

在Catalyst SD-WAN上配置SNMPv3

目录

[简介](#)

[背景](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

[参考](#)

简介

本文档介绍SNMPv3配置，并解释有关安全（身份验证）、加密（隐私）和限制（查看）的内容。

背景

通常，在我们知道需要做什么之前，SNMPv3配置会非常复杂且难以配置。SNMPv3存在的原因与HTTPS类似：安全性、加密和限制。

先决条件

了解SD-WAN功能模板和设备模板。

对SNMP MIB、SNMP轮询和SNMP Walk的一般了解

要求

SD-WAN控制器

思科边缘路由器

使用的组件

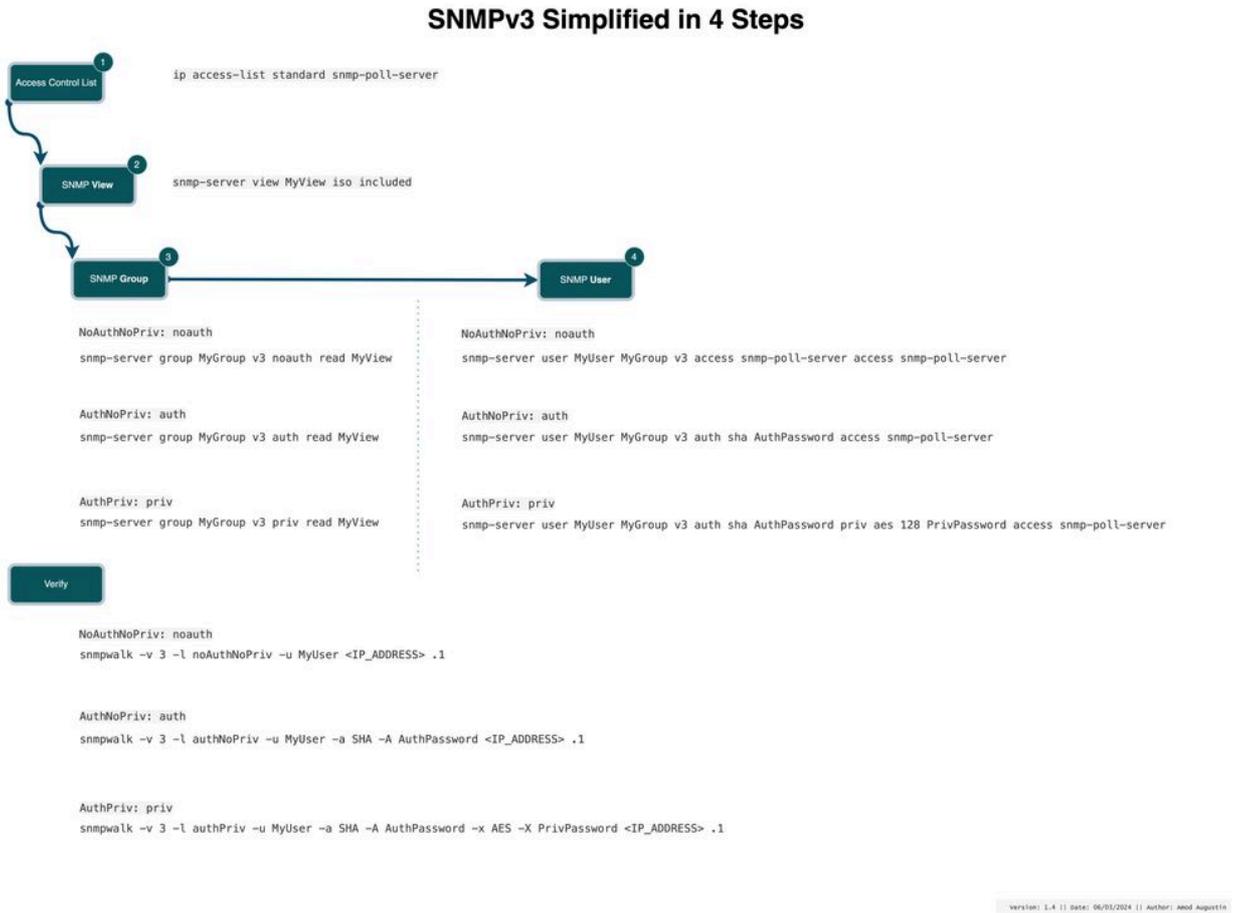
20.9上的SD-WAN控制器

17.9版的思科边缘路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

该图有助于您了解从CLI支架配置SNMPv3的所有要求。



SNMPv3简化为4步

一旦您了解了它很容易将概念放到CLI或功能模板中。让我们深入了解一下。

步骤 1 :

配置ACL以允许可以轮询系统的用户 (本例中为路由器)。

```
