CHAPTER 39

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、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。

この章は、次の項で構成されています。

- 「ロール ベースの許可」（P.39-1）
- 「ロールの配信」（P.39-7）
- 「ユーザ アカウント」（P.39-10）
- 「SSH サービス」（P.39-14）
- 「管理者パスワードの回復」（P.39-19）
- 「Cisco ACS サーバの設定」（P.39-20）
- 「デフォルト設定」（P.39-23）

ロール ベースの許可

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。

ユーザがコマンドの実行、コマンドの完了、またはコンテキスト ヘルプの取得を行った場合、ユーザにそのコマンドへのアクセス権があると、スイッチ ソフトウェアによって処理の続行が許可されます。

この項では、次のトピックについて取り上げます。

- 「ロールの概要」（P.39-2）
- 「ロールとプロファイルの設定」（P.39-2）
- 「共通ロールの削除」（P.39-3）
- 「VSAN ポリシーの概要」（P.39-3）
- 「VSAN ポリシーの変更」（P.39-4）
- 「各ロールに対するルールと機能の概要」（P.39-4）
- 「ルールの修正」（P.39-5）
- 「ロールベース情報の表示」（P.39-7）

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。

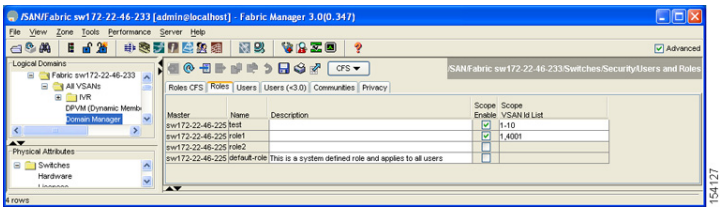
ロールとプロファイルの設定

Fabric Manager 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。[Information] ペインで [Roles] タブをクリックします。

図 39-1 の情報が表示されます。

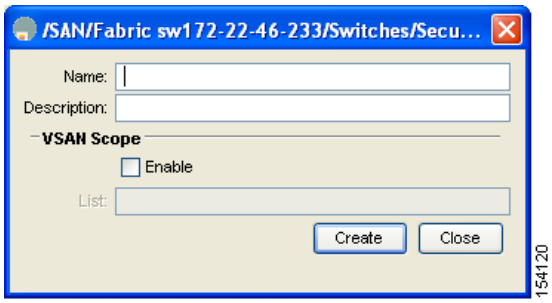
図 39-1　[Users and Roles] 画面の [Roles] タブ



ステップ 2　Fabric Manager でロールを作成するために [Create Row] アイコンをクリックします。

ロール作成のダイアログボックスが表示されます（図 39-2 を参照）。

図 39-2　ロール作成のダイアログボックス



ステップ 3　ロールの設定先のスイッチを選択します。

ステップ 4　[Name] フィールドに、ロールの名前を入力します。

ステップ 5　[Description] フィールドにロールの説明を入力します。

ステップ 6　任意で、[Enable] チェックボックスをオンにして VSAN 範囲をイネーブルにし、このロールを制限する VSAN のリストを [Scope] フィールドに入力します。

ステップ 7　ロールを作成するには、[Create] ボタンをクリックします。共通ロールを作成せずに [Roles - Create] ダイアログボックスを閉じるには、[Close] ボタンをクリックします。

（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

Fabric Manager 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。[Information] ペインで [Roles] タブをクリックします。

ステップ 2　削除するロールをクリックします。

ステップ 3　[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 4　[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。

VSAN ポリシーの概要

VSAN ポリシーを設定するには、ENTERPRISE_PKG ライセンスが必要です（第 10 章「ライセンスの入手とインストール」を参照）。

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。

VSAN ポリシーの変更

Fabric Manager 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。[Information] ペインで [Roles] タブをクリックします。

ステップ 2　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 3　[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 4　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。

各ロールに対するルールと機能の概要

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。ルールが適用される順序は、ユーザ指定のルール番号で決まります。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入らない、EXEC モード内のすべてのコマンドが対象になります。

