

Excluir OID no Nexus 5k,7k e 9K na configuração SNMP v2 e v3

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Etapas básicas](#)

[Configuração](#)

[Verificação](#)

Introdução

Este documento descreve como excluir o OID no Nexus 5k, 7k e 9K na configuração SNMP v2 e v3.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos antes de implementar exclusões do Identificador de objeto (OID):

- Familiaridade com o SNMP (Simple Network Management Protocol)
- Acesso ao modo de configuração do dispositivo
- Compreensão dos OIDs a serem excluídos
- Compreensão da comunidade SNMP e das configurações de usuário

Componentes Utilizados

As informações neste documento são baseadas no teste de laboratório com estes modelos Nexus:

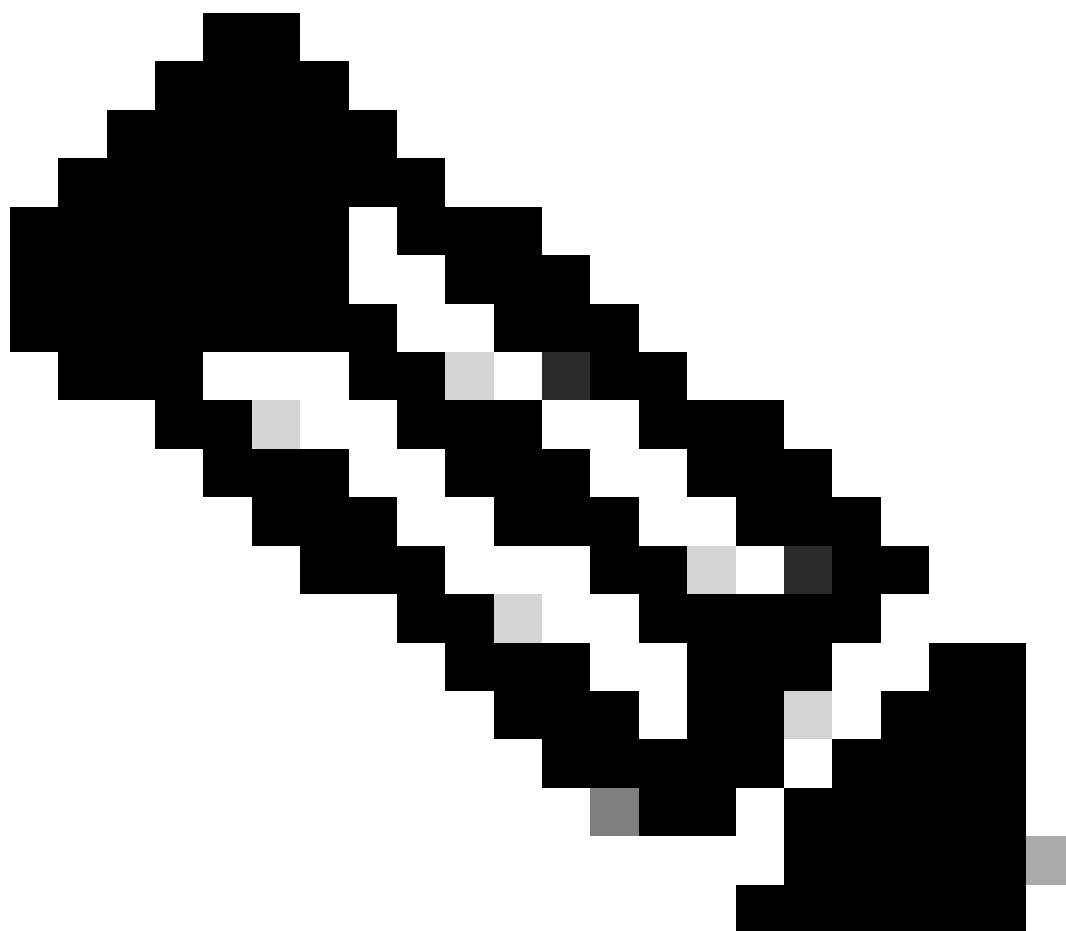
- Nexus 5K
- Nexus 7K
- Nexus 9K

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

No mundo do SNMP, você frequentemente encontra situações em que a análise da árvore da Base de Informações de Gerenciamento (MIB) enfrenta obstáculos, atingindo um impasse em OIDs específicos, às vezes levando a tempos limite de janela ou problemas semelhantes. Outro desafio comum surge quando a pesquisa contínua de um OID problemático aciona alertas que não são necessários nem impactantes. Uma maneira possível de se livrar desses tipos de cenários é criar exclusões, instruindo o dispositivo a ignorar esse OID específico e continuar com o restante da estrutura MIB. Ao direcionar o dispositivo para ignorar o OID problemático e continuar com o restante da estrutura MIB, você pode promover um fluxo suave da árvore MIB.



