OID uitsluiten in Nexus 5k,7k en 9K in SNMP v2 en v3 configuratie

Inhoud

Inleiding

Dit document beschrijft hoe u OID kunt uitsluiten in Nexus 5k, 7k en 9K in SNMP v2- en v3-configuratie.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen voordat u OID-uitsluitingen (Object Identifier) implementeert:

- Bekendheid met Simple Network Management Protocol (SNMP)
- Toegang tot de modus voor de apparaatconfiguratie
- Inzicht in uit te sluiten OID's
- Inzicht in SNMP-community- en gebruikersconfiguraties

Gebruikte componenten

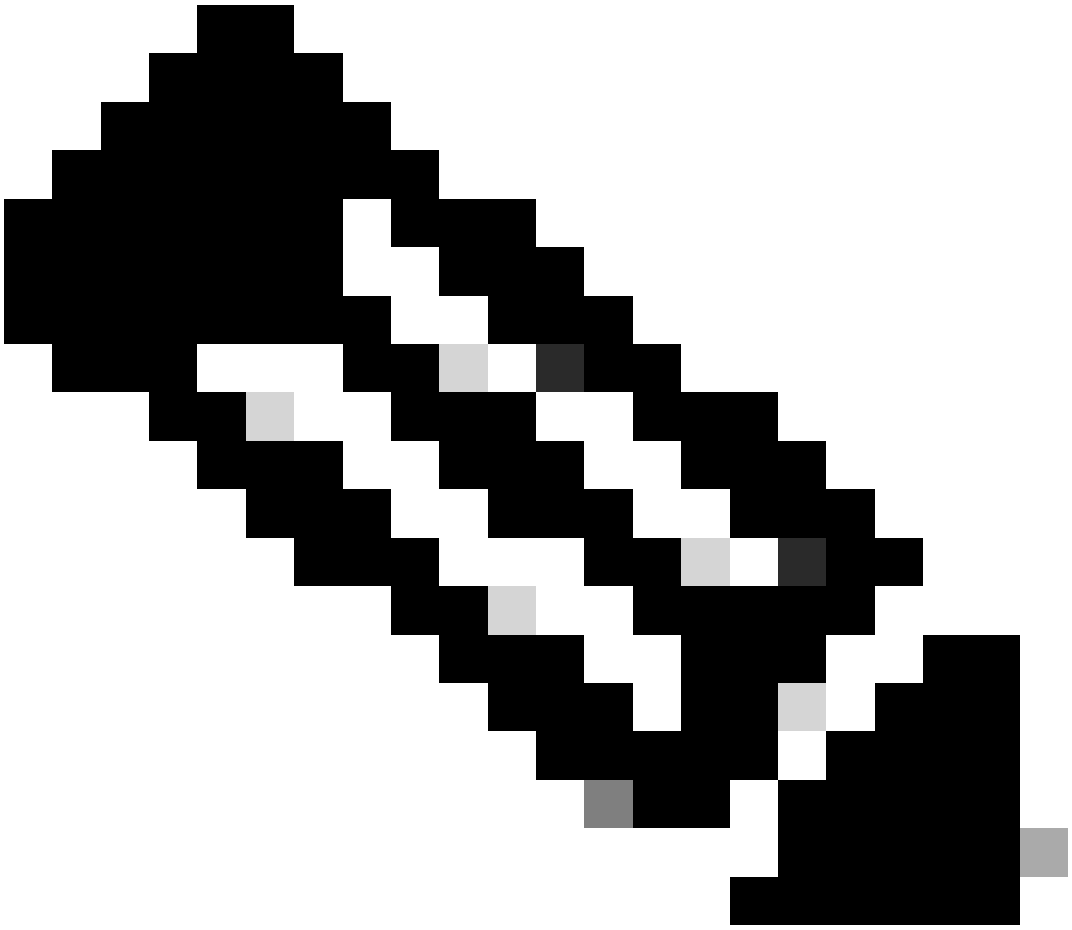
De informatie in dit document is gebaseerd op de Lab-test met deze Nexus-modellen:

- Nexus 5k
- Nexus 7k
- Nexus 9k

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.

