CHAPTER 3

ユーザ ロールおよび共通ロールの設定

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 を使用して作成したロールは CLI を使用して変更でき、その逆も可能です。

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 for SAN（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。

この章では、次の事項について説明します。

ロールベースの許可の概要

Cisco MDS 9000 ファミリ スイッチはロールに基づいた認証を行います。ロールベースの許可は、ユーザをロール（役割）に割り当てることによってスイッチ操作へのアクセスを制限します。この種類の認証では、ユーザに割り当てられたロールに基づいて管理操作が制限されます。

コマンドを実行したり、コマンドを完了させたり、コンテキスト ヘルプを取得したりする場合に、コマンドへのアクセス権限があれば、操作を継続できます。

ここで説明する内容は、次のとおりです。

ロールの概要

ロールごとに複数のユーザを含めることができ、各ユーザは複数のロールに所属できます。たとえば、role1 ユーザにはコンフィギュレーション コマンドへのアクセスだけが、role2 ユーザには **debug** コマンドへのアクセスだけが許可されているとします。この場合、role1 と role2 の両方に所属しているユーザは、コンフィギュレーション コマンドと **debug** コマンドの両方にアクセスできます。

（注） ユーザが複数のロールに所属している場合、各ロールで許可されているすべてのコマンドを実行できます。コマンドへのアクセス権は、コマンドへのアクセス拒否よりも優先されます。たとえば、TechDocs グループに属しているユーザが、コンフィギュレーション コマンドへのアクセスを拒否されているとします。ただし、このユーザはエンジニアリング グループにも属しており、コンフィギュレーション コマンドへのアクセス権を持っています。この場合、このユーザはコンフィギュレーション コマンドにアクセスできます。

ヒント ロールを作成した時点で、必要なコマンドへのアクセスが即時に許可されるわけではありません。管理者が各ロールに適切なルールを設定して、必要なコマンドへのアクセスを許可する必要があります。

各ロールに対するルールと機能

各ロールに、最大 16 のルールを設定できます。これらのルールは、どの CLI コマンドを使用できるかを示します。規則が適用される順序は、ユーザ指定の規則番号で決まります。たとえば、ルール 1 のあとにルール 2 が適用され、ルール 3 以降が順に適用されます。network-admin ロールに属さないユーザは、ロールに関連したコマンドを実行できません。

たとえば、ユーザ A にすべての **show** CLI コマンドの実行を許可されていても、ユーザ A が network-admin ロールに所属していないかぎり、ユーザ A は **show role** CLI コマンドの出力を表示できません。

ルールは特定のロールで実行できる操作を示します。ルールを構成する要素は、ルール番号、ルール タイプ（許可または拒否）、CLI コマンド タイプ（**config**、**clear**、**show**、**exec**、**debug** など）、および任意の機能名（FSPF、ゾーン、VSAN、fcping、インターフェイスなど）です。

（注） この場合、**exec** CLI コマンドでは、**show**、**debug** および **clear** の各 CLI コマンドのカテゴリに含まれない、EXEC モード内のすべてのコマンドが対象になります。

VSAN ポリシーの概要

VSAN ポリシーの設定には、ENTERPRISE_PKG ライセンスが必要です（詳細については、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください）。

選択した VSAN セットだけにタスクの実行が許可されるように、ロールを設定できます。デフォルトでは、どのロールの VSAN ポリシーも許可に設定されているため、すべての VSAN に対してタスクが実行されます。選択した VSAN セットだけにタスクの実行が許可されるロールを設定できます。1 つのロールに対して選択的に VSAN を許可するには、VSAN ポリシーを拒否に設定し、あとでその設定を許可に設定するか、または適切な VSAN を設定します。

（注） VSAN ポリシーが拒否に設定されているロールに設定されているユーザは、E ポートの設定を変更できません。これらのユーザが変更できるのは、（ルールの内容に応じて）F ポートまたは FL ポートの設定だけです。これにより、これらのユーザは、ファブリックのコア トポロジに影響する可能性のある設定を変更できなくなります。

ヒント ロールを使用して、VSAN 管理者を作成できます。設定したルールに応じて、これらの VSAN 管理者は他の VSAN に影響を与えることなく、VSAN に MDS 機能（ゾーン、fcdomain、VSAN プロパティなど）を設定できます。また、ロールが複数の VSAN での処理を許可している場合、VSAN 管理者はこれらの VSAN 間で F ポートまたは FL ポートのメンバーシップを変更できます。

