CHAPTER 7

SNMP の設定

CLI と SNMP は、Cisco MDS 9000 ファミリのすべてのスイッチで共通のロールを使用します。SNMP を使用して CLI で作成したロールを変更したり、その逆を行うことができます。

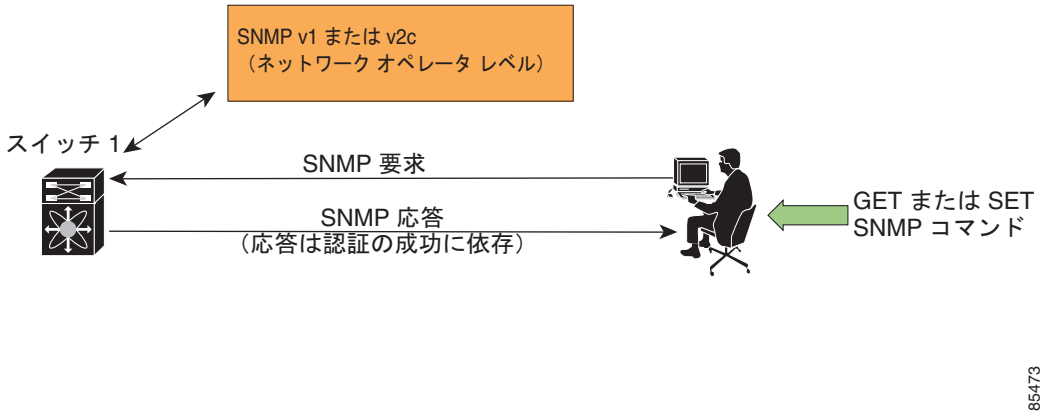
CLI ユーザと SNMP ユーザのユーザ、パスワード、ロールは、すべて同じです。CLI を通じて設定されたユーザは SNMP（たとえば、Fabric Manager や Device Manager）を使用してスイッチにアクセスでき、その逆も可能です。

この章の内容は、次のとおりです。

SNMP セキュリティの概要

SNMP は、ネットワーク デバイス間で管理情報をやり取りするためのアプリケーション レイヤ プロトコルです。すべての Cisco MDS 9000 ファミリ スイッチで、SNMPv1、SNMPv2c、および SNMPv3 の 3 つの SNMP バージョンが使用できます（図 7-1 を参照）。

図 7-1　　SNMP セキュリティ



ここで説明する内容は、次のとおりです。

SNMP バージョン 1 およびバージョン 2c

SNMP バージョン 1（SNMPv1）および SNMP バージョン 2c（SNMPv2c）は、コミュニティ ストリングを使用してユーザ認証を行います。コミュニティ ストリングは、SNMP の初期のバージョンで使用されていた弱いアクセス制御方式です。SNMPv3 は、強力な認証を使用することによってアクセス制御を大幅に改善しています。したがって、SNMPv3 がサポートされている場合は、SNMPv1 および SNMPv2c に優先して使用してください。

SNMP バージョン 3

SNMP バージョン 3（SNMPv3）は、ネットワーク管理のための相互運用可能な標準ベースのプロトコルです。ネットワーク上でのフレームの認証および暗号化を組み合わせることによって、デバイスへの安全なアクセスを提供します。SNMPv3 で提供されるセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：有効な送信元からのメッセージであるかどうかを判別します。
- 暗号化：パケット内容をスクランブルし、不当に読み取られないようにします。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザおよびユーザが所属するロールに対して設定する認証ストラテジです。セキュリティ レベルは、セキュリティ モデルの中で許容されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットの取り扱いに適用されるセキュリティ メカニズムが決まります。

SNMP スイッチの連絡先情報と場所情報の割り当て

32 文字以内（スペースを除く）のスイッチの連絡先情報と、スイッチの場所を割り当てることができます。

Fabric Manager を使用して、連絡先情報と場所情報を設定するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインの [Switches] を展開します。[Information] ペインにスイッチの設定が表示されます。

