SNMP の設定

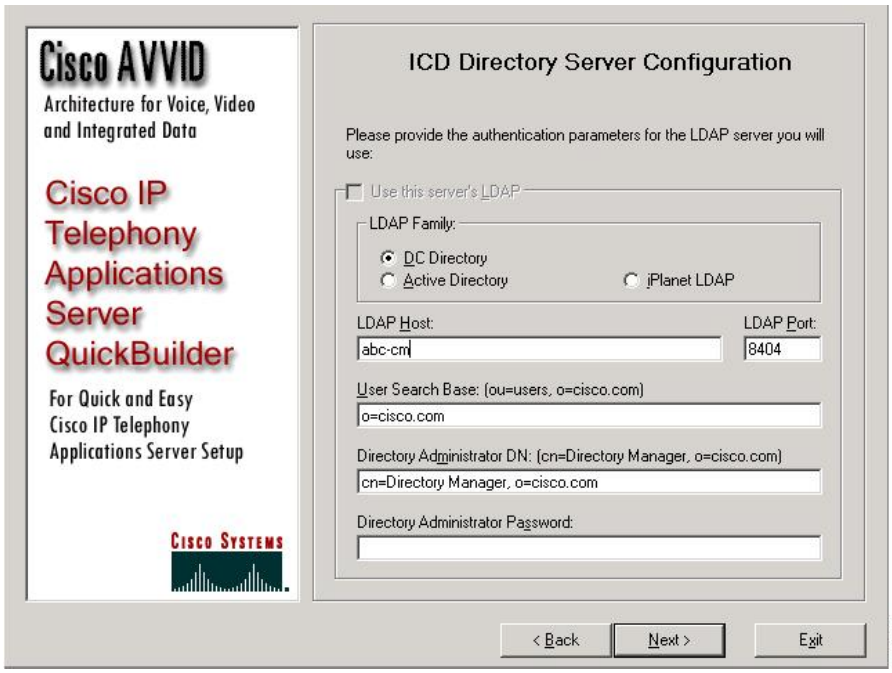
CLI と SNMP は、Cisco MDS 9000 ファミリのすべてのスイッチで共通のロールを使用します。SNMP を使用して CLI で作成したロールを変更したり、その逆を行うことができます。

CLI ユーザーと SNMP ユーザーのユーザー、パスワード、ロールは、すべて同じです。CLI を通じて構成されたユーザは SNMP（たとえば、Cisco 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。

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（Figure 1: SNMPセキュリティ, on page 2 を参照）。

*Figure 1: SNMP*セキュリティ



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

Note Cisco MDS NX-OS リリース 8.5(1) 以降、AES-128 は強力な暗号化アルゴリズムであるため、推奨される暗号化アルゴリズムです。ただし、DES 暗号化もサポートされています。

DES プライバシー プロトコルを持つユーザが SNMP データベースに存在する場合、**install all** コマンドによる In-Service System Downgrade（ISSD）が中断されます。ユーザはデフォルトの AES-128 を使用して再構成または削除する必要があります。この動作は、Cisco MDS NX-OS リリース 8.5(1) で見られます。ISSD の場合の DES ユーザ サポートは、将来のリリースで追加される予定です。ただし、コールドリブートの場合、DES プライバシー プロトコルを持つ SNMP ユーザは削除されます。

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、ユーザベース セキュリティ モデル（USM）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 スイッチ上で稼働する 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 ユーザの同期

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。

SNMP または CLI ユーザを作成するには、**username** コマンドまたは **snmp-server user** コマンドを使用します。

- **snmp-server user** コマンドで指定された パスフレーズは、CLI ユーザのパスワードと同期します。
- **username** コマンドで指定したパスワードは、SNMP ユーザ用の auth および priv パスフレーズとして同期されます。

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。

Note 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。

- 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。

SNMPv3 サーバーの AAA 排他動作

AAA の排他的な動作機能を使用して、ロケーションに基づいてユーザを認証できます。

ユーザがローカル ユーザまたはリモート AAA ユーザでない場合、一意の SNMPv3 ユーザは認証されません。ユーザがローカルおよびリモート データベースの両方に存在する場合、ユーザは AAA の排他的な動作が有効かそうでないかに基づいて許可または拒否されます。

表 *1: AAA* の排他的な動作のシナリオ

ユーザの場所	AAA サーバー	AAA の排他的な動作	ユーザー認証
ローカル ユーザ データベース	無効	有効	ユーザが認証されました。
ローカル ユーザ データベース	有効	有効	ユーザは認証されません。
ローカル ユーザ データベース	有効	無効	ユーザが認証されました。
ローカル ユーザ データベース	無効	無効	ユーザが認証されました。
リモートおよびローカル ユーザー データベース（同一ユーザ名）	有効	有効	リモート ユーザは認証されますが、ローカル ユーザは認証されません。
リモートおよびローカル ユーザー データベース（同一ユーザ名）	無効	有効	ローカル ユーザは認証されますが、リモート ユーザは認証されません。

