Configurar SNMPv3 nos dispositivos Cisco ONS15454/NCS2000

Contents

Introduction

Este documento descreve instruções passo a passo sobre como configurar o SNMP versão 3 (Simple Network Management Protocol versão 3) em dispositivos ONS15454/NCS2000. Todos os tópicos incluem exemplos.

> **Note**: A lista de atributos fornecida neste documento não é exaustiva ou autoritativa e pode ser alterada a qualquer momento sem uma atualização deste documento.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- GUI do Cisco Transport Controller (CTC)
- Conhecimento básico do servidor
- Comandos básicos do Linux/Unix

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Em um nó autônomo/de vários prateleiras

Configurar o modo authPriv no dispositivo ONS15454/NCS2000

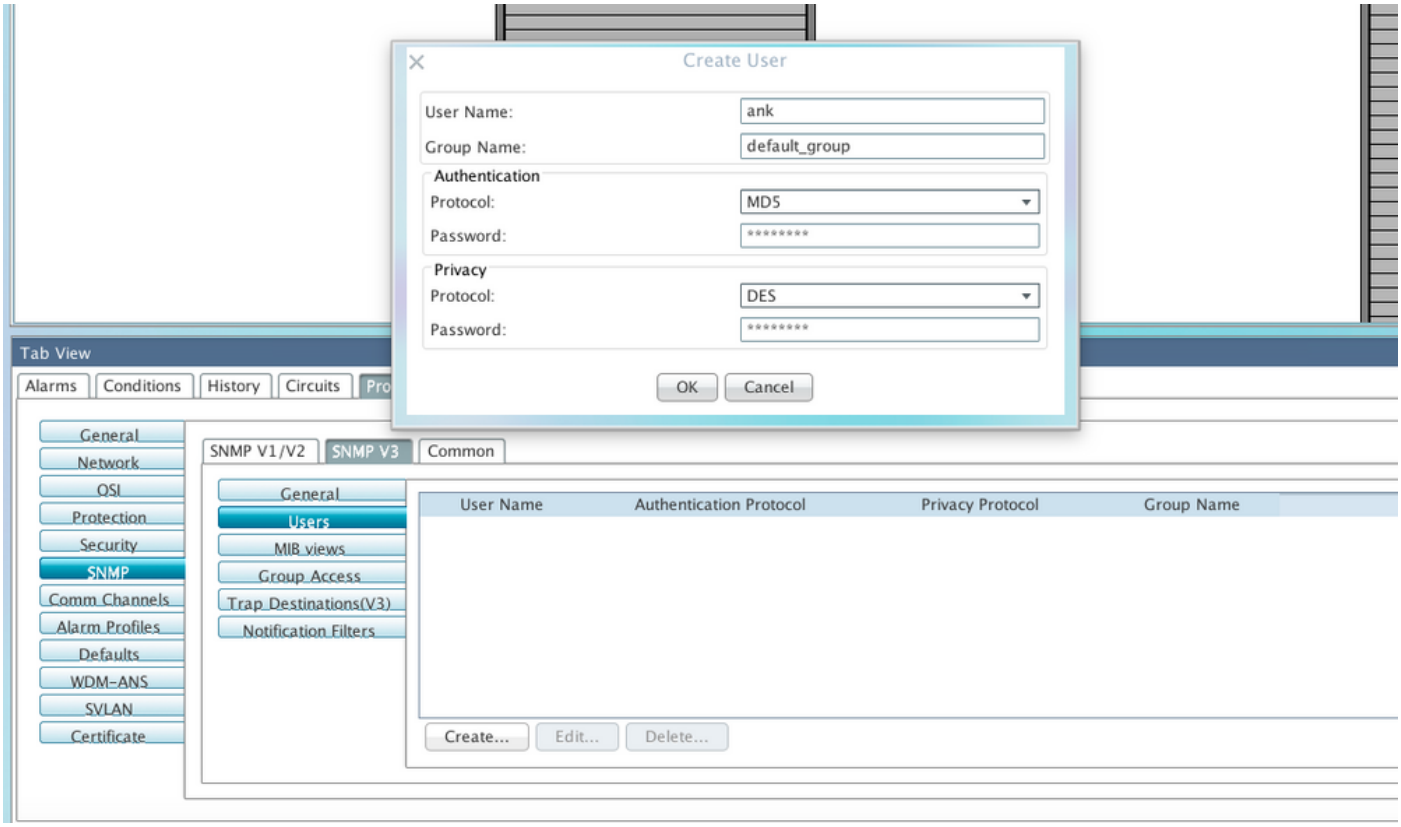
Etapa 1. Faça login no nó via CTC com o uso das credenciais de superusuário.

Etapa 2. Navegue até **Node view > Provisioning > SNMP > SNMP V3**.

Etapa 3. Navegue até a guia **Usuários**. Criar usuários.

```
User Name:<anything based on specifications>

Group name:default_group

Authentication

      Protocol:MD5

      Password:<anything based on specifications>

   Privacy

         Protocol:DES

         Password:<anythingbased on specifications>
```

Etapa 4. Clique em **OK** conforme mostrado na imagem.



Especificações:

Nome de usuário - Especifique o nome do usuário no host que se conecta ao agente. O nome de usuário deve ter no mínimo 6 e no máximo 40 caracteres (até 39 caracteres para a autenticação TACACS e RADIUS). Inclui caracteres alfanuméricos (a-z, A-Z, 0-9) e os caracteres especiais permitidos são @, "-" (hífen) e "." (ponto). Para compatibilidade TL1, o nome de usuário deve ter de 6 a 10 caracteres.

Nome do grupo - Especifique o grupo ao qual o usuário pertence.

Autenticação:

Protocolo - Selecione o algoritmo de autenticação que deseja usar. As opções são NONE, MD5 e SHA.

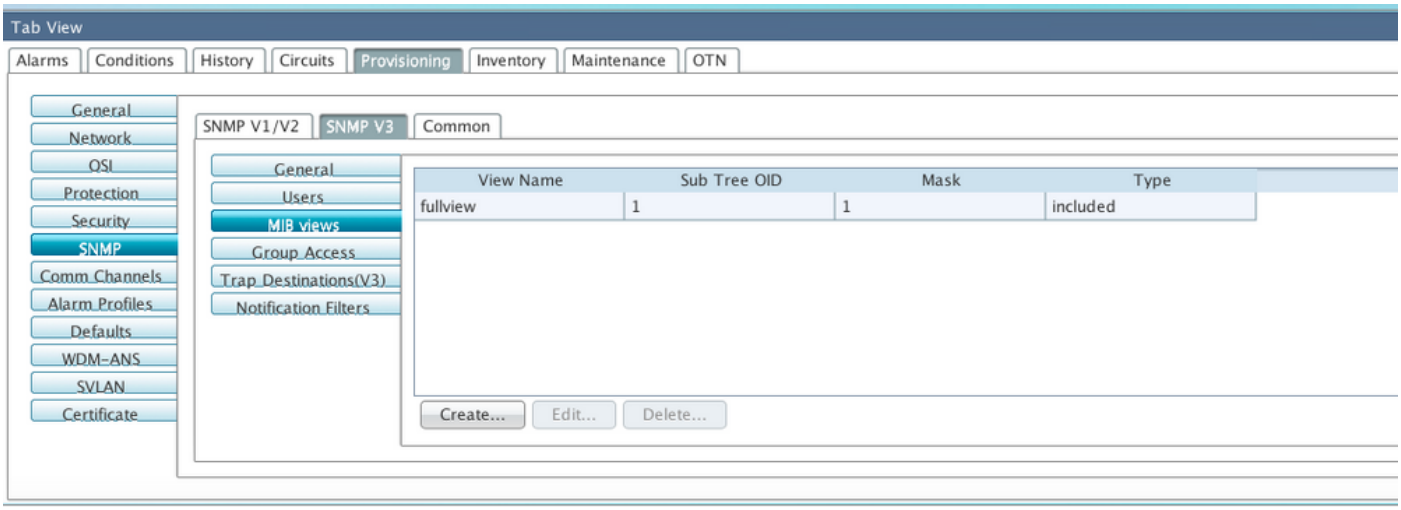
Password (Senha) - Insira uma senha se você selecionar MD5 ou SHA. Por padrão, o comprimento da senha é definido para um mínimo de oito caracteres.

Privacidade - Inicia uma sessão de configuração de nível de autenticação de privacidade que permite ao host criptografar o conteúdo da mensagem enviada ao agente.

Protocolo - Selecione o algoritmo de autenticação de privacidade. As opções disponíveis são None, DES e AES-256-CFB.

Password - (Senha) Insira uma senha se você selecionar um protocolo diferente de None (Nenhum).

Etapa 5. Certifique-se de que as visualizações de MIB estejam configuradas de acordo com esta imagem.



Especificações:

Nome - nome da exibição.

OID da subárvore - A subárvore MIB que, quando combinada com a máscara, define a família das subárvores.

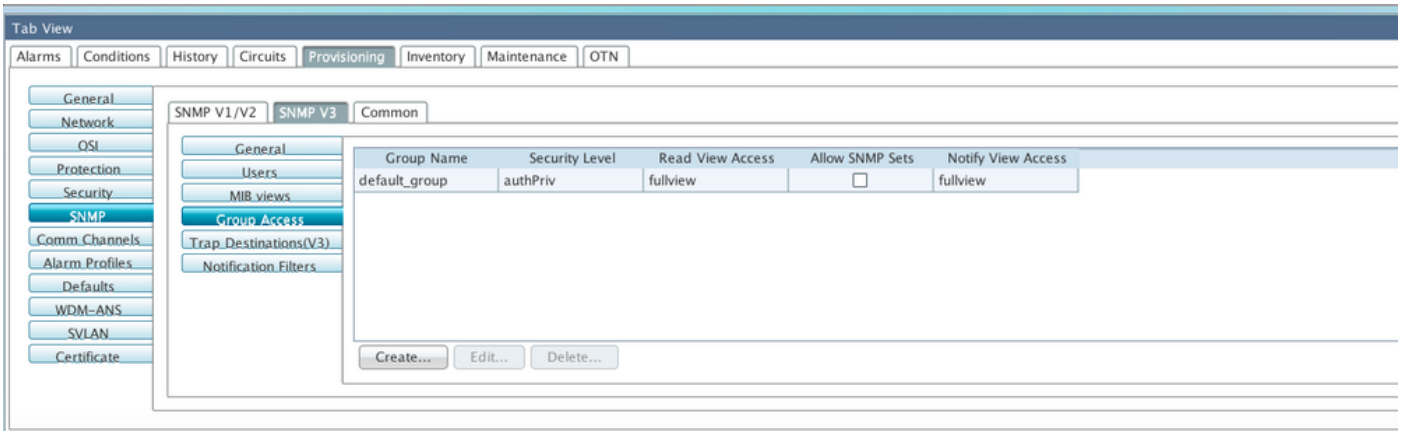
Máscara de Bit - Uma família de subárvores visuais. Cada bit na Máscara de Bit corresponde a um subidentificador do OID da subárvore.

