Configurer SNMPv3 sur les périphériques Cisco ONS15454/NCS2000

Contenu

Introduction Conditions préalables Conditions requises **Components Used** Configuration Sur un noeud autonome/multitablette Configurer le mode authPriv sur le périphérique ONS15454/NCS2000 Configurer le serveur NMS (blr-ong-lnx10) Vérifier le mode authPriv Configurer le mode authNoPriv sur le périphérique ONS15454/NCS2000 Vérifier le mode authNoPriv Configurer le mode noAuthNoPriv sur le périphérique ONS15454/NCS2000 Vérifier le mode noAuthNoPriv Interruption SNMP V3 pour la configuration GNE/ENE Sur le noeud GNE Sur le noeud ENE Vérifier la configuration GNE/ENE Dépannage

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.

	X User Name:	Create User			
	Group Name: Authentication Protocol: Password: Privacy Protocol: Password:	default_group MD5 ******* DES			
Tab View Alarms Conditions History Circuits Pro General Network SNMP V1/V2 SNMP V3	Common	OK Cancel			
OSI General Protection Users Security MIB views SNMP Group Access Comm Channels Trap Destinations(V3) Alarm Profiles Notification Filters Defaults WDM-ANS SVLAN	User Name	Authentication Protocol	Privacy Protocol	Group Name	
Certificate	Create Edit	Delete			

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.

Tab View								
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN								
General Network	SNMP V1/V2 SNMP V3	Common						
QSI	General	View Name	Sub Tree OID	Mask	Type			
Protection	Users	fullview	1	1	included			
Security SNMP Comm Channels Alarm Profiles Defaults	MIB views Group Access Trap Destinations(V3) Notification Filters			·				
WDM-ANS SVLAN								
Certificate		Create Edit	Delete					
	L							

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.

Tab View							
Alarms Conditions	History Circuits Provis	ioning Inventory M	aintenance OTN				
			I I				
General							
Network	SNMP V1/V2 SNMP V3	Common					
OSI	Conoral						
Protection	General	Group Name	Security Level	Read View Access	Allow SNMP Sets	Notify View Access	
Convitu	Users	default_group	authPriv	fullview		fullview	
security	MIB views						
SNMP	Group Access						
Comm Channels	Trap Destinations(V3)						
Alarm Profiles	Notification Filters						
Defaults							
WDM-ANS							
SVLAN							
Certificate		Create Edit.	Delete				
_							

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.

	L			- 000
	Configure SnmpV3 Trap		×	
	Target Address:	bir-ong-inx10		6
	UDP Port:	4545		5
	User Name:	ank	· ·	4
	Security Level:	authPriv	· ·	з
Tak Man	Filter Profile:			
Alarms Conditions History Circuits	Proxy Traps Only:			
Gamaral	Proxy Tags:			
Network SNMP V1/V2 S		OK Cancel	-	
OSI General				Level Filter Profile
Protection Users				
Security MIB views				
SNMP Group Access				
Comm Channels Trap Destinations	((/3)			
Timing Notification Filt	ers			
Alarm Profiles				
Defaults	4			
WDM-ANS	Create	Delete		
SVLAN	Createn	Deletem		
Alarm Extenders	·			

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.

Tab View	
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN	
General Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server Legal Disclaimer UN Access Protection NA Access: Front Craft & E Restore Timeout: 5 - minute(s)	Pseudo IOS Access Access State: Non-sec •
SNNP Comm.Channels. Disable IPv4 access for IPv6 enabled ports Alarm Profiles Defaults	Port: 65000 EMS Access
WDM-ANS PACES state Inter-sec SVLAN Telnet Port: 23 Use Standard Port	CCC CORRA (IIOP) Listene Port Default - TCC Fixed Standard Constant (683)
Enable Shell Password	Other Constant:
Access State: Non-sec *	Access State: Secure •
Other PM Clearing Privilege: Provisioni *	Serial Craft Access Image: Serial Craft Port

Étape 2. Accédez au serveur NMS et effectuez snmpwalk.

