Configuración de SNMPv3 en dispositivos Cisco ONS15454/NCS2000

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Configurar En un nodo independiente/de varias estanterías Configuración del modo authPriv en el dispositivo ONS15454/NCS2000 Configuración del servidor NMS (blr-ong-lnx10) Verificar el modo authPriv Configuración del modo authNoPriv en el dispositivo ONS15454/NCS2000 Verificar el modo authNoPriv Configuración del modo noAuthNoPriv en el dispositivo ONS15454/NCS2000 Verificar el modo noAuthNoPriv Trampa SNMP V3 para la configuración GNE/ENE En el nodo GNE En el nodo ENE Verificar la configuración de GNE/ENE **Troubleshoot**

Introducción

Este documento describe instrucciones paso a paso sobre cómo configurar el protocolo simple de administración de red versión 3 (SNMPv3) en dispositivos ONS15454/NCS2000. Todos los temas incluyen ejemplos.

Nota: La lista de atributos proporcionada en este documento no es exhaustiva ni fidedigna y podría cambiar en cualquier momento sin actualizar este documento.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- GUI de Cisco Transport Controller (CTC)
- Conocimiento básico del servidor
- Comandos Linux/Unix básicos

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

En un nodo independiente/de varias estanterías

Configuración del modo authPriv en el dispositivo ONS15454/NCS2000

Paso 1. Inicie sesión en el nodo a través de CTC con las credenciales de superusuario.

Paso 2. Vaya a Vista de nodos > Provisioning > SNMP > SNMP V3.

Paso 3. Vaya a la pestaña Usuarios. Crear usuarios.

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>

Paso 4. Haga clic en Aceptar como se muestra en la imagen.

	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			

Especificaciones:

Nombre de usuario: especifique el nombre del usuario en el host que se conecta al agente. El nombre de usuario debe tener un mínimo de 6 y un máximo de 40 caracteres (hasta sólo 39 caracteres para la autenticación TACACS y RADIUS). Incluye caracteres alfanuméricos (a-z, A-Z, 0-9) y los caracteres especiales permitidos son @, "-" (guión) y "." (punto). Para la compatibilidad con TL1, el nombre de usuario debe tener entre 6 y 10 caracteres.

Group Name (Nombre de grupo): especifique el grupo al que pertenece el usuario.

Autenticación:

Protocol (Protocolo): Seleccione el algoritmo de autenticación que desea utilizar. Las opciones son NONE, MD5 y SHA.

Password (Contraseña): Introduzca una contraseña si selecciona MD5 o SHA. De forma predeterminada, la longitud de la contraseña se establece en un mínimo de ocho caracteres.

Privacidad: inicia una sesión de configuración de nivel de autenticación de privacidad que permite al host cifrar el contenido del mensaje que se envía al agente.

Protocol (Protocolo): Seleccione el algoritmo de autenticación de privacidad. Las opciones disponibles son None, DES y AES-256-CFB.

Password (Contraseña): Introduzca una contraseña si selecciona un protocolo distinto de None (Ninguno).

Paso 5. Asegúrese de que las vistas MIB estén configuradas según esta imagen.

ab View								
Alarms Conditions	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					

Especificaciones:

Nombre: nombre de la vista.

OID de subárbol - El subárbol MIB que, cuando se combina con la máscara, define la familia de subárboles.

Máscara de bits: una familia de subárboles de vista. Cada bit de la Máscara de Bit corresponde a un sub-identificador del OID del subárbol.

Type (Tipo): Seleccione el tipo de vista. Las opciones se incluyen y excluyen.

El tipo define si la familia de subárboles definidos por el OID del subárbol y la combinación de Máscara de bits se incluyen o se excluyen del filtro de notificación.

Paso 6. Configure el acceso de grupo como se muestra en la imagen. De forma predeterminada, el nombre de grupo será default_group y el nivel de seguridad como authPriv.

Nota: El nombre de grupo debe ser el mismo que el utilizado al crear el usuario en el paso 3.

Tab View							
Alarms Conditions	History Circuits Provis	ioning Inventory M	laintenance OTN				
Ceneral							
Network	SNMP V1/V2 SNMP V3	Common					
QSI	General	Crown Name	Security Level	Road View Accord	Allow SNMD Sote	Notify View Access	
Protection	Users	default_group	authPriv	fullview		fullview	
Security	MIB views						
Comm Channels	Group Access						
Alarm Profiles	Notification Filters						
Defaults							
WDM-ANS							
SVLAN		Create	Delete				
		Creatern	Deleten				
	L						

Especificaciones:

Group Name (Nombre de grupo): nombre del grupo SNMP o colección de usuarios que comparten una política de acceso común.

