



R コマンド

この章のコマンドは、Cisco MDS 9000 ファミリのマルチレイヤディレクタおよびファブリック スイッチに対応しています。ここでは、コマンドモードに関係なく、すべてのコマンドがアルファベット順に記載されています。各コマンドの適切なモードを確認するには、「コマンドモード」を参照してください。詳細については、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

radius abort

進行中の Remote Authentication Dial-In User Service (RADIUS) Cisco Fabric Services (CFS) 配信セッションを廃棄するには、コンフィギュレーション モードで **radius abort** コマンドを使用します。

radius abort

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンドモード コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、進行中の RADIUS CFS 配信セッションを廃棄する例を示します。

```
switch# config terminal
switch(config)# radius abort
```

関連コマンド	コマンド	説明
	radius distribute	RADIUS CFS 配信をイネーブルにします。
	show radius	RADIUS CFS 配信ステータスおよびその他の詳細を表示します。

radius commit

ファブリック内で進行中の Remote Authentication Dial-In User Service (RADIUS) Cisco Fabric Services (CFS) 配信セッションに関する未決定コンフィギュレーションを適用するには、コンフィギュレーションモードで **radius commit** コマンドを使用します。

radius commit

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、RADIUS コンフィギュレーションをファブリックのスイッチに適用する例を示します。

```
switch# config terminal  
switch(config)# radius commit
```

関連コマンド	コマンド	説明
	radius distribute	RADIUS CFS 配信をイネーブルにします。
	show radius	RADIUS CFS 配信ステータスおよびその他の詳細を表示します。

radius distribute

Remote Authentication Dial-In User Service (RADIUS) の Cisco Fabric Services (CFS) 配信をイネーブルにするには、**radius distribute** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

radius distribute

no radius distribute

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、RADIUS ファブリック配信をイネーブルにする例を示します。

```
switch# config terminal
switch(config)# radius distribute
```

関連コマンド	コマンド	説明
	radius commit	一時的な RADIUS コンフィギュレーション変更をアクティブ コンフィギュレーションに確定します。
	show radius	RADIUS CFS 配信ステータスおよびその他の詳細を表示します。

radius-server deadtime

応答性について、到達できない（応答しない）RADIUS サーバを定期的に監視するタイム インターバルを設定するには、**radius-server deadtime** コマンドを使用します。応答しない RADIUS サーバのモニタリングをディセーブルにするには、コマンドの **no** 形式を使用します。

radius-server deadtime time

no radius-server deadtime time

シンタックスの説明	<i>time</i>	時間間隔を分で指定します。有効範囲は 1 ～ 1440 です。
------------------	-------------	---------------------------------

デフォルト	ディセーブル
--------------	--------

コマンドモード	コンフィギュレーションモード
----------------	----------------

コマンド履歴	リリース	変更内容
	3.0(1)	このコマンドが導入されました。

使用上のガイドライン 時間間隔の設定をゼロにすると、タイマーがディセーブルになります。個々の RADIUS サーバのデッドタイム インターバルがゼロ（0）より大きい場合は、サーバグループに設定された値より、その値の方が優先されます。

デッドタイム インターバルが 0 分の場合、RADIUS サーバがサーバグループに属しており、そのグループのデッドタイム インターバルが 0 分より大きい値でないかぎり、RADIUS サーバモニタリングは実行されません。

例 次に、期間を 10 分に設定する例を示します。

```
switch# config terminal
switch(config)# radius-server deadtime 10
```

関連コマンド	コマンド	説明
	<code>deadtime</code>	応答のない RADIUS サーバを監視するタイム インターバルを設定します。
	<code>show radius-server</code>	設定されたすべての RADIUS サーバパラメータを表示します。

radius-server directed-request

ログイン時に認証要求を送信するよう RADIUS サーバを指定するには、**radius-server directed-request** コマンドを使用します。認証要求の送信を設定されたグループに戻すには、コマンドの **no** 形式を使用します。

radius-server directed-request

no radius-server directed-request

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	3.0(1)	このコマンドが導入されました。

使用上のガイドライン ログイン時、ユーザは `username@servername` を指定できます。ユーザ名が認証用にサーバ名に送信されます。

例 次に、ログイン時に認証要求を送信するよう RADIUS サーバを指定する例を示します。

```
switch# config terminal
switch(config)# radius-server directed-request
```

関連コマンド	コマンド	説明
	<code>show radius-server</code>	設定されたすべての RADIUS サーバ パラメータを表示します。
	<code>show radius-server directed request</code>	転送された要求 RADIUS サーバ設定を表示します。

radius-server host

Remote Authentication Dial-In User Service (RADIUS) サーバパラメータを設定するには、**radius-server host** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
radius-server host {server-name | ipv4-address | ipv6-address}
  [key [0 | 7] shared-secret] [accounting]
  [acct-port port-number] [auth-port port-number] [authentication] [retransmit count]
  [test {idle-time time | password password | username name}]
  [timeout seconds [retransmit count]]

no radius-server host {server-name | ipv4-address | ipv6-address}
  [key [0 | 7] shared-secret] [accounting]
  [acct-port port-number] [auth-port port-number] [authentication] [retransmit count]
  [test {idle-time time | password password | username name}]
  [timeout seconds [retransmit count]]
```

シンタックスの説明

<i>server-name</i>	RADIUS サーバの Domain Name System (DNS; ドメイン ネーム システム) 名を指定します。1 最大 256 文字まで可能です。
<i>ipv4-address</i>	フォーマット <i>A.B.C.D</i> で RADIUS サーバの IP アドレスを指定します。
<i>ipv6-address</i>	フォーマット <i>X::X::X</i> で RADIUS サーバの IP アドレスを指定します。
auth-port <i>port-number</i>	認証用の RADIUS サーバのポートを設定します。
acct-port <i>port-number</i>	アカウント用 RADIUS サーバのポートを設定します。
authentication	認証を設定します。
accounting	アカウントを設定します。
key	RADIUS サーバ共有秘密鍵を設定します。
0	RADIUS クライアントおよびサーバ間の通信を認証する、平文で指定された事前共有鍵 (0 で表示) を設定します。これがデフォルトです。
7	RADIUS クライアントおよびサーバ間の通信を認証する、暗号文で指定された事前共有鍵 (7 で表示) を設定します。
<i>shared-secret</i>	RADIUS クライアントおよびサーバ間の通信を認証する事前共有鍵を設定します。
retransmit <i>count</i>	スイッチがローカル認証に戻る前に RADIUS サーバ (複数可) への接続試行を行う回数を設定します。有効範囲は 1 ~ 5 回で、デフォルトは 1 回です。
test	RADIUS サーバにテストパケットを送信するようパラメータを設定します。
idle-time <i>time</i>	サーバをモニタリングするための時間間隔を分で指定します。時間の範囲は 1 ~ 1440 分です。
password <i>password</i>	テストパケット内のユーザパスワードを指定します。最大文字サイズは 32 です。
username <i>name</i>	テストパケット内のユーザ名を指定します。最大文字サイズは 32 です。
timeout <i>seconds</i>	RADIUS サーバへの再送信タイムアウト (秒単位) を設定します。デフォルトは 1 秒で、有効な範囲は 1 ~ 60 秒です。

デフォルト

アイドル時間は設定されません。サーバモニタリングはオフです。

Timeout は 1 秒です。

Username は test です。

Password は test です。

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。
	3.0(1)	<i>ipv6-address</i> 引数および test オプションが追加されました。

使用上のガイドライン アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

例 次に、RADIUS サーバ認証パラメータを設定する例を示します。

