CHAPTER 9

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。

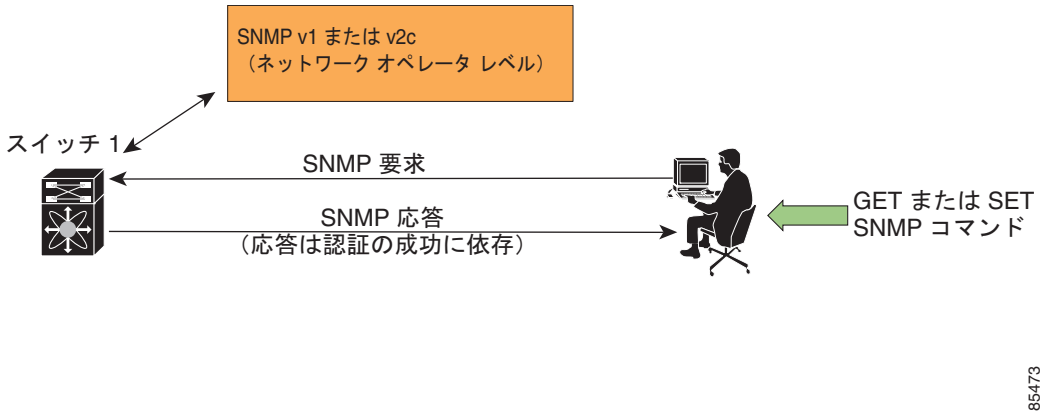
CLI ユーザと SNMP ユーザのユーザ、パスワード、ロールは、すべて同じです。CLI を通じて設定されたユーザは SNMP（たとえば、DCNM-SAN や Device Manager）を使用してスイッチにアクセスでき、その逆も可能です。

この章の内容は、次のとおりです。

SNMP セキュリティについて

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。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 9-1 を参照）。

図 9-1　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 コントロール方式です。SNMPv3 は、強力な認証を使用することによってアクセス コントロール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。SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。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：メッセージのソースが有効かどうかを判別します。
- 暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可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り、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

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 コントロールが含まれています。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。ユーザ認証が検証されると、SNMP PDU の処理が進行します。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 ポリシーまたはロール ポリシーを適用します。

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の変更は、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) からは、DCNM-SAN に対して作成された一時的 SNMP ログインは 24 時間ではなく、1 時間になりました。

- 既存の SNMP ユーザは、特に変更しなくても、引き続き auth および priv のパスフレーズを維持できます。
- 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 アクセス コントロール リスト（IP-ACL）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）　グループが業界全体で使用されている標準 SNMP 用語なので、この SNMP の項では、ロールのことをグループと言います。

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは 3 つのアクセス権により定義されます。つまり、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です。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、DCNM-SAN、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、クローンの秘密キーを変更してから、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。
- DCNM-SAN。
- 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（DCNM-SAN 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、DCNM-SAN 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 DCNM-SAN 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。

AES 暗号ベースの機密保全

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ー 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 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、プライバシー パスワードは 128 ビット AES キーの生成に使用されます。AES のプライバシー 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ープロトコルに AES を指定して、SNMP PDU を暗号化する必要があります。

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。通知を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。

SNMP 中央インフラ機能では、イネーブルまたはディセーブルにする必要のあるトラップを追加できます。MIB ブラウザを使用して通知の生成を制御できるようにするために、MIB CISCO-NOTIFICATION-CONTROL-MIB がサポートされています。

スイッチの LinkUp/LinkDown 通知

スイッチに対して、イネーブルにする LinkUp/LinkDown 通知を設定できます。次のタイプの LinkUp/LinkDown 通知をイネーブルにできます。

- Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。
- IETF：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）のみが送信されます。通知定義で定義された変数バインドのみが、それらの通知とともに送信されます。
- IEFT extended：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）のみが送信されます。通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも送信されます。これがデフォルト設定です。
- IEFT Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。通知定義で定義された変数バインドのみが、linkUp 通知や linkDown 通知とともに送信されます。
- IEFT extended Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。linkUp と linkDown の通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも LinkUp 通知や LinkDown 通知とともに送信されます。

（注）　シスコの実装に固有の IF-MIB で定義される変数バインドの詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

LinkUp および LinkDown トラップ設定の範囲

インターフェイスに対する LinkUp および LinkDown トラップ設定は、次の範囲に基づいてトラップを生成します。

スイッチレベルのトラップ設定	インターフェイスレベルのトラップ設定	インターフェイス リンクについて生成されるトラップか？
イネーブル（デフォルト）	イネーブル（デフォルト）	Yes
イネーブル	ディセーブル	No
ディセーブル	イネーブル	No
ディセーブル	ディセーブル	No