Nivel de seguridad: nivel de seguridad para el que se definen los parámetros de acceso. Seleccione entre estas opciones:

noAuthNoPriv: utiliza una coincidencia de nombre de usuario para la autenticación.

AuthNoPriv - Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA.

AuthPriv - Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA. Proporciona cifrado DES de 56 bits basado en el estándar CBC-DES (DES-56), además de autenticación.

Si selecciona authNoPriv o authPriv para un grupo, el usuario correspondiente debe configurarse con un protocolo de autenticación y una contraseña, con protocolo de privacidad y contraseña, o ambos.

Vistas

Leer el nombre de la vista: leer el nombre de la vista del grupo.

Notificar nombre de vista: notifica el nombre de vista del grupo.

Allow SNMP sets (Permitir conjuntos SNMP): Active esta casilla de verificación si desea que el agente SNMP acepte solicitudes SNMP SET. Si esta casilla de verificación no está activada, se rechazarán las solicitudes SET.

Nota: El acceso de solicitud SNMP SET se implementa para muy pocos objetos.

Paso 7. Vaya a Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3). Haga clic en Crear y 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

Paso 8. Haga clic en Aceptar como se muestra en la imagen.

	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 es el servidor NMS.

Especificaciones:

Dirección de destino: Destino al que se deben enviar las trampas. Utilice una dirección IPv4 o IPv6.

Puerto UDP: número de puerto UDP que utiliza el host. El valor predeterminado es 162.

Nombre de usuario: especifique el nombre del usuario en el host que se conecta al agente.

Nivel de seguridad: seleccione una de estas opciones:

noAuthNoPriv: utiliza una coincidencia de nombre de usuario para la autenticación.

AuthNoPriv - Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA.

AuthPriv - Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA. Proporciona cifrado DES de 56 bits basado en el estándar CBC-DES (DES-56), además de autenticación.

Filter Profile (Perfil de filtro): active esta casilla de verificación e introduzca el nombre del perfil de filtro. Las trampas se envían sólo si se proporciona un nombre de perfil de filtro y se crea un filtro de notificación.

Proxy Traps Only (Sólo capturas de proxy): si se selecciona, sólo reenvía las trampas de proxy
del ENE. Las trampas de este nodo no se envían al destino de trampa identificado por esta
entrada.

Etiquetas de proxy: especifique una lista de etiquetas. La lista de etiquetas es necesaria en un GNE sólo si un ENE necesita enviar trampas al destino de trampa identificado por esta entrada y

desea utilizar el GNE como proxy.

Configuración del servidor NMS (blr-ong-lnx10)

Paso 1. En el directorio de inicio del servidor, cree un directorio con el nombre snmp.

Paso 2. Bajo este directorio, cree un archivo snmptrapd.conf.

Paso 3. Cambie el archivo snmptrapd.conf a:

vi snmptrapd.conf createUser -e 0xEngine ID <user_name>< MD5> <password > DES <password> Por ejemplo: createUser -e 0x0000059B1B00F0005523A71C ank MD5 cisco123 DES cisco123 En este ejemplo: user_name=ank MD5 password = cisco123 DES password = cisco123

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

Verificar el modo authPriv

Paso 1. En CTC, navegue hasta **Node View > Provisioning > Security > Access > change snmp** access state to Secure como se muestra en la imagen.

Tab View	
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN	
General Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server Lega OSU LAN Access Protection LAN Access: Front Craft & E Storrity	al Disclaimer Pseudo IOS Access Access State: Non-sec
SNMP Restore filmeou. S inimiaecis) Comm Channels Disable IPv4 access for IPv6 enabled ports Alarm Profiles Shell Access	Port: 65000 EMS Access
WDM-ANS Access State: Non-sec *	Access State: Non-sec *
SVLAN Teinet Port: 23 Use Standard Port	Default - TCC Fixed Standard Constant (683)
Enable Shell Password	Other Constant:
TLI Access Access State: Non-sec *	SNMP Access Access State: Secure •
Other PM Clearing Privilege: Provisioni *	Serial Craft Access Image: Serial Craft Port

Paso 2. Navegue hasta el servidor NMS y haga snmpwalk.