リモートおよびローカル ユーザーデータベース（同一ユーザ名）	無効	無効	ローカル ユーザは認証されますが、リモート ユーザは認証されません。
リモートおよびローカル ユーザーデータベース（同一ユーザ名）	有効	無効	ローカル ユーザは認証されますが、リモート ユーザは認証されません。

（注） AAA サーバが到達不能な場合、ユーザがローカル ユーザーデータベースに対して検証されるようにフォールバック オプションをサーバーで構成することができます。ユーザがローカルデータベースまたはリモートユーザーデータベースで使用できない場合、SNMPv3 サーバーはエラーを返します。SNMPv3 サーバはー、リモート ユーザーデータベースにユーザが存在しない場合、AAA サーバの可用性をチェックせずに「Unknown user」メッセージを返します。

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

Note *group* が業界全体で使用されている標準規格 SNMP 用語なので、この SNMP のセクションでは、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。

Tip 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 暗号化を選択できます。Cisco MDS NX-OS リリース 8.5(1) 以前では、**aes-128** トークンと連動する **priv** オプションは、128 ビットの AES キーを生成するためのプライバシ パスワードであることを示します。AES-128 は、Cisco MDS NX-OS リリース 8.5(1) からデフォルトのプライバシー オプションになりました。これは、Cisco MDS NX-OS リリース 8.5(1) から構成または変更されたすべてのユーザが **aes-128** をプライバシー オプションとして使用することを示しています。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。

Note 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。

トラップ、通知、およびインフォーム

トラップは、SNMP エージェントから SNMPv1 の SNMP マネージャに送信される未確認のメッセージです。SNMPv2 および SNMPv3 では通知と呼ばれます。インフォームは、SNMP エージェントから SNMP マネージャに送信される確認応答メッセージです。エージェントが応答を受信しない場合は、インフォーム要求を再度送信します。

ただし、インフォームは、エージェントやネットワークでより多くのリソースを消費します。送信と同時にエージェントによって廃棄されるトラップまたは通知とは異なり、インフォーム要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。トラップと通知は 1 回だけ送信できますが、インフォームは複数回送信できます。インフォームの再送信によりトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因になります。同じトラップ、通知、およびインフォームを複数のホスト受信者に送信できます。

Note SNMPv3 インフォームを機能させるには、**snmp-server user***name* **engineID** コマンドを使用して、SNMP ユーザでネットワーク管理サーバー（NMS）engineID を構成する必要があります。

NMS から Linux engineID を取得するには、**snmptarpd** を起動し、出力で **lcd_set_enginetime** 文字列を探します。

```
#snmptrapd -f -D -Le 3162
lcd_set_enginetime: engineID 80 00 1F 88 80 14 D4 89 07 46 D5 74 5A 00 00 00
00 : boots=96, time=0
```

EngineID

SNMP engineID は、送信元アドレスに関係なくエンティティを識別するために使用されます。エンティティは、SNMP エンジンと SNMP アプリケーションで構成されます。プロトコルデータユニット（PDU）がプロキシまたはネットワーク アドレス変換（NAT）を通過する必要がある場合、または送信元エンティティ自体に動的に割り当てられたトランスポートアドレスまたは複数の送信元アドレスがある場合、engineID は重要です。

SNMPv3 では、安全な PDU のエンコードとデコードにも engineID が使用されます。これは、SNMPv3 ユーザーベース セキュリティ モデル（USM）の要件です。

engineID には、ローカルとリモートの 2 種類があります。Cisco MDS 9000 シリーズ スイッチでは、リモート engineID のみを構成できます。ローカル engineID は、MAC アドレスに基づいてスイッチによって自動的に生成され、変更されません。

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。

Note 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?
有効（デフォルト）	有効（デフォルト）	はい
有効	無効	いいえ
無効	有効	いいえ
無効	無効	不可

デフォルト設定

Table 2: SNMP のデフォルト設定 , on page 9 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。

***Table 2: SNMP* のデフォルト設定**

パラメータ	デフォルト
ユーザー 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。

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。

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。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server contact NewUser**

