Configurar SNMPv3 no Catalyst SD-WAN

Contents

Introdução

Este documento descreve a configuração do SNMPv3 e explica sobre segurança (autenticação), criptografia (privacidade) e restrição (exibição).

Background

Frequentemente, a configuração do SNMPv3 é considerada complexa e difícil de configurar, até sabermos o que precisa ser feito. O motivo para a existência do SNMPv3 é semelhante ao HTTPS: para segurança, criptografia e restrição.

Pré-requisitos

Conhecimento de modelos de recursos de SD-WAN e modelos de dispositivos.

Conhecimento geral sobre SNMP MIB, SNMP Poll e SNMP Walk

Requisitos

Controladores SD-WAN

Roteador Cisco Edge

Componentes Utilizados

Controladores SD-WAN em 20.9

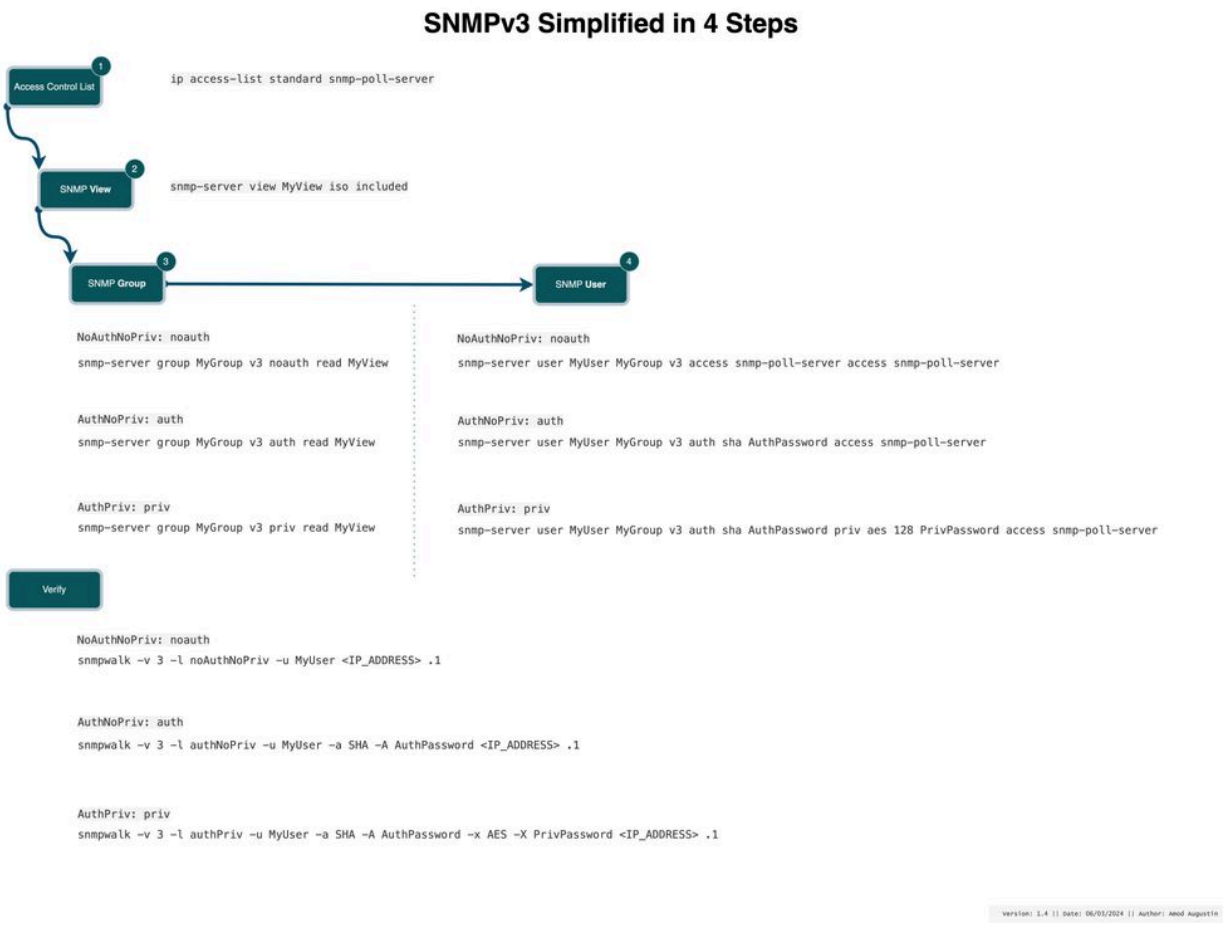
Cisco Edge Router em 17.9

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

O diagrama o ajuda a entender o que é necessário para configurar o SNMPv3 a partir de um ponto de vista da CLI.



- SNMPv3 simplificado em 4 etapas

Assim que você compreender, será fácil colocar o conceito na CLI ou em um modelo de recurso. Vamos mergulhar.

Passo 1:

Configure uma ACL para permitir quem pode pesquisar o sistema (roteador no nosso caso).

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

Passo 2:

Defina uma visualização snmp, pois o termo implica a quais mibs a pesquisa tem acesso. Essa é nossa restrição.

