ユーザ アカウントおよび RBAC の設定

この章では、Cisco MDS 9000 デバイス上でユーザー アカウントおよびロールベース アクセス コントロール（RBAC）を構成する手順について説明します。

この章は、次の項で構成されています。

- ユーザー アカウントおよび RBAC の概要, on page 1
- ロール ベースの認証, on page 6
- ロールの配信, on page 14
- 共通ロールの設定, on page 20
- デフォルト設定, on page 22

ユーザー アカウントおよび RBAC の概要

ユーザー アカウントの作成および管理を行い、Cisco MDS 9000 デバイス上で実行できる操作を制限するロールを割り当てることができます。ロールベースアクセスコントロール（RBAC）を使用すると、割り当てたロールにルールを定義して、ユーザが行える管理操作の権限を制限できます。

ユーザーの認証情報、ユーザー名、ユーザーパスワード、パスワードの有効期限、およびロール メンバーシップが、そのユーザーのユーザー 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、ユーザーの作成および既存ユーザー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ーに制限されます。

ユーザ アカウント

最大256のユーザアカウントを作成できます。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。

ユーザーを作成する際、次の点に注意してください。

- 次の単語は予約済みのため、ユーザー設定には使用できません：bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、rpc、rpcuser、xfs、gdm、mtsuser、ftpuser、man、および sys。
- ユーザー 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。
- **snmp-server user**コマンドで指定したパスフレーズと、パスワード仕様**username** コマンドが同期します。
- デフォルトでは、明示的に期限を指定しないかぎり、ユーザー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、ユーザー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。
- 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。
- 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。

⚠

Caution Cisco MDS NX-OS では、ユーザ名が英数字で始まる限り、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ー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ー名が AAA サーバーに存在し、ログイン時に入力されると、そのユーザー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
- 正しい名前を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

強力なパスワードの例を次に示します。

- If2CoM18

- 2004AsdfLkj30
- Cb1955S21

パスワードの強度確認をイネーブルにすると、パスワードが単純である場合（短く、簡単に解読されるパスワードなど）に、Cisco MDS NX-OS ソフトウェアによってパスワード設定が拒否されます。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。パスワードは大文字と小文字が区別されます。

パスワードを生成するための上記のルールは、TACACS+、RADIUS、LDAP などの AAA サーバーを介したリモート ユーザー認証に適用できます。

パスワード強度の確認

ユーザアカウントに対して弱いパスワードを設定しないように、パスワードの強度確認機能をイネーブルにすることができます。

Note パスワード確認をイネーブル化にしても、既存パスワードの強度確認は行われません。

パスワードの強度の確認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**

構成モードに入ります。

ステップ 2 switch(config)# **password strength-check**

パスワードの強度確認をイネーブルにします。デフォルトではイネーブルになっています。

パスワードの強度確認をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 3 switch(config)# **exit**

（任意）グローバル コンフィギュレーション モードを終了します。

ステップ 4 switch(config)# **show password strength-check**

（任意）パスワードの強度確認の設定を表示します。

ステップ 5 switch(config)# **copy running-config startup-config**

（任意）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。

ユーザーの設定

新規ユーザーの設定または既存ユーザーのプロファイル修正を行うには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **username usam password abcd123AAA expire 2003-05-31**

ユーザー アカウント（usam）を作成または更新し、パスワード（abcd123AAA）および有効期限 2003-05-31 を設定します。

ステップ 3 switch(config)# **username msam password 0 abcd12AAA role network-operator**

ユーザー アカウント（msam）を作成または更新し、クリア テキスト（0 で示される）のパスワード（abcd12AAA）を指定します。パスワードの長さは 64 文字に制限されています。

ステップ 4 switch(config)# **username user1 password 5 1UgOR6Xqb$z.HZlMk.ZGr9VH67a**

ユーザー アカウント（user1）に暗号化（5 で指定される）パスワード（!@*asdsfsdfjh!@df）を指定します。

Note
ユーザーが暗号化パスワード オプションを指定して作成された場合、対応する SNMP ユーザーは作成されません。

ステップ 5 switch(config)# **username usam role network-admin**

network-admin ロールに指定のユーザー（usam）を追加します。

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

（オプション）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)# **username admin sshkey ssh-rsa**
AAAB[illegible]

