

# 在SNMP v2和v3配置中，排除Nexus 5k、7k和9K中的OID

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[基本步骤](#)

[配置](#)

[确认](#)

---

## 简介

本文档介绍如何在SNMP v2和v3配置中排除Nexus 5k、7k和9K中的OID。

## 先决条件

### 要求

思科建议您在实施对象标识符(OID)排除之前了解以下主题：

- 熟悉简单网络管理协议(SNMP)
- 访问设备配置模式
- 了解要排除的OID
- 了解SNMP社区和用户配置

### 使用的组件

本文档中的信息基于对以下Nexus型号的实验室测试：

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

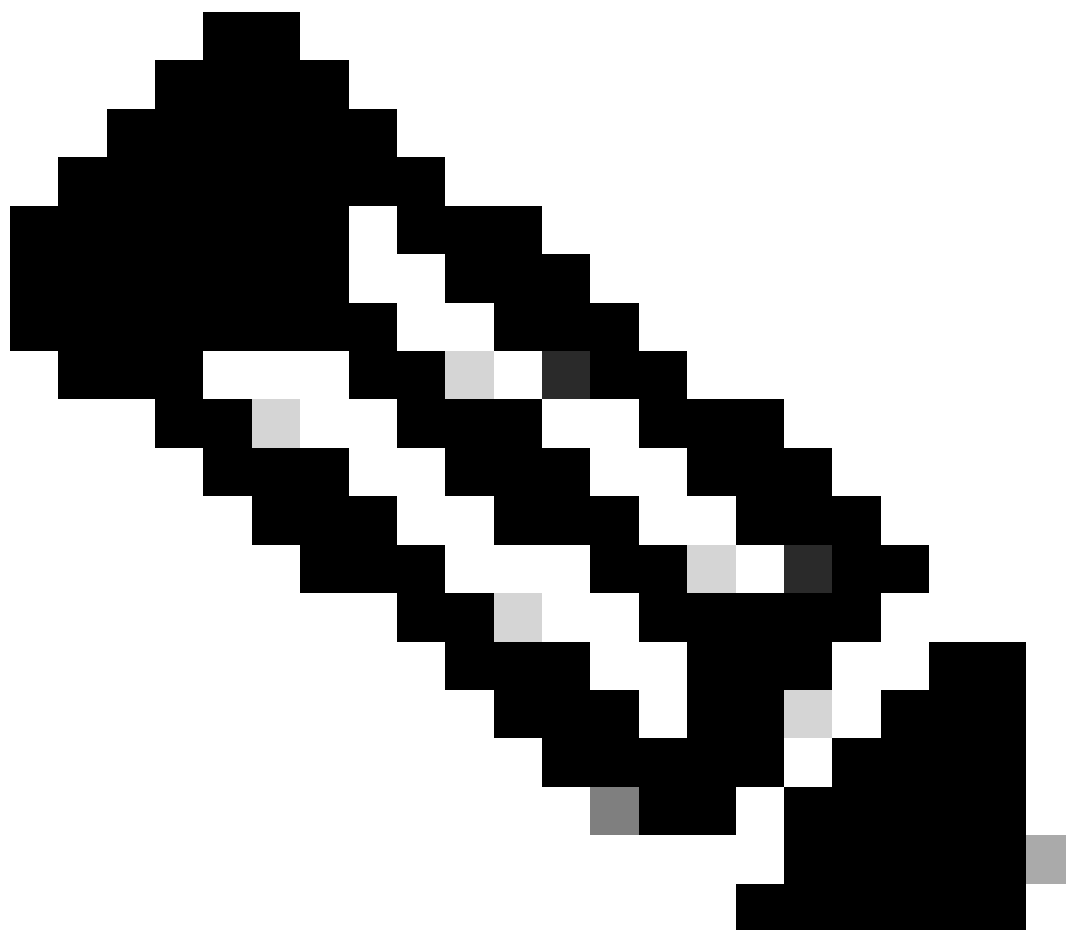
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

