

Configuration de SNMPv3 sur Catalyst SD-WAN

Table des matières

[Introduction](#)

[Fond](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Vérifier](#)

[Références](#)

Introduction

Ce document décrit la configuration SNMPv3 et explique la sécurité (authentification), le chiffrement (confidentialité) et la restriction (affichage).

Fond

Souvent, la configuration SNMPv3 est considérée comme complexe et difficile à configurer, jusqu'à ce que nous sachions ce qui doit être fait. La raison de l'existence de SNMPv3 est similaire à HTTPS : pour la sécurité, le chiffrement et les restrictions.

Conditions préalables

Connaissance des modèles de fonctionnalités SD-WAN et des modèles de périphériques.

Compréhension générale de SNMP MIB, SNMP Poll et SNMP Walk

Exigences

Contrôleurs SD-WAN

Routeur de périphérie Cisco

Composants utilisés

Contrôleurs SD-WAN sur 20.9

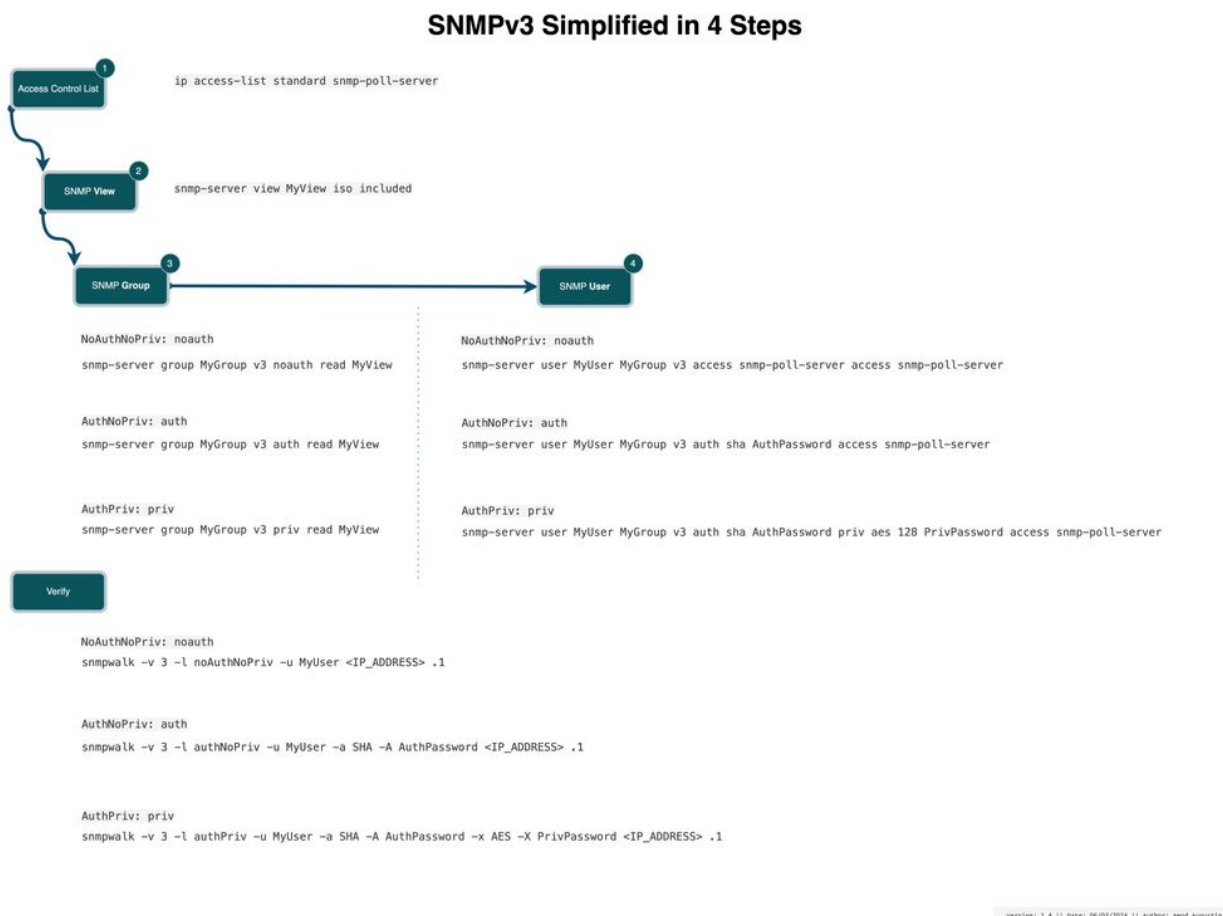
Routeur de périphérie Cisco sur 17.9

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

Le schéma vous aide à comprendre tous les éléments requis pour configurer SNMPv3 du point de vue de l'interface de ligne de commande.



SNMPv3 simplifié en 4 étapes