Observação: é importante observar que essa exclusão pode afetar a forma como lemos os dados da árvore MIB. Tenha cuidado e verifique a necessidade do OID antes de continuar com essas exclusões.

Embora a exclusão de OIDs normalmente siga um processo simples em dispositivos como Roteador de Serviços de Agregação (ASR - Aggregation Services Router)/Switches Catalyst (CAT - Catalyst Switches)/Roteador de Serviços Integrados (ISR - Integrated Service Router), a navegação por esse desafio em dispositivos Nexus se mostra mais complexa devido à ausência de visualizações. Este artigo aborda uma abordagem inovadora ao introduzir funções e mapeá-las para a comunidade/usuário, apresentando uma solução para excluir OIDs em configurações SNMP v2 e v3 em dispositivos Nexus 5k, 7k e 9K.

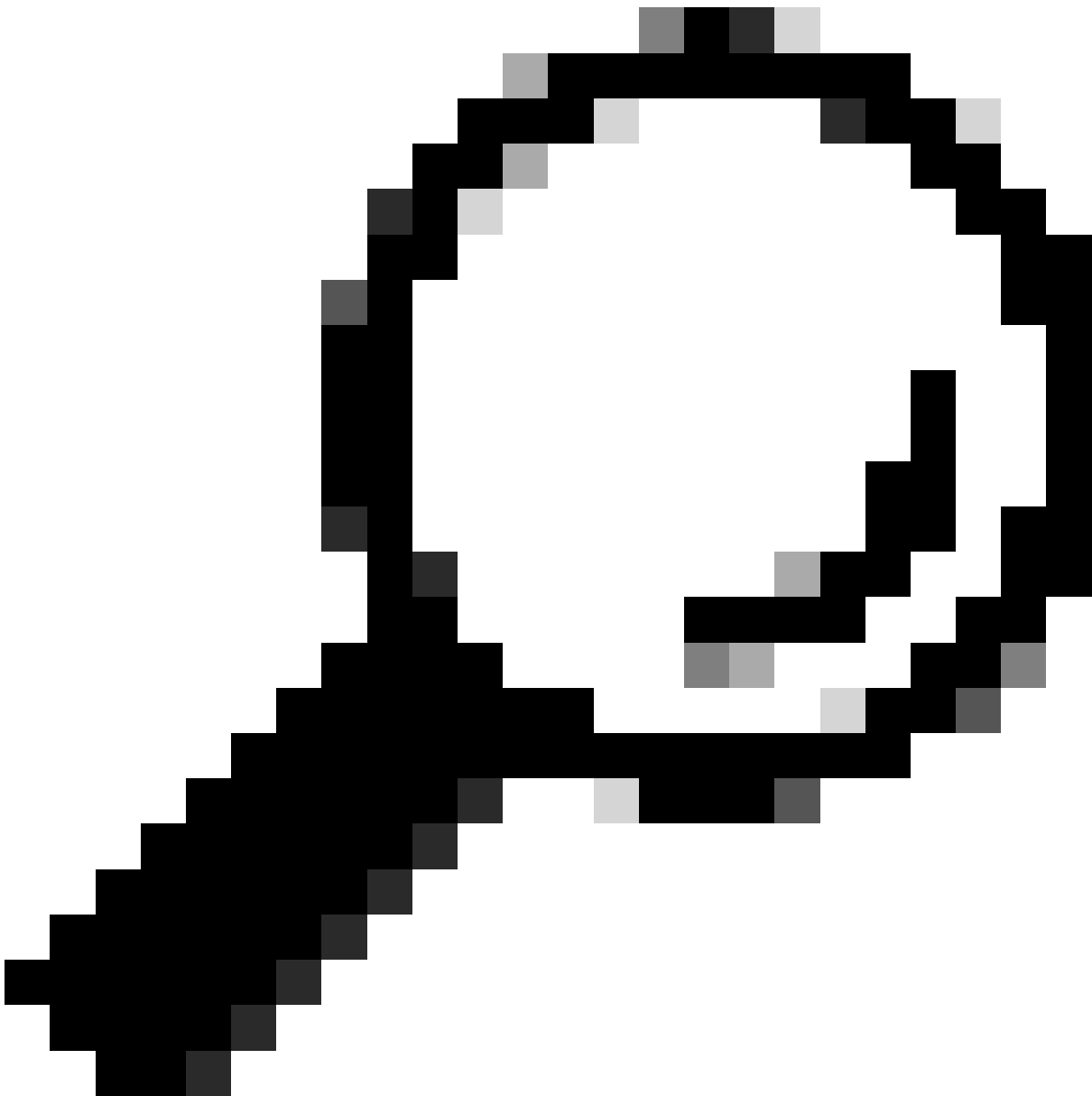
Etapas básicas