既存のユーザー アカウント（admin）の SSH キーを指定します。

ステップ 8 switch(config)# **no username admin sshkey ssh-rsa**
AAAB[illegible]

（オプション）ユーザー アカウント（admin）の SSH キーを削除します。

ステップ 9 switch(config)# **username usam ssh-cert-dn usam-dn dsa**

既存のユーザー アカウント（usam）の認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。

ステップ 10 switch(config)# **username user1 ssh-cert-dn user1-dn rsa**

既存のユーザー アカウント（user1）の認証に使用する SSH X.509 証明書の識別名と RSA アルゴリズムを指定します。

ステップ 11 switch(config)# **no username admin ssh-cert-dn admin-dn dsa**

ユーザー アカウント（admin）の SSH X.509 証明書の識別名を削除します。

ユーザーのログアウト

スイッチの他のユーザーをログアウトするには、**clear user** コマンドを使用します。

次の例では、vsam という名前のユーザーが、スイッチからログアウトされます。

```
switch# clear user vsam
```

ログインしているすべてのユーザーの表示

ログインしているユーザーのリストを表示するには、**show users** コマンドを使用します（次の例を参照）。

```
switch# show users

admin    pts/7        Jan 12 20:56 (10.77.202.149)
admin    pts/9        Jan 12 23:29 (user.example.com)
admin    pts/10       Jan 13 03:05 (dhcp-10-10-1-1.example.com)
admin    pts/11       Jan 13 01:53 (dhcp-10-10-2-2.example.com)
```

ユーザー アカウント情報の表示

指定したユーザーに関する情報の表示

ユーザー アカウントに関して設定されている情報を表示するには、**show user-account** コマンドを使用します。次の例を参照してください。

```
switch# show user-account user1

user:user1
        this user account has no expiry date
        roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS is possible
```

すべてのユーザーに関する情報の表示

```
switch# show user-account
show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:usam
```

```
        expires on Sat May 31 00:00:00 2003
        roles:network-admin network-operator
user:msam
        this user account has no expiry date
        roles:network-operator
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. local login not allowed
Remote login through RADIUS is possible
```

ロール ベースの認証

ユーザー アカウントの作成および管理を行い、Cisco MDS 9000 デバイス上で実行できる操作を制限するロールを割り当てることができます。ロールベース アクセス コントロール（RBAC）を使用すると、割り当てたロールにルールを定義して、ユーザが行える管理操作の権限を制限できます。

ユーザーがコマンドの実行、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、ユーザーにそのコマンドへのアクセス権がある場合のみ、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。

ユーザ ロール

ユーザー ロールには、そのロールを割り当てられたユーザーが実行できる操作を定義するルールが含まれています。各ユーザー ロールに複数のルールを含めることができ、各ユーザーが複数のロールを持つことができます。たとえば、ロール1ユーザーには構成 コマンドへのアクセスだけが、ロール2ユーザーにはデバッグ 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、ロール1 と ロール2 の両方に所属しているユーザーは、構成 コマンドとデバッグ コマンドにアクセスできます。

Note ユーザー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ーが、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、このユーザー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、このユーザー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。

Cisco NX-OS ソフトウェアには、デフォルトで次のユーザー ロールが用意されています。

- network-admin： Cisco NX-OS デバイス全体への完全な読み取り/書き込みアクセス権ただし、このロールには他のユーザーのプロファイルを変更する権限は含まれません。他のユーザーのプロファイルを変更するには、ユーザー管理に関する特定の権限を持つ別のロールが必要です。

- network-operator：少数の show sub コマンドを除く、Cisco NX-OS デバイス全体への完全な読み取りアクセス権
- server-admin：Cisco NX-OS デバイス全体およびアップグレード機能への完全な読み取りアクセス。

network-operator がアクセスできない特権 show sub コマンドの例を次に示します：

- アカウンティング：`show accounting configuration`
- 起動：`show bootvar Variables`
- 整合性チェッカー：`consistency checker`
- data-corruption：`display data inconsistency errors`
- eemtest： `EEM test publisher commands`
- fcdroplatency：`show switch or network latency`
- hosts：`show information about DNS`
- line：`show the line configuration`
- locked-users：`all locked users`
- port-group-monitor：`show port-group-monitor information`
- port-monitor：`show port-monitor information`
- pss：`display pss information`
- radius-cfs：`show radius cfs state`
- 実行構成：`show running system information`
- セキュリティ: `show security information`
- startup-config：`show startup system information`
- トランク：`show trunk information`

