



Cisco MDS 9000 シリーズ ファブリック構成ガイド、リリース 9.x

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ www.cisco.com/jp/go/safety_warning/ ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.



目次

Full Cisco Trademarks with Software License ?

はじめに :

はじめに **xxi**

対象読者 **xxi**

表記法 **xxi**

関連資料 **xxii**

通信、サービス、およびその他の情報 **xxiii**

第 1 章

新機能と更新情報 **1**

変更点 **1**

第 2 章

ファブリックの概要 **5**

仮想 SAN **5**

ダイナミック ポート VLAN メンバーシップ **6**

SAN デバイス仮想化 **6**

ゾーン分割 **6**

分散デバイス エイリアス サービス **7**

ファイバチャネルルーティング サービスおよびプロトコル **8**

マルチプロトコル サポート **8**

第 3 章

VSAN の設定と管理 **9**

VSAN について **9**

VSAN トポロジ **10**

VSAN の利点 **12**

VSAN とゾーン	12
VSAN の設定	13
予約済み VSAN 範囲と分離された VSAN 範囲のガイドライン	14
VSAN の作成	15
VSAN の静的な作成	15
VSAN の作成	15
ポート VSAN メンバーシップ	16
スタティック ポート VSAN メンバーシップの概要	16
VSAN スタティック メンバーシップの表示	17
デフォルト VSAN	18
分離された VSAN	18
分離された VSAN メンバーシップの概要	19
VSAN の動作ステート	19
スタティック VSAN の削除	19
スタティック VSAN の削除	20
ロード バランシング	20
ロード バランシングの設定	20
interop モード	21
FICON VSAN	22
スタティック VSAN 設定の表示	22
デフォルト設定	23
ファブリック スイッチ情報の表示	23

第 4 章

ダイナミック VSAN の作成	25
DPVM の概要	25
DPVM 設定の概要	26
DPVM のイネーブル化	27
DPVM デバイス構成 (静的)	27
DPVM の構成	27
DPVM のアクティベート	29
DPVM 自動学習	29

自動学習の有効化	30
学習エントリの消去	31
自動学習の無効化	31
DPVM 配信	31
DPVM 配信について	32
DPVM 配信の無効化	32
ファブリックのロックの概要	33
ファブリックのロック	33
変更のコミット	33
変更の破棄	34
ロック済みセッションのクリア	34
DPVM 構成マージのガイドライン	35
DPVM 構成のコピーについて	35
DPVM アクティブ構成のコピー	35
データベースの差分の比較	35
DPVM マージのステータスおよび統計情報の表示	36
DPVM 設定の表示	37
DPVM の設定例	38
デフォルト設定	41

第 5 章

ゾーンの設定と管理	43
機能情報の確認	44
ゾーン構成およびゾーン管理の機能履歴	44
ゾーン分割の概要	45
ゾーン分割の例	47
ゾーン実装	48
ゾーンメンバー設定に関する注意事項	48
アクティブゾーンセットおよびフルゾーンセットに関する考慮事項	49
Quick Config ウィザードの使用	50
自動ゾーン	53
自動ゾーンに関する注意事項と制約事項	54

自動モードでの自動ゾーンの設定	56
自動モードでの自動ゾーンの有効化	56
自動保存を有効にする	56
手動モードでの自動ゾーンの実行	56
リモート認証 (AAA) ユーザーによる自動ゾーンの自動モードでの有効化	56
自動保存の無効化	57
自動ゾーンの自動モードの無効化	57
すべてのゾーン設定の表示	57
保留中のゾーン設定の表示	58
保留中のゾーン設定の適用 (手動モード)	58
自動ゾーンによって作成されたゾーンおよびゾーンセットの削除	58
例：自動ゾーンの設定	58
自動ゾーン設定の確認	60
自動ゾーンのシナリオの例	62
ゾーン設定	64
Edit Local Full Zone Database ツールの概要	64
ゾーンの設定	66
Zone Configuration Tool を使用したゾーンの設定	68
ゾーンメンバーの追加	71
名前、WWN、または FC ID に基づくエンドデバイスのフィルタリング	72
複数のゾーンへの複数のエンドデバイスの追加	73
ゾーンセットと FC エイリアス	73
ゾーンセットの作成	74
ゾーンセットの非アクティブ化	74
DCNM SAN クライアントを使用したゾーンセットのアクティブ化	75
ゾーンセットの非アクティブ化	77
ゾーンメンバーシップ情報の表示	77
アクティブなゾーンセットの上書き制御	78
デフォルトゾーン	79
デフォルトゾーンのアクセス権限の設定	81
DCNM SAN クライアントを使用したデフォルトゾーンのアクセス権限の構成	81

FC エイリアスの作成の概要	82
FC エイリアスの作成	83
DCNM SAN クライアントを使用した FC エイリアスの作成	84
エイリアスへのメンバーの追加	85
ゾーン メンバーの pWWN ベース メンバーへの変換	87
ゾーン セットの作成とメンバゾーンの追加	88
名前に基づくゾーン、ゾーンセット、およびデバイス エイリアスのフィルタリング	89
複数のゾーンセットへの複数のゾーンの追加	90
ゾーンの実行	90
ゾーンセットの配信	91
フルゾーンセットの配信の有効化	91
DCNM SAN クライアントを使用したフルゾーンセット配信の有効化	92
ワンタイム配信のイネーブル化	92
DCNM SAN クライアントを使用したワンタイム配信の有効化	93
リンクの分離からの回復の概要	94
ゾーンセットのインポートおよびエクスポート	94
DCNM SAN クライアントを使用したゾーンセットのインポートおよびエクスポート	95
ゾーンセットの複製	96
ゾーンセットのコピー	96
DCNM SAN クライアントを使用したゾーンセットのコピー	97
ゾーンのバックアップおよび復元の概要	98
DCNM SAN クライアントを使用したゾーンのバックアップ	98
ゾーンの復元	99
ゾーン、ゾーンセット、およびエイリアスの名前の変更	101
DCNM SAN クライアントを使用したゾーン、ゾーンセット、およびエイリアスの名前の変更	102
ゾーン、ゾーンセット、FC エイリアス、およびゾーン属性グループのコピー	103
DCNM SAN クライアントを使用したゾーン、ゾーンセット、FC エイリアス、およびゾーン属性グループのコピー	103
MDS 以外のデータベースの移行	104
ゾーン サーバー データベースのクリア	104

詳細なゾーン属性	105
ゾーンベースのトラフィック プライオリティの概要	105
ゾーンベースのトラフィック プライオリティの設定	105
DCNM SAN クライアントを使用したゾーンベースのトラフィック 優先順位の構成	107
デフォルト ゾーンの QoS プライオリティ属性の設定	107
DCNM SAN クライアントを使用したデフォルト ゾーンの QoS 優先順位属性の構成	108
デフォルト ゾーン ポリシーの設定	109
スマート ゾーン分割の概要	110
スマート ゾーン分割のメンバー設定	110
VSAN でのスマート ゾーン分割の有効化	111
スマート ゾーン分割のデフォルト値の設定	111
スマート ゾーン分割へのゾーンの自動変換	112
ゾーン メンバーのデバイス タイプの設定	113
スマート ゾーン分割設定の削除	113
基本ゾーン分割モードにおけるゾーン レベルでのスマート ゾーン分割の無効化	114
拡張ゾーン分割モードの VSAN に対するゾーン レベルでのスマート ゾーン分割の無効化	114
DCNM SAN クライアントを使用したゾーン レベルでのスマート ゾーン分割の無効化	115
ゾーン情報の表示	116
拡張ゾーン分割	124
拡張ゾーン分割の概要	124
基本ゾーン分割から拡張ゾーン分割への変更	125
拡張ゾーン分割から基本ゾーン分割への変更	126
拡張ゾーン分割のイネーブル化	126
DCNM SAN クライアントを使用した拡張ゾーン分割の有効化	127
ゾーン データベースの変更	127
ゾーンの保留中差分の自動表示の有効化	128
ゾーン データベース ロックの解除	129
属性グループの作成	129
データベースのマージ	130
マージ プロセス	131

ゾーン マージの分析	141
ゾーン マージ制御ポリシーの設定	142
ゾーンによる FC2 バッファのフラッディングの防止	142
デフォルト ゾーンでのトラフィックの許可または拒否	142
ゾーンのブロードキャスト	143
システムのデフォルト ゾーン分割設定値の設定	144
ゾーンの Generic Service アクセス権限の設定	145
拡張ゾーン情報の表示	145
ゾーン分割構成セッションの制御	147
ゾーン分割セッション制限の構成	148
ダウングレード用のゾーン データベースの圧縮	149
ゾーンおよびゾーンセットの分析	149
ゾーン分割のベスト プラクティス	152
TCAM リージョン	152
ゾーン分割のタイプ	154
フォワーディング エンジン	157
F、TF、NP、および TNP ポート チャネル	162
E および TE ポート チャネルと IVR	163
ゾーン サーバー パフォーマンスの強化	165
ゾーン サーバー - ファイバ チャネル ネーム サーバー共有データベース	165
ゾーン サーバー - FCNS 共有データベースの有効化	166
ゾーン サーバー - FCNS 共有データベースの無効化	166
ゾーン サーバー SNMP 最適化	167
ゾーン サーバー SNMP 最適化の有効化	167
ゾーン サーバー SNMP 最適化の無効化	168
ゾーン サーバー差分配信	168
ゾーン サーバー差分配信の有効化	169
ゾーン サーバー差分配信の無効化	169
デフォルト設定	170

デバイス エイリアスについて	171
デバイス エイリアスのモード	171
注意事項と制約事項	172
モード設定の変更	173
デバイス エイリアス モード配信	174
デバイス エイリアス 差分限定配信	174
デバイス エイリアス 差分限定配信の設定	174
差分限定配信機能が有効なデバイス エイリアスのマージ	175
さまざまなモードのデバイス エイリアスのマージ	176
マージ失敗およびデバイス エイリアス モード不一致の解決	176
デバイス エイリアスの機能	177
デバイス エイリアスの前提条件	177
ゾーン エイリアスとデバイス エイリアスの比較	178
デバイス エイリアス データベース	179
デバイス エイリアスの作成	179
デバイス エイリアスの配布について	180
デバイス エイリアスの作成の概要	180
デバイス エイリアス設定のベスト プラクティスの概要	180
変更のコミット	182
デバイス エイリアスの保留中差分表示の有効化	182
変更の破棄	183
ファブリックのロックの上書き	184
データベースの内容のクリア	184
統計情報のクリア	184
デバイス エイリアスの配布のディセーブル化とイネーブル化	184
レガシー ゾーン エイリアス設定の変換の概要	185
ゾーン エイリアスのインポート	186
デバイス エイリアス統計情報のクリア	187
データベース マージの注意事項	187
デバイス エイリアス設定の確認	188
デフォルト設定	190

デバイスエイリアスのマージ失敗の解決	190
デバイスエイリアスのベストプラクティス	191
デバイスエイリアスの不一致の解決	193
マージ失敗の解決	194
重複するデバイスエイリアス名（デバイスエイリアス名は同じでもpWWNが異なる）の解決	194
重複するpWWN（デバイスエイリアス名が異なっているのにpWWNが同じ）の解決	196
モード不一致の解決	198
検証失敗の解決	200
データベース競合の解決	202
デバイスエイリアスデータベースのステータスの確認	203

第 7 章

ファイバチャネルルーティング サービスおよびプロトコルの設定	205
FSPF の概要	205
FSPF の例	206
フォールトトレラントファブリック	206
冗長リンク	206
PortChannel および FSPF リンクのフェールオーバーシナリオ	207
FSPF のグローバル設定	208
SPF 計算ホールドタイムの概要	208
Link State Record のデフォルトの概要	209
VSAN での FSPF の設定	209
FSPF のデフォルト設定へのリセット	210
FSPF のイネーブル化またはディセーブル化	210
VSAN の FSPF カウンタのクリア	210
FSPF インターフェイスの設定	211
FSPF リンク コストの概要	211
FSPF リンク コストの設定	211
FSPF コスト乗数について	211
FSPF コスト乗数の設定	212

FSPF コスト乗数の表示	213
ハロー タイム インターバルの概要	214
ハロー タイム インターバルの設定	214
デッド タイム インターバルの概要	214
デッド タイム インターバルの設定	215
再送信インターバルの概要	215
再送信インターバルの設定	215
インターフェイス単位での FSPF のディセーブル化	216
特定のインターフェイスに対する FSPF のディセーブル化	216
インターフェイスの FSPF カウンタのクリア	217
FSPF ルート	217
ファイバチャネルルートの概要	217
ブロードキャストおよびマルチキャストルーティングの概要	218
マルチキャストルート スイッチの概要	218
マルチキャストルート スイッチの設定	219
ロード バランシング	219
ロード バランシング スキーム	220
ハッシュ メソッド	221
順序どおりの配信	224
ネットワーク フレーム順序の再設定の概要	225
ポート チャネル フレーム順序の再設定の概要	225
順序どおりの配信のイネーブル化の概要	226
順序どおりの配信のグローバルなイネーブル化	227
特定の VSAN に対する順序どおりの配信のイネーブル化	227
順序どおりの配信のステータスの表示	228
ドロップ遅延時間の設定	228
遅延情報の表示	229
フロー統計情報の設定	229
フロー統計の概要	229
集約フロー統計情報のカウント	230
個々のフロー統計情報のカウント	230

FIB 統計情報のクリア	231
フロー統計情報の表示	231
グローバル FSPF 情報の表示	232
FSPF データベースの表示	232
FSPF インターフェイスの表示	234
デフォルト設定	234

第 8 章

FLOGI、ネーム サーバー、FDMI、および RSCN データベースの管理 237

FLOGI の概要	237
FLOGI スケール最適化	237
FLOGI 休止タイムアウト	238
[Restrictions (機能制限)]	238
FLOGI スケール最適化および休止タイムアウトの有効化	238
FLOGI スケール最適化および休止タイムアウトの無効化	239
FLOGI の詳細の表示	240
ネーム サーバー	242
ネーム サーバーから送信される一括通知	242
ネーム サーバーの一括通知の有効化	242
ネーム サーバーの一括通知の無効化	243
NX-OS リリース 6.2(9) のネーム サーバー一括通知の無効化	243
ネーム サーバーの一括通知の再有効化	244
ネーム サーバー プロキシ登録	244
ネーム サーバー プロキシの登録	244
重複 pWWN の拒否の概要	244
重複 pWWN の拒否	245
ネーム サーバー データベース エントリ	245
ネーム サーバーのデータベース同期の最適化	245
ネーム サーバー データベースのエントリ数の確認	246
ネーム サーバーのデータベース エントリの表示	246
FDMI	248
FDMI の表示	248

VMID	250
VMID に関する注意事項と制約事項	253
VMID サーバーの構成	253
VMID サーバーの有効化	253
VMID サーバーの無効化	254
VMID の範囲の設定	254
例 : VMID サーバーの構成	254
VMID 設定の確認	255
RSCN	258
RSCN 情報の概要	259
RSCN 情報の表示	259
multi-pid オプション	260
multi-pid オプションの設定	260
ドメインフォーマット SW-RSCN の抑制	261
結合 SW-RSCN	261
結合 SW RSCN の有効化	261
結合 SW-RSCN の無効化	262
RSCN 統計情報のクリア	262
CFS を使用した RSCN タイマー設定の配布	263
RSCN タイマーの設定	264
RSCN タイマー設定の確認	265
RSCN タイマー設定の配布	265
RSCN タイマー設定の配布のイネーブル化	266
ファブリックのロック	266
RSCN タイマー設定の変更のコミット	266
RSCN タイマー設定の変更の廃棄	267
ロック済みセッションのクリア	267
RSCN 設定の配布情報の表示	268
デフォルト設定	268
ポート ペーシングの有効化	269

第 9 章

SCSI ターゲットの検出 271

SCSI LUN 検出の概要 271

SCSI LUN 検出の開始について 271

SCSI LUN 検出の開始 272

カスタマイズ検出の開始について 272

カスタマイズ検出の開始 273

SCSI LUN 情報の表示 273

第 10 章

FICON の設定 277

FICON の概要 277

FICON の要件 278

MDS 固有 FICON のメリット 279

VSAN によるファブリックの最適化 279

FCIP のサポート 281

ポートチャネルのサポート 281

VSAN による、FICON と FCP の混在への対応 281

Cisco MDS でサポートされている FICON 機能 282

FICON のカスケード化 284

FICON VSAN の前提条件 284

FICON ポート番号の設定 285

デフォルトの FICON ポート番号設定方式 286

ポートアドレス 290

実装ポートおよび非実装ポートのアドレス 291

予約済み FICON ポート番号設定方式の概要 291

インストレーション ポートおよび非インストレーション ポート 291

FICON ポート番号設定に関するガイドライン 292

スロットへの FICON ポート番号の割り当て 292

FICON ポート番号割り当ての表示 293

FCIP およびポートチャネルのポート番号の概要 293

FICON およびポートチャネル インターフェイス用の FICON ポート番号の予約 294

FC ID の割り当て	295
FICON の設定	295
VSAN の FICON をイネーブルにする操作の概要	295
スイッチでの FICON の有効化	296
基本 FICON 設定のセットアップ	297
VSAN での手動での FICON のイネーブル化	300
[code-page] オプションの設定	301
ホストでスイッチをオフラインに移行できるようにするには	302
ホストで FICON ポートパラメータを変更できるようにするには	302
ホストでタイムスタンプを制御できるようにする	303
タイムスタンプのクリア	304
FICON パラメータの SNMP 制御の設定	304
FICON デバイスの従属関係の概要	304
FICON デバイスの従属関係のクリア	305
実行コンフィギュレーションの自動保存	305
FICON ポートの設定	307
PortChannel へのポート番号のバインド	307
FCIP インターフェイスへのポート番号のバインド	308
ポートブロッキングの設定	308
ポートの禁止	309
ポート禁止のデフォルト状態の設定	310
ポート禁止の設定	310
ポートアドレス名の割り当て	311
RLIR の概要	311
RLIR 優先ホストの指定	312
RLIR 情報の表示	313
RLIR 情報のクリア	317
FICON コンフィギュレーションファイル	317
FICON コンフィギュレーションファイルの概要	318
保存済みコンフィギュレーションファイルの実行コンフィギュレーションへの適用	319
FICON コンフィギュレーションファイルの編集	319

FICON コンフィギュレーション ファイルの表示	320
FICON コンフィギュレーション ファイルのコピー	321
ポート スワッピング	321
ポート スワッピングの概要	322
ポート スワッピング	323
ポート番号が重複しているスイッチのポートのスワッピング	324
FICON テープ アクセラレーション	324
FICON テープ アクセラレーション設定	326
FICON テープ読み取りアクセラレーション設定	327
XRC アクセラレーションの設定	328
FICON VSAN のオフライン状態への移行	329
CUP インバンド管理	329
ゾーンへの CUP の配置	329
制御ユニットの情報の表示	330
FICON 情報の表示	330
FICON アラートの受信	331
FICON ポート アドレス情報の表示	331
FICON コンフィギュレーション ファイル情報の表示	333
設定された FICON の状態の表示	334
ポート管理状態の表示	334
バッファ情報の表示	335
履歴バッファの表示	336
実行コンフィギュレーションの FICON 情報の表示	336
スタートアップ コンフィギュレーションの FICON 情報の表示	337
FICON 関連のログ情報の表示	338
デフォルト設定	338
第 11 章	高度な機能および概念 341
	共通情報モデル (CIM) 341
	ファイバチャネル タイムアウト値 342
	すべての VSAN のタイマー設定 342

VSAN ごとのタイマー設定	343	
fctimer 配信の概要	343	
fctimer 配信の有効化	344	
fctimer 設定変更のコミット	344	
fctimer 設定変更の廃棄	345	
ファブリックのロックの上書き	345	
データベース マージの注意事項	345	
設定された fctimer 値の表示	346	
組織固有識別子	346	
注意事項と制約事項	347	
OUI の追加および削除	347	
OUI の追加と削除の設定例	347	
例：OUI の追加と削除	347	
例：OUI の表示	347	
World Wide Names (WWN)	347	
WWN 情報の表示	348	
リンク初期化 WWN の使用方法	349	
セカンダリ MAC アドレスの設定	349	
HBA の FC ID 割り当て	350	
デフォルトの企業 ID リスト	350	
企業 ID の設定の確認	351	
スイッチの相互運用性	352	
Interop モードの概要	353	
interop モード 1 の設定	355	
interop モード 1 の設定	356	
デフォルト設定	360	
第 12 章	Fibre Channel Common Transport 管理セキュリティの設定	361
	Fibre Channel Common Transport の概要	361
	設定のガイドライン	362
	Fibre Channel Common Transport クエリーの設定	362

Fibre Channel Common Transport 管理セキュリティの確認 363
デフォルト設定 363



はじめに

ここでは、『Cisco MDS 9000 Series Configuration Guide』を使用している対象読者、構成、および表記法について説明します。また、関連資料の入手方法の情報を説明し、次の章にも続きます。

- [対象読者 \(xxi ページ\)](#)
- [表記法 \(xxi ページ\)](#)
- [関連資料 \(xxii ページ\)](#)
- [通信、サービス、およびその他の情報 \(xxiii ページ\)](#)

対象読者

このインストレーションガイドは、電子回路および配線手順に関する知識を持つ電子または電気機器の技術者を対象にしています。

表記法

このマニュアルでは、次の表記法を使用しています。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次のように表しています。



警告 「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。ステートメント 1071。

関連資料

Cisco MDS 9000 シリーズ スイッチのドキュメンテーションには、次のマニュアルが含まれます。

Release Notes

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-release-notes-list.html>

『Regulatory Compliance and Safety Information』

<http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/hw/regulatory/compliance/RCSI.html>

互換性に関する情報

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-device-support-tables-list.html>

インストールおよびアップグレード

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-guides-list.html>

Configuration

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-and-configuration-guides-list.html>

CLI

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-command-reference-list.html>

トラブルシューティングおよび参考資料

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/tsd-products-support-troubleshoot-and-alerts.html>

オンラインでドキュメントを検索するには、次の Web サイトにある Cisco MDS NX-OS Documentation Locator を使用してください。

http://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/doclocator.html

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

Cisco バグ検索ツール

[Cisco Bug Search Tool](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



CHAPTER 1

新機能と更新情報

- [変更点, on page 1](#)

変更点

この章では、このガイドで追加および変更された機能を示します。

Table 1: 新機能および変更された機能

特長	追加または変更された内容	変更が行われたリリース	参照先
デバイス エイリアス	デフォルトのデバイスエイリアスモードが拡張モードに変更されます。	8.5(1)	デバイス エイリアスについて
シングルセッションのゾーン分割	拡張ゾーン分割モードのときに、スイッチで一度に1つの構成セッションのみ許可する新しいオプション。	8.4(2)	ゾーン分割の概要
自動ゾーン	自動ゾーンには、ゾーニングの変更後に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自動的に保存することを有効または無効にするオプションがあり、それぞれ enableautosave および disableautosave オプションを使用します。	8.4(1)	ゾーン分割の概要
自動ゾーン	自動ゾーン機能とは、1つのコマンドでゾーン分割を自動化するメカニズムであり、32 Gbps 以上の速度のファイバチャネルインターフェイスをサポートするファブリックスイッチを最小限の労力で展開することを可能にするメカニズムでもあります。	8.3(1)	ゾーン分割の概要
FLOGI スケール最適化	デフォルトの FLOGI 休止タイムアウト値が 2000 ミリ秒から 0 ミリ秒に変更されました。	8.3(1)	FLOGIの概要

特長	追加または変更された内容	変更が行われたリリース	参照先
仮想マシン識別子 (VMID)	VMIDのサポートにより、SAN ファブリック インフラストラクチャは、仮想マシン (VM) を一意に識別できます。	8.2(1)	FLOGIの概要
FLOGI スケール最適化	FLOGI スケール最適化機能により、ユーザーは、シャーシ全体の FLOGI スケールの上限値を増やすことができます。この機能は、Cisco MDS 9718 ディレクタでのみサポートされます。	8.1(1)	FLOGI スケール最適化, on page 237
ゾーンサーバーの機能拡張	次の機能によりゾーンサーバーのパフォーマンスが強化されました。 <ul style="list-style-type: none"> • ゾーン サーバー FCNS 共有データベース • ゾーン サーバー SNMP 最適化 • ゾーン サーバー 差分配信 	7.3(0)D1(1)	ゾーン分割の概要
デバイスエイリアス差分限定配信	ファブリック内のすべてのスイッチでこの機能を有効にすると、拡張性が向上します。	7.3(0)D1(1)	デバイスエイリアスについて
組織固有識別子	この機能により、組織固有識別子 (OUI) をシステム OUI データベースに動的に追加するための新しいコマンドが導入されました。	7.3(0)D1(1)	組織固有識別子, on page 346
デバイスエイリアスコミットの確認 ゾーンコミットの確認	ゾーンおよびデバイスエイリアスのコミット時に保留中差分の表示が追加されました。	6.2(9)	デバイスエイリアスについて ゾーン分割の概要
FC および FCOE スケール: デバイスエイリアス	「デバイスエイリアス設定のベストプラクティスの概要」の項が追加されました。	6.2(9)	デバイスエイリアスについて
Fibre Channel Common Transport 管理サーバークエリー	Fibre Channel Common Transport 管理サーバークエリーの設定	6.2(9)	Fibre Channel Common Transport 管理セキュリティの設定, on page 361
FCNS、RSCN	FCNS データベース変更をリッスンするすべてのコンポーネントのパフォーマンスを向上する一括通知機能が追加されました。 RSCN のパフォーマンス向上のため結合 SWRSCN が追加されました。	6.2(7)	FLOGIの概要
	「ファブリックスイッチ情報の表示」の項が追加されました。	6.2(7)	ゾーン分割の概要

特長	追加または変更された内容	変更が行われたリリース	参照先
スマートゾーン分割	コマンド出力が追加されました。	6.2(7)	ゾーン分割の概要
スマートゾーン分割	「スマートゾーン分割」の項が追加されました。	5.2.6	ゾーン分割の概要
FICONテープ読み取りアクセラレーション	「FICONテープアクセラレーション」の項が追加されました。	5.0(1a)	FICONの概要



CHAPTER 2

ファブリックの概要

Cisco MDS 9000 ファミリー NX-OS コマンドラインインターフェイス (CLI) では、VSAN、SAN デバイスの仮想化、動的 VSAN、ゾーン、Distributed Device Alias Service、ファイバチャネルルーティングサービスおよびプロトコル、FLOGI、ネームサーバー、FDMI、RSCN データベース、SCSI ターゲット、FICON、その他の高度な機能などの機能を設定および管理できます。

この章では、これらの機能のいくつかについて、次の内容を説明します。

- [仮想 SAN, on page 5](#)
- [ダイナミック ポート VLAN メンバーシップ, on page 6](#)
- [SAN デバイス仮想化, on page 6](#)
- [ゾーン分割, on page 6](#)
- [分散デバイス エイリアス サービス, on page 7](#)
- [ファイバチャネルルーティング サービスおよびプロトコル, on page 8](#)
- [マルチプロトコル サポート, on page 8](#)

仮想 SAN

仮想 SAN (VSAN) テクノロジーは、単一の物理 SAN を複数の VSAN に分割します。VSAN 機能を使用すると、Cisco NX-OS ソフトウェアで、大規模な物理ファブリックを個々の分離された環境に論理的に分割して、ファイバチャネル SAN のスケーラビリティ、アベイラビリティ、管理性、およびネットワークセキュリティを高めることができます。FICON の場合、VSAN により、FICON およびオープンシステムのハードウェアベースの分離が容易になります。

それぞれの VSAN は、独自の一連のファイバチャネルファブリックサービスを持つ論理的および機能的に別個の SAN です。ファブリックサービスのこの分割は、個々の VSAN 内にファブリック設定およびエラー条件を含めることにより、ネットワークの不安定さを大幅に軽減します。VSAN が実現する厳密なトラフィック分離は、特定の VSAN の制御およびデータトラフィックを VSAN 独自のドメイン内に限定することにより、SAN セキュリティを高めるために役立ちます。VSAN は、アベイラビリティを低下させることなく、分離された SAN アイランドを共通のインフラストラクチャに容易に統合できるようにすることで、コスト削減に貢献します。

ユーザーは、特定の VSAN の範囲内に限定される管理者ロールを作成できます。たとえば、ネットワーク管理者ロールは、すべてのプラットフォーム固有の機能を設定できるように設定できます。一方、その他のロールは、特定の VSAN 内だけで設定および管理を行えるように設定できます。この手法は、スイッチ ポートまたは接続されたデバイスの WWN (World Wide Name) に基づいてメンバーシップを割り当てることができる、特定の VSAN に対するユーザー操作の効果を分離することにより、SAN の管理性を高め、人為的エラーを原因とする中断を減らします。

VSAN は、離れた場所にあるデバイスを含めるために VSAN を拡張する、SAN 間の FCIP リンク全体にわたりサポートされます。Cisco MDS 9000 ファミリースイッチは、VSAN のトランッキングも実装します。トランッキングでは、ISL (スイッチ間リンク) によって、同じ物理リンク上で複数の VSAN のトラフィックを伝送できます。

ダイナミック ポート VLAN メンバーシップ

スイッチのポート VSAN メンバーシップは、ポート単位で割り当てられます。デフォルトでは、各ポートはデフォルト VSAN に属します。VSAN をデバイス WWN に基づいて割り当てることにより、VSAN メンバーシップをポートに動的に割り当てることができます。この方法は Dynamic Port VSAN Membership (DPVM) 機能とといいます。DPVM により、柔軟性が高まり、ホストまたはストレージデバイスの接続が 2 つの Cisco MDS スイッチ間またはスイッチ内の 2 つのポート間で移動される場合に、ファブリック トポロジを維持するためにポート VSAN メンバーシップを再設定する必要がなくなります。DPVM ではデバイスが接続されているか、移動されているかに関係なく、設定済みの VSAN を保持します。

SAN デバイス仮想化

Cisco SAN デバイス仮想化 (SDV) では、物理エンドデバイスを表す仮想デバイスを SAN 設定のために使用できます。SAN デバイスの仮想化によって、ハードウェアの交換に要する時間を大幅に削減できます。たとえば、ストレージアレイが SDV を使用せずに交換された場合、SAN ゾーン分割の変更およびホスト オペレーティング システム設定の更新のためにサーバーのダウンタイムが必要になります。SDV を使用すると、ハードウェアの交換後には仮想デバイスと物理デバイス間のマッピングを変更するだけで済み、広範囲の設定変更から SAN とエンドデバイスを分離することができます。



Note SDV は、Cisco MDS NX-OS Release 4.x 以降ではサポートされていません。

ゾーン分割

ゾーン分割は、SAN 内のデバイスのアクセス コントロールを提供します。Cisco NX-OS ソフトウェアは、次の種類のゾーン分割をサポートしています。

- Nポートゾーン分割：エンドデバイス（ホストおよびストレージ）ポートに基づいてゾーンメンバーを定義します。
 - WWN
 - ファイバチャネル ID (FC-ID)
- Fxポートゾーン分割：スイッチポートに基づいてゾーンメンバーを定義します。
 - WWN
 - WWNおよびインターフェイスインデックス、またはドメインIDおよびインターフェイスインデックス
- ドメインIDおよびポート番号（Brocadeの相互運用性用）。
- iSCSIゾーン分割：ホストゾーンに基づいてゾーンメンバーを定義します。
 - iSCSI名
 - IPアドレス
- LUNゾーン分割：Nポートゾーン分割と組み合わせて使用すると、LUNゾーン分割は、特定のホストだけがLUNにアクセスできるようにし、異種ストレージサブシステムアクセスを管理するための単一制御点を提供します。
- 読み取り専用ゾーン：属性を設定して、任意のゾーンタイプでのI/O操作をSCSI読み取り専用コマンドに制限できます。この機能は、バックアップ、データウェアハウジング用などのサーバー間でボリュームを共有する場合に特に役立ちます。



Note LUNゾーン分割および読み取り専用ゾーンは、Cisco MDS NX-OS Release 5.x以降ではサポートされていません。

- ブロードキャストゾーン：任意のゾーンタイプ用の属性を設定して、ブロードキャストフレームを特定のゾーンのメンバーに制限できます。

厳密なネットワークセキュリティを実現するため、入力スイッチで適用されるアクセスコントロールリスト（ACL）を使用して、ゾーン分割はフレームごとに常に適用されます。すべてのゾーン分割ポリシーはハードウェアで適用され、パフォーマンスの低下を引き起こすことはありません。拡張ゾーン分割セッション管理機能では、一度に1人のユーザーだけがゾーンを変更できるようにすることで、セキュリティがさらに高まります。

分散デバイス エイリアス サービス

Cisco MDS 9000 ファミリのすべてのスイッチは、VSAN単位およびファブリック全体でのDistributed Device Alias Service（デバイスエイリアス）をサポートしています。デバイスエイリアス配信により、エイリアス名を手動で再度入力することなく、VSAN間でHBA（ホストバスアダプタ）を移動できます。

ファイバチャネルルーティング サービスおよびプロトコル

Fabric Shortest Path First (FSPF) は、ファイバチャネルファブリックで使用される標準パス選択プロトコルです。FSPF 機能は、どのファイバチャネルスイッチでも、デフォルトでイネーブルになっています。特に考慮が必要な設定を除いて、FSPF サービスを設定する必要はありません。FSPF はファブリック内の任意の2つのスイッチ間の最適パスを自動的に計算します。特に、FSPF は次の機能を実行するために使用されます。

- 任意の2つのスイッチ間の最短かつ最速のパスを確立して、ファブリック内のルートを動的に計算します。
- 指定されたパスに障害が発生した場合に、代替パスを選択します。FSPF は複数のパスをサポートし、障害リンクを迂回する代替パスを自動的に計算します。2つの同等パスを使用できる場合は、推奨ルートを設定します。

マルチプロトコルサポート

ファイバチャネルプロトコル (FCP) のサポートに加え、Cisco NX-OS ソフトウェアでは、単一プラットフォーム内で IBM Fibre Connection (FICON)、Small Computer System Interface over IP (iSCSI)、および Fibre Channel over IP (FCIP) をサポートしています。Cisco MDS 9000 ファミリスイッチでの Native iSCSI のサポートは、顧客が広範囲に及ぶサーバーのストレージを SAN 内の共通プールに統合するのに役立ちます。



CHAPTER 3

VSAN の設定と管理

Cisco MDS 9000 ファミリ スイッチおよび Cisco Nexus 5000 シリーズ スイッチで仮想 SAN (VSAN) を使用すると、ファイバチャネルファブリックでより高度なセキュリティと高い安定性を得ることができます。VSANは同じファブリックに物理的に接続されたデバイスを分離します。VSAN では、一般の物理インフラストラクチャで複数の論理 SAN を作成できます。各 VSAN には最大 239 台のスイッチを組み込みます。それぞれの VSAN は、異なる VSAN で同じファイバチャネル ID (FCID) を同時に使用できる独立したアドレス領域を持ちます。この章は、次の項で構成されています。

- [VSAN について, on page 9](#)
- [VSAN の設定, on page 13](#)
- [スタティック VSAN 設定の表示, on page 22](#)
- [デフォルト設定, on page 23](#)
- [ファブリック スイッチ情報の表示, on page 23](#)

VSAN について

VSAN は、仮想ストレージエリア ネットワーク (SAN) です。SAN は、主に SCSI トラフィックを交換するためにホストとストレージデバイス間を相互接続する専用ネットワークです。SAN では、この相互接続を行うために物理リンクを使用します。一連のプロトコルは SAN 上で実行され、ルーティング、ネーミングおよびゾーン分割を処理します。異なるトポロジで複数の SAN を設計できます。

VSAN を導入することによって、ネットワーク管理者はスイッチ、リンク、および 1 つまたは複数の VSAN を含むトポロジを 1 つ作成できます。このトポロジの各 VSAN では、SAN の動作およびプロパティが同じです。VSAN には次の特徴もあります。

- 複数の VSAN で同じ物理トポロジを共有できます。
- 同じ Fibre Channel ID (FCID) を別の VSAN 内のホストに割り当てて、VSAN のスケールビリティを高めることができます。
- VSAN の各インスタンスは、FSPF、ドメインマネージャ、およびゾーン分割などの必要なすべてのプロトコルを実行します。
- VSAN 内のファブリック関連の設定は、別の VSAN 内の関連トラフィックに影響しません。

- ある VSAN 内のトラフィック中断を引き起こしたイベントはその VSAN 内にとどまり、他の VSAN に伝播されません。

ここでは VSAN について説明します。具体的な内容は次のとおりです。

VSAN トポロジ

Figure 1: 論理 VSAN の区分け, on page 10 と Figure 2: 2 つの VSAN の例, on page 11 の両方に表示されているスイッチアイコンは、これらの機能が Cisco MDS 9000 ファミリのすべてのスイッチに適用されることを示します。

Figure 1: 論理 VSAN の区分け, on page 10 に、3 つのスイッチによるファブリック（各階にスイッチは1つ）を示します。スイッチと接続された装置の地理的な配置は、論理 VSAN の区分けには依存しません。VSAN 間では通信できません。各 VSAN 内では、すべてのメンバが相互に対話できます。

Figure 1: 論理 VSAN の区分け

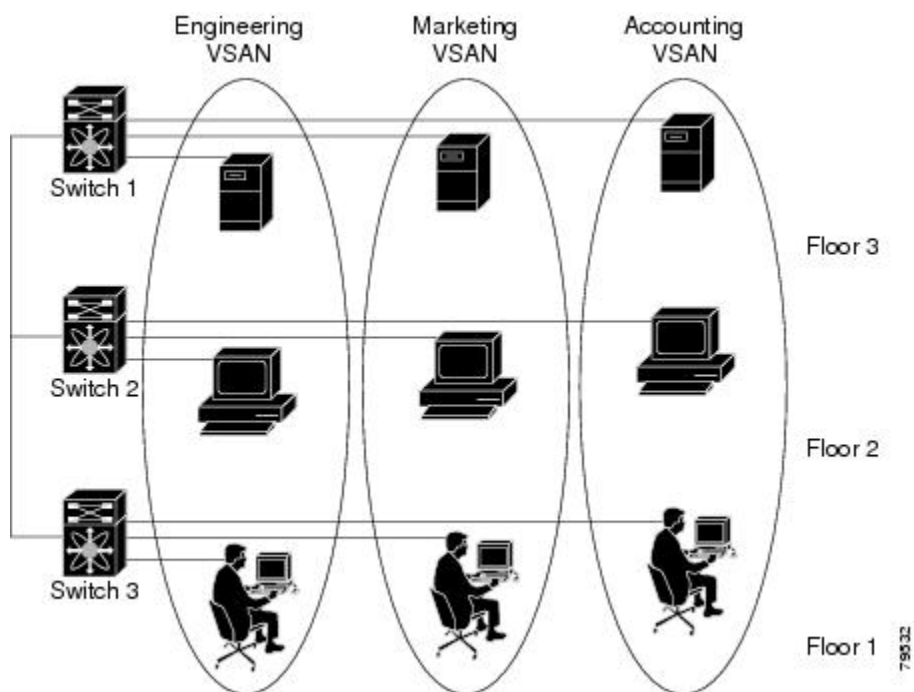
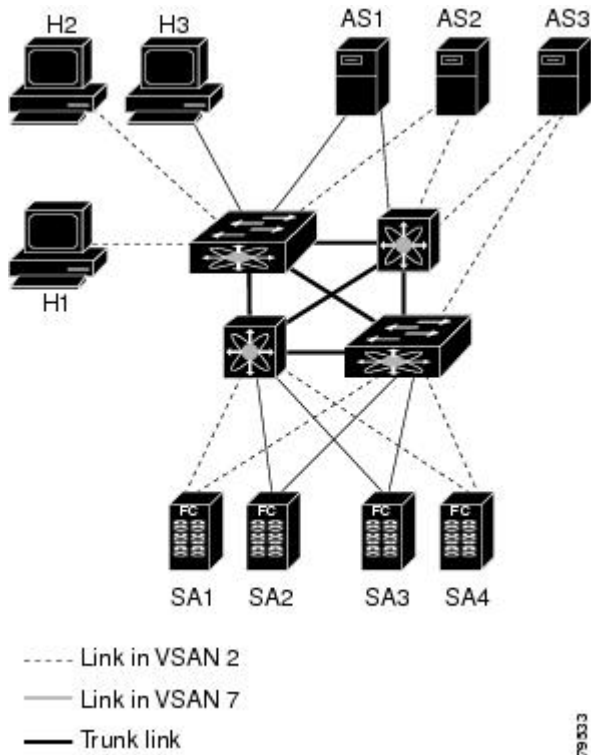


Figure 2: 2 つの VSAN の例, on page 11 に、VSAN 2（破線）と VSAN 7（実線）の2つの定義済み VSAN からなるファイバチャネルスイッチングの物理インフラストラクチャを示します。VSAN 2 には、ホスト H1 と H2、アプリケーションサーバー AS2 と AS3、ストレージアレイ SA1 と SA4 が含まれます。VSAN 7 は、H3、AS1、SA2、および SA3 と接続します。

Figure 2: 2つの VSAN の例



このネットワーク内の4つのスイッチは、VSAN 2 と VSAN 7 の両方のトラフィックを伝送するトランクリンクによって相互接続されます。VSAN 2 と VSAN 7 の両方のスイッチ間トポロジは同じです。これは要件ではないため、ネットワーク管理者は特定のリンクで特定の VSAN をイネーブルにして別の VSAN トポロジを作成できます。

VSAN がもしなれば、SAN ごとに別個のスイッチとリンクが必要です。VSAN をイネーブルにすることによって、同一のスイッチとリンクが複数の VSAN で共有されることがあります。VSAN では、スイッチ精度ではなく、ポート精度で SAN を作成できます。Figure 2: 2つの VSAN の例, on page 11 は、VSAN が物理 SAN で定義された仮想トポロジを使用して相互に通信するホストまたはストレージデバイスのグループであることを表しています。

このようなグループを作成する基準は、VSAN トポロジによって異なります。

- VSAN は、次の条件に基づいてトラフィックを分離できます。
 - ストレージプロバイダー データセンター内の異なるお客様
 - 企業ネットワークの業務またはテスト
 - ローセキュリティおよびハイセキュリティの要件
 - 別個の VSAN によるバックアップトラフィック
 - ユーザートラフィックからのデータの複製
- VSAN は、特定の部門またはアプリケーションのニーズを満たせます。

VSAN の利点

VSAN には、次のような利点があります。

- **トラフィックの分離**：必要に応じて、トラフィックを VSAN 境界内に含み、1 つの VSAN 内だけに装置を存在させることによって、ユーザーグループ間での絶対的な分離を確保します。
- **スケーラビリティ**：VSAN は、1 つの物理ファブリック上でオーバーレイされます。複数の論理 VSAN 層を作成することによって、SAN のスケーラビリティが向上します。
- **VSAN 単位のファブリック サービス**：VSAN 単位のファブリック サービスの複製は、拡張されたスケーラビリティとアベイラビリティを提供します。
- **冗長構成**：同一の物理 SAN で作成された複数の VSAN は、冗長構成を保証します。1 つの VSAN に障害が発生した場合、ホストと装置の間にあるバックアップパスによって、同一の物理 SAN にある別の VSAN に冗長保護が設定されます。
- **設定の容易さ**：SAN の物理構造を変更することなく、VSAN 間でユーザーを追加、移動、または変更できます。ある VSAN から別の VSAN へ装置を移動する場合は、物理的な設定ではなく、ポート レベルの設定だけが必要となります。

最大 256 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN (VSAN 1)、もう 1 つが独立 VSAN (VSAN 4094) です。ユーザー指定の VSAN ID 範囲は 2 ~ 4093 です。

VSAN とゾーン

VSAN に複数のゾーンを定義できます。2 つの VSAN は未接続の 2 つの SAN に相当するので、VSAN 1 のゾーン A は、VSAN 2 のゾーン A とは異なる、別個のものです。[Table 2: VSAN とゾーンの比較](#), on page 12 に、VSAN とゾーンの相違点を示します。

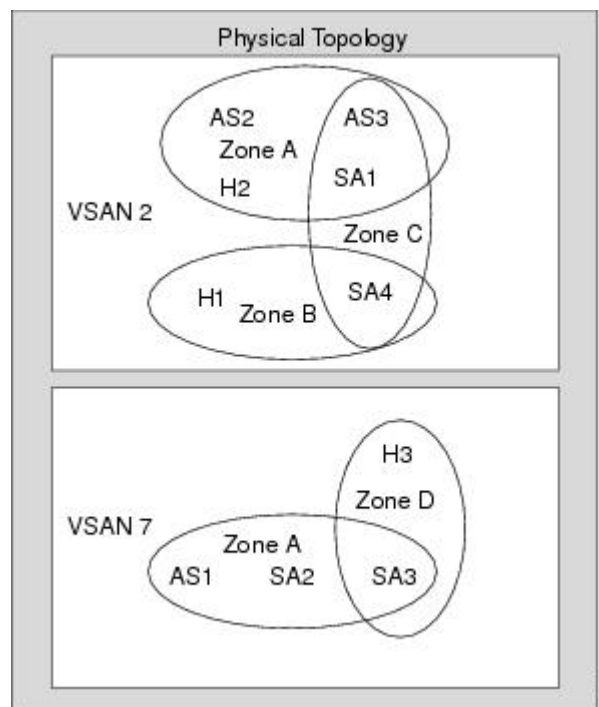
Table 2: VSAN とゾーンの比較

VSAN 特性	ゾーン特性
VSAN は、SAN とルーティング、ネーミング、およびゾーン分割プロトコルが同じです。	ルーティング、ネーミング、およびゾーニングプロトコルは、ゾーン単位で利用できません。
—	ゾーンは、VSAN 内に常に含まれます。ゾーンが 2 つの VSAN にわたることはありません。
VSAN は、ユニキャスト、マルチキャスト、およびブロードキャストトラフィックを制限します。	ゾーンは、ユニキャストトラフィックを制限します。
メンバーシップは、通常 VSAN ID を使用して Fx ポートに定義されます。	メンバーシップは、一般的に pWWN によって定義されません。
HBA またはストレージデバイスは、1 つの VSAN (Fx ポートに対応付けられた VSAN) だけに所属できます。	HBA またはストレージデバイスは、複数のゾーンに所属できます。

VSAN 特性	ゾーン特性
VSAN は、各 E ポート、送信元ポート、および宛先ポートでメンバーシップを実行します。	ゾーンは、送信元ポートおよび宛先ポートだけでメンバーシップを実行します。
VSAN は、規模が大きい環境（ストレージ サービス プロバイダー）で定義されます。	ゾーンは、ゾーンの外部に表示されないイニシエータおよびターゲットのセットで定義されます。
VSAN は、ファブリック全体を網羅します。	ゾーンは、ファブリック エッジで設定されます。

Figure 3: VSAN とゾーン分割, on page 13 に、VSAN とゾーンとの可能な組み合わせを示します。VSAN 2 には、ゾーン A、ゾーン B、ゾーン C の 3 つのゾーンが定義されています。ゾーン C は、ファイバチャネル標準に準拠してゾーン A とゾーン B にオーバーラップしています。VSAN 7 には、ゾーン A とゾーン D の 2 つのゾーンが定義されています。VSAN 境界を越えるゾーンはありません。ゾーン全体が VSAN 内に収まります。VSAN 2 に定義されたゾーン A は、VSAN 7 に定義されたゾーン A とは別個のものです。

Figure 3: VSAN とゾーン分割



VSAN の設定

VSAN には、次の属性があります。

- VSAN ID : VSAN ID は、デフォルト VSAN (VSAN 1)、ユーザー定義の VSAN (VSAN 2 ~ 4093)、および独立 VSAN (VSAN 4094) で VSAN を識別します。

- ステート：VSAN の管理ステートを **active**（デフォルト）または **suspended** ステートに設定できます。VSAN が作成されると、VSAN はさまざまな状態またはステートに置かれます。
 - VSAN の **active** ステートは、VSAN が設定されイネーブルであることを示します。VSAN をイネーブルにすることによって、VSAN のサービスをアクティブにします。
 - VSAN の **suspended** ステートは、VSAN が設定されているがイネーブルではないことを示します。この VSAN にポートが設定されている場合、ポートはディセーブルの状態です。このステートを使用して、VSAN の設定を失うことなく VSAN を非アクティブにします。suspended ステートの VSAN のすべてのポートは、ディセーブルの状態です。VSAN を suspended ステートにすることによって、ファブリック全体のすべての VSAN パラメータを事前設定し、VSAN をただちにアクティブにできます。
- VSAN 名：このテキスト スtring は、管理目的で VSAN を識別します。名前は、1 ～ 32 文字で指定できます。また、すべての VSAN で一意である必要があります。デフォルトでは、VSAN 名は VSAN と VSAN ID を表す 4 桁の String を連結したものです。たとえば、VSAN 3 のデフォルト名は VSAN0003 です。



Note VSAN 名は一意である必要があります。

- ロードバランシング属性：ロードバランシングパスの選択に発信元/宛先 ID（src-dst-id）または Originator Exchange ID（OX ID）（デフォルトでは、src-dst-ox-id）を使用するように指示する属性。



Note 第 1 世代スイッチング モジュールでは、IVR 対応スイッチからの IVR トラフィックに対しては、OX ID ベースのロードバランシングがサポートされませんでした。IVR 非対応の MDS スwitchからの IVR トラフィックに対しては、OX ID ベースのロードバランシングが機能します。第 2 世代のスイッチング モジュールでは、IVR 対応スイッチからの IVR トラフィックに対して、OX ID ベースのロードバランシングがサポートされるようになりました。

ここでは、VSAN の作成および設定方法について説明します。具体的な内容は次のとおりです。

予約済み VSAN 範囲と分離された VSAN 範囲のガイドライン

いずれかのインターフェイスでトランキングが設定されている NPV スwitch、またはトランキング F ポート チャネル機能を有効にするために f port-channel-trunk コマンドが実行される標準スswitchでは、以下の予約済み VSAN と分離された VSAN の設定ガイドラインに従います。

- いずれかのインターフェイスでトランク モードがオンであるか、NP ポートチャネルが稼働している場合、予約済み VSAN は 3040 ～ 4078 であり、ユーザー設定には使用できません。

- Exchange Virtual Fabric Protocol (EVFP) 分離 VSAN は 4079 であり、ユーザー設定には使用できません。

VSAN の作成

VSAN がアクティブの状態、最低 1 つのポートがアップの状態であれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートは設定できません。

VSAN の静的な作成

VSAN を作成する前には、VSAN に対してアプリケーション特有のパラメータを設定できません。

VSAN の作成

VSAN を作成するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **vsan database**

switch(config-vsan-db)#

VSAN に対するデータベースを設定します。アプリケーション特有の VSAN パラメータは、このプロンプトから設定できません。

ステップ 3 switch(config-vsan-db)# **vsan 2**

指定された ID (2) の VSAN が存在しない場合は、指定された ID で VSAN を作成します。

ステップ 4 switch(config-vsan-db)# **vsan 2 name TechDoc**

updated vsan 2

割り当てられた名前でも VSAN を更新します (TechDoc)。

ステップ 5 switch(config-vsan-db)# **vsan 2 suspend**

選択された VSAN を中断します。

ステップ 6 switch(config-vsan-db)# **no vsan 2 suspend**

前のステップで入力した **suspend** コマンドを無効にします。

ステップ 7 switch(config-vsan-db)# **end**

switch#

EXEC モードに戻ります。

ポート VSAN メンバーシップ

スイッチのポート VSAN メンバーシップは、ポート単位で割り当てられます。デフォルトでは、各ポートはデフォルト VSAN に属します。2つの方式のいずれかを使用して、ポートに VSAN メンバーシップを割り当てることができます。

- 静的 : VSAN をポートに割り当てる

[スタティック ポート VSAN メンバーシップの概要, on page 16](#)を参照してください。

- 動的 : デバイスの WWN に基づいて VSAN を割り当てるこの方式は、Dynamic Port VSAN Membership (DPVM) と呼ばれます。

[create_dynamic_vsan.ditamap#map_2861B3F48B334468BB9FBC52B85CC84A](#)を参照してください。

トランキング ポートは、許可リストの一部である VSAN の対応リストを持ちます (『Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide』を参照)。

スタティック ポート VSAN メンバーシップの概要

インターフェイス ポートの VSAN メンバーシップを静的に割り当てるには、次の手順を実行します。

ステップ 1 switch# **config terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **vsan database**

switch(config-vsan-db)#

VSAN に対するデータベースを設定します。

ステップ 3 switch(config-vsan-db)# **vsan 2**

指定された ID (2) の VSAN が存在しない場合は、指定された ID で VSAN を作成します。

ステップ 4 switch(config-vsan-db)# **vsan 2 interface fc1/8**

指定された VSAN (VSAN 2) に、fc1/8 インターフェイスのメンバーシップを割り当てます。

ステップ 5 switch(config-vsan-db)# **vsan 7**

指定された ID (7) の VSAN が存在しない場合は、指定された ID で VSAN を新規に作成します。

ステップ 6 switch(config-vsan-db)# **vsan 7 interface fc1/8**

変更された VSAN を反映させるために、インターフェイスのメンバーシップ情報を更新します。

ステップ7 switch(config-vsantdb)# vsan 1 interface fc1/8

VSAN 7 からインターフェイス fc1/8 を削除し、VSAN 1 (デフォルト VSAN) に割り当てます。

VSAN 7 からインターフェイス fc1/8 の VSAN メンバーシップを削除するには、別の VSAN に対して fc1/8 の VSAN メンバーシップを定義する必要があります。

ベスト プラクティスは、VSAN 1 に割り当て直すことです。

VSAN スタティック メンバーシップの表示

VSAN スタティック メンバーシップ情報を表示するには、**show vsan membership** コマンドを使用します ([指定された VSAN のメンバーシップ情報の表示, on page 17](#) ~ [Displays Static Membership Information for a Specified Interface, on page 17](#) を参照) 。

指定された VSAN のメンバーシップ情報の表示

```
switch # show vsan 1 membership
vsan 1 interfaces:
    fc1/1  fc1/2  fc1/3  fc1/4  fc1/5  fc1/6  fc1/7  fc1/9
    fc1/10 fc1/11 fc1/12 fc1/13 fc1/14 fc1/15 fc1/16 port-channel 99
```



Note インターフェイスがこの VSAN に設定されていない場合は、インターフェイス情報が表示されません。

すべての VSAN のスタティック メンバーシップ情報の表示

```
switch # show vsan membership

vsan 1 interfaces:
    fc2/16 fc2/15 fc2/14 fc2/13 fc2/12 fc2/11 fc2/10 fc2/9
    fc2/8  fc2/7  fc2/6  fc2/5  fc2/4  fc2/3  fc2/2  fc2/1
    fc1/16 fc1/15 fc1/14 fc1/13 fc1/12 fc1/11 fc1/10 fc1/9
    fc1/7  fc1/6  fc1/5  fc1/4  fc1/3  fc1/2  fc1/1

vsan 2 interfaces:
    fc1/8

vsan 7 interfaces:
vsan 100 interfaces:
vsan 4094(isolated vsan) interfaces:
```

Displays Static Membership Information for a Specified Interface

```
switch # show vsan membership interface fc1/1
```

```

fc1/1
  vsan:1
  allowed list:1-4093

```

デフォルト VSAN

Cisco MDS 9000 ファミリのスイッチの出荷時の設定値では、デフォルト VSAN 1 だけがイネーブルにされています。VSAN 1 を実稼働環境の VSAN として使用しないことを推奨します。VSAN が設定されていない場合、ファブリック内のすべてのデバイスはデフォルト VSAN に含まれていると見なされます。デフォルトでは、デフォルト VSAN にすべてのポートが割り当てられています。



Note VSAN 1 は削除できませんが、中断できます。



Note 最大 256 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN (VSAN 1)、もう 1 つが独立 VSAN (VSAN 4094) です。ユーザー指定の VSAN ID 範囲は 2 ~ 4093 です。

分離された VSAN

VSAN 4094 は独立 VSAN です。ポートが属する VSAN が削除された場合、非ランキングポートがすべて、この VSAN に転送されます。これにより、デフォルト VSAN または別の設定済みの VSAN へのポートの暗黙的な転送が回避されます。削除された VSAN のポートはすべて、分離されます (ディセーブルされます)。



Note VSAN 4094 内にポートを設定するか、ポートを VSAN 4094 に移動すると、このポートがすぐに分離されます。



Caution 独立 VSAN を使用してポートを設定しないでください。



Note 最大 256 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN (VSAN 1)、もう 1 つが独立 VSAN (VSAN 4094) です。ユーザー指定の VSAN ID 範囲は 2 ~ 4093 です。

分離された VSAN メンバーシップの概要

`show vsan 4094 membership` コマンドを実行すると、独立 VSAN に関連するすべてのポートが表示されます。

VSAN の動作ステート

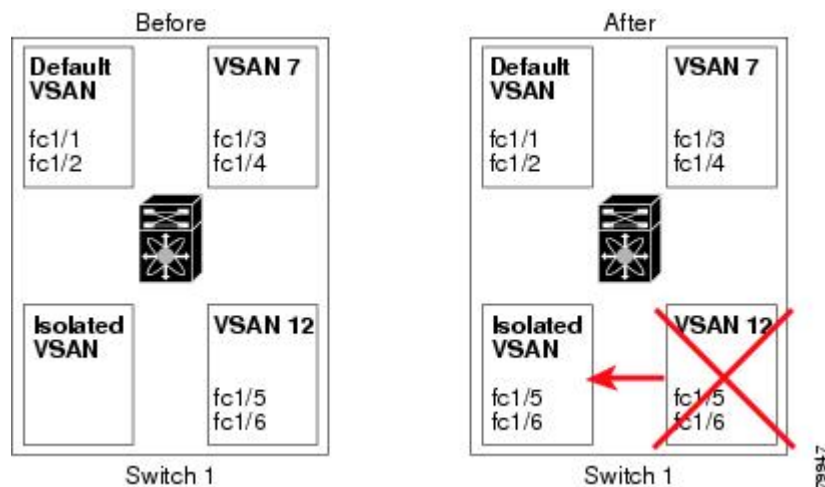
VSAN がアクティブの状態、最低 1 つのポートがアップの状態であれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートは設定できません。

スタティック VSAN の削除

アクティブな VSAN が削除されると、その属性が実行コンフィギュレーションからすべて削除されます。VSAN 関連情報は、次のようにシステム ソフトウェアによって保持されます。

- VSAN 属性およびポートメンバーシップの詳細は、VSAN マネージャによって保持されます。コンフィギュレーションから VSAN を削除すると、この機能が影響を受けます。VSAN が削除されると、VSAN 内のすべてのポートが非アクティブになり、ポートが独立 VSAN に移動されます。同一の VSAN が再作成されると、ポートはその VSAN に自動的に割り当てられることはありません。明示的にポート VSAN メンバーシップを再設定する必要があります (Figure 4: VSAN ポートメンバーシップの詳細, on page 19 を参照)。

Figure 4: VSAN ポートメンバーシップの詳細



- VSAN ベースのランタイム (ネームサーバー)、ゾーン分割、および設定 (スタティック ルート) 情報は、VSAN が削除されると削除されます。
- 設定された VSAN インターフェイス情報は、VSAN が削除されると削除されます。



Note 許可 VSAN リストは、VSAN が削除されても影響を受けません（『Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide』を参照）。

設定されていない VSAN のコマンドは拒否されます。たとえば、VSAN 10 がシステムに設定されていない場合、ポートを VSAN 10 に移動するコマンド要求が拒否されます。

スタティック VSAN の削除

VSAN とその各種属性を削除するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **vsan database**

VSAN データベースを設定します。

ステップ 3 switch(config-db)# **vsan 2**

switch(config-vsan-db)#

VSAN コンフィギュレーションモードを開始します。

ステップ 4 switch(config-vsan-db)# **no vsan 5**

switch(config-vsan-db)#

データベースおよびスイッチから VSAN 5 を削除します。

ステップ 5 switch(config-vsan-db)# **end**

switch#

EXEC モードに戻ります。

ロード バランシング

ロードバランシング属性は、ロードバランシングパス選択に対する発信元/宛先 ID (src-dst-id) または Originator Exchange (OX ID) (デフォルトでは、src-dst-ox-id) の使用を示します。

ロード バランシングの設定

既存の VSAN にロードバランシングを設定するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **vsan database**

switch(config-vsan-db)#

VSAN データベース 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-db)# **vsan 2**

既存の VSAN を指定します。

ステップ 4 switch(config-vsan-db)# **vsan 2 loadbalancing src-dst-id**

選択された VSAN に対してロードバランシングの保証をイネーブルにし、スイッチがパス選択プロセスで送信元/宛先 ID を使用するようになります。

ステップ 5 switch(config-vsan-db)# **no vsan 2 loadbalancing src-dst-id**

前のステップで実行したコマンドを無効にし、ロードバランシング パラメータのデフォルト値に戻します。

ステップ 6 switch(config-vsan-db)# **vsan 2 loadbalancing src-dst-ox-id**

送信元 ID、宛先 ID、OX ID（デフォルト）を使用するようにパス選択設定を変更します。

ステップ 7 switch(config-vsan-db)# **vsan 2 suspend**

選択された VSAN を中断します。

ステップ 8 switch(config-vsan-db)# **no vsan 2 suspend**

前のステップで入力した **suspend** コマンドを無効にします。

ステップ 9 switch(config-vsan-db)# **end**

switch#

EXEC モードに戻ります。

interop モード

相互運用性により、複数ベンダー製品間の相互接続が可能になっています。ファイバチャネル標準規格では、ベンダーに対して共通の外部ファイバチャネルインターフェイスを使用することを推奨しています。 [スイッチの相互運用性](#), [on page 352](#)を参照してください。

FICON VSAN

最大 8 つの VSAN で FICON をイネーブルできます。FICON VSAN の前提条件, on page 284 を参照してください。

スタティック VSAN 設定の表示

設定されている VSAN に関する情報を表示するには、**show vsan** コマンドを使用します(例 [特定の VSAN の設定の表示, on page 22](#) ~ [すべての VSAN の表示, on page 22](#) を参照)。

特定の VSAN の設定の表示

```
switch# show vsan 100
vsan 100 information
  name:VSAN0100 state:active
  in-order guarantee:no interoperability mode:no
  loadbalancing:src-id/dst-id/oxid
```

VSAN の使用状況の表示

```
switch# show vsan usage
4 vsan configured
configured vsans:1-4
vsans available for configuration:5-4093
```

すべての VSAN の表示

```
switch# show vsan
vsan 1 information
  name:VSAN0001 state:active
  in-order guarantee:no interoperability mode:no
  loadbalancing:src-id/dst-id/oxid
vsan 2 information
  name:VSAN0002 state:active
  in-order guarantee:no interoperability mode:no
  loadbalancing:src-id/dst-id/oxid
vsan 7 information
  name:VSAN0007 state:active
  in-order guarantee:no interoperability mode:no
  loadbalancing:src-id/dst-id/oxid
vsan 100 information
  name:VSAN0100 state:active
  in-order guarantee:no interoperability mode:no
  loadbalancing:src-id/dst-id/oxid
vsan 4094:isolated vsan
```

デフォルト設定

Table 3: デフォルト VSAN パラメータ, on page 23 では、設定されたすべての VSAN のデフォルト設定値を示します。

Table 3: デフォルト VSAN パラメータ

パラメータ	デフォルト
デフォルト VSAN	VSAN 1
状態	active ステート
名前	VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 は VSAN0003 です。
ロードバランシング属性	OX ID (src-dst-ox-id)

ファブリック スイッチ情報の表示

特定の VSAN のファブリック内の各スイッチに関する情報を表示するには、**show fabric switch information vsan** コマンドを使用します。

ファブリック内のすべてのスイッチに関する情報の表示

```
switch# show fabric switch information vsan 100
VSAN 1:
-----
SwitchName                Model                Version              SupMemory
-----
huashan12                 DS-C9148-48P-K9     5.2 (2d)             n/a
alishan-bgl-25            DS-C9250I-K9        6.2 (5a)             n/a
Hac18                     DS-C9506             6.2 (7)              2 GB
Hac17                     DS-C9506             6.2 (5)              n/a
Cocol                     DS-C9222I-K9        6.2 (7)              1 GB
switch#
```



Note このコマンドは、Cisco NX-OS Release 6.2(7) より古いリリースではサポートされていません。



Note Cisco NX-OS Release 6.2(7) より古いリリースが稼働しているスイッチでは、SUP メモリは表示されません。



Note VSAN オプションを使用していない場合、このコマンドではすべての VSAN のスイッチに関する情報が表示されます。



CHAPTER 4

ダイナミック VSAN の作成

この章は、次の項で構成されています。

- [DPVM の概要, on page 25](#)
- [DPVM 配信, on page 31](#)
- [DPVM 構成マージのガイドライン, on page 35](#)
- [DPVM 設定の表示, on page 37](#)
- [DPVM の設定例, on page 38](#)
- [デフォルト設定, on page 41](#)

DPVM の概要

スイッチのポート VSAN メンバーシップは、ポート単位で割り当てられます。デフォルトでは、各ポートはデフォルト VSAN に属します。

VSAN をデバイス WWN に基づいて割り当てることにより、VSAN メンバーシップをポートに動的に割り当てることができます。この方法は Dynamic Port VSAN Membership (DPVM) 機能といます。DPVM により、柔軟性が高まり、ホストまたはストレージデバイスの接続が 2 つの Cisco MDS スイッチ間またはスイッチ内の 2 つのポート間で移動される場合に、ファブリック トポロジを維持するためにポート VSAN メンバーシップを再設定する必要がなくなります。デバイスが接続されるか、移動されるかに関係なく、設定済みの VSAN が保持されます。VSAN を静的に割り当てるには、[ダイナミック VSAN の作成, on page 25](#)を参照してください。

DPVM 設定は、Port World Wide Name (pWWN) および Node World Wide Name (nWWN) の割り当てに基づきます。DPVM には、各デバイスの pWWN/nWWN 割り当ておよび対応する VSAN のマッピング情報が含まれます。Cisco NX-OS ソフトウェアは、デバイス FLOGI 中に DPVM アクティブ構成をチェックし、必要な VSAN の詳細を取得します。

pWWN はホストまたはデバイスを識別し、nWWN は複数のデバイスで構成されるノードを識別します。これらの ID のいずれかを割り当てるか、またはこれらの ID の組み合わせを割り当てて、DPVM をマッピングを設定できます。組み合わせると、pWWN が優先されます。

DPVM は、Cisco Fabric Services (CFS) インフラストラクチャを使用して、データベースを効率的に管理および配信できるようにします。DPVM では、アプリケーション駆動の調整済み配信モードが使用され、配信範囲はファブリック全体に及びます (CFS の詳細については、『[Cisco MDS 9000 シリーズ NX-OS System Management Configuration Guide](#)』を参照してください)。



Note DPVM はデバイスアドレス指定への変更を引き起こしません。DPVM はデバイスの VSAN メンバーシップだけに関連し、スイッチ上のいずれのポートでもホストが同じ VSAN メンバーシップを確実に取得するようにします。たとえば、スイッチ上のポートでハードウェア障害が発生した場合は、ホスト接続をスイッチ上の別のポートに移動でき、VSAN メンバーシップを手動で更新する必要はありません。



Note DPVM は FL ポートではサポートされません。DPVM がサポートされるのは F ポートだけです。

ここでは DPVM について、次の内容を説明します。

DPVM 設定の概要

DPVM 機能を設計どおりに使用するには、必ず次の要件が満たされていることを確認してください。

- ダイナミック デバイスが Cisco MDS 9000 シリーズ スイッチに接続するインターフェイスは、F ポートとして構成される必要があります。
- F ポートのスタティック ポート VSAN が有効になっている (分離されたり一時停止されたりしておらず、存在している) 必要があります。
- DPVM データベースのデバイスに対して設定されているダイナミック VSAN が有効になっている (分離されたり一時停止されたりしておらず、存在している) 必要があります。
- デバイス エイリアスは拡張モードにする必要があります。



Note DPVM 機能は、既存のスタティック ポート VSAN メンバーシップ設定を上書きします。ダイナミック ポートに対応する VSAN が削除または一時停止されると、ポートはシャットダウンされます。

DPVM のイネーブル化

DPVM の設定を始めるには、ファブリック内の必要なスイッチで DPVM を明示的にイネーブルにする必要があります。デフォルトでは、この機能は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルになっています。

DPVM の設定および確認コマンドを使用できるのは、スイッチ上で DPVM がイネーブルに設定されている場合だけです。この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

参加しているスイッチの DPVM を有効にするには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **feature dpvm**

スイッチ上で DPVM をイネーブルにします。

ステップ 3 switch(config)# **no feature dpvm**

スイッチ上の DPVM をディセーブルにします（デフォルト）。

Note 重複する pWWN ログインでログイン情報を上書きするには、**dpvm overwrite-duplicate-pwwn** コマンドを入力します。

DPVM デバイス構成（静的）

DPVM デバイス構成は、一連のデバイスマッピングエントリで構成されます。各エントリは、デバイス pWWN または nWWN 割り当て、および割り当てられるダイナミック VSAN で構成されます。最大 16,000 の DPVM エントリを DPVM データベース内で設定できます。このデータベースは、スイッチ全体（およびファブリック）に対してグローバルであり、VSAN ごとには保持されません。

DPVM の構成

DPVM を構成するには、次の手順を実行します。：

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **device-alias mode enhanced**

```
switch(config)# device-alias commit
```

拡張デバイス エイリアス モードを有効にします。

ステップ 3 switch(config)# **dpvm database**

DPVM コンフィギュレーション データベースを作成します。

ステップ 4 switch(config)# **no dpvm database**

(任意) DPVM コンフィギュレーション データベースを削除します。

ステップ 5 switch(config-dpvm-db)# **pwwn 12:33:56:78:90:12:34:56 vsan 100**

指定したデバイス pWWN を VSAN 100 にマッピングします。

ステップ 6 switch(config-dpvm-db)# **no pwwn 12:33:56:78:90:12:34:56 vsan 101**

(任意) DPVM コンフィギュレーション データベースから指定されたデバイス pWWN マッピングを削除します。

ステップ 7 switch(config-dpvm-db)# **nwwn 14:21:30:12:63:39:72:81 vsan 101**

指定したデバイス nWWN を VSAN 101 にマッピングします。

ステップ 8 switch(config-dpvm-db)# **no nwwn 14:21:30:12:63:39:72:80 vsan 101**

(任意) DPVM コンフィギュレーション データベースから指定されたデバイス nWWN マッピングを削除します。

ステップ 9 switch(config-dpvm-db)# **device-alias device1 vsan 102**

指定したデバイス エイリアスを VSAN 102 にマッピングします。

ステップ 10 switch(config-dpvm-db)# **no device-alias device1 vsan 102**

(任意) DPVM コンフィギュレーション データベースから指定されたデバイス エイリアス マッピングを削除します。

ステップ 11 switch(config-dpvm-db)# **show dpvm pending**

(オプション) DPVM 配布が有効になっている場合 (機能が有効になっている場合はデフォルトで有効になっています)、すべての構成変更はコミットされるまで保留されます。このコマンドを使用して、保留中の変更のリストをいつでも表示できます。

ステップ 12 switch(config-dpvm-db)# **dpvm commit**

(オプション) DPVM 配布が有効になっている場合 (機能が有効になっている場合はデフォルトで有効になっています)、構成の変更をコミットするためにこのコマンドが必要です。

ステップ 13 switch(config-dpvm-db)# **show dpvm database**

(オプション) DPVM 静的デバイス構成を表示します。

DPVM のアクティベート

DPVM をアクティブ化すると、DPVM 構成が適用されます。すでにアクティブな構成とアクティブ化する構成との間に競合がある場合、アクティブ化が失敗する可能性があります。アクティブ化を強制的に実行して、矛盾するエントリを上書きできます。

no dpvm activate コマンドを発行して、DPVM 構成を非アクティブ化することもできます。

DPVM をアクティブにするには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **dpvm activate**

DPVM 構成 をアクティベートします。

ステップ 3 switch(config)# **no dpvm activate**

現在アクティブな DPVM 構成を非アクティベートします。

ステップ 4 switch(config)# **dpvm activate force**

DPVM 構成を強制的にアクティブにし、競合するエントリを上書きします。

ステップ 5 switch(config)# **dpvm commit**

DPVM 配布が有効になっている場合（機能が有効になっている場合はデフォルトで有効になっています）、構成の変更をコミットするためにこのコマンドが必要です。

ステップ 6 switch(config)# **show dpvm database active**

（オプション）強制された DPVM デバイス構成を表示します。

DPVM 自動学習

DPVM は、各 VSAN 内の新規デバイスを自動的に学習（自動学習）するように構成できます。DPVM 自動学習は、いつでも有効化または無効化することができます。学習済みエントリは、デバイス pWWN および VSAN に入力することによって作成され、**show dpvm database active** を使用することができます。自動学習を有効にする前に、DPVM をアクティブにする必要があります。

自動学習エントリは手動で削除することもできます。DPVM 自動学習が無効になっている場合、自動学習エントリは永続的になります。



Note 自動学習がサポートされるのは F ポートに接続されているデバイスの場合だけです。DPVM は FL ポートではサポートされていないため、FL ポートに接続されているデバイスは DPVM データベースに入力されません。

学習済みエントリには次の条件が適用されます。

- 自動学習が有効化されているときにデバイスがログアウトした場合、対応する自動学習エントリは、アクティブ DPVM データベースから自動的に削除されます。
- 同じデバイスが異なるポートを通じてスイッチに複数回ログインした場合、最後のログインに対応する VSAN が認識されます。
- 学習済みエントリは、以前に設定されてアクティブにされたエントリを上書きしません。
- 学習は、自動学習をイネーブルにした後に自動学習をディセーブルにするという2つの部分から成るプロセスです。 **auto-learn** オプションがイネーブルの場合、次のようになります。
 - 現在ログインされているデバイスの学習：自動学習がイネーブルにされた時点から行われます。
 - 新規デバイスのログインの学習：新規デバイスがスイッチにログインした時点で行われます。

自動学習の有効化

自動学習を有効にするには、次の手順を実行します。：

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **dpvm auto-learn**

スイッチで自動学習を有効にします。

ステップ 3 switch(config)# **no dpvm auto-learn**

スイッチの自動学習を無効（デフォルト）にします。

ステップ 4 switch(config)# **clear dpvm auto-learn**

自動学習エントリのリストをクリアします。

ステップ 5 switch(config)# **clear dpvm auto-learn pwwn pwwn**

分散 DPVM データベースの自動学習 pWWN エントリのリストをクリアします。

ステップ 6 switch(config)# **dpvm commit**

DPVM 配布が有効になっている場合（機能が有効になっている場合はデフォルトで有効になっています）、DPVM 自動学習への変更は、ローカルおよびファブリックで有効にする前にコミットする必要があります。

学習エントリの消去

2つの方法のいずれかを使用して DPVM エントリをアクティブ DPVM データベースから消去できます（自動学習がイネーブルになっている場合）。

- 1つの自動学習エントリを消去するには、**clear dpvm auto-learn pwwn** コマンドを使用します。

```
switch# clear dpvm auto-learn pwwn 55:22:33:44:55:66:77:88
```

- すべての自動学習エントリを消去するには、**clear dpvm auto-learn** コマンドを使用します。

```
switch# clear dpvm auto-learn
```



Note これらの2つのコマンドはセッションを開始せず、ローカルスイッチ内だけで発行できます。

自動学習の無効化

自動学習を無効にするには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **no dpvm auto-learn**

スイッチの自動学習を無効にします。

- (注) **no dpvm auto-learn** コマンドを実行する前に、ファブリック内の他のスイッチで **dpvm commit** コマンドを実行すると、学習した競合を克服するのに役立ちます。

DPVM 配信

DPVM 構成をファブリック内のすべてのスイッチで使用できる場合、デバイスはどの場所にも移動でき、最も高い柔軟性を発揮します。近接スイッチへのデータベース配信をイネーブル

にするには、データベースが常に管理され、ファブリック内のすべてのスイッチにわたって配信される必要があります。Cisco NX-OS ソフトウェアは、Cisco Fabric Services (CFS) インフラストラクチャを使用して、この要件を満たします（『[Cisco MDS 9000 NX-OS System Management Configuration Guide](#)』を参照）。

このセクションでは DPVM を配信する方法について、次の内容を説明します。

DPVM 配信について

CFS インフラストラクチャを使用して、各 DPVM サーバーは、ISL 起動プロセス中に近接スイッチのそれぞれから DPVM 構成について学習します。ローカルで行われた構成変更はすべてファブリックに配布され、ファブリック内のすべてのスイッチによって更新されます。

DPVM 配布を有効にすると、すべての DPVM 構成の変更が一時的に保存され、**dpvm commit** コマンドの実行時にのみコミットされます。変更には次のタスクが含まれます。

- DPVM デバイス構成の追加、削除、または変更。
- DPVM のアクティブ化または非アクティブ化。
- 自動学習の有効化または無効化。
- DPVM のコピー アクティブ構成

これらの変更は、**dpvm commit** コマンドを使用してファブリック内のすべてのスイッチに配信されます。**dpvm abort** コマンドを使用して変更を破棄することもできます。



Tip 行った一時的な変更は、**show dpvm pending** コマンドまたは **show dovm pending-diff** コマンドで表示できます。

DPVM 配信の無効化

近接スイッチへの DPVM 配信を無効にするには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **no dpvm distribute**

近接スイッチへの DPVM 配信をディセーブルにします。

ステップ 3 switch(config)# **dpvm distribute**

近接スイッチへの DPVM 配信をイネーブルにします（デフォルト）。

ファブリックのロックの概要

既存の構成を変更するときの最初のアクションが実行されると、DPVM 一時ストレージが作成され、ファブリック内の機能がロックされます。一旦ファブリックがロックされると、他のユーザがこの機能の構成に変更を加えることができなくなります。

ファブリックのロック

ファブリックをロックし、変更を DPVM 一時ストレージに適用する手順は、次のとおりです。

ステップ 1 switch# **config terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **dpvm database**

switch(config-dpvm-db)#

DPVM 構成 にアクセスします。

ステップ 3 switch(config-dpvm-db)# **pwwn 11:22:33:44:55:66:77:88 vsan 11**

DPVM 構成に 1 つのエントリを追加します。

ステップ 4 switch(config-dpvm-db)# **exit**

コンフィギュレーション モードに戻ります。

ステップ 5 switch(config)# **dpvm activate**

このコマンドを実行して、最近の構成変更を有効にします。

変更のコミット

dpvm commit コマンドは、ローカルスイッチでこれまでに行われたすべての構成変更をコミットし、構成をファブリック内の他のスイッチにも配布します。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。

DPVM の構成変更をコミットする手順は、次のとおりです。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

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

保留中の変更をコミットします。 **show dpvm pending** または **show dpvm pending-diff** コマンドを使用して変更を表示できます。

変更の破棄

dpvm abort は、これまでに行われたすべての一時的な DPVM 変更を破棄します。構成は影響を受けず、ロックが解除されます。

DPVM の構成変更を廃棄するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **dpvm abort**

DPVM 保留データベースに現在含まれているデータベースエントリを廃棄します。保留中のすべての DPVM 変更を破棄します。

ロック済みセッションのクリア

DPVM ロックが保留されていて、変更をコミットまたは破棄してもリリースされていない場合でも、管理者はファブリック内の任意のスイッチから DPVM セッションをクリアできます。DPVM セッションがクリアされると、保留中のすべての DPVM 変更が破棄され、ファブリック ロックがリリースされます。



Tip 配布が有効になっているときに DPVM に加えられた変更は、構成の変更がコミットまたは破棄されるまで一時的に保留されます。スイッチを再起動すると、構成の変更は破棄されます。

管理者の特権を使用して、ロックされた DPVM セッションを解除するには、EXEC モードで **clear dpvm session** コマンドを使用します。

```
switch# clear dpvm session
```

DPVM 構成マージのガイドライン

DPVM マージは、ファブリック全体の DPVM 構成の結合を指します。CFS マージのサポートの詳細については、『[Cisco MDS 9000 Family NX-OS System Management Configuration Guide](#)』を参照してください。

2つのファブリック間でDPVMデータベースをマージする場合には、次の事項に注意してください。

- 両方のファブリックのアクティブ化および自動学習が同じ状態であることを確認してください。
- それぞれの構成内のデバイスエントリの総数が、16 K を超えていないことを確認してください。



Caution

これらの条件に合わない場合は、マージが失敗します。次の配信が構成とファブリック内のアクティベーションステートを強制的に同期化します。

ここでは、DPVM 構成をマージする方法について説明します。ここで説明する内容は、次のとおりです。

DPVM 構成のコピーについて



Note

ファブリック配布が有効になっており、変更をコミットする必要があります。

DPVM アクティブ構成のコピー

現在アクティブな DPVM 構成をDPVM 静的構成にコピーするには、**dpvm database copy** コマンドを使用します。

```
switch# dpvm database copy active
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
- pwwn 12:33:56:78:90:12:34:56 vsan 100
- nwwn 14:21:30:12:63:39:72:81 vsan 101
```

データベースの差分の比較

次のように DPVM 構成を比較します。

- **dpvm database diff active** コマンドを使用して、アクティブな DPVM 構成を静的な DPVM 構成と比較します。

```
switch# dpvm database diff active
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
- pwnn 44:22:33:44:55:66:77:88 vsan 44
* pwnn 11:22:33:44:55:66:77:88 vsan 11
```

- **dpvm database diff config** コマンドを使用して、静的 DPVM 構成をアクティブ DPVM 構成と比較します。

```
switch# dpvm database diff config
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
+ pwnn 44:22:33:44:55:66:77:88 vsan 44
* pwnn 11:22:33:44:55:66:77:88 vsan 22
```

- **show dpvm pending-diff** コマンドを使用して（CFS 配信が有効の場合）、保留中の DPVM 構成変更と比較します。

DPVM マージのステータスおよび統計情報の表示

DPVM 構成マージの統計を表示するには、次の手順を実行します。

コマンド	目的
switch# show dpvm merge statistics	DPVM 構成マージの統計を表示します。
switch(config)# clear dpvm merge statistics switch(config)#	DPVM 構成マージの統計をクリアします。

次に、DPVM 構成マージでの競合の例を示します。

```
switch# show dpvm merge status
Last Merge Time Stamp      : Fri Aug  8 15:46:36 2008
Last Merge State           : Fail
Last Merge Result          : Fail
Last Merge Failure Reason  : DPVM DB conflict found during merge [cfs_status: 76] Last
Merge Failure Details: DPVM merge failed due to database conflict
Local Switch WWN           : 20:00:00:0d:ec:24:e5:00
Remote Switch WWN          : 20:00:00:0d:ec:09:d5:c0
```

```
-----
Conflicting DPVM member(s)                                Loc VSAN   Rem VSAN
-----
dev-alias dpvm_dev_alias_1 [21:00:00:04:cf:cf:45:ba]      1313       1414
dev-alias dpvm_dev_alias_2 [21:00:00:04:cf:cf:45:bb]      1313       1414
dev-alias dpvm_dev_alias_3 [21:00:00:04:cf:cf:45:bc]      1313       1414
[Total 3 conflict(s)]
rbadri-excal13#
```

次に、DDAS モードでの競合の例を示します。

```

switch# show dpvm merge status
Last Merge Time Stamp      : Fri Aug  8 15:46:36 2008
Last Merge State          : Fail
Last Merge Result         : Fail
Last Merge Failure Reason : DPVM DB conflict found during merge [cfs_status: 76] Last
Merge Failure Details: DPVM merge failed due to DDAS mode conflict
Local Switch WWN          : 20:00:00:0d:ec:24:e5:00
Remote Switch WWN         : 20:00:00:0d:ec:09:d5:c0
Local DDAS mode           : Basic
Remote DDAS mode          : Enhanced

```

DPVM 設定の表示

VSAN 単位で設定されている WWN に関する情報を表示するには、**show dpvm** コマンドを使用します（以下の例を参照）。

DPVM 設定ステータスの表示

```

switch# show dpvm status
DB is activated successfully, auto-learn is on

```

指定された VSAN の現在の DPVM ダイナミック ポートの表示

```

switch# show dpvm ports vsan 10
-----
Interface Vsan Device pWWN                Device nWWN
-----
fc1/2      10    29:a0:00:05:30:00:6b:a0 fe:65:00:05:30:00:2b:a0

```

DPVM 構成の表示

```

switch# show dpvm database
pwnn 11:22:33:44:55:66:77:88 vsan 11
pwnn 22:22:33:44:55:66:77:88 vsan 22
pwnn 33:22:33:44:55:66:77:88 vsan 33
pwnn 44:22:33:44:55:66:77:88 vsan 44
[Total 4 entries]

```

DPVM アクティブ構成の表示

```

switch# show dpvm database active
pwnn 11:22:33:44:55:66:77:88 vsan 22
pwnn 22:22:33:44:55:66:77:88 vsan 22
pwnn 33:22:33:44:55:66:77:88 vsan 33
[Total 3 entries]
* is auto-learnt entry

```

DPVM 構成の表示

```

switch# show dpvm database
pwnn 11:22:33:44:55:66:77:88 vsan 11
pwnn 22:22:33:44:55:66:77:88 vsan 22
pwnn 33:22:33:44:55:66:77:88 vsan 33

```

```
pwn 44:22:33:44:55:66:77:88 vsan 44
[Total 4 entries]
```

DPVM 構成に関して保留中の変更を表示します

```
switch# show dpvm pending-diff
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
+ pwn 55:22:33:44:55:66:77:88 vsan 55
- pwn 11:22:33:44:55:66:77:88 vsan 11
* pwn 44:22:33:44:55:66:77:88 vsan 44
```

DPVM の設定例

基本的な DPVM シナリオを設定するには、次の手順を実行します。

ステップ 1 DPVM をイネーブルにし、DPVM 配信をイネーブルにします。

Example:

```
switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# feature dpvm
switch1(config)# end

switch1# show dpvm database
switch1# show dpvm database active
switch1# show dpvm status
```

この段階では、構成にアクティブ DPVM 構成がなく、**auto-learn** オプションはディセーブルです。

ステップ 2 ヌル（空の）構成をアクティブにして、自動学習されたエントリが入力されるようにします。

Example:

```
switch1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# dpvm activate
switch1(config)# dpvm commit
switch1(config)# end

switch1# show dpvm database

switch1# show dpvm database active

switch1# show dpvm status
```

この段階では、データベースが正常にアクティブ化され、**auto-learn** オプションはディセーブルのままです。

ステップ 3 **auto-learn** オプションを有効にし、構成の変更をコミットします。

Example:

```

switch1# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
switch1(config)# dpvm auto-learn
switch1(config)# dpvm commit
switch1(config)# end

switch1# show dpvm database active
pwn 21:00:00:e0:8b:0e:74:8a vsan 4(*)
pwn 21:01:00:e0:8b:2e:87:8a vsan 5(*)
[Total 2 entries]
* is auto-learnt entry
switch1# show dpvm ports
-----
Interface   Vsan      Device pWWN      Device nWWN
-----
fc1/24      4         21:00:00:e0:8b:0e:74:8a  20:00:00:e0:8b:0e:74:8a
fc1/27      5         21:01:00:e0:8b:2e:87:8a  20:01:00:e0:8b:2e:87:8a
switch1# show flogi database
-----
INTERFACE  VSAN      FCID              PORT NAME              NODE NAME
-----
fc1/24     4         0xe70100          21:00:00:e0:8b:0e:74:8a  20:00:00:e0:8b:0e:74:8a
fc1/27     5         0xe80100          21:01:00:e0:8b:2e:87:8a  20:01:00:e0:8b:2e:87:8a
Total number of flogi = 2.
switch195# show dpvm status
DB is activated successfully, auto-learn is on

```

この時点で、現在ログインしているデバイス（および現在の VSAN 割り当て）が、アクティブ DPVM 構成に入力されます。ただし、エントリーは、アクティブ DPVM 構成で永続的なものではありません。

show dpvm ports および **show flogi database** コマンドの出力には、ログインしている他の 2 台のデバイスが表示されます（この設定例では、switch9 および switch3）。

ステップ 4 switch9 にアクセスし、次のコマンドを実行します。

Example:

```

switch9# show dpvm database active
pwn 21:00:00:e0:8b:0e:87:8a vsan 1(*)
pwn 21:01:00:e0:8b:2e:74:8a vsan 1(*)
[Total 2 entries]
* is auto-learnt entry
switch9# show dpvm status
DB is activated successfully, auto-learn is on