```
switch# config terminal
switch(config)# radius-server host 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003
switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

関連コマンド	コマンド	説明
	show radius-server	RADIUS サーバ情報を表示します。

radius-server key

グローバル RADIUS 共有秘密鍵を設定するには、**radius-server key** コマンドを使用します。設定した共有秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

```
radius-server key [0 | 7] shared-secret
```

```
no radius-server key [0 | 7] shared-secret
```

シンタックスの説明		
	0	RADIUS クライアントおよびサーバ間の通信を認証する、平文で指定された事前共有鍵 (0 で表示) を設定します。これがデフォルトです。
	7	RADIUS クライアントおよびサーバ間の通信を認証する、暗号文で指定された事前共有鍵 (7 で表示) を設定します。
	<i>shared-secret</i>	RADIUS クライアントおよびサーバ間の通信を認証する事前共有鍵を設定します。

デフォルト なし

コマンドモード コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン RADIUS 事前共有鍵を設定して、RADIUS サーバに対してスイッチを認証する必要があります。鍵の長さは 65 文字に制限されており、出力可能な ASCII 文字の使用が可能です (空白文字は使用できません)。グローバル鍵は、スイッチにあるすべての RADIUS サーバ コンフィギュレーションで使用するよう設定できます。**radius-server host** コマンドで **key** オプションを明示的に使用することで、このグローバル鍵の割り当てを上書きできます。

例 次に、RADIUS 認証を設定する各種のシナリオを提供する例を示します。

```
switch# config terminal
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public
```

関連コマンド	コマンド	説明
	show radius-server	RADIUS サーバ情報を表示します。

radius-server retransmit

スイッチが RADIUS サーバで要求を試行する回数をグローバルに指定するには、**radius-server retransmit** コマンドを使用します。デフォルト値に戻すには、コマンドの **no** 形式を使用します。

radius-server retransmit *count*

no radius-server retransmit *count*

シンタックスの説明	<i>count</i>	スイッチがローカル認証に戻る前に RADIUS サーバ（複数可）への接続試行を行う回数を設定します。有効値は 1～5 回です。
------------------	--------------	---

デフォルト	再送信 1 回
--------------	---------

コマンドモード	コンフィギュレーションモード
----------------	----------------

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン	なし
-------------------	----

例 次に、再送信回数を 3 回に設定する例を示します。

```
switch# config terminal
switch(config)# radius-server retransmit 3
```

関連コマンド	コマンド	説明
	show radius-server	RADIUS サーバ情報を表示します。

radius-server timeout

RADIUS サーバへの再送信間隔を指定するには、**radius-server timeout** コマンドを使用します。再送信時間をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

radius-server timeout *seconds*

no radius-server timeout *seconds*

シンタックスの説明	<i>seconds</i>	Remote Authentication Dial-In User Service (RADIUS) サーバへの再送信間隔 (秒単位) を設定します。有効範囲は 1 ~ 60 です。
------------------	----------------	--

デフォルト	1 秒
--------------	-----

コマンドモード	コンフィギュレーションモード
----------------	----------------

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン	なし
-------------------	----

例	次に、タイムアウト値を 30 秒に設定する例を示します。
----------	------------------------------

```
switch# config terminal
switch(config)# radius-server timeout 30
```

関連コマンド	コマンド	説明
	show radius-server	RADIUS サーバ情報を表示します。

rate-mode bandwidth-fairness

ポート グループのポート間の帯域幅の公平性をイネーブ爾またはディセーブルにするには、コンフィギュレーション モードで **rate-mode bandwidth-fairness** コマンドを使用します。帯域幅の公平性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。

```
rate-mode bandwidth-fairness module module-id
```

```
no rate-mode bandwidth-fairness module module-id
```

シンタックスの説明

module *module-id* モジュール番号を指定します。

デフォルト

イネーブ爾

コマンド モード

コンフィギュレーション モード

コマンド履歴

リリース	変更内容
3.1(2)	このコマンドが導入されました。

使用上のガイドライン

帯域幅の公平性をイネーブ爾またはディセーブルにするモジュールごとに個別にコマンドを入力します。



(注)

この機能は、48 ポートおよび 24 ポート 4-Gbps ファイバチャネル スイッチング モジュールでのみサポートされます。

例

次に、帯域幅の公平性をイネーブ爾にする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rate-mode bandwidth-fairness module 1
```

次に、帯域幅の公平性をディセーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no rate-mode bandwidth-fairness module 1
```

関連コマンド

コマンド	説明
show module bandwidth-fairness	帯域幅の公平性のステータスを表示します。

rate-mode oversubscription-limit

加入過多率の制限をイネーブルまたはディセーブルにするには、**rate-mode oversubscription-limit** コマンドを使用します。

```
rate-mode oversubscription-limit module module number
```

```
no rate-mode oversubscription-limit module module number
```

シンタックスの説明	module <i>module-number</i> 加入過多率の制限がイネーブルまたはディセーブルになる特定のモジュールを特定します。
------------------	--

デフォルト	加入過多率は、すべての 24 ポートおよび 48 ポート スイッチング モジュールに対して制限されません。
--------------	---

コマンドモード	コンフィギュレーションモード
----------------	----------------

コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>3.1(1)</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	3.1(1)	このコマンドが導入されました。
リリース	変更内容				
3.1(1)	このコマンドが導入されました。				

使用上のガイドライン	加入過多率の制限がディセーブルの場合、共有ポートの間の帯域幅割り当ては設定速度に応じています（設定速度が auto の場合、帯域幅は 4 Gbps の速度で割り当てられます）。
-------------------	--

加入過多率の制限をディセーブルにする前に、共有ポートを明示的にシャットダウンし、アウトオブサービスにする必要があります。

明示的に **copy running-config startup-config** コマンドを入力しないと、設定はスタートアップ コンフィギュレーションに保存されません。



注意

モジュールを以前のリリースにダウングレードする前に、加入過多率の制限をイネーブルにする必要があります。

例	次に、モジュールの加入過多率の制限をディセーブルにする例を示します（専用ポートのみなのでシャットダウンする必要はありません）。
----------	---

```
switch# config t
switch(config)# no rate-mode oversubscription-limit module 2
```

次に、モジュールの加入過多率のステータスを表示する例を示します。

```
switch# show running-config
version 3.1(1)
...
no rate-mode oversubscription-limit module 2
interface fc2/1
  switchport speed 2000
interface fc2/1
...
```