ステップ 2　各スイッチの [Location] フィールドと [Contact] フィールドに値を設定します。

ステップ 3　これらの変更を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を廃棄する場合は、[Undo Changes] をクリックします。

SNMPv3 CLI のユーザ管理および AAA の統合

Cisco NX-OS ソフトウェアは RFC 3414 と RFC 3415 を実装しています。これには、User-based Security Model（USM; ユーザベース セキュリティ モデル）とロール ベースのアクセス制御が含まれています。SNMP と CLI のロール管理は共通化されており、同じ証明書とアクセス権限を共有しますが、以前のリリースではローカル ユーザ データベースは同期化されませんでした。

SNMPv3 のユーザ管理を AAA サーバ レベルで一元化できます。ユーザ管理を一元化すると、Cisco MDS スイッチ上で稼動する SNMP エージェントが AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が確認されると、SNMP PDU は次の段階へと処理されます。また、AAA サーバにはユーザ グループ名も格納されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス / ロール ポリシーを適用します。

ここで説明する内容は、次のとおりです。

CLI および SNMP のユーザ同期

ユーザ グループ、ロール、またはパスワードの設定が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

ユーザの同期化は、次のように処理されます。

- いずれかのコマンドを使用してユーザを削除すると、SNMP と CLI の両方の該当ユーザが削除されます。
- ユーザとロールの対応関係は、SNMP と CLI で同期化されます。

（注）　パスフレーズ / パスワードをローカライズド キー / 暗号化形式で指定すると、パスワードは同期化されません。

（注）　3.0(1) から、Fabric Manager 用に作成された一時的な SNMP ログインを使用できるのは、24 時間ではなく、1 時間になりました。

- 既存の SNMP ユーザは、auth および priv パスフレーズを現状どおり継続して使用します。
- 管理ステーションが usmUserTable 内に SNMP ユーザを作成する場合、対応する CLI ユーザはパスワードなし（ログインは無効）で作成され、network-operator のロールが付与されます。

スイッチ アクセスの制限

IP Access Control List（IP-ACL; IP アクセス コントロール リスト）を使用して、Cisco MDS 9000 ファミリ スイッチへのアクセスを制限できます。

グループベースの SNMP アクセス

（注）　*グループ*は業界全体で使用されている標準的な SNMP 用語であるため、SNMP に関するこの項では、「ロール」のことを「グループ」で表します。

SNMP アクセス権限は、グループ単位で編成します。SNMP の各グループは、CLI におけるロールと類似しています。各グループは、読み取りアクセス、書き込みアクセス、および通知アクセスの 3 つのアクセスで定義されます。それぞれのアクセスを、各グループでイネーブルまたはディセーブルに設定できます。

ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

ユーザの作成および変更

SNMP、Fabric Manager、または CLI を使用して、ユーザの作成、または既存のユーザの変更を実行できます。

- SNMP：スイッチ上の usmUserTable に存在するユーザのクローンとして、新規のユーザを作成します。ユーザを作成した後、クローンの秘密鍵を変更してから、そのユーザをアクティブにします。RFC 2574 を参照してください。
- Fabric Manager。
- CLI：**snmp-server user** コマンドを使用して、ユーザの作成または既存のユーザの変更を実行します。

Cisco MDS 9000 ファミリ スイッチ上で使用できるロールは、network-operator および network-admin です。GUI（Fabric Manager および Device Manager）を使用する場合は、default-role もあります。また、Common Roles データベースに設定されている任意のロールも使用できます。

ヒント　CLI セキュリティ データベースおよび SNMP ユーザ データベースに対する更新はすべて同期化されます。SNMP パスワードを使用して、Fabric Manager または Device Manager のいずれかにログインできます。ただし、CLI パスワードを使用して Fabric Manager または Device Manager にログインした場合、その後のログインには必ず CLI パスワードを使用する必要があります。Cisco MDS SAN-OS Release 2.0(1b) にアップグレードする前から SNMP データベースと CLI データベースの両方に存在しているユーザの場合、アップグレードすると、そのユーザに割り当てられるロールは両方のロールを結合したものになります。

