

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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[基本的な手順](#)

[コンフィギュレーション](#)

[検証](#)

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

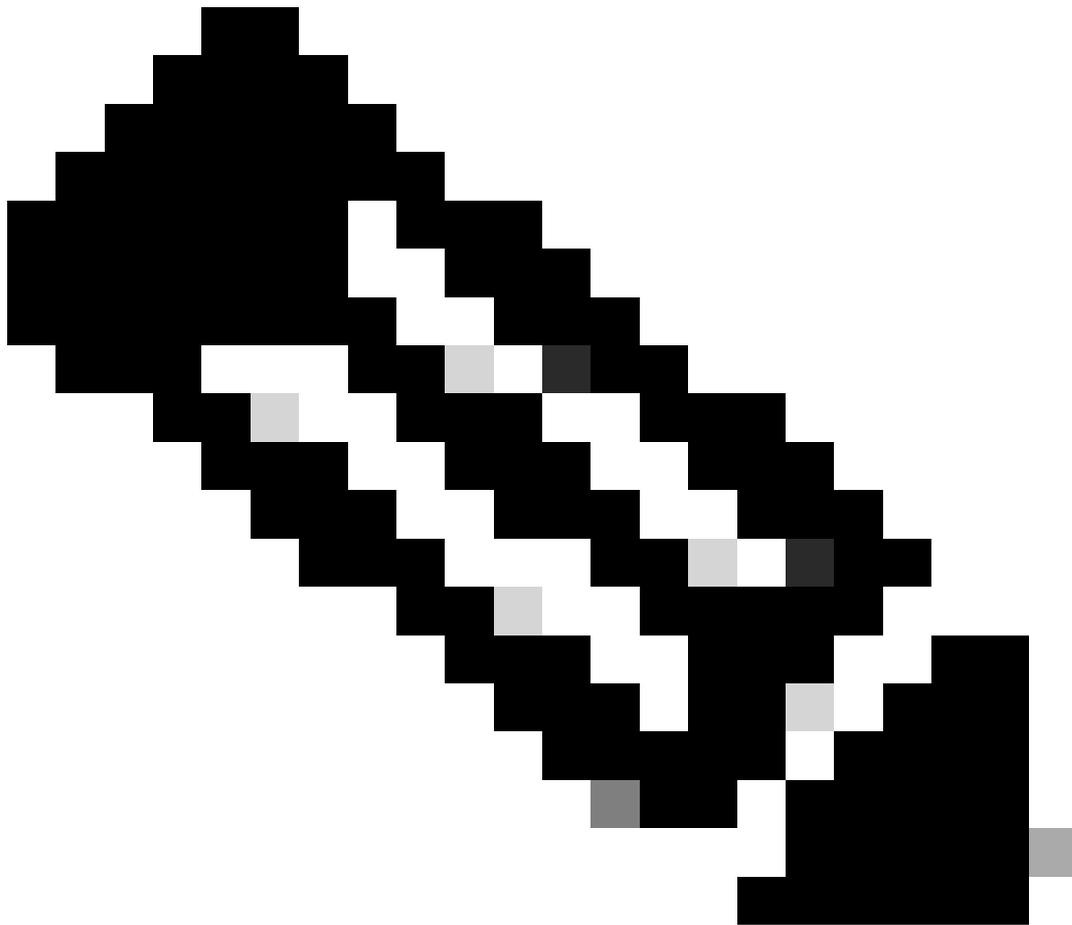
このドキュメントの情報は、次のNexusモデルを使用したラボテストに基づいています。

- Nexus 5000
- 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。もう1つの一般的な問題は、面倒なOIDを連続して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です。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を与え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。

OIDを除外すると、通常は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)などのデバイスで簡単なプロセスが実行されますが、Nexusデバイスでこの問

問題を解決するには、ビューがないため複雑さが増します。この記事では、ロールを導入してコミュニティ/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、および9000デバイス上の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