Tipo - Selecione o tipo de exibição. As opções estão Incluídas e Excluídas.

O tipo define se a família de subárvores definidas pela combinação de OID de subárvore e Máscara de Bit está incluída ou excluída do filtro de notificação.

Etapa 6. Configure o acesso de grupo como mostrado na imagem. Por padrão, o nome do grupo será default_group e o nível de segurança como authPriv.

Note: O nome do grupo deve ser o mesmo usado ao criar o usuário na Etapa 3.



Especificações:

Nome do grupo - O nome do grupo SNMP, ou coleção de usuários, que compartilham uma política de acesso comum.

Nível de segurança - O nível de segurança para o qual os parâmetros de acesso são definidos. Selecione uma destas opções:

noAuthNoPriv - Usa uma correspondência de nome de usuário para autenticação.

AuthNoPriv - Fornece autenticação com base nos algoritmos HMAC-MD5 ou HMAC-SHA.

AuthPriv - Fornece autenticação com base nos algoritmos HMAC-MD5 ou HMAC-SHA. Fornece criptografia DES de 56 bits baseada no padrão CBC-DES (DES-56), além da autenticação.

Se você selecionar authNoPriv ou authPriv para um grupo, o usuário correspondente deverá ser configurado com um protocolo de autenticação e uma senha, com protocolo de privacidade e senha, ou ambos.

Exibições

Read View Name - Ler o nome da exibição do grupo.

Notifique o nome de exibição - Notifique o nome de exibição do grupo.

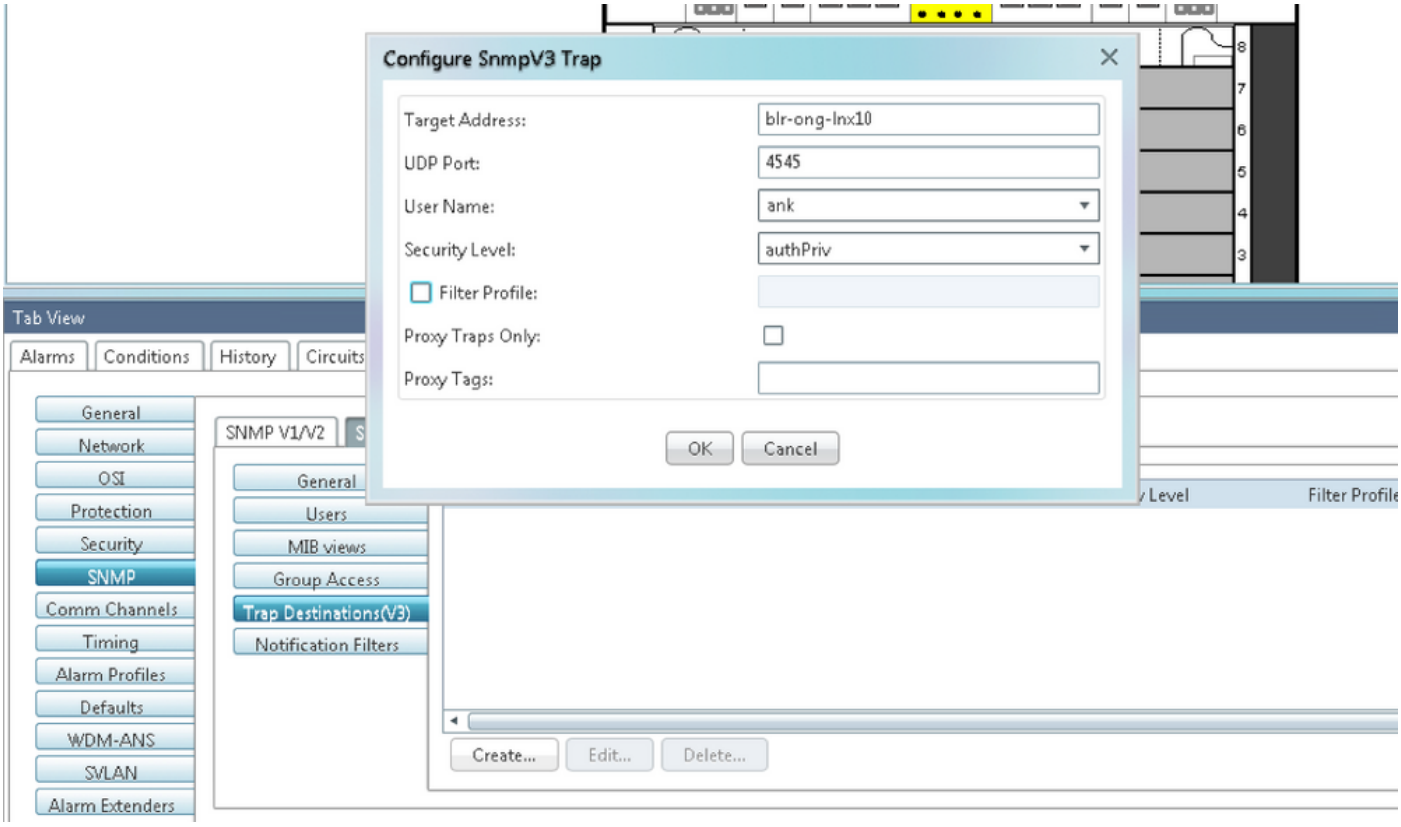
Permitir conjuntos de SNMP - Marque essa caixa de seleção se desejar que o agente SNMP aceite solicitações SNMP SET. Se esta caixa de seleção não estiver selecionada, as solicitações SET serão rejeitadas.

Note: O acesso à solicitação SNMP SET é implementado para muito poucos objetos.

Passo 7. Navegue até **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Clique em **Criar** e **Configurar**.

```
Target address:<any build server> (eg: blr-ong-lnx10)

UDP port: <anything between 1024 to 65535>

User name:<same as we created in step 3>

Security Level:AuthPriv
```

Etapa 8. Clique em **OK** conforme mostrado na imagem.



Nota: blr-ong-lnx10 é o servidor NMS.

Especificações:

Endereço de destino - Destino para o qual as interceptações devem ser enviadas. Use um endereço IPv4 ou IPv6.

Porta UDP - número da porta UDP que o host usa. O valor padrão é 162.

Nome de usuário - Especifique o nome do usuário no host que se conecta ao agente.

Nível de segurança - Selecione uma destas opções:

noAuthNoPriv - Usa uma correspondência de nome de usuário para autenticação.

AuthNoPriv - Fornece autenticação com base nos algoritmos HMAC-MD5 ou HMAC-SHA.

AuthPriv - Fornece autenticação com base nos algoritmos HMAC-MD5 ou HMAC-SHA. Fornece criptografia DES de 56 bits baseada no padrão CBC-DES (DES-56), além da autenticação.

Filtrar perfil - Marque essa caixa de seleção e digite o nome do perfil do filtro. As interceptações serão enviadas somente se você fornecer um nome de perfil de filtro e criar um filtro de notificação.

Somente interceptações de proxy - Se selecionado, encaminha somente interceptações de proxy do ENE. As interceptações desse nó não são enviadas ao destino de interceptação identificado por essa entrada.

Marcas de proxy - Especifique uma lista de marcas. A lista de marcas é necessária em um GNE somente se um ENE precisar enviar armadilhas para o destino de interceptação identificado por essa entrada e desejar usar o GNE como proxy.

Configurar o servidor NMS (blr-ong-lnx10)

Etapa 1. No diretório inicial do servidor, crie um diretório com o nome **snmp**.

Etapa 2. Neste diretório, crie um arquivo **snmptrapd.conf**.

Etapa 3. Altere o arquivo **snmptrapd.conf** para:

```
vi snmptrapd.conf

createUser -e 0xEngine ID <user_name>< MD5> <password > DES <password>
```

Por exemplo:

```
createUser -e 0x0000059B1B00F0005523A71C ank MD5 cisco123 DES cisco123
```

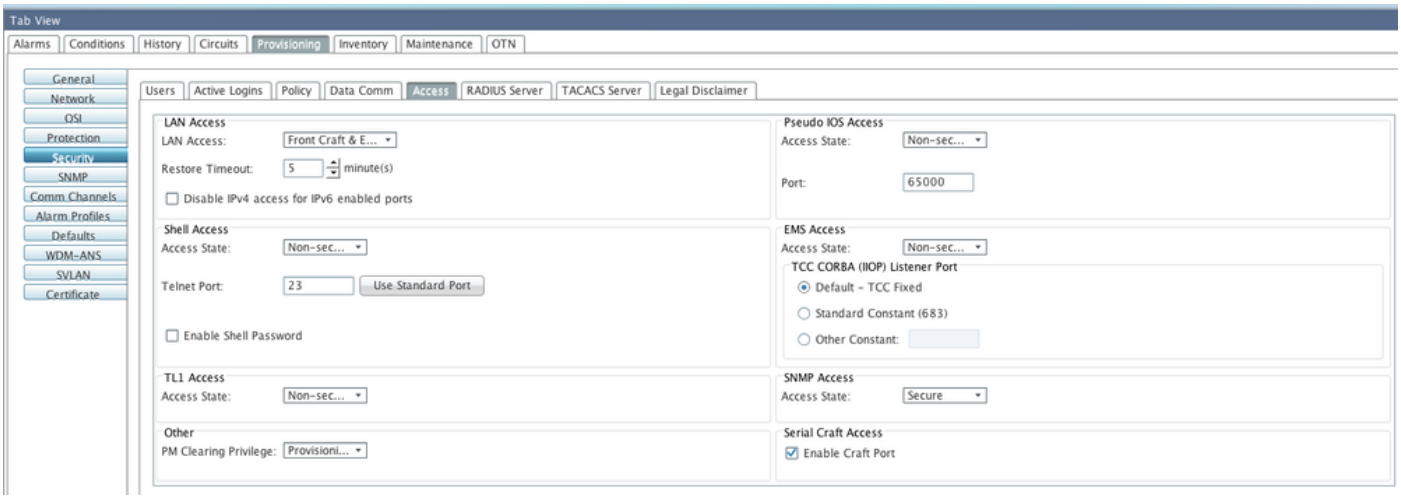
Neste exemplo:

```
user_name=ank

MD5 password = cisco123

DES password  = cisco123

Engine ID = can be available from CTC.
```

`Node view > Provisioning > SNMP > SNMP V3 > General`

Verificar o modo authPriv

Etapa 1. No CTC, navegue até **Node View > Provisioning > Security > Access > change snmp access state to Secure** como mostrado na imagem.



