SNMP v2およびv3設定でのNexus 5000、7000、9000でのOIDの除外

内容

はじめに

このドキュメントでは、SNMP v2およびv3設定でNexus 5000、7000、9000のOIDを除外する方法について説明します。

前提条件

要件

Object Identifier（OID；オブジェクト識別子）除外を実装する前に、次の項目に関する知識があることが推奨されます。

- Simple Network Management Protocol(SNMP)に精通していること
- デバイス設定モードへのアクセス
- 除外するOIDの理解
- SNMPコミュニティおよびユーザ設定の理解

使用するコンポーネント

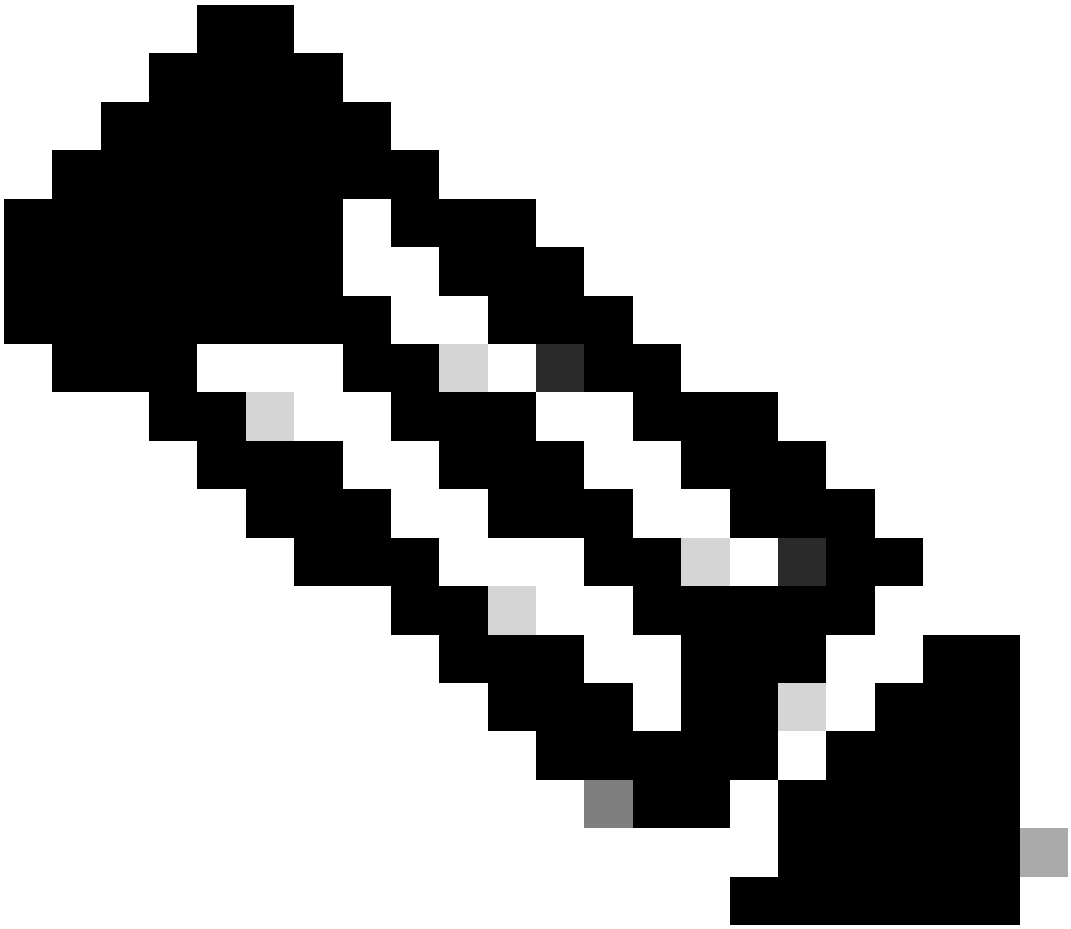
このドキュメントの情報は、次のNexusモデルを使用したラボテストに基づいています。