Une fois que vous avez compris, il est facile de placer le concept dans l'interface de ligne de commande ou un modèle de fonction. Plongeons à l'intérieur.

Étape 1 :

Configurez une liste de contrôle d'accès pour autoriser les personnes autorisées à interroger le système (le routeur dans notre cas).

```
ip access-list standard snmp-poll-server
```

Étape 2 :

Définissez une vue snmp, car le terme implique ce à quoi l'interrogateur a accès, c'est notre restriction.

```
snmp-server view MyView iso included
```

Étape 3 :

Définissez le groupe snmp, le groupe snmp comporte principalement deux parties a. Niveau de sécurité b. Restriction (affichage).

Niveaux de sécurité :

- noAuthNoPriv : Aucune authentification et aucune confidentialité (pas de cryptage).
- authNoPriv : L'authentification est requise, mais pas la confidentialité.
- authPriv : L'authentification et la confidentialité sont requises.

La restriction est ce que nous avons défini à l'étape 2, mettons-les tous ensemble.

```
!NoAuthNoPriv: noauth
snmp-server group MyGroup v3 noauth read MyView
```

```
!AuthNoPriv: auth
snmp-server group MyGroup v3 auth read MyView
```

```
!AuthPriv: priv
snmp-server group MyGroup v3 priv read MyView
```