```

ステップ 5 switch3 にアクセスし、次のコマンドを実行します。

Example:

```

switch3# show dpvm database active
pwn 21:00:00:e0:8b:0e:76:8a vsan 1(*)
pwn 21:01:00:e0:8b:2e:76:8a vsan 1(*)
[Total 2 entries]
* is auto-learnt entry
switch3# show dpvm status
DB is activated successfully, auto-learn is on

```

ステップ 6 switch1 で自動学習を無効にし、設定変更をコミットします。

Example:

```
switch1# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
switch1(config)# no dpvm auto-learn
switch1(config)# dpvm commit
switch1(config)# end

switch1# show dpvm status
DB is activated successfully, auto-learn is off
switch1# show dpvm database active
pwwn 21:00:00:e0:8b:0e:74:8a vsan 4
pwwn 21:01:00:e0:8b:2e:87:8a vsan 5
pwwn 21:00:00:e0:8b:0e:87:8a vsan 1
pwwn 21:01:00:e0:8b:2e:74:8a vsan 1
pwwn 21:00:00:e0:8b:0e:76:8a vsan 1
pwwn 21:01:00:e0:8b:2e:76:8a vsan 1
[Total 6 entries]
* is auto-learnt entry
switch1# show dpvm status
DB is activated successfully, auto-learn is off
```

この時点で、自動学習エントリは、アクティブ DPVM 構成で永続的なエントリになりました。

ステップ7 switch9 にアクセスし、次のコマンドを実行します。

Example:

```
switch9# show dpvm database active
pwwn 21:00:00:e0:8b:0e:87:8a vsan 1
pwwn 21:01:00:e0:8b:2e:74:8a vsan 1
pwwn 21:00:00:e0:8b:0e:76:8a vsan 1
pwwn 21:01:00:e0:8b:2e:76:8a vsan 1
pwwn 21:00:00:e0:8b:0e:74:8a vsan 4
pwwn 21:01:00:e0:8b:2e:87:8a vsan 5
[Total 6 entries]
* is auto-learnt entry
switch9# show dpvm status
DB is activated successfully, auto-learn is off
```

ステップ8 switch3 にアクセスし、次のコマンドを実行します。

Example:

```
switch3# show dpvm database active
pwwn 21:00:00:e0:8b:0e:76:8a vsan 1
pwwn 21:01:00:e0:8b:2e:76:8a vsan 1
pwwn 21:00:00:e0:8b:0e:87:8a vsan 1
pwwn 21:01:00:e0:8b:2e:74:8a vsan 1
pwwn 21:00:00:e0:8b:0e:74:8a vsan 4
pwwn 21:01:00:e0:8b:2e:87:8a vsan 5
[Total 6 entries]
* is auto-learnt entry
switch3# show dpvm status
DB is activated successfully, auto-learn is off
```

Note これらの基本手順は、情報がファブリック内のすべてのスイッチで同じであることを確認するのに役立ちます。

これで、Cisco MDS 9000 シリーズ スイッチで基本的な DPVM シナリオを構成しました。

デフォルト設定

[Table 4: デフォルトの DPVM パラメータ](#), [on page 41](#) に、DPVM パラメータのデフォルト設定を示します。

Table 4: デフォルトの DPVM パラメータ

パラメータ	デフォルト
DPVM	ディセーブル
DPVM 配信	イネーブル
自動学習	ディセーブル



CHAPTER 5

ゾーンの設定と管理

ゾーン分割により、ストレージ デバイス間またはユーザー グループ間でアクセス コントロールの設定ができます。ファブリックで管理者権限を持つユーザーは、ゾーンを作成してネットワークセキュリティを強化し、データ損失またはデータ破壊を防止できます。ゾーン分割は、送信元/宛先 ID フィールドを検証することによって実行されます。

FC-GS-4 および FC-SW-3 標準で指定された高度なゾーン分割機能が提供されています。既存の基本ゾーン分割機能または規格に準拠した高度なゾーン分割機能のどちらも使用できます。

- [機能情報の確認 \(44 ページ\)](#)
- [ゾーン構成およびゾーン管理の機能履歴 \(44 ページ\)](#)
- [ゾーン分割の概要, on page 45](#)
- [自動ゾーン \(53 ページ\)](#)
- [ゾーン設定, on page 64](#)
- [ゾーンセットと FC エイリアス, on page 73](#)
- [ゾーンセットの配信, on page 91](#)
- [ゾーンセットの複製, on page 96](#)
- [詳細なゾーン属性, on page 105](#)
- [ゾーン情報の表示, on page 116](#)
- [拡張ゾーン分割, on page 124](#)
- [ゾーン分割構成セッションの制御 \(147 ページ\)](#)
- [ダウングレード用のゾーン データベースの圧縮, on page 149](#)
- [ゾーンおよびゾーンセットの分析, on page 149](#)
- [ゾーン分割のベスト プラクティス, on page 152](#)
- [ゾーン サーバー パフォーマンスの強化, on page 165](#)
- [ゾーン サーバー SNMP 最適化, on page 167](#)
- [ゾーン サーバー差分配信, on page 168](#)
- [デフォルト設定, on page 170](#)

機能情報の確認

ご使用のソフトウェアリリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、<https://tools.cisco.com/bugsearch/>の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、「新機能および変更された機能に関する情報」の章、またはこの章の「機能の履歴」表を参照してください。

ゾーン構成およびゾーン管理の機能履歴

新規および変更された機能を示します。

表 5: 新機能および変更された機能

機能名	リリース	機能情報
自動ゾーン	8.5(1)	<ul style="list-style-type: none"> 自動ゾーンのゾーンでサポートされるデバイスの最大数が 250 に増えました。 VSAN 1 以外の他の VSAN で自動ゾーンを有効にできるようになりました。 <p>autozone --enable --vsan id コマンドが変更されました。</p>
シングルセッションのゾーン分割	8.4(2)	<p>拡張ゾーン分割モードのシングルセッション オプションが導入されました。</p> <p>次のコマンドが変更されました。</p> <ul style="list-style-type: none"> [no] zone mode enhanced vsan id [single-session] show zone status vsan id
自動ゾーン	8.4(1)	<p>enableautosave および disableautosave オプションが autozone コマンドに追加され、ゾーン分割の変更後に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自動的に保存することが有効化または無効化することができます。</p> <p>次のコマンドが導入されました。</p> <ul style="list-style-type: none"> autozone --enable autozone --enableautosave autozone --disableautosave

機能名	リリース	機能情報
自動ゾーン	8.3(1)	<p>自動ゾーン機能が導入されました。</p> <p>次のコマンドが導入されました。</p> <ul style="list-style-type: none"> • autozone --delete • autozone --disable • autozone --help • autozone --show • autozone --showpending • autozone --update

ゾーン分割の概要

ゾーン分割には、次の機能があります。

- ゾーンは、複数のゾーン メンバで構成されます。
 - ゾーンのメンバ同士はアクセスできますが、異なるゾーンのメンバ同士はアクセスできません。
 - ゾーン分割がアクティブでない場合、すべてのデバイスがデフォルトゾーンのメンバとなります。
 - ゾーン分割がアクティブの場合、アクティブ ゾーン（アクティブ ゾーンセットに含まれるゾーン）にないデバイスがデフォルト ゾーンのメンバーとなります。
 - ゾーンのサイズを変更できます。
 - デバイスは複数のゾーンに所属できます。
- ゾーンセットは、1つまたは複数のゾーンで構成されます。
 - ゾーンセットは、単一エンティティとしてファブリックのすべてのスイッチでアクティブまたは非アクティブにできます。
 - アクティブにできるのは、常に1つのゾーンセットだけです。
 - 1つのゾーンを複数のゾーンセットのメンバーにできます。
 - MDS スイッチあたりの最大ゾーンセット数は 1000 です。
- ゾーン分割は、ファブリックの任意のスイッチから管理できます。
 - 任意のスイッチからゾーンをアクティブにした場合、ファブリックのすべてのスイッチがアクティブゾーンセットを受信します。また、ファブリック内のすべてのスイッ

ちにフル ゾーン セットが配布されます（この機能が送信元スイッチでイネーブルである場合）。

- 既存のファブリックに新しいスイッチが追加されると、新しいスイッチによってゾーンセットが取得されます。
- ゾーンの変更を中断せずに設定できます。影響を受けないポートまたはデバイスのトラフィックを中断させることなく、新しいゾーンおよびゾーンセットをアクティブにできます。
- ゾーンメンバーシップ基準は、WWN または FC ID に基づきます。
 - Port World Wide Name (pWWN) : スwitchに接続された N ポートの pWWN をゾーンのメンバとして指定します。
 - ファブリック pWWN : ファブリック ポートの WWN (スイッチ ポートの WWN) を指定します。このメンバーシップは、ポートベース ゾーン分割とも呼ばれます。
 - FCID : スwitchに接続された N ポートの FCID をゾーンのメンバとして指定します。
 - インターフェイスおよび Switch WWN (sWWN) : sWWN によって識別されたスイッチのインターフェイスを指定します。このメンバーシップは、インターフェイスゾーン分割とも呼ばれます。
 - インターフェイスおよびドメイン ID : ドメイン ID によって識別されたスイッチのインターフェイスを指定します。
 - ドメイン ID およびポート番号 : MDS ドメインのドメイン ID を指定し、他社製スイッチに属するポートを追加指定します。
 - IPv4 アドレス : 接続されたデバイスの IPv4 アドレス (およびオプションでサブネットマスク) を指定します。
 - IPv6 アドレス : 接続された複数のデバイスをコロンで区切った 16 進表記の 128 ビットの IPv6 アドレス。
 - シンボル ノード名 : メンバー シンボル ノード名を指定します。最大長は 240 文字です。
- デフォルト ゾーン メンバーシップには、特定のメンバーシップとの関係を持たないすべてのポートまたは WWN が含まれます。デフォルトゾーンメンバ間のアクセスは、デフォルト ゾーン ポリシーによって制御されます。

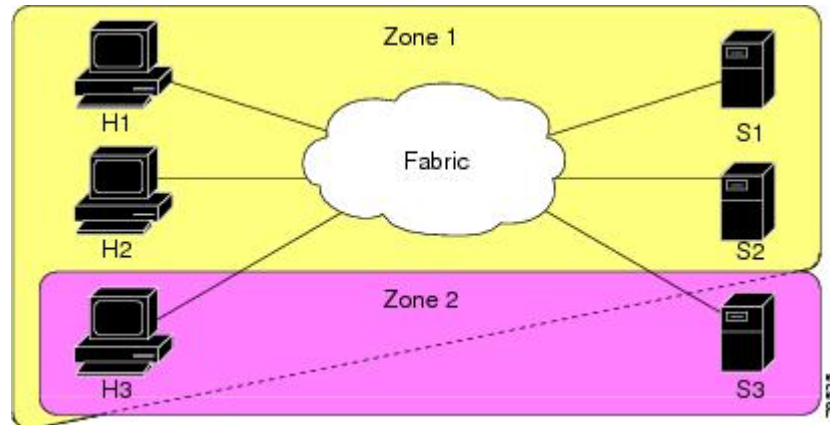
**Note**

ゾーン、ゾーンメンバー、およびゾーンセットの数の設定時の制限については、『[Cisco MDS NX-OS Configuration Limits](#)』を参照してください。

ゾーン分割の例

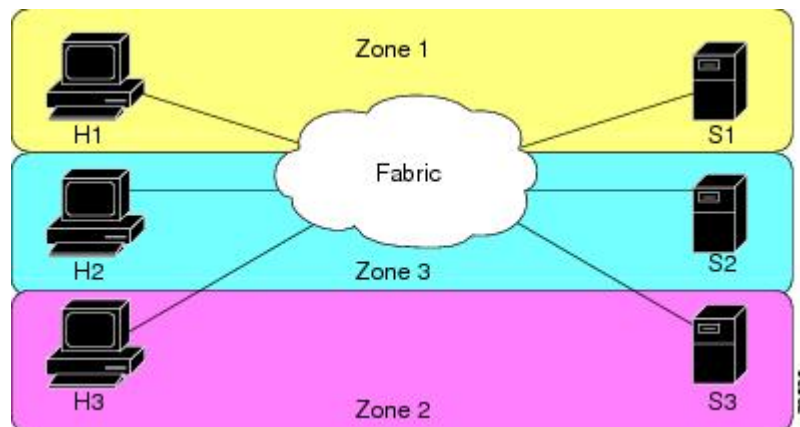
Figure 5: 2つのゾーンによるファブリック , on page 47 に、ファブリックの2つのゾーン（ゾーン1およびゾーン2）で構成されるゾーンセットを示します。ゾーン1は、3つすべてのホスト（H1、H2、H3）からストレージシステムS1とS2に存在するデータへのアクセスを提供します。ゾーン2では、S3のデータにH3からだけアクセスできます。H3は両方のゾーンに存在することに注意してください。

Figure 5: 2つのゾーンによるファブリック



このファブリックをゾーンに分割する方法は他にもあります。**Figure 6: 3つのゾーンによるファブリック** , on page 47 に、その他の方法を示します。新しいソフトウェアをテストするために、ストレージシステムS2を分離する必要があると想定します。これを実行するために、ホストH2とストレージS2だけを含むゾーン3が設定されます。ゾーン3ではアクセスをH2とS2だけに限定し、ゾーン1ではアクセスをH1とS1だけに限定できます。

Figure 6: 3つのゾーンによるファブリック



ゾーン実装

Cisco MDS 9000 シリーズのすべてのスイッチは、以下の基本ゾーン機能を自動的にサポートします（追加の設定は不要です）。

- ゾーンが VSAN に含まれます。
- ハード ゾーン分割をディセーブルにできません。
- ネーム サーバー クエリーがソフト ゾーン分割されます。
- アクティブ ゾーン セットだけが配布されます。
- ゾーン分割されていないデバイスは、相互にアクセスできません。
- 各 VSAN に同一名のゾーンまたはゾーン セットを含めることができます。
- 各 VSAN には、フル データベースとアクティブ データベースがあります。
- アクティブ ゾーン セットを変更するには、フル ゾーン データベースをアクティブ化する必要があります。
- アクティブ ゾーン セットは、スイッチの再起動後も維持されます。
- フル データベースに加えた変更は、明示的に保存する必要があります。
- ゾーンを再アクティブ化（ゾーン セットがアクティブの状態、別のゾーン セットをアクティブ化する場合）しても、既存のトラフィックは中断しません。

必要に応じて、さらに次のゾーン機能を設定できます。

- VSAN 単位ですべてのスイッチにフル ゾーン セットを伝播します。
- ゾーン分割されていないメンバのデフォルト ポリシーを変更します。
- VSAN を `interop` モードに設定することによって、他のベンダーと相互運用できます。相互に干渉することなく、同じスイッチ内で 1 つの VSAN を `interop` モードに、別の VSAN を基本モードに設定することもできます。
- E ポートを分離状態から復旧します。

ゾーンメンバー設定に関する注意事項

ゾーンのすべてのメンバーは互いに通信できます。メンバー数が N のゾーンの場合、 $N*(N-1)$ のアクセス権限をイネーブルにする必要があります。単一ゾーン内にターゲットまたは発信元を多数設定しないことを推奨します。多数設定してしまうと、実際には互いに通信することのない通信ペア（発信側と発信側間、ターゲットとターゲット間）の多くがプロビジョニング/管理の対象となるため、スイッチリソースの浪費になります。この理由から、1つの発信側に対して1つのターゲットを設定するのが最も効率的なゾーン分割方法といえます。

ゾーンメンバーを作成するときは、以下の注意事項について検討する必要があります。

- ゾーンに対して1つの発信側と1つのターゲットだけ設定すると、スイッチリソースの使用率が最も効率的になります。
- 複数のターゲットに同じ発信側を設定することは許容されます。
- 複数のターゲットに複数の発信側を設定することは推奨されません。

- インターフェイスに基づいてゾーンメンバーを設定するときには、ファブリック内でインターフェイス数が最も多い可能性があるファブリックスイッチを常に選択してください。

アクティブゾーンセットおよびフルゾーンセットに関する考慮事項

ゾーンセットを設定する場合は、次の点に注意してください。

- 各 VSAN は、複数のゾーンセットを持つことができますが、アクティブにできるのは常に1つのゾーンセットだけです。
- ゾーンセットを作成すると、そのゾーンセットは、フルゾーンセットの一部となります。
- ゾーンセットがアクティブな場合は、フルゾーンセットのゾーンセットのコピーがゾーン分割に使用されます。これは、アクティブゾーンセットと呼ばれます。アクティブゾーンセットは変更できません。アクティブゾーンセットに含まれるゾーンは、アクティブゾーンと呼ばれます。
- 管理者は、同一名のゾーンセットがアクティブであっても、フルゾーンセットを変更できます。ただし、加えられた変更が有効になるのは、再アクティブ化したときです。
- アクティブ化が実行されると、永続的なコンフィギュレーションにアクティブゾーンセットが自動保存されます。これにより、スイッチのリセットにおいてもスイッチはアクティブゾーンセット情報を維持できます。
- ファブリックのその他すべてのスイッチは、アクティブゾーンセットを受信するので、それぞれのスイッチでゾーン分割を実行できます。
- ハードおよびソフトゾーン分割は、アクティブゾーンセットを使用して実装されます。変更は、ゾーンセットのアクティブ化によって有効になります。
- アクティブゾーンセットに含まれない FC ID または Nx ポートは、デフォルトゾーンに所属します。デフォルトゾーン情報は、他のスイッチに配信されません。



Note 1つのゾーンセットがアクティブな場合に、別のゾーンセットをアクティブにすると、現在アクティブなゾーンセットが自動的に非アクティブになります。新しいゾーンセットをアクティブにする前に、現在のアクティブゾーンセットを明示的に非アクティブにする必要はありません。

次の図に、アクティブにされたゾーンセットに追加されるゾーンを示します。

Quick Config ウィザードの使用



(注) Quick Config ウィザードは、スイッチ インターフェイス ゾーン メンバーだけをサポートします。

Cisco SAN-OS Release 3.1(1) および NX-OS Release 4.1(2) 以降では、Cisco MDS 9124 スイッチの Quick Config ウィザードを使用して VSAN ごとにゾーン メンバーの追加または削除を行えます。Quick Config ウィザードを使用してインターフェイススペースのゾーン分割を実行し、Device Manager を使用して複数の VSAN にゾーン メンバーを割り当てることができます。



(注) Quick Config ウィザードは、Cisco MDS 9124、MDS 9134、MDS 9132T、MDS 9148、MDS 9148S、MDS 9148T、MDS 9396S、および MDS 9396T ファブリック スイッチ、Cisco Fabric Switch for HP c-Class BladeSystem、ならびに Cisco Fabric Switch for IBM BladeCenter でサポートされます。



注意 Quick Config ウィザードは、スイッチで既存のゾーン分割が定義されていないスタンドアロン スイッチでだけ使用できます。

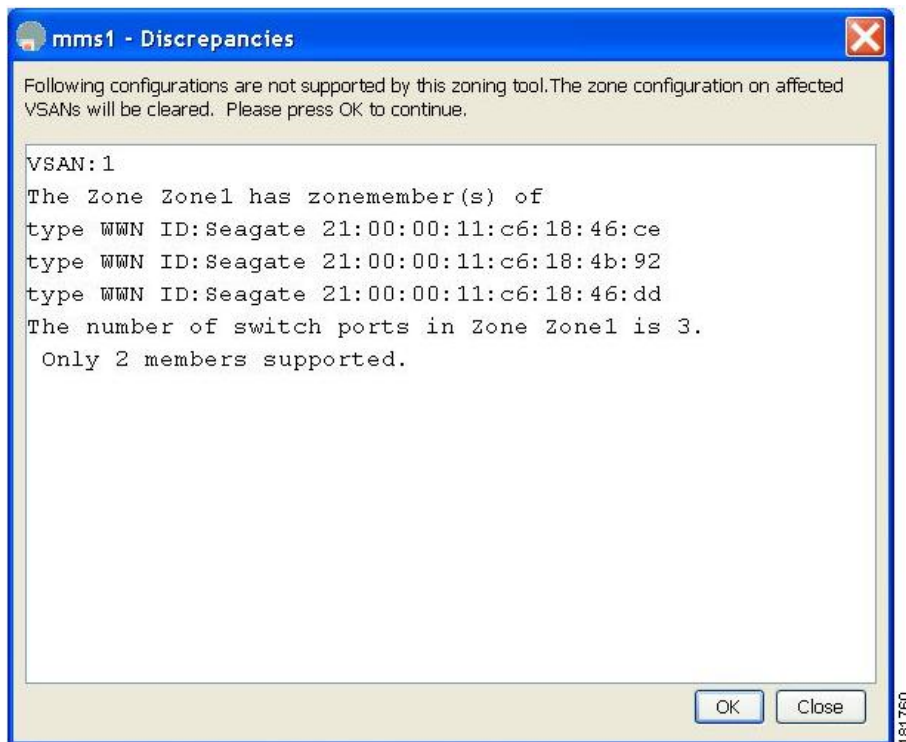
Cisco MDS 9124 スイッチで Device Manager を使用して、ゾーンにポートを追加またはゾーンからポートを削除し、特定の VSAN 内のデバイスだけをゾーン分割する手順は、次のとおりです。

ステップ 1 [FC] > [Quick Config] を選択するか、またはツールバーの [Zone] アイコンをクリックします。

すべてのコントロールがディセーブルになっている Quick Config ウィザード ([図 8 : Quick Config ウィザード \(52 ページ\)](#)) を参照) およびすべてのサポートされていない設定を表示する [Discrepancies] ダイアログボックス ([図 7 : \[Discrepancies\] ダイアログボックス \(51 ページ\)](#)) を参照) が表示されます。

(注) [Discrepancies] ダイアログボックスは、矛盾がある場合だけ表示されます。

図 7: [Discrepancies] ダイアログボックス

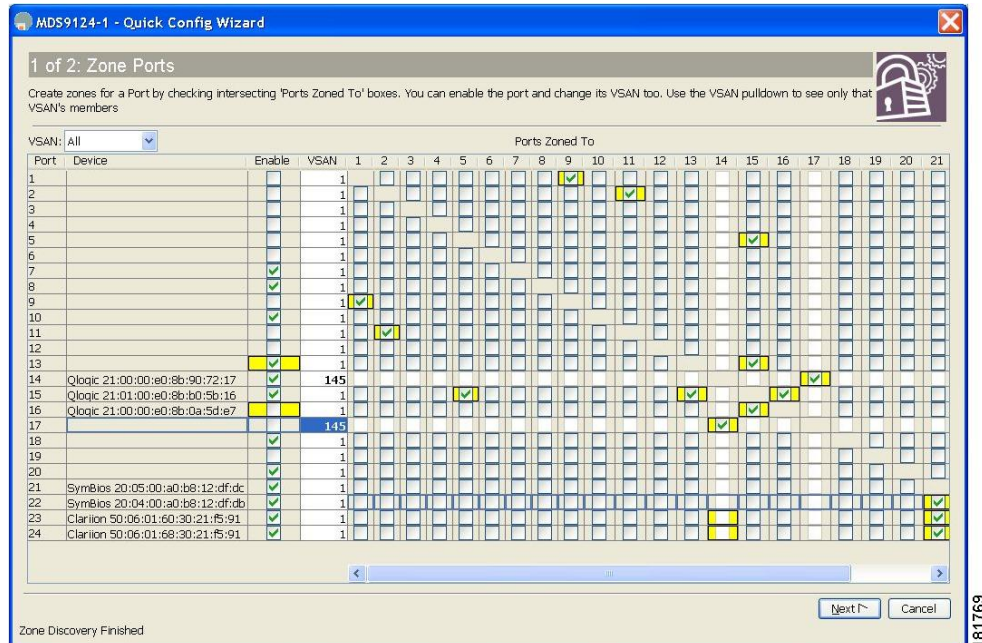


ステップ 2 [OK] をクリックして作業を続行します。

[Quick Config Wizard] ダイアログボックスが表示されます (図 8: Quick Config ウィザード (52 ページ) を参照)。

- (注) 不一致があり、[OK] をクリックした場合、ゾーン データベースで影響を受ける VSAN は削除されます。このため、スイッチが使用中の間、中断が生じることがあります。

図 8: Quick Config ウィザード



ステップ 3 ゾーンに追加する、またはゾーンから削除するポートの [Ports Zoned To] 列のチェックボックスをオンにします。一致するポートのチェックボックスが同様に設定されます。選択されたポートペアがゾーンに追加またはゾーンから削除され、2 デバイス ゾーンが作成されます。

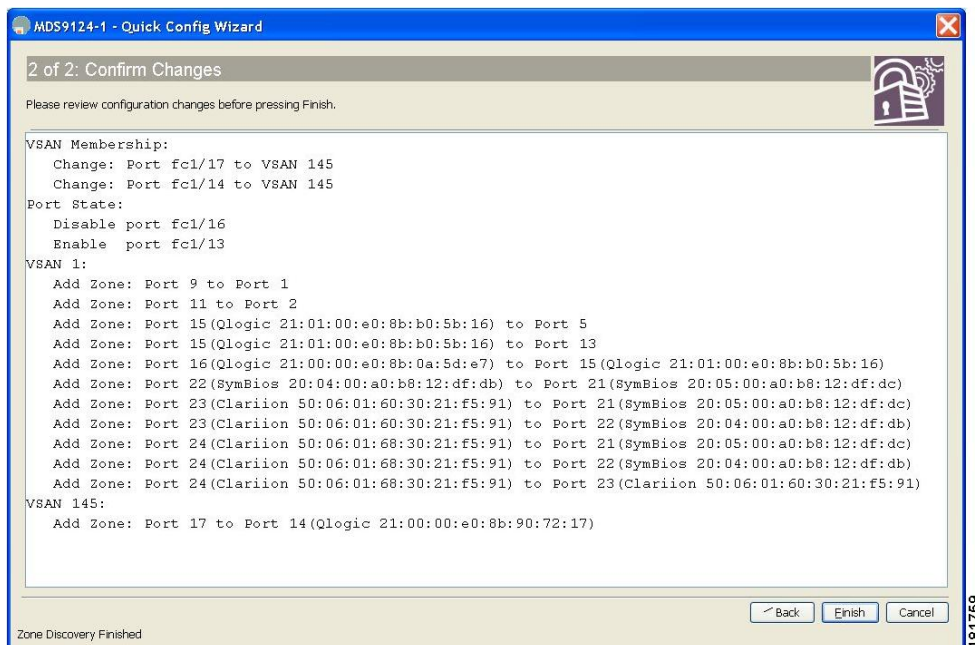
[VSAN] ドロップダウン メニューには、選択された VSAN 内のデバイスだけをゾーン分割できるフィルタが用意されています。

ステップ 4 列の表示と非表示を切り替えるには、列の名前を右クリックします。

ステップ 5 [Next] をクリックして変更の確認を行います。

[Confirm Changes] ダイアログボックスが表示されます (図 9: [Confirm Changes] ダイアログボックス (53 ページ) を参照)。

図 9: [Confirm Changes] ダイアログボックス



ステップ 6 CLI コマンドを表示する場合は、このダイアログボックスを右クリックして、ポップアップメニューで [CLI Commands] をクリックします。

ステップ 7 設定変更を保存するには、[Finish] をクリックします。

自動ゾーン

自動ゾーン機能は、デバイスのゾーン分割を自動化するメカニズムです。この機能を使用すると、デバイスが SAN に追加されるたびにスイッチゾーン構成を手動で作成および更新する一連の管理作業が、1 回のコマンドの実行に簡素化されます。管理者は、初期展開後に自動ゾーン機能を設定する必要がありますが、新しいデバイスがファブリックに追加されるたびにゾーン設定を手動で変更または修正する必要はありません。自動ゾーン機能は、接続されているデバイスが 100 台以下の単一のファブリックスイッチで構成されるファブリックを対象としています。

自動ゾーンは、最初に、各デバイスによって登録された FC4 タイプに基づいて、すべてのイニシエータからすべてのターゲットへの接続を可能にするゾーン分割を設定します。作成されたゾーンは、VSAN 1 内の 1 つのゾーンセットに配置され、アクティブ化されます。自動モードでは、5 分ごとに新しくログインしたデバイスをスキャンするスケジューラジョブが作成されます。新しいイニシエータはすべてのターゲットとともにゾーン分割され、新しいターゲットはすべてのイニシエータとともにゾーン分割されます。その後、新しいゾーンがアクティブゾーンセットに追加されます。このプロセスにより、新しいデバイスを接続するだけで、そのデバイスの自動接続性が数分以内に実現されるため、最小限の労力でスイッチを管理できます。新しくログインしたデバイスへの接続がその後の定期スキャンまでに必要な場合は、管理

者が手動で自動ゾーンを実行できます。自動ゾーンでは、自動ゾーンによって作成された、または管理者によって手動で作成された既存のゾーンは変更されません。これにより、自動ゾーンによる既存のゾーンの重複が防止されるとともに、管理者が特別なゾーンを手動で追加することが可能になります。

自動ゾーンには次の2つの動作モードがあります。

- 自動モード：自動ゾーン スケジューラ ジョブが5分ごとに実行されることにより、デバイス ログインの変更が確認され、それに応じてゾーンセットが更新されます。
- 手動モード：スケジューラ ジョブは作成されません。管理者は、新しいデバイスがスイッチに接続されるたびに **autozone --update** コマンドを実行して、そのデバイスをゾーン分割設定に追加する必要があります。

自動ゾーンに関する注意事項と制約事項

- Cisco MDS 9132T、MDS 9148T、および MDS 9396T ファブリック スイッチでのみ機能します。
- 単一スイッチのファブリックでのみ機能します。
- Cisco MDS NX-OS リリース 8.5(1) 以降、自動ゾーンは VSAN 1 以外の VSAN で有効にできますが、スイッチごとに1つの VSAN でのみ有効にできます。
- Cisco MDS NX-OS リリース 8.4(2b) 以前のリリースでは、自動ゾーンは VSAN 1 にログオンしているポートに対してのみ機能します。管理者がポートを別の VSAN に移動すると、それらが自動ゾーンで VSAN 1 に戻されたり、ゾーン分割されることはありません。
- 自動ゾーンが AUTOZONESET とは異なる名前のアクティブなゾーンセットを検出した場合、自動ゾーンは既存のゾーン構成を変更せずにメッセージを表示して終了します。
- 自動ゾーンによって Inter-Switch Link (ISL) が検出されると、メッセージが表示されて自動ゾーンが終了し、ゾーンは作成されません。
- デフォルト ゾーンが有効になっている場合、自動ゾーンは機能しません。
- 自動ゾーン機能では、FC4 タイプが *init* または *target* として登録されているデバイスだけが考慮されます。Cisco MDS NX-OS リリース 8.4(2) 以降、*both* として登録されているデバイスは *init* と *target* の両方と見なされるため、自動ゾーン機能はこれらのデバイスを *init*、*target*、および *both* として登録するデバイスでゾーン分割します。その他のタイプは無視されるため、管理者が手動でゾーン分割する必要があります。
- Cisco MDS NX-OS リリース 8.5(1) 以降、自動ゾーン機能は最大 250 のデバイスをゾーン分割します。Cisco MDS NX-OS リリース 8.5(1) より前のリリースでは、自動ゾーン機能により最大 100 個のデバイスがゾーン分割されます。
- 自動ゾーン機能はスマートゾーン分割をサポートしていません。
- VSAN 間ルーティング (IVR) 機能を使用する場合は、自動ゾーン機能を有効にしないでください。

- 自動ゾーンでは `AUTOZONE_<SwitchSerialNumber>_<number>` という形式でゾーン名が作成されるため、この形式の名前の手動ゾーンは作成しないでください。 `autozone --delete` コマンドを使用すると、この形式の名前を持つゾーンが自動ゾーンによって削除されます。
- 自動ゾーンを自動モードで初めて実行すると、「`AUTOZONE_SCHEDULER_JOB`」というスケジューラ ジョブと「`AUTOZONE_SCHEDULER_SCHEDULE`」というスケジュールが作成され、`autozone --update` コマンドが5分ごとに実行されます。スケジューラ ジョブまたはスケジュールが管理者によって削除されると、自動ゾーンによる定期的なゾーン更新は中止されます。
- 自動ゾーンが有効になっていて、ゾーン ロックまたはゾーンの単一セッション ロックが取得された場合は、`clear zone lock vsan` コマンドを使用してゾーン ロックをクリアしてから、自動ゾーン構成を再試行する必要があります。
- 自動ゾーンが自動モードで設定されているときに `show accounting log` コマンドを実行すると、自動ゾーン スケジューラ ジョブが実行されるたびに、コマンド フィールドが空のエントリが生成されます。これは予想どおりの結果です。
- 自動ゾーン機能をサポートする Cisco NX-OS リリースでは、スイッチの起動時に「`autozone`」という名前の CLI エイリアスが作成されます。 `autozone --enable` コマンドが実行されなくても、この設定の変更により、アップグレード時に「`Unsaved configuration`」という警告が表示されます。以降のアップグレード時にこのメッセージが表示されないように、必ず設定を保存してください。ベストプラクティスとして、アップグレードの前にスイッチで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することをお勧めします。
- 自動ゾーン機能が有効になっている場合、Cisco MDS NX-OS リリース 8.3(1) から自動ゾーン機能をサポートしていない以前のリリースにダウングレードすると、自動ゾーンのスケジューラ ジョブが新規のデバイス ログインを5分ごとにチェックするようになります。ただし、新規のデバイス ログインが検出されると、スケジューラ ジョブは失敗し、`syslog` が生成されます。そのため、ダウングレードの前に自動ゾーンを無効にすることをお勧めします。
- 自動ゾーン機能が有効になっている場合、Cisco MDS NX-OS リリース 8.4(1) から自動ゾーン機能をサポートしていない以前のリリースにダウングレードすると、 `autozone --enable` CLI エイリアス コマンドが使用可能になります。ただし、コマンドを実行すると失敗します。 `autozone` CLI エイリアス名は `cli alias name autozone` コマンドを使用して削除できます。
- このガイドで説明しているとおりに自動ゾーンが機能するように、 `autozone` CLI エイリアス名は削除しないでください。
- 自動ゾーン機能が有効になっている場合、アップグレード時またはダウングレード時に、自動ゾーン スケジューラ ジョブが一時的に失敗することがあります。アップグレードまたはダウングレードが完了すると、スケジューラ ジョブは正常に実行されるようになります。

自動モードでの自動ゾーンの設定

自動ゾーン機能により、ゾーン分割されていないデバイスに関して VSAN 1 にゾーンとゾーンセットが作成され、VSAN 1 に新しいデバイス ログインを定期的に追加するスケジューラジョブが作成されます。

自動モードでの自動ゾーンの有効化

始める前に

[自動ゾーンに関する注意事項と制約事項 \(54 ページ\)](#) を確認してください。

`autozone` を有効にして、ゾーンを自動的に作成し、それらをゾーンセットに追加し、必要に応じて 5 分ごとにゾーンセットをアクティブ化します。

```
switch# autozone --enable --vsan id
```

(注) `--vsan id` はオプションで、デフォルトは VSAN 1 です。

自動保存を有効にする

ゾーン分割の変更後に、自動ゾーンが `running-configuration` を `startup-configuration` に自動的に保存できるようにするには、次の手順を実行します。

始める前に

自動モードでの自動ゾーンの有効化

自動ゾーン構成の自動保存を有効にします。

```
switch# autozone --enableautosave
```

手動モードでの自動ゾーンの実行

新しいデバイスがスイッチにログインするたびにゾーン分割情報を更新するために、自動ゾーンを手動で実行できます。

自動ゾーンを手動モードで実行するには、次の手順を実行します。

```
switch# autozone --update
```

リモート認証 (AAA) ユーザーによる自動ゾーンの自動モードでの有効化

自動ゾーン スケジューラ ジョブは、スイッチで自動ゾーン機能を有効にしたユーザーのアイデンティティを使用して実行されます。このユーザーがリモート認証 (AAA) を持つ場合、定

期的な自動ゾーン スケジューラ ジョブを成功させるには、ユーザーのクレデンシャルをスケジューラ設定に手動で追加する必要があります。

リモート認証ユーザーに関して自動ゾーン機能を有効にするには、次の手順を実行します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
switch# configure
```

ステップ 2 コマンド スケジューラを有効にします。

```
switch(config)# feature scheduler
```

ステップ 3 リモート認証ユーザーのクリアテキスト パスワードを設定します。

```
switch(config)# scheduler aaa-authentication user name password password
```

ステップ 4 VSAN にゾーンとゾーンセットを自動作成し、新しいデバイス ログインを確認するタイマーをスケジュールします。

```
switch(config)# autozone --enable --vsan id
```

(注) **--vsan id** はオプションで、デフォルトは VSAN 1 です。

自動保存の無効化

ゾーン分割の変更後に、自動ゾーンが `running-configuration` を `startup-configuration` に自動的に保存しないようにするには、次の手順を実行します。

自動ゾーン構成の自動保存を無効にします。

```
switch# autozone --disableautosave
```

自動ゾーンの自動モードの無効化

新しいデバイスが自動的にゾーン分割され、既存のゾーン設定を保持しないようにするには、次のコマンドを実行します。

```
switch# autozone --disable
```

すべてのゾーン設定の表示

自動ゾーンのステータス、自動ゾーンによって作成された既存のゾーンおよびゾーンセットの設定、現在スイッチにログインしていてゾーン分割されていないデバイスに対して自動ゾーンが作成するゾーン分割設定を表示するには、次のコマンドを実行します。

```
switch# autozone --show
```

保留中のゾーン設定の表示

自動ゾーン スケジューラ ジョブが実行される前にゾーン分割されていないデバイスに関して自動ゾーンによって設定されたゾーン設定の変更だけを表示するには、次のコマンドを実行します。

```
switch# autozone --showpending
```

保留中のゾーン設定の適用（手動モード）

デフォルトでは、自動ゾーン機能が有効になっている場合、自動ゾーン スケジューラ ジョブが5分ごとに自動実行されます。ただし、必要に応じて、この5分周期の間に自動ゾーンを強制的に実行したり、自動ゾーンスケジューラジョブを作成せずに自動ゾーンを実行するには、次のコマンドを実行します。

```
switch# autozone --update
```

自動ゾーンによって作成されたゾーンおよびゾーン セットの削除

VSAN 1 で自動ゾーンによって作成されたすべてのゾーンおよびゾーン セットを削除するには、次のコマンドを実行します。

```
switch# autozone --delete
```



(注) 自動ゾーンによって作成されたゾーンおよびゾーン セットを削除しても、自動ゾーン機能は無効になりません。自動ゾーン機能を無効にするには、**autozone --disable** コマンドを使用します。**autozone --delete** コマンドを使用する前に **autozone --disable** コマンドを使用することをお勧めします。これは、自動ゾーンが有効になっており、デバイスがまだ接続されている場合、自動ゾーンによってすべてのゾーンが再設定されるためです。必要に応じて、**autozone --disable --delete** コマンドを使用して両方のオプションをいっしょに使用できます。

例：自動ゾーンの設定

次の例は、automatic モードで自動ゾーンを有効にする方法を示しています。このモードでは、現在ログインしているすべてのデバイスがゾーン分割され、新しいログインが定期的に自動追加されます。この例では、適切な FC4 タイプを持たないデバイスが検出され、ゾーン設定には含まれません。

```
switch# autozone --enable --vsan 1
This command will automatically create and activate single-initiator and single-target
zones for all end-devices currently logged-in to VSAN 1; all initiators will be zoned
to all targets. This may lead to a large TCAM and RSCN load on the switch. Please use
AutoZone judiciously.

AutoZone feature is enabled

Device with pwnn 10:00:00:de:fb:74:e8:31 is not registered with FC4-type Init or Target.
```

```
Hence, it will be ignored for AutoZone configuration.
Configuring zones for vsan 1
    AUTOZONE_JPG21190082_1

Configuring zoneset for vsan 1
Activating the zoneset. Please wait...
Configured zoneset AUTOZONESET for vsan 1 successfully.
```

次の例は、VSAN 2 での **automatic** モードで自動ゾーンを有効にする方法を示していません。

```
switch# autozone --enable --vsan 2
This command will automatically create and activate single-initiator and single-target
zones for all end-devices currently logged-in to VSAN 2; all initiators will be zoned
to all targets. This may lead to a large TCAM and RSCN load on the switch. Please use
AutoZone judiciously.

AutoZone feature is enabled

Device with pwwn 10:00:00:de:fb:74:e8:31 is not registered with FC4-type Init or Target.
Hence, it will be ignored for AutoZone configuration.
Configuring zones for vsan 2
    AUTOZONE_JPG21190082_1

Configuring zoneset for vsan 2
Activating the zoneset. Please wait...
Configured zoneset AUTOZONESET for vsan 2 successfully.
```

次の例は、自動ゾーンスケジューラ ジョブを作成せず、自動ゾーン機能を 1 回実行して、VSAN 1 にログインしているゾーン分割されていないすべてのデバイスをゾーン分割し、それらを VSAN 1 のアクティブゾーンセットに追加する方法を示していません。適切な FC4 タイプを持たないデバイスが検出され、ゾーン設定には含まれません。

```
switch# autozone --update
Device with pwwn 10:00:00:de:fb:74:e8:31 is not registered with FC4-type Init or Target.
Hence, it will be ignored for AutoZone configuration.
Configuring zones for vsan 1
    AUTOZONE_JPG21190082_1
    AUTOZONE_JPG21190082_2
    AUTOZONE_JPG21190082_3
    AUTOZONE_JPG21190082_4

Configuring zoneset for vsan 1
Activating the zoneset. Please wait...
Configured zoneset AUTOZONESET for vsan 1 successfully.
```

次の例は、既存のゾーン設定を維持しつつ、新しくログインしたデバイスがゾーン分割されないように自動ゾーン機能を無効にする方法を示しています。

```
switch# autozone --disable
This will disable the AutoZone feature. Do you wish to continue? [y/n]|y: y

AutoZone feature disabled successfully.
```

次の例は、VSAN 1 に関して作成された自動ゾーンおよびゾーン セットを削除する方法を示しています。

```
switch# autozone --delete
Checking if zoneset name AUTOZONESET present on switch...[Found]
Checking if AutoZone is enabled on switch...[Disabled]

This option will only delete the zone/zoneset configurations done by AutoZone feature.
Do you wish to continue? [n]|y: y
Deleting zoneset name AUTOZONESET and all zones for vsan 1 configured by AutoZone
Deleting following zones -
  AUTOZONE_JPG21190082_1
  AUTOZONE_JPG21190082_2
  AUTOZONE_JPG21190082_3
  AUTOZONE_JPG21190082_4
Deactivating zoneset for vsan 1.
Deactivated zoneset for vsan 1.
```

自動ゾーン設定の確認

次の例には、自動ゾーンのステータスと、自動ゾーンによって作成済みのゾーンおよび作成されていない（保留中の）ゾーンが表示されています。

```
switch# autozone --show
Feature AutoZone : Enabled
AutoSave Configuration : Enabled
The possible zone/zoneset configuration with AutoZone feature for currently logged-in
devices is :
zoneset name AUTOZONESET vsan 1
  zone name AUTOZONE_JPG21190082_1 vsan 1
    member pwn 20:00:00:11:0d:97:00:01
    member pwn 20:01:00:11:0d:97:01:01
  zone name AUTOZONE_JPG21190082_2 vsan 1
    member pwn 20:00:00:11:0d:97:00:01
    member pwn 20:01:00:11:0d:97:01:00
  zone name AUTOZONE_JPG21190082_3 vsan 1
    member pwn 20:00:00:11:0d:97:00:00
    member pwn 20:01:00:11:0d:97:01:01
  zone name AUTOZONE_JPG21190082_4 vsan 1
    member pwn 20:00:00:11:0d:97:00:00
    member pwn 20:01:00:11:0d:97:01:00
```

次の例は、自動ゾーンがゾーン分割されていないデバイスに関して作成したゾーン分割設定を確認し、それらの変更を適用する方法を示しています。この例では、自動ゾーンが無効になっているため、ゾーン分割は1回しか更新されず、自動ゾーンによる定期的なゾーン分割は行われません。

```
switch# autozone --showpending
Feature AutoZone : Disabled
zoneset name AUTOZONESET vsan 1
  zone name AUTOZONE_JPG21190082_1 vsan 1
    member pwn 20:00:00:11:0d:97:00:00
    member pwn 20:01:00:11:0d:97:01:00

switch# autozone --update
Configuring zones for vsan 1
```

```

AUTOZONE_JPG21190082_1
Configuring zoneset for vsan 1
Activating the zoneset. Please wait...
Configured zoneset AUTOZONESET for vsan 1 successfully.

```

次の例は、自動ゾーン機能がすでに有効になっているかどうかと、現在ゾーン分割されていないデバイスがあるかどうかを確認する方法を示しています。

```

switch# autozone --showpending
Feature AutoZone : Enabled
zoneset name AUTOZONESET vsan 1
  zone name AUTOZONE_JPG21190082_2 vsan 1
    member pwnn 20:00:00:11:0d:97:00:01
    member pwnn 20:01:00:11:0d:97:01:00
  zone name AUTOZONE_JPG21190082_3 vsan 1
    member pwnn 20:00:00:11:0d:97:00:00
    member pwnn 20:01:00:11:0d:97:01:01
  zone name AUTOZONE_JPG21190082_4 vsan 1
    member pwnn 20:00:00:11:0d:97:00:01
    member pwnn 20:01:00:11:0d:97:01:01

```

次の例は、**autozone** コマンドに関する情報を取得する方法を示しています。

```

switch# autozone --help
usage: autozone.py [-h] [--enable] [--disable] [--update] [--delete] [--show]
                  [--showpending] [--enableautosave] [--disableautosave]
                  [--vsan VSAN]

Enables AutoZone feature for vsan 1

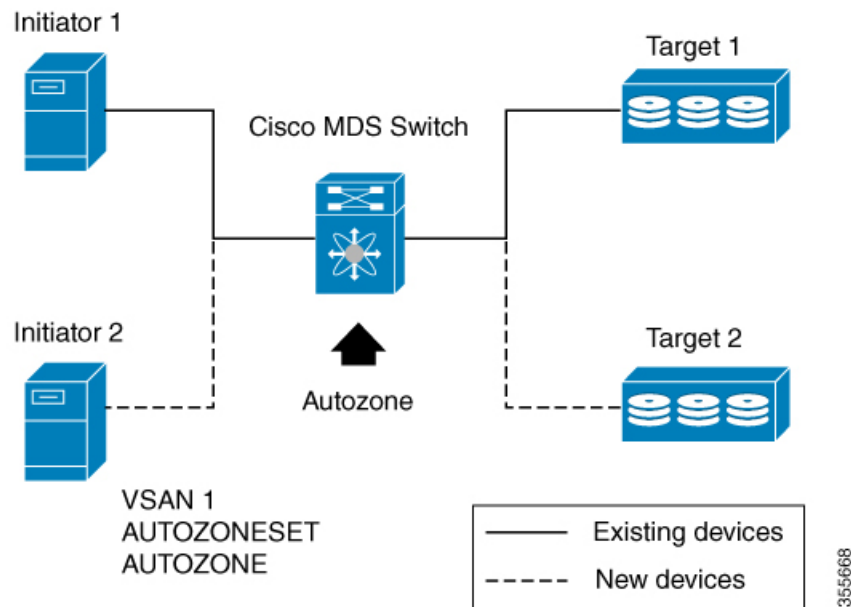
optional arguments:
  -h, --help            show this help message and exit
  --enable              Enables AutoZone automatic mode for VSAN 1. New devices
                        logging in will be zoned automatically. No changes will
                        be done for existing configuration. To have autozone
                        automatically save the running configuration to startup
                        configuration include the --enable argument followed by
                        --enableautosave argument.
  --disable             Disables AutoZone feature for VSAN 1. New devices logging
                        in will not be zoned automatically. No changes will be
                        done for existing configuration.
  --update              Computes and applies any pending AutoZone configuration
                        to switch for vsan 1
  --delete              Deletes zone/zoneset configuration done by AutoZone for VSAN
                        1
  --show               Displays the current active zone/zonset configuration done by
                        Autozone for VSAN 1.
  --showpending        Displays only zoning configuration that is pending and
                        not yet applied on the switch.
  --enableautosave     Enables Auto saving of running configuration to startup
                        configuration whenever an automatic zoning change is
                        done. Allowed with the --enable argument and --update
                        argument respectively.
  --disableautosave    Disables Auto saving of running configuration to startup
                        configuration whenever an automatic zoning change is
                        done.. To save any automatic zoning changes to startup,
                        "copy running-config startup-config" must be manually
                        executed.
  --vsan VSAN          Please provide VSAN between 1-4093

```

自動ゾーンのシナリオの例

2つのデバイス（Initiator 1 と Target 1）が Cisco MDS スイッチにログオンしているトポロジがあるとします。スイッチで自動ゾーン機能を設定し、これらのデバイスのゾーン設定を確認します。その後、2つの新しいデバイス（Initiator 2 と Target 2）をこのネットワークに導入し、それらがゾーン内で自動的に設定されたかどうかを確認します。

図 10: 自動ゾーンのトポロジの例



1. **show zoneset active vsan 1** コマンドを使用して、既存のゾーン設定を確認します。

```
switch# show zoneset active vsan 1
Zoneset not present
```

2. **show fcns database** コマンドを使用して、既存のデバイス ログインを確認します。

```
switch# show fcns database
VSAN 1:
-----
FCID          TYPE   PWWN                (VENDOR)          FC4-TYPE:FEATURE
-----
0xee0000     N     20:00:00:11:0d:97:00:00      scsi-fcp:init
0xee0020     N     20:01:00:11:0d:97:01:00      scsi-fcp:target
0xee0400     N     10:00:00:de:fb:74:e8:31 (Cisco) ipfc
Total number of entries = 2
```

3. **autozone --enable** コマンドを使用して、VSAN 1 でゾーンおよびゾーンセットを自動作成し、Cisco MDS スイッチへの新しいデバイス ログインを確認するためのタイマーをスケジューリングします。

```
switch# autozone --enable
This command will create and activate single-initiator and single-target zones for
all end-devices are already logged-in automatically; that may lead to more tcam
entries and also RSCN load on network. Please use AutoZone judiciously.
AutoZone feature is enabled
Device with pwnn 10:00:00:de:fb:74:e8:31 is not registered with FC4-type Init or
Target. Hence, it will be ignored for AutoZone configuration.
Configuring zones for vsan 1
      AUTOZONE_JPG21190082_1
Configuring zoneset for vsan 1
Activating the zoneset. Please wait...
Configured zoneset AUTOZONESET for vsan 1 successfully.
```

4. **show zoneset active vsan 1** コマンドを使用して、ゾーン設定を確認します。

```
switch# show zoneset active vsan 1
zoneset name AUTOZONESET vsan 1
  zone name AUTOZONE_JPG21190082_1 vsan 1
    * fcid 0xee0000 [pwnn 20:00:00:11:0d:97:00:00]
    * fcid 0xee0020 [pwnn 20:01:00:11:0d:97:01:00]
```

「*AUTOZONESET*」という名前の新しいゾーンセットが作成され、
「*AUTOZONE_<SwitchSerialNumber>_<number>*」形式の新しいゾーンが作成され、この
ゾーンセットにデバイスが追加されたことを確認できます。

5. Initiator 2 と Target 2 をネットワークに追加します。
6. **show fcns database** コマンドを使用して、新しいデバイス ログインを確認します。

```
switch# show fcns database
VSAN 1:
-----
FCID          TYPE  PWWN                (VENDOR)          FC4-TYPE:FEATURE
-----
0xee0000      N     20:00:00:11:0d:97:00:00
0xee0001      N     20:00:00:11:0d:97:00:01
0xee0020      N     20:01:00:11:0d:97:01:00
0xee0021      N     20:01:00:11:0d:97:01:01
0xee0400      N     10:00:00:de:fb:74:e8:31 (Cisco) ipfc
Total number of entries = 5
```

7. **autozone --showpending** コマンドを使用して、保留中のゾーン設定を確認します。

```
switch# autozone --showpending
Feature AutoZone : Enabled
zoneset name AUTOZONESET vsan 1
  zone name AUTOZONE_JPG21190082_2 vsan 1
    member pwnn 20:00:00:11:0d:97:00:01
    member pwnn 20:01:00:11:0d:97:01:00
  zone name AUTOZONE_JPG21190082_3 vsan 1
    member pwnn 20:00:00:11:0d:97:00:00
    member pwnn 20:01:00:11:0d:97:01:01
  zone name AUTOZONE_JPG21190082_4 vsan 1
    member pwnn 20:00:00:11:0d:97:00:01
    member pwnn 20:01:00:11:0d:97:01:01
```

8. (任意) 新しいデバイスがスイッチにログインするたびにゾーン分割情報を更新するために、**autozone --update** コマンドを使用して自動ゾーンを手動で実行できます。

```
switch# autozone --update
Device with pwwn 10:00:00:de:fb:74:e8:31 is not registered with FC4-type Init or
Target.
Hence, it will be ignored for AutoZone configuration.
Configuring zones for vsan 1
    AUTOZONE_JPG21190082_1
    AUTOZONE_JPG21190082_2
    AUTOZONE_JPG21190082_3
    AUTOZONE_JPG21190082_4
Configuring zoneset for vsan 1
Activating the zoneset. Please wait...
Configured zoneset AUTOZONESET for vsan 1 successfully.
```

9. **autozone --show** コマンドを使用して、新しいデバイスのゾーン設定を確認します。

```
switch# autozone --show
Feature AutoZone : Enabled
AutoSave Configuration : Enabled
The possible zone/zoneset configuration with AutoZone feature for currently logged-in
devices is :
zoneset name AUTOZONESET vsan 1
    zone name AUTOZONE_JPG21190082_1 vsan 1
        member pwwn 20:00:00:11:0d:97:00:00
        member pwwn 20:01:00:11:0d:97:01:00
    zone name AUTOZONE_JPG21190082_2 vsan 1
        member pwwn 20:00:00:11:0d:97:00:01
        member pwwn 20:01:00:11:0d:97:01:00
    zone name AUTOZONE_JPG21190082_3 vsan 1
        member pwwn 20:00:00:11:0d:97:00:00
        member pwwn 20:01:00:11:0d:97:01:01
    zone name AUTOZONE_JPG21190082_4 vsan 1
        member pwwn 20:00:00:11:0d:97:00:01
        member pwwn 20:01:00:11:0d:97:01:01
```

ゾーン設定

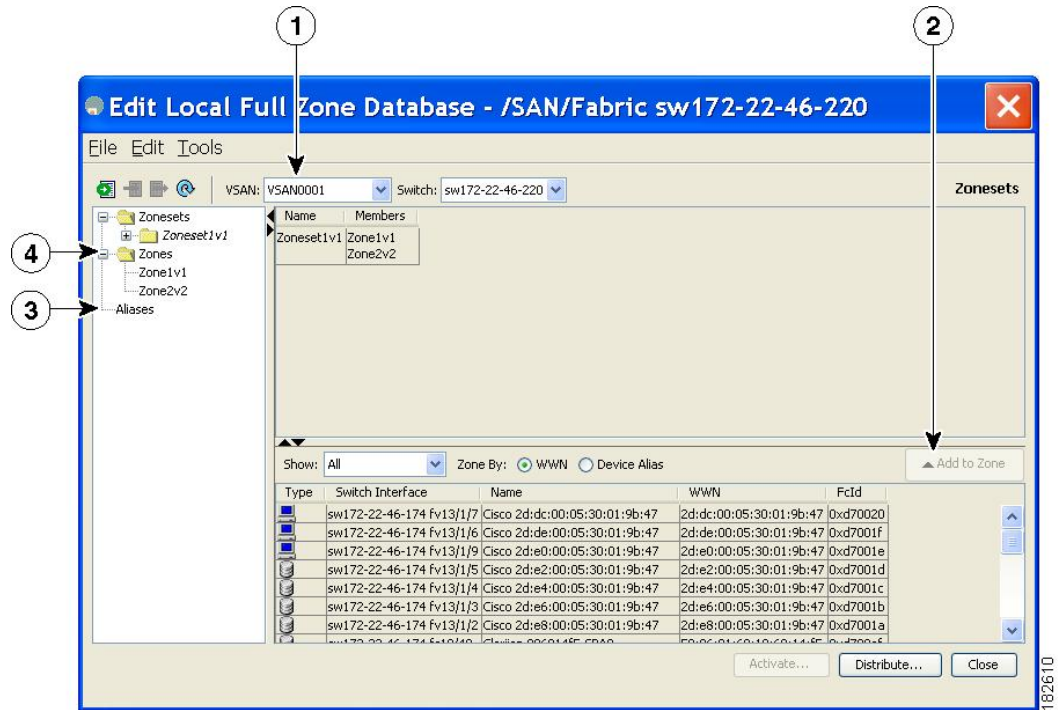
Edit Local Full Zone Database ツールの概要

Edit Local Full Zone Database ツールを使用して、次のタスクを実行します。

- ウィンドウから移動せずに、プルダウンメニューを使用して **VSAN** を選択して再入力することにより、**VSAN** 別の情報を表示します。
- [ゾーンまたはエイリアスの追加 (Add to zone or alias)] ボタンを使用して、エイリアスまたはゾーン単位でデバイスを上下に移動させます。
- 複数のフォルダ内のエイリアスに基づいてゾーン分割特性を追加します。
- ゾーンセット、ゾーン、またはエイリアスの名前を変更します。

Edit Local Full Zone Database ツールを使用すると、複数のスイッチでゾーン分割ができ、[Edit Local Full Zone Database] ダイアログボックスですべてのゾーン分割機能が使用可能になります (Figure 11: [Edit Local Full Zone Database] ダイアログボックス, on page 65を参照)。

Figure 11: [Edit Local Full Zone Database] ダイアログボックス



<p>1 ダイアログボックスを閉じずに、ドロップダウンメニューでVSANを選択して再入力すると、VSAN別の情報を表示できます。</p>	<p>3 複数のフォルダ内のエイリアスに基づいてゾーン分割特性を追加できます。</p>
<p>2 [ゾーンに追加 (Add to zone)] ボタンを使用すると、エイリアスまたはゾーン単位でデバイスを上下に移動できます。</p>	<p>4 ツリー内のゾーンセット、ゾーン、またはエイリアスの名前を変更するには、トリプルクリックします。</p>



Note [Device Alias] オプション ボタンは、デバイスのエイリアスが enhanced モードのときだけに表示されます。詳細については、[デバイスエイリアスの作成](#), on page 179の項を参照してください。

ゾーンの設定



Tip 該当する表示コマンド（たとえば、**show interface** または **show flogi database**）を使用して、必要な値を 16 進表記で取得します。



Tip **show wwn switch** コマンドを使用して sWWN を取得します。sWWN を指定しない場合、ソフトウェアは自動的にローカル sWWN を使用します。



Tip [Physical Attributes] ペインで [Switches] を開き、sWWN を検索します。sWWN を指定しない場合、ソフトウェアは自動的にローカル sWWN を使用します。



Note インターフェイスベースゾーン分割は、Cisco MDS 9000 シリーズスイッチでのみ機能します。インターフェイスベースゾーン分割は、その VSAN で interop モードが設定されている場合は動作しません。

設定されているゾーンの数が、すべての VSAN で許可されるゾーンの最大数を超えると、次のメッセージが表示されます。

```
switch(config)# zone name temp_zone1 vsan 300
cannot create the zone; maximum possible number of zones is already configured
```



Note ゾーン、ゾーンメンバー、およびゾーンセットの数の設定時の制限については、『[Cisco MDS NX-OS Configuration Limits](#)』を参照してください。

ゾーンを設定し、ゾーン名を割り当てるには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **zone name Zone1 vsan 3**

Example:

```
switch(config-zone)#
```

vsan3 という VSAN に Zone1 というゾーンを設定します。

Note すべての英数字か、または記号 (\$、-、^、_) のうち 1 つがサポートされます。

ステップ 3 switch(config-zone)# **member** *type value***Example:**

pWWN example:

Example:

```
switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab
```

Example:

Fabric pWWN example:

Example:

```
switch(config-zone)# member fwwn 10:01:10:01:10:ab:cd:ef
```

Example:

FC ID example:

Example:

```
switch(config-zone)# member fcid 0xce00d1
```

Example:

FC alias example:

Example:

```
switch(config-zone)# member fcalias Payroll
```

Example:

Domain ID example:

Example:

```
switch(config-zone)# member domain-id 2 portnumber 23
```

Example:

IPv4 address example:

Example:

```
switch(config-zone)# member ip-address 10.15.0.0 255.255.0.0
```

Example:

IPv6 address example:

Example:

```
switch(config-zone)# member ipv6-address 2001::db8:800:200c:417a/64
```

Example:

Local sWWN interface example:

Example:

```
switch(config-zone)# member interface fc 2/1
```

Example:

Remote sWWN interface example:

Example:

```
switch(config-zone)# member interface fc2/1 swwn 20:00:00:05:30:00:4a:de
```

Example:

Domain ID interface example:

Example:

```
switch(config-zone)# member interface fc2/1 domain-id 25
```

Example:

```
switch(config-zone)# member symbolic-nodename iqn.test
```

指定されたタイプ (pWWN、ファブリック pWWN、FCID、FCエイリアス、ドメインID、IPv4アドレス、IPv6アドレス、またはインターフェイス) および値に基づいて、指定されたゾーン (Zone1) にメンバーを設定します。

Caution 同じファブリック内に FabricWare を実行する Cisco MDS 9020 スイッチがある場合には、Cisco SAN-OS を実行するすべての MDS スイッチには、pWWN タイプのゾーン分割だけを設定する必要があります。

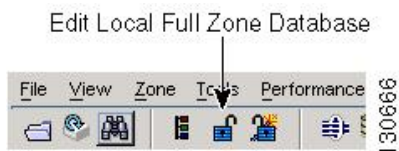
Note Cisco MDS 9396S スイッチには 96 個のポートがあります。その他の Cisco MDS スイッチのポートの数はこれよりも少なくなります。したがって、インターフェイスに基づいてゾーンメンバーを設定するときには、ファブリック内でインターフェイス数が最も多いと考えられるファブリックスイッチを常に選択してください。

Zone Configuration Tool を使用したゾーンの設定

DCNMSAN クライアントを使用してゾーンを作成し、これをゾーンセットに移動する手順は、次のとおりです。

ステップ 1 ツールバーにある [ゾーン (Zone)] アイコンをクリックします (図 12 : [Zone] アイコン (69 ページ) を参照)。

図 12: [Zone] アイコン



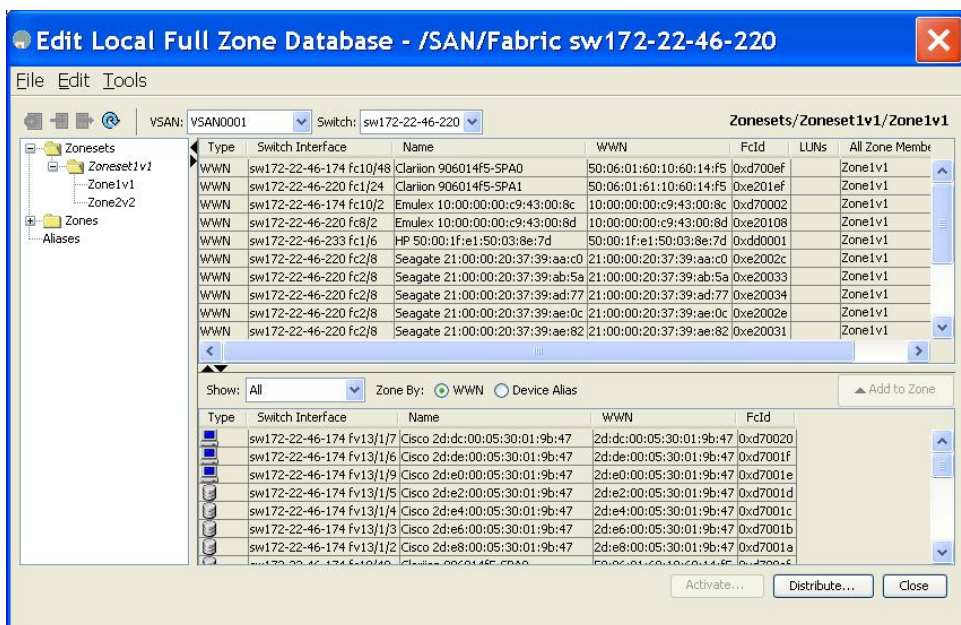
[Select VSAN] ダイアログボックスが表示されます。

ステップ 2 ゾーンを作成する VSAN を選択し、[OK] をクリックします。

```
switch(config)# callhome
```

[Edit Local Full Zone Database] ダイアログボックスが表示されます (図 13 : [Edit Local Full Zone Database] ダイアログボックス (69 ページ) を参照)。

図 13: [Edit Local Full Zone Database] ダイアログボックス



ゾーンメンバーシップ情報を表示する場合は、[すべてのゾーンメンバーシップ (All Zone Membership(s))] カラムを右クリックして、ポップアップメニューで現在の行またはすべての行の [詳細の表示 (Show Details)] をクリックします。

ステップ 3 左側ペインの [ゾーン (Zones)] をクリックし、[挿入 (Insert)] アイコンをクリックして、ゾーンを作成します。

[ゾーンの作成 (Create Zone)] ダイアログボックスが表示されます (図 14: [Create Zone] ダイアログボックス (70 ページ) を参照)。

図 14: [Create Zone] ダイアログボックス



ステップ 4 ゾーン名を入力します。

ステップ 5 次のチェックボックスのうち 1 つをオンにします。

1. **Read Only** : このゾーンでは読み込みを許可しますが、書き込みは拒否します。
2. **Permit QoS traffic with Priority** : ドロップダウンメニューでプライオリティを設定します。
3. **[Restrict Broadcast frames to Zone Members]**

ステップ 6 [OK] をクリックしてゾーンを作成します。

このゾーンを既存のゾーンセットに移動する場合は、手順 8 へスキップします。

ステップ 7 左側ペインの[ゾーンセット (Zoneset)] をクリックし、[挿入 (Insert)] アイコンをクリックして、ゾーンセットを作成します。

[ゾーンセット名 (Zoneset Name)] ダイアログボックスが表示されます (図 15: [Zoneset Name] ダイアログボックス (70 ページ) を参照)。

図 15: [Zoneset Name] ダイアログボックス



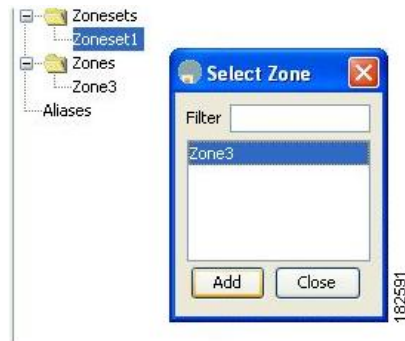
ステップ 8 ゾーンセット名を入力し、[OK] をクリックします。

(注) シンボル (\$、-、^、_) のうちの 1 つまたはすべての英数字がサポートされています。interop モード 2 と 3 では、シンボル (_) またはすべての英数字がサポートされています。

ステップ 9 ゾーンを追加するゾーンセットを選択して [挿入 (Insert)] アイコンをクリックするか、または [Zoneset1] に [Zone3] をドラッグアンドドロップします。

[ゾーンの選択 (Select Zone)] ダイアログボックスが表示されます (図 16: [Select Zone] ダイアログボックス (71 ページ) を参照)。

図 16: [Select Zone] ダイアログボックス



ステップ 10 [追加 (Add)] をクリックしてゾーンを追加します。

ゾーンメンバーの追加

ゾーンを作成すると、ゾーンにメンバーを追加できます。メンバーを追加するには、複数のポート識別タイプを使用します。

DCNM SAN クライアントを使用してゾーンにメンバーを追加する手順は、次のとおりです。

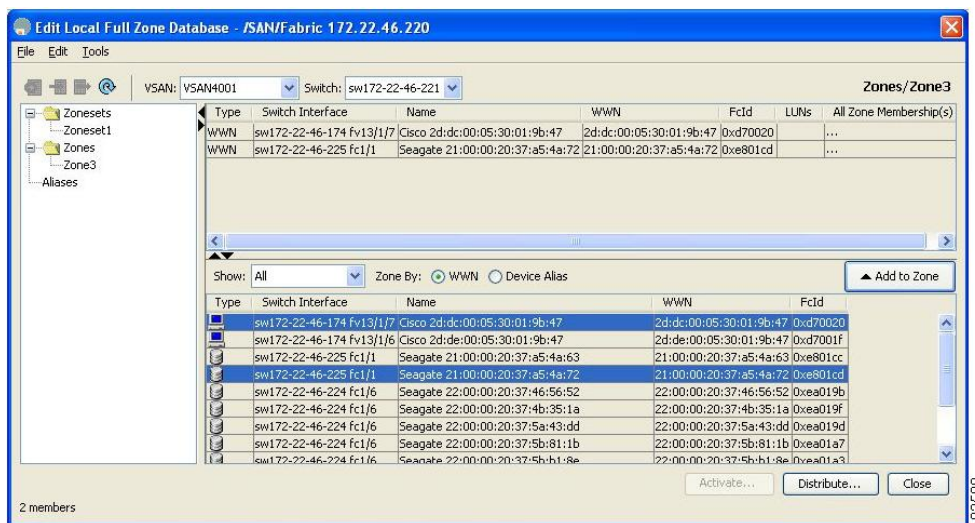
ステップ 1 [ゾーン (Zone)] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

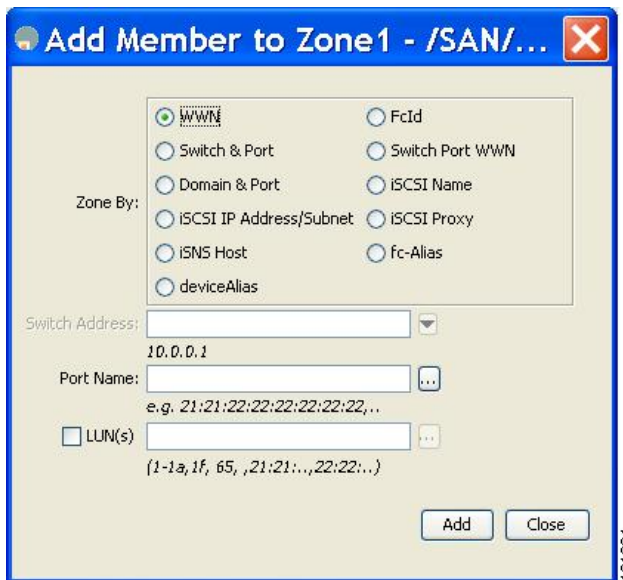
Figure 17: [Edit Local Full Zone Database] ダイアログボックス



ステップ 3 [ファブリック (Fabric)] ペイン (Figure 17: [Edit Local Full Zone Database] ダイアログボックス, on page 71 を参照) から追加するメンバーを選択し、[ゾーンに追加 (Add to Zone)] をクリックするか、メンバーを追加するゾーンをクリックし、[挿入 (Insert)] アイコンをクリックします。

[メンバーをゾーンに追加 (Add Member to Zone)] ダイアログボックスが表示されます (Figure 18: [Add Member to Zone] ダイアログボックス, on page 72 を参照) 。

Figure 18: [Add Member to Zone] ダイアログボックス



Note [Device Alias] オプション ボタンは、デバイスのエイリアスが enhanced モードのときにだけ表示されます。詳細については、「[デバイス エイリアスの作成](#)」の項を参照してください。

ステップ 4 ブラウズ ボタンをクリックしてポート名を選択するか、または [LUN] チェックボックスをオンにしてブラウズ ボタンをクリックし、LUN を設定します。

ステップ 5 [追加 (Add)] をクリックして、ゾーンにメンバーを追加します。

Note ゾーン メンバーを設定する場合は、オペレーティング システムごとに異なる複数の ID が 1 つの Logical Unit Number (LUN) に設定されるように指定することができます。6 つの異なるオペレーティング システムから選択できます。

名前、WWN、または FC ID に基づくエンド デバイスのフィルタリング

エンド デバイスおよびデバイス エイリアスをフィルタする手順は、次のとおりです。

ステップ 1 ツールバーにある [ゾーン (Zone)] アイコンをクリックします (Figure 12: [Zone] アイコン, on page 69 を参照) 。

ステップ 2 [With] ドロップダウン リストから名前、[WWN]、または [FC ID] を選択します。

ステップ3 [Filter] テキストボックスに *zo1* などのフィルタ条件を入力します。

ステップ4 [移動 (Go)] をクリックします。

複数のゾーンへの複数のエンド デバイスの追加

複数のゾーンに複数のエンド デバイスを追加する手順は、次のとおりです。

ステップ1 ツールバーにある [ゾーン (Zone)] アイコンをクリックします (図 12 : [Zone] アイコン, on page 69 を参照)。

ステップ2 Ctrl キーを使用して複数のエンド デバイスを選択します。

ステップ3 右クリックし、[ゾーンに追加 (Add to Zone)] を選択します。

ステップ4 表示されるポップアップ ウィンドウから、Ctrl キーを使用して複数のゾーンを選択します。

ステップ5 [Add] をクリックします。

選択されたエンド デバイスが選択されたゾーンに追加されます。

ゾーン セットと FC エイリアス

ゾーンは、アクセスコントロールを指定するための方式を提供します。ゾーンセットは、ファブリックでアクセス コントロールを実行するためのゾーンの分類です。

ゾーンセットはメンバー ゾーンおよび VSAN 名で設定します (設定された VSAN にゾーンセットが存在する場合)。

Zoneset Distribution : フルゾーンセットを配信するには、ワンタイム配信またはフルゾーンセット配信の2つの方法のうち、いずれかを使用します。

Zoneset Duplication : ゾーンセットのコピーを作成し、元のゾーンセットを変更することなく編集できます。アクティブゾーンセットを bootflash: ディレクトリ、volatile: ディレクトリ、または slot0 から次のいずれかのエリアにコピーすることができます。

- フルゾーンセット
- リモート ロケーション (FTP、SCP、SFTP、または TFTP を使用)

アクティブゾーンセットは、フルゾーンセットに含まれません。フルゾーンセットが失われた場合、または伝送されなかった場合に、既存のゾーンセットに変更を加え、アクティブにすることはできません。

ゾーンセットの作成

次の図では、それぞれ独自のメンバーシップ階層とゾーンメンバを持つセットが2つ作成されます。

ゾーンセット A またはゾーンセット B のいずれか（両方でなく）をアクティブにできます。



Tip ゾーンセットはメンバゾーンおよび VSAN 名で設定します（設定された VSAN にゾーンセットが存在する場合）。

ゾーンセットの非アクティブ化

ゾーンセットに加えた変更は、それがアクティブ化されるまで、フルゾーンセットには反映されません。



Tip アクティブゾーンセットを保存するのに、**copy running-config startup-config** コマンドを発行する必要はありません。ただし、明示的にフルゾーンセットを保存するには、**copy running-config startup-config** コマンドを発行する必要があります。ファブリックに複数のスイッチが含まれている場合は、**copy running-config startup-config fabric** コマンドを実行する必要があります。**fabric** キーワードを指定すると、**copy running-config startup-config** コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップ コンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。

既存のゾーンセットをアクティブまたは非アクティブにするには、次の手順を実行します。

ステップ 1 switch# config terminal

Example:

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# zoneset activate name Zoneset1 vsan 3

指定されたゾーンセットをアクティブにします。

フルゾーンセット配信が VSAN で設定されている場合、ゾーンセットのアクティブ化により、フルゾーン分割データベースがファブリック内の他のスイッチに配信されます。

VSAN で拡張ゾーン分割が設定されている場合、ゾーンセットのアクティブ化は、**zone commit vsan vsan-id** コマンドが有効になるまで保留されます。**show zone pending-diff vsan vsan-id** は、保留中の変更を表示します。

Note ゾーンセットをアクティブにするときに、`zoneset overwrite-control vsan id` コマンドが有効であり、ゾーンセット名が現在のアクティブなゾーンセットとは異なる場合、アクティブ化は失敗しエラーメッセージが表示されます。詳細については、[アクティブなゾーンセットの上書き制御, on page 78](#)を参照してください。

```
switch(config)# zoneset activate name Zoneset2 vsan 3
```

```
WARNING: You are trying to activate zoneset2, which is different from current active zoneset1. Do you want to continue? (y/n) [n] y
```

ステップ 3 `switch(config)# no zoneset activate name Zoneset1 vsan 3`

指定されたゾーンセットを非アクティブにします。

DCNM SAN クライアントを使用したゾーンセットのアクティブ化

DCNM SAN クライアントを使用して既存のゾーンをアクティブにする手順は、次のとおりです。

ステップ 1 [ゾーン (Zone)] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

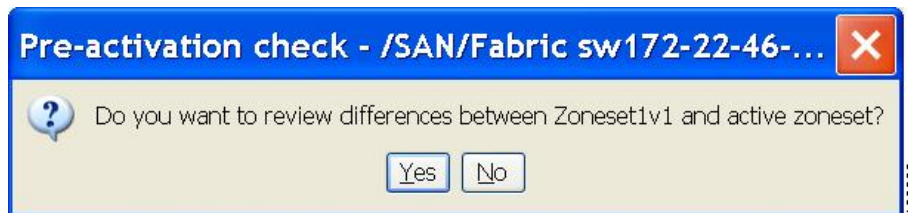
ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3 [アクティブ化 (Activate)] をクリックして、ゾーンセットをアクティブにします。

[アクティベーション前の確認 (Pre-Activation Check)] ダイアログボックスが表示されます (Figure 19: [Pre-Activation Check] ダイアログボックス, on page 75を参照)。

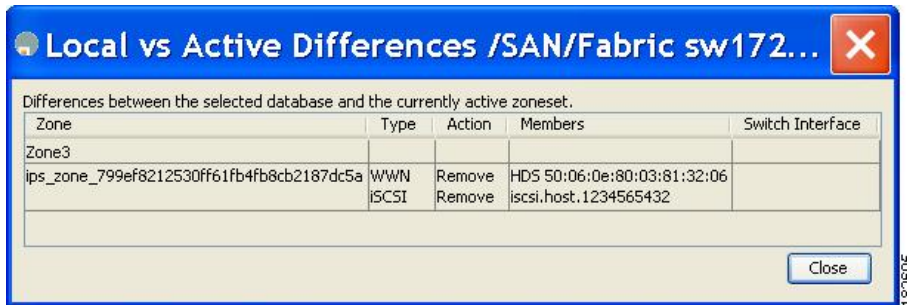
Figure 19: [Pre-Activation Check] ダイアログボックス



ステップ 4 [はい (Yes)] をクリックして、相違を確認します。

[ローカルとアクティブの相違 (Local vs. Active Differences)] ダイアログボックスが表示されます (Figure 20: [Local vs. Active Differences] ダイアログボックス, on page 76を参照)。

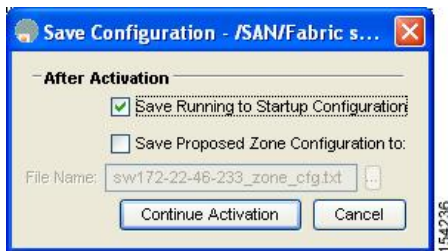
Figure 20: [Local vs. Active Differences] ダイアログボックス



ステップ 5 [Close] をクリックして、ダイアログボックスを閉じます。

[設定の保存 (Save Configuration)] ダイアログボックスが表示されます (Figure 21: [Save Configuration] ダイアログボックス, on page 76を参照)。

Figure 21: [Save Configuration] ダイアログボックス

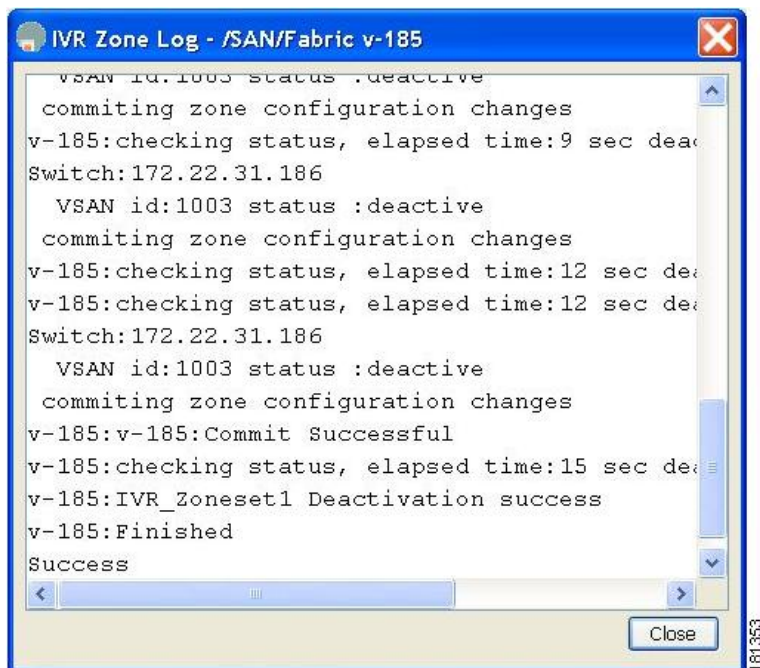


ステップ 6 [Save Running to Startup Configuration] チェックボックスをオンにして、すべての変更をスタートアップ コンフィギュレーションに保存します。

ステップ 7 ゾーンセットをアクティブにするには[アクティベーションを続行 (Continue Activation)]をクリックします。ダイアログボックスを閉じて、保存されていない変更を廃棄するには、[キャンセル (Cancel)]をクリックします。

ゾーンセットのアクティブ化に成功したかどうかを示す [Zone Log] ダイアログボックスが表示されます (Figure 22: [Zone Log] ダイアログボックス, on page 77 を参照)。

Figure 22: [Zone Log] ダイアログボックス



ゾーンセットの非アクティブ化

既存のゾーンを非アクティブ化する手順は、次のとおりです。

ステップ 1 非アクティブにするゾーンセットを右クリックし、ポップアップメニューで[非アクティブ化 (Deactivate)] を選択します。

[ゾーンセットの非アクティブ化 (Deactivate Zoneset)] ダイアログボックスが表示されます。

ステップ 2 テキストボックスに deactivate と入力し、[OK] をクリックします。

[入力 (Input)] ダイアログボックスが表示されます。

ステップ 3 テキストボックスに deactivate と入力し、[OK] をクリックしてゾーンセットを非アクティブにします。

Note このオプションをイネーブルにするには、server.properties ファイルを修正する必要があります。

ゾーンメンバーシップ情報の表示

DCNM SAN クライアントを使用してゾーンに割り当てられたメンバーのゾーンメンバーシップ情報を表示する手順は、次のとおりです。

ステップ 1 [ゾーン (Zone)] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3 左側ペインで、[ゾーン (Zones)] をクリックします。右側のペインに各ゾーンのメンバーが表示されます。

Note デフォルトゾーンメンバーは、デフォルトゾーンポリシーが **permit** に設定されている場合に限り、明示的に表示されます。デフォルトゾーンポリシーが **deny** に設定されている場合、このゾーンのメンバーは表示されません。 [ゾーン情報の表示](#), on page 116 を参照してください。

Tip アクティブゾーンセットを保存するのに、**copy running-config startup-config** コマンドを発行する必要はありません。ただし、明示的にフルゾーンセットを保存するには、**copy running-config startup-config** コマンドを発行する必要があります。ファブリックに複数のスイッチが含まれている場合は、**copy running-config startup-config fabric** コマンドを実行する必要があります。**fabric** キーワードを指定すると、**copy running-config startup-config** コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップコンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。

アクティブなゾーンセットの上書き制御

新しいゾーンセットをアクティブにするときに、ユーザーがゾーンセット名を誤って入力した場合、または入力した名前がすでにスイッチに存在している場合は、誤ったゾーンセットがアクティブになり、トラフィックが失われます。誤ったゾーンセットがアクティブになることを防ぐため、`zoneset overwrite-control vsan id` コマンドが導入されました。



Note `zoneset overwrite-control vsan id` コマンドが有効な場合でも、ユーザーは `zoneset activate name zoneset name vsan vsan -id force` コマンドを使用してこれを上書きし、新しいゾーンセットをアクティブにできます。

ステップ 1 `switch# configure terminal`

Example:

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# zoneset overwrite-control vsan 3`

指定した VSAN で上書き制御を有効にします。

```
switch(config)# zoneset overwrite-control vsan 1
```

```
WARNING: This will enable Activation Overwrite control. Do you want to continue?  
(y/n) [n]
```

Note zoneset overwrite-control vsan id コマンドは、拡張ゾーン モードでのみ有効にできます。

ステップ 3 switch(config)# show zone status vsan 3

VSAN のステータス（上書き制御が有効であるかどうか）を表示します。

What to do next

ゾーン ステータスの表示

```
switch(config)# show zone status vsan 3  
VSAN: 2 default-zone: deny distribute: full Interop: default  
mode: enhanced merge-control: allow  
session: none  
hard-zoning: enabled broadcast: unsupported  
smart-zoning: disabled  
rscn-format: fabric-address  
activation overwrite control: enabled  
Default zone:  
qos: none broadcast: unsupported ronly: unsupported  
Full Zoning Database :  
DB size: 348 bytes  
Zonesets:2 Zones:2 Aliases: 0 Attribute-groups: 1  
Active Zoning Database :  
DB size: 68 bytes  
Name: hellset Zonesets:1 Zones:1  
Current Total Zone DB Usage: 416 / 2097152 bytes (0 % used)  
Pending (Session) DB size:  
Full DB Copy size: 0 bytes  
Active DB Copy size: 0 bytes  
SFC size: 0 / 2097152 bytes (0 % used)  
Status: Commit completed at 15:19:49 UTC Jun 11 2015
```

デフォルト ゾーン

ファブリックの各メンバは（デバイスが Nx ポートに接続されている状態）、任意のゾーンに所属できます。どのアクティブゾーンにも所属しないメンバは、デフォルトゾーンの一部と見なされます。したがって、ファブリックにアクティブなゾーンセットがない場合、すべてのデバイスがデフォルトゾーンに所属するものと見なされます。メンバは複数のゾーンに所属できますが、デフォルトゾーンに含まれるメンバは、その他のゾーンに所属できません。接続されたポートが起動すると、スイッチは、ポートがデフォルトゾーンのメンバか判別します。



Note 設定されたゾーンとは異なり、デフォルトゾーン情報は、ファブリックの他のスイッチに配信されません。

トラフィックをデフォルトゾーンのメンバ間で許可または拒否できます。この情報は、すべてのスイッチには配信されません。各スイッチで設定する必要があります。



Note スイッチが初めて初期化されたとき、ゾーンは設定されておらず、すべてのメンバがデフォルトゾーンに所属するものと見なされます。メンバー同士で相互に通信することは許可されていません。

ファブリックの各スイッチにデフォルトゾーンポリシーを設定します。ファブリックの1つのスイッチでデフォルトゾーンポリシーを変更する場合、必ずファブリックの他のすべてのスイッチでも変更してください。



Note デフォルトゾーン設定のデフォルト設定値は変更できます。

デフォルトポリシーが **permit** として設定されている場合、またはゾーンセットがアクティブの場合、デフォルトゾーンメンバーが明示的に表示されます。デフォルトポリシーが **deny** として設定されている場合は、**show zoneset active** コマンドを発行しても、このゾーンのメンバは明示的に一覧表示されません。



Note 現在のデフォルトゾーン分割ポリシーは **deny** です。非表示のアクティブゾーンセットは MDS の **d_default_cfg** です。2つのスイッチのデフォルトゾーン分割ポリシーに不一致がある場合（一方で **permit**、もう一方で **deny**）、ゾーンマージが失敗します。2つの Brocade スイッチでこの動作は変わりません。次のようなエラーメッセージが表示されません。

次のようなエラーメッセージが表示されます。

Switch1 syslog:

```
switch(config-if)# 2014 Sep 2 06:33:21 hac15 %ZONE-2-ZS_MERGE_FAILED: %$VSAN 1%$ Zone merge failure, isolating interface fc2/10 received reason: Default zoning policy conflict. Received rjt from adjacent switch:[reason:0]
```

Switch2 syslog:

```
switch(config-if)# 2014 Sep 2 12:13:17 hac16 %ZONE-2-ZS_MERGE_FAILED: %$VSAN 1%$ Zone merge failure, isolating interface fc3/10 reason: Default zoning policy conflict.: [reason:0]
```

任意の VSAN のデフォルトゾーンポリシーを変更するには、DCNM SAN クライアントメニュー ツリーで **[VSANxx] > [デフォルトゾーン (Default Zone)]** を選択し、**[ポリシー**

(Policies)] タブをクリックします。デバイス間の接続を確立する場合は、これらのデバイスをデフォルト以外のゾーンに割り当てることを推奨します。

デフォルト ゾーンのアクセス権限の設定

デフォルトゾーン内のメンバーに対するトラフィックを許可または拒否するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **zone default-zone permit vsan 1**

デフォルトゾーンメンバへのトラフィック フローを許可します。

ステップ 3 switch(config)# **no zone default-zone permit vsan 1**

デフォルトゾーンメンバへのトラフィック フローを拒否（デフォルト）します。

DCNM SAN クライアントを使用したデフォルトゾーンのアクセス権限の構成

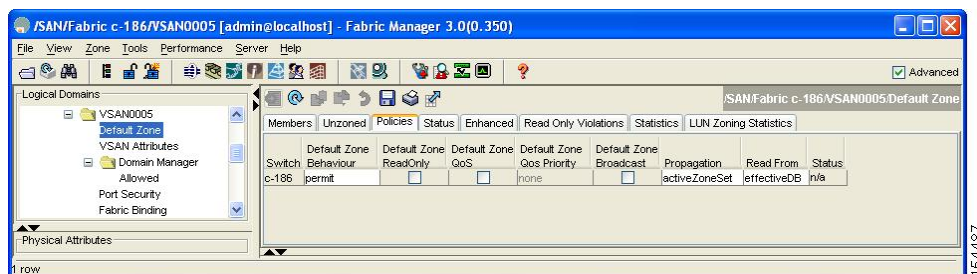
DCNM SAN クライアントを使用してデフォルトゾーンでトラフィックをメンバーに許可または拒否するには、次の手順を実行します。

ステップ 1 **[VSAN]** を開き、**[DCNM SAN クライアントの論理ドメイン (DCNM SAN Client Logical Domains)]** ペインで、**[デフォルト ゾーン (Default Zone)]** を選択します。

ステップ 2 **[情報 (Information)]** ペインで **[ポリシー (Policies)]** タブをクリックします。

[Information] ペインにゾーン ポリシー情報が表示されます ([Figure 23: デフォルトのゾーン ポリシー, on page 81](#) を参照)。

Figure 23: デフォルトのゾーン ポリシー



アクティブゾーンセットはイタリック体で表示されます。アクティブゾーンセットを変更してから変更をアクティブ化するまでの間は、このゾーンセットが太字のイタリック体で表示されます。

ステップ 3 [デフォルトのゾーン動作 (Default Zone Behavior)] フィールドのドロップダウンメニューから [許可 (permit)] または [拒否 (deny)] を選択します。

FC エイリアスの作成の概要

Cisco MDS スイッチでさまざまな機能を構成するには、エンドノードまたはファブリックポートの pWWN、fWWNなどを指定する必要がありますが、正しい値を割り当てる必要があります。たとえば、タイプミスから派生した誤った値は、予期しない結果を引き起こす可能性があります。この問題を回避するには、わかりやすい名前を定義し、必要に応じて、この名前をすべての構成コマンドで使用します。これらのわかりやすい名前は **FC** エイリアスと呼ばれ、すべての組織に固有の命名規則に従って定義されます。

FC エイリアスはゾーンサーバーのデータベース内に保存され、NX-OS ソフトウェアは FC エイリアスに対応するゾーンメンバーのタイプに自動的に変換します。デバイスエイリアス名は別のタイプのエイリアスであり、[DDAS, on page 171](#) 章で説明されています。デバイスエイリアスは FC エイリアスに割り当てることができますが、その逆はできません。

FC エイリアスは大文字と小文字が区別され、64 文字の英数字に制限されています。FC エイリアス名には、次の文字を 1 つ以上含めることができます。

- a ~ z および A ~ Z
- 1 ~ 9
- - (ハイフン) および _ (下線)
- \$ (ドル記号) および ^ (キャレット) 記号

次の値を使用して、FC エイリアス名を割り当て、FC エイリアスメンバーを構成できます。

- pWWN : N または NL ポートの WWN は、16 進形式です (10:00:00:23:45:67:89:ab など)。
- fWWN : ファブリックポートの 16 進表記の WWN (10:00:00:23:45:67:89:ab など)
- FC ID : 0xhhhhhh 形式の N ポート ID (0xce00d1 など)
- ドメイン ID : ドメイン ID は 1 ~ 239 の整数です。このメンバーシップ設定を完了するには、他社製スイッチの必須ポート番号が必要です。
- IPv4 アドレス : 接続されたデバイスの IPv4 アドレスは、ドット付きの 10 進表記の 32 ビットで、オプションでサブネットマスクを伴います。マスクが指定されている場合、サブネット内のすべてのデバイスが指定されたゾーンのメンバーになります。
- IPv6 アドレス : 接続されたデバイスの IPv6 アドレスは、コロン (:) で区切られた 16 進表記の 128 ビットです。

- インターフェイス：インターフェイスベースゾーン分割は、スイッチ インターフェイスがゾーンを設定するのに使用される点でポートベースゾーン分割と似ています。スイッチ インターフェイスをローカル スイッチとリモート スイッチの両方でゾーン メンバとして指定できます。リモート スイッチを指定するには、特定の VSAN 内のリモート Switch WWN (sWWN) またはドメイン ID を入力します。
- デバイスエイリアス：デバイスエイリアス名は別のタイプのエイリアスであり、メンバーとして FC エイリアスに割り当てることができます。



Tip Cisco NX-OS ソフトウェアは、VSAN ごとに最大 2048 個のエイリアスをサポートしています。

FC エイリアスの作成

エイリアスを作成するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fcalias name AliasSample vsan 3**

```
switch(config-fcalias)#
```

エイリアス名 (AliasSample) を設定します。

ステップ 3 switch(config-fcalias)# **member type value**

指定されたタイプおよび値に基づいて、指定された fcalias (AliasSample) にメンバーを構成します。

(pWWN、ファブリック pWWN、FC ID、ドメイン ID、IPv4 アドレス、IPv6 アドレス、またはインターフェイス)。

Multiple members can be inserted for a single FC alias on multiple lines:

```
switch(config-fcalias)# member pwwn 10:00:00:23:45:67:89:ab  
switch(config-fcalias)# member fwwn 10:01:10:01:10:ab:cd:ef  
switch(config-fcalias)# member fcid 0x222222
```

pWWN example:

```
switch(config-fcalias)# member pwwn 10:00:00:23:45:67:89:ab
```

fWWN example:

```
switch(config-fcalias)# member fwwn 10:01:10:01:10:ab:cd:ef
```

FC ID example:

```
switch(config-fcalias)# member fcid 0x222222
```

Domain ID example:

```
switch(config-fcalias)# member domain-id 2 portnumber 23
```

IPv4 address example:

```
switch(config-fcalias)# member ip-address 10.15.0.0 255.255.0.0
```

IPv6 address example:

```
switch(config-fcalias)# member ipv6-address 2001::db8:800:200c:417a/64
```

Local sWWN interface example:

```
switch(config-fcalias)# member interface fc 2/1
```

Remote sWWN interface example:

```
switch(config-fcalias)# member interface fc2/1 swwn 20:00:00:05:30:00:4a:de
```

Domain ID interface example:

```
switch(config-fcalias)# member interface fc2/1 domain-id 25
```

ステップ 4 switch(config-fcalias)# zone commit vsan id

指定された VSAN に対する変更をコミットします。

DCNM SAN クライアントを使用した FC エイリアスの作成

DCNM SAN クライアントを使用して FC エイリアスを作成する手順は、次のとおりです。

ステップ 1 [ゾーン (Zone)]> [Edit Local Full Zone Database] を選択します。

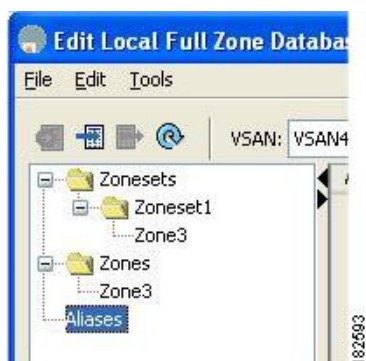
[Select VSAN] ダイアログボックスが表示されます。

ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3 左下のペインで、[エイリアス (Aliases)] をクリックします (Figure 24: FC エイリアスの作成, on page 84 を参照)。右側のペインに既存のエイリアスが表示されます。

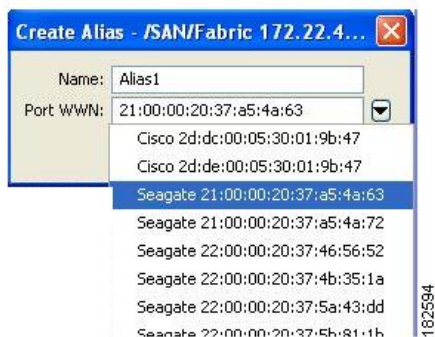
Figure 24: FC エイリアスの作成



ステップ 4 [挿入 (Insert)] アイコンをクリックして、エイリアスを作成します。

[エイリアスの作成 (Create Alias)] ダイアログボックスが表示されます (Figure 25: [Create Alias] ダイアログボックス, on page 85を参照)。

Figure 25: [Create Alias] ダイアログボックス



ステップ 5 エイリアス名および pWWN を設定します。

ステップ 6 [OK] をクリックしてエイリアスを作成します。

エイリアスへのメンバーの追加

DCNM SAN クライアントを使用してエイリアスにメンバーを追加する手順は、次のとおりです。

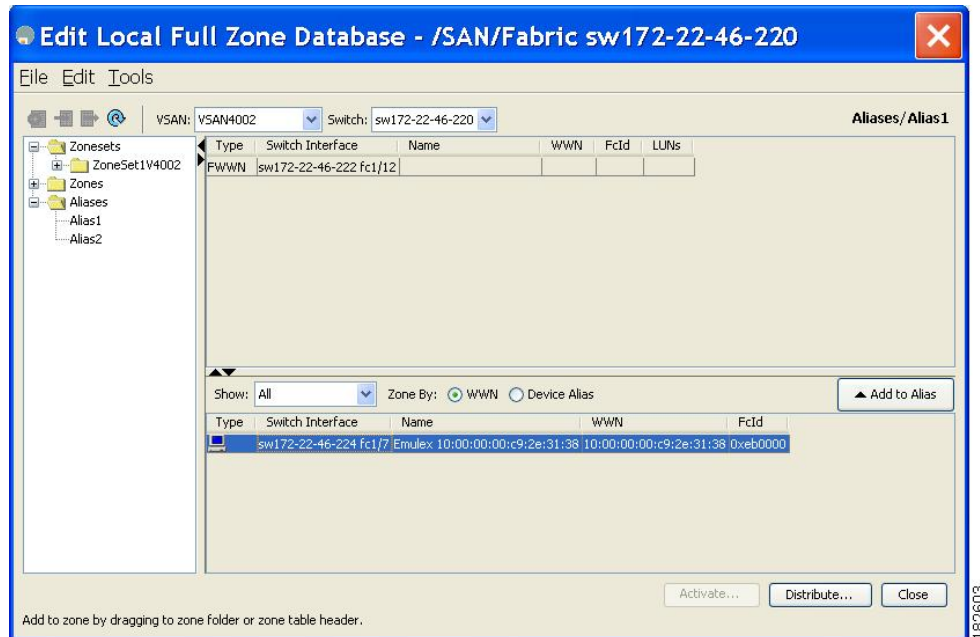
ステップ 1 [ゾーン (Zone)] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます (Figure 26: [Edit Local Full Zone Database] ダイアログボックス, on page 86 を参照)。

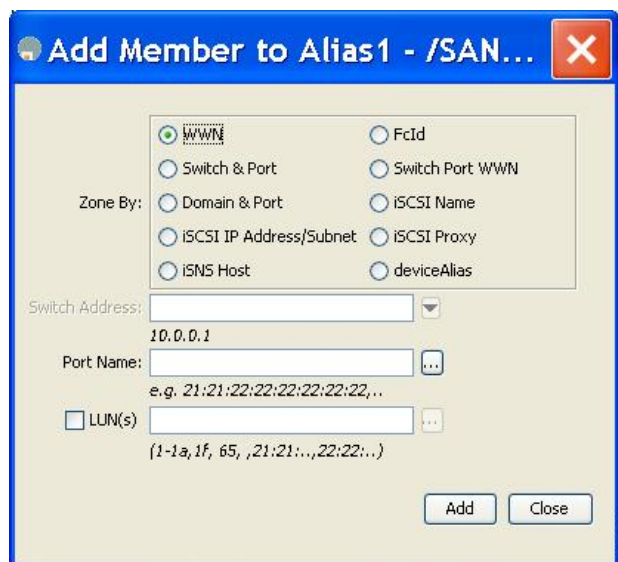
Figure 26: [Edit Local Full Zone Database] ダイアログボックス



ステップ 3 [ファブリック (Fabric)] ペインから追加するメンバーを選択し (Figure 26: [Edit Local Full Zone Database] ダイアログボックス, on page 86を参照)、[エイリアスに追加 (Add to Alias)]をクリックするか、メンバーを追加するエイリアスをクリックし、[挿入 (Insert)]アイコンをクリックします。

[メンバーをエイリアスに追加 (Add Member to Alias)]ダイアログボックスが表示されます (Figure 27: [Add Member to Alias] ダイアログボックス, on page 86を参照)。

Figure 27: [Add Member to Alias] ダイアログボックス



Note [Device Alias] オプションボタンは、デバイスのエイリアスが enhanced モードのときにだけ表示されます。詳細については、[デバイスエイリアスの作成](#), on page 179の項を参照してください。

ステップ 4 ブラウズボタンをクリックしてポート名を選択するか、または[LUN]チェックボックスをオンにしてブラウズボタンをクリックし、LUNを設定します。

ステップ 5 [追加 (Add)]をクリックして、エイリアスにメンバーを追加します。

ゾーンメンバーの pWWN ベースメンバーへの変換

ゾーンおよびエイリアスメンバーをスイッチポートまたはFC ID ベースのメンバーシップから pWWN ベースのメンバーシップに変換できます。この機能を利用して、pWWN へ変換すれば、カードまたはスイッチがファブリックで変更されてもゾーン設定は変更されません。

DCNMSAN クライアントを使用してスイッチポートと FC ID メンバーを pWWN メンバーに変換する手順は、次のとおりです。

ステップ 1 [ゾーン (Zone)] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3 変換するゾーンをクリックします。

ステップ 4 [ツール (Tools)] > [スイッチポート/FCID メンバーの pWWN ベースへの変換 (Convert Switch Port/FCID members to By pWWN)] を選択します。

変換するすべてのメンバーが列挙された [Conversion] ダイアログボックスが表示されます。

ステップ 5 変更を確認し、[変換を続行 (Continue Conversion)] をクリックします。

ステップ 6 確認ダイアログボックスで [はい (Yes)] をクリックして、そのメンバーを pWWN ベースのメンバーシップに変更します。

ゾーンセットの作成とメンバゾーンの追加



Tip アクティブゾーンセットを保存するのに、**copy running-config startup-config** コマンドを発行する必要はありません。ただし、明示的にフルゾーンセットを保存するには、**copy running-config startup-config** コマンドを発行する必要があります。ファブリックに複数のスイッチが含まれている場合は、**copy running-config startup-config fabric** コマンドを実行する必要があります。**fabric** キーワードを指定すると、**copy running-config startup-config** コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップ コンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。



Caution IVR に対しても設定されている VSAN 内のアクティブゾーンセットを非アクティブにした場合、アクティブ IVR ゾーンセット (IVZS) も非アクティブになり、スイッチとの間のすべての IVR トラフィックは停止されます。この非アクティブ化により、複数の VSAN でトラフィックが中断される場合があります。アクティブゾーンセットを非アクティブにする前に、VSAN のアクティブゾーン分析をチェックしてください ([ゾーンおよびゾーンセットの分析, on page 149](#)を参照)。IVZS を再度アクティブ化するには、標準ゾーンセットを再度アクティブ化する必要があります (『[Cisco MDS 9000 Series NX-OS Inter-VSAN Routing Configuration Guide](#)』を参照)。



Caution 現在アクティブなゾーンセットに IVR ゾーンが含まれている場合、IVR が有効になっていないスイッチからゾーンセットをアクティブにすると、その VSAN との間の IVR トラフィックが中断されます。常に IVR 対応のスイッチからゾーンセットをアクティブにして、IVR トラフィックの中断を回避することを強くお勧めします。



Note 仮想ターゲットの pWWN は、DCNM SAN クライアントのゾーン分割エンドデバイスのデータベースには表示されません。pWWN で仮想デバイスのゾーン分割を行う場合は、ゾーンを作成するときにこれを [Add Member to Zone] ダイアログボックスに入力する必要があります。ただし、デバイスエイリアスが拡張モードの場合、仮想デバイス名は DCNM SAN クライアントの [ゾーン分割 (Zoning)] ウィンドウの [デバイスエイリアス データベース (Device Alias Database)] に表示されます。この場合、デバイスエイリアス名を選択するか、[Add Member to Zone] ダイアログボックスで pWWN を入力することができます。

詳細については、[ゾーンメンバーの追加, on page 71](#)を参照してください。

複数のゾーンを含むゾーンセットを作成するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **zoneset name Zoneset1 vsan 3****Example:**

```
switch(config-zoneset)#
```

Zoneset1 というゾーンセットを設定します。

Tip ゾーンセットをアクティブにするには、まずゾーンとゾーンセットを1つ作成する必要があります。

ステップ 3 switch(config-zoneset)# **member Zone1**

指定されたゾーンセット (Zoneset1) に Zone1 をメンバーとして追加します。

Tip 指定されたゾーン名が事前に設定されていない場合、このコマンドを実行すると「Zone not present」エラーメッセージが返されます。

ステップ 4 switch(config-zoneset)# **zone name InlineZone1****Example:**

```
switch(config-zoneset-zone)#
```

指定されたゾーンセット (Zoneset1) にゾーン (InlineZone1) を追加します。

Tip ゾーンセットプロンプトからゾーンを作成する必要がある場合は、このステップを実行します。

ステップ 5 switch(config-zoneset-zone)# **member fcid 0x111112****Example:**

```
switch(config-zoneset-zone)#
```

新しいゾーン (InlineZone1) に新しいメンバー (FC ID 0x111112) を追加します。

Tip ゾーンセットプロンプトからゾーンにメンバーを追加する必要がある場合は、このステップを実行します。

名前に基づくゾーン、ゾーンセット、およびデバイス エイリアスのフィルタリング

ゾーン、ゾーンセット、またはデバイスエイリアスをフィルタする手順は、次のとおりです。

-
- ステップ 1** ツールバーにある [ゾーン (Zone)] アイコンをクリックします (図 12 : [Zone] アイコン, on page 69を参照)。
- ステップ 2** [Filter] テキストボックスに *zo1* などのフィルタ条件を入力します。
- ステップ 3** [移動 (Go)] をクリックします。
-

複数のゾーンセットへの複数のゾーンの追加

複数のゾーンセットに複数のゾーンを追加する手順は、次のとおりです。

-
- ステップ 1** ツールバーにある [ゾーン (Zone)] アイコンをクリックします (図 12 : [Zone] アイコン, on page 69を参照)。
- ステップ 2** ツリー表示から、[ゾーンセット (Zoneset)] を選択します。
- ステップ 3** Ctrl キーを使用して複数のエンド デバイスを選択します。
- ステップ 4** 右クリックし、[ゾーンセットに追加 (Add to Zoneset)] を選択します。
- ステップ 5** 表示されるポップアップ ウィンドウから、Ctrl キーを使用して複数のゾーンを選択します。
- ステップ 6** [Add] をクリックします。
- 選択されたゾーンが、選択されたゾーンセットに追加されます。
-

ゾーンの実行

ゾーン分割は、ソフトとハードの2つの方法で実行できます。各エンドデバイス (NポートまたはNLポート) は、ネームサーバーにクエリーを送信することでファブリックの他のデバイスを検出します。デバイスがネームサーバーにログインすると、ネームサーバーはクエリー元デバイスがアクセスできる他のデバイスのリストを返します。Nxポートがゾーンの外部にあるその他のデバイスのFCIDを認識しない場合、そのデバイスにアクセスできません。

ソフトゾーン分割では、ゾーン分割の制限がネームサーバーとエンドデバイス間の対話時にだけ適用されます。エンドデバイスが何らかの方法でゾーン外部のデバイスのFCIDを認識できる場合、そのデバイスにアクセスできます。

ハードゾーン分割は、Nxポートから送信される各フレームでハードウェアによって実行されます。スイッチにフレームが着信した時点で、発信元/宛先IDと許可済みの組み合わせが照合されるため、ワイヤスピードでフレームを送信できます。ハードゾーン分割は、ゾーン分割のすべての形式に適用されます。



Note ハードゾーン分割は、すべてのフレームでゾーン分割制限を実行し、不正なアクセスを防ぎます。

Cisco MDS 9000 シリーズのスイッチは、ハードおよびソフトの両方のゾーン分割をサポートしています。

ゾーンセットの配信

フルゾーンセットを配信するには、EXEC モード レベルでのワнтаイム配信またはコンフィギュレーション モード レベルでのフルゾーンセット配信のいずれかの方法を使用します。

フルゾーンセットを配信するには、ワнтаイム配信またはフルゾーンセット配信の2つの方法のうち、いずれかを使用します。

[Table 6: ゾーンセット配信 `zoneset distribution` コマンドの相違点](#), on page 91 に、これらの配信方法の相違を示します。

Table 6: ゾーンセット配信 `zoneset distribution` コマンドの相違点

ワнтаイム配信 <code>zoneset distribute vsan</code> コマンド (EXEC モード)	フルゾーンセット配信 <code>zoneset distribute full vsan</code> コマンド (コンフィギュレーション モード)
フルゾーンセットはすぐに配信されます。	フルゾーンセットはすぐには配信されません。
アクティブ化、非アクティブ化、またはマージ時には、アクティブゾーンセットと同時にフルゾーンセット情報を配信しません。	アクティブ化、非アクティブ化、またはマージ時には、アクティブゾーンセットと同時にフルゾーンセット情報を必ず配信してください。



Tip アクティブゾーンセットを保存するのに、`copy running-config startup-config` コマンドを発行する必要はありません。ただし、明示的にフルゾーンセットを保存するには、`copy running-config startup-config` コマンドを発行する必要があります。ファブリックに複数のスイッチが含まれている場合は、`copy running-config startup-config fabric` コマンドを実行する必要があります。`fabric` キーワードを指定すると、`copy running-config startup-config` コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップ コンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。

フルゾーンセットの配信の有効化

Cisco MDS 9000 シリーズのすべてのスイッチは、新しいEポートリンクが立ち上がったとき、または新しいゾーンセットが VSAN でアクティブ化されたときに、アクティブゾーンセットを配信します。ゾーンセットの配信は、隣接スイッチへの結合要求の送信時、またはゾーンセットのアクティブ化の際に行われます。

VSAN ベースですべてのスイッチへのフルゾーンセットおよびアクティブゾーンセットの配信を有効にするには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **zoneset distribute full vsan 33**

アクティブゾーンセットとともにフルゾーンセットの送信を有効にします。

DCNM SAN クライアントを使用したフルゾーンセット配信の有効化

DCNM SAN クライアントを使用して VSAN ベースですべてのスイッチへのフルゾーンセットおよびアクティブゾーンセットの配信を有効にするには、次の手順を実行します。

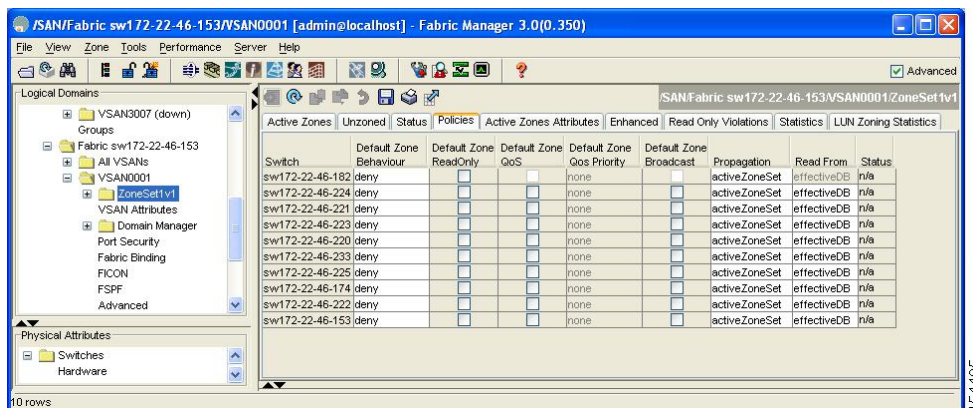
ステップ 1 [VSAN] を開き、[論理ドメイン (Logical Domains)] ペインでゾーンセットを選択します。

[Information] ペインにゾーンセットの設定が表示されます。[Active Zones] タブはデフォルトです。

ステップ 2 [Policies] タブをクリックします。

ゾーンの設定されたポリシーが表示されます (Figure 28: ゾーンに設定されたポリシー, on page 92 を参照)。

Figure 28: ゾーンに設定されたポリシー

**ステップ 3** [伝播 (Propagation)] カラムのドロップダウンメニューで [fullZoneset] を選択します。**ステップ 4** [変更の適用 (Apply Changes)] をクリックして、フルゾーンセットを伝播します。

ワンタイム配信のイネーブル化

この配信を実行するには、EXEC モードで **zoneset distribute vsan vsan-id** コマンドを使用します。

```
switch# zoneset distribute vsan 2
Zoneset distribution initiated. check zone status
```

この手順コマンドでは、フルゾーンセット情報が配信されるだけです。情報はスタートアップコンフィギュレーションには保存されません。フルゾーンセット情報をスタートアップコンフィギュレーションに保存するには、**copy running-config startup-config** コマンドを発行して、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明示的に保存する必要があります。



Note **zoneset distribute vsan vsan-id** コマンドによるフルゾーンセットのワンタイム配信は、**interop 2** および **interop 3** モードでサポートされていますが、**interop 1** モードではサポートされていません。

ゾーンセット一時配信要求のステータスを確認するには、**show zone status vsan vsan-id** コマンドを使用します。

```
switch# show zone status vsan 9
VSAN: 9 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
activation overwrite control:disabled
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 2002584 bytes
Zonesets:4 Zones:7004 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 94340 bytes
Name: zoneset-hac13-200 Zonesets:1 Zones:176
Current Total Zone DB Usage: 2096924 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Activation completed at 17:28:04 UTC Jun 16 2014
```

DCNM SAN クライアントを使用したワンタイム配信の有効化

ファブリック全体に、非アクティブで未変更のゾーンセットを一度だけ配信します。DCNM SAN クライアントを使用したフルゾーンセットのワンタイム配信を伝播する手順は、次のとおりです。

ステップ 1 [ゾーン (Zone)]> [Edit Local Full Zone Database] を選択します。

[Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ2 左側のペインでリストから適切なゾーンをクリックします。

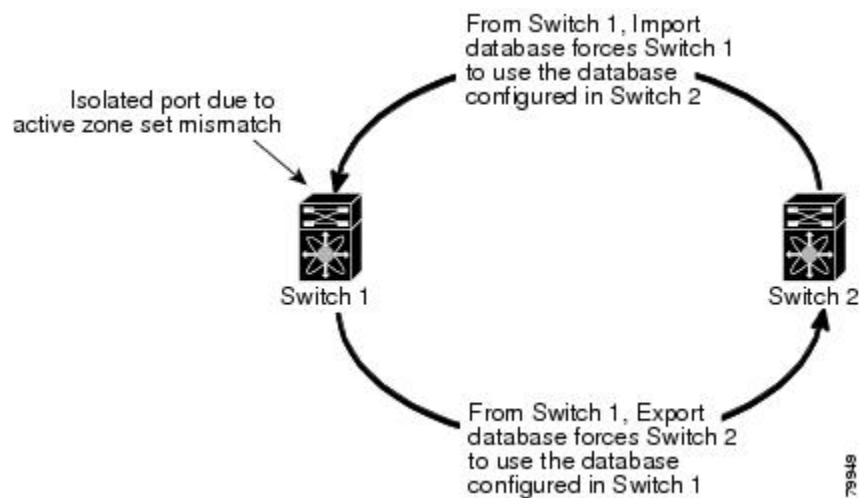
ステップ3 [配信 (Distribute)]をクリックして、ファブリック内でフルゾーンセットを配信します。

リンクの分離からの回復の概要

ファブリックの2つのスイッチがTEポートまたはEポートを使用してマージされる場合、アクティブゾーンセットのデータベースが2つのスイッチまたはファブリック間で異なると、このTEポートおよびEポートが分離することがあります。TEポートまたはEポートが分離した場合、次の3つのオプションのいずれかを使用して分離状態からポートを回復できます。

- 近接スイッチのアクティブゾーンセットのデータベースをインポートし、現在のアクティブゾーンセットと交換します (Figure 29: データベースのインポートとエクスポート, on page 94を参照)。
- 現在のデータベースを近接スイッチにエクスポートします。
- フルゾーンセットを編集し、修正されたゾーンセットをアクティブにしてから、リンクを立ち上げることにより、手動で矛盾を解決します。

Figure 29: データベースのインポートとエクスポート



ゾーンセットのインポートおよびエクスポート



Note **import** および **export** コマンドは、単一のスイッチから実行します。インポートとエクスポートをそれぞれ別のスイッチから行うと、再びリンクが分離する可能性があります。

ゾーンセット情報を隣接スイッチとの間でインポートまたはエクスポートするには、次の手順を実行します。

ステップ 1 switch# zoneset import interface fc1/3 vsan 2

VSAN 2 の fc 1/3 インターフェイスを介して接続された隣接スイッチからゾーンセットをインポートします。

ステップ 2 switch# zoneset import interface fc1/3 vsan 2-5

VSAN 範囲 2～5 の fc 1/3 インターフェイスを介して接続された隣接スイッチからゾーンセットをインポートします。

ステップ 3 switch# zoneset export vsan 5

VSAN 5 を介して接続された隣接スイッチにゾーンセットをエクスポートします。

ステップ 4 switch# zoneset export vsan 5-8

VSAN 5～8 の範囲を介して接続された隣接スイッチにゾーンセットをエクスポートします。

DCNM SAN クライアントを使用したゾーンセットのインポートおよびエクスポート

DCNM SAN クライアントを使用してゾーンセット情報を隣接スイッチとの間でインポートまたはエクスポートするには、次の手順を実行します。

ステップ 1 [ツール (Tools)] > [ゾーン マージ失敗のリカバリ (Zone Merge Fail Recovery)] を選択します。

[ゾーン マージ失敗のリカバリ (Zone Merge Fail Recovery)] ダイアログボックスが表示されます (Figure 30: [Zone Merge Failure Recovery] ダイアログボックス, on page 95を参照)。

Figure 30: [Zone Merge Failure Recovery] ダイアログボックス

**ステップ 2** [アクティブゾーンセットのインポート (Import Active Zoneset)]または[アクティブゾーンセットのエクスポート (Export Active Zoneset)] オプション ボタンを選択します。

- ステップ 3** ドロップダウンリストで、ゾーンセット情報のインポート元またはエクスポート先になるスイッチを選択します。
- ステップ 4** ドロップダウンリストで、ゾーンセット情報のインポート元またはエクスポート先になる VSAN を選択します。
- ステップ 5** インポート プロセスに使用するインターフェイスを選択します。
- ステップ 6** [OK] をクリックして、アクティブゾーンセットをインポートまたはエクスポートします。

import および **export** コマンドは、単一のスイッチから実行します。インポートとエクスポートをそれぞれ別のスイッチから行くと、再びリンクが分離する可能性があります。

ゾーンセットの複製

コピーを作成し、既存のアクティブゾーンセットを変更することなく編集できます。アクティブゾーンセットを **bootflash:** ディレクトリ、**volatile:** ディレクトリ、または **slot0** から次のいずれかのエリアにコピーすることができます。

- フルゾーンセット
- リモート ロケーション (FTP、SCP、SFTP、または TFTP を使用)

アクティブゾーンセットは、フルゾーンセットに含まれません。フルゾーンセットが失われた場合、または伝送されなかった場合に、既存のゾーンセットに変更を加え、アクティブにすることはできません。



Caution アクティブゾーンセットをフルゾーンセットにコピーする際に、同一名のゾーンがフルゾーンセットデータベースにすでに存在する場合は、上書きされる可能性があります。

ゾーンセットのコピー

Cisco MDS ファミリー シリーズでは、アクティブゾーンセットを編集できません。ただし、アクティブゾーンセットをコピーして、編集可能な新しいゾーンセットを作成できます。



Caution Inter-VSAN Routing (IVR) 機能が有効になっていて、IVR ゾーンがアクティブゾーンセット内に存在する場合、ゾーンセットコピー操作はすべての IVR ゾーンをフルゾーンデータベースにコピーします。IVR ゾーンへのコピーを防ぐには、コピー操作を実行する前に、フルゾーンセットデータベースから明示的に削除する必要があります。IVR 機能の詳細については、『[Cisco MDS 9000 Series NX-OS Inter-VSAN Routing Configuration Guide](#)』を参照してください。

ゾーンセットのコピーを作成するには、次の手順を実行します。

ステップ 1 switch# zone copy active-zoneset full-zoneset vsan 2

Example:

```
Please enter yes to proceed. (y/n) [n]? y
```

VSAN 2 のアクティブ ゾーンセットのコピーをフルゾーンセットに作成します。

ステップ 2 switch# zone copy vsan 3 active-zoneset scp://guest@myserver/tmp/active_zoneset.txt

SCP を使用して、VSAN 3 のアクティブゾーンをリモートロケーションにコピーします。

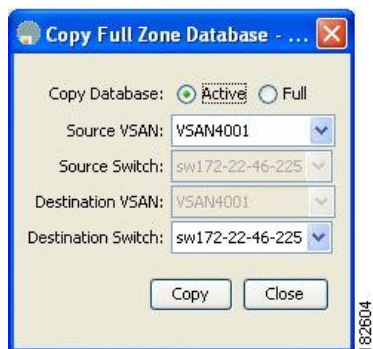
DCNM SAN クライアントを使用したゾーンセットのコピー

DCNM SAN クライアントを使用してゾーンセットをコピーする手順は、次のとおりです。

ステップ 1 [編集 (Edit)]> [フルゾーンデータベースのコピー (Copy Full Zone Database)] を選択します。

[フルゾーンデータベースのコピー (Copy Full Zone Database)] ダイアログボックスが表示されます (Figure 31: [Copy Full Zone Database] ダイアログボックス, on page 97 を参照)。

Figure 31: [Copy Full Zone Database] ダイアログボックス



ステップ 2 コピーするデータベースのタイプに応じて、[アクティブ (Active)] または [フル (Full)] オプションボタンをクリックします。

ステップ 3 ドロップダウンリストでコピー元 VSAN を選択します。

ステップ 4 [フルのコピー (Copy Full)] を選択した場合は、ドロップダウンリストでコピー元スイッチおよびコピー先 VSAN を選択します。

ステップ 5 ドロップダウンリストでコピー先のスイッチを選択します。

ステップ 6 [コピー (Copy)] をクリックしてデータベースをコピーします。

ゾーンのバックアップおよび復元の概要

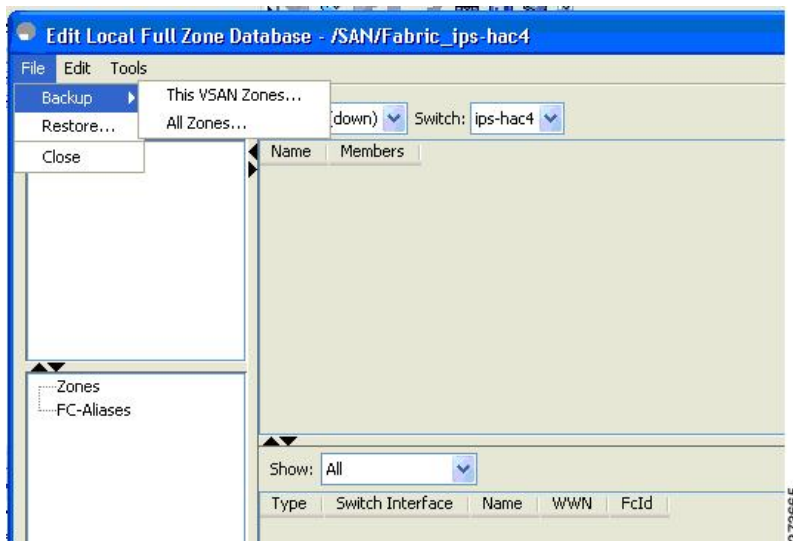
ゾーン設定をワークステーションにバックアップするには、TFTP 使用します。このゾーンバックアップファイルは、スイッチにゾーン設定を復元する場合に使用できます。ゾーン設定を復元すると、スイッチの既存のゾーン設定が上書きされます。

DCNM SAN クライアントを使用したゾーンのバックアップ

DCNM SAN クライアントを使用してフルゾーン構成をバックアップする手順は、次のとおりです。

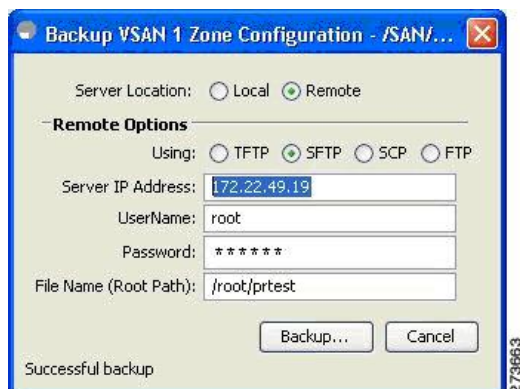
- ステップ 1 [Zone] > [Edit Local Full Zone Database] を選択します。[Select VSAN] ダイアログボックスが表示されます。
- ステップ 2 VSAN を選択して、[OK] をクリックします。選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます (Figure 32: [Edit Local Full Zone Database], on page 98 を参照)。

Figure 32: [Edit Local Full Zone Database]



- ステップ 3 [File] > [Backup] > [This VSAN Zones] を選択して、TFTP、SFTP、SCP、または FTP を使用して既存のゾーン設定をワークステーションにバックアップします。[ゾーン設定のバックアップ (Backup Zone Configuration)] ダイアログボックスが表示されます (Figure 33: [Backup Zone Configuration] ダイアログボックス, on page 99 を参照)。

Figure 33: [Backup Zone Configuration] ダイアログボックス



データをリモート サーバーにバックアップする前に、この設定を編集できます。

ステップ 4 次の [Remote Options] 情報を指定して、データをリモート サーバーにバックアップします。

- a) **Using** : プロトコルを選択します。
- b) **Server IP Address** : サーバーの IP アドレスを入力します。
- c) **UserName** : ユーザーの名前を入力します。
- d) **Password** : ユーザーのパスワードを入力します。
- e) **File Name(Root Path)** : パスとファイル名を入力します。

ステップ 5 [Backup] をクリックするか、[キャンセル (Cancel)] をクリックしてバックアップせずにダイアログボックスを閉じます。

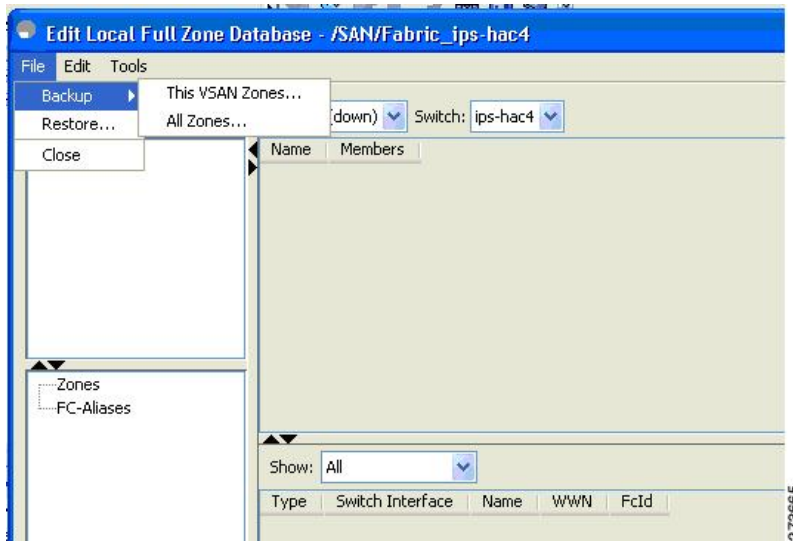
ゾーンの復元

DCNM SAN クライアントを使用してフル ゾーン構成を復元する手順は、次のとおりです。

ステップ 1 [Zone] > [Edit Local Full Zone Database] を選択します。[Select VSAN] ダイアログボックスが表示されます。

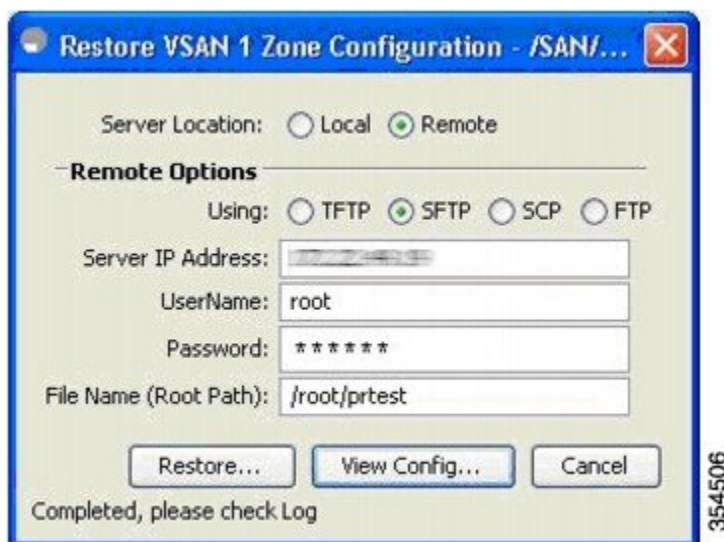
ステップ 2 VSAN を選択して、[OK] をクリックします。選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます (Figure 34: [Edit Local Full Zone Database], on page 100 を参照)。

Figure 34: [Edit Local Full Zone Database]



ステップ3 [File] > [Restore] を選択し、TFTP、SFTP、SCP、またはFTP を使用して、保存済みのゾーン設定を復元します。[ゾーン設定の復元 (Restore Zone Configuration)] ダイアログボックスが表示されます (Figure 35: [Restore Zone Configuration] ダイアログボックス, on page 100を参照)。

Figure 35: [Restore Zone Configuration] ダイアログボックス



スイッチにこの設定を復元する前に、設定を編集することもできます。

ステップ4 次の [Remote Options] 情報を指定して、データをリモートサーバーから復元します。

- a) [使用 (Using)]: プロトコルを選択します。
- b) [サーバーの IP アドレス (Server IP Address)]: サーバーの IP アドレスを入力します。
- c) [ユーザー名 (UserName)]: ユーザーの名前を入力します。
- d) [パスワード (Password)]: ユーザーのパスワードを入力します。

e) [ファイル名 (File Name)]: パスとファイル名を入力します。

ステップ 5 続行するには [Restore] をクリックします。復元を実行しないでダイアログボックスを閉じるには [キャンセル (Cancel)] をクリックします。

Note [設定の表示 (View Config)] をクリックして、リモート サーバーからゾーン設定ファイルを復元する方法に関する情報を確認します。このダイアログボックスで [はい (Yes)] をクリックすると、実行される CLI コマンドが表示されます。ダイアログボックスを閉じるには、[閉じる (Close)] をクリックします。

Note [Backup] および [Restore] のオプションは、Cisco NX-OS Release 4.1(3a) 以降が稼働しているスイッチで利用できます。

ゾーン、ゾーンセット、およびエイリアスの名前の変更



Note [Backup] オプションは、Cisco NX-OS Release 4.1(3) 以降を実行するスイッチで使用できません。復元オプションは、Cisco DCNM SAN クライアントリリース 4.1(3) 以降でのみサポートされています。

ゾーン、ゾーンセット、FC エイリアス、またはゾーン属性グループの名前を変更するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **zoneset rename oldname newname vsan 2**

指定された VSAN のゾーンセット名を変更します。

ステップ 3 switch(config)# **zone rename oldname newname vsan 2**

指定された VSAN のゾーン名を変更します。

ステップ 4 switch(config)# **fcalias rename oldname newname vsan 2**

指定された VSAN の fcalias 名を変更します。

ステップ 5 switch(config)# **zone-attribute-group rename oldname newname vsan 2**

指定された VSAN のゾーン属性グループ名を変更します。

ステップ 6 switch(config)# **zoneset activate name newname vsan 2**

ゾーンセットをアクティブにし、アクティブゾーンセット内の新しいゾーン名に更新します。

DCNM SAN クライアントを使用したゾーン、ゾーンセット、およびエイリアスの名前の変更

DCNM SAN クライアントを使用してゾーン、ゾーンセット、またはエイリアスの名前を変更する手順は、次のとおりです。

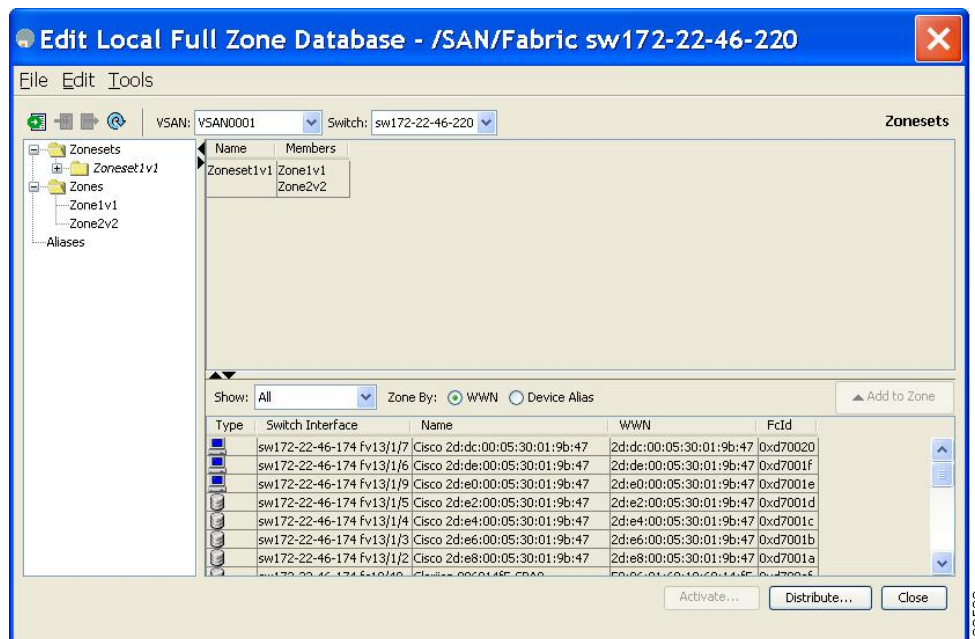
ステップ 1 [Zone] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます (Figure 36: [Edit Local Full Zone Database] ダイアログボックス, on page 102 を参照)。

Figure 36: [Edit Local Full Zone Database] ダイアログボックス



ステップ 3 左側のペインでゾーンまたはゾーンセットをクリックします。

ステップ 4 [編集 (Edit)] > [名前の変更 (Rename)] を選択します。

ゾーンまたはゾーンセット名の周囲にエディットボックスが表示されます。

ステップ 5 新しい名前を入力します。

ステップ 6 [アクティブ化 (Activate)] または [配信 (Distribute)] をクリックします。

ゾーン、ゾーンセット、FC エイリアス、およびゾーン属性グループのコピー

ゾーン、ゾーンセット、FC エイリアス、またはゾーン属性グループをコピーするには、次の手順を実行します。

ステップ 1 `switch# configure terminal`

コンフィギュレーション モードに入ります。

ステップ 2 `switch(config)# zoneset clone oldname newnamevsan 2`

指定された VSAN のゾーンセットをコピーします。

ステップ 3 `switch(config)# zone clone oldname newname vsan 2`

指定された VSAN 内のゾーンをコピーします。

ステップ 4 `switch(config)# fcalias clone oldname newnamevsan 2`

指定された VSAN の FC エイリアス名をコピーします。

ステップ 5 `switch(config)# zone-attribute-group clone oldname newname vsan 2`

指定された VSAN のゾーン属性グループをコピーします。

ステップ 6 `switch(config)# zoneset activate name newname vsan 2`

ゾーンセットをアクティブにし、アクティブ ゾーン セット内の新しいゾーン名に更新します。

DCNMSAN クライアントを使用したゾーン、ゾーンセット、FC エイリアス、およびゾーン属性グループのコピー

ゾーン、ゾーンセット、FC エイリアス、またはゾーン属性グループをコピーする手順は、次のとおりです。

ステップ 1 [ゾーン (Zone)]> [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3 [編集 (Edit)]> [クローン作成 (Clone)] を選択します。

[ゾーンセットのクローン作成 (Clone Zoneset)] ダイアログボックスが表示されます (Figure 37: [Clone Zoneset] ダイアログボックス, on page 104を参照)。デフォルトの名前は「Clone」の後ろに元の名前が付きます。

Figure 37: [Clone Zoneset] ダイアログボックス



ステップ 4 コピーされたエントリの名前を変更します。

ステップ 5 [OK] をクリックして新しいコピーを保存します。

コピーされたデータベースは、元のデータベースとともに表示されます。

MDS 以外のデータベースの移行

Zone Migration ウィザードを使用して DCNM SAN クライアントを使用した MDS 以外のデータベースを移行する手順は、次のとおりです。

ステップ 1 [ゾーン (Zone)] > [MDS 以外のデータベースの移行 (Migrate Non-MDS Database)] を選択します。

Zone Migration ウィザードが表示されます。

ステップ 2 ウィザードのプロンプトに従って、データベースを移行します。

ゾーン サーバー データベースのクリア

指定された VSAN のゾーン サーバー データベース内のすべての設定情報をクリアできます。

ゾーン サーバー データベースをクリアするには、次のコマンドを使用します。

```
switch# clear zone database vsan 2
```



Note ゾーンサーバーデータベースのクリアについては、『Cisco MDS 9000 Series NX-OS Fabric Configuration Guide』を参照してください。



Note `clear zone database` コマンドを実行した後に、明示的に `copy running-config startup-config` を実行して、スイッチの再起動時に確実に実行コンフィギュレーションが使用されるようにする必要があります。



Note ゾーンセットをクリアすると、フルゾーン データベースだけが消去され、アクティブゾーン データベースは消去されません。



Note ゾーン サーバー データベースをクリアした後に、明示的に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て、スイッチの再起動時に実行コンフィギュレーションが使用されるようにする必要があります。

詳細なゾーン属性

ゾーンベースのトラフィック プライオリティの概要

ゾーン分割機能は、ファブリック内の特定のゾーンのプライオリティを設定し、デバイス間のアクセスコントロールを設定するための追加の分離メカニズムを提供します。この機能を使用して、Quality Of Service (QoS) プライオリティをゾーン属性として設定できます。QoS トラフィックプライオリティを `high`、`medium`、または `low` に割り当てることができます。デフォルトでは、プライオリティが指定されていないゾーンは暗黙的に `low` プライオリティを割り当てられます。詳細については、『[Cisco MDS 9000 NX-OS Series Quality of Service Configuration Guide](#)』を参照してください。

この機能を使用するには、ENTERPRISE_PKG ライセンスを取得し（『[Cisco NX-OS Series Licensing Guide](#)』を参照）、スイッチで QoS を有効にする必要があります（『[Cisco MDS 9000 Series NX-OS Quality of Service Configuration Guide](#)』を参照）。

この機能により、SAN 管理者は使い慣れたデータ フロー識別パラダイムの観点から QoS を設定できます。この属性は、ゾーン メンバーごとではなく、ゾーン全体で設定できます。



Caution ゾーンベースの QoS がスイッチで実装される場合、その VSAN で `interop` モードを設定することはできません。

ゾーンベースのトラフィック プライオリティの設定

ゾーンプライオリティを設定するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **zone name QosZone vsan 2****Example:**

```
switch(config-zone)#
```

エリアス名 (QosZone) を設定し、ゾーン 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-zone)# **attribute-group qos priority high****Example:**

このゾーンを設定して、拡張モードでこのゾーンと一致する各フレームに高プライオリティの QoS トラフィックを割り当てます。

ステップ 4 switch(config-zone)# **attribute qos priority {high | low | medium}**

このゾーンを設定して、このゾーンと一致する各フレームに QoS トラフィックを割り当てます。

ステップ 5 switch(config-zone)# **exit****Example:**

```
switch(config)#
```

コンフィギュレーション モードに戻ります。

ステップ 6 switch(config)# **zoneset name QosZoneset vsan 2****Example:**

```
switch(config-zoneset)#
```

指定された VSAN (vsan 2) のゾーンセット QosZoneset を設定し、ゾーンセット コンフィギュレーション サブモードを開始します。

Tip ゾーンセットをアクティブにするには、まずゾーンとゾーンセットを1つ作成する必要があります。

ステップ 7 switch(config-zoneset)# **member QosZone**

指定されたゾーンセット (QosZoneset) に QosZone をメンバーとして追加します。

Tip 指定されたゾーン名が事前に設定されていない場合、このコマンドを実行すると「Zone not present」エラーメッセージが返されます。

ステップ 8 switch(config-zoneset)# **exit****Example:**

```
switch(config)#
```

コンフィギュレーションモードに戻ります。

ステップ 9 switch(config)# zoneset activate name QosZoneset vsan 2

指定されたゾーンセットをアクティブにします。

DCNM SAN クライアントを使用したゾーンベースのトラフィック優先順位の構成

DCNMSAN クライアントを使用してゾーン優先順位を構成するには、次の手順を実行します。

ステップ 1 [VSAN] を開き、[論理ドメイン (Logical Domains)] ペインでゾーンセットを選択します。

ステップ 2 [情報 (Information)] ペインで [ポリシー (Policies)] タブをクリックします。

[Information] ペインにゾーンポリシー情報が表示されます (Figure 38: [Information] ペインの [Zone Policies] ペイン, on page 107 を参照)。

Figure 38: [Information] ペインの [Zone Policies] ペイン

Switch	Default Zone Behaviour	Default Zone ReadOnly	Default Zone QoS	Default Zone Qos Priority	Default Zone Broadcast	Propagation	Read From	Status
sw172-22-46-182	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a
sw172-22-46-224	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a
sw172-22-46-221	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a
sw172-22-46-223	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a
sw172-22-46-220	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a
sw172-22-46-233	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a
sw172-22-46-225	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a
sw172-22-46-174	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a
sw172-22-46-222	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a
sw172-22-46-153	deny	<input type="checkbox"/>		none	<input type="checkbox"/>	activeZoneSet	effectiveDB	n/a

ステップ 3 チェックボックスとドロップダウンメニューを使用して、デフォルトゾーンの QoS を設定します。

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

デフォルトゾーンの QoS プライオリティ属性の設定

QoS プライオリティ属性の設定変更は、関連付けられたゾーンのゾーンセットをアクティブ化したときに有効になります。



Note メンバーが QoS プライオリティ属性が異なる 2 つのゾーンの一部の場合は、より高い QoS プライオリティ値が実装されます。最初の一致エントリが実装されるので、VSAN ベースの QoS ではこの状況は発生しません。

デフォルトゾーンの QoS プライオリティ属性を設定するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

Example:

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **zone default-zone vsan 1**

Example:

```
switch(config-default-zone)#
```

ゾーン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-default-zone)# **attribute qos priority high**

これらのゾーンと一致するフレームに対して QoS プライオリティ属性を設定します。

ステップ 4 switch(config-default-zone)# **no attribute qos priority high**

デフォルトゾーンの QoS プライオリティ属性を削除して、デフォルトの低プライオリティに戻します。

DCNM SAN クライアントを使用したデフォルトゾーンの QoS 優先順位属性の構成

DCNM SAN クライアントを使用してデフォルトゾーンの QoS 優先順位属性を構成するには、次の手順を実行します。

ステップ 1 [ゾーン (Zone)]> [Edit Local Full Zone Database] を選択します。

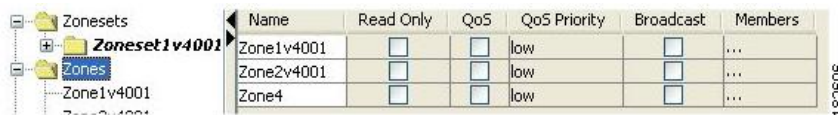
[Select VSAN] ダイアログボックスが表示されます。

ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3 デフォルトゾーンに QoS プライオリティ属性を設定するには、[編集 (Edit)]> [デフォルトゾーン属性の編集 (Edit Default Zone Attributes)] を選択します ([Figure 39: QoS プライオリティ属性, on page 109](#)を参照)。

Figure 39: QoS プライオリティ属性



Name	Read Only	QoS	QoS Priority	Broadcast	Members
Zone1v4001	<input type="checkbox"/>	<input type="checkbox"/>	low	<input type="checkbox"/>	...
Zone2v4001	<input type="checkbox"/>	<input type="checkbox"/>	low	<input type="checkbox"/>	...
Zone4	<input type="checkbox"/>	<input type="checkbox"/>	low	<input type="checkbox"/>	...

ステップ 4 [プライオリティを持つ QoS トラフィックを許可 (Permit QoS Traffic with Priority)] チェックボックスをオンにして、[QoS プライオリティ (Qos Priority)] ドロップダウンメニューを [低 (low)]、[中 (medium)]、または [高 (high)] に設定します。

ステップ 5 [OK] をクリックして変更を保存します。

デフォルトゾーンポリシーの設定

DCNM SAN クライアントを使用してデフォルトゾーンでトラフィックを許可または拒否するには、次の手順を実行します。

ステップ 1 [ゾーン (Zone)] > [Edit Local Full Zone Database] を選択します。

[Select VSAN] ダイアログボックスが表示されます。

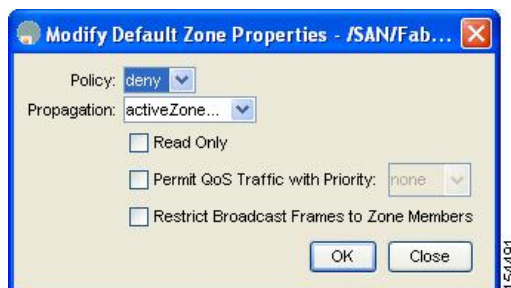
ステップ 2 VSAN を選択して、[OK] をクリックします。

選択した VSAN の [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3 デフォルトゾーンに QoS プライオリティ属性を設定するには、[編集 (Edit)] > [デフォルトゾーン属性の編集 (Edit Default Zone Attributes)] を選択します。

[デフォルトゾーンプライオリティの変更 (Modify Default Zone Properties)] ダイアログボックスが表示されます (Figure 40: [Modify Default Zone Properties] ダイアログボックス, on page 109 を参照)。

Figure 40: [Modify Default Zone Properties] ダイアログボックス



ステップ 4 デフォルトゾーンでトラフィックを許可するには [ポリシー (Policy)] ドロップダウンメニューを [許可 (permit)] に設定し、デフォルトゾーンでトラフィックをブロックするには [拒否 (deny)] に設定します。

ステップ 5 [OK] をクリックして変更を保存します。

スマート ゾーン分割の概要

スマートゾーン分割では、従来必要とされていたよりも少ないハードウェアリソースで、大きなゾーンのハードゾーン分割が行われます。従来のゾーン分割方式では、ゾーン内の各デバイスが相互に通信できます。管理者はゾーン設定ガイドラインに従って個々のゾーンを管理する必要があります。スマートゾーン分割では、1つのターゲットゾーンへの1つのイニシエータを作成する必要がありません。FCNS のデバイス タイプ情報を分析することで、Cisco MDS NX-OS ソフトウェアによりハードウェア レベルで有用な組み合わせが実装されます。使用されていない組み合わせは無視されます。たとえば、イニシエータとイニシエータのペアではなく、イニシエータとターゲットのペアが設定されます。次の場合、デバイスは不明なものとして扱われます。

- デバイスに関して FC4 タイプが登録されていない。
- ゾーン変換時に、デバイスがファブリックにログインしていない。
- ゾーンは作成されているが、イニシエータとターゲットのいずれかまたは両方が指定されていない。

スマートゾーン内の各デバイスのデバイス タイプ情報は、ファイバチャネルネームサーバー (FCNS) データベースから `host`、`target`、または `both` として自動的に取り込まれます。この情報により、イニシエータ ターゲット ペアが指定され、ハードウェアではそれらのペアだけが設定されるため、スイッチハードウェアをより効率的に使用できるようになります。特殊な状況 (別のディスク コントローラと通信する必要があるディスク コントローラなど) では、完全な制御を実現するため、スマートゾーン分割のデフォルトが管理者により上書きされることがあります。



Note

- スマートゾーン分割は VSAN レベルで有効にできますが、ゾーン レベルで無効にすることもできます。
- DMM、IOA、または SME アプリケーションが有効になっている VSAN では、スマートゾーン分割はサポートされていません。

スマート ゾーン分割のメンバー設定

次の表に、サポートされているスマートゾーン分割のメンバー設定を示します。

Table 7: スマートゾーン分割の設定

機能	サポートあり
PWWN	はい
FCID	はい

機能	サポートあり
FC エイリアス	はい
デバイスエイリアス	はい
インターフェイス	いいえ
IP アドレス	いいえ
シンボル ノード名	いいえ
FWWN	いいえ
ドメイン ID	不可

VSAN でのスマート ゾーン分割の有効化

VSAN に対して **smart zoning** を設定するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **zone smart-zoning enable vsan 1**

VSAN でスマート ゾーン分割を有効にします。

ステップ 3 switch(config)# **no zone smart-zoning enable vsan 1**

VSAN でスマート ゾーン分割を無効にします。

スマート ゾーン分割のデフォルト値の設定

デフォルト値を設定するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **system default zone smart-zone enable**

指定されたデフォルト値に基づいて作成された VSAN でスマート ゾーン分割を有効にします。

ステップ 3 switch(config)# **no system default zone smart-zone enable**

VSAN でスマート ゾーン分割を無効にします。

スマート ゾーン分割へのゾーンの自動変換

ネーム サーバーからデバイス タイプ情報を取得し、その情報をメンバーに追加するには、次の手順を実行します。これは、ゾーン、ゾーンセット、FC エイリアス、および VSAN のレベルで実行できます。ゾーンセットがスマート ゾーン分割に変換されたら、ゾーンセットをアクティブにする必要があります。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **zone convert smart-zoning fcalias name <alias-name> vsan <vsan no>**

FC エイリアス メンバーのデバイス タイプ情報をネーム サーバーから取得します。

Note zone convert コマンドを実行すると、FC4 タイプは SCSI-FCP になります。SCSI-FCP には、デバイスがイニシエータかターゲットかを決定するビットがあります。イニシエータとターゲットの両方が設定されている場合、デバイスは両方として扱われます。

ステップ 3 switch(config)# **zone convert smart-zoning zone name <zone name> vsan <vsan no>**

ゾーン メンバーのデバイス タイプ情報をネーム サーバーから取得します。

ステップ 4 switch(config)# **zone convert smart-zoning zoneset name <zoneset name> vsan <vsan no>**

指定されたゾーンセットで、すべてのゾーンと FC エイリアス メンバーのデバイス タイプ情報をネーム サーバーから取得します。

ステップ 5 switch(config)# **zone convert smart-zoning vsan <vsan no>**

VSAN 内に存在するすべてのゾーンセットのすべてのゾーンと FC エイリアス メンバーのデバイス タイプ情報をネーム サーバーから取得します。

ステップ 6 switch(config)# **show zone smart-zoning auto-conv status vsan 1**

VSAN の以前の自動変換ステータスが表示されます。

ステップ 7 switch(config)# **show zone smart-zoning auto-conv log errors**

スマート ゾーン分割自動変換のエラー ログが表示されます。

What to do next

デバイスがイニシエータ、ターゲット、またはその両方であるかどうかを確認するには、show fens database コマンドを使用します。


```
switch# show fcns database
VSAN 1:
-----
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
-----
0x9c0000 N 21:00:00:e0:8b:08:96:22 (Company 1) scsi-fcp:init
0x9c0100 N 10:00:00:05:30:00:59:1f (Company 2) ipfc
0x9c0200 N 21:00:00:e0:8b:07:91:36 (Company 3) scsi-fcp:init
0x9c03d6 NL 21:00:00:20:37:46:78:97 (Company 4) scsi-fcp:target
```

ゾーンメンバーのデバイスタイプの設定



Note デバイスタイプがスマートゾーン分割で明示的に構成されている場合、デバイスは、そのデバイスがメンバーであるすべてのゾーンで同じタイプで構成されている必要があります。ゾーンメンバーは、一部のゾーンでイニシエータとして、他のゾーンではターゲットとして構成されてはなりません。

ゾーンメンバーのデバイスタイプを設定するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config-zoneset-zone)# **member device-alias name both**

デバイスエイリアスメンバーのデバイスタイプを **both** として設定します。サポートされる各メンバータイプでは、**init**、**target**、および **both** がサポートされています。

ステップ 3 switch(config-zoneset-zone)# **member pwwn number target**

pwwn メンバーのデバイスタイプを **target** として設定します。サポートされる各メンバータイプでは、**init**、**target**、および **both** がサポートされています。

ステップ 4 switch(config-zoneset-zone)# **member fcid number**

FCID メンバーのデバイスタイプを設定します。設定されている特定のデバイスタイプがありません。サポートされる各メンバータイプでは、**init**、**target**、および **both** がサポートされています。

Note ゾーンメンバーに対して特定のデバイスタイプが設定されていない場合は、バックエンドで、生成されたゾーンエントリがデバイスタイプ **both** として作成されます。

スマートゾーン分割設定の削除

スマートゾーン分割設定を削除するには、次の手順を実行します。

ステップ 1 `switch(config)# clear zone smart-zoning fcalias name alias-name vsan number`

指定された FC エイリアスのすべてのメンバーのデバイス タイプ設定を削除します。

ステップ 2 `switch(config)# clear zone smart-zoning zone name zone name vsan number`

指定されたゾーンのすべてのメンバーのデバイス タイプ設定を削除します。

ステップ 3 `switch(config)# clear zone smart-zoning zoneset name zoneset name vsan number`

指定されたゾーンセットの FC エイリアスとゾーンのすべてのメンバーのデバイス タイプ設定を削除します。

ステップ 4 `switch(config)# clear zone smart-zoning vsan number`

VSAN の指定されたゾーンセットの FC エイリアスとゾーンのすべてメンバーのデバイス タイプ設定を削除します。

基本ゾーン分割モードにおけるゾーンレベルでのスマートゾーン分割の無効化

基本ゾーン分割モードの VSAN に対してゾーンレベルでスマートゾーン分割を無効にするには、次の手順を実行します。

ステップ 1 `switch# configure terminal`

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# zone name zone1 vsan 1`

ゾーン名を設定します。

ステップ 3 `switch(config-zone)# attribute disable-smart-zoning`

選択されたゾーンに対してスマートゾーン分割を無効にします。

Note このコマンドでは、選択されたゾーンのスマートゾーン分割が無効になるだけです。デバイス タイプ設定は削除されません。

拡張ゾーン分割モードの VSAN に対するゾーンレベルでのスマートゾーン分割の無効化

拡張ゾーン分割モードの VSAN に対してゾーンレベルでスマートゾーン分割を無効にするには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **zone-attribute-group name disable-sz vsan 1**

拡張ゾーン セッションを作成します。

ステップ 3 switch(config-attribute-group)#**disable-smart-zoning**

選択されたゾーンに対してスマート ゾーン分割を無効にします。

Note このコマンドでは、選択されたゾーンのスマート ゾーン分割が無効になるだけです。デバイス タイプ設定は削除されません。

ステップ 4 switch(config-attribute-group)# **zone name prod vsan 1**

ゾーン名を設定します。

ステップ 5 switch(config-zone)# **attribute-group disable-sz**

選択されたゾーンのグループ属性名を割り当てるように設定します。

ステップ 6 switch(config-zone)# **zone commit vsan 1**

選択された VSAN に対するゾーン分割の変更を確定します。

DCNM SAN クライアントを使用したゾーンレベルでのスマートゾーン分割の無効化

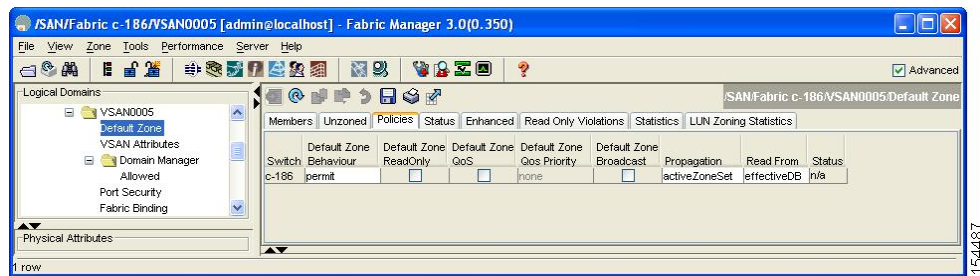
DCNM SAN クライアントを使用した基本ゾーン分割モードでフレームをブロードキャストするには、次の手順を実行します。

ステップ 1 [VSAN] を開き、[論理ドメイン (Logical Domains)] ペインでゾーンセットを選択します。

ステップ 2 [情報 (Information)] ペインで [ポリシー (Policies)] タブをクリックします。

[情報 (Information)] ペインにゾーン ポリシー情報が表示されます。

Figure 41: ゾーン ポリシー情報



ステップ 3 [ブロードキャスト (Broadcast)]チェックボックスをオンにして、デフォルトゾーン上でブロードキャストフレームをイネーブルにします。

ステップ 4 [変更の適用 (Apply Changes)]をクリックして、変更を保存します。

ゾーン情報の表示

ゾーン情報を表示するには、**show** コマンドを使用します。特定のオブジェクトの情報（たとえば、特定のゾーン、ゾーンセット、VSAN、エイリアス、または **brief** や **active** などのキーワード）を要求する場合、指定されたオブジェクトの情報だけが表示されます。特定の情報を要求しない場合、入手できるすべての情報が表示されます。

すべての VSAN のゾーン情報の表示

```
switch# show zone
zone name Zone3 vsan 1
  pwnn 21:00:00:20:37:6f:db:dd
  pwnn 21:00:00:20:37:9c:48:e5
zone name Zone2 vsan 2
  fwwn 20:41:00:05:30:00:2a:1e
  fwwn 20:42:00:05:30:00:2a:1e
  fwwn 20:43:00:05:30:00:2a:1e
zone name Zone1 vsan 1
  pwnn 21:00:00:20:37:6f:db:dd
  pwnn 21:00:00:20:37:a6:be:2f
  pwnn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
zone name Techdocs vsan 3
  ip-address 10.15.0.0 255.255.255.0
zone name Zone21 vsan 5
  pwnn 21:00:00:20:37:a6:be:35
  pwnn 21:00:00:20:37:a6:be:39
  fcid 0xe000ef
  fcid 0xe000e0
  symbolic-nodename iqn.test
  fwwn 20:1f:00:05:30:00:e5:c6
  fwwn 12:12:11:12:11:12:12:10
  interface fc1/5 swwn 20:00:00:05:30:00:2a:1e
  ip-address 12.2.4.5 255.255.255.0
  fcalias name Alias1 vsan 1
    pwnn 21:00:00:20:37:a6:be:35
zone name Zone2 vsan 11
```

```
interface fcl/5 pwwn 20:4f:00:05:30:00:2a:1e
zone name Zone22 vsan 6
  fcalias name Alias1 vsan 1
  pwwn 21:00:00:20:37:a6:be:35
zone name Zone23 vsan 61
  pwwn 21:00:00:04:cf:fb:3e:7b lun 0000
```

特定の VSAN のゾーン情報の表示

```
switch# show zone vsan 1
zone name Zone3 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5
zone name Zone2 vsan 1
  fwwn 20:4f:00:05:30:00:2a:1e
  fwwn 20:50:00:05:30:00:2a:1e
  fwwn 20:51:00:05:30:00:2a:1e
  fwwn 20:52:00:05:30:00:2a:1e
  fwwn 20:53:00:05:30:00:2a:1e
zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
```

設定されたゾーンセットを表示するには、**show zoneset** コマンドを使用します。

設定されたゾーンセット情報の表示

```
switch# show zoneset vsan 1
zoneset name ZoneSet2 vsan 1
  zone name Zone2 vsan 1
    fwwn 20:4e:00:05:30:00:2a:1e
    fwwn 20:4f:00:05:30:00:2a:1e
    fwwn 20:50:00:05:30:00:2a:1e
    fwwn 20:51:00:05:30:00:2a:1e
    fwwn 20:52:00:05:30:00:2a:1e
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
zoneset name ZoneSet1 vsan 1
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
```

VSAN 範囲の設定されたゾーンセット情報の表示

```
switch# show zoneset vsan 2-3
zoneset name ZoneSet2 vsan 2
  zone name Zone2 vsan 2
    fwwn 20:52:00:05:30:00:2a:1e
    fwwn 20:53:00:05:30:00:2a:1e
    fwwn 20:54:00:05:30:00:2a:1e
    fwwn 20:55:00:05:30:00:2a:1e
    fwwn 20:56:00:05:30:00:2a:1e
```

```

zone name Zone1 vsan 2
  pwn 21:00:00:20:37:6f:db:dd
  pwn 21:00:00:20:37:a6:be:2f
  pwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
zoneset name ZoneSet3 vsan 3
  zone name Zone1 vsan 1
    pwn 21:00:00:20:37:6f:db:dd
    pwn 21:00:00:20:37:a6:be:2f
    pwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1

```

特定のゾーンのメンバーを表示するには、**show zone name** コマンドを使用します。

ゾーンのメンバーの表示

```

switch# show zone name Zone1
zone name Zone1 vsan 1
  pwn 21:00:00:20:37:6f:db:dd
  pwn 21:00:00:20:37:a6:be:2f
  pwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1

```

FC エイリアス設定を表示するには、**show fcalias** コマンドを使用します。

FC エイリアス設定の表示

```

switch# show fcalias vsan 1
fcalias name Alias2 vsan 1
fcalias name Alias1 vsan 1
  pwn 21:00:00:20:37:6f:db:dd
  pwn 21:00:00:20:37:9c:48:e5

```

FC ID を使用してメンバーが所属するすべてのゾーンを表示するには、**show zone member** コマンドを使用します。

メンバーシップ ステータスの表示

```

switch# show zone member pwn 21:00:00:20:37:9c:48:e5
          VSAN: 1
zone Zone3
zone Zone1
fcalias Alias1

```

他のスイッチで交換された制御フレームの数を表示するには、**show zone statistics** コマンドを使用します。

ゾーン統計情報の表示

```

switch# show zone statistics
Statistics For VSAN: 1
*****
Number of Merge Requests Sent: 24
Number of Merge Requests Recvd: 25
Number of Merge Accepts Sent: 25
Number of Merge Accepts Recvd: 25

```

```

Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0
Statistics For VSAN: 2
*****
Number of Merge Requests Sent: 4
Number of Merge Requests Recvd: 4
Number of Merge Accepts Sent: 4
Number of Merge Accepts Recvd: 4
Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0

```

LUN ゾーン統計情報の表示

```

switch# show zone statistics lun-zoning
LUN zoning statistics for VSAN: 1
*****
S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:00
-----
Number of Inquiry commands received:          10
Number of Inquiry data No LU sent:            5
Number of Report LUNs commands received:      10
Number of Request Sense commands received:     1
Number of Other commands received:            0
Number of Illegal Request Check Condition sent: 0
S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:01
-----
Number of Inquiry commands received:          1
Number of Inquiry data No LU sent:            1
Number of Request Sense commands received:     1
Number of Other commands received:            0
Number of Illegal Request Check Condition sent: 0

```

LUN ゾーン統計情報の表示

```

Need the latest output
switch# show zone statistics read-only-zoning
Read-only zoning statistics for VSAN: 2
*****
S-ID: 0x33333, D-ID: 0x11111, LUN: 00:00:00:00:00:00:00:64
-----
Number of Data Protect Check Condition Sent:   12

```

アクティブゾーンセットの表示

```

switch# show zoneset active
zoneset name ZoneSet1 vsan 1
zone name zonel vsan 1

```

```

    fcid 0x080808
    fcid 0x090909
    fcid 0x0a0a0a
zone name zone2 vsan 1
* fcid 0xef0000 [pwn 21:00:00:20:37:6f:db:dd]
* fcid 0xef0100 [pwn 21:00:00:20:37:a6:be:2f]

```

ゾーンセットの簡単な説明の表示

```

switch# show zoneset brief
zoneset name ZoneSet1 vsan 1
  zone zone1
  zone zone2

```

アクティブゾーンの表示

```

switch# show zone active
zone name Zone2 vsan 1
* fcid 0x6c01ef [pwn 21:00:00:20:37:9c:48:e5]
zone name IVRZ_IvrZone1 vsan 1
  pwn 10:00:00:00:77:99:7a:1b
* fcid 0xce0000 [pwn 10:00:00:00:c9:2d:5a:dd]
zone name IVRZ_IvrZone4 vsan 1
* fcid 0xce0000 [pwn 10:00:00:00:c9:2d:5a:dd]
* fcid 0x6c01ef [pwn 21:00:00:20:37:9c:48:e5]
zone name Zone1 vsan 1667
  fcid 0x123456
zone name $default_zone$ vsan 1667

```

アクティブゾーンセットの表示

```

switch# show zoneset active
zoneset name ZoneSet4 vsan 1
  zone name Zone2 vsan 1
    * fcid 0x6c01ef [pwn 21:00:00:20:37:9c:48:e5]
  zone name IVRZ_IvrZone1 vsan 1
    pwn 10:00:00:00:77:99:7a:1b
    * fcid 0xce0000 [pwn 10:00:00:00:c9:2d:5a:dd]
zoneset name QosZoneset vsan 2
  zone name QosZone vsan 2
  attribute qos priority high
  * fcid 0xce0000 [pwn 10:00:00:00:c9:2d:5a:dd]
  * fcid 0x6c01ef [pwn 21:00:00:20:37:9c:48:e5]
Active zoneset vsan 1667
  zone name Zone1 vsan 1667
    fcid 0x123456
  zone name $default_zone$ vsan 1667

```

ゾーンステータスの表示

```

switch(config)# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address

```



```
activation overwrite control:disabled
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Current Total Zone DB Usage: 4 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 4 / 2097152 bytes (0 % used)
Status:
VSAN: 8 default-zone: deny distribute: full Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 1946498 bytes
Zonesets:6 Zones:8024 Aliases: 0
Active Zoning Database :
DB size: 150499 bytes
Name: zoneset-1000 Zonesets:1 Zones:731
Current Total Zone DB Usage: 2096997 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 2096997 / 2097152 bytes (99 % used)
Status: Zoneset distribution failed [Error: Fabric changing Dom 33]:
at 17:05:06 UTC Jun 16 2014
VSAN: 9 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 2002584 bytes
Zonesets:4 Zones:7004 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 94340 bytes
Name: zoneset-hac13-200 Zonesets:1 Zones:176
Current Total Zone DB Usage: 2096924 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Activation completed at 17:28:04 UTC Jun 16 2014
VSAN: 12 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
```

```

DB size: 84 bytes
Zonesets:0 Zones:1 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 144 bytes
Name: zs1 Zonesets:1 Zones:2
Current Total Zone DB Usage: 228 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Commit completed at 14:39:33 UTC Jun 27 201

```

設定されたすべてのゾーンのゾーン属性を表示するには、**show zone** コマンドを使用します。

ゾーン統計情報の表示

```

switch# show zone
zone name lunSample vsan 1          <-----Read-write attribute
zone name ReadOnlyZone vsan 2
    attribute read-only              <-----Read-only attribute

```

設定されたインターフェイスベースゾーンを表示するには、**show running** コマンドおよび**show zone active** コマンドを使用します。

インターフェイス ベース ゾーン の表示

```

switch# show running zone name if-zone vsan 1
    member interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2
    member fwwn 20:4f:00:0c:88:00:4a:e2
    member interface fc2/1 swwn 20:00:00:05:30:00:4a:9e
    member pwwn 22:00:00:20:37:39:6b:dd

```

アクティブゾーンのfWWNおよびインターフェイスの表示

```

switch# show zone active zone name if-zone vsan 1
* fcid 0x7e00b3 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
* fcid 0x7e00b1 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
* fcid 0x7e00ac [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
* fcid 0x7e00b3 [fwwn 20:4f:00:0c:88:00:4a:e2]
* fcid 0x7e00b1 [fwwn 20:4f:00:0c:88:00:4a:e2]
* fcid 0x7e00ac [fwwn 20:4f:00:0c:88:00:4a:e2]
    interface fc2/1 swwn 20:00:00:05:30:00:4a:9e

```

同様の出力は、リモートスイッチでも入手できます（次の例を参照）。

リモートスイッチのローカルインターフェイスのアクティブゾーン詳細の表示

```

switch# show zone active zone name if-zone vsan 1
* fcid 0x7e00b3 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
* fcid 0x7e00b1 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
* fcid 0x7e00ac [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
* fcid 0x7e00b3 [fwwn 20:4f:00:0c:88:00:4a:e2]
* fcid 0x7e00b1 [fwwn 20:4f:00:0c:88:00:4a:e2]
* fcid 0x7e00ac [fwwn 20:4f:00:0c:88:00:4a:e2]
    interface fc2/1 swwn 20:00:00:05:30:00:4a:9e

```

VSAN のゾーン ステータスの表示

```
switch(config)# show zone status vsan 1
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
activation overwrite control:disabled
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Current Total Zone DB Usage: 4 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 4 / 2097152 bytes (0 % used)
Status:
```

VSAN のゾーン ポリシーの表示

```
switch# show zone policy vsan 1
Vsan: 1
  Default-zone: deny
  Distribute: full
  Broadcast: enable
  Merge control: allow
  Generic Service: read-write
  Smart-zone: enabled
```

拡張モードで VSAN のゾーン属性グループを作成して個別ゾーン レベルでスマートゾーン分割を無効にする方法の表示



Note 属性グループの作成後に、スマートゾーン分割を無効にする必要があるゾーンにそれを適用する必要があります。

```
config# zone-attribute-group name <name> vsan 1
config-attribute-group# disable-smart-zoning
config-attribute-group# exit
config# zone commit vsan 1
```

ゾーンの自動変換方法の表示

```
config# show zoneset vsan 1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1
    device-alias Init2
    device-alias Init3
    device-alias Target1
```

```

config# zone convert smart-zoning vsan 1
smart-zoning auto_convert initiated. This operation can take few minutes. Please wait..
config# show zoneset vsan1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1  init
    device-alias Init2  init
    device-alias Init3  init
    device-alias Target1 target

```

メンバーのデバイス タイプ設定をクリアする方法の表示

```

config# show zoneset vsan 1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1  init
    device-alias Init2  init
    device-alias Init3  init
    device-alias Target1 target
config# clear zone smart-zoning vsan1
config# show zoneset vsan 1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1
    device-alias Init2
    device-alias Init3
    device-alias Target1

```

拡張ゾーン分割

ゾーン分割機能は、FC-GS-4 および FC-SW-3 規格に準拠しています。どちらの規格も、前の項で説明した基本ゾーン分割機能と、この項で説明する拡張ゾーン分割機能をサポートしています。

拡張ゾーン分割の概要

Table 8: 拡張ゾーン分割の利点, on page 124 に、Cisco MDS 9000 シリーズのすべてのスイッチの拡張ゾーン分割機能の利点を示します。

Table 8: 拡張ゾーン分割の利点

基本ゾーン分割	拡張ゾーン分割	拡張ゾーン分割の利点
複数の管理者が設定変更を同時に行うことができます。アクティブ化すると、ある管理者が別の管理者の設定変更を上書きできます。	単一のコンフィギュレーションセッションですべての設定を実行できます。セッションを開始すると、スイッチは変更を行うファブリック全体をロックします。	ファブリック全体を1つのコンフィギュレーションセッションで設定するため、ファブリック内の整合性が確保されます。

基本ゾーン分割	拡張ゾーン分割	拡張ゾーン分割の利点
ゾーンが複数のゾーンセットに含まれる場合、各ゾーンセットにこのゾーンのインスタンスを作成します。	ゾーンが定義されると、必要に応じて、ゾーンセットがゾーンを参照します。	ゾーンが参照されるため、ペイロードサイズが縮小されています。データベースが大きくなるほど、サイズの縮小も顕著になります。
デフォルトゾーンポリシーがスイッチごとに定義されます。ファブリックをスムーズに動作させるため、ファブリック内のスイッチはすべて同一のデフォルトゾーン設定を使用する必要があります。	ファブリック全体でデフォルトゾーン設定を実行および交換します。	ポリシーがファブリック全体に適用されるため、トラブルシューティングの時間が短縮されます。
スイッチ単位でのアクティブ化の結果を取得するため、管理スイッチはアクティブ化に関する複合ステータスを提供します。この場合、障害のあるスイッチは特定されません。	各リモートスイッチからアクティブ化の結果と問題の特性を取得します。	エラー通知機能が強化されているため、トラブルシューティングが容易です。
ゾーン分割データベースを配信するには、同じゾーンセットを再度アクティブ化する必要があります。再度アクティブ化すると、ローカルスイッチおよびリモートスイッチのハードゾーン分割のハードウェア変更に影響することがあります。	ゾーン分割データベースに対して変更を行い、再度アクティブ化することなく変更を配信します。	アクティブ化せずにゾーンセットを配信すると、スイッチのハードゾーン分割のハードウェア変更が回避されます。
MDS 固有のゾーンメンバータイプ (IPv4 アドレス、IPv6 アドレス、シンボリック ノード名、およびその他のタイプ) は他社製スイッチによって使用される場合があります。マージ時に、MDS 固有のタイプは他社製スイッチによって誤って解釈される可能性があります。	メンバタイプを一意に識別するために、ベンダー固有のタイプ値とベンダー ID が提供されます。	ベンダータイプが一意です。
fWWN ベースのゾーンメンバーシップは、シスコの interop モードでだけサポートされます。	標準の interop モード (interop モード 1) で fWWN ベースのメンバーシップがサポートされます。	fWWN ベースのメンバタイプは標準化されています。

基本ゾーン分割から拡張ゾーン分割への変更

基本ゾーン分割モードから拡張ゾーン分割モードに変更する手順は、次のとおりです。

ステップ 1 ファブリック内のすべてのスイッチが拡張モードで動作できることを確認します。

1 つ以上のスイッチが拡張モードで動作できない場合、拡張モードへ変更できません。

ステップ2 動作モードを拡張ゾーン分割モードに設定します。この操作を行うことにより、セッションが自動的に開始され、ファブリック全体のロックが取得され、拡張ゾーン分割データ構造を使用するアクティブおよびフルゾーン分割データベースが配信され、ゾーン分割ポリシーが配信され、ロックが解除されます。ファブリック内のすべてのスイッチは、拡張ゾーン分割モードに移行します。

Tip 基本ゾーン分割から拡張ゾーン分割への移行が完了したら、実行コンフィギュレーションを保存することを推奨します。

拡張ゾーン分割から基本ゾーン分割への変更

標準では、基本ゾーン分割に変更することを許可していません。ただし、Cisco MDS スイッチではこの変更を許可し、その他の Cisco SAN-OS または Cisco NX-OS リリースへのダウングレードおよびアップグレードを可能にしています。

拡張ゾーン分割モードから基本ゾーン分割モードに変更する手順は、次のとおりです。

ステップ1 アクティブおよびフルゾーンセットに拡張ゾーン分割モード固有の設定が含まれていないことを確認します。

このような設定が存在する場合は、次に進む前にこれらの設定を削除します。既存の設定は、削除しておかなくても Cisco NX-OS ソフトウェアにより自動的に削除されます。

ステップ2 動作モードを基本ゾーン分割モードに設定します。この操作を行うことによって、セッションが自動的に開始され、ファブリック全体のロックが取得され、基本ゾーン分割データ構造を使用するゾーン分割情報が配信され、設定変更が適用され、ファブリック内のすべてのスイッチのロックが解除されます。ファブリック内のすべてのスイッチは、基本ゾーン分割モードに移行します。

Note 拡張ゾーン分割をイネーブルにして Cisco SAN-OS Release 2.0(1b) および NX-OS 4(1b) 以降を実行しているスイッチが Cisco SAN-OS Release 1.3(4) 以前にダウングレードされた場合、スイッチは基本ゾーン分割モードになり、ファブリックに参加できません。これは、ファブリック内のその他すべてのスイッチが拡張ゾーン分割モードのままであるためです。

拡張ゾーン分割のイネーブル化

デフォルトでは、拡張ゾーン分割機能は Cisco MDS 9000 シリーズのすべてのスイッチで無効です。

VSAN で拡張ゾーン分割を有効にするには、次の手順を実行します。

ステップ1 `switch# configure terminal`

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# zone mode enhanced vsan id`

指定された VSAN で拡張ゾーン分割をイネーブルにします。

ステップ 3 `switch(config)# no zone mode enhanced vsan id`

指定された VSAN で拡張ゾーン分割をディセーブルにします。

DCNM SAN クライアントを使用した拡張ゾーン分割の有効化

DCNM SAN クライアントを使用して VSAN で拡張ゾーン分割を有効にするには、次の手順を実行します。

ステップ 1 VSAN を開き、[Logical Domains] ペインで、ゾーンセットを選択します。

[Information] ペインにゾーンセットの設定が表示されます。

ステップ 2 [拡張 (Enhanced)] タブをクリックします。

現在の拡張ゾーン分割設定が表示されます。

ステップ 3 [アクション (Action)] ドロップダウンメニューで [拡張 (enhanced)] を選択して、この VSAN の拡張ゾーン分割をイネーブルにします。**ステップ 4** [変更の適用 (Apply Changes)] をクリックして、変更を保存します。

ゾーン データベースの変更

ゾーンデータベースに対する変更は、セッション内で実行されます。セッションは、コンフィギュレーションコマンドが初めて正常に実行されたときに作成されます。セッションが作成されると、ゾーンデータベースのコピーが作成されます。セッションでの変更は、ゾーン分割データベースのコピー上で実行されます。ゾーン分割データベースのコピー上で行われる変更は、コミットするまで有効なゾーン分割データベースには適用されません。変更を適用すると、セッションはクローズします。

ファブリックが別のユーザーによってロックされ、何らかの理由でロックがクリアされない場合は、強制的に実行し、セッションをクローズします。このスイッチでロックをクリアする権限 (ロール) が必要です。また、この操作は、セッションが作成されたスイッチから実行する必要があります。

VSAN 内のゾーン分割データベースに対する変更をコミットまたは廃棄するには、次の手順を実行します。

ステップ 1 `switch# configure terminal`

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# zone commit vsan 2

拡張ゾーン データベースに変更を適用し、セッションをクローズします。

ステップ 3 switch(config)# zone commit vsan 3 force

拡張ゾーン データベースに変更を強制的に適用し、別のユーザーが作成したセッションをクローズします。

ステップ 4 switch(config)# no zone commit vsan 2

拡張ゾーン データベースへの変更を廃棄し、セッションをクローズします。

ステップ 5 switch(config)# no zone commit vsan 3 force

拡張ゾーンデータベースへの変更を強制的に廃棄し、別のユーザーが作成したセッションをクローズします。

Note アクティブ ゾーン セットを保存するのに、**copy running-config startup-config** コマンドを発行する必要はありません。ただし、明示的にフルゾーンセットを保存するには、**copy running-config startup-config** コマンドを発行する必要があります。ファブリックに複数のスイッチが含まれている場合は、**copy running-config startup-config fabric** コマンドを実行する必要があります。**fabric** キーワードを指定すると、**copy running-config startup-config** コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップ コンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。

ゾーンの保留中差分の自動表示の有効化

拡張モードでの zone commit 発行時の保留中差分の表示とそれ以降の確認を有効にするには、次の手順を実行します。

ステップ 1 switch# configure terminal

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# zone confirm-commit enable vsan vsan-id

特定の VSAN のゾーン データベースに対して confirm-commit オプションを有効にします。

ステップ 3 switch(config-zone)# zone commit vsan 12

VSAN に対して zone confirm-commit コマンドが有効な場合、保留中のデータベースがコミットされると、コンソールに保留中差分が表示され、ユーザーに対し [はい (Yes)] または [いいえ (No)] を選択するよう求めるプロンプトが表示されます。zone confirm-commit コマンドが無効な場合は、保留中差分は表示されず、ユーザーに対して [はい (Yes)] または [いいえ (No)] の選択は求められません。

ステップ 4 switch(config)# no zone commit vsan 12

VSANに対して `zone confirm-commit` コマンドが有効な場合、保留中のデータベースを廃棄すると、コンソールに保留中差分が表示され、ユーザーに対し [はい (Yes)] または [いいえ (No)] を選択するよう求めるプロンプトが表示されます。 `zone confirm-commit` コマンドが無効な場合は、保留中差分は表示されず、ユーザーに対して [はい (Yes)] または [いいえ (No)] の選択は求められません。

ゾーン データベース ロックの解除

VSAN 内のスイッチのゾーン分割 データベースのセッション ロックを解除するには、最初にデータベースをロックしたスイッチから `no zone commit vsan` コマンドを使用します。