Tip 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。

ロールの設定

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には、次の手順を実行します。

Note network-admin ロールに属するユーザーだけがロールを作成できます。

Procedure

ステップ 1 switch# **config terminal**

構成モードに入ります。

ステップ 2 switch(config)# **role name techdocs**
switch(config-role)#

指定したロール サブ モードを開始します。

ステップ 3 switch(config)# **no role name techdocs**

（オプション）ロール techdocs を削除します。

ステップ 4 switch(config-role)# **description Entire Tech Docs group**

新しいロールに記述を割り当てます。記述は1行に制限され、スペースを含めることができます。

ステップ 5 switch(config-role)# **no description**

（オプション）Tech Docs グループの記述をリセットします。

カスタム ロールによるロール変更の構成

Cisco MDS NX-OS リリース 8.3（1）から、ユーザーが他のユーザーのアカウント（ロールまたはパスワード）を変更できる「管理者」ユーザーに相当するカスタム ロールを作成できます。ロールを「admin」ユーザーと同等になるように変更するには、ロールで**attribute-admin[ルール（rule）]**を構成します。

Note

- **attribute-admin**[ルール（rule）]は、既存のルールと相互に排他的です。既存のルールを削除して、新しい**attribute-admin** ルールを構成します。
- サポートされていないソフトウェア イメージがファブリックに存在する場合、**attribute-admin** コマンドの設定中にロール配布機能が機能不全になることはありません。代わりに、それは受け入れられ、サポートされていないルールの無効なルールとして表示されます。
- サポートされていないソフトウェアイメージがファブリックに存在する場合、相互に排他的な構成のロール配布機能は機能不全にしません。
- **attribute-admin** 特権を持つユーザーは、Dplug のロードが機能しません。
- **attribute-admin** 特権を持つユーザーの場合、 の下の**show system internal kernel memory global detail**コマンド出力は **show tech-support details** 機能不全にします。

カスタム ロールを作成または、既存ロールのプロファイルを変更するには、次の手順を実行します。

Procedure

ステップ 1 switch# **config terminal**

構成モードに入ります。

ステップ 2 switch(config)# **role name techdocs**
switch(config-role)#

指定したロール サブ モードを開始します。

ステップ 3 switch(config)# **no role name techdocs**

（オプション）ロール techdocs を削除します。

ステップ 4 switch(config-role)# **rule** *rule-number* **attribute-admin**

新しいロールに権限を割り当てます。

ステップ 5 switch(config-role)# **no rule 1 attribute-admin**

(オプション) ロールに割り当てられている管理者権限を削除します。

ステップ 6 switch# **showuser-account** *user-name*

（任意）ユーザ アカウントの構成した情報を表示します。

ユーザ ロールとルール

ロールごとに最大 16 のルールを設定できます。ユーザ ロールを複数のユーザ アカウントに割り当てることができます。

ルールが適用される順序は、ユーザー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ーは、ロールに関連したコマンドを実行できません。

Note ユーザー ロールに設定された **read-write** ルールに関係なく、一部のコマンドは、あらかじめ定義された network-admin ロールでのみ実行できます。

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

rule コマンドでは特定のロールで実行できる動作を指定します。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）、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。

Note 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。

デフォルトのロールがすべてのユーザーに適用でき、設定済みロールが特定のユーザーに適用できる場合、次のシナリオについて検討します。

- 同じルール タイプ（許可または拒否）：デフォルト ロールと特定のユーザーに設定されているロールで同じルール タイプを使用する場合、特定のユーザーはデフォルトと設定済みの両方のロールのすべてのルールにアクセスできます。

Note 全て拒否するステートメントはルール 0 と見なされるため、明示的に許可されない限り、ユーザー ロールに対するアクションは実行できません。

デフォルト ロール A の場合、次のルールがあります。

```
rule 5 permit show feature environment
rule 4 permit show feature hardware
rule 3 permit config feature ssh
rule 2 permit config feature ntp
rule 1 permit config feature tacacs+
```