Modo de configuração de acesso:

```
#conf t
```

Definir a Função da Exclusão do OID:

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



Dica: o {read/ read- write} permite que você escolha entre as operações SNMP 'read' e 'read- write'. As operações de 'leitura' geralmente envolvem a recuperação de informações, enquanto as operações de 'leitura-gravação' envolvem a recuperação e a modificação de informações. Você pode escolher leitura/leitura/gravação conforme sua preferência.

Saia do modo de configuração:

```
#exit
```

Aplice a configuração à comunidade/usuário SNMP.

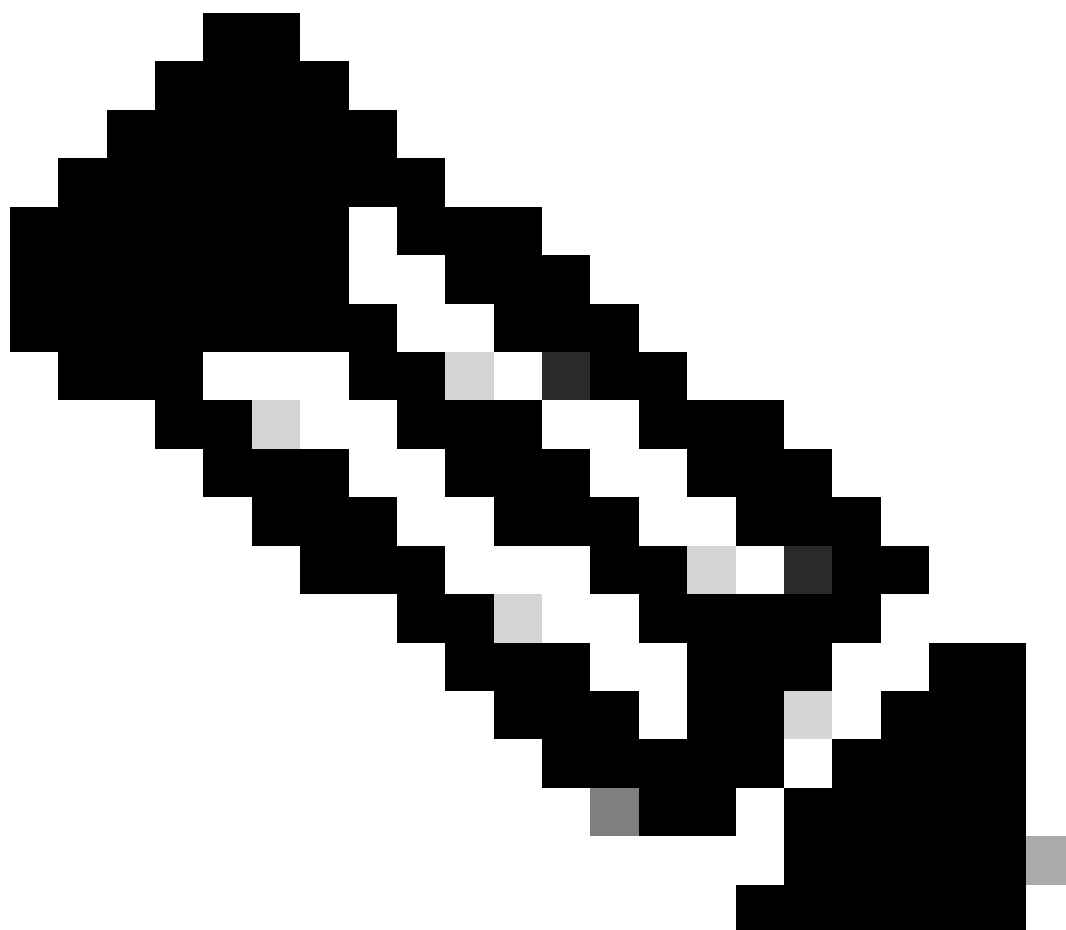
Para SNMPv2:

```
#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/
```

Configuração



Observação: este exemplo inclui a exclusão de OID 1.3.6.1.2.1.2.2.1.3 (ifType).
Certifique-se de substituir o OID ifType pelo que deseja excluir.