Syntaxe:

```
snmpwalk -v 3 -1 authpriv -u <user name> -a MD5 -A <password> -x DES -X <password> <node IP>
<MIE>
Exemple:
blr-ong-lnx10:151> snmpwalk -v 3 -1 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.

Tab View		1_
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN General Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server OSI Protection Security Telnet Port: 23 Use Standard Port	Legal Disclaimer Access state: TCC CORBA (IIOP) Listener Port	Apply Reset Help
Comm. Channels. Enable Snell Password Alarm.Profiles. Defaults WDM-ANS Access State: Non-sec • SVLAN Other PM Clearing Privilege: ProvisionI •	Other Constant: SNMP Access Access State: Non-sec ▼ Serial Craft Access ☑ Enable Craft Port	¥

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

		· · · · · · · · · · · · · · · · · · ·	
	Create User	×	
	User Name:	ank1	
	Group Name:	default_group	5
	Authentication		
	Protocol:	MD5 👻	
	Password:	skaladerakederake	3
Tab View	Privacy		
Alarms Conditions History Circuit	Protocol:	NONE	
	Password:		
General SNMP V1/V2			
Network	OK	Cancel	
Protection			Group Name
Security MIB view:	ank MD5	DES	default_group
SNMP Group Acce	255		
Comm Channels Trap Destinatio	ns(V3)		
Timing Notification F	ilters		
Alarm Profiles			
Defaults			
SVLAN	Create Edit Delet	2	
Alarm Extenders			

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.

	Create Group Access		×	
	Group Name: Security Level:	default_group authNoPriv	•	
	Views:			
Tab View	Read View Name:	fullview	· ·	
Alarms Conditions History Circuits Provisi	Notify View Name:	fullview		
General SNMP V1/V2 SNMP V3	Allow SNMP Sets:			
Protection Users		OK Cancel	fy 1	/iew Access
Security MIB views			V	
SNMP Group Access				
Comm Channels Trap Destinations(V3)				
Timing Notification Filters				
Alarm Profiles				
Defaults				
WDM-ANS	Create Edit Delete			
SVLAN	Column Column Deleter	J		
Alarm Extenders				

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.

	Carforn Carry 10 Tarr			
	Configure SnmpV3 Trap	~	7	
	Target Address:	blr-ong-Inx10		
	UDP Port:	4565	5	
	User Name:	ank1 *	4	
	Security Level:	suthNoPriv 👻	3	
	✓ Filter Profile:			1
Tab View	Proxy Traps Only:			/ _×
Alarms Conditions History Circuits	Proxy Tags:			
General SNMD V1A/2				
Network	OK	Cancel		
Protection Users			Level Filter Profile Name	Proxy Traps Only
Security MIB views	64.103.217.88 4545 a	authPriv		
SNMP Group Acces	5			
Comm Channels Trap Destination	1(V3)			
Alarm Profiles				
Defaults	•			
WDM-ANS	Create Edit Delete			Help
Alarm Extenders	L			

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 ankl -a MD5 -A ciscol23 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:
```

 $\label{eq: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.

			100 1	-		
	Create	User			×	
	G			[7
	User	Name:		ank2		• • • • • • • • • • • • • • • • • • •
	Grou	p Name:		default_group		6
	Aut	hentication				4
	Prot	ocol:		NONE	*	
	Pass	word:				3
Tab View	Priv	acy				
Alarma Conditions History Circuit	Prot	ocol:		NONE	*	
Manns Conditions Pristory Cencule	Pass	word:				
General						
Network SNMP V1/V2			ОК	Cancel		
OSI General						Group Name
Protection		ank	MD5		DES	default group
Security MIB view:	;	ank1	MD5		NONE	default_group
SNMP Group Acce	55					
Comm Channels Trap Destinatio	ns(V3)					
Timing Notification F	ilters					
Alarm Profiles						
Defaults						
WDM-ANS		Create Edit	Delete			
SVLAN	L					
Alarm Extenders						

