# 在Cisco ONS15454/NCS2000设备上配置 SNMPv3

## 目录

简介 <u>先决条件</u> 要求 使用的组件 配置 在独立/多机架节点上 在ONS15454/NCS2000设备上配置authPriv模式 配置NMS服务器(blr-ong-lnx10) 验证authPriv模式 在ONS15454/NCS2000设备上配置authNoPriv模式 验证authNoPriv模式 在ONS15454/NCS2000设备上配置noAuthNoPriv模式 验证noAuthNoPriv模式 用于GNE/ENE设置的SNMP V3陷阱 在GNE节点上 在ENE节点上 验证GNE/ENE设置 故障排除

## 简介

本文档介绍如何在ONS15454/NCS2000设备上配置简单网络管理协议第3版(SNMPv3)的分步说明 。所有主题都包括示例。

**注意:**本文档中提供的属性列表并非详尽或权威,在不更新本文档的情况下随时可能更改。

## 先决条件

要求

Cisco 建议您了解以下主题:

- 思科传输控制器(CTC)GUI
- •基本服务器知识
- •基本Linux/Unix命令

## 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

## 配置

## 在独立/多机架节点上

#### 在ONS15454/NCS2000设备上配置authPriv模式

步骤1.使用超级用户凭证通过CTC登录节点。

#### 步骤2.导航至"节点"视图>"调配">"SNMP">"SNMP V3"。

步骤3.导航至"用户"选项卡。创建用户。

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> 步骤4.单击"确定",如图所示。

(	×	Create User			
	User Name:	ank default group			
	Authentication Protocol:	MD5			
	Password: Privacy Protocol:	******** DES			
Tab View	Password:				
Alarms Conditions History Circuits Pro General 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	User Name	Authentication Protocol	Privacy Protocol	Group Name	
WDM-ANS SVLAN Certificate	Create Edit	Delete			

规格:

用户名 — 指定连接到代理的主机上的用户名。用户名必须至少为6个字符,最多为40个字符 (TACACS和RADIUS身份验证最多只有39个字符)。 它包含字母数字(a-z、A-Z、0-9)字符,允许 的特殊字符为@、"-"(连字符)和""。 (点)。 为了与TL1兼容,用户名必须为6到10个字符。

组名 — 指定用户所属的组。

身份验证:

- 协议 选择要使用的身份验证算法。选项为NONE、MD5和SHA。
- 密码 如果选择MD5或SHA,请输入密码。默认情况下,密码长度设置为至少八个字符。
- 隐私 启动隐私身份验证级别设置会话,使主机能够加密发送到代理的消息的内容。
- 协议——选择隐私身份验证算法。可用选项为None、DES和AES-256-CFB。
- 密码 如果选择协议(None)以外的协议,请输入密码。

步骤5.确保根据此映像配置MIB视图。

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

规格:

名称 — 视图的名称。

子树OID - MIB子树, 与掩码结合时定义子树系列。

位掩码——不系列视图子树。位掩码中的每个位对应于子树OID的子标识符。

类型 — 选择视图类型。选项包括和排除。

该类型定义子树OID和位掩码组合定义的子树系列是否包含在通知过滤器中或从通知过滤器中排除 。

步骤6.配置组访问,如图所示。默认情况下,组名称将默认组和安全级别为authPriv。

注意:组名应与在步骤3中创建用户时使用的组名相同。

Tab View							
Alarms Conditions	History Circuits Provis	ioning Inventory M	faintenance OTN				
General		Common					
Network	SNMP V1/V2 SNMP V3	Common					
OSI	Ceneral						
Protection	General	Group Name	Security Level	Read View Access	Allow SNMP Sets	Notify View Access	
Fratection	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							
Cartificate		Create	Delete				
certilicate		Creatern	Delete				
	L						

规格:

组名—SNMP组的名称或共享通用访问策略的用户集合。

安全级别 — 为其定义访问参数的安全级别。从以下选项中选择:

noAuthNoPriv — 使用用户名匹配进行身份验证。

AuthNoPriv — 根据HMAC-MD5或HMAC-SHA算法提供身份验证。

AuthPriv — 根据HMAC-MD5或HMAC-SHA算法提供身份验证。除身份验证外,还根据CBC-DES(DES-56)标准提供DES 56位加密。

如果为组选择authNoPriv或authPriv,则必须为相应用户配置身份验证协议和密码、隐私协议和密 码或两者。

#### 视图

读取视图名称 — 读取组的视图名称。

- 通知视图名称 通知组的视图名称。
- 允许SNMP集 如果希望SNMP代理接受SNMP SET请求,请选中此复选框。如果未选中此复选框 ,则SET请求将被拒绝。

