# Excluir OID en Nexus 5000, 7000 y 9000 en configuración SNMP v2 y v3

## Contenido



## Introducción

Este documento describe cómo excluir OID en Nexus 5k, 7k y 9K en la configuración SNMP v2 y v3.

## Prerequisites

### Requirements

Cisco recomienda conocer estos temas antes de implementar las exclusiones del identificador de objeto (OID):

- Familiaridad con el protocolo simple de administración de red (SNMP)
- Acceso al modo de configuración del dispositivo
- Comprensión de los OID que deben excluirse
- Comprensión de la comunidad SNMP y configuraciones de usuario

### Componentes Utilizados

La información de este documento se basa en la prueba de laboratorio con estos modelos de Nexus:

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

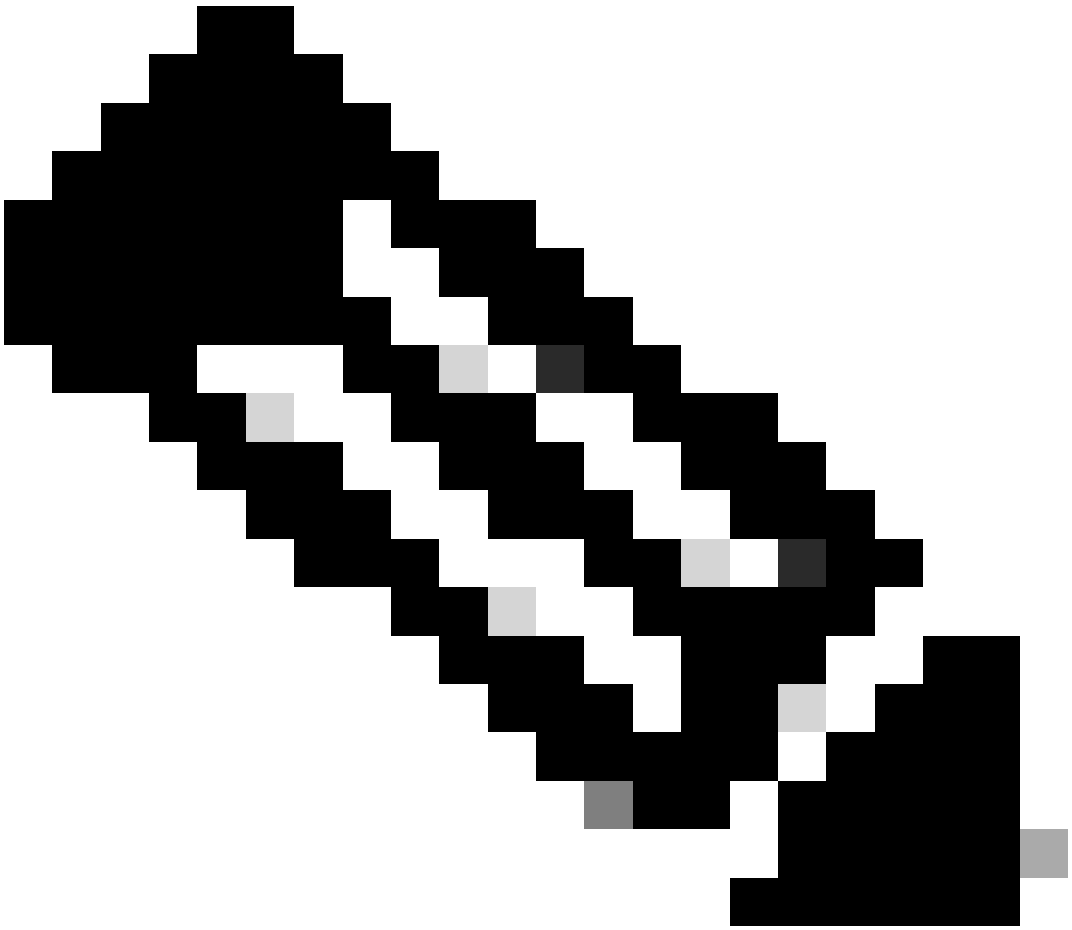
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

