# Configurazione di SNMPv3 sui dispositivi Cisco ONS15454/NCS2000

## Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Configurazione Su un nodo autonomo/multipiattaforma Configurazione della modalità authPriv sul dispositivo ONS15454/NCS2000 Configurazione del server NMS (blr-ong-lnx10) Verifica modalità authPriv Configurazione della modalità authNoPriv sul dispositivo ONS15454/NCS2000 Verifica modalità authNoPriv Configurazione della modalità noAuthNoPriv su un dispositivo ONS15454/NCS2000 Verifica modalità noAuthNoPriv Trap SNMP V3 per configurazione GNE/ENE Su nodo GNE Su nodo ENE Verifica configurazione GNE/ENE Risoluzione dei problemi

## Introduzione

Questo documento descrive le istruzioni dettagliate su come configurare il protocollo SNMPv3 (Simple Network Management Protocol versione 3) sui dispositivi ONS15454/NCS2000. Tutti gli argomenti includono esempi.

**Nota:** L'elenco degli attributi fornito in questo documento non è esaustivo né autorevole e può essere modificato in qualsiasi momento senza un aggiornamento del documento.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- GUI Cisco Transport Controller (CTC)
- Conoscenze base dei server
- Comandi Linux/Unix di base

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

Su un nodo autonomo/multipiattaforma

Configurazione della modalità authPriv sul dispositivo ONS15454/NCS2000

Passaggio 1. Accedere al nodo tramite CTC con le credenziali di Utente avanzato.

Passaggio 2. Passare a Vista nodo > Provisioning > SNMP > SNMP V3.

Passaggio 3. Passare alla scheda Utenti. Creare utenti.

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> Passaggio 4. Fare clic su OK come mostrato nell'immagine.

	X User Name: Group Name:	Create User ank default_group			
	Authentication Protocol: Password: Privacy Protocol:	MDS *******	• •		
Tab View       Alarms     Conditions       General     SNMP V1/V2       Network     SNMP V1/V2	Password:	OK Cancel			
OSI General Protection Users Security MIR views SNMP Group Access Comm Channels Alarm Profiles Defaults WDM-ANS SVLAN	User Name	Authentication Protocol	Privacy Protocol	Group Name	
Certificate	Create Edit	Delete			

#### Specifiche:

Nome utente: specificare il nome dell'utente sull'host che si connette all'agente. Il nome utente deve contenere da un minimo di 6 a un massimo di 40 caratteri (fino a un massimo di 39 caratteri per l'autenticazione TACACS e RADIUS). Include caratteri alfanumerici (a-z, A-Z, 0-9) e i caratteri speciali consentiti sono @, "-" (trattino) e "." (punto). Per la compatibilità con TL1, il nome utente deve contenere da 6 a 10 caratteri.

Nome gruppo: specificare il gruppo a cui appartiene l'utente.

Autenticazione:

Protocollo: selezionare l'algoritmo di autenticazione che si desidera utilizzare. Le opzioni sono NONE, MD5 e SHA.

Password: immettere una password se si seleziona MD5 o SHA. Per impostazione predefinita, la lunghezza della password è impostata su un minimo di otto caratteri.

Privacy - Avvia una sessione di impostazione del livello di autenticazione della privacy che consente all'host di crittografare il contenuto del messaggio inviato all'agente.

Protocollo: selezionare l'algoritmo di autenticazione della privacy. Le opzioni disponibili sono None, DES e AES-256-CFB.

Password: immettere una password se si seleziona un protocollo diverso da Nessuno.

Passaggio 5. Verificare che le visualizzazioni MIB siano configurate in base a questa immagine.

Fab View								
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN								
General SNMP V1/V2 SNMP V3	Common							
OSI General	View Name	Sub Tree OID	Mask	Type				
Protection Users	fullview	1	1	included				
SNMP Group Access								
Comm Channels Trap Destinations(V3)								
Alarm Profiles Notification Eilters								
Defaults								
WDM-ANS								
SVLANCertificate	Create Edit	Delete						

Specifiche:

Nome: nome della vista.

OID sottoalbero (Subtree OID) - Sottoalbero MIB che, se combinato con la maschera, definisce la famiglia di sottoalberi.

