

Exclure l'OID dans les configurations Nexus 5k, 7k et 9K dans SNMP v2 et v3

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Étapes de base](#)

[Configuration](#)

[Vérification](#)

Introduction

Ce document décrit comment exclure OID dans Nexus 5k, 7k, et 9K dans la configuration SNMP v2 et v3.

Conditions préalables

Exigences

Cisco recommande de connaître ces sujets avant d'implémenter des exclusions OID (Object Identifier) :

- Connaissance du protocole SNMP (Simple Network Management Protocol)
- Accès au mode de configuration des périphériques
- Compréhension des OID à exclure
- Compréhension de la communauté SNMP et des configurations utilisateur

Composants utilisés

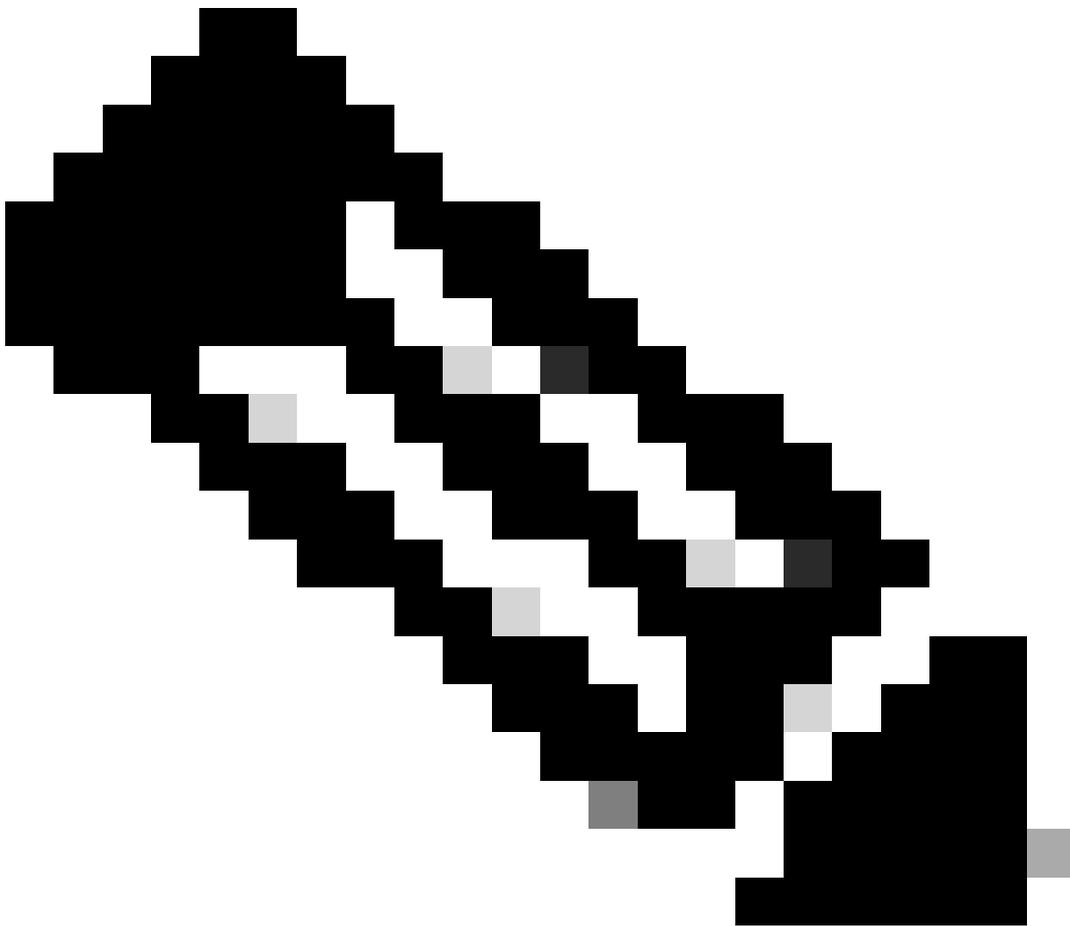
Les informations contenues dans ce document sont basées sur le test effectué en laboratoire avec les modèles Nexus suivants :

- Nexus 5K
- Nexus 7K
- Nexus 9K

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.