Sintaxis:

<MIB> Ejemplo:

```
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
Trampa 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 es el mismo para todas las versiones.

Configuración del modo authNoPriv en el dispositivo ONS15454/NCS2000

Paso 1. En CTC, navegue hasta **Node View > Provisioning > Security > Access > change snmp** access state to Non-secure mode como se muestra en la imagen.



Paso 2. Vaya a **Node View > Provisioning > SNMP > SNMP V3 > Users > Create User** y configure como se muestra en la imagen.

		· · · · · · · · · · · · · · · · · · ·	
	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			

Paso 3. Asegúrese de que las vistas MIB estén configuradas como se muestra en la imagen.

Tab Vie	W									
Alarms	Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN									
	General Network	SNN	MP V1/V2 SNMP V3	1	Common					
	QSI		General	1	View Name	Sub Tree OID		Mask	Type	
	Protection		Users	1	fullview	1		1	included	
	Security		MIB views				_			
	SNMP		Group Access							
Con	nm Channels		rap Destinations(V3)							
Ali	arm Profiles		Notification Filters	11						
	Defaults									
	VDM-ANS									
	SVLAN			ΙL						
	Certificate				Create Edit	Delete				
				L						
							_			

Paso 4. Configure Group Access como se muestra en la imagen para el modo authnopriv.

			6	
	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 OSI General Users Users	Allow SNMP Sets:	OK Cancel	fy V	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				
Alarm Extenders				

Paso 5. Vaya a **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Haga clic en **Crear** y **Configurar** como se muestra en la imagen.

	Configure SnmpV3 Trap	×		
	Target Address: UDP Port:	bir-ong-inx10 4565		
Tak 16	Security Level:	authNoPriv V	3	
Alarms Conditions History Circuits General	Proxy Traps Only: Proxy Tags:			r _2
Network SNMP V1/V2 S OSI General Protection Users	OK 64.103.217.88 4545	Cancel	/ Level Filter Profile Name	Proxy Traps Only
Security MIB views SNMP Group Acce Comm Channels Trap Destination	ss 1s(V3)			
Liming Notification Fi Alarm Profiles Defaults WDM-ANS	<			•
SVLAN Alarm Extenders	Create Edit Delete			Help

Verificar el modo authNoPriv

Paso 1. Navegue hasta el servidor NMS y haga snmpwalk.

Sintaxis:

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

```
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
```

```
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
Trampa SNMP:
```

PLATFORM=15454-M6"

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 es el mismo para todas las versiones.

Configuración del modo noAuthNoPriv en el dispositivo ONS15454/NCS2000

Paso 1. En CTC, navegue hasta **Node View > Provisioning > Security > Access > change snmp** access state to Non-secure mode como se muestra en la imagen.

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

Paso 2. Vaya a Node View > Provisioning > SNMP > SNMP V3 > Users > Create User and Configure como se muestra en la imagen.

			100	-			
	Create	User			×		
	User	Name:		ank2			
	Grou	p Name:		default_group		6	
	Aut	hentication				4	
	Prot	ocol:		NONE	-		
	Pass	word:				3	
Tak Mary	Priv	acv					
	Prot	ocol:		NONE	•		
Alarms Conditions History Circuit	Pass	word:				L	
General							
Network SNMP V1/V2			ОК	Cancel			
OSI General							- No
Protection Users		ank	MD5		DES	default o	roup
Security MIB view	s	ank1	MD5		NONE	default g	roup
SNMP Group Acce	255						- op
Comm Channels Trap Destinatio	ns(V3)						
Timing Notification F	ilters						
Alarm Profiles							
Defaults							
WDM-ANS		Create Edit	Delete				
SVLAN	L						
Alarm Extenders							

Paso 3. Asegúrese de que las vistas MIB se configuran como se muestra en la imagen.

Paso 4. Configure el acceso de grupo como se muestra en la imagen para el modo no authnopriv.

		Create G	Froup Access			×	7	
		Group	Name:	default	t_group		6	
		Security	y Level:	noAut	nNoPriv			
		Views	:				4	
		Read \	/iew Name:	fullviev	N	*	3	
		Notify	View Name:	fullviev	N			
Tab View		All	Chill 4D Color					
Alarms Condition	ns History Circ	Allow	SNIMP Sets:	U				
					_			
General	SNMP V1/V2			OK Cancel				
Network								
IZO	General		Group Name	Security Level A	Read View Access	Allow SNMP Sets	Notify View Access	_
Protection	Users		default_group	authPriv	fullview		fullview	
Security	MIB view	IS	default group	authNoPriv	fullview		fullview	
SNMP	Group Acc	ess						
Comm Channels	Trap Destination	ons(V3)						
Timing	Notification	Filters						
Alarm Profiles								
Defaults								
WDM-ANS			Create	Delete				
SVLAN			Create	Deleten				
Alarma Estandaria								
Alarm Extenders								

Paso 5. Vaya a **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Haga clic en **Crear** y **Configurar** como se muestra en la imagen.

	Config	gure SnmpV3 Tra	р		×		8
	Targ	get Address:		blr-ong-lnx10			6
	UDP	Port:		4576			6
	User	Name:		ank2 💌			4
	Secu	urity Level:		noAuthNoPriv	-		3
7 1 12		Filter Profile:					1
Tab View	Prox	y Traps Only:					
	Prox	y Tags:					
General SNMP V1/V2 S							
OSI General			OK	Cancel			
Protection Users		64.103.217.88	4545	ank	authPriv	/ Level	
Security MIB views		64.103.217.88	4565	ankl	authNoPri	v	
Comm Channels Tran Destination	ss hs(\/3)						
Timing Notification Fi	lters						
Alarm Profiles							
Defaults		•					
SVLAN		Create	Edit Delete				
Alarm Extenders							

Verificar el modo noAuthNoPriv

Paso 1. Navegue hasta el servidor NMS y haga snmpwalk.

