OID in Nexus 5000, 7000 und 9000 in SNMP v2- und v3-Konfiguration ausschließen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie OIDs in Nexus 5000, 7000 und 9000 in SNMP v2- und v3-Konfigurationen ausgeschlossen werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, vor der Implementierung von OID-Ausschlüssen (Object Identifier) über Kenntnisse in diesen Themen zu verfügen:

- Vertrautheit mit Simple Network Management Protocol (SNMP)
- Zugriff auf den Gerätekonfigurationsmodus
- Verständnis auszuschließender OIDs
- Verständnis der SNMP-Community und der Benutzerkonfigurationen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Labortests mit den folgenden Nexus-Modellen:

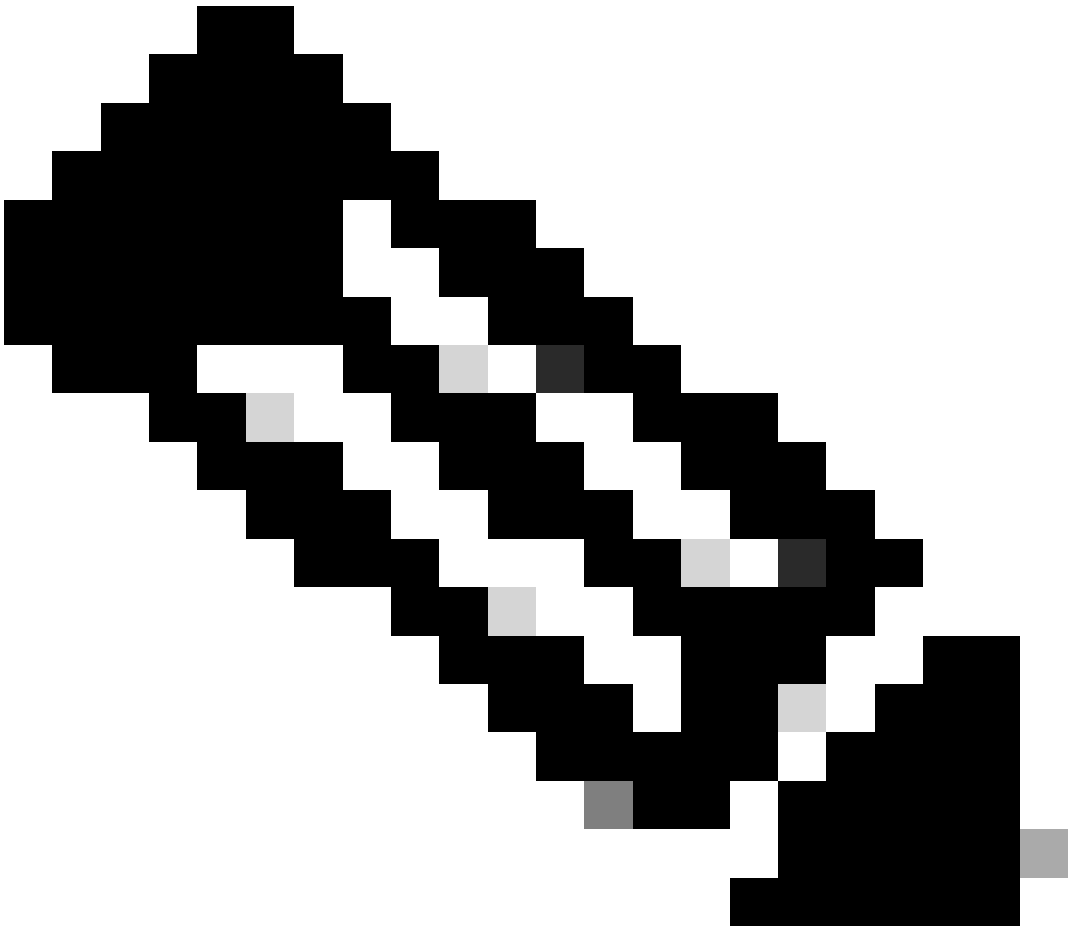
- Nexus 5000
- Nexus 7000
- Nexus 9000

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In der Welt von SNMP treten häufig Situationen auf, in denen das Parsen des MIB-Trees (Management Information Base) mit Hürden verbunden ist. Bei bestimmten OIDs kommt es zum Stillstand, was manchmal zu Zeitüberschreitungen oder ähnlichen Problemen führt. Eine weitere häufige Herausforderung besteht darin, dass durch kontinuierliches Polling für eine problematische OID Warnungen ausgelöst werden, die weder notwendig noch wirkungsvoll sind. Eine Möglichkeit, diese Szenarien zu beseitigen, besteht darin, Ausschlüsse zu erstellen und das Gerät anzuweisen, die spezifische OID zu überspringen und mit dem Rest der MIB-Struktur fortzufahren. Indem Sie das Gerät anweisen, die problematische OID zu umgehen und mit dem Rest der MIB-Struktur fortfahren, können Sie einen reibungslosen Fluss des MIB-Trees fördern.



> Hinweis: Beachten Sie, dass dieser Ausschluss sich darauf auswirken kann, wie Daten aus dem MIB-Tree gelesen werden. Gehen Sie vorsichtig vor, und stellen Sie sicher, dass die OID erforderlich ist, bevor Sie mit diesen Ausschlüssen fortfahren.

Während der Ausschluss von OIDs in Geräten wie Aggregation Services Router (ASR)/Catalyst Switches (CAT)/Integrated Service Router (ISR) in der Regel einen einfachen Prozess verfolgt, erweist sich die Bewältigung dieser Herausforderung in Nexus-Geräten aufgrund des Fehlens von Ansichten als komplizierter. In diesem Artikel wird ein innovativer Ansatz beschrieben. Es werden Rollen vorgestellt und dieser der Community bzw. dem Benutzer zugeordnet. Außerdem wird eine Lösung zum Ausschluss von OIDs in SNMP v2- und v3-Konfigurationen auf Nexus 5000-, 7k- und 9K-Geräten vorgestellt.

