

SIGMA**B**LADE

N8406-040/N8406-042
8G FC スイッチ
SNMP, Syslog 設定ガイド

2012 年 1 月 3 版
Jan 2012, 3rd Edition

著作権について

Copyright© 2012 NEC Corporation

ご注意

弊社の許可なく本書の複製や改変などを行うことはできません。

本書の内容の一部または全部を無断転載することは禁止されています。

本書の内容に関しては将来予告なしに変更することがあります。

NECが弊社の製品やサービスについて行う保証は、製品添付の保証文書に記載の内容のみに限定されます。

本書のどの個所であっても何ら新規の保証を行うものではありません。

本書に記載された内容は、本書作成時における参考情報の提供のみを目的としており、明示または黙示にかかわらず、本書の情報についてNECは一切の責任を負わないものとします。

本書の内容に基づき運用した結果の影響については、責任を負いかねますのでご了承ください。

目次

1.	はじめに.....	4
1. 1	本書の目的.....	4
1. 2	対象製品.....	4
2.	コマンドの詳細.....	5
	SNMPCONFIG SNMPエージェント構成を管理します。.....	5
	SNMPTRAPS SNMPのトラップを送出、あるいは表示します。.....	8
	SYSLOGDFACILITY SYSLOG FACILITYを変更します。.....	10
	SYSLOGDIPADD SYSLOGデーモンのIPアドレスを追加します。.....	11
	SYSLOGDIPREMOVE SYSLOGデーモンのIPアドレスを追加します。.....	12
	SYSLOGDIPSHOW 設定されているSYSLOGデーモンのIPアドレスを表示します。.....	13
3.	設定例.....	14
3. 1	SYSLOG設定例.....	14
3. 2	SNMP設定例.....	15

1. はじめに

1. 1 本書の目的

本書はNECブレードシステム「SIGMABLADE」の内蔵オプション製品、N8406-040/042 8G FCスイッチでのSNMP(Simple Network Management Protocol)、およびsyslogを使用した監視を行う場合のコマンド一覧、および実機での確認結果を基にした設定例について参考情報として示します。

なお、SNMPによる監視等を行う場合の本製品に対応したプライベートMIB(Management Information Base)ファイルの入手につきましては、製品サポート窓口までお問い合わせください。

また、MIB監視をするアプリケーションによっては、以下のMIBも別途必要になる場合がありますので、必要に応じ入手をお願いします。

FCマネージメントMIB入手先 (2012/1/28現在)

RFC4044 MIB: <http://www.icir.org/fenner/mibs/extracted/FC-MGMT-MIB-rfc4044.txt>

RFC2026 MIB: <http://www.icir.org/fenner/mibs/extracted/FCMGMT-MIB-ipfc-07.txt>

1. 2 対象製品

本書は、以下のFibre Channel スイッチ関連製品のSNMP、およびSyslogの転送設定についての説明を行います。

- | | | |
|---|-----------|------------------|
| ・ | N8406-040 | 8G FCスイッチ(12ポート) |
| ・ | N8406-042 | 8G FCスイッチ(24ポート) |

2. コマンドの詳細

snmpConfig SNMPエージェント構成を管理します。

構文

```
snmpConfig [--show | --set | --default] [snmpv1 | snmpv3 |  
accessControl | mibCapability | systemGroup | SecLevel]
```

機能

このコマンドを使用して、スイッチでの SNMP エージェントの構成を管理してください。

構成は SNMPv1、SNMPv3 構成、アクセスコントロールリスト (ACL)、MIB 能力、およびシステムグループを含んでいます。

このコマンドはデフォルトとして、設定、設定初期化及び設定表示機能をサポートします。

このコマンドは設定が終了した時点で内容が即時有効となり設定、表示されます。

オペランド

このコマンドには、次のオペランドがあります。

--Show 指定されたカテゴリに関する SNMP エージェントコンフィギュレーション・データを表示します。

--Set SNMP エージェントコンフィギュレーション・データを設定します。
指定したカテゴリの現在の設定を表示して、次に、ユーザが各パラメタの値を変えるようにうながします。