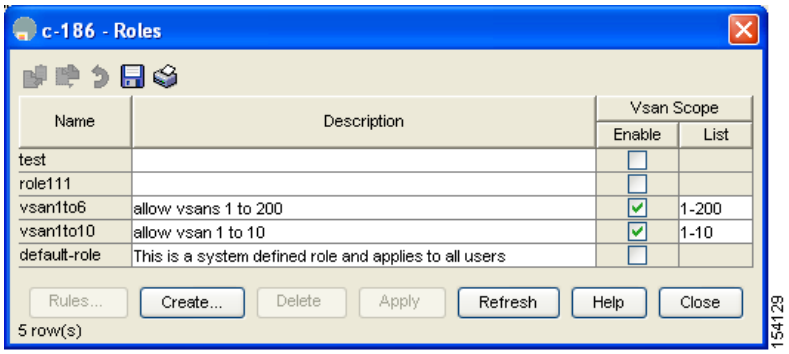
ルールの修正

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] をクリックします。

ステップ 2　[Common Roles] ダイアログボックスが表示されます（図 39-3 を参照）。

図 39-3　Device Manager の [Common Roles] ダイアログボックス

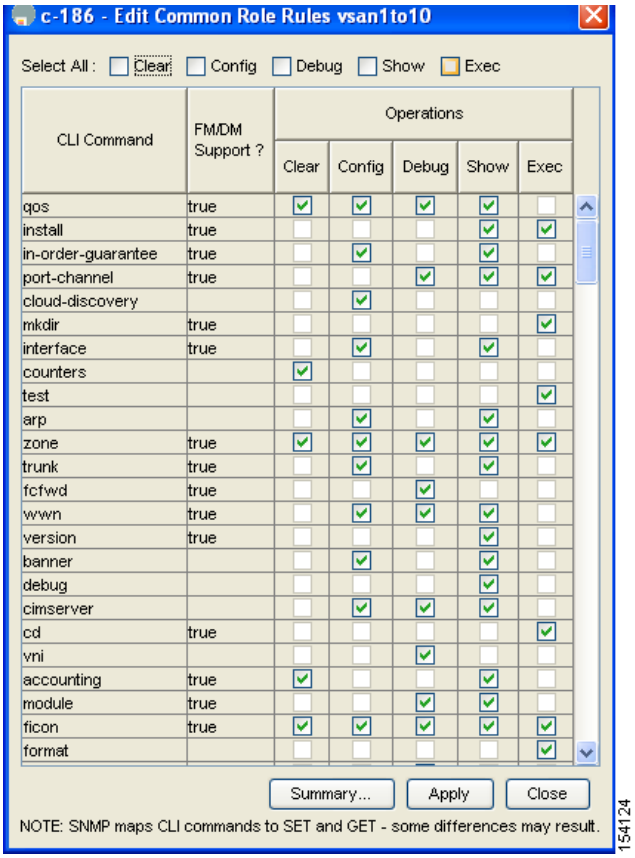


ステップ 3　ルールを編集するロールをクリックします。

ステップ 4　[Rules] をクリックして、そのロールのルールを表示します。

[Rules] ダイアログボックスが表示されます（図 39-4 を参照）。表示されるまでに数分かかる場合があります。

図 39-4　[Edit Common Role Rules] ダイアログボックス



ステップ 5　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 6　新しいルールを適用して [Rules] ダイアログボックスを閉じるには [Apply] をクリックします。ルールを適用しないで [Rules] ダイアログボックスを閉じるには [Close] をクリックします。

ルール 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。

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。

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（第 13 章「CFS インフラストラクチャの使用」を参照）。

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

この項では、次のトピックについて取り上げます。

- 「ロール データベースの概要」（P.39-7）
- 「ファブリックのロック」（P.39-8）
- 「変更のコミット」（P.39-8）
- 「変更の廃棄」（P.39-9）
- 「配信のイネーブル化」（P.39-9）
- 「セッションの消去」（P.39-9）
- 「データベース マージの注意事項」（P.39-10）
- 「配信がイネーブルの場合のロールの表示」（P.39-10）