スイッチの担当者名を割り当てます。

ステップ 3 switch(config)# **no snmp-server contact NewUser**

スイッチの担当者名を削除します。

ステップ 4 switch(config)# **snmp-server location SanJose**

スイッチのロケーションを割り当てます。

ステップ 5 switch(config)# **no snmp-server location SanJose**

スイッチのロケーションを削除します。

CLI から SNMP ユーザの構成

snmp-server userコマンドで指定したパスフレーズと、**username** コマンドが同期します。

Note パスフレーズまたはパスワードが **localizedkey** または暗号化フォーマットで指定されている場合、パスワードは同期されません。あるデバイスに別のデバイスで生成した構成ファイルをコピーした場合、パスワードが正しく設定されない可能性があります。構成ファイルをデバイスにコピーした場合は、望ましいパスワードを明示的に構成してください。

CLI から SNMP ユーザを作成または変更するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server user joe network-admin auth sha abcd1234**

HMAC-SHA-96 認証パスワード（abcd1234）を使用して、ネットワーク管理者ロールのユーザ（joe）の設定を作成または変更します。

Note Cisco MDS NX-OS リリース 8.5(1) 以降、AES-128 は SNMPv3 のデフォルトのプライバシー プロトコルです。

ステップ 3 switch(config)# **snmp-server user sam network-admin auth md5 abcdefgh**

HMAC-MD5-96 認証パスワード（abcdefgh）を使用して、ネットワーク管理者ロールのユーザ（sam）の設定を作成または変更します。

ステップ 4 switch(config)# **snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh**

HMAC-SHA-96 認証レベルを使用して、network-admin ロールのユーザ（Bill）の設定を作成または変更します。AES-128 は、Cisco MDS NX-OS リリース 8.5(1) のプライバシー暗号化パラメータとして使用されます。Cisco MDS NX-OS リリース 8.5(1) より前は、DES がプライバシープロトコルとして使用されていました。

ステップ 5 switch(config)# **no snmp-server user usernameA**

ユーザ（usernameA）および関連するすべてのパラメータを削除します。

ステップ 6 switch(config)# **no snmp-server usam role vsan-admin**

vsan-admin ロールから指定のユーザー（usam）を削除します。

ステップ 7 switch(config)# **snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342 localizedkey**

ローカライズされたキー フォーマット（RFC 2574）でパスワードを指定します。ローカライズされたキーは、16 進数フォーマット（0xacbdef など）で提供されます。

ステップ 8 switch(config)# **snmp-server user user2 auth md5 asdgfsadf priv aes-128 asgfsgkhkj**

MD5 認証プロトコルと AES-128 プライバシー プロトコルを使用して user2 を構成します。このコマンドは、Cisco NX-OS リリース 8.5(1) より前のリリースではサポートされています。AES-128 は、Cisco MDS NX-OS リリース 8.5(1) 以降、デフォルトのプライバシー オプションです。

ステップ 9 switch(config)# **snmp-server user joe sangroup**

指定したユーザ（joe）を sangroup ロールに追加します。

ステップ 10 switch(config)# **snmp-server user joe techdocs**

指定したユーザ（joe）を techdocs ロールに追加します。

パスワードの作成または変更

CLI から SNMP ユーザのパスワードを作成または変更するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server user user1 role1 auth md5 0xab0211gh priv 0x45abf342 localizedkey**

セキュリティ暗号化に DES オプションを使用して、ローカライズされたキー フォーマットでパスワードを指定します。

Note Cisco MDS NX-OS リリース 8.5(1) 以降、AES-128 は SNMPv3 のデフォルトのプライバシー プロトコルです。

ステップ 3 switch(config)# **snmp-server user user1 role2 auth sha 0xab0211gh priv aes-128 0x45abf342 localizedkey**

セキュリティ暗号化に 128 ビット AES オプションを使用して、ローカライズされたキー フォーマットでパスワードを指定します

Note このコマンドは、Cisco NX-OS リリース 8.5(1) より前のリリースではサポートされています。AES-128 は、Cisco MDS NX-OS リリース 8.5(1) 以降、デフォルトのプライバシー オプションです。

snmp-server user コマンドは、追加のパラメータとして engineID を受け取ります。engineID により、Notification（通告）対象ユーザが作成されます（通知ターゲットユーザの設定 , on page 22 を参照）。engineID が指定されていない場合、ローカルユーザが作成されます。

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。

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。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server user testUser enforcePriv**

このユーザに対して SNMPv3 メッセージのメッセージ暗号化を適用します。

Note auth および priv の両方のキーが構成された既存のユーザに対してだけ、このコマンドを使用できます。ユーザがプライバシーを適用するように構成されている場合、noAuthNoPriv または authNoPriv の securityLevel パラメータを使用している SNMPv3 PDU 要求に対して、SNMP エージェントは authorizationError で応答します。

ステップ 3 switch(config)# **no snmp-server user testUser enforcePriv**

SNMPv3 メッセージ暗号化の適用を無効にします。

SNMPv3 メッセージ暗号化のグローバルでの適用

または、次のコマンドを使用して、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こともできます。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server globalEnforcePriv**