En el mundo de SNMP, a menudo se dan situaciones en las que el análisis del árbol de la Base de información de administración (MIB) se enfrenta a obstáculos, que llegan a un punto muerto en OID específicos, lo que a veces conduce a tiempos de espera de ventana o problemas similares. Otro desafío común surge cuando el sondeo continuo de un OID problemático genera alertas que no son necesarias ni tienen impacto. Una manera posible de deshacerse de este tipo de escenarios es crear exclusiones, indicando al dispositivo que omita ese OID específico y continúe con el resto de la estructura MIB. Al indicar al dispositivo que omita el problemático OID y continúe con el resto de la estructura MIB, puede fomentar un flujo suave del árbol MIB.

---



> Nota: Es importante tener en cuenta que esta exclusión puede afectar al modo en que leemos los datos del árbol MIB. Proceda con cautela y garantice la necesidad del OID antes de proceder con estas exclusiones.

---

Aunque la exclusión de OID suele seguir un proceso sencillo en dispositivos como Aggregation Services Router (ASR)/Catalyst switches (CAT)/Integrated Service Router (ISR), la navegación por este reto en los dispositivos Nexus resulta más complicada debido a la ausencia de vistas. En este artículo se profundiza en un enfoque innovador mediante la introducción de roles y su asignación a la comunidad/usuario, y se presenta una solución para excluir OID en configuraciones SNMP v2 y v3 en dispositivos Nexus 5k, 7k y 9K.