```
switch# configure terminal
switch(config)# no zone commit vsan 2
```

`no zone commit vsan` コマンドを実行したあとも、リモート スイッチ上でセッションがロックされたままの場合、リモート スイッチ上で `clear zone lock vsan` コマンドを使用できます。

```
switch# clear zone lock vsan 2
```



Note ファブリック内のセッションロックを解除するには、最初に `no zone commit vsan` コマンドを使用することを推奨します。それが失敗した場合には、セッションがロックされたままのリモート スイッチで、`clear zone lock vsan` コマンドを使用してください。

属性グループの作成

拡張モードでは、属性グループを使用して属性を直接設定できます。

属性グループを設定するには、次の手順を実行します。

ステップ 1 属性グループを作成します。

Example:

```
switch# configure terminal
switch(config)# zone-attribute-group name SampleAttributeGroup vsan 2
switch(config-attribute-group)#
```

ステップ 2 属性グループ オブジェクトに属性を追加します。

Example:

```
switch(config-attribute-group)# readonly
switch(config-attribute-group)# broadcast
switch(config-attribute-group)# qos priority medium
readonly and broadcast commands are not supported from 5.2 release onwards.
```

ステップ 3 ゾーンに属性グループを対応付けます。

Example:

```
switch(config)# zone name Zone1 vsan 2
switch(config-zone)# attribute-group SampleAttributeGroup
switch(config-zone)# exit
switch(config)#
```

ステップ 4 ゾーンセットをアクティブ化します。

Example:

```
switch(config)# zoneset activate name Zoneset1 vsan 2
```

属性グループが展開され、アクティブゾーンセットには設定された属性だけが存在します。

属性グループの設定については、『[Cisco MDS 9000 Series NX-OS Fabric Configuration Guide](#)』を参照してください。

データベースのマージ

マージの動作は、ファブリック全体のマージ制御設定によって異なります。

- 制限：2つのデータベースが同一でない場合、スイッチ間の ISL は分離されます。
- 許可：2つのデータベースは、[Table 9: データベースのゾーン結合ステータス](#), on page 130 で指定された結合規則を使用して結合されます。

Table 9: データベースのゾーン結合ステータス

ローカル データベース	隣接データベース	結合ステータス	結合結果
データベースに、同じ名前のゾーンセットが含まれる。 ¹ 、異なるゾーン、エイリアス、属性グループになります。	成功	ローカル データベースおよび隣接データベースが結合されます。	
データベースに、名前は 1 で同じだが、異なる番号を持つゾーン、ゾーンエイリアス、またはゾーン属性グループ オブジェクトが含まれる。 Note 拡張ゾーン分割モードでは、interop モード 1 のアクティブゾーンセットには名前がありません。ゾーンセット名が存在するのは、フルゾーンセットの場合だけです。	失敗	ISL は分離されます。	

ローカル データベース	隣接データ ベース	結合ステータス	結合結果
データなし	データあり	成功	ローカルデータベースには隣接データベースの情報が存在します。
データあり	データなし	成功	隣接データベースにはローカルデータベースの情報が存在します。

¹ 拡張ゾーン分割モードでは、interop モード 1 のアクティブゾーンセットには名前がありません。ゾーンセット名はフルゾーンセットにのみ存在しますが



Caution

隣接ファブリックで FabricWare を実行している Cisco MDS 9020 スイッチがある場合は、ファブリックをマージする前に Cisco SAN-OS を実行しているすべての MDS スイッチで pWWN 以外のすべてのタイプを削除してください。

マージ プロセス

すでにアクティブゾーンセットが設定されており、まだ接続されていない2つのファイバチャネル (FC) スイッチが、拡張 ISL (EISL) リンクで接続されると、ゾーンセットがマージされます。ただし、新しいゾーンを設定してアクティブ化する前に、ゾーンの整合性を確保するための手順を実行する必要があります。

ベスト プラクティス

ゾーンがマージされる際は、競合する情報がない限り、スイッチは互いのゾーンを学習します。これにより、各スイッチには3つのコンフィギュレーション エンティティが設定されます。スイッチに設定されるコンフィギュレーション エンティティは次のとおりです。

- NVRAM に保存された設定。これは、**copy running-configuration startup-configuration** コマンドの最終実行時の設定です。
- 実行コンフィギュレーション。これは、前回 MDS が起動された時点でメモリに取り込まれたコンフィギュレーションと、そのコンフィギュレーションに加えられた変更です。ゾーン情報のコンテキストでは、実行コンフィギュレーションは設定可能データベースを意味します。これは、フルデータベースと呼ばれます。
- 実行コンフィギュレーションに含まれる設定済みゾーン情報とゾーンマージから学習されたゾーン情報。この設定されたゾーン分割情報と学習されたゾーン分割情報の組み合わせが、アクティブゾーンセットです。

結合プロセスは次のように動作します。

1. ソフトウェアがプロトコルバージョンを比較します。プロトコルバージョンが異なる場合、ISLは分離されます。
2. プロトコルバージョンが同じである場合、ゾーンポリシーが比較されます。ゾーンポリシーが異なる場合、ISLは分離されます。
3. ゾーン結合オプションが同じである場合、結合制御設定に基づいて比較が行われます。
 - a. 設定が「制限」の場合、アクティブゾーンセットとフルゾーンセットが同じになる必要があります。これらが同じでない場合、リンクは分離されます。
 - b. 設定が「許可」の場合、結合規則を使用して結合が行われます。

MDSは、起動時にNVRAMに以前に保存された設定を使用します。NVRAMから設定をロードした後でスイッチを設定した場合、実行コンフィギュレーションがスタートアップコンフィギュレーションに保存されるまでは、ブートアップコンフィギュレーションと実行コンフィギュレーションの間に差異があります。これは、PCのローカルハードドライブにファイルが保存されていることに関連している可能性があります。ファイルは保存されておりスタティックですが、ファイルを開いて編集すると、変更後のファイルと、保存ストレージに存在するファイルの間に差異が生じます。変更の保存時のみ、保存されたエンティティがファイルに対して行われた変更を表します。

ゾーンマージからゾーン分割情報が学習される場合、学習された情報は実行コンフィギュレーションには含まれません。学習された情報が実行コンフィギュレーションに組み込まれるのは、**zone copy active-zoneset full-zoneset vsan X** コマンドの実行時のみです。ゾーンマージが新しいEISLリンクにより開始されるか、またはゾーンセットのアクティブ化により開始された場合、ゾーンセット部分はもう一方のスイッチにより無視され、メンバーゾーン情報は局所的と見なされるため、これは重要です。



Caution **zone copy** コマンドは、FCエイリアス設定をすべて削除します。

例

たとえば、2つのスタンドアロンMDSスイッチがすでに配置されており、それぞれに固有のゾーンとゾーンセット情報が設定されているとします。スイッチ1のアクティブゾーンセットはセットA、スイッチ2のアクティブゾーンセットはセットBであり、スイッチ1のセットA内にゾーン1があり、スイッチ2のセットBにメンバーゾーン2があるとします。この2つのスイッチ間でISLリンクが作成されると、各スイッチは各自のゾーンセット（ゾーン情報を含む）をもう一方のスイッチに送信します。マージ時には、スイッチはASCII値が大きい方のゾーンセット名を選択し、その後ゾーンメンバーをマージします。マージ後は、両方のスイッチにセットBという名前のゾーンセットが含まれます。このゾーンセットにはメンバーゾーン1とゾーン2が含まれています。

ゾーン1とゾーン2のすべてのデバイスに対して、これまでと同様にすべてが適切に機能します。新しいゾーンを追加するには、新しいゾーンを作成してゾーンセットに追加し、そのゾーンセットをアクティブにする必要があります。

段階的にスイッチが起動します。スイッチにはゾーン分割情報は含まれません。スイッチでゾーンを作成し、そのゾーンをゾーンセットに追加する必要があります。

基本モード：ゾーンが基本モードの場合は、次に示すコマンド出力例を参照してください。

1. ゾーンとゾーンセットを作成します。スイッチ 1 でアクティブ化します。

```
Switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch1#(config)# vsan database
Switch1#(config-vsan-db)# vsan 100
Switch1#(config-vsan-db)# exit

Switch1#(config)# zone name zone1 vsan 100
Switch1#(config-zone)# member pwn 11:11:11:11:11:11:11:1a
Switch1#(config-zone)# member pwn 11:11:11:11:11:11:11:1b
Switch1#(config-zone)# exit

Switch1#(config)# zoneset name setA vsan 100
Switch1#(config-zoneset)# member zone1
Switch1#(config-zoneset)# exit

Switch1#(config)# zoneset activate name setA vsan 100
Zoneset activation initiated. check zone status
Switch1#(config)# exit

Switch1# show zoneset active vsan 100
zoneset name setA vsan 100
zone name zone1 vsan 100
pwn 11:11:11:11:11:11:11:1a
pwn 11:11:11:11:11:11:11:1bSwitch1#
```

2. ゾーンとゾーンセットを作成します。スイッチ 2 でアクティブ化します。

```
Switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch2#(config)# vsan database
Switch2#(config-vsan-db)# vsan 100
Switch2#(config-vsan-db)# exit

Switch2#(config)# zone name zone2 vsan 100
Switch2#(config-zone)# member pwn 22:22:22:22:22:22:22:2a
Switch2#(config-zone)# member pwn 22:22:22:22:22:22:22:2b
Switch2#(config-zone)# exit

Switch2#(config)# zoneset name setB vsan 100
Switch2#(config-zoneset)# member zone2
Switch2#(config-zoneset)# exit

Switch2#(config)# zoneset activate name setB vsan 100
Zoneset activation initiated. check zone status
Switch2#(config)# exit

Switch2# show zoneset active vsan 100
zoneset name setB vsan 100
zone name zone2 vsan 100
pwn 22:22:22:22:22:22:22:2a
```

```
pwwn 22:22:22:22:22:22:22:2b
```

- ISL リンクを起動し、スイッチ 1 でゾーン マージを確認します。

```
Switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)# interface fc1/5
Switch1(config-if)# no shutdown
Switch1(config-if)# exit
Switch1(config)# exit
```



Note 注 : VSAN 100 が ISL で許可されていることを確認してください。

```
Switch1# show zoneset active vsan 100
zoneset name setB vsan 100
zone name zone1 vsan 100
pwwn 11:11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:11:1b
```

```
Switch1# show zoneset vsan 100
zoneset name setA vsan 100
zone name zone1 vsan 100
pwwn 11:11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:11:1b
```

- ISL リンクを起動し、スイッチ 2 でゾーン マージを確認します。

```
Switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)# int fc2/5
Switch2(config-if)# no shut
Switch2(config-if)# exit
Switch2(config)# exit
```

```
Switch2# show zoneset active vsan 100 zoneset name setB vsan 100
zone name zone1 vsan 100
pwwn 11:11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:11:1b
```

```
zone name zone2 vsan 100
pwwn 22:22:22:22:22:22:22:2a
pwwn 22:22:22:22:22:22:22:2b
```

```
Switch2# show zoneset vsan 100 zoneset name setB vsan 100
zone name zone2 vsan 100
pwwn 22:22:22:22:22:22:22:2a
pwwn 22:22:22:22:22:22:22:2b
```



Note 新しくマージされたゾーンセットの名前は、アルファベット順で大きな値のゾーンセット名になります。上記の例では、アクティブゾーンセットはsetBです。今後ゾーンセットのアクティブ化の問題が発生しないようにするため、この時点でスイッチで **zone copy active-zoneset full-zoneset vsan 100** コマンドを実行する必要があります。このコマンドが実行されるかどうかと、新しいゾーン分割情報の処理方法を確認します。

zone copy コマンドを実行すると、学習したゾーン情報（この例ではゾーン2）が実行コンフィギュレーションに追加されます。ゾーン2がメモリ内から実行コンフィギュレーションにコピーされていない場合、ゾーン2情報はプッシュして戻されません。



Note zone copy コマンドは、FC エイリアス設定をすべて削除します。

Switch1 の実行コンフィギュレーション (zone copy active-zoneset full-zoneset vsan 100 コマンドの実行前)

```
Switch1# show run | b "Active Zone Database Section for vsan 100"
!Active Zone Database Section for vsan 100
zone name zone1 vsan 100
pwn 11:11:11:11:11:11:1a
pwn 11:11:11:11:11:11:1b

zone name zone2 vsan 100
pwn 22:22:22:22:22:22:2a
pwn 22:22:22:22:22:22:2b

zoneset name setB vsan 100
member zone1
member zone2

zoneset activate name setB vsan 100
do clear zone database vsan 100
!Full Zone Database Section for vsan 100
zone name zone1 vsan 100
pwn 11:11:11:11:11:11:1a
pwn 11:11:11:11:11:11:1b

zoneset name setA vsan 100
member zone1
```

Switch1 の実行コンフィギュレーション (「zone copy active-zoneset full-zoneset vsan 100」コマンドの実行後)

```
Switch1# zone copy active-zoneset full-zoneset vsan 100
WARNING: This command may overwrite common zones in the full zoneset. Do you want to
continue? (y/n) [n] y

Switch1# show run | b "Active Zone Database Section for vsan 100"
!Active Zone Database Section for vsan 100
zone name zone1 vsan 100
pwn 11:11:11:11:11:11:1a
```

```

pwnn 11:11:11:11:11:11:11:1b

zone name zone2 vsan 100
pwnn 22:22:22:22:22:22:22:2a
pwnn 22:22:22:22:22:22:22:2b

zoneset name setB vsan 100
member zone1
member zone2

zoneset activate name setB vsan 100
do clear zone database vsan 100
!Full Zone Database Section for vsan 100
zone name zone1 vsan 100
pwnn 11:11:11:11:11:11:11:1a
pwnn 11:11:11:11:11:11:11:1b

zone name zone2 vsan 100
pwnn 22:22:22:22:22:22:22:2a
pwnn 22:22:22:22:22:22:22:2b

zoneset name setA vsan 100
member zone1

zoneset name setB vsan 100
member zone1
member zone2

```

Switch2 の実行コンフィギュレーション (「zone copy active-zoneset full-zoneset vsan 100」コマンドの実行前)

```

Switch2# show run | b "Active Zone Database Section for vsan 100"
!Active Zone Database Section for vsan 100
zone name zone2 vsan 100
pwnn 22:22:22:22:22:22:22:2a
pwnn 22:22:22:22:22:22:22:2b

zone name zone1 vsan 100
pwnn 11:11:11:11:11:11:11:1a
pwnn 11:11:11:11:11:11:11:1b

zoneset name setB vsan 100
member zone2
member zone1

zoneset activate name setB vsan 100
do clear zone database vsan 100
!Full Zone Database Section for vsan 100
zone name zone2 vsan 100
pwnn 22:22:22:22:22:22:22:2
apwnn 22:22:22:22:22:22:22:2b
zoneset name setB vsan 100
member zone2

```

Switch2 の実行コンフィギュレーション (「zone copy active-zoneset full-zoneset vsan 100」コマンドの実行後)

```

Switch2# zone copy active-zoneset full-zoneset vsan 100
WARNING: This command may overwrite common zones in the full zoneset. Do you want to
continue? (y/n) [n] y

```



```
Switch2# show run | b "Active Zone Database Section for vsan 100"
!Active Zone Database Section for vsan 100
zone name zone2 vsan 100
pwn 22:22:22:22:22:22:2a
pwn 22:22:22:22:22:22:2b

zone name zone1 vsan 100
pwn 11:11:11:11:11:11:1a
pwn 11:11:11:11:11:11:1b

zoneset name setB vsan 100
member zone2
member zone1

zoneset activate name setB vsan 100
do clear zone database vsan 100
!Full Zone Database Section for vsan 100
zone name zone2 vsan 100
pwn 22:22:22:22:22:22:2a
pwn 22:22:22:22:22:22:2b

zone name zone1 vsan 100
pwn 11:11:11:11:11:11:1a
pwn 11:11:11:11:11:11:1b

zoneset name setB vsan 10
member zone2
member zone1
```

設定の3つの要素に戻ると、これらはゾーンマージ前のゾーン1では次のようになります。

- 保存済み設定：copy run start コマンドを実行してゾーン情報を保存する操作が行われていないため、何も保存されていません。
- 実行コンフィギュレーション：ゾーン1で構成されます。
- 設定および学習された情報：ゾーン1で構成されます。

ゾーンマージ後は、これらの要素は次のようになります。

- 保存済みコンフィギュレーション：何も保存されていません。
- 実行コンフィギュレーション：ゾーン1で構成されます。
- 設定および学習された情報：ゾーン1とゾーン2で構成されます。

ゾーン2は実行コンフィギュレーションの一部ではありません。ゾーン2は学習され、アクティブゾーンセットに含まれています。学習されたゾーン2がコピーされ、実行コンフィギュレーションに追加されるのは、**zone copy active-zoneset full-zoneset vsan 100** コマンドの実行時のみです。このコマンドの実行後のコンフィギュレーションは次のようになります。



Note zone copy コマンドは、FC エイリアス設定をすべて削除します。

- 保存済みコンフィギュレーション：何も保存されていません。

- 実行コンフィギュレーション：ゾーン1とゾーン2で構成されます。
- 設定および学習された情報：ゾーン1とゾーン2で構成されます。

コマンド

基本モードではデフォルトでアクティブゾーンセットデータベースだけが配信されます。このコマンドは 1.0.4 SAN-OS で導入されました。アクティブゾーンセットとフルゾーンセットデータベースを伝播します。

zoneset distribute full vsan vsan_id

ゾーン更新またはゾーンセットアクティブ化が進行中の場合、上記のコマンドを各スイッチの各 VSAN で明示的に有効にする必要があります。

拡張モード：ゾーンが拡張モードのときは、次に示すコマンド出力例を参照してください。

1. ゾーンとゾーンセットを作成します。Switch1 でアクティブにします。

```
Switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)# vsan database
Switch1(config-vsan-db)# vsan 200
Switch1(config-vsan-db)# zone mode enhanced vsan 200
WARNING: This command would distribute the zoning database of this switch throughout
the fabric. Do you want to continue? (y/n) [n] y
Set zoning mode command initiated.
Check zone status
Switch1(config-vsan-db)# zone name zone1 vsan 200
Enhanced zone session has been created. Please 'commit' the changes when done.
Switch1(config-zone)# member pwnn 11:11:11:11:11:11:11:1a
Switch1(config-zone)# member pwnn 11:11:11:11:11:11:11:1b
Switch1(config-zone)# zoneset name SetA vsan 200
Switch1(config-zoneset)# member zone1
Switch1(config-zoneset)# zoneset activate name SetA vsan 200
Switch1(config)# zone commit vsan 200
Commit operation initiated. Check zone status
Switch1(config)# exit
Switch1# show zoneset activate vsan 200
zoneset name SetA vsan 200
zone name zone1 vsan 200
pwnn 11:11:11:11:11:11:11:1a
pwnn 11:11:11:11:11:11:11:1b
Switch1# show zoneset vsan 200
zoneset name SetA vsan 200
zone name zone1 vsan 200
pwnn 11:11:11:11:11:11:11:1a
pwnn 11:11:11:11:11:11:11:1b
```

2. ゾーンとゾーンセットを作成します。Switch2 でアクティブにします。

```
Switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)# vsan database
Switch2(config-vsan-db)# vsan 200
Switch2(config-vsan-db)# zone mode enhanced vsan 200
WARNING: This command would distribute the zoning database of this switch throughout
the fabric. Do you want to continue? (y/n) [n] y
Set zoning mode command initiated. Check zone status
```

```
Switch2(config)# zone name zone2 vsan 200
Enhanced zone session has been created. Please 'commit' the changes when done.
Switch2(config-zone)# member pwnn 22:22:22:22:22:22:22:2a
Switch2(config-zone)# member pwnn 22:22:22:22:22:22:22:2b
Switch2(config-zone)# zoneset name SetB vsan 200
Switch2(config-zoneset)# member zone2
Switch2(config-zoneset)# zoneset act name SetB vsan 200
Switch2(config)# zone commit vsan 200
Commit operation initiated. Check zone status
Switch2(config)# exit
Switch2# show zoneset activate vsan 200
zoneset name SetB vsan 200
zone name zone2 vsan 200
pwnn 22:22:22:22:22:22:22:2a
pwnn 22:22:22:22:22:22:22:2b
Switch2# show zoneset vsan 200
zoneset name SetB vsan 200
zone name zone2 vsan 200
pwnn 22:22:22:22:22:22:22:2a
pwnn 22:22:22:22:22:22:22:2b
```

3. ISL リンクを起動し、Switch1 でゾーン マージを確認します。

```
Switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)# interface fc4/1
Switch1(config-if)# no shutdown
Switch1(config-if)# exit
Switch1(config)# exit

Switch1(config-if)# show zoneset activate vsan 200
zoneset name SetB vsan 200
zone name zone1 vsan 200
pwnn 11:11:11:11:11:11:11:1a
pwnn 11:11:11:11:11:11:11:1b
zone name zone2 vsan 200
pwnn 22:22:22:22:22:22:22:2a
pwnn 22:22:22:22:22:22:22:2b
Switch1(config-if)# show zoneset vsan 200
zoneset name SetA vsan 200
zone name zone1 vsan 200
pwnn 11:11:11:11:11:11:11:1a
pwnn 11:11:11:11:11:11:11:1b

zoneset name SetB vsan 200
zone name zone2 vsan 200
pwnn 22:22:22:22:22:22:22:2a
pwnn 22:22:22:22:22:22:22:2b
```



Note 基本モードとは異なり、拡張モードではゾーンデータベース全体がマージされ、Switch1 には元々 Switch2 で設定されたゾーンセットの情報が含まれ、Switch2 には元々 Switch1 で設定された情報が含まれます。

4. ISL リンクを起動し、Switch2 でゾーン マージを確認します。2つのスイッチ間での ISL の起動後：

```

Switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)# interface fc4/1
Switch2(config-if)# no shutdown
Switch2(config-if)# exit
Switch2(config)# exit

Switch2(config-zoneset)# show zoneset activate vsan 200
zoneset name SetB vsan 200
zone name zone2 vsan 200
pwwn 22:22:22:22:22:22:22:2a
pwwn 22:22:22:22:22:22:22:2b
zone name zone1 vsan 200
pwwn 11:11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:11:1b
Switch2(config-zoneset)# show zoneset vsan 200
zoneset name SetB vsan 200
zone name zone2 vsan 200
pwwn 22:22:22:22:22:22:22:2a
pwwn 22:22:22:22:22:22:22:2b

zoneset name SetA vsan 200
zone name zone1 vsan 200
pwwn 11:11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:11:1b

```

5. 拡張ゾーンに対して **zone copy** コマンドを実行します。

スイッチ 1

```

Switch1# zone copy active-zoneset full-zoneset vsan 200
WARNING: This command may overwrite common zones in the full zoneset. Do you want to
continue? (y/n) [n] y
Switch1(config-if)# show zoneset activate vsan 200
zoneset name SetB vsan 200
zone name zone1 vsan 200
pwwn 11:11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:11:1b
zone name zone2 vsan 200
pwwn 22:22:22:22:22:22:22:2a
pwwn 22:22:22:22:22:22:22:2b
Switch1(config-if)# show zoneset vsan 200
zoneset name SetB vsan 200
zone name zone1 vsan 200
pwwn 11:11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:11:1b
zone name zone2 vsan 200
pwwn 22:22:22:22:22:22:22:2a
pwwn 22:22:22:22:22:22:22:2b

```

スイッチ 2

```

Switch2# zone copy active-zoneset full-zoneset vsan 200
WARNING: This command may overwrite common zones in the full zoneset. Do you want to
continue? (y/n) [n] y
Switch2(config-zoneset)# show zoneset activate vsan 200
zoneset name SetB vsan 200
zone name zone2 vsan 200
pwwn 22:22:22:22:22:22:22:2a

```

```

pwn 22:22:22:22:22:22:22:2b
zone name zone1 vsan 200
pwn 11:11:11:11:11:11:11:1a
pwn 11:11:11:11:11:11:11:1b
Switch2(config-zoneset)# show zoneset vsan 200
zoneset name SetB vsan 200
zone name zone2 vsan 200
pwn 22:22:22:22:22:22:22:2a
pwn 22:22:22:22:22:22:22:2b
zone name zone1 vsan 200
pwn 11:11:11:11:11:11:11:1a
pwn 11:11:11:11:11:11:11:1b

```

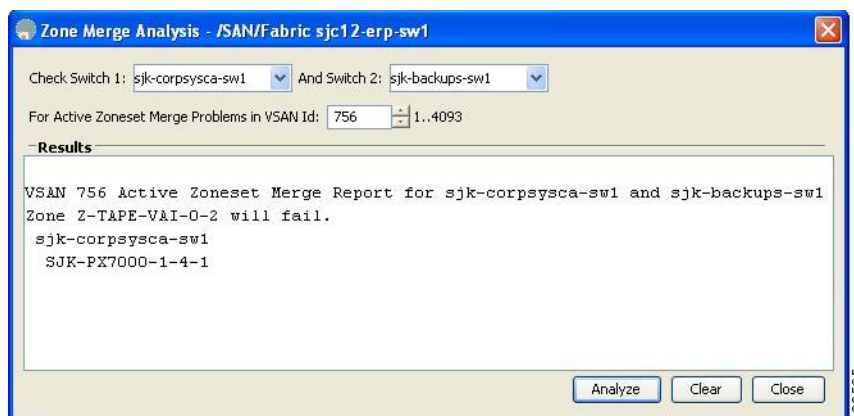
ゾーン マージの分析

DCNMSAN クライアントを使用してゾーンマージの分析を実行する手順は、次のとおりです。

ステップ 1 [ゾーン (Zone)]>[マージの分析 (Merge Analysis)] を選択します。

[Zone Merge Analysis] ダイアログボックスが表示されます。

Figure 42: [Zone Merge Analysis] ダイアログボックス



ステップ 2 [Check Switch 1] ドロップダウンリストで、最初に分析するスイッチを選択します。

ステップ 3 [And Switch 2] ドロップダウン リストで、2 番めに分析するスイッチを選択します。

ステップ 4 [For Active Zoneset Merge Problems in VSAN Id] フィールドに、ゾーンセット マージに失敗した VSAN の ID を入力します。

ステップ 5 [分析 (Analyze)] をクリックして、ゾーン マージを分析します。

ステップ 6 [削除 (Clear)] をクリックして [ゾーン マージの分析 (Zone Merge Analysis)] ダイアログボックスから分析データを削除します。

ゾーン マージ制御ポリシーの設定

マージ制御ポリシーを設定するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **zone merge-control restrict vsan 4**

現在の VSAN の結合制御設定を「制限」に設定します。

ステップ 3 switch(config)# **no zone merge-control restrict vsan 2**

現在の VSAN の結合制御設定をデフォルトの「許可」に設定します。

ステップ 4 switch(config)# **zone commit vsan 4**

VSAN 4 への変更をコミットします。

マージ制御ポリシーの設定については、『[Cisco MDS 9000 Series NX-OS Fabric Configuration Guide](#)』を参照してください。

ゾーンによる FC2 バッファのフラッディングの防止

zone fc2 merge throttle enable コマンドを使用して、ゾーンから FC2 に送信されるマージ要求をスロットルし、ゾーンによる FC2 バッファのフラッディングを防止できます。このコマンドは、デフォルトでイネーブルにされています。このコマンドは、多数のゾーンがある場合にゾーン マージの拡張性の問題を防ぐ目的で使用できます。ゾーン マージのスロットル情報を表示するには、**show zone status** コマンドを使用します。

デフォルト ゾーンでのトラフィックの許可または拒否

デフォルト ゾーンでトラフィックを許可または拒否するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **zone default-zone permit vsan 5**

デフォルト ゾーン メンバへのトラフィック フローを許可します。

ステップ 3 switch(config)# **no zone default-zone permit vsan 3**

デフォルト ゾーン メンバへのトラフィック フローを拒否し、出荷時の設定に戻します。

ステップ 4 switch(config)# **zone commit vsan 5**

VSAN 5 への変更をコミットします。

ゾーンのブロードキャスト

拡張ゾーンは、このゾーンのメンバーによって生成されたフレームのブロードキャストを、そのゾーン内のメンバーに制限するように指定できます。ホストまたはストレージデバイスがブロードキャストをサポートしている場合に、この機能を使用します。



Note broadcast コマンドは 5.x 以降のリリースではサポートされていません。

[Table 10: ブロードキャスト要件, on page 143](#) に、ブロードキャスト フレームの配信規則を示します。

Table 10: ブロードキャスト要件

アクティブなゾーン分割?	ブロードキャストがイネーブル?	フレームのブロードキャスト?
はい	はい	はい
いいえ	はい	はい
はい	いいえ	いいえ
データあり	データなし	成功



Tip FL ポートに接続されている NL ポートがブロードキャスト フレームの発信元とブロードキャストゾーンを共有する場合、フレームはループ内のすべてのデバイスにブロードキャストされます。

拡張ゾーン分割モードでフレームをブロードキャストするには、次の手順を実行します。

ステップ 1 switch# configure terminal

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# zone-attribute-group name BroadcastAttr vsan 2

目的の VSAN のゾーン属性グループを設定します。

ステップ 3 switch(config)# no zone-attribute-group name BroadAttr vsan 1

目的の VSAN のゾーン属性グループを削除します。

ステップ 4 switch(config-attribute-group)# broadcast

このグループのブロードキャスト属性を作成し、このサブモードを終了します。

ステップ 5 `switch(config-attribute-group)# no broadcast`

このグループのブロードキャスト属性を削除し、このサブモードを終了します。

ステップ 6 `switch(config)# zone name BroadcastAttr vsan 2`

VSAN 2 で BroadcastAttr という名前のゾーンを設定します。

ステップ 7 `switch(config-zone)# member pwwn 21:00:00:e0:8b:0b:66:56`

指定されたメンバーをこのゾーンに追加し、このサブモードを終了します。

ステップ 8 `switch(config)# zone commit vsan 1`

拡張ゾーン設定に変更を適用し、このサブモードを終了します。

ステップ 9 `switch# show zone vsan 1`

ブロードキャスト設定を表示します。

システムのデフォルト ゾーン分割設定値の設定

スイッチ上の新しい VSAN のデフォルトのゾーンポリシー、フルゾーン配信、および Generic Service アクセス権限のデフォルト設定を設定できます。スイッチ全体のデフォルト設定を設定するには、次の手順を実行します。

ステップ 1 `switch# configure terminal`

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# system default zone default-zone permit`

スイッチ上の新しい VSAN のデフォルト ゾーン分割ポリシーとして permit (許可) を設定します。

ステップ 3 `switch(config)# system default zone distribute full`

スイッチ上の新しい VSAN のデフォルトとして、フルゾーン データベース配信をイネーブルにします。

ステップ 4 `switch(config)# system default zone gs {read | read-write}`

スイッチ上の新しい VSAN のデフォルト Generic Service アクセス権限として読み取り専用または読み取り/書き込み (デフォルト) を設定します。

Note VSAN 1 はデフォルト VSAN であり、常にスイッチ上に存在するため、`system default zone` コマンドは VSAN 1 に対しては無効です。

ゾーンの Generic Service アクセス権限の設定

ゾーンの Generic Service アクセス権限設定は、Generic Service (GS) インターフェイス経由でのゾーン分割操作を制御するために使用されます。ゾーンの Generic Service アクセス権限は、読み取り専用、読み取りと書き込み、またはなし (拒否) にすることができます。

Generic Service (GS) 設定を設定する手順は、次のとおりです。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **zone gs {read | read-write} vsan 3000**

gs のアクセス権限の値を、指定された VSAN で読み取り専用または読み取り/書き込みとして設定します。

拡張ゾーン情報の表示

ゾーン情報を表示するには、**show** コマンドを使用します。

指定された VSAN のアクティブ ゾーン セット情報の表示

```
switch(config)# show zoneset active vsan 1
zoneset name qoscfg vsan 1
zone name qos1 vsan 1
* fcid 0xe80200 [pwnn 50:08:01:60:01:5d:51:11]
* fcid 0xe60000 [pwnn 50:08:01:60:01:5d:51:10]
* fcid 0xe80100 [pwnn 50:08:01:60:01:5d:51:13]

zone name qos3 vsan 1
* fcid 0xe80200 [pwnn 50:08:01:60:01:5d:51:11]
* fcid 0xe60100 [pwnn 50:08:01:60:01:5d:51:12]
* fcid 0xe80100 [pwnn 50:08:01:60:01:5d:51:13]

zone name sb1 vsan 1
* fcid 0xe80000 [pwnn 20:0e:00:11:0d:10:dc:00]
* fcid 0xe80300 [pwnn 20:0d:00:11:0d:10:da:00]
* fcid 0xe60200 [pwnn 20:13:00:11:0d:15:75:00]
* fcid 0xe60300 [pwnn 20:0d:00:11:0d:10:db:00]
```

指定された VSAN のゾーン セット情報の表示

```
switch(config)# show zoneset vsan 1
zoneset name qoscfg vsan 1
zone name qos1 vsan 1
zone-attribute-group name qos1-attr-group vsan 1
pwnn 50:08:01:60:01:5d:51:11
pwnn 50:08:01:60:01:5d:51:10
pwnn 50:08:01:60:01:5d:51:13

zone name qos3 vsan 1
zone-attribute-group name qos3-attr-group vsan 1
```

```

pwwn 50:08:01:60:01:5d:51:11
pwwn 50:08:01:60:01:5d:51:12
pwwn 50:08:01:60:01:5d:51:13

zone name sb1 vsan 1
pwwn 20:0e:00:11:0d:10:dc:00
pwwn 20:0d:00:11:0d:10:da:00
pwwn 20:13:00:11:0d:15:75:00
pwwn 20:0d:00:11:0d:10:db:00

```

指定された VSAN のゾーン属性グループ情報の表示

```

switch# show zone-attribute-group vsan 2
zone-attribute-group name $default_zone_attr_group$ vsan 2
  read-only
  qos priority high
  broadcast
zone-attribute-group name testattgrp vsan 2
  read-only
  broadcast
  qos priority high

```

指定された VSAN の FC エイリアス情報の表示

```

switch# show fcalias vsan 2
fcalias name testfcalias vsan 2
pwwn 21:00:00:20:37:39:b0:f4
pwwn 21:00:00:20:37:6f:db:dd
pwwn 21:00:00:20:37:a6:be:2f

```

指定された VSAN のゾーンステータスの表示

```

switch(config)# show zone status vsan 1
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
activation overwrite control:disabled
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Current Total Zone DB Usage: 4 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 4 / 2097152 bytes (0 % used)
Status:

```

コミットされる VSAN の保留中のゾーンセット情報の表示

```

switch# show zoneset pending vsan 2

```

```
No pending info found
```

コミットされる VSAN の保留中のゾーン情報の表示

```
switch# show zone pending vsan 2  
No pending info found
```

コミットされる VSAN の保留中のゾーン情報の表示

```
switch# show zone-attribute-group pending vsan 2  
No pending info found
```

コミットされる VSAN の保留中のアクティブ ゾーン セット情報の表示

```
switch# show zoneset pending active vsan 2  
No pending info found
```

指定された VSAN に関する保留中のゾーン情報と有効なゾーン情報の相違点の表示

```
switch# show zone pending-diff vsan 2  
zone name testzone vsan 2  
- member pwwn 21:00:00:20:37:4b:00:a2  
+ member pwwn 21:00:00:20:37:60:43:0c
```

Exchange Switch Support (ESS) は、2つのスイッチがサポートされている各種機能を交換するためのメカニズムを定義しています。

指定された VSAN のすべてのスイッチに関する ESS 情報の表示

```
switch# show zone ess vsan 2  
ESS info on VSAN 2 :  
Domain : 210, SWWN : 20:02:00:05:30:00:85:1f, Cap1 : 0xf3, Cap2 : 0x0
```

コミットされる VSAN の保留中の FC エイリアス情報の表示

```
switch# show fcalias pending vsan 2  
No pending info found
```

ゾーン分割構成セッションの制御

拡張モードゾーン分割では、ゾーン分割セッションが開始されたスイッチが、VSAN のファブリック全体のゾーン分割構成ロックを取得します。この構成ロックにより、ファブリック内の他のスイッチのユーザが同時に（競合する可能性がある）構成変更を行うことができなくなります。ただし、デフォルトでは、構成がロックされているスイッチに同じユーザが複数回ログインし、複数のゾーニング構成セッションを開始することが許可されています。これにより、競合または望ましくないゾーン構成が発生する可能性もあります。

シングルセッション オプションは、ゾーン構成ファブリック ロックを使用して、スイッチ上で VSAN ごとに一度に最大 1 つのゾーン分割構成セッションを実施します。この制限により、スイッチは同じ VSAN で新しいゾーン分割構成セッションを開始できなくなります。この制限は、別のユーザ、Cisco DCNM、または NX-API などの構成送信元にも適用されます。



- (注)
- スーパーバイザのスイッチオーバー後など、なんらかの理由でログインセッションが切断された場合、ゾーンセッションはファブリック全体のロックと保留中の変更のままになります。この場合、シングルセッション オプションが有効になっていると、他のログインからスイッチへのそれ以上のゾーン構成は許可されません。これを試みると、古いセッション所有者情報を表示するエラー メッセージが表示されて拒否されます。この情報は、**show zone status** コマンドを使用して表示することも可能です。回復するには、セッションがロックされたスイッチから **clear zone lock** コマンドを使用して、セッション ロックをクリアする必要があります。セッション ロックをクリアすると、保留中のゾーン分割構成がすべて削除され、ゾーン構成の変更を再入力する必要があります。**show zone pending-diff** コマンドを使用して、ゾーン ロックをクリアする前に、保留中のゾーン分割構成の変更を表示します。
 - このオプションは、Cisco MDS NX-OS リリース 8.4(2) から利用できます。
 - 以前の NX-OS リリースにダウングレードする前に、このオプションを必ず無効にしてください。この処理を実行しないと、ダウングレードプロセスが失敗します。

ゾーン分割セッション制限の構成

VSAN でゾーン分割セッション制限を構成するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **zone mode enhanced vsan id single-session**

指定された VSAN で単一セッション オプションを有効にします。

ステップ 3 switch(config)# **no zone mode enhanced vsan id single-session**

指定された VSAN の単一セッション オプションを無効にし、VSAN を拡張ゾーン分割モードのままにします。

ダウングレード用のゾーン データベースの圧縮

Cisco SAN-OS Release 6.2(7) 以前では、VSAN あたり 8000 ゾーンだけがサポートされます。VSAN に 8000 を超えるゾーンを追加した場合、以前のリリースにダウンロードすると制限超過分のゾーンが失われる可能性のあることを示す、コンフィギュレーションチェックが登録されます。コンフィギュレーションチェックを避けるには、過剰なゾーンを削除し、VSAN のゾーンデータベースをコンパクトにします。超過分のゾーンを削除した後、ゾーン数が 8000 以下になれば、圧縮プロセスによって新しい内部ゾーン ID が割り当てられ、設定は Cisco SAN-OS Release 6.2(5) 以前によってサポートされます。この手順は、8000 を超えるゾーンを含む、スイッチ上のすべての VSAN で実行します。



Note スイッチが VSAN あたり 8000 を超えるゾーンをサポートしていても、ネイバーがサポートしていない場合、結合は失敗します。また、そのスイッチが VSAN あたり 8000 を超えるゾーンをサポートしていても、ファブリック内のすべてのスイッチが VSAN あたり 8000 を超えるゾーンをサポートしていない場合には、ゾーンセットのアクティブ化に失敗することがあります。

VSAN のゾーンを削除し、ゾーンデータベースを圧縮するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **no zone name ExtraZone vsan 10**

ゾーンを削除し、ゾーン数を 8000 以下にします。

ステップ 3 switch(config)# **zone compact vsan 10**

VSAN 10 のゾーンデータベースを圧縮し、ゾーンが削除されたときに開放されたゾーン ID を回復します。ダウングレード用のゾーンデータベースの圧縮については、『[Cisco MDS 9000 Series NX-OS Fabric Configuration Guide](#)』を参照してください。

ゾーンおよびゾーンセットの分析

スイッチ上のゾーンおよびゾーンセットをよりの確に管理するために、**show zone analysis** コマンドを使用して、ゾーン情報とゾーンセット情報を表示できます。

フル ゾーン分割の分析

```
switch# show zone analysis vsan 1
```

```
Zoning database analysis vsan 1
Full zoning database
  Last updated at: 15:57:10 IST Feb 20 2006
  Last updated by: Local [ CLI ]
  Num zonesets: 1
  Num zones: 1
  Num aliases: 0
  Num attribute groups: 0
  Formatted size: 36 bytes / 2048 Kb
Unassigned Zones: 1
  zone name z1 vsan 1
```



Note VSAN あたりのフルゾーン データベースの最大サイズは 4096 KB です。

アクティブ ゾーン分割データベースの分析

```
switch(config-zone)# show zone analysis active vsan 1
Zoning database analysis vsan 1
  Active zoneset: qoscfg
  Activated at: 14:40:55 UTC Mar 21 2014
  Activated by: Local [ CLI ]
  Default zone policy: Deny
  Number of devices zoned in vsan: 8/8 (Unzoned: 0)
  Number of zone members resolved: 10/18 (Unresolved: 8)
  Num zones: 4
  Number of IVR zones: 0
  Number of IPS zones: 0
  Formatted size: 328 bytes / 4096 Kb
```



Note VSAN あたりのゾーン データベースの最大サイズは 4096 KB です。

ゾーンセットの分析

```
switch(config-zone)# show zone analysis zoneset qoscfg vsan 1
Zoning database analysis vsan 1
  Zoneset analysis: qoscfg
  Num zonesets: 1
  Num zones: 4
  Num aliases: 0
  Num attribute groups: 1
  Formatted size: 480 bytes / 4096 Kb
```

ゾーン ステータスの表示

```
switch(config-zone)# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
```

```
activation overwrite control:disabled
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Current Total Zone DB Usage: 4 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 4 / 2097152 bytes (0 % used)
Status:
VSAN: 8 default-zone: deny distribute: full Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 1946498 bytes
Zonesets:6 Zones:8024 Aliases: 0
Active Zoning Database :
DB size: 150499 bytes
Name: zoneset-1000 Zonesets:1 Zones:731
Current Total Zone DB Usage: 2096997 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 2096997 / 2097152 bytes (99 % used)
Status: Zoneset distribution failed [Error: Fabric changing Dom 33]:
at 17:05:06 UTC Jun 16 2014
VSAN: 9 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 2002584 bytes
Zonesets:4 Zones:7004 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 94340 bytes
Name: zoneset-hac13-200 Zonesets:1 Zones:176
Current Total Zone DB Usage: 2096924 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Activation completed at 17:28:04 UTC Jun 16 2014
VSAN: 12 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
```

```

DB size: 84 bytes
Zonesets:0 Zones:1 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 144 bytes
Name: zs1 Zonesets:1 Zones:2
Current Total Zone DB Usage: 228 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Commit completed at 14:39:33 UTC Jun 27 201

```

システムのデフォルトゾーンの表示

```

switch(config)# show system default zone
system default zone default-zone deny
system default zone distribute active only
system default zone mode basic
system default zone gs read-write
system default zone smart-zone disabled

```

コマンド出力に表示される情報の詳細については、『[Cisco MDS 9000 Series Command Reference](#)』を参照してください。

ゾーン分割のベストプラクティス

シスコのマルチレイヤディレクタスイッチ（MDS）では、ファイバチャネル（FC）ラインカードで「Ternary Content Addressable Memory」（TCAM）と呼ばれる特別な種類のメモリが使用されます。この特別なメモリにより、Cisco MDSのアクセスコントロールリスト（ACL）タイプの機能が提供されます。この機能を制御するプロセスは「ACLTCAM」と呼ばれます。E/TEポート（Inter Switch Link（ISL））とF（ファブリック）ポートには、それぞれのポートタイプに固有の独自のプログラミングがあります。

TCAM リージョン

TCAMは、さまざまなサイズのいくつかのリージョンに分割されます。主なリージョンと、各リージョンに含まれるプログラミングのタイプを [Table 11: TCAM リージョン, on page 152](#) に示します。

Table 11: TCAM リージョン

領域	プログラミングタイプ
リージョン1：最上位システム	ファブリック ログイン、ポート ログイン、診断機能（10～20%）
リージョン2：セキュリティ	セキュリティ、相互運用モード4機能、IVR ELS キャプチャ（5～10%）

領域	プログラミング タイプ
リージョン 3 : ゴーニング	ゾーン分割の機能 (IVR および SAN 分析を含む) (50 ~ 75%)
リージョン 4 : 最下位 ²	PLOGI、ACC、および FCSP トラップ、ISL、ECHO 許可 (10 ~ 20%)

² ハードゾーン分割障害が発生すると、リージョン 4 (最下位リージョン) を使用して、エニーツーエニー通信を可能にするワイルドカード エントリがプログラムされます。

TCAM リージョンは自動的に設定され、変更できません。TCAM は、モジュールごとおよびフォワーディング エンジン (fwd-eng) ごとに割り当てられます。

MDS 9148S および MDS 9250i ファブリック スイッチの TCAM スペースは、ディレクタクラス のファイバチャネルモジュールおよび新しいファブリック スイッチ (MDS 9396S、MDS 9132T など) や今後発売予定のスイッチよりもかなり少ないものになります。

ポートがオンラインになると、そのポートに関してある程度の基本的なプログラミングが必要 になります。このプログラミングはポートのタイプによって異なります。この基本的なプログ ラミングは最小限のものであり、多くの TCAM エントリを消費することはありません。通常、 このプログラミングは入力に関して行われ、スイッチで受信されるフレームがプログラミング の影響を受けますが、スイッチから送信されるフレームは影響を受けません。

ACL TCAM アラート

Cisco MDS NX-OS リリース 8.3(1) 以降、MDS 9148S および MDS 9250i スイッチを除くすべ ての Cisco MDS スイッチで ACL TCAM 使用率アラートの Syslog メッセージが導入されました。 Cisco MDS NX-OS リリース 8.3(2) 以降では、Cisco MDS 9148S および MDS 9250i スイッチでも ACL TCAM 使用率アラートの Syslog メッセージが導入されました。

- 示されているモジュール、方向、リージョン、およびフォワーディング エンジンで TCAM 使用率が 80% を超えると、次のシステム メッセージが生成されます。このシステム メッセージは、TCAM が使い果たされたこと、または TCAM プログラミングが失敗したことを示すものではありません。

```
%ACLTCAM-SLOT1-4-REGION_RISING_THRESHOLD: ACL (region) (input | output) region usage (num of in use entries of total entries) exceeded 80% on forwarding engine (num)
```

- 示されているモジュール、リージョン、方向、およびフォワーディング エンジンの TCAM 使用率が 80% のしきい値を下回ると、次のシステム メッセージが生成されます。このシ ステム メッセージは、TCAM が使い果たされたこと、または TCAM プログラミングが失 敗したことを示すものではありません。

```
%ACLTCAM-SLOT1-4-REGION_FALLING_THRESHOLD: ACL (region) (input | output) region usage (num of in use entries of total entries) fell below 80% on forwarding engine (num)
```

- フォワーディング エンジンに示される TCAM の全体的な使用率が、示されているモジュ ール、方向、およびフォワーディング エンジンの 60% を超えると、次のシステム メッセ ージが生成されます。

```
%ACLTCAM-SLOT1-4-TOTAL_RISING_THRESHOLD: ACL total (input | output) usage (num of
in use entries of total entries) exceeded 60% on forwarding engine (num)
```

- フォワーディングエンジンに示される TCAM の全体的な使用率が、示されているモジュール、方向、およびフォワーディングエンジンの 60% を下回ると、次のシステムメッセージが生成されます。

```
%ACLTCAM-SLOT1-4-TOTAL_FALLING_THRESHOLD: ACL total (input | output) usage (num of
in use entries of total entries) fell below 60% on forwarding engine (num)
```

Cisco MDS 9148S および MDS 9250i スイッチ以外の場合、ACLTCAM 使用率を表示するには、**show system internal acl tcam-usage** コマンドを使用します。Cisco MDS 9148S および MDS 9250i スイッチの場合は、**show system internal acltcam-soc tcam-usage** コマンドを使用してください。

TCAM 使用率アラートの Syslog メッセージが表示される場合は、ゾーン分割、ポートチャネルのポート割り当て、および分析の設定を調べる必要がある可能性があります。TCAM 使用率が 100% に達すると、一部のデバイスで、それらとともにゾーン分割されている他のデバイスと通信できなくなる可能性があります。このセクションに示されている推奨事項に従って TCAM 使用率を低下させてください。

ゾーン分割のタイプ

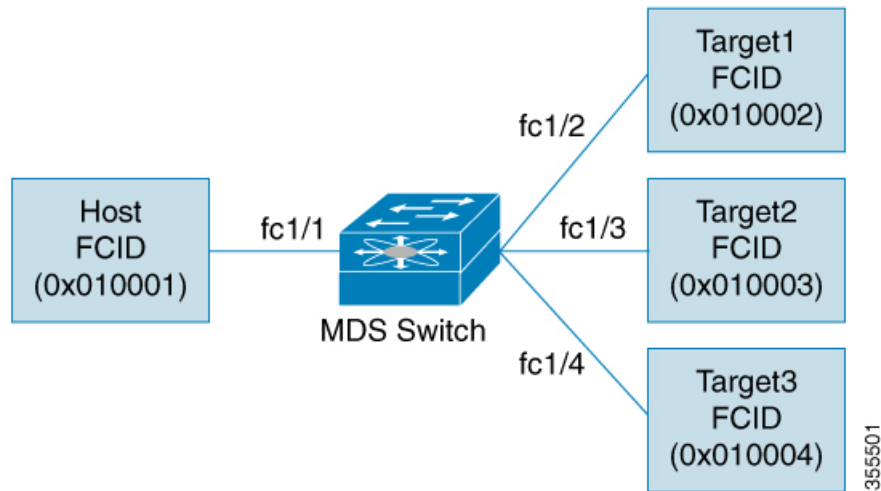
Cisco MDS プラットフォームでは、「ハード」ゾーン分割と「ソフト」ゾーン分割という 2 つのタイプのゾーン分割が使用されます。

ソフトゾーン分割：このモードでは、コントロールプレーントラフィックだけがスイッチスーパーバイザサービスによってポリシングされます。特に、ファイバチャネルネームサーバー (FCNS) は、FCNS 応答で許可されるデバイスのリストをゾーン設定内のものだけに制限します。ただし、エンドデバイスのデータプレーントラフィックはポリシングされません。これは、不正なエンドデバイスが、それとともにゾーン分割されていない他のデバイスに接続する可能性があることを意味します。

ハードゾーン分割：このモードでは、コントロールプレーントラフィックとデータプレーントラフィックの両方がポリシングされます。コントロールプレーントラフィックはスイッチスーパーバイザによってポリシングされ、データプレーントラフィックはハードウェアの支援により各入力ポートでポリシングされます。ポリシングルールは、各ラインカードにプログラムされたゾーンセットによって設定されます。各フレームの宛先はハードウェアによってチェックされ、ゾーン分割によって許可されていない場合はドロップされます。このモードでは、どのデバイスも、許可されているエンドデバイスだけと通信できます。

デフォルトでは、両方のタイプのゾーン分割が有効になっており、ハードゾーン分割がソフトゾーン分割よりも優先されます。ハードウェアリソースが使い果たされたためにシステムがハードゾーン分割を使用できなくなる場合、このゾーン分割は無効になり、システムはソフトゾーン分割の使用にフォールバックします。

次の例は、Cisco MDS がポートに関して TCAM をプログラムする方法を示しています。



次の例は、VSAN に対して設定されたアクティブ ゾーンセットのゾーンを示しています。これは、ハード ゾーン分割のためにインターフェイス上に存在する基本的なプログラミングです。

```
zone1
member host (FCID 0x010001)
member target1 (FCID 0x010002)
```

このようなシナリオでは、ACL プログラミングは次のようになります。

```
fc1/1 - Host interface
Entry#   Source ID   Mask      Destination ID   Mask      Action
1        010001     ffffffff  010002(target1) ffffffff  Permit
2        000000     000000   000000           000000   Drop
fc1/2 - Target1 interface
Entry#   Source ID   Mask      Destination ID   Mask      Action
1        010002     ffffffff  010001(Host)    ffffffff  Permit
2        000000     000000   000000           000000   Drop
```



Note ここに示されているもの以外に、追加のプログラミングが存在します。また、TCAM テーブルはすべて drop-all エントリで終了します。

マスクは、FCID のどの部分が入力フレームと照合されるのかを示しています。そのため、マスクが 0xffffffff の場合は、FCID を ACL エントリと照合するときに FCID 全体が考慮されます。マスクが 0x000000 の場合は、デフォルトではすべての FCID と一致するため、FCID のどの部分も考慮されません。

上記のプログラミング例では、fc1/1 でフレームを受信され、送信元 ID (FCID) が 0x010001 (ホスト)、宛先 ID (FCID) が 0x010002 (Target1) の場合、そのフレームは許可され、宛先にルーティングされます。その他のエンドツーエンド通信はすべてドロップされます。

次の例は、ゾーン分割が変更される別のシナリオを示しています。

```
zone1
```

```

member host (FCID 010001)
member target1 (FCID 010002)
member target2 (FCID 010003)
member target3 (FCID 010004)

```

このようなシナリオでは、ACLプログラミングは次のようになります。

```

fc1/1 Host interface
Entry#   Source ID   Mask   Destination ID   Mask   Action
1        010001   ffffff 010002(target1) ffffff Permit
2        010001   ffffff 010003(target2) ffffff Permit
3        010001   ffffff 010004(target3) ffffff Permit
4        000000   000000 000000           000000 Drop
fc1/2 - Target1 interface
Entry#   Source ID   Mask   Destination ID   Mask   Action
1        010002   ffffff 010001(host)     ffffff Permit
2        010002   ffffff 010003(target2) ffffff Permit
3        010002   ffffff 010004(target3) ffffff Permit
4        000000   000000 000000           000000 Drop
fc1/3 - Target2 interface
Entry#   Source ID   Mask   Destination ID   Mask   Action
1        010003   ffffff 010001(host)     ffffff Permit
2        010003   ffffff 010002(target1) ffffff Permit
3        010003   ffffff 010004(target3) ffffff Permit
4        000000   000000 000000           000000 Drop
fc1/4 - Target3 interface
Entry#   Source ID   Mask   Destination ID   Mask   Action
1        010004   ffffff 010001(host)     ffffff Permit
2        010004   ffffff 010002(target1) ffffff Permit
3        010004   ffffff 010003(target2) ffffff Permit
4        000000   000000 000000           000000 Drop

```

上記の例は、ゾーン (N) によって消費される TCAM エントリの数が $N*(N-1)$ に等しいことを示しています。このため、4つのメンバーを持つゾーンでは、合計 12 の TCAM エントリが使用されます ($4*3=12$)。drop-all エントリは、 $N*(N-1)$ ルールにカウントされないことに注意してください。

上記の例では、ターゲットインターフェイス (fc1/2 ~ fc1/4) のそれぞれに 2つのエントリが示されています。通常、複数のターゲットをまとめてゾーン分割することにはメリットがないため、それらのエントリは不要です。たとえば、fc1/2 には、Target1 が Target2 と通信することを許可するエントリと、Target1 が Target3 と通信することを許可するエントリがあります。

これらのエントリは不要であるだけでなく、悪影響をおよぼす可能性があるため、避ける必要があります。単一イニシエータのゾーンまたは単一ターゲットのゾーンを使用する（またはスマートゾーン分割を使用する）ことにより、このようなエントリの追加を回避できます。



Note 2つの同じデバイスがゾーンセット内の複数のゾーンに存在する場合、TCAM プログラミングは繰り返されません。

次の例は、3つの個別のゾーンに変更されるゾーンを示しています。

```

zone1
member host (FCID 010001)
member target1 (FCID 010002)
zone2

```

```

member host (FCID 010001)
member target2 (FCID 010003)
zone3
member host (FCID 010001)
member target3 (FCID 010004)

```

このようなシナリオでは、ACLプログラミングは次のようになります。

```

fc1/1 - Host interface - This would look the same
Entry#   Source ID   Mask      Destination ID   Mask   Action
1        010001     ffffffff  010002(target1) ffffff Permit
2        010001     ffffffff  010003(target2) ffffff Permit
3        010001     ffffffff  010004(target3) ffffff Permit
4        000000     000000   000000          000000 Drop
fc1/2 - Target1 interface
Entry#   Source ID   Mask      Destination ID   Mask   Action
1        010002     ffffffff  010001(host)    ffffff Permit
2        000000     000000   000000          000000 Drop
fc1/3 - Target2 interface
Entry#   Source ID   Mask      Destination ID   Mask   Action
1        010003     ffffffff  010001(host)    ffffff Permit
2        000000     000000   000000          000000 Drop
fc1/4 - Target3 interface
Entry#   Source ID   Mask      Destination ID   Mask   Action
1        010004     ffffffff  010001(host)    ffffff Permit
2        000000     000000   000000          000000 Drop

```

上記の例で、ターゲット間のエントリがないことと、12のエントリのうちの6つがプログラミングされなくなっていることに注意してください。これにより、TCAMの使用率が低下し、セキュリティが向上します（ホストだけが3つのターゲットと通信でき、ターゲット自体は1つのホストと通信できるだけで相互には通信できません）。

フォワーディング エンジン

シスコのマルチレイヤディレクタ スイッチ (MDS) では、ファイバチャネルモードで TCAM (Ternary Content Addressable Memory) と呼ばれる特別な種類のメモリが使用されます。この特別なメモリにより、Cisco MDS のアクセス コントロール リスト (ACL) タイプの機能が提供されます。この機能を制御するプロセスは「ACLTCAM」と呼ばれます。E または TE ポート (ISL) と F (ファブリック) ポートには、それぞれのポート タイプに固有の独自のプログラミングがあります。

TCAM は個別のフォワーディング エンジンに割り当てられ、フォワーディング エンジンにはポートのグループが割り当てられます。ディレクタクラスのファイバチャネルモジュールには、ファブリック スイッチよりも多くの TCAM スペースがあります。フォワーディング エンジンの数、各フォワーディング エンジンに割り当てられるポート、および各フォワーディング エンジンに割り当てられる TCAM の量は、ハードウェアによって異なります。

次の例は、Cisco MDS 9148S からの出力を示しています。

```

switch# show system internal acltcam-soc tcam-usage
TCAM Entries:
=====
Mod Fwd   Dir      Region1  Region2  Region3  Region4  Region5  Region6
Eng                                     Use/Total Use/Total Use/Total Use/Total Use/Total Use/Total
---
1   1   INPUT   19/407   1/407    1/2852 * 4/407    0/0      0/0

```

1	1	OUTPUT	0/25	0/25	0/140	0/25	0/12	1/25
1	2	INPUT	19/407	1/407	0/2852 *	4/407	0/0	0/0
1	2	OUTPUT	0/25	0/25	0/140	0/25	0/12	1/25
1	3	INPUT	19/407	1/407	0/2852 *	4/407	0/0	0/0
1	3	OUTPUT	0/25	0/25	0/140	0/25	0/12	1/25

* 1024 entries are reserved for LUN Zoning purpose.

上記の例は、次のことを示しています。

- 3つのフォワーディングエンジン（1～3）が存在します。
- Cisco MDS 9148 スイッチには48のポートがあるため、各フォワーディングエンジンは16のポートを処理します。
- 各フォワーディングエンジンは、入力に関してリージョン3（ゾーン分割リージョン）に2852のエントリを持っています。これが使用される主なリージョンであり、その結果、利用可能なエントリには最大量があります。
- フォワーディングエンジン3には、ゾーン分割リージョン内の合計2852のエントリのうち、現在使用中のエントリが1つだけあります。

次の例は、2/4/8/10/16 Gbps 拡張ファイバチャネル モジュール（DS-X9448-768K9）を搭載した Cisco MDS 9710 スイッチからの出力を示しています。

```
F241-15-09-9710-2# show system internal acl tcam-usage
TCAM Entries:
=====
Mod Fwd  Dir      Region1  Region2  Region3  Region4  Region5  Region6
   Eng                TOP SYS  SECURITY  ZONING    BOTTOM    FCC DIS  FCC ENA
                        Use/Total Use/Total Use/Total Use/Total Use/Total Use/Total
-----
1  0  INPUT    55/19664  0/9840   0/49136* 17/19664  0/0       0/0
1  0  OUTPUT   13/4075   0/1643   0/11467   0/4075   6/1649   21/1664
1  1  INPUT    52/19664  0/9840   2/49136* 14/19664  0/0       0/0
1  1  OUTPUT    7/4078   0/1646   0/11470   0/4078   6/1652   5/1651
1  2  INPUT    34/19664  0/9840   0/49136* 10/19664  0/0       0/0
1  2  OUTPUT    5/4078   0/1646   0/11470   0/4078   6/1652   1/1647
1  3  INPUT    34/19664  0/9840   0/49136* 10/19664  0/0       0/0
1  3  OUTPUT    5/4078   0/1646   0/11470   0/4078   6/1652   1/1647
1  4  INPUT    34/19664  0/9840   0/49136* 10/19664  0/0       0/0
1  4  OUTPUT    5/4078   0/1646   0/11470   0/4078   6/1652   1/1647
1  5  INPUT    34/19664  0/9840   0/49136* 10/19664  0/0       0/0
1  5  OUTPUT    5/4078   0/1646   0/11470   0/4078   6/1652   1/1647
...
```

上記の例は、次のことを示しています。

- 6つのフォワーディングエンジン（0～5）が存在します。
- Cisco MDS DS-X9448-768K9 モジュールには48のポートがあるため、各フォワーディングエンジンは8つのポートを処理します。
- 各フォワーディングエンジンは、入力に関してリージョン3（ゾーン分割リージョン）に49136のエントリを持っています。これが使用される主なリージョンであり、その結果、利用可能なエントリには最大量があります。

- フォワーディング エンジン 2 には、ゾーン分割リージョン内の合計 49136 のエントリのうち、現在使用中のエントリが 2 つだけあります。



Note ファブリック スイッチでの TCAM 使用率を表示するために使用されるコマンドは、ディレクタクラスのスイッチで使用されるものとは異なります。MDS 9148、MDS 9148S、および MDS 9250i ファブリック スイッチの場合は、**show system internal acltcam-soc tcam-usage** コマンドを使用します。ディレクタクラス スイッチ、MDS 9396S、および 32 Gbps ファブリック スイッチの場合は、**show system internal acl tcam-usage** コマンドを使用します。

次の表に、ポートからフォワーディング エンジンへのマッピングに関する情報を示します。

Table 12: ポートからフォワーディング エンジンへのマッピング

スイッチまたはモジュール	フォワーディング エンジン	ポートグループ	フォワーディング エンジン 番号	ゾーン分割リージョン エントリ	最下位リージョンのエントリ
MDS 9132T	2	1-16	0	49136	19664
		17 ~ 32	1	49136	19664
MDS 9148	3	fc1/25 ~ 36、 fc1/45 ~ 48	1	2852	407
		fc1/5 ~ 12、 fc1/37 ~ 44	2	2852	407
		fc1 ~ 4、 fc1/13 ~ 24	3	2852	407
MDS 9148S	3	fc1/1 ~ 16	1	2852	407
		fc1/17 ~ 32	2	2852	407
		fc1/33 ~ 48	3	2852	407
MDS 9148T	3	1-16	0	49136	19664
		17 ~ 32	1	49136	19664
		33 ~ 48	2	49136	19664

スイッチまたはモジュール	フォワーディングエンジン	ポートグループ	フォワーディングエンジン番号	ゾーン分割リージョンエントリ	最下位リージョンのエントリ
MDS 9250i	4	fc1/5 ~ 12、 eth1/1 ~ 8	1	2852	407
		fc1/1 ~ 4、 fc1/13 ~ 20、 fc1/37 ~ 40	2	2852	407
		fc1/21 ~ 36	3	2852	407
		ips1/1 ~ 2	4	2852	407
MDS 9396S	12	fc1/1 ~ 8	0	49136	19664
		fc1/9 ~ 16	1	49136	19664
		fc1/17 ~ 24	2	49136	19664
		fc1/25 ~ 32	3	49136	19664
		fc1/33 ~ 40	4	49136	19664
		fc1/41 ~ 48	5	49136	19664
		fc1/49 ~ 56	6	49136	19664
		fc1/57 ~ 64	7	49136	19664
		fc1/65 ~ 72	8	49136	19664
		fc1/73 ~ 80	9	49136	19664
		fc1/81 ~ 88	10	49136	19664
		fc1/89 ~ 96	11	49136	19664
MDS 9396T	6	1-16	0	49136	19664
		17 ~ 32	1	49136	19664
		33 ~ 48	2	49136	19664
		49 ~ 64	3	49136	19664
		65 ~ 80	4	49136	19664
		81 ~ 96	5	49136	19664
DS-X9248-48K9	1	1 ~ 48	0	27168	2680

スイッチまたはモジュール	フォワーディングエンジン	ポートグループ	フォワーディングエンジン番号	ゾーン分割リージョンエントリ	最下位リージョンのエントリ
DS-X9248-96K9	2	1 ~ 24	0	27168	2680
		25 ~ 48	1	27168	2680
DS-X9224-96K9	2	1 ~ 12	0	27168	2680
		13 ~ 24	1	27168	2680
DS-X9232-256K9	4	1 ~ 8	0	49136	19664
		9 ~ 16	1	49136	19664
		17 ~ 24	2	49136	19664
		25 ~ 32	3	49136	19664
DS-X9248-256K9	4	1 ~ 12	0	49136	19664
		13 ~ 24	1	49136	19664
		25 ~ 36	2	49136	19664
		37 ~ 48	3	49136	19664
DS-X9448-768K9	6	1 ~ 8	0	49136	19664
		9 ~ 16	1	49136	19664
		17 ~ 24	2	49136	19664
		25 ~ 32	3	49136	19664
		33 ~ 40	4	49136	19664
		41 ~ 48	5	49136	19664
DS-X9334-K9	3	1 ~ 8	0	49136	19664
		9 ~ 16	1	49136	19664
		17 ~ 24	2	49136	19664
DS-X9648-1536K9	3	1-16	0	49136	19664
		17 ~ 32	1	49136	19664
		33 ~ 48	2	49136	19664

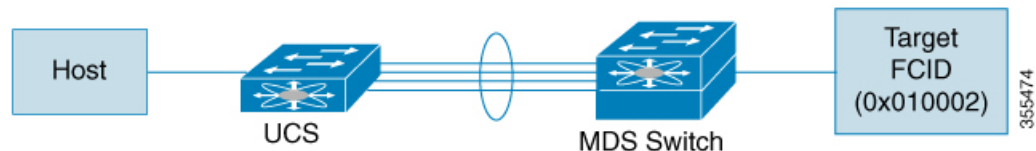
F、TF、NP、および TNP ポート チャンネル



Note エッジの Cisco N ポート仮想化 (NPV) スイッチに接続されているデバイスについては、インターフェイス、fWWN、またはドメイン ID ベースのゾーン分割を使用することは推奨されません。

F ポート チャンネルにより、Cisco UCS ファブリック インターコネクト (FI) を含む N ポート仮想化 (NPV) スイッチへの接続において、フォールトトレランスおよびパフォーマンス上の利点が得られます。F ポート チャンネルは、ACL TCAM プログラミングに関する固有の課題をもたらします。F ポートがポート チャンネルに集約されると、ACL TCAM プログラミングが各メンバー インターフェイスについて繰り返されます。その結果、これらのタイプのポート チャンネルでは必要な TCAM エントリの量を増加させます。このため、メンバー インターフェイスが可能なかぎり最適に割り当てられるとともに、ゾーン分割のベストプラクティスが実行される必要があります。これらの F ポート チャンネルに 100 を超えるホスト ログインを含めることができるという事実も考慮すると、特にファブリック スイッチの場合にベストプラクティスに従わなければ、TCAM を簡単に超過する可能性があります。

次にトポロジの例を示します。



この例では、ポート チャンネル (PC) に 8 つのインターフェイス (fc1/1 ~ fc1/8) が含まれていると想定されています。

さらに、次の 2 つのゾーンがアクティブです。

```

zone1
member host (host 0x010001)
member target1 (target1 0x010002)
zone2
member host (host 0x010001)
member target2 (target2 0x010003)
  
```

このようなシナリオでは、次の ACL プログラミングが PC の各メンバーに存在します。

```

fc1/1(through fc1/8) (port-channel)
Entry#    Source ID    Mask        Destination ID    Mask        Action
1         010001      ffffffff    010002(target1)  ffffffff    Permit
2         010001      ffffffff    010003(target2)  ffffffff    Permit
3         000000      000000     000000           000000     Drop
  
```

上記の例は、F ポート チャンネルの各メンバーで複製される ACL TCAM プログラミングを示しています。その結果、F ポート チャンネル上の多数の FLOGI のために多数のプログラミングが必要な場合、または多数のデバイスが F ポート チャンネル上のデバイスとともにゾーン分割されている場合、フォワーディング エンジンで TCAM が使い果たされる可能性があります。F

ポートおよび F ポートチャネルに関して TCAM を効率的に使用するためのベストプラクティスは次のとおりです。

- 特にファブリックスイッチでは、ポートチャネルメンバーインターフェイスを異なるフォワーディングエンジンに分散させます。
- 多数のインターフェイスを持つポートチャネルの場合、TCAM 使用率が依然として高すぎる場合は、ポートチャネルを 2 つの個別のポートチャネル（それぞれ半分のインターフェイスを持つ）に分割します。これでも冗長性は提供されますが、個々のポートチャネルの FLOGI の数が減るため、TCAM 使用率が低下します。
- メンバーインターフェイスをディレクタクラススイッチ上の異なるラインカードに分散させます。
- メンバーインターフェイスを TCAM ゾーン分割リージョンの使用量が少ないフォワーディングエンジンに分散させます。
- 単一イニシエータのゾーン、単一ターゲットのゾーン、またはスマートゾーン分割を使用します。

E および TE ポートチャネルと IVR

E ポートチャネルは、ファブリックスイッチ間の Inter Switch Link (ISL) を提供します。通常、これらのタイプのインターフェイスには最小限の TCAM プログラミングが存在します。そのため、異なるラインカードや、ディレクタクラスのスイッチのポートグループにそれらを分散させるだけでなく、もう少し追加の作業を実行します。ただし、VSAN 間ルーティング (IVR) 機能が展開されている場合、IVR トポロジは VSAN 間で移行するため、ISL 上に多数の TCAM プログラミングが存在する可能性があります。そのため、F/TF ポートチャネルに適用される考慮事項のほとんどが、ここでも適用可能です。

次にトポロジの例を示します。



このトポロジは、次のようになっています。

- Cisco MDS 9148S-1 と MDS 9148S-2 の両方が IVR VSAN トポロジに含まれます。

```

MDS9148S-1 vsan 1 and vsan 2
MDS9148S-2 vsan 2 and vsan 3
  
```

- IVR NAT が設定されています。
- VSAN 2 は中継 VSAN です。

```

FCIDs per VSAN:
      VSAN 1  VSAN 2  VSAN 3
  
```

```
Host          010001  210001  550002
Target1      440002  360002  030001
```



Note VSAN 1 のドメイン 0x44、VSAN 2 の 0x21 と 0x36、および VSAN 3 の 0x55 は、IVR NAT によって作成された仮想ドメインです。

- 次に IVR ゾーン分割トポロジを示します。

```
ivr zone zone1
member host vsan 1
member target1 vsan3
```

- 次に IVR ゾーン分割トポロジの ACL TCAM プログラミングを示します。

```
MDS9148S-1 fc1/1(Host) - VSAN 1
Entry#   Source ID      Mask      Destination ID      Mask      Action
1        010001(host)   fffffff  440002(target1)   fffffff  Permit
- Forward to fc1/2
- Rewrite the following information:
  VSAN to 2
  Source ID to 210001
  Destination ID to 360002
2        000000         000000   000000              000000   Drop
MDS9148S-1 fc1/2(ISL) - VSAN 2
Entry#   Source ID      Mask      Destination ID      Mask      Action
1        360002(Target1) fffffff  210001(host)       fffffff  Permit
- Forward to fc1/2
- Rewrite the following information:
  VSAN to 1
  Source ID to 440002
  Destination ID to 010001
MDS9148S-2 fc1/2(ISL) - VSAN 2
Entry#   Source ID      Mask      Destination ID      Mask      Action
1        210001(host)   fffffff  360002(target1)   fffffff  Permit
- Forward to fc1/2
- Rewrite the following information:
  VSAN to 3
  Source ID to 550002
  Destination ID to 030001
MDS9148S-2 fc1/1(Target1) - VSAN 3
Entry#   Source ID      Mask      Destination ID      Mask      Action
1        030001(Target1) fffffff  550002(host)       fffffff  Permit
- Forward to fc1/2
- Rewrite the following information:
  VSAN to 2
  Source ID to 360002
  Destination ID to 210001
2        000000         000000   000000              000000   Drop
```



Note この例のエントリのほかに、IVR が PLOGI、PRILI、ABTS などの重要なフレームをキャプチャするために追加するエントリがあります。

ホストポートと Target1 ポートでのプログラミングは、FCIDおよびVSANが明示的に出力ポートに転送され、中継 VSAN (VSAN 2) に適した値に書き換えられる点を除いて、IVR がない場合と同様です。これらの転送エントリと書き換えエントリは個別のものであり、TCAM使用率の値には含まれません。

ただし、今回、両方のスイッチの ISL には、以前には存在しなかったプログラミングが存在します。ホストから Target1 へのフレームが Cisco MDS 9148S-2 fc1/2 によって受信されると、ターゲットが存在する VSAN 3 の値に書き換えられます。逆方向では、Target1 からホストへのフレームが Cisco MDS 9148S-1 fc1/2 で受信されると、ホストが存在する VSAN 1 の値に書き換えられます。そのため、ISL での各 VSAN 移行 (通常、中継 VSAN をまたいで発生) について、IVR ゾーンセット内の各デバイスに対して TCAM プログラミングが存在します。

その結果、TCAM が次の目的で確実に可能なかぎり効率的に利用されるように、F および TF ポート チャネルに関して実行されるベスト プラクティスのほとんどに従う必要があります。



Note F および TF ポート チャネルとは異なり、ISL での ACLTCAM プログラミングは、ISL がポート チャネルの一部であるかどうかにかかわらず、同じ量になります。2つの MDS スイッチの間に「n」の ISL がある場合、それらが1つのポートチャネルにあるか、2つのポートチャネルにあるか、または個別のリンクだけにあるかは関係ありません。ACLTCAM プログラミングは同じになります。

- 特にファブリック スイッチでは、ポートチャネルメンバー インターフェイスを異なるフォワーディング エンジンに分散させます。
- メンバー インターフェイスをディレクタクラス スイッチ上の異なるラインカードに分散させます。
- メンバー インターフェイスを TCAM ゾーン分割リージョンの使用量が少ないフォワーディング エンジンに分散させます。
- 単一イニシエータのゾーン、単一ターゲットのゾーン、またはスマートゾーン分割を使用します。

ゾーン サーバー パフォーマンスの強化

ゾーン サーバー - ファイバチャネル ネーム サーバー 共有データベース

このオプションは、ゾーン サーバーとファイバチャネル ネーム サーバー (FCNS) が相互に通信できるようにするための共有データベースを提供します。データベースを共有すると、ソフトゾーン分割の管理におけるゾーン サーバーの FCNS への依存が軽減されます。



Note デフォルトでは、ゾーンサーバー - FCNS 共有データベース オプションは有効になっています。

ゾーンサーバー - FCNS 共有データベースの有効化

ゾーンサーバー - FCNS 共有データベースを有効にするには、次の手順を実行します。

ステップ1 コンフィギュレーション モードを開始します。

```
switch # configure terminal
```

ステップ2 VSAN 1 でアクティブ ゾーンセットのデータベース共有を有効にします。

```
switch(config)# zoneset capability active mode shared-db vsan 1
```

Example

ゾーンサーバー - FCNS 共有データベースの有効化

次に、VSAN 1 でのみアクティブ ゾーンセットのデータベース共有を有効にする例を示します。

```
switch(config)# zoneset capability active mode shared-db vsan 1  
SDB Activation success
```

ゾーンサーバー - FCNS 共有データベースの無効化

VSAN 1 でアクティブ ゾーンセットを無効にするには、次の手順を実行します。

ステップ1 グローバル コンフィギュレーション モードを開始します。

```
switch# configure terminal
```

ステップ2 VSAN 1 で設定されているアクティブ ゾーンを無効にします。

```
switch(config)# no zoneset capability active mode shared-db vsan 1
```

Example

ゾーンサーバー - FCNS 共有データベースの無効化

次に、VSAN 1 でアクティブ ゾーン セットのデータベース共有を無効にする例を示します。

```
switch(config)# no zoneset capability active mode shared-db vsan 1
SDB Deactivation success
```

ゾーン サーバー SNMP 最適化

このオプションでは、Simple Network Management Protocol (SNMP) 操作のためのゾーン サーバー スケーリング 拡張が有効になります。これにより、SNMP により実行されるすべてのゾーン クエリーにゾーン サーバーが使用されなくなります。



Note デフォルトでは、ゾーン サーバー SNMP 最適化オプションは有効になっています。

ゾーン サーバー SNMP 最適化の有効化

SNMP 操作のためにゾーン サーバー スケーリング 拡張を有効にするには、次の手順を実行します。

ステップ 1 コンフィギュレーション モードを開始します。

```
switch # configure terminal
```

ステップ 2 ゾーン サーバー SNMP 最適化を有効にします。

```
switch(config)# zone capability shared-db app snmp
```

ステップ 3 設定のステータスを表示します。

```
switch(config)# show running | i shared-db
```

Example

ゾーン サーバー SNMP 最適化の有効化

次に、ゾーン サーバー SNMP 最適化を有効にする例を示します。

```
switch(config)# zone capability shared-db app snmp
```

ゾーン サーバー SNMP 最適化の無効化

ゾーン サーバー SNMP 最適化を無効にするには、次の手順を実行します。

ステップ 1 コンフィギュレーション モードを開始します。

```
switch # configure terminal
```

ステップ 2 ゾーン サーバー SNMP 最適化を無効にします。

```
switch(config)# no zone capability shared-db app snmp
```

Example

ゾーン サーバー SNMP 最適化の無効化

次に、ゾーン サーバー SNMP 最適化を無効にする例を示します。

```
switch(config)# no zone capability shared-db app snmp
```

ゾーン サーバー 差分配信

この機能により、既存のゾーン データベースと更新されたゾーン データベース間でのゾーン 変更の差分を、ファブリック内のすべてのスイッチに配信できます。この差分変更の配信により、ゾーン データベースが変更されるたびにスイッチ間で大きなペイロードの配信が発生することを回避できます。



Note

- デフォルトでは、ゾーン サーバー 差分配信機能は無効です。この機能は拡張モードでのみ動作します。
- ファブリック内のすべてのスイッチで、ゾーン サーバー 差分配信機能が有効になっている必要があります。ゾーン サーバー 差分配信機能が無効なファブリックにスイッチを追加すると、ファブリック内のすべてのスイッチでゾーン サーバー 差分配信機能が無効になります。
- ゾーン サーバー 差分配信機能は Cisco MDS スイッチ（Cisco MDS NX-OS Release 7.3(0)D1(1)以降）でのみサポートされています。
- ゾーン サーバー 差分配信機能は、自動音声応答（IVR）機能に対応した VSAN では使用できません。

ゾーン サーバー差分配信の有効化

ゾーン サーバーでのデータ変更の配信を有効にするには、次の手順を実行します。

ステップ 1 コンフィギュレーション モードを開始します。

```
switch # configure terminal
```

ステップ 2 拡張モードでゾーンのデータ変更の配信を有効にします。

```
switch(config)# zone capability mode enhanced distribution diffs-only
```

ステップ 3 ファブリックの差分配信（データ変更）ステータスを表示します。

```
switch(config)# show running | include diffs-only
```

Example

ゾーン サーバー差分配信の有効化

次に、ゾーン サーバーでのデータ変更の配信を有効にする例を示します。

```
switch(config)# zone capability mode enhanced distribution diffs-only
```

ゾーン サーバー差分配信の無効化

ゾーン サーバーでのデータ変更の配信を無効にするには、次の手順を実行します。

ステップ 1 コンフィギュレーション モードを開始します。

```
switch # configure terminal
```

ステップ 2 ゾーンのデータ変更の配信を無効にします。

```
switch(config)# no zone capability mode enhanced distribution diffs-only
```

Example

ゾーン サーバー差分配信の無効化

次に、ゾーン サーバーでデータ変更の配信を無効にする例を示します。

```
switch(config)# no zone capability mode enhanced distribution diffs-only
```

デフォルト設定

次の表に、基本ゾーンパラメータのデフォルト設定値を示します。

Table 13: デフォルトの基本ゾーンパラメータ

パラメータ	デフォルト
デフォルトゾーンポリシー	すべてのメンバで拒否
フルゾーンセット配信	フルゾーンセットは配信されない
ゾーンベースのトラフィックプライオリティ	低。
ブロードキャストフレーム	サポート対象外
拡張ゾーン分割	ディセーブル
スマートゾーン分割	ディセーブル



CHAPTER 6

DDAS

Cisco MDS 9000 シリーズのすべてのスイッチは、ファブリック全体での Distributed Device Alias Service (デバイスエイリアス) をサポートしています。デバイスエイリアス配信により、エイリアス名を手動で再度入力することなく、VSAN 間で HBA (ホストバスアダプタ) を移動できます。

この章は、次の項で構成されています。

- [デバイスエイリアスについて, on page 171](#)
- [デバイスエイリアスのモード, on page 171](#)
- [デバイスエイリアス データベース, on page 179](#)
- [レガシーゾーンエイリアス設定の変換の概要, on page 185](#)
- [データベース マージの注意事項, on page 187](#)
- [デバイスエイリアス設定の確認, on page 188](#)
- [デフォルト設定, on page 190](#)
- [デバイスエイリアスのマージ失敗の解決 \(190 ページ\)](#)

デバイスエイリアスについて

Cisco MDS 9000 ファミリスイッチで機能 (ゾーン分割、QoS、ポートセキュリティなど) を設定するために、デバイスの port WWN (pWWN) を指定する必要がある場合は、これらの機能を設定するたびに、正しいデバイス名を割り当てる必要があります。デバイス名が正しくないと、予期しない結果が生じることがあります。この問題を回避するには、わかりやすい pWWN 名を定義し、必要に応じて、この名前をすべてのコンフィギュレーションコマンドで使用します。この章では、これらのわかりやすい名前をデバイスエイリアスと表します。

デバイスエイリアスのモード

デバイスエイリアス基本モードおよび拡張モード

デバイスエイリアスの機能は、基本モードと拡張モードの2つをサポートしています。

**Note**

- NX-OS プロセス (zone、dpvm、ivr など) などのアプリケーションの場合、device-alias が基本モードの場合、device-alias 構成はそれらの PWWN にマッピングされます。一方、デバイスエイリアスが拡張モードの場合、アプリケーションのデバイスエイリアス構成は PWWN にすぐにマッピングされませんが、ネイティブ フォームまたはフォーマットと呼ばれるアプリケーションで構成されたままになります。
- Cisco MDS NX-OS リリース 8.5(1) 以降、デフォルトのデバイスエイリアス モードは拡張モードです。

基本モードでデバイスエイリアスを使用する場合、ゾーン、DPVM、IVR などの NX-OS プロセスは、デバイスエイリアス名を構成内の関連付けられた pWWN にすぐに展開します。たとえば、デバイスエイリアスメンバーをゾーンに追加すると、デバイスエイリアスメンバーではなく pWWN メンバーとして追加されます。したがって、デバイスエイリアス エントリの pWWN を変更しても、(デバイスエイリアスを除く) すべての構成は更新されません。古い エントリを削除してゾーンを再構成することで、そのデバイスエイリアスを含むゾーンを手動で編集する必要があり、古い PWWN エントリを削除し、現在更新された PWWN を持つ同じデバイスエイリアス名でそれを追加し直すことで、PWWN が使用されるその他の構成を再構成する必要があります。それが完了したら、変更に適した方法で構成をアクティブにする必要があります。たとえば、ゾーンが変更された場合、必要に応じてゾーンセットを再アクティブ化してコミットする必要があります。

拡張モードでデバイスエイリアスを使用する場合、ゾーン、DPVM、IVR などの NX-OS プロセスは、デバイスエイリアス名を pWWN に拡張するのではなく、指定されたとおりの構成内にネイティブに保存します。アプリケーションは、デバイスエイリアス データベースの変更を追跡し、すべての変更 (たとえば、デバイスエイリアスの名前変更) を適用するために必要な処理を行います。

このモードでは、構成がネイティブ形式で受け付けられるため、デバイスエイリアスの pWWN が変更されると、そのデバイスエイリアスが含まれているゾーンまたはその他の構成が自動的に更新されます。

注意事項と制約事項

ネイティブデバイスエイリアス設定は、interop モードの VSAN では受け入れられません。IVR ゾーンセットのアクティブ化は、注入対象の対応する不明瞭なゾーンがネイティブ デバイスエイリアス メンバーでない場合、interop モードの VSAN で失敗します。

デバイスエイリアス モードのデフォルト

Cisco MDS NX-OS リリース 8.5(1) 以降、デフォルトのデバイスエイリアス モードは拡張モードです。Cisco MDS NX-OS リリース 8.5(1) より前は、デフォルトのデバイスエイリアス モードは基本モードでした。以前のリリースから Cisco MDS NX-OS Release 8.5(1) 以降のリリースにアップグレードした後、デバイスエイリアスモードは、デバイスエイリアス エントリが構成されておらず、デバイスエイリアス モードが基本である場合にのみ拡張モードに設定され

ます。デバイスエイリアスエントリが存在する場合、またはデバイスエイリアスモードがすでに拡張モードになっている場合、デバイスエイリアスモードは変更されません。スイッチが Cisco MDS NX-OS Release 8.5(1) 以降のリリースを最初に起動すると、デフォルトのデバイスエイリアスモードは拡張モードに設定されます。スイッチが Cisco MDS NX-OS Release 8.5(1) 以降のリリースから Cisco MDS NX-OS Release 8.4(2b) 以前のリリースにダウングレードされており、デバイスエイリアスエントリが構成されておらず、デバイスエイリアスモードが設定されていない場合、デフォルトのエイリアスモードが基本モードに戻ります。デバイスエイリアスエントリが存在するか、デバイスエイリアスモードが設定されている場合、デバイスエイリアスモードは変更されません。

Cisco MDS NX-OS リリース 8.5(1) からリリース 8.4(2c) へのダウングレードは、中断を伴う操作です。したがって、デバイスエイリアス構成はスイッチに保持されず、デフォルトのデバイスエイリアスモードは、ダウングレード後にリリース 8.4(2c) のデフォルトのデバイスエイリアスモードである基本モードに変更されます。

デフォルトが拡張モードに設定されている場合、次の `syslog` メッセージが表示されます。