スイッチのすべてのユーザに SNMPv3 メッセージの暗号化を適用します。

ステップ 3 switch(config)# **no snmp-server globalEnforcePriv**

グローバル SNMPv3 メッセージ暗号化の適用を無効にします。

SNMPv3 ユーザに対する複数のロールの割り当て

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。

Note 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。

CLI から SNMPv3 ユーザに複数のロールを構成するには、次の手順に従います。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server user NewUser role1**

role1 ロールの SNMPv3 ユーザ（NewUser）の設定を作成または変更します。

ステップ 3 switch(config)# **snmp-server user NewUser role2**

role2 ロールの SNMPv3 ユーザ（NewUser）の設定を作成または変更します。

ステップ 4 switch(config)# **no snmp-server user User5 role2**

指定されたユーザー (User5) の role2 を削除します。

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。

SNMPv1 または SNMPv2c のコミュニティを作成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server community snmp_Community ro**

指定された SNMP コミュニティに読み取り専用アクセスを追加します。

ステップ 3 switch(config)# **snmp-server community snmp_Community rw**

指定された SNMP コミュニティの読み取り/書き込みアクセスを追加します。

ステップ 4 switch(config)# **no snmp-server community snmp_Community**

指定された SNMP コミュニティのアクセスを削除します（デフォルト）。

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。

Note 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。SNMP 用に 11 番目のターゲット ホストを構成しようとすると、次のメッセージが表示されます。

```
switch(config)# snmp-server host 10.4.200.173 traps version 2c noauth
reached maximum allowed targets limit
```

- 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 を参照してください。
- 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。

Tip SNMPv1 オプションは、**snmp-server host** *ip-address* **informs** コマンドでは使用できません。

Note 0. または 127. で始まる DSN サーバー名を使用した SNMP ホスト名はサポートされていません。

SNMPv2c 通知の設定

IPv4 を使用した SNMPv2c 通知の構成

IPv4 を使用して SNMPv2c 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server host 171.71.187.101 traps version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c トラップを受信するように指定されたホストを構成します。

ステップ 3 switch(config)# **no snmp-server host 171.71.187.101 traps version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c トラップを受信しないようにします。

ステップ 4 switch(config)# **snmp-server host 171.71.187.101 informs version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c インフォームを受信するように指定されたホストを構成します。

ステップ 5 switch(config)# **no snmp-server host 171.71.187.101 informs version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c インフォームを受信しないようにします。

IPv6 を使用した SNMPv2c 通知の構成

IPv6 を使用して SNMPv2c 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c トラップを受信するように指定されたホストを構成します。

ステップ 3 switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c トラップを受信しないようにします。

ステップ 4 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c インフォームを受信するように指定されたホストを構成します。

ステップ 5 switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c インフォームを受信しないようにします。

DNS ネームを使用した SNMPv2c 通知の構成

SNMP 通知ホスト myhost.cisco.com の DNS 名を使用して SNMPv2c 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server host myhost.cisco.com traps version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c トラップを受信するように指定されたホストを構成します。

ステップ 3 switch(config)# **no snmp-server host myhost.cisco.com traps version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c トラップを受信しないようにします。

ステップ 4 switch(config)# **snmp-server host myhost.cisco.com informs version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c インフォームを受信するように指定されたホストを構成します。

ステップ 5 switch(config)# **no snmp-server host myhost.cisco.com informs version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c インフォームを受信しないようにします。

Note 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

IPv4 を使用した SNMPv3 通知の構成

IPv4 を使用して SNMPv3 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server host 16.20.11.14 traps version 3 noauth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 トラップを受信できるように構成し、noAuthNoPriv の securityLevel を構成します。

ステップ 3 switch(config)# **snmp-server host 16.20.11.14 informs version 3 auth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthNoPriv の securityLevel を構成します。

ステップ 4 switch(config)# **snmp-server host 16.20.11.14 informs version 3 priv testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthPriv の securityLevel を構成します。

ステップ 5 switch(config)# **no snmp-server host 172.18.2.247 informs version 3 testuser noauth udp-port 2162**

指定済みホストが SNMPv3 情報を受信できないようにします。

IPv6 を使用した SNMPv3 通知の構成

IPv6 を使用して SNMPv3 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 3 noauth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 トラップを受信できるように構成し、noAuthNoPriv の securityLevel を構成します。

ステップ 3 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 auth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthNoPriv の securityLevel を構成します。

ステップ 4 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 priv testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthPriv の securityLevel を構成します。

ステップ 5 switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 3 testuser noauth udp-port 2162**

指定済みホストが SNMPv3 情報を受信できないようにします。

DNS ネームを使用した SNMPv3 通知の構成

SNMP 通知ホスト myhost.cisco.com の DNS 名を使用して SNMPv3 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server host myhost.cisco.com traps version 3 noauth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 トラップを受信できるように構成し、noAuthNoPriv の securityLevel を構成します。