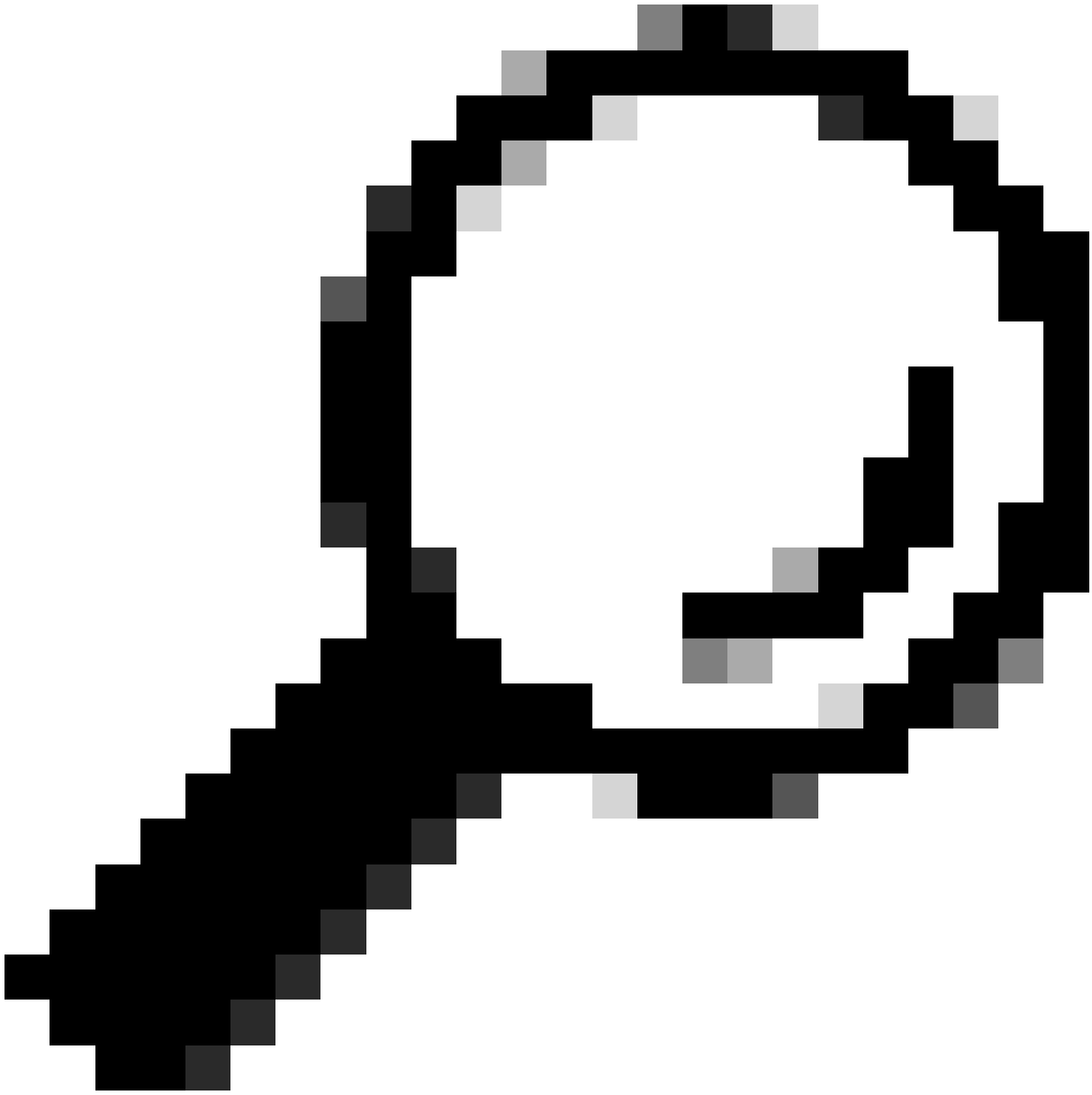
# Pasos básicos

Acceso al modo de configuración:

```
#conf t
```

Defina la función de la exclusión de OID:

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



Sugerencia: {read/ read-write} le permite elegir entre operaciones SNMP 'read' y 'read-write'. Las operaciones de 'lectura' normalmente implican la