ip access-list standard snmp-poll-server
```

步骤 2 :

定义snmp视图，因为术语表示轮询器可以访问什么，这是我们的限制。

```
snmp-server view MyView iso included
```

步骤 3 :

定义snmp组，snmp组主要包括两部分a。安全级别b。限制（视图）。

安全级别：

- noAuthNoPriv:无身份验证和隐私（无加密）。
- authNoPriv:身份验证是必需的，但不需要隐私。
- authPriv:身份验证和隐私都是必需的。

限制是我们在步骤2中定义的限制，我们将其全部放在一起。

```
!NoAuthNoPriv: noauth  
snmp-server group MyGroup v3 noauth read MyView
```

```
!AuthNoPriv: auth  
snmp-server group MyGroup v3 auth read MyView
```

```
!AuthPriv: priv  
snmp-server group MyGroup v3 priv read MyView
```

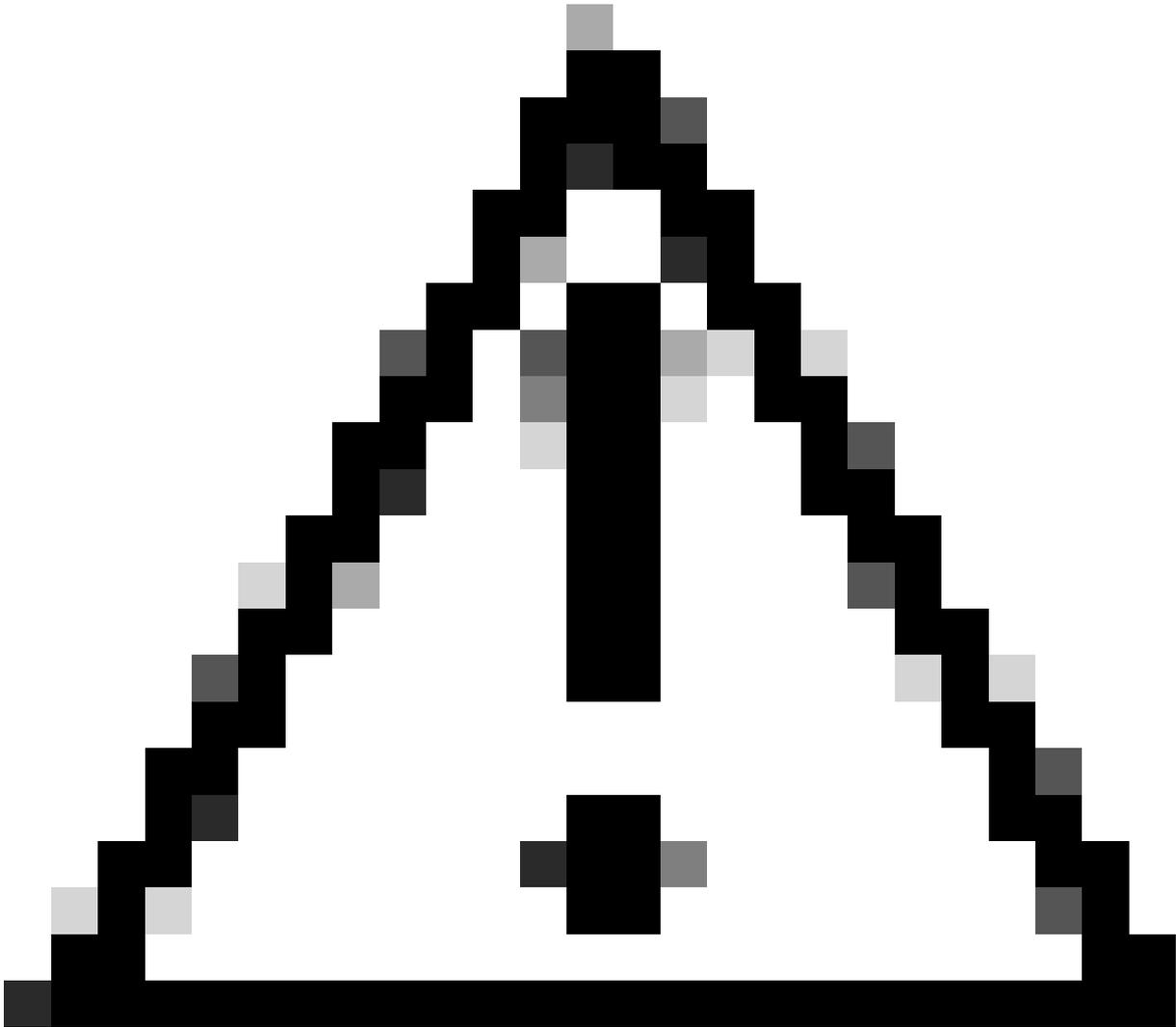
步骤 4 :