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

Passo 3:

Defina snmp group, snmp group tem principalmente duas partes a. Nível de segurança b. Restrição (exibir).

Níveis de segurança:

- noAuthNoPriv: Sem autenticação e sem privacidade (sem criptografia).
- authNoPriv: A autenticação é necessária, mas não a privacidade.
- authPriv: A autenticação e a privacidade são necessárias.

Restrição é o que definimos na Etapa 2, vamos reuni-los.

```
!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
```

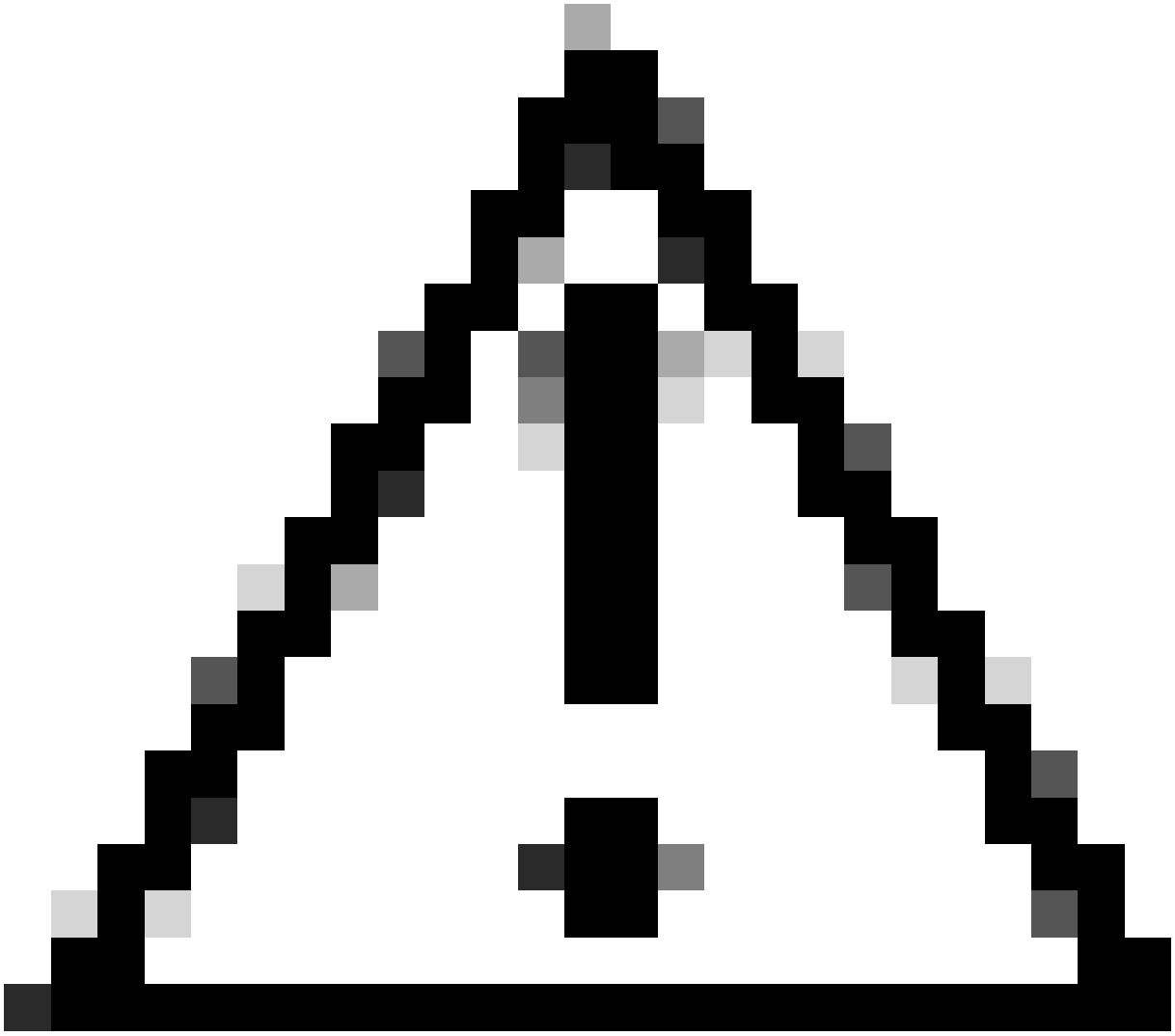
Passo 4:

Nesta etapa, associamos o grupo a um usuário, associamos cada grupo a usuários que definem a respectiva autenticação e privacidade (criptografia) e podemos ter mais segurança usando a lista de controle de acesso.

```
!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-ser
```



