

SNMPv3 configureren op Catalyst SD-WAN

Inhoud

[Inleiding](#)

[Achtergrond](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Referenties](#)

Inleiding

In dit document wordt de SNMPv3-configuratie beschreven en wordt uitleg gegeven over beveiliging (verificatie), codering (privacy) en beperking (weergave).

Achtergrond

Vaak wordt SNMPv3-configuratie gezien als complex en moeilijk te configureren, totdat we weten wat er moet worden gedaan. De reden voor het bestaan van SNMPv3 is vergelijkbaar met HTTPS: voor beveiliging, codering en beperking.

Voorwaarden

Kennis van SD-WAN-functiesjablonen en apparaatsjablonen.

Algemeen inzicht in SNMP MIB, SNMP Poll en SNMP Walk

Vereisten

SD-WAN-controllers

Cisco Edge Router

Gebruikte componenten

SD-WAN-controllers op 20.9

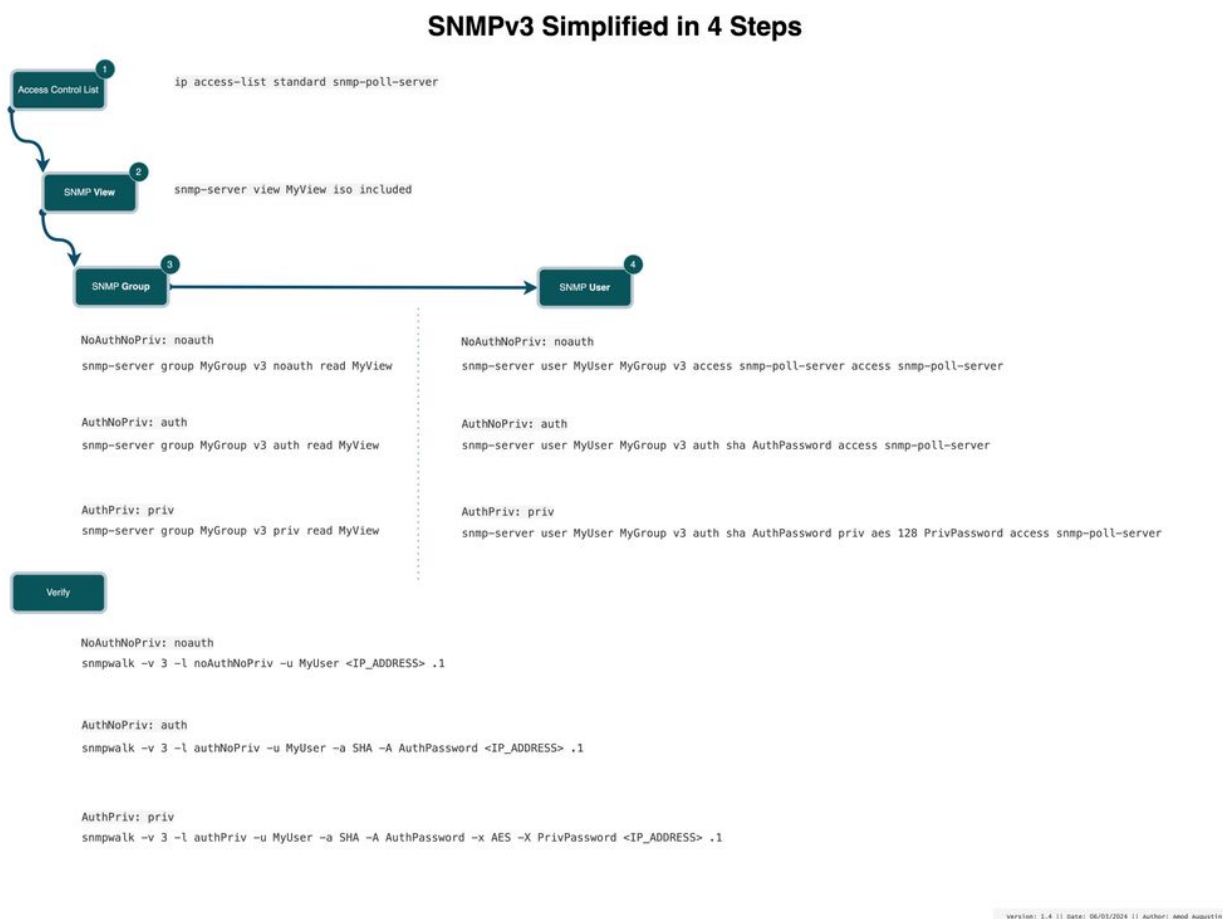
Cisco Edge Router op 17,9

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Het diagram helpt u te begrijpen wat er allemaal nodig is om SNMPv3 vanuit een CLI-standpunt te configureren.