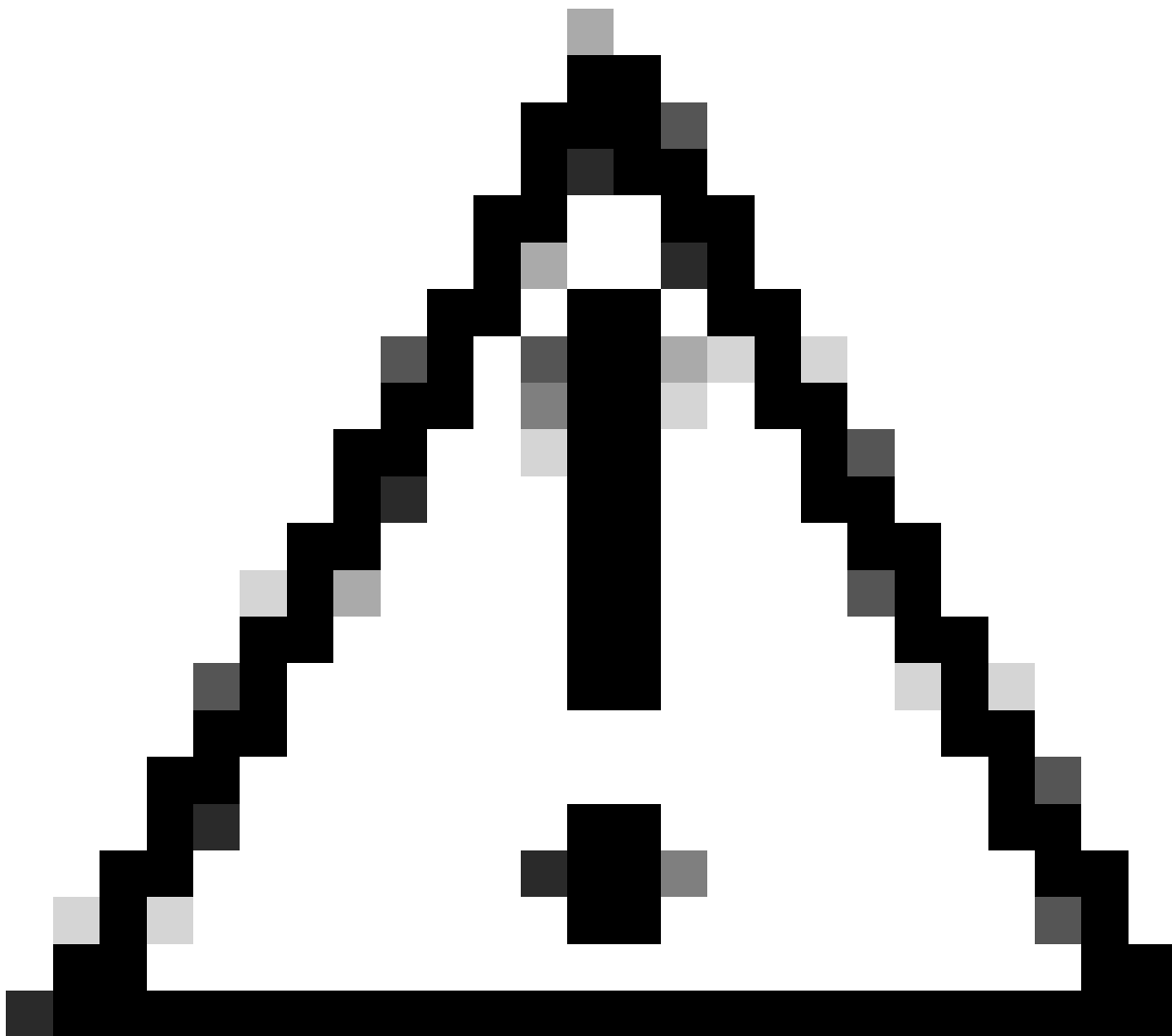
Étape 4 :

Dans cette étape, nous associons le groupe à un utilisateur, associons chaque groupe à des utilisateurs définissant l'authentification et la confidentialité respectives (cryptage) et pouvons être sécurisés davantage à l'aide de la liste de contrôle d'accès.

```
!NoAuthNoPriv: noauth
snmp-server user MyUser MyGroup v3 access snmp-poll-server
```

```
!AuthNoPriv: auth
snmp-server user MyUser MyGroup v3 auth sha AuthPassword access snmp-poll-server
```

```
!AuthPriv: priv
snmp-server user MyUser MyGroup v3 auth sha AuthPassword priv aes 128 PrivPassword access snmp-poll-server
```