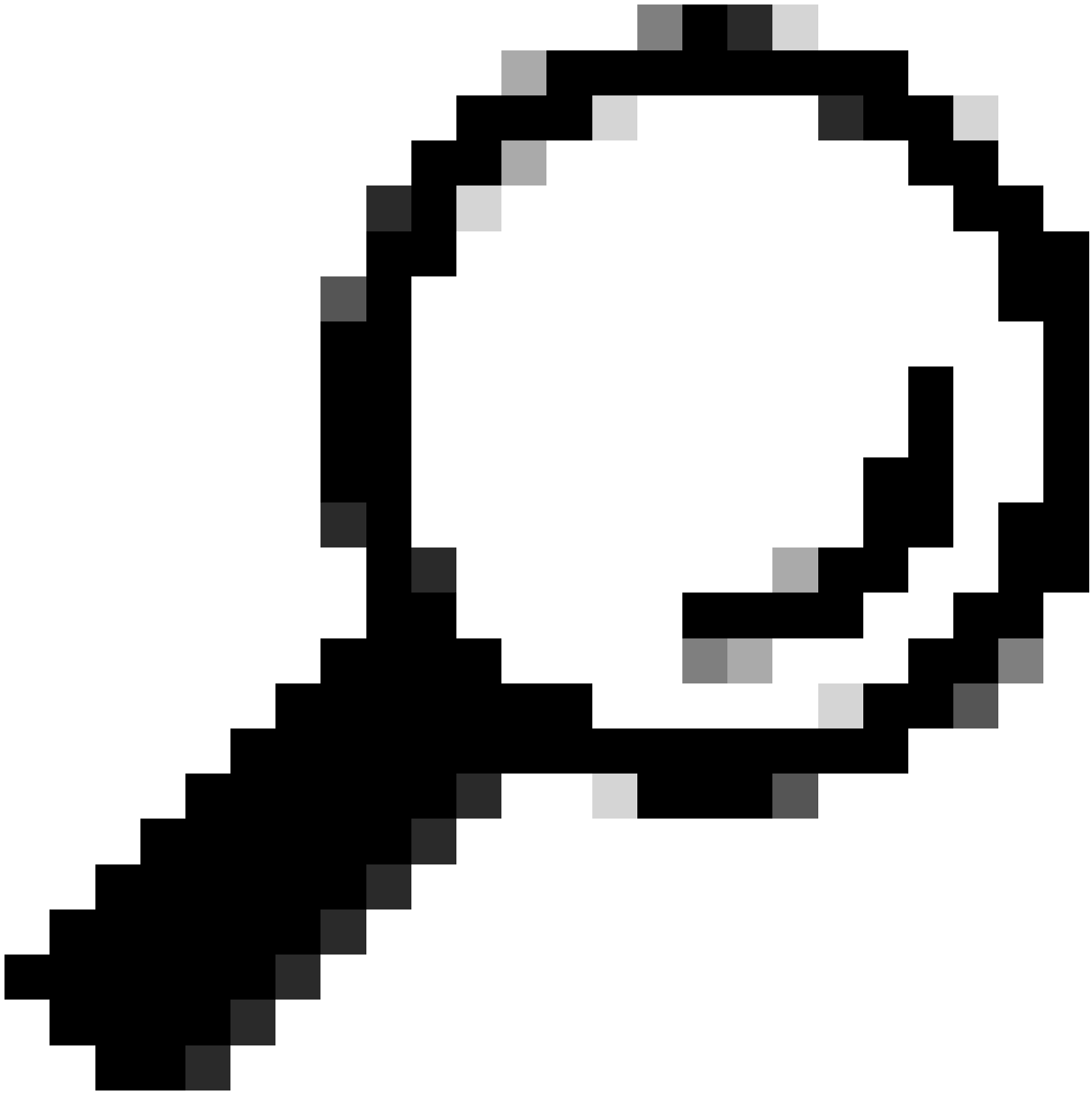
Grundlegende Schritte

Zugriffs-Konfigurationsmodus:

```
#conf t
```

Rolle des OID-Ausschlusses definieren:

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



Tipp: {read/read-write} ermöglicht Ihnen die Auswahl zwischen 'read' und 'read-write' SNMP-Vorgängen. Lesevorgänge umfassen in der