デフォルト設定

表 9-1 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 9-1　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

SNMP の設定

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。

ここで説明する内容は、次のとおりです。

- 「SNMPv3 ユーザの複数のロールへの割り当て」（P.9-8）
- 「SNMPv3 メッセージ暗号化の適用」（P.9-7）
- 「SNMPv3 ユーザの複数のロールへの割り当て」（P.9-8）
- 「コミュニティの追加または削除」（P.9-8）
- 「コミュニティ ストリングの削除」（P.9-9）

SNMP スイッチの連絡先および場所の情報の割り当て

スイッチの連絡先情報（スペースを含めず、最大 32 文字まで）およびスイッチの場所を割り当てることができます。

手順の詳細

連絡先および場所の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 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。

手順の詳細

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　[Physical Attributes] ペインから [Switches] を展開し、[Security] を展開し、[Users and Roles] を選択します。

ステップ 2　[Information] ペインで [Users] タブをクリックして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。

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。

ステップ 8　[Enforce SNMP Privacy Encryption] チェックボックスにチェックを入れて、管理用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。

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　[Physical Attributes] ペインで [Switches] を展開し、[Security] を展開し、[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。

制約事項

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

手順の詳細

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　[Physical Attributes] ペインから [Switches] を展開し、[Security] を展開し、[Users and Roles] を選択します。

ステップ 2　[Information] ペインで [Users] タブをクリックして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。

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または削除

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。

手順の詳細

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　[Physical Attributes] ペインから [Switches] を展開し、[Security] を展開し、[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。

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

手順の詳細

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　[Physical Attributes] ペインから [Switches] を展開し、[Security] を展開し、[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の設定

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）　SNMP 設定で RMON トラップをイネーブルにする必要があります。詳細については、「RMON の設定」（P.8-1）を参照してください。

（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

手順の詳細

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　[Physical Attributes] ペインで [Events] を展開し、[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　[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 Destinations] ダイアログボックスが表示されます。

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

手順の詳細

SNMPv3 通知を設定するには、次の手順を実行します。

ステップ 1　[Create Destinations] ダイアログボックスで [Security] ドロップダウン リストから [v3] を選択します。

ステップ 2　（オプション）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。

ステップ 3　[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

表 9-2 に、DCNM-SAN で Cisco NX-OS MIB の通知をイネーブルにする手順を示します。

[Events] > [SNMP Traps] を展開して、この表に一覧されているチェックボックスを表示します。

（注）　[Events] > [SNMP Traps] を選択すると、SNMP 通知をどのように設定したかに応じて、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.9-10）で表示される通知を参照してください。

表 9-2　SNMP 通知のイネーブル化

MIB	DCNM-SAN チェックボックス
CISCO-ENTITY-FRU-CONTROL-MIB	[Other] タブをクリックし、[FRU Changes] をオンにします。
CISCO-FCC-MIB	[Other] タブをクリックし、[FCC] をオンにします。
CISCO-DM-MIB	[FC] タブをクリックし、[Domain Mgr RCF] をオンにします。
CISCO-NS-MIB	[FC] タブをクリックし、[Name Server] をオンにします。
CISCO-FCS-MIB	[Other] タブをクリックし、[FCS Rejects] をオンにします。
CISCO-FDMI-MIB	[Other] タブをクリックし、[FDMI] をオンにします。
CISCO-FSPF-MIB	[FC] タブをクリックし、[FSPF Neighbor Change] をオンにします。
CISCO-LICENSE-MGR-MIB	[Other] タブをクリックし、[License Manager] をオンにします。
CISCO-IPSEC-SIGNALLING-MIB	[Other] タブをクリックし、[IPSEC] をオンにします。
CISCO-PSM-MIB	[Other] タブをクリックし、[Port Security] をオンにします。
CISCO-RSCN-MIB	[FC] タブをクリックし、[RSCN ILS] と [RCSN ELS] をオンにします。
SNMPv2-MIB	[Other] タブをクリックし、[SNMP AuthFailure] をオンにします。
VRRP-MIB, CISCO-IETF-VRRP-MIB	[Other] タブをクリックし、[VRRP] をオンにします。
CISCO-ZS-MIB	[FC] タブをクリックし、[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