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。

変更のコミット

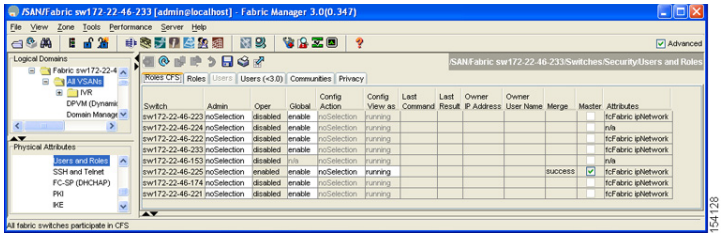
保留中のデータベースに行われた変更をコミットすると、その設定はそのファブリック内のすべてのスイッチにコミットされます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。コンフィギュレーション データベースはこれ以降、コミットされた変更を保持し、保留中のデータベースは消去されます。

Fabric Manager 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。[Information] ペインで [Roles CFS] タブをクリックします。

図 39-5 に示す画面が表示されます。

図 39-5　[Roles CFS] タブ



ステップ 2　[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 3　[Apply Changes] をクリックして、この変更を保存します。

ステップ 4　[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 5　[Apply Changes] をクリックして、この変更を保存します。

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。

Fabric Manager 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。[Information] ペインで [Roles CFS] タブをクリックします。

ステップ 2　[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 3　[Apply Changes] をクリックして、この変更を保存します。

配信のイネーブル化

Fabric Manager 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。[Information] ペインで [Roles CFS] タブをクリックします。

ステップ 2　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 3　[Apply Changes] をクリックして、この変更を保存します。

セッションの消去

Fabric Manager 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。[Information] ペインで [Roles CFS] タブをクリックします。

ステップ 2　[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 3　[Apply Changes] をクリックして、この変更を保存します。

（注）　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。

データベース マージの注意事項

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、「CFS マージのサポート」（P.13-9）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。

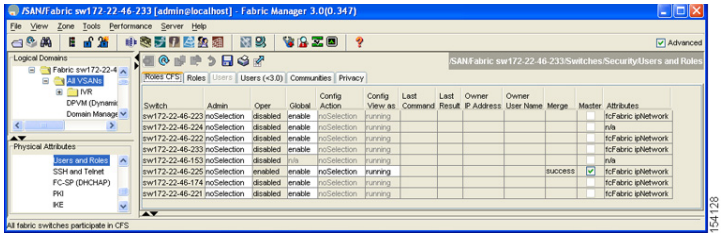
配信がイネーブルの場合のロールの表示

ロールの配信をイネーブルにすると、保留中のロール データベース（配信される前のデータベース）または実行中のデータベースのいずれも表示できます。

Fabric Manager 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。[Information] ペインで [Roles CFS] タブをクリックします（図 39-6 を参照）。

図 39-6　[Roles CFS] タブ



ステップ 2　[View Config 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、[View Config 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 3　[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

Cisco MDS 9000 ファミリ スイッチでは、すべてのユーザのアカウント情報がシステムに保管されます。ユーザの認証情報、ユーザ名、ユーザ パスワード、パスワードの有効期限、およびロール メンバーシップが、そのユーザのユーザ プロファイルに保存されます。

ここで説明するタスクを利用すると、ユーザの作成および既存ユーザのプロファイルの修正を実行できます。これらのタスクは管理者によって定義されている特権ユーザに制限されます。

パスワードには、次のような強力な特徴が備えられている必要があります。

- 最低 8 文字の長さ
- 連続した文字が多数続かない（「abcd」など）
- 同じ文字が多数繰り返さない（「aaabbb」など）
- 辞書にある単語を含まない
- 大文字小文字を混ぜる
- 数値を混ぜる

強力なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

（注） クリア テキストのパスワードには、アルファベットと数字だけを含めることができます。ドル記号（$）またはパーセント記号（%）などの特殊記号は使用できません。

この項では、次のトピックについて取り上げます。

- 「ユーザの概要」（P.39-11）
- 「ユーザの設定」（P.39-12）
- 「ユーザの削除」（P.39-14）
- 「ユーザ アカウント情報の表示」（P.39-14）