ここで説明する内容は、次のとおりです。

AES 暗号化ベースのプライバシ

Advanced Encryption Standard（AES）は対称暗号アルゴリズムです。Cisco NX-OS ソフトウェアは、SNMP メッセージ暗号化用のプライバシ プロトコルの 1 つとして AES を使用し、RFC 3826 に準拠しています。

priv オプションで SNMP セキュリティ暗号化方式として、DES または 128 ビット AES 暗号化を選択できます。**priv** オプションを **aes-128** トークンと併用すると、プライバシ パスワードは 128 ビット AES キーの生成に使用されます。AES のプライバシ パスワードは最小で 8 文字です。パスフレーズをクリアテキストで指定する場合、最大 64 文字を指定できます。ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

（注） 外部の AAA サーバを使用して SNMPv3 を使う場合、外部 AAA サーバのユーザ設定でプライバシ プロトコルに AES を指定して、SNMP PDU を暗号化する必要があります。

SNMPv3 メッセージ暗号化の適用

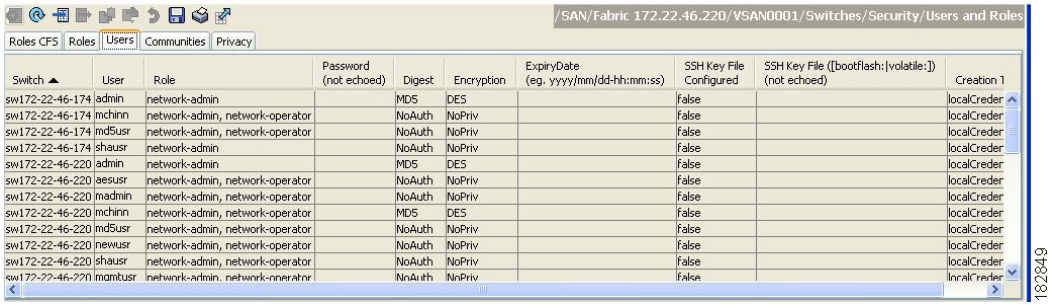
デフォルトでは、SNMP エージェントは、auth キーと priv キーを使用したユーザ設定の SNMPv3 メッセージ暗号化を使用する。SNMPv3 メッセージの authNoPriv および authPriv の securityLevel パラメータを許可します。

Fabric Manager を使用してユーザのメッセージ暗号化を適用するには、次の手順を実行します。

ステップ 1　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [Users and Roles] を選択します。

ステップ 2　[Information] ペインの [Users] タブをクリックし、図 7-2 に示すようなユーザのリストを表示します。

図 7-2　[Users] タブのユーザ情報



ステップ 3　[Create Row] をクリックします。

[Create Users] ダイアログボックスが表示されます。

ステップ 4　[New User] フィールドにユーザ名を入力します。

ステップ 5　[Role] ドロップダウン メニューからロールを選択します。ドロップダウン メニューから選択しない場合は、フィールドに新しいロール名を入力できます。その場合、前に戻ってこのロールを適切に設定する必要があります。

ステップ 6　[Password] フィールドにユーザのパスワードを入力します。

ステップ 7　[Privacy] タブをクリックします（図 7-3 を参照）。

図 7-3　[Privacy] タブ

ステップ 8　[Enforce SNMP Privacy Encryption] チェックボックスをオンにし、管理トラフィックを暗号化します。

ステップ 9　[Create] をクリックして新しいエントリを作成します。

Fabric Manager を使用し、SNMPv3 メッセージ暗号化を、すべてのユーザに対してグローバルに適用するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで [VSAN] を選択します。この操作は、[All VSANS] を選択する場合は実行できません。

ステップ 2　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [Users and Roles] を選択します。[Information] ペインで [Global] タブをクリックします。

ステップ 3　[GlobalEnforcePriv] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

SNMPv3 ユーザの複数のロールへの割り当て

SNMP サーバのユーザ設定が強化され、SNMPv3 ユーザに複数のロール（グループ）を割り当てることが可能になっています。最初に SNMPv3 ユーザを作成した後で、そのユーザにロールを追加できます。

