# Configurar SNMPv3 nos dispositivos Cisco ONS15454/NCS2000

# Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Configurar Em um nó autônomo/de vários prateleiras Configurar o modo authPriv no dispositivo ONS15454/NCS2000 Configurar o servidor NMS (blr-ong-lnx10) Verificar o modo authPriv Configurar o modo authNoPriv no dispositivo ONS15454/NCS2000 Verificar o modo authNoPriv Configurar o modo noAuthNoPriv no dispositivo ONS15454/NCS2000 Verificar modo noAuthNoPriv Configuração de armadilha SNMP V3 para GNE/ENE No nó GNE No nó ENE Verificar a configuração do GNE/ENE **Troubleshoot** 

# 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.

	X User Name:	Create User			
	Group Name: Authentication Protocol: Password: Privacy Protocol:	default_group MD5 *******	· ·		
Tab View Alarms Conditions History Circuits Pro General SNMP V1/V2 SNMP V3	Password:	OK Cancel			
OSI General Protection Users Security MIR 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			

### 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.

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

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.

Tab View							
Alarms Conditions	History Circuits Provis	ioning Inventory M	faintenance OTN				
General	SNMP V1/V2 SNMP V3	Common					
Protection	General	Group Name	Security Level	Read View Access	Allow SNMP Sets	Notify View Access	
Socurity	Users	default_group	authPriv	fullview		fullview	
SNIMP	MIB views						
Comm Channels	Group Access						
Alarm Profiles	Trap Destinations(V3)						
Defaults	Notification Filters						
WDM_ANS							
SVI AN							
Cartificate		Create	Delete				
		Creatern	Delete				
L							

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.

	000	• • • •	
	Configure SnmpV3 Trap		×
	Target Address:	blr-ong-lnx10	7
	UDP Port:	4545	5
	User Name:	ank 🔻	4
	Security Level:	authPriv -	3
Tak Mana	Eilter Profile:		
Alarms Conditions History Circuits	Proxy Traps Only:		
	Proxy Tags:		
General SNMP V1/V2 S	ОК	Cancel	
OSI General			/Level Filter Profile
Protection Users			
SNMP Group Access			
Comm Channels Trap Destinations	(/3)		
Timing Notification Filte	ers		
Defaults			
WDM-ANS	Create Edit Delete		
SVLAN			

Nota: blr-ong-Inx10 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:



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 ciscol23 -x DES -X 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: (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 SNIMP:

snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\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.

Tab View	,	
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN		
General Users Active Logins Policy Data Comm Access RADIUS Server TACACS Serve	r Legal Disclaimer	
	ACCESS State. INVIT-Sec	
Protection	TCC CORBA (IIOP) Listener Port	
Security Telnet Port: 23 Use Standard Port	Default - TCC Fixed  Reset	
SNMP	O Standard Constant (683)	
Comm Channels Enable Shell Password	Other Constant:	
Alarm Profiles	Child Assess	
Defaults ILL Access	Access State: Non-sec *	
WDM-ANS Other	Sarial Craft Accase	
Certificate PM Clearing Privilege: Provisioni *	Enable Craft Port	
	▼ Endote Charton	

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

		1	
	Create User	×	
	User Name:	ank1	6
	Group Name:	default_group	5
	Authentication		
	Protocol:	MD5 *	
	Password:	stealacturatestation	3
Tab View	Privacy		
Alarms Conditions History Circuit	Protocol:	NONE	
	Password:		
General SNMP V1/V2			
Network	0	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 De	ete	
Alarm Extenders			

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

Tab View								
Alarms Conditions History Circuits Prov	Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN							
General SNMP V1/V2 SNMP V3	Common							
OSI General	View Name	Sub Tree OID	Mask	Туре				
Security MIB views	fullview	1	1	included				
SNMP Group Access Comm Channels Tran Destinations(V3)								
Alarm Profiles Notification Filters								
WDM-ANS								
SVLAN	Create Edit	Delete						
		Deleten						

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

	Create Group Access		×
	Group Name: Security Level:	default_group authNoPriv	• •
Tab View         Alarms       Conditions         General       Circuits         Network       SNMP V1/V2         OSI       General         Protection       Users         SNMP       Group Access         Comm Channels       Trap Destinations(V3)         Timing       Notification Filters         Alarm Profiles       Defaults         WDM-ANS       SVLAN	Views: Read View Name: Notify View Name: Allow SNMP Sets: Create Edit Delete	fullview       fullview       OK       Cancel	Image: state