--Default デフォルト値に SNMP エージェントを設定します。

--Show NTP サーバの動作するサーバ IP アドレスを指定します。

このコマンドは次のオペランドをサポートします；

snmpv1 SNMPv1 の関連する構成を選択します。
SNMPv1 パラメタはコミュニティストリング、送信先 IP アドレスと Trap Severity Level の関連づけます。

snmpv3 SNMPv3 の関連する構成を選択します。
SNMPv3 パラメタはユーザ名、認証プロトコル/パスワード、プライバシープロトコル/パスワード、ip アドレス、ユーザインデックス、および Trap Severity Level を関連づけます。

accessControl アクセス制御関連するパラメタを選択します。
accessControl パラメタは Access ホストサブネット領域と参照許可を含んでいます(Read-Write)。

mibCapability SNMP エージェント MIBS と TRAP 能力パラメタに関連する構成パラメタを選択します。
mibCapability パラメタは SNMP エージェントによってサポートされた mibs と Trap を含んでいます。

systemGroup システムグループに関連する構成パラメタを選択します。
systemGroup パラメタは sysDescr、sysLocation、sysContact、および認証失敗時の Trap を含んでいます。

secLevel SNMP セキュリティレベルを設定します。

SNMPv1 構成パラメタ :

エージェントによって支持された 6 つの Community、それぞれの Trap 受取先、および Severity Level があります。最初の 3 つの Community が Read-Write(rw)アクセスのためのものです、そして、最後の 3 は読み込み専用(ro)アクセスのためのものです。

注意 : それぞれの Community の Trap 受取先のデフォルト値は'0.0.0.0'となります。

Community 名の長さは 2--16 のキャラクタの範囲で変更可能です。 Community 名デフォルトは以下の通りです。

Community 1: Secret C0de
Community 2: OrigEquipMfr
Community 3: private
Community 4: public
Community 5: common
Community 6: FibreChannel

Severity Level 設定 :

Severity Level によりイベントの Trap レベルを変更する。

イベントが起こったとき、Severity Level の設定値がイベントレベル以下の場合、SNMP Trap は Event Trap(swEventTrap、connUnitEventTrap、および swFabricWatchTrap)を送信します。

Severity Level の設定はデフォルトで、0 に設定されています。(Event Trap は送信されません)

0 - none
1 - critical
2 - error
3 - warning
4 - informational
5 - debug

SNMPv3 構成パラメタ :

エージェントによって支持された 6 つの Community、それぞれの Trap 受取先、および Severity Level があります。最初の 3 つの Community が Read-Write(rw)アクセスのためのものです、そして、最後の 3 は読み込み専用(ro)アクセスのためのものです。

注意 : それぞれの Community の Trap 受取先のデフォルト値は'0.0.0.0'となります。

Community 名の長さは 2--16 のキャラクタの範囲で変更可能です。 Community 名デフォルトは以下の通りです。

Snmpadmin および snmpuser の 2 つのユーザ定義が規定されています。Snmpadmin は読み取り - 書き込みアクセスを許可し、snmpuser は読み取り専用アクセスを許可します。エントリはそれぞれの規定に対応する USM テーブルに追加されます。Snmpadmin の 3 つのエントリと snmpuser の 3 つのエントリの合計がサポートされます。別々のデフォルトパスワードが、各エントリに authKey および privKey を生成するために与えられます。デフォルトパスワードのセットが発行され、デフォルトのアルゴリズム (MD5/SHA) が、認証キーの最初のセットを生成するために使用されます。これらのパスワードの変更はこのオプションを使用して行うことができます。認証プロトコル MD5/ SHA またはエントリ認証なしの選択は任意です。