```
snmpwalk -v 3 -1 noauthnopriv -u <user name> <node IP> <MIB>
Ejemplo:
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>
Trampa 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 es el mismo para todas las versiones.
```

Trampa SNMP V3 para la configuración GNE/ENE

En el nodo GNE

Paso 1. Vaya a Provisioning > SNMP > SNMP V3 y CCrear acceso de grupo (ficha Acceso de grupo): proporcione un nombre de grupo con el nivel de seguridad (noAuthnoPriv|AuthnoPriv|authPriv) y la vista completa Leer y notificar acceso, como se muestra en la imagen.

- : 36 - PTS	A_GE	1 0	Create Group Access	×	6
Summary 📲 Ne	twork	Group Name:	gnegrp1		
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		
Comm Channels	Notification		OK Cancel		
Timing	Notrication				
Alarm Profiles	L				
Defaults					
WDM-ANS					
SVLAN					
Alarm Extenders					
		Create E	dit Delete		
	[N.			

Paso 2. Crear acceso de usuario (ficha Usuarios): cree un usuario con el mismo nombre de grupo que el creado anteriormente en la ficha Acceso de grupo. También, proporcione la autenticación basada en el nivel de acceso como se muestra en la imagen.

8 - TSC 36 - PTS/	A_GE ▼ twork	SUSER Name:	FiliAn 🛄 Creat	gneuser1	×		
Alarms Condition	107.114 ns History Circ	Authentication Protocol:		MD5	-		
Network OSI	General	Password: Privacy		•••••		tocol	and
Protection Security	MIB views Group Access	Protocol:		DES	-		def
SNMP Comm Channels	Trap Destination Notification Filt	Password:		·····			
Alarm Profiles			ОК	Cancel			
WDM-ANS SVLAN							
Alarm Extenders							
		Create	Edit Del	ete			

Paso 3. Ficha Destino de trampa (V3):

Dirección de destino: Dirección del servidor NMS desde el que se ejecutará la trampa(p. ej. Blrong-Inx10).

Puerto UDP: Cualquier número de puerto en el que se escuche la trampa(p. ej. 9977).

User Name: Nombre del usuario en la ficha Usuario.

Nivel de seguridad: Tal y como se configuró anteriormente en la ficha Usuario.

Etiquetas de proxy: Proporcione una etiqueta de proxy (p. ej. Tag75).

- 1- 8 - 15C - 1: 36 - PTS	A_GE	鍧	Configure SnmpV3 Trap	×	
		Target Address:	bir-ong-inx10		s -
15454 M6 ANS	107.114	UDP Port:	9999		
Alarms Conditio	ns History Circ	User Name:	gneuser1	-	
General	SNMP V1/V2 St	Security Level:	auth Priv	-	
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				
SVLAN					
Alarm Extenders					
		4			
		Create	Edit Delete		

En el nodo ENE

Paso 1. Vaya a **Provisioning > SNMP > SNMP V3** y **Create Group Access** (Ficha Group Access): proporcione un nombre de grupo con acceso de nivel de acceso (noAuthnoPriv|AuthnoPriv|authPriv) y vista completa Leer y notificar, como se muestra en la imagen.

				,		
ENE]Node2	10 -	9	Create Gr	oup Access	×	
Summary 🚏 Ne	twork	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	User MIR vie	Allow SNMP Sets				
Security	Croup Ac	Allow SIMME Sets.	1			
SNMP	Tran Destina					
Comm Channels	Notification		ОК	Cancel		
Timing	Notification					
Alarm Profiles	L]
Defaults						
WDM-ANS						
SVLAN						
		Create	Edit De	lete		