recuperación de información, mientras que las operaciones de 'lectura y escritura' implican la recuperación y modificación de información. Puede elegir lectura/lectura-escritura según sus preferencias.

---

Salga del modo de configuración:

```
#exit
```

Aplicar configuración a comunidad/usuario SNMP.

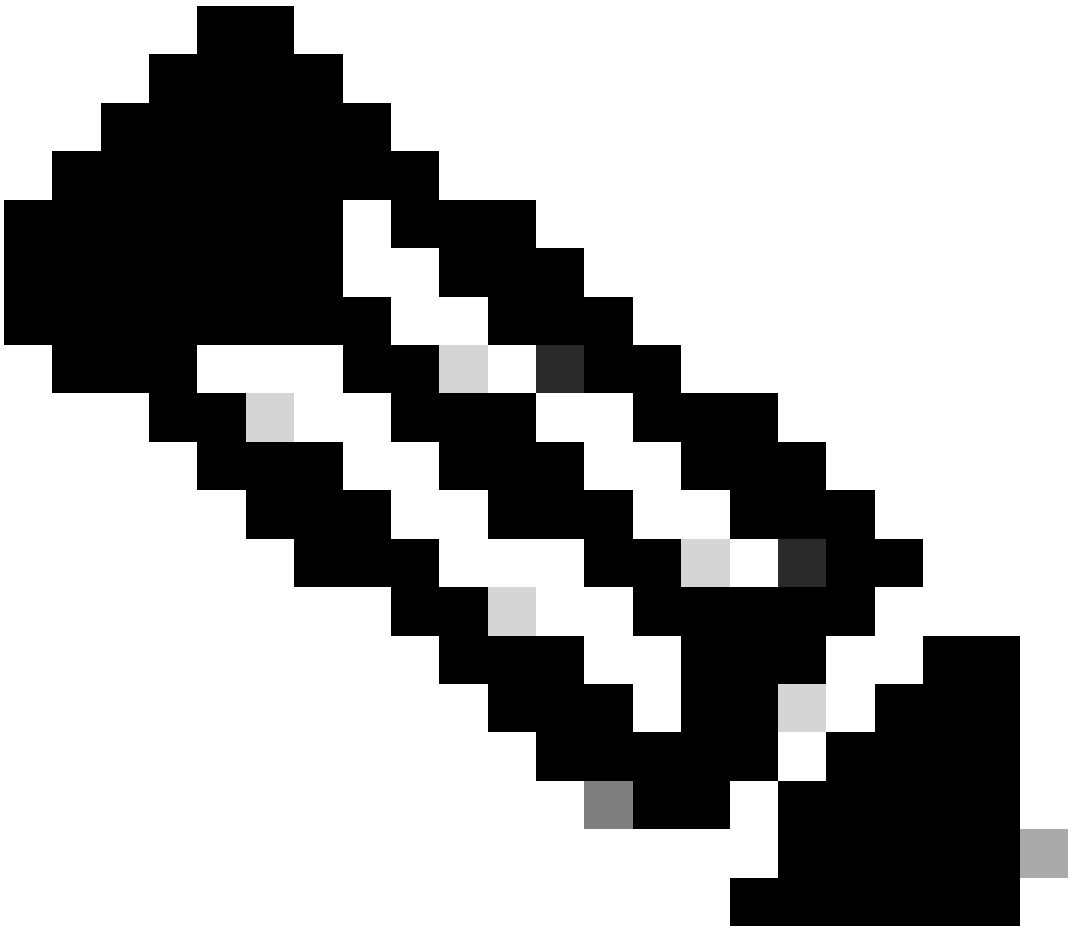
Para SNMPv2:

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

Para SNMPv3:

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

## Configuración



Nota: Este ejemplo incluye la exclusión de OID 1.3.6.1.2.1.2.2.1.3 (ifType). Asegúrese de reemplazar el ifType OID por el que desee excluir.

Definición de un rol para excluir 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#
```

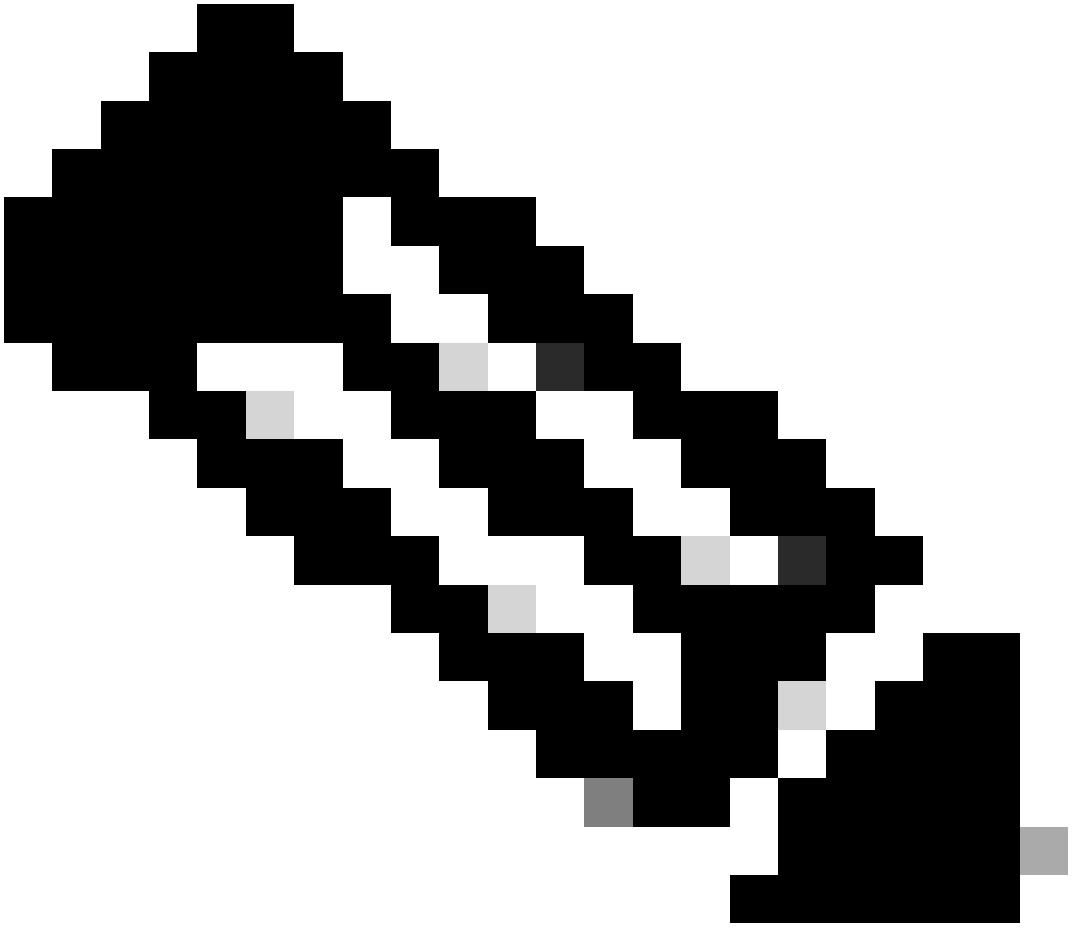
Creación de una comunidad SNMPv2 con deny_oid el rol:

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

Creación de un usuario SNMPv3 con el rol **deny_oid**:

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

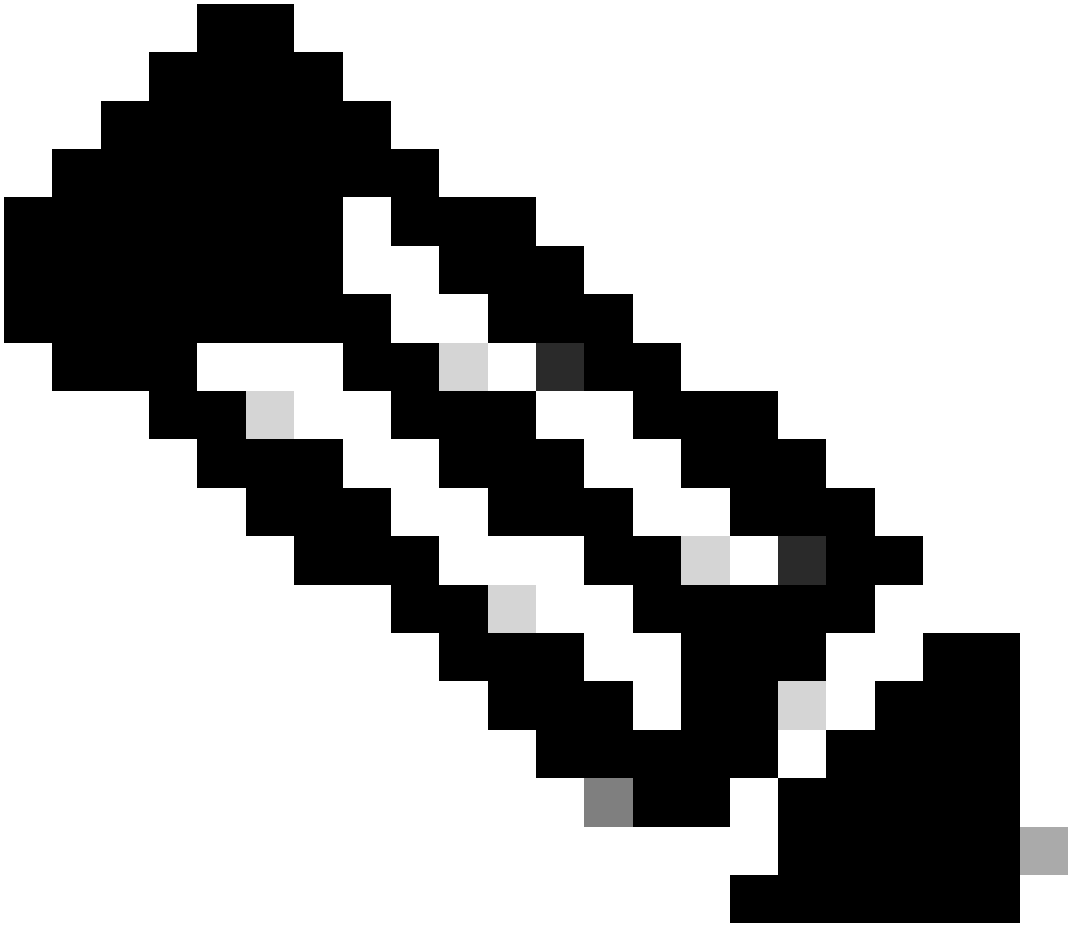
Verificación