Maschera di bit - Famiglia di sottoalberi di visualizzazione. Ogni bit nella maschera di bit corrisponde a un identificatore secondario dell'OID della sottostruttura.

Tipo (Type) - Consente di selezionare il tipo di vista. Le opzioni sono Incluso ed Escluso.

Il tipo definisce se la famiglia di sottostrutture definite dalla combinazione di OID sottostruttura e Maschera di bit vengono incluse o escluse dal filtro di notifica.

Passaggio 6. Configurare l'accesso al gruppo come mostrato nell'immagine. Per impostazione predefinita, il nome del gruppo sarà default\_group e il livello di protezione authPriv.

**Nota:** Il nome del gruppo deve essere uguale a quello utilizzato quando si crea l'utente nel passaggio 3.

Tab View							
Alarms Conditions	History Circuits Provis	ioning Inventory M	aintenance OTN				
General							
Network	SNMP V1/V2 SNMP V3	Common					
051	Convert						
Brotestion	General	Group Name	Security Level	Read View Access	Allow SNMP Sets	Notify View Access	
Protection	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				
L							

Specifiche:

Nome gruppo: il nome del gruppo SNMP o della raccolta di utenti che condividono un criterio di accesso comune.

Livello di protezione: il livello di protezione per il quale vengono definiti i parametri di accesso.

Selezionare una delle seguenti opzioni:

noAuthNoPriv - Utilizza un nome utente corrispondente per l'autenticazione.

AuthNoPriv: fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA.

AuthPriv: fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA. Crittografia DES a 56 bit basata sullo standard CBC-DES (DES-56), oltre all'autenticazione.

Se si seleziona authNoPriv o authPriv per un gruppo, l'utente corrispondente deve essere configurato con un protocollo di autenticazione e una password, con protocollo di privacy e password o entrambi.

Visualizzazioni

Read View Name: nome della visualizzazione di lettura per il gruppo.

Notifica nome vista - Notifica il nome della vista per il gruppo.

Consenti set SNMP: selezionare questa casella di controllo se si desidera che l'agente SNMP accetti le richieste SET SNMP. Se questa casella di controllo non è selezionata, le richieste SET vengono rifiutate.

Nota: L'accesso alle richieste SET SNMP è implementato per un numero limitato di oggetti.

Passaggio 7. Passare a Vista nodo > Provisioning > SNMP > SNMP V3 > Destinazione trap (V3). Fare clic su Create and Configure (Crea e configura).

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

Passaggio 8. Fare clic su OK come mostrato nell'immagine.

	00	J —   — — —   • • • •   — — —	000
	Configure SnmpV3 Trap		×
	Target Address:	blr-ong-lnx10	
	UDP Port:	4545	5
	User Name:	ank	• 4
	Security Level:	authPriv	▼ 3
T-1-1-1/2	Filter Profile:		
Alarms Conditions History Circuits	Proxy Traps Only:		_
	Proxy Tags:		
Network	OK	Cancel	
OSI General			/Level Filter Profile
Protection Users			
SNMP Group Access			
Comm Channels Trap Destinations	(V3)		
Timing Notification Filt	ers		
Alarm Profiles			
WDM-ANS	•		
SVLAN	Create Edit Delet	à	
Alarm Extenders	L		

Nota: blr-ong-lnx10 è il server NMS.

Specifiche:

Target Address: destinazione alla quale devono essere inviate le trap. Utilizzare un indirizzo IPv4 o IPv6.

Porta UDP: numero di porta UDP utilizzato dall'host. Il valore predefinito è 162.

Nome utente: specificare il nome dell'utente sull'host che si connette all'agente.

Livello di protezione: selezionare una delle seguenti opzioni:

noAuthNoPriv - Utilizza un nome utente corrispondente per l'autenticazione.

AuthNoPriv: fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA.

AuthPriv: fornisce l'autenticazione basata sugli algoritmi HMAC-MD5 o HMAC-SHA. Crittografia DES a 56 bit basata sullo standard CBC-DES (DES-56), oltre all'autenticazione.