在此步骤中，我们将组与用户关联，将每个组与定义各自身份验证和隐私（加密）的用户关联，并可使用访问控制列表进行进一步保护。

```
!NoAuthNoPriv: noauth  
snmp-server user MyUser MyGroup v3 access snmp-poll-server
```

```
!AuthNoPriv: auth  
snmp-server user MyUser MyGroup v3 auth sha AuthPassword access snmp-poll-server
```

```
!AuthPriv: priv  
snmp-server user MyUser MyGroup v3 auth sha AuthPassword priv aes 128 PrivPassword access snmp-poll-server
```



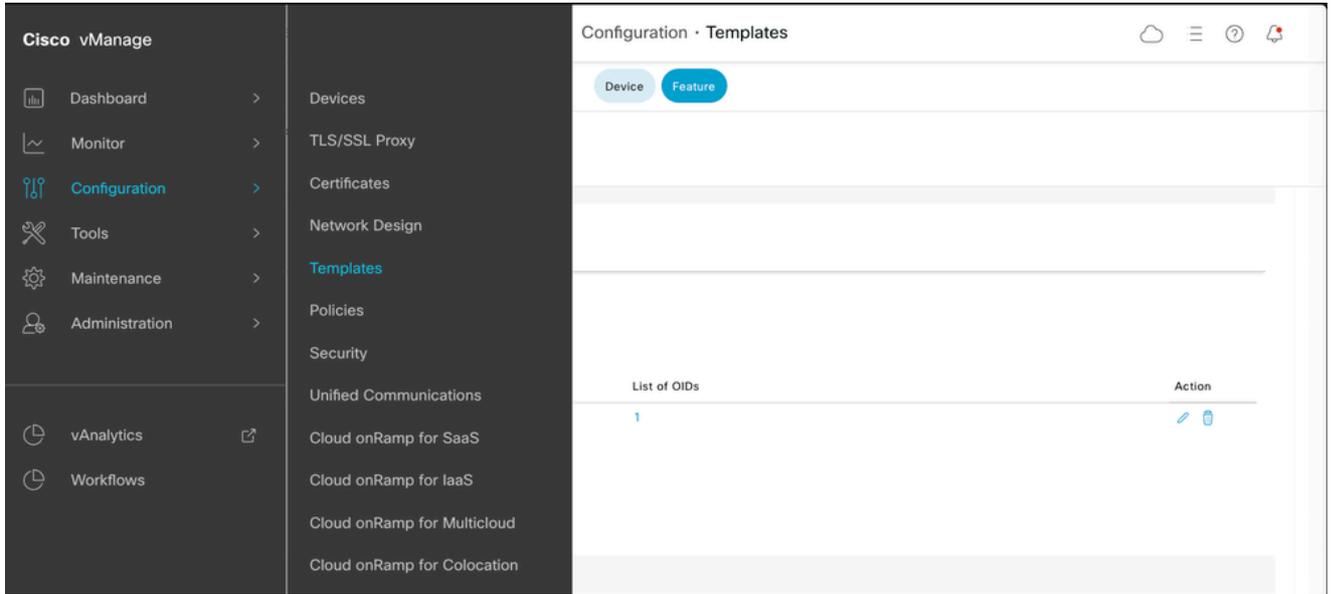
警告：在尝试配置`snmp-server user`时，您会发现上下文帮助不可用，并且未显示在运行配置中，这是为了符合RFC 3414。键入完整命令，解析器接受配置

```
cEdge-RT01(config)# snmp-server user ? ^ % Invalid input detected at '^' marker.
```

