Cisco ONS15454/NCS2000デバイスでの SNMPv3の設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 設定 スタンドアロン/マルチシェルフノードの場合 ONS15454/NCS2000デバイスでのauthPrivモードの設定 NMSサーバの設定(blr-ong-lnx10) authPrivモードの確認 ONS15454/NCS2000デバイスでのauthNoPrivモードの設定 authNoPrivモードの確認 ONS15454/NCS2000デバイスでのnoAuthNoPrivモードの設定 noAuthNoPrivモードの確認 GNE/ENEセットアップのSNMP V3トラップ GNEノード上 ENEノード上 GNE/ENE設定の確認 トラブルシュート

概要

このドキュメントでは、ONS15454/NCS2000デバイスで簡易ネットワーク管理プロトコルバージョン3(SNMPv3)を設定する手順について説明します。これらにはすべて例が示されます。

注:このドキュメントで提供されている属性のリストは、すべてを網羅しているわけでも、 信頼できるものでもなく、このドキュメントを更新しなければ随時変更される可能性があり ます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Transport Controller(CTC)GUI
- サーバに関する基本的な知識
- •基本的なLinux/Unixコマンド

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの ではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

設定

スタンドアロン/マルチシェルフノードの場合

ONS15454/NCS2000デバイスでのauthPrivモードの設定

ステップ1:スーパーユーザクレデンシャルを使用してCTC経由でノードにログインします。

ステップ2:[Node view] > [Provisioning] > [SNMP] > [SNMP V3]に移動します。

ステップ3:[Users]タブに移動します。ユーザを作成します。

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> ステップ4:図に示すように[OK]をクリックします。

Tab View Alarms Conditions History Circuits Pro	X User Name: Group Name: Authentication Protocol: Privacy Protocol: Password: Password:	Create User ank default_group MDS DES 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 Certificate	User Name User Name Create Edit	Authentication Protocol	Privacy Protocol	Group Name	

仕様:アナログ FXS インターフェイス

[User Name]:エージェントに接続するホスト上のユーザの名前を指定します。ユーザ名は、6文 字以上40文字以下にする必要があります(TACACSおよびRADIUS認証では39文字以下)。 英数 字(a ~ z、A ~ Z、0 ~ 9)を含み、特殊文字として@、"-"(ハイフン)、および"を使用できます 。(ドット)を表します。 TL1互換の場合、ユーザ名は6 ~ 10文字である必要があります。

[Group Name]: ユーザが属するグループを指定します。

認証:

[Protocol] : 使用する認証アルゴリズムを選択します。オプションは、NONE、MD5、および SHAです。

[パスワード(Password)]:MD5またはSHAを選択する場合は、パスワードを入力します。デフォル トでは、パスワードの長さは8文字以上に設定されています。

[Privacy] : ホストがエージェントに送信されるメッセージの内容を暗号化できるようにするプラ イバシー認証レベル設定セッションを開始します。

[Protocol] : プライバシー認証アルゴリズムを選択します。使用できるオプションは、[なし (None)]、[DES]、および[AES-256-CFB]です。

[パスワード(Password)]:[なし(None)]以外のプロトコルを選択した場合は、パスワードを入力します。

ステップ5:MIBビューがこのイメージに従って設定されていることを確認します。

Tab View									
Alarms Conditions History Circuits Provisioning Inventory Maintenance OTN									
General Network	SNMP V1/V2 SNMP V3	Common							
OSI	General	View Name	Sub Tree OID	Mask	Туре				
Security	MIB views	fullview	1	1	included				
SNMP	Group Access								
Alarm Profiles	Trap_Destinations(V3) Notification Filters								
Defaults									
SVLAN									
Certificate		Create Edit	Delete						
	L								
_									