```
%DEVICE-ALIAS-2-DDAS_DEFAULT_MODE: Device alias mode has been set to enhanced mode
```



- (注) Cisco MDS NX-OS Release 8.5(1) 以降のリリースを実行している新しいスイッチが、デバイスエイリアスの基本モードで実行されている既存のファブリックに導入されている場合は、新しいスイッチまたはデバイスでデバイスエイリアスモードを基本モードに構成する必要があります。エイリアスモードは、既存のファブリック内のスイッチに対して拡張モードに設定できます。

モード設定の変更

デバイスエイリアスモードが基本モードから拡張モードに変更されると、対応するアプリケーションはこの変更について通知されます。アプリケーションでは、ネイティブフォーマットでデバイスエイリアスペース設定を受け付け始めます。



- Note** デバイスエイリアスは以前に基本モードで実行されていたため、アプリケーションには前のネイティブデバイスエイリアス設定はありません。

アプリケーションはネイティブフォーマットの既存のデバイスエイリアス設定をチェックします。デバイスエイリアスがネイティブフォーマットである場合、アプリケーションは要求を拒否し、デバイスエイリアスモードを基本に変更できません。

すべてのネイティブのデバイスエイリアス設定（ローカルスイッチとリモートスイッチの両方を含む）が明示的に削除されるか、またはモードを基本モードに戻す前にすべてのデバイスエイリアスメンバーが対応する pWWN に置き換えられる必要があります。

デバイスエイリアスモード配信

デバイスエイリアス配信が有効になっていると、モードの変更があった場合は常に、デバイスエイリアスがネットワーク内の他のスイッチに配信されます。

デバイスエイリアス差分限定配信

Cisco MDS NX-OS リリース 7.3(0)D1(1) 以降、Cisco MDS スイッチではデバイスエイリアス差分限定配信機能がサポートされています。

この機能がファブリック内のすべてのスイッチで有効な場合は、ファブリック内でデータベース全体ではなくセッションコマンドだけが送信されます。これにより、拡張性が向上します。

ファブリック内のすべてのスイッチでデバイスエイリアス差分限定配信機能が有効な場合、DDAS では 20,000 エントリに対応できます。この機能は、デフォルトでイネーブルにされています。



Note ファブリック内のすべてのスイッチで Cisco MDS NX-OS リリース 7.3(0)D1(1) 以上が稼働しており、デバイスエイリアス差分限定配信機能が有効であることを確認してください。

デバイスエイリアス差分限定配信の設定

デバイスエイリアス差分限定配信機能を設定するには、次の手順を実行します。

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **device-alias distribute diffs-only**

スイッチで差分限定配信を有効にします。

次に、スイッチでデバイスエイリアス差分限定配信機能を有効にし、この機能のステータスを表示する例を示します。

Example:

```
switch(config)# device-alias distribute diffs-only
switch(config)# show device-alias status
Fabric Distribution: Enabled
Diffs-only Distribution: Enabled
Database:- Device Aliases 1 Mode: Basic
Checksum: 0x43a9fe35852e91354543d712c3ec9d3
```

デバイスエイリアス差分限定配信ステータスの表示

次に、ファブリックとスイッチでデバイスエイリアス差分限定配信機能が有効である場合に、アクティブセッション中のデバイスエイリアスのステータスを表示する例を示します。

Example:

```
switch(config-device-alias-db)# show device-alias status
Fabric Distribution: Enabled
Diffs-only Distribution: Disabled
Database:- Device Aliases 0 Mode: Basic
Checksum: 0xf6bd6b3389b87233d462029172c8612
Locked By:- User "CLI/SNMPv3:admin" SWWN 20:00:54:7f:ee:1c:2d:40
Pending Database:- Device Aliases 1 Mode: Basic
Diffs-only Distribution capability in the fabric: Enabled

Diffs-only distribution in Session: Enabled
```

次に、ファブリックとスイッチでデバイスエイリアス差分限定配信機能が無効である場合に、アクティブセッション中のデバイスエイリアスのステータスを表示する例を示します。

Example:

```
switch(config-device-alias-db)# show device-alias status
Fabric Distribution: Enabled
Diffs-only Distribution: Disabled
Database:- Device Aliases 0 Mode: Basic
Checksum: 0xf6bd6b3389b87233d462029172c8612
Locked By:- User "CLI/SNMPv3:admin" SWWN 20:00:54:7f:ee:1c:2d:40
Pending Database:- Device Aliases 1 Mode: Basic
Diffs-only Distribution capability in the fabric: Disabled
SWWN which doesnot support Diffs-only Distribution:
20:00:54:7f:ee:1c:2d:40
20:00:54:7f:e1:1c:2c:40
Diffs-only distribution in Session: Disabled
```

Note セッション中は、*Diffs-only distribution in session* のステータスは変化しません。

ステップ 3 switch(config)# no device-alias distribute diffs-only

デバイスエイリアス差分限定配信を無効にします。

次に、スイッチでデバイスエイリアス差分限定配信機能を無効にし、この機能のステータスを表示する例を示します。

Example:

```
switch(config)# no device-alias distribute diffs-only
switch(config)# show device-alias status
Fabric Distribution: Enabled
Diffs-only Distribution: Disabled
Database:- Device Aliases 1 Mode: Basic
Checksum: 0x43a9fe35852e91354543d712c3ec9d3
```

差分限定配信機能が有効なデバイス エイリアスのマージ

次の状況では、デバイスエイリアスのマージが失敗します。

- 12,000 を超えるエントリが設定されており、デバイスエイリアス差分限定配信機能が有効なスイッチを、この機能をサポートしていないファブリックに追加する場合。
- デバイスエイリアス差分限定配信機能が無効なスイッチを、12,000 を超えるエントリが設定されており、デバイスエイリアス差分限定配信機能が有効なファブリックに追加する場合。

マージ失敗の表示

次に、ファブリックの1つで12,000を超えるエントリがサポートされていない場合にデバイスエイリアスのマージに失敗する例を示します。

```
switch(config)# show cfs merge status name device-alias
Physical-fc Merge Status: Failed [ Wed Jan 20 10:00:34 2016 ]
Failure Reason: One of the merging fabrics cannot support more than 12Kdevice-aliases
```



Note 12,000 を超えるデバイスエイリアスエントリをサポートするには、ファブリック内のすべてのスイッチで差分限定配信機能を有効にする必要があります。ファブリック内のすべてのスイッチで差分限定配信機能が有効になっていない場合は、12,000 を超えるエントリを設定しないことを推奨します。

さまざまなモードのデバイスエイリアスのマージ

2つのファブリックが異なるデバイスエイリアスモードで稼働している場合は、デバイスエイリアスのマージが失敗します。マージプロセス中に、モードの自動変換は発生しません。この問題は解決する必要があります。

アプリケーションレベルでは、マージはアプリケーションとファブリックの間で行われます。たとえば、ゾーンマージはEポートが稼働しているときに発生し、IVR、PSM/DPVMマージはCFSが原因で発生します。このマージは、デバイスエイリアスマージに全面的に依存するわけではありません。

拡張ファブリックで実行されているアプリケーションに、ネイティブデバイスエイリアス設定がある場合は、他のファブリックがネイティブデバイスエイリアススペースの設定をサポートできるが、基本モードで実行されている場合でも、アプリケーションはマージに失敗します。この問題は解決する必要があります。デバイスエイリアスマージの問題が解決されたら、各アプリケーションをそれに応じて修正する必要があります。

同じファブリック内にある複数のスイッチでデバイスエイリアスデータベースの不一致がある場合、次の問題が発生します。

pWWNに関連付けられているデバイスエイリアスのメンバーがスイッチに存在しない場合でも、そのデバイスエイリアスがポートセキュリティ/DPVMデータベースに含まれている。pWWNに関連付けられているデバイスエイリアスのメンバーがスイッチに存在している場合でも、そのデバイスエイリアスがポートセキュリティ/DPVMデータベースに含まれていない。

マージ失敗およびデバイスエイリアスモード不一致の解決

2つのファブリックが異なるモードで実行され、デバイスエイリアスマージがファブリック間で失敗する場合、1つのモードまたはもう1つのモードを選択することにより、矛盾を解決できます。そうでない場合には、拡張モードを有効にできません。基本モードを選択した場合、

拡張ファブリック上で実行されているアプリケーションはデバイス エイリアス マージに準拠している必要があります。

ネイティブのデバイスエイリアス設定がない場合、アプリケーションマージは成功しますが、モードの不一致のため、デバイス エイリアス マージは失敗します。



Note デバイスエイリアスが特定のスイッチ上で基本モードで実行されている場合、アプリケーションは SNMP 経由のネイティブのデバイス エイリアス設定を受け付けられないようにする必要があります。



Note 拡張モードが有効になると Confcheck が追加され、拡張モードが無効になると Confcheck は削除されます。ネイティブ フォーマットのデバイス エイリアス設定がある場合、アプリケーションは confcheck を追加し、設定の削除後に confcheck を削除する必要があります。

デバイス エイリアスの機能

デバイス エイリアスには、次のような特徴があります。

- デバイス エイリアスの情報は、VSAN 設定に依存しません。
- デバイス エイリアス設定および配信は、ゾーン サーバーおよびゾーン サーバー データベースとは無関係です。
- データを失うことなく、従来のゾーン エイリアス設定をインポートできます。
- デバイス エイリアス アプリケーションは Cisco Fabric Services (CFS) インフラストラクチャを使用して、効率的なデータベースの管理および配布を実現します。デバイス エイリアスでは調整済み配信モードが使用され、配信範囲はファブリック全体に及びます（『Cisco MDS 9000 Family NX-OS System Management Configuration Guide』を参照）。
- デバイス エイリアスを使用してゾーン、IVR ゾーン、または QoS 機能を設定した場合に、これらの設定を表示すると、自動的にそれぞれの pWWN とともにデバイス エイリアスが表示されます。

デバイス エイリアスの前提条件

デバイス エイリアスには、次の要件があります。

- デバイス エイリアスを割り当てることができるのは pWWN だけです。
- pWWN とそれがマッピングされるデバイス エイリアスとの間のマッピングは、1 対 1 の関係になる必要があります。pWWN は 1 つのデバイス エイリアスにだけマッピングでき、デバイス エイリアスは 1 つの pWWN にだけマッピングできます。
- Cisco MDS NX-OS リリース 9.2(2) より前では、デバイス エイリアス名は 64 文字の英数字に制限されていました。Cisco MDS NX-OS リリース 9.2(2) 以降、デバイス エイリアス名

は 63 文字の英数字に制限されています。デバイスエイリアス名には、次の文字を 1 つ以上含めることができます。

- a ~ z および A ~ Z
- 1 ~ 9
- - (ハイフン) および _ (下線)
- \$ (ドル記号) および ^ (キャレット) 記号



Note Cisco MDS NX-OS リリース 9.2(2) より前のリリースでは、デバイスエイリアス名の長さが 64 文字の場合、DPVM とその他のアプリケーションデータベースが適切に更新されません。デバイスエイリアス名の長さを 63 文字に制限してください。

ゾーンエイリアスとデバイスエイリアスの比較

Table 14: [ゾーンエイリアスとデバイスエイリアスの比較, on page 178](#) に、ゾーンベースのエイリアス設定とデバイスエイリアス設定の違いを示します。

Table 14: ゾーンエイリアスとデバイスエイリアスの比較

ゾーンベースのエイリアス	デバイスエイリアス
エイリアスは指定した VSAN に限定されます。	VSAN 番号を指定せずにデバイスエイリアスを定義できます。また、同一の定義を何の制約もなく 1 つまたは複数の VSAN で使用できます。
ゾーンエイリアスは、ゾーン分割設定の一部です。他の機能の設定にはエイリアスマッピングを使用できません。	pWWN を使用するすべての機能にデバイスエイリアスを使用できます。
エンドデバイスを指定するのにすべてのゾーンメンバタイプを使用できます。	pWWN は、IP アドレスなどの新しいデバイスエイリアスと使用するときだけサポートされます。
設定はゾーンサーバーデータベースに格納されていて、他の機能には使用できません。	デバイスエイリアスは、ゾーン分割に限定されていません。デバイスエイリアスの設定は、FCNS、ゾーン、fcping、traceroute、および IVR アプリケーションに使用できます。
show zoneset active、show flogi database、show fcns database などの show コマンドの出力には、FC エイリアスは関連付けられている WWN と共に表示されません。	show zoneset active、show flogi database、show fcns database などの show コマンドの出力には、デバイスエイリアスは関連付けられている WWN と共に表示されます。

ゾーンベースのエイリアス	デバイスエイリアス
FC エイリアスはアクティブ ゾーンセットの一部として配信されず、FC 標準に基づき完全なゾーンデータベースの一部としてのみ配信されます。	デバイスエイリアスは CFS を介して配信されます。

デバイスエイリアス データベース

デバイスエイリアス機能は2つのデータベースを使用して、デバイスエイリアス設定を受け入れ、実装します。

- 有効なデータベース：ファブリックが現在使用しているデータベース
- 保留中のデータベース：保留中のデバイスエイリアス設定の変更は保留中のデータベースに保存されます。

デバイスエイリアス設定を変更する場合、変更している間はファブリックがロックされたままの状態なので、変更をコミットまたは廃棄する必要があります。

ここでは、次の内容について説明します。

デバイスエイリアスの作成

保留データベースにデバイスエイリアスを作成する手順は、次のとおりです。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **device-alias database**

```
switch(config-device-alias-db)#
```

保留データベース 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-device-alias-db)# **device-alias name Device1 pwwn 21:01:00:e0:8b:2e:80:93**

pWWN によって識別されるデバイスのデバイス名 (Device1) を指定します。これが最初に入力されたデバイスエイリアス コンフィギュレーション コマンドであるため、保留データベースへの書き込みを開始し、同時にファブリックをロックします。

ステップ 4 switch(config-device-alias-db)# **no device-alias name Device1**

pWWN によって識別されるデバイスのデバイス名 (Device1) を削除します。

ステップ 5 switch(config-device-alias-db)# **device-alias rename Device1 Device2**

既存のデバイスエイリアス (Device1) を新しい名前 (Device2) に変更します。

デバイスエイリアス設定を表示するには、**show device-alias name** コマンドを使用します。

```
switch# show device-alias name x
device-alias name x pwnn 21:01:00:e0:8b:2e:80:93
```

デバイスエイリアスの配布について

デフォルトでは、デバイスエイリアスの配布はイネーブルになっています。デバイスエイリアス機能は、調整済み配信メカニズムを使用して、変更をファブリック内のすべてのスイッチに配信します。

変更をコミットしていない状態で配布をディセーブルにすると、コミット作業は失敗します。

失敗ステータスの表示

```
switch# show
  device-alias status
Fabric Distribution: Disabled
Database:- Device Aliases 25
Status of the last CFS operation issued from this switch:
=====
Operation: Commit
Status: Failed (Reason: Operation is not permitted as the fabric distribution is
currently disabled.)
```



Note Cisco MDS NX-OS Release 6.2.9 以降では、write erase コマンドを使用しない場合、DDAS (分散デバイスエイリアス サービス) の ASCII 設定の再生に長い時間がかかります。

デバイスエイリアスの作成の概要

最初のデバイスエイリアスタスクを実行すると、どのデバイスエイリアスタスクであるかに関係なく、デバイスエイリアス機能に対してファブリックが自動的にロックされます。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。
- 有効なデータベースのコピーが取得され、保留データベースとして使用されます。この時点からの変更は、保留データベースに対して行われます。保留データベースへの変更をコミットするかまたは破棄 (**abort**) するまで、保留データベースは有効のままです。

デバイスエイリアス設定のベストプラクティスの概要

デバイスエイリアス設定のベストプラクティスの一部として、デバイスエイリアスセッションでは次のガイドラインを取り入れる必要があります。

rename コマンドの設定時にデバイスエイリアス名を再利用する場合、コマンドが失敗し、拒否リストに移動されます。

拒否された **device-alias** コマンドの表示

```
switch(config-device-alias-db)# device-alias name dev10 pwwn 10:10:10:10:10:10:10:10
switch(config-device-alias-db)# device-alias rename dev10 new-dev10
Command rejected. Device-alias reused in current session :dev10
Please use 'show device-alias session rejected' to display the rejected set of commands
and for the device-alias best-practices recommendation.
switch(config-device-alias-db)#
```

add または **delete** コマンドの設定時に PWWN を再利用する場合、コマンドが失敗し、拒否リストに移動されます。

拒否された **device-alias** コマンドの表示

```
switch(config-device-alias-db)# device-alias name dev11 pwwn 11:11:11:11:11:11:11:11
switch(config-device-alias-db)# no device-alias name dev11
Command rejected. Pwwn reused in current session: 11:11:11:11:11:11:11:11 is mapped to
device-alias dev11
Please use 'show device-alias session rejected' to display the rejected set of commands
and for the device-alias best-practices recommendation.
switch(config-device-alias-db)#
```

以前に **rename** コマンドで名前が変更されたデバイスエイリアス名を **add** コマンドで再利用する場合、コマンドが失敗し、拒否リストに移動されます。

```
switch(config-device-alias-db)# device-alias rename da3 new-da3
switch(config-device-alias-db)# device-alias name da3 pwwn 2:2:2:2:3:3:3:3
Command rejected. Device-alias name reused in current session: da3
Please use 'show device-alias session rejected' to display the rejected set of commands
and for the device-alias best-practices recommendation.
switch(config-device-alias-db)#
```

拒否された **device-alias** コマンドの表示

拒否されたコマンドのセットを表示するには、**show device-alias session rejected** コマンドを使用します。

```
switch(config-device-alias-db)# show device-alias session rejected
To avoid command rejections, within a device alias session
Do not reuse:
a) a device alias name while configuring a rename command
b) a PWWN while configuring an add or delete command
c) a device alias name already renamed while configuring add command

Rejected commands must be committed in a separate device alias session
which may cause traffic interruption for those devices. Plan accordingly.
Refer to this command in the NX-OS Command Reference Guide
for more information about device alias configuration best practices

Rejected Command List
-----
device-alias rename dev10 new-dev10
no device-alias name dev11
```

```
device-alias name da3 pwnn 02:02:02:02:03:03:03:03
switch(config-device-alias-db)# #
```

変更のコミット

保留中のデータベースに行われた変更内容をコミットした場合、次のイベントが発生します。

1. 有効データベースの内容が、保留データベースの内容で上書きされます。
2. 保留中のデータベースの内容が空になります。
3. ファブリック ロックがこの機能に対して解除されます。

変更をコミットするには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **device-alias commit**

現在アクティブなセッションに対する変更をコミットします。

ファブリック内のスイッチがロックされ、ブランク コミットになるたびに、次の警告が表示されます。

```
WARNING: Device-alias DB is empty in this switch.
Initiating a commit from this switch will clear [wipe out] Device-alias DB across all the
switches in the fabric, losing Device-alias full DB config permanently.
Do you want to continue? (y/n) [n]
```

Note **device-alias commit** の完了後、デバイス エイリアス配信に参加しているすべてのスイッチで実行コンフィギュレーションが変更されます。その後、**copy running-config startup-config fabric** コマンドを使用して、ファブリック内のすべてのスイッチで **running-config** を **startup-config** に保存できます。

ステップ 3 switch(config)# **device-alias commit force**

現在のアクティブセッションに対して、変更を強制的にコミットし、変更を上書きします。

デバイス エイリアスの保留中差分表示の有効化

device-alias commit 実行時の保留中差分の表示とその後の確認を有効にするには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ2 switch(config)# device-alias confirm-commit

デバイスエイリアスの confirm commit オプションを有効にします。

ステップ3 switch(config)# device-alias commit

```
The following device-alias changes are about to be committed
+ device-alias name Device1 pwnn 21:01:00:e0:8b:2e:80:93
Do you want to continue? (y/n) [n] y
```

device-alias confirm-commit コマンドが有効な場合、保留中のデータベースがコミットされると、コンソールに保留中差分が表示され、ユーザーに対し [Yes] または [No] を選択するよう求めるプロンプトが表示されます。device-alias confirm-commit コマンドが無効な場合は、保留中差分は表示されず、ユーザーに対して [Yes] または [No] の選択は求められません。

変更の破棄

保留中のデータベースで行われた変更内容を廃棄した場合、次のイベントが発生します。

1. 有効なデータベースの内容は影響を受けません。
2. 保留中のデータベースの内容が空になります。
3. ファブリック ロックがこの機能に対して解除されます。

デバイスエイリアスセッションを廃棄する手順は、次のとおりです。

ステップ1 switch# config terminal

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ2 switch(config)# device-alias abort

現在アクティブなセッションを廃棄します。

廃棄操作のステータスを表示するには、show device alias status コマンドを使用します。

```
switch# show
device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
=====
Operation: Abort
Status: Success
```

ファブリックのロックの上書き

ユーザーがデバイスエイリアス作業を行ったが、変更のコミットや廃棄を行ってロックを解除するのを忘れていた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザーによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。



Tip 変更は `volatile` ディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

デバイスエイリアスセッションをクリアするには、CONFIGURATION モードで `clear device-alias session` コマンドを使用します。

```
switch(config)# clear device-alias session
```

クリア操作のステータスを確認するには、`show device-alias session status` コマンドを使用します。

```
switch(config)# show device-alias session status
Last Action Time Stamp      : None
Last Action                 : None
Last Action Result         : None
Last Action Failure Reason : none
```

データベースの内容のクリア

すべてのデータベースの内容をクリアするには、CONFIGURATION モードで `clear device-alias database` コマンドを使用します。

```
switch(config)# clear device-alias database
To verify the status of the clear device-alias database
command, use the show device-alias database
command.
switch(config)# show device-alias database
```

統計情報のクリア

すべての統計情報をクリアするには、CONFIGURATION モードで `clear device-alias statistics` コマンドを使用します。

```
switch# clear device-alias statistics
```

デバイス エイリアスの配布のディセーブル化とイネーブル化

デバイスエイリアスの配布をディセーブルまたはイネーブルにする手順は、次のとおりです。

ステップ 1 switch# **config t**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **no device-alias distribute**

配布をディセーブルにします。

ステップ 3 switch(config)# **device-alias distribute**

配布をイネーブルにします (デフォルト)。

デバイスエイリアス配信のステータスを表示するには、**show device-alias status** コマンドを使用します (次の例を参照)。

配信が有効な場合のデバイス エイリアス ステータスの表示

配信がディセーブルの場合のデバイス エイリアス ステータスの表示

```
switch# show
device-alias status
Fabric Distribution: Enabled <-----Distribution is enabled
Database:-Device Aliases 24
Locked By:-User "Test" SWWN 20:00:00:0c:cf:f4:02:83<-Lock holder's user name and switch
ID
Pending Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
=====
Operation: Enable Fabric Distribution
Status: Success
```

```
switch# show
device-alias status
Fabric Distribution: Disabled
Database:- Device Aliases 24
Status of the last CFS operation issued from this switch:
=====
Operation: Disable Fabric Distribution
Status: Success
```

レガシー ゾーン エイリアス設定の変換の概要

次の制約事項を満たす場合、レガシー ゾーンエイリアス設定をインポートし、データを失うことなくこの機能を使用できます。

- 各ゾーンエイリアスには、メンバが1つだけあります。
- メンバのタイプはpWWNです。

- ゾーンエイリアスの名前および定義は、既存のデバイスエイリアス名のものと同じであってはならない。

名前の競合がある場合、ゾーンエイリアスはインポートされません。



Tip ご使用の設定の要件に応じて、必要なゾーンエイリアスをデバイスエイリアスデータベースにコピーしてください。

インポート操作が終了し、**commit** 操作を行うと、変更されたエイリアスデータベースが物理ファブリック内のほかのすべてのスイッチに配布されます。この時点で、ファブリック内の他のスイッチに設定を配信する必要がない場合は、**abort** 処理を実行して、マージ変更内容をすべて破棄できます。

このセクションは、次のトピックで構成されています。

ゾーンエイリアスのインポート



Note デバイスエイリアスでは、同じセッションでデバイスエイリアスエントリをデータベースにインポートして手動で追加することはできません。

特定の VSAN のゾーンエイリアスをインポートするには、次の手順を実行します。

SUMMARY STEPS

1. switch# **config t**
2. switch(config)# **device-alias import fcalias vsan 3**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# config t Example: switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# device-alias import fcalias vsan 3	指定された VSAN の fcalias 情報をインポートします。 ゾーンセットのデバイスエイリアス情報を表示するには、 show zoneset コマンドを使用します（次の例を参照）。

ゾーンセット情報のデバイスエイリアスの表示

```
switch# show zoneset
zoneset name s1 vsan 1
zone name z1 vsan 1
  pwnn 21:01:00:e0:8b:2e:80:93 [x] <-----Device alias displayed for each
pWNN.
  pwnn 21:00:00:20:37:39:ab:5f [y]
zone name z2 vsan 1
  pwnn 21:00:00:e0:8b:0b:66:56 [SampleName]
  pwnn 21:00:00:20:37:39:ac:0d [z]
```

例：アクティブゾーンセットのデバイスエイリアスの表示

```
switch# show zoneset active
zoneset name s1 vsan 1
zone name z1 vsan 1
  * fcid 0x670100 [pwnn 21:01:00:e0:8b:2e:80:93] [x]
  pwnn 21:00:00:20:37:39:ab:5f [y]
zone name z2 vsan 1
  * fcid 0x670200 [pwnn 21:00:00:e0:8b:0b:66:56] [SampleName]
  pwnn 21:00:00:20:37:39:ac:0d [z]
```

デバイスエイリアス統計情報のクリア

(デバッグ目的で) デバイスエイリアス統計情報をクリアするには、**clear device-name statistics** コマンドを使用します。

```
switch# clear device-alias statistics
```

データベース マージの注意事項

CFS マージのサポートの詳細については、『Cisco MDS 9000 シリーズ NX-OS システム管理構成ガイド』を参照してください。

2つのデバイスエイリアスデータベースを結合する場合は、次の注意事項に従ってください。

- 名前が異なる2つのデバイスエイリアスが同一のpWWNにマッピングされていないことを確認します。
- 異なる2つのpWWNが同一のデバイスエイリアスにマッピングされていないことを確認します。
- マージ対象の両方のファブリックで類似のデバイスエイリアスモードであることを確認します。

デバイスエイリアス設定の確認

デバイスエイリアス情報を表示するには、**show device-alias** コマンドを使用します。次の例を参照してください。

有効なデータベースの設定されているすべてのデバイスエイリアスの表示

```
switch# show
device-alias database
device-alias name SampleName pwnn 21:00:00:e0:8b:0b:66:56
device-alias name x pwnn 21:01:00:e0:8b:2e:80:93
Total number of entries = 2
```

変更のない保留中のデータベースの表示

```
switch# show
device-alias database pending
There are no pending changes
```

変更された保留中のデータベースの表示

```
switch# show
device-alias database pending
device-alias name x pwnn 21:01:00:e0:8b:2e:80:93
device-alias name SampleName pwnn 21:00:00:e0:8b:0b:66:56
device-alias name y pwnn 21:00:00:20:37:39:ab:5f
device-alias name z pwnn 21:00:00:20:37:39:ac:0d
Total number of entries = 4
```

保留中のデータベースの指定されたデバイス名の表示

```
switch# show
device-alias name x pending
device-alias name x pwnn 21:01:00:e0:8b:2e:80:93
```

保留中のデータベースの指定されたpWWNの表示

```
switch# show
device-alias pwnn 21:01:00:e0:8b:2e:80:93 pending
device-alias name x pwnn 21:01:00:e0:8b:2e:80:93
```

保留中のデータベースと有効なデータベースの差異の表示

```
switch# show
device-alias database pending-diff
- device-alias name Doc pwnn 21:01:02:03:00:01:01:01
+ device-alias name SampleName pwnn 21:00:00:e0:8b:0b:66:56
```

指定された pWWN の表示

```
switch# show
device-alias pwwn 21:01:01:01:01:11:01:01
device-alias name Doc pwwn 21:01:01:01:01:11:01:01
```

FLOGI データベースのデバイスエイリアスの表示

```
switch# show flogi database
-----
INTERFACE  VSAN    FCID          PORT NAME          NODE NAME
-----
fc2/9      1       0x670100     21:01:00:e0:8b:2e:80:93  20:01:00:e0:8b:2e:80:93
                                     [x
] <-----Device alias name
fc2/12     1       0x670200     21:00:00:e0:8b:0b:66:56  20:00:00:e0:8b:0b:66:56
                                     [SampleName
] <-----Device alias name
Total number of flogi = 2
```

FCNS データベースのデバイスエイリアスの表示

```
switch# show fcns database
VSAN 1:
-----
FCID        TYPE  PWWN          (VENDOR)          FC4-TYPE:FEATURE
-----
0x670100    N     21:01:00:e0:8b:2e:80:93 (Qlogic)          scsi-fcp:init
                                     [x
]
0x670200    N     21:00:00:e0:8b:0b:66:56 (Qlogic)          scsi-fcp:init
                                     [SampleName
]
Total number of entries = 2
```

指定デバイスエイリアスの fcping 統計情報の表示

```
switch# fcping device-alias x vsan 1
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 358 usec
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 226 usec
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 372 usec
```

指定デバイスエイリアスの fctrace 情報の表示

```
switch# fctrace device-alias x vsan 1
Route present for : 21:01:00:e0:8b:2e:80:93
20:00:00:05:30:00:4a:e2(0xfffc67)
```

デバイスエイリアスは、使用可能な場合、**device-alias** コマンドまたはゾーン固有の **member pwwn** コマンドを使用して設定されるメンバに関係なく表示されます。

デバイスエイリアスアプリケーションの統計情報の表示

```
switch# show
```

```

device-alias statistics
    Device Alias Statistics
=====
Lock requests sent: 2
Database update requests sent: 1
Unlock requests sent: 1
Lock requests received: 1
Database update requests received: 1
Unlock requests received: 1
Lock rejects sent: 0
Database update rejects sent: 0
Unlock rejects sent: 0
Lock rejects received: 0
Database update rejects received: 0
Unlock rejects received: 0
Merge requests received: 0
Merge request rejects sent: 0
Merge responses received: 2
Merge response rejects sent: 0
Activation requests received: 0
Activation request rejects sent: 0
Activation requests sent: 2
Activation request rejects received: 0

```

デフォルト設定

Table 15: デフォルトのデバイスエイリアスパラメータ, on page 190 に、デバイスエイリアスパラメータのデフォルト設定値を示します。

Table 15: デフォルトのデバイスエイリアスパラメータ

パラメータ	デフォルト
使用中のデータベース	有効なデータベース
変更を受け入れるデータベース	保留中のデータベース
デバイスエイリアスファブリックロックの状態	最初のデバイスエイリアス作業でロックされる

デバイスエイリアスのマージ失敗の解決

データベースをマージする際に発生する最も一般的な問題は、デバイスエイリアスのマージの失敗です。デバイスエイリアスのマージに失敗する場合は、問題を特定するために、マージが開始されたスイッチの Syslog メッセージを確認することをお勧めします。各ファブリック内のマージを処理したアプリケーションサーバーでは、このメッセージに「Merge Master」の用語が表示されます。

この例では、Syslog メッセージに、データベースの不一致の結果としてマージに失敗したことが示されています。

```
2007 Apr 9 15:52:42 switch-1 %CFS-3-MERGE_FAILED: Merge failed for app device-alias,
local switch wwn 20:00:00:0d:ec:2f:c1:40, ip 172.20.150.38, remote switch wwn
20:00:00:0d:ec:04:99:40, ip 172.20.150.30
2007 Apr 9 15:52:42 switch-1 %DEVICE-ALIAS-3-MERGE_FAILED: Databases could not be merged
due to mismatch.
```



- (注) デバイスエイリアスデータベースのマージまたは再マージを開始するには、**device-alias distribute** コマンドを使用します。スイッチのデバイスエイリアスデータベースをファブリック内の他のすべてのスイッチにプッシュするには、**device-alias commit** コマンドを使用します。スイッチのデバイスエイリアスデータベースがマージされていない (**show cfs merge status name device-alias** コマンドの出力に複数の「Merge Master」が表示されている) 場合、**device-alias commit** コマンドを実行すると、マージされていないデバイスエイリアスデータベースが上書きされます。

Cisco MDS NX-OS リリース 9.2(2) より前のバージョンの NX-OS を実行している MDS スイッチを、リリース 9.2(2) を実行している MDS スイッチに接続すると、デバイスエイリアスとゾーンのマージエラーが発生する場合があります。スイッチ 1 が Cisco MDS NX-OS リリース 9.2(2) 以降のリリースを実行し、スイッチ 2 が Cisco MDS NX-OS リリース 9.2(2) より前のリリースを実行している 2 つのスイッチについて考えてみます。両方のスイッチがデバイスエイリアス拡張モードになっています。スイッチ 2 には、64 文字の英数字で構成された 1 つ以上のデバイスエイリアス名があります。スイッチ 2 が 64 文字の英数字を使用して構成されたデバイスエイリアス名を使用しているため、ゾーンとデバイスエイリアスの両方のマージがスイッチ 1 とスイッチ 2 の間で失敗します。このような場合、64 文字の英数字で構成されているすべてのデバイスエイリアス名を、63 文字以下の英数字に再構成することが推奨されます。それが完了したら、**no device-alias distribute** コマンドに続けて **device-alias distribute** コマンドを使用して、デバイスエイリアスデータベースを再マージする必要があります。次に、ゾーンセットを再マージし、VSAN を ISL から削除し、ISL を再読み込みするか、ISL をシャットダウンして、単一の VSAN のみを転送している場合は再び起動することにより、VSAN を ISL で分離から外すことができます。

デバイスエイリアスのベストプラクティス

ここでは、デバイスエイリアスを作成して使用するときに実行する必要があるベストプラクティスを示します。

- 可能な場合はいつでも、デバイスエイリアスを使用してワールドワイドネーム (WWN) の管理を簡素化する必要があります。WWN ではなくエイリアスを使用してデバイスを識別する方が簡単です。そのため、WWN を簡単に識別するには、エイリアスを WWN に割り当てる必要があります。
- デバイスエイリアス名は大文字と小文字が区別されます。
- 可能なかぎり、デバイスエイリアスは拡張モードで操作してください。拡張モードでは、アプリケーションは、エイリアスをポートワールドワイドネーム (pWWN) に拡張せずに、ネイティブ形式のデバイスエイリアス名を受け入れます。ゾーンサーバー、VSAN

間ルーティング (IVR)、Port Security Manager (PSM)、ダイナミックポート VSAN メンバーシップなどのアプリケーションは、デバイスエイリアスメンバーシップの変更を自動的に追跡して適用するため、変更は 1 ヶ所で行うことができます。



(注) 相互運用モードの VSAN は拡張モード設定を受け入れません。

- デバイスエイリアス設定を事前にプランニングし、一貫した命名規則を実装します。
- すべてのデバイスエイリアス設定の文書化されたバックアップを保持します。
- マージの失敗の解決を試みる前に、マージ後の最終的なデバイスエイリアスデータベースがどのようなものになるかをプランニングします。これにより、誤ってデバイスエイリアスエントリが上書きされてトラフィックが中断することを回避できます。



注意 Cisco Fabric Services (CFS) のマージの失敗を解決するためにブランクコミットを実行しないでください。ブランクコミットでは、すべてのスイッチのデバイスエイリアスデータベースが、ローカルスイッチのデバイスエイリアスデータベースで上書きされます。



(注) ブランクコミットは、変更がない (モード変更を含む) 場合またはリモートスイッチのデバイスエイリアスデータベースがローカルスイッチのデバイスエイリアスデータベースで上書きされても問題がない場合に使用されるデバイスエイリアスコミットです。

次の理由により、デバイスエイリアスの不一致が発生する場合があります。

- デバイスエイリアス名の重複：デバイスエイリアス名は同じでも pWWN が異なります。このようなシナリオでは、**show device-alias merge status** コマンドによりマージの失敗の理由が「Reason: Another device-alias already present with the same name」と表示されます。
- pWWN の重複：デバイスエイリアス名は異なっているのに pWWN が同じです。このようなシナリオでは、**show device-alias merge status** コマンドによりマージの失敗の理由が「Reason: Another device-alias already present with the same pwwn」と表示されます。



(注) デバイスエイリアスの変更が適用されるたびに、更新されたすべてのスイッチで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する必要があります。ファブリック内のすべてのスイッチについて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するには、**copy running-config startup-config fabric** コマンドを使用します。デバイスエイリアスの変更が適用された後に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ない場合、スイッチがリロードするかスイッチの電源が切れて再起動すると、スタートアップコンフィギュレーションに正しいデバイスエイリアスデータベースがないために、マージに失敗します。

- 64文字の英数字を使用してデバイスエイリアス名を構成している場合、Cisco MDS NX-OS リリース 9.2(2) 以降のリリースにアップグレードすることはできません。詳細については、『[Cisco MDS 9000 NX-OS ソフトウェアアップグレードおよびダウングレードガイド、リリース 9.x](#)』を参照してください。

デバイスエイリアスの不一致の解決

既存のデバイスエイリアスデータベースを持つスイッチを既存のファブリックに追加しようとすると、次の理由により、競合が発生する場合があります。

- 同じデバイスエイリアス名が使用されているのに、pWWN が異なっている。
- 同じ pWWN が使用されているのに、デバイスエイリアス名が異なっている。

デバイスエイリアス名の重複を解決するには、次の手順を実行します。

ステップ 1 **show cfs merge status name device-alias** コマンドを実行して CFS またはデバイスエイリアス マージ失敗の Syslog を調べて、マージが失敗したことを確認します。

```
switch-1# show cfs merge status name device-alias

Physical-fc Merge Status: Failed
[Sun Sep 25 14:45:55 2016]
Failure Reason: Another device-alias already present with the same pwn

Local Fabric
-----
Switch WWN                IP Address
-----
20:00:54:7f:ee:1b:0e:b0  10.127.103.211    [Merge Master] <<< Merge Master#1
                        [switch-1]

Total number of switches = 1
```

```

Remote Fabric
-----
Switch WWN                IP Address
-----
20:00:54:7f:ee:1b:0e:50  10.197.111.54          [Merge Master] <<< Merge Master#2

Total number of switches = 1

```

(注) 適切にマージされたデバイスエイリアスアプリケーションでは、「Merge Master」が1つだけ表示されます。上記の例のように複数の「Merge Master」がある場合は、デバイスエイリアスデータベースがマージされていないことを示しています。

ステップ2 デバイスエイリアスの配布を無効にするために、マージが失敗したスイッチで **no device-alias distribute** コマンドを使用します。

```

switch-1# configure terminal
switch-1(config)# no device-alias distribute

```

ステップ3 スイッチでマージの失敗を解決します。[マージ失敗の解決 \(194 ページ\)](#) を参照してください。

マージ失敗の解決

ここでは、マージの失敗を解決する方法に関する情報を提供します。

重複するデバイスエイリアス名（デバイスエイリアス名は同じでも pWWN が異なる）の解決



(注) 同じデバイスエイリアス名が異なる pWWN を指すために使用されている場合、デバイスエイリアス名は重複していると見なされます。

ファブリックに重複するデバイスエイリアス名が存在するかどうかを確認するには、次の手順を実行します。

ステップ1 **show device-alias merge status** コマンドを実行して、マージが失敗した理由がデータベースの不一致であるかどうかを確認します。

```

switch# show device-alias merge status
Result: Failure
Reason: Another device-alias already present with the same name

```

(注) 適切にマージされたデバイスエイリアスアプリケーションでは、「Merge Master」が1つだけ表示されます。上記の例のように複数の「Merge Master」がある場合は、デバイスエイリアスデータベースがマージされていないことを示しています。

ステップ2 CFS またはデバイスエイリアス マージ失敗の Syslog を調べて、マージが失敗したことを確認します。または、**show cfs merge status name device-alias** コマンドを実行して、マージのステータスを確認します。

```
switch# show cfs merge status name device-alias
Physical-fc Merge Status: Failed [ Mon Apr 9 15:57:58 2007 ] <===Merge status
  Local Fabric
-----
Switch WWN                IP Address
-----
20:00:00:0d:ec:2f:c1:40  172.20.150.38      [Merge Master] <<< Merge Master#1
                        switch-1
Total number of switches = 1

  Remote Fabric
-----
Switch WWN                IP Address
-----
20:00:00:0d:ec:04:99:40  172.20.150.30      [Merge Master] <<< Merge Master#2
                        switch-2
Total number of switches = 1
```

ステップ3 スイッチで使用されている Cisco MDS NX-OS のリリースに応じて、次のいずれかのコマンドを実行します。

- Cisco MDS NX-OS リリース 8.1(1) 以降

show device-alias merge conflicts コマンドを実行して、マージ失敗の原因となっているデバイスエイリアスと pWWN を表示します。

(注) Merge Master として示されているスイッチから **show device-alias merge conflicts** コマンドを実行します。

次の例では、同じデバイスエイリアス名 (A1) が2つの異なる pWWN (ローカルスイッチの pWWN とピアスイッチの pWWN) に割り当てられています。

```
switch-1# show device-alias merge conflicts
Merge Status : Failure
Peer Switch SWWN : 20:00:00:0d:ec:24:f5:00
Conflicts :
1. Conflicting Pwwns : 1
-----
Local PWWN      Peer PWWN      Device-alias
-----
pwwn 0:01:01:01:01:01:02  pwwn :01:01:01:01:01:03  A1
```

- Cisco MDS NX-OS リリース 7.3 とそれ以前のリリース

デバイスエイリアスデータベースを手動で比較して、重複するデバイスエイリアス名を特定します。

次の例では、同じデバイスエイリアス名 (A1) が2つの異なる pWWN (ローカルスイッチの pWWN とピアスイッチの pWWN) に割り当てられています。

Merge Master#1 からの結果 :

```
switch-1# show device-alias database
...output trimmed to show only mismatched device-alias
```

重複する pWWN（デバイスエイリアス名が異なっているのに pWWN が同じ）の解決

```
device-alias name A1 pwn 21:01:01:01:01:01:01:02

switch-2# show device-alias database
...output trimmed to show only mismatched device-alias
device-alias name A1 pwn 21:01:01:01:01:01:01:03
```

ステップ 4 `device-alias name name pwn id` コマンドを実行して、一方のスイッチの pWWN をもう一方のスイッチの pWWN と一致するように変更します。

(注) この手順は、**no device-alias distribute** コマンドを実行してデバイスエイリアスの配布を無効にした後に実行してください。

次の例では、switch-1 の pWWN 21:01:01:01:01:01:01:02 が switch-2 の pWWN 21:01:01:01:01:01:01:03 と一致するように変更されます。

```
switch-1# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# device-alias database
switch-1(config-device-alias-db)# no device-alias name A1
switch-1(config-device-alias-db)# show device-alias database | i A1
switch-1(config-device-alias-db)# device-alias name A1 pwn 21:01:01:01:01:01:01:03
switch-1(config-device-alias-db)# show device-alias database | i A1
device-alias name A1 pwn 21:01:01:01:01:01:01:03
```

ステップ 5 重複するデバイスエイリアス名がさらに存在する場合は、手順 [ステップ 3（195 ページ）](#) と手順 [ステップ 4（196 ページ）](#) を実行して、重複デバイスエイリアス名の問題を解決します。

ステップ 6 `device-alias distribute` コマンドを使用して、デバイスエイリアスの配布を有効にしてマージを開始します。

```
switch-1(config)# device-alias distribute
```

ステップ 7 `show cfs merge status name device-alias` コマンドを使用して、マージが成功したかどうかを出力で確認します。

重複する pWWN（デバイスエイリアス名が異なっているのに pWWN が同じ）の解決

同じ pWWN がファブリック内の異なるデバイスエイリアス名にマッピングされていることを確認するには、次の手順を実行します。

ステップ 1 `show device-alias merge status` コマンドを実行して、マージが失敗した理由がデータベースの不一致であるかどうかを確認します。

```
switch# show device-alias merge status
Result: Failure
Reason: Another device-alias already present with the same pwn.
```

(注) 適切にマージされたデバイスエイリアスアプリケーションでは、「Merge Master」が1つだけ表示されます。上記の例のように複数の「Merge Master」がある場合は、デバイスエイリアスデータベースがマージされていないことを示しています。

ステップ 2 CFS またはデバイスエイリアス マージ失敗の Syslog を調べて、マージが失敗したことを確認します。または、**show cfs merge status name device-alias** コマンドを実行して、マージのステータスを確認します。

```
switch# show cfs merge status name device-alias
Physical-fc Merge Status: Failed [ Mon Apr 9 15:57:58 2007 ] <===Merge status
  Local Fabric
-----
Switch WWN                IP Address
-----
20:00:00:0d:ec:2f:c1:40    172.20.150.38      [Merge Master] <<< Merge Master#1
                        switch-1
Total number of switches = 1

  Remote Fabric
-----
Switch WWN                IP Address
-----
20:00:00:0d:ec:04:99:40    172.20.150.30      [Merge Master] <<< Merge Master#2
                        switch-2
Total number of switches = 1
```

ステップ 3 スイッチで使用されている Cisco MDS NX-OS のリリースに応じて、次のいずれかのコマンドを実行します。

- Cisco MDS NX-OS リリース 8.1(1) 以降

show device-alias merge conflicts コマンドを使用して、マージ失敗の原因となっているデバイスエイリアスと pWWN を表示します。 **no device-alias distribute** コマンドを実行し、その後に **device-alias distribute** コマンドを実行して、マージの競合に関する情報を更新します。

(注) Merge Master として示されているスイッチから **show device-alias merge conflicts** コマンドを実行します。

次の例では、pWWN 21:01:01:01:01:01:02 が switch-1 のデバイスエイリアス A3 と switch-2 のデバイスエイリアス A1 にマッピングされています。

```
switch-1# show device-alias merge conflicts
Merge Status : Failure
Peer Switch SWWN : 20:00:00:0d:ec:24:f5:00
Conflicts :
1. Conflicting Device-aliases : 1
-----
Local Device-alias  Peer Device-alias  PWWN
-----
A3  A1  pwwn      21:01:01:01:01:01:02
```

- Cisco MDS NX-OS リリース 7.3 とそれ以前のリリース

デバイスエイリアスデータベースを手動で比較して、マージ失敗の原因となっている pWWN を特定します。

手順 [ステップ 1 \(196 ページ\)](#) でマージが失敗したスイッチで、**show device-alias database** コマンドを使用して、2つの異なるデバイスエイリアス名にマッピングされている pWWN が存在するかどうかを確認します。

この例では、pWWN 21:01:01:01:01:01:02 が switch-1 のデバイス エイリアス A3 と switch-2 のデバイス エイリアス A1 にマッピングされています。

```
switch-1# show device-alias database
device-alias name A3 pwn 21:01:01:01:01:01:02
Total number of entries = 1
```

```
switch-2# show device-alias database
device-alias name A1 pwn 21:01:01:01:01:01:02
```

ステップ 4 **device-alias name name pwn id** コマンドを実行して、一方のスイッチのデバイス エイリアス名をもう一方のスイッチのデバイス エイリアス名と一致するように変更します。

(注) この手順は、**no device-alias distribute** コマンドを実行してデバイス エイリアスの配布を無効にした後に実行してください。

次の例では、switch-1 のデバイス エイリアス名 A3 が switch-2 のデバイス エイリアス名 A1 と一致するように変更されています。

```
switch-1# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# device-alias database
switch-1(config-device-alias-db)# no device-alias name A3
switch-1(config-device-alias-db)# device-alias name A1 pwn 21:01:01:01:01:01:02
```

ステップ 5 重複するデバイス エイリアス名がさらに存在する場合は、手順 [ステップ 3 \(197 ページ\)](#) と手順 [ステップ 4 \(198 ページ\)](#) を実行して、重複デバイス エイリアス名の問題を解決します。

ステップ 6 **device-alias distribute** コマンドを使用して、デバイスエイリアスの配布を有効にしてマージを開始します。

```
switch-1(config)# device-alias distribute
```

ステップ 7 **show cfs merge status name device-alias** コマンドを使用して、マージが成功したかどうかを出力で確認します。

モード不一致の解決

デバイス エイリアス機能は、基本モードまたは拡張モードのいずれかで動作します。2つのファブリックでモードが異なる場合、ファブリック間の CFS マージは失敗します。

2つのファブリックでデバイスエイリアスモードが異なっていることを確認するには、次の手順を実行します。

- ステップ 1** CFS またはデバイスエイリアス マージ失敗の Syslog を調べて、マージが失敗したことを確認します。または、**show cfs merge status name device-alias** コマンドを実行して、マージのステータスを確認します。

```
switch# show cfs merge status name device-alias
Physical-fc Merge Status: Failed [ Mon Apr  9 15:57:58 2007 ] <===Merge status
  Local Fabric
-----
Switch WWN                IP Address
-----
20:00:00:0d:ec:2f:c1:40    172.20.150.38      [Merge Master] <<< Merge Master#1
                        switch-1
Total number of switches = 1
  Remote Fabric
-----
Switch WWN                IP Address
-----
20:00:00:0d:ec:04:99:40    172.20.150.30      [Merge Master] <<< Merge Master#2
                        switch-2
Total number of switches = 1
```

- ステップ 2** **show device-alias merge status** コマンドを使用して、マージが失敗した理由がモードの不一致であることを確認します。モードの不一致がある場合、出力には理由として「Databases could not be merged due to mode mismatch」または「One of the merging fabrics cannot support device-alias Enhanced mode.」と表示されます。

```
switch# show device-alias merge status
Result: Failure
Reason: Databases could not be merged due to mode mismatch.
```

- ステップ 3** **show device-alias status** コマンドを使用して、各ファブリックのデバイスエイリアスモードを確認します。この例では、switch-1 は拡張モードで動作していますが switch-2 は基本モードで動作しています。

```
switch-1# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 2 Mode: Enhanced

switch-2# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 2 Mode: Basic
```

- ステップ 4** デバイスエイリアスモードの不一致が検出されたら、**no device-alias distribute** コマンドを使用して、デバイスエイリアスの配布を無効にします。
- ステップ 5** スイッチで変更するモードに応じて、**device-alias mode enhanced** コマンドを使用して拡張モードに変更するか、**no device-alias mode enhanced** コマンドを使用してスイッチモードを基本モードに変更します。

- (注)
- Cisco MDS NX-OS リリース 8.5(1) より以前では、デフォルトのデバイスエイリアスモードは基本モードでした。Cisco MDS NX-OS リリース 8.5(1) 以降、デフォルトのデバイスエイリアスモードは拡張モードです。
 - デバイスエイリアスモードを拡張から基本に変更する必要があるのにアプリケーションにネイティブ形式のデバイスエイリアス設定が含まれている場合は、すべてのネイティブデバイスエイリアス設定を明示的に削除するか、すべてのデバイスエイリアスメンバーを対応する pWWN で置き換えるまで、デバイスエイリアスモードを変更できません。

ステップ 6 **device-alias distribute** コマンドを使用して、デバイスエイリアスの配布を有効にしてマージを開始します。

検証失敗の解決

デバイスエイリアスのマージが競合なく実行される場合、結果のデバイスエイリアスデータベースは、マージされる両方のファブリックの各スイッチ上の登録されているアプリケーションで検証されます。何らかの理由でアプリケーションがマージされたデータベースの検証に失敗した場合、デバイスエイリアスのマージは失敗します。

アプリケーションの検証の失敗が原因でデバイスエイリアスデータベースのマージが失敗したことを確認するには、次の手順を実行します。

ステップ 1 CFS またはデバイスエイリアスマージ失敗の Syslog を調べて、マージが失敗したことを確認します。または、**show cfs merge status name device-alias** コマンドを実行して、マージのステータスを確認します。

ステップ 2 **show device-alias merge status** コマンドを使用して、マージが失敗した理由がアプリケーションの検証失敗であることを確認します。

```
switch# show device-alias merge status
Result: Failure
Reason: This is a non device-alias error.
```

ステップ 3 Syslog メッセージを調べます。検証が拒否されたスイッチの Syslog と、マージを管理しているスイッチの Syslog には、関連するエラーメッセージが表示されます。

この例は、検証が拒否されたスイッチのメッセージの例を示しています。

```
2007 Apr 10 00:00:06 switch-2 %DEVICE-ALIAS-3-MERGE_VALIDATION_REJECTED:
Failed SAP: 110 Reason: inter-VSAN zone member cannot be in more than one
VSAN Expln:
```

この例は、マージを管理している、検証が拒否されたスイッチの Syslog メッセージを示しています。

```
2007 Apr 9 16:41:22 switch-1 %DEVICE-ALIAS-3-MERGE_VALIDATION_FAILED: Failed
SWWN: 20:00:00:0d:ec:04:99:40 Failed SAP: 110 Reason: inter-VSAN zone member cannot be in more than
one
VSAN Expln:
```


ステップ 4 マージを管理しているスイッチで **show device-alias internal validation-info** コマンドを使用して、出力を調べます。

この例は、スイッチ 20:00:00:0d:ec:04:99:40 (switch-2) 上の SAP 110 によって検証が拒否されたことを示しています。ステータスメッセージには、失敗の理由とシステムアプリケーション番号が示されています。

```
switch# show device-alias internal validation-info
Validation timer:    0s
Per SAP Info Table:
=====
SAPS: 0
MTS Buffer Array Details:
=====
Buffers: 0
Local Status:
=====
Num Reqs Sent: 0 20:00:00:0d:ec:04:99:40
Num SAPs Done: 0
Failed SAP : 0 Status: success Expln:
Remote Status:
=====
CFS Resp Rcvd: TRUE
Failed SWWN : 20:00:00:0d:ec:04:99:40
SAP : 110 Status: inter-VSAN zone member cannot be in more than one VSAN <=== Status
Expln:
```

ステップ 5 **show system internal mts sup sap number description** コマンドを使用して、検証を拒否したスイッチ上の設定を拒否したアプリケーションを確認します。

この例では、デバイスエイリアスの検証を拒否したアプリケーションは IVR プロセスです。

```
switch# show system internal mts sup sap 110 description
IVR-SAP
```

ステップ 6 デバイスエイリアスの検証の失敗を分析します。この分析は、検証に失敗したアプリケーションおよびデバイスエイリアスデータベース設定によって異なります。

この例では、IVR が検証に失敗しています。この問題をトラブルシューティングするには、まず、マージされているデバイスエイリアスデータベースを確認します。各ファブリックのマージを管理しているスイッチから **show device-alias database** コマンドを使用します。

```
switch# show device-alias database
device-alias name A1 pwnn 21:01:01:01:01:01:01:01
device-alias name A2 pwnn 21:01:01:01:01:01:01:02 => Pre-merge: A2 defined on switch-1
Total number of entries = 2

switch# show device-alias database
device-alias name A1 pwnn 21:01:01:01:01:01:01:01 => Pre-merge: A2 not defined on switch-2
Total number of entries = 1
Because IVR is enabled on switch-2, review the IVR zone set.
switch# show ivr zoneset
zoneset name s1
zone name z1
pwnn 21:01:01:01:01:01:01:02 vsan 1 autonomous-fabric-id 1
device-alias A2 vsan 2 autonomous-fabric-id 1
```

データベース マージの前にデバイスエイリアス A2 が switch-2 で定義されていません。switch-1 と switch-2 の間のマージのために、デバイスエイリアス A2 は switch-2 で使用可能になり、A2 は pWWN 21:01:01:01:01:01:02 にマッピングされます。

IVR ゾーン z1 のデバイスエイリアス ベースのメンバー A2 は解決され、pWWN 21:01:01:01:01:01:02 にマッピングされて、VSAN2 のメンバーになります。ただし、pWWN 21:01:01:01:01:01:02 はすでに VSAN 1 のメンバーです。デバイスエイリアスのマージのために実行されるマッピングにより、IVR 設定が不適切なものになります。同じ pWWN を複数の VSAN のメンバーにすることはできません。

IVR 設定が不適切なものになると、VSAN 2 の pWWN はデバイスエイリアス (A2) を使用して定義される一方で、VSAN 1 のメンバーは実際の pWWN を使用して定義されます。IVR は、この状況を検出し、デバイスエイリアスの検証を拒否します。その結果、デバイスエイリアスのマージに失敗します。

データベース競合の解決

デバイスエイリアスデータベースのエントリが登録済みアプリケーションの設定と競合する場合、デバイスエイリアスデータベースのコミットで検証プロセスに失敗します。デバイスエイリアスデータベースまたはアプリケーション設定を修正してください。

検証に失敗したアプリケーションと失敗の理由を確認するには、次の手順を実行します。

ステップ 1 `device-alias commit` コマンドを使用して、出力を確認します。

次の例は、デバイスエイリアスデータベースとアプリケーション設定の間に競合があるためにコミットが失敗したことを示しています。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# device-alias commit
inter-VSAN zone member cannot be in more than one VSAN ==> reason for commit failure
```

ステップ 2 コミットによって発行されたスイッチの Syslog を調べて、どのアプリケーション設定がデバイスエイリアスデータベースと競合しているのかを確認します。

この例は、sWWN 20:00:00:0d:ec:04:99:40 (switch-2) 上の SAP 110 (IVR) が検証を拒否したためにデバイスエイリアスのコミットが失敗したことを示しています。

```
2007 Apr 10 11:54:24 switch-1 %DEVICE-ALIAS-3-VALIDATION_FAILED: Failed=>Validation Status
SWWN: 20:00:00:0d:ec:04:99:40 Failed SAP: 110 Reason: inter-VSAN zone ==>Switch and SAP member cannot
be in more than one VSAN Expln: ==>Reason
2007 Apr 10 11:54:24 switch-1 %DEVICE-ALIAS-3-COMMIT_FAILED: Failed to ==>Commit status commit the
pending database: inter-VSAN zone member cannot be in more ==>Reason than one VSAN
```

ステップ 3 検証が拒否されたスイッチの Syslog を確認します。

この例は、次の Syslog がスイッチ 2 で出力されることを示しています。

```
2007 Apr 10 19:13:08 switch-2 %DEVICE-ALIAS-3-VALIDATION_REJECTED: Failed
SAP: 110 Reason: inter-VSAN zone member cannot be in more than one VSAN ==>SAP and reason
```

ステップ4 既存のデバイスエイリアスデータベース（目的の変更点を含む）とアプリケーション設定を比較して、競合を確認します。

この例では、**show device-alias database** コマンドおよび **show ivr zoneset** コマンドと、コミットの前に実行されたデバイスエイリアスデータベースの変更のコンソールログが使用されています。この比較から、新しいデバイスエイリアス A2 の定義により IVR ゾーン z1 の拡張デバイスエイリアスメンバー A2 が、すでにゾーン z1 のメンバーになっている pWWN 21:01:01:01:01:01:02 に解決されていることが分かります。この pWWN は VSAN 1 のメンバーとして直接定義されていますが、拡張デバイスエイリアス A2 は VSAN 2 のメンバーとして定義されています。この設定は IVR では許可されません。IVR は、この設定上の問題を検出し、デバイスエイリアスデータベースの検証を拒否します。

```
switch# show device-alias database          ==> existing device alias database
device-alias name A1 pwn 21:01:01:01:01:01:01
Total number of entries = 1
switch# show ivr zoneset                   ==> display existing IVR zone set
zoneset name s1
zone name z1
pwn 21:01:01:01:01:01:02 vsan 1 autonomous-fabric-id 1
device-alias A2 vsan 2 autonomous-fabric-id 1
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# device-alias database
switch(config-device-alias-db)# device-alias name A2 pwn 21:01:01:01:01:01:02
switch(config-device-alias-db)# exit
switch(config)# device-alias commit
inter-VSAN zone member cannot be in more than one VSAN
```

ステップ5 アプリケーション設定を調整するか、デバイスエイリアスデータベースを変更して **device-alias commit** コマンドを再実行することにより、競合を修正します。

デバイスエイリアス データベースのステータスの確認

ここでは、デバイスエイリアスデータベースのステータスの確認に関する情報を提供します。

表 16: デバイスエイリアスデータベースのステータスの確認

コマンド名	説明
show cfs merge status name device-alias	デバイスエイリアスデータベースのCFSマージのステータスに関する情報が表示されます。
show device-alias database	デバイスエイリアスデータベース全体が表示されます。
show device-alias internal validation info	検証プロセス（コミットまたはマージの一部）のステータスに関する情報が表示されます。

コマンド名	説明
show device-alias merge conflicts	Cisco MDS NX-OS リリース 8.1(1) 以降でマージ失敗の原因となっているデバイスエイリアス名または pWWN が表示されます。
show device-alias merge status	デバイスエイリアスマージ操作の結果と結果の原因が表示されます。
show device-alias session status	最後の CFS コマンド (clear 、 commit 、 terminate など) のステータスが表示されます。最後に使用された CFS コマンドの結果と原因のフィールドは、失敗の原因を特定するために役立ちます。
show device-alias status	ファブリック配布が有効かどうか、データベース内のデバイスエイリアスの数、ロック情報、データベースモード (基本または拡張) といったデバイスエイリアスサービスの設定情報が表示されます。



CHAPTER 7

ファイバチャネルルーティングサービス およびプロトコルの設定

Fabric Shortest Path First (FSPF) は、ファイバチャネルファブリックで使用される標準パス選択プロトコルです。FSPF 機能は、どのファイバチャネルスイッチでも、デフォルトでイネーブルになっています。特殊な考慮事項を必要とする設定を除き、FSPF サービスを設定する必要はありません。FSPF はファブリック内の任意の2つのスイッチ間の最適パスを自動的に計算します。具体的に、FSPF は次の目的で使用されます。

- 任意の2つのスイッチ間の最短かつ最速のパスを確立して、ファブリック内のルートを動的に計算します。
- 指定されたパスに障害が発生した場合に、代替パスを選択します。FSPF は複数のパスをサポートし、障害リンクを迂回する代替パスを自動的に計算します。同等な2つのパスが使用可能な場合は、推奨ルートが提供されます。

この章では、ファイバチャネルルーティング サービスおよびプロトコルの詳細について説明します。内容は次のとおりです。

- [FSPF の概要, on page 205](#)
- [FSPF のグローバル設定, on page 208](#)
- [FSPF インターフェイスの設定, on page 211](#)
- [FSPF ルート, on page 217](#)
- [ロード バランシング, on page 219](#)
- [順序どおりの配信, on page 224](#)
- [フロー統計情報の設定, on page 229](#)
- [デフォルト設定, on page 234](#)

FSPF の概要

FSPF は、ファイバチャネル ネットワーク内でのルーティング用として、T11 委員会によって現在標準化されているプロトコルです。FSPF プロトコルには、次の特性および特徴があります。

- 複数パスのルーティングをサポートします。

- パス ステータスはリンク ステート プロトコルによって決まります。
- ドメイン ID だけに基づいて、ホップ単位ルーティングを行います。
- E ポートまたは TE ポートだけで稼働し、ループのないトポロジを形成します。
- VSAN (仮想 SAN) 単位で稼働します。ファブリック内の各 VSAN では、この VSAN に設定されたスイッチとの接続が保証されます。
- トポロジデータベースを使用して、ファブリック内のすべてのスイッチのリンク ステートを追跡し、各リンクにコストを対応付けます。
- トポロジが変更された場合、高速な再コンバージェンス タイムを保証します。標準ダイクストラ アルゴリズムを使用します。ただし、より強固で、効率的な差分ダイクストラ アルゴリズムを静的に、あるいは動的に選択することができます。VSAN 単位でルートが計算されるため、再コンバージェンス タイムは高速かつ効率的です。

FSPF の例

ここでは、FSPF の利点を示すトポロジおよびアプリケーション例について説明します。

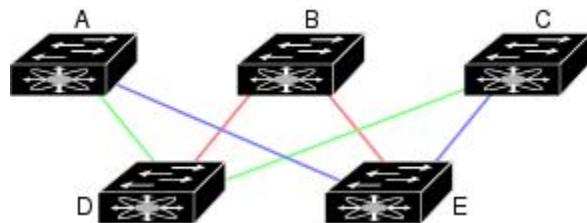


Note FSPF 機能は任意のトポロジで使用できます。

フォールトトレラントファブリック

[Figure 43: フォールトトレラントファブリック, on page 206](#) に、部分的メッシュトポロジを使用するフォールトトレラントファブリックを示します。ファブリック内のどの部分でリンクダウンが発生しても、各スイッチはファブリック内の他のすべてのスイッチと通信できます。同様に、どのスイッチがダウンしても、ファブリックの残りの接続は維持されます。

Figure 43: フォールトトレラントファブリック



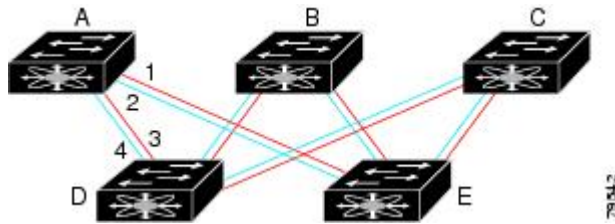
たとえば、すべてのリンク速度が等しい場合、FSPF は A ~ C 2 つの同等なパス (A-D-C [グリーン] と A-E-C [ブルー]) を計算します。

冗長リンク

[Figure 43: フォールトトレラントファブリック, on page 206](#) のトポロジを改良するには、任意のスイッチペア間の接続をそれぞれ重複させます。スイッチペア間には、リンクを複数設定できます。[Figure 44: 冗長リンクを持つフォールトトレラントファブリック, on page 207](#) に、この配置例を示します。Cisco MDS 9000 ファミリのスイッチはポートチャネル機能をサポートしているため、物理リンクの各ペアは単一の論理リンクとして FSPF プロトコルに認識されます。

物理リンク ペアをバンドルすることにより、データベース サイズは小さくなり、リンク アップデート頻度が減少するため、FSPF の効率が大幅に改善されます。物理リンクを集約すると、障害は単一のリンクだけにとどまらずポート チャネル全体に波及します。この設定により、ネットワークの復元力も向上します。ポートチャネルのリンクに障害が発生しても、ルートは変更されないため、ルーティングループ、トラフィック消失、またはルート再設定のためのファブリック ダウンタイムが生じるリスクが軽減されます。

Figure 44: 冗長リンクを持つフォールトトレラントファブリック



たとえば、すべてのリンクの速度が等しく、PortChannel が存在しない場合、FSPF では A から C への同等パス 4 つ (A1-E-C、A2-E-C、A3-D-C、および A4-D-C) が計算されます。PortChannel が存在する場合は、これらのパスが 2 つに削減されます。

PortChannel および FSPF リンクのフェールオーバー シナリオ

SmartBits トラフィック ジェネレータを使用して、Figure 45: トラフィック ジェネレータを使用したフェールオーバー シナリオ, on page 207 に示されたシナリオを評価しました。スイッチ 1 とスイッチ 2 の間に存在する 2 つのリンクは、等コストの ISL リンクまたはポートチャネルリンクのどちらかです。トラフィック ジェネレータ 1 からトラフィック ジェネレータ 2 へのフローは、1 つ存在します。次のような 2 とおりのシナリオを想定して、100% の利用率、1 Gbps のトラフィックをテストしました。

- ケーブルを物理的に取り外して、トラフィック リンクをディセーブルにする (Table 17: SmartBits ケーブルの物理的取り外しのシナリオ, on page 207 を参照)。
- スイッチ 1 またはスイッチ 2 のどちらか一方のリンクをシャットダウンする (Table 18: SmartBits スイッチでのリンクのシャットダウンシナリオ, on page 208 を参照)。

Figure 45: トラフィック ジェネレータを使用したフェールオーバー シナリオ

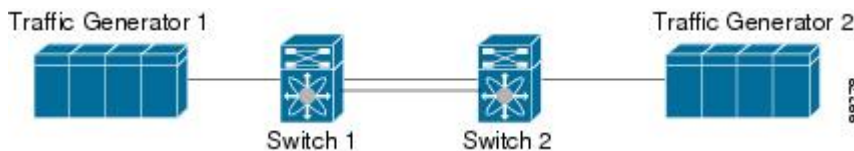


Table 17: SmartBits ケーブルの物理的取り外しのシナリオ

ポートチャネル シナリオ		FSPF シナリオ (等コスト ISL)	
スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2
110 ミリ秒 (削除フレーム数は 2 K 以下)		130+ ミリ秒 (削除フレーム数は 4 K 以下)	

ポートチャネル シナリオ	FSPF シナリオ (等コスト ISL)
100 ミリ秒 (標準の規定に従って信号損失を通知するときのホールドタイム)	

Table 18: SmartBits スイッチでのリンクのシャットダウン シナリオ

ポートチャネル シナリオ		FSPF シナリオ (等コスト ISL)	
スイッチ 1	スイッチ 2	スイッチ 1	スイッチ 2
~0 ミリ秒 (削除フレーム数は 8 以下)	110 ミリ秒 (削除フレーム数は 2 K 以下)	130+ ミリ秒 (削除フレーム数は 4 K 以下)	
ホールドタイム 不要	スイッチ 1 での信号損失	ホールドタイム 不要	スイッチ 1 での信号損失

FSPF のグローバル設定

Cisco MDS 9000 ファミリのスイッチでは、FSPF はデフォルトでイネーブルです。

一部の FSPF 機能は、VSAN ごとにグローバルに設定できます。VSAN 全体に機能を設定すると、コマンドごとに VSAN 番号を指定する必要がなくなります。このグローバル設定機能を使用すると、タイプミスや、その他の軽微な設定エラーが発生する可能性も低減されます。



Note FSPF はデフォルトでイネーブルになっています。通常、これらの高度な機能は設定する必要がありません。



Caution バックボーン リージョンのデフォルトは 0 (ゼロ) です。この設定を変更する必要があるのは、デフォルト以外のリージョンを使用する場合だけです。バックボーン リージョンを使用して別のベンダー製品と併用する場合は、これらの製品の設定と互換性が保たれるようにこのデフォルトを変更できます。

このセクションは、次のトピックで構成されています。

SPF 計算ホールドタイムの概要

SPF 計算のホールドタイムは、VSAN での 2 つの連続した SPF 計算間の最小時間に設定されます。これを小さい値に設定すると、VSAN 上のパスの再計算によるファブリックの変更に対して、FSPF の処理が速くなります。SPF 計算のホールドタイムが短いと、スイッチの CPU 時間は長くなります。

Link State Record のデフォルトの概要

ファブリックに新しいスイッチが追加されるたびに、Link State Record (LSR) が近接スイッチに送信されて、ファブリック全体にフラッディングされます。Table 19: LSR のデフォルト設定, on page 209 に、スイッチ応答に関するデフォルト設定を示します。

Table 19: LSR のデフォルト設定

LSR のオプション	デフォルト	説明
ACK インターバル (RxmtInterval)	5 秒	再送信するまで、スイッチが LSR からの ACK を待機する期間
リフレッシュ タイム (LSRefreshTime)	30 分	LSR リフレッシュを送信するまで、スイッチが待機する期間
最大エージング (MaxAge)	60 分	データベースから LSR を削除するまで、スイッチが待機する期間

LSR の最小着信時間は、この VSAN の LSR アップデートの受信間隔です。LSR の最小着信時間よりも前に着信した LSR アップデートは廃棄されます。

LSR 最小間隔は、このスイッチが VSAN 上の LSR アップデートを送信する頻度です。

VSAN での FSPF の設定

VSAN 全体に FSPF 機能を設定するには、次の手順を実行します。

ステップ 1 switch# config terminal

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# fspf config vsan 1

指定された VSAN に対して FSPF グローバル コンフィギュレーション モードを開始します。

ステップ 3 switch-config-(fspf-config)# spf static

ダイナミック (デフォルト) 差分 VSAN に対してスタティック SPF 計算を強制実行します。

ステップ 4 switch-config-(fspf-config)# spf hold-time 10

VSAN 全体に対して、2つのルート計算間のホールドタイムをミリ秒 (msec) 単位で設定します。デフォルト値は 0 です

Note 指定期間が短いほど、ルーティングは高速化されます。ただし、それに応じて、プロセッサ消費量が増大します。

ステップ 5 switch-config-(fspf-config)# region 7

現在の VSAN に自律リージョンを設定し、リージョン ID (7) を指定します。

FSPF のデフォルト設定へのリセット

FSPF VSAN のグローバル設定を出荷時のデフォルト設定に戻すには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **no fspf config vsan 3**

VSAN 3 の FSPF 設定を削除します。

FSPF のイネーブル化またはディセーブル化

FSPF ルーティング プロトコルを有効または無効にするには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **fspf enable vsan 7**

VSAN 7 内で FSPF ルーティング プロトコルを有効にします。

ステップ 3 switch(config)# **no fspf enable vsan 5**

VSAN 5 内で FSPF ルーティング プロトコルを無効にします。

VSAN の FSPF カウンタのクリア

VSAN 全体の FSPF 統計情報カウンタをクリアするには、次の手順を実行します。

```
switch# clear fspf counters vsan 1
```

指定された VSAN の FSPF 統計情報カウンタをクリアします。インターフェイス参照番号を指定しない場合は、すべてのカウンタがクリアされます。

FSPF インターフェイスの設定

一部の FSPF コマンドは、インターフェイス単位で使用できます。次に示す設定手順は、特定の VSAN 内の 1 つのインターフェイスに適用されます。

このセクションは、次のトピックで構成されています。

FSPF リンク コストの概要

FSPF はファブリック内のすべてのスイッチのリンク ステータスを追跡し、データベース内の各リンクにコストを対応付け、コストが最小なパスを選択します。インターフェイスに対応付けられたコストを管理上変更して、FSPF ルート選択を実行できます。コストは、1～30000 の整数値で指定できます。1 Gbps のデフォルト コストは 1000 であり、2 Gbps では 500 です。

FSPF リンク コストの設定

FSPF リンク コストを設定する手順は、次のとおりです。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **interface fc1/4**

```
switch(config-if)#
```

指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。

ステップ 3 switch(config-if)# **fspf cost 5 vsan 90**

VSAN 90 の選択されたインターフェイスのコストを設定します。

FSPF コスト乗数について

FSPF はリンク コストを使用して、ファブリック内のデバイス間の最短パスを決定します。より大きな容量のポートチャネルのコストを計算する場合、デフォルトのリンク コストは非効率になります。このようなパスのコストは同じに見える場合がありますが、帯域幅が異なるた

め、FSPF によるパス選択が不十分になります。FSPF コスト乗数機能を使用すると、FSPF が最適な高速パスを計算して選択できるように、リンク コストを再割り当てできます。

リンク帯域幅の合計が 128 Gbps を超えると、パス コスト計算の非効率性が発生する可能性があります。このしきい値を超えるパラレルパスがファブリックに存在する場合は、FSPF が予想どおりにパスを選択するように、この機能を構成する必要があります。ポートチャネルには最大 16 のメンバー リンクを含めることができるため、16 Gbps のメンバーが 9 つ（以上）のポートチャネルが存在する場合、パスの非効率性が発生する可能性があります。

ファブリック内のすべてのスイッチは、同じ FSPF コスト乗数を使用して、パスコスト計算に同じ基準を使用する必要があります。この機能は、構成された FSPF コスト乗数を、この機能をサポートする Cisco NX-OS バージョンを備えたファブリック内のすべての Cisco MDS スイッチに自動的に配布します。この機能をサポートしていないスイッチがファブリックに存在する場合、構成は失敗し、どのスイッチにも適用されません。コスト乗数がすべてのスイッチによって受け入れられた後、すべてのスイッチが更新を同時に適用するように、適用される前に 20 秒の遅延が発生します。リンク コストが変わらなければ、トラフィックの中断は発生しません。ただし、更新によって FSPF によって異なるパスが選択される場合、新しいパスが適用されるときに、トラフィックが一時的に 1 回だけ中断されることがあります。

インターフェイスのリンク コストは、デフォルト値で手動で変更することもできます。詳細については、「[FSPF リンク コストの概要 \(211 ページ\)](#)」の項を参照してください。

FSPF コスト乗数の設定

FSPF コスト計算乗数は、ポートチャネル リンクのコストが最適になるように構成されています。コストの計算は、高速ポートチャネル（16 Gbps 以降の速度のメンバー）には最適ではありませんでした。このソリューションは次のことを提供します。

- FSPF コスト計算乗数値 20 は、リンクのコストを最適化するように構成されています。
- FSPF コストの計算は、最大 128 Gbps の速度の 16 メンバーのポートチャネルに最適です。
- 特定の VSAN のファブリック全体に FSPF コスト計算乗数を分散すると、VSAN のファブリック内のすべてのリンクがリンクの FSPF コスト計算に同じ係数を使用するようになります。



(注) FSPF Cost Multiplier の構成は、メンテナンス ウィンドウ中に行うことが推奨されています。これは、新しいリンク コストに基づいたルートの変更によりトラフィックに影響が及ぶ可能性があるためです。

コスト管理要素を設定するには、次の手順に従います。

ステップ 1 switch# config terminal

コンフィギュレーション モードに入ります。

ステップ 2 switch# **fspf config vsan**

```
switch(config-fspf-config)#
```

Fabric Shortest Path First (FSPF) ルーティング プロトコルを開始します。

ステップ 3 switch(config-fspf-config)# **cost-multiplier 20**

FSPF コスト乗数を 20 に設定します。

次のメッセージが表示されます。

このパラメータは、ファブリック内のすべてのスイッチに分散されます。新しいルートは 20 秒後に計算されます。

ファブリック内のいずれかのスイッチが新しいコスト計算管理係数値をサポートしていないか、バージョンが Cisco MDS NX-OS 9.3(1) よりも前の場合、次のメッセージが表示されます。

```
Unable to distribute fspf cost-multiplier due to one or more domains not supporting it. fspf
cost-multiplier supported on NX-OS 9.3(1) and later only.
VSAN 7
  FSPF cost multiplier is not supported on the following devices:
  Domain VSAN SWWN
  -----
  58 20:07:00:de:fb:b1:8d:e1
```

FSPF コスト乗数の表示

次に、VSAN 1 の FSPF コスト乗数を表示する例を示します。

```
switch# show fspf vsan1
```

VSAN 1 に使用される FSPF コスト乗数を表示します。

コマンドの次の結果が表示されます

```
switch(config)# show fspf vsan 1
FSPF routing for VSAN 1
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 0
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 2000 msec
Cost Multiplier = 1
Local Domain is 0x66(102)
Number of LSRs = 3, Total Checksum = 0x000198dd

Protocol constants :
  LS_REFRESH_TIME = 30 minutes (1800 sec)
  MAX_AGE          = 60 minutes (3600 sec)

Statistics counters :
  Number of LSR that reached MaxAge = 0
  Number of SPF computations        = 6
  Number of Checksum Errors         = 0
```

```
Number of Transmitted packets : LSU 30 LSA 32 Hello 984 Retransmitted LSU 0
Number of received packets : LSU 33 LSA 28 Hello 981 Error packets 3
```

ハロータイムインターバルの概要

FSPF hello タイムインターバルを設定すると、リンク状態を確認するために送信される定期的な hello メッセージの間隔を指定できます。指定できる整数値は 1 ～ 65,535 秒です。



Note この値は、ISL の両端のポートで同じでなければなりません。

ハロータイムインターバルの設定

FSPF の hello タイムインターバルを設定するには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **interface fc1/4**

```
switch(config-if)#
```

指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーションモードを開始します。

ステップ 3 switch(config-if)# **fspf hello-interval 15 vsan 175**

```
switch(config-if)#
```

VSAN 175 のリンクのヘルスを確認するために、hello メッセージインターバル（15 秒）を指定します。デフォルトは 20 秒です。

デッドタイムインターバルの概要

FSPF デッドタイムインターバルを設定すると、hello メッセージを受信しなければならない最大間隔を指定できます。この期間が経過すると、ネイバーは消失したと見なされ、データベースから削除されます。指定できる整数値は 1 ～ 65,535 秒です。



Note この値は、ISL の両端のポートで同じでなければなりません。

- 設定したデッドタイムインターバルが hello タイムインターバルより短い場合、コマンドプロンプトでエラーが報告されます。
- ソフトウェアアップグレード中に、fspf デッドタイムインターバルが ISSU ダウンタイム(80 秒)よりも長いことを確認します。fspf デッドタイムインターバルが ISSU ダウンタイムよりも短いと、ソフトウェアアップグレードが失敗し、次のエラーメッセージが表示されます。

```
Service "fspf" returned error: Dead interval for interface is less than ISSU upgrade time.
```

デッドタイムインターバルの設定

FSPF のデッドタイムインターバルを設定するには、次の手順を実行します。

ステップ 1 switch# config terminal

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# interface fc1/4

```
switch(config-if)#
```

指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーションモードを開始します。

ステップ 3 switch(config-if)# fspf dead-interval 25 vsan 7

```
switch(config-if)#
```

VSAN 7 に、選択されたインターフェイスで hello メッセージを受信しなければならない最大間隔を指定します。この期間が経過すると、ネイバーは消失したと見なされます。デフォルトは 80 秒です。

再送信インターバルの概要

インターフェイス上で未確認応答リンク ステート アップデートを送信するまでの期間を指定します。再送信インターバルを指定する整数値の有効範囲は、1 ~ 65,535 秒です。



Note この値は、インターフェイスの両端のスイッチで同じでなければなりません。

再送信インターバルの設定

FSPF の再送信タイムインターバルを設定するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **interface fc1/4**

```
switch(config-if)#
```

指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーション モードを開始します。

ステップ 3 switch(config-if)# **fspf retransmit-interval 15 vsan 12**

```
switch(config-if)#
```

VSAN 12 における未確認応答リンク状態アップデートの再送信間隔を指定します。デフォルトは 5 秒です。

インターフェイス単位での FSPF のディセーブル化

選択したインターフェイスで FSPF プロトコルをディセーブルにできます。デフォルトでは、FSPF はすべての E ポートおよび TE ポートでイネーブルです。このデフォルト設定をディセーブルにするには、インターフェイスをパッシブに設定します。



Note プロトコルを機能させるには、インターフェイスの両端で FSPF をイネーブルにする必要があります。

特定のインターフェイスに対する FSPF のディセーブル化

選択したインターフェイスで FSPF プロトコルをディセーブルにできます。デフォルトでは、FSPF はすべての E ポートおよび TE ポートでイネーブルです。このデフォルト設定をディセーブルにするには、インターフェイスをパッシブに設定します。

特定のインターフェイスに対して FSPF を無効にするには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **interface fc1/4**

```
switch(config-if)#
```


指定されたインターフェイスを設定します。すでに設定されている場合は、指定されたインターフェイスに対してコンフィギュレーションモードを開始します。

ステップ 3 `switch(config-if)# fspf passive vsan 1`

```
switch(config-if)#
```

指定された VSAN 内の特定のインターフェイスに対して FSPF プロトコルをディセーブルにします。

ステップ 4 `switch(config-if)# no fspf passive vsan 1`

```
switch(config-if)#
```

指定された VSAN 内の特定のインターフェイスに対して FSPF プロトコルを再度イネーブルにします。

選択したインターフェイスで FSPF プロトコルをディセーブルにできます。デフォルトでは、FSPF はすべての E ポートおよび TE ポートでイネーブルです。このデフォルト設定をディセーブルにするには、インターフェイスをパッシブに設定します。

インターフェイスの FSPF カウンタのクリア

インターフェイスの FSPF 統計情報カウンタをクリアするには、次の手順を実行します。

```
switch# clear fspf counters vsan 200 interface fc1/1
```

VSAN 200 内の指定インターフェイスの FSPF 統計情報カウンタをクリアします。

FSPF ルート

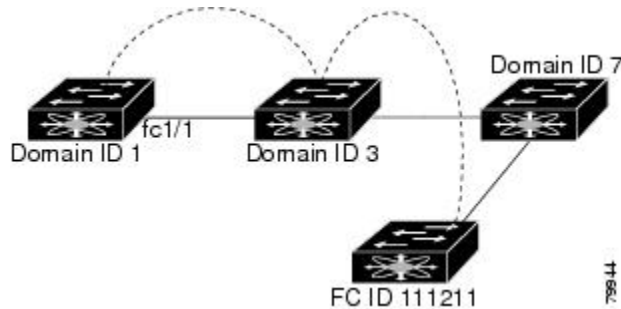
FSPF は、FSPF データベース内のエントリに基づいて、ファブリックを経由するトラフィックをルーティングします。これらのルートは動的に学習させるか、または静的に設定することもできます。

このセクションは、次のトピックで構成されています。

ファイバチャネル ルートの概要

各ポートは、FC ID に基づいてフレームを転送する転送ロジックを実行します。特定のインターフェイスおよびドメイン用の FC ID を使用することにより、ドメイン ID 1 のスイッチで特定のルート（例：FC ID 111211、ドメイン ID 3）を設定できます（[Figure 46: ファイバチャネルのルート](#), on page 218 を参照）。

Figure 46: ファイバチャネルのルート



Note VSAN 外部では、設定済みスタティックルートおよび一時停止中のスタティックルートに対してランタイムチェックは実行されません。

ブロードキャストおよびマルチキャストルーティングの概要

ファイバチャネルファブリック内のブロードキャストおよびマルチキャストは、配信ツリー概念に基づいて、ファブリック内のすべてのスイッチに到達します。

配信ツリーを計算するためのトポロジ情報は、FSPFによって提供されます。ファイバチャネルには、VSANごとに256個のマルチキャストグループ、および1個のブロードキャストアドレスが定義されます。Cisco MDS 9000ファミリスイッチで使用されるのは、ブロードキャストルーティングだけです。デフォルトでは、ルートノードとして主要スイッチが使用され、VSAN内でマルチキャストルーティングおよびブロードキャストルーティング用のループフリー配信ツリーが取得されます。



Caution 同じ配信ツリーが得られるようにするために、ファブリック内のすべてのスイッチで同一のマルチキャストおよびブロードキャスト配信ツリーアルゴリズムを実行する必要があります。