ユーザの概要

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（「SNMPv3 CLI のユーザ管理および AAA の統合」（P.40-3）を参照）。

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。

ヒント 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。

（注） 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。

ヒント 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　TACACS+、RADIUS、またはローカルのいずれで作成されたものであっても、Cisco MDS SAN-OS はすべてが数字のユーザ名はサポートしません。すべて数字の名前を持つローカル ユーザは作成できません。AAA サーバに数字だけのユーザ名が存在する場合、ログイン時に入力しても、そのユーザはログインできません。

ユーザの設定

Fabric Manager 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。[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（図 39-7 を参照）。

図 39-7　[Users] タブに表示されるユーザ リスト

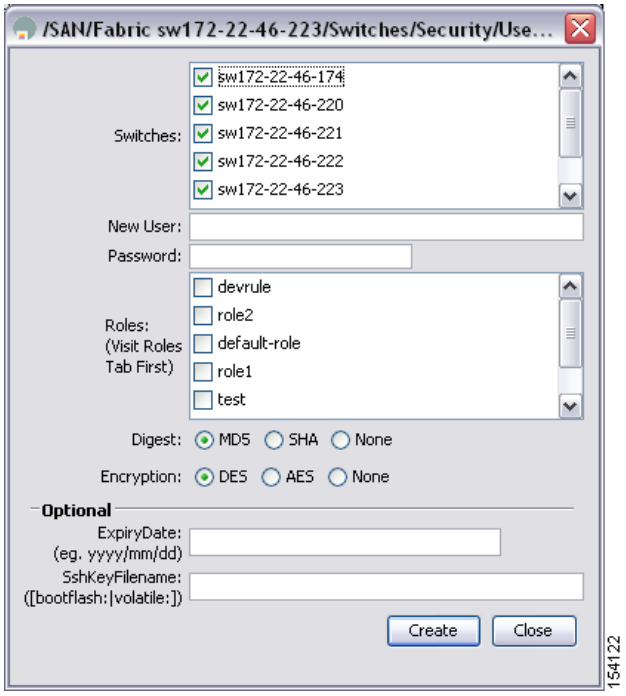
Switch	User	Primary Role	Other Role	Digest	Encryption
sw172-22-46-182	admin	network-admin		MD5	NoPriv
sw172-22-46-224	abcd	network-operator	network-admin	MD5	DES
sw172-22-46-153	admin	network-admin		MD5	NoPriv
sw172-22-46-182	md5usr	network-operator		MD5	DES
sw172-22-46-224	admin	network-admin		MD5	DES
sw172-22-46-224	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	md5usr	network-admin		MD5	DES
sw172-22-46-153	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	mchinn1	network-operator	network-admin	MD5	NoPriv
sw172-22-46-224	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	md5usr	network-admin		MD5	DES
sw172-22-46-153	junknew	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn1	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn5	network-operator	network-admin	MD5	NoPriv
sw172-22-46-153	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	testUser	network-operator	test	MD5	DES

154126

ステップ 2　[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 39-8 を参照）。

図 39-8　[Create Users] ダイアログボックス



ステップ 3　任意で、1 つまたは複数のスイッチを示すように [Switches] チェックボックスを変更します。

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、新しいロール名をフィールドに入力できます。この場合には、前の手順に戻ってこのロールを適切に設定します（「ユーザ アカウント」（P.39-10）を参照）。

ステップ 6　[New Password] および [Confirm Password] フィールドにユーザのパスワードを入力します。[New Password] フィールドと [Confirm Password] フィールドには同じ新規パスワードを入力します。

ステップ 7　[Privacy] チェックボックスをオンにし、パスワード フィールドへの入力を完了して、管理トラフィックを暗号化します。

ステップ 8　エントリを作成するには [Create] をクリックします。保存されていない変更を廃棄してダイアログボックスを閉じるには [Close] をクリックします。

ユーザの削除

Fabric Manager 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。[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 2　削除するユーザの名前をクリックします。

ステップ 3　[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 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

Fabric Manager 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 39-9 に示す SNMP ユーザのリストが [Information] ペインに表示されます。