関連コマンド	コマンド	説明
	<code>copy running-config startup-config</code>	新しい加入過多率をスタートアップ コンフィギュレーションに保存します。
	<code>show port-resources module</code>	ポートのレート モード ステータスを表示します。

reload

スイッチ全体、アクティブ スーパーバイザ モジュール、スタンバイ スーパーバイザ モジュール、または指定のモジュールをリロードしたり、指定したモジュールを強制的にネットブートしたりするには、EXEC モードで **reload** コマンドを使用します。

reload [*module module-number force-dnld*]

シンタックスの説明	パラメータ	説明
	module <i>module-number</i>	指定のモジュールや、アクティブまたはスタンバイ スーパーバイザ モジュールをリロードします。
	force-dnld	指定したモジュールに対して、リロード、ネットブートの開始、最新バージョンのモジュール ファームウェアの強制ダウンロードを実行します。

デフォルト スイッチ全体を再起動します。

コマンド モード EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン システムの再起動、指定したモジュールの再起動、または指定したモジュールでの強制的なネットブートを実行するには、**reload** コマンドを使用します。**reload** コマンドをシステム自体が使用すると、すべてのモジュールの電源が切断されてスーパーバイザ モジュールが再起動します。

指定したスロットにモジュールまたはスタンバイ スーパーバイザ モジュールがある場合に、**reload module module-number** コマンドを使用して、モジュールの電源をいったん切ってから再投入します。指定したスロットにアクティブ スーパーバイザ モジュールがある場合、現在アクティブなスーパーバイザ モジュールを再起動し、スタンバイ スーパーバイザ モジュールをアクティブにします。

reload module module-number force-dnld コマンドは、前述のコマンドと類似したコマンドです。このコマンドを実行すると、強制的にネットブートが実行されます。スロットにモジュールが含まれている場合、モジュールは最新のファームウェアでネットブートし、対応するフラッシュ メモリをそのイメージで更新します。

例 次に、**reload** コマンドを使用してシステムを再起動する例を示します。

```
switch# reload
This command will reboot the system. (y/n)? y
```

次に、**reload** コマンドを使用して指定したモジュールでネットブートを開始する例を示します。

```
switch# reload module 8 force-dnld
```

次に、**reload** コマンドを使用して特定のモジュールを再起動する例を示します。

```
switch# reload module 8
reloading module 8 ...
```

次に、**reload** コマンドを使用してアクティブなスーパーバイザ モジュールを再起動する例を示します。

```
switch# reload module 5
This command will cause supervisor switchover. (y/n)? y
```

関連コマンド

コマンド	説明
install	新しいソフトウェア イメージをインストールします。
copy system:running-config nvram:startup-config	コピー元からコピー先へファイルをコピーします。

read command-id

ストレージエリア ネットワーク チューナー拡張 N ポートの SCSI 読み取りコマンドを設定するには、**read command-id** コマンドを使用します。

```
read command-id cmd-id target pwwn transfer-size bytes [outstanding-ios value [continuous |
num-transactions number]]
```

シンタックスの説明

<i>cmd-id</i>	コマンド ID を指定します。有効範囲は 0 ～ 2147483647 です。
<i>target pwwn</i>	ターゲット ポート World Wide Name (WWN) を指定します。名前のフォーマットは、 <i>hh:hh:hh:hh:hh:hh:hh:hh</i> です。
<i>transfer-size bytes</i>	転送サイズを 512 バイトの倍数で指定します。有効範囲は 512 ～ 8388608 です。
<i>outstanding-ios value</i>	未決定の I/O 数を指定します。有効範囲は 1 ～ 1024 です。
<i>continuous</i>	コマンドの継続的な実行を指定します。
<i>num-transactions number</i>	トランザクション回数を指定します。有効範囲は 1 ～ 2147483647 です。

デフォルト

なし

コマンドモード

SAN 拡張 N ポート コンフィギュレーション サブモード

コマンド履歴

リリース	変更内容
2.0(x)	このコマンドが導入されました。

使用上のガイドライン

進行中の SCSI 読み取りコマンドを停止するには、**stop** コマンドを使用します。

例

次に、継続的な SCSI 読み取りコマンドを設定する例を示します。

```
switch# san-ext-tuner
switch(san-ext)# nwwn 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet
1/2
switch(san-ext-nport)# read command-id 100 target 22:22:22:22:22:22:22:22
transfer-size 512000 outstanding-ios 2 continuous
```

関連コマンド

コマンド	説明
nport pwwn	SAN 拡張チューナー N ポートを設定します。
san-ext-tuner	SAN 拡張チューナー機能をイネーブルにします。
show san-ext-tuner	SAN 拡張チューナー情報を表示します。
stop	SAN 拡張チューナー N ポートで進行中の SCSI コマンドを取り消します。

read-only

ゾーン アトリビュート グループの読み取り専用アトリビュートを設定するには、ゾーン アトリビュート コンフィギュレーションサブモードで **read-only** コマンドを使用します。デフォルトの設定に戻すには、コマンドの **no** 形式を使用します。

read-only

no read-only

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト 読み書き

コマンドモード ゾーンアトリビュート コンフィギュレーションサブモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン このコマンドは、拡張ゾーニングの読み取り専用アトリビュートを設定するだけです。ベーシックモードのブロードキャスト ゾーニングをイネーブルにするには、**zone name** コマンドを使用してゾーン コンフィギュレーションモードを開始して、**attribute read-only** サブコマンドを使用します。

例 次に、ゾーンアトリビュート グループの読み取り専用アトリビュートを設定する例を示します。

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)# read-only
```

関連コマンド	コマンド	説明
	show zone-attribute-group	ゾーンアトリビュートグループ情報を表示します。
	zone mode enhanced vsan	VSAN の拡張ゾーン分割をイネーブルにします。
	zone name	ゾーンアトリビュートを設定します。
	zone-attribute-group name	ゾーンアトリビュートグループを設定します。

revocation-check

トラストポイントの失効チェック方式を設定するには、トラストポイントコンフィギュレーションサブモードで **revocation-check** コマンドを使用します。失効チェック設定を廃棄するには、コマンドの **no** 形式を使用します。

```
revocation-check {crl [none | obsp [none]] | none | obsp [crl [none] | none]}
```