VSAN ポリシーが拒否に設定されているロールに属すユーザのことを、VSAN 制限付きユーザと呼びます。

ロールの配信

ロールベース設定は、Cisco Fabric Services（CFS）インフラストラクチャを利用して効率的なデータベース管理を可能にし、ファブリック全体に対するシングル ポイントでの設定を提供します。

次の設定が配信されます。

- ロール名と説明
- ロールに対するルールのリスト
- VSAN ポリシーと許可されている VSAN のリスト

ロール データベースの概要

ロールベース設定は 2 つのデータベースを利用して設定内容の受け取りと実装を行います。

- コンフィギュレーション データベース：ファブリックで現在実行されているデータベースです。
- 保留中のデータベース：以降の設定変更は保留中のデータベースに保存されます。設定を修正した場合は、保留中のデータベースの変更内容をコンフィギュレーション データベースにコミットするかまたは廃棄する必要があります。その間、ファブリックはロックされた状態になります。保留中のデータベースへの変更は、その変更をコミットするまでコンフィギュレーション データベースに反映されません。

ファブリックのロック

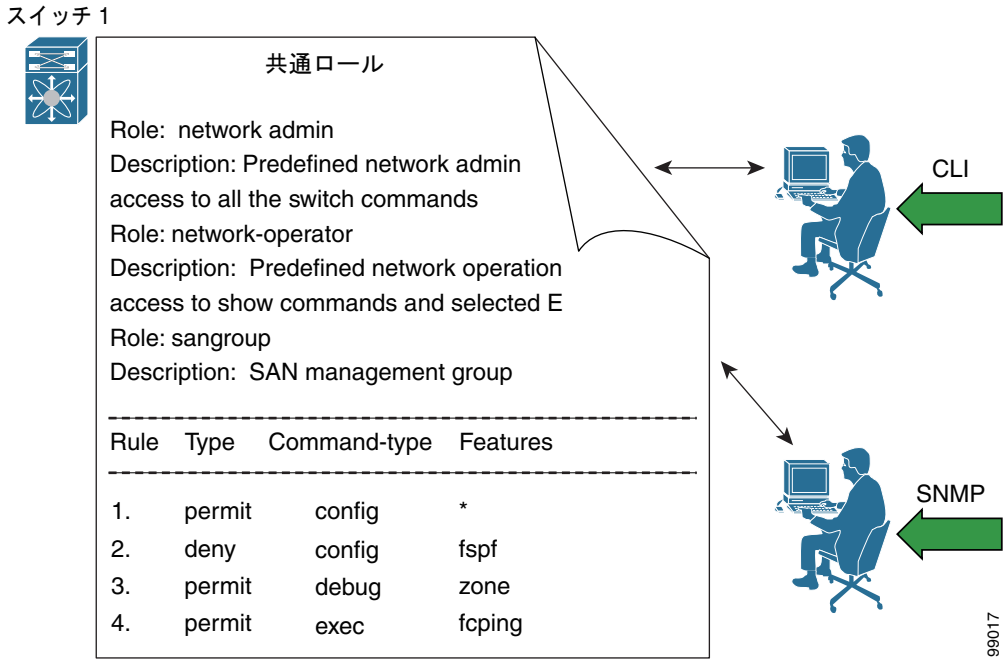
データベースを修正する最初のアクションで保留中のデータベースが作成され、ファブリック全体の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーション データベースの複製が、最初の変更とともに保留中のデータベースになります。

共通ロールの概要

Cisco MDS 9000 ファミリのすべてのスイッチで、CLI と SNMP は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（図 3-1 を参照）。

図 3-1　　共通ロール



SNMP の各ロールは、CLI を通じて作成または変更されたロールと同じです（「ロールベースの許可の概要」（P.3-1）を参照）。

各ロールは、必要に応じて 1 つ以上の VSAN に制限できます。

SNMP または CLI を使用して、新しいロールの作成、または既存のロールの変更を実行できます。

- SNMP：CISCO-COMMON-ROLES-MIB を使用してロールを設定または変更します。詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。
- CLI：**role name** コマンドを使用します。