Etapa 2. Navegue até o servidor NMS e faça snmpwalk.

Sintaxe:

```
snmpwalk -v 3 -l authpriv -u <user name> -a MD5 -A <password> -x DES -X <password> <node IP>
<MIB>
```

Exemplo:

```
blr-ong-lnx10:151> snmpwalk -v 3 -l authpriv -u ank -a MD5 -A cisco123 -x DES -X cisco123
10.64.106.40 system

RFC1213-MIB::sysDescr.0 = STRING: "Cisco ONS 15454 M6 10.50-015E-05.18-SPA Factory Defaults
PLATFORM=15454-M6"

RFC1213-MIB::sysObjectID.0 = OID: CERENT-GLOBAL-REGISTRY::cerent454M6Node

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (214312) 0:35:43.12

RFC1213-MIB::sysContact.0 = ""

RFC1213-MIB::sysName.0 = STRING: "Ankit_40"

RFC1213-MIB::sysLocation.0 = ""

RFC1213-MIB::sysServices.0 = INTEGER: 79
```

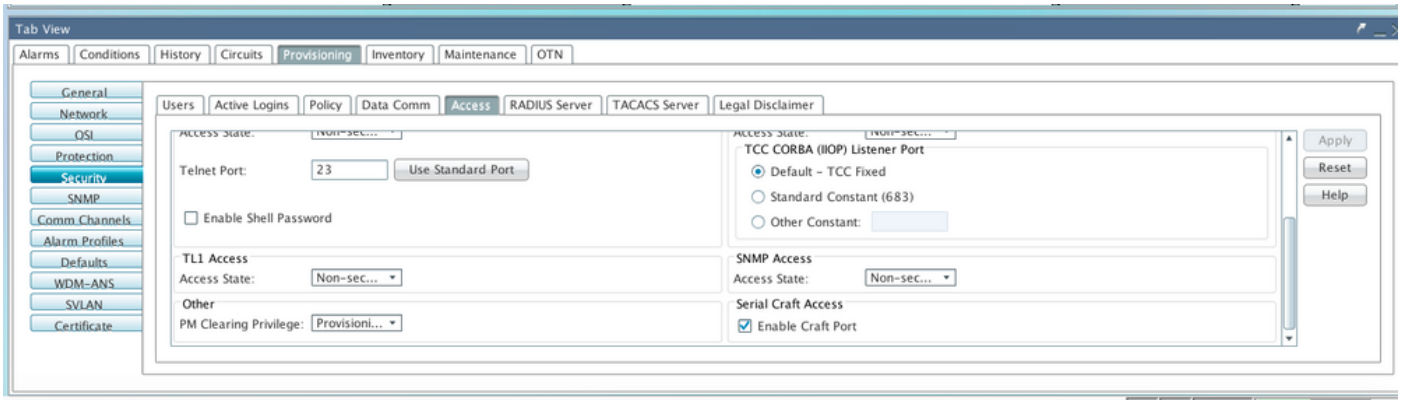
Interceptação SNMP:

```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

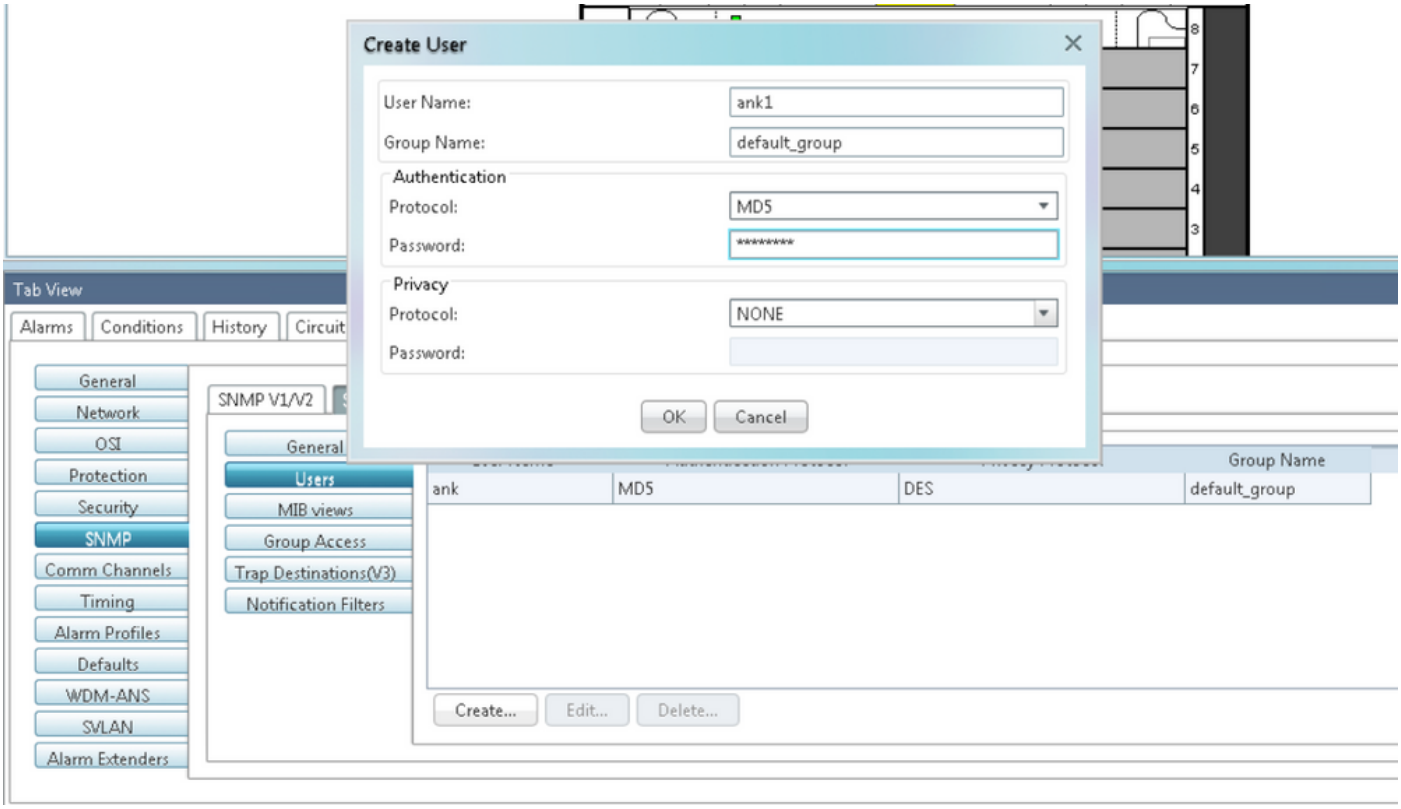
O comando Trap cmd é o mesmo para todas as versões.

Configurar o modo authNoPriv no dispositivo ONS15454/NCS2000

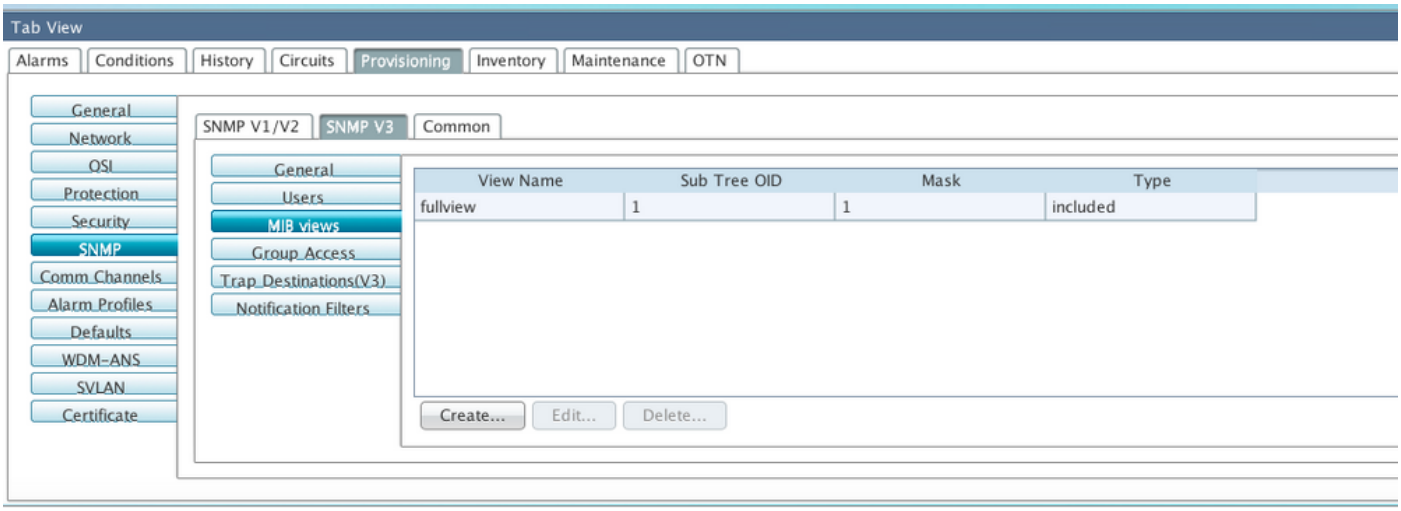
Etapa 1. No CTC, navegue para **Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode, como** mostrado na imagem.



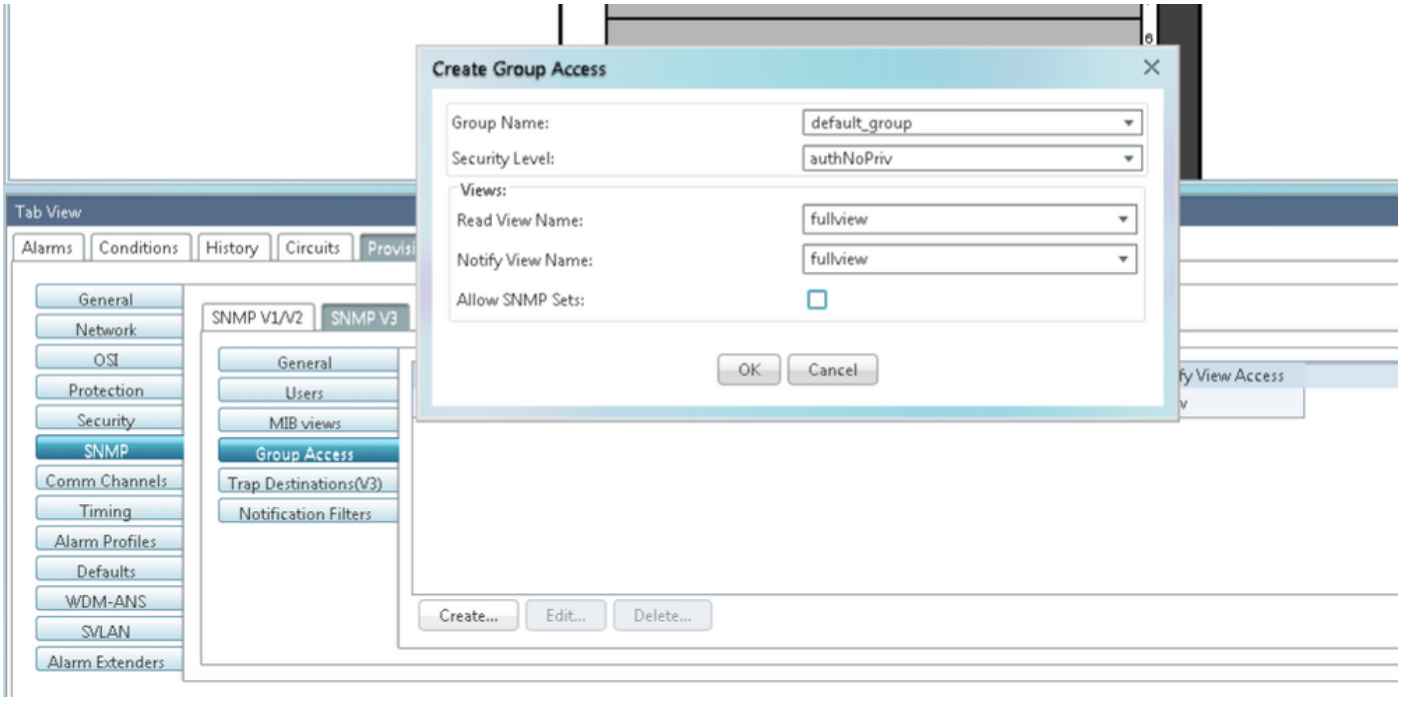
Etapa 2. Navegue até **Node View > Provisioning > SNMP > SNMP V3 > Users > Create User** e configure como mostrado na imagem.



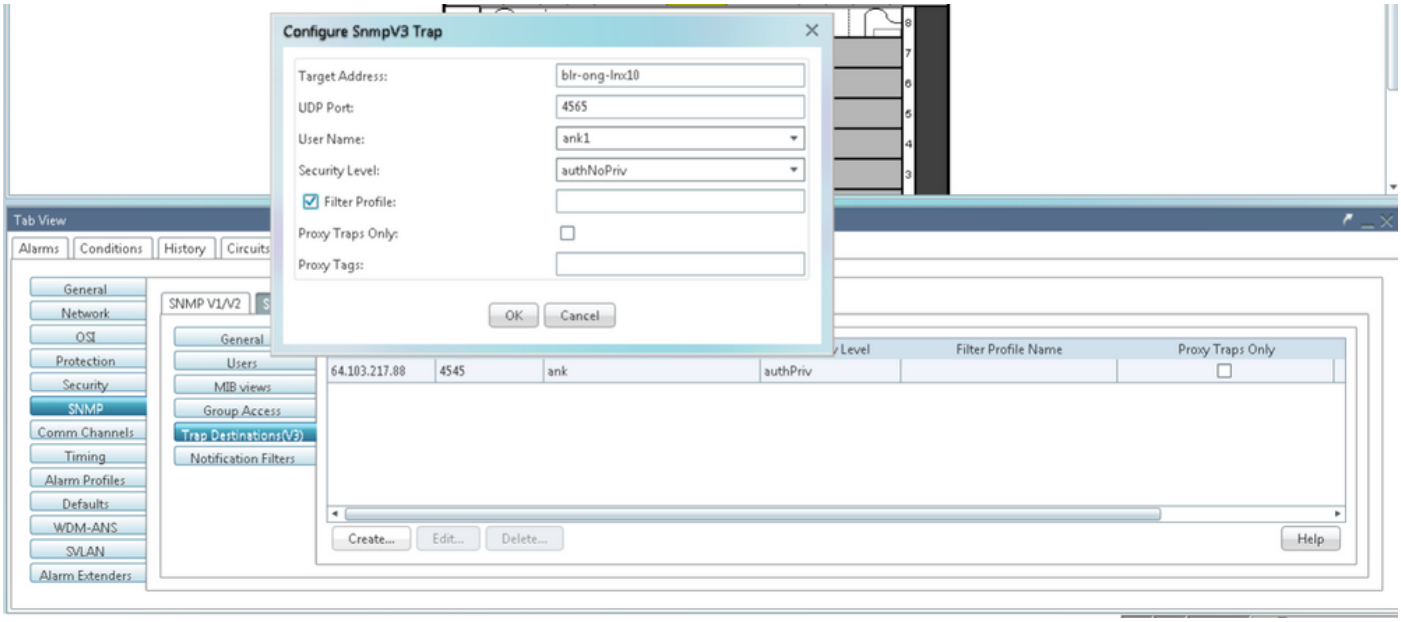
Etapa 3. Certifique-se de que as exibições MIB estejam configuradas conforme mostrado na imagem.



Etapa 4. Configure Group Access (Acesso de grupo) como mostrado na imagem para o modo authnopriv.



Etapa 5. Navegue até **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Clique em **Criar** e **Configurar** como mostrado na imagem.



Verificar o modo authNoPriv

Etapa 1. Navegue até o servidor NMS e faça snmpwalk.

Sintaxe:

```
snmpwalk -v 3 -l authnopriv -u <user name> -a MD5 -A <password> <node IP> <MIB>
```

Exemplo:

```
blr-ong-lnx10:154> snmpwalk -v 3 -l authnopriv -u ank1 -a MD5 -A cisco123  10.64.106.40 system

RFC1213-MIB::sysDescr.0 = STRING: "Cisco ONS 15454 M6 10.50-015E-05.18-SPA Factory Defaults
```

```
PLATFORM=15454-M6"

RFC1213-MIB::sysObjectID.0 = OID: CERENT-GLOBAL-REGISTRY::cerent454M6Node

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (430323) 1:11:43.23

RFC1213-MIB::sysContact.0 = ""

RFC1213-MIB::sysName.0 = STRING: "Ankit_40"

RFC1213-MIB::sysLocation.0 = ""

RFC1213-MIB::sysServices.0 = INTEGER: 79
```

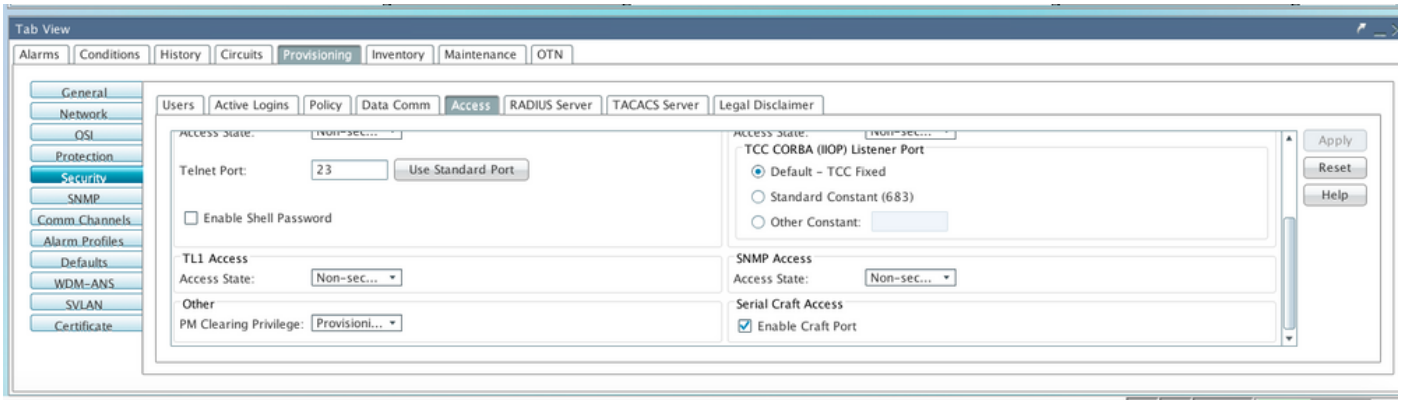
Interceptação SNMP:

```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

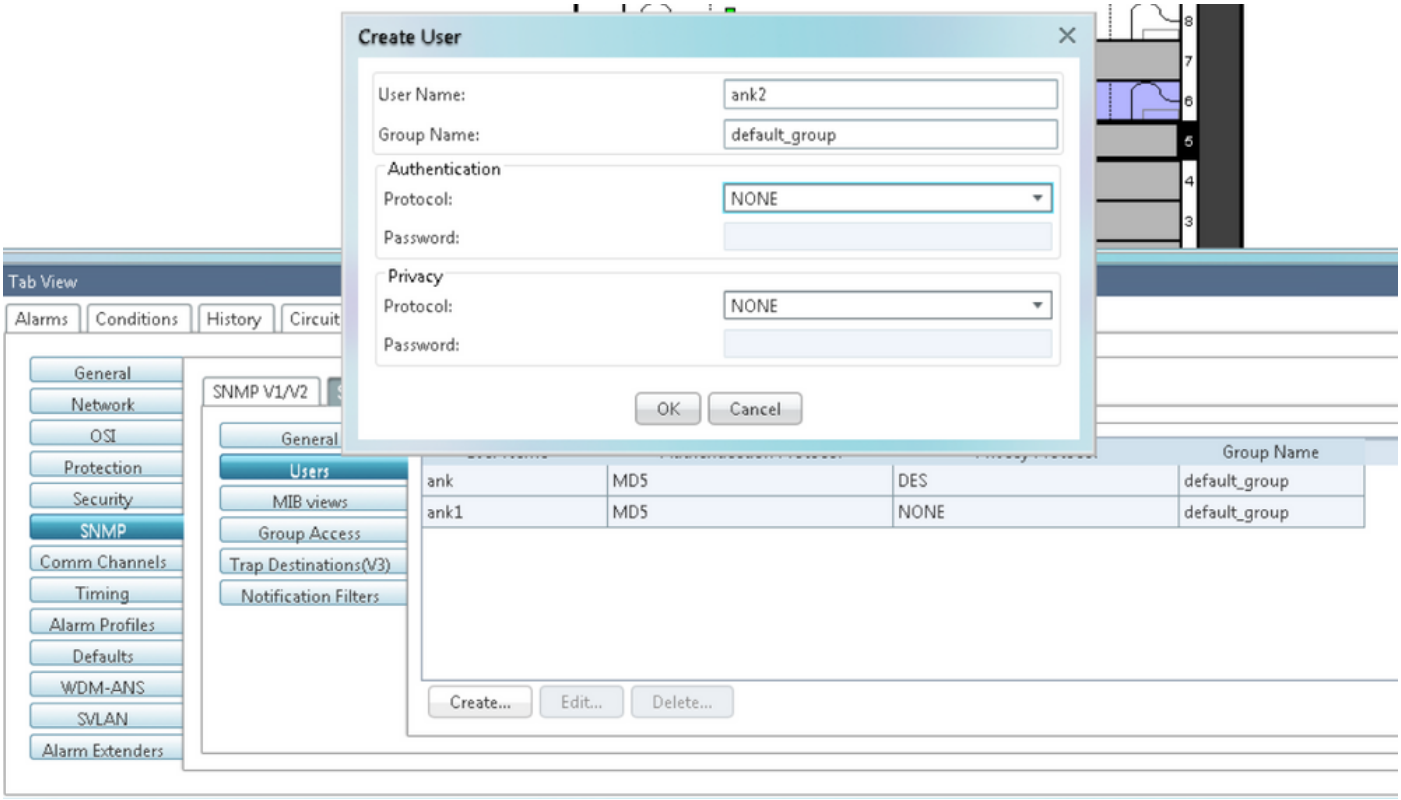
O comando Trap cmd é o mesmo para todas as versões.

