SNMPv3 configureren op Cisco ONS 15454/NCS 2000 apparaten

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Configureren Op een standalone/meervoudig knooppunt Instellen van de automatische modus priv op ONS 15454/NCS 2000 apparaat NMS Server configureren (blr-ong-lnx10) Controleer de modus AutoPriv Instellen van de toegangsmodus voor NoPriv op ONS 15454/NCS 2000 apparaat Controleer de modus AutoNoPriv Instellen van geen AutoNoPriv-modus op ONS 15454/NCS 2000 apparaat Controleer of AutoNoPriv Mode SNMP V3 Trap voor GNE/ENE Setup **Over BNE-knooppunt** betreffende ENE-knooppunt Controleer de installatie van BNE/ENE Problemen oplossen

Inleiding

Dit document beschrijft stap-voor-stap instructies hoe u de Simple Network Management Protocol, versie 3 (SNMPv3), kunt configureren op ONS 15454/NCS 2000-apparaten. Alle onderwerpen omvatten voorbeelden.

Opmerking: De lijst van eigenschappen in dit document is niet volledig of gezaghebbend en kan te allen tijde zonder bijwerking van dit document worden gewijzigd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Transport Controller (CTC) GUI
- Basisserverkennis
- Basis Linux/Unix-opdrachten

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Op een standalone/meervoudig knooppunt

Instellen van de automatische modus priv op ONS 15454/NCS 2000 apparaat

Stap 1. Meld u aan bij het knooppunt via CTC met de Super User-referenties.

Stap 2. Navigeer naar Node view > Provisioning > SNMP > SNMP V3.

Stap 3. Navigeer naar het tabblad Gebruikers. Gebruikers maken

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> Stap 4. Klik op OK zoals in de afbeelding.

	×	Create User			
	User Name:	ank			
	Group Name:	default_group			
	Authentication				
	Protocol:	MD5	T		
	Password:	***			
	Privacy				
	Protocol:	DES	Ψ		
	Password:	*****			
Tab View					
Alarms Conditions History Circuits Pro		OK Cancel	-		
General SNMP V1/V2 SNMP V3	Common				
OSI General	User Name	Authentication Protocol	Privacy Protocol	Group Name	
Protection Users	oser Hume		intacy indicion	oroup runne	
Security					
SNMP Group Access					
Comm Channels Trap Destinations(V3)					
Alarm Protiles Notification Eilters					
Defaults					
SVI AN					
Certificate	Create	Delete			
Solution State	Createn	Lo to the training			

Specificaties:

Gebruikersnaam - Specificeer de naam van de gebruiker op de host die met de agent verbonden is. De gebruikersnaam moet minimaal 6 en maximaal 40 tekens zijn (maximaal 39 tekens voor de TACACS- en RADIUS-verificatie). Het bevat alfanumerieke (a-z, A-Z, 0-9) tekens en de toegestane speciale tekens zijn @, "-" (koppelteken) en "." (punt). Voor TL1-compatibiliteit moet de gebruikersnaam uit 6 tot 10 tekens bestaan.

Naam groep - Specificeer de groep waartoe de gebruiker behoort.

Verificatie:

Protocol - Selecteer het verificatiealgoritme dat u wilt gebruiken. De opties zijn ONE, MD5 en SHA.

Wachtwoord - Voer een wachtwoord in als u MD5 of SHA selecteert. Standaard is de wachtwoordlengte ingesteld op minimaal acht tekens.

Privacy - initieert een instellingssessie voor de privacy-verificatie die de host in staat stelt de inhoud van het bericht te versleutelen dat naar de agent wordt verzonden.

Protocol - Selecteer het algoritme voor de verificatie van de privacy. De beschikbare opties zijn geen, DES en AES-256-CFB.

Wachtwoord - Voer een wachtwoord in als u een ander protocol selecteert dan geen.