CLI オペレーションから SNMP へのマッピング

SNMP では、GET、SET、および NOTIFY の 3 つの操作だけを行うことができます。CLI では、DEBUG、SHOW、CONFIG、CLEAR、および EXEC の 5 つの操作を行うことができます。

（注）　NOTIFY には、CLI の syslog メッセージのような制限はありません。

表 3-1 は、CLI オペレーションが SNMP オペレーションにどのようにマッピングされるかを示します。

表 3-1　CLI オペレーションから SNMP オペレーションへのマッピング

CLI オペレーション	SNMP オペレーション
DEBUG	Ignored
SHOW	GET
CONFIG	SET
CLEAR	SET
EXEC	SET

ユーザの作成に関する注意事項

snmp-server user オプションで指定したパスフレーズと **username** オプションで指定したパスワードは同期されます。

デフォルトでは、明示的に期限を指定しないかぎり、ユーザ アカウントは無期限に有効です。**expire** オプションを使用すると、ユーザ アカウントをディセーブルにする日付を設定できます。日付は YYYY-MM-DD 形式で指定します。

ユーザを作成する際、次の点に注意してください。

- 1 つのスイッチには、最大 256 ユーザを設定できます。
- bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、rpc、rpcuser、xfs、gdm、mtsuser、ftpuser、man、sys は予約語で、ユーザの設定には使用できません。
- ユーザ パスワードはスイッチ コンフィギュレーション ファイルに表示されません。
- パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードでは大文字と小文字が区別されます。「admin」は Cisco MDS 9000 ファミリ スイッチのデフォルト パスワードではなくなりました。強力なパスワードを明確に設定する必要があります。

注意　Cisco MDS NX-OS では、リモートで作成するか（TACACS+ または RADIUS を使用）ローカルで作成するかに関係なく、英数字または特定の特殊文字（+（プラス）、=（等号）、_（下線）、-（ハイフン）、\（バックスラッシュ）、および .（ピリオド））を使って作成したユーザ名がサポートされます。特殊文字（指定された特殊文字を除く）を使用してローカル ユーザ名を作成することはできません。サポートされていない特殊文字によるユーザ名が AAA サーバに存在し、ログイン時に入力されると、そのユーザはアクセスを拒否されます。

強力なパスワードの特性

強力なパスワードは、次の特性を持ちます。

- 長さが 8 文字以上である。
- 複数の連続する文字（「abcd」など）を含んでいない。
- 複数の同じ文字の繰り返し（「aaabbb」など）を含んでいない。
- 辞書に載っている単語を含んでいない。
- 固有名詞を含んでいない。
- 大文字と小文字の両方を含んでいない。
- 数字を含んでいる。

強力なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

SSH の概要

SSH は Cisco NX-OS CLI にセキュアなコミュニケーションを提供します。SSH キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, Adelman（RSA）を使用する SSH2
- DSA を使用する SSH2

ブート モード SSH

セキュリティやセキュリティ関連の問題がますます強調されているため、このリリースの **ssh** コマンドはブート モードで実行されます。SSH は、セキュア チャネル上で通信し、チャネル上で送信する前にデータが暗号化されるため、ネットワーク上で推奨される、よりセキュアなデータ交換の方法です。

例 3-1 に、**ssh** コマンドを使用して、任意のスイッチからリモート サーバに接続する方法を示します。

例 3-1　　任意のスイッチからのリモート サーバの接続

```
switch# ssh admin @ hostname
```

デジタル証明書を使用した SSH 認証

Cisco MDS 9000 ファミリ スイッチ製品の SSH 認証はホスト認証に X.509 デジタル証明書のサポートを提供します。X.509 デジタル証明書は出処と完全性を保証する 1 つのデータ項目です。保護された通信を行うための暗号キーを含み、提出者の身元を証明するために、信頼できる認証局（CA）によって「署名」されています。X.509 デジタル証明書のサポートにより、認証に DSA と RSA のいずれかのアルゴリズムを使用します。

証明書インフラストラクチャは Secure Socket Layer（SSL）をサポートする最初の証明書を使用し、セキュリティ インフラストラクチャにより照会または通知の形で返信を受け取ります。証明書が信頼できる CA のいずれかから発行されたものであれば、証明書の検証は成功です。