仕様:アナログ FXS インターフェイス

[名前]:ビューの名前。

サブツリーOID:マスクと組み合わせると、サブツリーのファミリを定義するMIBサブツリー。

ビットマスク:ビューサブツリーのファミリ。ビットマスクの各ビットは、サブツリーOIDのサ ブ識別子に対応します。

[タイプ]:ビュータイプを選択します。オプションは[含める(Included)]と[除外(Excluded)]です。

このタイプは、サブツリーのOIDとビットマスクの組み合わせで定義されるサブツリーのファミリを、通知フィルタに含めるか除外するかを定義します。

ステップ6:図に示すように、グループアクセスを設定します。デフォルトでは、グループ名は default_groupで、セキュリティレベルはauthPrivです。

注:グループ名は、ステップ3でユーザを作成するときに使用したものと同じである必要がありま す。

ab View						
Alarms Conditions History Circuits Provi	sioning Inventory M	faintenance OTN				
General Network SNMP V1/V2 SNMP V3	Common					
Osi 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				

仕様:アナログ FXS インターフェイス

[Group Name]:共通のアクセスポリシーを共有するSNMPグループまたはユーザのコレクション の名前。

[セキュリティレベル(Security Level)]:アクセスパラメータが定義されるセキュリティレベル。次のオプションから選択します。

noAuthNoPriv:認証にユーザ名の一致を使用します。

AuthNoPriv:HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を提供します。

AuthPriv:HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を提供します。認証に加えて、CBC-DES(DES-56)標準に基づくDES 56ビット暗号化を提供します。

グループに対してauthNoPrivまたはauthPrivを選択する場合、対応するユーザに認証プロトコル とパスワード、プライバシープロトコルとパスワード、またはその両方を設定する必要がありま す。

[Views]

Read View Name – グループのビュー名を読み取ります。

[Notify View Name]: グループのビュー名を通知します。

[Allow SNMP Sets]:SNMPエージェントがSNMP SET要求を受け入れるようにするには、このチェックボックスをオンにします。このチェックボックスをオフにすると、SET要求は拒否されます。

注: SNMP SET要求アクセスは、ごく少数のオブジェクトに対して実装されます。

ステップ7:[Node View] > [**Provisioning] > [SNMP] > [SNMP V3] > [Trap Destination (V3)]に移動し** ます。 [**Create** and **Configure**]をク**リックし**てください。

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

ステップ8:図に示すように[OK]をクリックします。

			000	_
	Configure SnmpV3 Trap		×	
	Target Address:	bir-ong-Inx10		
	UDP Port:	4545	5	
	User Name:	ank	• 4	
	Security Level:	authPriv	₹ 3	
Tak Mara	Filter Profile:			
Alarms Conditions History Circuits	Proxy Traps Only:			
	Proxy Tags:			
Network	F	OK Cancel		
OSI General			/ Level	Filter Profile
Protection Users			,	
SNMP Crown Arrows				
Comm Channels	s (C/)			
Timing Notification Filt	ters			
Alarm Profiles				
Defaults	•			
WDM-ANS	Create Edit	Delete		
SVLAN Alarm Extenders				

注: blr-ong-Inx10はNMSサーバです。

仕様:アナログ FXS インターフェイス

Target Address(ターゲットアドレス):トラップの送信先のターゲット。IPv4またはIPv6アド レスを使用します。

UDPポート:ホストが使用するUDPポート番号。デフォルト値は 162 です。

[User Name]:エージェントに接続するホスト上のユーザの名前を指定します。

[Security Level]:次のいずれかのオプションを選択します。

noAuthNoPriv:認証にユーザ名の一致を使用します。

AuthNoPriv:HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を提供します。

AuthPriv:HMAC-MD5またはHMAC-SHAアルゴリズムに基づく認証を提供します。認証に加えて、CBC-DES(DES-56)標準に基づくDES 56ビット暗号化を提供します。

[Filter Profile]:このチェックボックスをオンにして、フィルタプロファイル名を入力します。ト ラップは、フィルタプロファイル名を指定し、通知フィルタを作成した場合にのみ送信されます 。

[Proxy Traps Only] : オンにすると、ENEからプロキシトラップのみを転送します。このノードか らのトラップは、このエントリによって識別されるトラップ宛先には送信されません。

プロキシタグ:タグのリストを指定します。タグリストは、ENEがこのエントリによって識別さ れるトラップ宛先にトラップを送信する必要があり、GNEをプロキシとして使用する場合にのみ 、GNEで必要になります。