Configurar o modo noAuthNoPriv no dispositivo ONS15454/NCS2000

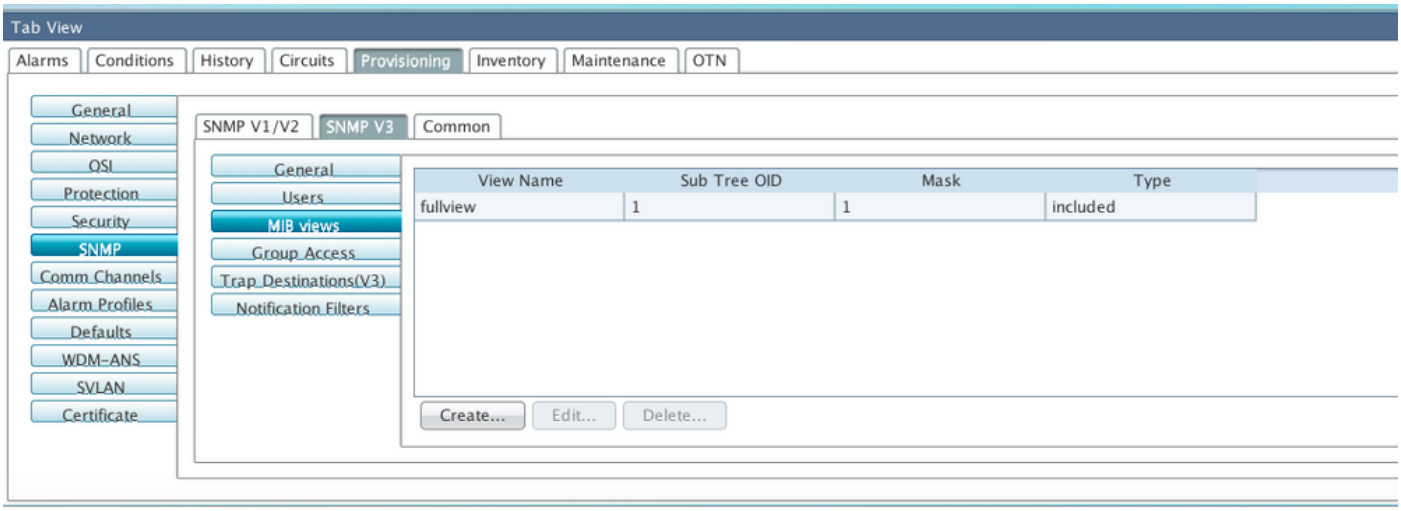
Etapa 1. No CTC, navegue para **Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode, como** mostrado na imagem.



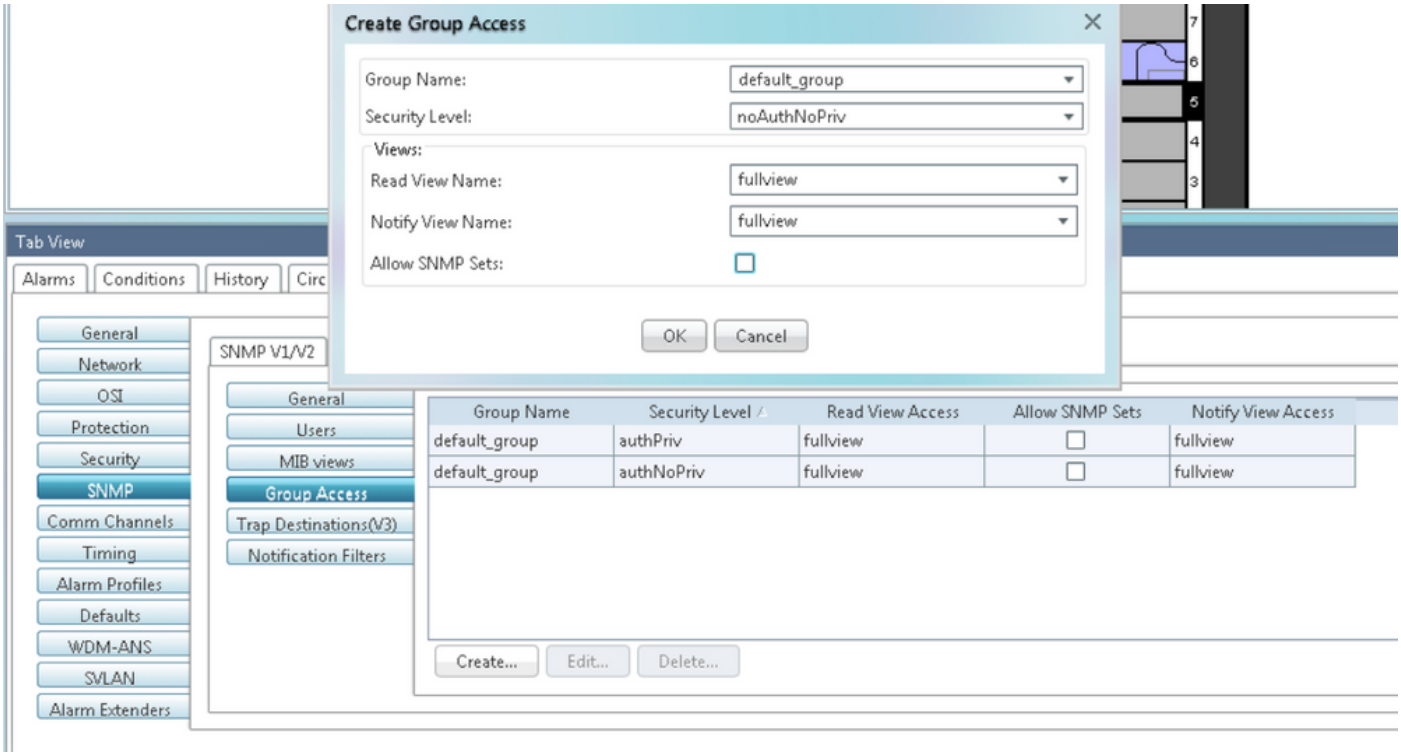
Etapa 2. Navegue até **Node View > Provisioning > SNMP > SNMP V3 > Users > Create User and Configure** conforme mostrado na imagem.



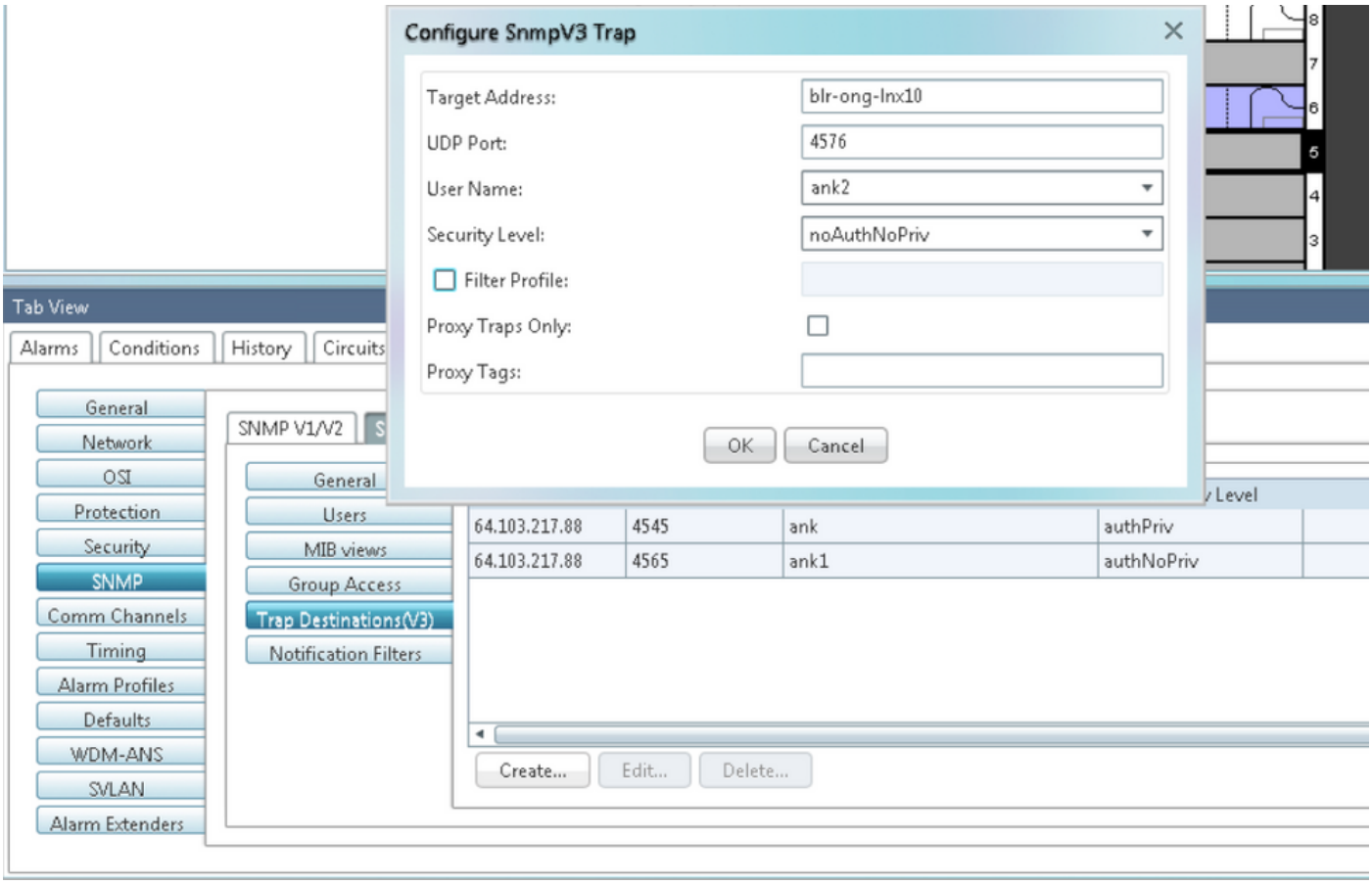
Etapa 3. Certifique-se de que **as exibições MIB** estejam configuradas conforme mostrado na imagem.