Profilo filtro: selezionare questa casella di controllo e immettere il nome del profilo di filtro. I trap vengono inviati solo se si specifica un nome di profilo di filtro e si crea un filtro di notifica.

Solo trap proxy: se questa opzione è selezionata, inoltra solo le trap proxy dalla rete ENP. I trap da questo nodo non vengono inviati alla destinazione di trap identificata da questa voce.

Tag proxy: specificare un elenco di tag. L'elenco di tag è necessario su un GNE solo se l'ENE deve inviare trap alla destinazione identificata da questa voce e desidera utilizzare il GNE come proxy.

#### Configurazione del server NMS (blr-ong-Inx10)

Passaggio 1. Nella home directory del server, creare una directory con il nome snmp.

Passaggio 2. In questa directory, creare un file snmptrapd.conf.

Passaggio 3. Modificare il file snmptrapd.conf in:

```
vi snmptrapd.conf
createUser -e 0xEngine ID <user_name>< MD5> <password > DES <password>
Ad esempio:
createUser -e 0x0000059B1B00F0005523A71C ank MD5 cisco123 DES cisco123
In questo esempio:
```

```
user_name=ank
MD5 password = cisco123
DES password = cisco123
Engine ID = can be available from CTC.
Node view > Provisioning > SNMP > SNMP V3 > General
Verifica modalità authPriv
```

Passaggio 1. In CTC, selezionare Node View > Provisioning > Security > Access > change snmp access state to Secure (Vista nodi > Provisioning > Sicurezza > Accesso > cambia lo stato di accesso snmp su Secure (Protetto)), come mostrato nell'immagine.

Tab View	
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN	
General Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server Legal Disclaimer OSI LAN Access Protection Security Restore Timeout: 5	Pseudo IOS Access Access State: Non-sec *
SMMP Comm Channels Disable IPv4 access for IPv6 enabled ports Alarm Profiles Defaults Shell Access Shell Acces Shell Access Shell Acces Shell Access Shell Acces Shel	Port: 65000 EMS Access Access State: Non-sec
SVLAN Certificate Teinet Port: 23 Use Standard Port	TCC CORBA (IIOP) Listener Port <ul> <li>Default - TCC Fixed</li> <li>Standard Constant (683)</li> </ul>
TL1 Access	Other Constant:
Access State: Non-sec • Other PM Clearing Privilege: Provisioni •	Access State: Secure   Serial Craft Access  Enable Craft Port

Passaggio 2. Passare al server NMS ed eseguire lo snmpwalk.

Sintassi:

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

#### Esempio:

```
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::sysServices.0 = INTEGER: 79
Trap 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>
Il comando Trap è lo stesso per tutte le versioni.

#### Configurazione della modalità authNoPriv sul dispositivo ONS15454/NCS2000

Passaggio 1. In CTC, selezionare **Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode** (Visualizzazione nodo > Provisioning > Sicurezza > Accesso > Modifica stato accesso snmp in modalità non protetta), come mostrato nell'immagine.



Passaggio 2. Passare a Vista nodo > Provisioning > SNMP > SNMP V3 > Utenti > Crea utente e configurare come mostrato nell'immagine.

		· •	
	Create User	×	
	User Name:	ank1	6
	Group Name:	default_group	5
	Authentication		
	Protocol:	MD5 👻	
	Password:	skalanderske kalender som	3
Tab View	Privacy		
Alarms Conditions History Circuit	Protocol:	NONE	
	Password:		
General SNMP V1/V2			
	OK	Cancel	
Protection Users			Group Name
Security MIB views	s ank MD5	DES	default_group
SNMP Group Acce	255		
Comm Channels Trap Destinatio	ns(V3)		
Timing Notification F	ilters		
Defaults			
WDM-ANS			
SVLAN	Create Edit Delet	2	
Alarm Extenders	·		

Passaggio 3. Verificare che le viste MIB siano configurate come mostrato nell'immagine.

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

Passaggio 4. Configurare l'accesso al gruppo come mostrato nell'immagine per la modalità authnopriv.

			6
	Create Group Access		×
	Group Name: Security Level:	default_group	<b>•</b>
Tab View	Views: Read View Name:	fullview	
Alarms Conditions History Circuits Provis	Notify View Name:	fullview	
General SNMP V1/V2 SNMP V3	Allow SNMP Sets:		
OSI General Protection Users		OK Cancel	fy View Access v
Security MIB views SNMP Group Access	-		
Comm Channels Trap Destinations(V3) Timing Notification Filters			
Alarm Profiles Defaults			
WDM-ANS SVLAN	Create Edit Delete		
Alarm Extenders			

Passaggio 5. Passare a Vista nodo > Provisioning > SNMP > SNMP V3 > Destinazione trap (V3). Fare clic su Create and Configure (Crea e configura) come mostrato nell'immagine.

	Configure SnmpV3 Trap	×	8	
	Target Address:	bir-ong-inx10	6	
	UDP Port: User Name:	4303	5 4	
Tah View	Security Level:           Filter Profile:	authNoPriv	3	
Alarms Conditions History Circuits	Proxy Traps Only: Proxy Tags:			
General Network OSL General	ОК	Cancel		]
Protection Users Security MIB views	64.103.217.88 4545 a	ank authPriv	Filter Profile Name Proxy Trap	os Only
SNMP Group Acces Comm Channels Trap Destination Timing	55 15(V3)			
Alarm Profiles Defaults	Iters			
WDM-ANS SVLAN	Create Edit Delete			Help

#### Verifica modalità authNoPriv

Passaggio 1. Passare al server NMS ed eseguire lo snmpwalk.

Sintassi:

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