Achtergrondinformatie

In de wereld van SNMP, ontmoet u vaak situaties waar het ontleden van de Management Information Base (MIB) boom hindernissen, het bereiken van een stilstand bij specifieke OIDs soms leidend tot venster timeouts of gelijkaardige kwesties. Een andere veel voorkomende uitdaging ontstaat wanneer continue polling voor een lastige OID waarschuwingen veroorzaakt die noch noodzakelijk noch beïnvloedbaar zijn. Een mogelijke manier om van dit soort scenario's af te komen is dat je uitsluitingen maakt, het apparaat instrueert om dat specifieke OID over te slaan en verder te gaan met de rest van de MIB structuur. Door het apparaat te leiden om de lastige OID te omzeilen en met de rest van de MIB structuur verder te gaan, kunt u een vlotte stroom van de MIB boom bevorderen.



Opmerking: het is belangrijk om op te merken dat deze uitsluiting kan beïnvloeden hoe we gegevens van de MIB-boom lezen. Voorzichtigheid betrachten en de noodzaak van de OID waarborgen alvorens deze uitsluitingen uit te voeren.

Terwijl de uitsluiting van OID's doorgaans een eenvoudig proces nastreeft in apparaten zoals Aggregation Services Router (ASR)/Catalyst switches (CAT)/Integrated Service Router (ISR), blijkt het navigeren op deze uitdaging in Nexus-apparaten ingewikkelder te zijn vanwege de afwezigheid van weergaven. Dit artikel duikt in een innovatieve benadering door rollen te introduceren en hen in kaart te brengen aan de gemeenschap/gebruiker, die een oplossing voor het uitsluiten van OIDs in SNMP v2 en v3 configuraties op Nexus 5k, 7k, en 9K apparaten presenteert.

