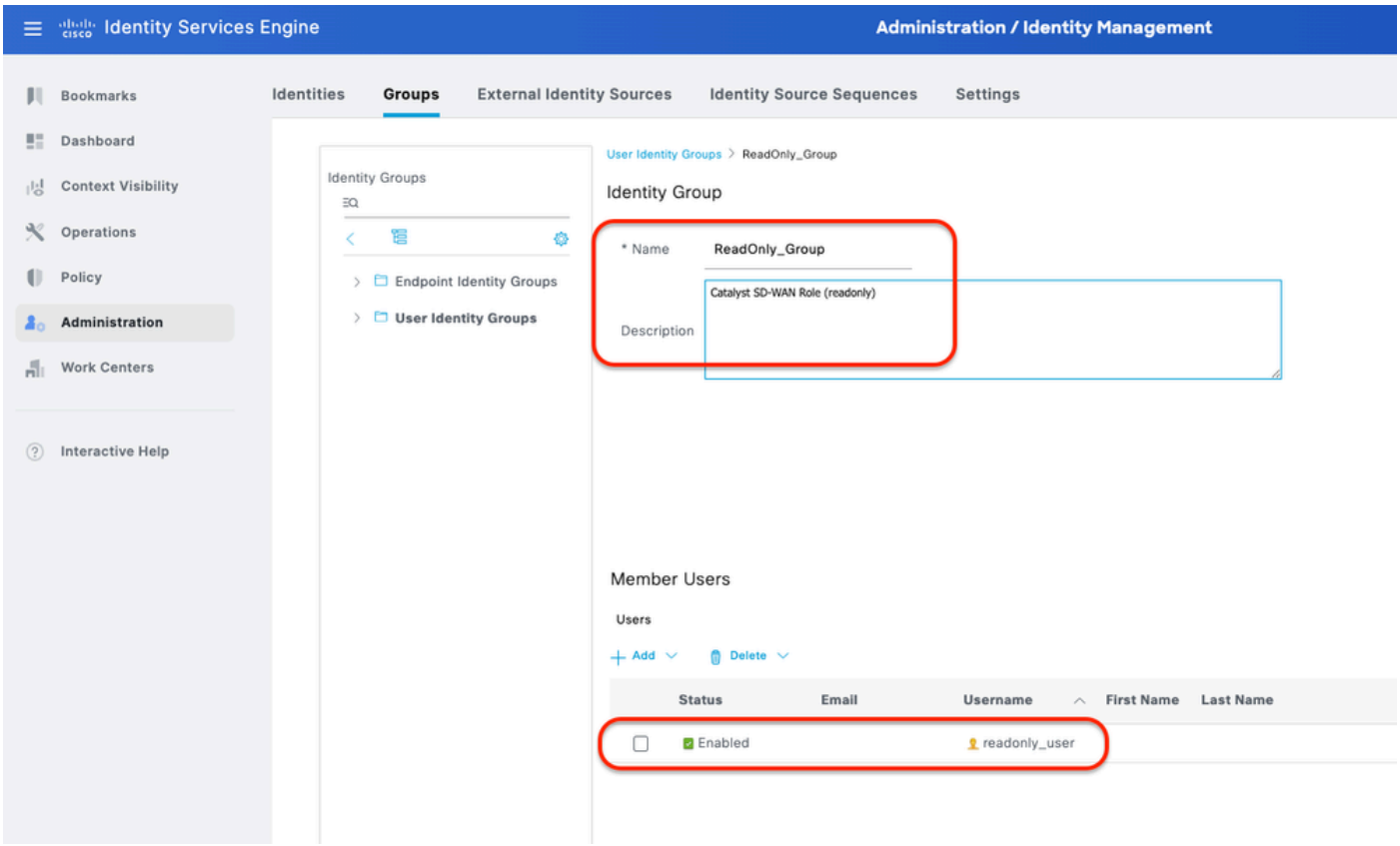
Pour ce faire, accédez à l'onglet Work Centers > Device Administration > User Identity Groups.