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

Tab Viev	N										
Alarms	Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN										
	General										
	Network.	SNMP V1	L/V2 SNM	IP V3	Common						
	OSL		General	_	View Nam	e	Sub Tree OID		Mask	Туре	
	Security		Users MIB views		fullview		1	1		included	
	SNMP	G	roup Access								
Com	m Channels	Trap [Destinations	(V3)							
Ala	rm Profiles	Noti	fication Filte	rs							
	Detaults										
	ertificate				Create	Edit	Delete				
				L							
	L										

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

	(Create G	roup Access				×	7	
		Group Name:			default_group 💌		-	•	
		Security	Level:		noAuth	NoPriv	· -	•	
		Views:						4	
		Read V	iew Name:		fullview	1	*	3	
		Notify	View Name:		fullview	r			
Tab View					_				
Alarms Conditions	History Circ	Allow S	SNMP Sets:						
General	SNIN4D VILAZ			ОК	Cancel				
Network	SIMIAIN ATLAS								
IZO	General	_	Group Name	Security Le	vel A	Read View Access	Allow SNMP Set	s Notify View Access	_
Protection	Users		default group	authPriv	PCI /	fullview		fullview	
Security	MIB views	5	default group	authNoPriv		fullview		fullview	
SNMP	Group Acce	:55							
Comm Channels	Trap Destinatio	ns(V3)							
Timing	Notification F	ilters							
Alarm Profiles									
Defaults									
WDM-ANS			Create Edit	Delete					
SVLAN			Creatern	Deleter					
Alarm Extenders									

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.

	Confi	gure SnmpV3 Tra	p		×	
	Tar	get Address:		blr-ong-lnx10		6
	UDF	P Port:		4576		6
	Use	r Name:		ank2	~	4
	Sec	urity Level:		noAuthNoPriv	~	3
		Filter Profile:				-
Tab View	Pro	xy Traps Only:				
Alarms Conditions History	Circuits	xy Tags:				
General						
Network	ATLAS 2		ОК	Cancel		
	General				/ Level	
Protection	Users	64.103.217.88	4545	ank	authPriv	
Security	MIB views	64.103.217.88	4565	ank1	authNoPriv	
SNMP	Group Access					
Comm Channels Trap	Destinations(V3)					
Timing	tification Filters					
Alarm Profiles						
Defaults		1				
WDM-ANS						
SVLAN		Create	Edit Delete			
Alarm Extenders						