Cisco Bug ID [CSCvn71472](#)

祝贺您，您只需要这些。既然您已经了解了cli和概念，现在我们来了解如何在Catalyst SD-WAN Manager上使用SNMP功能模板进行配置

导航到Cisco vManage > Configuration > Templates > Feature



功能模板

导航至Cisco SNMP，可在其他模板部分找到

Select Devices

Q c8300

- C8300-1N1S-4T2X
- C8300-1N1S-6T
- C8300-2N2S-4T2X
- C8300-2N2S-6T

WAN

OTHER TEMPLATES

Cli Add-On Template
WAN

AppQoE

Cellular Controller
WAN

Cellular Profile
WAN

Cisco Banner

Cisco BGP
WAN LAN

Cisco DHCP Server
LAN

Cisco IGMP
LAN

Cisco Logging

Cisco Multicast

Cisco OSPF
WAN LAN

Cisco OSPFV3
WAN LAN

Cisco PIM
LAN

Cisco SIG Credentials

Cisco SNMP

EIGRP
LAN

GPS
WAN

Probes

SNMP功能

定义SNMP视图 (限制) , 这是我们的步骤2

Device Type C8300-1N1S-6T

Template Name

Description

SNMP SNMP Version

SNMP

Shutdown Yes No

Contact Person

Location of Device

SNMP VERSION

SNMP Version V2 V3

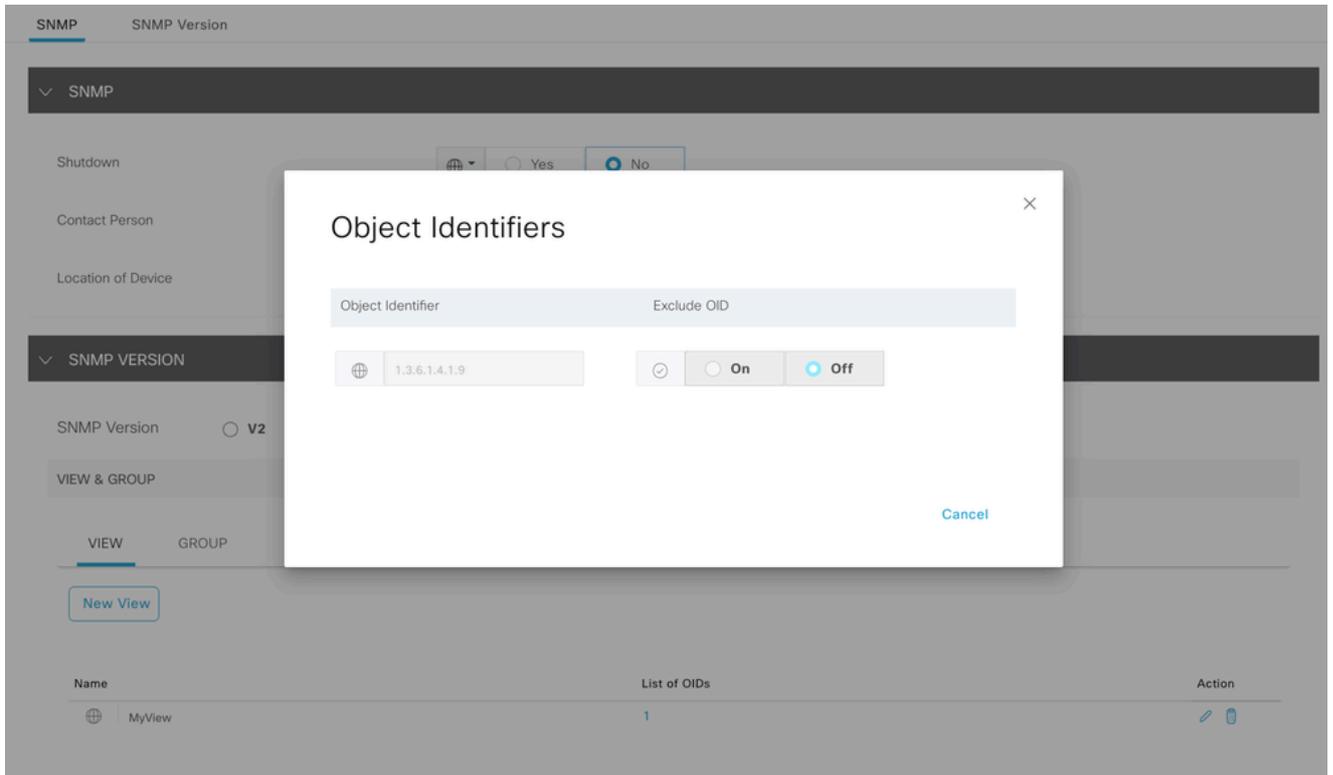
VIEW & GROUP

2 VIEW GROUP

[New View](#)

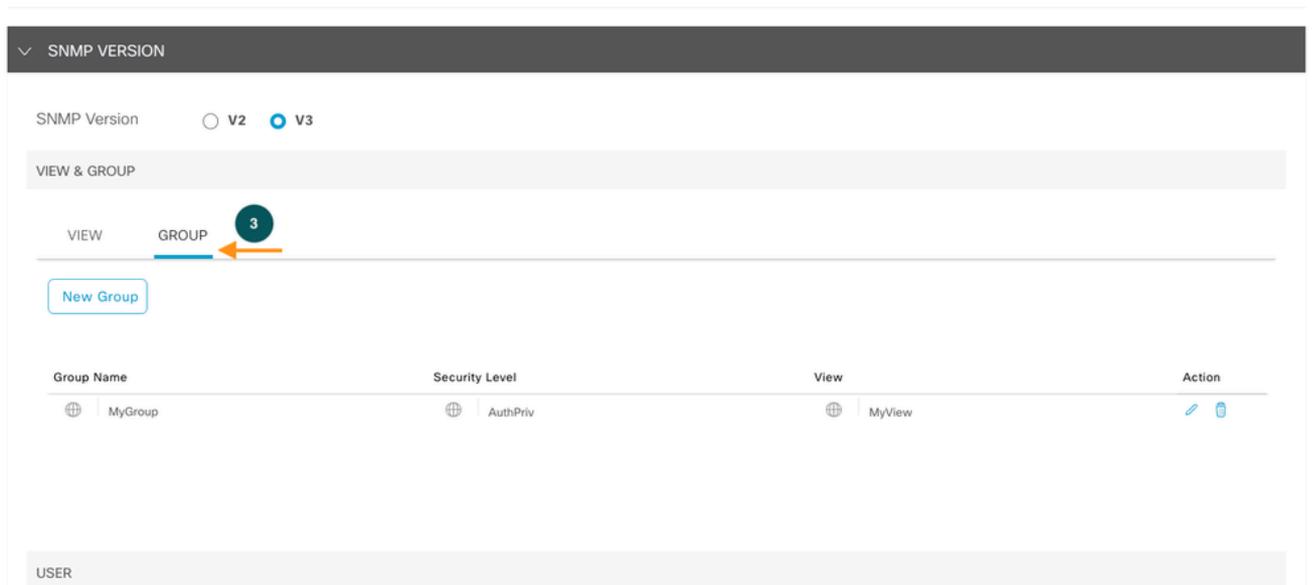
Name	List of OIDs	Action
<input type="checkbox"/> MyView	1	Edit Delete