特定のユーザーにはロール B が割り当てられ、ルールは 1 つあります。

```
rule 1 permit config feature dpvm
```

特定のユーザーは、A と B の両方のルールにアクセスできます。

- 異なるルール タイプ：デフォルト ロールと特定のユーザーに設定されているロールで特定のルールのルール タイプが異なる場合、デフォルト ロールによって設定済みロールの競合するルール ステートメントが上書きされます。

  デフォルト ロール A の場合、次のルールがあります。

```
rule 5 permit show feature environment
rule 4 permit show feature hardware
rule 3 permit config feature ssh
rule 2 permit config feature ntp
rule 1 permit config feature tacacs+
```

  特定のユーザーにはロール B が割り当てられ、ルールは 2 つあります。

```
rule 6 permit config feature dpvm
rule 2 deny config feature ntp
```

  A と B のルール 2 が競合します。この場合、A は B の競合するルールを上書きし、ユーザーには、上書きルールを含む、A と B の残りのルールが割り当てられます。

```
rule 6 permit config feature dpvm
rule 5 permit show feature environment
rule 4 permit show feature hardware
rule 3 permit config feature ssh
rule 2 permit config feature ntp ------------> Overridden rule
rule 1 permit config feature tacacs+
```

プロファイルの変更

既存ロールのプロファイルを変更するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **role name sangroup**

switch(config-role)#

既存のロール sangroup のロール コンフィギュレーション サブモードを開始します。

ステップ 3 switch(config-role)# **rule 1 permit config**

switch(config-role)# **rule 2 deny config feature fspf**

switch(config-role)# **rule 3 permit debug feature zone**

switch(config-role)# **rule 4 permit exec feature fcping**

sangroup ロールに属すユーザーが、**spf config** コマンドを除くすべてのコンフィギュレーション コマンドを実行できるようにします。これらのユーザーは、**zone debug** コマンドおよび **fcping** EXEC モード コマンドも実行できます。

ステップ 4 switch(config-role)# **no rule 4**

ルール 4 を削除し、sangroup が **fcping** コマンドを実行できないようにします。

Example

ステップ 3 で、ルール 1 が最初に適用され、sangroup ユーザーがすべての **config** 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 ユーザーには FSPF 設定が拒否されます。結果として、sangroup ユーザーは **fspf** 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** コマンドを実行できます。

VSAN ポリシーの設定

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。

Note 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）。

Note 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ーは、E ポートの設定を変更できません。これらのユーザーが変更できるのは、（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、これらのユーザーは、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。

Tip 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ーのことを、VSAN 制限付きユーザーと呼びます。

VSAN ポリシーの変更

既存ロールの VSAN ポリシーを変更するには、次の手順を実行します。

Note

- VSAN の適用は、非 show コマンドに対してのみ実行されます。show コマンドは除外されます。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **role name sangroup**

switch(config-role)#

sangroup ロールのロール コンフィギュレーション サブモードを開始します。

ステップ 3 switch(config)# **vsan policy deny**

switch(config-role-vsan)#

このロールの VSAN ポリシーを **deny** に変更し、VSAN を選択的に許可できるサブモードを開始します。

ステップ 4 switch(config-role)# **no vsan policy deny**

（オプション）設定されている VSAN ロール ポリシーを削除し、工場出荷時のデフォルト（**permit**）に戻します。

ステップ 5 switch(config-role-vsan)# **permit vsan 10-30**

このロールが、VSAN 10 ～ 30 に許可されたコマンドを実行できるようにします。

ステップ 6 switch(config-role-vsan)# **no permit vsan 15-20**

（オプション）このロールの権限を、VSAN 15 ～ 20 のコマンドの実行について除外します。したがって、このロールは、VSAN 10 ～ 14、および 21 ～ 30 でコマンドを実行できることになります。

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

このセクションは、次のトピックで構成されています。

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。

Note お客様に「syslog"%VSHD-4-VSHD_ROLE_DATABASE_OUT_OF_SYNC"」が発生するとすぐに、ロール コンフィギュレーション データベースがマージ時にスイッチ間で異なることが検出されます。ファブリック内のすべてのスイッチで、ロール コンフィギュレーション データベースを一致させることを推奨します。いずれかのスイッチで設定を編集し、目的のロール コンフィギュレーション データベースを取得してからコミットします。