次のプロトコルの組合せを選択します。

NoAuth/NoPriv
Auth/NoPriv
Auth/Priv

ユーザ名の文字列の長さは 2 から 32 文字以内でなければなりません。デフォルトのユーザ名は noAuth および noPriv プロトコルで定義されることに注意してください。出荷時の SNMPv3 ユーザ名設定は次のとおりです。

User 1: snmpadmin1

```
User 2: snmpadmin2
User 3: snmpadmin3
User 4: snmpuser1
User 5: snmpuser2
User 6: snmpuser3
```

ユーザがオプション `--default` を選択する場合には、ユーザ名とパスワードはデフォルトに設定されます。

ユーザのコンフィグレーションは、セキュアモードでも非セキュアモードでも利用することができます。セキュアモードにおいては、上記のコンフィグレーションは、プライマリおよび非プライマリスイッチの両方で個別にユーザにより更新されなければなりません。そして、コミュニティの文字列とは違い、ユーザ名とパスワード はファブリック内の他のスイッチには配信されません。 何らかのユーザエントリに対し新しいパスワードが入力されると、新しい `authKey` および `privKey` が生成されます。クライアント（MIB ブラウザのような）上で、この新しいパスワードを更新する必要があります。

また、`authKey` および `privKey` は、SNMPv3 プロトコルにより与えられる `delta key` メカニズムを使用して更新することもできます。 `NoAuth/NoPriv` 以外のプロトコルが選択される場合には、パスワードとパスワードの再確認がプロンプトされます。プロトコルのパスワードの長さは 1 から 20 文字以内でなければなりません。

SNMP 管理ステーションが、エージェントにより作成された SNMPv3 トラップを検索するために、管理者は、管理ステーションの IP アドレスに対応する トラップ受信者の値をコンフィグしなければなりません。加えて、トラップ 受信者は、`accessControl` の項で説明のとおり、ACL のチェックをパスできなければなりません。トラップ受信者の値は、SNMPv3 の 6 ユーザの内の 1 つ およびトラップの重大度レベルと関連していなければなりません。各ユーザ の SNMPv3 のトラップ受信者に対する工場出荷時のデフォルト設定が '0.0.0.0' であることに注意してください。

アクセスコントロールパラメータ：

このオプションを指定することで、スイッチでの **SNMP** アクセスを特定のサブネットやホストに制限をする（アクセスコントロール）を実施することができます。

Mib Capability コンフィグレーションパラメータ：

このオプションを指定することで、スイッチでの **SNMP** エージェントの構成を管理することができます。このオプションで、ユーザは特定の **MIBS** とトラップを有効または無効にできます。また、**SW** トラップメッセージとグループ情報も有効または無効にできます。最初に現行の設定を表示し、その後でユーザは、各パラメータの値を変更するようプロンプトされます。

FA-MIB	yes を指定すると、ユーザは SNMP マネジャで FA-MIB 変数 にアクセスできます。デフォルト値は yes です。
HA-MIB	yes を指定すると、ユーザは SNMP マネジャで HA-MIB 変数 にアクセスできます。デフォルト値は yes です。
SW-TRAP	yes を指定すると、SNMP 管理アプリケーションはそのスイッチから SW-TRAPS を受信できます。デフォルト値は yes です。
FA-TRAP	yes を指定すると、SNMP 管理アプリケーションはそのスイッチから FA-TRAPS を受信できます。デフォルト値は yes です。
SW-EXTTRAP	yes を指定すると、SNMP 管理アプリケーションはそのスイッチから SW-EXTTRAPS を受信できます。デフォルト値は yes です。
HA-TRAP	yes を指定すると、SNMP 管理アプリケーションはそのスイッチから HA-TRAPS を受信できます。デフォルト値は yes です。

Security Level 設定：

Security Level により SNMP Security レベルを変更する。

- 0 - No Security
- 1 - Authentication Only
- 2 - Authentication and Privacy
- 3 - OFF

snmpTraps SNMPのトラップを送出、あるいは表示します。

構文

```
snmptraps -- send [-trap_name trap_name] [-ip_address ipaddress]
snmptraps -- show
snmptraps -- help
```

