Configurer SNMPv3 sur les périphériques Cisco ONS15454/NCS2000

Contenu

Introduction

Ce document décrit les instructions pas à pas sur la configuration du protocole SNMPv3 (Simple Network Management Protocol version 3) sur les périphériques ONS15454/NCS2000. Tous les sujets incluent des exemples.

> **Note**: La liste d'attributs fournie dans ce document n'est ni exhaustive ni faisant autorité et peut changer à tout moment sans mise à jour de ce document.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Interface graphique du contrôleur de transport Cisco (CTC)
- Connaissances de base sur les serveurs
- Commandes Linux/Unix de base

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Sur un noeud autonome/multitablette

Configurer le mode authPriv sur le périphérique ONS15454/NCS2000

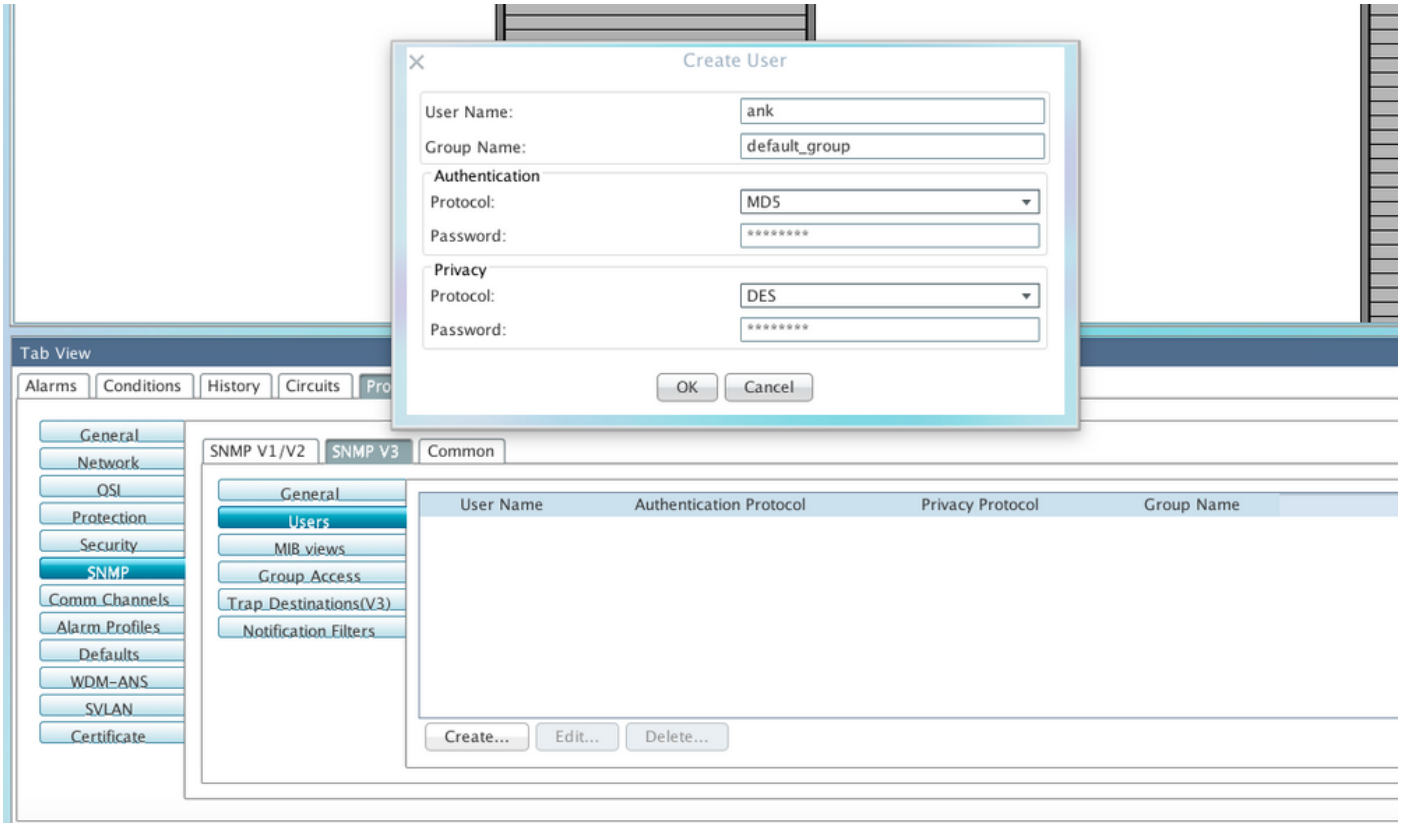
Étape 1. Connectez-vous au noeud via CTC à l'aide des informations d'identification du super utilisateur.

Étape 2. Accédez à **Vue du noeud > Provisioning > SNMP > SNMP V3**.

Étape 3. Accédez à l'onglet **Utilisateurs**. Créer des utilisateurs.

```
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>
```

Étape 4. Cliquez sur **OK** comme indiqué dans l'image.



Spécifications :

User Name (Nom d'utilisateur) : spécifiez le nom de l'utilisateur sur l'hôte qui se connecte à l'agent. Le nom d'utilisateur doit comporter au moins 6 et au maximum 40 caractères (jusqu'à 39 caractères pour l'authentification TACACS et RADIUS). Il inclut des caractères alphanumériques (a-z, A-Z, 0-9) et les caractères spéciaux autorisés sont @, "-" (tiret) et « . » (point). Pour la compatibilité TL1, le nom d'utilisateur doit comporter entre 6 et 10 caractères.

Nom du groupe : spécifiez le groupe auquel appartient l'utilisateur.

Authentification:

Protocole : sélectionnez l'algorithme d'authentification que vous souhaitez utiliser. Les options sont NONE, MD5 et SHA.

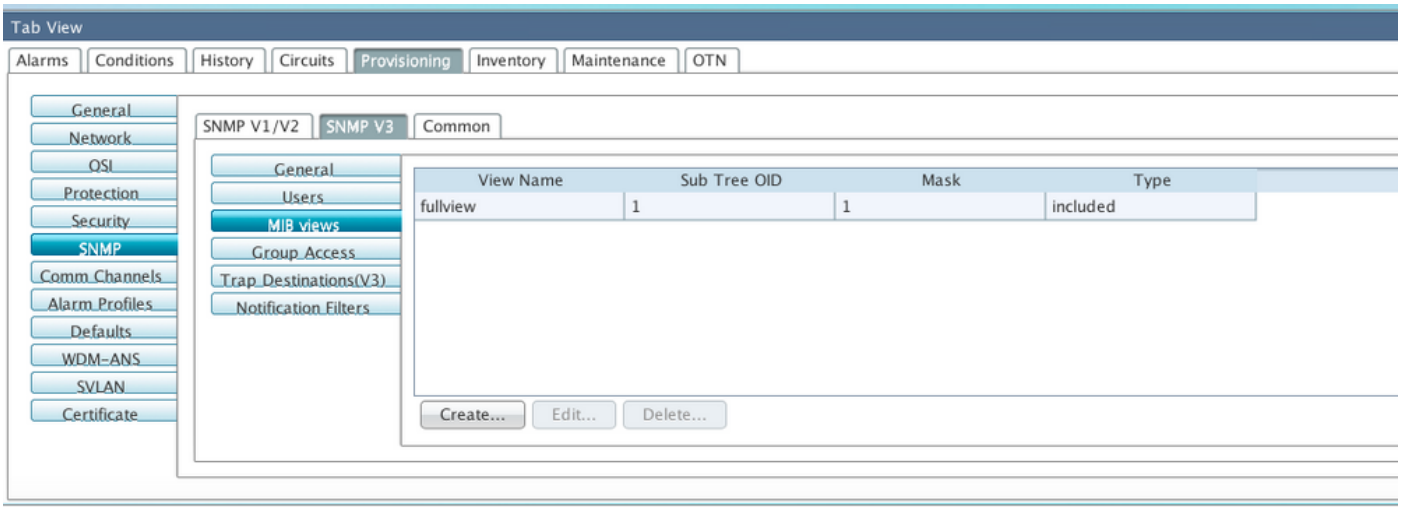
Password (Mot de passe) : saisissez un mot de passe si vous sélectionnez MD5 ou SHA. Par défaut, la longueur du mot de passe est définie sur un minimum de huit caractères.

Confidentialité : initie une session de définition du niveau d'authentification de la confidentialité qui permet à l'hôte de chiffrer le contenu du message envoyé à l'agent.

Protocole : sélectionnez l'algorithme d'authentification de la confidentialité. Les options disponibles sont None, DES et AES-256-CFB.

Password (Mot de passe) : saisissez un mot de passe si vous sélectionnez un protocole autre que None (Aucun).

Étape 5. Vérifiez que les vues MIB sont configurées conformément à cette image.



Spécifications :

Nom : nom de la vue.

OID de sous-arborescence : sous-arborescence MIB qui, lorsqu'elle est combinée au masque, définit la famille des sous-arborescences.

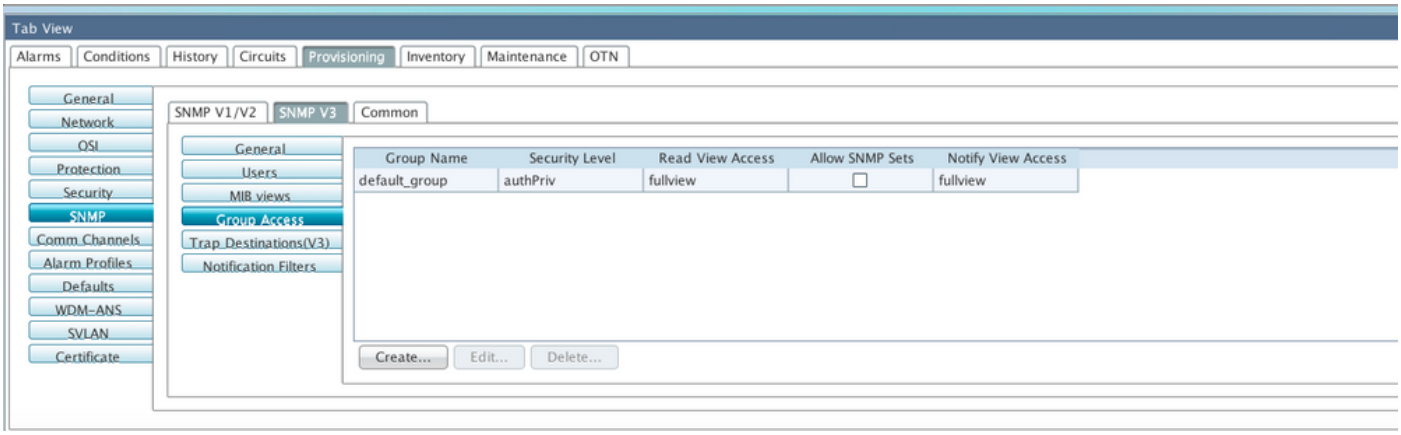
Masque de bits - Une famille de sous-arbres de vue. Chaque bit du masque de bits correspond à un sous-identificateur de l'OID de sous-arborescence.