注意: SNMP SET请求访问针对极少数对象实施。

步骤7.导航至Node View > Provisioning > SNMP > SNMP V3 > Trap Destination(V3)。单击"创建 并配置"。

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 步骤8.单击"确定",如图所示。

		<mark>••••</mark>		
	Configure SnmpV3 Trap		×	
	Target Address:	bir-ong-inx10		6
	UDP Port:	4545		5
	User Name:	ank	<b>T</b>	4
	Security Level:	authPriv	<b>T</b>	3
	Filter Profile:			
Tab View           Alarms         Conditions         History         Circuits	Proxy Traps Only:			
General SNMP V1/V2 S OSI General	Proxy Tags:	K Cancel		Eilter Drofil
Protection Users Security MIB views SNMP Group Acce	55		y Lever	Filler Profile
Comm Channels Trap Destinatio	ns(V3) ilters			
Alarm Profiles				
WDM-ANS				
SVLAN	Create Edit De	lete		
Alarm Extenders				

注意:blr-ong-Inx10是NMS服务器。

规格:

目标地址 — 陷阱应发送到的目标。使用IPv4或IPv6地址。

UDP端口 — 主机使用的UDP端口号。默认值为 162。

用户名 — 指定连接到代理的主机上的用户名。

安全级别 — 选择以下选项之一:

noAuthNoPriv — 使用用户名匹配进行身份验证。

AuthNoPriv — 根据HMAC-MD5或HMAC-SHA算法提供身份验证。

AuthPriv — 根据HMAC-MD5或HMAC-SHA算法提供身份验证。除身份验证外,还根据CBC-DES(DES-56)标准提供DES 56位加密。

过滤器配置文件 — 选中此复选框并输入过滤器配置文件名称。仅当您提供过滤器配置文件名称并创 建通知过滤器时,才会发送陷阱。

仅代理陷阱(Proxy Traps Only) — 如果选中,则仅从ENE转发代理陷阱。来自此节点的陷阱不会发 送到此条目标识的陷阱目标。

代理标记 — 指定标记列表。仅当ENE需要将陷阱发送到此条目标识的陷阱目标并希望将GNE用作 代理时,才需要在GNE上使用标记列表。

#### 配置NMS服务器(blr-ong-lnx10)

步骤1.在服务器的主目录中,创建名为snmp的目录。

第二步:在此目录下,创建文件snmptrapd.conf。

步骤3.将snmptrapd.conf**文件更**改为:

vi snmptrapd.conf

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

createUser -e 0x0000059B1B00F0005523A71C ank MD5 cisco123 DES cisco123 在本例中:

user\_name=ank

MD5 password = cisco123

DES password = cisco123

Engine ID = can be available from CTC.
Node view > Provisioning > SNMP > SNMP V3 > General

验证authPriv模式

步骤1.在CTC中,导航至Node View > Provisioning > Security > Access > Change snmp access state to Secure,如图所示。

Tab View							
Alarms Conditions	History Circuits Provisioning Inventory Maintenance OTN						
General Network	Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server Legal Disclaimer						
OSI	LAN Access Pseudo IOS Access						
Protection	LAN Access: Front Craft & E *	Access State: Non-sec *					
Security SNMP Comm Channels	Restore Timeout: 5 4 minute(s) Disable IPv4 access for IPv6 enabled ports	Port: 65000					
Alarm Profiles	Shell Arress	EMS Arrass					
Defaults	Access State: Non-sec *	Arress State: Non-Sec *					
SVLAN Certificate	Telnet Port: 23 Use Standard Port	TCC CORA (IIOP) Listener Port					
	Enable Shell Password	Other Constant:					
	TLI Access	SNMP Access					
	ACCESS STATE:	Access state: Jecure					
	Other PM Clearing Privilege: Provisioni *	Serial Craft Access					