スイッチは、X.509 証明書を使用する SSH 認証、または公開キー証明書を使用する SSH 認証のいずれかに設定できますが、両方に設定することはできません。いずれかに設定されている場合は、その認証が失敗すると、パスワードの入力を求められます。

CA およびデジタル証明書の詳細については、第 6 章「認証局およびデジタル証明書の設定」を参照してください。

パスワードのないファイル コピーおよび SSH

セキュア シェル（SSH）公開キー認証は、パスワードのないログインを行うために使用できます。SCP および SFTP は SSH をバックグラウンドで使用するため、これらのコピー プロトコルを使用することにより、公開キー認証によるパスワードのないコピーが可能になります。この NX-OS バージョンは、SCP および STFP クライアント機能だけをサポートしています。

SSH による認証に使用できる RSA および DSA ID を作成できます。この ID は、公開キーと秘密キーという 2 つの部分から構成されています。公開キーおよび秘密キーはスイッチによって生成されますが、外部で生成してスイッチにインポートすることもできます。インポートするためには、キーが OPENSSH 形式であることが必要です。

SSH サーバをホストしているホスト マシン上でキーを使用するには、そのマシンに公開キー ファイルを転送し、サーバの SSH ディレクトリ（たとえば、$HOME/.ssh）にある許可済みキー ファイルに内容を追加します。秘密キーをインポートおよびエクスポートする場合、キーは暗号化によって保護されます。ユーザは、キーのパスフレーズを入力するように求められます。パスフレーズを入力すると、秘密キーは暗号化によって保護されます。パスワード フィールドを空白のままにしておくと、キーは暗号化されません。

キーを別のスイッチにコピーする必要がある場合は、スイッチからホスト マシンにキーをエクスポートし、そのマシンから他のスイッチにキーをインポートします。

キー ファイルは、リブート後も維持されます。

注意事項と制限

ファブリックのマージではスイッチ上のロール データベースは変更されません。2 つのファブリックをマージし、それらのファブリックが異なるロール データベースを持つ場合は、ソフトウェアがアラート メッセージを発します。

概念の詳細については、「RADIUS および TACACS+ 設定のマージに関する注意事項」（P.4-15）を参照してください。

- ファブリック全体のすべてのスイッチでロール データベースが同一であることを確認してください。
- 必ず目的のデータベースになるように任意のスイッチのロール データベースを編集してから、コミットしてください。これによりファブリック内のすべてのスイッチ上のロール データベースの同期が保たれます。

デフォルト設定

表 3-2 に、スイッチのすべてのスイッチ セキュリティ機能のデフォルト設定を示します。

表 3-2　スイッチ セキュリティのデフォルト設定

パラメータ	デフォルト
Cisco MDS スイッチでのロール	ネットワーク オペレータ（network-operator）
AAA 設定サービス	ローカル
認証ポート	1812
アカウンティング ポート	1813
事前共有キーの送受信	クリア テキスト
RADIUS サーバ タイムアウト	1 秒
RADIUS サーバ再試行	1 回
TACACS+	ディセーブル
TACACS+ サーバ	未設定
TACACS+ サーバのタイムアウト	5 秒
AAA サーバへの配信	ディセーブル
ロールに対する VSAN ポリシー	許可
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
パスワード強度	イネーブル
アカウンティング ログ サイズ	250 KB
SSH サービス	イネーブル
Telnet サービス	ディセーブル

ユーザ ロールおよび共通ロールの設定

ここで説明する内容は、次のとおりです。

ロールとプロファイルの設定

手順の詳細

（注）　network-admin ロールに属するユーザだけがロールを作成できます。

DCNM-SAN を使用して、追加ロールの作成または既存ロールのプロファイル修正を行う手順は、次のとおりです。

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

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

ステップ 3　DCNM-SAN で [Create Row] をクリックして、ロールを 1 つ作成します。

ステップ 4　ロールの設定先のスイッチを選択します。

ステップ 5　[Name] フィールドに、ロールの名前を入力します。

ステップ 6　[Description] フィールドにロールの説明を入力します。

ステップ 7　（任意）[Enable] チェックボックスをオンにして仮想ストレージ エリア ネットワーク（VSAN）範囲をイネーブルにし、このロールを適用できる VSAN のリストを [Scope] フィールドに入力します。