- Nexus 5k
- Nexus 7000
- Nexus 9000

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

SNMPの世界では、Management Information Base（MIB；管理情報ベース）ツリーの解析が困難になり、特定のOIDで停止に達すると、ウィンドウタイムアウトなどの問題が発生する場合があります。また、問題のあるOIDを継続的にポーリングすることで、不要で影響のないアラートがトリガーされる場合にも、一般的な問題が発生します。このようなシナリオを取り除く方法の1つとして、除外を作成し、その特定のOIDをスキップしてMIB構造の残りの部分に進むようにデバイスに指示する方法があります。面倒なOIDをバイパスし、MIB構造の残りの部分を続行するようにデバイスを設定することで、MIBツリーの円滑なフローを促進できます。



> 注：この除外は、MIBツリーからのデータの読み取り方法に影響する可能性があることに注意してください。これらの除外に進む前に、注意してOIDの必要性を確認してください。

通常、OIDを除外すると、アグリゲーションサービスルータ(ASR)、Catalystスイッチ(CAT)、統合サービスルータ(ISR)などのデバイスで単純なプロセスが実行されますが、Nexusデバイスでこ

の課題を解決するには、ビューがないため複雑になります。この記事では、ロールを紹介し、それらをコミュニティ/ユーザにマッピングすることで革新的なアプローチを考察し、Nexus 5000、7000、9000デバイスでのSNMP v2およびv3設定でOIDを除外するためのソリューションを示します。