```
no revocation-check {crl [none | obsp [none]] | none | obsp [crl [none] | none]}
```

シンタックスの説明

crl	失効した証明書をチェックする場所としてローカルに保存された Certificate Revocation List (CRL; 証明書失効リスト) を指定します。
none	失効した証明書のチェックを実行しないように指定します。
obsp	失効した証明書のチェックのため、Online Certificate Status Protocol (OCSP) を指定します。

デフォルト

デフォルトでは、トラストポイントの失効チェック方式は CRL です。

コマンドモード

信頼点コンフィギュレーションサブモード

コマンド履歴

リリース	変更内容
3.0(1)	このコマンドが導入されました。

使用上のガイドライン

CA を認証し、OCSP URL を設定してから、失効チェック方式として OCSP を設定する必要があります。

失効チェック設定により、1 つまたは複数の方式を失効チェックの順序リストとして指定できます。ピア証明書の確認中、失効ステータスを提供することで、ある方式が成功するまで指定された順序で各方式が試行されます。方式として何も指定されていない場合、失効ステータスをチェックする必要はなく、ピア証明書は取り消されていないものとして処理されます。方式リストに最初の方式が指定されていない場合、チェックは必要ないものとして以後の方式を指定することはできません。

例

次に、事前に設定する必要があった URL の OCSP を使用して、失効した証明書をチェックする例を示します。

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# revocation-check obsp
```

次に、ローカルに保存された CRL の失効した証明書をチェックする例を示します。

```
switch(config-trustpoint)# revocation-check crl
```

次に、最初にローカルにキャッシュされた CRL を使用してから、必要に応じて OCSP を使用して、失効ステータスをチェックします。CRL がローカルにキャッシュされていない場合、OCSP チェックのみが試行されます。

```
switch(config-trustpoint)# revocation-check crl obsp
```

次に、失効した証明書をチェックしない例を示します。

```
switch(config-trustpoint)# revocation-check none
```

関連コマンド

コマンド	説明
crypto ca crt-request	CRL を設定するか、既存の トラスト ポイント CA の 1 つを上書きします。
ocsp url	トラスト ポイント OSCP の詳細を設定します。
show crypto ca crt	設定された CRL を表示します。

rlir preferred-cond fcid

Registered Link Incident Report (RLIR) フレームを優先的に受信するホストを指定するには、コンフィギュレーションモードで **rlir preferred-cond fcid** コマンドを使用します。優先的に受信するホストを削除するには、コマンドの **no** 形式を使用します。

```
rlir preferred-cond fcid fc-id vsan vsan-id
```

```
no rlir preferred-cond fcid fc-id vsan vsan-id
```

シンタックスの説明

fcid <i>fc-id</i>	FC ID を指定します。フォーマットは 0xhhhhhh です。
vsan <i>vsan-id</i>	VSAN ID を指定します。有効範囲は 1 ~ 4093 です。

デフォルト

デフォルトでは、登録機能が「always receive」に設定されているホストがない場合、MDS スイッチは RLIR フレームを登録機能が「conditionally receive」に設定されている VSAN のホストの 1 つに送信します。

コマンドモード

コンフィギュレーションモード

コマンド履歴

リリース	変更内容
3.0(3)	このコマンドが導入されました。

使用上のガイドライン

次の条件が満たされた場合のみ、MDS スイッチは RLIR フレームを優先ホストに送信します。

- RLIR に関して、登録機能が「always receive」に設定されているホストが VSAN 内にありません。VSAN に「always receive」として登録されているホストが 1 つまたは複数ある場合、RLIR はそれらのホストのみに送信され、設定された優先ホストには送信されません。
- 優先ホストが登録され、その登録機能が「conditionally receive」に設定されています。



(注)

登録されているすべてのホストの登録機能が「conditionally receive」に設定されている場合、優先ホストが RLIR フレームを受信します。

指定できる RLIR 優先ホストは、VSAN ごとに 1 つだけです。

例

次に、VSAN 2 の RLIR 優先ホストとして FC ID 0x654321 を指定する例を示します。

```
switch# config t
switch(config)# rlr preferred-cond fcid 0x654321 vsan 2
```

次に、VSAN 2 の RLIR 優先ホストとして FC ID 0x654321 を削除する例を示します。

```
switch# config t
switch(config)# no rlr preferred-cond fcid 0x654321 vsan 2
```

関連コマンド

コマンド	説明
show rlr	RILR、Link Incident Record Registration (LIPR)、および Distribute Registered Link Incident Record (DRLIR) フレームの情報を表示します。
clear rlr	RLIR をクリアします。
debug rlr	RLIR デバッグをイネーブルにします。

rmdir

既存のディレクトリをフラッシュ ファイル システムから削除するには、EXEC モードで **rmdir** コマンドを使用します。

```
rmdir [bootflash: | slot0: | volatile:]directory
```

シンタックスの説明

bootflash:	内蔵ブート フラッシュ メモリの送信元または宛先ロケーション
slot0:	CompactFlash メモリや PCMCIA カードの送信元または宛先ロケーション
volatile:	揮発性ファイル システムの送信元または宛先ロケーション
directory	削除するディレクトリ名

デフォルト

現在のデフォルト ディレクトリを使用します。

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
1.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、フラッシュ ファイル システムでのみ有効です。

rmdir コマンドを使用すると、現在のディレクトリ レベルまたは指定のディレクトリ レベルで、既存のディレクトリを削除できます。削除対象のディレクトリは空である必要があります。

例

次に、slot0 ディレクトリにある test というディレクトリを削除する例を示します。

```
switch# rmdir slot0:test
```

次に、現在のディレクトリ レベルにある test というディレクトリを削除する例を示します。現在のディレクトリが slot0:mydir の場合、このコマンドでは slot0:mydir/test が削除されます。

```
switch# rmdir test
```

関連コマンド


コマンド	説明
dir	ファイル システムのファイルの一覧を表示します。
mkdir	フラッシュ ファイル システム内に新規ディレクトリを作成します。

rmon alarm

32 ビット Remote Monitoring (RMON; リモート モニタリング) アラームを設定するには、コンフィギュレーション モードで **rmon alarm** コマンドを使用します。RMON アラームを削除するには、コマンドの **no** 形式を使用します。

```
rmon alarm alarm-number mib-object sample-interval {absolute | delta} rising-threshold value
[rising-event] falling-threshold value [falling-event] [owner alarm-owner]
```

```
no rmon alarm alarm-number
```

シンタックスの説明	
<i>alarm-number</i>	RMON アラーム番号を指定します。有効範囲は 1 ～ 65535 です。
<i>mib-object</i>	モニタリングする MIB (管理情報ベース) オブジェクトを指定します。1 最大 80 文字まで可能です。
	 (注) MIB オブジェクト ID は、ドットで区切られた 10 進数のみとする必要があります。文字列の記述は使用しません。
<i>sample-interval</i>	サンプルインターバルを秒で指定します。有効範囲は 1 ～ 2147483647 です。
absolute	それぞれのサンプルを直接テストします。
delta	現在のサンプルと以前のサンプル間の差異 (デルタ) をテストします。
rising-threshold value	上昇しきい値を指定します。有効範囲は -2147483648 ～ 2147483647 です。
<i>rising-event</i>	(任意) 上昇しきい値を超えたときにトリガーするイベントを指定します。有効範囲は 1 ～ 65535 です。イベントが指定されていない場合は、イベント 0 が使用されます。
falling-threshold value	下限しきい値を指定します。有効範囲は -2147483648 ～ 2147483647 です。
<i>falling-event</i>	(任意) 上昇しきい値を超えたときにトリガーするイベントを指定します。有効範囲は 1 ～ 65535 です。イベントが指定されていない場合は、イベント 0 が使用されます。
owner alarm-owner	(任意) アラームのオーナーを指定します。最大サイズは 80 文字です。