他の通知はすべて、デフォルトではディセーブルです。

手順の詳細

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　[Physical Attributes] ペインで [Events] を展開し、[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、ファイバ チャネル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。

ステップ 6　[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。

[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 7　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 8　[Apply Changes] アイコンをクリックして、エントリを作成します。

（注）　Device Manager で、**no snmp-server enable traps link** コマンドを実行すると、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。

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。

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。

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。

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。

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。

インターフェイスの Up/Down SNMP リンクステート トラップの設定

デフォルトでは、SNMP リンクステート トラップがすべてのインターフェイスに対してイネーブルになっています。リンクの状態が Up と Down の間で切り替わるたびに、SNMP トラップが生成されます。

何百ものインターフェイスを装備したスイッチが多数存在し、それらの多くでリンクの状態をモニタする必要がない場合があります。そのような場合には、リンクステート トラップをディセーブルにすることも選択できます。

イベント セキュリティの設定

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。DCNM-SAN 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。

制約事項

- 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。

手順の詳細

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　[Events] を展開し、[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

前提条件

- イベント ログを表示する前に、MDS Syslog マネージャをセットアップする必要があります。

制約事項

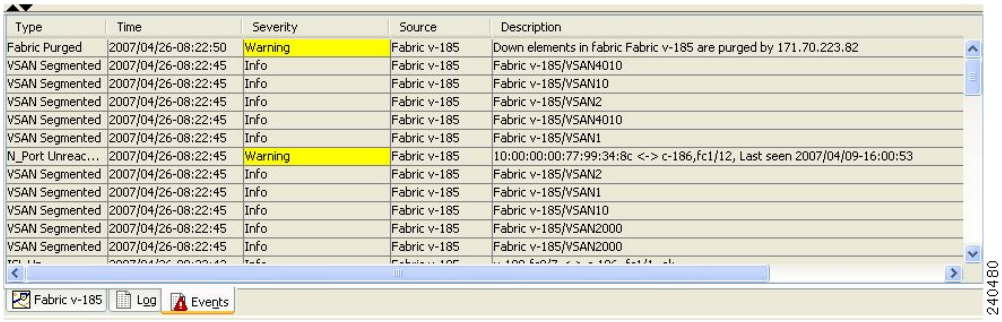
- これらの値を別の DCNM-SAN ワークステーションから同時に変更すると、予測できない結果が生じるおそれがあります。

手順の詳細

DCNM-SAN から SNMP イベント ログを表示するには、[Events] タブをクリックします。

[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 9-2 を参照）。

図 9-2　イベント情報



SNMP のフィールドの説明

ここでは、SNMP のフィールドの説明を示します。

IP 統計情報 SNMP

フィールド	説明
BadVersions	SNMP プロトコル エンティティに配信され、未サポートの SNMP バージョン用だった SNMP メッセージの合計数。
BadCommunityNames	認識されない SNMP コミュニティ名を使用している SNMP エンティティに配信された SNMP メッセージの合計数。
BadCommunityUses	SNMP エンティティに配信され、指定された名前の SNMP コミュニティで許可されていない SNMP 処理を示していた SNMP メッセージの合計数。
ASNParseErrs	受信した SNMP メッセージをデコードするときに、SNMP エンティティで発生した ASN.1 エラーまたは BER エラーの合計数。

フィールド	説明
TooBigs	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が tooBig だった SNMP PDU の合計数。
SilentDrops	SNMP エンティティに配信され、空の変数バインディング フィールドを持つ別の Response-PDU を格納した応答のサイズがローカルな制約または要求の送信元に関連付けられた最大メッセージ サイズよりも大きかったため自動的にドロップされた、GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の合計数。
ProxyDrops	SNMP エンティティに配信され、返信できた Response-PDU がなかった状態（タイムアウトを除く）でプロキシ ターゲットへのメッセージ（変換されたものを含む）の送信に失敗したため自動的にドロップされた、GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の合計数。
NoSuchNames	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が noSuchName だった SNMP PDU の合計数。
BadValues	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が badValue だった SNMP PDU の合計数。
ReadOnlys	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が readOnly だった有効な SNMP PDU の合計数。エラーステータス フィールドに値 readOnly が格納された SNMP PDU を生成することは、SNMP の誤った実装を検出する手段として提供されているので、これはプロトコル エラーであることを意味します。
GenErrs	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が genErr だった SNMP PDU の合計数。
Pkts	転送サービスから SNMP エンティティに配信されたメッセージの合計数。
GetRequests	SNMP プロトコル エンティティによって受け入れられ、処理された SNMP Get-Request PDU の合計数。
GetNexts	SNMP プロトコル エンティティによって受け入れられ、処理された SNMP Get-Next PDU の合計数。
SetRequests	SNMP プロトコル エンティティによって受け入れられ、処理された SNMP Set-Request PDU の合計数。
OutTraps	SNMP プロトコル エンティティによって生成された SNMP Trap PDU の合計数。
OutGetResponses	SNMP プロトコル エンティティによって生成された SNMP Get-Response PDU の合計数。
OutPkts	SNMP プロトコル エンティティから転送サービスに渡された SNMP メッセージの合計数。
TotalReqVars	有効な SNMP Get-Request PDU と Get-Next PDU を受信した結果として、SNMP プロトコル エンティティによって正常に取得された MIB オブジェクトの合計数。
TotalSetVars	有効な SNMP Set-Request PDU を受信した結果として、SNMP プロトコル エンティティによって正常に変更された MIB オブジェクトの合計数。