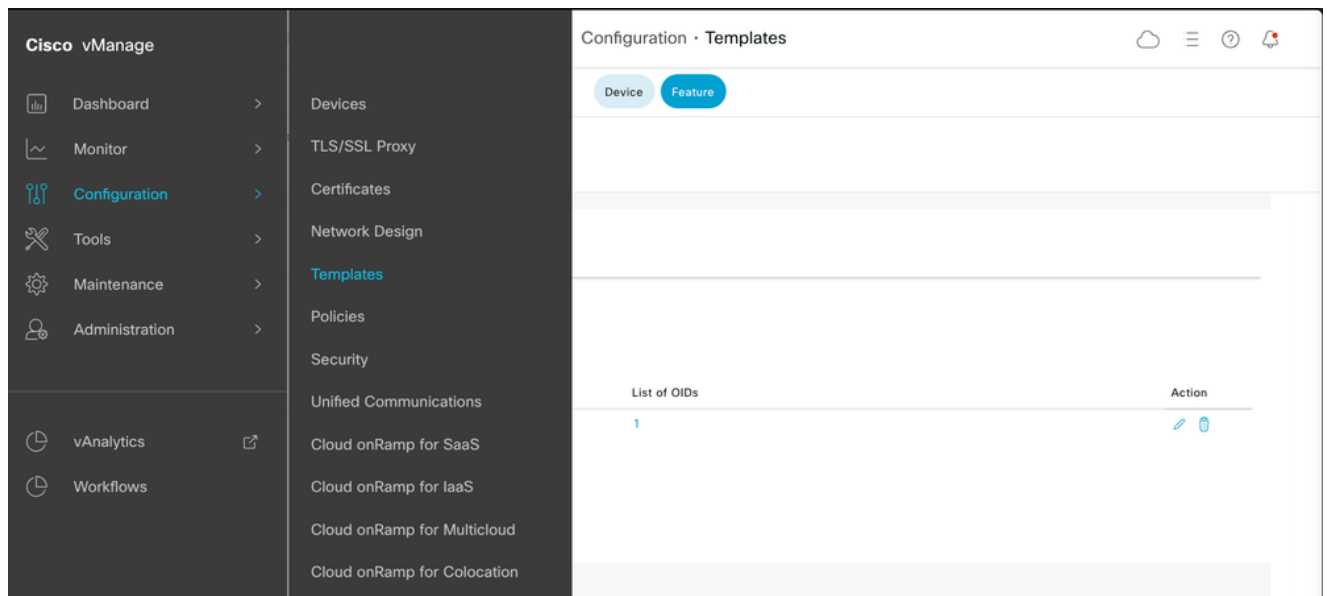
Mise en garde : Vous pouvez remarquer que lorsque vous essayez de configurer l'utilisateur `snmp-server`, l'aide contextuelle n'est pas disponible et n'apparaît pas non plus dans la configuration en cours, ceci est conforme à la RFC 3414. Entrez la commande complète et l'analyseur accepte la configuration

```
cEdge-RT01(config)# snmp-server user ? ^ % Invalid input detected at '^' marker.
```

ID de bogue Cisco [CSCvn71472](https://tools.cisco.com/tips/configuration/CSCvn71472.html)

Félicitations, c'est tout ce dont nous avons besoin. Maintenant que vous connaissez l'interface de ligne de commande et le concept, voyons comment configurer à l'aide du modèle de fonction SNMP sur un gestionnaire SD-WAN Catalyst