デフォルト デイセーブル

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン アラームのイベントを設定するには、**rmon event** コマンドを使用します。

RMON アラームの最大数は、現時点では Device Manager および Threshold Manager の GUI を使用することでのみ設定できます。CLI コマンドでは、この最大値を変更できません。



(注) システムに過重な負荷をかけないようにするには、アラーム サンプル インターバルを 30 秒またはそれより長く設定することを推奨します。

例 次に、インターフェイス fc 1/1 上の ifInErrors (OID 1.3.6.1.2.1.2.2.1.14) に、32 ビットアラーム番号 20 を設定する例を示します。サンプルインターバルは 30 秒で、デルタ サンプルはテストされません。上昇しきい値はサンプル ウィンドウにつき 15 エラーで、このレベルに到達するとイベント 1 がトリガーされます。下限しきい値はサンプル ウィンドウ内で 0 エラーで、イベント 0 (アクションなし) がトリガーされます。オーナーは、ifInErrors.fc1/1@test です。

```
switch# config terminal
switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 30 delta rising-threshold
15 1 falling-threshold 0 owner ifInErrors.fc1/1@test
```

関連コマンド

コマンド	説明
rmon event	RMON イベントを設定します。
rmon hcalarm	64 ビット RMON アラームを設定します。
show rmon	RMON 設定およびロギング情報を表示します。
show snmp host	SNMP (簡易ネットワーク管理プロトコル) トラップ宛先情報を表示します。
snmp-server host	SNMP 通知の受信側を指定します。

rmon event

Remote Monitoring (RMON; リモート モニタリング) イベントを設定するには、コンフィギュレーション モードで **rmon event** コマンドを使用します。RMON イベントを削除するには、コマンドの **no** 形式を使用します。

```
rmon event event-number [description text [owner owner-name] | log [trap community-string]
[description text] [owner owner-name] | trap community-string [description text] [owner
owner-name] | owner owner-name]
```

```
no rmon event event-number
```

シンタックスの説明

<i>event-number</i>	RMON イベント番号を指定します。有効範囲は 1 ~ 65535 です。
description text	(任意) イベントの記述を指定します。1 最大 80 文字まで可能です。
owner owner-name	(任意) アラームのオーナーを指定します。最大 80 文字まで可能です。
log	(任意) イベントがアラームによってトリガーされた場合は、オンボード RMON ログに RMON ログ エントリを生成します。
trap community-string	(任意) イベントがアラームによってトリガーされた場合は、指定のコミュニティ名で SNMP (簡易ネットワーク管理プロトコル) トラップを生成します。最大 32 文字まで可能です。

デフォルト

ディセーブル

コマンド モード

コンフィギュレーション モード

コマンド履歴

リリース	変更内容
2.0(x)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより作成されたイベントは、**rmon alarm** または **rmon hcalarm** コマンドを使用して設定されたアラームによってトリガーできます。

ログ オプションによって、イベントは MDS スイッチ上のローカル ログに記録されます。トラップ オプションは、オンボード SNMP エージェントを使用して、リモート NMS に SNMP トラップを送信します。



(注)

イベントは **rmon alarm** (32 ビット) および **hcalarm** (64 ビット) コマンドの両方で使用できます。

例

次に、オンボード RMON ログに記録して、パブリック コミュニティ トラップ宛に SNMP トラップを送信するように RMON イベント 2 を設定する例を示します。記述は **CriticalErrors** であり、オーナーは **test** です。

```
switch# config terminal
switch(config)# rmon event 2 log trap public description CriticalErrors owner test
```


関連コマンド

コマンド	説明
rmon alarm	32 ビット RMON アラームを設定します。
rmon hcalarm	64 ビット RMON アラームを設定します。
show rmon	RMON 設定およびロギング情報を表示します。


rmon hcalarm

64 ビット Remote Monitoring (RMON; リモート モニタリング) 高容量アラーム (hcalarm) を設定するには、コンフィギュレーションモードで **rmon alarm** コマンドを使用します。rmon hcalarm を削除するには、コマンドの **no** 形式を使用します。

```
rmon hcalarm alarm-number mib-object sample-interval {absolute | delta}
    {rising-threshold-high value rising-threshold-low value [rising-event] [falling-threshold-high
    value falling-threshold-low value [falling-event]] | falling-threshold-high value
    falling-threshold-low value [falling-event]}[owner alarm-owner]

no rmon hcalarm alarm-number
```

シンタックスの説明

<i>alarm-number</i>	RMON hcalarm 番号を指定します。有効範囲は 1 ～ 65535 です。
<i>mib-object</i>	モニタリングする MIB (管理情報ベース) オブジェクトを指定します。1 最大 80 文字まで可能です。
	 (注) MIB オブジェクト ID は、ドットで区切られた 10 進数のみとする必要があります、文字列の記述は使用しません。
<i>sample-interval</i>	サンプル インターバルを秒で指定します。有効範囲は 1 ～ 65535 です。
absolute	それぞれのサンプルを直接テストします。
delta	現在のサンプルと以前のサンプル間の差異 (デルタ) をテストします。
rising-threshold-high value	64 ビット上昇しきい値の上位 32 ビットを設定します。有効範囲は 0 ～ 4294967295 です。
rising-threshold-low value	64 ビット上昇しきい値の下位 32 ビットを設定します。有効範囲は 0 ～ 4294967295 です。
<i>rising-event</i>	(任意) 上昇しきい値を超えたときにトリガーするイベントを指定します。有効範囲は 1 ～ 65535 です。
falling-threshold-high value	64 ビット下限しきい値の上位 32 ビットを設定します。有効範囲は 0 ～ 4294967295 です。
falling-threshold-low value	64 ビット下限しきい値の下位 32 ビットを設定します。有効範囲は 0 ～ 4294967295 です。
<i>falling-event</i>	(任意) 下限しきい値を下回ったときにトリガーするイベントを指定します。有効範囲は 0 ～ 65535 です。
owner alarm-owner	(任意) アラームのオーナーを指定します。最大サイズは 80 文字です。

デフォルト

64 ビットアラーム

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	3.0(1)	このコマンドが導入されました。

使用上のガイドライン イベント番号 0 は、定義済みのヌル（または操作なし）イベントです。ユーザがアラーム内でイベントを指定しない場合は、このイベントが自動的にシステムによって使用されます。イベントがトリガーされてもアクションは発生しませんが、アラームはリセットされたままになります。ユーザは、イベントの再定義を行うことができません。これは定義済みのイベントであり、作成できるのは 1 ~ 65535 の範囲内のイベントのみです。

HC RMON アラームを設定するには `ACISCO-HC-ALARM-MIB` を使用します。

RMON アラームの最大数は、現時点では Device Manager および Threshold Manager の GUI を使用することで設定できます。CLI コマンドでは、この最大値を変更できません。