Stap 5. Zorg ervoor dat de MIB-weergave in deze afbeelding is ingesteld.

ab View					
Alarms Conditions History	Circuits Provisioning Inventory	Maintenance OTN			
General Network OSI Protection Security SNMP Comm Channels Alarm Profiles Defaults WDM-ANS SVLAN Certificate	I/V2 SNMP V3 Common General View Name Users fullview MIB views roup Access Destinations(V3) fication Filters Ed	Sub Tree OID	Mask 1	Type included	

Specificaties:

Naam - Naam van de weergave.

Subtree OID - De MIB-subboom die, wanneer gecombineerd met het masker, de reeks subbomen definieert.

Beetje masker - Een familie van uitzicht subbomen. Elke bit in het bit Mask correspondeert met een sub-identifier van de subtree OID.

Type - Selecteer het type weergave. Opties zijn opgenomen en uitgesloten.

Het type definieert of de reeks subbomen die wordt gedefinieerd door de subboom OID en de combinatie bitmasker zijn opgenomen of uitgesloten van het aanmeldingsfilter.

Stap 6. Het configureren van groepstoegang zoals in de afbeelding. Standaard zal de naam van de groep default_group en security niveau als authPriv zijn.

Opmerking: De naam van de groep moet hetzelfde zijn als de naam die wordt gebruikt wanneer u in Stap 3 de gebruiker maakt.

Tab View							
Alarms Conditions	History Circuits Provis	ioning Inventory M	aintenance OTN]			
General Network OSI	SNMP V1/V2 SNMP V3	Common	Cognitive Louise	Road View Access	Allow SNMD Sote	Notifi View Accore	
Protection Security SNMP Comm.Channels Alarm.Profiles Defaults WDM-ANS	Users MB views Group Access Trap.Destinations(V3) Notification Filters	default_group	authPriv	fullview		fullview	
Certificate		Create Edit.	Delete				

Specificaties:

Naam van de groep - de naam van de SNMP groep, of de verzameling gebruikers, die een gemeenschappelijk toegangsbeleid delen.

Beveiligingsniveau - het beveiligingsniveau waarvoor de toegangsparameters worden

gedefinieerd. Selecteer uit deze opties:

NoAuthNoPriv - Gebruikt een gebruikersnaammatch voor authenticatie.

AuthNoPriv - biedt verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen.

AuthPriv - levert verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen. Biedt DES 56-bits codering op basis van de CBC-DES (DES-56)-standaard, naast verificatie.

Als u authNoPriv of authPriv voor een groep selecteert, moet de betreffende gebruiker worden geconfigureerd met een verificatieprotocol en een wachtwoord, met een privacy-protocol en een wachtwoord, of beide.

Bekijk

Lees View Name - Lees de naam van de weergave voor de groep.

Melden van View Name - Melden de naam van de weergave voor de groep.

Geef SNMP-bestanden toe - Selecteer dit aankruisvakje als u wilt dat de SNMP-agent SNMPverzoeken accepteert. Als dit selectieteken niet is geselecteerd, worden de SET-aanvragen afgewezen.

Opmerking: SNMP SET-aanvraagtoegang wordt voor heel weinig objecten geïmplementeerd.

Stap 7. Navigeer naar Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3). Klik op Maken en Configureren.

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

Stap 8. Klik op **OK** zoals in de afbeelding.

	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		

Opmerking: blr-ong-lnx10 is de NMS-server.

Specificaties:

Doel - Doel waarvoor de vallen dienen te worden verzonden. Gebruik een IPv4- of IPv6-adres.

UDP Port - UDP-poortnummer dat de host gebruikt. De standaardwaarde is 162.

Gebruikersnaam - Specificeer de naam van de gebruiker op de host die met de agent verbonden is.

Beveiligingsniveau - Selecteer een van deze opties:

NoAuthNoPriv - Gebruikt een gebruikersnaammatch voor authenticatie.

AuthNoPriv - biedt verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen.

AuthPriv - levert verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen. Biedt DES 56-bits codering op basis van de CBC-DES (DES-56)-standaard, naast verificatie.

Filterprofiel - Selecteer dit aankruisvakje en voer de naam van het filterprofiel in. Splitsen worden alleen verzonden als u een naam van het filterprofiel geeft en een waarschuwing van het filter maakt.