ステップ 8　[Create] をクリックして、ロールを作成します。

（注）　Device Manager では、スイッチのビューを表示するために、Device Manager に必要な 6 つのロールが自動的に作成されます。作成されるロールは、**system**、**snmp**、**module**、**interface**、**hardware**、および **environment** です。

共通ロールの削除

手順の詳細

DCNM-SAN を使用して共通ロールを削除する手順は、次のとおりです。

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

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

ステップ 3　削除するロールをクリックします。

ステップ 4　[Delete Row] アイコンをクリックして共通ロールを削除します。

ステップ 5　[Yes] をクリックして削除を確認するか、[No] でキャンセルします。

ルールの修正

手順の詳細

Device Manager を使用して既存ロールのルールを修正する手順は、次のとおりです。

ステップ 1　[Security] > [Roles] を選択します。

ステップ 2　ルールを編集するロールをクリックします。

ステップ 3　[Rules] をクリックして、そのロールのルールを表示します。

[Edit Role Rules] ダイアログボックスが表示されます。

ステップ 4　共通ロールについて、イネーブルまたはディセーブルにするルールを編集します。

ステップ 5　[Apply] をクリックして、新しいルールを適用します。

rule 1 が最初に適用され、たとえば sangroup ユーザがすべての **config** CLI コマンドにアクセスすることが許可されます。次にルール 2 が適用され、sangroup ユーザには FSPF 設定が拒否されます。結果として、sangroup ユーザは **fspf** CLI コンフィギュレーション コマンドを除く、他のすべての **config** CLI コマンドを実行できます。

（注）　ルールは適用する順序が重要です。これらの 2 つのルールを入れ替え、**deny config feature fspf** ルールを最初に置き、次に **permit config** ルールを置いた場合は、2 番めのルールがグローバルに効果を持って最初のルールに優先するため、sangroup ユーザの全員にすべてのコンフィギュレーション コマンドの実行を許可することになります。

VSAN ポリシーの変更

手順の詳細

DCNM-SAN を使用して既存ロールの VSAN ポリシーを修正する手順は、次のとおりです。

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

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

ステップ 3　VSAN 範囲をイネーブルにして、このロールを VSAN のサブセットに制限する場合は、[Scope Enable] チェックボックスをオンにします。

ステップ 4　[Scope VSAN Id List] フィールドに、このロールを制限する VSAN のリストを入力します。

ステップ 5　[Apply Changes] をクリックして、変更を保存します。

ロールベース設定変更のコミット

保留中のデータベースに行われた変更をコミットすると、その設定はそのファブリック内のすべてのスイッチにコミットされます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。コンフィギュレーション データベースはこれ以降、コミットされた変更を保持し、保留中のデータベースは消去されます。

手順の詳細

DCNM-SAN を使用してロールベース設定変更をコミットする手順は、次のとおりです。

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

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

ステップ 3　[Global] ドロップダウン メニューを [enable] に設定して CFS をイネーブルにします。

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。

ステップ 5　[Config Action] ドロップダウン メニューを [commit] に設定し、CFS を使用してこのロールをコミットします。

ステップ 6　[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。

ロールベース設定変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、コンフィギュレーション データベースは影響を受けないまま、ロックが解除されます。

手順の詳細

DCNM-SAN を使用してロールベース設定変更を廃棄する手順は、次のとおりです。

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

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

ステップ 3　[Config Action] ドロップダウン メニューを [abort] に設定して、コミットされていないすべての変更を廃棄します。

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。

ロールベース設定の配布のイネーブル化

手順の詳細

DCNM-SAN を使用してロールベース設定配信をイネーブルにする手順は、次のとおりです。

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

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

ステップ 3　Global ドロップダウン メニューを [enable] に設定して CFS 配信をイネーブルにします。

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。

セッションの消去

手順の詳細

DCNM-SAN を使用して強制的にファブリック内の既存のロール セッションを消去する手順は、次のとおりです。

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

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

ステップ 3　[Config Action] ドロップダウン メニューを [clear] に設定して、保留中のデータベースを消去します。

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。

注意　セッションを消去すると、保留中のデータベース内のすべての変更が失われます。

ユーザの設定

ユーザを設定する前に、作成するユーザに関連付けるロールを設定したことを確認します。

（注）　Cisco SAN-OS Release 3.1(2b) では、暗号化がイネーブルであるかどうかを DCNM-SAN が自動的にチェックするため、ユーザを作成することができます。