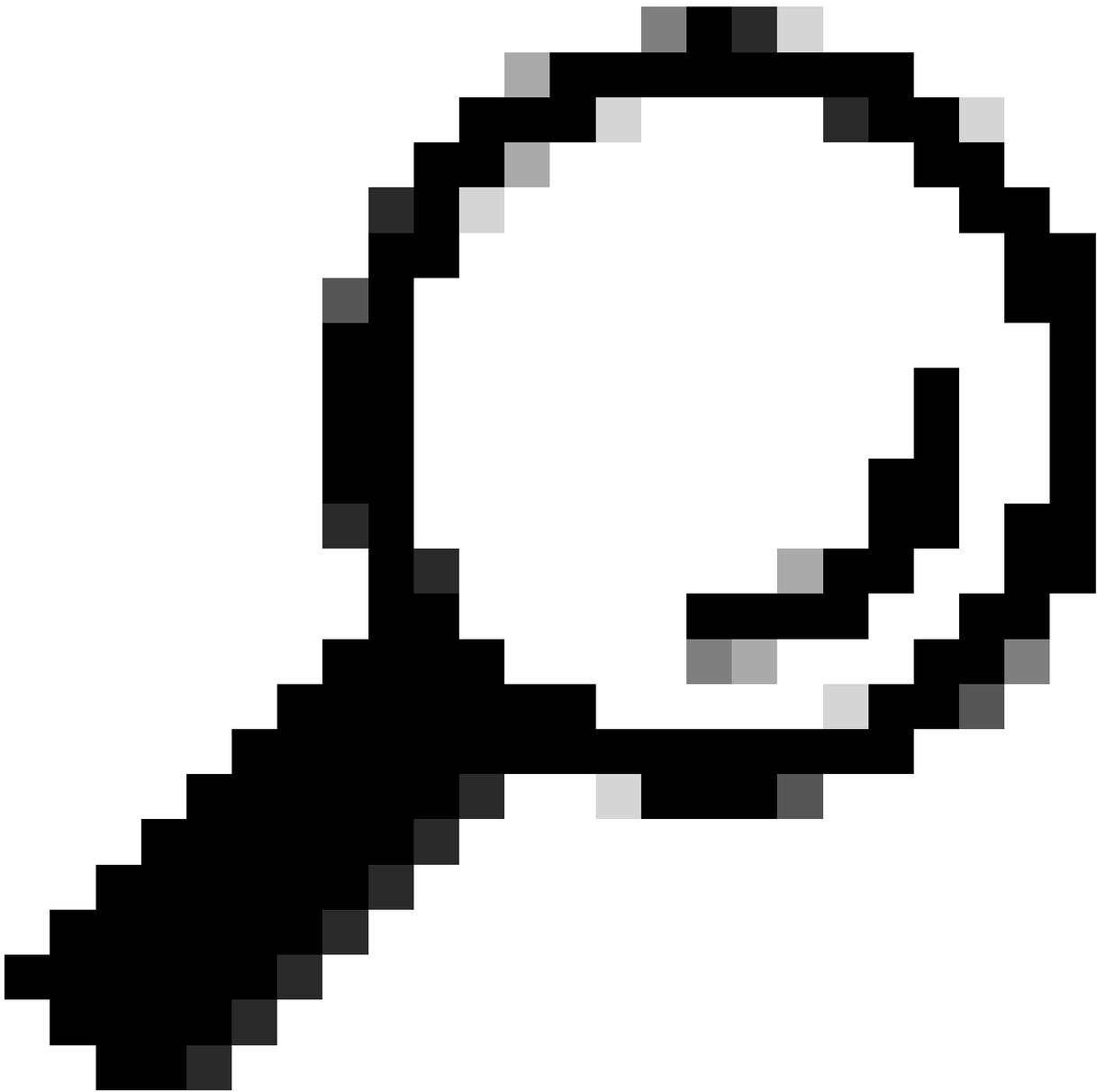
アクセスコンフィギュレーションモード：

```
#conf t
```

OID除外のロールの定義：

```
#role name
```

```
#rule 1 permit read feature snmp  
#rule 2 deny {read/ read-write} oid
```



ヒント:{read/read-write}を使用すると、SNMP操作を「読み取り」または「読み取り/書き込み」から選択できます。通常、「読み取り」操作は情報の取得を伴い、「読み取り/書き込み」操作は情報の取得と変更を伴います。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
```