機能

このコマンドは SNMP トラップの受け取り等確認等のために使用します。

このコマンドを使用して、特殊な Simple Network Management Protocol (SNMP) のトラップを送出したり、あるいはトラップの受け取り側の受信確認を実施したり、MIB オブジェクトと関連したトラップを有効にしたりすることができます。

‘— send’ オプションを使用して SNMP トラップの送出行います。IP アドレスを設定することでトラップの送先を指定します。また、トラップ名を設定することで、設定したトラップを送出することができます。

また ‘— send’ オプションをオペランドなしで使用することですべての IP アドレスに対して、サポートしているすべての MIB および SNMP トラップを送出します。

‘— show’ を使用することで FabricOS でサポートしているすべての MIB および SNMP トラップを表示します。

なお、本コマンドを使用して IPv6 で定義されたアドレスに SNMP トラップを送出することはできません。

オペランド

このコマンドには、次のオペランドがあります。

—Send 指定されたカテゴリに関する SNMP エージェントコンフィギュレーション・データを表示します。

—Show FabricOS でサポートしているすべての MIB および SNMP トラップを表示します。

—Help コマンドの使用方法を表示します。

使用例

サポートしているすべての SNMP トラップと MIB を表示します。

```
switch:admin> snmpTraps --show
# |Mib Name |Supported Traps
---|-----|-----
001|SW-MIB |sw-track-changes-trap
   |      |sw-fabric-watch-trap
   |      |sw-fault
   |      |sw-fc-port-scn
   |      |sw-sensor-scn
   |      |ip-v6-change-trap
002|FICON-MIB |link-rnid-device-registration
   |      |link-rnid-device-deregistration
   |      |link-lirr-listerner-added
   |      |link-lirr-listerner-removed
003|FA-MIB |conn-unit-status-change
   |      |conn-unit-sensor-status-change
   |      |conn-unit-port-status-change
   |      |conn-unit-port-status-change-end
004|RFC1157 |cold-restart-trap
   |      |warm-restart-trap
   |      |if-link-up-trap
   |      |if-link-down-trap
   |      |snmp-authetication-trap
005|HA-MIB |fru-status-change-trap
   |      |fru-history-trap
   |      |cp-status-change-trap
```

Link-rnid-device-registration メッセージを 172.16.0.12 で受け取ります。

```
switch:admin> snmptraps --send -trap_name link-rnid-device-registration -ip_address 172.16.0.12.
```

syslogdFacility Syslog facilityを変更します。

構文

syslogdFacility [-l level]

機能

このコマンドを使用し、syslog のログの出力先を規定する facility レベルを変更することができます。

LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3, LOG_LOCAL4, LOG_LOCAL5, LOG_LOCAL6, 又は LOG_LOCAL7 に変更してください。Syslog デーモン(syslogd)は殆どの UNIX システムで利用可能なプロセスでありユーザーによるシステム設定により Log ファイルへの書き込み、適切なユーザーへの転送が可能です。

指定された facility はメッセージをコマンド syslogdIpAdd で追加されたサーバに送信するときに使用されます。Facility のデフォルトは LOG_LOCAL7 です。

オペランド

-l level syslog facility を指定します。指定範囲は 0~7 です。このオペランドは任意であり、もし省略すると現在の facility を表示します。

参照コマンド

syslogdIpAdd

syslogdIpRemove

syslogdIpShow

syslogdIpAdd SyslogデーモンのIPアドレスを追加します。

構文

syslogdipadd ip_address

機能

このコマンドを使用し、syslog を転送するサーバの IP アドレスを追加します。1 つ以上の IP アドレスが設定された場合スイッチはすべてのエラーログエントリを、指定されたサーバ上の syslog デーモン (syslogd) に送ります。syslog デーモンは、システムメッセージを読み取り、システムコンフィグレーションに基づいて、該当するログファイルまたはユーザに転送を行うプロセスであり、ほとんどの UNIX システム上で利用可能なプロセスです。6 つのサーバまでサポートされます。