ステップ 3 switch(config)# **snmp-server host myhost.cisco.com informs version 3 auth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthNoPriv の securityLevel を構成します。

ステップ 4 switch(config)# **snmp-server host myhost.cisco.com informs version 3 priv testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthPriv の securityLevel を構成します。

ステップ 5 switch(config)# **no snmp-server host myhost.cisco.com informs version 3 testuser noauth udp-port 2162**

指定済みホストが SNMPv3 情報を受信できないようにします。

場所に基づく SNMPv3 ユーザの認証

場所に基づいて、ローカルまたはリモートの SNMPv3 ユーザを認証できます。

SNMPv3 サーバーの AAA 排他的動作を有効にするには、グローバル構成モードで次のコマンドを使用します。

コマンド	目的
snmp-server aaa exclusive-behavior enable	場所に基づいてユーザを認証するために SNMPv3 サーバーの AAA 排他的動作を有効にします。 ユーザの場所および AAA サーバーが有効かどうかによって、排他的動作は以下のようになります。 • ユーザがローカル ユーザであり、AAA サーバーが有効の場合、ユーザに対するクエリは失敗し、「Unknown user」というメッセージが表示されます。 • ユーザがリモート AAA ユーザであり、AAA サーバーが無効の場合、ユーザに対するクエリは失敗し、「Unknown user」というメッセージが表示されます。 • ユーザがローカル ユーザとリモート ユーザの両方である場合 AAA ユーザと AAA サーバーが有効の場合、リモート ログイン情報を持つクエリは成功し、ローカル ログイン情報を持つクエリは失敗し、「Incorrect password」というメッセージが表示されます。AAA サーバーが無効の場合、ローカル リモート ログイン情報を持つクエリは成功し、リモート ログイン情報を持つクエリは失敗し、「Incorrect password」というメッセージが表示されます。

SNMP 通知のイネーブル化

Table 3: SNMP 通知のイネーブル化 , on page 20 に、Cisco NX-OS MIB の通知を有効化する CLI コマンドを示します。

***Table 3: 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	**Click the Other tab and check FRU Changes.**
CISCO-FCC-MIB	**Click the Other tab and check FCC.**
CISCO-DM-MIB	**Click the FC tab and check Domain Mgr RCF.**

MIB	DCNM-SAN チェックボックス
CISCO-NS-MIB	**Click the FC tab and check Name Server.**
CISCO-FCS-MIB	**Click the Other tab and check FCS Rejects.**
CISCO-FDMI-MIB	**Click the Other tab and check FDMI.**
CISCO-FSPF-MIB	**Click the FC tab and check FSPF Neighbor Change.**
CISCO-LICENSE-MGR-MIB	**Click the Other tab and check License Manager.**
CISCO-IPSEC-SIGNALLING-MIB	**Click the Other tab and check IPSEC.**
CISCO-PSM-MIB	**Click the Other tab and check Port Security.**
CISCO-RSCN-MIB	**Click the FC tab and check RSCN ILS, and RCSN ELS.**
SNMPv2-MIB	**Click the Other tab and check SNMP AuthFailure.**
VRRP-MIB, CISCO-IETF-VRRP-MIB	**Click the Other tab and check VRRP.**
CISCO-ZS-MIB	**Click the FC tab and check Zone Rejects, Zone Merge Failures, Zone Merge Successes, Zone Default Policy Change, and Zone Unsuppd Mode.**

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
- ライセンス
- 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。

サポートされているトラップは、次のレベルで有効または無効にできます。

- スイッチ レベル：snmp-server enable traps コマンドを使用して、サポートされている MIB のすべてのトラップをスイッチ レベルで有効にできます。
- 機能レベル：機能名を指定して snmp-server enable traps コマンドを使用すると、機能レベルでトラップを有効にできます。

```
switch =>snmp-server enable traps callhome ?
event-notify    Callhome External Event Notification
smtp-send-fail  SMTP Message Send Fail notification
```

- 個々のトラップ：機能名を指定して snmp-server enable traps コマンドを使用して、個々のレベルでトラップを有効にできます。

```
switch =>snmp-server enable traps callhome event-notify ?
```

Note snmp-server enable traps CLI コマンドを使用すると、SNMP に行った構成に応じて、トラップとインフォームの両方を有効にできます。snmp-server host CLI コマンドによって表示される通知を参照してください。

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。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server enable traps fcdomain**

指定された SNMP（fcdomain）通知を有効にします。

ステップ 3 switch(config)# **no snmp-server enable traps**

指定した SNMP 通知を無効にします。通知名を指定しないと、すべての通知が無効になります。

通知ターゲット 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。

通知ターゲット ユーザを構成するには次のコマンドを使用します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03**