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。

- 他のユーザー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。

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。

ロールベースの設定変更をコミットするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

構成モードに入ります。

ステップ 2 switch(config)# **role commit**

ロールベースの設定変更をコミットします。

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（終了）する場合、構成データベースは影響を受けないまま、ロックがリリースされます。

ロールベースの設定変更を廃棄するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

構成モードに入ります。

ステップ 2 switch(config)# **role abort**

ロールベースの設定変更を廃棄し、保留中のコンフィギュレーションデータベースをクリアします。

ロールベース設定の配布のイネーブル化

ロールベース設定の配信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**

switch(config)#

構成モードに入ります。

ステップ 2 switch(config)# **role distribute**

ロールベース設定の配信をイネーブルにします。

ステップ 3 switch(config)# **no role distribute**

（オプション）ロールベース設定の配信をディセーブル（デフォルト）にします。

セッションのクリア

ファブリック内の既存のロールセッションを強制的にクリアするには、開始されたセッションに参加中のスイッチから **clear role session** コマンドを発行します。

Caution このコマンドを発行すると、保留中のデータベース内のすべての変更が失われます。

switch# clear role session

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。

- 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。

ロールベース情報の表示

スイッチに設定されたルールを表示するには、**show role** コマンドを使用します。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。次の例を参照してください。

すべてのロールに関する情報の表示

```
switch# show role

Role: network-admin
  Description: Predefined Network Admin group. This role cannot be modified.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  clear           *
  2       permit  config          *
  3       permit  debug           *
  4       permit  exec            *
  5       permit  show            *
Role: network-operator
  Description: Predefined Network Operator group. This role cannot be modified.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            *(excluding show running-config, show startup-config)
  2       permit  exec            copy licenses
  3       permit  exec            dir
  4       permit  exec            ssh
  5       permit  exec            terminal
  6       permit  config          username
Role: server-admin
  Description: Predefined system role for server administrators. This role
  cannot be modified.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            *
  2       permit  exec            install
Role: priv-15
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            *
  2       permit  config          *
  3       permit  clear           *
  4       permit  debug           *
  5       permit  exec            *
Role: priv-14
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-13
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-12
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-11
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-10
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-9
  Description: This is a system defined privilege role.
```

```
  Vsan policy: permit (default)
Role: priv-8
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-7
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-6
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-5
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-4
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-3
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-2
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-1
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
Role: priv-0
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            *
  2       permit  exec            enable
  3       permit  exec            ssh
  4       permit  exec            ping
  5       permit  exec            telnet
  6       permit  exec            traceroute
Role: default-role
  Description: This is a system defined role and applies to all users.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            system
  2       permit  show            snmp
  3       permit  show            module
  4       permit  show            hardware
  5       permit  show            environment
```

配信がイネーブルの場合のロールの表示

コンフィギュレーション データベースを表示するには、**show role** コマンドを使用します。

配信がロール設定に対してイネーブルかどうか、現在のファブリック ステータス（ロックまたはロック解除）、および最後に実行された動作を表示するには、**show role status** コマンドを使用します。次の例を参照してください。

ロール ステータス情報の表示

```
switch# show role status
Distribution: Enabled
```

```
Session State: Locked
Last operation (initiated from this switch): Distribution enable
Last operation status: Success
```

保留中のロール データベースを表示するには、 **show role pending** コマンドを使用します。

下記の例は、次の手順に従って **show role pending** コマンドを実行した出力を示しています。

1. **role name myrole** コマンドを使用して myrole というロールを作成します。
2. **rule 1 permit config feature fspf** コマンドを入力します。
3. **show role pending** コマンドを入力して出力を確認します。

保留中のロール データベース情報の表示

```
switch# show role pending

Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands
Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands
Role: svc-admin
Description: Predefined SVC Admin group. This role cannot be modified
Access to all SAN Volume Controller commands
Role: svc-operator
Description: Predefined SVC Operator group. This role cannot be modified
Access to selected SAN Volume Controller commands
Role: TechDocs
  vsan policy: permit (default)
Role: sangroup
  Description: SAN management group
  vsan policy: deny
  Permitted vsans: 10-30
  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config                  *
    2.     deny    config               fspf
    3.   permit     debug               zone
    4.   permit      exec             fcping
Role: myrole
  vsan policy: permit (default)
  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config               fspf
```