Alleen proxy-trappen - indien geselecteerd, alleen proxy-traps van de ENE doorsturen. Vraps van dit knooppunt worden niet naar de valbestemming verzonden die door deze ingang wordt geïdentificeerd.

Proxy-tags - geeft een lijst met tags aan. De labellijst is alleen nodig op een BNE als een ENE vallen naar de doelmap moet sturen die door deze vermelding geïdentificeerd is, en de GNE als de proxy wil gebruiken.

NMS Server configureren (blr-ong-lnx10)

Stap 1. Maak in uw adresmap van de server een directory met de naam snmp.

Stap 2. Maak onder deze folder een bestand snmptrapd.conf.

Stap 3. Verander het bestand SNMP.conf in:

```
vi snmptrapd.conf
createUser -e 0xEngine ID <user_name>< MD5> <password > DES <password>
Bijvoorbeeld:
createUser -e 0x0000059B1B00F0005523A71C ank MD5 cisco123 DES cisco123
In dit voorbeeld:
user_name=ank
MD5 password = cisco123
DES password = cisco123
```

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

Stap 1. In CTC, navigeer naar Node Beeld > Provisioning > Beveiliging > Access > Verander de status van SNMP om beveiligde zoals in de afbeelding te bevestigen.

Tab View	
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN	
General Ukars, Arthus Logins, Data Comm. Trends Sanuar, TACACS Sanuar, Login Discharger	
Network Osers Active Logins Poncy Data Comm Access (ADIOS Server TACACS Server Legal Disclaimer	
OSI LAN Access	Pseudo IOS Access
Protection LAN Access: Front Craft & E *	Access State: Non-sec *
Security Restore Timeout: 5 - minute(s)	
SNMP Concernation	Port: 65000
Comm Channels Disable IPv4 access for IPv6 enabled ports	
Alarm Profiles Shell Access	EMS Access
Defaults Access State: Non-sec *	Access State: Non-sec *
WDM-ANS	TCC CORBA (IIOP) Listener Port
Telnet Port: 23 Use Standard Port	Default - TCC Fixed
Ceruncate	Standard Constant (683)
Enable Shall Parcured	Standard Constant (005)
Li Enable Shell Password	Other Constant:
Access States Non-soc x	SIMP ACCess
Access suite.	Access state.
Other	Serial Craft Access
PM Clearing Privilege: Provisioni *	C Enable Craft Port

Stap 2. Navigeer naar de NMS server en wandel de computer.

Syntaxis:

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

Voorbeeld:

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 SNMP-trap:

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 is voor alle versies hetzelfde.

Instellen van de toegangsmodus voor NoPriv op ONS 15454/NCS 2000 apparaat

Stap 1. In CTC, navigeer naar Node View > Provisioning > Beveiliging > Access > Verander de status van toegang tot niet-beveiligde modus zoals in de afbeelding.

Tah Viaw	
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN	
General Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server	r] Legal Disclaimer
OSI MCCess state.	Apply
Protection Telnet Port: 23 Use Standard Port	Default - TCC Fixed Reset
SNMP Enable Shell Password	O Standard Constant (683) Other Constant:
Alarm.Profiles Defaults WDM-ANS Access State: Non-sec *	SNMP Access Access State: Non-sec *
SVLAN Other Certificate PM Clearing Privilege: Provisioni •	Serial Craft Access

Stap 2. Navigeer naar Node View > Provisioning > SNMP > SNMP V3 > Gebruikers > Gebruikers maken en configureren zoals in de afbeelding.

		· •	
	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		
Alarm Profiles			
WDM-ANS			
SVLAN	Create Edit Delet	2	
Alarm Extenders	·		

Stap 3. Zorg ervoor dat de MIB-weergave is ingesteld zoals in de afbeelding.

Tab View					
Alarms Conditions History Circuits Provis	ioning Inventory Mainte	nance OTN			
General SNMP V1/V2 SNMP V3	Common				
OSI General	View Name	Sub Tree OID	Mask	Туре	
Security MIB views SNMP Group Access	fullview	1	1	included	
Comm Channels Trap Destinations(V3) Alarm Profiles Notification Filters					
Defaults WDM-ANS SVLAN					
Certificate	Create Edit	Delete			

Stap 4. Het configureren van groepstoegang zoals in de afbeelding voor autorisatie-modus.