Informations générales

Dans le monde du SNMP, vous rencontrez souvent des situations où l'analyse de l'arborescence de la base d'informations de gestion (MIB) fait face à des obstacles, atteignant un arrêt à des OID spécifiques, conduisant parfois à des délais d'attente de fenêtre ou à des problèmes similaires. Un autre défi courant survient lorsque l'interrogation continue d'un OID problématique déclenche des alertes qui ne sont ni nécessaires ni percutantes. Une façon possible de se débarrasser de ces types de scénarios est de créer des exclusions, en demandant au périphérique d'ignorer cet OID spécifique et de poursuivre avec le reste de la structure MIB. En demandant au périphérique de contourner l'OID problématique et de poursuivre avec le reste de la structure MIB, vous pouvez favoriser un flux fluide de l'arborescence MIB.



Remarque : il est important de noter que cette exclusion peut affecter la façon dont nous lisons les données de l'arborescence MIB. Faites preuve de prudence et assurez-vous de la nécessité du RAO avant de procéder à ces exclusions.

Alors que l'exclusion des OID suit généralement un processus simple dans les périphériques tels que les routeurs à services d'agrégation (ASR)/commutateurs Catalyst (CAT)/routeurs à services intégrés (ISR), la navigation dans ce défi dans les périphériques Nexus s'avère plus complexe en raison de l'absence de vues. Cet article explore une approche innovante en présentant les rôles et en les mappant à la communauté/l'utilisateur, et présente une solution pour exclure les OID dans les configurations SNMP v2 et v3 sur les périphériques Nexus 5k, 7k et 9K.