指定されたエンジン ID を持つ SNMP マネージャの指定されたログイン情報を使用して、通知ターゲット ユーザを構成します。

Note Cisco MDS NX-OS リリース 8.5(1) 以降、AES-128 は SNMPv3 のデフォルトのプライバシー プロトコルです。

ステップ 3 switch(config)# **no snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03**

通知ターゲット ユーザを削除します。

通知ターゲット ユーザのログイン情報は、構成した SNMPmanager へ送る SNMPv3 インフォーム通知メッセージの暗号化に使用されます（**snmp-server host** コマンドに表記されているとおり）。

スイッチの LinkUp/LinkDown 通知の構成

NX-OS リリース 4.2(1) 以降を使用してスイッチの LinkUp/LinkDown 通知を構成するには、次の手順に従います。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **snmp-server enable traps link extended-link**

IETF 拡張 linkUp 通知のみを有効にします。

ステップ 3 switch(config)# **snmp-server enable traps link extended-linkDown**

IETF 拡張 linkDown 通知のみを有効にします。

ステップ 4 switch(config)# **snmp-server enable traps link cieLinkDown**

シスコ拡張リンク ステート ダウン通知を有効にします。

ステップ 5 switch(config)# **snmp-server enable traps link cieLinkUp**

シスコ拡張リンク ステート アップ通知を有効にします。

ステップ 6 switch(config)# **snmp-server enable traps link connUnitPortStatusChange**

FCMGMT を有効にします。接続ユニットの全体的なステータス 通知。

ステップ 7 switch(config)# **snmp-server enable traps link delayed-link-state-change**

遅延リンク ステートの変更を有効にします。

遅延リンク ステート トラップを無効にして、デバイスがポート ダウン SNMP アラートをすぐに生成できるようにします。

- NX-OS バージョン 6.2(5) 以前で、**no system delayed-traps enable mode FX** コマンドを使用します。
- NX-OS バージョン 6.2(7) 以降で、**no snmp-server enable traps link delayed-link-state-change** コマンドを使用します。

Note 特定の NX-OS リリース バージョン間のアップグレードについては、遅延リンク ステート トラップが無効になっていることを確認してください。5.(x)、6.1(x)、6.2(x) などの以前のリリースから 6.2(7) 以降のリリースに移行する場合は、**no snmp-server enable traps link delayed-link-state-change** コマンドを使用して遅延リンク ステート トラップを明示的に無効にしてください。

ステップ 8 switch(config)# **snmp-server enable traps link extended-linkDown**

IETF 拡張リンク ステート ダウン通知を有効にします。

ステップ 9 switch(config)# **snmp-server enable traps link extended-linkUp**

IETF 拡張リンク ステート ダウン通知を有効にします。

ステップ 10 switch(config)# **snmp-server enable traps link fcTrunkIfDownNotify**

FCFE リンク ステート ダウン通知を有効にします。

ステップ 11 switch(config)# **snmp-server enable traps link fcTrunkIfUpNotify**

FCFE リンク ステート アップ通知を有効にします。

ステップ 12 switch(config)# **snmp-server enable traps link fcot-inserted**

FCOT 情報トラップを有効にします。

ステップ 13 switch(config)# **snmp-server enable traps link fcot-removed**

FCOT 情報トラップを有効にします。

ステップ 14 switch(config)# **snmp-server enable traps link linkDown**

IETF リンク ステート ダウン通知を有効にします。

ステップ 15 switch(config)# **snmp-server enable traps link linkUp**

IETF リンク ステート アップ通知を有効にします。

ステップ 16 switch(config)# **no snmp-server enable traps link**

デフォルト設定に戻します（IETF 拡張済み）。

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。

特定のインターフェイスに対してSNMP リンクステートを無効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **interface fc** *slot/port*

SNMP リンクステート トラップを無効にするインターフェイスを指定します。

ステップ 3 switch(config-if)# **no link-state-trap**

インターフェイスの SNMP リンクステート トラップをディセーブルにします。

ステップ 4 switch(config-if)# **link-state-trap**

インターフェイスの SNMP リンクステート トラップを有効にします。

エンティティ（FRU）トラップの構成

個々の SNMP トラップ制御を有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 **switch(config)# snmp-server enable traps entity**