SNMPv3 in 4 stappen vereenvoudigd

Zodra u begrijpt dat het gemakkelijk is om het concept in CLI of een functiesjabloon te plaatsen. Laten we erin duiken.

Stap 1:

Configureer een ACL om te bepalen wie het systeem kan pollen (router in ons geval).

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

Stap 2:

Definieer een snmp-weergave, omdat de term impliceert waartoe mibs de poller toegang heeft, dit is onze beperking.

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

Stap 3:

Definieer de snmp groep, de snmp groep bestaat voornamelijk uit twee delen a. Beveiligingsniveau b. Beperking (weergave).

Beveiligingsniveaus:

- noAuthNoPriv: Geen authenticatie en geen privacy (geen encryptie).
- authNoPriv: Authenticatie is vereist, maar geen privacy.
- authPriv: Zowel authenticatie als privacy zijn vereist.

Beperking is wat we in stap 2 hebben gedefinieerd, laten we ze allemaal samenvoegen.

```
!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
```

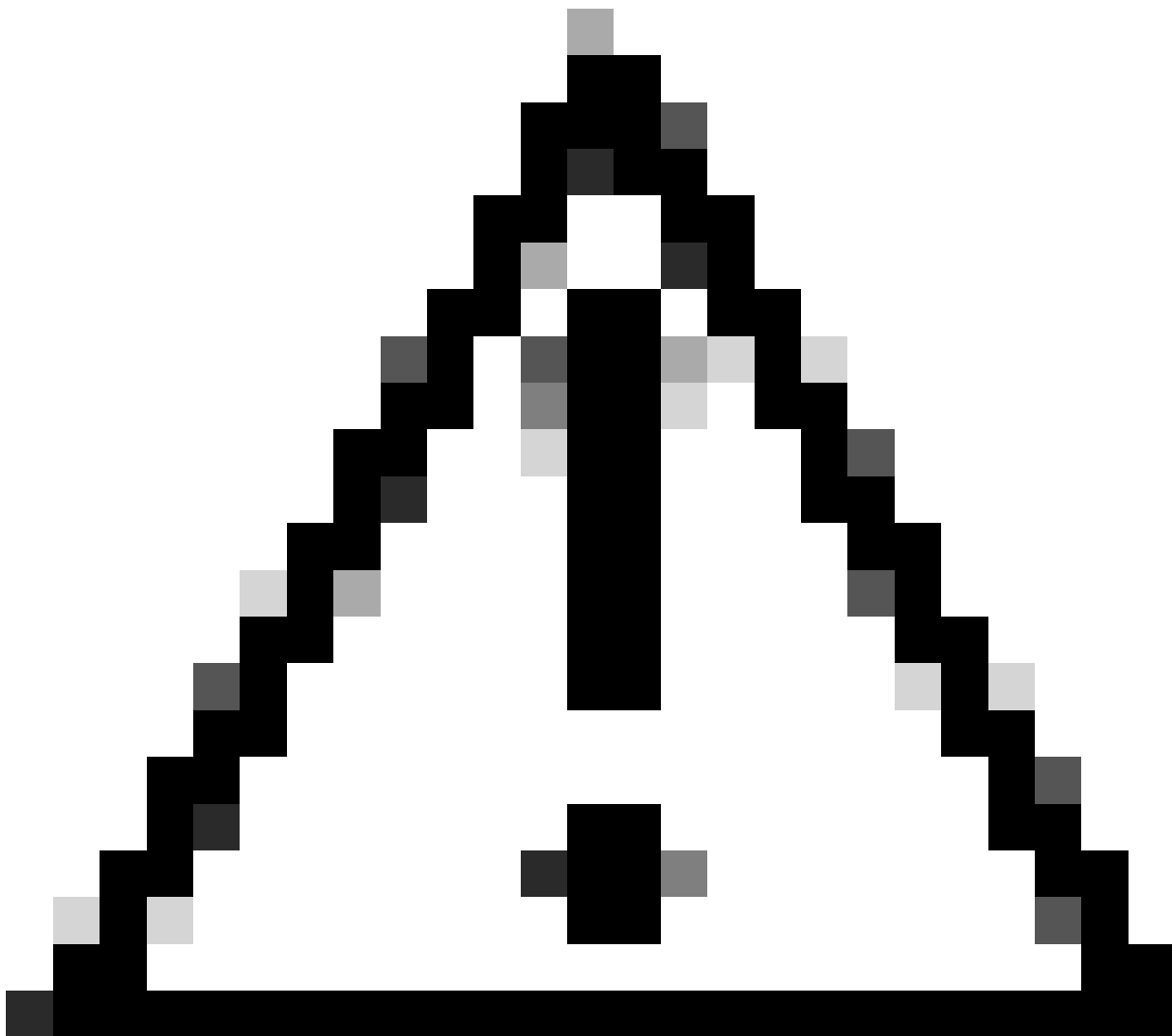
Stap 4:

In deze stap koppelen we de groep aan een gebruiker, koppelen we elke groep aan gebruikers die de respectieve verificatie en privacy (codering) definiëren en kunnen we verder worden beveiligd met behulp van de toegangscontrolelijst.

```
!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
```



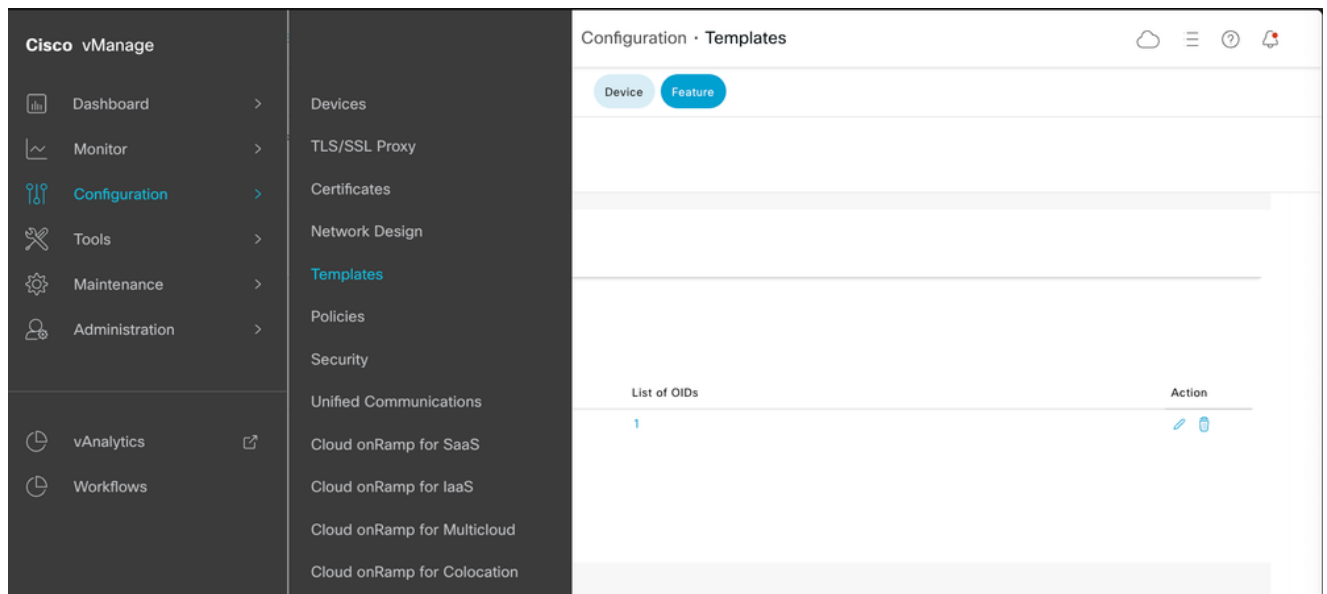
Let op: U kunt merken wanneer u probeert te configureren snmp-server gebruiker de context hulp is niet beschikbaar en ook niet getoond in lopende configuratie dit is om te voldoen aan RFC 3414. Typ de volledige opdracht in en de parser accepteert de configuratie