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

				1
	Configure SnmpV3 Trap	× .		
	Target Address:	blr-ong-Inx10	7	
	UDP Port:	4565	6	
	User Name:	ank1 💌	4	
	Security Level:	authNoPriv 💌	3	
	Filter Profile:			
Tab View	Proxy Traps Only:			/ _×
Alarms Conditions History Circuits	Proxy Tags:			
General SNMP V1/V2	ОК	Cancel		]
OSI General			Level Filter Profile Name	Proxy Traps Only
Security MIB views	64.103.217.88 4545	ank authPriv		
SNMP Group Acce	55			
Comm Channels Trap Destinatio	ns(V3)			
Timing Notification F	ilters			
Alarm Profiles				
WDM-ANS	•			<b></b>
SVLAN	Create Edit Delete			Help
Alarm Extenders	L			

### 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 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
Interceptação SNMP:
```

#### 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.

			100	-		103	
	Create	User			×		
	User	Name:		ank?			
	0701	i vonte.		VIIKe			6
	Grou	ıp Name:		default_group			5
	Aut	thentication					4
	Prof	tocol:		NONE	-		
	Pas	sword:					3
Tak Mara	Priv	vacv					
	Prot	tocol:		NONE	•		
Alarms Conditions History Circuit	Dac	sword					
General	F d).	300010.					
Network SNMP V1/V2				Cancel			
I I I I I I I I I I I I I I I I I I I				Cancer			
Protection						_	Group Name
Security MID city		ank	MD5		DES		default_group
SNMP		ank1	MD5		NONE		default_group
Comm Chappels	55						
Timina	ns(V3)						
Alama Das Glass	lters						
Alarm Profiles							
Defaults							
WDM-ANS		Create Edit	Delete				
SVLAN	l						
Alarm Extenders							

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

Tab View								
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN								
General SNMP V1/V2 SNMP V3	Common							
Protection Users	View Name	Sub Tree OID	Mask	Туре				
Security MID closes	fullview	1	1	included				
SNMP Crown Access								
Comm Channels								
Alarm Profiles								
Defaults								
WDM-ANS								
SVLAN								
Certificate	Create Edit	Delete						

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

		Create G	Froup Access				×	7		
		Group Name:			default_group 💌			6		
		Security	y Level:	n	noAuthl	NoPriv	-	°		
		Views	:					4		
		Read \	/iew Name:	f	ullview		*	3		
		Notify	View Name:	f	ullview					
Tab View				-	_					
Alarms Condition	IS History Circ	Allow	SNMP Sets:	L						
						_				
General	SNIMD VI A/2			ок С	ancel					
Network	SINIVIP #1/#2					-				
IZO	General		Group Name	Security Leve	A I	Read View Access	Allow SNMP S	iets Ni	otify View Access	_
Protection	Users		default group	authPriv	.1 ~	fullview		fully	iew	
Security	MIB view	rs .	default group	authNoPriv		fullview		fully	iew.	-
SNMP	Group Acc	ess	acroant_group				0			
Comm Channels	Trap Destinatio	ons(V3)								
Timing	Notification	Filters								
Alarm Profiles										
Defaults										
WDM-ANS			Create	Delete						
SVLAN			Create	Deleten						
Alarm Extenders										

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

	Config	gure SnmpV3 Tra	р		×		8
	Targ	jet Address:		blr-ong-lnx10			6
	UDP	Port:		4576			5
	User	Name:		ank2	-		4
	Secu	irity Level:		noAuthNoPriv	•		3
		Filter Profile:					4
Tab View	Prox	y Traps Only:					
Alarms Conditions History Circuits	Prox	y Tags:					
General SNMD V1 A/2							
Network			ОК	Cancel			
OSI General						/ Level	
Protection Users		64.103.217.88	4545	ank	authPriv		
Security MIB views		64.103.217.88	4565	ank1	authNoPri	v	
SNMP Group Acce	55						
Comm Channels Trap Destination	ns(V3)						
Timing Notification Fi	lters						
Alarm Profiles							
Defaults		4					
WDM-ANS		Create	Edit Delete				
SVLAN		Create	Deleten				
Alarm Extenders							

### Verificar modo noAuthNoPriv

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

```
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:
```

```
\label{eq:snmptrapd-f-lo-OQ-Ob-Ot-F} $$V\n&B\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

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

#### 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.

-  :  36 - PTS	A_GE	<b>1</b> 0	Create Group Access	×	6
Summary 📲 Ne	twork	Group Name:	gnegrp1	<b></b>	
15454 M6 ANS	107.114	Security Level:	authPriv		
Alarms Condition	ns History [	Views:			
General	SNMP V1/V2	Read View Name:	fullview		
OSI	Gener	Notify View Name:	fullview	-	Sets Notify Vi
Protection	User: MIR via	Allow SNMP Sate			fullview
Security		Allow SIMIF Sets.			
SNMP	Tran Destina		<b>b</b>		
Comm Channels	Notification		OK Cancel		
Timing	Notrication				
Alarm Profiles	L				
Defaults					
WDM-ANS					
SVLAN					
Alarm Extenders					
		Create E	dit Delete		
	[	N.			