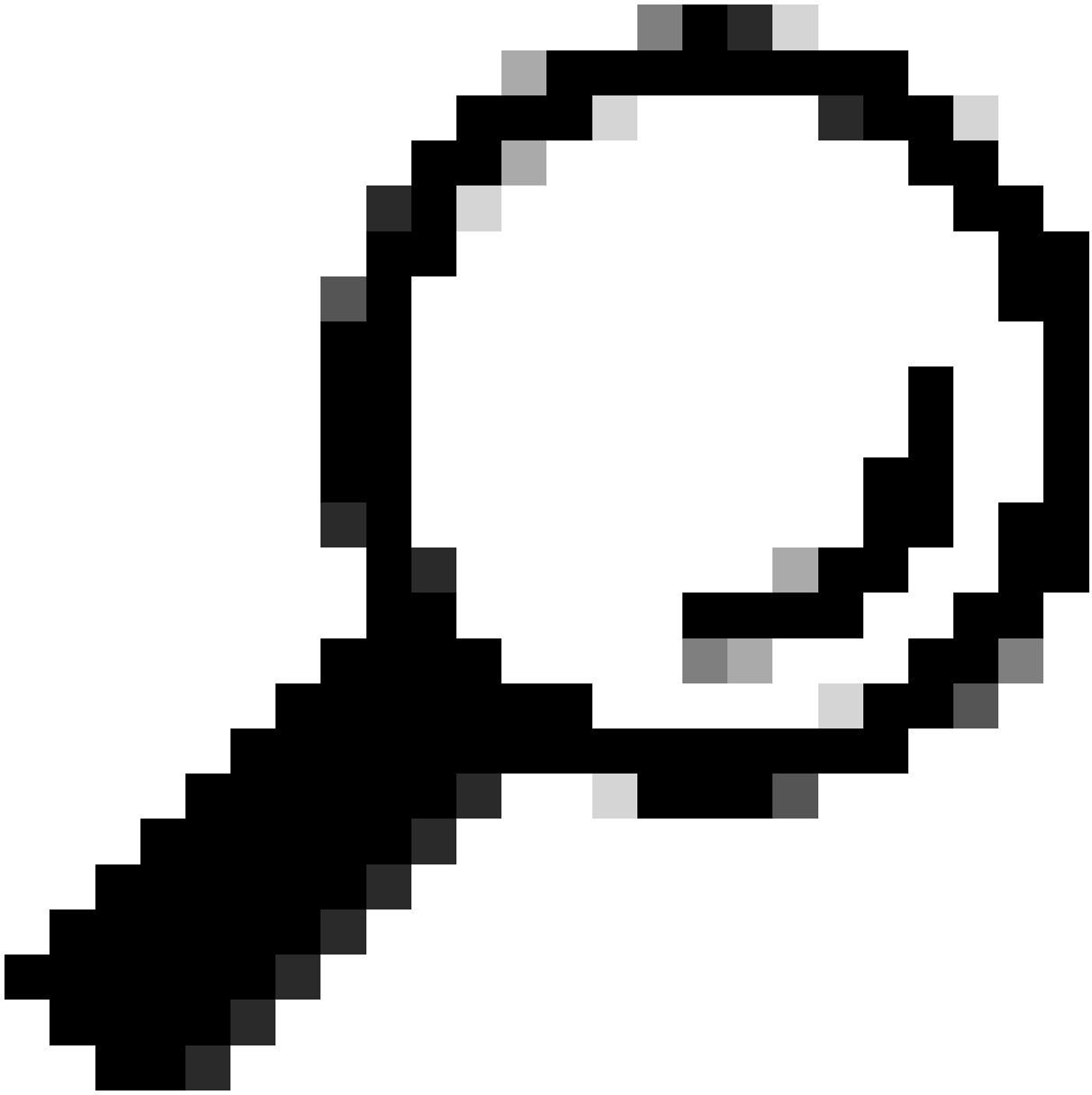
基本的な手順

アクセスコンフィギュレーションモード：

```
#conf t
```

OID除外のロールの定義：

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



ヒント:{read/ read-write}を使用すると、SNMP操作を「read」または「read-write」から選択できます。通常、「読み取り」操作には情報の取得が含まれ、「読み取り/書き込み」操作には情報の取得と変更が含まれます。必要に応じて、読み取り/読み取り/書き込みを選択できます。