Etapa 4. Configure Group Access (Acesso de grupo) como mostrado na imagem para o modo noauthnopriv.



Etapa 5. Navegue até **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Clique em **Criar** e **Configurar** como mostrado na imagem.



Verificar modo noAuthNoPriv

Etapa 1. Navegue até o servidor NMS e faça snmpwalk.

```
snmpwalk -v 3 -l noauthnopriv -u <user name> <node IP> <MIB>
```

Exemplo:

```
blr-ong-lnx10:155> snmpwalk -v 3 -l noauthnopriv -u ank2 10.64.106.40 system

RFC1213-MIB::sysDescr.0 = STRING: "Cisco ONS 15454 M6 10.50-015E-05.18-SPA Factory Defaults
PLATFORM=15454-M6"

RFC1213-MIB::sysObjectID.0 = OID: CERENT-GLOBAL-REGISTRY::cerent454M6Node

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (486910) 1:21:09.10

RFC1213-MIB::sysContact.0 = ""

RFC1213-MIB::sysName.0 = STRING: "Ankit_40"

RFC1213-MIB::sysLocation.0 = ""

RFC1213-MIB::sysServices.0 = INTEGER: 79

blr-ong-lnx10:156>
```

Interceptação SNMP:

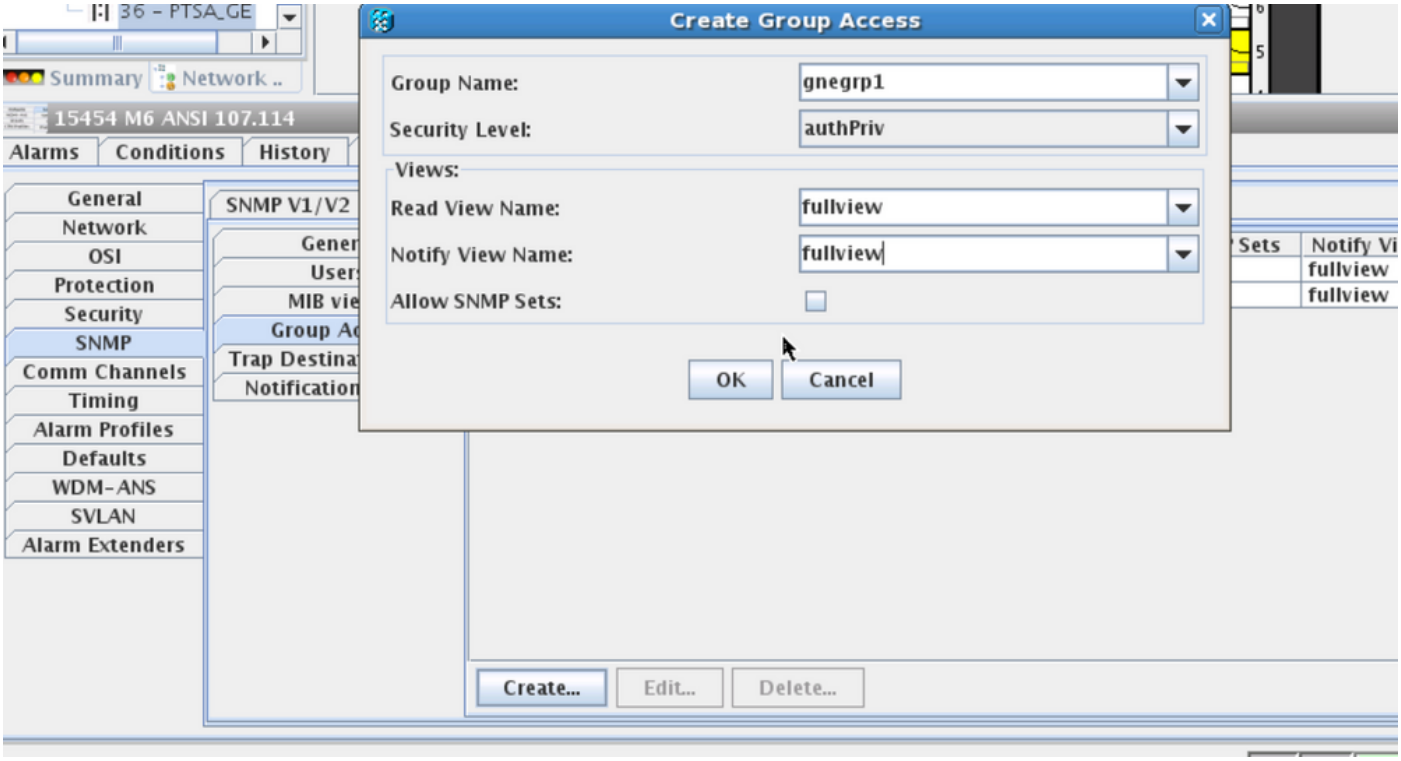
```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

O comando Trap cmd é o mesmo para todas as versões.

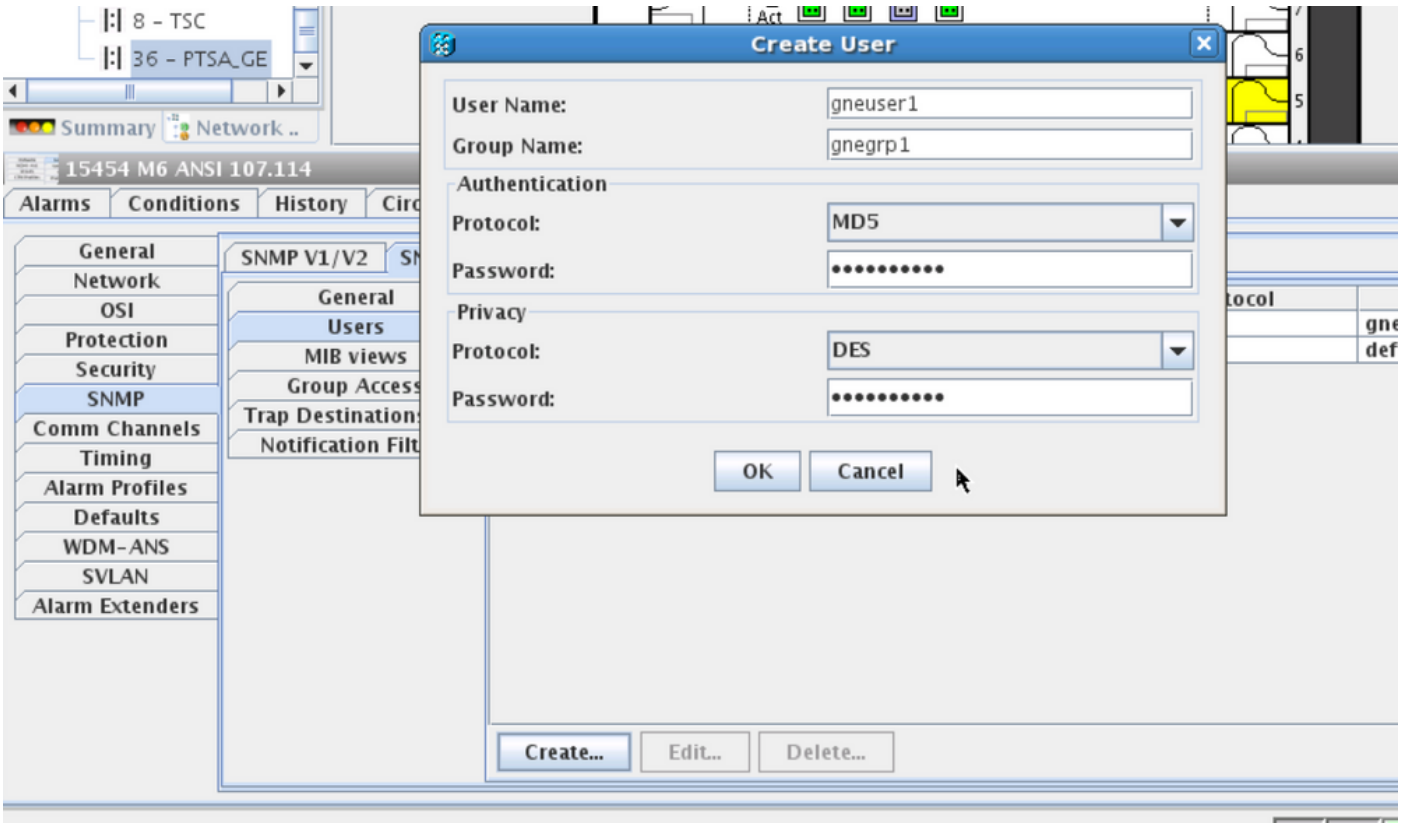
Configuração de armadilha SNMP V3 para GNE/ENE

No nó GNE

Etapa 1. Navegar para **Provisionamento > SNMP > SNMP V3 e CCriar acesso de grupo (guia Acesso de grupo): forneça um nome de grupo com nível de segurança (noAuthnoPriv|AuthnoPriv|authPriv) e acesso de leitura e notificação de visualização completa, como mostrado na imagem.**