Type : sélectionnez le type de vue. Les options sont incluses et exclues.

Le type définit si la famille de sous-arborescences définies par l'OID de sous-arborescence et la combinaison de masques de bits sont incluses ou exclues du filtre de notification.

Étape 6. Configurez l'accès au groupe comme indiqué dans l'image. Par défaut, le nom du groupe sera default_group et le niveau de sécurité authPriv.

Note: Le nom du groupe doit être identique à celui utilisé lors de la création de l'utilisateur à l'étape 3.



Spécifications :

Group Name (Nom du groupe) : nom du groupe SNMP ou de la collection d'utilisateurs qui partagent une stratégie d'accès commune.

Niveau de sécurité : niveau de sécurité pour lequel les paramètres d'accès sont définis.

Sélectionnez l'une des options suivantes :

noAuthNoPriv : utilise une correspondance de nom d'utilisateur pour l'authentification.

AuthNoPriv - Fournit une authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA.

AuthPriv - Fournit une authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA. Fournit un cryptage DES 56 bits basé sur la norme CBC-DES (DES-56), en plus de l'authentification.

Si vous sélectionnez authNoPriv ou authPriv pour un groupe, l'utilisateur correspondant doit être configuré avec un protocole d'authentification et un mot de passe, avec un protocole de confidentialité et un mot de passe, ou les deux.

Vues

Nom de la vue de lecture : nom de la vue de lecture du groupe.

Notify View Name : nom de la vue Notify pour le groupe.

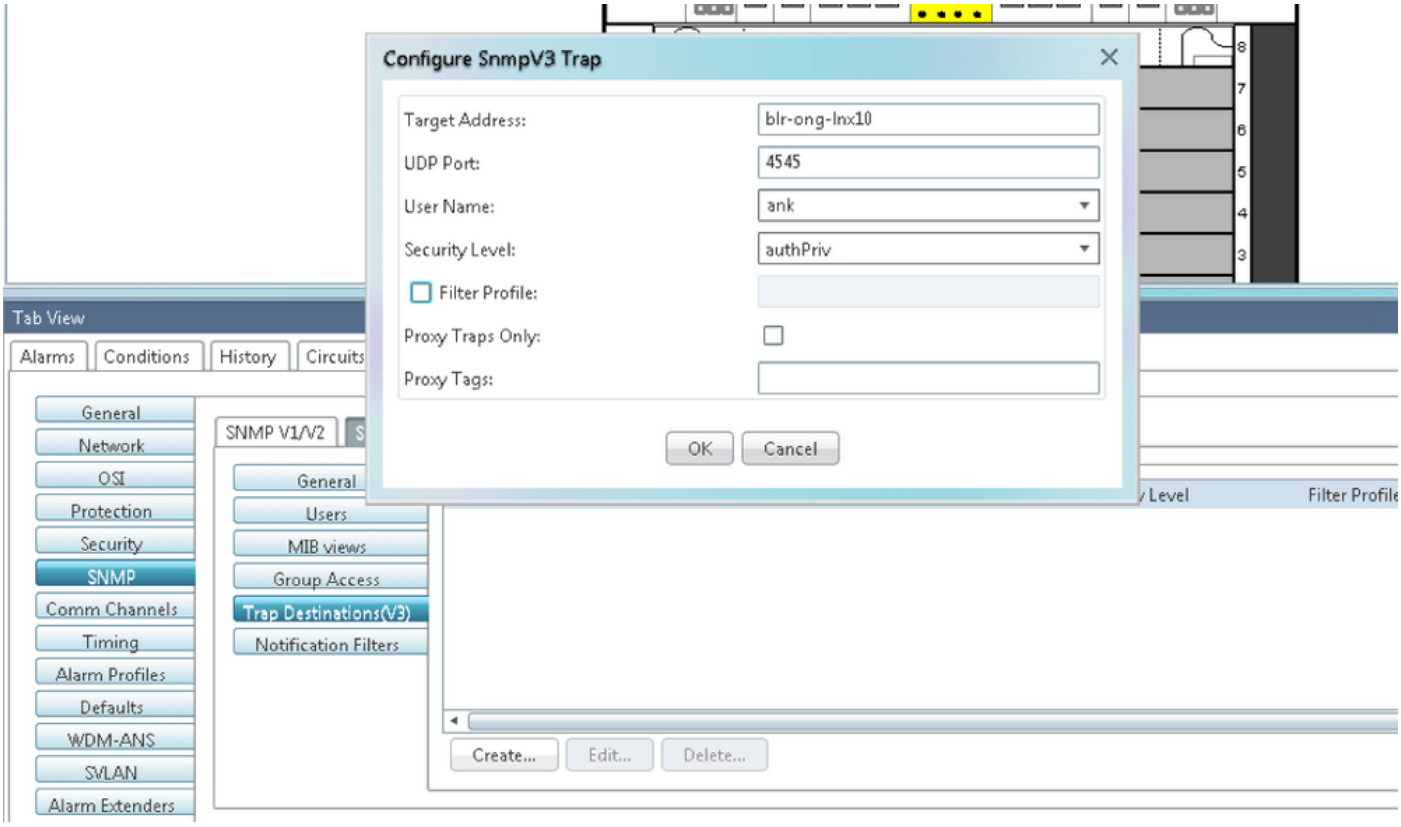
Allow SNMP Sets : activez cette case à cocher si vous souhaitez que l'agent SNMP accepte les requêtes SNMP SET. Si cette case n'est pas cochée, les demandes SET sont rejetées.

Note: L'accès à la requête SET SNMP est mis en oeuvre pour très peu d'objets.

Étape 7. Naviguez jusqu'à **Vue du noeud > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Cliquez sur **Créer** et **Configurer**.

```
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
```

Étape 8. Cliquez sur **OK** comme indiqué dans l'image.



Remarque : blr-ong-lnx10 est le serveur NMS.

Spécifications :

Target Address (Adresse cible) : cible vers laquelle les interruptions doivent être envoyées. Utilisez une adresse IPv4 ou IPv6.

Port UDP : numéro de port UDP utilisé par l'hôte. La valeur par défaut est 162.

User Name (Nom d'utilisateur) : spécifiez le nom de l'utilisateur sur l'hôte qui se connecte à l'agent.

Niveau de sécurité : sélectionnez l'une des options suivantes :

noAuthNoPriv : utilise une correspondance de nom d'utilisateur pour l'authentification.

AuthNoPriv - Fournit une authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA.

AuthPriv - Fournit une authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA. Fournit un cryptage DES 56 bits basé sur la norme CBC-DES (DES-56), en plus de l'authentification.

Filter Profile (Profil de filtre) : activez cette case à cocher et entrez le nom du profil de filtre. Les interruptions ne sont envoyées que si vous fournissez un nom de profil de filtre et créez un filtre de notification.

Proxy Traps Only (Interruptions de proxy uniquement) : si cette option est sélectionnée, seuls les interruptions de proxy de l'ENE sont transmises. Les interruptions de ce noeud ne sont pas envoyées à la destination de déroutement identifiée par cette entrée.

Balises de proxy : spécifiez une liste de balises. La liste de balises n'est nécessaire sur un GNE

que si un ENE doit envoyer des déroutements vers la destination de déroutement identifiée par cette entrée et souhaite utiliser le GNE comme proxy.

Configurer le serveur NMS (blr-ong-lnx10)

Étape 1. Dans votre répertoire personnel du serveur, créez un répertoire portant le nom **snmp**.

Étape 2. Sous ce répertoire, créez un fichier **snmptrapd.conf**.

Étape 3. Remplacez le fichier **snmptrapd.conf** par :

```
vi snmptrapd.conf

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

Exemple :

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

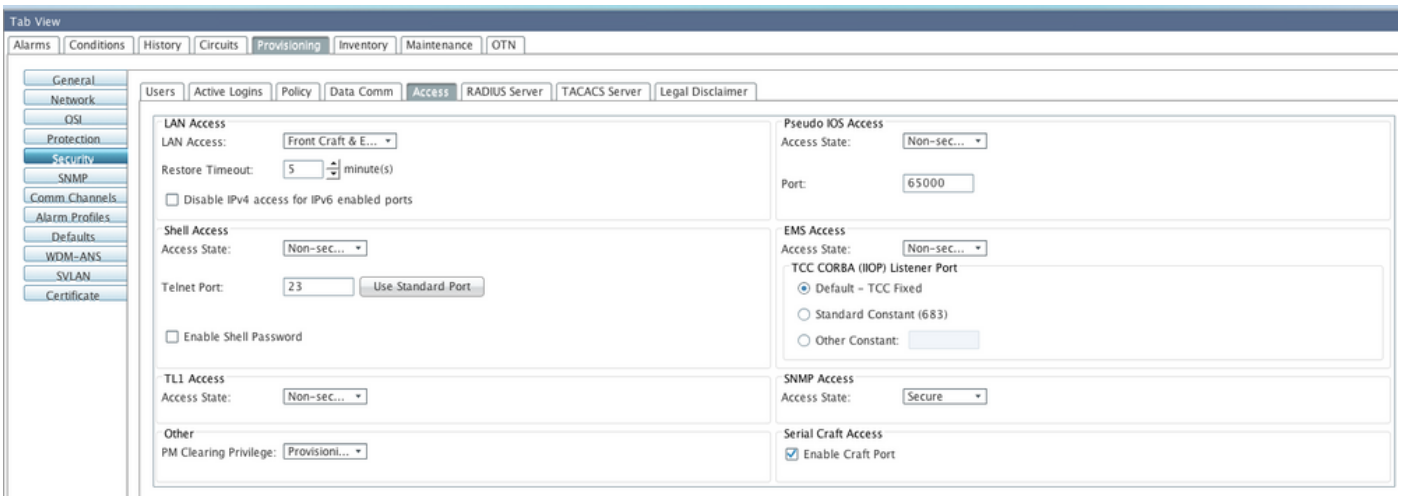
Dans cet exemple :

```
user_name=ank

MD5 password = cisco123

DES password  = cisco123

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

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

Vérifier le mode authPriv

Étape 1. Dans CTC, naviguez jusqu'à **Vue du noeud > Provisioning > Security > Access > change snmp access state to Secure** tel qu'illustré dans l'image.