(注)

システムに過重な負荷をかけないようにするには、アラーム サンプルインターバルを 30 秒またはそれより長く設定することを推奨します。

例 次に、インターフェイス fc 12/1 上の ifHCInOctets (OID 1.3.6.1.2.1.31.1.1.1.6) に、64 ビットアラーム番号 2 を設定する例を示します。サンプルインターバルは 30 秒で、デルタ サンプルはテストされます。上昇しきい値はサンプル ウィンドウにつき 240,000,000,000 バイト (平均 8,000,000,000 Bps) で、このレベルに到達するとイベント 4 がトリガーされます。下限しきい値はサンプル ウィンドウ内で 180,000,000,000 バイト (平均 6,000,000,000 Bps) で、イベント 0 (アクションなし) がトリガーされ、アラームがリセットされます。オーナーは ifHCInOctets.fc12/1@test です。

```
switch#config terminal
switch#(config) rmon hcalarm 2 1.3.6.1.2.1.31.1.1.1.6.22544384 30 delta
rising-threshold-high 55 rising-threshold-low 3776798720 4 falling-threshold-high 41
falling-threshold-low 3906340864 owner ifHCInOctets.fc12/1@test
```

関連コマンド	コマンド	説明
	<code>rmon alarm</code>	32 ビット RMON アラームを設定します。
	<code>rmon hcalarm</code>	64 ビット RMON アラームを設定します。
	<code>rmon event</code>	RMON イベントを設定します。
	<code>show rmon</code>	RMON 設定およびロギング情報を表示します。
	<code>show snmp host</code>	SNMP (簡易ネットワーク管理プロトコル) トラップ宛先情報を表示します。
	<code>snmp-server host</code>	SNMP 通知の受信側を指定します。

role abort

進行中の許可役割 Cisco Fabric Services (CFS) 配信セッションを廃棄するには、コンフィギュレーションモードで **role abort** コマンドを使用します。

role abort

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、進行中の許可役割 CFS 配信セッションを廃棄する例を示します。

```
switch# config terminal  
switch(config)# role abort
```

関連コマンド	コマンド	説明
	role distribute	許可役割の CFS 配信をイネーブルにします。
	show role	許可役割情報を表示します。

role commit

ファブリック内で進行中の許可役割 Cisco Fabric Services (CFS) 配信セッションに関する未決定コンフィギュレーションを適用するには、コンフィギュレーションモードで **role commit** コマンドを使用します。

role commit

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、許可役割コンフィギュレーションをファブリックのスイッチに適用する例を示します。

```
switch# config terminal
switch(config)# role commit
```

関連コマンド	コマンド	説明
	role distribute	許可役割の CFS 配信をイネーブルにします。
	show role	許可役割情報を表示します。

role distribute

許可役割の Cisco Fabric Services (CFS) 配信をイネーブルにするには、**role distribute** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

role distribute

no role distribute

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、許可役割のファブリック配信をイネーブルにする例を示します。

```
switch# config terminal  
switch(config)# role distribute
```

関連コマンド	コマンド	説明
	role commit	一時的な許可役割コンフィギュレーションの変更をアクティブ コンフィギュレーションに確定します。
	show role	許可役割情報を表示します。

role name

ユーザに新しい役割を設定して割り当てたり、既存の役割のプロファイルを変更したりするには、コンフィギュレーションモードで **role name** コマンドを使用します。設定した役割を削除するには、このコマンドの **no** 形式を使用します。

```
role name name [description user description] [rule number permit clear feature name | permit config feature name | permit debug feature name | permit show feature name] [rule number deny clear feature name | deny config feature name | deny debug feature name | deny exec feature name | deny show feature name]
```

```
no role name name [description user description] [rule number permit clear feature name | permit config feature name | permit debug feature name | permit show feature name] [rule number deny clear feature name | deny config feature name | deny debug feature name | deny exec feature name | deny show feature name]
```

シンタックスの説明

name	作成または変更対象の役割名。役割の最大数は 64 です。
description	役割の記述を追加します。最大文字サイズは 80 です。
user description	ユーザの記述を役割に追加します。
exit	このサブモードを終了します。
no	コマンドを無効にするか、またはデフォルト設定にします。
rule	rule キーワードを入力します。
number	役割の番号 (1 ~ 16) を入力します。
permit	役割にコマンドを追加します。
deny	役割からコマンドを削除します。
clear	クリア コマンド
config	コンフィギュレーション コマンド
debug	デバッグ コマンド
show	表示コマンド
feature	機能名を入力します。
exec	EXEC コマンド
name	機能名を入力します (最大文字サイズ - 32)。

デフォルト

なし

コマンドモード

コンフィギュレーションモード

コマンド履歴

リリース	変更内容
1.0(2)	このコマンドが導入されました。

使用上のガイドライン

役割は割り当てられたルールでユーザが特定のコマンドにアクセスすることを定義したルールの集合です。ユーザは役割を割り当てられます。役割内のルールは、以下のコマンドに対してアクセスの許可または拒否を割り当てられます。

clear クリアコマンド

config コンフィギュレーション コマンド

debug デバッグ コマンド

exec EXEC コマンド

show 表示コマンド

これらのコマンドは、**permit** または **deny** オプションをコマンドラインで指定できます。

例

次に、ユーザに新しい役割を割り当てる例を示します。

```
switch# config terminal
switch(config)# role name techdocs
switch(config-role)#
switch(config)# no role name techdocs
switch(config)#
switch(config-role)# description Entire Tech. Docs. group
switch(config-role)# no description
switch# config terminal
switch(config)# role name sangroup
switch(config-role)#
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
switch(config-role)# no rule 4
```

Role: network-operator

Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands

関連コマンド

コマンド	説明
show role	各役割に基づいたルールなどの、スイッチに割り当てられたすべての役割を表示します。

rsakeypair

RSA キー ペアの詳細をトラスト ポイントに設定し、関連付けるには、トラスト ポイント コンフィギュレーション サブモードで **rsakeypair** コマンドを使用します。トラスト ポイントから RSA キー ペアの関連付けを解除するには、コマンドの **no** 形式を使用します。

```
rsakeypair key-pair-label [key-pair-size]
```

```
no rsakeypair key-pair-label [key-pair-size]
```

シンタックスの説明

<i>key-pair-label</i>	RSA キー ペアの名前を指定します。最大文字サイズは 64 です。
<i>key-pair-size</i>	RSA キー ペアのサイズを指定します。サイズは 512 ~ 2048 です。