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.

— <b> : </b> 8 – ТSC — <b> : </b> 36 – РТSA		8	Creat	e User	×	
Summary Re	twork	User Name: Group Name:		gneuser1 gnegrp1		
Alarms Condition	107.114 History Circ	Authentication Protocol:		MD5		
Network OSI Protection	General Users MIB views	Password: Privacy Protocol:		DES		tocol gn dei
Security SNMP Comm Channels	Group Access Trap Destination Notification Filt	Password:		·····		
Alarm Profiles Defaults WDM-ANS			ОК	Cancel		
SVLAN Alarm Extenders						
		Create	Edit Del	ete		

Etapa 3. Guia Destino da interceptação (V3):

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

8 - ISC   36 - PTS	A.GE	<b>1</b>	Configure SnmpV3 Trap	×	
4		Target Address:	blr-ong-lnx10		s s
Summary Revealed Ansi	etwork	UDP Port:	9999		<b></b> .
Alarms Condition	ns History Circ	User Name:	gneuser1	-	
General	SNMP V1/V2 St	Security Level:	aut <mark>e</mark> Priv	-	
Network OSI	General	Filter Profile:			Security Level
Protection	Users MIB views	Proxy Traps Only:			thPriv
Security	Group Access	Proxy Tags:	TagV3		
Comm Channels	Notification Filt				
Alarm Profiles			OK Cancel		
Defaults WDM-ANS	L				1
SVLAN					
Alarm Extenders					
		•	II		
		Create	Edit Delete		

### 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.

<b>A</b>			· · · · · · · · · · · · · · · · · · ·	,		
enter [ENE]Node2	210	80	Create Gro	oup Access	×	
Summary 🔡 No	etwork	Group Name:		enegrp1	-	
15454 M2 ANS	l Node-75	Security Level:		authPriv	•	_
Alarms Conditio	ns History	Views:				
General	SNMP V1/V2	Read View Name:		fullview	-	
OSL	Gener	Notify View Name:		fullview	-	Sets
Protection	User		•			1
Security		Allow SNMP Sets:	٦			
SNMP	Trap Destina					
Comm Channels Timing	Notification		ОК	Cancel		
Alarm Profiles	l l					J
Defaults						
WDM-ANS						
SVLAN						
		Create	Edit Del	ete		
	L					

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.

- 🖂 36 - PTS		<b>↓</b>	● Creat	e User	×
	<b>I</b>	User Name:		eneuser1	
15454 M2 ANS	I Node-75	Group Name:		enegrp1	
Alarms Conditio	ns History Circ	Protocol:		MD5	-
General Network	SNMP V1/V2 SN	Password:		•••••	
OSI Protection Security SNMP	General Users MIB views Group Access	Privacy Protocol: Password:		DE <b>X</b>	
Comm Channels Timing Alarm Profiles Defaults	Notification Filt		ОК	Cancel	
WDM-ANS SVLAN					
		Create	Edit Del	ete	

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).

PL26 DTSA	CE E			
1. 30 - FISA			Configure SnmpV3 Trap	×
- 🔂 [ENE]Node21	0 🖵 🗖			
		Target Address:	10.64.107.114	
Summary Net	work	UDP Port:	162	
Alarms Conditions	s History Circ	User Name:	eneuser <u>)</u>	<b>_</b>
General	SNMP V1/V2 St	Security Level:	authPriv	<b>•</b>
Network OSI	General	Filter Profile:		Securit
Protection	Users MIB views	Proxy Traps Only:		thPriv
Security	Group Access	Proxy Tags:	TagENE	
Comm Channels	Notification Filt			
Alarm Profiles			OK Cancel	
Defaults				
WDM-ANS				
SVLAN				
		Create	dit Delete	

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.

Network Explorer 🗆 ×	107.114° 107.114° 10.64.107.18 Automatic Configuration of SNMPv3 Proxy Trap Forwar X	
	Target Tag: TagV3	
Summary 🔡 Network	Remote Trap Source List	9.4×
Alarms Conditions History Security Alarm Profiles	Circui 10.64.107.114 10.64.107.187 10.64.107.210	
BLSR	10.64.107.75	
Overhead Circuits		
Provisionable Patchcords (PPC)	Man	
Server Trails		
SNMPv3	SNMPv OK Cancel Help	
		note User Security Level
	0000005982DFAA0003E0A8362 Tag114 ons trap user	authPriv
	Manual Create Auto Create Delete SNMPv3 Remote Users	ication Protocol Drivery Deate
		Help

# 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.