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

Cisco bug ID [CSCvn71472](#)

Gefeliciteerd, dat is alles wat nodig is. Nu u de cli en het concept kent, kunt u zien hoe u kunt configureren met behulp van SNMP-functiesjabloon op een Catalyst SD-WAN-beheer

Navigeer naar Cisco vManage > Configuratie > Sjablonen > Functie



• Functiesjabloon

Navigeer naar Cisco SNMP, die u kunt vinden in de sectie Andere sjablonen

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

WANLAN

Cisco DHCP Server

LAN

Cisco IGMP

LAN

Cisco Logging

Cisco Multicast

Cisco OSPF

WANLAN

Cisco OSPFV3

WANLAN

Cisco PIM

LAN

Cisco SIG Credentials

Cisco SNMP

EIGRP

LAN

GPS

WAN

Probes

SNMP-voorziening

SNMP-weergave definiëren (beperking), dit is onze stap 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

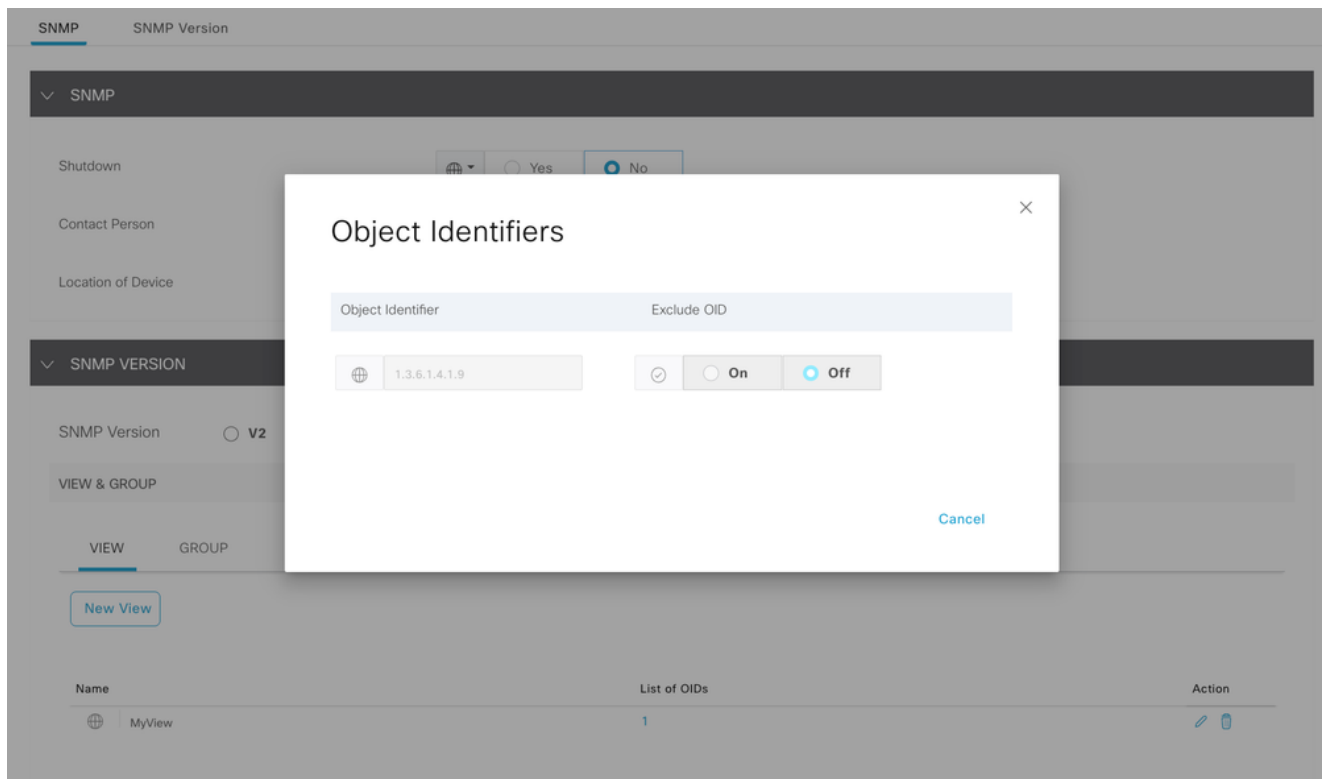
VIEW

GROUP

New View

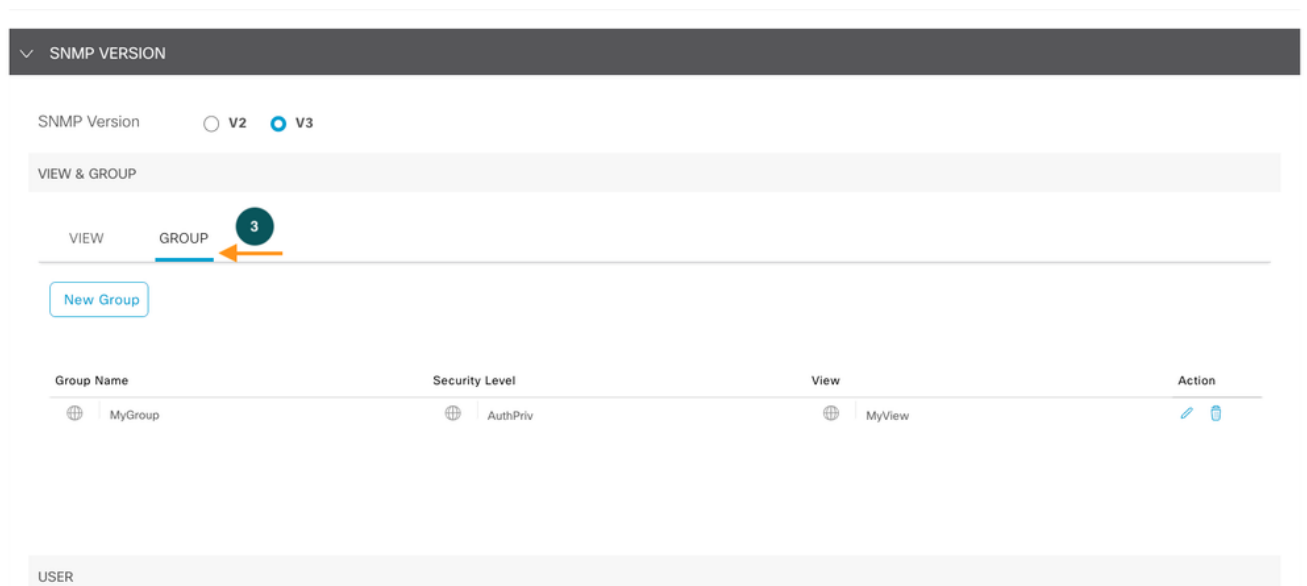
Name	List of OIDs	Action
MyView	1	

SNMP-weergave



SNMP OID

Definieer de SNMP-groep. Dit is onze stap 3



SNMP-groep

3

Update Group

Name

MyGroup

Security Level

AuthPriv

View

MyView

Save Changes

Cancel

SNMP-groep

Definieer gebruikersgroep, dit is onze stap 4 waarin we het verificatie- en coderingswachtwoord definiëren.

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

4

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

SNMP-gebruiker

4

Update User

User

MyUser

Authentication Protocol

SHA

Authentication Password

.....

Privacy Protocol

AES-CFB-128

Privacy Password

.....