Créez deux groupes d'identités utilisateur :

1. Groupe_Admin_Supérieur
2. Groupe_LectureSeule



Groupe d'identités utilisateur - (Super_Admin_Group)



Groupe d'identités utilisateur - (ReadOnly_Group)

Étape 5. (Facultatif) Ajouter un jeu de stratégies TACACS+.

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets.

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

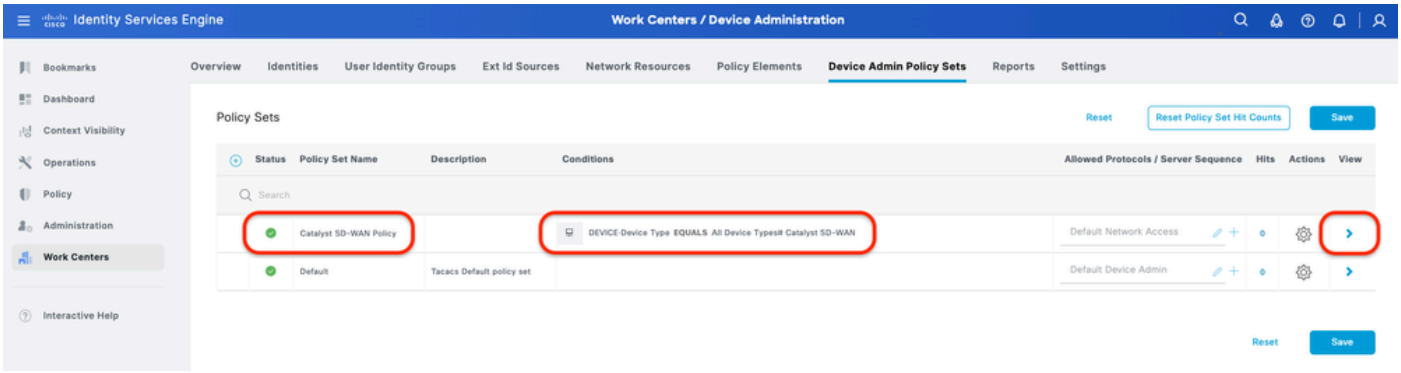
b. Définissez le nom du jeu de stratégies.

c. Définissez la condition du jeu de stratégies sur Sélectionner le type de périphérique précédemment créé (Étape 2 > b).

d. Définissez les protocoles autorisés.

e. Cliquez sur Save.

f. Cliquez sur (>) Policy Set View pour configurer les règles d'authentification et d'autorisation.



Ensemble de stratégies ISE

Étape 6 : configuration de la stratégie d’authentification TACACS+

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets > Cliquez sur (>).