NMSサーバの設定(blr-ong-lnx10)

ステップ1:サーバのホームディレクトリで、snmpという名前のディレクトリを作成します。

ステップ2: このディレクトリの下に、snmptrapd.confファイルを作成します。

ステップ3: snmptrapd.confファイルを次のように変更します。

vi snmptrapd.conf

createUser -e 0xEngine ID <user_name>< MD5> <password > DES <password> 以下に、いくつかの例を示します。

createUser -e 0x0000059B1B00F0005523A71C ank MD5 cisco123 DES cisco123 この例では、

user_name=ank

MD5 password = cisco123

DES password = cisco123

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

authPrivモードの確認

ステップ1:CTCで、図に示すように、[Node View] > [Provisioning] > [Security] > [Access] > [snmp access state]を[Secure]に変更します。

Tab View		
Alarms Conditions	History Circuits Provisioning Inventory Maintenance OTN	
General	Users Active Logins Policy Data Comm Access RADIUS Server TACACS Server Legal Disclaimer	
Network		
USI	LAN Access	Pseudo IOS Access
Frotection	LAN Access: Front Craft & E *	Access State: Non-Sec *
SNMP	Restore Timeout: 5 🚽 minute(s)	Port: 65000
Comm Channels	Disable IPv4 access for IPv6 enabled ports	
Alarm Protiles	Shell Access	EMS Access
UPERALITY AND	Access State: Non-sec *	Access State: Non-sec *
SVI AN		TCC CORBA (IIOP) Listener Port
Certificate	Telnet Port: 23 Use Standard Port	Default – TCC Fixed
		Standard Constant (683)
	Enable Shell Password	O Other Constant:
		O other Constant.
	TL1 Access	SNMP Access
	Access State: Non-sec *	Access State: Secure •
	Other	Serial Craft Arress
	PM Clearing Privilege: Provisioni *	Stable Craft Port
	the entering to the first the first terms of ter	
	[

ステップ2:NMSサーバに移動し、snmpwalkを実行します。

構文:

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

blr-ong-lnx10:151> snmpwalk -v 3 -l authpriv -u ank -a MD5 -A ciscol23 -x DES -X ciscol23 l0.64.106.40 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はすべてのバージョンで同じです。

ONS15454/NCS2000デバイスでのauthNoPrivモードの設定

ステップ1:CTCで、[Node View] > [Provisioning] > [Security] > [Access] > [snmp access state]を [Non-secure mode]に移動します(図を参照)。

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 PROTECTION Protection Telnet Port: 23	ACCESS State: [YOIP Sec] TCC CORBA (IIOP) Listener Port Default – TCC Fixed Apply Reset
Comm Channels Enable Shell Password	Standard Constant (683) Other Constant:
Defaults TL1 Access WDM-ANS Access State:	SNMP Access Access State: Non-sec *
SVLAN Other Certificate PM Clearing Privilege: Provisioni *	Serial Craft Access

ステップ2:[Node View] > [Provisioning] > [SNMP] > [SNMP V3] > [Users] > [Create User]に移動し、図に示すように</mark>設定します。

	FF	\sim		
	Create User		×	
	User Name:	ank1		(
	Group Name:	default_group		
	Authentication			
	Protocol:	MD5		
	Password:	- Verdendendendendenden		3
Tab View	Privacy			
Alarms Conditions History Circuit	Protocol:	NONE	T	
	Password:			
General SNMP V1/V2				
Network		OK Cancel	F	
Protection				Group Name
Security MIB view	s ank ME	5	DES	default_group
SNMP Group Acce	255			
Comm Channels Trap Destinatio	ns(V3)			
Timing Notification F	ilters			
Alarm Profiles				
WDM-ANS				
SVLAN	Create Edit	Delete		
Alarm Extenders	L			

ステップ3:図に示すようにMIBビューが設定されていることを確認します。

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

ステップ4: authnoprivモードの図に示すように、グループアクセスを設定します。

			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 Network 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				

ステップ5:[Node View] > [**Provisioning] > [SNMP] > [SNMP V3] > [Trap Destination (V3)]に移動し** ます。 図に示すように、[**Create** and **Configure**]をクリックします。