設定モードを終了します。

```
#exit
```

SNMPコミュニティ/ユーザに設定を適用します。

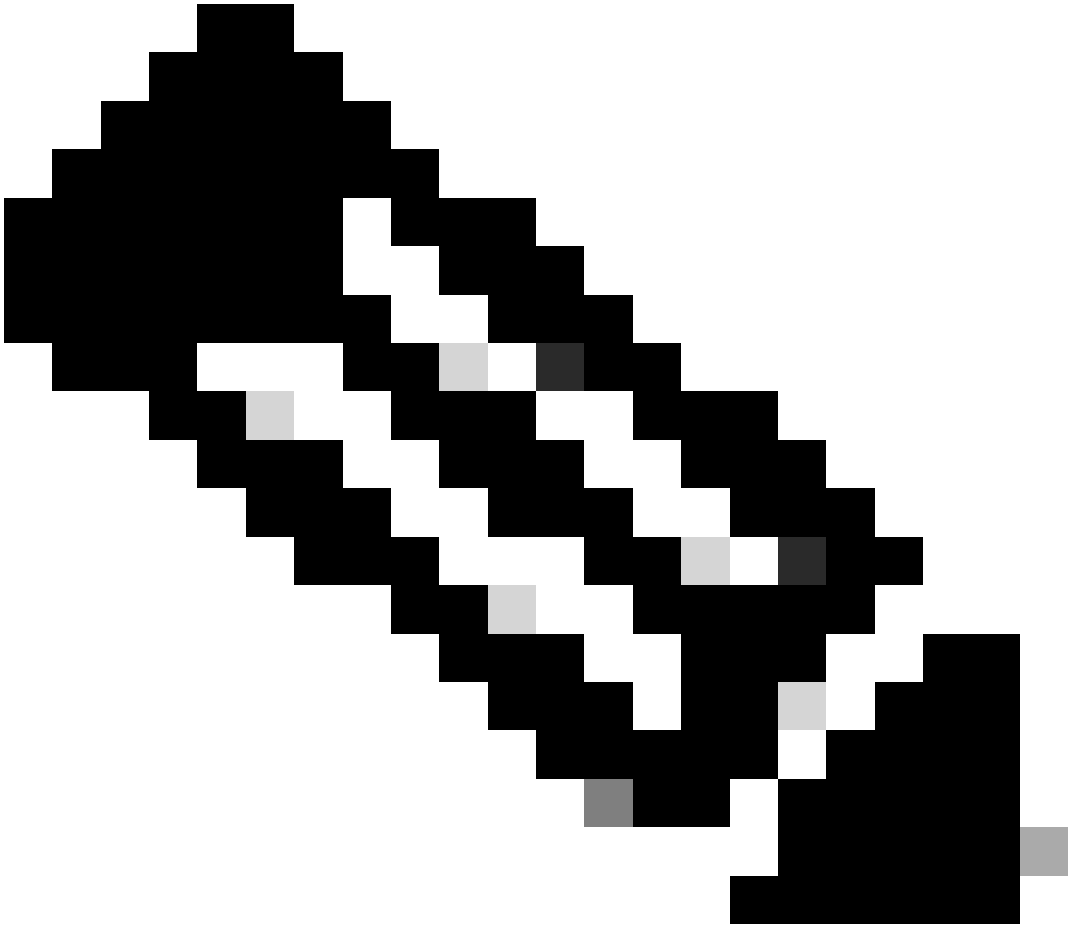
SNMPv2の場合

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

SNMPv3の場合

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

コンフィギュレーション



注：この例では、OID 1.3.6.1.2.1.2.2.1.3(ifType)が除外されています。ifType OIDは、必ず除外するOIDに置き換えてください。

OIDのifTypeを除外するロールの定義：

```
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#
```

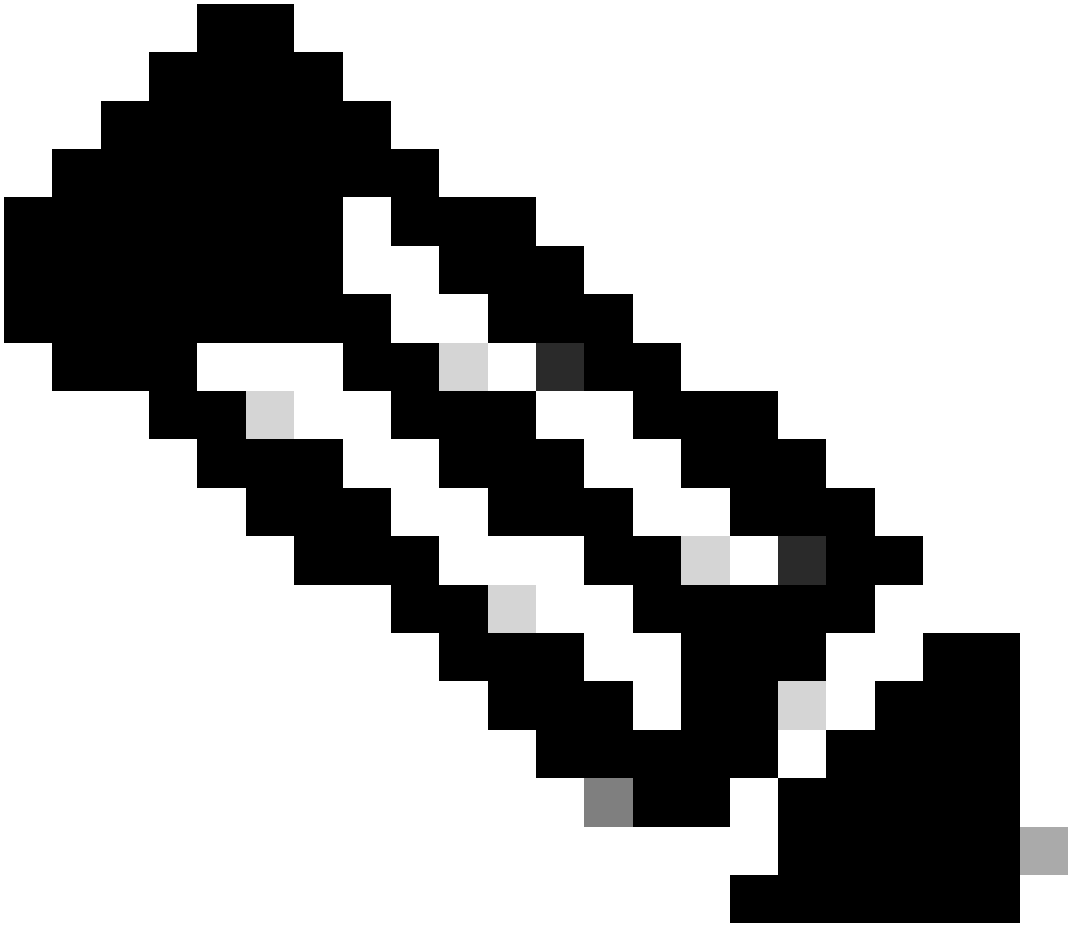
deny_oidの役割を持つSNMPv2コミュニティの作成:

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

deny_oidロールを持つSNMPv3ユーザを作成します。

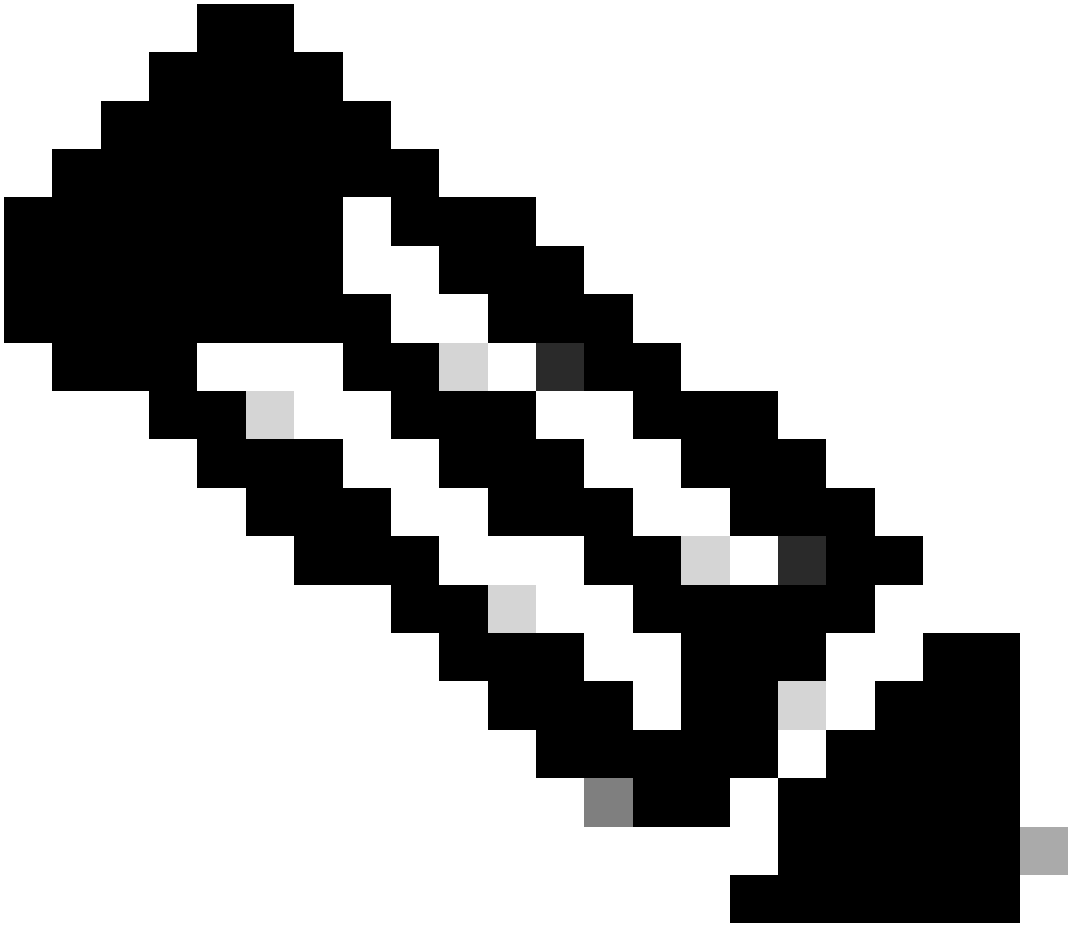
```
switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)# snmp-serv
```