#### 步骤2.导航到NMS服务器并执行snmpwalk。

语法:

snmpwalk -v 3 -l authpriv -u <user name> -a MD5 -A <password> -x DES -X <password> <node IP> <MIB> 示例: 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::sysLocation.0 = "" RFC1213-MIB::sysLocation.0 = "" RFC1213-MIB::sysServices.0 = INTEGER: 79 SNMP 陷阱:

snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number> 陷阱cmd对所有版本都相同。

#### 在ONS15454/NCS2000设备上配置authNoPriv模式

步骤1.在CTC中,导航至Node View > Provisioning > Security > Access > Change snmp access state to Non-secure mode,如图所示。

Tab View	/_
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN	
General     Users     Active Logins     Policy     Data Comm     Access     RADIUS Server     TACACS Server       OSL     Protection     Stature     Telnet Port:     23     Use Standard Port       SNMP     Enable Shell Password     Enable Shell Password	Legal Disclaimer
Defaults         TL1 Access           WDM-ANS         Access State:         Non-sec *	SNMP Access Access State: Non-sec
SVLAN Other Certificate PM Clearing Privilege: Provisioni *	Serial Craft Access

步骤2.导航至Node View > Provisioning > SNMP > SNMP V3 > Users > Create User,并按照图中 所示进行配置。

	Create User	×	
	User Name:	ank1	7
	Group Name:	default_group	5
	Authentication		
	Protocol:	MD5 💌	
	Password:	stratestatestate	3
Tak Vinor	Privacy		
	Protocol:	NONE	
Alarms Conditions History Circuit	Password:		
General			
Network SNMP V1/V2	ОК	Cancel	
OSI General			Group Name
Protection	ank MD5	DES	default group
Security MIB views			
SNMP Group Acce	55		
Comm Channels Trap Destination	ns(V3)		
Timing Notification Fi	ilters		
Alarm Profiles			
Defaults			
WDM-ANS	Create Edit Delete		
Alarm Extender			
Alarm extenders			

## 步骤3.确保MIB视图的配置如图所示。

Tab View						
Alarms Conditions	History Circuits Provis	ioning Inventory Mainte	nance OTN			
Network	SNMP V1/V2 SNMP V3	Common				
OSI	General	View Name	Sub Tree OID	Mask	Туре	
Security	Users MIR views	fullview	1	1	included	
SNMP	Group Access					
Comm Channels	Trap_Destinations(V3)					
Alarm Profiles	Notification Filters					
Defaults						
SVI AN						
Certificate		Create Edit	Delete			
	Ll					

步骤4.配置组访问(如图所示)以进行authnopriv模式。

	Create Group Access		×	
	Group Name: Security Level:	default_group authNoPriv	* *	
Tab View         Alarms       Conditions       History       Circuits       Provisi         General       SNMP V1/V2       SNMP V3         OSI       General       Users         Protection       Users       MIB views         SNMP       Group Access       Trap Destinations(V3)         Timing       Notification Filters         Defaults       WText ANG	Views: Read View Name: Notify View Name: Allow SNMP Sets:	fullview fullview OK Cancel	T T	View Access
WDM-ANS SVLAN Alarm Extenders	Create Edit Delete			

步骤5.导航至Node View > Provisioning > SNMP > SNMP V3 > Trap Destination(V3)。单击"创建 并配置",如图所示。

		• • • • • •		
	Configure SnmpV3 Trap	×		
	Target Address:	bir-ong-Inx10		
	UDP Port:	4565	5	
	User Name:	ank1 *	4	
	Security Level:	authNoPriv 🔻	3	
	Filter Profile:			
Tab View	Proxy Traps Only:			<i>د</i> _×
Alarms Conditions History Circuits	Proxy Tags:			
General Network OSI General	ок	Cancel		]
Protection			/ Level Filter Profile Name	Proxy Traps Only
Security MIB views	64.103.217.88 4545 at	nk authPriv		
SNMP Group Acces	ess			
Comm Channels Trap Destination	ons(V3)			
Timing Notification Fi	Filters			
Alarm Profiles				
Defaults	•			•
WDM-ANS	Create Edit Delete			Help
SVLAN				
Alarm Extenders				

### 验证authNoPriv模式

步骤1.导航到NMS服务器并执行snmpwalk。

语法:

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

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

```
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
SNMP 陷阱:
```

snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number> 陷阱cmd对所有版本都相同。

### 在ONS15454/NCS2000设备上配置noAuthNoPriv模式

PLATFORM=15454-M6"

步骤1.在CTC中,导航至Node View > Provisioning > Security > Access > Change snmp access state to Non-secure mode,如图所示。

Tab View	/_: /_:
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN	
General     Users     Active Logins     Policy     Data Comm     Access     RADIUS Server     TACACS Server       OSL     Protection     Status     Invoir-sec     Invoir-sec     Invoir-sec     Invoir-sec       SNMP     Comm     Channels     Enable Shell Password	Legal Disclaimer  Access state:
Defaults         TL1 Access           WDM-ANS         Access State:         Non-sec *           SVLAN         Other         PM Classing Privilence:         *	SNMP Access Access State: Non-sec  Serial Craft Access

步骤2.导航至Node View > Provisioning > SNMP > SNMP V3 > Users > Create User and Configure,如图所示。

			100 1	-			
	Create	User				×	
							7
	User	User Name:		ank2			6
	Grou	up Name:		default_group			6
	Au	thentication					4
	Pro	tocol:		NONE	*	_	-1
	Pas	sword:				_	3
Tah View	Pri	vacy					
Alarma Canditions History Circuit	Pro	tocol:		NONE	*		
Alarms Conditions Pristory Circuit	Pas	sword:					
General							
Network SNMP V1/V2			ОК	Cancel			
OSI General							Group Name
Protection Users		ank	MD5		DES		default group
Security MIB view:	;	ank1	MD5		NONE		default group
SNMP Group Acce	\$\$						
Comm Channels Trap Destinatio	ns(V3)						
Timing Notification F	ilters						
Alarm Profiles							
Defaults							
WDM-ANS		Create Edit	Delete				
Alarma Estan dara	l						
Alarmicklenuers							

## 步骤3.确保**MIB视**图配置如图所示。

Tab View								
Alarms	Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN							
6	Conorol							
Ne	twork	SNMP V1/V2 SNMP V3	Common					
Pro	OSI	General	View Name	Sub Tree OID	Mask	Туре		
Se	curity	MIB views	fullview	1	1	included		
s	NMP	Group Access						
Alarn	n Profiles	Trap Destinations(V3)						
De	efaults							
WD S	WDM-ANS SVI AN							
Cer	rtificate		Create Edit	Delete				

步骤4.配置组访问(如图所示),使其处于noauthnopriv模式。

	c	Create G	roup Access			3	×	7	
Group			Name:	d	default_group 💌			6	
		Security	/ Level:	n	oAuthNoPriv	-	_		
		Views:						4	
		Read V	ïew Name:	fu	ullview	-		3	
		Notify	View Name:	f	ullview	*			
Tab View					2				
Alarms Conditions	History Circ	Allow	SNMP Sets:	L	J				
General	SNMD V1 A/2			ОКСС	ancel				
Network	SINIAL 07165								
IZO	General		Group Name	Security Leve	LA Read View A	ccess Allow SNN	AP Sets	Notify View Access	
Protection	Users		default group	authPriv	fullview			fullview	
Security	MIB views	5	default group	authNoPriv	fullview			fullview	
SNMP	Group Acce	:55							
Comm Channels	Trap Destination	ns(V3)							
Timing	Notification Fi	ilters							
Alarm Profiles									
Defaults									
WDM-ANS			Create	Delete					
SVLAN			Creatern	Deletern					
Alarm Extenders									
	<u></u>								

步骤5.导航至Node View > Provisioning > SNMP > SNMP V3 > Trap Destination(V3)。 单击"**创建** 并**配置**",如图所示。

	Confi	gure SnmpV3 Tr	ар		
	Targ	get Address:		bir-ong-inx10	
	UDF	Port:		4576	6
	Use	r Name:		ank2	• 4
	Sec	urity Level:		noAuthNoPriv	- 3
		Filter Profile:			
Tab View	Pro	xy Traps Only:			
Alarms Conditions History Circuit	s Pro:	xy Tags:			
General Network	s		ОК	Cancel	
OSI General					. I wal
Protection Users		64.103.217.88	4545	ank	authPriv
Security MIB view	15	64.103.217.88	4565	ank1	authNoPriv
SNMP Group Acc	ess				
Timing Notification	ilters				
Alarm Profiles	incerty				
Defaults		4			
WDM-ANS		Create	Edit Delete		
SVLAN	l				
Alarm Extenders					