```
group
```

SNMPv3の場合：

```
#snmp-server user
```

```
auth {sha/md5}
```

```
priv {aes/des}
```

コンフィギュレーション

注：この例には、OID 1.3.6.1.2.1.2.2.1.3(ifType)の除外が含まれています。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コミュニティを作成します。

```

switch(config)# snmp-server community snmpv2user group deny_oid
switch(config)# exit
switch# sh snmp community
Community          Group / Access    context    acl_filter
-----
snmpv2user         deny_oid
switch#

```

deny_oidルールを持つ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-server user snmpv3user deny_oid auth sha password!123 priv ?
WORD Privacy password for user (Max Size 134)
switch(config)# snmp-server user snmpv3user deny_oid auth sha password!123 priv password!123
switch(config)# do sh snmp user

```

```

-----
SNMP USERS
-----
User          Auth    Priv(enforce) Groups    acl_filter
-----
admin         md5     aes-128(no)  network-admin
snmpv3user    sha     aes-128(no)  deny_oid

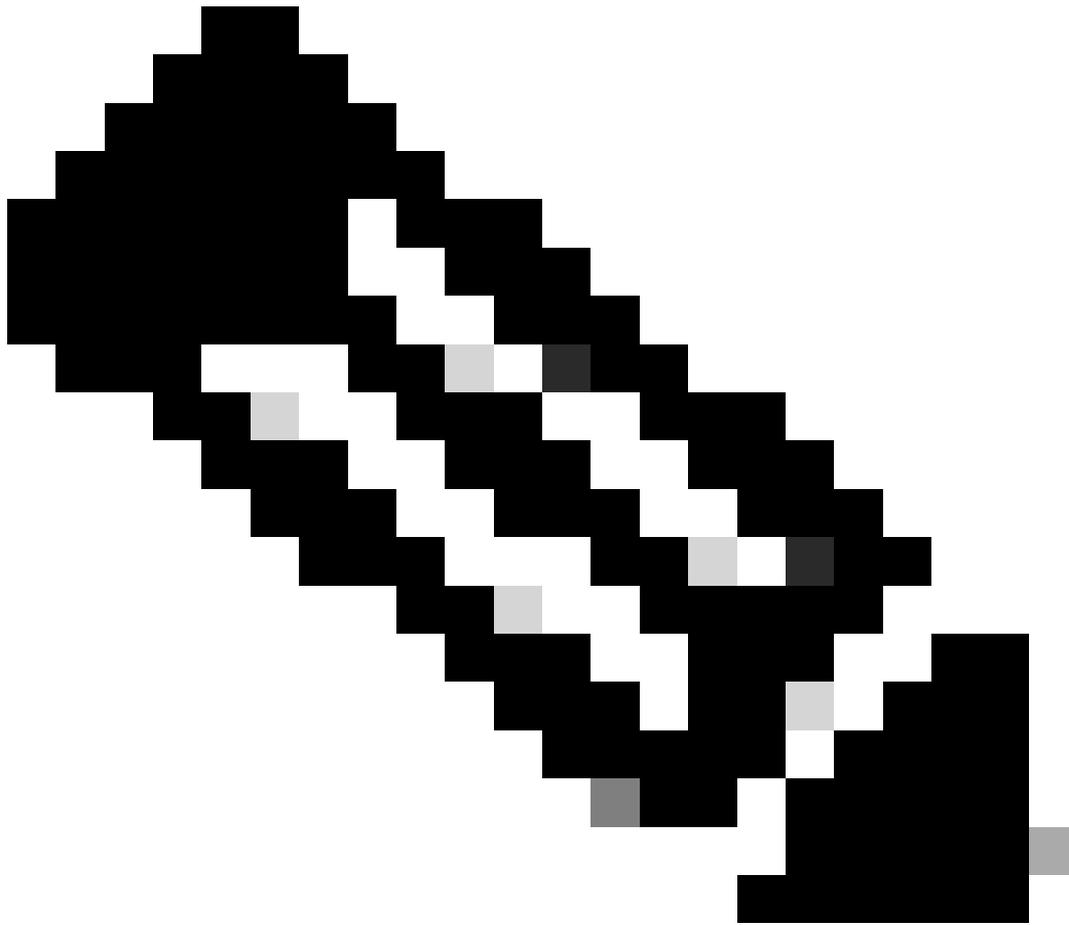
```

```

NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
User          Auth    Priv
-----
switch(config)#