Accédez à Cisco vManage > Configuration > Templates > Feature



Modèle de fonction

Accédez à Cisco SNMP, que vous trouverez dans la section Other Template

DeviceFeature

Feature Template > Add Template

Select Devices

Q c8300

☐ C8300-1N1S-4T2X

☒ C8300-1N1S-6T

☐ C8300-2N2S-4T2X

☐ C8300-2N2S-6T

WAN

OTHER TEMPLATES

Cli Add-On Template

WAN

AppQoE

Cellular Controller

WAN

Cellular Profile

WAN

Cisco Banner

Cisco BGP

WAN

LAN

Cisco DHCP Server

LAN

Cisco IGMP

LAN

Cisco Logging

Cisco Multicast

Cisco OSPF

WAN

LAN

Cisco OSPFV3

WAN

LAN

Cisco PIM

LAN

Cisco SIG Credentials

Cisco SNMP

EIGRP

LAN

GPS

WAN

Probes

Fonction SNMP

Définissez la vue SNMP (restriction), c'est notre étape 2

Device TypeC8300-1N1S-6T

Template NameCisco_SNMPv3

DescriptionCisco_SNMPv3

SNMP SNMP Version

SNMP

Shutdown

Yes

No

Contact Person

Location of Device

SNMP VERSION

SNMP Version ☐ V2 ☒ V3

VIEW & GROUP