Regel das Abrufen von Informationen, während Lese-/Schreibvorgänge sowohl das Abrufen als auch das Ändern von Informationen umfassen. Sie können zwischen Lese-/Schreibzugriff wählen.

Beenden Sie den Konfigurationsmodus:

```
#exit
```

Konfiguration auf SNMP-Community/-Benutzer anwenden.

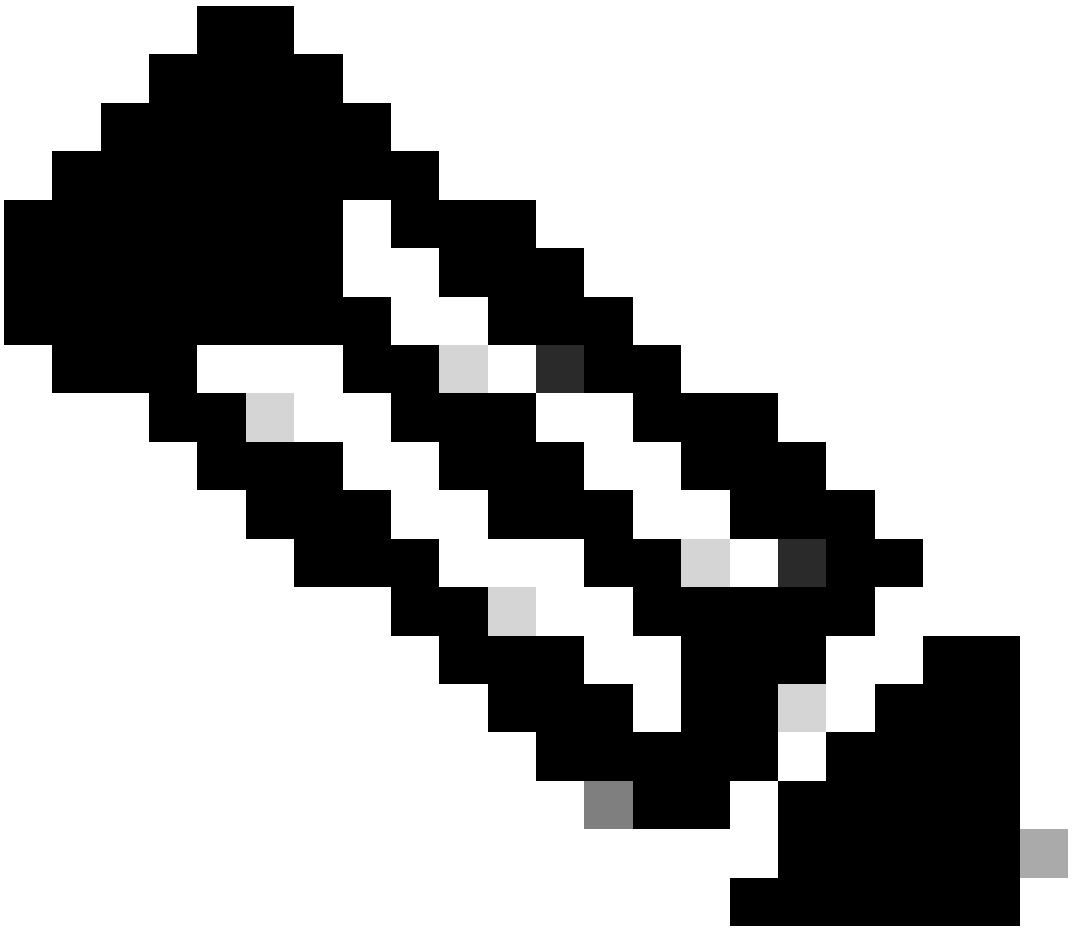
Für SNMPv2:

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

Für SNMPv3:

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

Konfiguration



Hinweis: In diesem Beispiel wird die OID 1.3.6.1.2.1.2.2.1.3 (ifType) ausgeschlossen. Ersetzen Sie die ifType-OID durch die auszuschließende.

Definieren einer Rolle zum Ausschließen einer OID, wennType:

```
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#
```

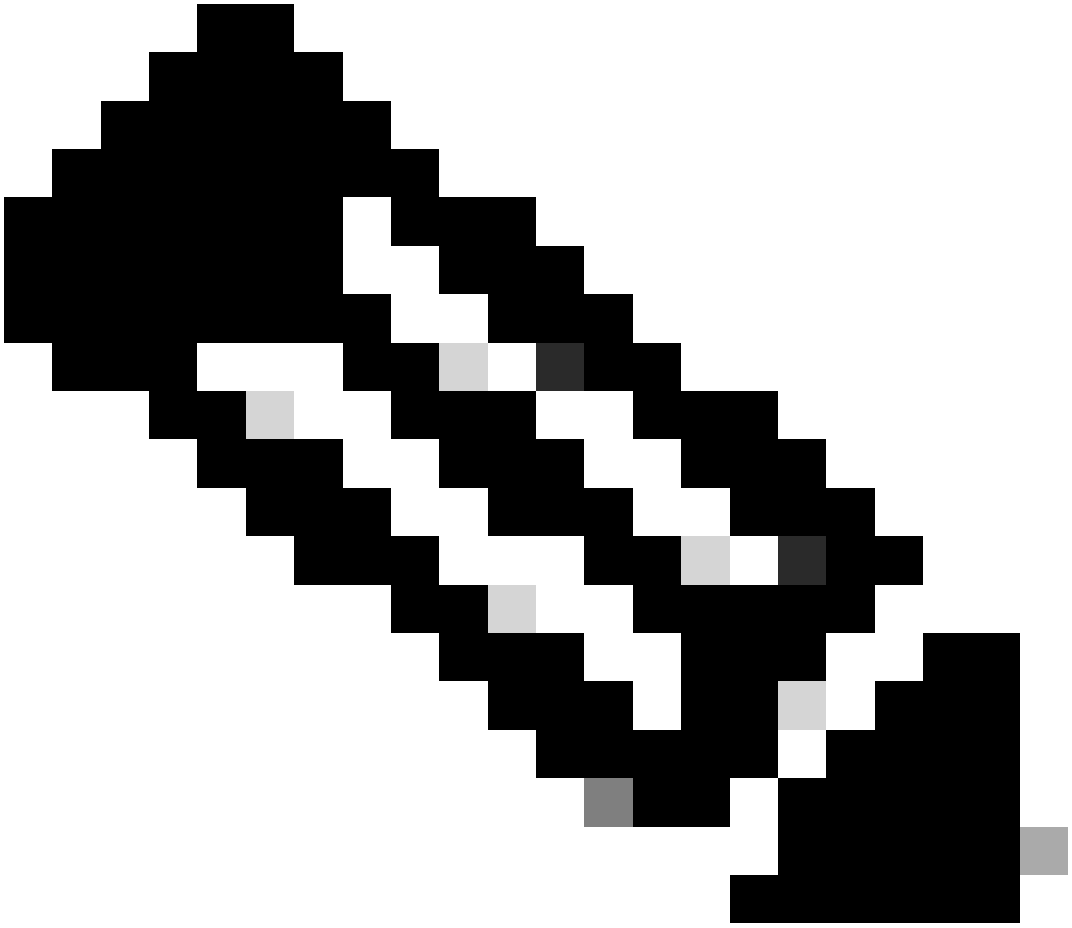
Erstellen einer SNMPv2-Community mit der deny_oid Rolle:

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

Erstellen eines SNMPv3-Benutzers mit der Rolle **deny_oid**:

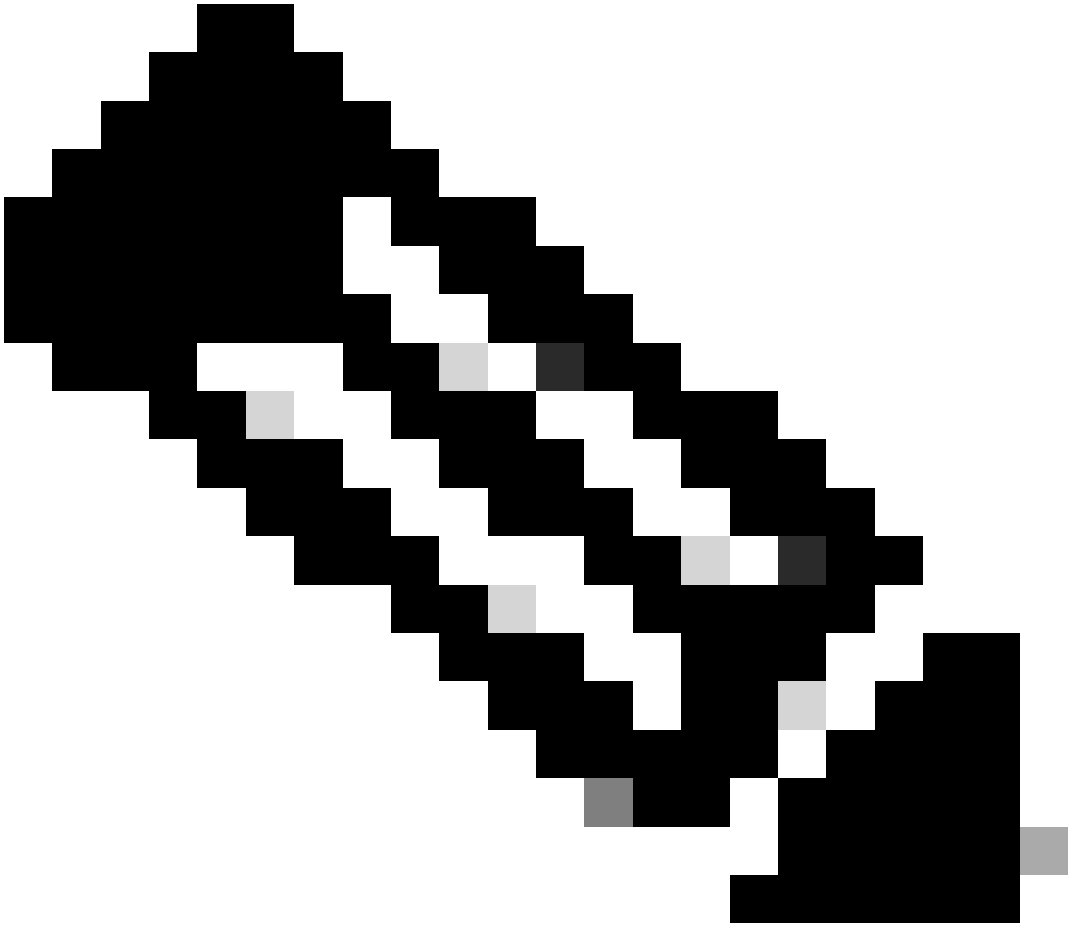
```
switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)# snmp-serv
```

Verifizierung



Hinweis: Ein Testbenutzer 'Testversion' wurde verwendet, um das Polling der ifType-OID zu überprüfen. Den übrigen Benutzern wurde die Rolle **deny_oid** zugeordnet, und es wurden keine Daten für ifType-OID angezeigt, wie dargestellt.