	Configure SnmpV3 Trap	×		
	Target Address:	bir-ona-inx10	7	
	LIDP Port:	4565	°	L
	Her Name	anki	6	
	Oser Ivarrie:			
	Security Level:	authNoPriv 👻	3	
T-1-1/6	Filter Profile:			
	Proxy Traps Only:			r _ ×
Alarms Conditions History Circuit	Proxy Tags:			
General				
Network SNMP V1/V2	ок	Cancel		
OSI General			/ Level Filter Profile Name	Proxy Traps Only
Protection Users	64.103.217.88 4545	ank authPriv		
SNMP Group Acc	3			
Comm Channels Tran Destinatio	ns(/3)			
Timing Notification	ilters			
Alarm Profiles				
Defaults	4			
WDM-ANS	Create Edit Delete			Help
SVLAN				
Alarm Extenders				

authNoPrivモードの確認

ステップ1:NMSサーバに移動し、snmpwalkを実行します。

構文:

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

```
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 :

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はすべてのバージョンで同じです。

ONS15454/NCS2000デバイスでのnoAuthNoPrivモードの設定

ステップ1:CTCで、[Node View] > [Provisioning] > [Security] > [Access] > [snmp access state]を [Non-secure mode]に移動します(図を参照)。



ステップ2:図に示すように、[Node View] > [Provisioning] > [SNMP] > [SNMP V3] > [Users] > [Create User and Configure]に移動します。

			100	-		- 1 ()	
	Create	User			;	< LL	
	User	Name:		ank2			6
	Grou	ıp Name:		default_group			5
	Aut	thentication				_	
	Prot	tocol:		NONE	*	_	
	Pass	sword:					3
T + 14	Pris	201					
Tab View	Prot	tocol:		NONE	•		
Alarms Conditions History Circuit	Dave	rword:					
General	Pass	swora.					
Network SNMP V1/V2			OK	Cancel			
OSI General				Gancer			
Protection							Group Name
Security MIB views		ank	MDS		DES		default_group
SNMP Group Acces	s	ankl	MD5		NONE		default_group
Comm Channels Trap Destination:	s(V3)						
Timing Notification Filt	ters						
Alarm Profiles							
Defaults							
WDM-ANS		Create	Deleta				
SVLAN		Create Eult	Delete				
Alarm Extenders							

ステップ3:図に示すようにMIBビューが設定されていることを確認します。

Tab View									
Alarms	ns	History Circuits Provi	sioning Inventory Maint	enance OTN					
General Cattoria Company Company									
Network		SNMP V1/V2 SNMP V3	Common						
QSL		General	View Name	Sub Tree OID	Mask	Type			
Protection	-	Users	fullview	1	1	included			
Security		MIB views Group Access							
Comm Channel	s	Trap Destinations(V3)							
_Alarm_Profiles	-	Notification Filters							
Defaults	-								
SVLAN									
Certificate			Create Edit	Delete					
			L						
	_								

ステップ4:図に示すように、noauthnoprivモードのグループアクセスを設定します。

		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								

ステップ5:[Node View] > [**Provisioning] > [SNMP] > [SNMP V3] > [Trap Destination (V3)]に移動し ます**。 図に示すように、[**Create** and **Configure**]をクリックします。

		Config	jure SnmpV3 Tra	р		×		8
Targ			et Address:		blr-ong-lnx10			6
		UDP	Port:		4576			6
		User	Name:		ank2	•		4
	Sec				noAuthNoPriv	•		з
			Filter Profile:					1
Tab View		Prox	y Traps Only:					
Alarms Conditions	History Circuits	Prox	y Tags:					
General Network	SNMP V1/V2 S			OK	Cancel			
IZO	General						1	
Protection	Users		64.103.217.88	4545	ank	authPriv	_V Level	
Security	MIB views		64.103.217.88	4565	ank1	authNoPriv	v	
SNMP	Group Access							
Comm Channels	Trap Destinations(V3)						
Liming	Notification Filte	rs						
Alarm Profiles								
			•					
SVLAN			Create	Edit Delete				
Alarm Extenders								

noAuthNoPrivモードの確認

ステップ1:NMSサーバに移動し、snmpwalkを実行します。