Procédure

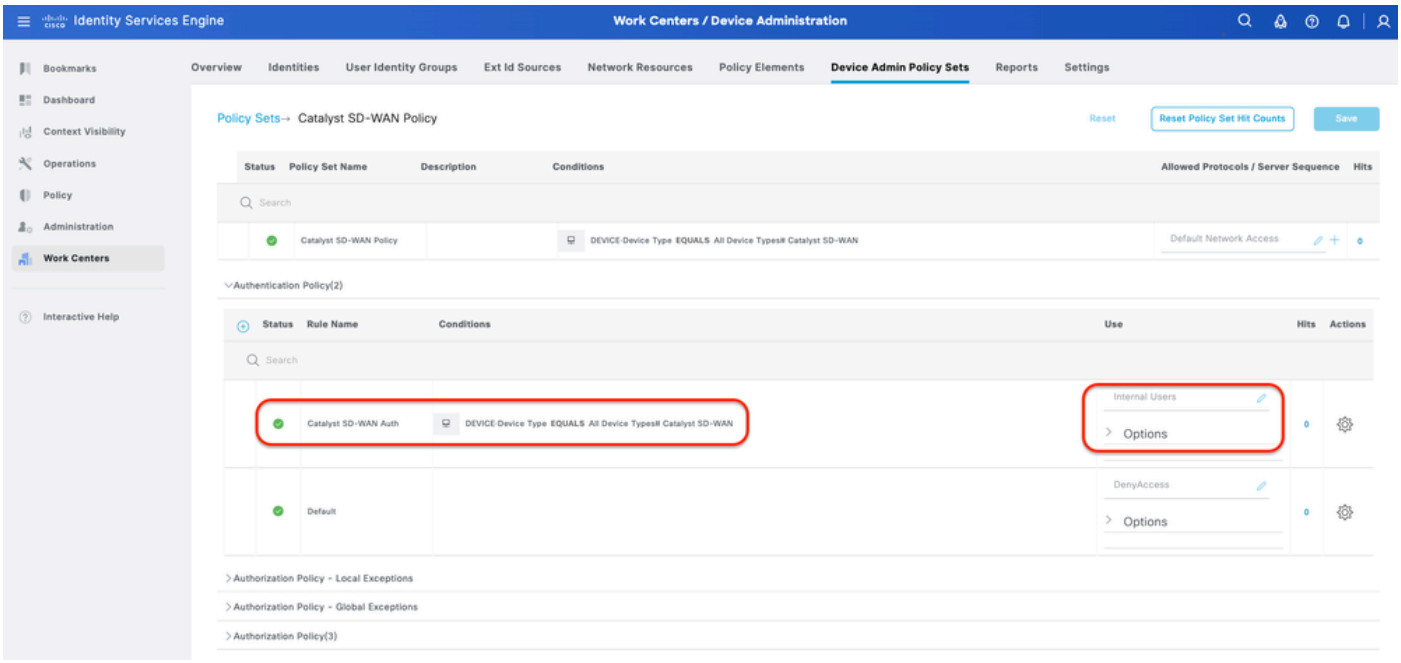
a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom de la stratégie d'authentification.

c. Définissez la condition de stratégie d'authentification et sélectionnez le type de périphérique que vous avez créé précédemment (Étape 2 > b).

d. Définissez l'option Authentication Policy Use for Identity source.

e. Cliquez sur Save.



Stratégie d'authentification

Étape 7 : configuration de la stratégie d’autorisation TACACS+