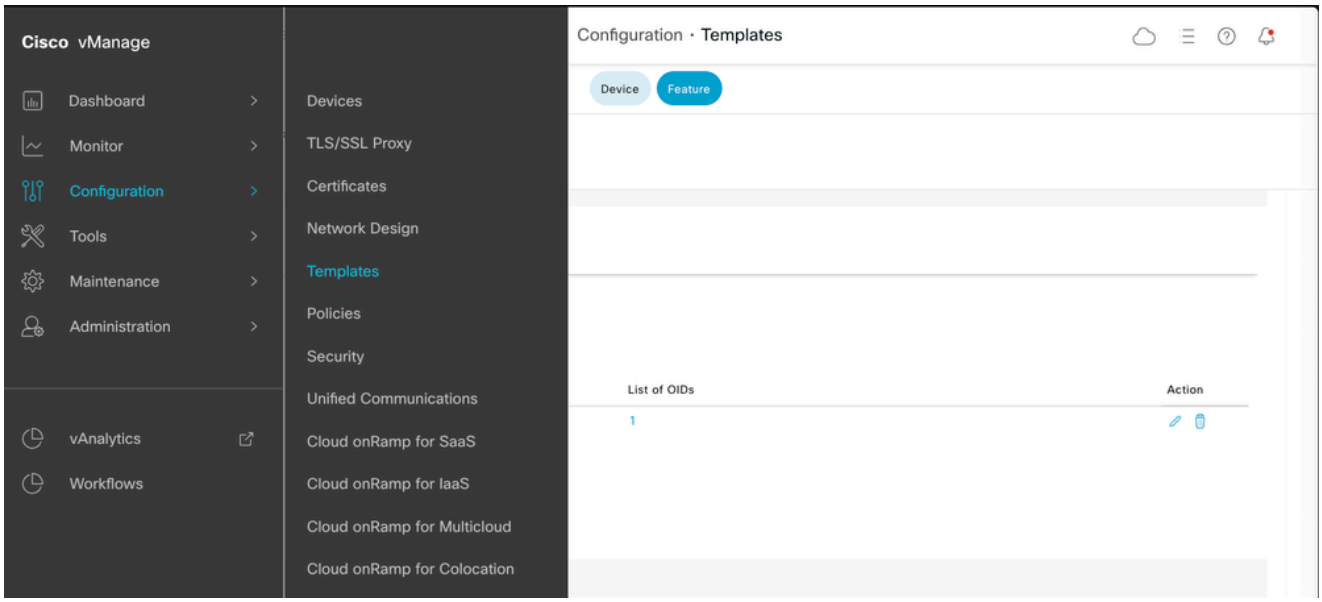
Caution: Você pode observar que, ao tentar configurar snmp-server user, a ajuda de contexto não está disponível e também não é mostrada na configuração de execução; isso é compatível com o RFC 3414. Digite o comando completo e o analisador aceitará a configuração

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

ID de bug da Cisco CSCvn71472

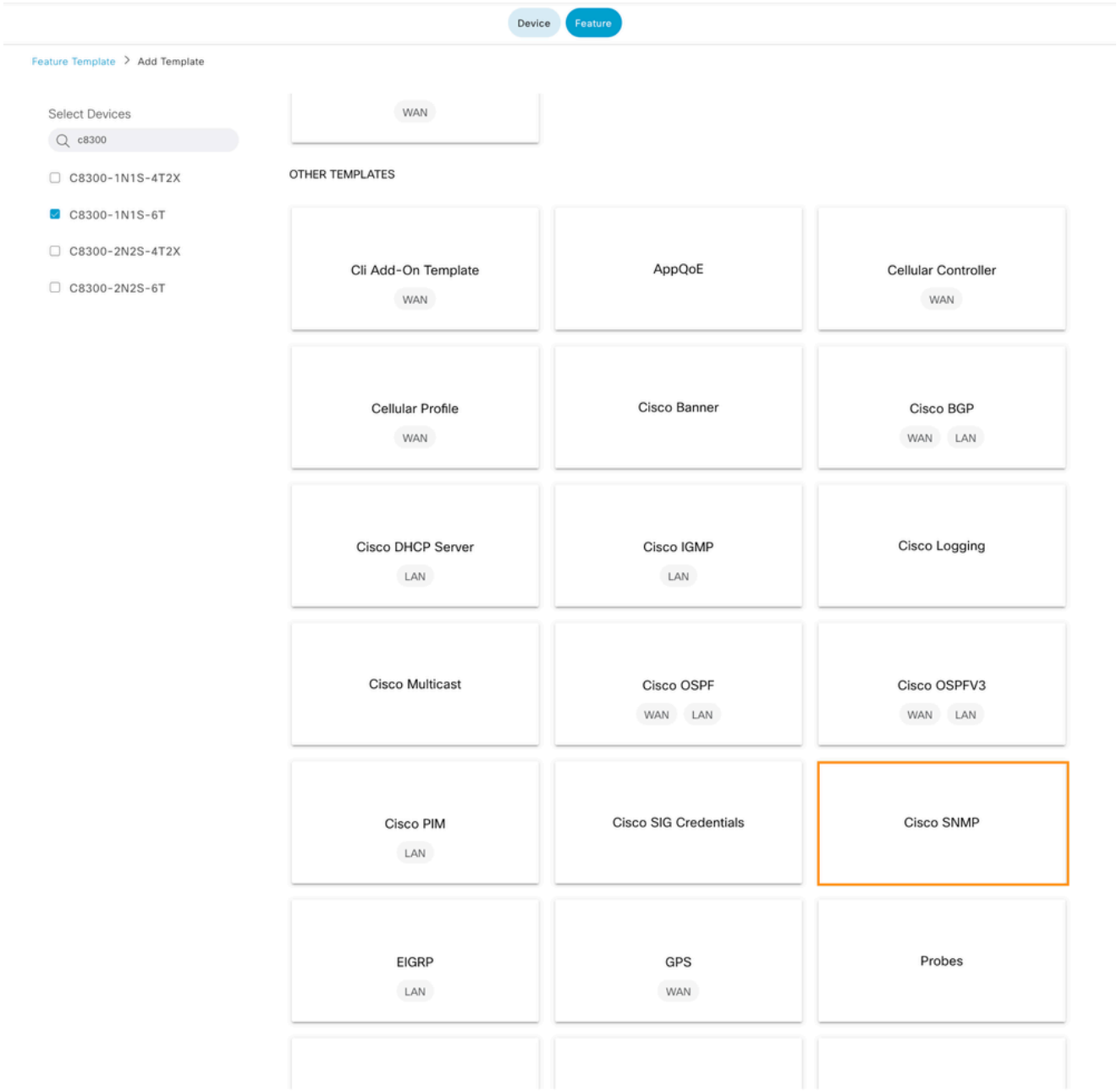
Parabéns, é tudo o que é necessário. Agora que você conhece a cli e o conceito permite ver como configurar usando o modelo de recurso SNMP em um Catalyst SD-WAN Manager