Etapa 2. Criar acesso de usuário (guia Usuários): crie um usuário com o nome do grupo como criado anteriormente na guia Acesso ao grupo. Além disso, forneça a Autenticação com base no nível de acesso como mostrado na imagem.



Etapa 3. Guia Destino da interceptação (V3):

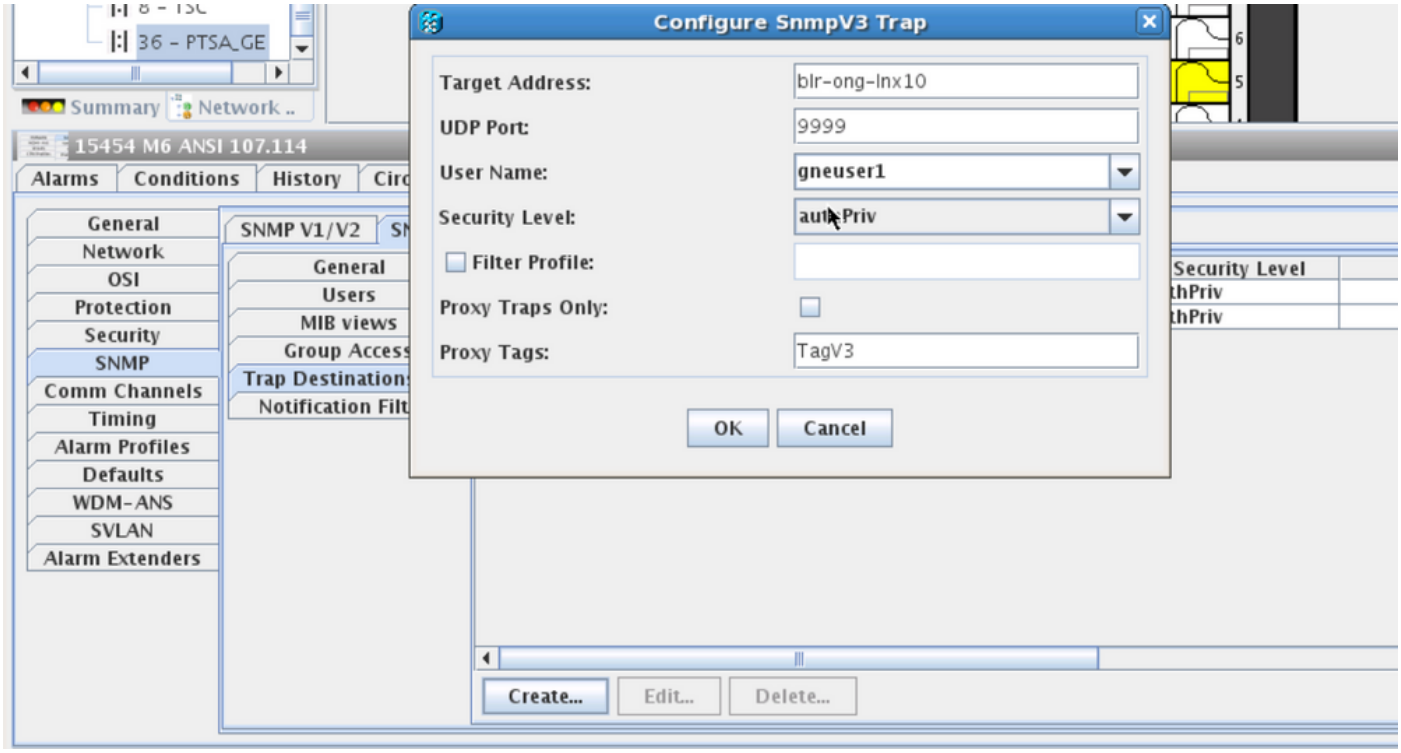
Endereço de destino: Endereço do servidor NMS de onde a armadilha será executada (ex. Blr-ong-lnx10).

Porta UDP: Qualquer número de porta onde a armadilha será ouvida(Ex.: 9977).

User Name: Nome do usuário na guia Usuário.

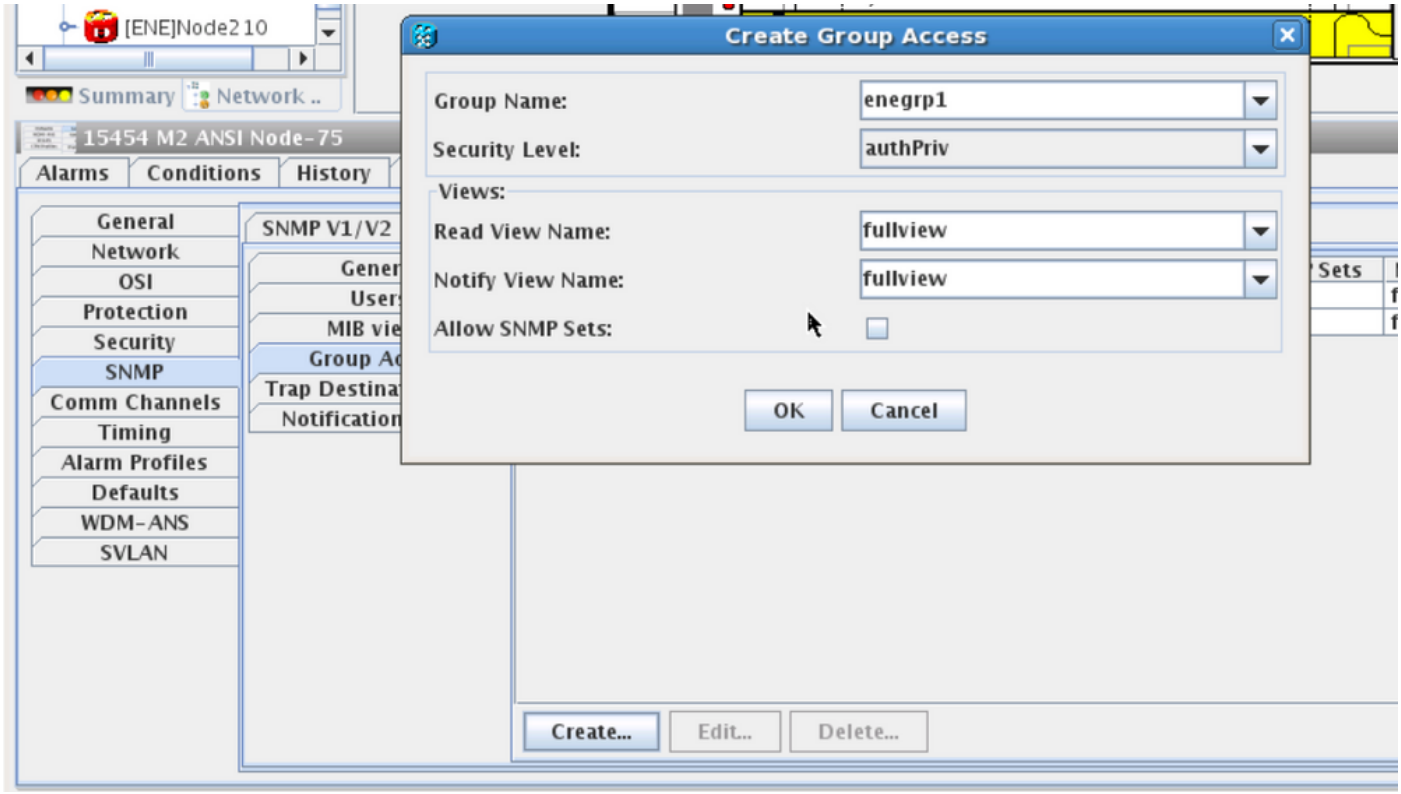
Nível de segurança: Conforme configurado anteriormente na guia Usuário.

Marcas de proxy: Forneça uma marca de proxy (Ex.: Tag75).

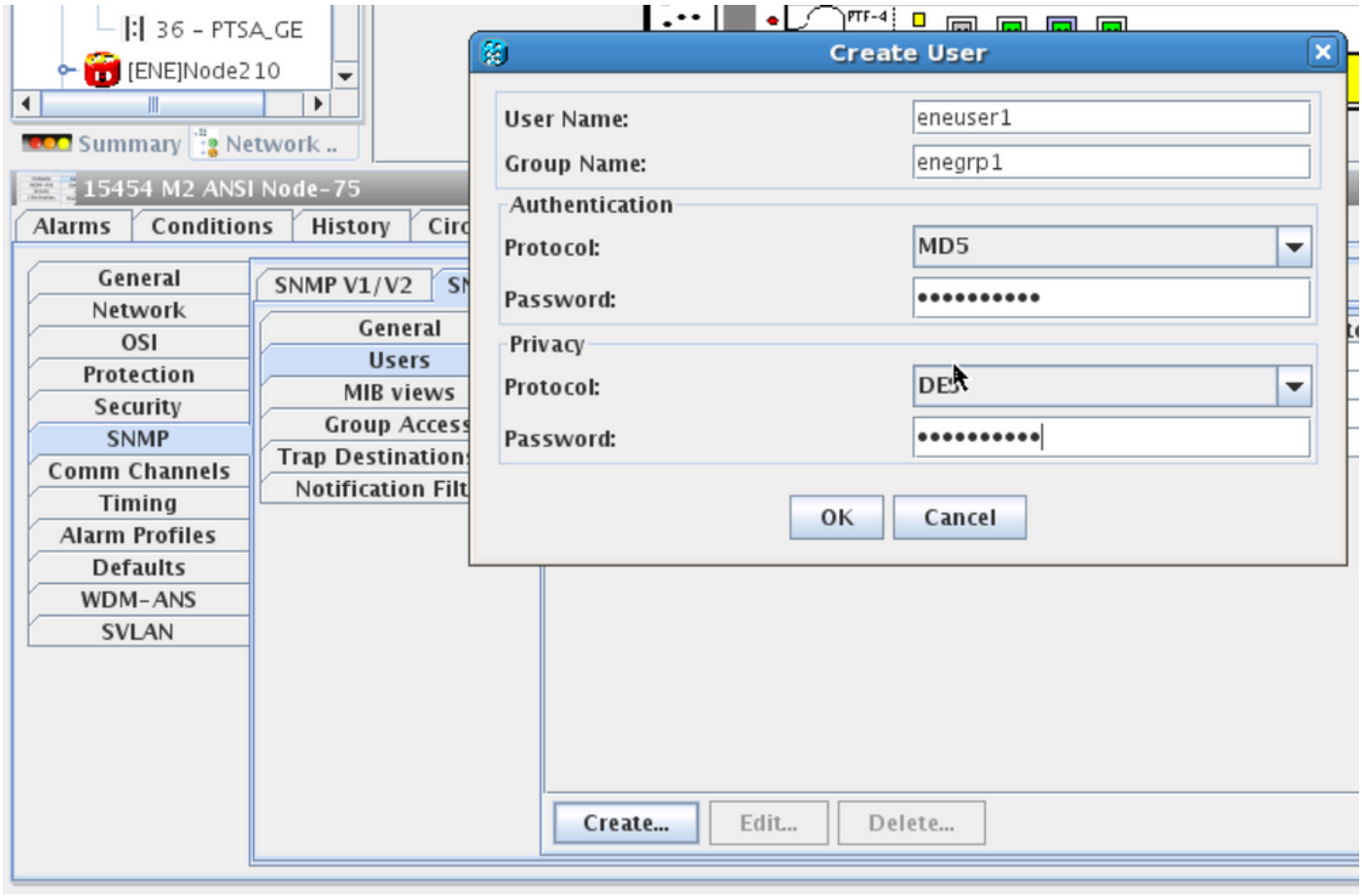


No nó ENE

Etapa 1. Navegue até **Provisioning > SNMP > SNMP V3 e Create Group Access (Guia Group Access):** forneça um nome de grupo com nível de acesso (noAuthnoPriv|AuthnoPriv|authPriv) e acesso de leitura e notificação de visualização completa, como mostrado na imagem.



Etapa 2. Criar acesso de usuário (guia Usuários): crie um usuário com o nome do grupo como criado anteriormente na guia Acesso ao grupo. Além disso, forneça a Autenticação com base no nível de acesso.



Certifique-se de que um grupo_padrão, se mostrado na guia Usuário, seja criado na guia Acesso de grupo, caso esteja ausente na guia Acesso de grupo.

Etapa 3. Guia Destino da interceptação (V3):

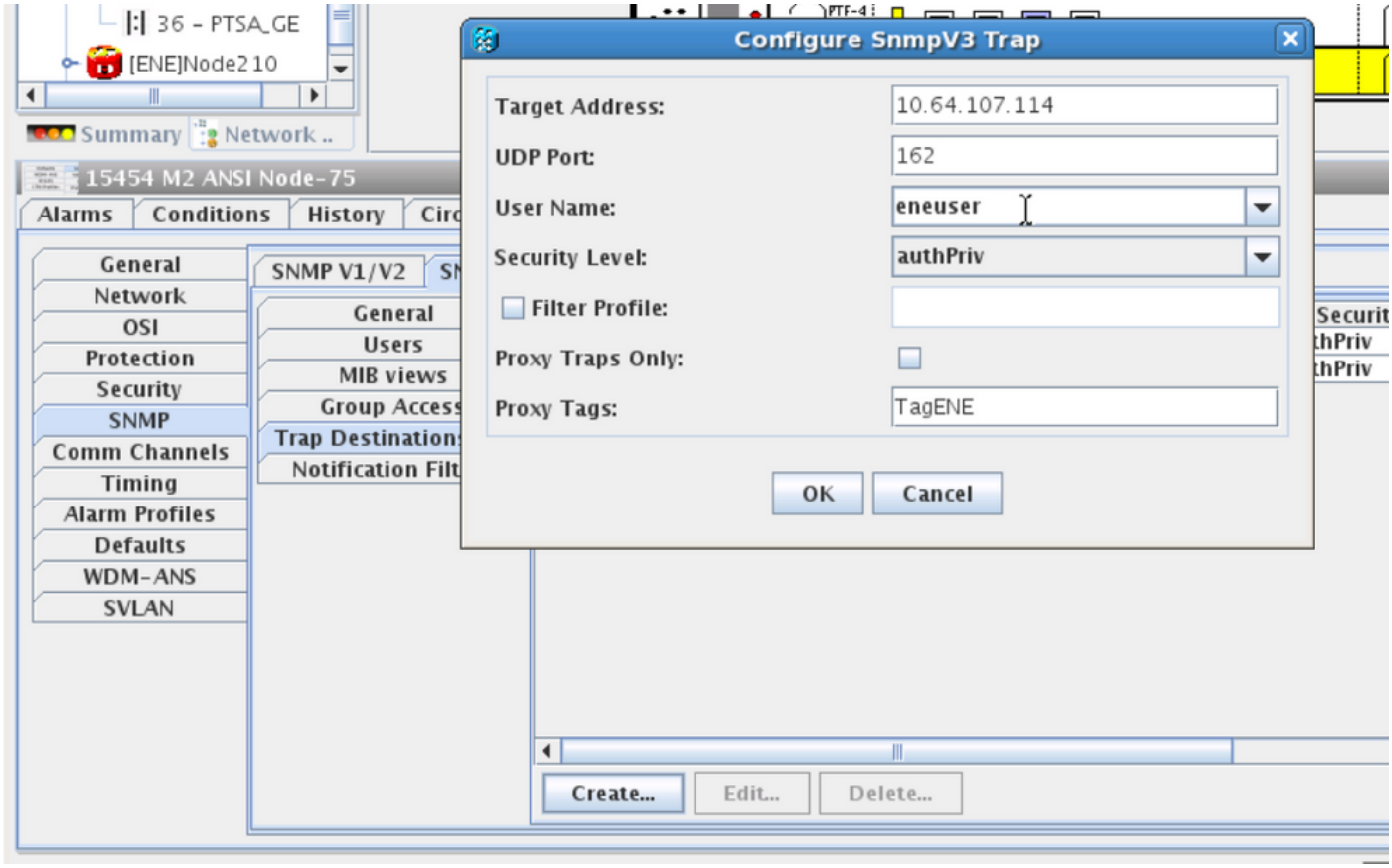
Endereço de destino: IP do nó GNE.

Porta UDP: 162.

User Name: Nome do usuário na guia Usuário.