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

Stap 5. Navigeer naar Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3). Klik op Maken en Configureren zoals in de afbeelding wordt weergegeven.

	Configure SnmpV3 Trap	*		
	Target Address:	bir-ong-Inx10		
	UDP Port:	4565	5	
	User Name:	ank1 *		
	Security Level:	suthNoPriv 👻	3	
	Filter Profile:			
Tab View	Proxy Traps Only:			/ _×
Alarms Conditions History Circuits	Proxy Tags:			
General SNMP V1/V2				
Network	ОК	Cancel		
Protection Users			/ Level Filter Profile Name	Proxy Traps Only
Security MIB views	64.103.217.88 4545 a	nk authPriv		
SNMP Group Acces	3			
Comm Channels Trap Destination	s (v/3)			
Alarm Profiles	sers			
Defaults	•			→
WDM-ANS	Create Edit Delete			Help
Alarm Extenders	L			

Controleer de modus AutoNoPriv

Stap 1. Navigeer naar de NMS server en wandel.

Syntaxis:

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

```
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
```

```
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
SNMP-trap:
```

 $\label{eq:snmptrapd-f-lo-OQ-Ob-Ot-F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" rot number> Trap cmd is voor alle versies hetzelfde.$

Instellen van geen AutoNoPriv-modus op ONS 15454/NCS 2000 apparaat

Stap 1. In CTC, navigeer naar Node View > Provisioning > Beveiliging > Access > Verander de status van toegang tot niet-beveiligde modus zoals in de afbeelding.

Tab View	/_:
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN	
General Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server OSL Protection State: Invol=sec Telnet Port: 23 Use Standard Port SNMP Enable Shell Password Enable Shell Password Enable Shell Password	r 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

Stap 2. Navigeer naar Node View > Provisioning > SNMP > SNMP V3 > Gebruikers > Gebruikers maken en configureren zoals in de afbeelding.

Create User User Name: ank2 Group Name: default_group Authentication Protocol: NONE Password: Privacy Protocol: NONE			1 () : .		
User Name: ank2 Group Name: default_group Authentication Protocol: Protocol: Password: Privacy Protocol: NONE		Create User		×	
Group Name: default_group Authentication Protocol: Password: Tab View Privacy Protocol: NONE		User Name:	ank2		
Authentication Protocol: Password:		Group Name:	default_group		5
Protocol: NONE Password: 3 Tab View Privacy Protocol: NONE		Authentication			4
Tab View Privacy Protocol: NONE		Protocol:	NONE	.	
Tab View Privacy Protocol: NONE		Password:			3
Alexan Constitional Utimes Constit	Tah View	Privacy			
	Alarma Conditions History Circuit	Protocol:	NONE	•	
Password:	Manns Conditions History Circuit	Password:			
General	General				
Network OK Cancel	Network SNMP V1/V2		OK Cancel		
OSI General Group Name	OSI General				Group Name
Protection Users ank MD5 DES default_group	Protection Users	ank	MD5	DES	default_group
Security MIB views ank1 MD5 NONE default_group	Security MIB view	s ank1	MD5	NONE	default_group
SNMP Group Access	SNMP Group Acce	ess			
Timina NetGenia Silver	Timing	(ns(V3)			
Alarm Profiles	Alarm Profiles	liters			
Defaults	Defaults				
WDM-ANS	WDM-ANS				
SVLAN Edit Delete	SVLAN	Create Edit	Delete		
Alarm Extenders	Alarm Extenders				

Stap 3. Zorg ervoor dat de MIB-beelden zijn geconfigureerd zoals in de afbeelding.