手順の詳細

DCNM-SAN を使用して、新規ユーザの設定または既存ユーザのプロファイル修正を行う手順は、次のとおりです。

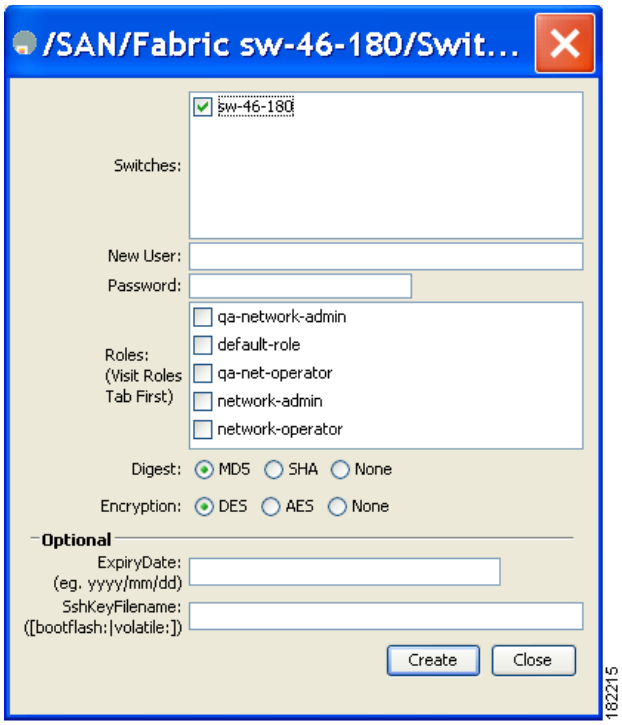
ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。

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] アイコンをクリックします。

[Users - Create] ダイアログボックスが表示されます（図 3-2 を参照）。

図 3-2　[Users - Create] ダイアログボックス



ステップ 4　（任意）[Switches] チェックボックスを変更して 1 つ以上のスイッチを指定することもできます。

ステップ 5　[New User] フィールドにユーザ名を入力します。

ステップ 6　ユーザのパスワードを入力します。

ステップ 7　このユーザに関連付けるロールのチェックをオンにします。

「各ロールに対するルールと機能」（P.3-2）を参照してください。

ステップ 8　使用する認証プロトコルのタイプに対応する適切なオプションを選択します。デフォルト値は MD5 です。

ステップ 9　使用するプライバシー プロトコルのタイプに対応する適切なオプションを選択します。デフォルト値は DES です。

ステップ 10　（任意）このユーザの有効期限を入力します。

ステップ 11　（任意）SSH キーのファイル名を入力します。

ステップ 12　[Create] をクリックしてエントリを作成します。

ユーザの削除

手順の詳細

DCNM-SAN を使用してユーザを削除する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [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　削除するユーザ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、選択したユーザを削除します。

ステップ 5　[Apply Changes] をクリックして、この変更を保存します。

SSH サービスの設定

RSA キーによるセキュア SSH 接続は、Cisco MDS 9000 ファミリのすべてのスイッチでデフォルトで使用できます。DSA キーによるセキュア SSH 接続が必要な場合は、デフォルトの SSH 接続をディセーブルにし、DSA キーを作生成して、SSH 接続をイネーブルにする必要があります（「SSH サーバ キー ペアの生成」（P.3-14）を参照）。

注意　SSH を使用してスイッチにログインするときに、**aaa authentication login default none** コマンドが発行済みの場合、ログインするには 1 つまたは複数のキー ストロークを入力する必要があります。キー ストロークをまったく入力しないで Enter キーを押すと、ログインが拒否されます。

ここで説明する内容は、次のとおりです。

SSH サーバ キー ペアの生成

SSH サービスを確立する前に、SSH サーバ キー ペアおよび適切なバージョンが存在することを確認します。使用中の SSH クライアント バージョンに従って、SSH サーバ キー ペアを生成します。各キー ペアに指定するビット数は、768 ～ 2048 です。

SSH サービスは、SSH バージョン 2 で使用する 2 種類のキー ペアを受け入れます。

- **dsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キー ペアが生成されます。
- **rsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キー ペアが生成されます。