デフォルト

キー ペアが生成されていない場合、デフォルトのキー ペアのサイズは 512 です。

コマンドモード

信頼点コンフィギュレーション サブモード

コマンド履歴

リリース	変更内容
3.0(1)	このコマンドが導入されました。

使用上のガイドライン

同じキー ペアを多くのトラスト ポイント CA に関連付けることができる場合でも、1つの RSA キー ペアのみをトラスト ポイント CA に関連付けることができます。アイデンティティ証明書を取得するために CA に登録する前に、この関連付けを行う必要があります。事前にキー ペアが生成され (**crypto key generate** コマンドを使用して)、キー ペアのサイズが指定されている場合、そのサイズは生成中に使用したサイズと同じでなければいけません。指定されたキー ペアが生成されていない場合、**crypto ca enroll** コマンドを使用して登録時に生成されます。

rsakeypair コマンドの **no** 形式を使用すると、トラスト ポイントからキー ペアの関連付けを解除します (破棄はしません)。**no rsakeypair** コマンドを実行する前に、まずアイデンティティ証明書があれば、トラスト ポイント C から削除します。削除すると、アイデンティティ証明書とトラスト ポイントのキー ペアの間のアソシエーションの一貫性を保ちます。

例

次に、RSA キー ペアをトラスト ポイントに関連付ける例を示します。

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# rsakeypair adminid-key
```

次に、トラスト ポイントから RSA キー ペアの関連付けを解析する例を示します。

```
switch(config-trustpoint)# no rsakeypair adminid-key
```

関連コマンド

コマンド	説明
crypto ca enroll	トラスト ポイント CA 用に作成されたスイッチの RSA キー ペアの証明書を要求します。
crypto key generate rsa	RSA キー ペア情報を設定します。
show crypto key mypubkey rsa	設定された RSA キー ペアに関する情報を表示します。

rscn

ファブリック内の変更を Nx ポートに通知するファイバチャネルサービスである Registered State Change Notification (RSCN) を設定するには、コンフィギュレーションモードで **rscn** コマンドを使用します。

```
rscn {multi-pid | suppress domain-swrsen} vsan vsan-id
```

シンタックスの説明	multi-pid	RSCN をマルチ PID フォーマットで送信します。
	suppress domain-swrsen	ドメインフォーマット SW-RCSN の伝送を抑制します。
	vsan vsan-id	VSAN (仮想 SAN) 情報またはメンバシップを設定します。VSAN ID の有効範囲は、1 ~ 4093 です。

デフォルト なし

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、RSCN をマルチ PID フォーマットで設定する例を示します。

```
switch# config terminal
switch(config)# rscn multi-pid vsan 1
```

関連コマンド	コマンド	説明
	show rscn src-table	状態変更登録テーブルを表示します。
	show rscn statistics	RSCN 統計情報を表示します。

rscn abort vsan

VSAN の Registered State Change Notification (RSCN) 設定を取り消すには、コンフィギュレーションモードで **rscn abort vsan** コマンドを使用して、取り消しを戻すには、コマンドの **no** 形式を使用します。

```
rscn abort vsan vsan-id
```

```
no rscn abort vsan vsan-id
```

シンタックスの説明	<i>vsan-id</i>	RSCN 設定を取り消す VSAN を指定します。VSAN ID の有効範囲は、1 ~ 4093 です。
-----------	----------------	--

デフォルト	なし
-------	----

コマンドモード	コンフィギュレーションモード
---------	----------------

コマンド履歴	リリース	変更内容
	3.0(1)	このコマンドが導入されました。

使用上のガイドライン	なし
------------	----

例 次に、VSAN 1 の RSCN 設定を取り消す例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn abort vsan 1
```

関連コマンド	コマンド	説明
	rscn commit vsan	指定された VSAN の未決定の RSCN 設定を確定します。
	rscn distribute	RSCN 設定の配信をイネーブルにします。
	rscn event-tov	RSCN イベント タイムアウトを設定します。
	clear rscn session vsan	指定された VSAN の RSCN セッションをクリアします。
	show rscn	RSCN 設定情報を表示します。

rscn commit vsan

未決定の Registered State Change Notification (RSCN) 設定を適用するには、コンフィギュレーションモードで **rscn commit vsan** コマンドを使用します。未決定の RSCN 設定を廃棄するには、コマンドの **no** 形式を使用します。

```
rscn commit vsan vsan-id
```

```
no rscn commit vsan vsan-id
```

シンタックスの説明	<i>vsan-id</i>	RSCN 設定を確定する VSAN を指定します。VSAN ID の有効範囲は、1 ~ 4093 です。
-----------	----------------	--

デフォルト	なし
-------	----

コマンドモード	コンフィギュレーションモード
---------	----------------

コマンド履歴	リリース	変更内容
	3.0(1)	このコマンドが導入されました。

使用上のガイドライン	アクティブ データベースに加えられた変更を確定する場合、ファブリック内のすべてのスイッチに設定が確定されます。確定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。
------------	--

例	次に、VSAN 1 の RSCN 設定を確定する例を示します。
---	---------------------------------

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn commit vsan 1
```

関連コマンド	コマンド	説明
	rscn abort vsan	指定された VSAN の未決定の RSCN 設定を取り消します。
	rscn distribute	RSCN 設定の配信をイネーブルにします。
	rscn event-tov	RSCN イベント タイムアウトを設定します。
	clear rscn session vsan	指定された VSAN の RSCN セッションをクリアします。
	show rscn	RSCN 設定情報を表示します。

rscn distribute

Registered State Change Notification (RSCN) 設定の配信をイネーブルにするには、コンフィギュレーション モードで **rscn commit vsan** コマンドを使用します。配信をディセーブルにするには、コマンドの **no** 形式を使用します。

rscn distribute

no rscn distribute

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト RSCN タイマー配信はディセーブルです。

コマンド モード コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	3.0(1)	このコマンドが導入されました。

使用上のガイドライン RSCN タイマー設定は VSAN 内のすべてのスイッチで同じである必要があります。そうでないと、リンクが開始しません。Cisco Fabric Service (CFS) は、RSCN タイマー設定をファブリック内のすべてのスイッチに自動的に配信します。RSCN タイマー設定のみが配信されます。



(注) RSCN タイマー設定に関して CFS 配信を正常に動作させるには、ファブリック内のすべてのスイッチで Cisco SAN-OS Release 3.0(1) 以降を稼働している必要があります。

例 次に、RSCN 設定の配信をイネーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn distribute
```

関連コマンド	コマンド	説明
	rscn abort vsan	指定された VSAN の未決定の RSCN 設定を取り消します。
	rscn commit vsan	未決定の RSCN 設定を適用します。
	rscn event-tov	RSCN イベント タイムアウトを設定します。
	clear rscn session vsan	指定された VSAN の RSCN セッションをクリアします。
	show rscn	RSCN 設定情報を表示します。

rscn event-tov

指定された VSAN の Registered State Change Notification (RSCN) のイベント タイムアウト値を設定するには、コンフィギュレーションモードで **rscn event-tov** コマンドを使用します。イベント タイムアウト値を取り消し、デフォルトの値に戻すには、コマンドの **no** 形式を使用します。

```
rscn event-tov timeout vsan vsan-id
```

```
no rscn event-tov timeout vsan vsan-id
```