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets > Cliquez sur (>).

Cette étape de création d'une politique d'autorisation pour chaque rôle SD-WAN Catalyst :

- Catalyst SD-WAN Authz (super-admin) : super-administrateur
- Catalyst SD-WAN Authz (lecture seule) : en lecture seule

Procédure

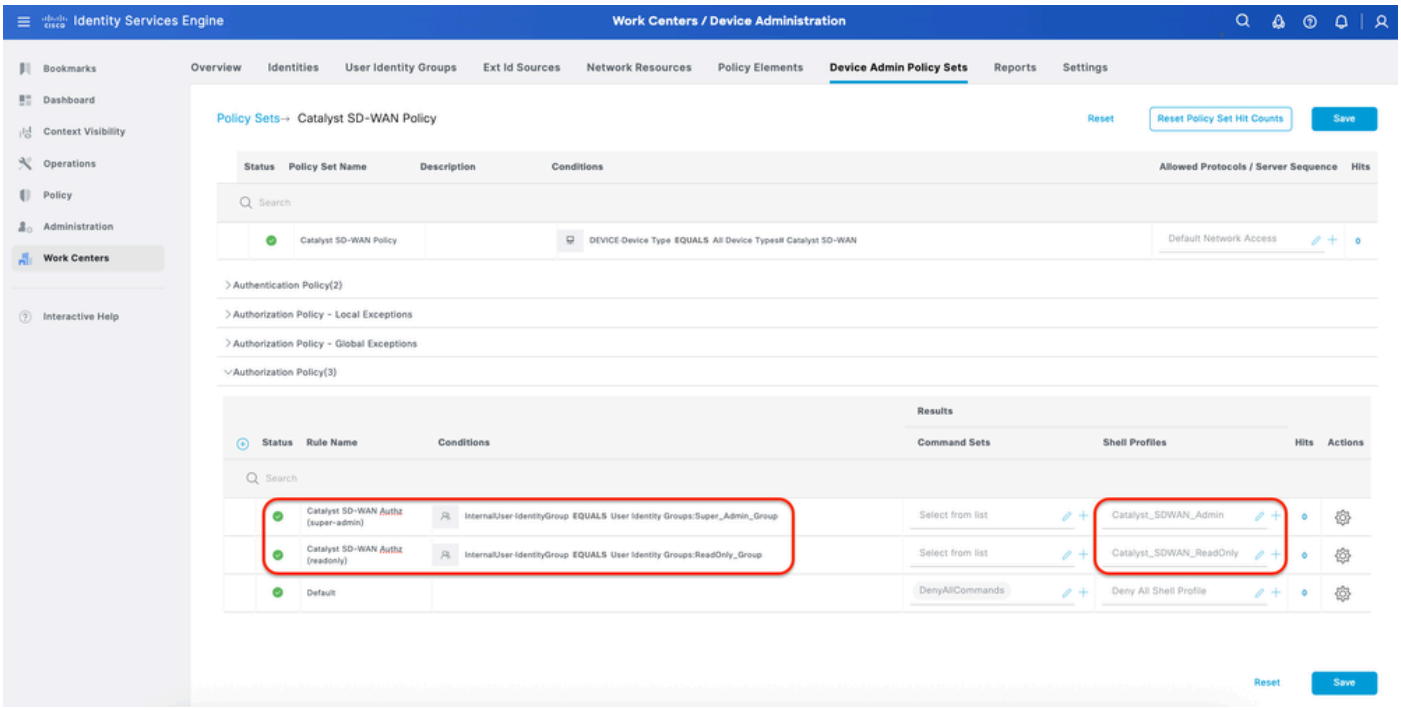
a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom de la stratégie d'autorisation.