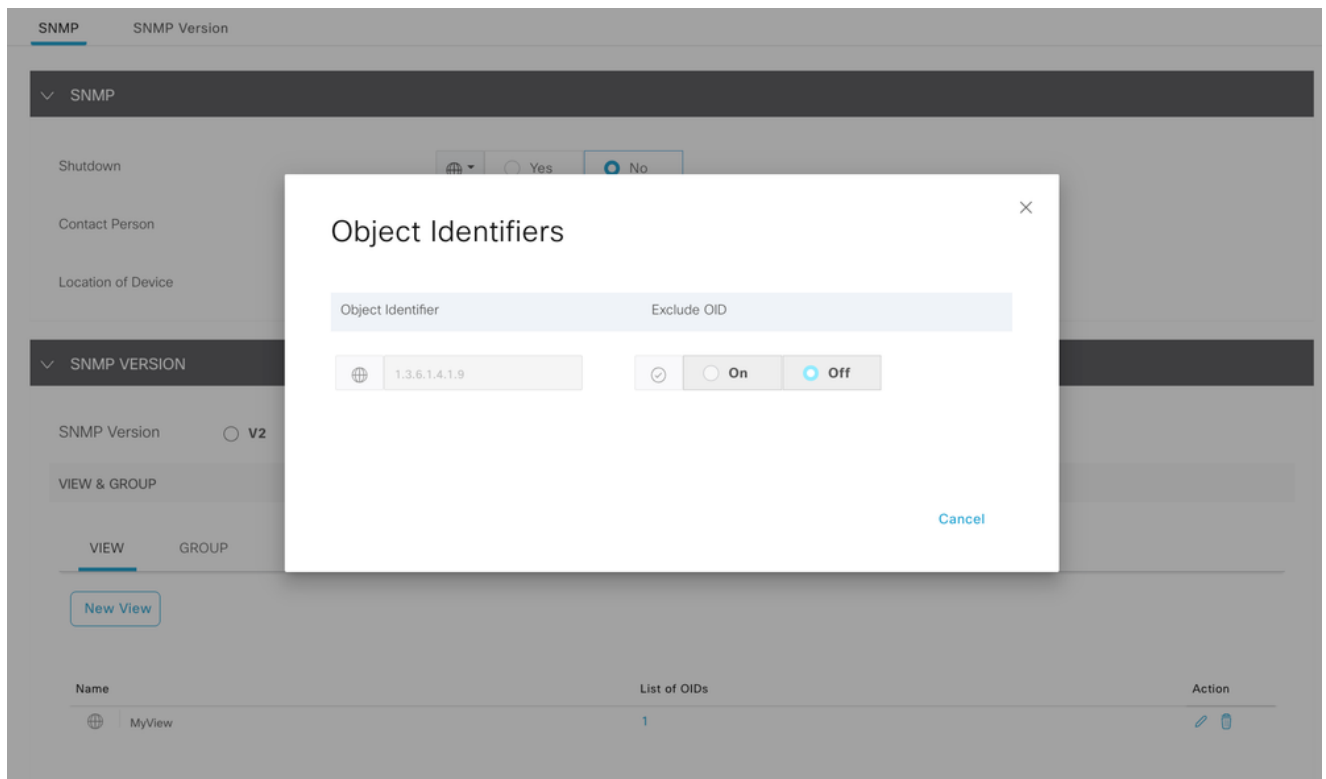
2

VIEWGROUP

New View

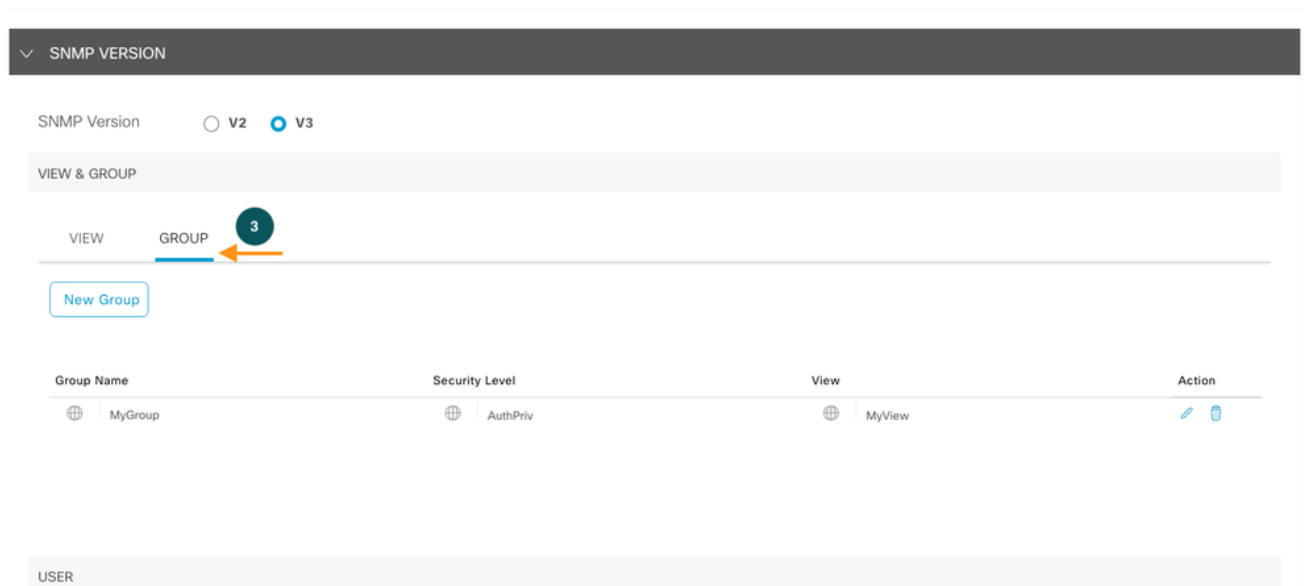
Name	List of OIDs	Action
MyView	1	

Vue SNMP



OID SNMP

Définissez le groupe SNMP. Il s'agit de l'étape 3



Groupe SNMP

3

Update Group

Name

MyGroup

Security Level

AuthPriv

View

MyView

Save Changes

Cancel

Groupe SNMP

Définissez le groupe d'utilisateurs. Il s'agit de l'étape 4 au cours de laquelle nous définissons l'authentification et le mot de passe de cryptage.

Feature Template > Cisco SNMP > Cisco_SNMPv3

SNMP

SNMP Version

VIEW

GROUP

New Group

Group Name	Security Level	View	Action
MyGroup	AuthPriv	MyView	

USER

New User

Username	Authentication Type	Authentication Password	Privacy Type	Privacy Password	Action
MyUser	SHA		AES-CFB-128		
MyGroup					

Utilisateur SNMP

4

Update User

User

MyUser

Authentication Protocol

SHA

Authentication Password

.....

Privacy Protocol

AES-CFB-128

Privacy Password

.....