Étape 2. Accédez au serveur NMS et effectuez snmpwalk.

Syntaxe:

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

Exemple :

```
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
```

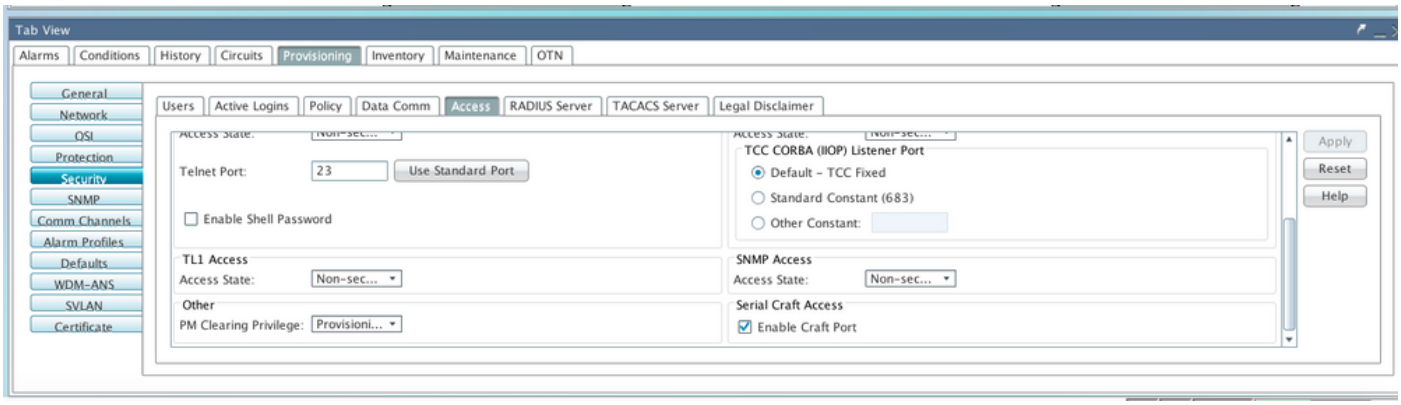
Interruption SNMP :

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

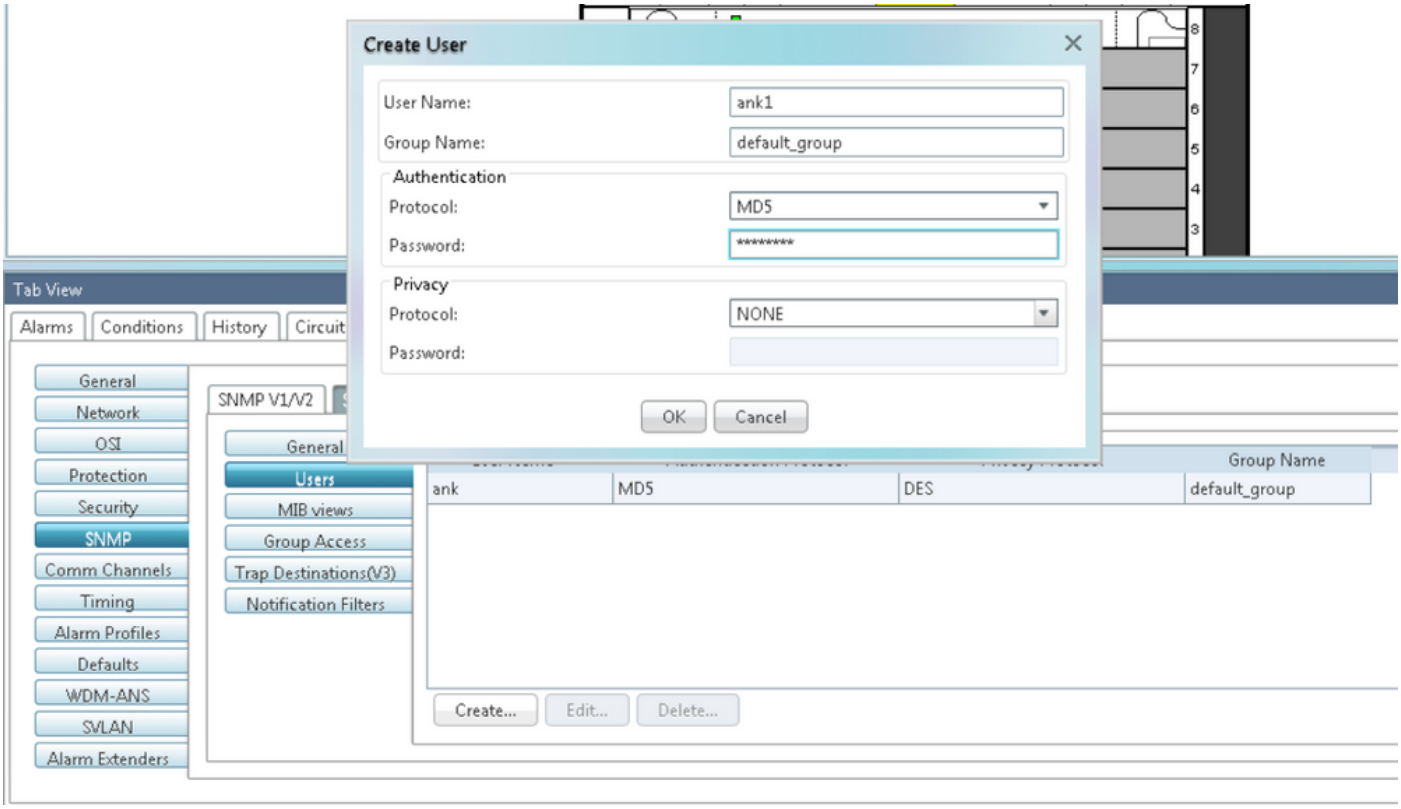
Trap cmd est identique pour toutes les versions.

Configurer le mode authNoPriv sur le périphérique ONS15454/NCS2000

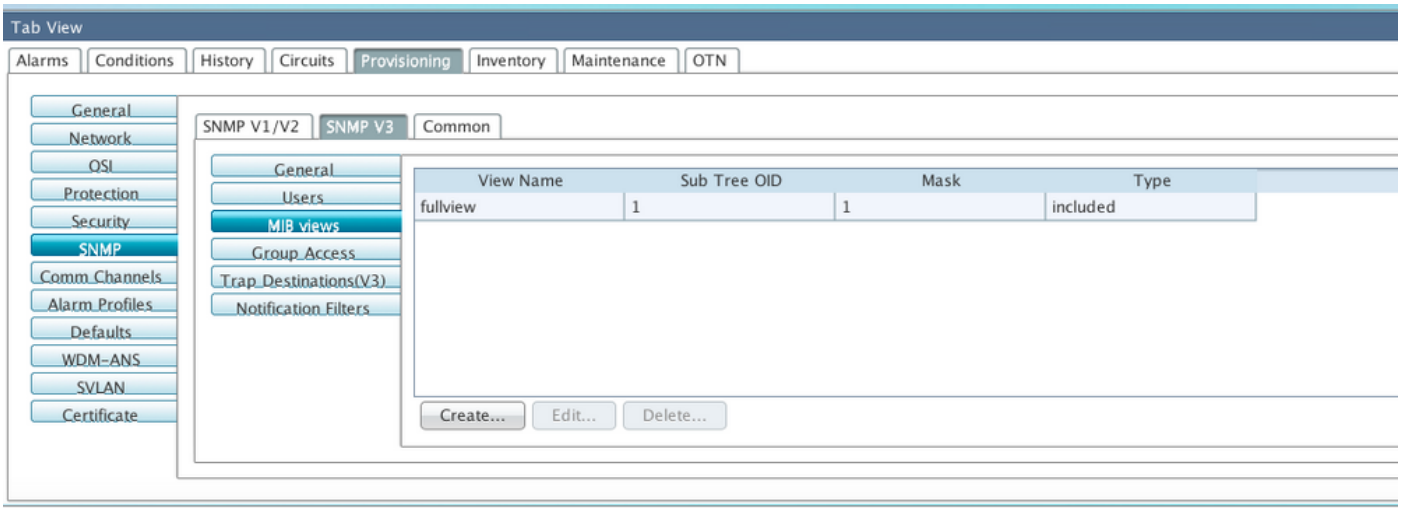
Étape 1. Dans CTC, accédez à **Vue du noeud > Provisioning > Security > Access > change snmp access state to Non secure mode** comme illustré dans l'image.