```
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
Trap SNMP:
```

PLATFORM=15454-M6"

snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%q\n%P\n%v\n\n" <port number>
Il comando Trap è lo stesso per tutte le versioni.

#### Configurazione della modalità noAuthNoPriv su un dispositivo ONS15454/NCS2000

Passaggio 1. In CTC, selezionare Node View > Provisioning > Security > Access > change snmp access state to Non-secure mode (Visualizzazione nodo > Provisioning > Sicurezza > Accesso > Modifica stato accesso snmp in modalità non protetta), come mostrato nell'immagine.

Alarms       Conditions       History       Circuits       Provisioning       Inventory       Maintenance       OTN         General       Users       Active Logins       Policy       Data Comm       Access       RADIUS Server       Legal Disclaimer         OSL       Access State:       Inventory       Maintenance       OTN         Protection       Security       Access State:       Inventory       Apply         Protection       Security       Telnet Port:       23       Use Standard Port       O Efault - TCC Fixed       Standard Constant (683)       O ther Constant:       Help         Comm Channels       Enable Shell Password       Standard Constant (683)       O ther Constant:       Standard Constant (683)       O ther State:       Non-sec •         WDM-ANS       Mon-sec •       Access State:       Non-sec •       Access State:       Non-sec •	Tab View	
Steturity     Teinet Port:     23     Use Standard Port       SNMP     Image: Standard Port     Image: Standard Port       Comm. Channels     Image: Standard Port       Alarm Profiles     Image: TL1 Access       Defaults     Access State:       NDM-ANS     Other       Other     Standard Constant:	Alarms     Conditions     History     Circuits     Provisioning     Inventory     Maintenance     OTN       General     Users     Active Logins     Policy     Data Comm     Access     RADIUS Server     TACACS Server       OSL     Protection     Access State.     Wolf-sec	
Defaults         TLL Access         SNMP Access           WDM-ANS         Access State:         Non-sec •           Other         Credit Credit Access	Steurity     Telnet Port:     23     Use Standard Port       SNMP	Default - TCC Fixed     Standard Constant (683)     Other Constant:
SvLAN     Other     Serial Call Access       Certificate     PM Clearing Privilege: ProvisionI •     Image: Provision Privilege: ProvisionI •	Defaults     TL1 Access       WDM-ANS     Access State: Non-sec *       SVLAN     Other       Certificate     PM Clearing Privilege: Provisioni *	SNMP Access Access State: Non-sec • Serial Craft Access Finable Craft Port

Passaggio 2. Passare a Vista nodo > Provisioning > SNMP > SNMP V3 > Utenti > Crea utente e Configura come mostrato nell'immagine.

		I	1 < >	-			
	Create	User			×	<u> </u>	
						7	
	User	Name:		ank2			
	Grou	ıp Name:		default_group		6	
	Aut	thentication				4	
	Prof	tocol:		NONE	-		
	Pas	sword:				3	
Tab View	Priv	vacy					
Alarma Conditions History Circuit	Prot	tocol:		NONE	•		
	Pas	sword:					
General							
Network SNMP V1/V2			ОК	Cancel			