c. Définissez la condition de stratégie d'autorisation et sélectionnez le groupe d'utilisateurs que vous avez créé à l' (étape 4).

d. Définissez les profils PolicyShell d'autorisation et sélectionnez le profil TACACS que vous avez créé à l' (étape 3).

e. Cliquez sur Save.

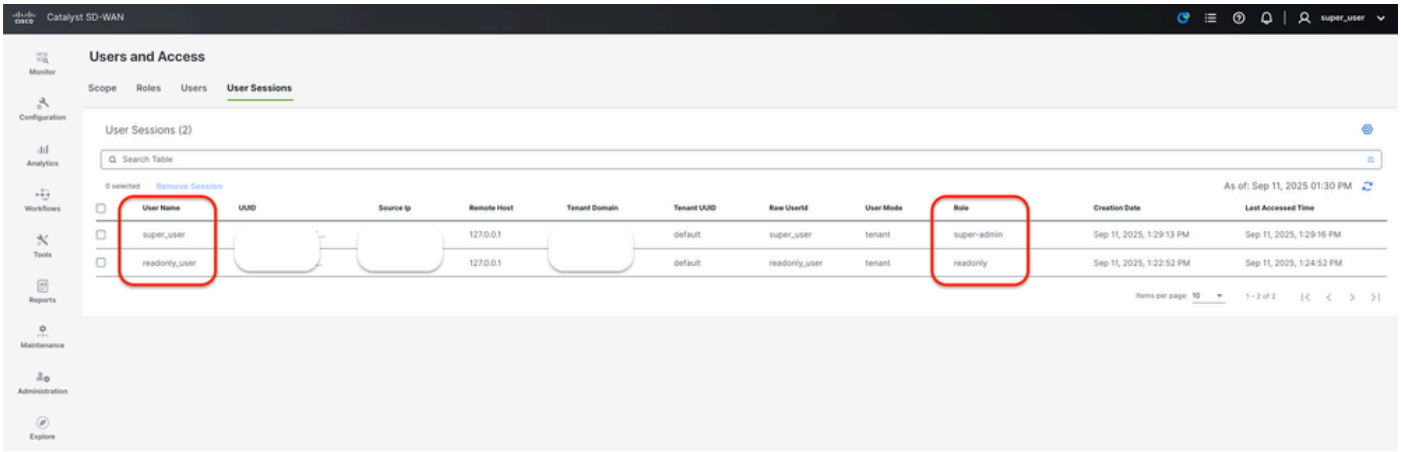


Politique d'autorisation

Vérification de la configuration TACACS+

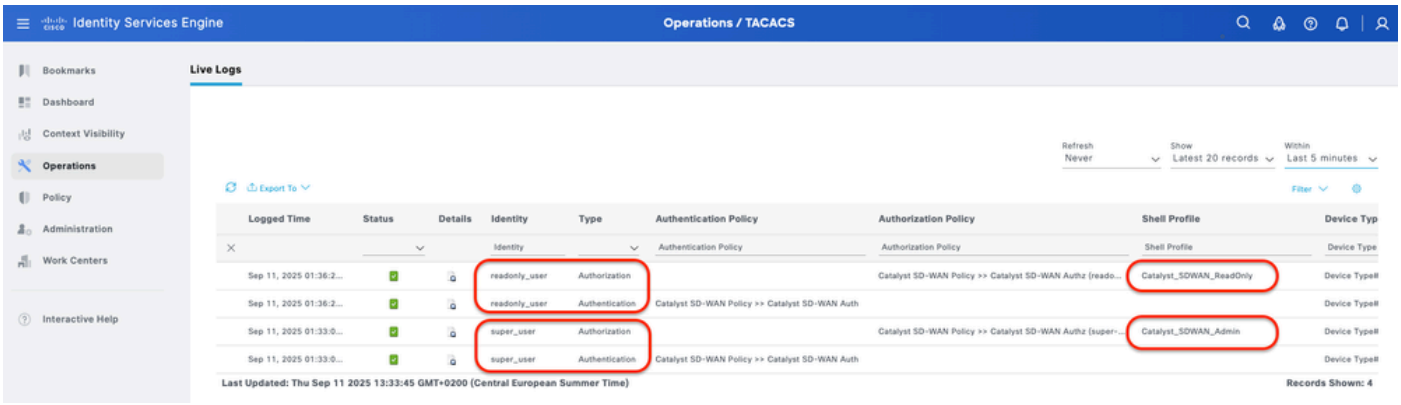
1- Afficher les sessions utilisateur Catalyst SD-WAS Catalyst SD-WAN : Administration > Users and Access > User Sessions.

Vous pouvez afficher la liste des utilisateurs externes qui se sont connectés via RADIUS pour la première fois. Les informations affichées incluent leurs noms d'utilisateur et leurs rôles.



Sessions utilisateur Catalyst SD-WAS

2- ISE - Opérations TACACS Live-Logs > TACACS > Live-Logs.



Journaux en direct

Protocol	Tacacs
Type	Authorization
Service-Argument	ppp
Protocol-Argument	ip
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Network Access
RequestLatency	27
IdentityGroup	User Identity Groups:ReadOnly_Group
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	316584755210.127.198.7438561Authorization3165847552
IdentitySelectionMatchedRule	Catalyst SD-WAN Auth
StepLatency	1=0;2=0;3=4;4=3;5=4;6=0;7=2;8=1;9=0;10=8;11=2;12=3;13=0;14=0;15=0
TotalAuthenLatency	27
ClientLatency	0
TacacsPlusTLS	false
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Viptela-User-Group=readonly; }

Journaux en direct détaillés - (lecture seule)

Protocol	Tacacs
Type	Authorization
Service-Argument	ppp
Protocol-Argument	ip
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Network Access
RequestLatency	30
IdentityGroup	User Identity Groups:Super_Admin_Group
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	354536652810.127.198.7460535Authorization3545366528
IdentitySelectionMatchedRule	Catalyst SD-WAN Auth
StepLatency	1=1;2=0;3=3;4=3;5=3;6=0;7=2;8=0;9=0;10=10;11=4;12=4;13=0;14=1;15=0
TotalAuthenLatency	30
ClientLatency	0
TacacsPlusTLS	false
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Viptela-User-Group=super-admin; }

Dépannage

Aucune information de diagnostic spécifique n'est actuellement disponible pour cette configuration.

Références

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.4
- Guide de configuration des interfaces et systèmes SD-WAN de Cisco Catalyst, Cisco IOS XE Catalyst SD-WAN version 17.x

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.