（注）　他のユーザにロールを割り当てることができるのは、ロール network-admin に属するユーザだけです。

Fabric Manager を使用して複数のロールを新しいユーザに追加するには、次の手順を実行します。

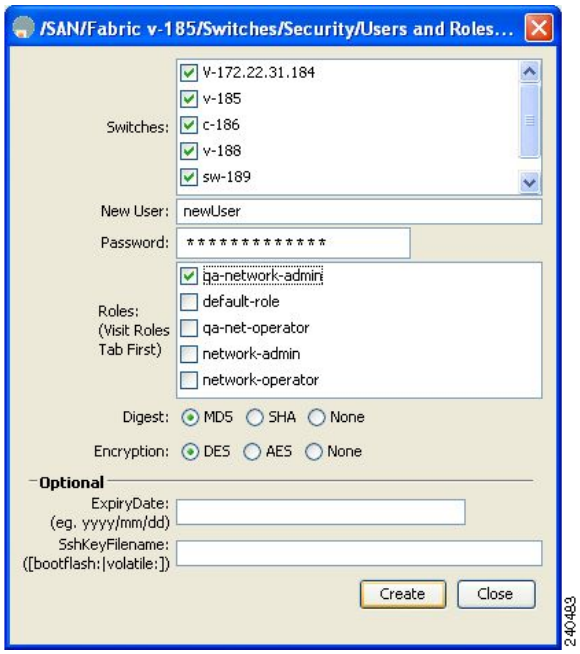
ステップ 1　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [Users and Roles] を選択します。

ステップ 2　[Information] ペインの [Users] タブをクリックし、図 7-2 に示すようなユーザのリストを表示します。

ステップ 3　[Create Row] をクリックします。

[Create Users] ダイアログボックスが表示されます（図 7-4 を参照）。

図 7-4　[Create Users] ダイアログボックス



ステップ 4　チェックボックスを使用してロールを選択します。

ステップ 5　[Digest] と [Encryption] のそれぞれのオプションを選択します。

ステップ 6　（オプション）ユーザの有効期限と、SSH キーのファイル名を入力します。

ステップ 7　[Create] をクリックして新しいロールを作成します。

コミュニティの追加

SNMPv1 および SNMPv2 のユーザの場合は、読み取り専用または読み取り / 書き込みアクセスを設定できます。RFC 2576 を参照してください。

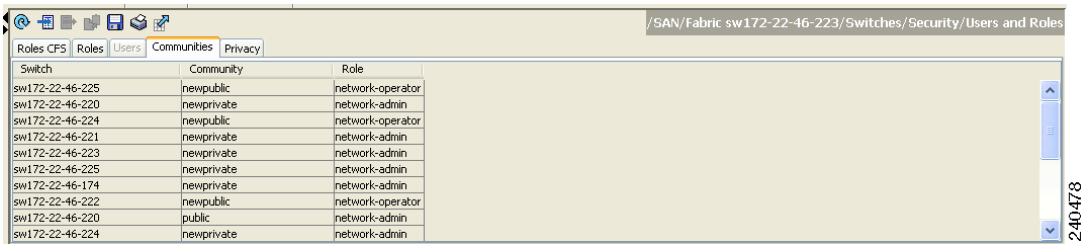
Fabric Manager を使用して SNMPv1 または SNMPv2c のコミュニティ ストリングを作成するには、次の手順を実行します。

ステップ 1　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [Users and Roles] を選択します。

ステップ 2　[Information] ペインで [Communities] タブをクリックします。

既存のコミュニティが表示されます（図 7-5 を参照）。

図 7-5　[Users and Roles] の [Communities] タブ



ステップ 3　[Create Row] をクリックします。

[Create Community String] ダイアログボックスが表示されます。

ステップ 4　[Switch] のチェックボックスをオンにし、1 つ以上のスイッチを指定します。

ステップ 5　[Community] フィールドにコミュニティ名を入力します。

ステップ 6　[Role] ドロップダウン リストからロールを選択します。

（注）　ドロップダウン リストから選択しない場合は、フィールドに新しいロール名を入力できます。その場合、前に戻ってこのロールを適切に設定する必要があります。

ステップ 7　[Create] をクリックして新しいエントリを作成します。

コミュニティ ストリングの削除

Fabric Manager を使用してコミュニティ ストリングを削除するには、次の手順を実行します。

ステップ 1　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [Users and Roles] を選択します。