Definindo uma função 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#
```

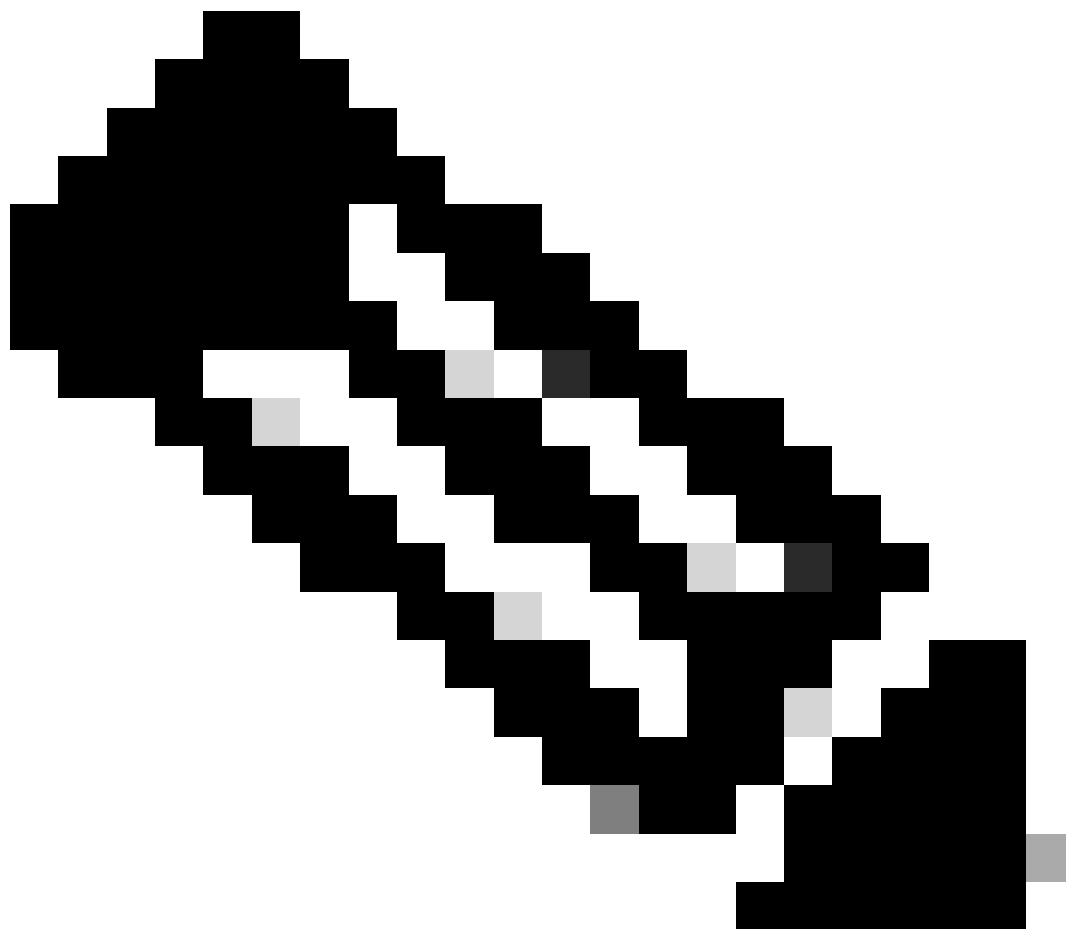
Criando uma comunidade SNMPv2 com deny_oid função:

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

Criando usuário SNMPv3 com a função deny_oid:

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

Verificação



Observação: um usuário de teste 'trial' foi usado para verificar a sondagem de ifType OID. O restante dos usuários foi mapeado com a função **deny_oid** e não mostrou nenhum dado para ifType OID como ilustrado.

SNMPwalk sem exclusão:



Nota: a.b.c.d é usado no lugar do endereço IP do dispositivo em todo o artigo.

```
[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 com OID excluído:

```
[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
```




Observação: um novo usuário 'trialv3' foi criado para ilustrar a pesquisa sem a exclusão do OID.

SNMPwalk sem excluir o OID:

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

SNMPwalk para usuário de SNMPv3 com OID excluído:

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.