SNMPwalk ohne Ausschluss:

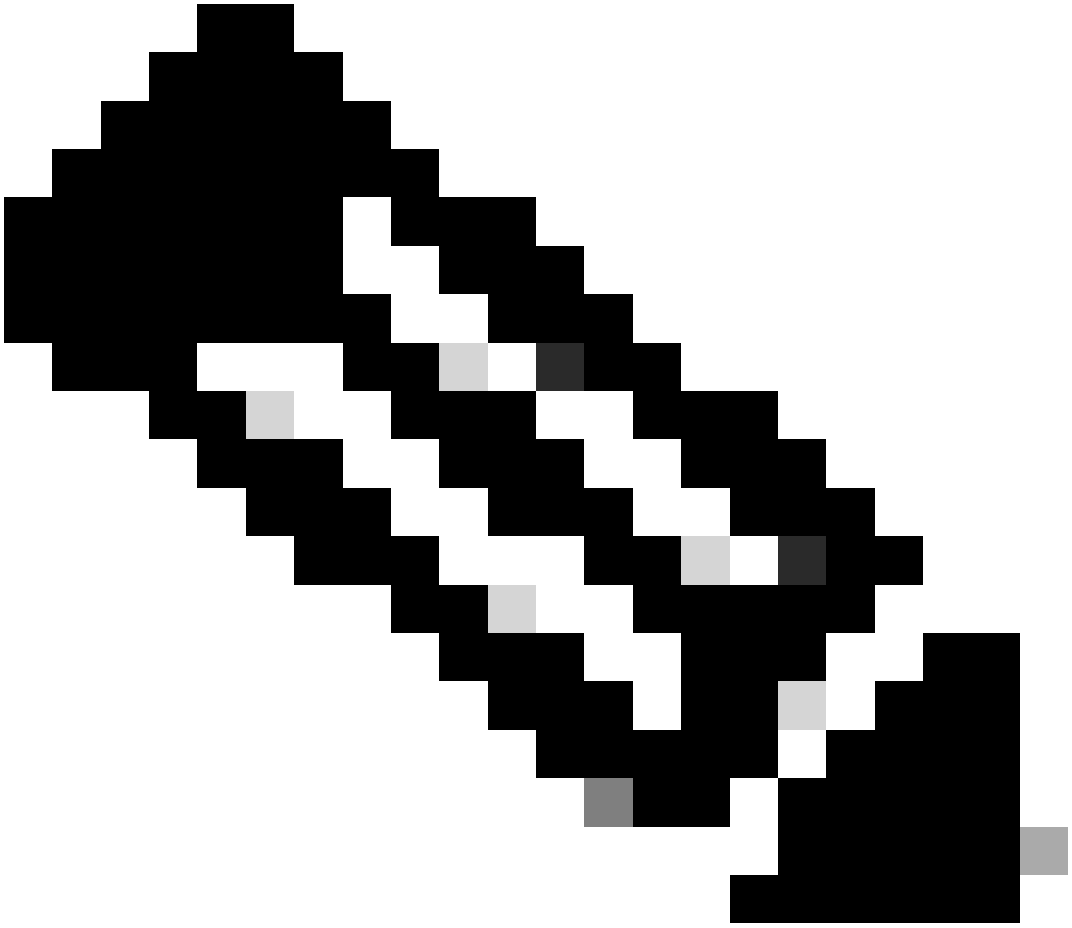


Hinweis: a.b.c.d wird anstelle der IP-Adresse des Geräts im gesamten Artikel verwendet.

```
[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 für SNMPv2 mit ausgeschlossener 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
```



Hinweis: Es wurde ein neuer Benutzer "trialv3" erstellt, um die Abfrage ohne Ausschluss der OID zu veranschaulichen.

SNMPwalk ohne Ausschluss der OID:

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

SNMPwalk für SNMPv3-Benutzer mit ausgeschlossener OID:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.