個別の SNMP トラップ制御を有効にします。

ステップ 3 **switch(config)# snmp-server enable entity_fan_status_change**

エンティティ ファン ステータスの変更を有効にします。

ステップ 4 **switch(config)# snmp-server enable entity_mib_change**

エンティティ MIB の変更を有効にします。

ステップ 5 **switch(config)# snmp-server enable entity_module_inserted**

エンティティ モジュールを挿入できるようにします。

ステップ 6 **switch(config)# snmp-server enable entity_module_removed**

エンティティ モジュールを削除できるようにします。

ステップ 7 **switch(config)# snmp-server enable entity_module_status_change**

エンティティ モジュールのステータス変更を有効にします。

ステップ 8 **switch(config)# snmp-server enable entity_power_out_change**

エンティティの電源切断の変更を有効にします。

ステップ 9 **switch(config)# snmp-server enable entity_power_status_change**

エンティティの電源ステータスの変更を有効にします。

ステップ 10 **switch(config)# snmp-server enable entity_unrecognised_module**

エンティティが認識されないモジュールを有効にします。

Note これらのトラップはすべて、従来の FRU トラップに関係しています。

AAA 同期時間の変更

同期したユーザ設定を Cisco NX-OS に維持させる時間の長さを変更できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**snmp-server aaa-user cache-timeout** *seconds* **例：** `switch(config)# snmp-server aaa-user cache-timeout 1200`	ローカル キャッシュで AAA 同期ユーザ設定を維持する時間を設定します。値の範囲は 1 ～ 86400 秒です。デフォルトは 60000 です。
ステップ 3	（任意） **copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SNMP の設定の確認

SNMP のコンフィギュレーション情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show running-config	実行構成を表示します。 **Note** Cisco MDS NX-OS リリース 8.5(1) 以降、構成されたプライバシー プロトコル AES-128 または DES を持つ SNMP ユーザが実行構成に表示されます。これは、実行構成で AES-128 ユーザだけが **aes-128** オプションとして表示されていた Cisco MDS NX-OS リリース 8.5(1) より前のリリースとは異なります。Cisco MDS NX-OS リリース 8.5(1) 以降、ユーザはデフォルトで AES-128 プロトコルで構成されます。
show interface	特定のインターフェイスの SNMP リンク ステート トラップ構成を表示します。
show snmp trap	すべての通知とそのステータスを表示します
show snmp	構成された SNMP 情報、SNMP 連絡先のカウンタ情報、場所、およびパケット設定を表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

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

インターフェイスの SNMP リンクステート トラップを無効にするたびに、コマンドがシステムの実行構成にも追加されます。

実行構成を表示するには、インターフェイスに **show running-config** コマンドを使用します。

```
switch# no link-state-trap
switch# show running-config interface fc2/25

!Command: show running-config interface fc2/25
!Running configuration last done at: Fri Sep 20 11:28:19 2019
!Time: Fri Sep 20 11:28:22 2019

version 8.4(1)

interface fc2/25
  no link-state-trap
  no shutdown
```

特定のインターフェイスの SNMP リンクステート トラップ構成を表示するには、**show interface** コマンドを入力します。

```
switch# show interface fc2/25

fc2/25 is trunking
```

```
    Hardware is Fibre Channel, SFP is long wave laser cost reduced
    Port WWN is 20:59:54:7f:ee:ea:c0:00
    Peer port WWN is 20:1d:00:de:fb:b1:7b:80
    Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Admin Speed is auto max 32 Gbps
    Operating Speed is 32 Gbps
    Rate mode is dedicated
    Port flow-control is ER_RDY
.
.
.
```