```
snmptrapd -f -Lo -OQ -Ob -Ot -F "%V\n%B\n%N\n%q\n%P\n%v\n\n" <port number>
Trap cmdはすべてのバージョンで同じです。
```

GNE/ENEセットアップのSNMP V3トラップ

GNEノード上

ステップ1: [Provisioning] > [SNMP] > [SNMP V3 and C]グループアクセス権の作成([Group Access]タブ):図に示すように、セキュリティレベル(noAuthnoPriv|AuthnoPriv|authPriv)とフルビ ューの読み取りおよび通知アクセスを持つグループ名を指定します。

- 1:1 36 - PTS	A_GE	8	Create Group Access		
🚥 Summary 📲 Ne	etwork	Group Name:	gnegrp 1	-	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 Notify Vi
Protection	User	Allow Child Cotes			fullview
Security		Allow SNMP Sets:			runnen
SNMP	Group Ac		h		
Comm Channels	Notification		OK Cancel		
Timing	Notification				
Alarm Profiles	L]
Defaults					
WDM-ANS					
SVLAN					
Alarm Extenders					
		Create	Edit Delete		

ステップ2:ユーザアクセス権の作成([Users]タブ):[グループアクセス(Group Access)]タブで以 前に作成したものと同じグループ名を持つユーザを作成します。また、図に示すように、アクセ スレベルに基づいて認証を提供します。

- : 8 - TSC - : 36 - PTS/	⊂GE ↓	約 User Name:	Create	e User		
Summary Reserved Summary Summary Summary Summary Summary Summary Alarms Condition	twork 107.114 ns History Circ SNMP V1/V2 St	Group Name: Authentication Protocol: Password:		gnegrp1 MD5		
OSI Protection Security SNMP Comm Channels Timing Alarm Profiles	General Users MIB views Group Access Trap Destination: Notification Filt	Privacy Protocol: Password:	ОК	DES ••••••••• Cancel		gne def
WDM-ANS SVLAN Alarm Extenders		Create	Edit Del	ete		

ステップ3:[Trap Destination(V3)]タブ:

ターゲットアドレス:トラップの実行元となるNMSサーバのアドレス(例:Blr-ong-Inx10)。

UDPポート:トラップが受信されるポート番号(例:9977)。

ユーザ名:[ユーザ(User)]タブのユーザの名前。

セキュリティレベル:[ユーザ(User)]タブで設定したとおり。

プロキシタグ:プロキシタグ(例:Tag75)。

- 1.1 8 - 15C	A_GE	1 0	Configure SnmpV3 Trap	×	Γ.
		Target Address:	bir-ong-inx10		
Summary Summary	etwork	UDP Port:	9999		
Alarms Condition	ns History Circ	User Name:	gneuser1	-	
General	SNMP V1/V2 SI	Security Level:	aut <mark>h</mark> Priv	-	
Network	General	Filter Profile:			Security Level
Protection	Users MIR views	Proxy Traps Only:			thPriv thPriv
Security SNMP	Group Access	Proxy Tags:	TagV3		
Comm Channels	Notification Filt				
Alarm Profiles			OK Cancel		
Defaults	L				
WDM-ANS					
Alarm Extenders					
		•	III		
		Create	Edit Delete		

ENEノード上

ステップ1:[Provisioning] > [SNMP] > [SNMP V3]に移動し、[Create Group Access]([Group Access]タブ)に移動します。図に示すように、アクセスレベル (noAuthnoPriv|AuthnoPriv|authPriv)とフルビューの読み取りおよび通知アクセスを持つグループ 名を指定します。

			l ── <mark>─ ⊢──</mark> ─────────────────────────────			
e 📅 [ENE]Node2	10 -	8	Create Gr	oup Access	×	
Summary 📲 Ne	twork	Group Name:		enegrp1	-	
15454 M2 ANS	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	*			1
Security	Crown Ad	Allow Shini Sets.	•	<u> </u>		
SNMP	Group Ac					
Comm Channels	Trap Destina		ОК	Cancel		
Timing	Notification					
Alarm Profiles	L					J
Defaults						
WDM-ANS						
SVLAN						