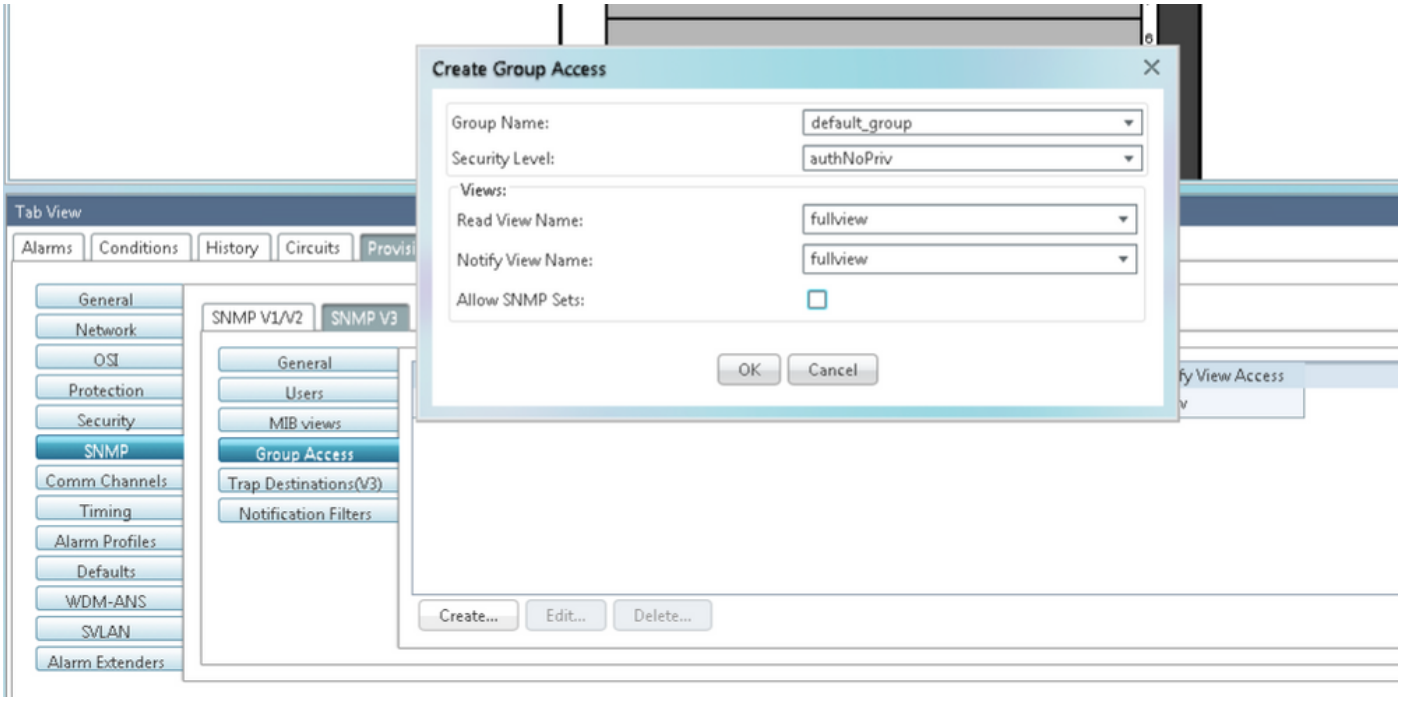
Étape 2. Accédez à **Vue du noeud > Provisioning > SNMP > SNMP V3 > Users > Create User** et configurez comme indiqué dans l'image.



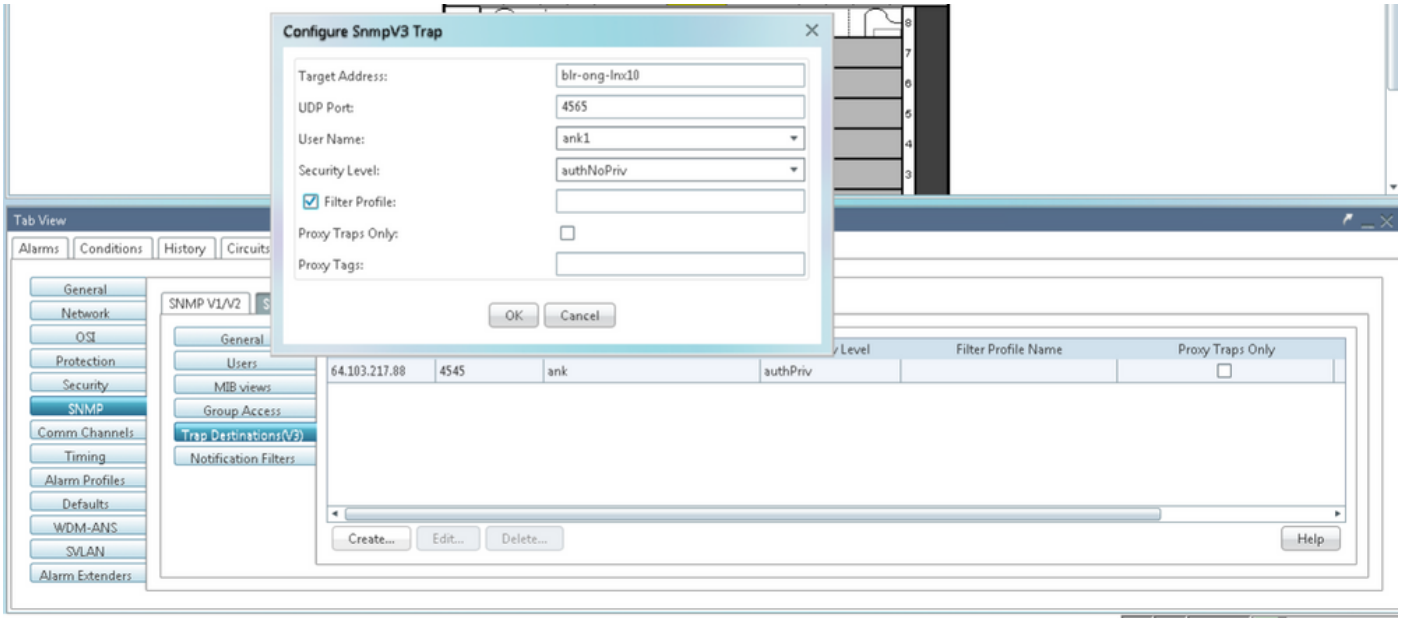
Étape 3. Assurez-vous que les vues MIB sont configurées comme indiqué dans l'image.



Étape 4. Configurez l'accès au groupe comme indiqué dans l'image pour le mode authnopriv.



Étape 5. Naviguez jusqu'à **Vue du noeud > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Cliquez sur **Créer** et **Configurer** comme indiqué dans l'image.



Vérifier le mode authNoPriv

Étape 1. Accédez au serveur NMS et faites snmpwalk.

Syntaxe:

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

Exemple :

```
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
```

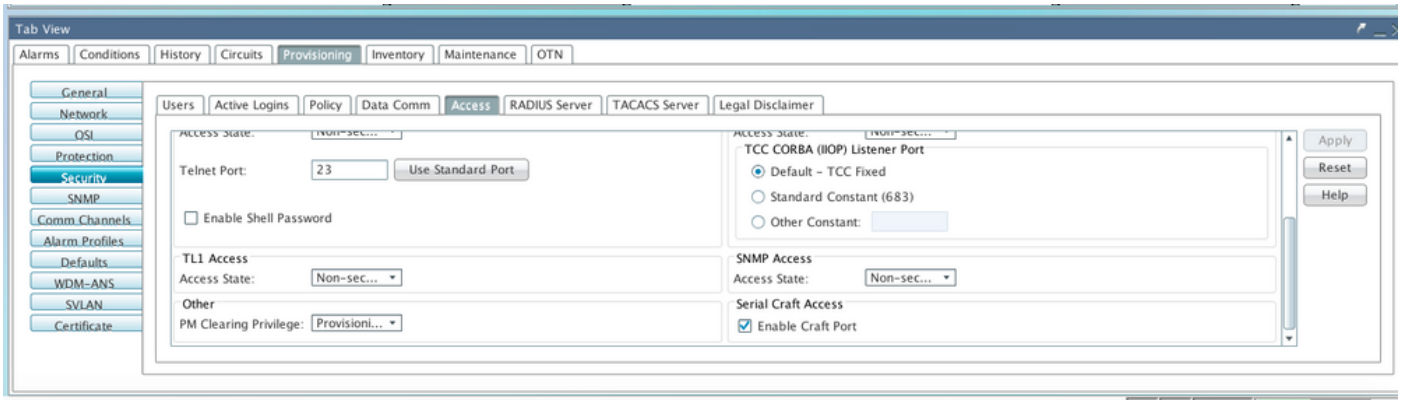
Interruption SNMP :

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

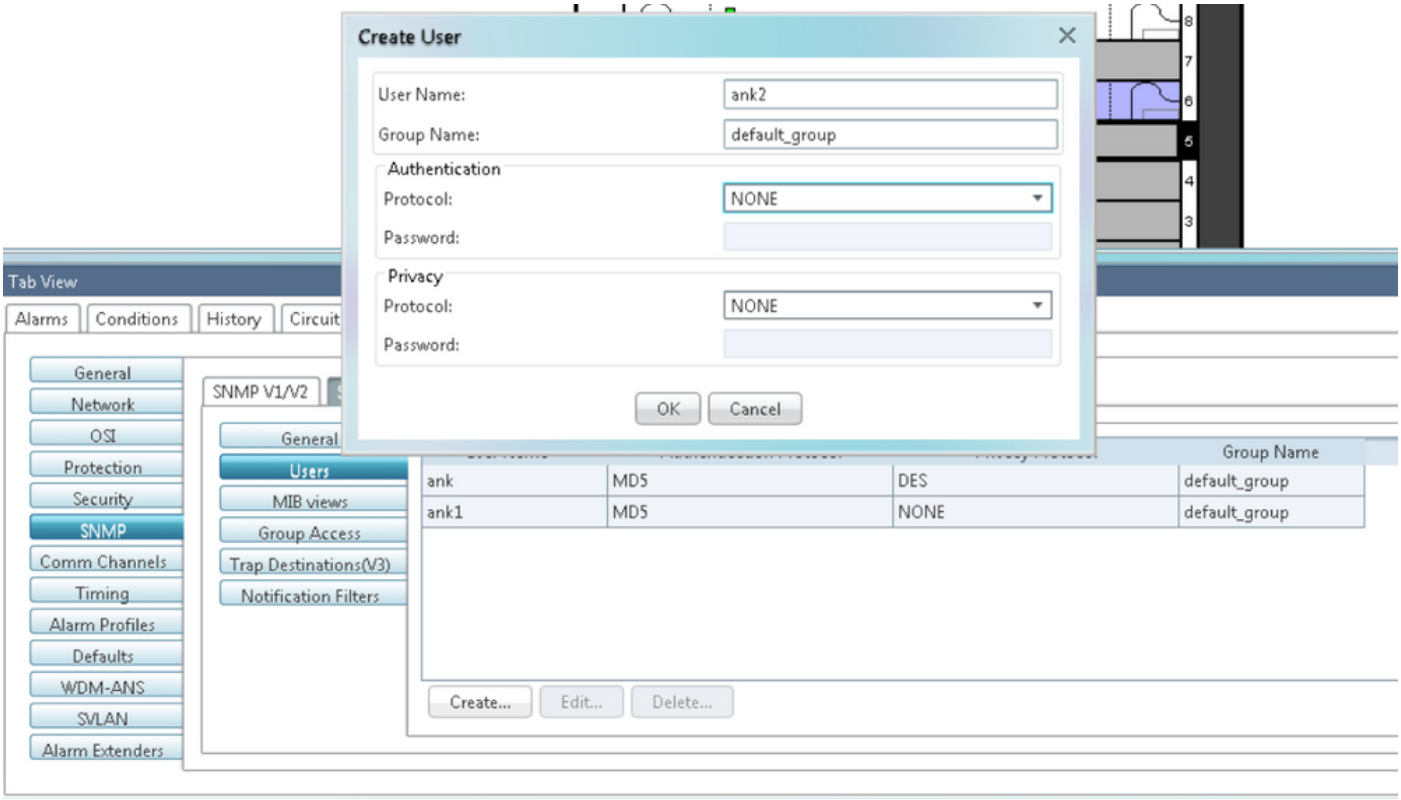
Trap cmd est identique pour toutes les versions.