他のベンダーのスイッチ（FC-SW3ガイドラインに準拠）と相互運用するために、SAN-OSおよびNX-OS 4.1(1b)以降のソフトウェアは最も小さなドメインスイッチをルートとして使用し、interopモードでマルチキャストツリーを計算します。

マルチキャストルートスイッチの概要

native（非 interop）モードでは、主要スイッチがデフォルトのルートとして使用されます。デフォルトを変更する場合は必ず、ファブリック内のすべてのスイッチに同じモードを設定してください。同じモードを設定しないと、マルチキャストトラフィックがループし、フレームが削除されるなどの問題が発生する可能性があります。



Note 動作モードが、設定されている **interop** モードと異なる場合があります。interop モードでは常に、最も小さなドメインスイッチがルートとして使用されます。

主要スイッチから最も小さなドメインスイッチにマルチキャストルートを変更するには、**mcast root lowest vsan** コマンドを使用します。

マルチキャストルートスイッチの設定

マルチキャストツリー計算に最も小さなドメインスイッチを使用するには、次の手順を実行します。

ステップ 1 switch# config terminal

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# mcast root lowest vsan 1

最も小さなドメインスイッチを使用してマルチキャストツリーを計算します。

ステップ 3 switch(config)# mcast root principal vsan 1

デフォルトでは、主要スイッチを使用してマルチキャストツリーを計算します。

設定されており稼働しているマルチキャストモードと選択されたルートドメインを表示するには、**show mcast** コマンドを使用します。

```
switch# show mcast vsan 1
Multicast root for VSAN 1
  Configured root mode : Principal switch
  Operational root mode : Principal switch
  Root Domain ID : 0xef(239)
```

ロードバランシング

ロードバランシングは、等コストマルチパス (ECMP) およびポートチャネルを介してトラフィックを分散する転送メカニズムです。ロードバランシングでは、ハッシュメソッドを使用して出力リンクを識別します。ハッシュは、フレームヘッダーのパラメーターを使用して、フレームの転送先の一意のリンクを識別する関数です。使用されるロードバランシングスキームは、入力ポートのタイプと出力ルーティングの両方に依存します。トラフィックが同じリンク上で両方向に流れることを意図している場合は、リンクの両端で同じロードバランシングスキームとハッシュメソッドが使用されていることを確認してください。

ロードバランシングスキーム

次のタイプのロードバランシングスキームがサポートされています。

- フローベース：所定の送信元 FCID と接続先 FCID 間のすべてのフレームが同一のリンクで送信されます。つまり、送信元と接続先ペア間の最初の通信で選択されたリンクが、後続のすべての通信で使用されます。
- 交換ベース：所定の送信元 FCID と接続先 FCID 間の通信の最初のフレームは、出力リンクを選択するために使用され、その通信の後続フレームは同一のリンクで送信されます。ただし、送信元と接続先ペア間のその後の通信は、別のリンクで送信される可能性があります。これにより、通信ごとにフレームの順序を維持しながら、より細かいロードバランシングが可能になります。

図 47: フローベースのロードバランシング (220 ページ) に、フローベースのロードバランシングがどのように機能するかを示します。この例では、送信元 FCID が sid1 で接続先 FCID が did1 の最初のフレームが転送用に受信されると、ポートチャネル 2 が選択されます。そのフローの各後続のフレームが、同一のポートチャネル上に送信されます。sid1 から did1 へのフレームは、ポートチャネル 1 を使用しません。同様に、sid2 および did2 を持つすべてのフレームは、ポートチャネル 1 を介して送信されます。Exchange ID は、このタイプのロードバランシングでは使用されません。

図 47: フローベースのロードバランシング

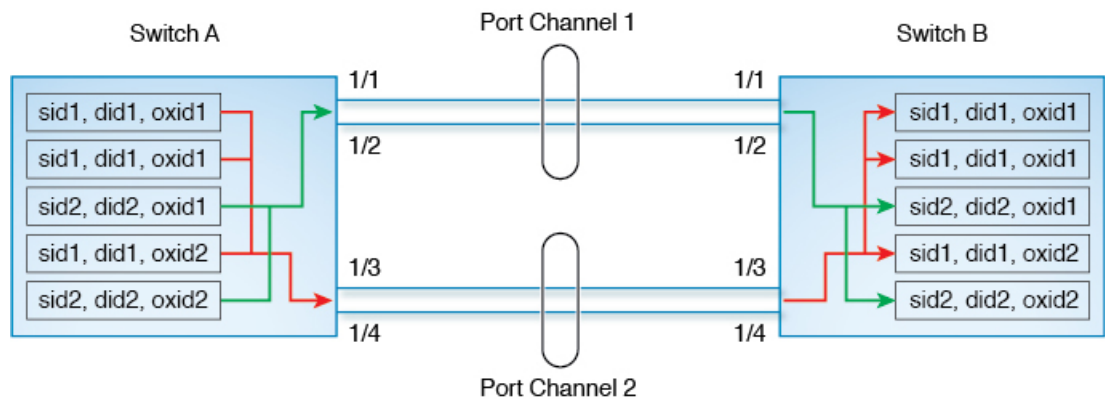
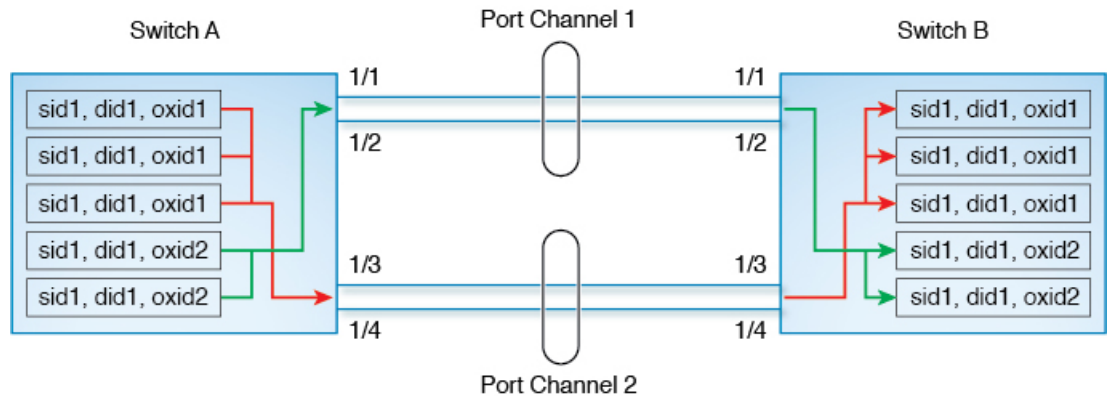


図 48: 通信ベースのロードバランシング (221 ページ) に、通信ベースのロードバランシングがどのように機能するかを示します。この例では、送信元 FCID sid1 と接続先 FCID did1 間の交換の最初のフレームが転送のために受信されると、ポートチャネル 2 が選択されます。その特定の通信の残りのフレームはすべて同じポートチャネルで送信され、ポートチャネル 1 では送信されません。次の交換では、ハッシュアルゴリズムはポートチャネル 1 を選択します。したがって、同じ送信元と接続先ペア間の通信 2 のすべてのフレームは、ポートチャネル 1 で送信されます。

図 48: 通信ベースのロードバランシング



ハッシュメソッド

ロードバランシングは2つのレベルで入力フレームに適用されます。最初のレベルでは、ECMP ハッシュを使用して出力ECMP インターフェイスを選択します（これは、物理インターフェイスまたはポートチャネルインターフェイスなどの論理インターフェイスのいずれかです）。第2レベルでは、ポートチャネルハッシュを使用して出力ポートチャネルメンバーを選択します。

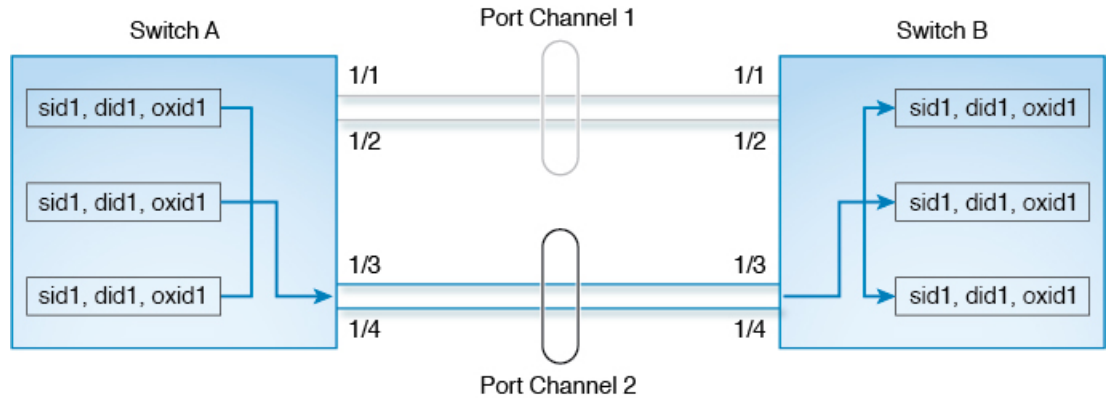
デフォルトでは、使用されるハッシュメソッドは、入力ハードウェアタイプによって異なります。いずれかのレベルのハッシュが出力ルートに適用されない場合、ハッシュ方式は適用されません。

次のタイプのハッシュメソッドがサポートされています。

- ECMP ハッシュメソッド：同じコストの接続先への複数のパスがスイッチに存在する場合、入力ポートの FIB は、その接続先のこれらのパスで更新されます。このハッシュメソッドは、フレームを送信するパスの1つを選択するために使用されます。
- ポートチャネルのハッシュ方法メソッド：このハッシュメソッドは、出力ポートチャネルの動作可能なインターフェイスを選択するために使用されます。

図 49: ECMP ハッシュメソッド (222 ページ) は、ECMP ハッシュメソッドがどのように機能するかを示しています。2つの等速リンクをそれぞれ含む2つのポートチャネルがあります。ポートチャネルの FSPF コストは同じであるため、両方のポートチャネルがハッシュに使用されます。この例では、ECMP レベルのハッシュメソッドはポートチャネル2を出力ポートとして選択します。

図 49: ECMP ハッシュメソッド



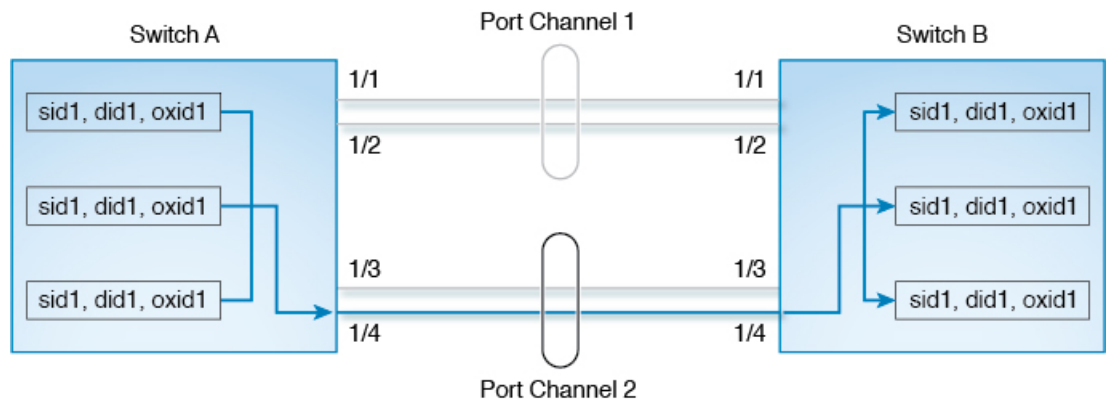
入力ポートのタイプに応じて、ECMP ハッシュメソッドの次のサブタイプがサポートされています。

- タイプ 1a
- タイプ 1b

特定の入力ポートにどのハッシュメソッドが選択されているかについては、[表 20: ハッシュマトリックス \(223 ページ\)](#) を参照してください。

[図 50: ポートチャネルのハッシュメソッド \(222 ページ\)](#) に、ポートチャネルハッシュメソッドの動作を示します。ポートチャネル2が出力ポートとして選択された [図 49: ECMP ハッシュメソッド \(222 ページ\)](#) の例を続けると、続いてポートチャネルハッシュが適用されて、ポートチャネル内の出力ポートが選択されます。この例では、フレームは選択されたポートチャネルのインターフェイス 1/4 によって送信されます。

図 50: ポートチャネルのハッシュメソッド



入力ポートのタイプに応じて、次のタイプのポートチャネルハッシュメソッドがサポートされます。

- タイプ 2a
- タイプ 2b

特定の入力ポートにどのハッシュメソッドが選択されているかについては、[表 20: ハッシュマトリックス \(223 ページ\)](#) を参照してください。

表 20: ハッシュマトリックス

入力インターフェイス	出力インターフェイス	ECMP ハッシュメソッド	ポートチャネルハッシュメソッド
第3世代または第4世代モジュールを搭載した Cisco MDS 9500 のファイバチャネルまたは FCIP ポート	ファイバチャネルまたは FCIP ISL	タイプ 1a	タイプ 2b (少なくとも1つの FCIP ポートが稼働している場合のみ)
第3世代または第4世代モジュールを搭載した Cisco MDS 9500 のファイバチャネルポート	ファイバチャネル ISL	タイプ 1a	タイプ 2a (注) スイッチで FCIP トンネルが起動された場合、ハッシュメソッドはタイプ 2b に変更されません。FCIP モジュールが削除されても、次のスイッチのリロードまでハッシュメソッドはタイプ 2b のままです。
Cisco MDS 9250i のファイバチャネル、FCIP、または FCoE ポート	ファイバチャネル、FCIP、または FCoE ISL	タイプ 1a	タイプ 2b
Cisco MDS 9250i のファイバチャネル、FCIP、または FCoE ポート	FCIP が拡張された Cisco MDS 24/10 ポート SAN 拡張モジュールに接続された FCIP ISL。	タイプ 1a	タイプ 1a

入力インターフェイス	出力インターフェイス	ECMP ハッシュ メソッド	ポートチャネルハッシュ メソッド
Cisco MDS 9700 のファイバチャネルポート	FCIP ISL	タイプ 1a	タイプ 1a
	ファイバチャネルまたは FCoE ISL	タイプ 1a	タイプ 2a
Cisco MDS 24/10 ポート SAN 拡張モジュールの FCIP ポート	FCIP ISL	タイプ 1b	タイプ 1b
	ファイバチャネルまたは FCoE ISL	タイプ 1b	タイプ 2a
Cisco MDS 9700 の FCoE ポート	FCIP ISL	タイプ 1b	タイプ 1b
	ファイバチャネルまたは FCoE ISL	タイプ 1b	タイプ 2a
Cisco MDS 9148S のファイバチャネルポート Cisco MDS 9396S のファイバチャネルポート Cisco MDS 9132T のファイバチャネルポート Cisco MDS 9396T および 9148T のファイバチャネルポート	ファイバチャネル ISL	タイプ 1a	タイプ 2a

順序どおりの配信

データフレームの順序どおりの配信 (IOD) 機能を使用すると、フレームは送信元から送信されたときと同じ順番で宛先に配信されます。

一部のファイバチャネルプロトコルまたはアプリケーションでは、順序外のフレーム配信を処理できません。このような場合、Cisco MDS 9000 ファミリのスイッチではフレームフローのフレーム順序が維持されます。フレームのフローは SID (ソース ID)、DID (宛先 ID)、およびオプションの OX ID (送信元交換 ID) で識別されます。

IOD がイネーブルのスイッチでは、特定の入力ポートで受信されて特定の出力ポートに送信されるすべてのフレームは常に、受信時と同じ順序で配信されます。

IOD を使用するのには、順序外のフレーム配信をサポートできない環境の場合だけにしてください。



Tip 順序どおりの配信機能をイネーブルにすると、グレースフルシャットダウン機能は実行されません。

このセクションは、次のトピックで構成されています。

ネットワーク フレーム順序の再設定の概要

ネットワーク内でルートが変更されると、新しく選択されたパスが元のルートよりも高速になったり、輻輳が軽減されたりすることがあります。

Figure 51: ルート変更の配信

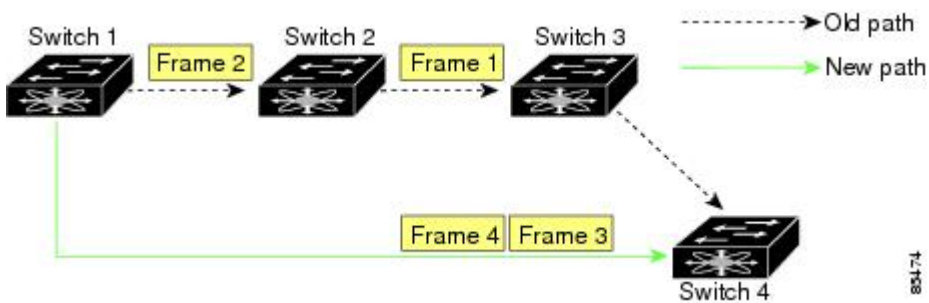


Figure 51: ルート変更の配信, on page 225 では、スイッチ 1 からスイッチ 4 への新しいパスの方が高速です。したがって、フレーム 3 およびフレーム 4 は、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

順序保証機能がイネーブルな場合、ネットワーク内のフレームは次のように配信されます。

- ネットワーク内のフレームは送信された順番で配信されます。
- ネットワーク遅延ドロップ期間内に順番どおりに配信できないフレームは、ネットワーク内でドロップされます。

ポート チャネル フレーム順序の再設定の概要

ポートチャネル内でリンクが変更されると、同じ通信フローまたは同じイニシエーターとターゲット間のフロー内のフレームが、元のパスから、より高速な別のパスに切り替えられることがあります。

Figure 52: リンクが輻輳している場合の配信

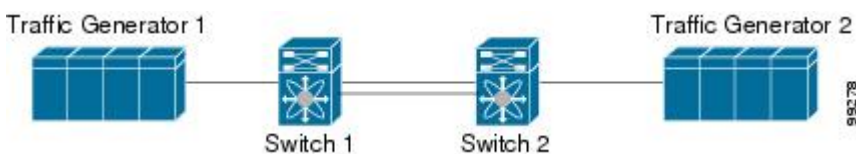


Figure 52: リンクが輻輳している場合の配信, on page 225 では、元のパス（黒い点線）のポートが輻輳しています。したがって、フレーム 3 およびフレーム 4 は、フレーム 1 およびフレーム 2 よりも先に配信されることがあります。

該当ポートチャネルのすべてのフレームをフラッシュする要求を、ポートチャネル上のリモートスイッチに送信して、順序どおりの配信機能をイネーブルにしておくと、ポートチャネルリンクの変更時に削除されるフレーム数が最小限に抑えられます。



Note Lossless IOD として知られるこの IOD 拡張機能を実行するには、ポートチャネル上の両方のスイッチで Cisco SAN-OS Release 3.0(1) が稼働している必要があります。これより古いリリースでは、IOD はスイッチ遅延期間だけ待機してから、新しいフレームを送信しません。

順序どおりの配信機能がイネーブルになっているときに、ポートチャネルリンクの変更が発生した場合、ポートチャネルを経由するフレームは、次のように扱われます。

- 古いパスを使用するフレームが配信されてから、新しいフレームが許可されます。
- ネットワーク遅延ドロップ期間が経過して古いフレームがすべてフラッシュされると、新しいフレームは新しいパス経由で配信されます。

ネットワーク遅延ドロップ期間が経過した時点で、古いパス経由で順序どおりに配信できないフレームはドロップされます。[ドロップ遅延時間の設定, on page 228](#)を参照してください。

順序どおりの配信のイネーブル化の概要

順序どおりの配信機能は、特定の VSAN またはスイッチ全体に対してイネーブルにできます。Cisco MDS 9000 シリーズのスイッチでは、順序どおりの配信はデフォルトで無効になります。



Note IOD 機能を有効または無効にしても、トラフィックは中断されません。



Tip この機能を有効化するのは、順序に従わないフレームを処理できないデバイスがファブリックに接続されている場合に限定してください。Cisco MDS 9000 シリーズのロードバランシングアルゴリズムによって、通常のファブリック処理中に、フレームの順序どおりの配信が保証されます。送信元 FC ID、宛先 FC ID、および交換 ID に基づくロードバランシングアルゴリズムをハードウェアで実行しても、パフォーマンスは低下しません。ただし、ファブリックに障害が発生した場合、順序どおりの配信機能がイネーブルになっていると、ファブリック転送の意図的な一時停止によって、無秩序に転送された可能性のある常駐フレームがファブリックから除去されるため、リカバリが遅延します。

順序どおりの配信のグローバルなイネーブル化

MDS スイッチ上のどの VSAN に対しても、順序どおりの配信パラメータを一様に設定するには、順序どおりの配信をグローバルにイネーブルにします。

順序どおりの配信をグローバルにイネーブルにするのは、ファブリック全体にこの機能が必要な場合だけにしてください。そうでない場合は、この機能を必要とする VSAN に対してだけ IOD をイネーブルにします。



Note Cisco MDS SAN-OS Release 1.3(3) 以前のリリースにダウングレードする際は、事前にスイッチ全体に対する順序どおりの配信をイネーブルにしてください。

スイッチで順序どおりの配信を有効にするには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **in-order-guarantee**

スイッチ内で順序どおりの配信をイネーブルにします。

ステップ 3 switch(config)# **no in-order-guarantee**

スイッチを出荷時の設定に戻し、順序どおりの配信機能をディセーブルにします。

特定の VSAN に対する順序どおりの配信のイネーブル化

VSAN を作成した場合、作成された VSAN には、グローバルな順序保証値が自動的に継承されます。このグローバル値を上書きするには、新しい VSAN の順序保証をイネーブルまたはディセーブルにします。

マルチキャスト ツリー計算に最も小さなドメイン スイッチを使用するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **in-order-guarantee vsan 3452**

VSAN 3452 の順序どおりの配信を有効にします。

ステップ3 switch(config)# no in-order-guarantee vsan 101

スイッチを出荷時の設定に戻し、VSAN 101 の順序どおりの配信機能をディセーブルにします。

順序どおりの配信のステータスの表示

現在の設定ステータスを表示するには、**show in-order-guarantee** コマンドを使用します。

```
switch# show in-order-guarantee
global inorder delivery configuration:guaranteed
VSAN specific settings
vsan 1 inorder delivery:guaranteed
vsan 101 inorder delivery:not guaranteed
vsan 1000 inorder delivery:guaranteed
vsan 1001 inorder delivery:guaranteed
vsan 1682 inorder delivery:guaranteed
vsan 2001 inorder delivery:guaranteed
vsan 2009 inorder delivery:guaranteed
vsan 2456 inorder delivery:guaranteed
vsan 3277 inorder delivery:guaranteed
vsan 3451 inorder delivery:guaranteed
vsan 3452 inorder delivery:guaranteed
```

ドロップ遅延時間の設定

ネットワーク、ネットワーク内の指定された VSAN、またはスイッチ全体のデフォルトの遅延時間を変更できます。

ネットワークおよびスイッチのドロップ遅延時間を設定する手順は、次のとおりです。

ステップ1 switch# configure terminal

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ2 switch(config)# fcdroplateny network 5000

ネットワークのネットワーク ドロップ遅延時間を 5000 ミリ秒に構成します。有効値は 0 ～ 60000 ミリ秒です。デフォルトは 2000 ミリ秒です。

Note ネットワークのドロップ遅延時間は、ネットワーク内の最長パスのすべてのスイッチ遅延の合計として計算する必要があります。

ステップ3 switch(config)# fcdroplateny network 6000 vsan 3

VSAN 3 のネットワーク ドロップ遅延時間を 6000 ミリ秒に構成します。

ステップ4 switch(config)# no fcdroplateny network 4500

現在の fcdroplateny ネットワーク設定 (4500) を削除し、出荷時の初期状態に戻します。

遅延情報の表示

設定された遅延パラメータを表示するには、**show fcdroplateny** コマンドを使用できます ([アドミニストレーティブ ディスタンスの表示, on page 229](#) を参照)。

アドミニストレーティブ ディスタンスの表示

```
switch# show fcdroplateny

switch latency value:500 milliseconds
global network latency value:2000 milliseconds
VSAN specific network latency settings
vsan 1 network latency:5000 milliseconds
vsan 2 network latency:2000 milliseconds
vsan 103 network latency:2000 milliseconds
vsan 460 network latency:500 milliseconds
```

フロー統計情報の設定

フロー統計情報は、集約統計情報テーブル内の入力トラフィックをカウントします。次の2種類の統計情報を収集できます。

- VSAN のトラフィックをカウントする集約フロー統計情報
- VSAN 内の送信元/宛先 ID ペアに対応するトラフィックをカウントするフロー統計情報。

このセクションは、次のトピックで構成されています。

フロー統計の概要

フローカウンタを有効にすると、第1世代のモジュールの集約フロー統計とフロー統計に最大 1000 のエントリ、第2世代のモジュールでは最大 2000 のエントリが使用可能になります。各新フローのモジュールに必ず未使用のフロー インデックスを割り当ててください。フロー インデックスはモジュール全体で繰り返し使用できます。フローインデックスの番号の間は、集約フロー統計情報とフロー統計情報間で共有します。

第1世代のモジュールは、モジュールあたり最大 1024 のフロー ステートメントを許容します。第2世代のモジュールは、モジュールあたり最大 2048 ~ 128 のフロー ステートメントを許容します。



Note 各セッションでは、ローカル接続デバイスでのみ fcflow カウンタが増加します。このカウンタは、イニシエータが接続しているスイッチで設定する必要があります。

集約フロー統計情報のカウント

VSAN の集約フロー統計情報をカウントするには、次の手順を実行します。

-
- ステップ 1** switch# config t
switch(config)#
コンフィギュレーション モードに入ります。
- ステップ 2** switch(config)# fcflow stats aggregated module 1 index 1005 vsan 1
switch(config)#
集約フロー カウンタをイネーブルにします。
- ステップ 3** switch(config)# no fcflow stats aggregated module 1 index 1005 vsan 1
switch(config)#
集約フロー カウンタをディセーブルにします。
-

個々のフロー統計情報のカウント

VSAN 内の送信元および宛先 FC ID のフロー統計情報をカウントするには、次の手順を実行します。

-
- ステップ 1** switch# config t
switch(config)#
コンフィギュレーション モードに入ります。
- ステップ 2** switch(config)# fcflow stats module 1 index 1 0x145601 0x5601ff 0xffffffff vsan 1
switch(config)#
フロー カウンタをイネーブルにします。
- Note** ソース ID および宛先 ID は、16 進形式の FC ID (0x123aff など) で指定します。使用できるマスクは、0xff0000 または 0xffffffff のどちらかです。
- ステップ 3** switch(config)# no fcflow stats aggregated module 2 index 1001 vsan 2
switch(config)#
フロー カウンタをディセーブルにします。
-

FIB 統計情報のクリア

集約フローカウンタをクリアするには、**clear fcflow stats** コマンドを使用します（例 [集約フローカウンタのクリア, on page 231](#) と [送信元 FC ID と宛先 FC ID のフローカウンタのクリア, on page 231](#) を参照）。

集約フローカウンタのクリア

```
switch# clear fcflow stats aggregated module 2 index 1
```

送信元 FC ID と宛先 FC ID のフローカウンタのクリア

```
switch# clear fcflow stats module 2 index 1
```

フロー統計情報の表示

フロー統計情報を表示するには、**show fcflow stats** コマンドを使用します（例 [指定されたモジュールの集約フロー詳細情報の表示, on page 231](#) ～ [指定されたモジュールのフローインデックス使用状況の表示, on page 231](#) を参照）。

指定されたモジュールの集約フロー詳細情報の表示

```
switch# show fcflow stats aggregated module 6
Idx  VSAN  frames      bytes
----  ----  -
1    800   20185860    1211151600
```

指定されたモジュールのフロー詳細情報の表示

```
switch# show fcflow stats module 6
Idx  VSAN  DID      SID      Mask      frames      bytes
----  ----  -
2    800   0x520400 0x530260 0xffffffff 20337793 1220267580
```

指定されたモジュールのフローインデックス使用状況の表示

```
switch# show fcflow stats usage module 6
Configured flows for module 6: 1-2
```

グローバル FSPF 情報の表示

指定した VSAN の FSPF 情報の表示, on page 232 に、特定の VSAN に対するグローバルな FSPF 情報を表示します。

- スイッチのドメイン番号。
- スイッチの自律リージョン。
- Min_LS_arrival : スイッチが LSR 更新を受け入れるまでに経過する必要がある最小時間。
- Min_LS_interval : スイッチが LSR を送信できるまでに経過する必要がある最小時間。



Tip Min_LS_interval が 10 秒よりも長い場合、グレースフルシャットダウン機能が実装されません。

- LS_refresh_time : 更新 LSR 送信間の時間間隔。
- Max_age : LSR が削除されるまでの LSR の最大維持期間。

指定した VSAN の FSPF 情報の表示

```
switch# show fspf vsan 1
FSPF routing for VSAN 1
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 0
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 5000 msec
Local Domain is 0x65(101)
Number of LSRs = 3, Total Checksum = 0x0001288b
Protocol constants :
  LS_REFRESH_TIME = 1800 sec
  MAX_AGE          = 3600 sec
Statistics counters :
  Number of LSR that reached MaxAge = 0
  Number of SPF computations         = 7
  Number of Checksum Errors          = 0
  Number of Transmitted packets :   LSU 65 LSA 55 Hello 474 Retranmsitted LSU 0
  Number of received packets :     LSU 55 LSA 60 Hello 464 Error packets 10
```

FSPF データベースの表示

FSPF データベース情報の表示, on page 233 に、指定された VSAN の FSPF データベースの要約を示します。その他のパラメータを指定しない場合、データベース内のすべての LSR が表示されます。

- LSR タイプ
- LSR 所有者のドメイン ID
- アドバタイジング ルータのドメイン ID
- LSR の経過時間

- LSR を示す番号
- リンク数

LSR 所有者のドメイン ID の追加パラメータを発行して、特定の情報を取得するために表示を絞り込むことができます。各インターフェイスについて、次の情報も確認できます。

- 隣接スイッチのドメイン ID
- E ポート インデックス
- 近接スイッチのポート インデックス
- リンク タイプとコスト

FSPF データベース情報の表示

```
switch# show fspf database vsan 1
FSPF Link State Database for VSAN 1 Domain 0x0c(12)
LSR Type = 1
Advertising domain ID = 0x0c(12)
LSR Age = 1686
LSR Incarnation number = 0x80000024
LSR Checksum = 0x3caf
Number of links = 2
  NbrDomainId      IfIndex      NbrIfIndex      Link Type      Cost
-----
    0x65(101) 0x0000100e    0x00001081          1          500
    0x65(101) 0x0000100f    0x00001080          1          500
FSPF Link State Database for VSAN 1 Domain 0x65(101)
LSR Type = 1
Advertising domain ID = 0x65(101)
LSR Age = 1685
LSR Incarnation number = 0x80000028
LSR Checksum = 0x8443
Number of links = 6
  NbrDomainId      IfIndex      NbrIfIndex      Link Type      Cost
-----
    0xc3(195) 0x00001085    0x00001095          1          500
    0xc3(195) 0x00001086    0x00001096          1          500
    0xc3(195) 0x00001087    0x00001097          1          500
    0xc3(195) 0x00001084    0x00001094          1          500
    0x0c(12) 0x00001081    0x0000100e          1          500
    0x0c(12) 0x00001080    0x0000100f          1          500
FSPF Link State Database for VSAN 1 Domain 0xc3(195)
LSR Type = 1
Advertising domain ID = 0xc3(195)
LSR Age = 1686
LSR Incarnation number = 0x80000033
LSR Checksum = 0x6799
Number of links = 4
  NbrDomainId      IfIndex      NbrIfIndex      Link Type      Cost
-----
    0x65(101) 0x00001095    0x00001085          1          500
    0x65(101) 0x00001096    0x00001086          1          500
    0x65(101) 0x00001097    0x00001087          1          500
    0x65(101) 0x00001094    0x00001084          1          500
```

FSPF インターフェイスの表示

FSPF インターフェイスの情報の表示, on page 234 に、選択された各インターフェイスの次の情報を表示します。

- リンク コスト
- タイマー値
- ネイバーのドメイン ID (既知の場合)
- ローカル インターフェイス番号
- リモート インターフェイス番号(既知の場合)
- インターフェイスの FSPF 状態。
- インターフェイス カウンタ

FSPF インターフェイスの情報の表示

```
switch# show fspf vsan 1 interface fc1/1
FSPF interface fc1/1 in VSAN 1
FSPF routing administrative state is active
Interface cost is 500
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is FULL
Neighbor Domain Id is 0x0c(12), Neighbor Interface index is 0x0f100000
Statistics counters :
  Number of packets received : LSU 8 LSA 8 Hello 118 Error packets 0
  Number of packets transmitted : LSU 8 LSA 8 Hello 119 Retransmitted LSU 0
  Number of times inactivity timer expired for the interface = 0
```

デフォルト設定

Table 21: FSPF のデフォルト設定値, on page 234 に、FSPF 機能のデフォルト設定値を示します。

Table 21: FSPF のデフォルト設定値

パラメータ	デフォルト
FSPF	すべての E ポートおよび TE ポートでイネーブルです。
SPF 計算	ダイナミック
SPF ホールド タイム	0.
バックボーン リージョン	0.
ACK インターバル (RxmtInterval)	5 秒
リフレッシュ タイム (LSRefreshTime)	30 分

パラメータ	デフォルト
最大エージング (MaxAge)	60 分
hello 間隔	20 秒
デッド間隔	80 秒
配信ツリー情報	主要スイッチ (ルート ノード) から取得します。
ルーティング テーブル	FSPF は指定された宛先への等コスト パスを 16 まで格納します。
ロード バランシング	複数の等コスト パスの宛先 ID およびソース ID に基づきます。
順序どおりの配信	ディセーブル
ドロップ遅延	ディセーブル
スタティック ルート コスト	ルートのコスト (メトリック) を指定しない場合、デフォルトは 10 です。
リモート宛先スイッチ	リモート宛先スイッチを指定しない場合、デフォルトは、direct です。
マルチキャスト ルーティング	主要スイッチを使用してマルチキャスト ツリーを計算します。



CHAPTER 8

FLOGI、ネームサーバー、FDMI、および RSCN データベースの管理

この章では、Cisco MDS 9000 ファミリが提供するファブリック ログイン (FLOGI) データベース、ネームサーバー機能、Fabric-Device Management Interface、Registered State Change Notification (RSCN) の情報について説明します。内容は次のとおりです。

- [FLOGIの概要, on page 237](#)
- [ネームサーバー, on page 242](#)
- [FDMI, on page 248](#)
- [FDMI の表示, on page 248](#)
- [VMID \(250 ページ\)](#)
- [RSCN, on page 258](#)
- [デフォルト設定, on page 268](#)
- [ポート ペーシングの有効化, on page 269](#)

FLOGIの概要

ファイバチャネルファブリックでは、ホストまたはディスクごとにファイバチャネル ID が必要です。FLOGI テーブルにストレージデバイスが表示されるかどうかを確認するには、次の項で説明するように **show flogi database** コマンドを使用します。必要なデバイスが FLOGI テーブルに表示されていれば、FLOGI が正常に行われます。ホスト Host Bus Adapter (HBA) および接続ポートに直接接続されているスイッチ上の FLOGI データベースを検査します。

FLOGI スケール最適化

FLOGI スケール最適化機能により、MDS スイッチは、モジュールおよびシャーシに関して増やされた FLOGI の数をサポートできます。FLOGI スケール最適化は、スイッチまたはモジュールのリロード後にデバイスのルーティング情報をプリロードします。これにより、FLOGI 承認にかかる時間が短縮されます。Cisco MDS NX-OS リリース 8.1(1) 以降では、この機能が Cisco MDS 9250i マルチサービス ファブリック スイッチおよび Cisco MDS 9148S 16G マルチレイヤ ファブリック スイッチを除くすべての MDS スイッチでサポートされ、デフォルトで有効にな

ります。Cisco MDS リリース 8.2(2) 以降では、MDS 9718 についてのみ、FLOGI スケールのさらに高い上限がパブリッシュされます。詳細については、FLOGI の制限に関する資料の『[Cisco MDS NX-OS Configuration Limits](#)』を参照してください。

FLOGI 休止タイムアウト

FLOGI 休止タイムアウト機能により、デバイスがファブリックからログアウトしたときやインターフェイスが停止したときに、ルーティング情報やファイバチャネル ネーム サーバーなどの他のファイバチャネルサービス FLOGI プロセスによる通知を遅らせることができます。デバイスが FLOGI 休止タイムアウト値以内にファブリックにログバックすると、他のファイバチャネル サービスに通知されずに FLOGI 承認がただちに返されます。フェールオーバー状態でファブリック内の異なるスイッチにログインすることによって pWWN を異なる時点で共有できるデバイスがファブリック内に存在する場合は、タイムアウト値をゼロに設定することにより、この機能が無効にする必要があります。

[Restrictions (機能制限)]

- FLOGI スケール最適化が有効になっている場合、Cisco MDS NX-OS リリース 8.1(1) からそれ以前のリリースへのダウングレードはサポートされません。ダウングレードの前にこの機能が無効にする必要があります。この機能の無効化の詳細については、「[FLOGI スケール最適化および休止タイムアウトの無効化](#)」の項を参照してください。
- Cisco MDS NX-OS リリース 8.1 およびリリース 8.2 では、デフォルトの FLOGI 休止タイムアウト値は 2000 ミリ秒です。

ただし、Cisco MDS NX-OS リリース 8.3(1) 以降では、デフォルトの FLOGI 休止タイムアウト値が 2000 ミリ秒から 0 ミリ秒に変更されています。設定された FLOGI 休止タイムアウト値はアップグレード時に保持されます。Cisco MDS NX-OS リリース 8.3(1) 以降へのアップグレード時に FLOGI 休止タイムアウト値が設定されていないと、新しいデフォルト値の 0 ミリ秒が使用されます。

- この機能は Cisco MDS 9250i マルチサービス ファブリック スイッチおよび Cisco MDS 9148S 16G マルチレイヤ ファブリック スイッチを除くすべての MDS スイッチでサポートされています。
- この機能では Cisco DCNM および SNMP のサポートを使用できません。
- この機能は、Cisco MDS 24/10 ポート SAN 拡張モジュールのファイバチャネルポートでのみサポートされます。

FLOGI スケール最適化および休止タイムアウトの有効化

FLOGI スケール最適化および休止タイムアウトを有効にするには、次の手順を実行します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
switch# configure terminal
```

ステップ 2 FLOGI スケール最適化を有効にします。

```
switch(config)# flogi scale enable
```

ステップ 3 FLOGI 休止タイムアウト値を設定してデバイス ログイン情報を保持します。

```
switch(config)# flogi quiesce timeout milliseconds
```

デフォルトの FLOGI 休止タイムアウト値については、「[\[Restrictions \(機能制限\)\]](#)」の項を参照してください。

ステップ 4 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。

```
switch(config)# exit
```

ステップ 5 (任意) FLOGI スケール最適化が有効になっていることを確認します。

```
switch# show flogi internal info | i scale
```

```
switch# show flogi internal info | i quiesce
```

例：FLOGI スケール最適化の有効化

次の実行コンフィギュレーションは、FLOGI スケール最適化を有効にして、休止タイムアウト値を 2000 ミリ秒に設定する方法を示しています。

```
configure terminal
flogi scale enable
flogi quiesce timeout 2000
exit
```



(注) FLOGI スケール番号の詳細については、『Cisco MDS NX-OS Configuration Limits』を参照してください。

`show flogi internal info | i scale` コマンドと `show flogi internal info | i quiesce` コマンドからの次の出力例には、FLOGI スケール最適化に関する詳細情報が示されています。

```
switch# show flogi internal info | i scale
Stats: fs_flogi_scale_enabled: 1
switch# show flogi internal info | i quiesce
Stats: fs_flogi_quiesce_timerval: 2000
```

FLOGI スケール最適化および休止タイムアウトの無効化

FLOGI スケール最適化および休止タイムアウトを無効にするには、次の手順を実行します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
switch# configure terminal
```

ステップ 2 FLOGI スケール最適化を無効にします。

```
switch(config)# no flogi scale enable
```

ステップ 3 FLOGI 休止タイムアウト値を 0 に設定します。

```
switch(config)# flogi quiesce timeout 0
```

デフォルトの休止タイムアウト値は 2000 ミリ秒です。

ステップ 4 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。

```
switch(config)# exit
```

ステップ 5 (任意) FLOGI スケール最適化が無効になっていることを確認します。

```
switch# show flogi internal info | i scale
```

```
switch# show flogi internal info | i quiesce
```

例 : FLOGI スケール最適化の無効化

次の実行コンフィギュレーションは、FLOGI スケール最適化を無効にして、休止タイムアウト値を 0 ミリ秒に設定する方法を示しています。

```
configure terminal
no flogi scale enable
flogi quiesce timeout 0
exit
```

show flogi internal info | i scale コマンドと **show flogi internal info | i quiesce** コマンドからの次の出力例には、FLOGI スケール最適化に関する詳細情報が示されています。

```
switch# show flogi internal info | i scale
Stats: fs_flogi_scale_enabled: 0
switch# show flogi internal info | i quiesce
Stats: fs_flogi_quiesce_timerval: 0
```

FLOGI の詳細の表示

FLOGI データベースの詳細を表示するには、`show flogi database` コマンドを使用します。例 [FLOGI データベースの詳細の表示](#) , [on page 241](#) ~ [FC ID 別の FLOGI データベースの表示](#), [on page 241](#) を参照してください。

FLOGI データベースの詳細の表示

```
switch# show flogi database
-----
INTERFACE  VSAN    FCID          PORT NAME          NODE NAME
-----
sup-fc0    2       0xb30100     10:00:00:05:30:00:49:63  20:00:00:05:30:00:49:5e
fc9/13    1       0xb200e2     21:00:00:04:cf:27:25:2c  20:00:00:04:cf:27:25:2c
fc9/13    1       0xb200e1     21:00:00:04:cf:4c:18:61  20:00:00:04:cf:4c:18:61
fc9/13    1       0xb200d1     21:00:00:04:cf:4c:18:64  20:00:00:04:cf:4c:18:64
fc9/13    1       0xb200ce     21:00:00:04:cf:4c:16:fb  20:00:00:04:cf:4c:16:fb
fc9/13    1       0xb200cd     21:00:00:04:cf:4c:18:f7  20:00:00:04:cf:4c:18:f7
Total number of flogi = 6.
```

インターフェイス別の FLOGI データベースの表示

```
switch# show flogi database interface fc1/11
-----
INTERFACE  VSAN    FCID          PORT NAME          NODE NAME
-----
fc1/11    1       0xa002ef     21:00:00:20:37:18:17:d2  20:00:00:20:37:18:17:d2
fc1/11    1       0xa002e8     21:00:00:20:37:38:a7:c1  20:00:00:20:37:38:a7:c1
fc1/11    1       0xa002e4     21:00:00:20:37:6b:d7:18  20:00:00:20:37:6b:d7:18
fc1/11    1       0xa002e2     21:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
fc1/11    1       0xa002e1     21:00:00:20:37:39:90:6a  20:00:00:20:37:39:90:6a
fc1/11    1       0xa002e0     21:00:00:20:37:36:0b:4d  20:00:00:20:37:36:0b:4d
fc1/11    1       0xa002dc     21:00:00:20:37:5a:5b:27  20:00:00:20:37:5a:5b:27
fc1/11    1       0xa002da     21:00:00:20:37:18:6f:90  20:00:00:20:37:18:6f:90
fc1/11    1       0xa002d9     21:00:00:20:37:5b:cf:b9  20:00:00:20:37:5b:cf:b9
fc1/11    1       0xa002d6     21:00:00:20:37:46:78:97  0:00:00:20:37:46:78:97
Total number of flogi = 10.
```

VSAN 別の FLOGI データベースの表示

```
switch# show flogi database vsan 1
-----
INTERFACE  VSAN    FCID          PORT NAME          NODE NAME
-----
fc1/3     1       0xef02ef     22:00:00:20:37:18:17:d2  20:00:00:20:37:18:17:d2
fc1/3     1       0xef02e8     22:00:00:20:37:38:a7:c1  20:00:00:20:37:38:a7:c1
fc1/3     1       0xef02e4     22:00:00:20:37:6b:d7:18  20:00:00:20:37:6b:d7:18
fc1/3     1       0xef02e2     22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
fc1/3     1       0xef02e1     22:00:00:20:37:39:90:6a  20:00:00:20:37:39:90:6a
fc1/3     1       0xef02e0     22:00:00:20:37:36:0b:4d  20:00:00:20:37:36:0b:4d
fc1/3     1       0xef02dc     22:00:00:20:37:5a:5b:27  20:00:00:20:37:5a:5b:27
fc1/3     1       0xef02da     22:00:00:20:37:18:6f:90  20:00:00:20:37:18:6f:90
fc1/3     1       0xef02d9     22:00:00:20:37:5b:cf:b9  20:00:00:20:37:5b:cf:b9
fc1/3     1       0xef02d6     22:00:00:20:37:46:78:97  20:00:00:20:37:46:78:97
Total number of flogi = 10.
```

FC ID 別の FLOGI データベースの表示

```
switch# show flogi database fcid 0xef02e2
-----
```

```

INTERFACE  VSAN      FCID          PORT NAME          NODE NAME
-----
fc1/3      1          0xef02e2     22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
Total number of flogi = 1.

```

詳細については、[デフォルトの企業 ID リスト, on page 350](#)と『*Cisco MDS 9000 Family Troubleshooting Guide*』の「Loop Monitoring」の項を参照してください。

ネーム サーバー

ネーム サーバー機能は、各 VSAN 内のすべてのホストおよびストレージデバイスの属性を含むデータベースを維持します。ネーム サーバーでは、情報を最初に登録したデバイスによるデータベース エントリの変更が認められます。

別のデバイスによって登録済みのデータベース エントリの内容を変更（アップデートまたは削除）する必要がある場合は、プロキシ機能が便利です。

このセクションは、次のトピックで構成されています。

ネーム サーバーから送信される一括通知

Cisco MDS 9000 スイッチでのファイバ チャネル プロトコルのパフォーマンスを向上させるため、ネーム サーバーは1つの MTS ペイロードで複数の通知を送信することで、リモート エントリ 変更通知を最適化します。この MTS 通知を受け取るその他の約 10 個のコンポーネントは、複数の通知ではなく1つの一括通知を処理する必要があります。

ネーム サーバーの一括通知の有効化

NX-OS Release 6.2(1) ~ 6.2(7) では、一括通知はデフォルトでは無効です。1つのスイッチでこの機能を有効にしても、同じファブリック内のその他のスイッチには影響しません。



Note NX-OS Release 6.2(9) 以降では、一括送信はデフォルトで有効です。

[Restrictions (機能制限)]

- DMM、IOA、SME などのインテリジェント アプリケーションが有効な場合は常に、一括通知機能はサポートされません。
- FC リダイレクトの設定は、一括通知機能と常に競合します。



Note 前述の制約はリリース 6.2.7 のみに適用されます。

ネーム サーバーの一括通知を有効にするには、NX-OS Release 6.2(1) ~ 6.2(7) で次の手順を実行します。

ステップ 1 switch# **config t**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fcns bulk-notify**

switch(config)#

1 つの Messaging and Transaction Services (MTS) ペイロードでの複数ネーム サーバー エントリ変更通知の送信を有効にします。

ネーム サーバーの一括通知の無効化

ネーム サーバーの一括通知を無効にするには、NX-OS Release 6.2(1) ~ 6.2(7) で次の手順を実行します。

ステップ 1 switch# **config t**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **no fcns bulk-notify**

switch(config)#

1 つの Messaging and Transaction Services (MTS) ペイロードでの複数ネーム サーバー エントリ変更通知の送信を無効にします。

NX-OS リリース 6.2(9) のネーム サーバー一括通知の無効化

ネーム サーバーの一括通知を無効にするには、NX-OS Release 6.2(9) 以降で次の手順を実行します。

ステップ 1 switch# **config t**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fcns no-bulk-notify**

switch(config)#

1 つの Messaging and Transaction Services (MTS) ペイロードでの複数ネーム サーバー エントリ変更通知の送信を無効にします。

ネーム サーバーの一括通知の再有効化

NX-OS Release 6.2(9) 以降ですでに無効にした設定を再度有効にするには、次の手順を実行します。

ステップ 1 switch# **config terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **no fcns no-bulk-notify**

switch(config)#

1 つの Messaging and Transaction Services (MTS) ペイロードでの複数ネーム サーバー エントリ変更通知の送信を再び有効にします。

ネーム サーバー プロキシ登録

ネーム サーバー登録要求はすべて、パラメータが登録または変更されたポートと同じポートから送信されます。そのポートにパラメータがないと、要求は拒否されます。

この許可を使用すると、WWN が他のノードに代わって特定のパラメータを登録できるようになります。

ネーム サーバー プロキシの登録

ネーム サーバー プロキシを登録するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fcns proxy-port 21:00:00:e0:8b:00:26:d0 vsan 2**

指定した VSAN のプロキシ ポートを設定します。

重複 pWWN の拒否の概要

FC 標準では、NX-OS は同一スイッチ、同一 VSAN、および同一 FC ドメインですでにログインしている pWWN の任意のインターフェイスでのログインを受け入れません。同じ pWWN が、異なるインターフェイスで同じスイッチにログインしないようにするには、ポートセキュリティ機能を使用します。

デフォルトでは、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて拒否され、以前の FLOGI が維持されます。これは FC 標準に準拠していません。このオプションを無効にすると、以前の FCNS エントリを削除することで、同一 VSAN の異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて許可されます。

重複 pWWN の拒否

重複 pWWN を拒否するには、次の手順を実行します。

ステップ 1 switch# configure terminal

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# fcns reject-duplicate-pwwn vsan 1

異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて拒否され、以前の FLOGI が維持されます。（デフォルト）

ステップ 3 switch(config)# no fcns reject-duplicate-pwwn vsan 1

以前の FLOGI エントリを削除することで、異なるスイッチでの（重複する pWWN による）今後の FLOGI はすべて許可されます。

ただし、他のスイッチの FLOGI データベースには以前のエンタリがまだ含まれています。

ネーム サーバー データベース エントリ

ネーム サーバーはすべてのホストのネーム エントリを FCNS データベースに保管しています。ネーム サーバーは、Nx ポートが他のホストの属性を取得するために（ネーム サーバーへの）FLOGI を実行するときに、Nx ポートによる属性の登録を許可します。Nx ポートが明示的または暗黙的にログアウトする時点で、これらの属性は登録解除されます。

マルチスイッチ ファブリック構成では、各スイッチ上で稼働するネーム サーバー インスタンスが分散型データベースで情報を共有します。スイッチごとに 1 つのネーム サーバー プロセスのインスタンスが実行されます。

ネーム サーバーのデータベース同期の最適化

エンドデバイスが FC4 機能をネーム サーバー データベースに登録しない場合、VHBA（scsi-target と呼ばれる）コンポーネントがエンドデバイスに対して PRLI を実行し、FC4 機能を検出し、エンドデバイスの代理でネーム サーバーに登録します。VHBA からのこの検出は、ローカル接続デバイスと

リモート接続デバイスの両方に対して実行されています。リモート接続デバイスに対してこの検出を実行する必要はありません。これは、ネーム サーバーは標準ネーム サーバー同期プロトコルを使用してリモート接続デバイスのFC4機能を取得するためです。したがって、ローカル接続デバイスだけを検出するように、VHBA コンポーネントのデフォルトの動作が変更されました。この動作を変更するには、次の手順を実行します。

ステップ 1 switch(config)# scsi-target discovery

スイッチが、リモート デバイスの fc-4 機能も

検出できるようにします。ただしこれは、

ユーザーがスイッチをリロードするか、またはスイッチをスイッチオーバーする場合のデフォルトの動作ではありません。

ステップ 2 switch(config)# scsi-target discovery local-only

デフォルトの動作に戻ります。

ネーム サーバー データベースのエントリ数の確認

ネーム サーバー データベースのエントリ数を確認するには、次の手順に従います。

ステップ 1 switch# show fcns internal info global

ネーム サーバー データベースのデバイス エントリの数を表示します。

ステップ 2 switch# show fcns internal info

出力の終わりに、ネーム サーバー データベースのデバイスの数を表示します。

ネーム サーバーのデータベース エントリの表示

指定した VSAN またはすべての VSAN のネーム サーバーのデータベースおよび統計情報を表示するには、**show fcns** コマンドを使用します（例 [ネーム サーバー データベースの表示, on page 246](#) ~ [ネーム サーバー統計情報の表示, on page 248](#) を参照）。

ネーム サーバー データベースの表示

```
switch# show fcns database
-----
FCID          TYPE  PWWN                               (VENDOR)          FC4-TYPE:FEATURE
-----
0x010000     N     50:06:0b:00:00:10:a7:80           scsi-fcp fc-gs
```

```

0x010001  N    10:00:00:05:30:00:24:63 (Cisco)          ipfc
0x010002  N    50:06:04:82:c3:a0:98:52 (Company 1)     scsi-fcp 250
0x010100  N    21:00:00:e0:8b:02:99:36 (Company A)     scsi-fcp
0x020000  N    21:00:00:e0:8b:08:4b:20 (Company A)
0x020100  N    10:00:00:05:30:00:24:23 (Cisco)          ipfc
0x020200  N    21:01:00:e0:8b:22:99:36 (Company A)     scsi-fcp

```

指定した VSAN のネーム サーバー データベースの表示

```

switch# show fcns database vsan 1
VSAN 1:
-----
FCID          TYPE  PWWN                               (VENDOR)          FC4-TYPE:FEATURE
-----
0x030001     N    10:00:00:05:30:00:25:a3 (Cisco)          ipfc
0x030101     NL   10:00:00:00:77:99:60:2c (Interphase)
0x030200     N    10:00:00:49:c9:28:c7:01
0xec0001     NL   21:00:00:20:37:a6:be:14 (Seagate)       scsi-fcp
Total number of entries = 4

```

ネーム サーバー データベースの詳細の表示

```

switch# show fcns database detail
-----
VSAN:1      FCID:0x030001
-----
port-wwn (vendor)      :10:00:00:05:30:00:25:a3 (Cisco)
node-wwn               :20:00:00:05:30:00:25:9e
class                  :2,3
node-ip-addr           :0.0.0.0
ipa                    :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:ipfc
symbolic-port-name     :
symbolic-node-name     :
port-type              :N
port-ip-addr           :0.0.0.0
fabric-port-wwn       :00:00:00:00:00:00:00:00
hard-addr              :0x000000
-----
VSAN:1      FCID:0xec0200
-----
port-wwn (vendor)      :10:00:00:5a:c9:28:c7:01
node-wwn               :10:00:00:5a:c9:28:c7:01
class                  :3
node-ip-addr           :0.0.0.0
ipa                    :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:
symbolic-port-name     :
symbolic-node-name     :
port-type              :N
port-ip-addr           :0.0.0.0
fabric-port-wwn       :22:0a:00:05:30:00:26:1e
hard-addr              :0x000000
Total number of entries = 2

```

ネームサーバー統計情報の表示

```
switch# show fcns statistics

registration requests received = 27
deregistration requests received = 0
queries received = 57
queries sent = 10
reject responses sent = 14
RSCNs received = 0
RSCNs sent = 0
```

FDMI

Cisco MDS 9000 ファミリースイッチでは、FC-GS-4 規格に記述されている FDMI 機能がサポートされます。FDMI を使用すると、ファイバチャネル HBA などのデバイスをインバンド通信によって管理できます。この機能を追加することにより、既存のファイバチャネルネームサーバーおよび管理サーバーの機能を補完します。

FDMI機能を使用すると、独自のホストエージェントをインストールしなくても、Cisco NX-OS ソフトウェアは接続先 HBA およびホスト OS（オペレーティングシステム）に関する次の管理情報を抽出できます。

- 製造元、モデル、およびシリアル番号
- ノード名およびノードのシンボリック名
- ハードウェア、ドライバ、およびファームウェアのバージョン
- ホストオペレーティングシステム（OS）の名前およびバージョン番号

FDMI エントリはすべて永続ストレージに保存され、FDMI プロセスを起動した時点で取り出されます。

FDMI の表示

FDMI データベース情報を表示するには、**show fDMI** コマンドを使用します（例 [すべての HBA 管理サーバーの表示, on page 248](#) ~ [指定された HBA エントリの詳細の表示, on page 250](#) を参照）。

すべての HBA 管理サーバーの表示

```
switch# show fDMI database
Registered HBA List for VSAN 1
  10:00:00:00:c9:32:8d:77
  21:01:00:e0:8b:2a:f6:54
switch# show fDMI database detail
Registered HBA List for VSAN 1
-----
HBA-ID: 10:00:00:00:c9:32:8d:77
```



```

-----
Node Name          :20:00:00:00:c9:32:8d:77
Manufacturer       :Emulex Corporation
Serial Num         :0000c9328d77
Model              :LP9002
Model Description  :Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver       :2002606D
Driver Ver         :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver           :3.11A0
Firmware Ver       :3.90A7
OS Name/Ver        :Window 2000
CT Payload Len     :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
-----
HBA-ID: 21:01:00:e0:8b:2a:f6:54
-----
Node Name          :20:01:00:e0:8b:2a:f6:54
Manufacturer       :QLogic Corporation
Serial Num         :\74262
Model              :QLA2342
Model Description  :QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver       :FC5010409-10
Driver Ver         :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver           :1.24
Firmware Ver       :03.02.13.
OS Name/Ver        :500
CT Payload Len     :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54

```

指定された VSAN の HBA の詳細の表示

```

switch# show fDMI database detail vsan 1
Registered HBA List for VSAN 1
-----
HBA-ID: 10:00:00:00:c9:32:8d:77
-----
Node Name          :20:00:00:00:c9:32:8d:77
Manufacturer       :Emulex Corporation
Serial Num         :0000c9328d77
Model              :LP9002
Model Description  :Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver       :2002606D
Driver Ver         :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver           :3.11A0
Firmware Ver       :3.90A7
OS Name/Ver        :Window 2000
CT Payload Len     :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
-----
HBA-ID: 21:01:00:e0:8b:2a:f6:54
-----
Node Name          :20:01:00:e0:8b:2a:f6:54
Manufacturer       :QLogic Corporation
Serial Num         :\74262
Model              :QLA2342
Model Description  :QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver       :FC5010409-10
Driver Ver         :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver           :1.24
Firmware Ver       :03.02.13.
OS Name/Ver        :500

```

```
CT Payload Len :2040
Port-id: 21:01:00:e0:8b:2a:f6:54
```

指定された HBA エントリの詳細の表示

```
switch# show fDMI database detail hba-id 21:01:00:e0:8b:2a:f6:54 vsan 1
Node Name          :20:01:00:e0:8b:2a:f6:54
Manufacturer       :QLogic Corporation
Serial Num         :\74262
Model              :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver       :FC5010409-10
Driver Ver         :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver           :1.24
Firmware Ver       :03.02.13.
OS Name/Ver        :500
CT Payload Len     :2040
Port-id: 21:01:00:e0:8b:2a:f6:54
```

VMID



- (注) VMID 機能は現在、実稼働環境以外でのみ使用するためのプレビュー（ベータ）状態です。このプレビュー（ベータ）ステータスと制限は、今後のリリースで通常の製品ステータスに変更されます。

スイッチベースの仮想マシン識別子（VMID）機能により、SAN ファブリックインフラストラクチャによって個々の仮想マシン（VM）レベルでトラフィック送信元を識別することが可能になります。

MDS スイッチの VMID は、ホストハイパーバイザにさまざまな識別子を提供します。その後、これらの識別子は、ハイパーバイザによってローカル VM に割り当てられます。識別子に割り当てられた VM に関する補足情報がスイッチにレポートされます。その後、ハイパーバイザによって VM からのトラフィックの CS_CTL フィールドに識別子が挿入され、SAN ファブリックによるトラフィック送信元の識別が可能になります。

VMID 機能では次の ID が使用されます。

- 仮想エンティティ（VE）：任意の仮想デバイスを指します。
- 仮想エンティティ マネージャ（VEM）：ハイパーバイザを指します。
- 仮想エンティティ 識別子（VE ID）：VE に割り当てられるさまざまなタイプの識別子を指します。次の 4 つのタイプの VE ID があります。
 - ローカル VE ID：ローカル VE ID は、VEM N_Port 内の VE を一意に識別するために使用されます。ローカル VE ID は、仮想マシンの起動時、停止時、または VEM 間の移行時に変更されます。

- **ファブリック VE ID** : ファブリック VE ID は、ファブリック内の VE を一意に識別するために使用されます。これは VEM N_Port FCID とローカル VE ID の組み合わせです。
 - **グローバル VE ID** : グローバル VE ID は VE を一意に識別するために使用される 16 バイトの汎用一意識別子 (UUID) です。グローバル VE ID は、SAN ファブリックの外部のサービス (VM 管理プラットフォームなど) によって割り当てられます。グローバル VE ID が割り当てられると、期限切れにはなりません。
 - **VEM ID** : VEM ID は VEM を一意に識別するために使用される 16 バイトの UUID です。VEM ID は、SAN ファブリックの外部のサービス (VM 管理プラットフォームなど) によって割り当てられます。
- **VEM のファブリック ポート** は、次の N_Port で構成されます。
 - **物理ネットワーク ポート (PN_Port)** : ハイパーバイザ ホスト バス アダプタ (HBA) の物理ネットワーク ポートです。
 - **仮想ネットワーク ポート (VN_Port)** : 一連の VE で共有できるオプションの仮想ネットワーク ポートです。PN_Port は複数の VN_Port を持つことができます。各 VN ポートには固有の FCID が割り当てられます。
 - **物理ファブリック ポート (PF_Port)** : スイッチの物理ファブリック ポートです。

HBA ポートの起動時

HBA ドライバによって物理または仮想 HBA ポートがファブリックにログインすると、ドライバはポートを介してファブリックからのローカル VE ID を要求する場合があります。ローカル接続されたスイッチ上の仮想マシン識別サーバー (VMIS) は、応答でローカル VE ID の範囲 (最大 255) を提供します。その後、ドライバはポートの FCID に識別子を割り当てます。

VM のディスクへの初期アクセス時

ファブリックの外部では、VM はグローバル VE ID によって識別されます。ファブリック内では、VM はファブリック VE ID によって識別されます。VM が初めて仮想ディスクにアクセスすると、ハイパーバイザは HBA ポートを介して対応する物理ディスクへのアクセスを開始します。物理ディスクへのパスごとに、FCID のプールからの未使用のローカル VE ID が割り当てられます。FCID とローカル VE ID を組み合わせて、HBA ドライバによって一意のファブリック VE ID が作成されます。その後、HBA ドライバは、ローカル接続された VMIS に、割り当てられた VE ID のグローバル VE ID へのマッピングについて通知します。このマッピングは、ハイパーバイザを経由するファブリックへの VM パスごとに実行され、すべての VM トラフィックを SAN ツール (Cisco MDS SAN Analytics など) がパス別に識別することを可能にします。

VM の停止時またはファブリック内での移行時

グローバル VE ID とローカル VE ID の違いは、VM が VEM 間を移行するときに見られます。VM がインスタンス化を解除されるか VEM 間で移行されると、ローカル VE ID が HBA ドライバによってプールに返されますが、スイッチ VMIS には通知されません。1~4 時間にわたってトラフィックがないと、スイッチによりローカル VE ID または VM マッピングがタイムアウト

トになります。VM が同じ VEM で再インスタンス化されると、以前に割り当てられたローカル VE ID がこの VM の停止時に別の VM に割り当てられている可能性があるため、VM は同じ FCID のプールから異なるローカル VE ID を取得することがあります。VM が別の VEM に移行すると、その VM には異なる FCID が使用される可能性があり、FCID のプールとは異なるローカル VE ID が割り当てられる可能性があります。そのため、VM が再起動したり VEM 間で移行すると、グローバル VE ID は変わりませんが、ローカル VE ID は変更される可能性があります。

図 53 : VMID の構成要素 (252 ページ) に、VMID の構成要素を示します。

図 53 : VMID の構成要素

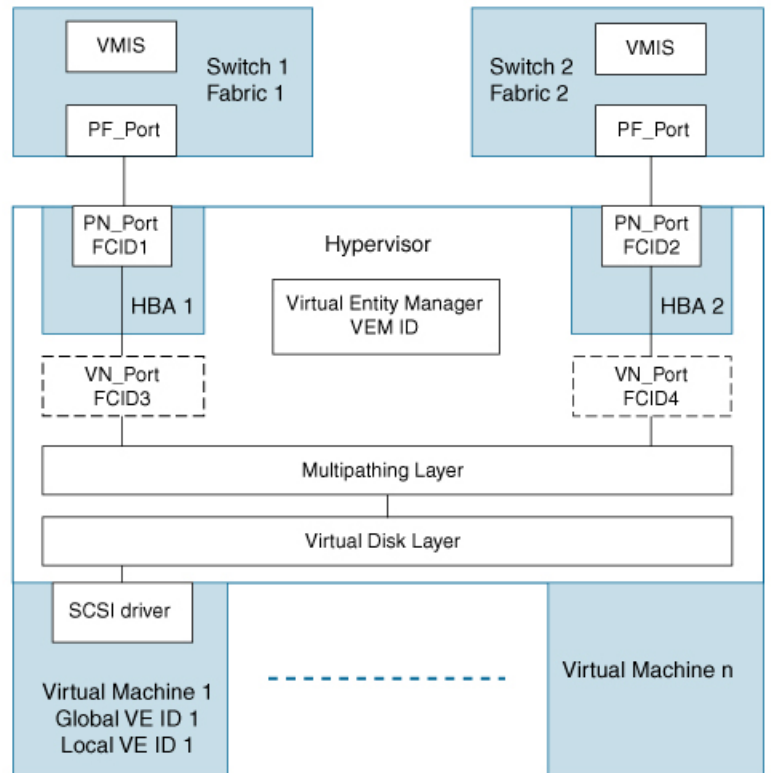
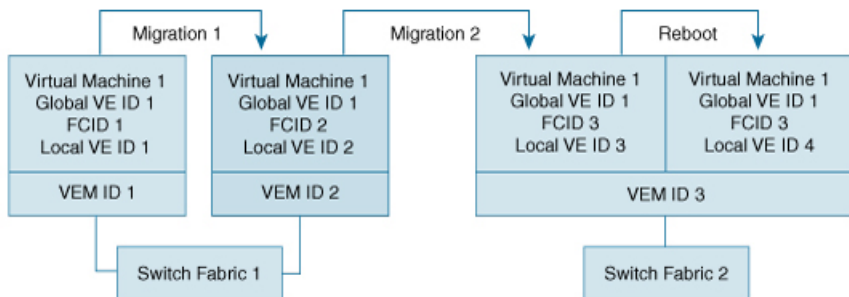


図 54 : VE ID ライフ サイクル (253 ページ) は、VM ライフ サイクル中に VE ID を変更する方法を示しています。

図 54: VE ID ライフ サイクル



365325

VMID に関する注意事項と制約事項

- VMID 機能は、Cisco N-Port Virtualizer (Cisco NPV) スイッチではサポートされていません。
- VMID プロトコルには、接続されたハイパーバイザ HBA ドライバクライアントに新しい VE ID 範囲を通知するメカニズムはありません。クライアントが新しい範囲を検出するには、VMIS へのクエリをもう一度実行する必要があります。範囲の変更後にクライアントにもう一度クエリを実行させるには、手動で FCID をログアウトしてファブリックに戻す必要があります。その結果、ローカルクライアントは、これが発生するまで、VM トラフィックを以前の範囲で引き続きタグ付けします。この制限事項は、VMID を有効または無効にする場合と VSAN の VE ID 範囲を変更する場合に適用されます。
- Extended Receiver Ready (ER_RDY) 機能は、CSCTL 1 ~ 15 を使用します。VMID 機能は、CSCTL 16 ~ 255 を使用します。VMID データベースに VMIS の範囲 1 ~ 15 で構成されているインターフェイスがある場合、および Cisco MDS NX-OS リリース 9.2(1) 以降のリリースにアップグレードする場合は、範囲を 16 ~ 255 に変更し、アップグレードする前にインターフェイスをフラップします。
- VMID 機能は、相互運用性が有効になっている VSAN ではサポートされません。相互運用性モードの詳細については、『[Cisco MDS 9000 Series Switch-to-Switch Interoperability Configuration Guide](#)』を参照してください。

VMID サーバーの構成

VMID サーバーの有効化

VMID サーバーの機能を有効にするには、次の手順を実行します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
switch# configure terminal
```

ステップ 2 VMID サーバーの機能を有効にします。

```
switch(config)# feature vmis
```

VMID サーバーの無効化

VMID サーバーの機能を無効にするには、次の手順を実行します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
switch# configure terminal
```

ステップ 2 VMID サーバーの機能を無効にします。

```
switch(config)# no feature vmis
```

VMID の範囲の設定

VMID の範囲は、HBA ドライバが使用するローカル VE ID を制限するために使用されます。CS_CTL フィールドのビットのサブセットを使用するようにローカル VE ID の範囲を制限することにより、それをパーティション化して将来のファイバチャネル機能と共有することができます。

VMID の範囲を設定するには、次の手順を実行します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
switch# configure terminal
```

ステップ 2 VSAN 内で使用する VE ID の範囲を設定します。

```
switch(config)# vmis range range vsan id
```

例：VMID サーバーの構成

次の例は、VMID サーバー機能を有効化する方法を示します。

```
switch# configure terminal
switch(config)# feature vmis
```

次の例は、VMID サーバー機能を無効化する方法を示します。

```
switch# configure terminal
switch(config)# no feature vmis
```

次の例は、VSAN 内のハイパーバイザ HBA ドライバが使用するために複数のローカル VE ID の範囲を設定する方法を示しています。

```
switch# configure terminal
switch(config)# vmis range 3-45,51-70 vsan 1
```

VMID 設定の確認

この例は、VMID サーバー機能を使用できる FCID を示しています。**FLAGS** フィールドの下の文字 *M* は、対応する FCID が VMID サーバー機能を使用できることを示しています。

```
switch# show flogi database details
```

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME	FLAGS
fc1/7	1	0xef0000	20:07:8c:60:4f:10:0f:e0	20:01:8c:60:4f:10:0f:e1	P
fc1/7	1	0xef0001	20:19:8c:60:4f:19:bf:25	21:00:00:20:38:de:c3:9f	VPM

```
Total number of flogi = 2.
```

この例は、VMIS データベースのすべてのエントリを示しています。これは、SAN ファブリック内のすべての ID のデータベースです。ローカル接続された ID は接続インターフェイスを示し、リモート接続された ID は出力で「--」というインターフェイス名を示します。

```
switch# show vmis database
Total 17 entries
```

INTERFACE	VSAN	FCID	LOCAL VEID	GLOBAL VEID
fc1/7	1	0xef000a	0x01	9a07686b-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x02	66fb6a4e-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x03	325de425-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x04	0d509b51-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x05	b7d71b43-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x32	1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x01	e8e9161f-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x02	e7cd9011-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x03	8d43ef66-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x04	760f0e14-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x05	5a255233-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x1e	1b231602-0405-0607-0809-0a0b0c0d0e0f
--	10	0x4c0020	0x1e	ba581b3d-0405-0607-0809-0a0b0c0d0e0f
--	10	0x4c0020	0x1f	abd77e50-0405-0607-0809-0a0b0c0d0e0f
--	10	0x4c0020	0x20	f241b12e-0405-0607-0809-0a0b0c0d0e0f
--	10	0x4c0020	0x21	fb1eb741-0405-0607-0809-0a0b0c0d0e0f
--	10	0x4c0020	0x22	e3a9e279-0405-0607-0809-0a0b0c0d0e0f

この例は、指定されたローカル VSAN ドメインの VMIS データベースエントリを示しています。

```
switch# show vmis database local vsan 1
Total 12 entries
```

INTERFACE	VSAN	FCID	LOCAL VEID	GLOBAL VEID
fc1/7	1	0xef000a	0x01	9a07686b-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x02	66fb6a4e-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x03	325de425-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x04	0d509b51-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x05	b7d71b43-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x32	1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x01	e8e9161f-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x02	e7cd9011-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x03	8d43ef66-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x04	760f0e14-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x05	5a255233-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x1e	1b231602-0405-0607-0809-0a0b0c0d0e0f

この例は、ホスティング ドメインによってフィルタリングされた VSAN 内のエントリを示しています。

```
switch# show vmis database domain 0xef vsan 1
Total 12 entries
```

INTERFACE	VSAN	FCID	LOCAL VEID	GLOBAL VEID
fc1/7	1	0xef000a	0x01	9a07686b-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x02	66fb6a4e-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x03	325de425-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x04	0d509b51-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x05	b7d71b43-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x32	1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x01	e8e9161f-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x02	e7cd9011-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x03	8d43ef66-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x04	760f0e14-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x05	5a255233-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x1e	1b231602-0405-0607-0809-0a0b0c0d0e0f

この例は、インターフェイスによってフィルタリングされた VSAN 内のエントリを示しています。

```
switch# show vmis database interface fc1/7 vsan 1
Total 12 entries
```

INTERFACE	VSAN	FCID	LOCAL VEID	GLOBAL VEID
fc1/7	1	0xef000a	0x01	9a07686b-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x02	66fb6a4e-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x03	325de425-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x04	0d509b51-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x05	b7d71b43-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000a	0x32	1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x01	e8e9161f-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x02	e7cd9011-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x03	8d43ef66-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x04	760f0e14-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x05	5a255233-0405-0607-0809-0a0b0c0d0e0f
fc1/7	1	0xef000b	0x1e	1b231602-0405-0607-0809-0a0b0c0d0e0f

この例は、VSAN 内のエントリを示しています。


```
switch# show vmis database vsan 10
Total 5 entries
-----
INTERFACE          VSAN  FCID      LOCAL VEID      GLOBAL VEID
-----
--                  10    0x4c0020  0x1e            ba581b3d-0405-0607-0809-0a0b0c0d0e0f
--                  10    0x4c0020  0x1f            abd77e50-0405-0607-0809-0a0b0c0d0e0f
--                  10    0x4c0020  0x20            f241b12e-0405-0607-0809-0a0b0c0d0e0f
--                  10    0x4c0020  0x21            fb1eb741-0405-0607-0809-0a0b0c0d0e0f
--                  10    0x4c0020  0x22            e3a9e279-0405-0607-0809-0a0b0c0d0e0f
```

この例は、FCIDによってフィルタリングされたエントリを示しています。この例は、リモートハイパーバイザのN_Port FCIDによってフィルタリングされています。

```
switch# show vmis database fcid 0x4c0020 vsan 10
Total 5 entries
-----
INTERFACE          VSAN  FCID      LOCAL VEID      GLOBAL VEID
-----
--                  10    0x4c0020  0x1e            ba581b3d-0405-0607-0809-0a0b0c0d0e0f
--                  10    0x4c0020  0x1f            abd77e50-0405-0607-0809-0a0b0c0d0e0f
--                  10    0x4c0020  0x20            f241b12e-0405-0607-0809-0a0b0c0d0e0f
--                  10    0x4c0020  0x21            fb1eb741-0405-0607-0809-0a0b0c0d0e0f
--                  10    0x4c0020  0x22            e3a9e279-0405-0607-0809-0a0b0c0d0e0f
```

この例は、グローバル VM ID と VSAN によってフィルタリングされた VMIS エントリを示しています。

```
switch# show vmis database global-vmid e8e9161f-0405-0607-0809-0a0b0c0d0e0f vsan 1
Total 1 entries
-----
INTERFACE          VSAN  FCID      LOCAL VEID      GLOBAL VEID
-----
fc1/7              1     0xef000b  0x01            e8e9161f-0405-0607-0809-0a0b0c0d0e0f
```

この例は、VSAN に登録されている VEM ID を示しています。

```
switch# show vmis database vem vsan 1
Total 2 entries
-----
INTERFACE          VSAN  FCID      LOCAL VEID      VEM ID
-----
fc1/7              1     0xef000a  11223344-5566-7788-99aa-bbccddeeffaa
fc1/7              1     0xef000b  00010203-0405-0607-0809-0a0b0cef000b
```

この例は、VEM 間で移行された VM エントリを示しています。

出力には、VM が VEM 間で移行される前と後の VM に対応する 2 つのエントリが示されています。移行前に VM に関連付けられていた ID は、すぐには削除されません。これらの ID は、スイッチの I/O タイマーが期限切れになると VMIS データベースで削除されます。I/O タイマーが期限切れになるまでは、VMIS データベースに同じ VM の 2 つのエントリが表示されます。

```
switch# show vmis database vmotion vsan 1
Total 2 entries
```

```
-----
INTERFACE          VSAN  FCID      LOCAL VEID      GLOBAL VEID
-----
fc1/7              1      0xef000b  0x1e            1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7              1      0xef000a  0x32            1b231602-0405-0607-0809-0a0b0c0d0e0f
-----
```

この例は、各 VSAN に設定されているローカル VE ID の範囲を示しています。

```
switch# show vmis range
VSAN      VEID Range
-----
1         1-255
10        1-255
20        1-255
30        1-255
```

この例は、VSAN によって、ローカル接続されたハイパーバイザ HBA ドライバクライアント（ホスト側）およびファブリック内の他のスイッチ上の他の VMIS エージェント（スイッチ側）と交換されるローカルスイッチの VMIS の統計情報を示しています。

```
switch# show vmis statistics
VSAN : 1
-----Host Side-----
qfpa/qfpa_rsp/qfpa_rjt : 1/1/0
uvem/uvem_rsp/uvem_rjt : 1/1/0
ggvid/ggvid_rsp/ggvid_rjt : 0/0/0
gfvid/gfvid_rsp/gfvid_rjt : 0/0/0
gvemid/gvemid_rsp/gvemid_rjt : 0/0/0
gvem/gvem_rsp/gvem_rjt : 0/0/0

-----Switch Side-----
gvemd_tx/gvemd_rsp_tx/gvemd_rjt_tx : 0/0/0
gvemd_rx/gvemd_rsp_rx/gvemd_rjt_rx : 0/0/0
uvemd_tx/uvemd_rsp_tx/uvemd_rjt_tx : 0/0/0
uvemd_rx/uvemd_rsp_rx/uvemd_rjt_rx : 0/0/0
```

RSCN

Registered State Change Notification (RSCN) は、ファブリック内で行われた変更について各ホストに通知するためのファイバチャネルサービスです。ホストは (SCR を通じて) ファブリックコントローラに登録することにより、この情報を受信できます。次のいずれかのイベントが発生した場合、適宜通知されます。

- ファブリックへのディスクの追加または削除
- ネーム サーバーの登録内容の変更
- 新しいゾーンの適用
- IP アドレスの変更
- ホストの動作に影響するその他の同様なイベント

このセクションは、次のトピックで構成されています。

RSCN 情報の概要

登録先ホストにこれらのイベントを送信するだけでなく、スイッチ RSCN (SW-RSCN) がファブリック内のすべての到達可能なスイッチに送信されます。



Note スイッチは RSCN を送信して、登録済みのノードに変更が発生したことを通知します。ネームサーバーに再度クエリを発行して新しい情報を取得するのは、各ノードの責任範囲です。スイッチが各ノードに送信する RSCN には、変更に関する詳細情報は含まれていません。

RSCN 情報の表示

RSCN 情報を表示するには、**show rscn** コマンドを使用します (例 [登録デバイス情報の表示, on page 259](#) および [RSCN のカウンタ情報の表示, on page 259](#) を参照)。

登録デバイス情報の表示

```
switch# show rscn scr-table vsan 1
SCR table for VSAN: 1
-----
FC-ID          REGISTERED FOR
-----
0x1b0300      fabric detected rscns
Total number of entries = 1
```



Note SCR テーブルは設定不可能です。ホストが RSCN 情報と一緒に SCR フレームを送信する場合にかぎり、入力されます。ホストが RSCN 情報を受信しない場合、**show rscn scr-table** コマンドはエントリを返しません。

RSCN のカウンタ情報の表示

```
switch(config)# show rscn statistics vsan 106
Statistics for VSAN: 106
-----
Number of SCR received           = 0
Number of SCR ACC sent           = 0
Number of SCR RJT sent           = 0
Number of RSCN received          = 0
Number of RSCN sent              = 0
Number of RSCN ACC received      = 0
Number of RSCN ACC sent          = 0
Number of RSCN RJT received      = 0
Number of RSCN RJT sent          = 0
Number of SW-RSCN received       = 0
Number of SW-RSCN sent           = 0
```

```

Number of SW-RSCN ACC received = 0
Number of SW-RSCN ACC sent     = 0
Number of SW-RSCN RJT received = 0
Number of SW-RSCN RJT sent     = 0
Number of CSWR received        = 3137
Number of CSWR sent            = 0
Number of CSWR ACC received    = 0
Number of CSWR ACC sent        = 3137
Number of CSWR RJT received    = 0
Number of CSWR RJT sent        = 0
Number of CSWR RJT not sent    = 0

```

multi-pid オプション

RSCN の **multi-pid** オプションをイネーブルに設定すると、登録済み Nx ポートに対して生成される RSCN に、影響を受けた複数のポート ID が含まれる場合があります。この場合、ゾーン分割ルールを適用してから、影響を受けた複数のポート ID が 1 つの RSCN にまとめられます。このオプションをイネーブルにすることによって、RSCN の数を減らすことができます。たとえば、2 つのディスク (D1 と D2) およびホスト (H) がスイッチ 1 に接続されているとします。ホスト H は、RSCN を受信するように登録済みです。D1、D2、および H は同じゾーンに属します。ディスク D1 および D2 が同時にオンラインになると、次のいずれかの処理が適用されます。

- スイッチ 1 で **multi-pid** オプションがディセーブルになります。ホスト H に対して 2 つの RSCN が生成されます (1 つはディスク D1 用、もう 1 つはディスク D2 用)。
- スイッチ 1 で **multi-pid** オプションがイネーブルになります。ホスト H に対して RSCN が 1 つ生成され、RSCN ペイロードによって関連ポート ID がリストされます (この場合は D1 および D2)。



Note 一部の Nx ポートでは、multi-pid RSCN ペイロードをサポートできないことがあります。その場合は、RSCN の **multi-pid** オプションを無効にしてください。

multi-pid オプションの設定

multi-pid オプションを設定するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **rscn multi-pid vsan 105**

VSAN 105 の RSCN を multi-pid フォーマットで送信します。

ドメインフォーマット SW-RSCN の抑制

ドメインフォーマット SW-RSCN は、ローカル スイッチ名またはローカル スイッチ管理 IP アドレスが変更されるとすぐに送信されます。この SW-RSCN は、ISL を介して、他のすべてのドメインおよびスイッチに送信されます。リモート スイッチから、ドメインフォーマット SW-RSCN を開始したスイッチに対して GMAL コマンドおよび GIELN コマンドを発行すると、変更内容を判別できます。ドメインフォーマット SW-RSCN によって、一部の他社製の MDS スイッチで問題が発生することがあります（を参照）。

これらの SW-RSCN の ISL を介した送信を抑制するには、次の手順を実行します。

ステップ 1 switch# config terminal

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# rscn suppress domain-swrsn vsan 105

VSAN 105 のドメインフォーマット SW-RSCN の送信を抑制します。

Note ポートアドレスフォーマット RSCN またはエリアアドレスフォーマット RSCN の送信は抑制できません。

結合 SW-RSCN

Cisco MDS 9000 スイッチでのファイバチャネルプロトコルのパフォーマンス向上のため、SW-RSCN は遅延され、収集され、1 つの結合 SW-RSCN として単一ファイバチャネル交換でファブリック内のすべてのスイッチに送信されます。

結合 SW RSCN の有効化

[Restrictions（機能制限）]

- ファブリック内のすべてのスイッチで Cisco MDS 6.2(7) 以降が実行されている必要があります。
- この機能には、Cisco MDS 以外のスイッチとの相互運用性はありません。

結合 SW-RSCN を有効にするには、次の手順を実行します。

ステップ 1 switch# config terminal

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# rscn coalesce swrsn vsan 1

```
switch(config)#
```

VSAN 1 の Switch Registered State Change Notification (SWRSCN) の結合を有効にします。デフォルト遅延は 500 ミリ秒です。

ステップ 3 switch(config)# rscn coalesce swrscn vsan 1 delay 800

```
switch(config)#
```

VSAN 1 の Switch Registered State Change Notification (SWRSCN) の結合を有効にします。SW-RSCN を最大で 800 ミリ秒遅延します。

(注) 6.2(7) 以降稼働しているすべてのスイッチでは、デフォルトで結合 SW-RSCN を処理できますが、結合 SW-RSCN の送信は CLI で有効にした後でのみ可能です。

結合 SW-RSCN の無効化

結合 SW-RSCN を無効にするには、次の手順を実行します。

ステップ 1 switch# **config terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# no rscn coalesce swrscn vsan 1

```
switch(config)#
```

VSAN 1 の Switch Registered State Change Notification (SWRSCN) の結合を無効にします。

RSCN 統計情報のクリア

カウンタをクリアしたあとに、それらのカウンタを別のイベントに関して表示することができます。たとえば、特定のイベント (ONLINE または OFFLINE イベントなど) で生成された RSCN または SW-RSCN の個数を追跡できます。このような統計情報を利用して、VSAN 内で発生する各イベントへの応答を監視できます。

指定された VSAN の RSCN 統計情報をクリアするには、**clear rscn statistics** コマンドを使用します。

```
switch# clear rscn statistics vsan 1
```

RSCN 統計情報をクリアした後に **show rscn** コマンドを実行すると、クリアされたカウンタを表示できます。

```
switch# show rscn statistics vsan 1
Statistics for VSAN: 1
-----
Number of SCR received           = 0
Number of SCR ACC sent           = 0
```

```

Number of SCR RJT sent           = 0
Number of RSCN received         = 0
Number of RSCN sent              = 0
Number of RSCN ACC received     = 0
Number of RSCN ACC sent         = 0
Number of RSCN RJT received     = 0
Number of RSCN RJT sent         = 0
Number of SW-RSCN received      = 0
Number of SW-RSCN sent          = 0
Number of SW-RSCN ACC received  = 0
Number of SW-RSCN ACC sent      = 0
Number of SW-RSCN RJT received  = 0
Number of SW-RSCN RJT sent      = 0
Number of CSWR received         = 0
Number of CSWR sent             = 0
Number of CSWR ACC received     = 0
Number of CSWR ACC sent         = 0
Number of CSWR RJT received     = 0
Number of CSWR RJT sent         = 0
Number of CSWR RJT not sent     = 0

```

CFS を使用した RSCN タイマー設定の配布

各スイッチのタイムアウト値は、手動で設定されるため、異なるスイッチが別々の時間にタイムアウトになると、誤設定が生じます。つまり、ネットワーク内の異なる N ポートが別々の時間に RSCN を受信してしまうことがあります。Cisco Fabric Services (CFS) を使用すると、設定情報がファブリック内のすべてのスイッチに自動配信されて、この状況が回避されます。また、SW-RSCN の数も削減します。

RSCN は、配布と非配布の 2 つのモードをサポートしています。配布モードでは、RSCN は CFS を使用して、ファブリック内のすべてのスイッチに設定を配布します。非配布モードでは、影響を受けるのはローカルスイッチに対するコンフィギュレーションコマンドだけです。



Note すべてのコンフィギュレーションコマンドが配布されるわけではありません。 **rscn event-tov tov vsan vsan** コマンドだけが配布されます。

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 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 タイマー配布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。



Note ダウングレードを実行する場合は、事前に、ネットワーク内の RSCN タイマー値をデフォルト値に戻してください。デフォルト値に戻しておかないと、VSAN およびその他のデバイスを經由するリンクがディセーブルになります。

アップグレードまたはダウングレード中の各 Cisco MDS NX-OS リリースの互換性は、CFS が提供する **conf-check** によってサポートされます。Cisco MDS SAN-OS Release 30 からダウング

ロードしようとする、**conf-check** 警告が表示されます。ダウングレードの前に、RSCN タイマー配信サポートをディセーブルにするように要求されます。

デフォルトでは、RSCN タイマー配信機能はディセーブルになっているため、Cisco MDS SAN-OS Release 3.0 よりも前のリリースからアップグレードするときに互換性があります。

RSCN タイマーの設定

RSCN は、VSAN 単位のイベント リスト キューを維持します。RSCN イベントは、生成されると、このキューに入れられます。最初の RSCN イベントがキューに入ると、VSAN 単位のタイマーが始動します。タイムアウトになると、すべてのイベントがキューから出され、結合 RSCN が登録済みユーザーに送信されます。デフォルトのタイマー値の場合に、登録済みユーザーに送信される結合 RSCN の数が最小になります。配置によっては、ファブリック内の変更を追跡するために、イベント タイマー値をさらに小さくする必要が生じることがあります。



Note RSCN タイマー値は、VSAN 内のすべてのスイッチで同一にする必要があります。[RSCN タイマー設定の配布](#), on page 265 を参照してください。



Note ダウングレードを実行する場合は、事前に、ネットワーク内の RSCN タイマー値をデフォルト値に戻してください。デフォルト値に戻しておかないと、VSAN およびその他のデバイスを経由するリンクがディセーブルになります。

RSCN タイマーを設定するには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

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

RSCN タイマーの設定の配布をイネーブルにします。

ステップ 3 switch(config)# **rscn event-tov 300 vsan 10**

選択した VSAN のイベント タイムアウト値 (ミリ秒) を設定します。この例では、VSAN 12 のイベント タイムアウト値は 300 ミリ秒に設定されます。有効値は 0 ~ 2000 ミリ秒です。値をゼロ (0) に設定すると、タイマーはディセーブルになります。

ステップ 4 switch(config)# **no rscn event-tov 300 vsan 10**

デフォルト値 (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) に戻ります。

ステップ 5 switch(config)# rscn commit vsan 10

配信する RSCN タイマー設定を VSAN 10 内のスイッチにコミットします。

RSCN タイマー設定の確認

RSCN タイマー設定を確認するには、**show rscn event-tov vsan** コマンドを使用します。