Tab View						
Alarms Conditions History Circuits	ovisioning Inventory Mainte	enance OTN				
General SNIMP V1 (V2) SNIMP	V2 Common					
NetworkSNMP V1/V2SNMP	V3 Common					
OSI General	View Name	Sub Tree OID	Mack	Tuno		
Protection Users	fullview	1	1	included		
Security MIB views	Tullview	1	1	Included		
SNMP Group Access						
Comm Channels Trap Destinations(V	3)					
Alarm Profiles Notification Filters						
Defaults						
WDM-ANS						
SVLAN						
Certificate	Create Edit	Delete				

Stap 4. Configureer de groepstoegang zoals in de afbeelding voor de automatische modus.

		C	reate G	roup Access				×	7	
			Group N	Name:		default	_group	•	- <u>-</u> -	
			Security	/ Level:		noAuth	NoPriv	.	*	
			Views:						4	
			Read V	iew Name:		fullview		Ψ	3	
			Notify	View Name:		fullview	,			
Tab View						_				
Alarms Condition	ons History	Circ	Allows	SNMP Sets:						
							_			
General	SNIMD	1102			_ ок][Cancel				
Network	SIMIP	ATLAS								
IZO		General		Group Name	Security Le	wel A	Read View Access	Allow SNMP Se	ets Notify View Acce	
Protection		Users		default group	authPriv	.rei	fullview		fullview	
Security		MIB views		default group	authNoPriv		fullview		fullview	_
SNMP		Broup Acces	5	acroant_group						
Comm Channe	ls Trap	Destination	s(V3)							
Timing	No	tification Fil	ters							
Alarm Profiles										
Defaults										
WDM-ANS				Crasta	Delete					
SVLAN				Createn	Delete					
Alarm Extende	s									
11										

Stap 5. Navigeer naar **Node View > Provisioning > SNMP > SNMP V3 > Trap Destination (V3)**. Klik op **Maken** en **Configureren** zoals in de afbeelding wordt weergegeven.

	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							

Controleer of AutoNoPriv Mode

Stap 1. Navigeer naar de NMS server en wandel.

```
Voorbeeld:
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-trap:
```

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

```
\label{eq:snmptrapd-f-lo-OQ-Ob-Ot-F "%V\n%B\n%N\n%w\n%q\n%P\n%v\n\n" rort number> Trap cmd is voor alle versies hetzelfde.
```

SNMP V3 Trap voor GNE/ENE Setup

Over BNE-knooppunt

Stap 1. navigeren naar Provisioning > SNMP > SNMP V3 en CToegang tot groep maken (tabblad Toegang groep): Geef een groepsnaam op met Beveiligingsniveau (noAuthnoPriv|AuthnoPriv|authPriv) en volledige weergave Lezen en Melden van de toegang zoals in de afbeelding getoond.

- : 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.			

Stap 2. Maak gebruikerstoegang (tabblad Gebruikers): om een gebruiker met de groepsnaam te maken zoals eerder is gemaakt in het tabblad Toegang voor groep. Typ ook de verificatie op basis van het toegangsniveau zoals in de afbeelding.

: 8 - TSC : 36 - PTS.	A_GE	19) User Name:	Art Create User	• •	
Alarms Condition General Network OSI Protection Security SNMP	107.114 ns History Circ SNMP V1/V2 St General Users MIB views Group Access	Group Name: Authentication Protocol: Password: Privacy Protocol: Password:	gnegrp1 MD5 •••••••••••••••••••••••••••••••••••		gne def
Comm Channels Timing Alarm Profiles Defaults WDM-ANS SVLAN Alarm Extenders	Trap Destination: Notification Filt	Create	OK Cancel Edit Delete	*	

Stap 3. Tabblad Bestemming van trap (V3):

Doeladres: Adres van de NMS server van waar de val zal lopen (bijv. Blr-ong-lnx10).

UDP-poort: Elk havennummer waar de val wordt gehoord (ex 9977).

Gebruikersnaam: Naam van de gebruiker in het tabblad Gebruiker.

Beveiligingsniveau: Zoals eerder ingesteld in het tabblad Gebruiker.

Proxytags: Geef een proxy-tag op (Ex). Tag75).