ステップ 2　[Information] ペインで [Communities] タブをクリックします。

ステップ 3　削除するコミュニティの名前をクリックします。

ステップ 4　[Delete Row] をクリックしてこのコミュニティを削除します。

SNMP トラップとインフォーム通知

特定のイベントが発生したときに SNMP マネージャに通知を送信するように Cisco MDS スイッチを設定できます。

（注）　通知をトラップまたはインフォームとして送信する宛先の詳細情報を入手するには、SNMP-TARGET-MIB を使用します。詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

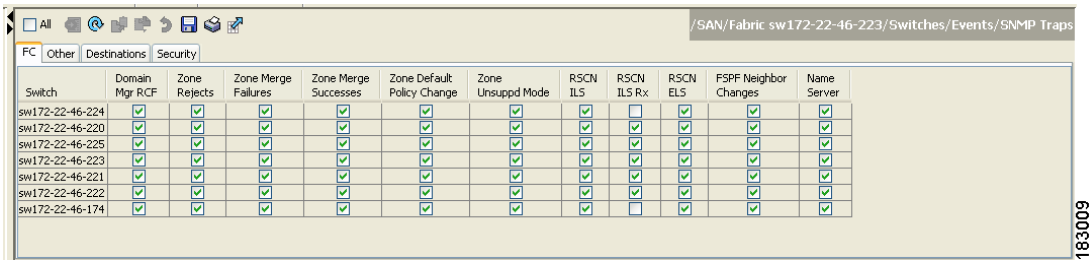
ここで説明する内容は、次のとおりです。

SNMPv2c 通知の設定

Fabric Manager を使用して SNMPv2c 通知を設定するには、次の手順を実行します。

ステップ 1　[Switches] > [Events] の順に展開し、[Physical Attributes] ペインで [SNMP Traps] を選択します。
[Information] ペインに SNMP 通知の設定が表示されます（図 7-6 を参照）。

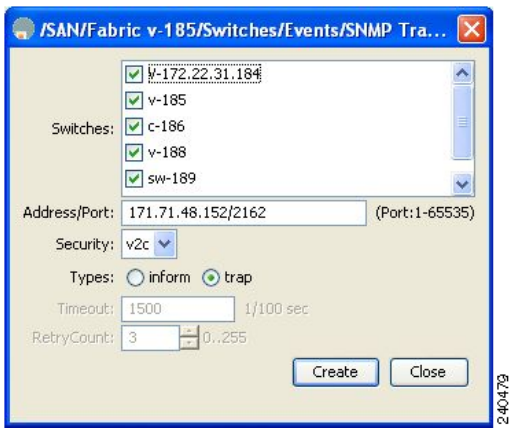
図 7-6　SNMP 通知



ステップ 2　[Destinations] タブをクリックして、SNMP 通知の宛先を追加または変更します。

ステップ 3　[Create Row] をクリックして、新しい通知先を作成します。
[Create Destination] ダイアログボックスが表示されます（図 7-7 を参照）。

図 7-7　[Create Destinations] ダイアログボックス



ステップ 4　新しい宛先を設定するスイッチをオンにします。

ステップ 5　宛先の IP アドレスと UDP ポートを設定します。

ステップ 6　[trap] または [inform] オプション ボタンを選択します。

ステップ 7　（オプション）タイムアウトまたはリトライ回数の値を設定します。

ステップ 8　[Create] をクリックして、選択したスイッチにこの宛先を追加します。

ステップ 9　（オプション）[Other] タブをクリックして、特定の通知タイプをスイッチごとにイネーブルにします。

ステップ 10　[Apply Changes] アイコンをクリックして、エントリを作成します。

（注）　スイッチは、イベント（SNMP トラップおよびインフォーム）を、最大 10 件の宛先に転送できます。

SNMPv3 通知の設定

（注）　Fabric Manager を使用して、IPv4 を使用した SNMPv3 通知を設定するには、[Create Destinations] ダイアログボックスの [Security] ドロップダウン リストから [v3] を選択します（図 7-7 を参照）。必要に応じて、インフォームのタイムアウトとリトライの値を設定します。[Create] をクリックして、選択したスイッチにこの宛先を追加します。