在SNMP的世界中，您经常遇到管理信息库(MIB)树解析遇到障碍的情况，在特定OID处停滞有时会

导致窗口超时或类似问题。当持续轮询故障的OID触发既不必要也不具影响的警报时，就会出现另一个常见问题。摆脱这些类型的场景的一种可能方法是创建例外项，指示设备跳过该特定OID并继续执行MIB结构的其余部分。通过引导设备绕过故障的OID并继续执行MIB结构的其余部分，您可以促进MIB树的顺利流动。

---



注意：请务必注意，此排除项会影响我们从MIB树中读取数据的方式。在继续这些排除之前，请谨慎并确保必须使用OID。

---

在聚合服务路由器(ASR)/Catalyst交换机(CAT)/集成服务路由器(ISR)等设备中，排除OID通常遵循简单流程，但是在Nexus设备中克服这一挑战因缺少视图而显得更为复杂。本文引入角色并将其映射到社区/用户，从而深入探讨了一种创新方法，提出了在Nexus 5k、7k和9K设备上的SNMP v2和v3配置中排除OID的解决方案。

## 基本步骤

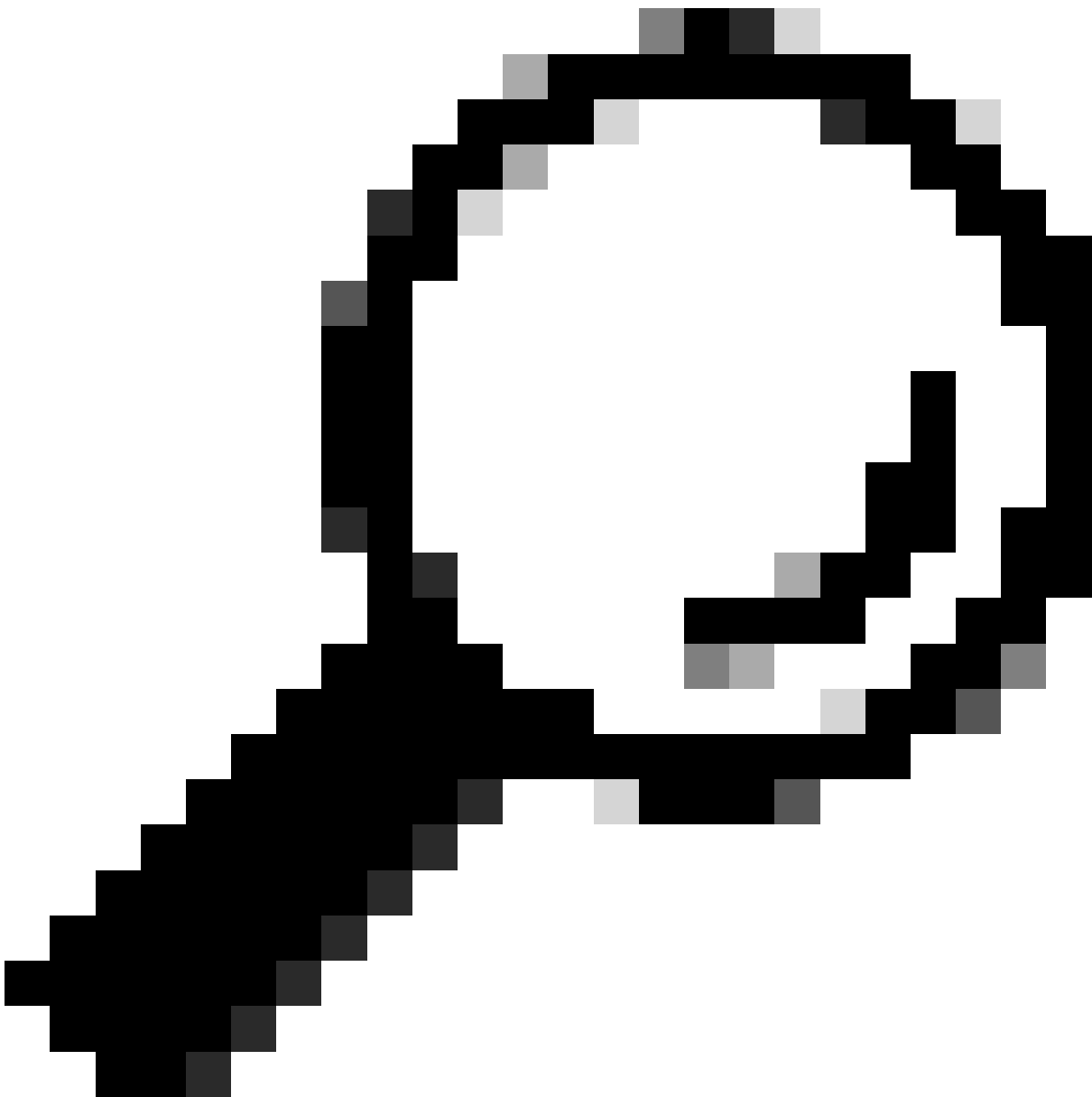
访问配置模式：

```
#conf t
```

定义OID排除的作用：

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

---



提示：{read/ read-write}允许您在“read”和“read-write”SNMP操作之间进行选择。“读取”操作通常涉及检索信息，而“读写”操作涉及检索和修改信息。您可以根据自己的喜好选择读/写