図 39-9　[Users] タブに表示されるユーザ リスト

Switch	User	Primary Role	Other Role	Digest	Encryption
sw172-22-46-182	admin	network-admin		MD5	NoPriv
sw172-22-46-224	abcd	network-operator	network-admin	MD5	DES
sw172-22-46-153	admin	network-admin		MD5	NoPriv
sw172-22-46-182	md5usr	network-operator		MD5	DES
sw172-22-46-224	admin	network-admin		MD5	DES
sw172-22-46-224	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	md5usr	network-admin		MD5	DES
sw172-22-46-153	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	mchinn1	network-operator	network-admin	MD5	NoPriv
sw172-22-46-224	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	md5usr	network-admin		MD5	DES
sw172-22-46-153	junknew	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn1	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn5	network-operator	network-admin	MD5	NoPriv
sw172-22-46-153	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	testUser	network-operator	test	MD5	DES

154126

SSH サービス

Cisco MDS 9000 ファミリのすべてのスイッチで、Telnet サービスはデフォルトでイネーブルです。SSH サービスをイネーブルにする場合は、事前にサーバ キー ペアを生成してください（「SSH サーバ キー ペアの生成」（P.39-16）を参照）。

この項では、次のトピックについて取り上げます。

- 「SSH の概要」（P.39-15）

- 「SSH サーバ キー ペアの概要」（P.39-15）
- 「SSH サーバ キー ペアの生成」（P.39-16）
- 「生成したキー ペアの上書き」（P.39-17）
- 「SSH または Telnet サービスのイネーブル化」（P.39-17）
- 「SSH または Telnet サービスのイネーブル化」（P.39-17）
- 「デジタル証明書を使用した SSH 認証」（P.39-18）

SSH の概要

SSH は Cisco SAN-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。

- SSH1
- RSA を使用する SSH2
- DSA を使用する SSH2

SSH サーバ キー ペアの概要

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバ キー ペアを取得してください。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 サービスでは、SSH バージョン 1 と 2 で使用される 3 種類のキー ペアが受け入れられます。

- **rsa1** オプションを使用すると、SSH バージョン 1 プロトコルに対応する RSA1 キー ペアが生成されます。
- **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。

SSH サーバ キー ペアの生成

SSH サーバ 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。

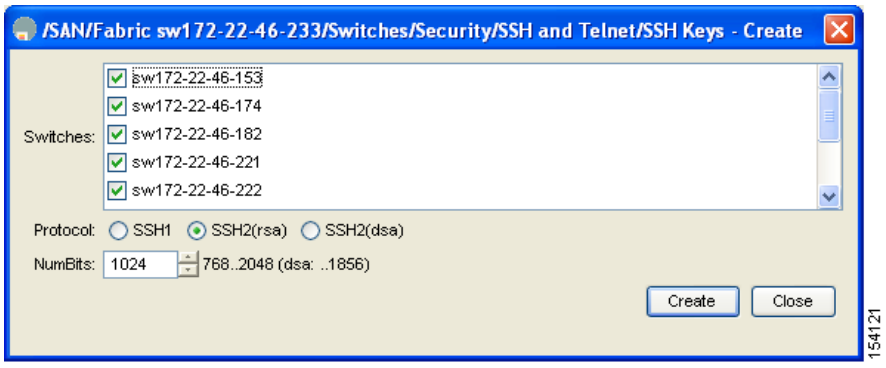
図 39-10 に示す設定が [Information] ペインに表示されます。

図 39-10　SSH および Telnet の設定

ステップ 2　[Create Row] をクリックします。

SSH および Telnet キー作成のダイアログボックスが表示されます（図 39-11 を参照）。

図 39-11　SSH および Telnet キー作成の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　これらのキーを生成するには [Create] をクリックします。変更を保存しないで終了するには [Close] をクリックします。

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。

Fabric Manager 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　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。

ステップ 4　[Create Row] をクリックします。

[SSH and Telnet Key Create] 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　これらのキーを生成するには [Create] をクリックします。変更を保存しないで終了するには [Close] をクリックします。