```
switch# show rscn event-tov vsan 10
Event TOV : 1000 ms
```

RSCN タイマー設定の配布

各スイッチのタイムアウト値は、手動で設定されるため、異なるスイッチが別々の時間にタイムアウトになると、誤設定が生じます。つまり、ネットワーク内の異なる N ポートが別々の時間に RSCN を受信してしまうことがあります。Cisco Fabric Service (CFS) インフラストラクチャでは、RSCN タイマー設定情報をファブリック内のすべてのスイッチに自動的に配布することで、この状況を解消します。また、SW-RSCN の数も削減します。『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

RSCN は、配布と非配布の 2 つのモードをサポートしています。配布モードでは、RSCN は CFS を使用して、ファブリック内のすべてのスイッチに設定を配布します。非配布モードでは、影響を受けるのはローカルスイッチに対するコンフィギュレーションコマンドだけです。



Note すべてのコンフィギュレーションコマンドが配布されるわけではありません。 **rscn event-tov vsan vsan** コマンドだけが配布されます。



Note RSCN タイマー設定だけが配布されます。

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 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 タイマー配布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。



Note **show incompatibility system** コマンドを使用して以前の Cisco MDS NX-OS リリースにダウングレードする場合に、互換性を指定できます。以前のリリースへのダウングレードの前に、RSCN タイマー配信サポートを無効にする必要があります。



Note デフォルトでは、RSCN タイマー配信機能は無効になっているため、Cisco MDS SAN-OS Release 3.0 よりも前のリリースからアップグレードするときに互換性があります。



Note RSCN タイマー設定で CFS 配信が正しく行われるようにするには、ファブリック内のすべてのスイッチで Cisco SAN-OS Release 3.0(1) 以降または Cisco NX-OS 4.1(1b) が稼働している必要があります。

このセクションは、次のトピックで構成されています。

RSCN タイマー設定の配布のイネーブル化

RSCN タイマー設定の配布を有効にするには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

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

RSCN タイマーの設定の配布をイネーブルにします。

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

RSCN タイマーの配布をディセーブル（デフォルト）にします。

ファブリックのロック

データベースを変更するときの最初のアクションによって、保留中のデータベースが作成され、VSAN内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コピーが、最初のアクティブ変更と同時に保留中のデータベースになります。

RSCN タイマー設定の変更のコミット

アクティブデータベースに加えられた変更をコミットする場合、ファブリック内のすべてのスイッチに設定がコミットされます。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。

RSCN タイマー設定の変更をコミットするには、次の手順を実行します。

ステップ 1 switch# **config t**
switch(config)#
コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **rscn commit vsan 10**
RSCN タイマーの変更をコミットします。

RSCN タイマー設定の変更の廃棄

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、ロックが解除されます。

RSCN タイマー設定の変更を廃棄するには、次の手順を実行します。

ステップ 1 switch# **config t**
switch(config)#
コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **rscn abort vsan 10**
RSCN タイマーの変更を廃棄し、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。

ロック済みセッションのクリア

RSCN タイマー設定を変更したが、変更をコミットまたは廃棄してロックを解除するのを忘れた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザーによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。



Tip 保留中のデータベースは揮発性ディレクトリでだけ有効で、スイッチが再起動されると廃棄されます。

管理者の特権を使用して、ロックされた DPVM セッションを解除するには、EXEC モードで **clear rscn session vsan** コマンドを使用します。

```
switch# clear rscn session vsan 10
```

RSCN 設定の配布情報の表示

RSCN 設定の配信の登録ステータスを表示するには、**show cfs application name rscn** コマンドを使用します。

```
switch# show cfs application name rscn
Enabled       : Yes
Timeout      : 5s
Merge Capable : Yes
Scope        : Logical
```

RSCN 設定の配信のセッション ステータス情報を表示するには、**show rscn session status vsan** コマンドを使用します。



Note 結合対象のファブリックの RSCN タイマー値が異なる場合、結合は失敗します。

```
switch# show rscn session status vsan 1
Session Parameters for VSAN: 1
-----
Last Action           : Commit
Last Action Result    : Success
Last Action Failure Reason : None
```

設定をコミットした際に有効になる一連のコンフィギュレーションコマンドを表示するには、**show rscn pending** コマンドを使用します。



Note 保留中のデータベースには、既存設定と変更された設定の両方が含まれます。

```
switch# show rscn pending
rscn event-tov 2000 ms vsan 1
rscn event-tov 2000 ms vsan 2
rscn event-tov 300 ms vsan 10
```

保留中の設定とアクティブな設定の違いを表示するには、**show rscn pending-diff** コマンドを使用します。次の例では、VSAN 10 のタイムアウト値が 2000 ミリ秒（デフォルト）から 300 ミリ秒に変更されています。

```
switch# show rscn pending-diff
- rscn event-tov 2000 ms vsan 10
+ rscn event-tov 300 ms vsan 10
```

デフォルト設定

Table 22: デフォルトの RSCN 設定値, on page 269 に、RSCN のデフォルト設定値を示します。

Table 22: デフォルトの RSCN 設定値

パラメータ	デフォルト
RSCN タイマー値	2,000 ミリ秒 (ファイバチャネル VSAN の場合) 1,000 ミリ秒 (FICON VSAN の場合)
RSCN タイマー設定の配布	ディセーブル

ポート ページングの有効化

詳細については、『Cisco MDS 9000 Family NX-OS System Management』を参照してください。



CHAPTER 9

SCSI ターゲットの検出

この章では、Cisco MDS 9000 ファミリのスイッチが提供する SCSI LUN 検出機能について説明します。内容は次のとおりです。

- [SCSI LUN 検出の概要, on page 271](#)
- [SCSI LUN 情報の表示, on page 273](#)

SCSI LUN 検出の概要

SCSI ターゲットにはディスク、テープ、およびその他のストレージデバイスが含まれます。これらのターゲットは、ネーム サーバーに論理ユニット番号 (LUN) を登録しません。

ネーム サーバーには、次の理由により、LUN 情報が必要となります。

- LUN ストレージデバイス情報を表示して NMS がこの情報にアクセスできるようにするため
- デバイスのキャパシティ、シリアル番号、およびデバイス ID 情報を表示するため。
- ネーム サーバーにイニシエータおよびターゲット機能を登録するため。

SCSI LUN 検出機能には、ローカル ドメイン コントローラ ファイバチャネル アドレスが使用されます。この機能はローカル ドメイン コントローラをソース FC ID として使用し、SCSI デバイス上で SCSI INQUIRY、REPORT LUNS、および READ CAPACITY コマンドを実行します。

SCSI LUN 検出機能は、CLI (コマンドライン インターフェイス) または SNMP (簡易ネットワーク管理プロトコル) を通じて、オンデマンドで開始されます。隣接スイッチが Cisco MDS 9000 ファミリーに含まれる場合、この情報は隣接スイッチとも同期されます。

このセクションは、次のトピックで構成されています。

SCSI LUN 検出の開始について

SCSI LUN 検出はオンデマンドで実行されます。

ネーム サーバー データベース内の Nx ポートのうち、FC4 Type = SCSI_FCP として登録されたものだけが検出されます。

SCSI LUN 検出の開始

SCSI LUN 検出を開始するには、次の手順を実行します。

ステップ 1 switch# **discover scsi-target local os all**

Example:

```
discovery started
```

すべてのオペレーティング システム (OS) のローカル SCSI ターゲットを検出します。オペレーティング システムのオプションは **aix**、**all**、**hpux**、**linux**、**solaris**、または **windows** です。

ステップ 2 switch# **discover scsi-target remote os aix**

Example:

```
discovery started
```

AIX OS に割り当てられたリモート SCSI ターゲットを検出します。

ステップ 3 switch# **discover scsi-target vsan 1 fcid 0x9c03d6**

Example:

```
discover scsi-target vsan 1 fcid 0x9c03d6
VSAN:      1 FCID: 0x9c03d6 PWWN: 00:00:00:00:00:00:00:00
PRLI RSP: 0x01 SPARM: 0x0012
SCSI TYPE: 0 NLUNS: 1
Vendor: Company 4 Model: ST318203FC   Rev: 0004
Other: 00:00:02:32:8b:00:50:0a
```

指定された VSAN (1) および FC ID (0x9c03d6) の SCSI ターゲットを検出します。

ステップ 4 switch# **discover scsi-target custom-list os linux**

Example:

```
discovery started
```

Linux OS に割り当てられたカスタマイズ リストから SCSI ターゲットを検出します。

カスタマイズ検出の開始について

カスタマイズ検出は、検出を開始するように選択的に設定された VSAN とドメインのペア リストによって行われます。ドメイン ID は 0 ~ 255 の数値 (10 進数)、または 0x0 ~ 0xFF の数値 (16 進数) です。

この検出を開始するには、**custom-list** オプションを使用します。

カスタマイズ検出の開始

カスタマイズ検出を開始するには、次のいずれかの手順を実行します。

ステップ 1 switch# **discover custom-list add vsan 1 domain 0X123456**

指定されたエントリをカスタム リストに追加します。

ステップ 2 switch# **discover custom-list delete vsan 1 domain 0X123456**

指定されたドメイン ID をカスタム リストから削除します。

SCSI LUN 情報の表示

検出結果を表示するには、**show scsi-target** コマンドと **show fcns database** コマンドを使用します。例 [検出ターゲットの表示, on page 273](#) ~ [自動検出されたターゲットの表示, on page 275](#) を参照してください。

検出ターゲットの表示

```
switch# show scsi-target status
discovery completed
```



Note このコマンドを完了するには、数分間かかることがあります（特に、ファブリックが大規模である場合や、複数のデバイスの応答速度が遅い場合）。

FCNS データベースの表示

```
switch# show fcns database
VSAN 1:
-----
FCID          TYPE  PWWN                               (VENDOR)          FC4-TYPE:FEATURE
-----
0xeb0000      N     21:01:00:e0:8b:2a:f6:54 (Qlogic)          scsi-fcp:init
0xeb0201      NL    10:00:00:00:c9:32:8d:76 (Emulex)          scsi-fcp:init
Total number of entries = 2
VSAN 7:
-----
FCID          TYPE  PWWN                               (VENDOR)          FC4-TYPE:FEATURE
-----
0xed0001      NL    21:00:00:04:cf:fb:42:f8 (Seagate)        scsi-fcp:target
Total number of entries = 1
VSAN 2002:
-----
```

```

FCID          TYPE  PWWN                               (VENDOR)          FC4-TYPE:FEATURE
-----
0x9c03d6     N    20:03:00:05:30:00:2a:20 (Cisco)          FICON:CUP
Total number of entries = 1

```

検出されたターゲット ディスクの表示

```

switch# show scsi-target disk
-----
VSAN          FCID          PWWN                               VENDOR            MODEL             REV
-----
1             0x9c03d6     21:00:00:20:37:46:78:97          Company 4         ST318203FC        0004
1             0x9c03d9     21:00:00:20:37:5b:cf:b9          Company 4         ST318203FC        0004
1             0x9c03da     21:00:00:20:37:18:6f:90          Company 4         ST318203FC        0004
1             0x9c03dc     21:00:00:20:37:5a:5b:27          Company 4         ST318203FC        0004
1             0x9c03e0     21:00:00:20:37:36:0b:4d          Company 4         ST318203FC        0004
1             0x9c03e1     21:00:00:20:37:39:90:6a          Company 4         ST318203 CLAR18   3844
1             0x9c03e2     21:00:00:20:37:18:d2:45          Company 4         ST318203 CLAR18   3844
1             0x9c03e4     21:00:00:20:37:6b:d7:18          Company 4         ST318203 CLAR18   3844
1             0x9c03e8     21:00:00:20:37:38:a7:c1          Company 4         ST318203FC        0004
1             0x9c03ef     21:00:00:20:37:18:17:d2          Company 4         ST318203FC        0004

```

すべてのオペレーティング システムで検出された LUN の表示

```

switch# show scsi-target lun os all
ST336607FC from SEAGATE (Rev 0006)
FCID is 0xed0001 in VSAN 7, PWWN is 21:00:00:04:cf:fb:42:f8
-----
OS  LUN      Capacity Status  Serial Number  Device-Id
   (MB)
-----
WIN 0x0    36704   Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
AIX 0x0    36704   Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
SOL 0x0    36704   Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
LIN 0x0    36704   Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
HP  0x0     36704   Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8

```

Solaris OS で検出された LUN の表示

```

switch# show scsi-target lun os solaris
ST336607FC from SEAGATE (Rev 0006)
FCID is 0xed0001 in VSAN 7, PWWN is 21:00:00:04:cf:fb:42:f8
-----
OS  LUN      Capacity Status  Serial Number  Device-Id
   (MB)
-----
SOL 0x0    36704   Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8

```

次のコマンドを実行すると、各 OS (Windows、AIX、Solaris、Linux、または HPUX) に割り当てられたポート WWN が表示されます。

各 OS の pWWN の表示

```
switch# show scsi-target pwn
-----
OS      PWWN
-----
WIN     24:91:00:05:30:00:2a:1e
AIX     24:92:00:05:30:00:2a:1e
SOL     24:93:00:05:30:00:2a:1e
LIN     24:94:00:05:30:00:2a:1e
HP      24:95:00:05:30:00:2a:1e
```

カスタマイズされた検出ターゲットの表示

```
switch# show scsi-target custom-list
-----
VSAN    DOMAIN
-----
1       56
```

オンラインになった SCSI ターゲットの自動検出を確認するには、**show scsi-target auto-poll** コマンドを使用します。内部 UUID 番号は、シャーシに CSM または IPS モジュールが装着されていることを示します。

自動検出されたターゲットの表示

```
switch(config)# show scsi-target auto-poll
name server polling is enabled
auto-polling is disabled, poll_start:0 poll_count:0 poll_type:0
USERS OF AUTO POLLING
-----
```




CHAPTER 10

FICON の設定

Fibre Connection (FICON) インターフェイスの機能は、開放型システムとメインフレーム ストレージネットワーク環境の両方をサポートすることによって、Cisco MDS 9000 ファミリーを拡張します。Control Unit Port (CUP) をサポートしたことで、FICON プロセッサからスイッチのインバンド管理ができるようになりました。

この章は、次の項で構成されています。

- [FICON の概要, on page 277](#)
- [FICON ポート番号の設定, on page 285](#)
- [FICON の設定, on page 295](#)
- [FICON ポートの設定, on page 307](#)
- [FICON コンフィギュレーション ファイル, on page 317](#)
- [ポート スワッピング, on page 321](#)
- [FICON テープ アクセラレーション, on page 324](#)
- [XRC アクセラレーションの設定, on page 328](#)
- [FICON VSAN のオフライン状態への移行, on page 329](#)
- [CUP インバンド管理, on page 329](#)
- [FICON 情報の表示, on page 330](#)
- [デフォルト設定, on page 338](#)

FICON の概要

Cisco MDS 9000 ファミリーは、単一のハイアベイラビリティプラットフォーム内でFibre Channel Protocol (FCP)、FICON、iSCSI、およびFCIP 機能をサポートします ([Figure 55: 共有システム ストレージ ネットワーク, on page 278](#)を参照)。

FICON 機能は、以下ではサポートされていません。

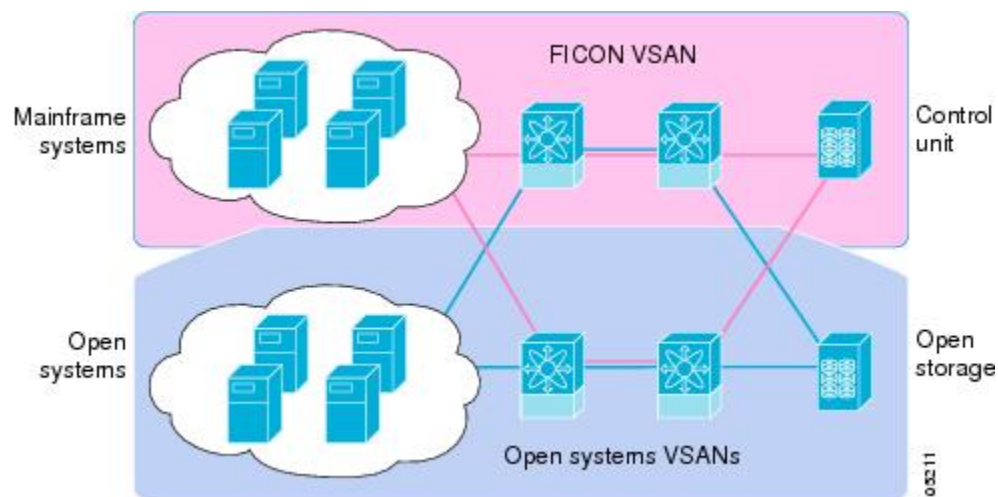
- Cisco MDS 9120 スイッチ
- Cisco MDS 9124 スイッチ
- Cisco MDS 9140 スイッチ

- 32 ポート ファイバチャネル スイッチング モジュール
- HP c-Class BladeSystem 用の Cisco ファブリック スイッチ
- IBM BladeSystem 用の Cisco ファブリック スイッチ

FCP と FICON は別個の FC4 プロトコルであり、トラフィックは互いに独立しています。これらのプロトコルを使用しているデバイス間の切り離しには、VSAN を使用する必要があります。

ファブリック バインディング 機能は、無許可のスイッチがファブリックに接続したり、現在のファブリック操作を中断するのを防止するのに役立ちます（『Cisco MDS 9000 Family NX-OS Security Configuration Guide』を参照）。Registered Link Incident Report (RLIR) アプリケーションを使用することにより、スイッチ ポートから登録済み Nx ポートに LIR を送信できます。

Figure 55: 共有システムストレージネットワーク



このセクションは、次のトピックで構成されています。

[FICON の要件, on page 278](#)

[MDS 固有 FICON のメリット, on page 279](#)

[FICON のカスケード化, on page 284](#)

[FICON VSAN の前提条件, on page 284](#)

FICON の要件

FICON 機能の要件として、次のものが挙げられます。

- FICON 機能を実装できるスイッチは、次のとおりです。
 - Cisco MDS 9500 シリーズのあらゆるスイッチ
 - Cisco MDS 9200 シリーズのあらゆるスイッチ（例：Cisco MDS 9222i マルチサービス モジュラ スイッチ）

- Cisco MDS 9134 マルチレイヤ ファブリック スイッチ
- MDS 9000 ファミリの 18/4 ポート マルチサービス モジュール
- FICON パラメータを設定するには、MAINFRAME_PKG のライセンスが必要です。
- FCIP が使用されている WAN 回線を介して FICON 設定を展開するには、使用しているモジュールに対応した所定の SAN_EXTN_OVER_IP ライセンスが必要です。詳細については、『Cisco NX-OS Family Licensing Guide』を参照してください。

MDS 固有 FICON のメリット

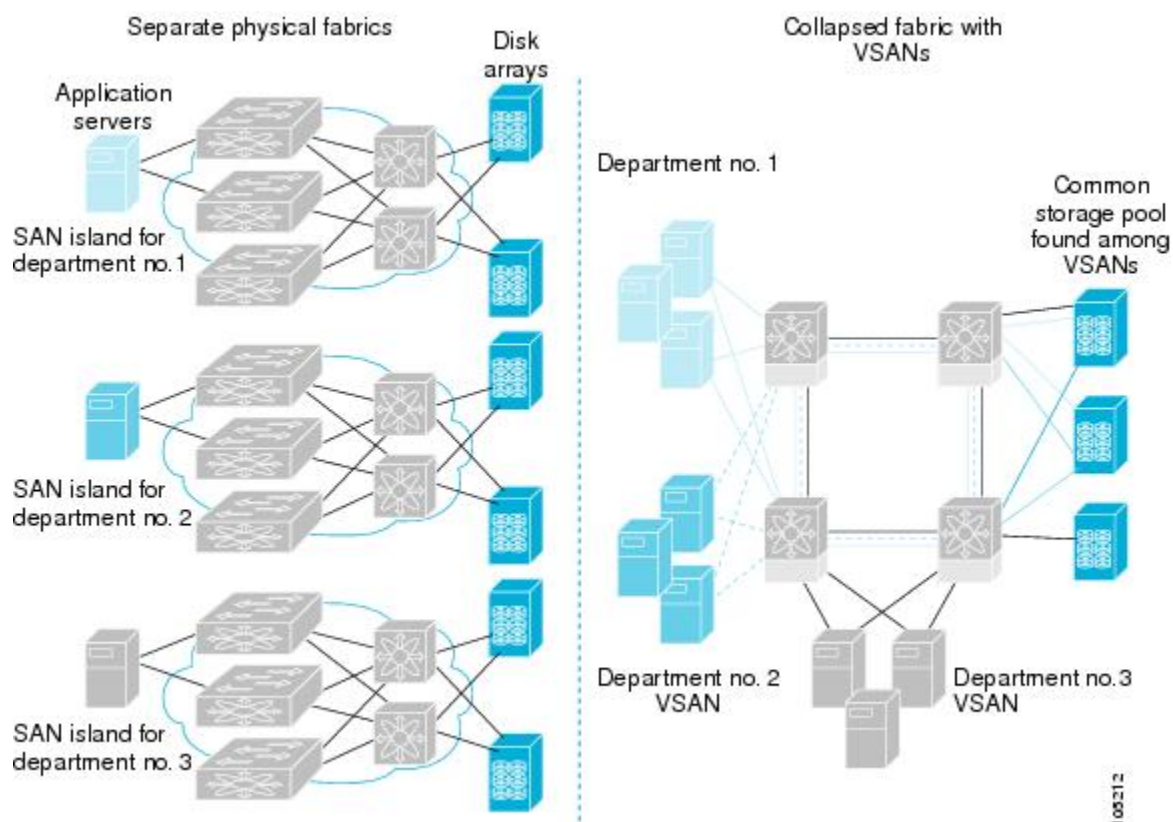
ここでは、Cisco MDS スイッチのその他の FICON のメリットについて説明します。また、次のトピックを取り上げます。

VSAN によるファブリックの最適化

別々の物理ファブリックを実装すると、高度なスイッチ管理が必要になるため、実装コストがかさむのが一般的です。ファブリック設定によっては、各アイランド内のポートのプロビジョニングが過剰になることがあります。

Cisco MDS 固有の VSAN テクノロジーを導入すると、過剰なプロビジョニングコストの節減、および管理対象スイッチ数の軽減につながるため、これらの物理ファブリック間の効率を向上できます。また、VSAN を使用すると、中断せずに未使用ポートを移動し、共通の冗長物理インフラストラクチャを提供できます (Figure 56: VSAN 固有ファブリックの最適化, on page 280 を参照)。

Figure 56: VSAN 固有ファブリックの最適化



VSANを使用すると、SANのグローバル統合が可能になり、単一の物理ネットワーク上の既存のSANアイランドを仮想SANアイランドに変換できます。これにより、ハードウェアレベルでセキュリティが適用され、アプリケーションどうしまたは部門どうしが切り離されて単一のネットワーク上で共存できるようになります。また、仮想再配線が可能になり、ストレージインフラストラクチャが強化されます。機器に経費をかけたり機器の物理的再配置を破壊したりせず、部門間またはアプリケーション間でアセットを移動できます。



Note どのCisco MDSスイッチにもVSANを設定できます。ただし、FICONを有効にできるVSANは8つ以下に限られます。設定可能なVSANの数は、プラットフォームごとに異なります。

メインフレームユーザーであれば、VSANをMDS SANファブリック内のFICON LPARと同様のものと考えればわかりやすいでしょう。スイッチリソースは、互いに切り離されたFICON LPAR (VSAN) にパーティション化できます。このパーティション化の操作は、zSeriesまたはDS8000上でリソースをパーティション化する操作とほぼ同じです。各VSANは、固有のファブリックサービス（たとえば、ファブリックサーバーやネームサーバー）、FICON CUP、ドメインID、Fabric Shortest Path First (FSPF) ルーティング、動作モード、IPアドレス、およびセキュリティプロファイルのセットで構成されています。FICON LPARは複数のラインカードにわたって設置でき、そのサイズが動的に調整されます。たとえば、10ポート付きFICON

LPAR 1 つを 10 のラインカードにわたって設置することもできます。FICON LPAR には、カスケード設定の複数のスイッチのポートを含めることもできます。Cisco MDS 9000 スイッチングアーキテクチャには一貫した公正さがあるため、「すべてのポートは等しく作成」されます。これにより、他のベンダー製プラットフォームで発生する「ローカルスイッチング」問題を除去して、プロビジョニングを簡素化することができます。FICON LPAR へのポートの追加は、無中断プロセスです。FICON アドレス指定の制限を受けるため、FICON LPAR の最大ポート数は 255 です。

FCIP のサポート

Cisco MDS 9000 ファミリのマルチレイヤアーキテクチャは、プロトコルを認識しないスイッチファブリックを介して一貫したフィーチャセットを可能にしています。Cisco MDS 9500 シリーズおよび 9200 シリーズスイッチは、ファイバチャネル、FICON、および Fibre Channel over IP (FCIP) を 1 つのシステムに透過的に統合します。FICON over FCIP 機能を使用すると、遠く離れた場所にあるメインフレームリソースにも、コスト効率よくアクセスできます。Cisco MDS 9000 ファミリのプラットフォームでは、ビジネス継続ストラテジをシンプルにするユビキタス IP インフラストラクチャを使用して、IBM PPRC や XRC などのストレージレプリケーションサービスを、メトロを介してグローバルな距離にまで展開できます。

『Cisco MDS 9000 Family NX-OS IP Services Configuration Guide』を参照してください。

ポートチャネルのサポート

FICON の Cisco MDS 実装では、効率的利用がサポートされているため、安定した大規模 SAN 環境の構築に要するスイッチ間リンク (ISL) のアベイラビリティが向上しています。Cisco MDS スイッチ内での ISL のアベイラビリティおよびパフォーマンスは、ポートチャネルによって強化されます。

ポートチャネルの詳細については、『Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide』を参照してください。

VSAN による、FICON と FCP の混在への対応

Cisco MDS 9000 ファミリの FICON 対応スイッチは、きわめて複雑な混在環境にも簡単に導入できるようになっています。各サービスに必要な VSAN を簡単に作成して、複数の論理 FICON、Z-Series Linux/FCP、および Open-Systems Fibre Channel Protocol (FCP) ファブリックを 1 つの物理ファブリックにオーバーレイできます。VSAN にはハードウェア独立サービスとプロトコル固有のファブリックサービスの両方が用意されているため、ゾーンベースの混在方式のような複雑さがなく、不安定になるおそれ也没有ありません。

Cisco MDS 9000 ファミリのどのスイッチにおいても、FICON 機能はデフォルトでディセーブルになっています。FICON 機能がディセーブルのときは、FCID をシームレスに割り当てることが可能です。Cisco NX-OS ソフトウェアは混在環境に対応しています。FCP プロトコルと FICON プロトコルの混在に関する問題は、VSAN を実装すれば、Cisco MDS スイッチによって対処されます。

Cisco MDS 9000 ファミリのスイッチおよびディレクタは、FCP プロトコルと FICON プロトコルの混在をポートレベルでサポートしています。これらのプロトコルが同一スイッチ内に混在している場合は、VSAN を使用して FCP ポートと FICON ポートを切り離せます。



Tip 混在環境を作成する際は、すべての FICON デバイスを（デフォルト VSAN 以外の）1 つの VSAN に配置し、FCP スイッチ ポートを（デフォルト VSAN 以外の）別個の VSAN に隔離してください。このようにして FCP と FICON を切り離すことにより、接続しているすべてのデバイスに対して正常な通信が保証されます。

Cisco MDS でサポートされている FICON 機能

Cisco MDS 9000 ファミリの FICON 機能としては、次のものがあります。

- 柔軟性と投資の保護：Cisco MDS 9500 シリーズおよび 9200 シリーズ間で共通のスイッチング モジュールとサービス モジュールは、Cisco MDS 9000 ファミリによって共有されます。
『Cisco MDS 9500 Series Hardware Installation Guide』および『Cisco MDS 9200 Series Hardware Installation Guide』を参照してください。
- ハイ アベイラビリティ FICON 対応ディレクタ：Cisco MDS 9500 シリーズは、すべての主要コンポーネントに対して稼働中のソフトウェアアップグレード、ステートフルなプロセス再起動/フェールオーバー、および十分な冗長性を可能にしたことで、ディレクタ クラスの可用性の新標準に準拠しています。4/2/1 Gbps、10 Gbps の自動検知 FICON ポートまたは FCP ポートの任意の組み合わせを最大 528 個まで 1 つのシャーシに搭載できます。『Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide』を参照してください。
- インフラストラクチャの保護：共通ソフトウェアリリースによって、すべての Cisco MDS 9000 プラットフォーム間でインフラストラクチャを保護できます。『Cisco MDS 9000 Family NX-OS Software Upgrade and Downgrade Guide』を参照してください。
- VSAN テクノロジー：Cisco MDS 9000 ファミリには、ハードウェアレベルで適用される VSAN テクノロジーが採用されています。VSAN テクノロジーは、単一物理ファブリック内の独立環境に対応しているため、物理インフラストラクチャを安全に共有しながら、FICON 混在のサポートを強化できます。[VSAN の設定と管理, on page 9](#)を参照してください。
- ポートレベルでの設定：BB_credits、ビーコンモード、およびポートセキュリティをポートごとに設定できます。バッファ間クレジット、ビーコン LED、およびトランッキングについては、『Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide』を参照してください。
- エイリアス名の設定：スイッチおよび接続されているノードデバイスに、WWN でなくユーザーフレンドリなエイリアスを設定できます。を参照してください。

- 包括的なセキュリティ フレームワーク : Cisco MDS 9000 ファミリは、RADIUS および TACACS+ 認証、簡易ネットワーク管理プロトコルバージョン 3 (SNMPv3)、ロールベース アクセス コントロール、セキュア シェル プロトコル (SSH)、セキュア ファイル 転送 プロトコル (SFTP)、VSAN、ハードウェアベースのゾーン分割、ACL、ファブリック バインディング、Fibre Channel Security Protocol (FC-SP)、LUN ゾーン分割、読み取り専用 ゾーン、および VSAN ベースのアクセス コントロールをサポートしています。RADIUS、TACACS+、FC-SP、および DHCHAP の詳細については、『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。



Note LUN ゾーン分割および読み取り専用ゾーンは、Cisco MDS NX-OS Release 5.x 以降ではサポートされていません。

- トラフィックの暗号化 : FCIP を介した IP セキュリティがサポートされています。FCIP を介して伝送された FICON および ファイバチャネル トラフィックを暗号化できます。『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。
- ローカル アカウンティング ログ : ローカル アカウンティング ログを表示して、FICON イベントを検出できます。MSCHAP 認証およびローカル AAA サービスの詳細については、『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。
- 統合型ストレージ管理 : Cisco MDS 9000 FICON 対応スイッチは、IBM CUP 規格に適合しており、IBM S/A OS/390 I/O 操作コンソールを使用した帯域内管理が可能です。[CUP インバンド管理, on page 329](#)を参照してください。
- ポートアドレスベースの設定 : ポート名、ブロック状態またはブロック解除状態を設定します。また、接続制限属性をポートに設定できます。[FICON ポートの設定, on page 307](#)を参照してください。
- 表示できる情報には、次のものがあります。
 - 個別のファイバチャネルポート (例 : ポート名、ポート番号、ファイバチャネルアドレス、動作ステート、ポートタイプ、ログインデータなど)
 - ポートに接続されているノード
 - ポートのパフォーマンスおよび統計情報
- コンフィギュレーションファイル : コンフィギュレーションファイルを保存し、適用します。[FICON コンフィギュレーションファイル, on page 317](#)を参照してください。
- FICON および開放型システム管理サーバー機能 (インストール済みの場合)。[VSAN による、FICON と FCP の混在への対応, on page 281](#)を参照してください。
- 拡張カスケードサポート : [CUP インバンド管理, on page 329](#)を参照してください。
- 日時 : スイッチの日時設定を行います。[ホストでタイムスタンプを制御できるようにする, on page 303](#)を参照してください。

- SNMP トラップの受け取り側およびコミュニティ名を設定します ([FICON パラメータの SNMP 制御の設定, on page 304](#) を参照)。
- Call Home の設定 : ディレクタ名、場所、説明、および担当者を設定します。『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- 優先するドメイン ID、FC ID の永続性、および主要スイッチの優先度の設定 : ドメインパラメータの設定の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- 詳細な SPAN (スイッチドポートアナライザ) 診断 : Cisco MDS 9000 ファミリには、業界初のインテリジェント診断、プロトコルデコーディング、ネットワーク分析ツール、および統合された Call Home 機能が組み込まれているため、信頼性の向上、迅速な問題解決、およびサービスコストの削減が実現します。SPAN を使用したネットワークトラフィックのモニタリングの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- R_A_TOV、E_D_TOV の設定 : [Cisco MDS でサポートされている FICON 機能](#)を参照してください。
- ディレクタレベルのメンテナンス作業 : 障害分析をサポートするために、ディレクタのメンテナンス作業 (たとえば、ファームウェアレベルのメンテナンス、ディレクタログへのアクセス、データ収集など) を実行します。システムプロセスおよびログのモニタリングの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- ポートレベルのインシデントアラート:ポートレベルのインシデントアラートを表示およびクリアします。[RLIR 情報のクリア, on page 317](#)を参照してください。

FICON のカスケード化

Cisco MDS NX-OS ソフトウェアを使用して、FICON ネットワーク内で複数のスイッチの共存が可能になります。複数のスイッチを設定するには、該当スイッチ内でファブリックバインディングを有効にし、設定する必要があります (『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照)。

FICON VSAN の前提条件

FICON VSAN を稼働状態にするには、次の前提条件を満たしているかどうか確認してください。

- ゾーン分割機能を使用していない場合は、デフォルトゾーンを許可するように設定します。次のヒントを参照してください。



Tip アクティブゾーンセットを保存するのに、**copy running-config startup-config** コマンドを発行する必要はありません。ただし、明示的にフルゾーンセットを保存するには、**copy running-config startup-config** コマンドを発行する必要があります。ファブリックに複数のスイッチが含まれている場合は、**copy running-config startup-config fabric** コマンドを実行する必要があります。**fabric** キーワードを指定すると、**copy running-config startup-config** コマンドがファブリック内のすべてのスイッチで実行され、フルゾーン情報がファブリック内のすべてのスイッチのスタートアップ コンフィギュレーションに保存されます。これは、スイッチのリロードおよび電源再投入時に重要です。

- VSAN 上で順序どおりの配信をイネーブルにします。 [ファイバチャネルルーティングサービスおよびプロトコルの設定, on page 205](#)を参照してください。
- VSAN 上でファブリック バインディングをイネーブルにします（必要に応じて設定します）。ファブリック バインディングの詳細については、『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。
- スイッチ内に衝突する永続FCIDが存在していないことを確認します。ドメインパラメータの設定の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- 設定済みドメインIDと要求したドメインIDが一致していることを確認します。ドメインパラメータの設定の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。
- ゾーン分割を使用している場合は、ゾーンにCUP（エリアFE）を追加します。 [CUP インバンド管理, on page 329](#)を参照してください。

上記の前提条件がいずれか1つでも満たされていないと、FICON機能をイネーブルにできません。

FICON ポート番号の設定

FICON機能に関しては、Cisco MDS スイッチ内のポートが、静的に定義された8ビット値（ポート番号）で識別されます。ポート番号は、最大255個まで使用できます。使用できるポート番号設定方式には、次のものがあります。

- シャーシタイプに基づくデフォルトポート番号
- 予約済みポート番号

この項では、次のトピックについて取り上げます。

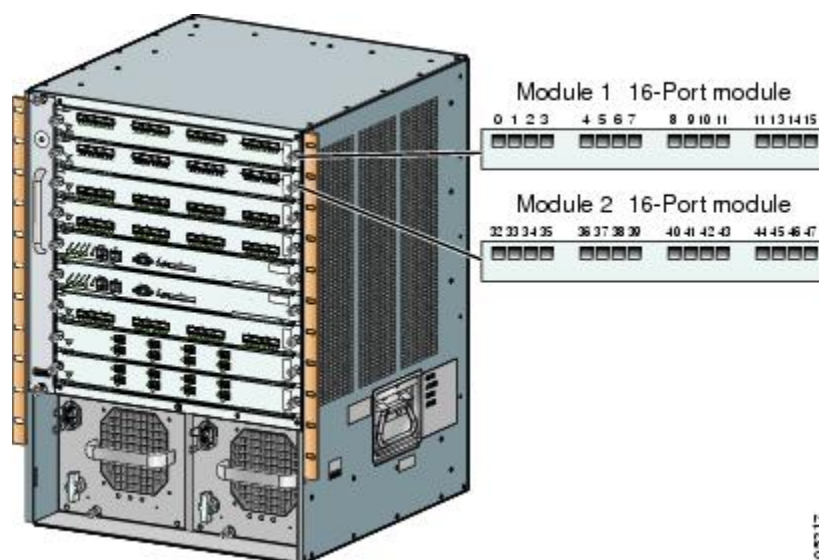


Note FICON ポート番号を予約する前に、スイッチ上で FICON をイネーブルにしておく必要があります (VSAN の FICON をイネーブルにする操作の概要, on page 295 を参照)。

デフォルトの FICON ポート番号設定方式

Cisco MDS NX-OS ソフトウェアは、シャーシ内のモジュールとスロットに基づいて、デフォルトの FICON ポート番号を割り当てます。スイッチ内の最初のポートは、常にゼロ (0) で開始します (Figure 57: Cisco MDS 9000 ファミリ スイッチのデフォルトの FICON ポート番号設定, on page 286 を参照)。

Figure 57: Cisco MDS 9000 ファミリ スイッチのデフォルトの FICON ポート番号設定



デフォルトの FICON ポート番号は、前面パネル上のポートの位置に基づいて、モジュールが属しているスロットに固有の値が割り当てられます。Cisco MDS 9513 ディレクタの場合、各スロットに16個のポート番号が割り当てられています。それ以外の Cisco MDS 9000 ファミリ スイッチではいずれも、各スロットに32個のポート番号が割り当てられています。これらのデフォルト番号は、シャーシ内にモジュールが物理的に存在するかどうか、ポートのステータス (アップまたはダウン)、またはモジュールのポート数 (4、12、16、24、または 48) に関係なく割り当てられます。モジュールのポートの数の方が、スロットに割り当てられたポート番号の個数よりも少ない場合、超過分のポート番号は使用されません。モジュールのポート数が、スロットに割り当てられたポート番号の個数よりも多い場合、ポート番号を手動で割り当てない限り、超過分のポートは FICON に使用できません。



Note スロットにポート番号を手動で割り当てて超過分のポートを使用するには、[スロットへの FICON ポート番号の割り当て](#)、[on page 292](#) コマンドを使用できます。**ficon slot assign port-numbers** の手順を使用します。ただし、この手順を実行する前に、Cisco MDS 9000 スイッチのデフォルトのポート番号の割り当て ([Table 25: FICON のデフォルト設定](#)、[on page 338](#) [Table 23: Cisco MDS 9000 ファミリのデフォルト FICON ポート番号](#)、[on page 287](#)) を確認し、[予約済み FICON ポート番号設定方式の概要](#)、[on page 291](#) セクション、[FICON ポート番号設定に関するガイドライン](#)、[on page 292](#) セクション、および [スロットへの FICON ポート番号の割り当て](#)、[on page 292](#) セクションを読んで、FICON ポートの番号設定を十分に理解しておくことをお勧めします。



Note FICON ポート番号にマッピングされるのは、ファイバチャネル、ポートチャネル、および FCIP ポートだけです。それ以外のタイプのインターフェイスでは、対応するポート番号が生成されません。

[Table 23: Cisco MDS 9000 ファミリのデフォルト FICON ポート番号](#)、[on page 287](#) は、Cisco MDS 9000 ファミリのスイッチおよびディレクタ用のデフォルトのポート番号の割り当ての一覧です。

Table 23: Cisco MDS 9000 ファミリのデフォルト FICON ポート番号

製品	スロット番号	実装ポート割り当て	割り当て先ポートチャネル/FCIP	非実装ポート	
割り当て先ポート	注記				
Cisco MDS 9200 シリーズ	スロット 1	0 ~ 31	64 ~ 89	90 ~ 253、およびポート 255	スイッチングモードと同様。
	スロット 2	32 ~ 63			

製品	スロット番号	実装ポート割り当て	割り当て先ポート チャンネル/FCIP	非実装ポート	
Cisco MDS 9222i シリーズ	スロット 1	0 ~ 31	64 ~ 89	90 ~ 253、およびポート 255	4 ポート、12 ポート、16 ポート、または 24 ポートのモジュールでは、最初の 4、12、16、または 24 個のポート番号が使用され、残りは未使用のままです。48 ポートモジュール上の余分な 16 個のポートには、ポート番号が割り当てられません。
	スロット 2	32 ~ 63			
Cisco MDS 9506 ディレクタ	スロット 1	0 ~ 31	128 ~ 153	154 ~ 253、およびポート 255	スーパーバイザモジュールにはポート番号が割り当てられません。
	スロット 2	32 ~ 63			
	スロット 3	64 ~ 95			
	スロット 4	96 ~ 127			
	スロット 5	なし			
	スロット 6	なし			
Cisco MDS 9134 ディレクタ	スロット 1	0 ~ 33	34 ~ 59	60 ~ 253、およびポート 255	

製品	スロット番号	実装ポート割り当て	割り当て先ポート チャンネル/FCIP	非実装ポート	
Cisco MDS 9509 ディレクタ	スロット 1	0 ~ 31	224 ~ 249	250 ~ 253、および ポート 255	4 ポート、12 ポート、16 ポート、または 24 ポートのモジュールでは、最初の 4、12、16、または 24 個のポート番号が使用され、残りは未使用のままです。48 ポートモジュール上の余分な 16 個のポートには、ポート番号が割り当てられません。
	スロット 2	32 ~ 63			
	スロット 3	64 ~ 95			
	スロット 4	96 ~ 127			
	スロット 5	なし			スーパーバイザモジュールにはポート番号が割り当てられません。
	スロット 6	なし			
	スロット 7	128 ~ 159			4 ポート、12 ポート、16 ポート、または 24 ポートのモジュールでは、最初の 4、12、16、または 24 個のポート番号が使用され、残りは未使用のままです。48 ポートモジュール上の余分な 16 個のポートには、ポート番号が割り当てられません。
	スロット 8	160 ~ 191			
	スロット 9	192 ~ 223			

製品	スロット番号	実装ポート割り当て	割り当て先ポートチャンネル/FCIP	非実装ポート	
Cisco MDS 9513 ディレクタ	スロット 1	0 ~ 15	224 ~ 249	250 ~ 253、および ポート 255	4 ポート、12 ポート、または 16 ポートのモジュールでは、最初の 4、12、または 16 個のポート番号が使用され、残りは未使用のままです。24 ポート、32 ポート、および 48 ポートのモジュール上の余分なポートには、ポート番号が割り当てられません。
	スロット 2	16 ~ 31			
	スロット 3	32 ~ 47			
	スロット 4	48 ~ 63			
	スロット 5	64 ~ 79			
	スロット 6	80 ~ 95			
	スロット 7	なし	スーパーバイザモジュールにはポート番号が割り当てられません。		
	スロット 8	なし			
	スロット 9	96 ~ 111	4 ポートまたは 12 ポートのモジュールでは、最初の 4 または 12 個のポート番号が使用され、残りは未使用のままです。24 ポート、32 ポート、および 48 ポートのモジュール上の余分なポートには、ポート番号が割り当てられません。		
	スロット 10	112 ~ 127			
	スロット 11	128 ~ 143			
	スロット 12	144 ~ 159			
	スロット 13	160 ~ 175			

ポートアドレス

デフォルトでは、ポート番号はポートアドレスと同じです。ポートアドレスはスワッピングできます（[ポート スワッピング](#) , on page 321 を参照）。

ポートアドレスをスワッピングするには、**ficon swap portnumber** コマンドを実行します。

実装ポートおよび非実装ポートのアドレス

実装ポートとは、デフォルトでシャーシ内のスロットに割り当てられるすべてのポートアドレスです（[デフォルト設定, on page 338](#)を参照）。非実装ポートとは、デフォルトでシャーシ内のスロットに割り当てられないすべてのポートアドレスです（[デフォルト設定, on page 338](#)を参照）。

予約済み FICON ポート番号設定方式の概要

250 個のポート番号のいずれかを使用して、スイッチ上のすべてのポートへの割り当てができます。[デフォルト設定, on page 338](#) に示すように、スイッチの物理ポート数が 250 個を超えた場合、デフォルト番号設定方式では超過分のポートにポート番号を設定できません。スイッチの物理ポート数が 250 個を超えた場合は、FICON VSAN に存在しないポートにはポート番号を割り当てないでよく、あるいは同一の FICON VSAN で使用されていない重複ポート番号を割り当てるなどの方法で対処できます。たとえば、FICON VSAN 10 のインターフェイス fc1/1、および FICON VSAN 20 のインターフェイス fc10/1 に、ポート番号 1 を設定できます。



Note 1 つの VSAN に設定できるポート数は、最大 250 個です。



Note アクティブになっているポートの FICON ポート番号は変更されません。最初に **shutdown** コマンドを使用して、インターフェイスをディセーブルにする必要があります。



Note スロットにモジュールが設置されていない場合でも、ポート番号を設定できます。

インストレーションポートおよび非インストレーションポート

インストレーションポートとは、必要なすべてのハードウェアが搭載されているポートです。次の条件のいずれか 1 つが適用される場合、VSAN 内の指定のポート番号を実装ポートにできます。ただし、インストレーションポートにはできません。

- モジュールが存在しない場合（たとえば、モジュール 1 が Cisco MDS 9509 ディレクタのスロット 1 に物理的に存在していない場合）、ポート番号 0～31 は非インストレーションポートと見なされます。
- Small Form-Factor Pluggable (SFP) ポートが存在しない場合（たとえば、Cisco MDS 9509 ディレクタのスロット 2 に 16 ポートモジュールが挿入されている場合）、ポート 48～63 は非インストレーションポートと見なされます。
- スロット 1 には、ポート 0～31、またはポート 0～15 が割り当てられています。VSAN 2 内に存在する物理ポートは、ポート番号 4 の物理ポート fc1/5 だけです。残りの物理ポートは VSAN 2 内に存在していません。FICON 対応 VSAN では常に、ポート番号 0～249

は実装ポートと見なされます。つまり、VSAN2に存在しているのは、ポート番号0～249と、1つの物理ポート fc1/4 です。対応する物理ポート 0～3、および 5～249 は VSAN 2 内に存在しません。これらのポート番号は VSAN 2 内に物理ポートが存在しないため、FICON VSAN ポート アドレスを表示したときにインストレーション ポート（例：ポート 0～3、5～249 など）としては表示されません。

もう1つのシナリオは、VSAN 1～5 が FICON に対応していて、トランキング対応インターフェイス fc1/1 に VSAN 3～10 が設定してある場合です。この場合、VSAN 1 と VSAN 2 ではポートアドレス 0 が非インストレーション ポートになります。

- 該当のポートがポートチャネルの一部であると想定した場合（たとえば、インターフェイス fc 1/1 がポートチャネル 5 に属している場合）、すべての FICON VSAN でポートアドレス 0 が非インストレーション ポートになります。「[デフォルト設定, on page 338](#)」を参照してください。

FICON ポート番号設定に関するガイドライン

FICON ポート番号には、次のガイドラインが適用されます。

- スーパーバイザ モジュールには、ポート番号割り当てがありません。
- ポート番号は TE ポートに応じて変更されません。TE ポートは複数の VSAN で使用されるため、TE ポート用にシャーシ規模の一意のポート番号を予約しておく必要があります。
- 各ポートチャネルを FICON ポート番号に明示的に関連付ける必要があります。
- 物理ポートチャネルのポート番号が非インストレーションポートと一致したとき、その物理ポートには、関連するポートチャネルの設定が適用されます。
- 各 FCIP トンネルを FICON ポート番号に明示的に関連付ける必要があります。ポートチャネルまたは FCIP トンネルに対してポート番号が割り当てられていない場合、関連付けられているポートは起動しません。

[FCIP およびポートチャネルのポート番号の概要, on page 293](#)を参照してください。

スロットへの FICON ポート番号の割り当て

`show ficon port-number assign` コマンドと `show ficon first-available port-number` コマンドを使用して、使用するポート番号を決定することができます。



Caution ポート番号を割り当て、変更、またはリリースすると、ポートが再ロードされます。

FICON ポート番号をスロットに割り当てる手順は、次のとおりです。

ステップ 1 switch# `config t`

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ficon slot 3 assign port-numbers 0-15, 48-63**

スロット 3 の最大 32 のインターフェイス用に FICON ポート番号 0 ~ 15 と 48 ~ 63 を予約します。

ステップ 3 switch(config)# **ficon slot 3 assign port-numbers 0-15, 17-32**

スロット 3 の最初の 16 インターフェイス用に FICON ポート番号 0 ~ 15 を予約し、次の 16 のインターフェイス用に 17 ~ 32 を予約します。

ステップ 4 switch(config)# **ficon slot 3 assign port-numbers 0-63**

スロット 3 の最大 64 のインターフェイス用に FICON ポート番号 0 ~ 63 を予約します。

ステップ 5 switch(config)# **ficon slot 3 assign port-numbers 0-15, 56-63**

スロット 3 の最大 24 のインターフェイス用に予約されている FICON ポート番号を変更します。

ステップ 6 switch(config)# **no ficon slot 3 assign port-numbers 0-15, 56-63**

(任意) FICON ポート番号を解放します。

FICON ポート番号割り当ての表示

スイッチに割り当てられているポート番号を表示するには、**show ficon port-numbers assign** コマンドを使用します。

```
switch# show ficon port-numbers assign
ficon slot 1 assign port-numbers 0-31
ficon slot 2 assign port-numbers 32-63
ficon slot 3 assign port-numbers 64-95
ficon slot 4 assign port-numbers 96-127
ficon logical-port assign port-numbers 128-153
```

特定のスロットに割り当てられているポート番号を表示するには、**show ficon port-numbers assign slot** コマンドを使用します。

```
switch# show ficon port-numbers assign slot 2
ficon slot 2 assign port-numbers 32-63
```

論理ポート用に予約されているポート番号を表示するには、**show ficon port-numbers assign** コマンドを使用します。

```
switch# show ficon port-numbers assign logical-port
ficon logical-port assign port-numbers 128-153
```

FCIP およびポートチャネルのポート番号の概要

FCIP および PortChannel は、ポート番号に明示的にバインドしておかないと、FICON 対応 VSAN で使用できません。

FICON ポートの設定, on page 307、FICON およびポートチャネルインターフェイス用の FICON ポート番号の予約, on page 294、および FCIP インターフェイスへのポート番号のバインド, on page 308 を参照してください。

デフォルト ポート番号が使用可能な場合 (Table 23: Cisco MDS 9000 ファミリのデフォルト FICON ポート番号, on page 287 を参照)、あるいはファイバチャネルインターフェイス用に予約されていないポート番号のプールからポート番号を予約する場合 (予約済み FICON ポート番号設定方式の概要, on page 291 を参照)、デフォルト ポート番号を使用できます。

FCIP または PortChannel インターフェイスのバインドに最初に使用できるポート番号を確認するには、**show ficon first-available port-number** コマンドを使用します (使用可能なポート番号の表示, on page 332 を参照)。



Tip マッピングのインターフェイスとなるポート番号を表示するには、**show ficon vsan portaddress brief** コマンドを使用します。ポートチャネル/FCIP 範囲内で、PortChannel または FCIP インターフェイスに割り当てられていないポート番号を割り当てることができません (要約形式でのポート番号情報の表示, on page 332) を参照)。

FICON およびポートチャネルインターフェイス用の FICON ポート番号の予約

FCIP やポートチャネルなどの論理インターフェイスを使用する予定がある場合は、使用する論理インターフェイス用にポート番号を予約しておく必要があります。

FICON ポート番号を論理インターフェイス用に予約するには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ficon logical-port assign port-numbers 230-249**

FCIP および PortChannel インターフェイス用にポート番号 230 ~ 249 を予約します。

ステップ 3 switch(config)# **ficon logical-port assign port-numbers 0xe6-0xf9**

FCIP および PortChannel インターフェイス用にポート番号 0xe6 ~ 0xf9 を予約します。

Note アクティブなポート番号は変更できません。**shutdown** コマンドを使用してインターフェイスを無効にし、**no ficon portnumber** コマンドを使用してポート番号をアンバインドする必要があります。[FICON ポートの設定, on page 307](#) を参照してください。

ステップ 4 switch(config)# **no ficon logical-port assign port-numbers 230-249**

ポート番号を解放します。

Note アクティブなインターフェイスのポート番号は解放できません。shutdown コマンドを使用してインターフェイスを無効にし、no ficon portnumber コマンドを使用してポート番号をアンバインドする必要があります。FICON ポートの設定, on page 307を参照してください。

FC ID の割り当て

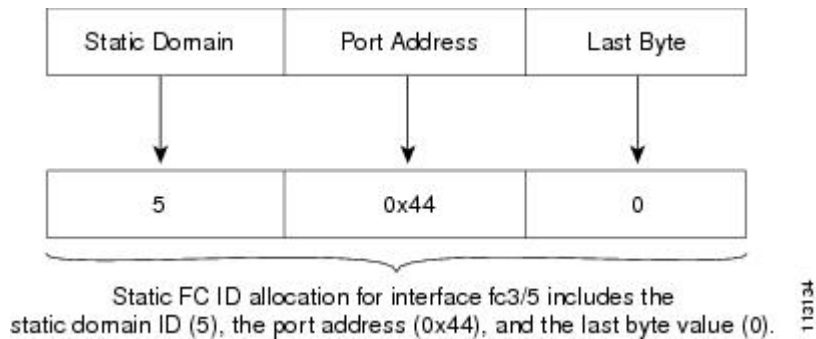
FICON には予測可能なスタティック FC ID 割り当て方式が必要です。FICON がイネーブルのときは、接続先ポートのポートアドレスに応じた FC ID がデバイスに割り当てられます。ポートアドレスは、ファブリックアドレスの中央バイトを構成しています。また、ファブリック内のデバイスはすべて、ファブリックアドレスの最終バイトが同一である必要があります。最終バイト値はデフォルトでは 0 ですが、他の値を設定することも可能です。



Note FICON 対応 VSAN では、固定的 FC ID を設定できません

Cisco MDS スイッチ用に、ダイナミック FC ID 割り当て方式が用意されています。VSAN 上で FICON を有効または無効にすると、すべてのポートがシャットダウンし、ダイナミック FC ID からスタティック FC ID に、あるいはその逆方向にスイッチングされます (Figure 58: FICON 用スタティック FC ID の割り当て, on page 295を参照)。

Figure 58: FICON 用スタティック FC ID の割り当て



FICON の設定

Cisco MDS 9000 ファミリのどのスイッチにおいても FICON はデフォルトでディセーブルになります。Device Manager を使用すると、VSAN 単位で FICON をイネーブルにできます。

このセクションは、次のトピックで構成されています。

VSAN の FICON をイネーブルにする操作の概要

スイッチ上のどの VSAN においても FICON はデフォルトでディセーブルになります。

VSAN 単位で FICON をイネーブルにするには、次の方法があります。

- 自動 **setup ficon** コマンドを使用します。

[基本 FICON 設定のセットアップ, on page 297](#)を参照してください。

- 各前提条件を手動でアドレッシングします。

[FICON の概要, on page 277](#)を参照してください。

- Device Manager を使用します。

Cisco MDS スイッチで FICON FICON 機能をイネーブルにすると、次の制約が適用されます。

- FICON 対応 VSAN では、順序どおりの配信をディセーブルにできません。
- FICON 対応 VSAN では、ファブリック バインディングまたはスタティック ドメイン ID 設定をディセーブルにできません。
- ロードバランシング方式が Source ID (SID) -Destination ID (DID) に変更されます。SID—DID—OXID に戻すことはできません。
- IPL コンフィギュレーションファイルが自動的に作成されます。

[FICON コンフィギュレーションファイルの概要, on page 318](#)を参照してください。



Tip 同一の FICON 対応スイッチにログインしている複数ユーザーは、Device Manager を使用して、FICON の自動保存を起動できます。Device Manager は FICON 対応スイッチであれば機種に関係なく定期自動保存を実行するため、結果として FICON キーカウンタが増加します。キーカウンタの増加から、実際には発生しなかった変更を特定できます。こうした変更を回避するために、FICON 対応スイッチを Device Manager の 1 インスタンスだけに監視させる設定を推奨します。

スイッチでの FICON の有効化

Cisco MDS 9000 ファミリのどのスイッチにおいても FICON はデフォルトでディセーブルになります。VSAN で FICON を有効にすることで、スイッチで FICON を明示的または暗黙的に有効にできます。ただし、すべての VSAN で FICON を無効にしても、スイッチの FICON は無効になりません。FICON を明示的に無効にする必要があります。

スイッチの FICON をグローバルに有効または無効にするには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **feature ficon**

スイッチの FICON をグローバルにイネーブルにします。

ステップ 3 switch(config)# no feature ficon

スイッチで FICON をグローバルに無効化し、すべての FICON 設定を削除します。

基本 FICON 設定のセットアップ

ここでは、Cisco MDS 9000 ファミリ スイッチの特定の VSAN で FICON をセットアップする方法を、手順を追って説明します。



Note 任意のプロンプトで **Ctrl-C** キーを押すと、残りの設定オプションを飛ばして、設定手順を先に進めることができます。



Tip 事前に設定された質問に回答しない場合、または任意の質問の回答を省略する場合は、**Enter** キーを押します。デフォルトの回答が見つからない場合（たとえば、スイッチ名）、スイッチは以前の設定を使用して、次の質問にスキップします。

FICON を有効にして設定するには、次の手順を実行します。

ステップ 1 EXEC コマンドモードで **setup ficon** コマンドを入力します。

```
switch# setup ficon
      --- Ficon Configuration Dialog ---
This setup utility will guide you through basic Ficon Configuration
on the system.
Press Enter if you want to skip any dialog. Use ctrl-c at anytime
to skip all remaining dialogs.
```

ステップ 2 **yes** と入力して（デフォルトは **yes**）、基本 FICON 設定セットアップを開始します。

```
Would you like to enter the basic configuration dialog (yes/no) [yes]: yes
```

FICON セットアップユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。どのプロンプトでも、**Ctrl-C** キーを押すと、設定プロセスが終了します。

ステップ 3 FICON を有効にする必要がある VSAN の番号を入力します。

```
Enter vsan [1-4093]:2
```

ステップ 4 VSAN を作成するには、**yes** と入力します（デフォルトは **yes**）。

```
vsan 2 does not exist, create it? (yes/no) [yes]: yes
```

ステップ 5 VSAN の選択を確定するには、**yes** と入力します（デフォルトは **yes**）。

Enable ficon on this vsan? (yes/no) [yes]: **yes**

Note この時点で VSAN がまだ作成されていない場合は、ソフトウェアにより作成されます。

ステップ 6 指定された FICON VSAN のドメイン ID 番号を入力します。

Configure domain-id for this ficon vsan (1-239):**2**

ステップ 7 カスケードモードで FICON を設定するには、**yes** と入力します（デフォルトは **no**）。**no** を入力する場合は、ステップ 8 に進みます（[CUP インバンド管理, on page 329](#)を参照）。

Would you like to configure ficon in cascaded mode: (yes/no) [no]: **yes**

a) FICON: CUP のピア WWN の割り当て

Configure peer wwn (hh:hh:hh:hh:hh:hh:hh:hh): **11:00:02:01:aa:bb:cc:00**

b) FICON: CUP のピア ドメイン ID の割り当て

Configure peer domain (1-239) :**4**

c) 追加のピアを設定する場合は **yes** と入力します（ステップ 7a と 7b を繰り返します）。追加のピアを設定しない場合は **no** と入力します。

Would you like to configure additional peers: (yes/no) [no]: **no**

ステップ 8 SNMP に対し既存のポート接続パラメータの変更を許可するには、**yes** と入力します（デフォルトは **yes**）（[FICON パラメータの SNMP 制御の設定, on page 304](#)を参照）。

Enable SNMP to modify port connectivity parameters? (yes/no) [yes]: **yes**

ステップ 9 必要に応じて、ホスト(メインフレーム) がポート接続パラメータを変更できるようにするには、**no** と入力します（デフォルトは **no**）（[ホストで FICON ポート パラメータを変更できるようにするには, on page 302](#)を参照）。

Disable Host from modifying port connectivity parameters? (yes/no) [no]: **no**

ステップ 10 **yes** と入力し（デフォルトは **yes**）、**active equals saved** 機能を有効にします（[実行コンフィギュレーションの自動保存, on page 305](#)を参照）。

Disable Host from modifying port connectivity parameters? (yes/no) [no]: **no**

ステップ 11 追加の FICON VSAN を設定するには、**yes** と入力します（デフォルトは **yes**）。

Disable Host from modifying port connectivity parameters? (yes/no) [no]: **no**

ステップ 12 ここまでに入力した設定を確認して修正します。

ステップ 13 設定に問題がなければ、**no** と入力します（デフォルトは **no**）。

Note 説明のため、次の設定では異なる FICON 設定の VSAN を 3 つ示しています。次に、さまざまな FICON シナリオでのこれらの設定による出力の例を示します。

```
The following configuration will be applied:
fcdomain domain 2 static vsan 1
fcdomain restart disruptive vsan 1
fabric-binding database vsan 1
swrn 11:00:02:01:aa:bb:cc:00 domain 4
fabric-binding activate vsan 1
zone default-zone permit vsan 1
ficon vsan 1
no host port control
fcdomain domain 3 static vsan 2
fcdomain restart disruptive vsan 2
fabric-binding activate vsan 2 force
zone default-zone permit vsan 2
ficon vsan 2
no host port control
no active equals saved
vsan database
vsan 3
fcdomain domain 5 static vsan 3
fcdomain restart disruptive vsan 3
fabric-binding activate vsan 3 force
zone default-zone permit vsan 3
ficon vsan 3
no snmp port control
no active equals saved
Would you like to edit the configuration? (yes/no) [no]: no
```

ステップ 14 この設定を使用および保存する場合は、yes と入力します（デフォルトは yes）。実装されたコマンドが表示されます。指定された VSAN で FICON が有効になった後で、EXEC モード スイッチ プロンプトが再び表示されます。

```
Use this configuration and apply it? (yes/no) [yes]: yes
`fcdomain domain 2 static vsan 1`
`fcdomain restart disruptive vsan 1`
`fabric-binding database vsan 1`
`swrn 11:00:02:01:aa:bb:cc:00 domain 4`
`fabric-binding activate vsan 1`
`zone default-zone permit vsan 1`
`ficon vsan 1`
`no host port control`
`fcdomain domain 3 static vsan 2`
`fcdomain restart disruptive vsan 2`
`fabric-binding activate vsan 2 force`
`zone default-zone permit vsan 2`
`ficon vsan 2`
`no host port control`
`no active equals saved`
```

Note 新しい VSAN が作成された場合、2 つの追加コマンド（**vsan database** と **vsan number**）が表示されます。

```
`vsan database`
`vsan 3`
`in-order-guarantee vsan 3`
`fcdomain domain 2 static vsan 3`
`fcdomain restart disruptive vsan 3`
`fabric-binding activate vsan 3 force`
```

```
`zone default-zone permit vsan 3`
`ficon vsan 3`
`no snmp port control`
Performing fast copy config...done.
switch#
```

VSAN での手動での FICON のイネーブル化



Note ここでは、VSAN 上で手動で FICON をイネーブルにする手順について説明します。自動セットアップを使用して（推奨）、所定の VSAN 上で FICON をイネーブルにしてある場合は、[実行コンフィギュレーションの自動保存, on page 305](#)に進んでください。

VSAN 上で FICON を手動で有効にするには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
コンフィギュレーションモードに入ります。
```

ステップ 2 switch(config)# **vsan database**

```
switch(config-vsan-db) # vsan 5
switch(config-vsan-db) # do show vsan usage
4 vsan configured
configured vsans:1-2,5,26
vsans available for configuration:3-4,6-25,27-4093
switch(config-vsan-db) # exit
```

VSAN 5 を有効にします。

ステップ 3 switch(config)# **in-order-guarantee vsan 5**

VSAN 5 の順序どおりの配信をアクティブにします。

[ファイバチャネルルーティングサービスおよびプロトコルの設定, on page 205](#)を参照してください。

ステップ 4 switch(config)# **fcdomain domain 2 static vsan 2**

VSAN 2 のドメイン ID を設定します。

ドメインパラメータの設定の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

ステップ 5 switch(config)# **fabric-binding activate vsan 2 force**

VSAN 2 のファブリック バインディングをアクティブにします。

『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。

ステップ 6 switch(config)# **zone default-zone permit vsan 2**

VSAN 2 に許可するデフォルトゾーンを設定します。

[CUP インバンド管理, on page 329](#)を参照してください。

ステップ 7 switch(config)# **ficon vsan 2**

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 8 switch(config)# **no ficon vsan 6**

VSAN 6 で FICON 機能を無効にします。

ステップ 9 switch(config-ficon)# **no host port control**

メインフレームユーザーに対し、スイッチをオフライン状態に移行することを禁止します。

ホストでスイッチをオフラインに移行できるようにするには、[on page 302](#)を参照してください。

[code-page] オプションの設定

FICON スtring は、拡張 2 進化 10 進コード (EBCDIC) フォーマットで符号化されます。コード ページ オプションの詳細については、メインフレームのマニュアルを参照してください。

Cisco MDS スイッチは、**international-5**、**france**、**brazil**、**germany**、**italy**、**japan**、**spain-latinamerica**、**uk**、および **us-canada** (デフォルト) EBCDIC フォーマット オプションをサポートします。



Tip この設定は、オプションです。使用する EBCDIC フォーマットが不明な場合は、**us-canada** (デフォルト) オプションを引き続き使用することを推奨します。

VSAN で **code-page** オプションを設定するには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **ficon vsan 2**

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 3 switch(config-ficon)# **code-page italy**

■ ホストでスイッチをオフラインに移行できるようにするには

italy EBCDIC フォーマットを設定します。

ステップ 4 `switch(config-ficon)# no code-page`

(任意) **us-canada** EBCDIC フォーマットを使用する出荷時デフォルトに戻します。

ホストでスイッチをオフラインに移行できるようにするには

デフォルトでは、ホストでスイッチをオフライン状態に移行できます。スイッチをオフラインにするには、ホストから「Set offline」コマンド (x'FD') を CUP に送信します。

ホストでスイッチをオフライン状態に移行できるようにするには、次の手順を実行します。

ステップ 1 `switch# config terminal`

`switch(config)#`

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# ficon vsan 2`

`switch(config-ficon)#`

VSAN 2 で FICON を有効にします。

ステップ 3 `switch(config-ficon)# no host control switch offline`

メインフレームユーザーに対し、スイッチをオフライン状態に移行することを禁止します。

ステップ 4 `switch(config-ficon)# host control switch offline`

ホストでスイッチをオフライン状態 (デフォルト) に移行できるようにし、ポートをシャットダウンします。

ホストで FICON ポートパラメータを変更できるようにするには

デフォルトでメインフレームユーザーに許可されるのはスイッチのクエリーだけであり、Cisco MDS スイッチの FICON パラメータ設定は許可されません。

メインフレームユーザーが FICON パラメータを設定できるようにするには、**host port control** コマンドを使用します。

ホスト (メインフレーム) で Cisco MDS スイッチの FICON パラメータの設定を許可するには、次の手順を実行します。

ステップ 1 `switch# config terminal`

`switch(config)#`

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ficon vsan 2**

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 3 switch(config-ficon)# **no host port control**

メインフレーム ユーザーに対し、Cisco MDS スイッチで FICON パラメータの設定を禁止します。

ステップ 4 switch(config-ficon)# **host port control**

メインフレーム ユーザーに対し、Cisco MDS スイッチで FICON パラメータの設定を許可します（デフォルト）。

ホストでタイムスタンプを制御できるようにする

デフォルトでは、各 VSAN のクロックはスイッチハードウェアと同一のクロックになります。Cisco MDS 9000 ファミリー スイッチにおいて各 VSAN は、仮想ディレクタとなっています。仮想ディレクタごとに、表示されるクロックと時刻が異なることがあります。VSAN ごとの別々のクロックを保守するために、VSAN 固有のクロックとハードウェアベースのディレクタクロックとの差分が Cisco NX-OS ソフトウェアによって保守されています。ホスト（メインフレーム）で時刻が設定されると、クロック間の差異が Cisco NX-OS ソフトウェアにより更新されます。ホストがクロックを読み取ると、VSAN クロックと現在のディレクタ ハードウェアクロックとの差分が計算され、値がメインフレームに提示されます。

VSAN クロックの現行時刻は、**show ficon vsan vsan-id**、**show ficon**、および **show accounting log** コマンドの出力に示されます。

タイムスタンプのホスト制御を設定するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ficon vsan 2**

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 3 switch(config-ficon)# **no host set-timestamp**

メインフレーム ユーザーに対し、VSAN 固有のクロックを変更することを禁止します。

ステップ 4 switch(config-ficon)# **host set-timestamp**

ホストでこのスイッチのクロックを設定できるようにします（デフォルト）。

タイムスタンプのクリア



Note タイムスタンプは、メインフレームではなく Cisco MDS スイッチでのみクリアできます。

VSAN クロックをクリアするには、EXEC モードで **clear ficon vsan vsan-id timestamp** コマンドを使用します。

```
switch# clear ficon vsan 20 timestamp
```

FICON パラメータの SNMP 制御の設定

FICON パラメータの SNMP 制御を設定するには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ficon vsan 2**

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 3 switch(config-ficon)# **no snmp port control**

SNMP ユーザーに対し FICON パラメータの設定を禁止します。

ステップ 4 switch(config-ficon)# **snmp port control**

SNMP ユーザーに対し FICON パラメータの設定を許可します（デフォルト）。

FICON デバイスの従属関係の概要

FICON では、現在実行されているセッションのデバイス従属関係を制御することによって、Cisco MDS 9000 ファミリー スイッチ上で複数のメインフレーム、CLI、および SNMP セッション間のアクセスをシリアル化する必要があります。他のセッションに設定変更の実行を許可するには、所定の従属関係を使用可能にする必要があります。



Caution この作業により、現在実行中のセッションが破棄されます。

FICON デバイスの従属関係のクリア

現在のデバイス従属関係をクリアするには、EXEC モードで **clear ficon vsan vsan-id allegiance** コマンドを実行します。

```
switch# clear ficon vsan 1 allegiance
```

実行コンフィギュレーションの自動保存

Cisco MDS NX-OS には、スタートアップ コンフィギュレーションに加えられた設定変更を自動保存するオプションが用意されています。この自動保存によって、スイッチのリブート後も、新しい設定が消去されずに済みます。デフォルトでは、Active=Saved **active equals saved** オプションがすべての FICON VSAN で自動的に有効になっています。

[Table 24: アクティブな FICON およびスイッチ設定の保存, on page 306](#) は、さまざまなシナリオでの **Active = Saved** オプション **active equals saved** コマンドの結果と、実行 コンフィギュレーションからスタートアップコンフィギュレーションに暗黙的にコピーした結果 (**copy running start**) **copy running-config startup-config** コマンドを示したものです。

ファブリック内の任意の FICON 対応 VSAN で Active=Saved オプション **active equals saved** コマンドがイネーブルな場合は、次のようになります ([Table 24: アクティブな FICON およびスイッチ設定の保存, on page 306](#)の番号 1 と番号 2 を参照)。

- 設定変更はすべて (FICON 固有のものかどうかに関係なく)、永続ストレージに自動的に保存され (暗黙的に **copy running start** が実行され)、さらにスタートアップコンフィギュレーション内に保管されます。
- FICON 固有の設定変更は、ただちに IPL ファイルに保存されます ([FICON コンフィギュレーション ファイル, on page 317](#) を参照)。

[Active=Saved] オプション **active equals saved** コマンドがファブリック内のすべての FICON 対応 VSAN でも有効になっていない場合、FICON 固有の設定変更が IPL ファイルに保存されず、暗黙の **copy running startup** コマンドが実行されないため、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明示的に保存する必要があります **copy running start** コマンドを明示的に実行する必要があります ([Table 24: アクティブな FICON およびスイッチ設定の保存, on page 306](#) の 3 を参照)。

Table 24: アクティブな FICON およびスイッチ設定の保存

番号	FICON 対応 VSAN かどうか	active equals saved がイネーブルかどうか	暗黙的 copy running start が発行されたかどうか	注意事項
1	はい	(すべての FICON VSAN で) イネーブル	暗黙的	FICON の変更内容は IPL ファイルに書き込まれました。 FICON 以外の変更内容は、スタートアップ コンフィギュレーションおよび永続ストレージに保存されます。
2	はい	(1つの FICON VSAN で) イネーブル	暗黙的	active equals saved オプションがイネーブルな VSAN でだけ、FICON の変更は IPL ファイルに書き込まれました。 FICON 以外の変更内容は、スタートアップ コンフィギュレーションおよび永続ストレージに保存されます。
3	はい	(すべての FICON VSAN で) ディセーブル	非暗黙的	FICON の変更内容は IPL ファイルに書き込まれません。 copy running start コマンドを明示的に発行した場合に限り、FICON 以外の変更内容が永続ストレージに保存されます。
4	非対応	該当なし		



Note **active equals saved** が有効な場合、Cisco NX-OS ソフトウェアでは、FICON 設定で **copy running startup** コマンドを実行する必要がありません。スイッチまたはファブリックが複数の FICON 対応 VSAN で構成されており、これらの VSAN の 1 つで **active equals saved** が有効な場合、FICON 以外の変更内容を変更すると、すべての設定がスタートアップ コンフィギュレーションに保存されます。

実行コンフィギュレーションを自動的に保存するには、次の手順を実行します。

ステップ 1 switch# config terminal

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# ficon vsan 2

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 3 `switch(config-ficon)# active equals saved`

スイッチまたはファブリック内のすべての VSAN の自動保存機能をイネーブルにします。

ステップ 4 `switch(config-ficon)# no active equals saved`

(任意) この VSAN の自動保存を無効にします。

FICON ポートの設定

Cisco MDS 9000 ファミリ スイッチでは、ポートアドレス単位で FICON の設定を実行できません。

ポートが非インストレーションポートの場合でも、Cisco MDS スイッチではポートアドレスベースの設定が可能です。この設定がポートに適用されるのは、ポートがインストレーションポートになった場合です。

このセクションは、次のトピックで構成されています。

PortChannel へのポート番号のバインド



Caution FICON がすべての VSAN で無効になっていると、PortChannel または FCIP インターフェイスへのポート番号割り当てがすべて失われます（復元できません）。

PortChannel を FICON ポート番号にバインドする（関連付ける）と、そのインターフェイスを起動できます。

FICON ポート番号に PortChannel をバインドするには、次の手順を実行します。

ステップ 1 `switch# config terminal`

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 `switch(config)# interface Port-channel 1`

```
switch(config-if)#
```

PortChannel インターフェイス コンフィギュレーション モードを開始します。

ステップ 3 `switch(config-if)# ficon portnumber 234`

選択された PortChannel ポートに FICON ポート番号を割り当てます。

FCIP インターフェイスへのポート番号のバインド

FICON ポート番号に FCIP インターフェイスをバインドする（関連付ける）ことで、そのインターフェイスを起動できます。

FICON ポート番号に FCIP インターフェイスをバインドするには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch1(config)# **interface fcip 51**

```
switch1(config-if)#
```

FCIP インターフェイス（51）を作成します。

ステップ 3 switch(config-if)# **ficon portnumber 208**

選択された FCIP インターフェイスに FICON ポート番号を割り当てます。

ポート ブロッキングの設定

ポートをブロックした場合、ポートは運用停止状態のままになります。ポートのブロックを解除すると、ポートの初期化が試行されます。ブロックされているポート上では、データおよび制御トラフィックが許可されません。

物理ファイバチャネルポートをブロックした場合は引き続き、ブロックされたポート上に Off-Line State（OLS）プリミティブシーケンスが転送されます。



Note FICON VSAN 内のゾーン分割デバイスは、現在禁止されている FICON ポートと競合する可能性があるため、使用しないでください。ゾーン分割とポート禁止を同一 VSAN 内で使用することは推奨されません。



Caution CUP ポート（0XFE）は、ブロックまたは禁止できません。

シャットダウンしているポートは、ブロック解除しても初期化されません。



Note **shutdown/no shutdown** ポート状態は、**block/no block** ポート状態に依存しません。

VSAN のポート アドレスをブロックまたはブロック解除するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ficon vsan 2**

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 3 switch(config-ficon)# **portaddress 1 - 5**

```
switch(config-ficon-portaddr)#
```

詳細な設定を行うため、ポート アドレス 1 ~ 5 を選択します。

ステップ 4 switch(config-ficon-portaddr)# **block**

一連のポート アドレスを無効にし、運用停止状態で維持します。

ステップ 5 switch(config-ficon-portaddr)# **no block**

選択されたポート アドレスを有効にし、工場出荷時デフォルト（ポート アドレスがブロックされていない状態）に戻します。

ポートの禁止

実装ポート間の相互通信を禁止するには、複数ポート間の禁止を設定します。複数ポート間の禁止により、指定されたポート間の相互通信は禁止されます。



Tip ポートチャネルインターフェイスまたはFCIPインターフェイスは、使用禁止には設定できません。

非実装ポートは、常に使用禁止になります。また、禁止設定は常に対称的に適用されます。ポート 0 に対してポート 15 との通信を禁止すると、ポート 15 に対しても自動的にポート 0 との通信が禁止されます。



Note インターフェイスがすでに E モードまたは TE モードに設定されている場合は、対象のポートを使用禁止にしようとしても、禁止設定が拒否されます。同様に、非稼働状態のポートは、使用禁止にしてしまうと E モードまたは TE モードで起動できません。

ポート禁止のデフォルト状態の設定

デフォルトでは、スイッチに実装されるインターフェイスではポート禁止が無効になっています。Cisco MDS SAN-OS Release 3.0(2) の時点では、各自が作成した VSAN でデフォルトのポート禁止状態を有効に変更し、実装されるポートで必要に応じてポート禁止を無効にすることができます。また、デフォルトの変更後に作成された FICON コンフィギュレーションファイルでのみ、新しいデフォルト設定が反映されます ([FICON コンフィギュレーションファイル](#), on page 317を参照)。

スイッチに実装されているすべてのインターフェイスでデフォルトのポート禁止設定を変更するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **ficon port default-state prohibit-all**

スイッチで実装されているすべてのインターフェイスのデフォルトとして、ポート禁止を有効にします。

ステップ 3 switch(config)# **no ficon port default-state prohibit-all**

スイッチで実装されているすべてのインターフェイスのデフォルトとして、ポート禁止を無効にします (デフォルト)。

ポート禁止の設定

VSAN のポート アドレスを禁止する手順は、次のとおりです。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **ficon vsan 2**

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 3 switch(config-ficon)# portaddress 7

```
switch(config-ficon-portaddr)#
```

詳細な設定を行うため、ポートアドレス 7 を選択します。

ステップ 4 switch(config-ficon-portaddr)# prohibit portaddress 3-5

VSAN 2 のポートアドレス 7 に対し、ポート 3、4、および 5 に対する通信を禁止します。

ステップ 5 switch(config-ficon-portaddr)# no prohibit portaddress 5

以前の禁止状態からポートアドレス 5 を解除します。

ポートアドレス名の割り当て

ポートアドレス名を割り当てるには、次の手順を実行します。

ステップ 1 switch# config t

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# ficon vsan 2

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 3 switch(config-ficon)# portaddress 7

```
switch(config-ficon-portaddr)#
```

詳細な設定を行うため、ポートアドレス 7 を選択します。

ステップ 4 switch(config-ficon-portaddr)# name SampleName

ポートアドレスに名前を割り当てます。

Note ポートアドレス名は、24 文字までの英数字に制限されています。

ステップ 5 switch(config-ficon-portaddr)# no name SampleName

以前に設定されたポートアドレス名を削除します。

RLIR の概要

Registered Link Incident Report (RLIR) アプリケーションを使用することにより、スイッチポートから登録済み Nx ポートに Link Incident Record (LIR) を送信できます。

Cisco MDS 9000 ファミリの FICON 対応スイッチでは、RLIR Extended Link Service (ELS) から検出された LIR が、Established Registration List (ERL) に登録済みのメンバーに送信されます。

マルチスイッチトポロジの場合、Distribute Registered Link Incident Record (DRLIR) の Inter-Link Service (ILS) が RLIR ELS とともに、到達可能なすべてのリモートドメインに送信されます。スイッチは DRLIR ILS を受信すると、RLIR ELS を抽出して ERL のメンバーに送信します。

RLIR ELS の受信に関与する Nx ポートは、Link Incident Record Registration (LIRR) ELS 要求をスイッチ上の管理サーバーに送信します。RLIR は VSAN 単位で処理されます。

copy running-config startup-config コマンドを入力すると、RLIR データが永続ストレージに書き込まれます。

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 **copy** すると、RLIR データが永続的ストレージに書き込まれます。

RLIR 優先ホストの指定

Cisco MDS SAN-OS Release 3.0(3) では、RLIR フレームを受信する優先ホストを指定できます。MDS スイッチが優先ホストに RLIR フレームを送信するのは、次の条件が満たされた場合だけです。

- VSAN 内に、登録機能が「always receive」に設定され、RLIR に登録されているホストがない。VSAN に「always receive」として登録されているホストが1つ以上ある場合、RLIR はそれらのホストにのみ送信され、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、登録機能が「conditionally receive」に設定されて登録されている。



Note 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は優先ホストが 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。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、スイッチは登録機能が「conditionally receive」に設定されている VSAN のホストの1つに RLIR フレームを送信します。

VSAN の RLIR 優先ホストを指定するには、次の手順を実行します。

ステップ 1 switch# config terminal

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# rlr preferred-cond fcid 0x772c00 vsan 5

VSAN 5 の RLIR 優先ホストとして FC ID 0x772c00 を指定します。(FC ID 0x772c00 は一例です。)

ステップ 3 switch(config)# no rlr preferred-cond fcid 0x654321 vsan 2

(任意) VSAN 5 の RLIR 優先ホストとして FC ID 0x772c00 を削除します。

RLIR 優先ホスト設定を表示するには、**show rlir erl** コマンドを使用します。

```
switch# show rlir erl
Established Registration List for VSAN: 5
-----
FC-ID LIRR FORMAT REGISTERED FOR
-----
0x772c00 0x18 conditional receive(*)
0x779600 0x18 conditional receive
0x779700 0x18 conditional receive
0x779800 0x18 conditional receive
Total number of entries = 4
(*) - Denotes the preferred host
```

RLIR 情報の表示

show rlir statistics コマンドは、LIRR、RLIR、および DRLIR フレームの完全な統計情報を表示します。受信フレーム数、送信フレーム数、および拒否フレーム数が表示されます。特定の VSAN の VSAN 統計情報を取得するため、VSANID を指定します。VSANID を指定しないと、アクティブなすべての VSAN の統計情報が表示されます（例 [すべての VSAN の RLIR 統計情報の表示, on page 313](#) および [指定した VSAN の RLIR 統計情報の表示, on page 314](#) を参照）。

すべての VSAN の RLIR 統計情報の表示

```
switch# show rlir statistics
Statistics for VSAN: 1
-----
Number of LIRR received           = 0
Number of LIRR ACC sent           = 0
Number of LIRR RJT sent           = 0
Number of RLIR sent               = 0
Number of RLIR ACC received       = 0
Number of RLIR RJT received       = 0
Number of DRLIR received          = 0
Number of DRLIR ACC sent          = 0
Number of DRLIR RJT sent          = 0
Number of DRLIR sent              = 0
Number of DRLIR ACC received      = 0
Number of DRLIR RJT received      = 0
Statistics for VSAN: 100
-----
Number of LIRR received           = 26
Number of LIRR ACC sent           = 26
Number of LIRR RJT sent           = 0
Number of RLIR sent               = 815
Number of RLIR ACC received       = 815
Number of RLIR RJT received       = 0
Number of DRLIR received          = 417
Number of DRLIR ACC sent          = 417
Number of DRLIR RJT sent          = 0
Number of DRLIR sent              = 914
Number of DRLIR ACC received      = 828
Number of DRLIR RJT received      = 0
```

指定した VSAN の RLIR 統計情報の表示

```
switch# show rlir statistics vsan 4
Statistics for VSAN: 4
-----
Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received    = 0
Number of DRLIR ACC sent    = 0
Number of DRLIR RJT sent    = 0
Number of DRLIR sent        = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0
```

show rlir erl コマンドは、スイッチで RLIR 受信のために登録されている Nx ポートのリストを表示します。VSANID を指定しない場合は、すべてのアクティブ VSAN の詳細が表示されます（例 [すべての ERL の表示, on page 314](#) および [指定された VSAN の ERL の表示, on page 315](#) を参照）。

すべての ERL の表示

```
switch# show rlir erl
Established Registration List for VSAN: 2
-----
FC-ID          LIRR FORMAT    REGISTERED FOR
-----
0x0b0200      0x18           always receive
Total number of entries = 1
Established Registration List for VSAN: 100
-----
FC-ID          LIRR FORMAT    REGISTERED FOR
-----
0x0b0500      0x18           conditional receive
0x0b0600      0x18           conditional receive
Total number of entries = 2
```

[すべての ERL の表示, on page 314](#) では [Registered For] 列に FC ID が conditional receive であると示されている場合に、後続の RLIR の有効な受信者として送信元ポートが登録されます。他の ERL の受信者が選択されない場合にのみ、この送信元ポートが RLIR の受信者として選択されます。

[すべての ERL の表示, on page 314](#) では [Registered For] 列に FC ID が always receive であると示されている場合に、後続の RLIR の有効な受信者として送信元ポートが登録されます。この送信元ポートは LIR の受信者として常に選択されます。



Note どの N ポートにも always receive RLIR が登録されていない場合、または RLIR の配信がいずれかのポートで失敗する場合は、conditional receive RLIR に登録されているポートに RLIR が送信されます。

指定された VSAN の ERL の表示

```
switch# show rlir erl vsan 100
Established Registration List for VSAN: 100
-----
FC-ID          LIRR FORMAT    REGISTERED FOR
-----
0x0b0500      0x18           conditional receive
0x0b0600      0x18           conditional receive
Total number of entries = 2
```



Note LIR 履歴の表示, on page 315 から 指定されたポート番号の最近の LIR の表示, on page 316 では、ホストのタイムスタンプ (*で示す) が使用可能な場合、スイッチのタイムスタンプと共に出力されます。ホストのタイムスタンプが使用可能ではない場合は、スイッチのタイムスタンプだけが出力されます。