（注）　SNMPv3 通知の場合、SNMP マネージャは、SNMP メッセージを認証および復号化するために、スイッチの engineID に基づくユーザ資格情報（authKey/PrivKey）を知っていることが期待されます。

SNMP 通知のイネーブル化

通知（トラップおよびインフォーム）は、特定のイベントが発生したときにスイッチによって生成されるシステム アラートです。通知はイネーブルまたはディセーブルにできます。デフォルトでは、通知は 1 つも定義されておらず、通知が生成されることはありません。通知名を指定しないと、すべての通知が無効または有効になります。

表 7-1 に、4.2(1) よりも前のバージョンの Cisco NX-OS MIB に対して通知をイネーブルにするための、Fabric Manager での手順を示します。[Switches] > [Events] > [SNMP Traps] の順に選択し、この表に示すチェックボックスを表示します。

（注）　[Switches] > [Events] > [SNMP Traps] を選択すると、SNMP 通知の設定方法に応じて、トラップとインフォームの両方がイネーブルになります。「SNMPv3 通知の設定」（P.7-10）で表示される通知を参照してください。

表 7-1　SNMP 通知のイネーブル化

MIB	Fabric Manager のチェックボックス
CISCO-ENTITY-FRU-CONTROL-MIB	[Other] タブを選択し、[FRU Changes] をオンにします。
CISCO-FCC-MIB	[Other] タブを選択し、[FCC] をオンにします。

表 7-1　SNMP 通知のイネーブル化 （続き）

MIB	Fabric Manager のチェックボックス
CISCO-DM-MIB	[FC] タブを選択し、[Domain Mgr RCF] をオンにします。
CISCO-NS-MIB	[FC] タブを選択し、[Name Server] をオンにします。
CISCO-FCS-MIB	[Other] タブを選択し、[FCS Rejects] をオンにします。
CISCO-FDMI-MIB	[Other] タブを選択し、[FDMI] をオンにします。
CISCO-FSPF-MIB	[FC] タブを選択し、[FSPF Neighbor Change] をオンにします。
CISCO-LICENSE-MGR-MIB	[Other] タブを選択し、[License Manager] をオンにします。
CISCO-IPSEC-SIGNALLING-MIB	[Other] タブを選択し、[IPSEC] をオンにします。
CISCO-PSM-MIB	[Other] タブを選択し、[Port Security] をオンにします。
CISCO-RSCN-MIB	[FC] タブを選択し、[RSCN ILS] および [RCSN ELS] をオンにします。
SNMPv2-MIB	[Other] タブを選択し、[SNMP AuthFailure] をオンにします。
VRRP-MIB, CISCO-IETF-VRRP-MIB	[Other] タブを選択し、[VRRP] をオンにします。
CISCO-ZS-MIB	[FC] タブを選択し、[Zone Rejects]、[Zone Merge Failures]、[Zone Merge Successes]、[Zone Default Policy Change]、および [Zone Unsuppd Mode] をオンにします。

次の通知はデフォルトでイネーブルになっています。

- entity fru
- license
- link ietf-extended

その他の通知はすべてデフォルトでディセーブルになっています。

Fabric Manager Release 4.3(1b) およびそれ以前を使用した個々の通知のイネーブル化

4.2(1) よりも前のバージョンに対し Fabric Manager を使用して個々の通知をイネーブルにするには、次の手順を実行します。

ステップ 1　[Switches] > [Events] の順に展開し、[Physical Attributes] ペインで [SNMP Traps] を選択します。