注意　SSH キーをすべて削除した場合、新しい SSH セッションを開始できません。

手順の詳細

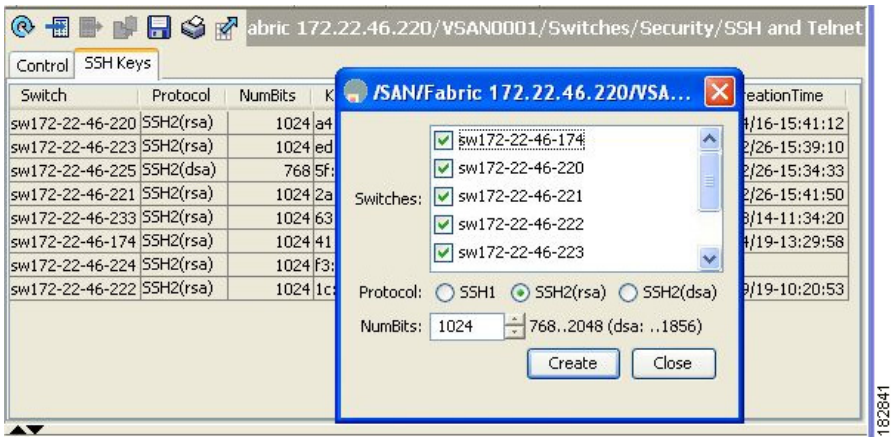
DCNM-SAN を使用して SSH キー ペアを生成する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開して [SSH and Telnet] を選択します。

ステップ 2　[Create Row] アイコンをクリックします。

SSH および Telnet キーの作成ダイアログボックスが表示されます（図 3-3 を参照）。

図 3-3　SSH および Telnet の作成ダイアログボックス



ステップ 3　この SSH キー ペアに割り当てるスイッチのチェックをオンにします。

ステップ 4　表示された [Protocols] からキー ペアのオプション タイプを選択します。表示されるプロトコルは、[SSH1]、[SSH2(rsa)]、および [SSH2(dsa)] です。

ステップ 5　[NumBits] ドロップダウン メニューで、キー ペアの生成に使用するビット数を設定します。

ステップ 6　[Create] をクリックして、キーを作成します。

（注）　1856 DSA NumberKeys は、Cisco MDS NX-OS ソフトウェア バージョン 4.1(1) 以降が稼働しているスイッチではサポートされません。

生成したキー ペアの上書き

必要なバージョンの SSH キー ペア オプションがすでに生成されている場合は、前回生成されたキー ペアをスイッチに上書きさせることができます。

手順の詳細

DCNM-SAN を使用して前回生成されたキー ペアを上書きする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開して [SSH and Telnet] を選択します。

[Information] ペインに設定が表示されます。

ステップ 2　上書きするキーを強調表示して [Delete Row] をクリックします。

ステップ 3　[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。

ステップ 4　[Create Row] アイコンをクリックします。

SSH および Telnet キーの作成ダイアログボックスが表示されます。

ステップ 5　この SSH キー ペアを割り当てるスイッチのチェックをオンにします。

ステップ 6　[Protocols] オプション ボタンで、キー ペアのオプション タイプを選択します。

ステップ 7　[NumBits] ドロップダウン メニューで、キー ペアの生成に使用するビット数を設定します。

ステップ 8　[Create] をクリックして、キーを作成します。

SSH または Telnet サービスのイネーブル化

デフォルトでは、SSH サービスは、RSA キーによってイネーブルになっています。

手順の詳細

（注）　SSH を介してスイッチにログインし、**aaa authentication login default none** CLI コマンドを発行した場合は、ログインするために 1 つ以上のキー ストロークを入力する必要があります。キー ストロークをまったく入力しないで Enter キーを押すと、ログインが拒否されます。

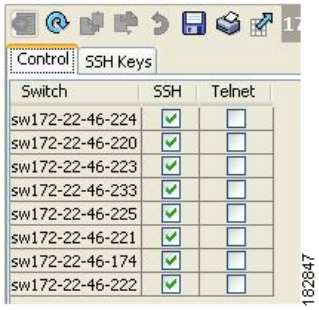
SSH を設定すると、DCNM-SAN によって SSH が自動的にイネーブルになります。

DCNM-SAN を使用して SSH をイネーブルまたはディセーブルにする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開して [SSH and Telnet] を選択します。

