Escludere OID in Nexus 5k, 7k e 9K nella configurazione SNMP v2 e v3

Sommario

Introduzione

In questo documento viene descritto come escludere OID in Nexus 5k, 7k e 9K nella configurazione SNMP v2 e v3.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti prima di implementare le esclusioni OID (Object Identifier):

- Familiarità con il protocollo SNMP (Simple Network Management Protocol)
- Accesso alla modalità di configurazione del dispositivo
- Informazioni sugli OID da escludere
- Informazioni sulla community SNMP e sulle configurazioni degli utenti

Componenti usati

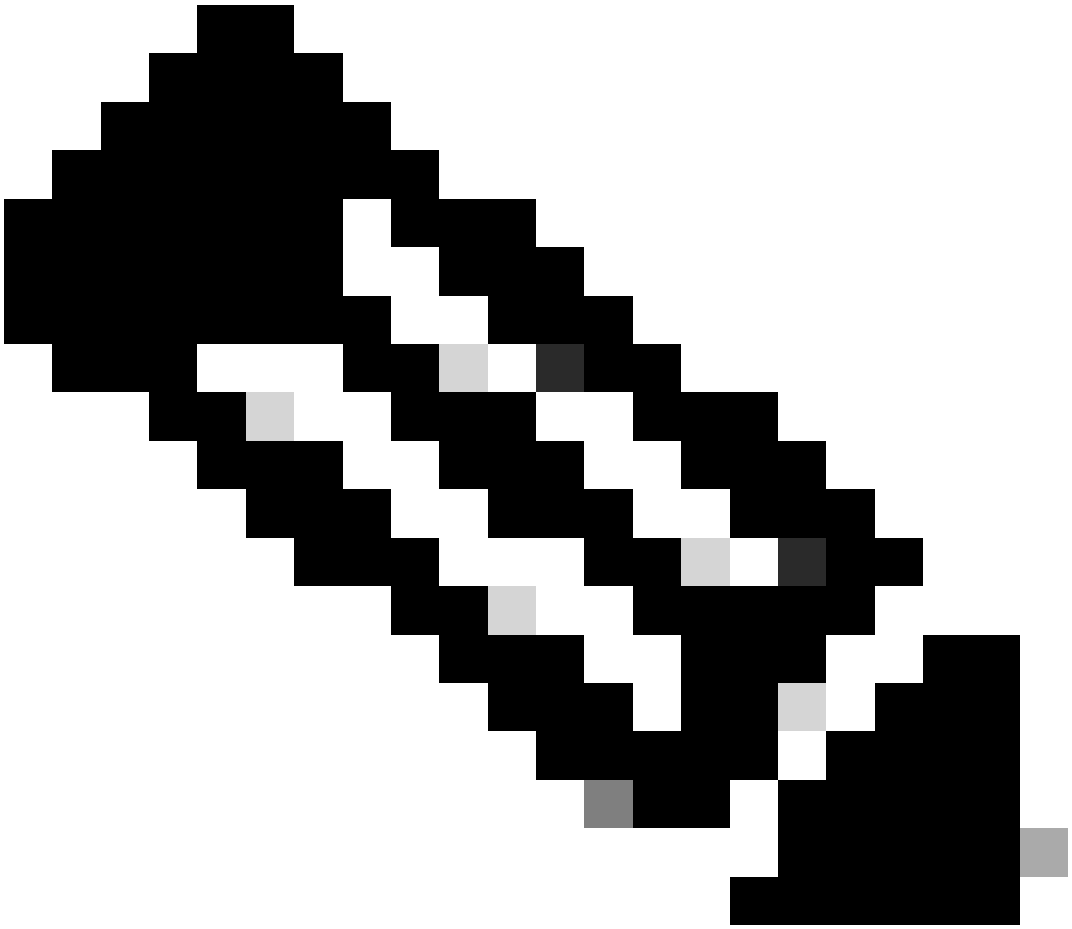
Le informazioni fornite in questo documento si basano sul test Lab con i seguenti modelli Nexus:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Nel mondo del protocollo SNMP, spesso si verificano situazioni in cui l'analisi della struttura MIB (Management Information Base) incontra difficoltà, raggiungendo un punto morto in corrispondenza di OID specifici e causando talvolta timeout di finestre o problemi simili. Un'altra sfida comune si presenta quando il polling continuo per un OID problematico attiva avvisi che non sono né necessari né impattanti. Un possibile modo per eliminare questo tipo di scenari consiste nel creare esclusioni, indicando al dispositivo di ignorare l'OID specifico e procedere con il resto della struttura MIB. Indicando al dispositivo di ignorare l'OID problematico e procedere con il resto della struttura MIB, è possibile favorire un flusso uniforme della struttura MIB.