Vérifier le mode noAuthNoPriv

Étape 1. Accédez au serveur NMS et effectuez snmpwalk.

```
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 SNMPP:
```

```
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

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

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.

- 1:1 36 - PTS	A_GE 🚽	8		Create Gro	oup Access			
🚥 Summary 📲 Ne	Summary 🗒 Network Group 1		ame:		gnegrp1	-	Ë.	
15454 M6 ANS	107.114	Security	Level:		authPriv	-		
Alarms Conditio	ns History	Views:					-	
General	SNMP V1/V2	Read Vie	w Name:		fullview	-		
OSI	Gener	Notify V	iew Name:		fullview	-	Sets	Notify Vi
Protection	User:	Allow Ch	MD Cate					fullview
Security		Allow SP	IMP Sets:					runnen
SNMP	Group Ac				•			
Comm Channels	Notification			ок	Cancel			
Timing	Notification							
Alarm Profiles	L							
Defaults								
WDM-ANS								
SVLAN								
Alarm Extenders								
			Create	Edit Del	ete			

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.

 : 8 - TSC : 36 - PTSA III Summary [™]:: Net 	A_GE	ジ User Name: Group Name:	Creat:	gneuser1	×	
Alarms Condition General Network	107.114 hs History Circ SNMP V1/V2 St	Authentication Protocol: Password:		MD5	•	
OSI Protection Security SNMP	General Users MIB views Group Access Trap Destination:	Privacy Protocol: Password:		DES	-	gne def
Timing Alarm Profiles Defaults WDM-ANS	Notification Filt		ОК	Cancel 🍂		
Alarm Extenders						
		Create	Edit Del	ete		

Étape 3. Onglet Trap Destination(V3) :

Adresse cible : Adresse du serveur NMS à partir duquel le déroutement sera exécuté (ex. Blr-onglnx10).

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).

- 1- 8 - 15C - 11 36 - PTS	A_GE	\$D	Configure SnmpV3 Trap	×	l l l l l l l l l l l l l l l l l l l
		Target Address:	blr-ong-lnx10		<mark>┌──</mark> s
Summary Summary Ne	etwork	UDP Port:	9999		
Alarms Condition	ns History Circ	User Name:	gneuser 1	•	
General	SNMP V1/V2 St	Security Level:	aut k Priv	-	
Network	General	Eilter Profile:			Security Level
Protection	Users MIR views	Proxy Traps Only:			thPriv thPriv
Security	Group Access	Proxy Tags:	TagV3		
SNMP	Trap Destination	rioxy rugs.			
Comm Channels	Notification Filt				
Alarm Profiles			OK Cancel		
Defaults					
WDM-ANS	_				_
SVLAN					
Alarm Extenders					
		4			
		Create	Edit Delete		
	L				

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.

				,		<u></u>
ENE]Node2	10 -	8	Create Gr	oup Access	×	
Summary 📲 Ne	etwork	Group Name:		enegrp1	-	
15454 M2 ANS	l Node-75	Security Level:		authPriv	•	_
Alarms Condition	ns History	Views:				
General	SNMP V1/V2	Read View Name:		fullview	-	
OSI	Gener	Notify View Name:		fullview	-	Sets
Protection	MIR vie	Allow SNMP Sets				1
Security	Group Ac	Allow Shini Sees.	•			
SNMP	Tran Destina					
Comm Channels	Notification		OK	Cancel		
Timing	Notification					
Alarm Profiles	L					1
Defaults						
WDM-ANS						
SVLAN						
		Create	Edit De	lete		

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.

- 1:1 36 - PTS • 📆 [ENE]Node2	A_GE	\$) \$)	●P⊓F-4 Creat	e User	×
Summary : Network		User Name: Group Name:		eneuser1 enegrp1	
Alarms Conditio	ns History Circ	Protocol:		MD5	
Network OSI Protection Security SNMP	General Users MIB views Group Access	Privacy Protocol: Password:		DE*	
Comm Channels Timing Alarm Profiles Defaults	Trap Destination Notification Filt		ОК	Cancel	
WDM-ANS SVLAN					
		Create	Edit Del	ete	

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).

- 1:1 36 - PTSA	CE 🗐			
		🕄 Co	onfigure SnmpV3 Trap	
Condition General	Node-75 SNMP V1 /V2	Target Address: UDP Port: User Name: Security Level:	10.64.107.114 162 eneuser <u>χ</u> authPriv	
Network OSI Protection Security SNMP Comm Channels Timing Alarm Profiles Defaults	General Users MIB views Group Access Trap Destination Notification Filt	Filter Profile: Proxy Traps Only: Proxy Tags:	TagENE OK Cancel	Securit thPriv thPriv
WDM-ANS SVLAN		✓ Create Edit	III Delete	

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.

Network Explorer 🛛 🗙	107.114° 107.114° 10.64.107.18 Automatic Configuration of SNMPv3 Proxy Trap Forwar ×	
	Target Tag: TagV3	
Summary 🐩 Network	Remote Trap Source List	
Alarms Conditions History	Circui 10.64.107.114	
Security	00000. 10.64.107.187	
Alarm Profiles	10.64.107.210	
BLSR	10.04.107.73	
Overhead Circuits		
Provisionable Patchcords (PPC)	Man	
Server Trails		
SNMPv3	SNMPv. OK Cancel Help	
		note User Security Level
	0000059820FA40003E848362 Tag114 ons trap user	authPriv
	Manual Create Delete SNMPv3 Remote Users Context Engine ID User Name Authentie	cation Protocol Prince Protocol

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.