Navegue até Cisco vManage > Configuration > Templates > Feature

- 

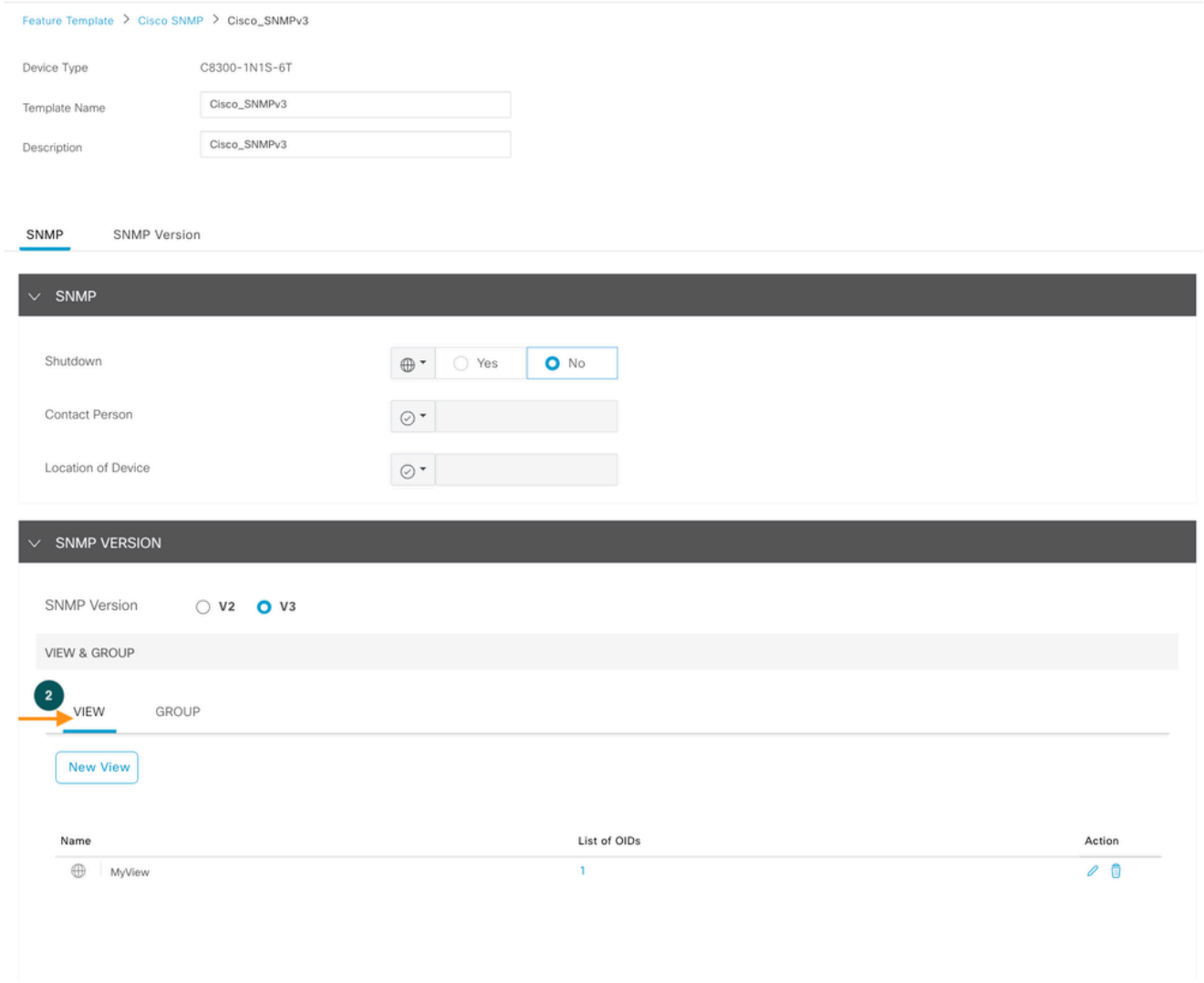
  Modelo de recurso

Navegue até o Cisco SNMP, que