SNMP 视图

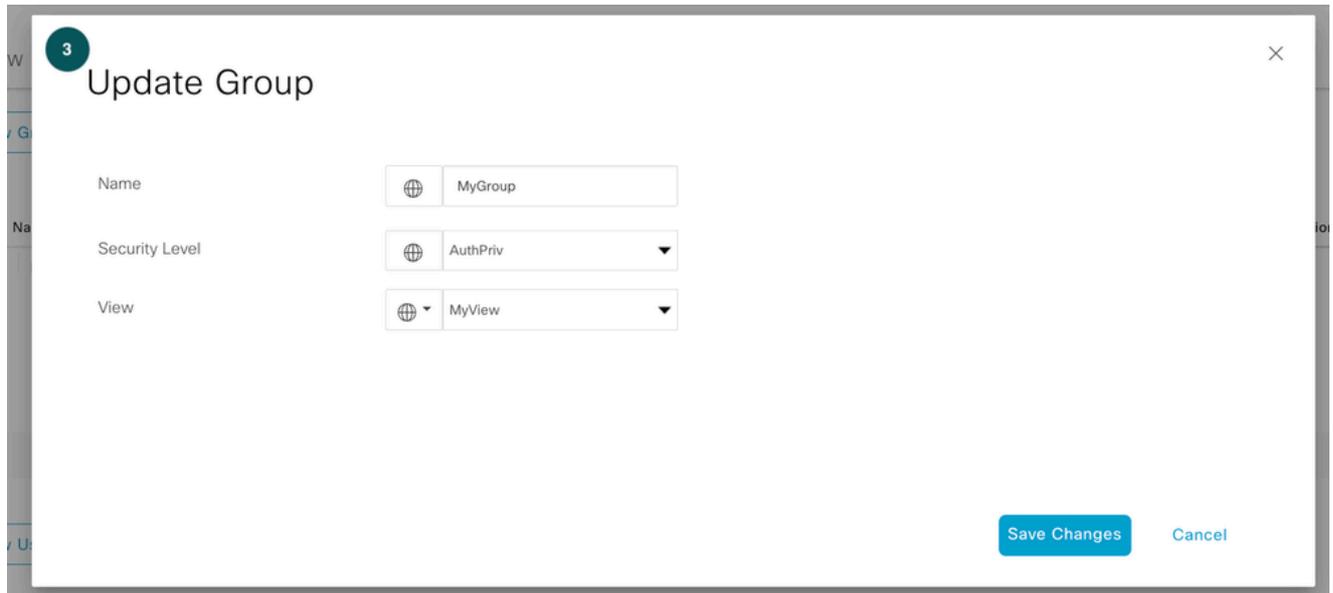


SNMP OID

定义SNMP组这是我们的步骤3

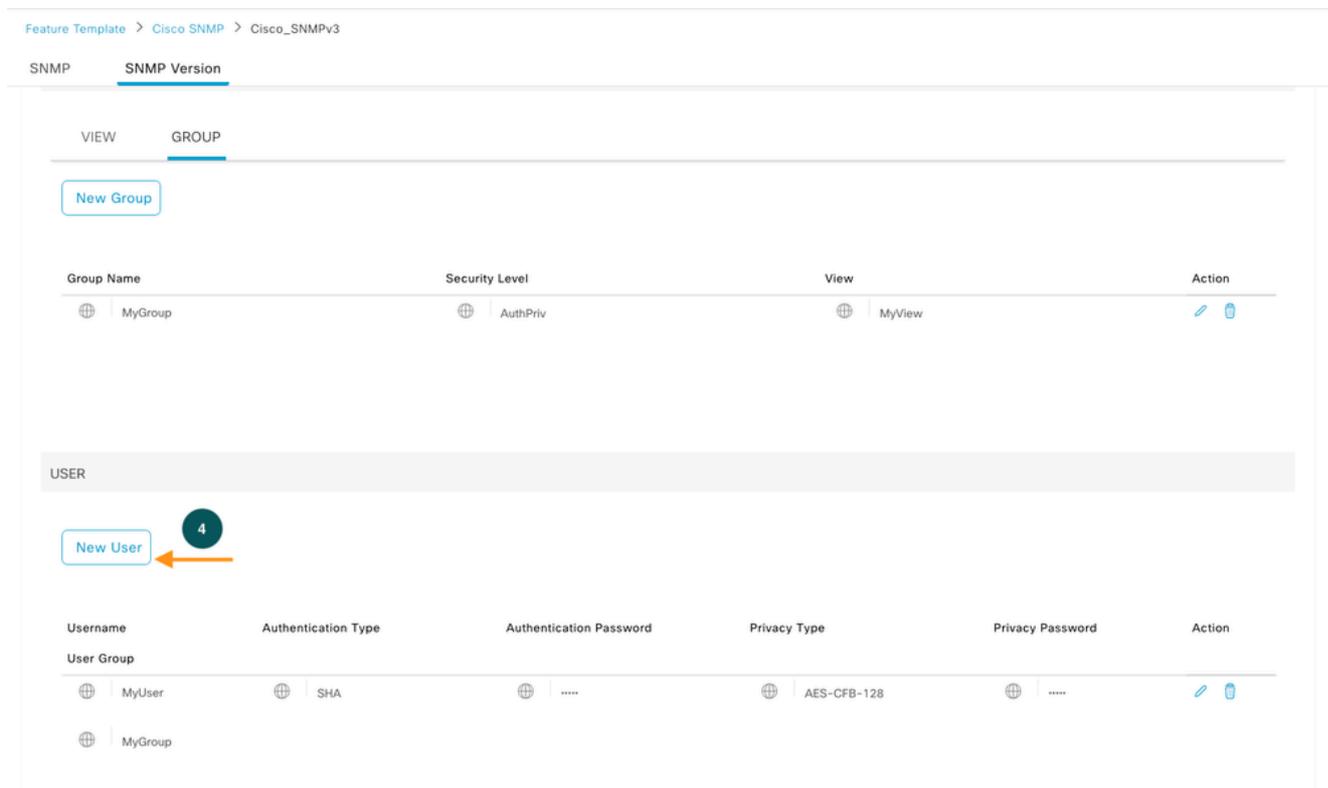


SNMP组



SNMP组

定义用户组，这是我们定义身份验证和加密密码的第4步。



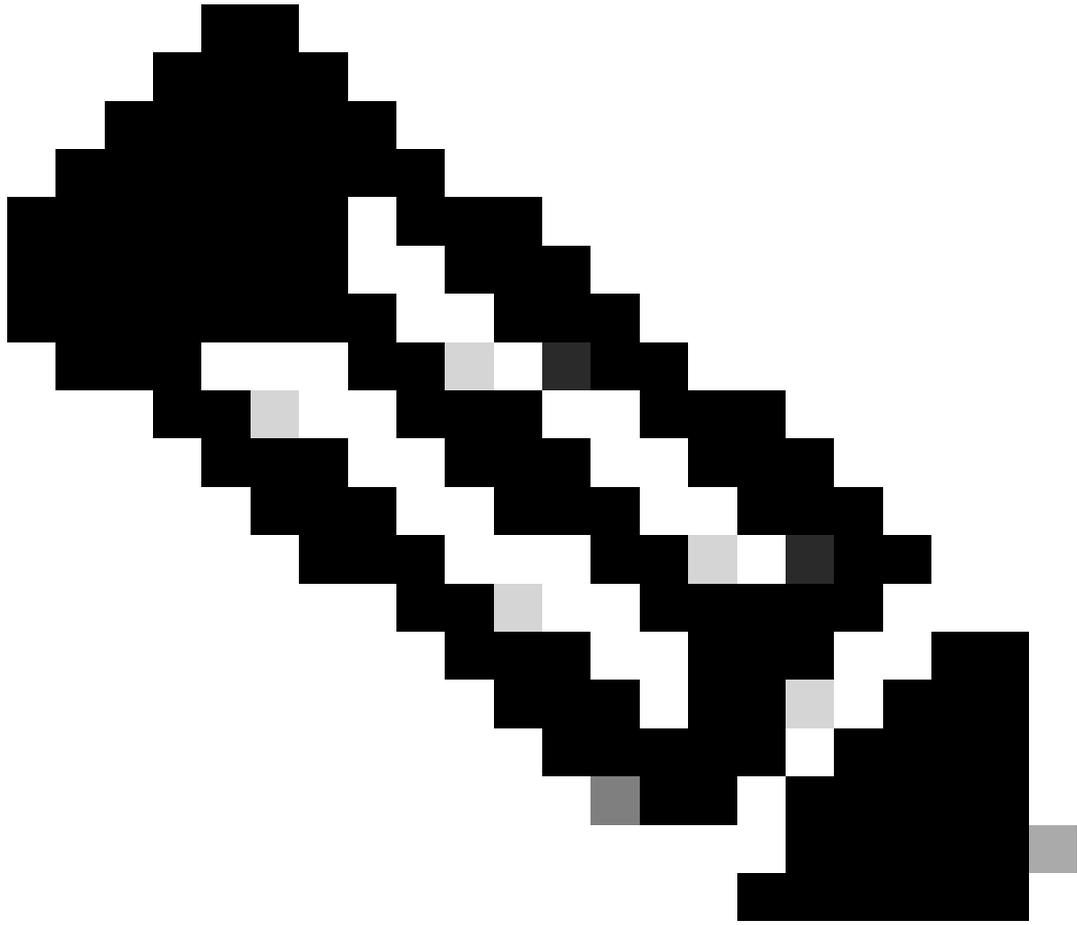
SNMP用户

4 Update User ×

User	<input type="text" value="MyUser"/>
Authentication Protocol	<input type="text" value="SHA"/>
Authentication Password	<input type="text" value="....."/>
Privacy Protocol	<input type="text" value="AES-CFB-128"/>
Privacy Password	<input type="text" value="....."/>
Group	<input type="text" value="MyGroup"/>