## 验证noAuthNoPriv模式

步骤1.导航至NMS服务器并执行snmpwalk。

```
snmpwalk -v 3 -1 noauthnopriv -u <user name> <node IP> <MIB>
示例:
blr-ong-lnx10:155> snmpwalk -v 3 -1 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>
SNMP 陷阱:
```

snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" <port number> 陷阱cmd对所有版本都相同。

## 用于GNE/ENE设置的SNMP V3陷阱

#### 在GNE节点上

### 步骤1.导航至 调配> SNMP > SNMP V3和C创建组访问("组访问"选项卡):提供具有安全级别 (noAuthnoPriv|AuthnoPriv|authPriv)和全视图读取和通知访问权限的组名,如图所示。

- 1:1 36 - PTSA_GE		1	Create Gro	oup Access	×	, ,	
Summary 📲 Ne	twork	Group Name:		gnegrp1		5	
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 M	Notify Vi
Protection	MIB vie	Allow SNMP Sets:			f	ullview	
SNMP	Group Ac		k				
Comm Channels	Notification		ОК	Cancel			
Alarm Profiles							
Defaults							
WDM-ANS							
Alarm Extenders							
		Create	Edit Dele	ete			

步骤2.创建用户访问权限(用户选项卡):创建组名与之前在"组访问"选项卡中创建的组名相同的用 户。此外,根据访问级别提供身份验证,如图所示。

–  :  8 - TSC	Act 📟		
- 🛛 36 - PTSA_GE 🚽 💴	Create	user x	[6
Use Summary "R Network	ser Name:	gneuser1	<mark>⊂</mark> s
GI	roup Name:	gnegrp1	
Alarms Conditions History Circ	Authentication		
Alaritis Condicions History Circ	rotocol:	MD5 🗸	
General SNMP V1/V2 St Pa	assword		
Network General	assworu.		tocol
OSI Users Pi	rivacy		gne
Security MIB views Pr	rotocol:	DES	def
SNMP Group Access	assword:	•••••	
Comm Channels Trap Destination			
Timing Notification Filt	OK	Cancel	
Alarm Profiles	UK	Cancer	
Defaults			_
WDM-ANS			
Alarm Extenders			
Alarm Extenders			
	Create Edit Dele	ete	

步骤3.陷阱目标(V3)选项卡:

目标地址:将运行陷阱的NMS服务器的地址(例如Blr-ong-Inx10)。

UDP 端口:将侦听陷阱的任何端口号(例如9977)。

用户名:"用户"(User)选项卡中的用户名称。

安全级别:如之前在"用户"选项卡中配置的。

代理标记:提供代理标记(例如Tag75)。

I·I 8 - ISC  :  36 - PTSA_GE ↓	🕅 Con	figure SnmpV3 Trap	X	
Summary <sup>2</sup> Network	Target Address:	bir-ong-inx10		<mark></mark> s
15454 M6 ANSI 107.114	UDP Port:	9999		
Alarms Conditions History C	rc User Name:	gneuser1	-	
General SNMP V1/V2	Security Level:	aut <mark>h</mark> Priv	-	
Network General	Filter Profile:			Security Level
Protection Users	Proxy Traps Only:			thPriv thPriv
Security Group Acce	ss Proxy Tags:	TagV3		
Comm Channels Notification F				
Alarm Profiles		OK Cancel		
Defaults WDM_ANS				
SVLAN				
Alarm Extenders				
	•	III		
	Create Edit	Delete		

### 在ENE节点上

步骤1.导航至**Provisioning > SNMP > SNMP V3和Create Group Access(Group Access选项卡** ):提供具有访问级别(noAuthnoPriv|AuthnoPriv|authPriv)和全视图读取和通知访问权限的组名 ,如图所示。