pode ser encontrado na seção Outro modelo

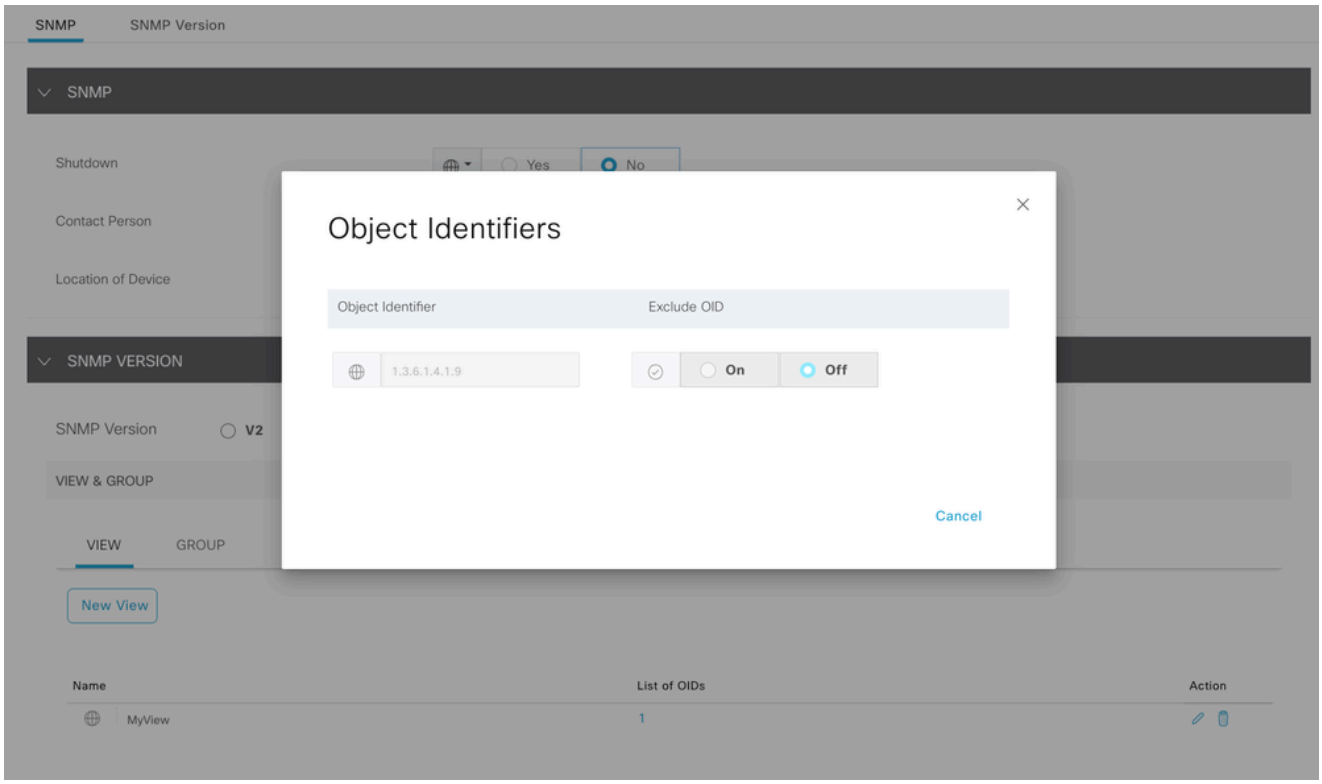


- Recurso SNMP

Definir SNMP View (restrição); esta é a nossa Etapa 2