シンタックスの説明

<i>timeout</i>	イベント タイムアウト値をミリ秒単位で指定します。有効範囲は 0 ～ 2000 です。
<i>vsan-id</i>	RSCN イベント タイマーを使用する VSAN を指定します。VSAN ID の有効範囲は、1 ～ 4093 です。

デフォルト

デフォルトのタイムアウト値は、ファイバチャネル VSAN の場合は 2000 ミリ秒、FICON VSAN の場合は 1000 ミリ秒です。

コマンドモード

コンフィギュレーションモード

コマンド履歴

リリース	変更内容
3.0(1)	このコマンドが導入されました。

使用上のガイドライン

タイムアウト値を変更する前に、**rscn distribute** コマンドを使用して RSCN 設定の配信をイネーブルにする必要があります。

RSCN タイマーは、初期化およびスイッチオーバーの実行時に Cisco Fabric Services (CFS) に登録されます。ハイ アベイラビリティを実現するため、RSCN タイマー配信がクラッシュし再起動する場合、またはスイッチオーバーが発生した場合には、クラッシュまたはスイッチオーバーが発生する前の状態から、通常の機能が再開されます。



(注)

以前の Cisco MDS SAN-OS リリースにダウングレードする場合は、**show incompatibility system** コマンドを使用して互換性を確認できます。以前のリリースにダウングレードする前に、RSCN タイマー配信のサポートをディセーブルにする必要があります。

例

次に、VSAN 1 の RSCN イベント タイムアウト値を設定する例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn event-tov 20 vsan 1
Successful. Commit should follow for command to take effect.
```

関連コマンド

コマンド	説明
rscn abort vsan	指定された VSAN の未決定の RSCN 設定を取り消します。
rscn commit vsan	未決定の RSCN 設定を適用します。
rscn distribute	RSCN 設定の配信をイネーブルにします。
clear rscn session vsan	指定された VSAN の RSCN セッションをクリアします。
show rscn	RSCN 設定情報を表示します。

rule

テープ ボリューム グループの正規表現を指定するには、**rule** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

```
rule {range range | regexp regular expression}
```

```
no rule {range range | regexp regular expression}
```

シンタックスの説明	range <i>range</i>	クリプト テープ ボリューム バーコードの範囲を指定します。最大 32 文字まで可能です。
	regexp <i>regular expression</i>	ボリューム グループの正規表現を指定します。最大 32 文字まで可能です。

デフォルト なし

コマンド モード Cisco SME クリプト テープ ボリューム グループ コンフィギュレーション サブモード

コマンド履歴	リリース	変更内容
	3.2(2)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、ボリューム グループの正規表現を指定する例を示します。

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp tbg1
switch(config-sme-cl-tape-bkgrp)# tape-volgrp tv1
switch(config-sme-cl-tape-bkgrp-volgrp)#rule regexp r1
```

関連コマンド	コマンド	説明
	show sme cluster	Cisco SME クラスタに関する情報を表示します。
	tape-bkgrp <i>groupname</i>	クリプト バックアップ グループを設定します。
	tape-volgrp <i>volume groupname</i>	クリプト バックアップ ボリューム グループを設定します。

run-script

ファイル内にて指定されたコマンドを実行するには、**run-script** コマンドを使用します。

```
run-script [bootflash: | slot0: | volatile:]filename
```

シンタックスの説明	
bootflash:	内蔵ブート フラッシュ メモリの送信元または宛先ロケーション
slot0:	CompactFlash メモリや PCMCIA カードの送信元または宛先ロケーション
volatile:	揮発性ファイル システムの送信元または宛先ロケーション
filename	コマンドを含むファイル名

デフォルト 現在のデフォルト ディレクトリを使用します。

コマンド モード EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。
	3.0(1)	ユーザ定義の変数に関する情報を含んだ使用上のガイドラインおよび例にアップデートされました。

使用上のガイドライン このコマンドを使用する場合、ファイルが作成され、正しい順番でコマンドが指定されていることを確認してください。

run-script コマンドは、ユーザ定義の変数をパラメータとして受け入れます。

例 次に、slot0 ディレクトリに常駐するテストファイルで指定された CLI (コマンドライン インターフェイス) コマンドを実行する例を示します。

```
switch# show file slot0:testfile
conf t
interface fc 1/1
no shutdown
end
sh interface fc1/1
```

run-script コマンドの応答として、次のようなファイルが出力されます。

```
switch# run-script slot0:testfile
'conf t'
Enter configuration commands, one per line. End with CNTL/Z.

'interface fc 1/1'

'no shutdown'

'end'

'sh interface fc1/1'
fc1/1 is down (Fcot not present)
  Hardware is Fibre Channel
  Port WWN is 20:01:00:05:30:00:48:9e
  Admin port mode is auto, trunk mode is on
  vsan is 1
  Beacon is turned off
  Counter Values (current):
    0 frames input, 0 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 0 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    0 frames output, 0 bytes, 0 discards
    Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
  Counter Values (5 minute averages):
    0 frames input, 0 bytes, 0 discards
    0 runts, 0 jabber, 0 too long, 0 too short
    0 input errors, 0 CRC, 0 invalid transmission words
    0 address id, 0 delimiter
    0 EOF abort, 0 fragmented, 0 unknown class
    0 frames output, 0 bytes, 0 discards
    Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
```

次に、ユーザ定義の変数を **run-script** コマンドに渡す例を示します。

```
switch# run-script bootflash:test2.vsh var1="fc1/1" var2="brief"
switch # show interface $(var1) $(var2)
-----
Interface Vsan Admin Admin Status SFP Oper Oper Port
Mode Trunk Mode Speed Channel
Mode (Gbps)
-----
fc1/1 1 auto on sfpAbsent -- -- --
```


rspan-tunnel

SPAN Tunnel (ST; SPAN トンネル) ポートと Remote SPAN (RSPAN; リモート SPAN) トンネルを関連付けて結合するには、**rspan-tunnel** コマンドを使用します。

```
rspan-tunnel interface fc-tunnel tunnel-id
```

```
rspan-tunnel
```

シンタックスの説明	コマンド	説明
	rspan-tunnel	RSPAN トンネルを設定します。
	interface	このトンネルを設定するインターフェイスを指定します。
	fc-tunnel tunnel-id	FC トンネルインターフェイスを指定します。有効範囲は 1 ~ 255 です。

デフォルト なし

コマンドモード インターフェイス コンフィギュレーション サブモード

コマンド履歴	リリース	変更内容
	1.2(1)	このコマンドが導入されました。

使用上のガイドライン ファイバチャネル トンネル マッピングが送信元または宛先スイッチに設定されるまで、インターフェイスはオプションで立ち上がりません。

例 次に、ST ポートと RSPAN トンネルを関連付けて結合するようにインターフェイスを設定して、このインターフェイスを介したトラフィック フローをイネーブルにする例を示します。

```
switchS# config t
switchS(config)# interface fc2/1
switchS(config-if)# rspan-tunnel interface fc-tunnel 100
switchS(config-if)# no shutdown
```