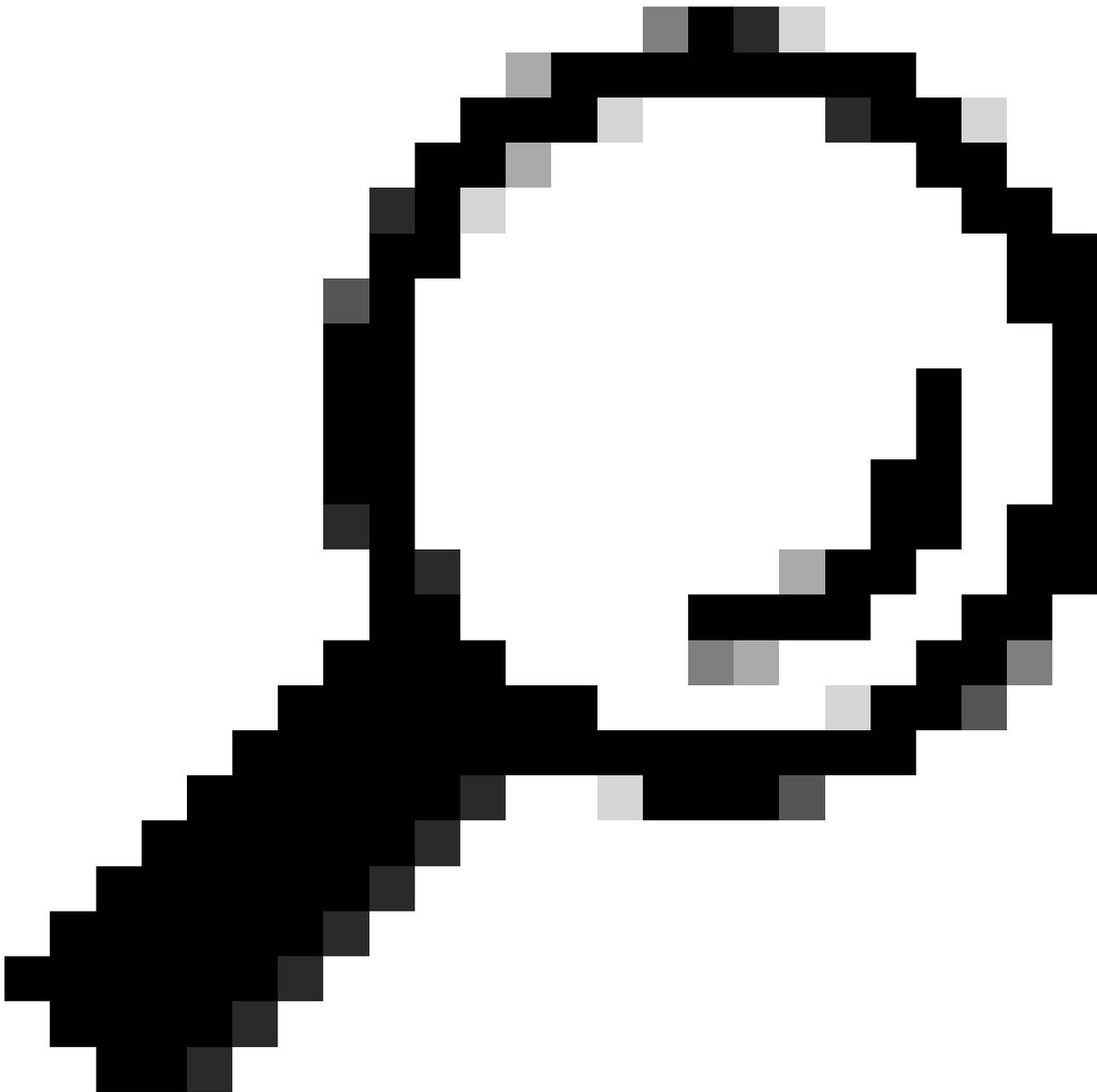
Étapes de base

Accéder au mode de configuration :

```
#conf t
```

Définir le rôle de l'exclusion OID :

```
#role name <name_of_role>  
#rule 1 permit read feature snmp  
#rule 2 deny {read/ read-write} oid <oid_you_want_to_exclude>
```



Conseil : {read/ read-write} vous permet de choisir entre les opérations SNMP 'read' et 'read-write'. Les opérations de lecture impliquent généralement la récupération d'informations, tandis que les opérations de lecture-écriture impliquent à la fois la récupération et la modification d'informations. Vous pouvez choisir lecture/lecture-écriture selon vos préférences.

Quittez le mode de configuration :

`#exit`

Application de la configuration à la communauté/utilisateur SNMP.

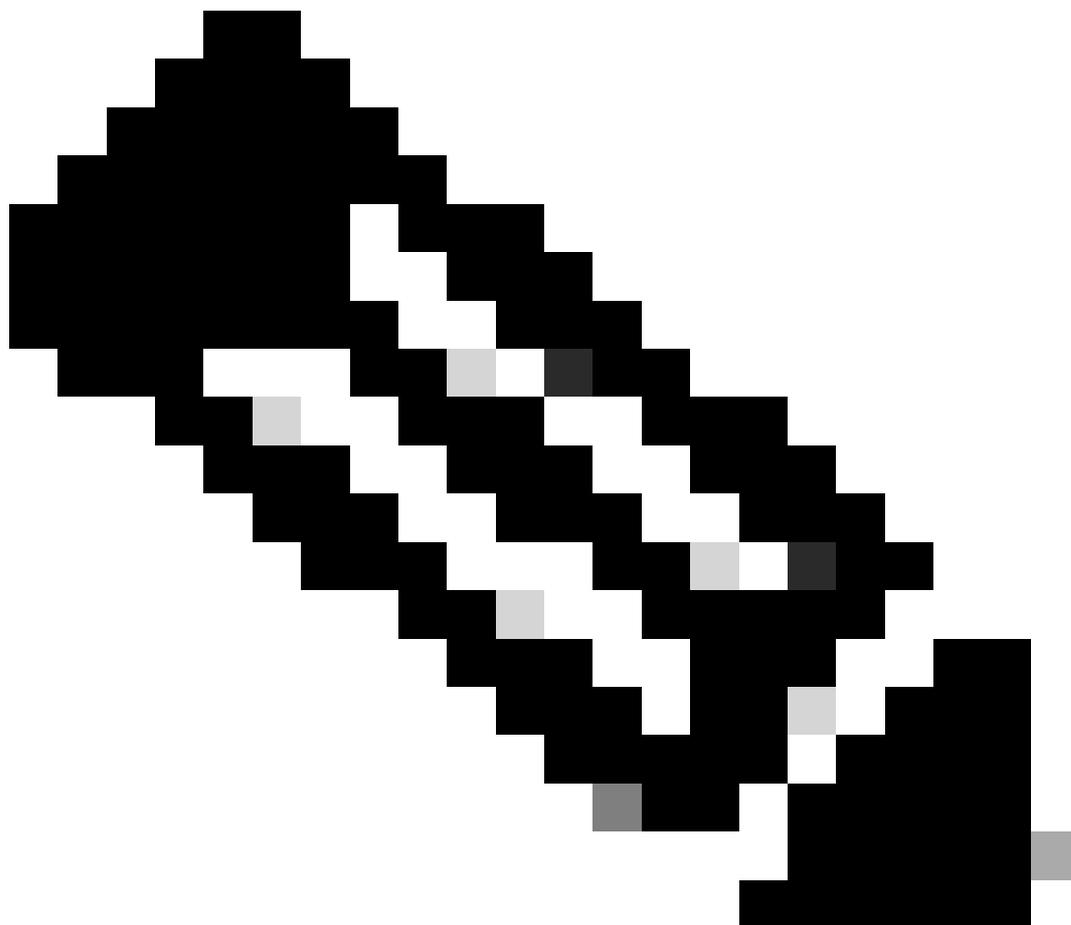
Pour SNMPv2 :

```
#snmp-server community <name_of_community_you_want_to_map> group <name_of_role>
```