> Nota: è importante notare che questa esclusione può influire sulla modalità di lettura dei dati dalla struttura MIB. Prima di procedere con queste esclusioni, prestare attenzione e verificare la necessità dell'OID.

Mentre l'esclusione degli OID in genere ha un processo semplice in dispositivi come Aggregation

Services Router (ASR)/ Switch Catalyst (CAT)/Integrated Service Router (ISR), affrontare questa sfida nei dispositivi Nexus si dimostra più complesso a causa dell'assenza di visualizzazioni. In questo articolo viene descritto un approccio innovativo introducendo i ruoli e mappandoli alla community/utente, presentando una soluzione per l'esclusione degli OID nelle configurazioni SNMP v2 e v3 sui dispositivi Nexus 5k, 7k e 9K.

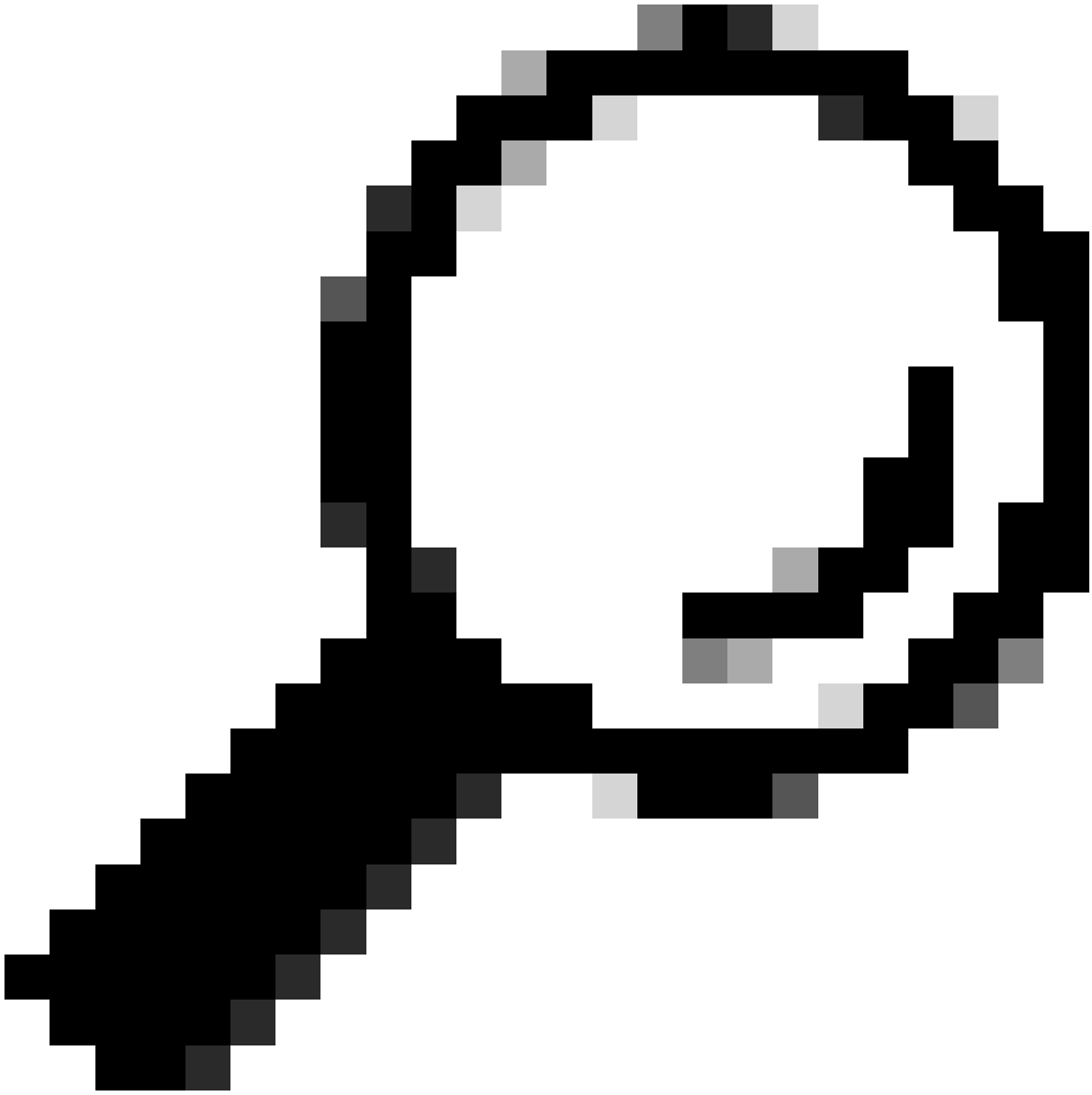
Operazioni di base

Modalità di configurazione accesso:

```
#conf t
```

Definire il ruolo dell'esclusione OID:

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



Suggerimento: {read/ read-write} consente di scegliere tra le operazioni SNMP "read" e "read-write". Le operazioni 'Read' in genere implicano il recupero di informazioni, mentre le operazioni 'read-write' implicano sia il recupero che la modifica di informazioni. È possibile scegliere le opzioni di lettura/lettura/scrittura in base alle proprie preferenze.

Uscire dalla modalità di configurazione:

```
#exit
```

Applicazione della configurazione alla community/utente SNMP.

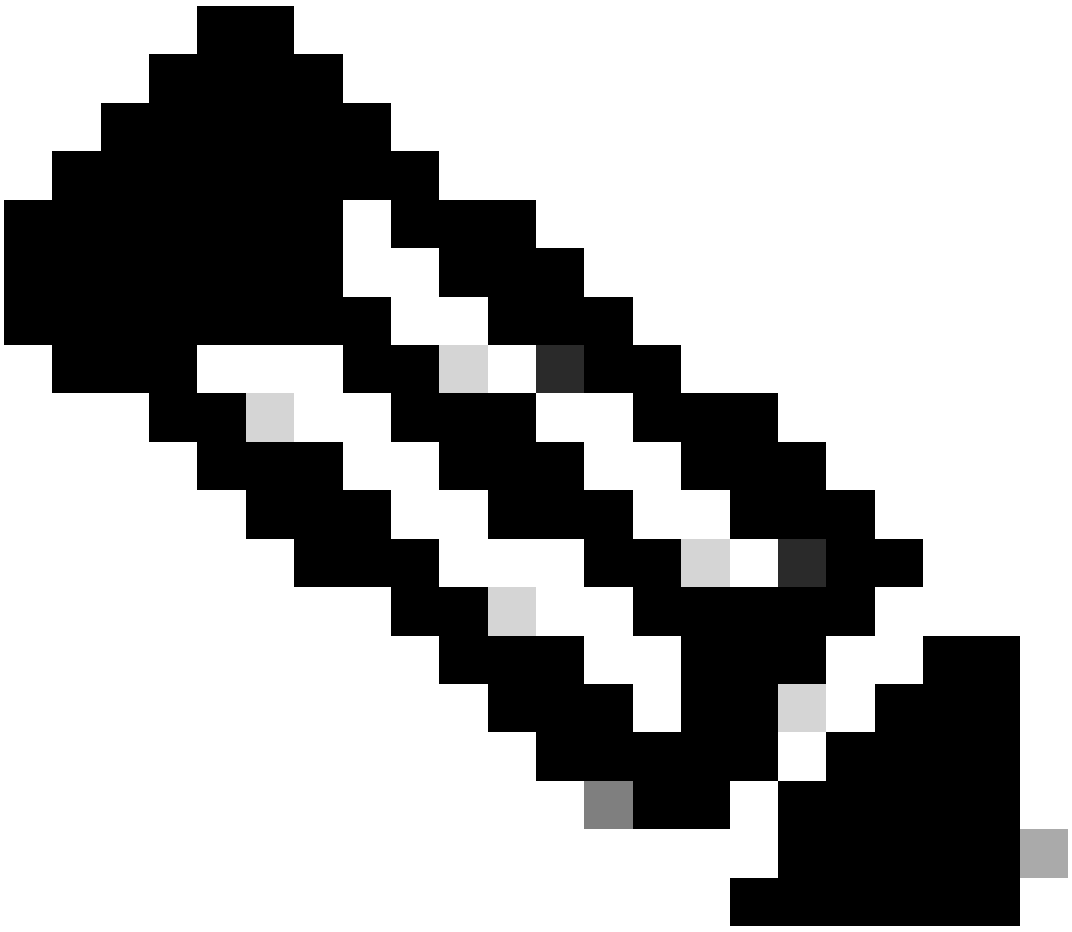
Per SNMPv2:

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

Per SNMPv3:

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

Configurazione



Nota: l'esempio include l'esclusione di OID 1.3.6.1.2.1.2.2.1.3 (ifType). Assicurarsi di sostituire l'OID ifType con quello che si desidera escludere.

Definizione di un ruolo per escludere 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#
```

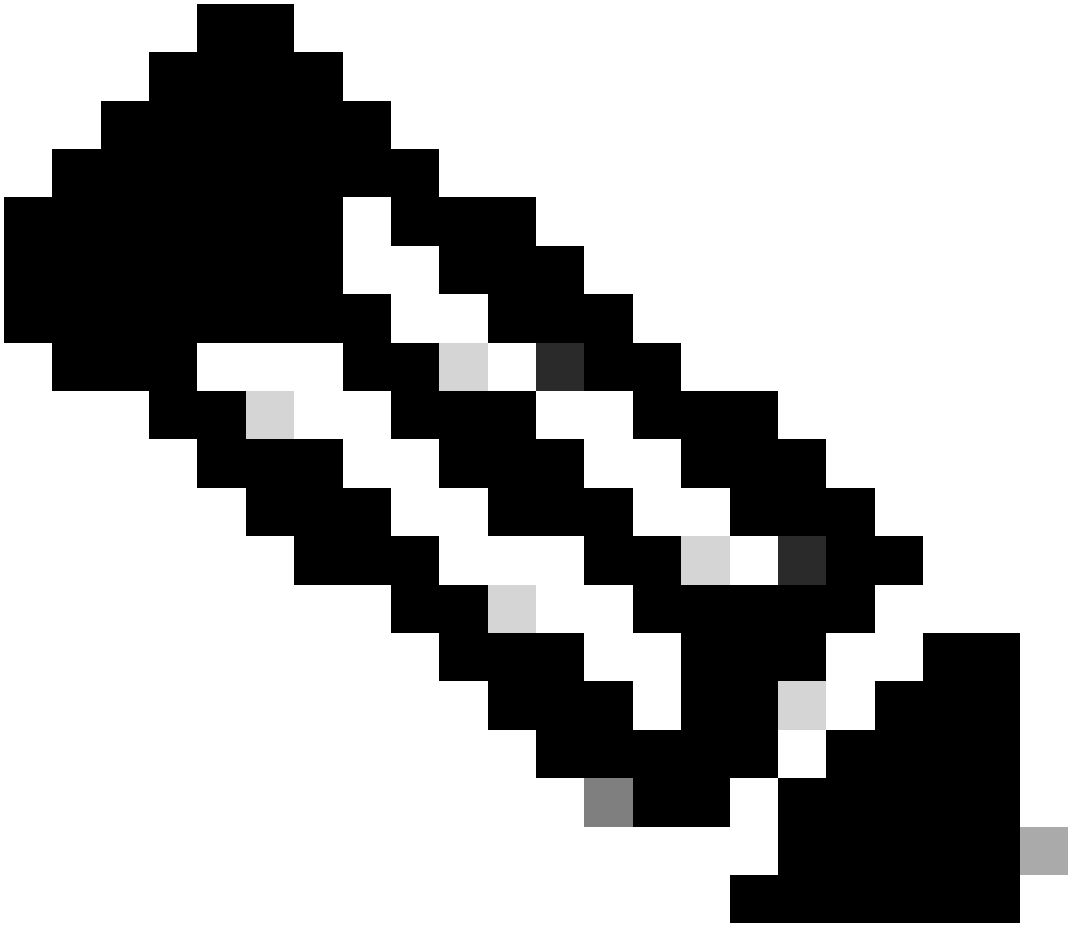
Creazione di una community SNMPv2 con deny_oid ruolo:

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

Creazione dell'utente SNMPv3 con ruolo **deny_oid**:

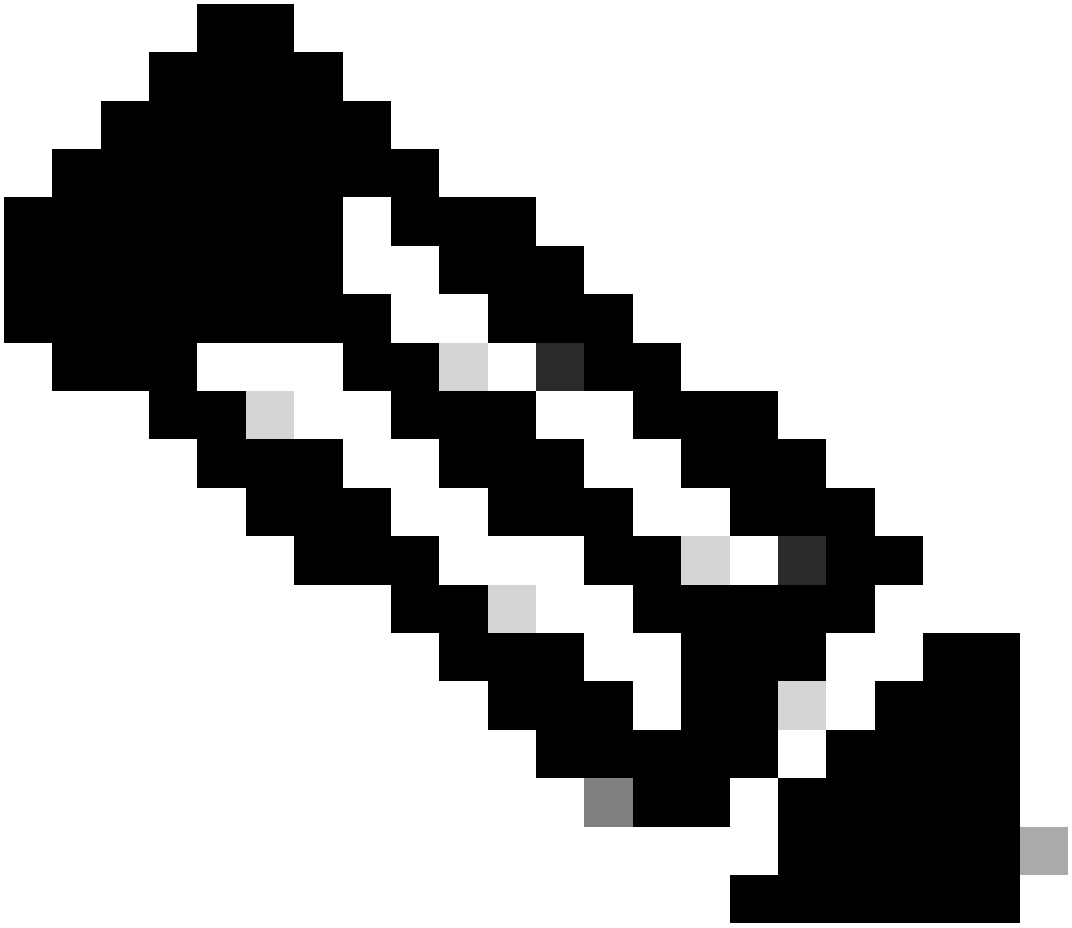
```
switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)# snmp-serv
```

Verifica



Nota: è stato utilizzato un test 'prova' dell'utente per verificare il polling di ifType OID. Gli altri utenti sono stati mappati con il ruolo **deny_oid** e non sono stati visualizzati dati per IfType OID come illustrato.

SNMPwalk senza esclusione:

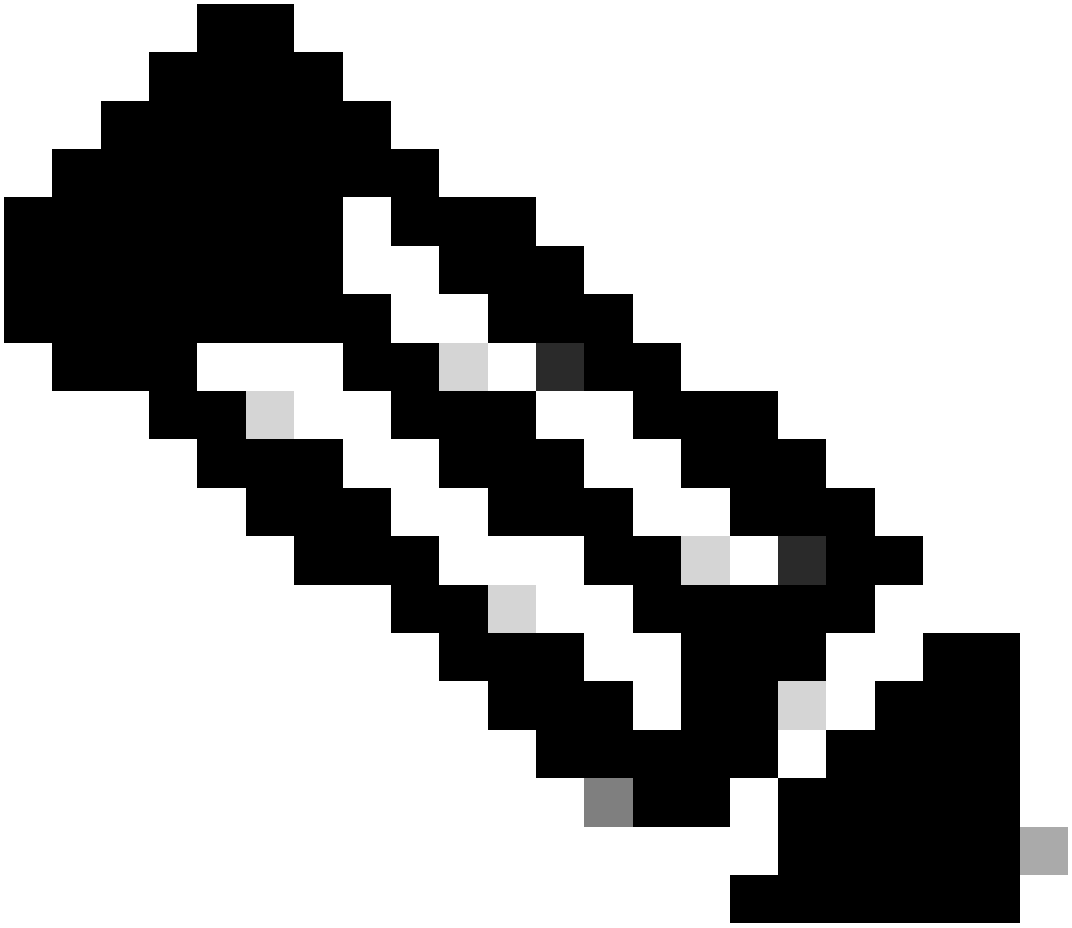


Nota: nell'articolo completo, l'indirizzo IP del dispositivo è sostituito da a.b.c.d.

```
[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 per SNMPv2 con OID escluso:

```
[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: è stato creato un nuovo utente 'trialv3' per illustrare il polling senza l'esclusione dell'OID.

SNMPwalk senza escludere OID:

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

SNMPwalk per utente SNMPv3 con OID escluso:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).