OSI General							Group Name
Protection Users		ank	MD5		DES	defau	It aroup
Security MIB view	s	ank1	MD5		NONE	defau	lt_group
SNMP Group Acce	55				1		
Comm Channels Trap Destinatio	ns(V3)						
Timing Notification F	ilters						
Alarm Profiles							
Defaults							
WDM-ANS		Create Edit	Delete				
Alarma Estan dara	l						
Alarm Extenders							

Passaggio 3. Verificare che le viste MIB siano configurate come mostrato nell'immagine.

Tab Viev	N								
Alarms	Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN								
	General		Common						
	letwork	SINIMP V1/V2 SINIMP V3	Common						
	QSI	General	View Name	Sub Tree OID	Mask	Type			
E L	rotection	Users	fullview	1	1	included			
	Security	MIB views		-	-	include cu			
	SNMP	Group Access							
Com	m Channels	Trap Destinations(V3)							
Alar	rm Profiles	Notification Filters							
	Defaults								
W	DM-ANS								
	SVLAN								
C.	ertificate		Create Edit	Delete					
	L	۰ <u>ــــــــــــــــــــــــــــــــــــ</u>							

Passaggio 4. Configurare l'accesso al gruppo come mostrato nell'immagine per la modalità noauthnopriv.

	Crea	ate Group Access			×	7	
	G	roup Name:	default	_group		6	
	Se	ecurity Level:	noAuth	NoPriv	· ·	5	
		Views:				4	
	R	Read View Name:	fullview	/	*	з	
		Notify View Name:	fullview	1			
Tab View							
Alarms Conditions H	History Circ	Allow SNMP Sets:					
beneral S	SNMP V1/V2		OK Cancel				
Destruction	General	Group Name	Security Level 🛆	Read View Access	Allow SNMP Sets	Notify View Access	
Protection	Users	default_group	authPriv	fullview		fullview	
Security	MIB views	default_group	authNoPriv	fullview		fullview	
SNMP	Group Access						
Comm Channels	Trap Destinations(\	V3)					
Timing	Trap Destinations(\ Notification Filter	V3) rs					
Timing Alarm Profiles	Trap Destinations() Notification Filter	V3) IS					
Comm Channels Timing Alarm Profiles Defaults	Trap Destinations() Notification Filter	V3) IS					
Comm Channels Timing Alarm Profiles Defaults WDM-ANS	Trap Destinations() Notification Filter	V3) rs	Delata				
Comm Channels Timing Alarm Profiles Defaults WDM-ANS SVLAN	Trap Destinations(\ Notification Filter	rs Create Edit	. Delete				
Comm Channels Timing Alarm Profiles Defaults WDM-ANS SVLAN Alarm Extenders	Trap Destinations(\ Notification Filter	rs Create Edit	. Delete				

Passaggio 5. Passare a Vista nodo > Provisioning > SNMP > SNMP V3 > Destinazione trap (V3). Fare clic su Create and Configure (Crea e configura) come mostrato nell'immagine.

	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
		Filter Profile:					4
Tab View	Prox	y Traps Only:					
Alarms Conditions History Circuits	Prox	y Tags:					
General SNMP V1/V2 S				Concol			
OSI General				Cancer			
Protection Users		64.103.217.88	4545	ank	authPriv	/ Level	1
Security MIB views		64.103.217.88	4565	ank1	authNoPri	v	
SNMP Group Acce	\$ \$						
Comm Channels Trap Destination	ns(V3)						
Alarm Profiles	Iters						
Defaults							
WDM-ANS		( Create	Edit Dolata				
SVLAN		Create	Delete.	•			
Alarm Extenders							

#### Verifica modalità noAuthNoPriv

Passaggio 1. Passare al server NMS ed eseguire lo snmpwalk.