					1 /		-	<del></del>
- 📅 [ENE]Node2	10 -	<b>10</b>		Create G	iroup Access	<b>&gt;</b>	•	
Summary 📲 Ne	twork	Group Na	me:		enegrp1	-		
15454 M2 ANS	l Node-75	Security L	evel:		authPriv	-	E	
Alamis Conditio		Views:					E	
General	SNMP V1/V2	Read View	v Name:		fullview	-		
OSI	Gener	Notify Vie	w Name:		fullview	-	15	iets 1
Protection	MIB vie	Allow SN	MP Sets:	k			E	1
Security	Group Ac							
Comm Channels	Trap Destina			OK	Cancel			
Timing	Notification			UK	Callee			
Alarm Profiles	L							
Defaults WDM_ANG								
WDM-ANS SVLAN								
JVEAN	•							
		[	Create	Edit D	elete			
	L							

步骤2.创建用户访问权限(用户选项卡):创建组名与之前在"组访问"选项卡中创建的组名相同的用 户。此外,根据访问级别提供身份验证。

- 1: 36 - PTS	A_GE	•-119	
- CENEINode2	10 -	🕄 Creat	e User 🛛 🗙
Summary "" Ne	etwork	User Name: Group Name:	eneuser1
Alarms Condition	l Node-75 ns History Circ	Authentication	
		Protocol:	MD5
General Network	SNMP V1/V2 SN	Password:	•••••
OSI Protection Security SNMP	General Users MIB views Group Access	Privacy Protocol: Password:	
Comm Channels Timing Alarm Profiles Defaults WDM-ANS SVLAN	s Notification Filt	OK Create Edit De	Cancel

如果显示在"用户"选项卡中,则确保在"组访问"选项卡中创建default\_group,以防"组访问"选项卡中 缺少它。

步骤3.陷阱目标(V3)选项卡:

目标地址:GNE节点IP。

UDP 端口:162.

用户名:"用户"(User)选项卡中的用户名称。

安全级别:如之前在"用户"选项卡中配置的。

代理标记:提供与GNE相同的任何代理标记(例如Tag75)。

- 1. SO - PISALGE	😥 Co	Configure SnmpV3 Trap				
► 11 [ENE]Node210						
	Target Address:	10.64.107.114				
Summary Retwork	UDP Port:	162				
Alarms Conditions History Cire	User Name:	eneuser 🗎	<b>_</b>			
General SNMP V1/V2 S	Security Level:	authPriv	<b>_</b>			
OSI General	Filter Profile:		Securit			
Protection Users MIB views	Proxy Traps Only:		thPriv			
SNMP Group Acces	Proxy Tags:	TagENE				
Comm Channels Notification File		OK Cancel				
Alarm Profiles		OK Cancel				
WDM-ANS						
SVLAN						
	•					
	Create Edit.	Delete				

在CTC中,导航至网络视图:

步骤1.导航至SNMPv3选项卡。

第二步: SNMPv3代理陷阱转发器表:可以执行手动或自动创建。

选择"**自动创建**"。在这种情况下:

- •目标标记:在GNE中设置代理标记。
- •远程陷阱源列表:选择ENE节点IP,如图所示。

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	a + ×
Alarms Conditions History Security Alarm Profiles BLSR Overhead Circuits Provisionable Patchcords (PPC) Server Trails	Circui 10.64.107.114 10.64.107.187 10.64.107.210 10.64.107.75	
SINMEVS	OK         Cancel         Help           000005982DFAA0003E8A8362         7 Stag         015_trap_user	note User Security Level authPriv r authPriv
	Manual Create Delete SNMPv3 Remote Users Context Engine ID User Name Authors	ication Protocol Prince Protocol

### 验证GNE/ENE设置

配置NMS服务器(blr-ong-lnx10):

步骤1.在服务器的主目录中,创建一个目录并将其命名为snmp。

第二步:在此目录下,创建文**件snmptrapd.conf**。

第三步:在snmptrapd.conf中,创建以下配置:

createUser -e 0x

Engine\_NO = can be available from CTC. Open GNE node-->Node view->Provisioning->SNMP->SNMP V3-->General. SNMP 陷阱:

snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" ENE上的snmpwalk:

### 对于身份验证模式:

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>
对于authnopriv模式:

snmpwalk -v 3 -l authnopriv -u <user\_name> -a MD5 -A <auth\_password> -E <ene\_engine\_id>
<gne\_ip\_address> <OID>

## 对于noauthnopriv模式:

snmpwalk -v 3 -l authpriv -u

## 故障排除

目前没有针对此配置的故障排除信息。