SSH または Telnet サービスのイネーブル化

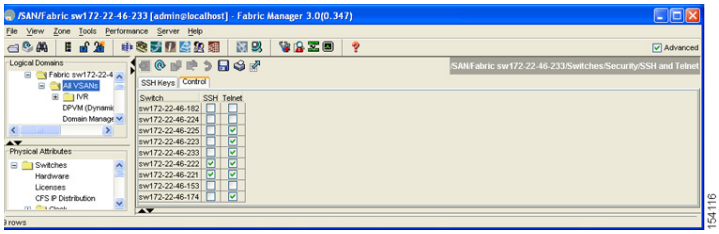
デフォルトでは、SSH サービスはディセーブルです。SSH を設定すると、Fabric Manager によって SSH が自動的にイネーブルになります。

Fabric Manager 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 39-12 を参照）。

図 39-12　[SSH and Telnet] の [Control] タブ



ステップ 3　こ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。

（注）　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 CLI** 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。

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 43 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。

ユーザの作成または更新

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。

ヒント　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。

（注）　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。

ヒント　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　TACACS+、RADIUS、またはローカルのいずれで作成されたものであっても、Cisco MDS SAN-OS はすべてが数字のユーザ名はサポートしません。すべて数字の名前を持つローカル ユーザは作成できません。すべてが数字のユーザ名が AAA サーバに存在し、ログインの際に入力されても、そのユーザはログインされません。

ヒント　トラブルシューティングのために **internal** キーワードを指定してコマンドを発行するには、network-admin グループのメンバーであるアカウントが必要です。

（注）　他のユーザの権限を変更できるのは、network-admin ユーザだけです。

Fabric Manager 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。[Information] ペインで [Users] タブをクリックして、ユーザ情報を表示します。

ステップ 2　ユーザを作成するには [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 3　このユーザにアクセスを許可するスイッチを選択します。

ステップ 4　新しいユーザ名およびパスワードを割り当てます。

（注）　ユーザ アカウント名には、数値以外の文字を含める必要があります。

ステップ 5　この新規ユーザに割り当てるロールを選択します。

ステップ 6　作成または更新しているユーザのダイジェストおよび暗号化を選択します。

ステップ 7　任意で、有効期限およびユーザの SSH ファイル名を入力します。

ステップ 8　ユーザを作成するには [Create] をクリックします。変更を廃棄するには [Close] をクリックします。

管理者パスワードの回復

次の 2 通りの方法のいずれかで管理者パスワードを回復できます。

- network-admin 権限を持つユーザ名による CLI の使用
- スイッチの電源再投入

（注）　管理者パスワードを回復する手順は、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

Cisco ACS サーバの設定

Cisco Access Control Server（ACS）は TACACS+ と RADIUS のプロトコルを利用して、セキュアな環境を作り出す AAA サービスを提供します。AAA サーバを使用する際のユーザ管理は、通常 Cisco ACS を使用して行われます。図 39-13、図 39-14、図 39-15、および図 39-16 に、TACACS+ または RADIUS を利用した ACS サーバの network-admin ロールおよび複数ロールのユーザ セットアップ設定を示します。

注意　TACACS+、RADIUS、またはローカルのいずれで作成されたものであっても、Cisco MDS SAN-OS はすべてが数字のユーザ名はサポートしません。すべて数字の名前を持つローカル ユーザは作成できません。AAA サーバに数字だけのユーザ名が存在する場合、ログイン時に入力しても、そのユーザはログインできません。

（注）　cisco-av-pair で指定されている各ロールが MDS に存在している必要があります。存在していない場合、ユーザに「network-operator」ロールが割り当てられます。

図 39-13　RADIUS を使用する場合の network-admin ロールの設定

図 39-14　RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定

図 39-15　TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定

図 39-16　TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定

デフォルト設定

表 39-1 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 39-1　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	ネットワーク管理者（network-operator）
AAA 設定サービス	Local
認証ポート	1821
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

表 39-1　スイッチ セキュリティのデフォルト設定 （続き）

パラメータ	デフォルト
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（設定しない場合）
Password	なし
アカウンティング ログ サイズ	250 KB
SSH サービス	ディセーブル
Telnet サービス	イネーブル