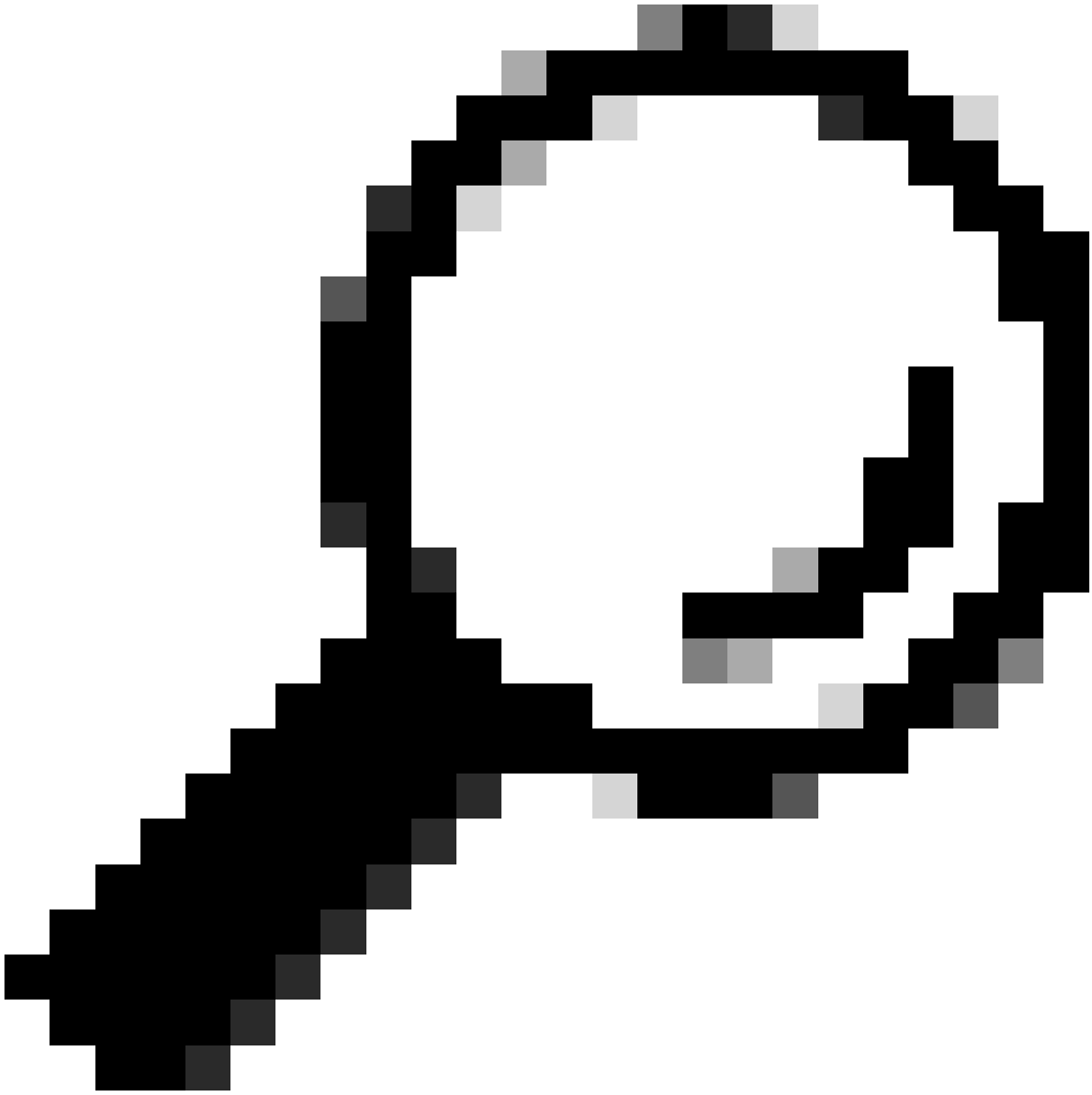
Basisstappen

Access Configuration Mode:

```
#conf t
```

Definieer de rol van OID-uitsluiting:

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



Tip: {read/read-write} kunt u kiezen tussen 'read' en 'read-write' SNMP-bewerkingen. Bij 'Lezen'-bewerkingen gaat het meestal om het ophalen van informatie, terwijl 'lezen-schrijven'-bewerkingen zowel het ophalen als het wijzigen van informatie omvatten. U kunt lezen/lezen-schrijven kiezen volgens uw voorkeur.

Verlaat de configuratiemodus:

```
#exit
```

Configuratie op SNMP-community/gebruiker toepassen.

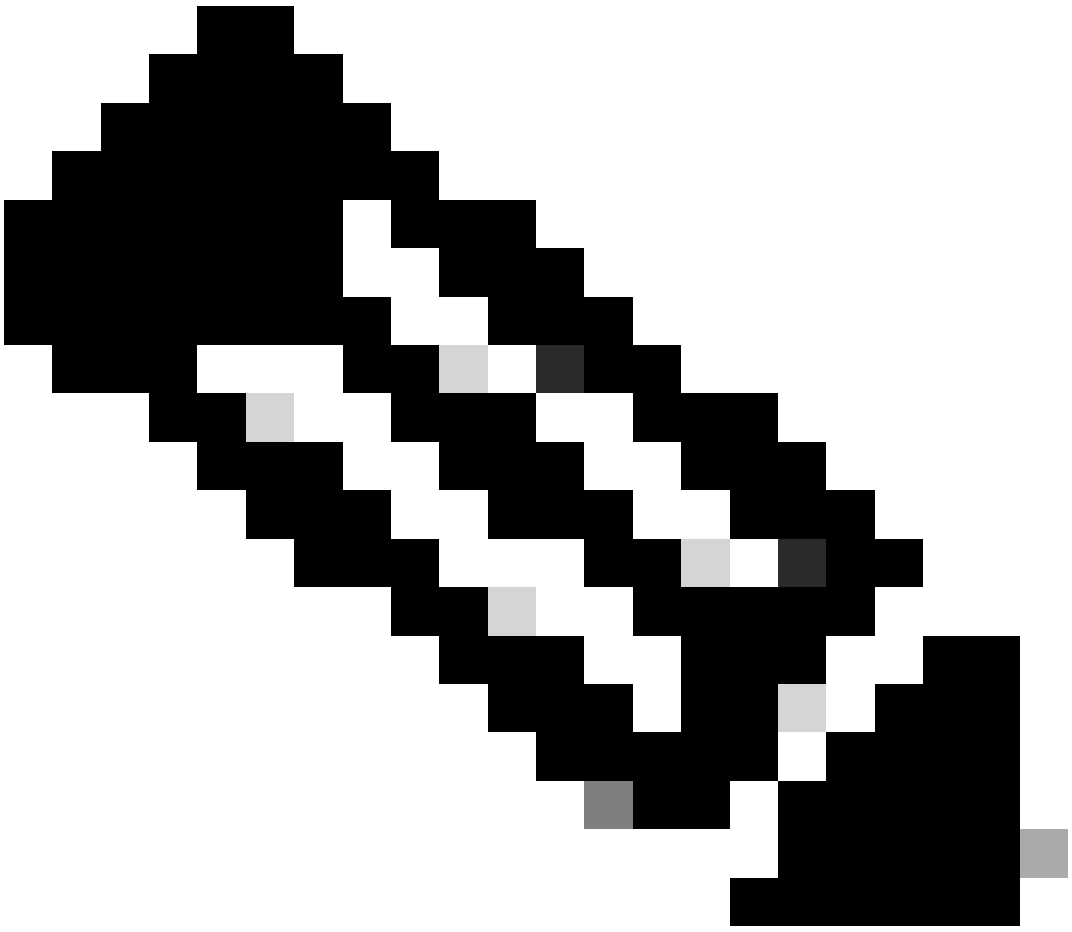
Voor SNMPv2:

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

Voor SNMPv3:

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

Configuratie



Opmerking: dit voorbeeld omvat de uitsluiting van OID 1.3.6.1.2.1.2.2.1.3 (ifType). Verzeker u ervan om de ifType OID te vervangen door de naam die u wilt uitsluiten.

Een rol definiëren om OID ifType uit te sluiten:

```
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#
```

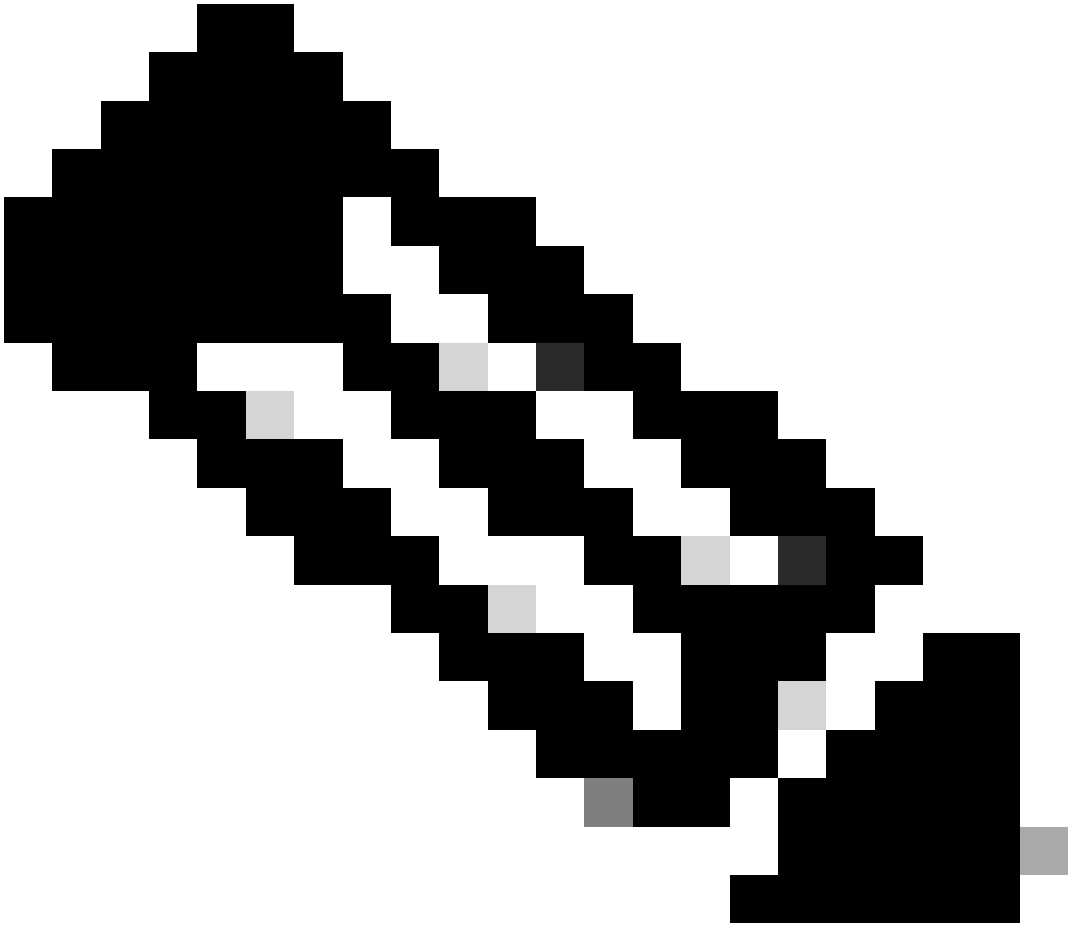
Een SNMPv2-community maken met een deny_oid rol:

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

SNMPv3-gebruiker maken met **deny_oid** rol:

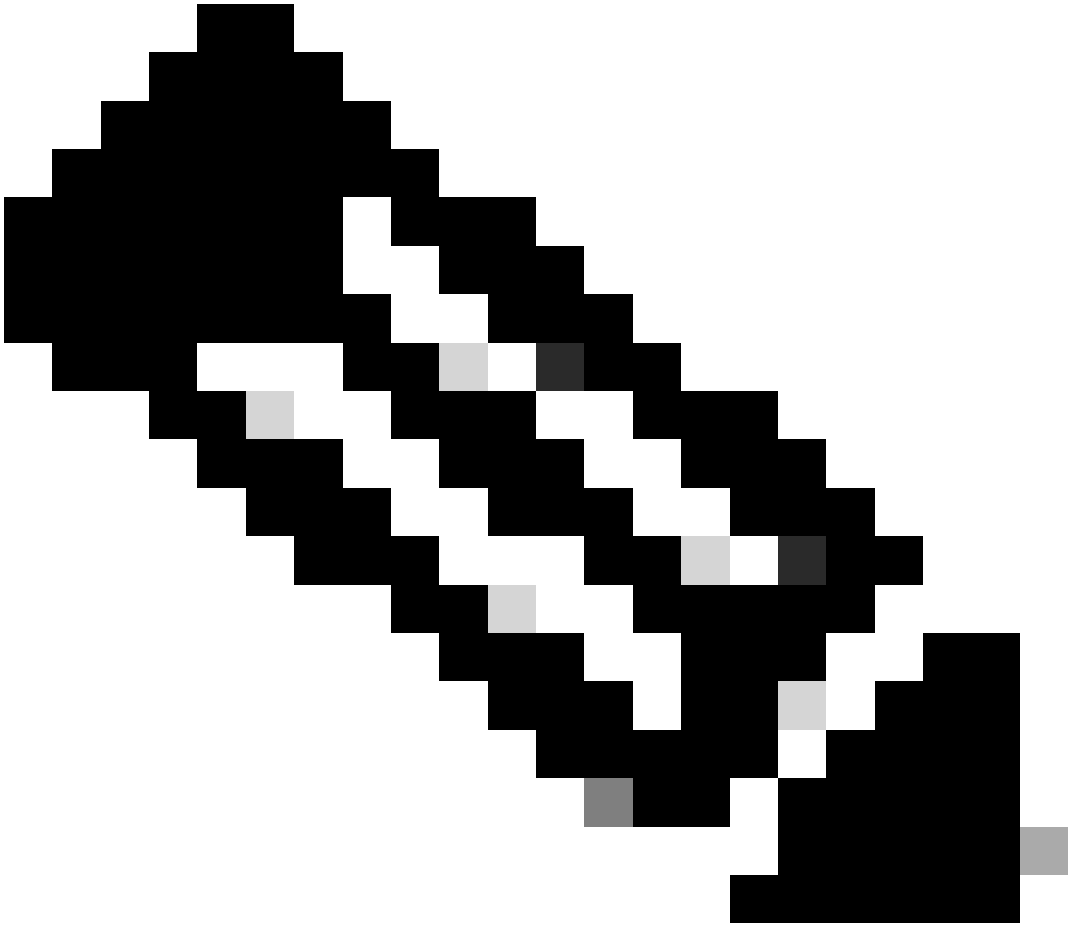
```
switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)# snmp-serv
```

Verificatie



Opmerking: er is een proefgebruiker 'trial' gebruikt om de polling van ifType OID te controleren. De rest van de gebruikers werd in kaart gebracht met de **deny_oid** rol en het toonde geen gegevens voor ifType OID zoals geïllustreerd.