**Nota**: Se utilizó un usuario de prueba 'trial' para verificar el sondeo de ifType OID. El resto de los usuarios se asignaron con el rol **deny_oid** y no mostró datos para ifType OID como se muestra en la ilustración.

---

SNMPwalk sin exclusión:

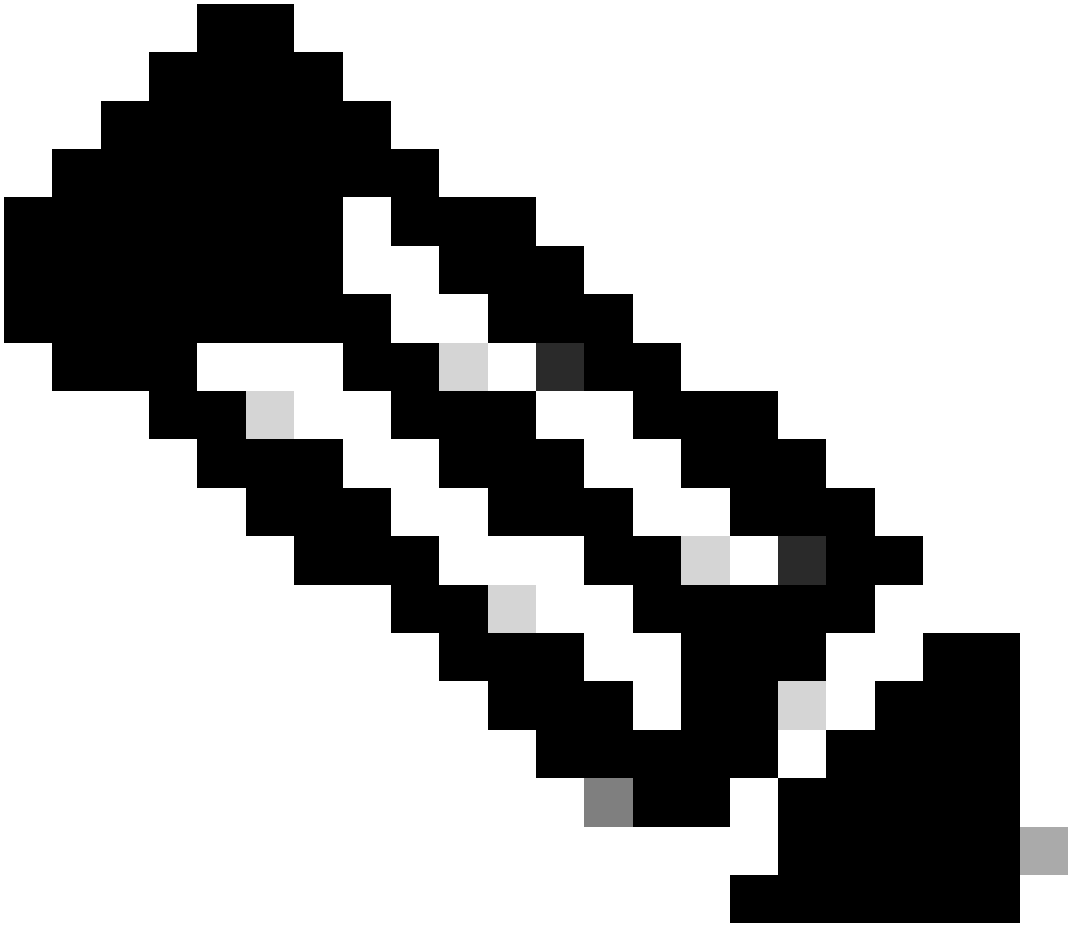


**Nota**: a.b.c.d se utiliza en lugar de la dirección IP del dispositivo en todo el artículo.

```
[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 para SNMPv2 con OID excluido:

```
[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
```



**Nota**: Se creó un nuevo usuario 'trialv3' para ilustrar el sondeo sin la exclusión del OID.

SNMPwalk sin excluir el OID:

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

SNMPwalk para usuario SNMPv3 con OID excluido:

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).