Configurer le mode noAuthNoPriv sur le périphérique ONS15454/NCS2000

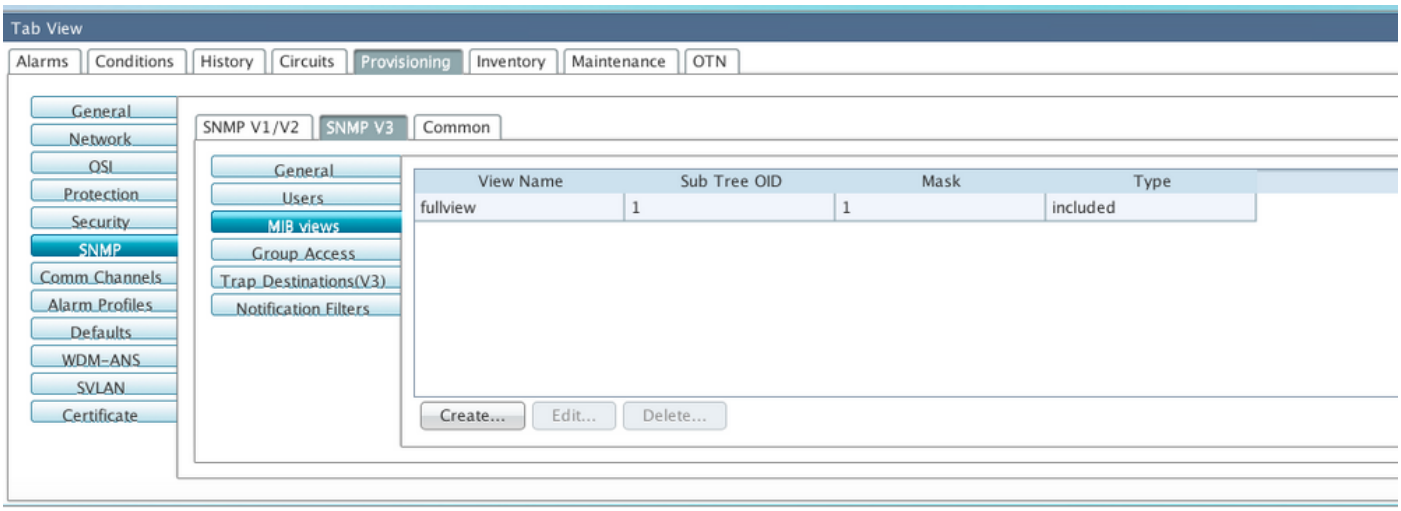
Étape 1. Dans CTC, accédez à **Vue du noeud > Provisioning > Security > Access > change snmp access state to Non secure mode** comme illustré dans l'image.



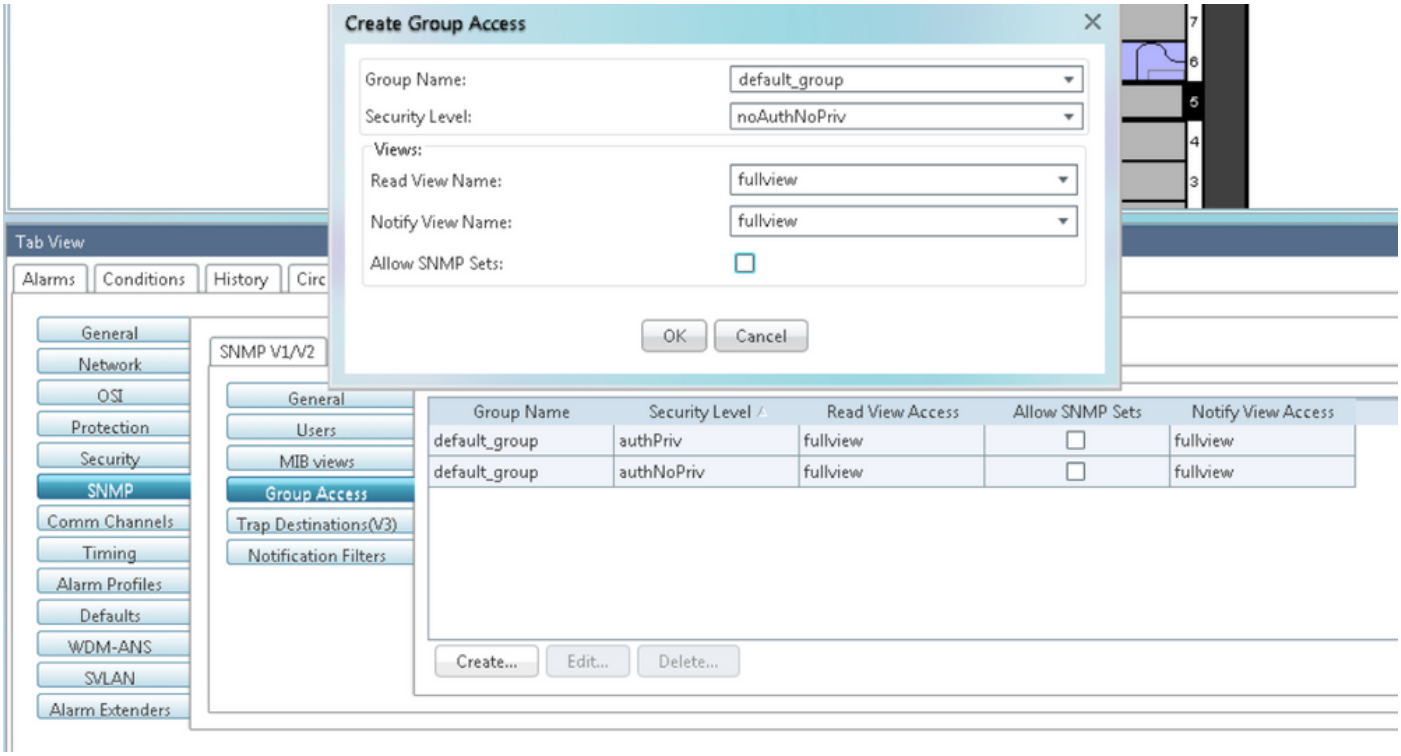
Étape 2. Accédez à **Vue du noeud > Provisioning > SNMP > SNMP V3 > Users > Create User and Configure** comme indiqué dans l'image.



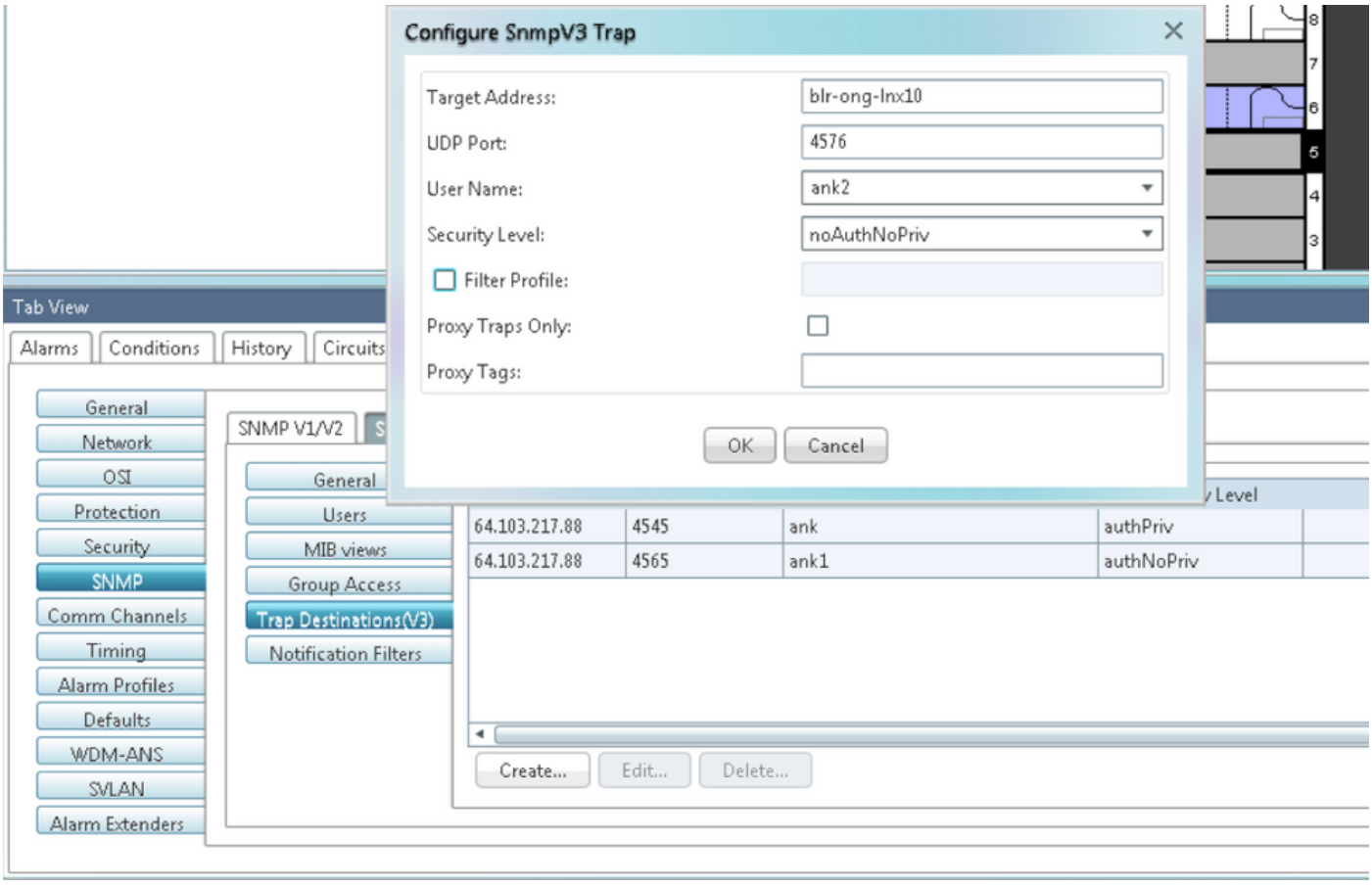
Étape 3. Assurez-vous que **les vues MIB** sont configurées comme indiqué dans l'image.