[Information] ペインに SNMP 通知の設定が表示されます。

ステップ 2　[FC] タブをクリックして、Fibre Channel 関連の通知をイネーブルにします。

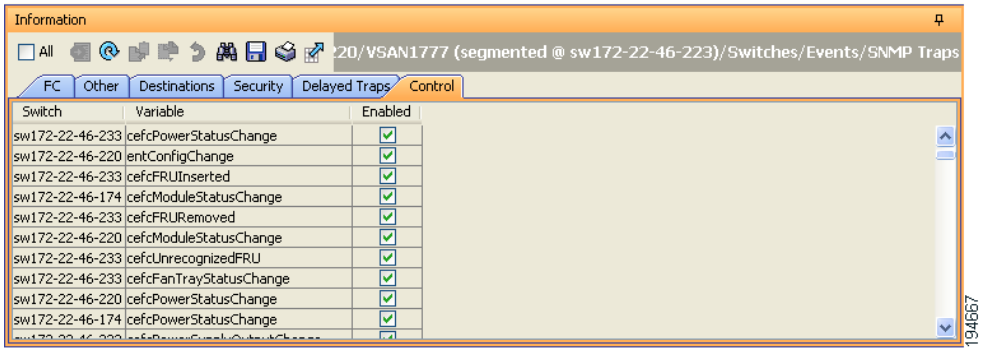
ステップ 3　イネーブルにする各通知のチェックボックスをオンにします。

ステップ 4　[Other] タブをクリックしてその他の通知をイネーブルにします。

ステップ 5　イネーブルにする各通知のチェックボックスをオンにします。

NX-OS Release 4.2(1) から、通知制御機能のための [Control] タブが利用できるようになりました。この機能を使用すると、通知に該当するすべての変数を、SNMP を通じてイネーブルまたはディセーブルにできます（図 7-8 を参照）。

図 7-8　SNMP トラップ ウィンドウ



（注） [Control] タブは、NX-OS Release 4.2(1) 以降でだけ使用できます。Fabric Manager Release 4.2(1) 以降を使用して個別の通知をイネーブルにするには、[Control] タブをクリックします。

ステップ 6　[Apply Changes] アイコンをクリックして、エントリを作成します。

Device Manager を使用した個々の通知のイネーブル化

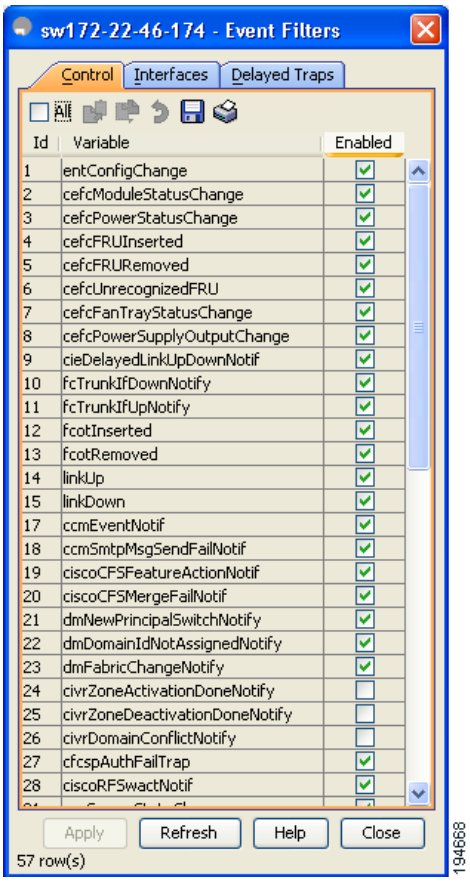
Device Manager を使用して個々の通知をイネーブルにするには、次の手順を実行します。

（注） Device Manager で、コマンド **no snmp-server enable traps link** を実行すると、スイッチでリンク トラップの生成がディセーブルになりますが、個々のインターフェイスでリンク トラップがイネーブルになっている可能性があります。