Group

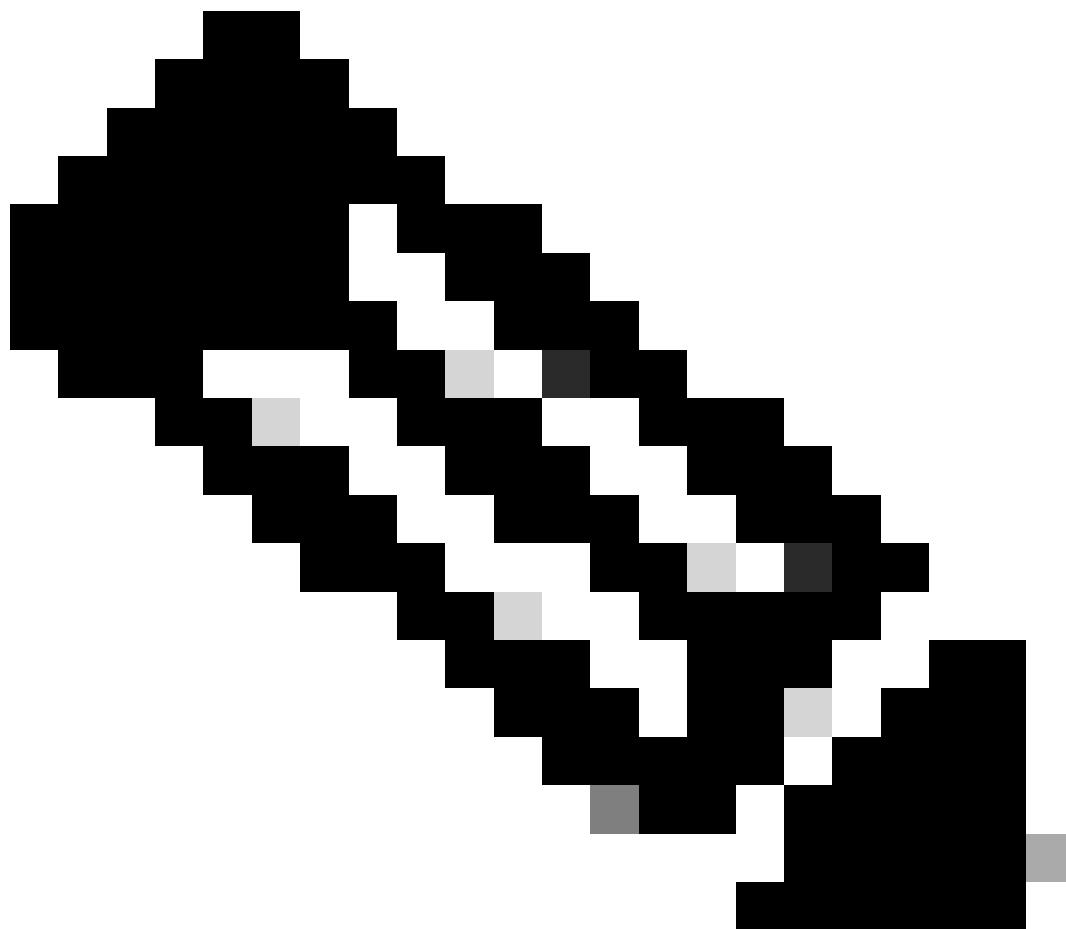
MyGroup

Save Changes

Cancel

- TARGET SERVER

Cryptage utilisateur SNMP



Remarque : En fonction du niveau de sécurité du groupe SNMP, les champs associés à l'utilisateur sont activés.

Maintenant, joignez le modèle de fonction au modèle de périphérique.

Additional Templates

AppQoE	Choose...
Global Template *	Factory_Default_Global_CISCO_Templ... ⓘ
Cisco Banner	Choose...
Cisco SNMP	Cisco_SNMPv3
ThousandEyes Agent	Choose...
TrustSec	Choose...
CLI Add-On Template	Choose...
Policy	Choose...
Probes	Choose...
Security Policy	Choose...

Modèle de fonctionnalité SNMP

Vérifier

```
Router#show snmp user
```

```
User name: MyUser
Engine ID: 800000090300B8A3772FF870
storage-type: nonvolatile    active    access-list: snmp-poll-server
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: MyGroup
```

À partir d'une machine sur laquelle snmpwalk est installé, vous pouvez exécuter la commande pour vérifier la réponse SNMP pour le niveau de sécurité correspondant

```
!NoAuthNoPriv: noauth
snmpwalk -v 3 -l noAuthNoPriv -u MyUser
```

.1

```
!AuthNoPriv: auth
snmpwalk -v 3 -l authNoPriv -u MyUser -a SHA -A AuthPassword
```

.1

```
!AuthPriv: priv
```

```
snmpwalk -v 3 -l authPriv -u MyUser -a SHA -A AuthPassword -x AES -X PrivPassword
```

.1

-v : Version (3)

-l : Niveau de sécurité

-A : phrase de passe du protocole d'authentification

-X : phrase de passe du protocole de confidentialité

Références

- [Configuration du déroulement SNMPv3 sur le routeur de périphérie Cisco](#)
- [Modèle de configuration pour SNMPv3](#) par Tim Glen

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.