SNMP トラップの表示

すべての通知とそのステータスを表示するには、**show snmp trap** コマンドを使用します。

```
switch# show snmp trap
--------------------------------------------------------------------------------
Trap type                                                              Enabled
--------------------------------------------------------------------------------
entity               : entity_mib_change                               Yes
entity               : entity_module_status_change                     Yes
entity               : entity_power_status_change                      Yes
entity               : entity_module_inserted                          Yes
entity               : entity_module_removed                           Yes
entity               : entity_unrecognised_module                      Yes
entity               : entity_fan_status_change                        Yes
entity               : entity_power_out_change                         Yes
link                 : linkDown                                        Yes
link                 : linkUp                                          Yes
link                 : extended-linkDown                               Yes
link                 : extended-linkUp                                 Yes
link                 : cieLinkDown                                     Yes
link                 : cieLinkUp                                       Yes
link                 : connUnitPortStatusChange                        Yes
link                 : fcTrunkIfUpNotify                               Yes
link                 : fcTrunkIfDownNotify                             Yes
link                 : delayed-link-state-change                       Yes
link                 : fcot-inserted                                   Yes
link                 : fcot-removed                                    Yes
callhome             : event-notify                                    No
callhome             : smtp-send-fail                                  No
cfs                  : state-change-notif                              No
cfs                  : merge-failure                                   No
fcdomain             : dmNewPrincipalSwitchNotify                      No
fcdomain             : dmDomainIdNotAssignedNotify                     No
fcdomain             : dmFabricChangeNotify                            No
rf                   : redundancy_framework                            Yes
aaa                  : server-state-change                             No
license              : notify-license-expiry                           Yes
license              : notify-no-license-for-feature                   Yes
license              : notify-licensefile-missing                      Yes
license              : notify-license-expiry-warning                   Yes
scsi                 : scsi-disc-complete                              No
fcns                 : reject-reg-req                                  No
fcns                 : local-entry-change                              No
fcns                 : db-full                                         No
fcns                 : remote-entry-change                             No
```

```
rscn                : rscnElsRejectReqNotify                    No
rscn                : rscnIlsRejectReqNotify                    No
rscn                : rscnElsRxRejectReqNotify                  No
rscn                : rscnIlsRxRejectReqNotify                  No
fcs                 : request-reject                            No
fcs                 : discovery-complete                        No
fctrace             : route                                     No
zone                : request-reject1                           No
zone                : merge-success                             No
zone                : merge-failure                             No
zone                : default-zone-behavior-change              No
zone                : unsupp-mem                                No
port-security       : fport-violation                           No
port-security       : eport-violation                           No
port-security       : fabric-binding-violation                  No
vni                 : virtual-interface-created                 No
vni                 : virtual-interface-removed                 No
vsan                : vsanStatusChange                          No
vsan                : vsanPortMembershipChange                  No
fspf                : fspfNbrStateChangeNotify                  No
upgrade             : UpgradeOpNotifyOnCompletion               No
upgrade             : UpgradeJobStatusNotify                    No
feature-control     : FeatureOpStatusChange                     No
vrrp                : cVrrpNotificationNewMaster                No
fdmi                : cfdmiRejectRegNotify                      No
snmp                : authentication                            No
```

SNMP セキュリティ情報の表示

show snmp コマンドを使用して、構成済みの SNMP 情報を表示します（以下の例を参照）。

SNMPユーザの詳細

次の SNMP ユーザの詳細の例：

```
switch# show snmp user
_____________________________________________________________________
                   SNMP USERS
_____________________________________________________________________
User                            Auth  Priv(enforce) Groups
____                            ____  ______________ ______
admin                           md5   des(no)       network-admin
testusr                         md5   aes-128(no)   role111
                                                     role222
_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________
User                            Auth  Priv
____                            ____  ____
testtargetusr                   md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

SNMPコミュニティ情報

次の例では、SNMP コミュニティ情報を表示します。

```
switch# show snmp community
```

```
Community             Group / Access      context
_________             ______________      _______
dcnm_user             network-admin
admin                 network-admin
```

SNMP ホスト情報

次の例は、SNMP ホスト情報を表示します。

```
switch# show snmp host
Host                              Port Version  Level  Type   SecName
____                              ____ _______  ______ ____  _______
171.16.126.34                     2162 v2c      noauth trap   public
171.16.75.106                     2162 v2c      noauth trap   public
...
171.31.58.97                      2162 v2c      auth   trap   public
...
```

show snmp コマンドは、SNMP の連絡先、場所、およびパケット設定のカウンタ情報を表示します。このコマンドは、Cisco MDS 9000 ファミリ DCNM-SAN 全体で使用される情報を提供します（『System Management Configuration Guide、Cisco DCNM for SAN』を参照）。次の例を参照してください。

SNMP 情報

次の例では、SNMP 情報を表示します。

```
switch# show snmp
sys contact:
sys location:
1631 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        64294 Number of requested variables
        1 Number of altered variables
        1628 Get-request PDUs
        0 Get-next PDUs
        1 Set-request PDUs
152725 SNMP packets output
        0 Too big errors
        1 No such name errors
        0 Bad values errors
        0 General errors
Community                      Group / Access
---------                      ------
public                          rw

_____________________ SNMP USERS ____________________________________________
User                           Auth  Priv(enforce) Groups
____                           ____  ______________ ______
admin                          md5   des(no)        network-admin
testusr                        md5   aes-128(no)    role111
                                                    role222
```

```
_____________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________
User                            Auth  Priv

____                            ____  ____
testtargetusr                   md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

SNMP エンジン ID を表示します

次の例では、SNMP エンジン ID を表示します。

```
switch# show snmp engineID
Local SNMP engineID: [Hex] 8000000903000DEC2CF180
                     [Dec] 128:000:000:009:003:000:013:236:044:241:128
```

SNMP セキュリティ グループに関する情報

次の例では、SNMP セキュリティ グループに関する情報を表示します。

```
switch# show snmp group
groupname: network-admin
security model: any
security level: noAuthNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-admin
security model: any
security level: authNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-operator
security model: any
security level: noAuthNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
groupname: network-operator
security model: any
security level: authNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
```

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

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。