```
Esempio:

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>

Trap SNMP:
```

```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%q\n%P\n%v\n\n" <port number>
Il comando Trap è lo stesso per tutte le versioni.
```

#### Trap SNMP V3 per configurazione GNE/ENE

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

#### Su nodo GNE

Passaggio 1. Passare a Provisioning > SNMP > SNMP V3 e CCrea accesso gruppo (scheda Accesso gruppo): fornire un nome di gruppo con il livello di protezione (noAuthnoPriv|AuthnoPriv|authPriv) e l'accesso in lettura e notifica della visualizzazione completa, come mostrato nell'immagine.

- 1:1 36 - PTS	A_GE 🚽	8)	Create Group Access	×	- 6
🚥 Summary 🖹 Ne	twork	Group Name:	gnegrp 1	-	
🗮 🚦 15454 M6 ANSI	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 fullview
Protection	MIR vie	Allow SNMP Sets			fullview
Security	Group Ac	Allow Shini Sets.			
SNMP	Tran Destina		<b>h</b>		
Comm Channels	Notification		OK Cancel		
Timing	Notification				
Alarm Profiles	L				
Defaults					
WDM-ANS					
SVLAN					
Alarm Extenders					
		Create Ed	lit Delete		

Passaggio 2. Creazione dell'accesso utente (scheda Utenti): creare un utente con lo stesso nome di gruppo creato in precedenza nella scheda Accesso gruppo. Fornire inoltre l'autenticazione basata sul livello di accesso, come mostrato nell'immagine.

<ul> <li>I: 8 - TSC</li> <li>I: 36 - PTS.</li> <li>Summary I: Ne</li> <li>I5454 M6 ANSI</li> <li>Alarms Condition</li> <li>General</li> <li>Network</li> <li>OSI</li> <li>Protection</li> <li>Security</li> <li>SNMP</li> <li>Comm Channels</li> <li>Timing</li> <li>Alarm Profiles</li> <li>Defaults</li> <li>Webb Ablic</li> </ul>	A_GE  twork 107.114 105 History Circ SNMP V1/V2 St General Users MIB views Group Access Trap Destination: Notification Filt	Ø         User Name:         Group Name:         Authentication         Protocol:         Password:         Privacy         Protocol:         Password:	Creat	e User  gneuser1  gnegrp1  MD5  DES  Cancel  k		gne def
Alarm Profiles Defaults WDM-ANS			ОК	Cancel		
Alarm Extenders						
		Create	Edit Del	ete		

Passaggio 3. Scheda Destinazione trap (V3):

Target Address: Indirizzo del server NMS da cui verrà eseguita la trap, ad esempio Blr-ong-Inx10).

Porta UDP: Qualsiasi numero di porta in cui verrà ascoltata la trap (ad esempio, 9977).

Nome utente: Nome dell'utente nella scheda Utente.

Livello di protezione: Come configurato in precedenza nella scheda Utente.

Tag proxy: Fornire un tag proxy (es. Tag75).

1. 8 - ISC 1. 36 - PTS	A.GE	8	Configure SnmpV3 Trap	×	
		Target Address:	bir-ong-inx10		s s
Summary : Ne	twork	UDP Port:	9999		
Alarms Condition	ns History Circ	User Name:	gneuser1	-	
General	SNMP V1/V2 St	Security Level:	aut <mark>h</mark> Priv	-	
Network	General	Filter Profile:			Security Level
Protection	Users	Provy Trans Only			thPriv
Security	MIB views	rioxy riups only.			thPriv
SNMP	Group Access	Proxy Tags:	TagV3		
Comm Channels	Trap Destination:				
Timing	Notification Filt		OK Cancel		
Alarm Profiles					
Defaults	L				
WDM-ANS					
SVLAN					
Alarm Extenders					
		•	II		
		Create	Edit Delete		

#### Su nodo ENE

Passaggio 1. Passare a Provisioning > SNMP > SNMP V3 e Crea accesso gruppo (scheda

Accesso gruppo): fornire un nome di gruppo con livello di accesso

(noAuthnoPriv|AuthnoPriv|authPriv) e accesso in lettura e notifica della visualizzazione completa, come mostrato nell'immagine.

				,		
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		