8 - ISC 36 - PTS	A_GE	1 0	Configure SnmpV3 Trap	×	
		Target Address:	blr-ong-lnx10		<mark>r ∼</mark> s
15454 M6 ANS	twork	UDP Port:	9999		
Alarms Conditio	ns History Circ	User Name:	gneuser1	•	
General	SNMP V1/V2 SN	Security Level:	aut <mark>h</mark> Priv	-	
Network OSI	General	Eilter 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					
		•	III		
		Create	Edit Delete		
	1				

betreffende ENE-knooppunt

Stap 1. navigeren naar Provisioning > SNMP > SNMP V3 en Groepstoegang (tabblad

Groepstoegang): Geef een groepsnaam een toegangsniveau op

(noAuthnoPriv|AuthnoPriv|authPriv) en de volledige weergave Lezen en Melden van de toegang zoals in de afbeelding getoond.

				,		
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		
·						

Stap 2. Maak gebruikerstoegang (tabblad Gebruikers): om een gebruiker met de groepsnaam te maken zoals eerder is gemaakt in het tabblad Toegang voor groep. Typ ook de verificatie op basis van het toegangsniveau.

- : 36 - PTS.	A_GE	() ()	●/™-4 Creat	e User	×
Summary	etwork	User Name: Group Name:		eneuser1 enegrp 1	
Alarms Condition	l Node-75 ns History Circ	Authentication		MD5	
General Network	SNMP V1/V2 St General	Password:		•••••	
OSI Protection Security	Users MIB views Group Access	Privacy Protocol: Password:		DE	
Comm Channels Timing	Trap Destination Notification Filt	rassworu.	ОК	Cancel	
Alarm Profiles Defaults WDM-ANS	L				
SVLAN					
		Create	Edit Del	ete	

Verzeker een default_group als deze optie in het tabblad User is aangemaakt in het tabblad Group Access voor het geval dit ontbreekt in het tabblad Group Access.

Stap 3. Tabblad Bestemming van trap (V3):

Doeladres: GNE-knooppunt IP.

UDP-poort: 162.

Gebruikersnaam: Naam van de gebruiker in het tabblad Gebruiker.

Beveiligingsniveau: Zoals eerder ingesteld in het tabblad Gebruiker.

Proxytags: Geef een proxy-tag op die gelijk is aan BNE (Ex). Tag75).

- 1:1 36 - PTS	A GE			
- CENEINode2	10	8	Configure SnmpV3 Trap	×
		Target Address:	10.64.107.114	
15454 M2 ANS	twork	UDP Port:	162	
Alarms Condition	ns History Circ	User Name:	eneuser 🗎	-
General	SNMP V1/V2 St	Security Level:	authPriv	
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	Trap Destination Notification Filt		OK Cancel	
Defaults WDM-ANS	L			
SVLAN				
		Create	Edit Delete	

In CTC, navigeer naar netwerkweergave:

Stap 1. Navigeer naar het tabblad SNMPv3.

Stap 2. SNMPv3 Proxy-trap voor doorsturen van tabellen: U kunt **handmatig** of **automatisch maken** doen.

Selecteer Automatisch maken. In dat geval:

- Streepjesmarkering: Proxytag wordt ingesteld in BNE.
- Remote Trap-bronlijst: Selecteer het ENE-knooppunt van IP zoals in de afbeelding.

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	Circui 10.64.107.114	
Security	00000. 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	
		note User Security Level
	0000059B2DFAA0003E8A8362 Tag114 ons_trap_user	authPriv
	Manual Create Delete	
	SNMPv3 Remote Users	
	Contaxt Engine ID User Name Authenti	Cation Protocol Prince Proto
	• ///	Help

Controleer de installatie van BNE/ENE

NMS Server configureren (blr-ong-lnx10):

Stap 1. Voer in de adresmap van de server een directory aan en noem deze snel.

Stap 2. Maak onder deze folder een bestand snmptrapd.conf.

Stap 3. Creëer in snmptrapd.conf deze configuratie:

createUser -e 0x

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

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

Voor aupriv-modus:

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>
Voor authentieke modus:

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

Voor de nieuwe modus:

snmpwalk -v 3 -l authpriv -u

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.