ステップ 2　[Control] タブを選択し、各スイッチの [SSH] チェックボックスまたは [Telnet] チェックボックスをオンにします（図 3-4 を参照）。

図 3-4　[SSH and Telnet] の [Control] タブ



ステップ 3　[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。

DCNM-SAN を使用した管理者パスワードの変更

手順の詳細

DCNM-SAN で管理パスワードを変更する手順は、次のとおりです。

ステップ 1　コントロール パネルの [Open] タブをクリックします。

ステップ 2　パスワード フィールドを選択して、ファブリックの既存ユーザのパスワードを変更します。

ステップ 3　[Open] をクリックして、ファブリックに接続します。

（注）　ファブリックに接続すると、新しいパスワードが保存されます。ユーザ名とパスワードのフィールドは、ファブリックの接続を解除した後に限り、[Fabric] タブで編集できます。

ユーザ ロールおよび共通ロール設定の確認

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。

ここで説明する内容は、次のとおりです。

ロールベース情報の表示

ルールはルール番号別、およびそれぞれのロールに基づいて表示されます。ロール名を指定しなかった場合はすべてのロールが表示されます。

Device Manager を使用して特定のロールのルールを表示する手順は、次のとおりです。

ステップ 1　[Security] > [Roles] をクリックします。

[Roles] ダイアログボックスが表示されます。

ステップ 2　ロール名を選択して [Rules] をクリックします。

[Rules] ダイアログボックスが表示されます。

ステップ 3　このロールに設定されたルールの要約を表示するには [Summary] をクリックします。

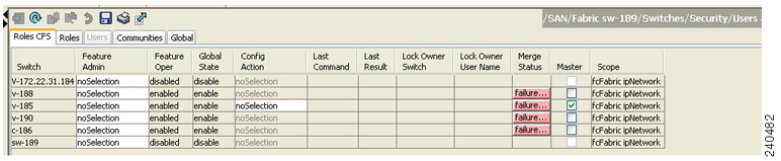
配信がイネーブルの場合のロールの表示

DCNM-SAN を使用してロールを表示する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [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] タブをクリックします（図 3-5 を参照）。

図 3-5　[Roles CFS] タブ



ステップ 3　[Config View As] ドロップダウン メニューの値を [pending] に設定して保留中のデータベースを表示するか、[Config View as] ドロップダウン メニューを [running] に設定して実行中のデータベースを表示します。

ステップ 4　[Apply Changes] をクリックして、この変更を保存します。

ユーザ アカウント情報の表示

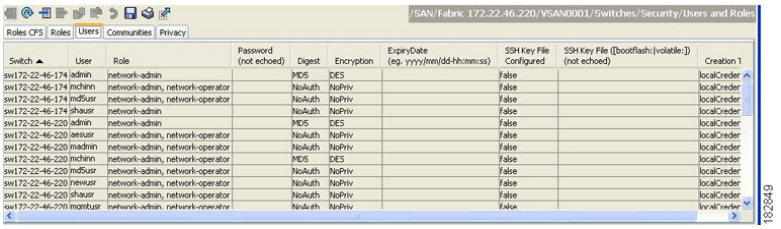
DCNM-SAN を使用して、設定したユーザ アカウントに関する情報を表示する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Security] を展開し、[Users and Roles] を選択します。

ステップ 2　[Users] タブをクリックします。

図 3-6 に示す SNMP ユーザのリストが [Information] ペインに表示されます。

図 3-6　[Users] タブに表示されるユーザ リスト



ユーザ ロールおよび共通ロールのフィールドの説明

共通ロール

（注）　共通ロールは、displayFCoE モードでは使用できません（セキュリティ ロールを使用してください）。

フィールド	説明
Description	共通ロールの説明。
Enable	共通ロールに VSAN の制約があるかどうかを指定します。
List	ユーザが制限された VSAN のリスト。

ユーザ ロールおよび共通ロール機能の履歴

表 3-3 に、この機能のリリース履歴を示します。5.x 以降のリリースで追加または変更された機能だけが、表に示されています。

表 3-3　FIPS 機能の履歴

機能名	リリース	機能情報
SSH への変更	5.0(1a)	ブート モード SSH、パスワードのないファイル、および SSH。
ロールの配信	5.0(1a)	ロールベース設定の配布のイネーブル化。
ユーザの作成に関する注意事項	5.0(1a)	注意事項が変更されました。