検証



注:ifType OIDのポーリングを確認するために、テストユーザ「trial」が使用されました。残りのユーザは**deny_oid**ロールでマッピングされ、図に示すようにifType OIDのデータは表示されませんでした。

除外しないSNMPwalk:

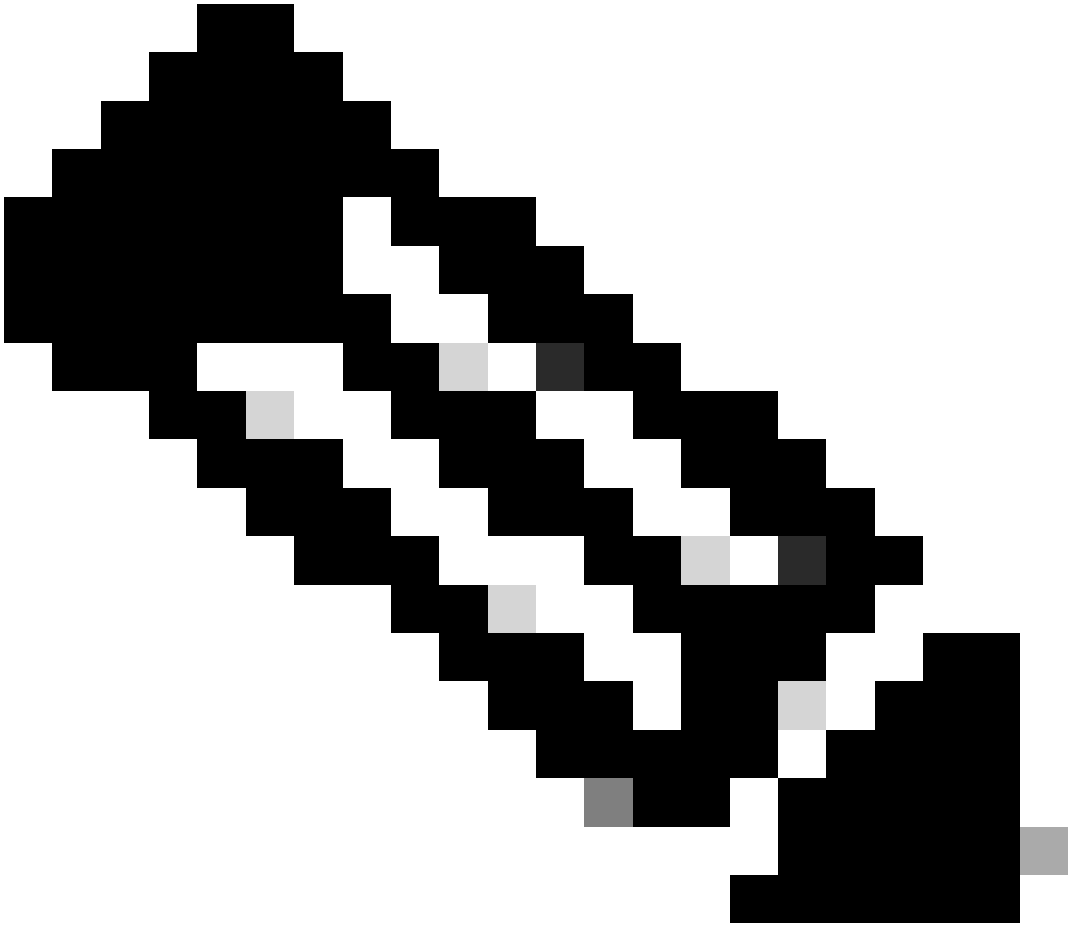


注：記事全体では、デバイスのIPアドレスの代わりにa.b.c.dが使用されています。

```
[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
```

除外されたOIDを持つSNMPv2の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:OIDを除外しないポーリングを示すために、新しいユーザ「trialv3」が作成されました。

OIDを除外しないSNMPwalk:

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

除外されたOIDを持つSNMPv3ユーザのSNMPwalk:

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。