SNMPwalk zonder uitsluiting:

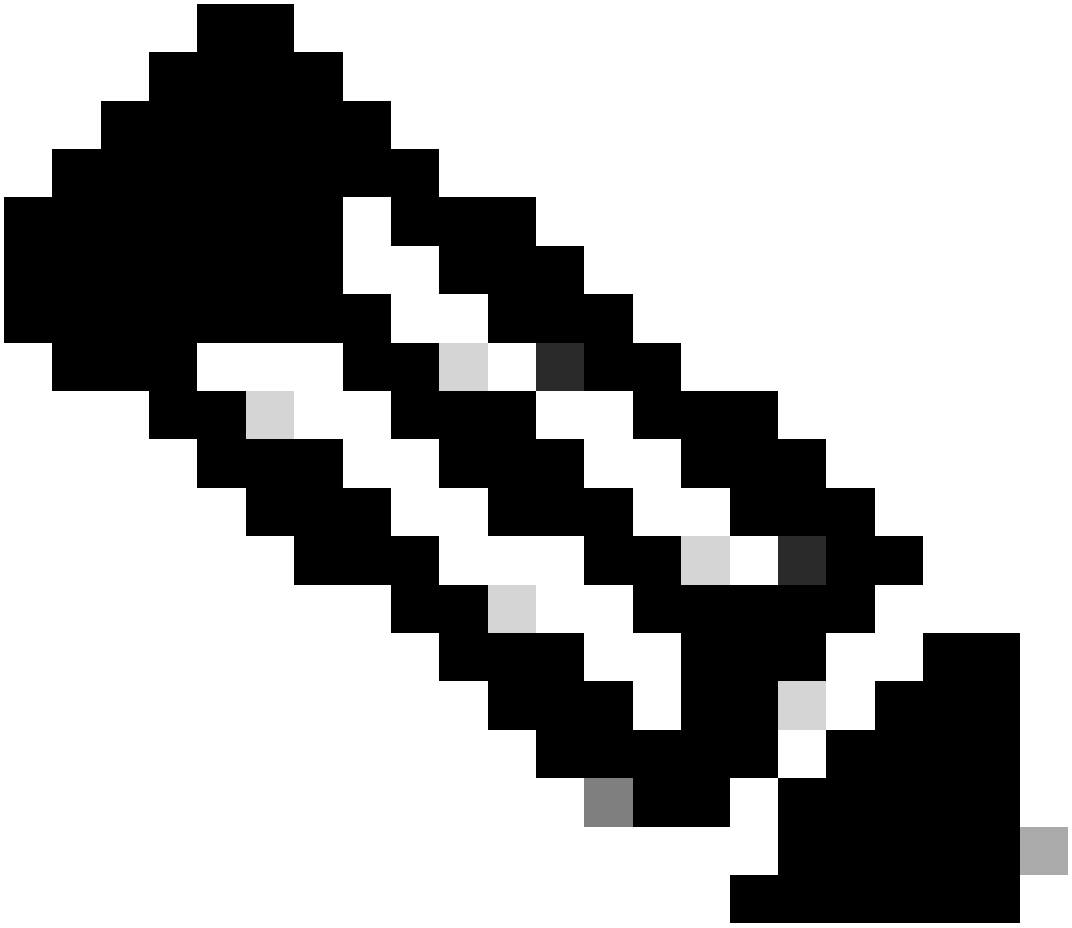


Opmerking: a.b.c.d wordt gebruikt in plaats van het IP-adres van het apparaat in het hele artikel.

```
[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 voor SNMPv2 met uitgesloten OID:

```
[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
```



Opmerking: Er is een nieuwe gebruiker 'trialv3' gemaakt om de opiniepeiling zonder uitsluiting van de OID te illustreren.

SNMPwalk zonder OID uit te sluiten:

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

SNMPwalk voor SNMPv3 gebruiker met uitgesloten OID:

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

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.