TARGET SERVER

SNMP用户加密



注意：根据SNMP组安全级别，与用户关联的相应字段将启用。

现在将功能模板附加到设备模板。

Additional Templates

AppQoS	Choose...
Global Template *	Factory_Default_Global_CISCO_Templ... ⓘ
Cisco Banner	Choose...
Cisco SNMP	Cisco_SNMPv3
ThousandEyes Agent	Choose...
TrustSec	Choose...
CLI Add-On Template	Choose...
Policy	Choose...
Probes	Choose...
Security Policy	Choose...

SNMP功能模板

验证

```
Router#show snmp user
```

```
User name: MyUser  
Engine ID: 800000090300B8A3772FF870  
storage-type: nonvolatile active access-list: snmp-poll-server  
Authentication Protocol: SHA  
Privacy Protocol: AES128  
Group-name: MyGroup
```

在安装了snmpwalk的计算机上，您可以运行命令以验证各安全级别的SNMP响应

```
!NoAuthNoPriv: noauth  
snmpwalk -v 3 -l noAuthNoPriv -u MyUser
```

.1

```
!AuthNoPriv: auth  
snmpwalk -v 3 -l authNoPriv -u MyUser -a SHA -A AuthPassword
```

.1

```
!AuthPriv: priv
```

```
snmpwalk -v 3 -l authPriv -u MyUser -a SHA -A AuthPassword -x AES -X PrivPassword
```

.1

-v:版本(3)

-l:安全级别

-A:身份验证协议口令

-X:隐私协议口令

参考

- [在思科边缘路由器上配置SNMPv3陷阱](#)
- Tim [Glen的SNMPv3配置模板](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。