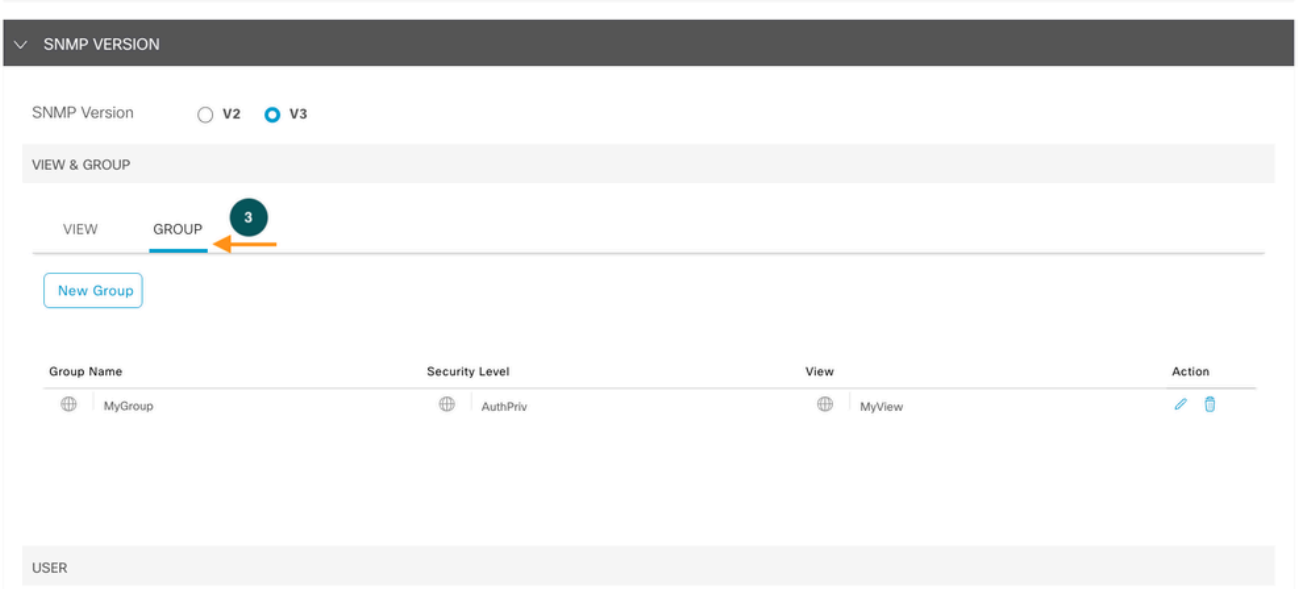


- Visualização de SNMP



- OID SNMP

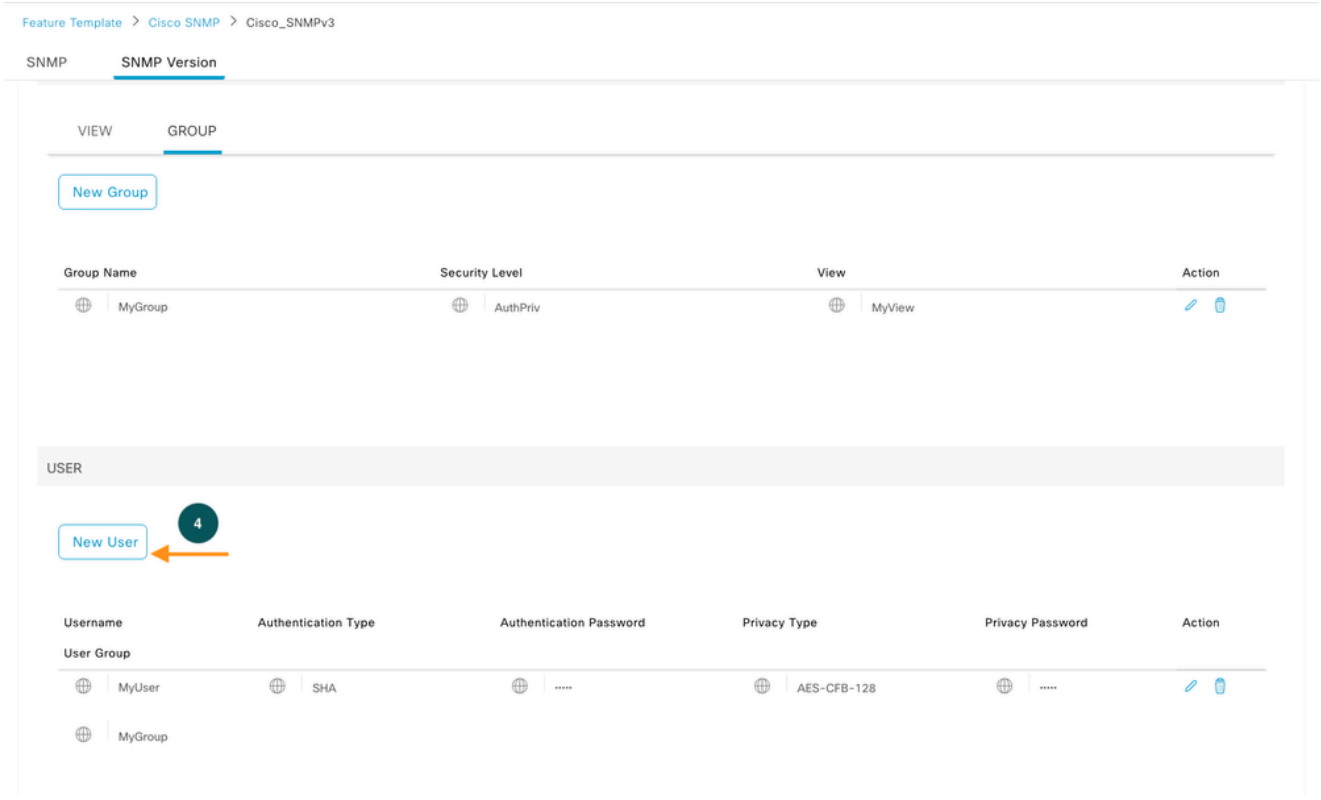
Defina o grupo SNMP Esta é a nossa Etapa 3