Passaggio 2. Creazione dell'accesso utente (scheda Utenti): creare un utente con lo stesso nome di gruppo creato in precedenza nella scheda Accesso gruppo. Fornire inoltre l'autenticazione basata sul livello di accesso.

- 1:1 36 - PTS	A_GE	() ()	● Creat	e User	×
Summary 15454 M2 ANS	etwork	User Name: Group Name: Authentication		eneuser1 enegrp1	
Alarms Conditio	ns History Circ	Protocol:		MD5	
Network OSI Protection Security	General Users MIB views Group Access	Password: Privacy Protocol:		DER	
Comm Channels Timing Alarm Profiles	Trap Destination: Notification Filt	Passworu:	ОК	Cancel	
WDM-ANS SVLAN					
		Create	Edit Del	ete	

Assicurarsi che venga creato un default\_group se visualizzato nella scheda Utente nella scheda Accesso al gruppo nel caso in cui non sia presente nella scheda Accesso al gruppo.

Passaggio 3. Scheda Destinazione trap (V3):

Target Address: IP nodo GNE.

Porta UDP: 162.

Nome utente: Nome dell'utente nella scheda Utente.

Livello di protezione: Come configurato in precedenza nella scheda Utente.

Tag proxy: Fornire un tag proxy uguale a quello di GNE (ad es. Tag75).

- 1:1 36 - PTS				
	10	8	Configure SnmpV3 Trap	×
		Target Address:	10.64.107.114	
15454 M2 ANS	Node-75	UDP Port:	162	
Alarms Condition	ns History Circ	User Name:	eneuser 🚶	-
General	SNMP V1/V2 St	Security Level:	authPriv	<b>_</b>
Network	General	Filter Profile:		Securit
Protection	Users MIB views	Proxy Traps Only:		thPriv thPriv
SNMP	Group Access	Proxy Tags:	TagENE	
Comm Channels Timing Alarm Profiles Defaults	Trap Destination Notification Filt		OK Cancel	
WDM-ANS				
SVLAN				
		Create	III Edit	

In CTC, passare alla visualizzazione rete:

Passaggio 1. Passare alla scheda SNMPv3.

Passaggio 2. Tabella del server di inoltro delle trap proxy SNMPv3: È possibile eseguire la creazione manuale o automatica.

Selezionare Creazione automatica. Ai sensi di tale articolo:

- Tag di destinazione: Tag proxy impostato in GNE.
- Elenco origini trap remote: selezionare il nodo ENE IP come mostrato nell'immagine.

Network Explorer 🛛 🗙	107.114 <sup>2</sup> 107.114 <sup>2</sup> 10.64.107.18 Automatic Configuration of SNMPv3 Proxy Trap Forwar X	
	Target Tag: TagV3	
Summary 🖹 Network	Remote Trap Source List	9 <del>4</del> ×
Alarms Conditions History	Circui 10.64.107.114	
Security	10.64.107.187	
Alarm Profiles	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
	000005-00005-00005-00005-00005-00005-0000-0005-00000-0005-0000-0000-0005-00000-0005-0005-0005-0000-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0005-0000-0005-0005-0005-0005-0000-0000-0000-0000-0000-0000-0000-0000	authPriv
	0000059B2DFAA0003E8A8362  Tag114  ons_trap_user	r  authPriv
	Manual Create Auto Create Delete	
	SNMPv3 Remote Users	
	Context Engine ID Licer Name Authenti	ication Protocol Privacy Proto
		Help

#### Verifica configurazione GNE/ENE

Configurare il server NMS (blr-ong-lnx10):

Passaggio 1. Nella home directory del server, creare una directory e denominarla snmp.

Passaggio 2. In questa directory, creare un file snmptrapd.conf.

Passaggio 3. In snmptrapd.conf, creare la configurazione seguente:

createUser -e 0x

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

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

#### Per la modalità di autenticazione:

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>
Per la modalità authnopriv:

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

Per la modalità noauthnopriv:

snmpwalk -v 3 -l authpriv -u

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.