LIR 履歴の表示

```
switch# show rlir history
Link incident history
-----
*Host Time Stamp
Switch Time Stamp          Port    Interface    Link Incident
-----
*Sun Nov 30 21:47:28 2003
Sun Nov 30 13:47:55 2003      2      fc1/2      Implicit Incident
*Sun Nov 30 22:00:47 2003
Sun Nov 30 14:01:14 2003      2      fc1/2      NOS Received
*Sun Nov 30 22:00:55 2003
Sun Nov 30 14:01:22 2003      2      fc1/2      Implicit Incident
*Mon Dec 1 20:14:26 2003
Mon Dec 1 12:14:53 2003      4      fc1/4      Implicit Incident
*Mon Dec 1 20:14:26 2003
Mon Dec 1 12:14:53 2003      4      fc1/4      Implicit Incident
*Thu Dec 4 04:43:32 2003
Wed Dec 3 20:43:59 2003      2      fc1/2      NOS Received
*Thu Dec 4 04:43:41 2003
Wed Dec 3 20:44:08 2003      2      fc1/2      Implicit Incident
*Thu Dec 4 04:46:53 2003
Wed Dec 3 20:47:20 2003      2      fc1/2      NOS Received
*Thu Dec 4 04:47:05 2003
Wed Dec 3 20:47:32 2003      2      fc1/2      Implicit Incident
*Thu Dec 4 04:48:07 2003
Wed Dec 3 20:48:34 2003      2      fc1/2      NOS Received
```

```
*Thu Dec 4 04:48:39 2003
Wed Dec 3 20:49:06 2003      2      fc1/2  Implicit Incident
*Thu Dec 4 05:02:20 2003
Wed Dec 3 21:02:47 2003      2      fc1/2  NOS Received
...
```

指定されたインターフェイスの最近の LIR の表示

```
switch# show rllr recent interface fc1/1-4
Recent link incident records
-----
Host Time Stamp          Switch Time Stamp      Port Intf  Link Incident
-----
Thu Dec 4 05:02:29 2003  Wed Dec 3 21:02:56 2003  2    fc1/2  Implicit Incident
Thu Dec 4 05:02:54 2003  Wed Dec 3 21:03:21 2003  4    fc1/4  Implicit Incident
```

指定されたポート番号の最近の LIR の表示

```
switch# show rllr recent portnumber 1-4
Recent link incident records
-----
Host Time Stamp          Switch Time Stamp      Port Intf  Link Incident
-----
Thu Dec 4 05:02:29 2003  Wed Dec 3 21:02:56 2003  2    fc1/2  Implicit Incident
Thu Dec 4 05:02:54 2003  Wed Dec 3 21:03:21 2003  4    fc1/4  Implicit Incident
```

Cisco SAN-OS Release 3.0(3) 以降、**show rllr history** コマンド出力には、他のスイッチから DRLIR として受信したリモートリンク インシデントが示されます。RLIR は、以前の Cisco NX-OS リリースと同様に DRLIR の結果として生成されます ([Cisco SAN-OS Release 3.0\(3\) の LIR 履歴の表示, on page 316](#) を参照)。

Cisco SAN-OS Release 3.0(3) の LIR 履歴の表示

```
switch# show rllr history
Link incident history
-----
Host Time Stamp          Switch Time Stamp      VSAN  Domain  Port  Intf
Link Incident            Loc/Rem
-----
Sep 20 12:42:44 2006     Sep 20 12:42:44 2006  ****   ****   0x0b  fc1/12
Loss of sig/sync        LOC
Reported Successfully to: [0x640001] [0x640201]
Sep 20 12:42:48 2006     Sep 20 12:42:48 2006  ****   ****   0x0b  fc1/12
Loss of sig/sync        LOC
Reported Successfully to: [0x640001] [0x640201]
*** ** **:**:** ****   Sep 20 12:42:51 2006  1001   230    0x12  ****
Loss of sig/sync        REM
Reported Successfully to: [0x640001] [0x640201]
Sep 20 12:42:55 2006     Sep 20 12:42:55 2006  ****   ****   0x0b  fc1/12
Loss of sig/sync        LOC
Reported Successfully to: None [No Registrations]
*** ** **:**:** ****   Sep 20 12:45:56 2006  1001   230    0x12  ****
```

```

Loss of sig/sync      REM
  Reported Successfully to: None [No Registrations]
  *** ** **:**:** **** Sep 20 12:45:56 2006    1001    230    0x12    ****
Loss of sig/sync      REM
  Reported Successfully to: None [No Registrations]
  Sep 20 12:52:45 2006    Sep 20 12:52:45 2006    ****    ****    0x0b    fc1/12
Loss of sig/sync      LOC
  Reported Successfully to: None [No Registrations]
**** - Info not required/unavailable

```

RLIR 情報のクリア

指定された VSAN の既存の統計情報をすべてクリアするには、**clear rlir statistics** コマンドを使用します。

```
switch# clear rlir statistics vsan 1
```

すべてのインターフェイスのすべてのリンク インシデント レコードが記録されている RLIR 履歴をクリアするには、**clear rlir history** コマンドを使用します。

```
switch# clear rlir history
```

指定したインターフェイスの最近の RLIR 情報をクリアするには、**clear rlir recent interface** コマンドを使用します。

```
switch# clear rlir recent interface fc 1/2
```

指定したポート番号の最近の RLIR 情報をクリアするには、**clear rlir recent portnumber** コマンドを使用します。

```
switch# clear rlir recent portnumber 16
```

FICON コンフィギュレーション ファイル

各 FICON 対応 VSAN 上で、最大 16 個の FICON コンフィギュレーション ファイルを（永続ストレージに）保存できます。ファイルフォーマットの所有権は IBM に帰属します。これらのファイルは、帯域内 CUP プロトコルを使用して IBM ホストから読み取りおよび書き込みできます。また、これらの FICON コンフィギュレーション ファイルを処理するには、Cisco MDS CLI を使用します。



Note 名前が同じ複数の FICON コンフィギュレーション ファイルは、それぞれ別個の VSAN に属している限り、同一のスイッチに配置できます。たとえば、VSAN 1 と VSAN 3 の両方で、XYZ という名前のコンフィギュレーション ファイルを作成することもできます。

VSAN で FICON 機能がイネーブルになっているときは常に、IPL という名前のスタートアップ FICON コンフィギュレーション ファイルが使用されます。この IPL ファイルは、VSAN で

FICON をイネーブルにするとただちに、デフォルトのコンフィギュレーションで作成されます。



Caution VSAN 上で FICON をディセーブルにした場合、FICON コンフィギュレーションファイルはすべて失われます。いったん失われると復元できません。

FICON コンフィギュレーション ファイルには、次のコンフィギュレーションが実装ポートアドレスごとに格納されています。

- ブロック
- 禁止マスク
- ポート アドレス名



Note Cisco MDS スイッチで使用される標準コンフィギュレーション ファイルには、VSAN の FICON 対応属性、ポートチャネル インターフェイスと FCIP インターフェイスに対するポート番号のマッピング、ポート番号とポートアドレスのマッピング、ポートおよびトランクで許可されている各ポートの VSAN 設定、順序保証、スタティック ドメイン ID の設定、ファブリック バインディング設定などが格納されています。

Cisco MDS スイッチで使用される標準コンフィギュレーション ファイルの詳細については、『Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide』を参照してください。

このセクションは、次のトピックで構成されています。

FICON コンフィギュレーション ファイルの概要

コンフィギュレーション ファイルに同時にアクセスできるのは、常に 1 人のユーザーだけです。

- このファイルにユーザー 1 がアクセスしている間、ユーザー 2 はアクセスできません。
- このファイルへのアクセスを試みたユーザー 2 に対しては、エラーが出されます。
- ユーザー 1 が非アクティブ状態のまま 15 秒が過ぎると、ファイルは自動的に閉じられ、許可されている他のユーザーが使用できるようになります。

スイッチへのアクセスを許可されているホスト、SNMP、または CLI ユーザーはいずれも、FICON コンフィギュレーション ファイルにアクセスできます。Cisco NX-OS ソフトウェアのロック メカニズムによって、同時アクセスは 1 人のユーザーだけに許可されます。このロックは、新規に作成されたファイル、および以前に保存されたファイルに適用されます。どのファイルにアクセスする際にも、あらかじめファイルをロックし、ファイルキーを取得する必要があります。ロック要求が発生するたびに毎回、新しいファイルキーがロック メカニズムによって使用されます。15 秒間のロック タイムアウト期限が切れると、キーは廃棄されます。ロック タイムアウト値は変更できません。

保存済みコンフィギュレーション ファイルの実行コンフィギュレーションへの適用

保存されているファイルの設定を実行コンフィギュレーションに適用するには、**ficon vsan number apply file filename** コマンドを使用します。

```
switch# ficon vsan 2 apply file SampleFile
```

FICON コンフィギュレーション ファイルの編集

コンフィギュレーション ファイル サブモードでは、FICON コンフィギュレーション ファイルの作成および編集が許可されます。指定したファイルが存在しない場合は、作成されます。保存可能なファイル数は最大 16 個です。各ファイル名には、最大 8 文字の英数字を使用できます。

指定された FICON コンフィギュレーション ファイルの内容を編集するには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ficon vsan 2**

```
switch(config-ficon)#
```

VSAN 2 で FICON を有効にします。

ステップ 3 switch(config-ficon)# **file IplFile1**

```
switch(config-ficon-file)#
```

VSAN 2 の FICON コンフィギュレーション ファイル **IplFile1** にアクセスします。このファイルが存在しない場合は、作成されます。

Note すべての FICON ファイル名は、最大 8 文字の英数字に制限されています。

ステップ 4 switch(config-ficon)# **no file IplFileA**

(任意) 以前に作成された FICON コンフィギュレーション ファイルを削除します。

ステップ 5 switch(config-ficon-file)# **portaddress 3**

```
switch(config-ficon-file-portaddr)#
```

ポート アドレス 3 のサブモードを開始して、**IplFile1** という名前のコンフィギュレーション ファイルの内容を編集します。

Note 実行コンフィギュレーションは現在の設定に適用されません。設定が適用されるのは、**ficon vsan number apply file filename** コマンドが実行される場合だけです。

ステップ 6 switch(config-ficon-file-portaddr)# **prohibit portaddress 5**

コンフィギュレーション ファイル IplFile1 の内容を編集し、ポート アドレス 5 に対してポート アドレス 3 へのアクセスを禁止します。

ステップ 7 switch(config-ficon-file-portaddr)# **block**

コンフィギュレーション ファイル IplFile1 の内容を編集し、特定のポート アドレス範囲をブロックし、運用停止状態で維持します。

ステップ 8 switch(config-ficon-file-portaddr)# **name P3**

コンフィギュレーション ファイル IplFile1 の内容を編集し、P3 という名前をポート アドレス 3 に割り当てます。この名前が存在ししない場合は、作成されます。存在する場合は上書きされます。

FICON コンフィギュレーション ファイルの表示

すべての FICON コンフィギュレーション ファイルの内容を表示するには、**show ficon vsan vsan-id file all** コマンドを使用します。

```
switch# show ficon vsan 2 file all
File IPL      is locked
FICON configuration file IPLFILEA in vsan 2
Description:
  Port address 0(0)
    Port name is
    Port is not blocked
    Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)
  Port address 1(0x1)
    Port name is
    Port is not blocked
    Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)
Port address 2(0x2)
  Port name is
  Port is not blocked
  Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)
Port address 3(0x3)
  Port name is P3
  Port is blocked
  Prohibited port addresses are 5,250-253,255(0x5,0xfa-0xfd,0xff)
..
```

特定の FICON コンフィギュレーション ファイルの内容を表示するには、**show ficon vsan vsan-id file name** コマンドを使用します。

```
switch# show ficon vsan 2 file name IPLfilea
FICON configuration file IPLFILEA in vsan 2
Description:
  Port address 0(0)
    Port name is
    Port is not blocked
    Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)
Port address 1(0x1)
  Port name is
  Port is not blocked
```



```

    Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)
Port address 2(0x2)
  Port name is
  Port is not blocked
  Prohibited port addresses are 250-253,255(0xfa-0xfd,0xff)
Port address 3(0x3)
  Port name is P3
  Port is blocked
  Prohibited port addresses are 5,250-253,255(0x5,0xfa-0xfd,0xff)

```

特定のFICONポートのFICONコンフィギュレーションファイルの情報を表示するには、**show ficon vsan vsan-id file name filename portaddress** コマンドを使用します。

```

switch# show ficon vsan 2 file name IPLfilea portaddress 3
FICON configuration file IPLFILEA in vsan 2
Description:
  Port address 3(0x3)
  Port name is P3
  Port is blocked
  Prohibited port addresses are 5,250-253,255(0x5,0xfa-0xfd,0xff)

```

FICON コンフィギュレーション ファイルのコピー

既存のFICONコンフィギュレーションファイルをコピーするには、EXECモードで**ficon vsan vsan-id copy file existing-file-name save-as-file-name** コマンドを使用します。

```
switch# ficon vsan 20 copy file IPL IPL3
```

既存のコンフィギュレーションファイルのリストを表示するには、**show ficon vsan vsan-id** コマンドを実行します。

```

switch# show
ficon vsan 20
Ficon information for VSAN 20
  Ficon is online
  VSAN is active
  Host port control is Enabled
  Host offline control is Enabled
  User alert mode is Disabled
  SNMP port control is Enabled
  Host set director timestamp is Enabled
  Active=Saved is Enabled
  Number of implemented ports are 250
  Key Counter is 5
  FCID last byte is 0
  Date/Time is same as system time (Wed Dec 3 20:10:45.924591 2003)
  Device Allegiance not locked
  Codepage is us-canada
Saved configuration files
  IPL
  IPL3

```

ポート スワッピング

FICON ポート スワッピング機能は、メンテナンス専用を提供されています。

FICON ポート スワッピング機能を実行すると、*old-port-number* および *new port-number* に関連付けられているすべての設定（例：VSAN 設定）がスワッピングされます。

Cisco MDS スイッチは、実在しないポートに対してもポートスワッピングを実行できますが、その際は次のような制約が伴います。

- スワッピング対象は、FICON 固有の設定（禁止、ブロック、およびポートアドレスのマッピング）だけです。
- 他のシステム設定はスワッピングされません。
- 他のシステム設定はいずれも、既存のポートでだけ維持されます。
- 無制限の加入過多率がイネーブルになっているモジュール内のポートを、加入過多率が制限されているモジュール内のポートとスワッピングすると、帯域幅が劣化することがあります。



Tip **Active=Saved** チェックボックスをオンにすると、任意の FICON VSAN 上で **active equals saved** が有効になり、スワッピングされた設定が自動的にスタートアップ コンフィギュレーションに保存されます。それ以外の場合は、ポートをスワッピングした後すぐに、実行コンフィギュレーションを明示的に保存しておく必要があります。

いったんポートをスワッピングし終わると、次の処理が自動的に実行されます。

- 古いポートと新しいポートがシャットダウンされます。
- ポート設定がスワッピングされます。

ポートを稼働状態にする際は、対象のポートを明示的にシャットダウンしてから、トラフィックを再開する必要があります。



Note 最新の FICON 情報を表示するには、[Refresh] ボタンをクリックする必要があります。実行コンフィギュレーションの自動保存, [on page 305](#)を参照してください。

ficon swap portnumber コマンドは、対象の 2 つのポートにのみ関連します。この VSAN に依存しないコマンドを EXEC モードで実行する必要があります。Cisco MDS NX-OS は、ポートスワップを実行する前に VSAN でポート番号の重複を調べます。

ficon swap portnumber old-port-number new-port-number after swap noshut コマンドを指定してポートを起動する場合は、**no shutdown** コマンドを明示的に実行してトラフィックを再開する必要があります。

このセクションは、次のトピックで構成されています。

ポートスワッピングの概要

FICON ポート スワッピング機能を使用する際は必ず、次のガイドラインに従ってください。

- 論理ポート（ポートチャンネル、FCIP リンク）に対しては、ポートスワッピングがサポートされません。 *old-port-number* と *new-port-number* はいずれも、論理ポートとして設定できません。
- ポートチャンネルに属する物理ポート間では、ポートスワッピングがサポートされません。 *old-port-number* と *new-port-number* はいずれも、ポートチャンネルに属する物理ポートとしては設定できません。
- ポートスワッピングを実行する前に、Cisco NX-OS ソフトウェアは互換性チェックを実行します。2つのポート設定に互換性がないと、ポートスワッピングが拒否され、該当する理由コードが出力されます。たとえば、BB_credits に 25 が割り当てられているポートと、BB_credits（設定不能なパラメータ）に許可されている最大値が 12 の OSM ポートとをスワッピングしようとした場合、ポートスワッピング操作は拒否されます。
- ポートスワッピングを実行する前に、Cisco NX-OS ソフトウェアは互換性チェックを実行して、拡張 BB_credits 設定を検証します。
- ポートに（一部の非互換パラメータ用の）デフォルト値がある場合、ポートスワッピング操作が許可され、ポートはそのデフォルト値を保持します。
- ポートスワッピングには、ポートトラッキング情報が取り込まれません。ポートトラッキング情報は、個別に設定する必要があります（『Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide』を参照）。



Note 32 ポート モジュール ガイドラインは、ポートスワップ設定にも適用されます（『Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide』を参照）。

ポートスワッピング

スイッチ上に重複するポート番号がない場合は、物理ファイバチャンネルポート（ポート番号を除く）を次の手順でスワップできます。

ステップ 1 EXEC モードで **ficon swap portnumber old-port-number new-port-number** コマンドを発行します。

Note MDS スイッチで、コマンドに指定されている *old-port-number* または *new-port-number* と同じポート番号のインターフェイスが複数ある場合、**ficon swap portnumber** コマンドは失敗する可能性があります。

指定したポートはシャットダウンされます。

ステップ 2 2つのポート間の前面パネルポートケーブルを物理的に交換できます。

ステップ 3 各ポートで **no shutdown** コマンドを実行し、トラフィックフローを許可します。

Note **ficon swap portnumber old-port-number new-port-number after swap noshut** コマンドを指定すると、ポートは自動的に初期化されます。

ポート番号が重複しているスイッチのポートのスワッピング

スイッチで重複するポート番号がある場合は、物理ファイバチャネルポート（重複するポート番号を含む）を次の手順でスワップできます。

ステップ 1 EXEC モードで **ficon swap interface old-interface new-interface** コマンドを実行します。

指定したインターフェイスはシャットダウンされます。

ステップ 2 2つのポート間の前面パネルポート ケーブルを物理的に交換できます。

ステップ 3 各ポートで **no shutdown** コマンドを実行し、トラフィックフローを許可します。

Note **ficon swap interface old-interface new-interface after swap noshut** コマンドを指定すると、ポートは自動的に初期化されます。

FICON テープ アクセラレーション

テープ デバイスには順次性があるため、FCIP リンクを介したテープ デバイスに対して I/O 操作が実行されるたびに、FCIP リンクに遅延が発生します。FCIP リンクを介したラウンドトリップ時間が増えると、スループットは著しく減少するため、結果としてバックアップ時間は長くなります。また、各 I/O 操作を終えてから次の I/O に達するまで、テープ デバイスはアイドル状態になります。I/O 操作が仮想テープを対象する場合を除き、テープ ヘッドの操作開始と停止によってテープ寿命が縮まります。

Cisco MDS NX-OS ソフトウェアは、次のリンクを介した FICON テープ書き込み操作に対してアクセラレーションを提供します。

- メインフレーム ドライブとネイティブテープ ドライブ（IBM と Sun/STK の両方）の間のリンク
- Virtual Storage Management（VSM）とテープ ドライブ（Sun/STK）の間のバックエンドリンク

FCIP を介した FICON テープ アクセラレーションにより、次のようなメリットがあります。

- アイドル時間が短縮される結果、テープ デバイスが効率的に利用されます。
- 遅延が増加したときのスループットの持続性が向上します。
- FCP テープ アクセラレーションと似ていますが、競合は発生しません。



Note FCIP を介した FICON テープ読み取りアクセラレーションは、Cisco MDS NX-OS Release 5.0(1) 以降でサポートされています。詳細については、[FICON テープ読み取りアクセラレーション設定, on page 327](#)を参照してください。

Figure 59: IBM/StorageTek (STK) ライブラリに直接アクセスするホスト, on page 325 ~ Figure 62: ピアツーピア Virtual Tape Server (VTS) にアクセスするホスト, on page 326 に、サポートされている設定を示します。

Figure 59: IBM/StorageTek (STK) ライブラリに直接アクセスするホスト



Figure 60: スタンドアロン IBM-Virtual Tape Server (VTS) /STK-Virtual Shared Memory (VSM) にアクセスするホスト

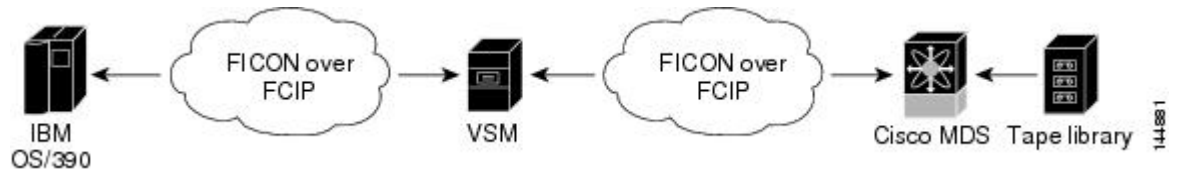


Figure 61: ピアツーピア Virtual Tape Server (VTS) にアクセスするホスト

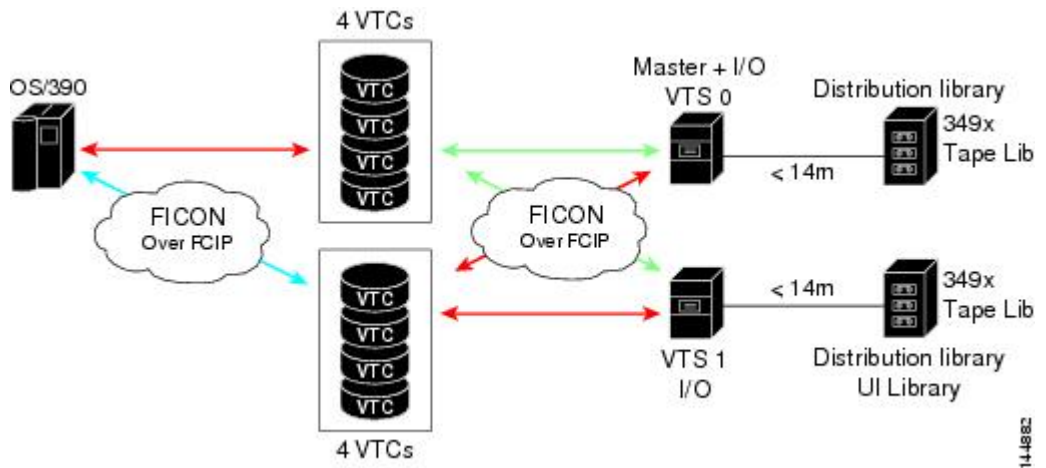
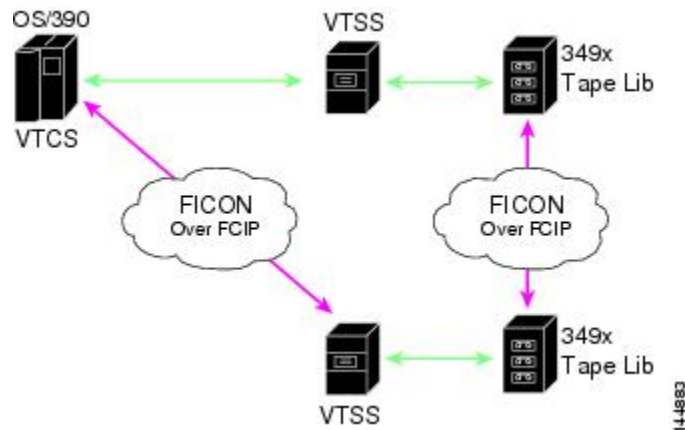


Figure 62: ピアツーピア Virtual Tape Server (VTS) にアクセスするホスト



Note FCIP テープ アクセラレーションの詳細については、『Cisco MDS 9000 Family NX-OS IP Services Configuration Guide』を参照してください。

FICON テープ アクセラレーション設定

FICON テープ アクセラレーションの設定に関しては、次のような考慮事項があります。

- 標準 FICON 設定だけでなく、FICON テープ アクセラレーションも、FCIP インターフェイスの両端でイネーブルにしておく必要があります。一端だけで FICON テープ アクセラレーションをイネーブルにした場合、アクセラレーションは発生しません。
- FICON テープ アクセラレーションは、VSAN 単位でイネーブルになります。
- 複数の ISL が同一の VSAN 内に存在する（ポートチャネルまたは FSPF でロードバランスされている）場合、FICON テープ アクセラレーション機能は無効になります。
- 同じ FCIP インターフェイス上で、ファイバチャネル書き込みアクセラレーションと FICON テープ アクセラレーションの両方をイネーブルに設定できます。
- FICON テープ アクセラレーションをイネーブルまたはディセーブルにすると、FCIP インターフェイス上のトラフィックが中断されます。

FICON テープ アクセラレーションを設定するには、次の手順を実行します。

ステップ 1 switch# **config t**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **interface fcip 2**

```
switch(config-if)#
```

FCIP インターフェイスを指定し、インターフェイス 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-if)# **fiction-tape-accelerator vsan 100**

This configuration change will disrupt all traffic on the FCIP interface in all VSANs. Do you wish to continue? [no] **y**

FCIP インターフェイスを介した FICON テープ アクセラレーションをイネーブルにします。

ステップ 4 switch(config-if)# **no fiction-tape-accelerator vsan 100**

This configuration change will disrupt all traffic on the FCIP interface in all VSANs. Do you wish to continue? [no] **y**

FCIP インターフェイスを介した FICON テープ アクセラレーションをディセーブルにします (デフォルト)。

What to do next

show running-config コマンドを使用して、FCIP 設定で FICON テープ アクセラレーションを確認します。

```
switch# show running-config | begin "interface fcip"
interface fcip2
  fiction-tape-accelerator vsan 100
  no shutdown
...
```

FICON テープ読み取りアクセラレーション設定

FICON テープ アクセラレーションに適用される設定のガイドラインと制限はすべて、FICON テープ読み取りアクセラレーションにも適用されます。FICON テープ アクセラレーションと FICON テープ読み取りアクセラレーションは共存可能です。

FICON テープ読み取りアクセラレーションを有効にするには、次の手順を実行します。

ステップ 1 switch# **config t**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **interface fcip 2**

switch(config-if)#

FCIP インターフェイスを指定し、インターフェイス 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-if)# **fiction-tape-read-accelerator**

This configuration change will disrupt all traffic on the FCIP interface in all VSANs. Do you wish to continue? [no]

FCIP インターフェイスを介した FICON テープ読み取りアクセラレーションを有効にします。

ステップ 4 switch(config-if)# no ficon-tape-read-accelerator

```
This configuration change will disrupt all traffic on the FCIP interface in all VSANs. Do you wish to continue? [no]
```

FCIP インターフェイスを介した FICON テープ読み取りアクセラレーションを無効にします (デフォルト)。

XRC アクセラレーションの設定

IBM z/OS Global Mirror eXtended Remote Copy (XRC) は、MSM-18+4 モジュールでサポートされています。XRC を正しく機能させるには、FCIP トンネルインターフェイスの両端で XRC アクセラレーションをイネーブルにする必要があります。XRC アクセラレーションはデフォルトではディセーブルです。

XRC テープ アクセラレーションを有効にするには、次の手順を実行します。

ステップ 1 switch# config t

```
switch(config)#
```

コンフィギュレーションモードを開始します。

ステップ 2 switch(config)# interface fcip 2

```
switch(config)#
```

FCIP トンネルインターフェイスを指定し、インターフェイス 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-if)# ficon-xrc-emulator

```
switch(config)#
```

FCIP インターフェイスを介した XRC アクセラレーションを有効にします。

ステップ 4 switch(config-if)# no ficon-xrc-emulator

```
switch(config)#
```

FCIP トンネルインターフェイスを介した XRC アクセラレーションを無効にします (デフォルト)。

Note XRC アクセラレーションと FICON テープ アクセラレーションは、同一の FCIP トンネルインターフェイス上ではイネーブルにできないため、同一の VSAN 上には存在できません。

FICON VSAN のオフライン状態への移行

VSAN で停止する必要があるすべてのポートをログアウトするには、EXEC モードで **ficon vsan vsan-id offline** コマンドを実行します。

オフライン状態を解除し、ポートが再びログオンできるようにするには、EXEC モードで EXEC レベルの **ficon vsan vsan-id online** コマンドを実行します。



Note このコマンドは、このコマンドの発行が許可されているホストから発行できます（ホストでスイッチをオフラインに移行できるようにするには、[on page 302](#) を参照）。

CUP インバンド管理

CUP プロトコルを介して、アクセスコントロールの設定が行われ、メインフレームコンピュータから統合型ストレージ管理機能が提供されます。Cisco MDS 9000 FICON 対応スイッチは、IBM CUP 規格に適合しており、IBM S/A OS/390 I/O 操作コンソールを使用した帯域内管理が可能です。



Note CUP 仕様の所有権は IBM に帰属します。

CUP は Cisco MDS 9000 ファミリのスイッチおよびディレクタによってサポートされます。CUP 機能を使用することにより、メインフレームで Cisco MDS スwitch を管理できます。

ホスト通信用に、制御（例：ポートのブロック/ブロック解除）、モニタリング、エラーレポートなどの機能が用意されています。

このセクションは、次のトピックで構成されています。

ゾーンへの CUP の配置

ゾーンに CUP を配置するには、次の手順を実行します。

ステップ 1 必要な VSAN に許可するデフォルト ゾーンを設定します。

```
switch# config terminal
switch(config)# zone default-zone permit vsan 20
```

ステップ 2 必要な VSAN に対して **show fcns database** コマンドを発行し、必須 FICON CUP WWN を取得します。

```
switch# show fcns database vsan 20
VSAN 20:
```

```

-----
FCID          TYPE  PWWN                               (VENDOR)          FC4-TYPE:FEATURE
-----
0x0d0d00     N    50:06:04:88:00:1d:60:83 (EMC)             FICON:CU
0x0dfe00     N    25:00:00:0c:ce:5c:5e:c2
(Cisco)      FICON:CUP
0x200400     N    50:05:07:63:00:c2:82:d3 (IBM)             scsi-fcp FICON:CU f..
0x200800     N    50:05:07:64:01:40:15:0f (IBM)             FICON:CH
0x20fe00     N    20:00:00:0c:30:ac:9e:82 (Cisco)             FICON:CUP
Total number of entries = 5

```

Note このファブリック内に複数の FICON:CUP WWN が存在する場合は、所定のゾーンに FICON:CUP WWN の pWWN をすべて追加する必要があります。前述の出力例には複数の FICON:CUP が含まれており、これはカスケード設定を示しています。

ステップ 3 示されている FICON:CUP WWN をゾーン データベースに追加します。

```

switch(config)# zone name Zone1 vsan 20
switch(config-zone)# member pwn 25:00:00:0c:ce:5c:5e:c2

```

制御ユニットの情報の表示

[制御ユニットの情報の表示, on page 330](#) に、設定されている制御デバイスの情報を示します。

制御ユニットの情報の表示

```

switch# show ficon control-device sb3
Control Unit Image:0x80b9c2c
VSAN:20 CU:0x20fe00 CUI:0 CUD:0 CURLP:(nil)
ASYNC LP:(nil) MODE:1 STATE:1 CQ LEN:0 MAX:0
PRIMARY LP: VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0
ALTERNATE LP: VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0
Logical Path:0x80b9fb4
VSAN:20 CH:0x200600 CHI:15 CU:0x20fe00 CUI:0 STATE:1 FLAGS:0x1
LINK: OH:0x0 OC:0x0 IH:0x0 IC:0x0
DEV: OH:0x0 OC:0x0 IH:0x0 IC:0x0
SENSE: 00 00 00 00 00 00 00 00 46
        30 20 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00
IUI:0x0 DHF:0x0 CCW:0x0 TOKEN:0x0 PCCW:0x0 FCCW:0x0 PTOKEN:0x0 FTOKEN:0x0
CMD:0x0 CCW_FLAGS:0x0 CCW_COUNT:0 CMD_FLAGS:0x0 PRIO:0x0 DATA_COUNT:0
STATUS:0x0 FLAGS:0x0 PARAM:0x0 QTP:0x0 DTP:0x0
CQ LEN:0 MAX:0 DESTATUS:0x0

```

FICON 情報の表示

このセクションは、次のトピックで構成されています。

FICON アラートの受信

設定された FICON 情報の表示, [on page 331](#) では、ユーザーアラートモードが Enabled であり、FICON 設定の変更を示すアラートを受信することが出力に示されています。

設定された FICON 情報の表示

```
switch# show ficon
Ficon information for VSAN 20
  Ficon is online
  VSAN is active
  Host port control is Enabled
  Host offline control is Enabled
  User alert mode is Enabled
  SNMP port control is Enabled
  Host set director timestamp is Enabled
  Active=Saved is Disabled
  Number of implemented ports are 250
  Key Counter is 73723
  FCID last byte is 0
  Date/Time is set by host to Sun Jun 26 00:04:06.991999 1904
  Device allegiance is locked by Host
  Codepage is us-canada
  Saved configuration files
    IPL
    _TSIRN00
```

FICON ポート アドレス情報の表示

例 [ポートアドレス情報の表示, on page 331](#) ~ [ポートアドレスカウンタ情報の表示, on page 332](#) では、FICON ポート アドレス情報を表示します。

ポート アドレス情報の表示

```
switch# show ficon vsan 2 portaddress
Port Address 1 is not installed in vsan 2
  Port number is 1, Interface is fc1/1
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255
Port Address 2 is not installed in vsan 2
  Port number is 2, Interface is fc1/2
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255
...
Port Address 249 is not installed in vsan 2
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255
Port Address 250 is not installed in vsan 2
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255
```

使用可能なポート番号の表示

```
switch# show ficon first-available port-number
Port number 129(0x81) is available
```

要約形式でのポート番号情報の表示, [on page 332](#) では、ポート番号がインストールされている場合、対応するインターフェイスが [Interface] 列に示されています。ポート番号がアンインストールされている場合、この列には何も表示されず、アンバインドされているポート番号であることを示します。たとえば、[要約形式でのポート番号情報の表示, on page 332](#) ではアンバインドされているポート番号は 56 です。

要約形式でのポート番号情報の表示

```
switch# show ficon vsan 2 portaddress 50-55 brief
```

Port Address	Port Number	Interface	Admin Blocked	Status	Oper Mode	FCID
50	50	fc2/18	on	fcotAbsent	--	--
51	51	fc2/19	off	fcotAbsent	--	--
52	52	fc2/20	off	fcotAbsent	--	--
53	53	fc2/21	off	fcotAbsent	--	--
54	54	fc2/22	off	notConnected	--	--
55	55	fc2/23	off	up	FL	0xea0000
56	56		off	up	FL	0xea0000

ポートアドレスカウンタ情報の表示, [on page 332](#) では、FICON のバージョン形式 1 (32 ビット形式) のカウンタを表示します。

ポートアドレスカウンタ情報の表示

```
switch# show ficon vsan 20 portaddress 8 counters
```

```
Port Address 8(0x8) is up in vsan 20
Port number is 8(0x8), Interface is fc1/8
Version presented 1, Counter size 32b
242811 frames input, 9912794 words
  484 class-2 frames, 242302 class-3 frames
  0 link control frames, 0 multicast frames
  0 disparity errors inside frames
  0 disparity errors outside frames
  0 frames too big, 0 frames too small
  0 crc errors, 0 eof errors
  0 invalid ordered sets
  0 frames discarded c3
  0 address id errors
116620 frames output, 10609188 words
  0 frame pacing time
  0 link failures
  0 loss of sync
  0 loss of signal
  0 primitive seq prot errors
  0 invalid transmission words
```

```
1 lrr input, 0 ols input, 5 ols output
0 error summary
```

FICON コンフィギュレーション ファイル情報の表示

例 指定した FICON コンフィギュレーション ファイルの内容の表示, on page 333 ~ FICON コンフィギュレーションファイルの指定したポートアドレスの表示, on page 334 では、FICON コンフィギュレーション ファイル情報を表示します。

指定した FICON コンフィギュレーション ファイルの内容の表示

```
switch# show ficon vsan 3 file IPL
FICON configuration file IPL      in vsan 3
  Port address 1
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255
  Port address 2
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255
  Port address 3
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255
  Port address 4
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255
  ...
  Port address 80
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255
  Port address 254
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,81-253,255
```

すべての FICON コンフィギュレーション ファイルの表示

```
switch# show ficon vsan 2
Ficon information for VSAN 2
  Ficon is enabled
  VSAN is active
  Host control is Enabled
  Host offline control is Enabled
  Clock alert mode is Disabled
  User alert mode is Disabled
  SNMP control is Disabled
  Active=Saved is Disabled
  Number of implemented ports are 250
  Key Counter is 9
  FCID last byte is 0
  Date/Time is same as system time(Sun Dec 14 01:26:30.273402 1980)
```

```

Device Allegiance not locked
Codepage is us-canada
Saved configuration files
  IPL
  IPLFILE1

```

FICON コンフィギュレーション ファイルの指定したポート アドレスの表示

```

switch# show ficon vsan 2 file iplfile1 portaddress 1-7
FICON configuration file IPLFILE1 in vsan 2
  Port address 1
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,241-253,255
  Port address 2
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,241-253,255
  Port address 3
    Port name is P3
    Port is not blocked
    Prohibited port addresses are 0,241-253,255
  ...
  Port address 7
    Port name is
    Port is not blocked
    Prohibited port addresses are 0,241-253,255

```

設定された FICON の状態の表示

VSAN で FICON が有効な場合は、その VSAN のポート アドレス情報を表示できます（[FICON が有効な場合の指定したポート アドレスの表示, on page 334](#) を参照）。

FICON が有効な場合の指定したポート アドレスの表示

```

switch# show ficon
vsan 2 portaddress 55
Port Address 55 is not installed in vsan 2
  Port number is 55, Interface is fc2/23
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255
  Admin port mode is FL
  Port mode is FL, FCID is 0xea0000

```

ポート管理状態の表示

例 [管理上ブロック解除されたポートの表示, on page 335](#) ~ [管理上ブロック解除されたポートの表示, on page 335](#) では、FICON ポートの管理状態を表示します。ポートがブロックされた場合、**show ficon vsan number portaddress number** コマンドはポートのブロック ステータスを表示します。特定のポートが禁止されている場合、このコマンドは、禁止されている具体的なポー

ト (3) とデフォルトで禁止されているポート (0, 241～253、および255) も表示します。名前が割り当てられている場合は、その名前も表示されます。

管理上ブロック解除されたポートの表示

```
switch# show ficon vsan 2 portaddress 2
Port Address 2(0x2) is not installed in vsan 2
  Port number is 2(0x2), Interface is fc1/2
  Port name is
  Port is not admin blocked
  Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
  Admin port mode is auto
  Peer is Unknown
```

管理上ブロックされたポートの表示

```
switch# show ficon vsan 2 portaddress 1
Port Address 2(0x2) is not installed in vsan 2
  Port number is 2(0x2), Interface is fc1/2
  Port name is SampleName
  Port is admin blocked
  Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
  Admin port mode is auto
  Peer is Unknown
```

バッファ情報の表示

[指定された VSAN の履歴バッファの表示, on page 335](#) では、[Key Counter] 列に、Cisco MDS スイッチに保持されている 32 ビット値が表示されます。この値は、該当する VSAN のいずれかのポートの状態が変わったときに増加します。キーカウンタ (32 ビット値) は、FICON 関連の設定が変更されたときに増加します。チャンネルプログラムの起動時に、この値がホストプログラムによって増加し、複数のポートに対して操作が実行されることがあります。ディレクトリ履歴バッファには、キーカウンタ値ごとに、変更されたポートアドレス設定のログが記録されます。

ディレクトリ履歴バッファは、前回キーカウンタに値が格納された後にポート状態が変わったかどうかを判別するためのメカニズムを備えています。

指定された VSAN の履歴バッファの表示

```
switch# show ficon vsan 20 director-history
Director History Buffer for vsan 20
-----
Key Counter          Ports Address
                    Changed
-----
74556                43
74557                44
74558                45
74559                46
```

74560	47
74561	48
74562	49
74563	50
74564	51
74565	52
74566	53
74567	54
74568	55
74569	56
74570	57
74571	58
74572	59
74573	60
74574	61
74575	62
74576	63
74577	64
74578	
74579	
74580	1-3, 5, 10, 12, 14-16, 34-40, 43-45, 47-54, 56-57, 59-64
74581	3, 5
74582	64
74583	
74584	1-3, 10, 12, 14-16, 34-40, 43-45, 47-54, 56-57, 59-64
74585	1
74586	2
74587	3

履歴バッファの表示

ディレクトリ履歴バッファの [Key Counter] 列に、Cisco MDS スイッチに保持されている 32 ビット値が表示されます。この値は、該当する VSAN のいずれかのポートの状態が変わったときに増加します。キーカウンタ（32 ビット値）は、FICON 関連の設定が変更されたときに増加します。チャンネルプログラムの起動時に、この値がホストプログラムによって増加し、複数のポートに対して操作が実行されることがあります。ディレクトリ履歴バッファには、キーカウンタ値ごとに、変更されたポートアドレス設定のログが記録されます。

ディレクトリ履歴バッファは、前回キーカウンタに値が格納された後にポート状態が変わったかどうかを判別するためのメカニズムを備えています。

実行コンフィギュレーションの FICON 情報の表示

実行コンフィギュレーション情報の表示, on page 336 では、実行コンフィギュレーションの FICON 関連情報を表示します。

実行コンフィギュレーション情報の表示

```
switch# show running-config
Building Configuration ...
in-order-guarantee
vsan database
  vsan 11 name "FICON11" loadbalancing src-dst-id
  vsan 75 name "FICON75" loadbalancing src-dst-id
```



```

fcdomain domain 11 static vsan 11
fcdomain domain 119 static vsan 75
fcdroplacency network 100 vsan 11
fcdroplacency network 500 vsan 75
feature fabric-binding
fabric-binding database vsan 11
  swwn 20:00:00:0d:ec:01:20:c0 domain 10
fabric-binding database vsan 75
  swwn 20:00:00:0d:ec:00:d6:40 domain 117
fabric-binding activate vsan 11
fabric-binding activate vsan 75
ficon vsan 75
interface port-channel 1
  ficon portnumber 0x80
  switchport mode E
snmp-server user mblair network-admin auth md5 0x688fa3a2e51ba5538211606e59ac292
7 priv 0x688fa3a2e51ba5538211606e59ac2927 localizedkey
snmp-server user wwilson network-admin auth md5 0x688fa3a2e51ba5538211606e59ac292
27 priv 0x688fa3a2e51ba5538211606e59ac2927 localizedkey
snmp-server host 171.71.187.101 traps version 2c public udp-port 1163
snmp-server host 172.18.2.247 traps version 2c public udp-port 2162
vsan database
  vsan 75 interface fc1/1
...
interface mgmt0
  ip address 172.18.47.39 255.255.255.128
  switchport speed 100
  switchport duplex full
no system health
ficon vsan 75
  file IPL

```

スタートアップ コンフィギュレーションの FICON 情報の表示

スタートアップ コンフィギュレーションの表示, on page 337 では、スタートアップ コンフィギュレーションの FICON 関連情報を表示します。

スタートアップ コンフィギュレーションの表示

```

switch# show startup-config
...
ficon vsan 2
file IPL

```

スタートアップ コンフィギュレーション ステータスの表示, on page 337 では、暗黙的に発行された `copy running start` コマンドに対するスイッチの応答を表示します。この場合、明示的に `copy running start` コマンドを再度発行するまで、バイナリ コンフィギュレーションのみが保存されます (Table 24: アクティブな FICON およびスイッチ設定の保存, on page 306 を参照)

スタートアップ コンフィギュレーション ステータスの表示

```

switch# show startup-config
No ASCII config available since configuration was last saved internally

```

```
on account of 'active=saved' mode.
Please perform an explicit 'copy running startup` to get ASCII configuration
```

FICON 関連のログ情報の表示

FICON 機能のログ レベルの表示, on page 338 および FICON 関連ログ ファイルの内容の表示, on page 338 では、FICON 関連の設定のロギング情報を表示します。

FICON 機能のログ レベルの表示

```
switch# show logging level ficon
Facility           Default Severity      Current Session Severity
-----
ficon              2                      2
0(emergencies)    1(alerts)             2(critical)
3(errors)         4(warnings)           5(notifications)
6(information)    7(debugging)
```

FICON 関連ログ ファイルの内容の表示

```
switch# show logging logfile
...
2004 Feb 25 15:38:50 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 13:22:04.
131183%$ Interface fc1/8 is up in mode F
  2004 Feb 25 15:38:50 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 13:22:04.
131217%$ Interface fc1/9 is up in mode F
...
2004 Feb 25 15:39:09 vegas6 %PORT-5-IF_TRUNK_UP: %$VSAN 75: 2004 Wed Feb 25 13:
22:23.131121%$ Interface fc2/1, vsan 75 is up
  2004 Feb 25 15:39:09 vegas6 %PORT-5-IF_TRUNK_UP: %$VSAN 75: 2004 Wed Feb 25 13:
22:23.131121%$ Interface fc2/2, vsan 75 is up
  2004 Feb 25 15:39:09 vegas6 %PORT-5-IF_TRUNK_UP: %$VSAN 75: 2004 Wed Feb 25 13:
...
2004 Feb 25 23:22:36 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 21:05:42.
99916%$ Interface fc3/6 is up in mode F
  2004 Feb 25 23:22:37 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 21:05:43.
...
```

デフォルト設定

Table 25: FICON のデフォルト設定, on page 338 に、FICON 機能のデフォルト設定を示します。

Table 25: FICON のデフォルト設定

パラメータ	デフォルト
FICON 機能	ディセーブル
ポート番号	ポートアドレスと同じ

パラメータ	デフォルト
FC ID の最終バイト値	0 (ゼロ)
EBCDIC フォーマット オプション	US-Canada
スイッチのオフライン状態	ホストでスイッチをオフライン状態に移行可能
メインフレーム ユーザー	Cisco MDS スイッチで FICON パラメータを設定可能
各 VSAN のクロック	スイッチのハードウェア クロックと同じ
ホストのクロック制御	このスイッチのクロックを、ホストで設定可能
SNMP ユーザー	FICON パラメータの設定
ポートアドレス	ブロックされない
使用禁止ポート	Cisco MDS 9200 シリーズ スイッチのポート 90 ~ 253、およびポート 255 Cisco MDS 9500 シリーズ スイッチのポート 250 ~ 253、およびポート 255



CHAPTER 11

高度な機能および概念

この章では、Cisco MDS 9000 ファミリのスイッチが提供する高度な機能について説明します。内容は次のとおりです。

- 共通情報モデル (CIM) , on page 341
- ファイバチャネルタイムアウト値, on page 342
- 組織固有識別子, on page 346
- World Wide Names (WWN) , on page 347
- HBA の FC ID 割り当て, on page 350
- スイッチの相互運用性, on page 352
- デフォルト設定, on page 360

共通情報モデル (CIM)

共通情報モデル (CIM) は、既存の規格を拡張してネットワークやエンタープライズ環境の管理情報を記述するオブジェクト指向の情報モデルです。

CIM メッセージは、NExtensible Markup Language (XML) で符号化されるため、プラットフォームおよび実装に依存しません。CIM は仕様とスキーマで構成されます。仕様には、管理データの記述および他の管理モデルとの統合に用いられる、構文とルールが定義されています。スキーマは、システム、アプリケーション、ネットワーク、およびデバイスの実際のモデルの説明を提供します。

CIM の詳細については、次の URL にある Distributed Management Task Force (DMTF) の Web サイトから入手可能な仕様を参照してください。 <http://www.dmtf.org/>



Note CIM 機能および SMI-S は現在 Cisco Prime Data Center Network Manager (DCNM) でサポートされています。『Cisco Prime DCNM Installation Guide』および『SMI-S and Web Services Programming Guide, Cisco DCNM for SAN』を参照してください。

ファイバチャネル タイムアウト値

ファイバチャネルプロトコルに関連するスイッチのタイマー値を変更するには、次の Timeout Value (TOV) 値を設定します。

- Distributed Services TOV (D_S_TOV) : 有効範囲は 5,000 ~ 10,000 ミリ秒です。デフォルトは 5,000 ミリ秒です。
- Error Detect TOV (E_D_TOV) : 有効範囲は 1,000 ~ 4,000 ミリ秒です。デフォルトは 2,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。
- Resource Allocation TOV (R_A_TOV) : 有効範囲は 5,000 ~ 10,000 ミリ秒です。デフォルトは 10,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。



Note Fabric Stability TOV (F_S_TOV) 定数は設定できません。

このセクションは、次のトピックで構成されています。

すべての VSAN のタイマー設定

ファイバチャネルプロトコルに関連するスイッチのタイマー値を変更できます。



Caution D_S_TOV、E_D_TOV、および R_A_TOV 値をグローバルに変更するには、スイッチのすべての VSAN (仮想 SAN) を中断する必要があります。



Note タイマー値を変更するときに VSAN を指定しない場合は、変更された値がスイッチ内のすべての VSAN に適用されます。

すべての VSAN にファイバチャネル タイマーを設定する手順は、次のとおりです。

ステップ 1 switch# config terminal

```
switch(config)
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# fctimer R_A_TOV 6000

すべての VSAN の R_A_TOV 値を 6000 ミリ秒に設定します。このタイプの設定は、すべての VSAN が一時停止されていないかぎり、許可されません。

VSAN ごとのタイマー設定

VSAN を指定して `fctimer` を発行し、VSAN に異なる TOV 値を設定して FC や IP トンネルなどに特別にリンクさせることができます。VSAN ごとに異なる `E_D_TOV`、`R_A_TOV`、および `D_S_TOV` 値を設定できます。アクティブ VSAN のタイマー値を変更すると、VSAN は一時停止されてからアクティブになります。

**Caution**

以前のバージョンでは VSAN ごとの FC タイマーをサポートしておらず、中断のないダウングレードは実行できません。

**Note**

この設定はファブリックのすべてのスイッチに伝播する必要があります。ファブリックのすべてのスイッチが同じ値に設定されていることを確認してください。

タイマーを VSAN 用に設定した後にスイッチが Cisco MDS SAN-OS Release 1.2 または 1.1 にダウングレードされると、厳密に互換性がないことを警告するエラーメッセージが表示されます。『*Cisco MDS 9000 Family Troubleshooting Guide*』お参照してください。

VSAN ごとのファイバチャネルタイマーを設定するには、次の手順を実行します。

ステップ 1 `switch# config terminal`

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# fctimer D_S_TOV 6000 vsan 2`

```
Warning: The vsan will be temporarily suspended when updating the timer value This configuration would impact whole fabric. Do you want to continue? (y/n) y
```

```
Since this configuration is not propagated to other switches, please configure the same value in all the switches
```

VSAN 2 の `D_S_TOV` 値を 6000 ミリ秒に設定します。VSAN が一時的に停止します。必要に応じて、このコマンドを終了することもできます。

fctimer 配信の概要

ファブリック内のすべての Cisco MDS スイッチで、VSAN 単位の `fctimer` ファブリック配信をイネーブルにできます。`fctimer` の設定を実行して、配布をイネーブルにすると、ファブリック内のすべてのスイッチにその設定が配布されます。

スイッチでの配信をイネーブルにした後で最初のコンフィギュレーションコマンドを発行すると、ファブリック全体が自動的にロックされます。fctimer アプリケーションは、有効データベースと保留データベースモデルを使用し、使用中のコンフィギュレーションに基づいてコマンドを格納またはコミットします。

CFS アプリケーションの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

fctimer 配信の有効化

fctimer ファブリック配信を有効または無効にするには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

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

ファブリック内のすべてのスイッチに対する fctimer 設定の配布をイネーブルにします。ファブリックのロックを取得して、その後の設定変更をすべて保留データベースに格納します。

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

ファブリック内のすべてのスイッチに対する fctimer 設定の配布をディセーブル（デフォルト）にします。

fctimer 設定変更のコミット

fctimer の設定変更をコミットすると、有効データベースは保留データベースの設定変更によって上書きされ、ファブリック内のすべてのスイッチが同じ設定を受け取ります。セッション機能を実行せずに fctimer の設定変更をコミットすると、fctimer 設定は物理ファブリック内のすべてのスイッチに配布されます。

fctimer の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 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

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

ファブリック内のすべてのスイッチに対して fctimer の設定変更を配布し、ロックを解除します。保留データベースに対する変更を有効データベースに上書きします。

fctimer 設定変更の廃棄

設定変更を加えたあと、変更内容をコミットする代わりに廃棄すると、この変更内容を廃棄できます。いずれの場合でも、ロックは解除されます。

fctimer の設定変更を廃棄するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fctimer abort**

保留データベースの fctimer の設定変更を廃棄して、ファブリックのロックを解除します。

ファブリックのロックの上書き

ユーザーが fctimer を設定して、変更のコミットや廃棄を行ってロックを解除するのを忘れていた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザーによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。



Tip 変更は volatile ディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

管理者特権を使用して、ロックされた fctimer セッションを解除するには、**clear fctimer session** コマンドを使用します。

```
switch# clear fctimer session
```

データベース マージの注意事項

CFS マージサポートの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

2つのファブリックを結合する場合は、次の注意事項に従ってください。

- 次の結合条件を確認します。
 - マージプロトコルが実装済みでも fctimer 値は配信されとはかぎりません。ファブリックをマージするときは、fctimer 値を手動でマージする必要があります。VSAN 単位の fctimer 設定は、物理ファブリック内に配信されます。
 - fctimer 設定は、変更された fctimer 値を持つ VSAN が含まれるスイッチだけに適用される。

- グローバルな **fctimer** 値は配布されない。



Note 保留できる **fctimer** 設定操作の回数は 15 回以内です。この数に達した時点で、さらに処理を実行するには、保留中の構成をコミットするか、終了する必要があります。

設定された **fctimer** 値の表示

設定された **fctimer** 値を表示するには、**show fctimer** コマンドを使用します（次の例を参照）。

設定されたグローバル **TOV** の表示

```
switch# show fctimer

F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
-----
5000 ms   5000 ms   2000 ms   10000 ms
```



Note **show fctimer** コマンドの出力には、（設定されていない場合でも）**F_S_TOV** 定数が表示されます。

指定した **VSAN** の設定済み **TOV** の表示

```
switch# show fctimer vsan 10

vsan no.  F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
-----
10         5000 ms   5000 ms   3000 ms   10000 ms
```

組織固有識別子

組織固有識別子（OUI）は、組織をグローバルに識別する一意の 24 ビット数値です。OUI が割り当てられている組織は、その OUI を拡張して 48 ビットまたは 60 ビットの拡張固有識別子（EUI）を作成します。シスコは IEEE から取得した OUI を使用して EUI を作成しています。これらの識別子が各システムに割り当てられ、保存されています。システムには 1 つ以上の EUI が割り当てられていることがあります。EUI は、MAC アドレス、WWN、SNMP ID などさまざまな形式で使用されます。

Cisco MDS NX-OS ソフトウェアには、使用可能になっている特定のソフトウェア機能に基づく OUI データベースが含まれています。ファブリックに追加される新しいシスコデバイスの OUI を認識できない場合、一部の機能が影響を受けることがあります。この問題を回避するため、CLI を使用して OUI データベースに OUI を手動で追加できます。

注意事項と制約事項

- ISSU : アップグレード後に、デフォルト (組み込み) リストとスタティック (ユーザー定義) リストで OUI が重複することがあります。このような場合には、スタティック OUI とデフォルト リストの OUI を比較し、重複するスタティック OUI を削除することをお勧めします。
- ISSD : `wwn oui oui-id` コマンドをサポートしていないリリースにダウングレードする前に、設定されている OUI またはスタティック OUI をすべて削除します。

OUI の削除の詳細については、[OUI の追加および削除](#), on page 347 を参照してください。

OUI の追加および削除

OUI を OUI データベースに追加するには、グローバル コンフィギュレーション モードで `wwn oui oui-id` コマンドを入力します。OUI データベースから OUI を削除するには、グローバル コンフィギュレーション モードで `no wwn oui oui-id` コマンドを入力します。

`wwn oui` コマンドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

OUI の追加と削除の設定例

例 : OUI の追加と削除

```
switch# configure terminal
switch(config)# wwn oui 0x10001c
switch(config)# no wwn oui 0x10001c
switch(config)# end
```

例 : OUI の表示

```
switch# show wwn oui
OUI          Vendor          Default/Static
-----
0x0000fc     Cisco           Static
0x00000c     Cisco           Default
0x000196     Cisco           Default
0x000197     Cisco           Default
0x0001c7     Cisco           Default
0x0001c9     Cisco           Default
```

World Wide Names (WWN)

スイッチの World Wide Name (WWN) は、イーサネット MAC アドレスと同等です。MAC アドレスと同様に、デバイスごとに WWN を一意に対応付ける必要があります。主要スイッチを選択するとき、およびドメイン ID を割り当てるときは、WWN を使用します。WWN は、ス

スイッチのスーパーバイザ モジュールのプロセスレベル マネージャである WWN マネージャによって、各スイッチに割り当てられます。

Cisco MDS 9000 ファミリのスイッチは、3つの Network Address Authority (NAA) アドレスフォーマットをサポートしています (Table 26: 標準化された NAA WWN フォーマット, on page 348 を参照)。

Table 26: 標準化された NAA WWN フォーマット

NAA アドレス	NAA タイプ	WWN 形式	
		IEEE 48 ビット アドレス	タイプ1 = 0001b
IEEE 拡張	タイプ2 = 0010b	ローカルに割り当て	48 ビット MAC アドレス
IEEE 登録	タイプ5 = 0101b	IEEE 企業 ID : 24 ビット	VSID : 36 ビット



Caution WWNの変更は、管理者または、スイッチの操作に精通した担当者が実行してください。

このセクションは、次のトピックで構成されています。

WWN 情報の表示

WWN 設定のステータスを表示するには、**show wwn** コマンドを使用します。次の例を参照してください。

すべての WWN のステータスの表示

```
switch# show wwn status
      Type 1 WWNs: Configured:      64 Available:      48 (75%) Resvd.: 16
      Types 2 & 5 WWNs: Configured: 524288 Available: 450560 (85%) Resvd.: 73728
      NKAU & NKCR WWN Blks: Configured: 1760 Available: 1760 (100%)
      Alarm Status:      Type1:      NONE Types 2&5:      NONE
```

指定したブロック ID 情報の表示

```
switch# show wwn status block-id 51

WWNs in this block: 21:00:ac:16:5e:52:00:03 to 21:ff:ac:16:5e:52:00:03
Num. of WWNs:: Configured: 256 Allocated:      0 Available: 256
Block Allocation Status: FREE
```

特定スイッチの **WWN** の表示

```
switch# show wwn switch
Switch WWN is 20:00:ac:16:5e:52:00:00
```

リンク初期化 **WWN** の使用方法

Exchange Link Protocol (ELP) および Exchange Fabric Protocol (EFP) は、リンク初期化の際に **WWN** を使用します。使用方法の詳細は、Cisco NX-OS ソフトウェア リリースごとに異なります。

ELP と EFP のどちらも、リンク初期化中にデフォルトで **VSAN WWN** を使用します。ただし、ELP の使用法はピアスイッチの使用法に応じて変わります。

- ピアスイッチの ELP がスイッチの **WWN** を使用する場合、ローカルスイッチもスイッチの **WWN** を使用します。
- ピアスイッチの ELP が **VSAN** の **WWN** を使用する場合、ローカルスイッチも **VSAN** の **WWN** を使用します。



Note Cisco SAN-OS Release 2.0(2b) 時点で、ELP は FC-SW-3 に準拠するように機能拡張されました。

セカンダリ **MAC** アドレスの設定

セカンダリ **MAC** アドレスを割り当てるには、次の手順を実行します。

ステップ 1 switch# **config terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **wwn secondary-mac 00:99:55:77:55:55 range 64**

```
This command CANNOT be undone.
```

```
Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55
```

```
Please enter the mac address RANGE again: 64
```

```
From now on WWN allocation would be based on new MACs.
```

```
Are you sure? (yes/no) no
```

You entered: no. Secondary MAC NOT programmed

セカンダリ MAC アドレスを設定します。このコマンドは元に戻せません。

HBA の FC ID 割り当て

ファイバチャネル標準では、任意のスイッチの Fx ポートに接続された N ポートに、一意の FC ID を割り当てる必要があります。FC ID の使用数を節減するために、Cisco MDS 9000 ファミリスイッチには特殊な割り当て方式が使用されています。

一部の Host Bus Adapter (HBA) は、ドメインとエリアが同じ FC ID を持つターゲットを検出しません。Cisco SAN-OS Release 2.0(1b) よりも前の Cisco SAN-OS ソフトウェアでは、この動作をサポートしないテスト済みの企業 ID のリストを保持していました。これらの HBA には、単一の FCID が割り当てられ、残りにはエリア全体が割り当てられます。

Release 1.3 以前で使用可能な FC ID 割り当て方式では、これらの HBA に領域全体を割り当てます。このように割り当てることによって、これらの HBA が該当領域から分離され、ファブリック ログイン時に pWWN とともにリストされるようになります。割り当てられた FC ID は常にキャッシュされ、Cisco SAN-OS Release 2.0(1b) でも使用できます ([HBA の FC ID 割り当て, on page 350](#) を参照)。

多数のポートを備えたスイッチのスケラビリティを高めるために、Cisco NX-OS ソフトウェアはこの動作をサポートする HBA のリストを保持します。各 HBA はファブリック ログインの間、pWWN で使用される企業 ID (組織固有識別子 (OUI) としても知られる) によって識別されます。リストされた企業 ID を持つ N ポートには領域全体が割り当てられ、他のポートには単一の FC ID が割り当てられます。割り当てられる FC ID の種類 (領域全体または単一) に関係なく、FC ID エントリは保持されます。

このセクションは、次のトピックで構成されています。

デフォルトの企業 ID リスト

Cisco SAN-OS Release 2.0(1b) 以降または NX-OS 4.1(1) に付属の Cisco MDS 9000 ファミリ内のすべてのスイッチには、領域の割り当てが必要な企業 ID のデフォルトリストが格納されています。この企業 ID を使用すると、設定する永続的 FC ID エントリの数が少なくなります。これらのエントリは、CLI を使用して設定または変更できます。



Caution

永続的エントリは、企業 ID の設定よりも優先されます。HBA がターゲットを検出しない場合は、HBA とターゲットが同じスイッチに接続され、FC ID のエリアが同じであることを確認してから、次の手順を実行します。1. HBA に接続されているポートをシャットダウンします。2. 永続的 FC ID エントリをクリアします。3. ポート WWN から企業 ID を取得します。4. エリア割り当てを必要とするリストに企業 ID を追加します。5. ポートをアップにします。

企業 ID のリストには、次の特性があります。

- 永続的 FC ID の設定は常に企業 ID リストよりも優先されます。エリアを受け取るように企業 ID が設定されている場合でも、永続的 FC ID の設定によって単一の FC ID が割り当てられます。
- 後続のリリースに追加される新規の企業 ID は、既存の企業 ID に自動的に追加されます。
- 企業 ID のリストは、実行コンフィギュレーションおよび保存されたコンフィギュレーションの一部として保存されます。
- 企業 ID のリストが使用されるのは、`fcinterop` の FC ID 割り当て方式が `auto` モードの場合だけです。変更されないかぎり、`interop` の FC ID 割り当ては、デフォルトで `auto` に設定されています。



Tip `fcinterop` の FC ID 割り当て方式を `auto` に設定し、企業 ID リストと永続的 FC ID 設定を使用して、FC ID のデバイス割り当てを行うことをお勧めします。

FC ID の割り当てを変更するには、`fcinterop FCID allocation auto` コマンドを使用し、現在割り当てられているモードを表示するには、`show running-config` コマンドを使用します。

- `write erase` を実行すると、リストは該当するリリースに付属している企業 ID のデフォルト リストを継承します。

企業 ID を割り当てる手順は、次のとおりです。

ステップ 1 `switch# config terminal`

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 `switch(config)# fcid-allocation area company-id 0x003223`

デフォルト リストに新しい企業 ID を追加します。

ステップ 3 `switch(config)# no fcid-allocation area company-id 0x00E069`

デフォルト リストから企業 ID を削除します。

ステップ 4 `switch(config)# fcid-allocation area company-id 0x003223`

デフォルト リストに新しい企業 ID を追加します。

企業 ID の設定の確認

設定された企業 ID を表示するには、`show fcid-allocation area` コマンドを発行します（[デフォルトの企業 ID と設定された企業 ID のリストの表示, on page 352](#) を参照）。最初にデフォルト エントリが表示され、次にユーザーによって追加されたエントリが表示されます。エントリがデフォルト リストの一部で、あとで削除された場合でも、エントリは表示されます。

デフォルトの企業 ID と設定された企業 ID のリストの表示

```
switch# show fcid-allocation area
FCID area allocation company id info:
 00:50:2E <----- Default entry
 00:50:8B
 00:60:B0
 00:A0:B8
 00:E0:69
 00:30:AE + <----- User-added entry
 00:32:23 +
 00:E0:8B * <----- Explicitly deleted entry (from the original default list)
Total company ids: 7
+ - Additional user configured company ids.
* - Explicitly deleted company ids from default list.
```

削除済みエントリの印が付いていない企業 ID のリストを組み合わせると、特定のリリースに付属するデフォルト エントリを暗黙的に導き出すことができます。

また、**show fcid-allocation company-id-from-wwn** コマンドを発行すると、特定の WWN の企業 ID を表示または取得することもできます（[指定した WWN の企業 ID の表示](#)、[on page 352](#) を参照）。一部の WWN 形式では、企業 ID がサポートされていません。この場合、FC ID の永続的エントリを設定する必要があります。

指定した WWN の企業 ID の表示

```
switch# show fcid-allocation company-id-from-wwn 20:00:00:05:30:00:21:60
Extracted Company ID: 0x000530
```

スイッチの相互運用性

相互運用性を使用すると、複数ベンダーによる製品の間で相互接続できます。ファイバチャネル標準規格では、ベンダーに対して共通の外部ファイバチャネルインターフェイスを使用することを推奨しています。

すべてのベンダーが同じ方法で標準に従っていれば、異なる製品の相互接続が問題になることはありません。ただし、同じ方法で標準に従っていないベンダーもあるため、**interop** モードが開発されました。ここでは、これらのモードの基本的な概念について簡単に説明します。

各ベンダーには標準モード、および同等の相互運用性モードがあります。**interop** モードでは拡張機能または独自の機能が無効になり、より使いやすい標準準拠の実装が可能になります。



Note Cisco MDS 9000 ファミリー スイッチでの相互運用性の設定方法に関する詳細は、『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』を参照してください。

このセクションは、次のトピックで構成されています。

Interop モードの概要

Cisco NX-OS ソフトウェアは、次の 4 つの interop モードをサポートします。

- モード 1：ファブリック内のその他のすべてのベンダーを interop モードにする必要がある、標準ベースの interop モード
- モード 2：Brocade ネイティブ モード (Core PID 0)
- モード 3：Brocade ネイティブ モード (Core PID 1)
- モード 4：McData ネイティブ モード

interop モード 2、3、および 4 の設定方法については、『Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide』を参照してください。

[Table 27: 相互運用性がイネーブルの場合のスイッチ動作の変更点, on page 353](#) に、interop モードをイネーブルにした場合のスイッチ動作の変更点を示します。これらは、interop モードになっている Cisco MDS 9000 ファミリのスイッチに固有の変更点です。

Table 27: 相互運用性がイネーブルの場合のスイッチ動作の変更点

スイッチ機能	相互運用モードがイネーブルの場合の変更点
ドメイン ID	一部のベンダーは、ファブリック内の 239 のドメインを完全には使用できません。 ドメイン ID は 97 ~ 127 の範囲に制限されています。これは、McData の通常の制限をこの範囲に収めるためです。ドメイン ID の設定方法には、静的に設定する (Cisco MDS スイッチは 1 つのドメイン ID だけを受け入れ、そのドメイン ID を取得できない場合はファブリックから隔離する) 方法と、優先設定を使用する (スイッチが要求したドメイン ID を取得できない場合、割り当てられた任意のドメイン ID を受け入れる) 方法があります。
タイマー	ISL (スイッチ間リンク) を確立するときにファイバチャネル タイマー値が E ポートで交換されるので、すべてのスイッチでこれらのタイマーをすべて同じにする必要があります。タイマーには、F_S_TOV、D_S_TOV、E_D_TOV、および R_A_TOV があります。
F_S_TOV	Fabric Stability TOV タイマーが正確に一致するかどうかを確認してください。
D_S_TOV	Distributed Services TOV タイマーが正確に一致するかどうかを確認してください。
E_D_TOV	Error Detect TOV タイマーが正確に一致するかどうかを確認してください。

スイッチ機能	相互運用モードがイネーブルの場合の変更点
R_A_TOV	Resource Allocation TOV タイマーが正確に一致するかどうかを確認してください。
トランキン	2つの異なるベンダー製のスイッチ間では、トランキンはサポートされません。この機能はポート単位、またはスイッチ単位でディセーブルに設定できます。
デフォルトゾーン	ゾーンのデフォルトの許可動作（すべてのノードから他のすべてのノードを認識可能）または拒否動作（明示的にゾーンに配置されていないすべてのノードが隔離される）は、変更できます。
ゾーン分割属性	<p>ゾーンを pWWN に制限したり、その他の独自のゾーン分割方式（物理ポート番号）を除去することができます。</p> <p>Note Brocade では、cfgsave コマンドを使用して、ファブリック全体のゾーン分割設定を保存します。このコマンドは、同じファブリックに属す Cisco MDS 9000 ファミリースイッチには影響しません。Cisco MDS 9000 ファミリーの各スイッチに、設定を明示的に保存する必要があります。</p>
ゾーンの伝播	<p>一部のベンダーは、他のスイッチに完全なゾーン設定を受け渡さないで、アクティブゾーンセットだけを受け渡します。</p> <p>ファブリック内の他のスイッチにアクティブゾーンセットまたはゾーン設定が正しく伝播されたかどうかを確認してください。</p>
VSAN	<p>interop モードは、指定された VSAN にだけ有効です。</p> <p>Note interop モードは、FICON 対応の VSAN でイネーブルにできません。</p>
TE ポートとポートチャンネル	TE ポートとポートチャンネルを使用して、Cisco MDS を Cisco 以外の MDS スイッチに接続することはできません。Cisco MDS 以外のスイッチに接続できるのは、E ポートだけです。TE ポートとポートチャンネルを使用すると、interop モードの場合でも、Cisco MDS をその他の Cisco MDS スイッチに接続できます。
FSPF	interop モードにしても、ファブリック内のフレームのルーティングは変更されません。スイッチは引き続き src-id、dst-id、および ox-id を使用して、複数の ISL リンク間でロード バランスします。
ドメインの中断再設定	これは、スイッチ全体に影響するイベントです。Brocade および McData では、ドメイン ID を変更するときにスイッチ全体をオフラインモードにしたり、再起動したりする必要があります。

スイッチ機能	相互運用モードがイネーブルの場合の変更点
ドメインの非中断再設定	これは、関連する VSAN に限定されるイベントです。スイッチ全体ではなく、関連する VSAN の Domain Manager プロセスだけが再起動される機能は、Cisco MDS 9000 ファミリのスイッチだけに組み込まれています。
ネーム サーバー	すべてのベンダーのネーム サーバー データベースに正しい値が格納されているかを確認してください。
IVRivr	IVR 対応の VSAN は、 no interop (デフォルト) モード、または interop モードのいずれかで設定できます。

interop モード 1 の設定

Cisco MDS 9000 ファミリー スイッチの interop モード 1 のイネーブル化は、中断を伴うかまたは中断を伴わずに行うことができます。



Note Brocade スイッチから Cisco MDS 9000 ファミリー スイッチまたは McData スイッチに接続する前に、Brocade の `msplmgmtdeactivate` コマンドを明示的に実行する必要があります。このコマンドでは、Brocade 独自のフレームを使用して、Cisco MDS 9000 スイッチまたは McData スイッチが認識しないプラットフォーム情報を交換します。これらのフレームを拒否すると、一般的な E ポートが隔離されます。

Cisco MDS 9000 ファミリーの任意のスイッチに interop モード 1 を設定するには、次の手順を実行します。

ステップ 1 他ベンダー製スイッチに接続する E ポートの VSAN を相互運用モードにします。

```
switch# config terminal
switch(config)# vsan database
switch(config-vsan-db)# vsan 1 interop 1
switch(config-vsan-db)# exit
switch(config)#
```

Note FICON 対応 VSAN では、INTEROP モードをイネーブルにできません。

ステップ 2 97 (0x61) ~ 127 (0x7F) の範囲でドメイン ID を割り当てます。

Note これは、McData スイッチに適用される制限です。

```
switch(config)# fcdomain domain 100 preferred vsan 1
```

Cisco MDS 9000 スイッチの場合、デフォルトでは、主要スイッチから ID が要求されます。Preferred オプションを使用した場合、Cisco MDS 9000 スイッチは固有の ID を要求しますが、主要スイッチから別の ID が割り当てられた場合もファブリックに加入します。Static オプションを使用した場合、要求された ID を

主要スイッチが承認して、これを割り当てない限り、Cisco MDS 9000 スイッチはファブリックに参加しません。

Note ドメイン ID を変更すると、N ポートに割り当てられた FC ID も変更されます。

ステップ 3 FC タイマーを変更します（システム デフォルトから変更された場合）。

Note Cisco MDS 9000、Brocade、McData FC Error Detect (ED_TOV)、および Resource Allocation (RA_TOV) の各タイマーは、同じ値にデフォルト設定されています。これらの値は、必要に応じて変更できます。RA_TOV のデフォルト値は 10 秒、ED_TOV のデフォルト値は 2 秒です。FC-SW2 標準に基づく場合、これらの値は、ファブリック内の各スイッチで一致している必要があります。

```
switch(config)# fctimer e_d_tov ?
<1000-4000> E_D_TOV in milliseconds (1000-4000)
switch(config)# fctimer r_a_tov ?
<5000-100000> R_A_TOV in milliseconds (5000-100000)
```

ステップ 4 ドメインを変更するとき、変更された VSAN の Cisco MDS ドメイン マネージャ機能の再起動が必要な場合と、不要な場合があります。

- **disruptive** オプションを使用して、ファブリックを強制的に再設定する場合は次のようになります。

```
switch(config)# fcdomain restart disruptive vsan 1
```

または

- ファブリックを強制的に再設定しない場合は次のようになります。

```
switch(config)# fcdomain restart vsan 1
```

interop モード 1 の設定

コマンド Cisco MDS 9000 ファミリのスイッチで相互運用性コマンドを発行した結果のステータスを確認するには、次の手順を実行します。

SUMMARY STEPS

1. **show version** コマンドを使用してバージョンを検証します。
2. **show interface brief** コマンドを使用して、インターフェイスの状態が設定に必要な状態になっているかどうかを確認します。
3. 必要な設定を実行しているかどうかを確認するには、**show run** コマンドを使用します。
4. 相互運用性モードがアクティブであるかどうかを確認するには、**show vsan** コマンドを使用します。
5. ドメイン ID を確認するには **show fcdomain vsan** コマンドを使用します。
6. ローカル プリンシパル スイッチ ステータスを確認するには、**show fcdomain domain-list vsan** コマンドを使用します。

7. スイッチのネクスト ホップと宛先を確認するには、**show fspf internal route vsan** コマンドを使用します。
8. ネーム サーバー情報を確認するには、**show fens data vsan** コマンドを使用します。

DETAILED STEPS

ステップ1 show version コマンドを使用してバージョンを検証します。

```
switch# show version

Cisco Storage Area Networking Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2003, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
Cisco Systems, Inc. and/or other third parties and are used and
distributed under license. Some parts of this software are covered
under the GNU Public License. A copy of the license is available
at http://www.gnu.org/licenses/gpl.html.
Software
  BIOS:          version 1.0.8
  loader:        version 1.1(2)
  kickstart:     version 2.0(1) [build 2.0(0.6)] [gdb]
  system:        version 2.0(1) [build 2.0(0.6)] [gdb]
  BIOS compile time:      08/07/03
  kickstart image file is: bootflash:///m9500-sf1ek9-kickstart-mzg.2.0.0.6.bin
  kickstart compile time: 10/25/2010 12:00:00
  system image file is:   bootflash:///m9500-sf1ek9-mzg.2.0.0.6.bin
  system compile time:    10/25/2020 12:00:00
Hardware
  RAM 1024584 kB
  bootflash: 1000944 blocks (block size 512b)
  slot0:      0 blocks (block size 512b)
  172.22.92.181 uptime is 0 days 2 hours 18 minute(s) 1 second(s)
  Last reset at 970069 usecs after Tue Sep 16 22:31:25 1980
    Reason: Reset Requested by CLI command reload
    System version: 2.0(0.6)
  Service:
```

ステップ2 show interface brief コマンドを使用して、インターフェイスの状態が設定に必要な状態になっているかどうかを確認します。

```
switch# show int brief

Interface Vsan   Admin   Admin   Status      Oper   Oper   Port-channel
          Mode    Mode
          Mode
-----
fc2/1     1       auto   on        up        E      2      --
fc2/2     1       auto   on        up        E      2      --
fc2/3     1       auto   on        fcotAbsent --    --    --
fc2/4     1       auto   on        down      --    --    --
fc2/5     1       auto   on        down      --    --    --
fc2/6     1       auto   on        down      --    --    --
fc2/7     1       auto   on        up        E      1      --
fc2/8     1       auto   on        fcotAbsent --    --    --
fc2/9     1       auto   on        down      --    --    --
fc2/10    1       auto   on        down      --    --    --
```

ステップ3 必要な設定を実行しているかどうかを確認するには、**show run** コマンドを使用します。

```

switch# show run
Building Configuration...
 interface fc2/1
no shutdown
 interface fc2/2
no shutdown
 interface fc2/3
 interface fc2/4
 interface fc2/5
 interface fc2/6
 interface fc2/7
no shutdown
 interface fc2/8
 interface fc2/9
 interface fc2/10

<snip>

interface fc2/32
 interface mgmt0
ip address 6.1.1.96 255.255.255.0
switchport encap default
no shutdown
vsan database
vsan 1 interop
boot system bootflash:/m9500-system-253e.bin sup-1
boot kickstart bootflash:/m9500-kickstart-253e.bin sup-1
boot system bootflash:/m9500-system-253e.bin sup-2
boot kickstart bootflash:/m9500-kickstart-253e.bin sup-2
callhome
fcdomain domain 100 preferred vsan 1
ip route 6.1.1.0 255.255.255.0 6.1.1.1
ip routing
line console
  databits 5
  speed 110
logging linecard
ssh key rsa 512 force
ssh server enable
switchname MDS9509
username admin password 5 $1$Li8/fBYX$SNc72.xt4nTXpSnR9OUFB/ role network-admin

```

ステップ 4 相互運用性モードがアクティブであるかどうかを確認するには、**show vsan** コマンドを使用します。

```

switch# show vsan 1
vsan 1 information
  name:VSAN0001 stalactites
  interoperability mode:yes
<----->
verify mode
  loadbalancing:src-id/dst-id/oxid
  operational state:up

```

ステップ 5 ドメイン ID を確認するには **show fcdomain vsan** コマンドを使用します。

```

switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.
Local switch run time information:
  State: Stable
  Local switch WWN:      20:01:00:05:30:00:51:1f
  Running fabric name: 10:00:00:60:69:22:32:91

```

```

Running priority: 128
Current domain ID: 0x64(100)
<-----
verify domain id
Local switch configuration information:
  State: Enabled
  Auto-reconfiguration: Disabled
  Contiguous-allocation: Disabled
  Configured fabric name: 41:6e:64:69:61:6d:6f:21
  Configured priority: 128
  Configured domain ID: 0x64(100) (preferred)
Principal switch run time information:
  Running priority: 2
Interface          Role          RCF-reject
-----
fc2/1              Downstream   Disabled
fc2/2              Downstream   Disabled
fc2/7              Upstream     Disabled
-----

```

ステップ6 ローカルプリンシパルスイッチステータスを確認するには、**show fcdomain domain-list vsan** コマンドを使用します。

```

switch# show fcdomain domain-list vsan 1
Number of domains: 5
Domain ID          WWN
-----
0x61(97)           10:00:00:60:69:50:0c:fe
0x62(98)           20:01:00:05:30:00:47:9f
0x63(99)           10:00:00:60:69:c0:0c:1d
0x64(100)          20:01:00:05:30:00:51:1f [Local]
0x65(101)          10:00:00:60:69:22:32:91 [Principal]
-----

```

ステップ7 スイッチのネクストホップと宛先を確認するには、**show fspf internal route vsan** コマンドを使用します。

```

switch# show fspf internal route vsan 1
FSPF Unicast Routes
-----
VSAN Number  Dest Domain  Route Cost  Next hops
-----
1            0x61(97)    500         fc2/2
1            0x62(98)    1000        fc2/1
              fc2/2
1            0x63(99)    500         fc2/1
1            0x65(101)   1000        fc2/7

```

ステップ8 ネームサーバー情報を確認するには、**show fcns data vsan** コマンドを使用します。

```

switch# show fcns data vsan 1
VSAN 1:
-----
FCID          TYPE  PWWN                                (VENDOR) FC4-TYPE:FEATURE
-----
0x610400      N     10:00:00:00:c9:24:3d:90 (Emulex)   scsi-fcp
0x6105dc      NL    21:00:00:20:37:28:31:6d (Seagate)  scsi-fcp
0x6105e0      NL    21:00:00:20:37:28:24:7b (Seagate)  scsi-fcp
0x6105e1      NL    21:00:00:20:37:28:22:ea (Seagate)  scsi-fcp
0x6105e2      NL    21:00:00:20:37:28:2e:65 (Seagate)  scsi-fcp

```

```

0x6105e4    NL    21:00:00:20:37:28:26:0d (Seagate)    scsi-fcp
0x630400    N     10:00:00:00:c9:24:3f:75 (Emulex)     scsi-fcp
0x630500    N     50:06:01:60:88:02:90:cb          scsi-fcp
0x6514e2    NL    21:00:00:20:37:a7:ca:b7 (Seagate)     scsi-fcp
0x6514e4    NL    21:00:00:20:37:a7:c7:e0 (Seagate)     scsi-fcp
0x6514e8    NL    21:00:00:20:37:a7:c7:df (Seagate)     scsi-fcp
0x651500    N     10:00:00:e0:69:f0:43:9f (JNI)          scsi-fcp
Total number of entries = 12

```

デフォルト設定

Table 28: 拡張機能のデフォルト設定値, on page 360 に、この章で説明した機能のデフォルト設定値を示します。

Table 28: 拡張機能のデフォルト設定値

パラメータ	デフォルト
CIM サーバー	ディセーブル
CIM サーバー セキュリティプロトコル	HTTP
D_S_TOV	5,000 ミリ秒
E_D_TOV	2,000 ミリ秒
R_A_TOV	10,000 ミリ秒
fctrace を呼び出すタイムアウト時間	5 秒
fcping 機能によって送信されるフレーム数	5 フレーム
リモート キャプチャ接続プロトコル	TCP
リモート キャプチャ接続モード	パッシブ
ローカル キャプチャ フレームの制限	10 フレーム
FC ID の割り当てモード	auto モード
ループ モニタリング	ディセーブル
D_S_TOV	5,000 ミリ秒
E_D_TOV	2,000 ミリ秒
R_A_TOV	10,000 ミリ秒
interop モード	ディセーブル



CHAPTER 12

Fibre Channel Common Transport 管理セキュリティの設定

この章では、Cisco MDS 9000 シリーズ スイッチの Fibre Channel Common Transport (FC-CT) 管理セキュリティ機能について説明します。

- [Fibre Channel Common Transport の概要](#), on page 361
- [設定のガイドライン](#), on page 362
- [Fibre Channel Common Transport クエリーの設定](#), on page 362
- [Fibre Channel Common Transport 管理セキュリティの確認](#), on page 363
- [デフォルト設定](#), on page 363

Fibre Channel Common Transport の概要

FC-CT 管理セキュリティ機能により、ストレージ管理者またはネットワーク管理者だけが、スイッチに対してクエリーを送信し、情報にアクセスできるようにネットワークを設定できます。このような情報には、ファブリック内のログインデバイス、ファブリック内のスイッチなどのデバイス、デバイスの接続方法、各スイッチのポートの数、各ポートの接続先、設定済みゾーンの情報、ゾーンまたはゾーンセットの追加と削除の権限、ファブリックに接続するすべてのホストのホストバスアダプタ (HBA)の詳細などがあります。



Note Cisco MDS NX-OS Release 6.2(9) では、FC 管理機能はデフォルトで無効です。FC 管理機能を有効にするには、`fc-management enable` コマンドを使用します。

FC-CT 管理クエリーを送信し、管理サーバーへの要求を変更できる pWWN を設定できます。いずれかのモジュール (ゾーンサーバー、ゾーン分割されていないファイバチャネル ネームサーバー (FCNS)、またはファブリック コンフィギュレーションサーバー (FCS) など) が FC-CT 管理クエリーを受信すると、FC 管理データベースに対する読み取り操作が実行されます。FC 管理データベースでデバイスが検出されると、付与されている権限に基づいて応答が送信されます。デバイスが FC 管理データベースにない場合は、各モジュールが拒否を送信します。FC 管理が無効な場合、各モジュールが各管理クエリーを処理します。

設定のガイドライン

FC 管理セキュリティ機能には、次の設定に関する注意事項があります。

- Cisco MDS スイッチで FC 管理セキュリティ機能が有効な場合、管理クエリーを送信するデバイスのポート ワールドワイド ネーム (pWWN) が FC 管理データベースに追加されていないと、サーバーへのすべての管理クエリーが拒否されます。
- FC 管理を有効にすると、N_Port Virtualization (NPV) スイッチから N_Port Identifier Virtualization (NPIV) スイッチへの FC-CT 管理サーバー クエリーが拒否されます。FC 管理セキュリティ機能を有効にした後で、NPV スイッチのスイッチ ワールドワイド ネーム (sWWN) を NPIV スイッチの FC 管理データベースに追加することが推奨されます。

Fibre Channel Common Transport クエリーの設定

FC-CT 管理セキュリティを設定するには、次の手順を実行します。

ステップ 1 switch# **config terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fc-management enable**

FC-CT 管理セキュリティを有効にします。

ステップ 3 switch(config)# **fc-management database vsan 1**

FC-CT 管理セキュリティ データベースを設定します。

ステップ 4 switch(config-fc-mgmt)# **pwwn 1:1:1:1:1:1:1:1 feature all operation both**

pWWN を FC 管理データベースに追加します。また、pwwn コマンドを設定するときには次に示すオプションのキーワードも使用できます。

- **fc** : ファブリック コンフィギュレーション サーバーに対する FC-CT クエリーを有効または無効にします。
- **fdmi** : FDMI に対する FC-CT クエリーを有効または無効にします。
- **unzoned-ns** : ゾーン分割されていないネーム サーバーに対する FC-CT クエリーを有効または無効にします。
- **zone** : ゾーン サーバーに対する FC-CT クエリーを有効または無効にします。

ステップ 5 switch# **show fc-managment database**

設定された FC-CT 管理情報を表示します。

Fibre Channel Common Transport 管理セキュリティの確認

`show fc-management database` コマンドは、設定されている FC-CT 管理セキュリティ機能の情報を表示します (例 [Fibre Channel Common Transport クエリーの表示, on page 363](#) を参照)。

Fibre Channel Common Transport クエリーの表示

```
switch# show fc-management database
-----
VSAN PWWN FC-CT Permissions per FC services
-----
1 01:01:01:01:01:01:01:01 Zone (RW), Unzoned-NS (RW), FCS (RW), FDMI (RW)
1 02:02:02:02:02:02:02:02 Zone (R), Unzoned-NS (R), FCS (R), FDMI (R)
1 03:03:03:03:03:03:03:03 Zone (W), Unzoned-NS (W), FCS (W), FDMI (W)
-----
Total 3 entries
switch#
```

FC 管理セキュリティ機能が有効であるかどうかを確認するには、`show fc-management status` コマンドを使用します。

```
switch# show fc-management status
Mgmt Security Disabled
switch#
```

デフォルト設定

[Table 29: デフォルトの FC 管理設定, on page 363](#) に、Cisco MDS 9000 ファミリー スイッチの FC 管理セキュリティ機能のデフォルト設定を示します。

Table 29: デフォルトの FC 管理設定

パラメータ	デフォルト
FC-management	ディセーブル

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。