Nível de segurança: Conforme configurado anteriormente na guia Usuário.

Marcas de proxy: Forneça qualquer marca de proxy igual à GNE (Ex.: Tag75).



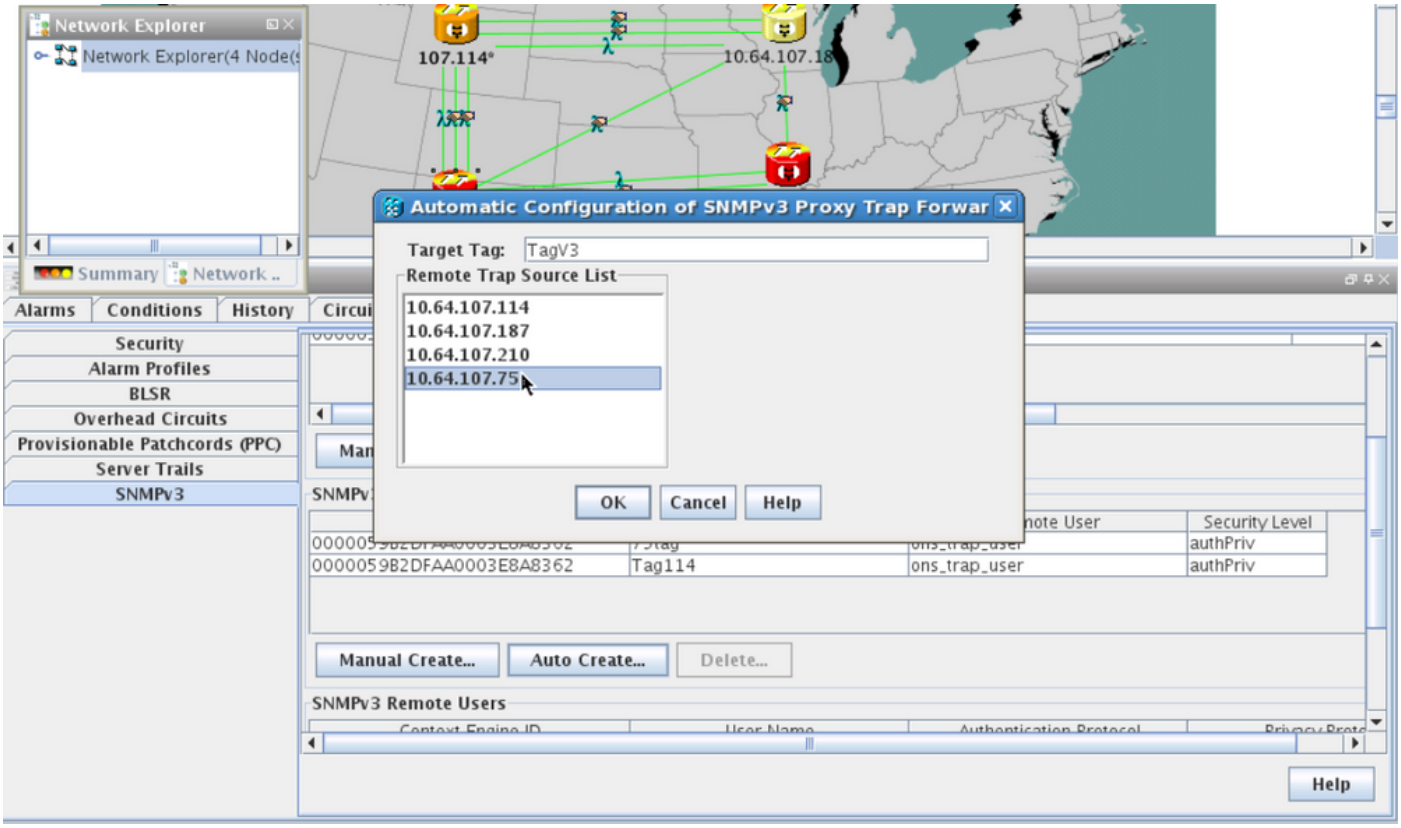
No CTC, navegue até a exibição de rede:

Etapa 1. Navegue até a guia **SNMPv3**.

Etapa 2. Tabela do Encaminhador de Interceptação de Proxy SNMPv3: Você pode fazer **Manual** ou **Criação automática**.

Selecione **Criação automática**. Nela:

- Etiqueta de destino: Marca de proxy definida em GNE.
- Lista de origem de interceptação remota: selecione o IP do nó ENE como mostrado na imagem.



Verificar a configuração do GNE/ENE

Configurar o servidor NMS (blr-ong-lnx10):

Etapa 1. No diretório inicial do servidor, crie um diretório e nomeie-o como **snmp**.

Etapa 2. Neste diretório, crie um arquivo **snmptrapd.conf**.

Etapa 3. Em **snmptrapd.conf**, crie esta configuração:

```
createUser -e 0x
```

Engine_NO = can be available from CTC. Open GNE node-->Node view->Provisioning->SNMP->SNMP V3-->General.

Interceptação SNMP:

```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n"
```

snmpwalk no ENE:

Para o modo autenticado:

```
snmpwalk -v 3 -l authpriv -u <user_name> -a MD5 -A <auth_password>123 -x DES -X <des_password> -E <ene_engine_id> <gne_ip_address> <OID>
```

Para o modo autenticado:

```
snmpwalk -v 3 -l authnopriv -u <user_name> -a MD5 -A <auth_password>  -E <ene_engine_id> <gne_ip_address> <OID>
```

Para o modo noauthnopriv:

```
snmpwalk -v 3 -l authpriv -u
```

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.