保留中のロール データベースとコンフィギュレーションのロール データベースの相違を表示するには、**show role pending-diff** コマンドを使用します。次の例を参照してください。

2 つのデータベースの相違の表示

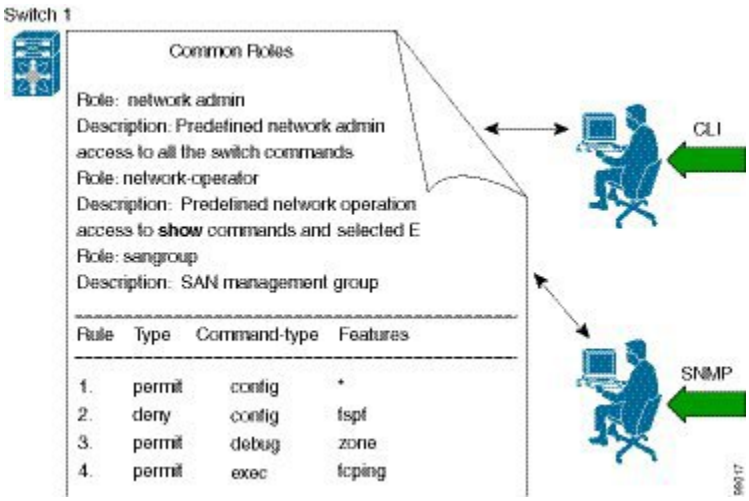
```
switch# show role pending-diff
    +Role: myrole
    +  vsan policy: permit (default)
    +  ----------------------------------------------
    +  Rule    Type    Command-type      Feature
    +  ----------------------------------------------
    +    1.   permit    config               fspf
```

共通ロールの設定

CLI と SNMP は、Cisco MDS 9000 シリーズ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ーは SNMP（たとえば、NDFC やデバイスマネージャ）を使用してスイッチにアクセスでき、その逆も可能です。

Figure 1: 共通ロール



ネットワーク管理者権限を持つカスタム ロール ユーザーは、他のユーザーのアカウントの変更が制限されています。ただし、管理者だけはすべてのユーザー アカウントを変更できます。

ユーザー権限を変更するには、次のタスクを実行します。

1. コンソール認証を使用してロールを変更します。

   コンソール認証を 'local' に設定している場合は、ローカル管理者ユーザーでログオンし、ユーザーを変更します。

2. リモート認証を使用してロールを変更します。

   リモート認証をオフにします。ローカル管理者権限でログオンし、ユーザーを変更します。リモート認証をオンにします。

3. LDAP/AAA を使用してロールを変更します。

   LDAP/AAA でグループを作成し、このグループの名前をネットワーク管理者に変更します。必要なユーザーをこのグループに追加します。このグループのユーザーに完全なネットワーク管理者権限が付与されました。

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 ベースの認証, on page 6 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。

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

次の表は、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。

***Table 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

次に、my_role という名前のロールの CLI オペレーションを SNMP オペレーションへマッピングする特権およびルールの例を示します。

CLI 操作から SNMP 操作へのマッピングの表示

```
switch# show role name my_role
Role:my_role
  vsan policy:permit (default)
  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit     clear                 *
    2.     deny     clear               ntp
    3.   permit    config                 *
    4.     deny    config               ntp
    5.   permit     debug                 *
    6.     deny     debug               ntp
    7.   permit      show                 *
```

```
8.     deny      show                  ntp
9.   permit      exec                    *
```

Note ルール 4 では、CONFIG は NTP では拒否されますが、ルール 9 によって、NTP MIB オブジェクトに対する SET は許可されます。これは、EXEC も SNMP SET 操作にマッピングされているためです。

デフォルト設定

次の表に、任意のスイッチにおける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。

Table 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	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 サーバー タイムアウト	1 秒
RADIUS サーバー再試行	1 回
TACACS+	ディセーブル
TACACS+ サーバー	未設定
TACACS+ サーバーのタイムアウト	5 秒
AAA サーバーへの配信	ディセーブル
ロールに対する VSAN ポリシー	Permit
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
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

パラメータ	デフォルト
SSH サービス	イネーブル
Telnet サービス	無効化

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。