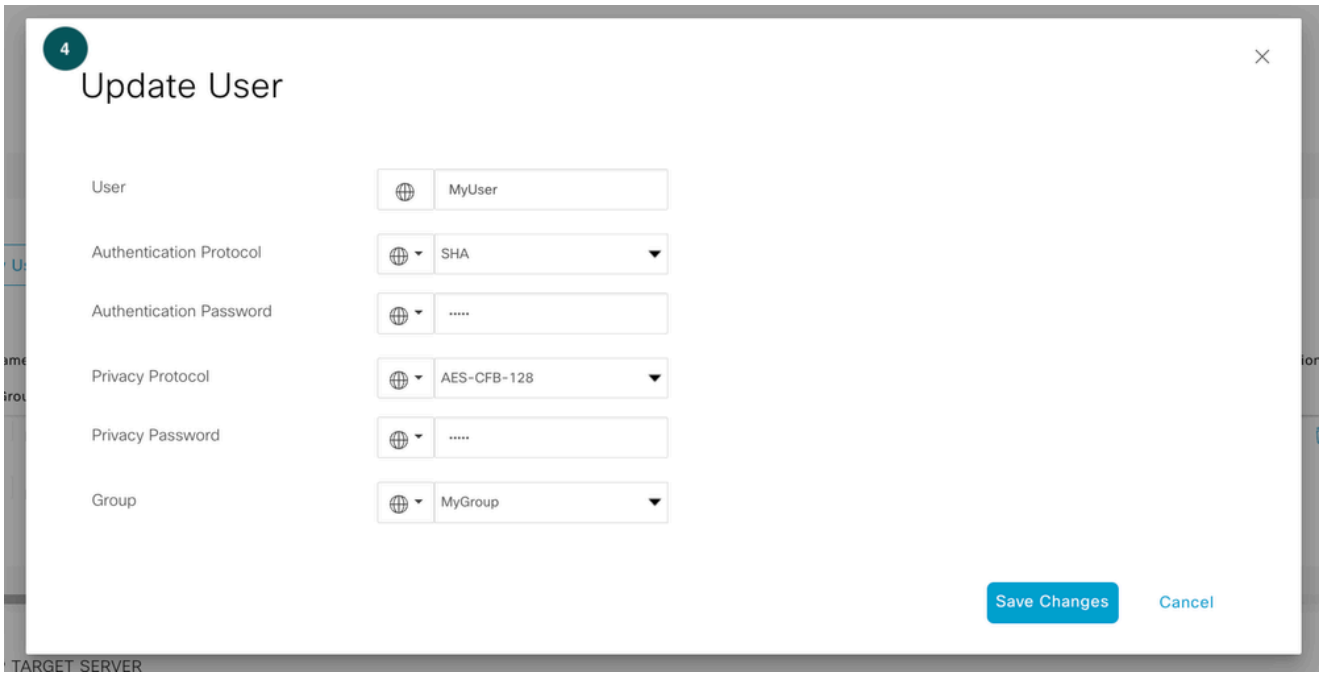
- Grupo SNMP

Grupo SNMP

Defina o grupo de usuários. Esta é nossa Etapa 4, na qual definimos a senha de autenticação e criptografia.