Pour SNMPv3 :

```
#snmp-server user <user_to_map_with> <name_of_role> auth {sha/md5} <authentication_password> priv {aes/
```

Configuration



Remarque : cet exemple inclut l'exclusion de l'OID 1.3.6.1.2.1.2.2.1.3 (ifType). Veillez à remplacer l'OID ifType par celui que vous souhaitez exclure.

Définition d'un rôle pour exclure OID ifType :

```
switch#
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# role name deny_oid
switch(config-role)# rule 1 permit read feature snmp
switch(config-role)# rule 2 deny read oid 1.3.6.1.2.1.2.2.1.3
switch(config-role)# exit
switch(config)# exit
switch# sh role name deny_oid
Role: deny_oid
  Description: new role
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
-----
Rule   Perm   Type   Scope   Entity
-----
  2    deny   read   oid     1.3.6.1.2.1.2.2.1.3
  1    permit read   feature snmp
switch#
```

Création d'une communauté SNMPv2 avec le rôle deny_oid suivant :

```
switch(config)# snmp-server community snmpv2user group deny_oid switch(config)# exit switch# sh snmp co
```

Création d'un utilisateur SNMPv3 avec le rôle deny_oid :

```
switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)# snmp-serv
```

Vérification



Remarque : un « trial » d'utilisateur test a été utilisé afin de vérifier l'interrogation de ifType OID. Les autres utilisateurs ont été mappés avec le rôle **deny_oid** et il n'a montré aucune donnée pour ifType OID comme illustré.

SNMPwalk sans exclusion :



Remarque : a.b.c.d est utilisé à la place de l'adresse IP du périphérique dans l'article entier.

```
[root@user ~]# snmpwalk -v2c -c trial a.b.c.d 1.3.6.1.2.1.2.2.1.3 IF-MIB::ifType.83886080 = INTEGER: et
```

SNMPwalk pour SNMPv2 avec OID exclu :

```
[root@user ~]# snmpwalk -v2c -c snmpv2user a.b.c.d 1.3.6.1.2.1.2.2.1.3 IF-MIB::ifType = No Such Object
```



Remarque : un nouvel utilisateur « trialv3 » a été créé afin d'illustrer l'interrogation sans l'exclusion de l'OID.

SNMPwalk sans exclure l'OID :

```
[root@user ~]# snmpwalk -v3 -u trialv3 -l authPriv -a sha -A 'password!123' -x aes -X 'password!123' a.
```

SNMPwalk pour l'utilisateur SNMPv3 avec l'OID exclu :

```
[root@user ~]# snmpwalk -v3 -u snmpv3user -l authPriv -a sha -A 'password!123' -x aes -X 'password!123'
```

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.