Paso 2. Crear acceso de usuario (ficha Usuarios): cree un usuario con el mismo nombre de grupo que el creado anteriormente en la ficha Acceso de grupo. También, proporcione la autenticación basada en el nivel de acceso.

- 1:1 36 - PTS		8)	●PTF-4] Creat	e User	×
Summary	etwork	User Name:		eneuser1	
Alarms Conditio	l Node-75 ns History Circ	Group Name: Authentication		enegrp1	
General Network	SNMP V1/V2 St	Protocol: Password:		MD5	
OSI Protection Security	Users MIB views Group Access	Privacy Protocol: Passavord:		Dest	
Comm Channels Timing Alarm Profiles	Trap Destination: Notification Filt	1 4550010.	ОК	Cancel	
Defaults WDM-ANS					
JULAN	-				
		Create	Edit Del	ete	

Asegúrese de que se cree un grupo_predeterminado si se muestra en la ficha Usuario en la ficha Acceso de grupo en caso de que falte en la ficha Acceso de grupo.

Paso 3. Ficha Destino de trampa (V3):

Dirección de destino: IP del nodo GNE.

Puerto UDP: 162.

User Name: Nombre del usuario en la ficha Usuario.

Nivel de seguridad: Tal y como se configuró anteriormente en la ficha Usuario.

Etiquetas de proxy: Proporcione cualquier etiqueta proxy igual que GNE (p. ej. Tag75).

- 11 36 - PTS				
		🕄 Co	nfigure SnmpV3 Trap	×
CENEJNode2	etwork	Target Address: UDP Port:	10.64.107.114 162	
Alarms Conditio	ns History Circ SNMP V1/V2 St	User Name: Security Level:	authPriv	
OSI Protection Security	General Users MIB views Group Access	Filter Profile: Proxy Traps Only:		Securit thPriv thPriv
SNMP Comm Channels Timing Alarm Profiles Defaults	Trap Destination Notification Filt	Troxy Tays.	OK Cancel	
WDM-ANS SVLAN				
		Create Edit.	Delete	

En CTC, vaya a la vista de red:

Paso 1. Vaya a la pestaña SNMPv3.

Paso 2. Tabla de Reenvío de Trampa de Proxy SNMPv3: Puede hacer Manual o Auto Create.

Seleccione Auto Create. En ese sentido:

- Etiqueta objetivo: Etiqueta proxy establecida en GNE.
- Lista de origen de trampa remota: seleccione la IP del nodo ENE como se muestra en la imagen.

Network Explorer 🛛 🗙	107.114° 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	000000. 10.64.107.187	
Alarm Profiles	10.64.107.210	
BLSR	10.04.107.75	
Overhead Circuits		
Provisionable Patchcords (PPC)	Man	
Server Trails		
SNMPv3	SNMPV OK Cancel Help	
	00000	note User Security Level
	000005982DFAA0003E8A8362 Tag114 ons trap user	authPriv
	Manual Create Delete SNMPv3 Remote Users Context Engine ID User Name Authentic	cation Protocol Prince Protocol V

Verificar la configuración de GNE/ENE

Configuración del servidor NMS (blr-ong-lnx10):

Paso 1. En el directorio de inicio del servidor, cree un directorio y asígnele el nombre snmp.

Paso 2. Bajo este directorio, cree un archivo snmptrapd.conf.

Paso 3. En snmptrapd.conf, cree esta configuración:

createUser -e 0x

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

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

Para el modo 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>
Para el modo authnopriv:

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

Para el modo noauthnopriv:

snmpwalk -v 3 -l authpriv -u

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.