オペランド

Ip_address syslog を記録させる syslog デーモン (syslogd) が実行されているサーバの IP アドレスを指定します。このオペランドは必須です。IP アドレスは IPv4、IPv6 どちらのフォーマットでも指定可能です。

参照コマンド

syslogdFacility

syslogdIpRemove

syslogdIpShow

syslogdIpRemove SyslogデーモンのIPアドレスを追加します。

構文

syslogdipremove *ip_address*

機能

このコマンドを使用し、syslog デーモンを実行しているサーバの IP アドレスを設定を削除します。

オペランド

Ip_addres syslog を記録させる syslog デーモン (syslogd) が実行されているサーバの IP アドレスを指定します。このオペランドは必須です。

参照コマンド

syslogdFacility

syslogdIpAdd

syslogdIpShow

syslogdIpShow 設定されているSyslogデーモンのIPアドレスを表示します。

構文

Syslogdipshow

機能

このコマンドは、本スイッチのコンフィギュレーションに設定されている syslog デーモン (syslogd) の IP アドレス情報を表示します。

オペランド

なし

参照コマンド

syslogdFacility

syslogdIpAdd

syslogdIpRemove

3. 設定例

3. 1 syslog設定例

コマンド: **syslogdipadd**

Syslog を記録するホストの IP アドレスを syslogdipadd コマンドを使用して設定します。

設定例)

```
switch:admin> syslogdipadd 192.168.1.60
Committing configuration...done.
switch:admin>
```

コマンド: **syslogdipshow**

syslog を記録させるホストの IP アドレスを確認するには syslogdipshow コマンドを使用します。

表示例)

```
switch:admin> syslogdipshow
syslog. IP.address.1: 192.168.1.60
switch:admin>
```

← IP アドレスが一致していることを確認します。

コマンド: **syslogdfacility**

Syslog のファシリティを変更するには syslogdfacility コマンドを使用します。

表示例)

```
switch:admin> syslogdfacility -l 1
Syslog facility changed to LOG_LOCAL1
switch:admin>
```

← LOCAL レベルが変更されてしていることを確認します。

3. 2 SNMP設定例

コマンド: `snmpConfig`

SNMP 関連の設定をするには `snmpConfig` コマンドを使用します。

実施例)

SNMPv1のコンフィグレーションを確認する：

```
switch:admin> snmpConfig --show snmpv1
SNMPv1 community and trap recipient configuration:
Community 1: Secret C0de (rw)
Trap recipient: 10.32.147.113
Trap recipient Severity Level: 0
Community 2: OrigEquipMfr (rw)
Trap recipient: 1080::8:800:200C:1234
Trap recipient Severity Level: 0
Community 3: private (rw)
No trap recipient configured yet
Community 4: public (ro)
No trap recipient configured yet
Community 5: common (ro)
No trap recipient configured yet
Community 6: FibreChannel (ro)
No trap recipient configured yet
```

SNMPv1のコンフィグレーションを設定する：

```
switch:admin> snmpConfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address: [0.0.0.0] 1080::8:800:200C:1234
Community (rw): [OrigEquipMfr]
string size must be between 2 and 16 - please re-enter
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address: [1080::8:800:200C:1230] 10.32.147.113
Community (rw): [private]
Trap Recipient's IP address: [0.0.0.0]
Community (ro): [public]
Trap Recipient's IP address: [0.0.0.0]
Community (ro): [common]
Trap Recipient's IP address: [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address: [0.0.0.0]
```