。

---

退出配置模式：

```
#exit
```

将配置应用到SNMP社区/用户。

对于SNMPv2：

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

对于SNMPv3：

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

## 配置

---

注意：本示例包括对OID 1.3.6.1.2.1.2.2.1.3 (ifType)的排除。确保将ifType OID替换为要排除的OID。

---

定义要排除OID ifType的角色：

```
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#

```

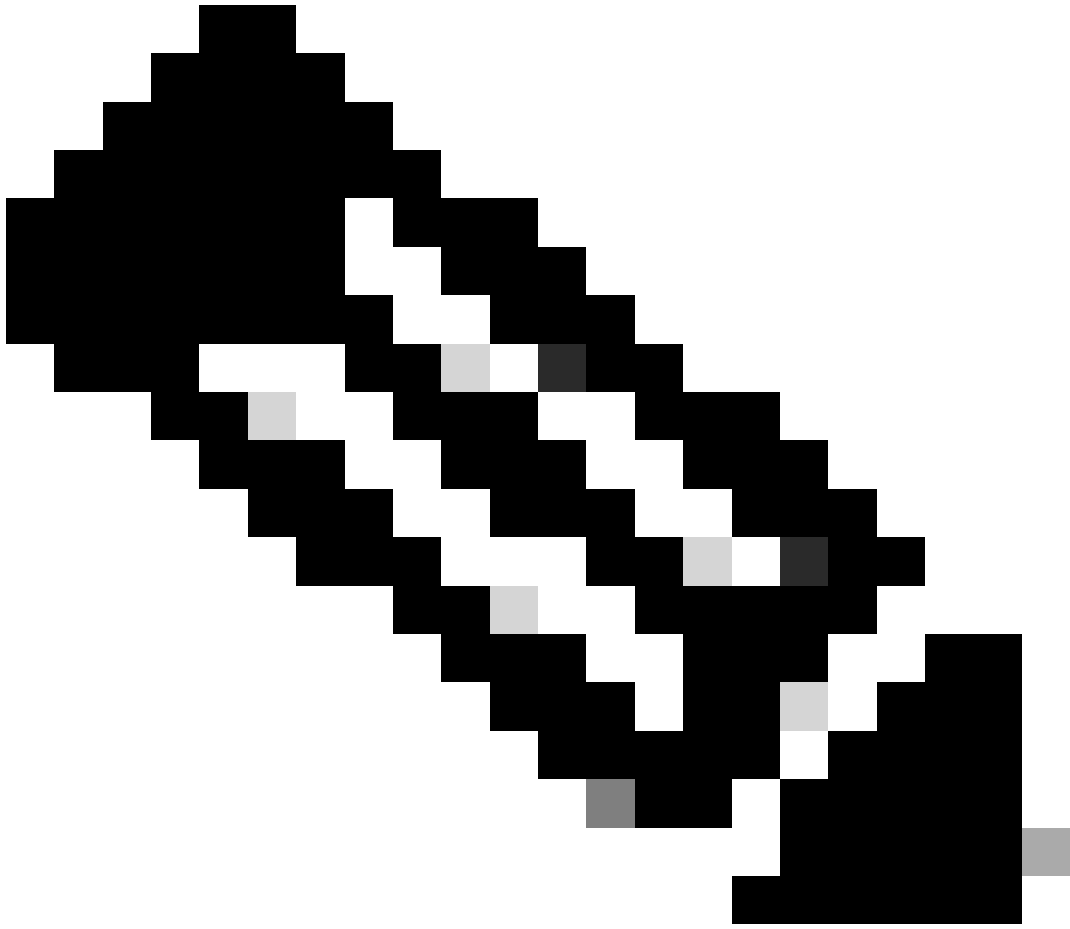
创建具有deny\_oid角色的SNMPv2社区：

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

正在创建具有deny\_oid角色的SNMPv3用户：

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

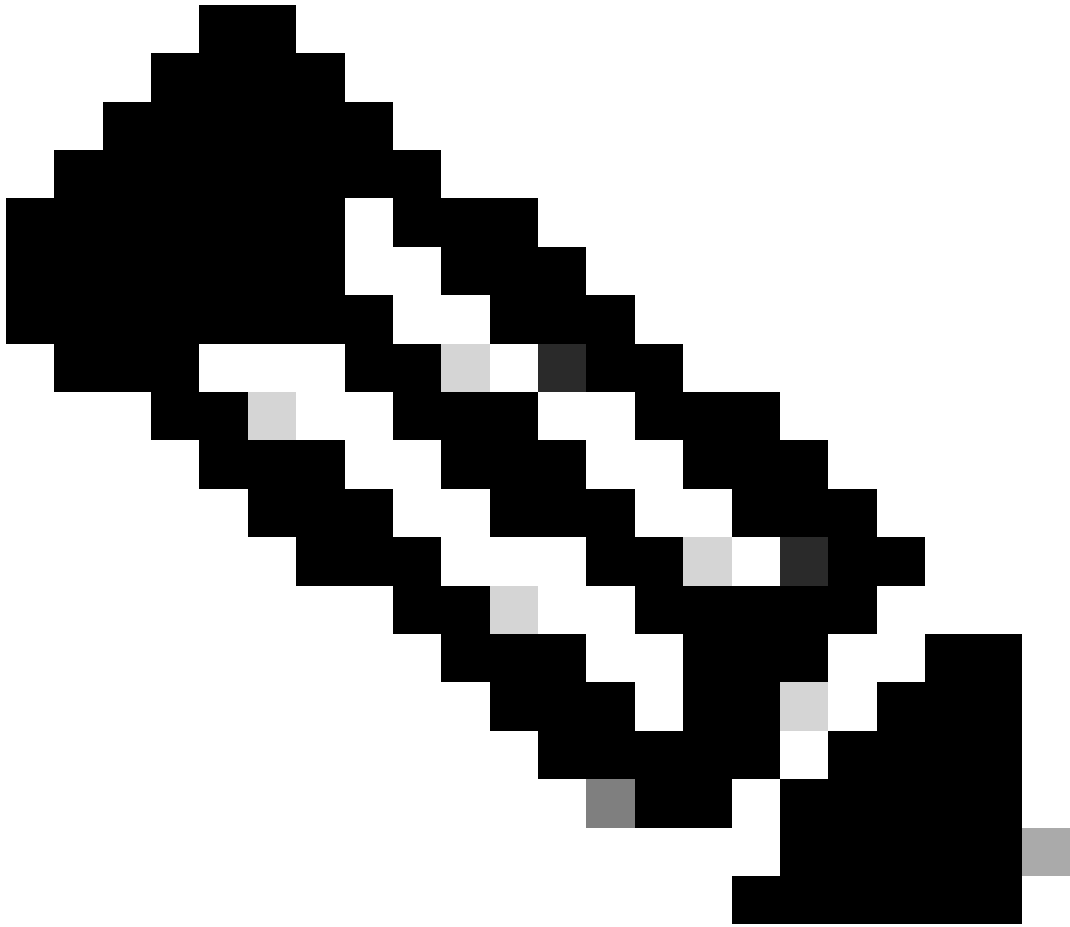
确认



注意：测试用户“trial”用于检查ifType OID的轮询。其余用户已使用deny\_oid角色进行映射，并且未显示ifType OID的任何数据，如下所示。