Étape 4. Configurez l'accès au groupe comme indiqué dans l'image pour le mode noauthnopriv.



Étape 5. Naviguez jusqu'à **Vue du noeud > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Cliquez sur **Créer** et **Configurer** comme indiqué dans l'image.



Vérifier le mode noAuthNoPriv

Étape 1. Accédez au serveur NMS et effectuez snmpwalk.

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

Exemple :

```
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>
```

Interruption SNMP :

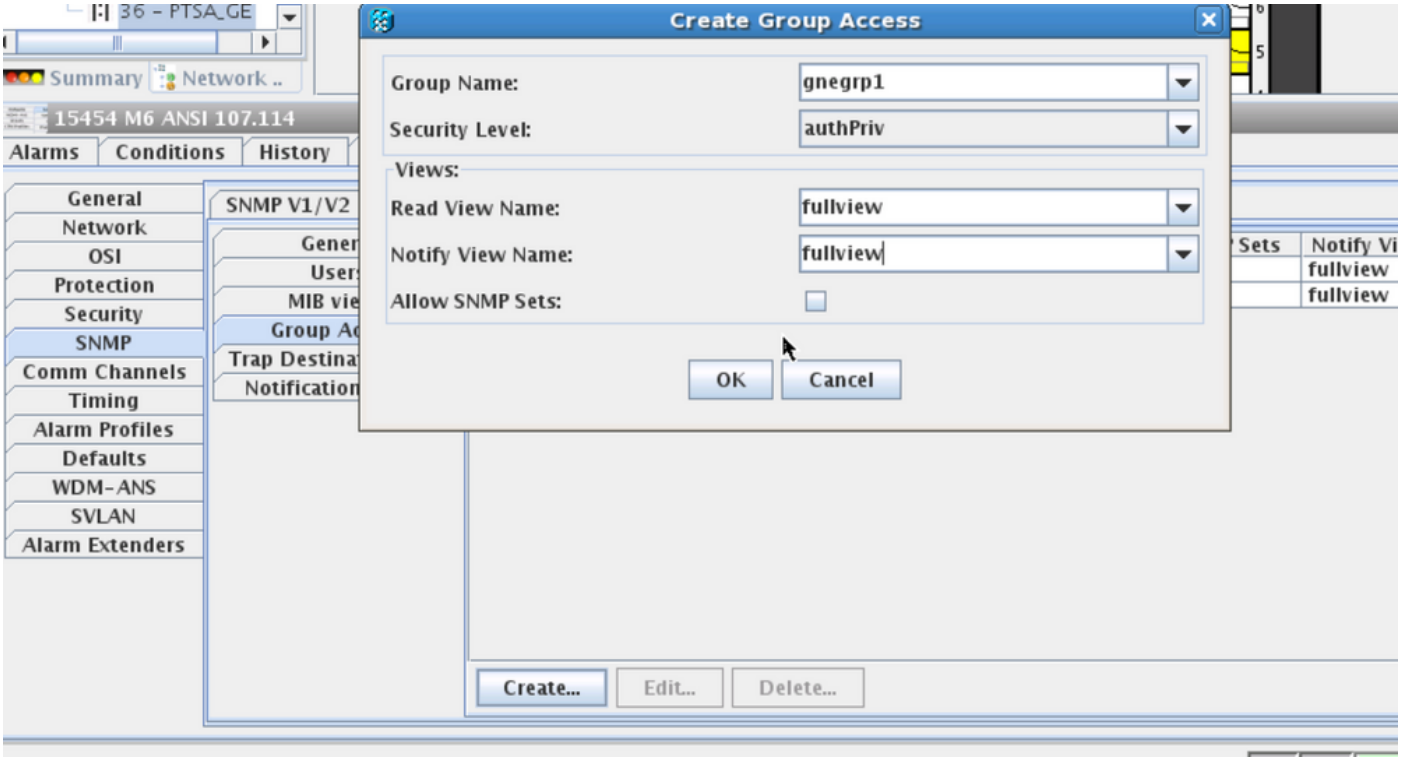
```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number>
```

Trap cmd est identique pour toutes les versions.

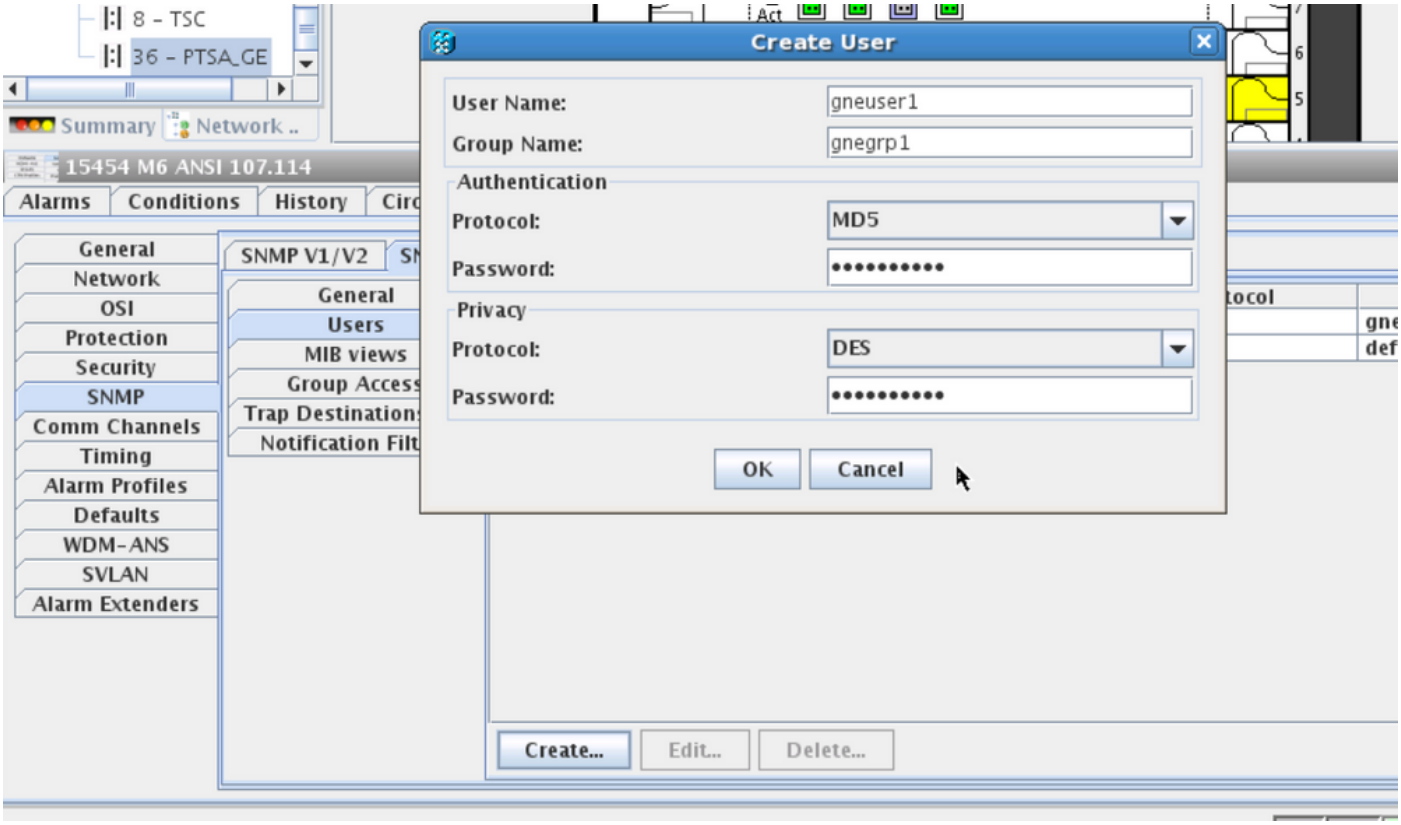
Interruption SNMP V3 pour la configuration GNE/ENE

Sur le noeud GNE

Étape 1. Accéder à **Provisioning > SNMP > SNMP V3 et CCréer un accès au groupe (onglet Accès au groupe) : fournissez un nom de groupe avec le niveau de sécurité (noAuthnoPriv|AuthnoPriv|authPriv) et l'accès en lecture et notification en mode complet, comme indiqué dans l'image.**



Étape 2. Créer un accès utilisateur (onglet Utilisateurs) : créez un utilisateur dont le nom de groupe est identique à celui précédemment créé dans l'onglet Accès au groupe. Fournissez également l'authentification en fonction du niveau d'accès, comme illustré dans l'image.