SNMP セキュリティ ユーザ

フィールド	説明
Role	セキュリティ モデルに依存しない形式でのユーザ。
Password	一般ユーザのパスワード。SNMP の場合、このパスワードは、認証と機密保全の両方に使用されます。CLI と XML の場合、認証のみに使用されます。
Digest	使用されるダイジェスト認証プロトコルのタイプ。
Encryption	使用される暗号化認証プロトコルのタイプ。
ExpiryDate	このユーザの有効期限が切れる日付。
SSH Key File Configured	ユーザが SSH 公開キーで設定されているかどうかを指定します。
SSH Key File	SSH 公開キーを保管しているファイルの名前。SSH 公開キーは、このユーザの SSH セッションを認証するために使用されます。これは、CLI ユーザに対してのみ適用されます。形式は次のいずれかになります。 • OpenSSH 形式の SSH 公開キー • IETF SECSH（商用の SSH 公開キー形式）の SSH 公開キー • 公開キーの抽出元となる PEM（Privacy-Enhanced Mail 形式）の SSH クライアント証明書 • 証明書ベースの認証用の SSH クライアント証明書 DN（識別名）
Creation Type	ユーザのクレデンシャル ストアのタイプ。ユーザによってこのテーブルに行が作成されると、デバイスに対してローカルなクレデンシャル ストアにユーザ エントリが作成されます。AAA サーバ ベースの認証などのリモート認証メカニズムの場合、資格情報は他の（リモートの）システムまたはデバイスに保管されます。
Expiry Date	このユーザの有効期限が切れる日付。

関連トピック

SNMP の設定

SNMP セキュリティ コミュニティ

フィールド	説明
Community	コミュニティ ストリング。
Role	セキュリティ モデル名。

関連トピック

コミュニティの追加または削除

コミュニティ ストリングの削除

セキュリティ ユーザ グローバル

フィールド	説明
Enforce SNMP Privacy Encryption	SNMP エージェントにより、SNMPv3 メッセージに対する暗号化の使用がシステム内のすべてのユーザに対してグローバルに適用されるかどうかを指定します。
Cache Timeout	これにより、ローカル システム内でユーザ資格情報をキャッシュするための最大タイムアウト値が指定されます。

（注）　管理者が Device Manager で新しいユーザを作成する場合または既存のユーザを削除する場合、プライバシー パスワードと認証パスワードが必要です。ただし、新しいユーザの作成時に管理者がこれらの資格情報を入力しなくても、Device Manager は、管理者の認証パスワードをプライバシー パスワードとして使用します。ユーザに対して定義されたプライバシー プロトコルが DES（デフォルト）ではない場合、MDS 内の SNMP エージェントはパケットを復号化できなくなり、SNMP エージェントはタイムアウトします。ユーザに対して定義されたプライバシー プロトコルが DES ではない場合、ユーザがログイン時にプライバシー パスワードとプロトコルの両方を入力する必要があります。

その他の参考資料

SNMP の実装に関する詳細情報については、次の各項を参照してください。

- 「MIB」（P.9-17）

MIB

MIB	MIB のリンク
• CISCO-SNMP-TARGET-EXT-MIB • CISCO-SNMP-VACM-EXT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

SNMP の機能履歴

表 9-3 に、この機能のリリース履歴を示します。Release 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 9-3　SNMP の機能履歴

機能名	リリース	機能情報
[SNMP Trap] の [Control] タブ	4.2(1)	NX-OS Release 4.2(1) で追加された新しい [Control] タブの詳細を追加。