---

无排除的SNMPwalk：



注意：在整个文章中，a.b.c.d用于代替设备的IP地址。

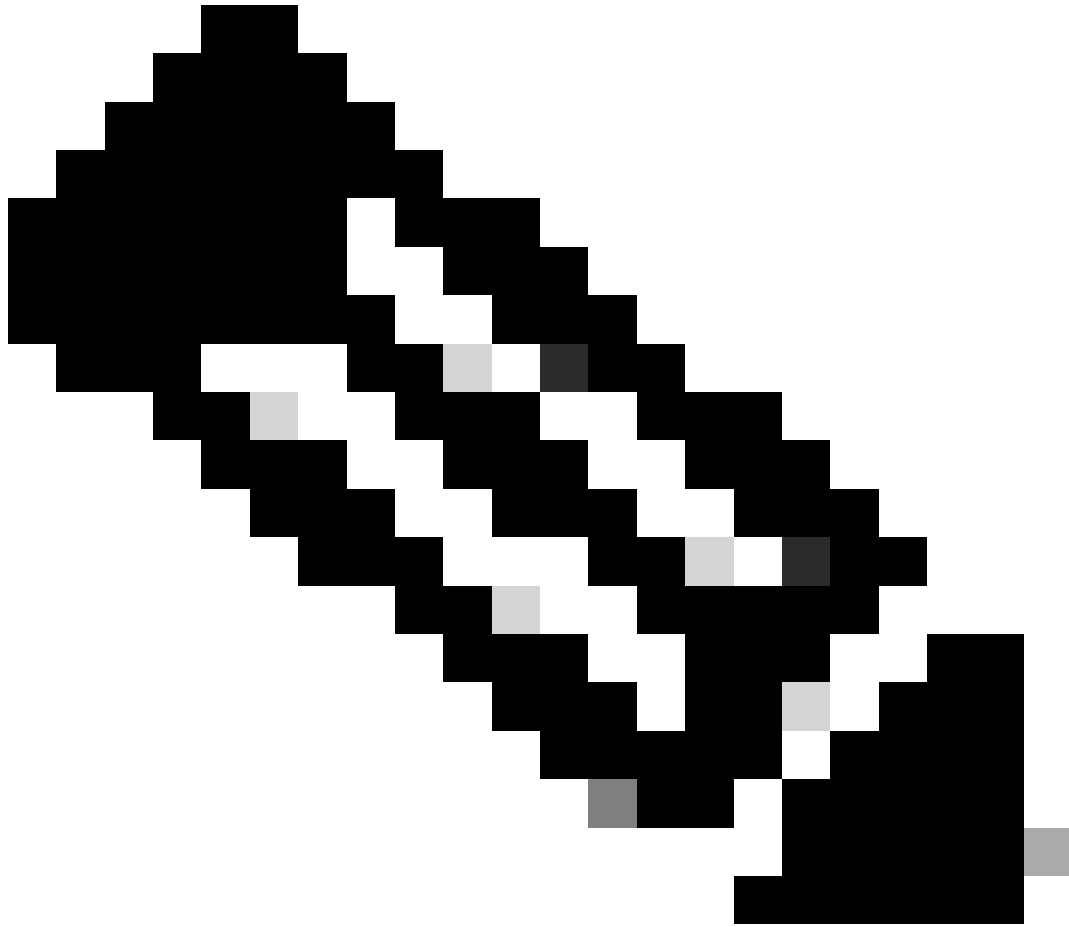
---

```
[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
```

具有已排除OID的SNMPv2的SNMPwalk：

```
[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
```





注意：创建了新用户“trialv3”来演示不排除OID的轮询。

---

不排除OID的SNMPwalk：

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

具有已排除OID的SNMPv3用户的SNMPwalk：

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

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。