Étape 3. Onglet Trap Destination(V3) :

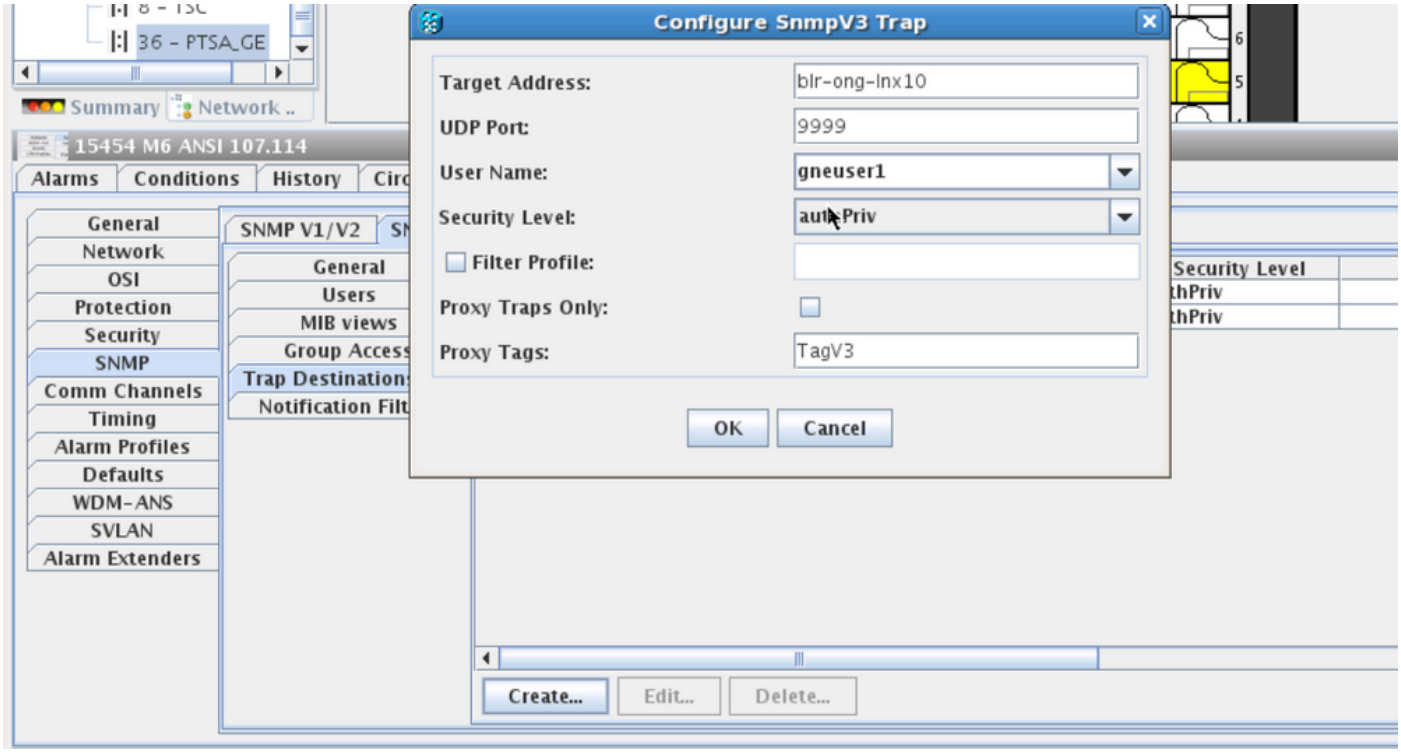
Adresse cible : Adresse du serveur NMS à partir duquel le déroutement sera exécuté (ex. Blr-ong-lnx10).

Port UDP : N'importe quel numéro de port où le déroutement sera écouté(Ex. 9977).

nom de l'utilisateur: Nom de l'utilisateur dans l'onglet Utilisateur.

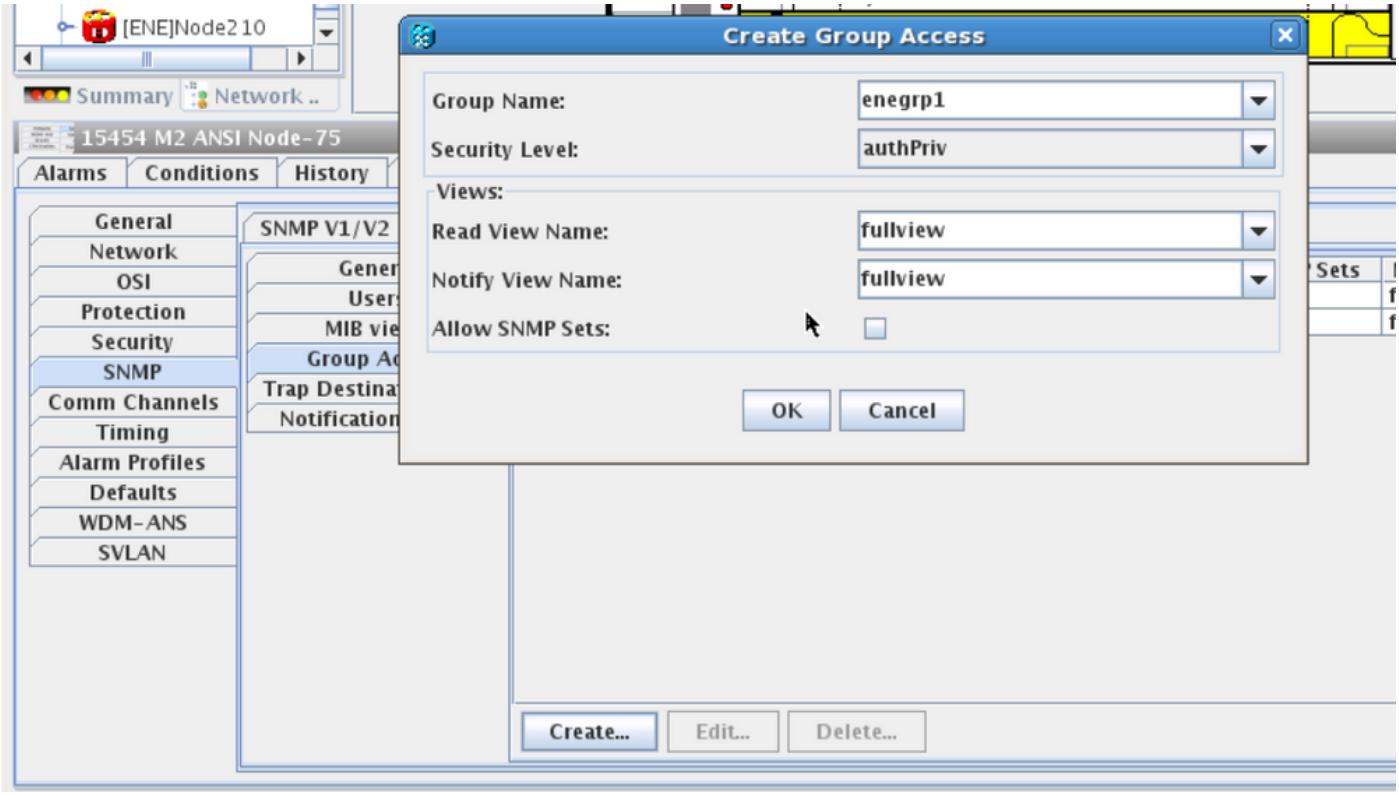
Niveau de sécurité : Tel que configuré précédemment dans l'onglet Utilisateur.

Balises de proxy : Fournir une étiquette proxy (par exemple, Tag75).

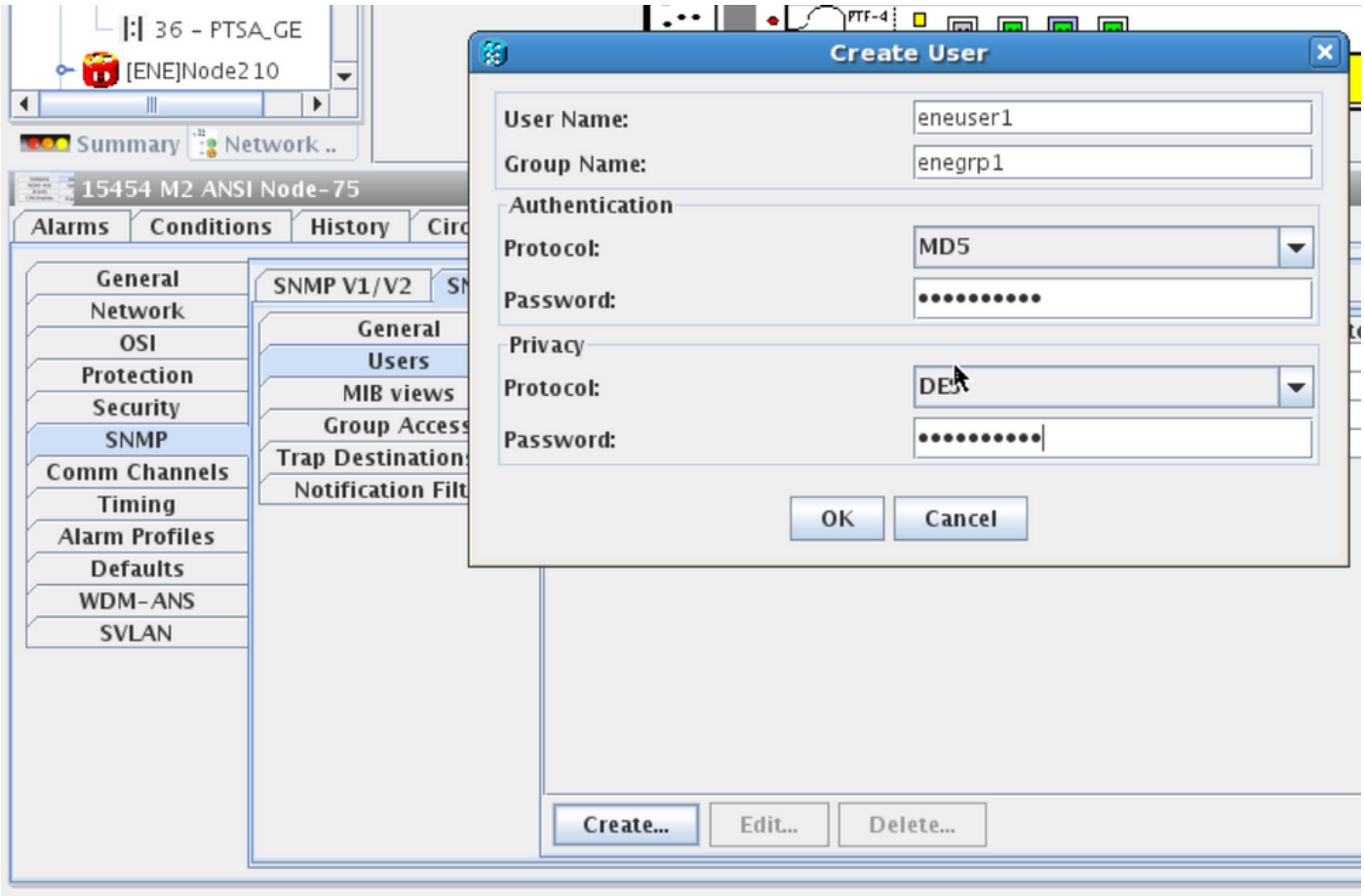


Sur le noeud ENE

Étape 1. Accédez à **Provisioning > SNMP > SNMP V3 et Create Group Access (onglet Group Access) :** fournissez un nom de groupe avec un niveau d'accès (noAuthnoPriv|AuthnoPriv|authPriv) et un accès en lecture et notification en mode complet, comme indiqué dans l'image.