SNMPアクセスを特定のサブネットやホストに制限をする（アクセスコントロールの実施）：

```
switch:admin> snmpconfig --set accessControl
SNMP access list configuration:
Access host subnet area in dot notation: [0.0.0.0] 192.168.0.0
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0] 10.32.148.0
Read/Write? (true, t, false, f): [true] f
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0] 10.33.0.0
Read/Write? (true, t, false, f): [true] f
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Committing configuration...done.
```

mibCapabilityコンフィグレーションの設定を確認する：

```
switch:admin> snmpconfig --show mibCapability
FE-MIB: YES
SW-MIB: YES
FA-MIB: YES
FICON-MIB: YES
HA-MIB: YES
FCIP-MIB: YES
ISCSI-MIB: YES
SW-TRAP: YES
swFCPortScn: YES
swEventTrap: YES
swFabricWatchTrap: YES
swTrackChangesTrap: YES
FA-TRAP: YES
connUnitStatusChange: YES
connUnitEventTrap: YES
connUnitSensorStatusChange: YES
connUnitPortStatusChange: YES
SW-EXTTRAP: YES
FICON-TRAP: YES
linkRNIDDeviceRegistration: YES
linkRNIDDeviceDeRegistration: YES
linkLIRRLListenerAdded: YES
linkLIRRLListenerRemoved: YES
linkRLIRFailureIncident: YES
HA-TRAP: YES
fruStatusChanged: YES
cpStatusChanged: YES
fruHistoryTrap: YES
FCIP-TRAP: YES
linkUpTrap: YES
linkDownTrap: YES
```


systemGroupのコンフィグレーションの設定を初期値に戻す：

```
switch:admin> snmpconfig --default systemGroup
*****
This command will reset the agent's system group
configuration back to factory default
*****
sysDescr = Fibre Channel Switch
sysLocation = End User Premise
sysContact = Field Support
authTraps = 0 (OFF)
*****
Are you sure? (yes, y, no, n): [no] y
```

セキュリティーレベルの設定をおこなう：

```
switch:admin> snmpconfig --set seclevel
Select SNMP Security Level
(0 = No security, 1 = Authentication only,
2 = Authentication and Privacy, 3 = No Access): (0..3) [0] 1
Select SNMP SET Security Level
(0 = No security, 1 = Authentication only,
2 = Authentication and Privacy, 3 = No Access): (1..3) [1]
```

SNMP3のコンフィグレーション設定を確認する：

```
switch:admin> snmpconfig --show snmpv3
SNMP Informs = 1 (ON)
SNMPv3 USM configuration:
User 1 (rw): snmpadmin1
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 00:00:00:00:00:00:00:00
User 2 (rw): snmpadmin2
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 80:00:05:23:01:0a:23:34:22
User 3 (rw): snmpadmin3
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 00:00:00:00:00:00:00:00
User 4 (ro): snmpuser1
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 00:00:00:00:00:00:00:00
User 5 (ro): snmpuser2
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 00:00:00:00:00:00:00:00
User 6 (ro): snmpuser3
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 00:00:00:00:00:00:00:00
SNMPv3 Trap configuration:
Trap Entry 1: No trap recipient configured yet
Trap Entry 2: 10.35.52.34
Trap Port: 162
Trap User: snmpadmin2
Trap recipient Severity level: 5
Trap Entry 3: No trap recipient configured yet
Trap Entry 4: No trap recipient configured yet
Trap Entry 5: No trap recipient configured yet
Trap Entry 6: No trap recipient configured yet
```

TRAP要求の代わりにinformリクエストをenableに設定する：

```
switch:admin>snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false] t
SNMPv3 user configuration(snmp user not configured in FOS user
database will have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0]
User (rw): [snmpadmin2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0]
User (rw): [snmpadmin3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0]
User (ro): [snmpuser1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0]
User (ro): [snmpuser2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0]
User (ro): [snmpuser3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0]
SNMPv3 trap recipient configuration:
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [10.32.147.6]
UserIndex: (1..6) [2]
Trap recipient Severity level : (0..5) [5]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
```

保護用紙

N8406-040/N8406-042
8G FC スイッチ
SNMP、Syslog 設定ガイド

2012 年 1 月 第 3 版

日 本 電 気 株 式 会 社
東京都港区芝五丁目7番1号
TEL (03) 3454-1111 (大代表)

© NEC Corporation 2012