		Create	Edit Del	ete		
	L					

ステップ2:ユーザアクセス権の作成([Users]タブ):[グループアクセス(Group Access)]タブで以 前に作成したものと同じグループ名を持つユーザを作成します。また、アクセスレベルに基づい て認証を提供します。

- 1:1 36 - PTS	A_GE	() ()	●	×
 I 36 - PTS I 36 - PTS IENE]Node2 IENE]Node2 IS454 M2 ANS Alarms Condition General Network OSI Protection Security SNMP Comm Channels Timing 	A_GE 10 etwork I Node-75 ns History Circ SNMP V1/V2 SP General Users MIB views Group Access Trap Destination: Notification Filt	User Name: Group Name: Authentication Protocol: Password: Privacy Protocol: Password:	Create User Create User eneuser1 enegrp1 MD5 DEX Of Consul	
Alarm Profiles Defaults WDM-ANS SVLAN		Create Ec	dit Delete	

[User]タブに示されているdefault_groupが[Group Access]タブにない場合は、[Group access]タブ に作成されていることを確認します。 ステップ3:[Trap Destination(V3)]タブ:

ターゲットアドレス:GNEノードIP。

UDPポート: 162.

ユーザ名:[ユーザ(User)]タブのユーザの名前。

セキュリティレベル:[ユーザ(User)]タブで設定したとおり。

プロキシタグ:GNE(例:Tag75)。

- 1:1 36 - PTS				
[-] 50 - FIS		89	Configure SnmpV3 Trap	×
P 10 [ENE]Node2	10 🗸			
		Target Address:	10.64.107.114	
Summary 📴 Ne	etwork	UDP Port	162	
15454 M2 ANS	Node-75	0011010		
Alarms Condition	ns History Circ	User Name:	eneuser)	~
General		Security Level:	authPriv	
Network		Filter Profile		
OSI	General	Filter Profile:		Securit
Protection	Users MIR views	Proxy Traps Only:		thPriv
Security	Group Access	Proxy Tags	TagENE	
SNMP	Trap Destination	rioxy rugsi		
Comm Channels	Notification Filt			
Liming			OK Cancel	
Defaults				
WDM-ANS	_			
SVLAN				
		Create	Edit Delete	

CTCで、ネットワークビューに移動します。

ステップ1:[SNMPv3]タブ**に移動**します。

ステップ 2: SNMPv3プロキシトラップフォワーダテーブル:手動または自動**作成を**実行**できま** す。

[自動作成]を選択します。その下:

- ターゲットタグ:GNEで設定されたプロキシタグ。
- [Remote Trap Source List]:図に示すように、ENEノードIPを選択します。

Network Explorer 🗆 ×	Automatic Configuration of SNMPv3 Proxy Trap Forwar X	
	Target Tag: TagV3	
Summary 🔡 Network	Remote Trap Source List	9.4×
Alarms Conditions History	Circui 10.64.107.114	
Security	10.64.107.187	
Alarm Profiles	10.64.107.210	
BLSR	10.04.101.15	
Overhead Circuits		
Provisionable Patchcords (PPC)	Man	
Server Trails		
SNMPV3	OK Cancel Help	Late User
		authPriv
	0000059B2DFAA0003E8A8362 Tag114 ons_trap_user	authPriv
	Manual Create Delete SNMPv3 Remote Users Context Engine JD User Name Authenti	ication Protocol Prince/ Protocol
		Help

GNE/ENE設定の確認

NMSサーバ(blr-ong-Inx10)を設定します。

ステップ1 : サーバのホーム・ディレクトリで、ディレクトリを作成し、snmpという名前を付**け** ます。

ステップ2: このディレクトリの下に、snmptrapd.confファイルを作成します。

ステップ3: snmptrapd.confで、次の構成を作成します。

createUser -e 0x

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

authprivモードの場合:

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> authnoprivモードの場合:

<gne_ip_address> <OID> noauthnoprivモードの場合:

snmpwalk -v 3 -l authpriv -u

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。