Group

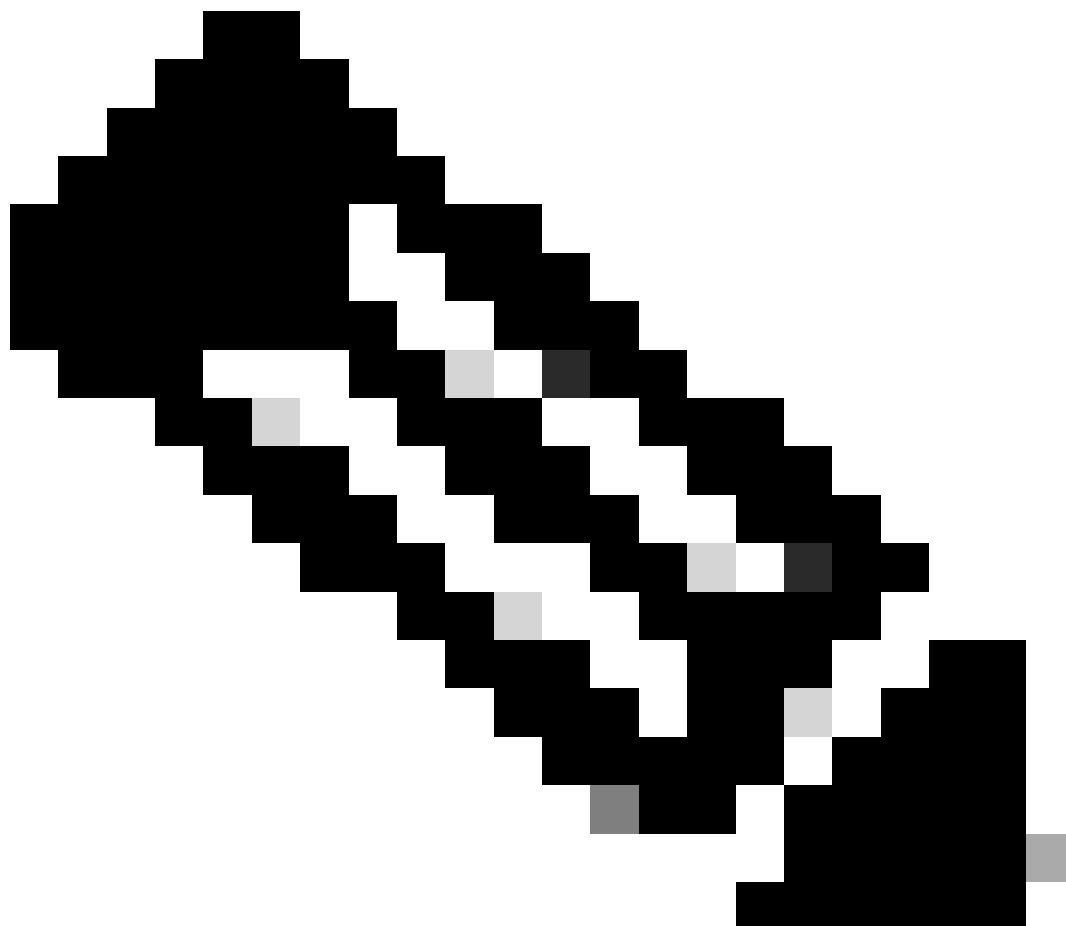
MyGroup

Save Changes

Cancel

- TARGET SERVER

SNMP-gebruikerscodering



Opmerking: op basis van het beveiligingsniveau van de SNMP-groep wordt het betreffende veld voor de gebruiker ingeschakeld.

Voeg nu de functiesjabloon toe aan de apparaatsjabloon.

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...

SNMP-functiesjabloon

Verifiëren

```
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
```

Vanaf een systeem waarop snmpwalk is geïnstalleerd, kunt u de opdracht uitvoeren om de SNMP-respons te verifiëren voor het respectieve beveiligingsniveau

```
!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: Versie (3)

-l: beveiligingsniveau

-A: wachtwoordgroep voor verificatieprotocol

-X: wachtwoordgroep voor privacyprotocol

Referenties

- [SNMPv3 Trap configureren op Cisco Edge Router](#)
- [Configuratiesjabloon voor SNMPv3](#) door Tim Glen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.