```

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のデータを示しませんでした。

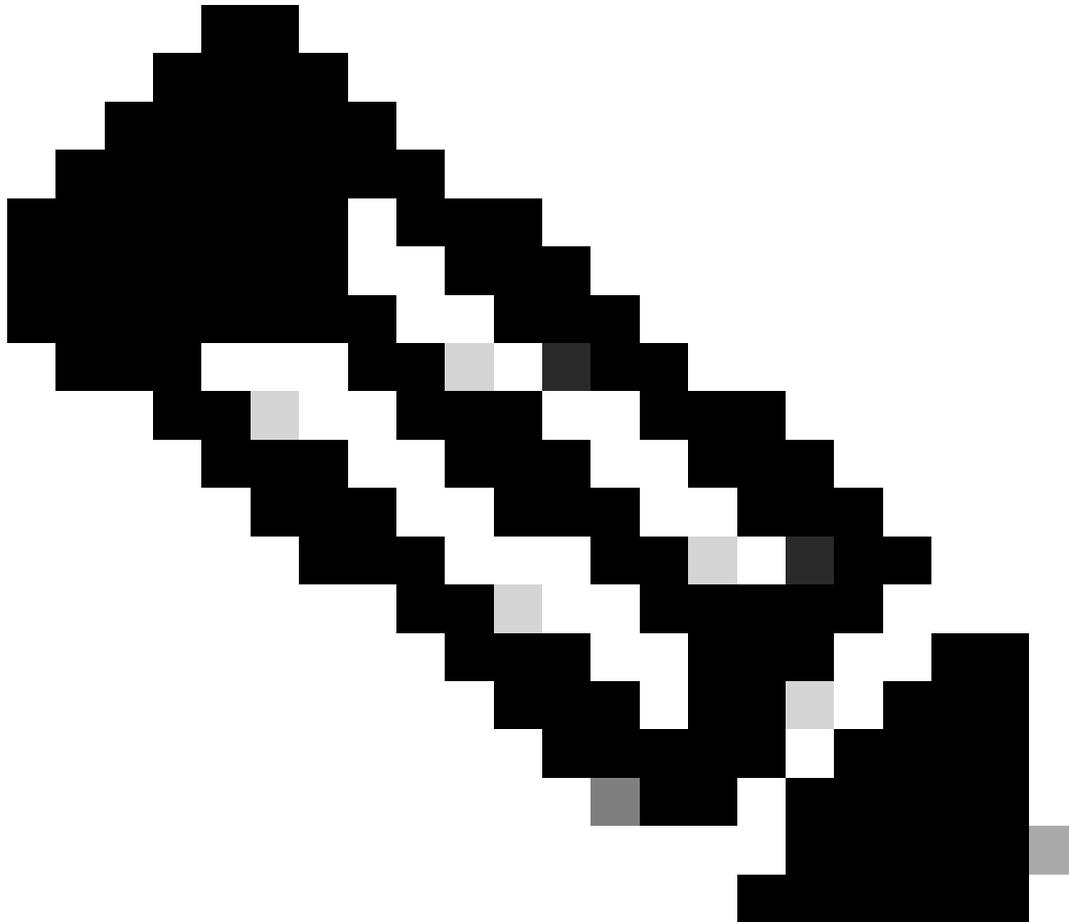
除外しないSNMPwalk:

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: ethernetCsmacd(6)
IF-MIB::ifType.436207616 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436208128 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436208640 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436209152 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436209664 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436210176 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436210688 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436211200 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436211712 = INTEGER: ethernetCsmacd(6)
^C
```

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 available on this agent at this OID
```



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.
IF-MIB::ifType.83886080 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436207616 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436208128 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436208640 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436209152 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436209664 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436210176 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436210688 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436211200 = INTEGER: ethernetCsmacd(6)
```

```
IF-MIB::ifType.436211712 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436212224 = INTEGER: ethernetCsmacd(6)
^C
[root@user ~]#
```

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'
IF-MIB::ifType = No Such Object available on this agent at this OID
[root@user ~]#
```

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。