Étape 2. Créer un accès utilisateur (onglet Utilisateurs) : créez un utilisateur dont le nom de groupe est identique à celui précédemment créé dans l'onglet Accès au groupe. Fournissez également l'authentification en fonction du niveau d'accès.



Assurez-vous qu'un groupe par défaut s'il est affiché dans l'onglet Utilisateur est créé dans l'onglet Accès au groupe au cas où il manquerait dans l'onglet Accès au groupe.

Étape 3. Onglet Trap Destination(V3) :

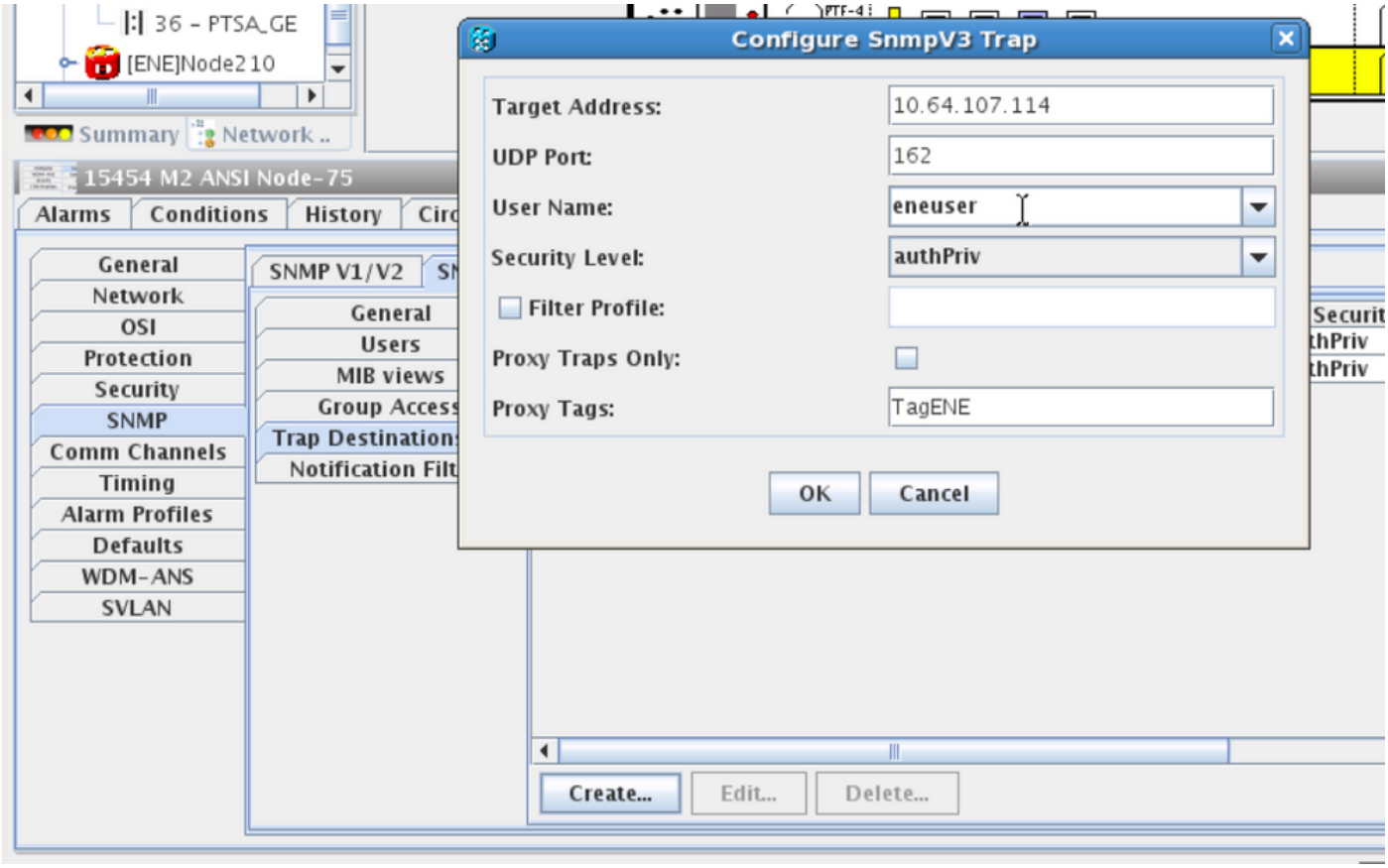
Adresse cible : IP du noeud GNE.

Port UDP : 162.

nom de l'utilisateur: Nom de l'utilisateur dans l'onglet Utilisateur.

Niveau de sécurité : Tel que configuré précédemment dans l'onglet Utilisateur.

Balises de proxy : Fournissez une balise proxy identique à GNE (par exemple, Tag75).



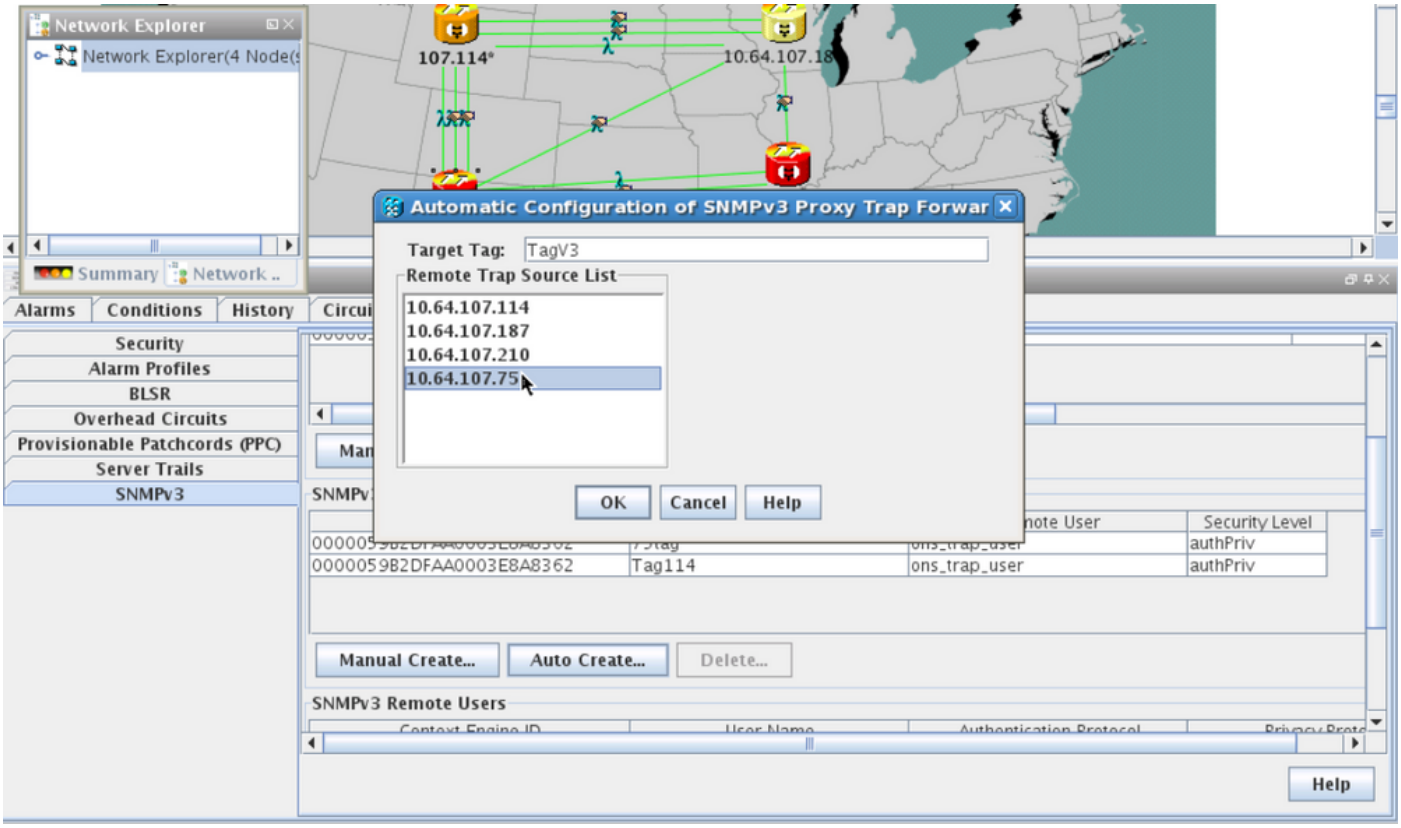
Dans CTC, accédez à la vue réseau :

Étape 1. Accédez à l'onglet **SNMPv3**.

Étape 2. Table de transfert de déroutement du proxy SNMPv3 : Vous pouvez effectuer **Manual** ou **Auto Create**.

Sélectionnez **Créer automatiquement**. En vertu de cette disposition :

- Balise cible : Balise proxy définie dans GNE.
- Liste des sources de déroutement distantes : sélectionnez l'adresse IP du noeud ENE comme indiqué dans l'image.



Vérifier la configuration GNE/ENE

Configurer le serveur NMS (blr-ong-lnx10) :

Étape 1. Dans votre répertoire personnel du serveur, créez un répertoire et nommez-le **snmp**.

Étape 2. Sous ce répertoire, créez un fichier **snmptrapd.conf**.

Étape 3. Dans **snmptrapd.conf**, créez cette configuration :

```
createUser -e 0x
```

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

Interruption SNMP :

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

snmpwalk on ENE :

Pour le mode authpriv :

```
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>
```

Pour le mode authnopriv :

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

Pour le mode noauthnopriv :

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

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.