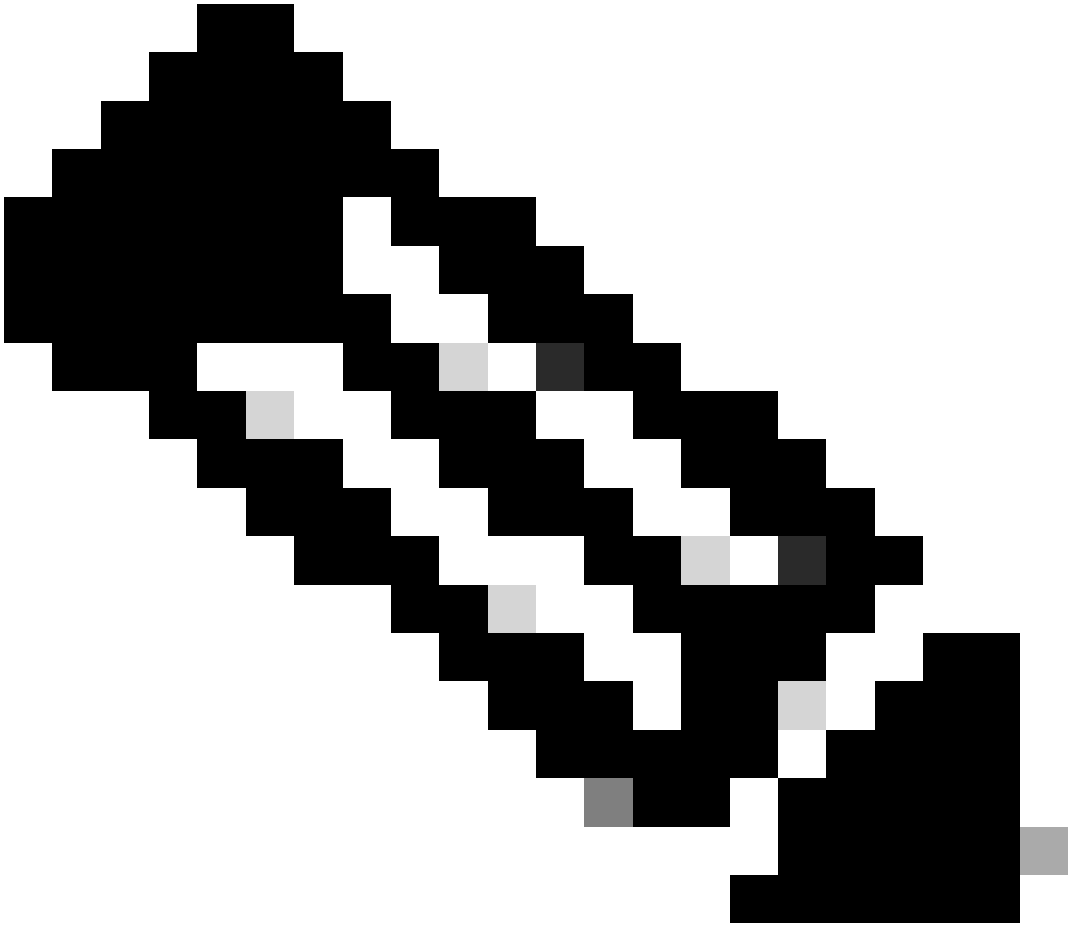


Usuário SNMP



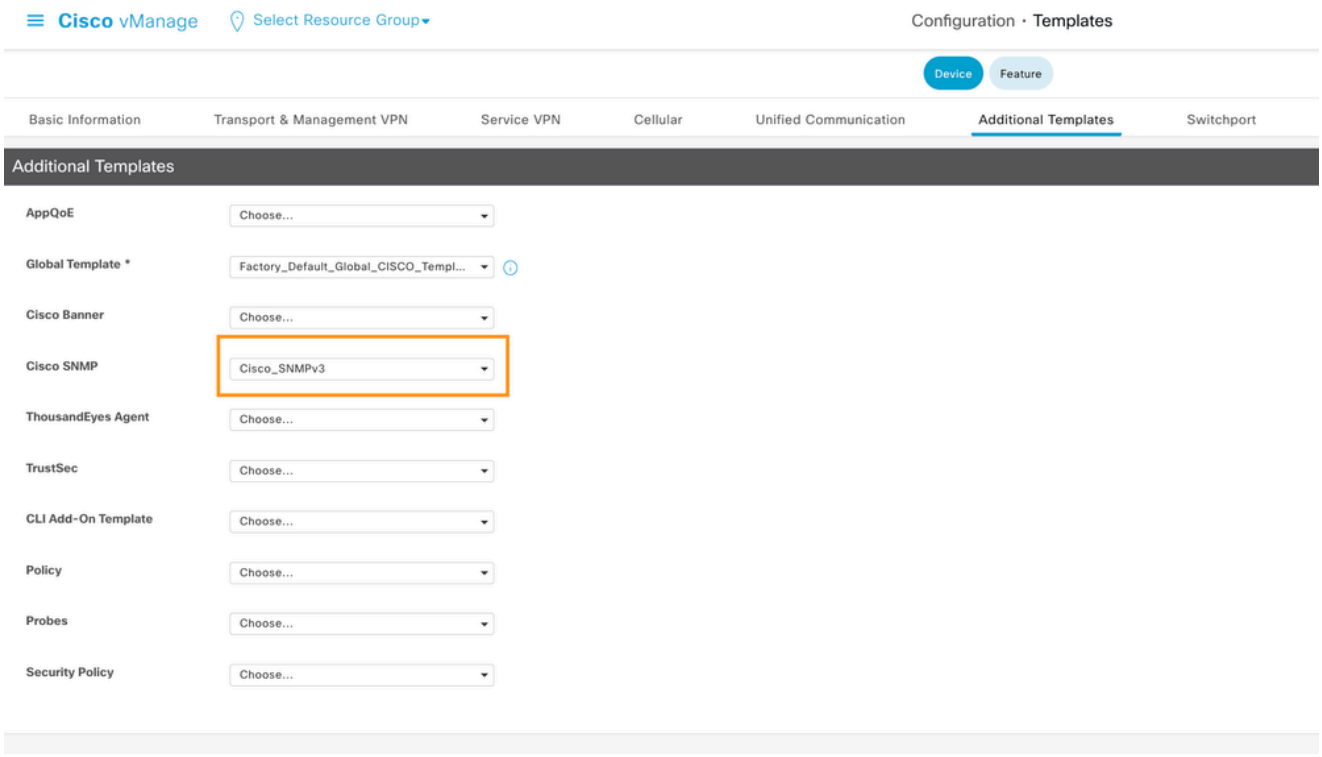
- TARGET SERVER

Criptografia de usuário SNMP



Note: Com base no nível de segurança do Grupo SNMP, o respectivo campo associado ao usuário é habilitado.

Agora, anexe o modelo de recurso ao modelo de dispositivo.



-

Modelo de recurso SNMP

Verificar

```
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
```

Em uma máquina que tenha o snmpwalk instalado, você pode executar o comando para verificar a resposta do SNMP para o respectivo nível de segurança

```
!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: Versão (3)

-l: Nível de segurança

-A: Frase secreta do protocolo de autenticação

-X: Senha do protocolo de privacidade

Referências

- Configurar interceptação SNMPv3 no Cisco Edge Router
- Modelo de configuração para SNMPv3 por Tim Glen

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.