ステップ 1　[Admin] > [Events] の順に展開し、[Filters] を選択します。

スイッチによってデータが設定されたテーブルがイベント フィルタ ウィンドウに表示されます（図 7-9 を参照）。

図 7-9　[Event Filters] ウィンドウ



ステップ 2　[Control] タブをクリックし、通知に該当する変数をイネーブルにします。

NX-OS Release 4.2(1) から、通知制御機能のための [Control] タブが利用できるようになりました。この機能を使用すると、通知に該当するすべての変数を、SNMP を通じてイネーブルまたはディセーブルにできます。

（注）　[Control] タブは、NX-OS Release 4.2(1) 以降でだけ使用できます。

ステップ 3　イネーブルにする各通知のチェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、エントリを作成します。

通知対象ユーザの設定

SNMPv3 インフォーム通知を SNMP マネージャに送信するには、スイッチ上で通知対象ユーザを設定する必要があります。

通知対象ユーザの設定については『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

通知対象ユーザの資格情報は、SNMPv3 インフォーム通知メッセージを設定された SNMP に暗号化するために使用されます。

（注）　SNMP マネージャは、受信した INFORM PDU を認証および復号化するために、同じユーザ資格情報をユーザのローカル設定データ ストアに持っている必要があります。

イベント セキュリティの設定

注意　これは高度な機能であるため、SNMPv3 の経験が豊富な管理者だけが使用することをお勧めします。

SNMP イベントは、SNMP メッセージと同じ方法で傍受や盗聴から保護できます。Fabric Manager または Device Manager では、スイッチが生成する SNMP イベントのメッセージ処理モデル、セキュリティ モデル、セキュリティ レベルを設定できます。

Fabric Manager を使用して SNMP イベント セキュリティを設定するには、次の手順を実行します。

ステップ 1　[Switches] > [Events] の順に展開し、[SNMP Traps] を選択します。

ステップ 2　[Information] ペインで [Security] タブをクリックします。

SNMP 通知のセキュリティ情報が表示されます。

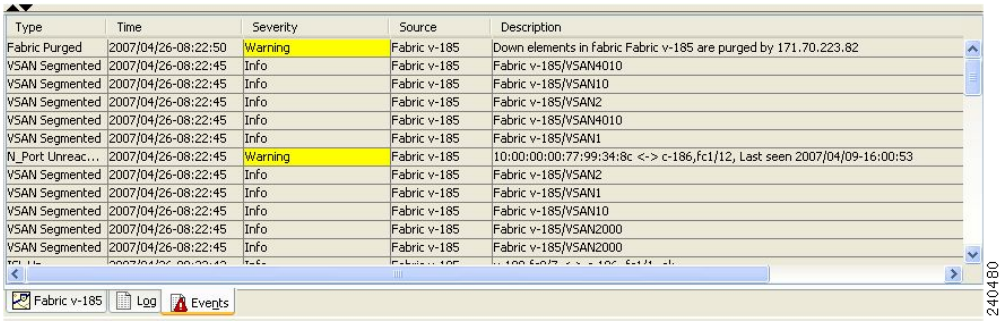
ステップ 3　メッセージ プロトコル モデル（MPModel）、セキュリティ モデル、セキュリティ名、およびセキュリティ レベルを設定します。

ステップ 4　[Apply Changes] アイコンをクリックし、変更を保存して適用します。

SNMP イベント ログの表示

SNMP イベント ログを Fabric Manager で表示するには、[Events] タブをクリックします（図 7-10 を参照）。[Events] に、単一のスイッチのイベント ログの一覧が表示されます。

図 7-10　イベント情報



（注）　イベント ログを表示するには、MDS syslog マネージャを設定しておく必要があります。

注意　これらの値を別の Fabric Manager ワークステーションから同時に変更すると、予測できない結果が生じる恐れがあります。

デフォルト設定

表 7-2 に、すべてのスイッチの SNMP 機能のデフォルト設定を示します。

表 7-2　SNMP のデフォルト設定

パラメータ	デフォルト
ユーザ アカウント	有効期限なし（設定されていない場合）
パスワード	なし